# Characterizations of highly non-associative quasigroups and associative triples 

Viacheslav A. Artamonov, Sucheta Chakrabarti, Saibal Kumar Pal


#### Abstract

Number of associative triples of quasigroup plays an important role in development of quasigroup based cryptographic schemes. In this paper we present algebraic properties of highly non-associative quasigroups and derive the criteria for polynomial completeness based on their multiplicative groups. We develop an algorithm to check the polynomial completeness of the quasigroup $Q$ from its Latin square representation, which is based on the criteria derived by using element of $\operatorname{Mult}(Q)$ with specific cycle structure. We also develop and implement an algorithm for deriving associative triples of finite quasigroups based on commutators of their Latin squares. Experimental results on quasigroups of different order and all quasigroups of order 4 of different classes are reported.


## 1. Introduction

Crypto community has focused on usage of non-commutative and non-associative algebraic structures in cryptography more intensively from the beginning of this century. Quasigroups are good choice of this type of algebraic structures for cryptographic purpose [2, 10, 11, 16]. The security of quasigroup based cryptographic primitives depend on its algebraic properties. Highly non-associative is one of the significant algebraic properties for cryptographic suitable choice of quasigroup [6].

Highly non-associative quasigroups were considered in [13, 18]. It was shown in [4] that almost all finite quasigroups $Q$ have the property that the multiplication group $\operatorname{Mult}(Q)$ contains symmetric or alternative group. In other words, the ratio of number of quasigroups having this property and total number of quasigroups of finite order $n$ tends to 1 as $n \rightarrow \infty$. From a practical point of view quasigroups of order $n, 4 \leqslant n \leqslant 256$ are frequently used in cryptography.

In the present paper we consider the problem of characterizing the highly nonassociative quasigroup $Q$ of finite order from its multiplicative group $\operatorname{Mult}(Q)$. Also one of our main aim is to develop an algorithm for testing polynomial completeness based on these algebraic properties. It is the main algebraic parameter

[^0]for cryptographically suitable choice of quasigroups. Another significant parameter for suitable choice of quasigroups is the number of associative triples. The number of associative triples of different classes of finite quasigroups was studied by different researchers $[6,7,8,9]$. In this paper we also deal with the problem of development of algorithm for derivation of associative triples of a quasigroup of finite order by algebraic approach from its Latin square. The smallest number of associative triples plays an important role to resist some known cryptographic attacks.

In this paper first we discuss the preliminaries of quasigroups, their Latin squares and polynomial completeness in $\S 2$. Some properties of affine quasigroups are discussed in $\S 3$. Section 4 deals with the characterization of highly nonassociative quasigroups, polynomial completeness and simplicity by using multiplicative group $\operatorname{Mult}(Q)$ of a quasigroup $Q$. Also in this section we present the algorithm for testing the polynomial completeness of a quasigroup from its Latin square by using the cycle structure of permutations of $Q$ which are belong to Mult $(Q)$. Section 5 deals with the development of algorithm and experiments of computation of associative triplets and its total numbers from a given Latin square. Also we present experimental results on associative triples over all quasigroups of order 4.

## 2. Preliminaries

A quasigroup is a set $Q$ with a binary operation of multiplication such that for all $a, b \in Q$ the equations $a x=b, \quad y a=b$ have unique solutions $x=a \backslash b, \quad y=b / a$. Then the class of quasigroups form a variety of algebras with three operations $x y, x \backslash y, \quad x / y$ which is defined by identities

$$
\begin{equation*}
(x y) / y=x=(x / y) y \quad x \backslash(x y)=y=x(x \backslash y) \tag{1}
\end{equation*}
$$

Each quasigroup $Q$ can be given by a Latin square

|  | $x_{1}$ | $\ldots$ | $x_{n}$ |
| :---: | :---: | :---: | :---: |
| $x_{1}$ | $a_{11}$ | $\ldots$ | $a_{1 n}$ |
| $\vdots$ | $\ldots$ | $\ldots$ | $\ldots$ |
| $x_{n}$ | $a_{n 1}$ | $\ldots$ | $a_{11}$ |

of size $n$. The elements of $Q$ are $\left\{x_{1}, \ldots, x_{n}\right\}$, each entry $a_{i j}$ stands for the product $x_{i} x_{j}$ in the quasigroup $Q$.

Let $x \cdot y, x * y$ be two quasigroup multiplications on a set $Q$. We say that multiplication $x * y$ is an isotope of multiplication $x \cdot y$ if there exists permutations $\pi, \pi_{1}, \pi_{2}$ on $Q$ such that

$$
\begin{equation*}
x * y=\pi\left(\pi_{1}^{-1}(x) \cdot \pi_{2}^{-1}(y)\right) \tag{3}
\end{equation*}
$$

for all $x, y \in Q$. Here $\left(\pi, \pi_{1}, \pi_{2}\right)$ is called an isotopy and the two quasigroups $(Q$, and $(Q, *)$ are said to be isotopic. If $\pi$ is an identity permutation then it is called principal isotopy.

In terms of the Latin square (2) it means that we replace it by the square

$$
\begin{array}{|c|ccc|}
\hline & x_{1} & \ldots & x_{n}  \tag{4}\\
\hline x_{1} & b_{11} & \ldots & b_{1 n} \\
\vdots & \ldots & \ldots & \ldots \\
x_{n} & b_{n 1} & \ldots & b_{11} \\
\hline
\end{array}
$$

where

$$
\begin{equation*}
b_{i j}=\pi\left(\pi_{1}^{-1}\left(x_{i}\right) \cdot \pi_{2}^{-1}\left(x_{j}\right)\right)=\pi\left(a_{\pi_{1}^{-1}\left(x_{i}\right), \pi_{2}^{-1}\left(x_{j}\right)}\right) \tag{5}
\end{equation*}
$$

It means that we rearrange columns and rows of $Q$ using permutations $\pi_{2}$ and $\pi_{1}$, respectively, and afterwards permute elements of the obtained Latin square using $\pi$.

The next Proposition follows from (3) and (5).
Proposition 2.1. Let $Q$ be a quasigroup of order $n$ with a Latin square (2). Denote the sets of its row and column permutations by

$$
\begin{equation*}
\left\{\sigma_{1}, \ldots, \sigma_{n}\right\}, \quad\left\{\tau_{1}, \ldots, \tau_{n}\right\} \tag{6}
\end{equation*}
$$

If ( $\pi, \pi_{1}, \pi_{2}$ ) is an isotopy of $Q$ then (6) is replaced by the sets

$$
\begin{align*}
\left\{\pi \sigma_{\pi_{1}^{-1}(1)} \pi_{2}^{-1}, \ldots, \pi \sigma_{\pi_{1}^{-1}(n)} \pi_{2}^{-1}\right\} & =\left\{\pi \sigma_{r} \pi_{2}^{-1}, 1 \leqslant r \leqslant n\right\}  \tag{7}\\
\left\{\pi \tau_{\pi_{2}^{-1}(1)} \pi_{1}^{-1}, \ldots, \pi \tau_{\pi_{2}^{-1}(n)} \pi_{1}^{-1}\right\} & =\left\{\pi \tau_{s} \pi_{1}^{-1}, 1 \leqslant s \leqslant n\right\} .
\end{align*}
$$

In particular the sets

$$
\begin{equation*}
\left\{\sigma_{i j}=\sigma_{i} \sigma_{j}^{-1} \mid 1 \leqslant i, j \leqslant n\right\}, \quad\left\{\tau_{i j}=\tau_{i} \tau_{j}^{-1} \mid 1 \leqslant i, j \leqslant n\right\} \tag{8}
\end{equation*}
$$

are replaced by the sets

$$
\begin{align*}
& \left\{\pi \sigma_{\pi_{1}^{-1}(i)} \sigma_{\pi_{1}^{-1}(j)}^{-1} \pi^{-1} \mid 1 \leqslant i, j \leqslant n\right\}=\left\{\pi \sigma_{r s} \pi^{-1} \mid 1 \leqslant r, s \leqslant n\right\}  \tag{9}\\
& \left\{\pi \tau_{\pi_{2}^{-1}(i)} \tau_{\pi_{2}^{-1}(j)}^{-1} \pi^{-1} \mid 1 \leqslant i, j \leqslant n\right\}=\left\{\pi \tau_{k l} \pi^{-1} \mid 1 \leqslant k, l \leqslant n\right\}
\end{align*}
$$

respectively.
The multiplication group $\operatorname{Mult}(Q)$ is the permutation group of the set $Q$ generated by permutations (6). By [13, Theorem 2] dihedral, symmetric, alternating, general linear, projective general linear groups as well as Mathieu groups $M_{11}, M_{12}$ can occur as $\operatorname{Mult}(Q)$ for some quasigroup $Q$.

Denote by $G(Q)$ the subgroup of $\operatorname{Mult}(Q)$ generated by elements (8). Note that $G(Q)$ is generated by elements $\sigma_{i 1}, \tau_{i 1}$ where $2 \leqslant i \leqslant n$. Since (4) is a Latin square the elements $\sigma_{i 1}, 2 \leqslant i \leqslant n$, are distinct and non-identical. Adding to them the identity element we can conclude that the order of the group $H(Q)$ generated by all elements $\sigma_{i 1}$ where $2 \leqslant i \leqslant n$ is at least $n=|Q|$. Since $G(Q) \supseteq H(Q)$, the order of $G(Q)$ is greater or equal to the order of $Q$.

The next Theorem is close to [13, Theorem 1].
Theorem 2.2. Under an isotopy $\left(\pi, \pi_{1}, \pi_{2}\right)$ the group $G(Q)$ is mapped to $\pi G(Q) \pi^{-1}$. In particular if by Albert theorem $Q$ is isotopic to a loop $Q^{\prime}$ then $G(Q)$ is conjugate to the group $G\left(Q^{\prime}\right)$ which coincides with Mult $Q^{\prime}$.

Proof. Let $e=x_{i}$ be the identity of a loop $Q^{\prime}$. Then $\sigma_{i}=\tau_{i}$ is the identity permutation. Then $\sigma_{j} \sigma_{i}^{-1}=\sigma_{j}$ and similarly $\tau_{j} \tau_{i}^{-1}=\tau_{j}$ for all $j$. Hence $\pi G(Q) \pi^{-1}=G\left(Q^{\prime}\right)=\operatorname{Mult} Q^{\prime}$. Now we can apply (9).

Note that $\sigma_{i}$ is a permutation $L_{x_{i}}$ of left multiplication by $x_{i}$, and $\tau_{j}$ is a permutation $R_{x_{j}}$ of right multiplication by $x_{j}$.

Theorem 2.3. The following conditions are equivalent:
(i) any pair of permutations $\sigma_{i j}, \tau_{r s}$ from (8) commute between themselves;
(ii) $Q$ is isotopic to a group;
(iii) the order of $H(Q)$ is equal to the order of $Q$.

Proof. Suppose that (ii) holds. Using Theorem 2.2 we can replace $Q$ by an isotopic copy $Q$ which is a group. By the associativity law, permutations $\sigma_{i}, \tau_{r}$ commute and (i) follows.

Suppose that (i) holds. We can assume that $Q$ is a loop. Taking $x_{1}=e$ we see that $\sigma_{i 1}=\sigma_{i}$ and $\tau_{r 1}=\tau_{r}$. So for any $a \in Q$ we have

$$
\left(x_{i} a\right) x_{r}=\tau_{r} \sigma_{i 1} a=\sigma_{i 1} \tau_{r} a=x_{i}\left(a x_{r}\right) .
$$

So $Q$ is associative and therefore a group.
Suppose that (iii) holds. Then $H(Q)=\left\{\sigma_{i 1} \mid 1 \leqslant i \leqslant n\right\}$. By (9), Theorem 2.2 and by Albert theorem we can assume that $Q$ is a loop with unit element $x_{1}=e$. Now for any indices $i, j$ there exists an index $k$ such that $\sigma_{i 1} \sigma_{j 1}=\sigma_{k 1}$. Applying these maps to $e=x_{1}$ we get $x_{i} x_{j}=x_{k}$. It means that the map $x_{i} \rightarrow \sigma_{i 1}$ is an isomorphism of $Q$ and the group $H(Q)$. Hence (ii) holds.

Suppose that (ii) holds. Without loss of generality we can assume that $Q$ is a group. Then the map $H(Q)$ is the group of left translations by elements of $Q$ and this group is isomorphic to $Q$. So (iii) follows.

Theorem 2.4. The following conditions are equivalent:
(i) any pair of permutations from (8) commute;
(ii) $Q$ is isotopic to an abelian group;
(iii) $G(Q)$ is an abelian group;
(iv) $Q$ is isotopic to the abelian group $G(Q)$;
(v) The order of $H(Q)$ is equal to the order of $G(Q)$ and to the order of $Q$.

Proof. Note that conditions (i) and (iii) are equivalent since the elements (8) generate $G(Q)$.

Now let (i) and (iii) hold. By Albert's theorem $Q$ is isotopic to a loop $Q^{\prime}$. Then $G(Q)=\operatorname{Mult} Q^{\prime}$ by Theorem 2.2 is an abelian group. Hence for any $x, y, a \in Q^{\prime}$ we have $(x a) y=x(a y)$ and $x(y a)=y(x a)$. It follows that mutiplication in $Q^{\prime}$ is associative and commutative. Thus $Q^{\prime}$ is a group and (ii) holds.

Conversely if (ii) holds then $G(Q)=$ Mult $Q^{\prime}$ is an abelian group by Theorem 2.2.

Finally if equivalent conditions (i) - (iii) hold, then $G(Q)$ is isomorphic to Mult $Q^{\prime}$ where $Q^{\prime}$ is an abelian group. In this case Mult $Q^{\prime} \simeq Q^{\prime}$. Thus $G(Q) \simeq Q^{\prime}$ and (iv) holds. Conversely (iv) implies (iii).

Suppose that (v) holds. Then $Q$ is isotopic to a group by Theorem 2.3. So we can assume that $Q$ is a group with a unit element $x_{1}$. By (v) we have $\tau_{i 1}=\sigma_{j 1}$ for some $j$. It means that $x_{i} x=x x_{j}$ for any $x \in Q$. Setting $x=x_{1}$ we get $x_{j}=x_{i}$ and obtain commutativity law in $Q$. So (ii) holds.

The same argument shows that (v) implies (ii).

## 3. Affine quasigroups

A universal algebra $Q$ is affine if there exists a structure of additive abelian group on $Q$ such that any basic $n$-ary operation $f$ on $Q$ has the form

$$
f\left(x_{1}, \ldots, x_{n}\right)=\alpha_{1}\left(x_{1}\right)+\cdots+\alpha_{n}\left(x_{n}\right)+c,
$$

where $\alpha_{1}, \ldots, \alpha_{n}$ are group endomorphisms of $(Q,+)$ and $c \in Q$. Following this definition we call a quasigroup $Q$ is affine or a T-quasigroup if there exists a structure of an abelian group $<Q,+, 0,->$ in $Q$ such that

$$
\begin{equation*}
x y=\alpha(x)+\beta(y)+c \tag{10}
\end{equation*}
$$

for some automorphisms $\alpha, \beta$ of the group $<Q,+, 0,->$ and for some element $c \in Q$. It is easy to see that a quasigroup is affine if and only if the group operations $<Q,+, 0,->$ are polynomials with respect to the quasigroup operations $<Q, \cdot, /, \backslash>$.

Note that the affine quasigroup is isotopic to the abelian group $\langle Q,+\rangle$. In fact take $\pi_{1}=\alpha^{-1}, \pi_{2}=\beta^{-1}$ and $\pi(x)=x+c$.

Hence we have

Proposition 3.1. If $Q$ is an affine quasigroup then $G(Q)$ is isomorphic to the group $<Q,+, 0,->$.

An equivalence relation $\wp$ in a quasigroup $Q$ is a congruence if $\wp$ is a subquasigroup in direct square $Q \times Q$. A quasigroup $Q$ is simple if it has only trivial congruences. It means in particular that any quasigroup homomorphism from $Q$ to any other quasigroup is either an embedding or its image is a one-element set.

Proposition 3.2. Let $Q$ be a finite simple affine quasigroup. Then $(Q,+)$ is an elementary abelian p-group for some prime $p$ and $|Q|=p^{d}$ for some positive integer d. The group $\operatorname{Mult}(Q)$ is embedded into the group of affine transformations $\operatorname{Aff}(Q)$ of $Q$ as a vector space over the field $\mathbb{F}_{p}$ with $p$ elements. In particular $G(Q)$ is a normal subgroup in $\operatorname{Mult}(Q)$ isomorphic to $\langle Q,+\rangle$.

Proof. Let $A$ be a subgroup in $(Q,+)$ which is stable under $\alpha, \beta$. Define a relation $u \sim v \Longleftrightarrow u-v \in A$. It is easy to check that $\sim$ is a congruence. So if $Q$ is a simple quasigroup then $(Q,+)$ has no non-trivial subgroups stable under $\alpha, \beta$. In particular for any divisor $p$ of the order of $Q$ the set $\{x \in Q \mid p x=0\}$ is non-zero and therefore it coincides with $(Q,+)$. Hence $Q$ is a vector space over the field $\mathbb{F}_{p}$.

Corollary 3.3. A simple finite quasigroup $Q$ is polynomially complete if either of conditions is satisfied:
(i) the order of $Q$ is not a prime power,
(ii) the order of $Q$ is a power of a prime $p$, and $G(Q)$ is not an elementary abelian p-group whose order is equal to the order of $Q$,
(iii) $\operatorname{Mult}(Q)$ has no normal abelian subgroups.

The class of quasigroups with the given property is stable under isotopies.
Use Proposition 3.2 and [1, Corollary 3.4]
Proposition 3.4. Let $Q$ be an affine quasigroup of a prime order $p$. Then the order of each cycle occurring in permutations $\tau_{j}, \sigma_{i}$ is a divisor of $p-1$. In particular the order of each permutation $\tau_{j}, \sigma_{i}$ is a divisor of $p-1$.

Proof. Affine quasigroup is defined on residue group $\mathbb{Z} / p$ by (10). So we can conclude that $\alpha(x)=k x, \beta(y)=m y$, where $k, m$ are coprime with $p$.

Fix an element $y=x_{j}$. Then $R_{y}=\tau_{j}$. By induction on $t$ we can prove that

$$
\tau_{j}^{t}(x)=k^{t} x+\left(k^{t-1}+\cdots+1\right)(m y+c)
$$

Let $\tau_{j}$ have a cycle of length $t$ generated by an element $x$, then

$$
x=k^{t} x+\left(k^{t-1}+\cdots+1\right)(m y+c)
$$

and therefore

$$
\left(k^{t}-1\right) x+\left(k^{t-1}+\cdots+1\right)(m y+c)=0 .
$$

Suppose first that

$$
a=k^{t-1}+\cdots+1 \in \mathbb{Z} / p \backslash 0
$$

Canceling by $a$, we obtain $(k-1) x+m y+c=0$ or $\tau_{j}(x)=x$. So $\tau_{j}$ has a cycle of length 1 .

Suppose now that

$$
a=k^{t-1}+\cdots+1=0
$$

in $\mathbb{Z} / p$. Then $k^{t}=1$. Since $k$ is coprime with $p$ we can conclude that $t$ is a divisor of $p-1$.

Proposition 3.5. Let $Q$ be an affine quasigroup of a prime order $p$. Then $\operatorname{Mult}(Q)$ is an extension of an abelian translation group by a cyclic group of order dividing $p-1$.

Proof. By (10) each map $R_{y}, L_{x}$ is an affine transformation of $Q=\mathbb{F}_{p}$ and therefore it has the form $x \rightarrow \alpha x+c$ where $\alpha$ is a non-zero element of $\mathbb{F}_{p}$.

There exists a surjective group homomorphism $\operatorname{Aff}\left(\mathbb{F}_{p}\right) \rightarrow \mathbb{F}_{p}^{*}$ sending each map $x \mapsto \alpha x+c$ to $\alpha \in \mathbb{F}_{p}^{*}$. The image is a subgroup of the cyclic group $\mathbb{F}_{p}^{*}$ and the kernel consists of translations $x \mapsto x+c, c \in Q$.

Proposition 3.6. Let $Q$ be an affine quasigroup. Then the operations $x \backslash y, x / y$ are also affine. Conversely, if an operation $x \backslash y(x / y)$ is affine then $Q$ is affine.

Proof. Let (10) holds. Then by (1)

$$
y=x(x \backslash y)=\alpha x+\beta(x \backslash y)+c
$$

and therefore

$$
x \backslash y=-\beta^{-1} \alpha x+\beta^{-1} y-\beta^{-1} c .
$$

Similarly

$$
x=(x / y) y=\alpha(x / y)+\beta y+c
$$

implies

$$
x / y=\alpha^{-1} x-\alpha^{-1} \beta y-\alpha^{-1} c .
$$

Thus the operations $x \backslash y, x / y$ are affine.
Suppose now that $x \backslash y=\gamma x+\delta y+d$ is affine. Then

$$
y=x \backslash(x y)=\gamma x+\delta(x y)+d
$$

and

$$
x y=-\delta^{-1} \gamma x+\delta^{-1} y-\delta^{-1} d
$$

is an affine operation. The case of affine operation $x / y$ is similar.

Take fundamental operations $x y, x \backslash y, y / x$ in a quasigroup $Q$ and of all nullary operations fixing elements from $Q$. Now consider all finitary operations in $Q$ which are obtained from fundamental ones by compositions, identifications and permutations of variables. The operations on $Q$ which are obtained by this process are called polynomial. A quasigroup $Q$ is polynomially complete if any finitary operation on $Q$ is polynomial.

Theorem 3.7 ([12]). A finite quasigroup $Q$ is polynomially complete, if and only if $Q$ is simple and non-affine quasigroup.

It is well known that a quasigroup $Q$ is simple if and only if $\operatorname{Mult}(Q)$ is primitive permutation group of $Q$. The following section deals with characterization of polynomial completeness of highly non-associative quasigroups and its invariant class under isotopy by using $\operatorname{Mult}(Q)$ and $G(Q)$.

## 4. Highly non-associative quasigroups

A quasigroup $Q$ is highly non-associative if $\operatorname{Mult}(Q)=\operatorname{Sym}(Q)$.
By a definition of a quasigroup the group $\operatorname{Mult}(Q)$ of a quasigroup $Q$ acts transitively on the set $Q$.

Proposition 4.1 ([17]). Let $Q$ be a quasigroup of order $n$ such that $\operatorname{Mult}(Q)$ is a doubly transitive permutation group on $Q$. Then $Q$ is simple. In particular, if $n \geqslant 4$ and $\operatorname{Mult}(Q) \supseteq \mathbf{A}_{n}$ then $Q$ is simple. A highly non-associative quasigroup of any order is simple.

Proof. Suppose $\wp$ is a congruence in $Q$. Let $\wp(c)$ be a class containing $c \in Q$ and $d \in \wp(c) \backslash c$. By double transitivity there exists $g \in \operatorname{Mult}(Q)$ such that $g(c)=c$ and $g(d) \notin \wp(c)$. Since $\wp$ is a congruence $(c, d) \in \wp$ implies $(g(c), g(d))=(c, g(d)) \in \wp$, which is not the class.

If a quasigroup $Q$ is highly non-associative then $\operatorname{Mult}(Q)=\operatorname{Sym}(Q)$ is a doubly transitive group. If $n \geqslant 4$, then $\mathbf{A}_{n}$ is again a doubly transitive group.

The next Proposition generalizes [1, Proposition 3.13].
Proposition 4.2. Let $Q$ be a quasigroup of order $n$. Suppose that $\operatorname{Mult}(Q)$ contains a simple non-identical subgroup $G$ whose images under any group homomorphisms into any symmetric group $\mathbf{S}_{q}$ is identical provided $q<n$ and $q \mid n$. Then $Q$ is simple.

Proof. Suppose that $Q$ has a proper congruence $\wp$. If $x \in Q$ then the maps $L_{x}, R_{x}$ permute congruence classes of $\wp$. Hence there exists a group homomorphism $\pi$ from Mult $Q$ into the group $\mathbf{S}_{q}$ of permutations of $Q / \wp$. As it was shown in [3] orders of each congruence classes of $\wp$ are equal and therefore the order $q$ of $Q / \wp$ is a divisor of the order of $Q$. By assumption $\pi(G)=1$ which means that $G$ acts
identically on $Q / \wp$. It means that each class of the congruence $\wp$ is stable under the action of $G$.

Let $x \in Q$ and $C$ the class of $\wp$ containing $x$. The order of $C$ is equal to $\frac{n}{q}<n$. Since $C$ is stable under action of $G$ there exists a group homomorphism $\xi: G \rightarrow \mathbf{S}_{\frac{n}{q}}$. By assumption $\xi(G)=1$. It means that $g(x)=x$ for any $g \in G$, a contradiction. Hence $Q$ is simple.

Corollary 4.3. Let $Q$ be a quasigroup of order $n$ and $G$ a simple non-identical subgroup of $\operatorname{Mult}(Q)$. Suppose that the order of $G$ does not divide $q$ ! for any proper factor $q$ of $n$. Then any homomorphisms of $G$ into any symmetric group $\mathbf{S}_{q}$ is identical provided $q<n$ and $q \mid n$. In particular $Q$ is simple.

Proof. Let $\pi: G \rightarrow \mathbf{S}_{q}$ be a homomorphism where $q<n$ and $q \mid n$. Then the order of the image $\pi(G)$ divides $q$ !. If $\pi$ is not identical then by simplicity of $G$ the order of $\pi(G)$ is equal to the order of $G$, a contradiction.

Theorem 4.4. Let $Q$ be a finite quasigroup of order $n$ and $\operatorname{Mult}(Q)$ contain a subgroup isomorphic the alternative subgroup $\mathbf{A}_{m}$, where

$$
\begin{equation*}
m \geqslant \max \left(\left[\frac{n}{2}\right]+1,5\right) \tag{11}
\end{equation*}
$$

Then $Q$ is polynomially complete. In particular a highly non-associative quasigroup of order $n \geqslant 5$ is polynomially complete.

Proof. To prove the theorem we need the following two lemmas.
Lemma 4.5. The group $G$, isomorphic to $\mathbf{A}_{m}$ yields the assumption of Proposition 4.2.

Proof. Let $\pi$ be a non-identical homomorphism of $G=\mathbf{A}_{m}$ into $\mathbf{S}_{r}$ where $r \mid n$ and $r<n$. Since $\mathbf{A}_{m}$ is simple the map $\pi$ is injective and therefore $\frac{m!}{2}$, the order of $\mathbf{A}_{m}$ divides $r!$, the order of $\mathbf{S}_{r}$. Thus $m!\mid 2 \cdot r!$. It is required to mention that

$$
r \leqslant\left[\frac{n}{2}\right]
$$

and

$$
m \geqslant\left[\frac{n}{2}\right]+1
$$

Hence

$$
\left(\left[\frac{n}{2}\right]+1\right)!\left\lvert\, 2 \cdot\left[\frac{n}{2}\right]!.\right.
$$

It follows that $\left.\left[\frac{n}{2}\right]+1 \right\rvert\, 2$ and $\left[\frac{n}{2}\right]=1$. In this case $r=1$ and

$$
\frac{5!}{2}\left|\frac{m!}{2}\right| r!=1,
$$

a contradiction.

Lemma 4.6. Let $p$ be an odd prime. Then $p+1 \leqslant\left[\frac{p^{2}}{2}\right]$.
Proof. Since $p \geqslant 3$ we have

$$
p^{2}-2 p-2=(p-1)^{2}-3 \geqslant 2^{2}-3=1>0 .
$$

Hence $p^{2}>2 p+2$ and the proof follows.
Now it follows from Lemma 4.5 and Propositions 4.2, 3.2 $Q$ is a vector space over the field $\mathbb{F}_{p}$ for some prime $p$ of dimension $d$.

The maps $L_{x}, R_{y}$ are affine transformations of the vector space $Q$ by (10). Therefore $\operatorname{Mult}(Q)$ consists of affine transformations of $(Q,+)$.

Recall some basic facts related to the group $\operatorname{Aff}(Q)$ of affine transformations of $(Q,+)$. Let $f \in \operatorname{Aff}(Q)$ and $f(x)=\alpha(x)+c$ where $\alpha \in \operatorname{GL}\left(d, \mathbb{F}_{p}\right)$ and $c \in Q$. Put $\zeta(f)=\alpha$. Then $\zeta: \operatorname{Aff}(q) \rightarrow \operatorname{GL}\left(d, \mathbb{F}_{p}\right)$ is a surjective group homomorphism with abelian kernel consisting of translations $f(x)=x+c, c \in Q$. Since $\mathbf{A}_{m}$ is a nonabelian simple group the homomorphism $\zeta$ maps $\mathbf{A}_{m}$ injectively into $\operatorname{GL}\left(d, \mathbb{F}_{p}\right)$. Moreover there is a surjective group homomorphism det : $\operatorname{GL}\left(d, \mathbb{F}_{p}\right) \rightarrow \mathbb{F}_{p}^{*}$ with kernel $\operatorname{SL}\left(d, \mathbb{F}_{p}\right)$. The group $\mathbb{F}_{p}^{*}$ of nonzero elements of the field $\mathbb{F}_{p}$ is abelian. Again by simplicity of $\mathbf{A}_{m}$ we have $\operatorname{det}\left(\zeta\left(\mathbf{A}_{m}\right)\right)=1$. It means that $\zeta$ embeds $\mathbf{A}_{m}$ into $\operatorname{SL}\left(d, \mathbb{F}_{p}\right)$ and by Lagrange's theorem $\frac{m!}{2}$ divides the order of $\operatorname{SL}\left(d, \mathbb{F}_{p}\right)$ which is equal to

$$
\frac{\left(p^{d}-1\right)\left(p^{d}-p\right) \cdots\left(p^{d}-p^{d-1}\right)}{p-1}=p^{\frac{d(d-1)}{2}}\left(p^{d}-1\right)\left(p^{d-1}-1\right) \cdots\left(p^{2}-1\right)
$$

Since $m \geqslant\left[\frac{p^{d}}{2}\right]+1$ we can conclude that

$$
\begin{equation*}
\left(\left[\frac{p^{d}}{2}\right]+1\right)!\left\lvert\, 2 p^{\frac{d(d-1)}{2}}\left(p^{d}-1\right)\left(p^{d-1}-1\right) \cdots\left(p^{2}-1\right)\right. \tag{12}
\end{equation*}
$$

Note that by definition $p^{d-1} \leqslant \frac{p^{d}}{2}$. Hence the product $\left(p^{d-1}-1\right) \cdots\left(p^{2}-1\right)$ occurs in $\left(\left[\frac{p^{d}}{2}\right]+1\right)$ !. After cancellation in (12) we obtain

$$
p^{d-1}\left(p^{d-1}+1\right) \left\lvert\, 2 p^{\frac{d(d-1)}{2}}\left(p^{d}-1\right)\right.
$$

and therefore $\left(p^{d-1}+1\right) \mid 2\left(p^{d}-1\right)$. Note that

$$
2 p+2=-2\left(p^{d}-1\right)+2 p\left(p^{d-1}+1\right)
$$

Hence

$$
\begin{equation*}
\left(p^{d-1}+1\right) \mid 2(p+1) \tag{13}
\end{equation*}
$$

Let $p=2$. Then $d \geqslant 3$, because $n=2^{d} \geqslant 5$. So in (13) we have $\left(2^{d-1}+1\right) \mid 6$. Then $d=1,2$, a contradiction.

Now let $p$ be an odd prime and (13) holds. If $d \geqslant 3$, then

$$
p^{d-1}+1 \geqslant p^{2}+1>2(p+1)
$$

a contradiction.
Let $d=2$. Then in (12) we have

$$
\begin{equation*}
\left.\left(\left[\frac{p^{d}}{2}\right]+1\right)!\right\rvert\, 2 p\left(p^{2}-1\right)=2 p(p-1)(p+1) \tag{14}
\end{equation*}
$$

Cancel (14) by $(p-1) p(p+1)$. Then by Lemma $4.6,1 \cdots \cdots(p-2) \cdot(p+2) \cdots \mid 2$, and therefore $p+2$ divides 2 , a contradiction, since $p$ is an odd prime.

So (12) is impossible and $Q$ is not affine. Therefore $Q$ is polynomially complete.
In particular, if $\operatorname{Mult}(Q)$ is highly non-associative, then $\operatorname{Mult}(Q)$ contains $\mathbf{S}_{n}$ and $\mathbf{A}_{m}$, where $m$ is from (11).

Proposition 4.7. Let $Q$ be a quasigroup of order $n \geqslant 5$. Suppose that there exists an element of $\operatorname{Mult}(Q)$ with a cycle decomposition containing a cycle of prime length $p>\frac{n}{2}$ and $n-p \neq 0,1$. Then Mult $Q$ is simple and $\operatorname{Mult} Q$ contains $\mathbf{A}_{n}$ if one of the following conditions is satisfied:
(i) $n \geqslant p+3$
(ii) $n=p+2$ and $n-1 \neq 2^{t}, t \in \mathbb{N}$.

Proof. Let $\sigma \in \operatorname{Mult}(Q)$ and $\sigma=\sigma_{1} \cdots \sigma_{m}$ a decomposition into a product of independent cycles and the length of $\sigma_{1}$ is equal to $p$. Then the lengths of other cycles $\sigma_{j}, j>1$ is less than $p$. Let $d$ be the least common multiple of orders of cycles $\sigma_{j}, j>1$. Then $d$ is coprime with $p$. Therefore $\sigma^{d}=\sigma_{1}^{d} \in \operatorname{Mult}(Q)$ is a cycle of prime length $p$ fixing $n-p$ elements of $Q$. Hence $\sigma_{1} \in \operatorname{Mult}(Q)$ and therefore

$$
\sigma_{2} \cdots \sigma_{m}=\sigma_{1}^{-1} \sigma \in \operatorname{Mult}(Q)
$$

The group $G=\left\langle\sigma_{1}\right\rangle$ has a prime order. Hence it is a simple subgroup in $\operatorname{Mult}(Q)$. Suppose there exists a homomorphism $f: G \rightarrow \mathbf{S}_{q}$ where $q<n$ and $q \mid n$. So $q \leqslant \frac{n}{2}, p>\frac{n}{2}$ so $\frac{n}{2}<p$ and therefore $q<p$.

The image $f(G)$ has order $p$ so $p \mid q$ ! where $(q, p)=1$. It follows that $p$ can't divide $q$ !, a contradiction. Hence $f(G)=1$.

By Proposition 4.2 we obtain that $Q$ is simple and therefore Mult $Q$ is primitive group of permutations.

Now since $n-p \neq 0,1$, so either
(i) $n-p \geqslant 3$, then, by [14, Theorem 1.2, Corollary 1.3], $\mathbf{A}_{n} \subseteq \operatorname{Mult}(Q)$, or
(ii) $n-p=2$ then by [14, Theorem 1.2, Corollary 1.3] we obtain $\mathbf{A}_{n} \subseteq \operatorname{Mult}(Q)$, if $n-1=p+1$ is not a prime power. Suppose that $p+1=q^{t}$ for some prime $q$. Then $q^{t}-1=p$ and $(q-1) \mid p$ which means that $q=2$. So in this case if $n-1 \neq 2^{t}$ then the proposition holds.
By using Proposition 4.7 in a restricted domain and Theorem 4.4 we develop an algorithm (Figure 1) to identify polynomially complete quasigroups of order $n>5$ based on their Latin square representations. Compute $\operatorname{Mult}(Q)$ from $Q$ is computationally expensive. Hence in this algorithm we choose the element from $Q$ of $\operatorname{Mult}(Q)$ and it able to identify a subclass of polynomially complete quasigroup using lesser computation. The algorithm is given below:

## Algorithm

Input : $n \times n$ Latin square of the quasigroup $Q$ of order $n$
Output : Decision - quasigroup is polynomially complete / unidentified
Steps:

1. flag $=0$
2. for $i=1: n$

- Decompose row permutation $\sigma_{i}$ of $Q$ into disjoint cycles
- Check whether there exists a sub-cycle of $\sigma_{i}$ of prime length $p \in\left[\left[\frac{n}{2}\right]+1, n-2\right]$
- if yes, then check whether

$$
(n-p \geqslant 3) \text { or }\left(n-p=2 \& n \neq 2^{t} \text { for } t \in \mathbb{N}\right)
$$

- if yes then flag=1; break; endif
endif
endfor

3. if flag $=0$ then repeat step 2 for column permutation $\tau_{j}, 1 \leqslant j \leqslant n$, of $Q$ endif
4. if flag=1 print : Polynomially Complete
else print: unidentified
endif

Figure 1: Algorithm for identifying polynomially complete quasigroup of order $>5$.
The following example shows the application of the algorithm to identify the polynomially complete quasigroup $Q$ from the given corresponding Latin square by testing the cycle structures of row / column permutations of $Q \subseteq \operatorname{Mult}(Q)$.

Let Q be a finite quasigroup Q of order $n=7$. The corresponding $7 \times 7$ Latin square is given below

|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 1 | 1 | 4 | 3 | 7 | 2 | 6 | 5 |
| 2 | 5 | 1 | 7 | 4 | 6 | 3 | 2 |
| 3 | 6 | 2 | 1 | 5 | 7 | 4 | 3 |
| 4 | 7 | 3 | 2 | 6 | 1 | 5 | 4 |
| 5 | 3 | 6 | 5 | 2 | 4 | 1 | 7 |
| 6 | 2 | 5 | 4 | 1 | 3 | 7 | 6 |
| 7 | 4 | 7 | 6 | 3 | 5 | 2 | 1 |

Following the steps of the algorithm described in Figure 1, for $i=4, \sigma_{4}$ has a sub-cycle of length $p=5$. Now $n-p=2 \& n-1=6 \neq 2^{t}$ for $t \in \mathbb{N}$. So by the algorithm it is identified as polynomially complete.

Recall that the Klein subgroup $V_{4}$ of $\mathbf{S}_{4}$ consists of an identity permutation and of all three $2 \times 2$-cycles. The order of $V_{4}$ is equal to 4 and it is isomorphic to $\mathbb{Z}_{2} \times \mathbb{Z}_{2}$.

Proposition 4.8. Let $Q$ be a quasigroup of order 4. Suppose that Mult $(Q)$ does not contain a cycle of length 3. Then $\operatorname{Mult}(Q)$ is contained in a Sylow 2-group $\mathrm{Syl}_{2}$ of $\mathbf{S}_{4}$ which is a semi-direct product of the Klein group $V_{4}$ and a subgroup of order 2 generated by 2-cycle.

Proof. By assumption each non-identical element from $\operatorname{Mult}(Q) \subseteq \mathbf{S}_{4}$ is either a 4-cycle or a product of independent 2-cycles. It means that each element of $\operatorname{Mult}(Q)$ has order 1, 2, 4. So it is contained in Sylow 2-subgroup of $\mathbf{S}_{4}$.

Proposition 4.9. Let $Q$ be a quasigroup of order 4 in which $\operatorname{Mult}(Q)$ has a 3 -cycle. Then the group $\operatorname{Mult}(Q)$ contains $\mathbf{A}_{4}$. Hence if there is also an odd permutation among its row or column permutations then $Q$ is highly non-associative and therefore polynomially complete.

Proof. Let a 3-cycle $\sigma$ exist. By [1, Proposition 3.13] the quasigroup $Q$ is simple.
Let $G=\operatorname{Mult}(Q)$ and $H$ a subgroup in $G$ fixing the same element as $\sigma$. Then $\sigma$ belongs to $H$. Hence the order of $H$ is divisible by 3 and also $|G|=4|H|$ because $G$ acts transitively on $Q$. Hence the order of $G$ is divisible by 12 .

Since $G$ is a subgroup of $\mathbf{S}_{4}$ we can conclude that the order of $G$ is either 12 or 24 . So either $G=\mathbf{A}_{4}$ or $G=\mathbf{S}_{4}$.

If in addition there exists an odd permutation from $\operatorname{Mult}(Q) \supset \mathbf{A}_{4}$, then $\operatorname{Mult}(Q)=\mathbf{S}_{4}$. By [1, Proposition 4.4] $Q$ is not a affine quasigroup.

Proposition 4.10. Let $Q$ be a non-simple quasigroup of order 4. Then $\operatorname{Mult}(Q)$ is contained in Sylow 2-subgroup $\operatorname{Syl}_{2}$ of $\mathbf{S}_{4}$. Note that the commutator of $\mathrm{Syl}_{2}$ is contained in $V_{4}$ and it has order 2.

Proof. If $Q$ is non-simple then $\operatorname{Mult}(Q)$ does not contain 3-cycles by Proposition 4.9. Apply Proposition 4.8.

Proposition 4.11. Let $|Q|=p^{d}$ for some prime $p$ and $\operatorname{Mult}(Q)$ is embedded into the group of all affine transformations of a vector space $V$ of dimension $d$ over the field $\mathbb{F}_{p}$ with $p$ elements. Then $Q$ can be identified with $V$ and

$$
x y=x * y+\alpha(x)+\beta(y)+c, \quad c \in Q
$$

where $x * y$ is a bilinear multiplication in $Q$ such that $\alpha, \beta$ and the maps

$$
\begin{equation*}
x \mapsto x * y+\alpha(x), \quad y \mapsto x * y+\beta(y) \tag{15}
\end{equation*}
$$

are invertible linear operators in $Q$.
Proof. By assumption on the order of $Q$ and on action of $\operatorname{Mult}(Q)$ we can identify $Q$ with the vector space $V$ of dimension $d$ over the field $\mathbb{F}_{p}$ such that the maps of left and right multiplication became affine transformations on $Q$. More precisely, for any $x, y \in Q$ we have

$$
\begin{array}{ll}
x y=L_{x} y=\beta_{x}(y)+\gamma(x), & \gamma(x) \in Q \\
x y=R_{y} x=\alpha_{y}(x)+\delta(y), & \delta(y) \in Q
\end{array}
$$

where $\beta_{x}, \alpha_{y}$ are invertible linear operators in $Q$ for any $x, y \in Q$.
Setting $\beta=\beta_{0}, \alpha=\alpha_{0}$ we get

$$
\begin{aligned}
& 0 y=\beta(y)+\gamma(0)=\delta(y) \\
& x 0=\alpha(x)+\delta(0)=\gamma(x)
\end{aligned}
$$

Hence

$$
x y=\beta_{x}(y)+\alpha(x)+\delta(0)=\alpha_{y}(x)+\beta(y)+\gamma(0)
$$

Setting $x=y=0$ we obtain $\delta(0)=\gamma(0)$ and therefore

$$
\beta_{x}(y)-\beta(y)=\alpha_{y}(x)-\alpha(x)
$$

is a bilinear multiplication $x * y$ in $Q$. Finally, $\alpha_{y}(x)=x * y+\alpha(x)$ and it follows that $x y$ has the required form.

As we have noticed above $\alpha, \beta$ are invertible linear operators. Since $Q$ is a quasigroup the maps (15) are also invertible linear operators for any $x, y \in Q$.

Consider a quasigroup

|  | 1 | 2 | 3 | 4 |
| :--- | :--- | :--- | :--- | :--- |
| 1 | 2 | 1 | 3 | 4 |
| 2 | 1 | 3 | 4 | 2 |
| 3 | 4 | 2 | 1 | 3 |
| 4 | 3 | 4 | 2 | 1 |.

In this example the fist row is the cycle $(1,2)$, the second row is the cycle $(2,3,4)$. It also contains a cycle $(1,3,2,4)$ and by Theorem 4.9 it is highly nonassociative. Therefore by Proposition 4.1 it is simple.

Consider another quasigroup

|  | 1 | 2 | 3 | 4 |
| :--- | :--- | :--- | :--- | :--- |
| 1 | 3 | 2 | 4 | 1 |
| 2 | 4 | 1 | 3 | 2 |
| 3 | 1 | 4 | 2 | 3 |
| 4 | 2 | 3 | 1 | 4 |.

In this example row permutations are

$$
\begin{equation*}
(1,3,4),(1,4,2),(2,4,3),(1,2,3) . \tag{17}
\end{equation*}
$$

Column permutations are

$$
\begin{equation*}
(1,3)(2,4), \quad(1,2)(3,4), \quad(1,4)(2,3), \quad \varepsilon, \tag{18}
\end{equation*}
$$

where $\varepsilon$ is the identity permutation. So by Proposition 4.9 this is a simple quasigroups whose $\operatorname{Mult}(Q)=\mathbf{A}_{4}$. So simplicity does no imply highly-nonassociativity.

Now we shall characterize invariant class of polynomially complete highly non associative quasigroup under isotopy.
Proposition 4.12. Let $Q$ be a finite quasigroup of order $n \geqslant 5$. Suppose that the group $G(Q)$ from $\S 2$ contains a subgroup isomorphic to $\mathbf{A}_{m}, m \geqslant \max \left(\frac{|Q|}{2}+1,5\right)$. The class of quasigroups $Q$ with given property is stable under isotopies. All of them are polynomially complete.

Apply Theorems 2.2 and 4.4.

## 5. Method for derivation of associative triples

In this section we present a method for deriving associative triples of quasigroups of order $n$. It is based on commutators of row and column permutations of its Latin squares. Here we also give an algorithm for this scheme.

Recall that a triple $(x, a, y)$ of elements of a quasigroup $Q$ is associative if $x(a y)=(x a) y$. In other words $L_{x} R_{y} a=R_{y} L_{x} a$, where $L_{x}, R_{y}$ are maps of left multiplication by $x$ and right multiplication by $y$.

Suppose that a finite quasigroup $Q$ of order $n$ is given by its Latin square (2) with row and column permutations $\sigma_{1}, \ldots, \sigma_{n}, \tau_{1}, \ldots, \tau_{n}$. Let $x=x_{i}, y=x_{j}$. So $L_{x}=\sigma_{i}, R_{y}=\tau_{j}$. Then $L_{x} R_{y} a=\sigma_{i} \tau_{j} a, \quad R_{y} L_{x} a=\tau_{j} \sigma_{i} a$. Hence a triple $\left(x_{i}, a, x_{j}\right)$ is associative if and only if $\sigma_{i} \tau_{j} a=\tau_{j} \sigma_{i} a$. It can be written in equivalent form $\sigma_{i}^{-1} \tau_{j}^{-1} \sigma_{i} \tau_{j} a=a$. If we use group commutator $\left[\sigma_{i}^{-1}, \tau_{j}^{-1}\right]=\sigma_{i}^{-1} \tau_{j}^{-1} \sigma_{i} \tau_{j}$ then we can write $\left[\sigma_{i}^{-1}, \tau_{j}^{-1}\right] a=a$.

So we have

Proposition 5.1. A triple $\left(x_{i}, a, x_{j}\right)$ is associative if and only if $a$ is a fixed element of the permutation $\left[\sigma_{i}^{-1}, \tau_{j}^{-1}\right]$.

So the number of associative triples is equal to a sum of numbers of all fixed elements under commutators $\left[\sigma_{i}^{-1}, \tau_{j}^{-1}\right]$ for all $i, j=1, \ldots, n$.

The algorithm for associative triples of a quasigroup $Q$ of order $n$ is developed based on commutators of column and row permutations of its Latin square by using Proposition 5.1. The algorithm is given below.

## Algorithm

Input : $n \times n$ Latin square of the quasigroup $Q$ of order $n$ Output: Associative triples of $Q$ and total number Steps:

1. Write all row $\left(\sigma_{1}, \ldots, \sigma_{n}\right) \&\left(\tau_{1}, \ldots, \tau_{n}\right)$ permutations of Latin square
2. Write all $\sigma_{1}^{-1}, \ldots, \sigma_{n}^{-1} \& \tau_{1}^{-1}, \ldots, \tau_{n}^{-1}$
3. Calculate $\left[\sigma_{i}^{-1}, \tau_{j}^{-1}\right]=\sigma_{i}^{-1} \tau_{j}^{-1} \sigma_{i} \tau_{j}$
4. Represent each $\left[\sigma_{i}^{-1}, \tau_{j}^{-1}\right]$ is cycle form
5. Write all elements $x_{k} \in Q$ such that $x_{k}$ does not belong to any nontrivial cycle of $\left[\sigma_{i}^{-1}, \tau_{j}^{-1}\right]$ and denote by $\overline{x_{k}}$
6. Associative triples for each $\left[\sigma_{i}^{-1}, \tau_{j}^{-1}\right]$ are $\left(x_{i}, \overline{x_{k}}, x_{j}\right) \forall \overline{x_{k}}$
7. Total number of associative triples $=\sum \# \overline{x_{k}}$ for each $i, j$ where $1 \leqslant i, j \leqslant n$

Figure 2: Algorithm for associative triples.
This algorithm first calculates $n^{2}$ number of commutators and directly calculate associative triples directly instead of calculations of $2 n^{3}$ triplets of the form $(x y) z, x(y z)$ and comparing them to derive associative triplets.

The following example shows application of the algorithm for a quasigroup of order 5 . Consider a quasigroup $Q$ of order 5 with the Latin square

|  | 1 | 2 | 3 | 4 | 5 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 1 | 4 | 2 | 3 | 5 | 1 |
| 2 | 5 | 1 | 4 | 2 | 3 |
| 3 | 2 | 3 | 5 | 1 | 4 |
| 4 | 3 | 5 | 1 | 4 | 2 |
| 5 | 1 | 4 | 2 | 3 | 5 |.

Then the row and column permutations are

$$
\begin{aligned}
& \sigma_{1}=(1,4,5), \sigma_{2}=(1,5,3,4,2), \sigma_{3}=(1,2,3,5,4), \\
& \sigma_{4}=(1,3)(, 2,5), \sigma_{5}=(2,4,3), \\
& \tau_{1}=(1,4,3,2.5), \tau_{2}=(1,2)(4,5), \tau_{3}=(1,3,5,2,4), \\
& \tau_{4}=(1,5,3), \tau_{5}=(2,3,4)
\end{aligned}
$$

A calculations by algorithm given in Figure 2 shows that the following commutators have fixed elements:

| commutators | fixed <br> elements | associative <br> triples | number of <br> associative <br> triples |
| :---: | :---: | :---: | :---: |
| $\left[\sigma_{1}^{-1}, \tau_{1}^{-1}\right]=(1,2,4)$ | $x_{3}, x_{5}$ | $\left(x_{1}, x_{3}, x_{1}\right),\left(x_{1}, x_{5}, x_{1}\right)$ | 2 |
| $\left[\sigma_{1}^{-1}, \tau_{2}^{-1}\right]=(1,5)(2,4)$ | $x_{3}$ | $\left(x_{1}, x_{3}, x_{2}\right)$ | 1 |
| $\left[\sigma_{1}^{-1}, \tau_{4}^{-1}\right]=(1,3)(4,5)$ | $x_{2}$ | $\left(x_{1}, x_{2}, x_{4}\right)$ | 1 |
| $\left[\sigma_{1}^{-1}, \tau_{5}^{-1}\right]=(1,3,4)$ | $x_{2}, x_{5}$ | $\left(x_{1}, x_{2}, x_{5}\right),\left(x_{1}, x_{5}, x_{5}\right)$ | 2 |
| $\left[\sigma_{2}^{-1}, \tau_{4}^{-1}\right]=(2,5,3)$ | $x_{1}, x_{4}$ | $\left(x_{2}, x_{1}, x_{4}\right),\left(x_{2}, x_{4}, x_{4}\right)$ | 2 |
| $\left.\left[\sigma_{2}^{-1}, \tau_{5}^{-1}\right]=(2,5,4)\right)$ | $x_{1}, x_{3}$ | $\left(x_{2}, x_{1}, x_{5}\right),\left(x_{2}, x_{3}, x_{5}\right)$ | 2 |
| $\left[\sigma_{4}^{-1}, \tau_{4}^{-1}\right]=(1,5)(2,3)$ | $x_{4}$ | $\left(x_{4}, x_{4}, x_{4}\right)$ | 1 |
| $\left[\sigma_{5}^{-1}, \tau_{1}^{-1}\right]=(1,2,3)$ | $x_{4}, x_{5}$ | $\left(x_{5}, x_{4}, x_{1}\right),\left(x_{5}, x_{5}, x_{1}\right)$ | 2 |
| $\left[\sigma_{5}^{-1}, \tau_{4}^{-1}\right]=(3,4,5)$ | $x_{1}, x_{2}$ | $\left(x_{5}, x_{1}, x_{4}\right),\left(x_{5}, x_{2}, x_{4}\right)$ | 2 |
| $\left[\sigma_{5}^{-1} \tau_{5}^{-1}\right]=\varepsilon$ | $x_{i}, \forall i$ | $\left(x_{5}, x_{i}, x_{5}\right) \forall i$ | 5 |

The total number of associative triples is equal to 20 . This algorithm can explicitly able to compute the associative triples of any finite order quasigroups and hence total number of associative triples. In our experiment we find the lowest number of associative triples for quasigroup of order 5 is 20.

In the following section we present experimental results of number of associative triples for all quasigroups of order 4 of different algebraic classes considered in [2].

## 6. Experimental results

The algorithm for derivation of associative triples of quasigroups of finite order is implemented. It has been succesfully applied on different order of quasigroups. From algebraic point of view we classify the the quasigroups of order 4 in four different classes [2] which are viz. (i) Simple and affine quasigroups (ii) Simple and non-affine quasigroups (Polynomially complete), (iii) Non-simple and affine quasigroups and (iv) Non-simple and non-affine quasigroups. Experiments are carried out on the set of all quasigroups of order 4 to find out the number of associative triples of different classes. Experimental results show that number of
associative triples are either 16 or 24 for simple cases and 32 or 64 for non-simple cases. So, 16 is the minimum number of associative triples of quasigroups of order 4 [9].

The table given below shows the number of quasigroups and corresponding associative triples of each class.

| Classes | Number of <br> quasigroups | Number of <br> associative triples |
| :---: | :---: | :---: |
| Simple and affine | 104 | 16 |
| Simple and non-affine | 240 | 16 |
| (polynomially complete) | 144 | 24 |
| Non-simple and affine | 48 | 32 |
|  | 8 | 64 |
| Non-simple and non-affine | 24 | 32 |
|  | 8 | 64 |

Figure 3: Associative triples of different classes of quasigroups of order 4
From algebraic point of view we know that cryptographic suitable quasigroups are polynomially complete [1]. Minimum number of associative triples is also an important algebraic property for good choice of cryptographic quasigroups. Experimental results show that cryptographic suitable quasigroups of order 4 are 240 beloging to the polynomially complete class. It is also observed that number of associative triples of non-simple quasigroups are always greater than simple quasigroups of order 4. Therefore, quasigroups belonging to the non-simple class are unsuitable for cryptographic purpose.

## 7. Acknowledgement

We are thankful to Dr. G.Athithan, DG (MED \& CoS), DRDO and Ms. Anu Khosla, Director SAG, DRDO for their support and encouragements to carry out the collaborative research work.

Our heartiest thanks to Professor Bimal K. Roy, ASU, ISI Kolkata for his support and hospitality.

Authors are also thankful to all professors of Indo-Russian joint project team for their technical support and cooperation.

## References

[1] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts. Quasigroups and Related Systems 21 (2013), 201 - 214.
[2] V.A. Artamonov, S. Chakrabarti, S.K. Pal, Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations, Discrete Appl. Math. 200 (2016), 5-17.
[3] V.D. Belousov, Foundations of the theory of quasigroups and loops, (Russian), Izdat. Nauka, Moscow, 1967.
[4] P.J. Cameron, Almost all quasigroups have rank 2, Discrete Math. 106/107 (1992), 111 - 115.
[5] J. Dénes, T. Dénes, Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack, Quasigroups and Related Topics, 8 (2001), 7-14.
[6] J. Dénes, A.D. Keedwell, A new authentication scheme based on Latin squares. Discrete Math. 106/107 (1992), 57-161.
[7] A. Drápal, On quasigroups rich in associative triples. Discrete Math. 44 (1983), 251-265.
[8] A. Drápal, T. Kepka, A note on the number of associative triples in quasigroups isotopic to groups. Comment. Math. Univ. Carol. 22 (1981), $735-743$.
[9] O. Grošek, P. Horák, On quasigroups with few associative triples. Des. Codes Cryptogr. 64 (2012), $221-227$.
[10] M.M. Glukhov, On application of quasigroups in cryptology, Applied Discrete Math. 2 (2008), 28 - 32.
[11] D. Gligoroski, S. Markovski, S.J. Knapskof, The stream cipher Edon-80, Lecture Notes Computer Sci. 4986 (2008), $152-169$.
[12] J. Hagemann, C. Herrmann, Arithmetically locally equational classes and representation of partial functions. Universal Algebra, Estergom (Hungary) 29, Colloq. Math. Soc. J. Bolyai, 1982, $345-360$.
[13] T. Ihringer, On multiplication groups of quasigroups, European J. Combin. 5 (1984), $137-141$.
[14] G.A. Jones, Primitive permutation groups containing a cycle, Bull. Aust. Math. Soc. 89 (2014), $159-165$.
[15] L. Guohao, Y. Xu, Cryptographic classification of quasigroups of order 4, Intern. Workshop on Cloud Computing and Information Security (2013), $278-281$.
[16] V.A. Shcherbacov, Quasigroups in cryptology, Computer Sci. J. Moldova 17 (2009), 193 - 227.
[17] K.K. Schukin, Simplicity of a quasigroup and primitivity of its of its multiplication group, Izv. Akad. Nauk. Mold. SSR. Mat. 3 (1990), $66-68$.
[18] J.D. Smith, Multiplication groups of quasigroups, Preprint No. 603, Technische Hochschule Darmstadt, 1981.

Received November 10, 2016
V.A. Artamonov

Faculty of Mchanics and Mathematics, Moscow Satate University, Leninsky Gory 1,
119992 Moscow, Russia
e-mail: artamon@mech.math.msu.su
S. Chakrabarti, S.K. Pal

Scientific Analysis Group, DRDO, India,
e-mail: suchetadrdo@hotmail.com, skptech@yahoo.com

# On some algebraic properties of order of an element of a multigroup 

Johnson Aderemi Awolola and Paul Augustine Ejegwa


#### Abstract

The concept of multigroups is a generalization of groups whereby the underlying structure is a multiset over a group $X$. As a continuation of the study of various algebraic structures of multisets, the concept of order of an element with respect to multigroup is introduced and some of its related results outlined. Also, the Lagrange's theorem for regular multigroup is described, and the restriction to regular multigroup makes the theorem flexible showing an analogy to that of group theory.


## 1. Introduction

The conception of multiset was introduced by N.G. de Bruijn under the idea of classical set theory. According to George Cantor,

By a set we are to understand any collection $M$ of definite and distinct objects $m$ of our intuition or thought (which will be called the "element" of M) into a whole.

One unavoidable consequence of Cantor's definition is that no element can occur more than once in a classical set. Indeed, this aspect of Cantorian set theory does not go hand in hand with many situations arising in solving real world problems. For example, the repeated roots of $x^{2}-2 x+1=0$, repeated observations in statistical samples, repeated hydrogen atoms in a water molecule, $\mathrm{H}_{2} \mathrm{O}$, etc. need to be considered significant. Once we admit the restriction of definiteness on the nature of objects forming a set, we have multisets. Details on fundamentals of multiset, multiset applications and various algebraic structures defined via multiset can be found in [3], [6], [7], [8], [9].

Very recently, [4] introduced multigroups as a natural generalization of the concept of groups which differs from the earlier definition given in [2], and established some of its fundamental properties. The recent definition of multigroup which follows [5] is adopted for the results presented in this paper. The aim of this paper is to present the notion of order of an element with respect to multigroup and outline some of its related results.

[^1]
## 2. Preliminaries

Definition 2.1. A multiset (mset) $A$ drawn from a crisp (ordinary) set $X$ is represented by a count function $C_{A}$ defined as $C_{A}: X \rightarrow D=\{0,1,2, \ldots\}$.

For $x \in X, C_{A}(x)$ denotes the number of times the element $x$ in the mset $A$ occurs. The representation of the mset $A$ drawn from $X=\left\{x_{1}, x_{2}, \ldots, x_{n}\right\}$ is

$$
\left[x_{1}, x_{2}, \ldots x_{n}\right]_{m_{1}, m_{2}, \ldots m_{n}}
$$

such that $x_{i}$ appears $m_{i}(i=1,2, \ldots, n)$ times in $A$.
Definition 2.2. An mset is called regular or constant if all its elements occur with the same multiplicity.

Definition 2.3. Let $X$ be a group. A multiset $A$ over $X$ is called a multigroup over $X$ if the count function $A$ or $C_{A}$ satisfies the following conditions.
(i) $C_{A}(x y) \geqslant C_{A}(x) \wedge C_{A}(y), \forall x, y \in X$,
(ii) $C_{A}\left(x^{-1}\right) \geqslant C_{A}(x), \forall x \in X$.

The set of all multigroups over $X$ is denoted by $M G(X)$.
If $A \in M G(X)$, it follows that $C_{A}\left(x^{-1}\right)=C_{A}(x)$ and $C_{A}(e) \geqslant C_{A}(x)$.
Definition 2.4. Let $H \in M G(X)$. For any $x \in X, x H$ and $H x$ defined by

$$
C_{x H}(y)=C_{H}\left(x^{-1} y\right)
$$

and

$$
C_{H x}(y)=C_{H}\left(y x^{-1}\right), \forall y \in X
$$

are respectively called the left and right mcosets of $H$ in $X$.
Definition 2.5. Let $A \in M G(X)$. Then $A$ is called regular if the count function $A$ occurs with the same multiplicity. The set of all regular multigroups over $X$ is denoted by $R M G(X)$.

Proposition 2.6. (cf. [4]) Let $A \in M G(X)$. Then the following assertions are equivalent.
(i) $C_{A}(x y)=C_{A}(y x), \forall x, y \in X$.
(ii) $C_{A}\left(x y x^{-1}\right)=C_{A}(y), \forall x, y \in X$.
(iii) $C_{A}\left(x y x^{-1}\right) \geqslant C_{A}(y), \forall x, y \in X$.
(iv) $C_{A}\left(x y x^{-1}\right) \leqslant C_{A}(y), \forall x, y \in X$.

Other definitions and facts one can find in [1].

## 3. Order of an element of a multigroup

Definition 3.7. Let $A \in M G(X)$ and $x \in X$. If there exists a positive integer $n$ such that $C_{A}\left(x^{n}\right)=C_{A}(e)$, then the least such positive integer is called the order of an element $x$ with respect to $A$. If no such $n$ exists, $x$ is said to be of infinite order with respect to $A$. The order of an element $x$ with respect to $A$ is denoted by $O_{A}(x)$.
Example 3.8. Let $X=(\mathbb{R}-\{0\}, \cdot)$ and $A=[1,-1]_{3,2}$. Then $C_{A}\left((-1)^{2}\right)=C_{A}(1)$. Therefore $O_{A}(-1)=2$. But for any $x \in \mathbb{R}-\{1,0,-1\}$, $\exists n \in \mathbb{Z}^{+}$such that $C_{A}\left(x^{n}\right)=C_{A}(1)$. Therefore $O_{A}(x)=\infty, \forall x \in \mathbb{R}-\{1,0,-1\}$.

Equality of $O(x)=O(y)$ does not imply $O_{A}(x)=O_{A}(y)$, as shown in the below.
Example 3.9. Let $\{e, a, b, c\}$ be the Klein's 4 -group and $A=[e, a, b, c]_{3,2,3,2}$.
Clearly, $O(a)=O(b)$ but $O_{A}(a)=2$ and $O_{A}(b)=1$, since $C_{A}(b)=C_{A}(e)$.
Remark 3.10. If $H=\left\{x \in X \mid C_{A}(x)=C_{A}(e)\right\} \leqslant X$, then $O_{A}(x)=\hbar$, the order of $x$ relative to $H$ (i.e., the smallest positive integer $n$ such that $x^{n} \in H$, if $\exists$ such a positive integer). In particular, if $H$ is trivial subgroup $\{e\}$ of $X$, then $O_{A}(x)=O(x)$, the (classical) order of $x$ in $X$.
Definition 3.11. Let $A \in M G(X)$. The order of $A$ denoted by $O(A)$ is defined as $O(A)=\Sigma_{x \in X} C_{A}(x)$, i.e., the total number of all multiplicities of its element.
Proposition 3.12. If $H \leqslant X$ and $A \in M G(X)$, then $O(A \mid H) \leqslant O(A)$, where $A \mid H$ means $A$ restricted to $H$.
Proof. Straightforward.
Proposition 3.13. (Lagrange's theorem for RMG)
Let $H \leqslant X, A \mid H \in R M G(H)$ and $A \in R M G(X)$. Then $O(A \mid H) \mid O(A)$.
Proof. Let $O(A)=n$. By Proposition 2.6, we have $O(A \mid H) \leqslant n$. If $O(A \mid H)=n$, then the result is trivial. Now, we assume that $O(A \mid H)<n$. Let $O(A \mid H)=m$, $\forall x \in H$. Then if $k$ is the count function of each left mcoset $A$ in $X$, then $O(A)=$ $C_{x A}(y) \cdot O(A \mid H) \forall y \in X$. By Lagrange's theorem for regular multigroup, $n \mid m$. Hence the proof.

Example 3.14. Consider the subgroup $H=\{1,-1\}$ of $X=\{1,-1, i,-i\}$ such that $A=[1,-1, i,-i]_{2,2,2,2}$ and $A \mid H=[1,-1]_{2,2}$. Then $O(A)=8, O(A \mid H)=4$ and $C_{i A}(-i)=C_{A}(1)=2$. Hence, $O(A \mid H) \mid O(A)$.
Corollary 3.15. If $H \leqslant X, x \in H$ and $A \mid H \in R M G(H)$, then $O_{A \mid H}(x) \mid O(A \mid H)$.
Proof. Since $A \mid H \in R M G(H)$, for some positive integer $m$ we have $C_{A \mid H}\left(x^{m}\right)=$ $C_{A \mid H}(e)$. Hence, $O_{A \mid H}(x)=m$. Now, $H$ is a subgroup of $X$ and $A \mid H \in R M G(H)$ such that $O(A \mid H)=n$. If for any $x \in H, r=C_{x(A \mid H)}(y)=C_{A \mid H}\left(x^{-1} y\right) \forall y \in H$, then $n=r m$. Hence $n \mid m$.

Proposition 3.16. Let $A \in M G(X)$. Then $O_{A}(x)=O_{A}\left(x^{-1}\right)$.
Proof. By definition, $O_{A}(x)=n$. So, $C_{A}\left(x^{n}\right)=C_{A}(e)$. Thus, $C_{A}\left(\left(x^{n}\right)^{-1}\right)=$ $C_{A}\left(e^{-1}\right)$, i.e., $C_{A}\left(\left(x^{-1}\right)^{n}\right)=C_{A}(e)$, which implies $O_{A}\left(x^{-1}\right) \geqslant n$. Hence $m \geqslant n$.

Also, $O_{A}\left(x^{-1}\right)=m$ implies $C_{A}\left(\left(x^{-1}\right)^{m}\right)=C_{A}(e)$. So, $C_{A}\left(\left(x^{m}\right)^{-1}\right)=C_{A}(e)$, i.e., $C_{A}\left(x^{m}\right)=C_{A}(e)$. Thus, $O_{A}(x) \geqslant m$. Hence $n \geqslant m$. Therefore, $n=m$.

Proposition 3.17. If $x \in X$ and $A \in M G(X)$ such that $O(A)$ is even, then $C_{A}\left(x^{O(A)}\right)=C_{A}(e)$.

Proof. Let $O_{A}(x)=n$. Then $O(A)=m \cdot O_{A}(x)$, where

$$
x^{O(A)}=x^{m} \cdot O_{A}(x)=\left(x^{n}\right)^{m} .
$$

Then

$$
C_{A}\left(x^{O(A)}\right)=C_{A}\left(\left(X^{n}\right)^{m}\right) \geqslant C_{A}\left(x^{n}\right)=C_{A}(e) .
$$

Therefore, $C_{A}\left(x^{O(A)}\right) \geqslant C_{A}(e)$.
Since $A \in M G(X)$, then $C_{A}(e) \geqslant C_{A}(y) \forall y \in X$. So, $C_{A}\left(x^{O(A)}\right) \leqslant C_{A}(e)$. Hence, $C_{A}\left(x^{O(A)}\right)=C_{A}(e)$.

Proposition 3.18. Let $A \in M G(X)$ and $x \in X$. If there exists $m \in \mathbb{Z}^{+}$, such that $C_{A}\left(x^{m}\right)=C_{A}(e)$, then $O_{A}(x) \mid m$.

Proof. Let $O_{A}(x)=n$. By division algorithm, there exists integers $s$ and $t$ such that $m=n s+t, 0 \leqslant t<n$. Then

$$
\begin{aligned}
C_{A}\left(x^{t}\right)=C_{A}\left(x^{m-n s}\right) & =C_{A}\left(x^{m}\left(x^{n}\right)^{-s}\right) \geqslant C_{A}\left(x^{m}\right) \wedge C_{A}\left(\left(x^{n}\right)^{-s}\right) \\
& =C_{A}(e) \wedge C_{A}\left(\left(x^{n s}\right)^{-1}\right)=C_{A}\left(\left(x^{n s}\right)^{-1}\right) \\
& =C_{A}\left(x^{n s}\right)=C_{A}\left(\left(x^{n}\right)^{s}\right) \geqslant C_{A}\left(x^{n}\right)=C_{A}(e)
\end{aligned}
$$

Thus, $C_{A}\left(x^{t}\right)=C_{A}(e)$. Hence, $t=0$ by minimality of $n$, i.e., $m=n s$.
Proposition 3.19. Let $A \in M G(X)$ and let $x, y \in X$ be such that $\left(O_{A}(x), O_{A}(y)\right)$ $=1$ and $x y=y x$. If $C_{A}(x y)=C_{A}(e)$, then $C_{A}(x)=C_{A}(y)=C_{A}(e)$.

Proof. Let $O_{A}(x)=n$ and $O_{A}(y)=m$. Then

$$
C_{A}(e)=C_{A}(x y) \leqslant C_{A}\left((x y)^{m}\right)=C_{A}\left(x^{m} y^{m}\right) .
$$

Hence, $C_{A}\left(x^{m} y^{m}\right)=C_{A}(e)$. Now,

$$
C_{A}\left(x^{m}\right)=C_{A}\left(x^{m} y^{m} y^{-m}\right) \geqslant C_{A}\left(x^{m} y^{m}\right) \wedge C_{A}\left(y^{-m}\right)=C_{A}(e) \wedge C_{A}(e)=C_{A}(e) .
$$

Thus, $C_{A}\left(x^{m}\right)=C_{A}\left(y^{m}\right)=C_{A}(e)$. Therefore, $n \mid m$ by Proposition 3.18. But $(n, m)=1$. Thus, $n=1$ i.e., $C_{A}(x)=C_{A}\left(x^{n}\right)=C_{A}(e)$. Similarly, $C_{A}(y)=$ $C_{A}(e)$.

Proposition 3.20. Let $A \in M G(X)$. Then $O_{A}\left(x^{m}\right) \leqslant O_{A}(x)$.

Proof. By definition, $O_{A}(x)=n$ means $C_{A}\left(x^{n}\right)=C_{A}(e)$. Then $C_{A}\left(\left(x^{n}\right)^{m}\right)=$ $C_{A}\left(e^{m}\right)$, hence $C_{A}\left(x^{n m}\right)=C_{A}(e)$. So, $C_{A}\left(\left(x^{m}\right)^{n}\right)=C_{A}(e)$, i.e, $O_{A}\left(x^{m}\right) \leqslant n$. Consequently, $O_{A}\left(x^{m}\right) \leqslant O_{A}(x)$.

Proposition 3.21. Let $A \in M G(X)$. Then $O_{A}\left(x y x^{-1}\right) \leqslant O_{A}(y)$.
Proof. Let $O_{A}\left(x y x^{-1}\right)=m$ and $O_{A}(y)=n$. Then

$$
\begin{aligned}
C_{A}\left(\left(x y x^{-1}\right)^{2}\right) & =C_{A}\left(\left(x y x^{-1}\right)\left(x y x^{-1}\right)\right)=C_{A}\left(x y\left(x^{-1} x\right) y x^{-1}\right) \\
& =C_{A}\left(x(y e) y x^{-1}\right)=C_{A}\left(x y^{2} x^{-1}\right) .
\end{aligned}
$$

In general, $C_{A}\left(\left(x y x^{-1}\right)^{n}\right)=C_{A}\left(x y^{n} x^{-1}\right) \leqslant C_{A}\left(y^{n}\right)=C_{A}(e)=O_{A}(y)$.
Remark 3.22. If $A \in M G(X)$, then $O_{A}\left(x y x^{-1}\right)=O_{A}(y)$.
Proposition 3.23. Let $A \in M G(X)$ and $O_{A}(x)=n$, where $x \in X$. If $m \in \mathbb{Z}$ with $(m, n)=d$, then $O_{A}\left(x^{m}\right)=\frac{n}{d}$.

Proof. Let $O_{A}\left(x^{m}\right)=t$. Now, for $\frac{m}{d}=k \in \mathbb{Z}^{+}$,

$$
C_{A}\left(\left(x^{m}\right)^{\frac{n}{d}}\right)=C_{A}\left(x^{n k}\right) \geqslant C_{A}\left(x^{n}\right)=C_{A}(e) .
$$

By Proposition 3.18, $t \left\lvert\,\left(\frac{n}{d}\right)\right.$. Since $(m, n)=d$, then $\exists i, j \in \mathbb{Z}$ such that $n i+m j=d$. Therefore,

$$
\begin{aligned}
C_{A}\left(x^{t d}\right)=C_{A}\left(x^{t(n i+m j}\right) & \geqslant C_{A}\left(\left(x^{n}\right)^{t i}\right) \wedge C_{A}\left(\left(\left(x^{m}\right)^{t}\right)^{j}\right) \\
& \geqslant C_{A}\left(x^{n}\right) \wedge C_{A}\left(\left(x^{m}\right)^{t}\right) \\
& \geqslant C_{A}(e) \wedge C_{A}(e)=C_{A}(e)
\end{aligned}
$$

Thus, $n \left\lvert\,\left(\frac{t}{d}\right)\right.$ by Proposition 3.18, this implies $\left.\left(\frac{n}{d}\right) \right\rvert\, t$, consequently $t=\frac{n}{d}$.
Putting in the above Proposition $d=1$ we obtain
Corollary 3.24. Let $A \in M G(X)$ and $O_{A}(x)=n$, where $x \in X$. If $m \in \mathbb{Z}$ with $(m, n)=1$, then $O_{A}\left(x^{m}\right)=O_{A}(x)$.

Proposition 3.25. Let $A \in M G(X)$ and $O_{A}(x)=n$, where $x \in X$. Then for all $i \equiv j(\bmod n), i, j \in \mathbb{Z}$, we have $O_{A}\left(x^{i}\right)=O_{A}\left(x^{j}\right)$.
Proof. Let $O_{A}\left(x^{i}\right)=t$ and $O_{A}\left(x^{j}\right)=s$. Assume $i=j+n k$ and $k \in \mathbb{Z}$. Then

$$
\begin{aligned}
C_{A}\left(\left(x^{i}\right)^{s}\right)=C_{A}\left(\left(x^{j+n k}\right)^{s}\right) & \geqslant C_{A}\left(\left(x^{j}\right)^{s}\right) \wedge C_{A}\left(\left(x^{n}\right)^{k s}\right) \\
& \geqslant C_{A}(e) \wedge C_{A}(e)=C_{A}(e)
\end{aligned}
$$

implies $C_{A}\left(\left(x^{i}\right)^{s}\right)=C_{A}(e)$. Therefore, $t \mid s$. Similarly, by $C_{A}\left(\left(x^{j}\right)^{t}\right)=C_{A}(e)$ we obtain $s \mid t$. Thus, $t=s$.

## References

[1] J.A. Awolola and A.M. Ibrahimm Some results on multigroups, Quasigroups and Related Systems 24 (2016), $169-177$.
[2] M. Dresher and O. Ore, Theory of multigroups, American J. Math. 60 (1938), $705-733$.
[3] K.P. Girish and J.J. Sunil, On multiset topolpgies, Theory Appl. Math. Computer Sci. 2 (2013), $37-52$.
[4] Sk. Nazmul, P. Majumdar and S.K. Samanta, On multisets and multigroups, Annals Fuzzy Math. Inform. 6 (2013), 643 - 656.
[5] A. Rosenfeld, Fuzzy groups, J. Math. Analysis and Appl. 35 (1971), 512 - 517.
[6] D. Singh, A.M. Ibrahim, T. Yohanna and J.N. Singh, An overview of the application of multisets, Novi Sad J. Math. 33 (2007), no. 2, $73-92$.
[7] D. Singh, A.M. Ibrahim, T. Yohanna and J.N. Singh, A systematization of fundamentals of multisets, Lecturas Matematicas 29 (2008), 33-48.
[8] A. Syropoulous, Mathematics of multisets, Springer-Verlag Berlin Heidelberge, (2001), 347 - 358.
[9] Y. Tella and S. Daniel, Symmetry groups under multiset perspective, IOSR J. Math. 7 (2013) , no. 5, $47-52$.

Department of Mathematics/Statistics/Computer Science
University of Agriculture, P.M.B. 2373
Makurdi, Nigeria
E-mails: remsonjay@yahoo.com (J.A. Awolola), ejegwa.augustine@uam.edu.ng (P.A. Ejegwa)

# Nilpotency of $g b$-triple systems 

Guy Roger Biyogmam


#### Abstract

Leibniz algebras (which includes Lie algebras) to ternary algebras. In this paper, we extend several results established on nilpotent Lie algebras to $g b$-triple systems. In particular we prove an analogue of Engel's theorem for $g b$ triple systems and establish some properties of nilpotent $g b$-triple systems in connection with their Frattini ideal. Also, we show the invariance of the nilradical under derivations.


## 1. Introduction

In recent years, Lie algebras have been generalized to several algebraic structures endowed with a multilinear operation. In particular, 3-Lie algebras [12] and Lie triple systems $[8,14]$ are generalizations of Lie algebras to ternary algebras. Another ternary algebra in this picture is Leibniz 3-algebras [10] which generalizes Leibniz algebras introduced by J. L. Loday [17] as a non commutative version of Lie algebras. A considerable amount of research (see [2, 3, 9, 11, 16]) has been devoted in extending classical theorems of Lie algebras to these generalizations. This paper is a continuation of investigations on $g b$-triple systems; a new algebraic structure recently introduced in [6] as another generalization of Leibniz algebras to ternary operations, and further investigated in [7].

Our purpose in this work is the study of nilpotency on $g b$-triple systems. In Section 3 we introduce the Frattini subalgebra and ideal of $g b$-triple systems and extend their classical properties known on Lie algebras to $g b$-triple systems. In Section 4 , we prove that a $g b$-triple system $\mathfrak{g}$ for which the Frattini ideal $\phi(\mathfrak{g})$ is a 3 -sided ideal is nilpotent if and only if the quotient $g b$-triple system $\mathfrak{g} / \phi(\mathfrak{g})$ is nilpotent. We also prove an analogue of Engel's theorem for $g b$-triple systems, thanks to the fact that the bracket operator generates the Lie algebra of inner derivations as in the case of all algebras mentioned above. In Section 5, we show that the nilradical 2-sided (right) ideal of a $g b$-triple system is invariant under derivations.

For the remainder of this paper, we assume that $\mathfrak{K}$ is a field of characteristic different to 2 , all tensor products are taken over $\mathfrak{K}$ and all algebras are finite dimensional.

2010 Mathematics Subject Classification: 17A30, 17A32, 17A40
Keywords: Triple systems, Leibniz 3-algebras, Leibniz algebras, nilpotency.

## 2. gb-triple systems

In this section, we recall preliminaries about $g b$-triple systems and define the quotient $g b$-triple system.

Definition 2.1. (cf. [6]) A gb-triple system is a $\mathfrak{K}$-vector space $\mathfrak{g}$ equipped with a trilinear operation $[-,-,-]_{\mathfrak{g}}: \mathfrak{g}^{\times 3} \longrightarrow \mathfrak{g}$ satisfying the identity

$$
\begin{equation*}
\left[x, y,[a, b, c]_{\mathfrak{g}}\right]_{\mathfrak{g}}=\left[a,[x, y, b]_{\mathfrak{g}}, c\right]_{\mathfrak{g}}-\left[[a, x, c]_{\mathfrak{g}}, y, b\right]_{\mathfrak{g}}-\left[x,[a, y, c]_{\mathfrak{g}}, b\right]_{\mathfrak{g}} . \tag{2.1}
\end{equation*}
$$

Definition 2.2. (cf. [6]) Let $\left(\mathfrak{g},[-,-,-]_{\mathfrak{g}}\right)$ be a $g b$-triple system. A subspace $S$ of $\mathfrak{g}$ is a subalgebra of $\mathfrak{g}$ if $\left(S,[-,-,-]_{\mathfrak{g}}\right)$ be a $g b$-triple system.

Example 2.3. See Example 2 and Example 8 in [6].
Definition 2.4. (cf. [6]) A subalgebra $\mathfrak{I}$ of a $g b$-triple system $\mathfrak{g}$ is called ideal (resp. left ideal, right ideal) of $\mathfrak{g}$ if it satisfies the condition $[\mathfrak{g}, \mathfrak{I}, \mathfrak{g}]_{\mathfrak{g}} \subseteq \mathfrak{I}$ (resp. $[\mathfrak{g}, \mathfrak{g}, \mathfrak{I}]_{\mathfrak{g}} \subseteq \mathfrak{I}$, resp. $\left.[\mathfrak{I}, \mathfrak{g}, \mathfrak{g}]_{\mathfrak{g}} \subseteq \mathfrak{I}\right)$. If $\mathfrak{I}$ satisfies these three conditions, then $\mathfrak{I}$ is called a 3-sided ideal.

Remark 2.5. (cf. [6]) If $S$ is a subalgebra of a $g b$-triple system $\mathfrak{g}$, then the left normalizer

$$
\mathfrak{N}_{\mathfrak{g}}^{l}(S):=\left\{x \in \mathfrak{g}: \quad[x, S, \mathfrak{g}]_{\mathfrak{g}} \subseteq S\right\}
$$

and the right normalizer

$$
\mathfrak{N}_{\mathfrak{g}}^{r}(S):=\left\{x \in \mathfrak{g}:[\mathfrak{g}, S, x]_{\mathfrak{g}} \subseteq S\right\}
$$

of $S$ in $\mathfrak{g}$ are also subalgebras of $\mathfrak{g}$. Note that this statement is not true for Leibniz algebras since the right normalizer of a subalgebra of a (left) Leibniz algebra need not be a subalgebra (see [5, Example 1.7]).

Moreover, $S$ is an ideal of $\mathfrak{g}$ if and only if $\mathfrak{N}_{\mathfrak{g}}^{l}(S)=\mathfrak{g}=\mathfrak{N}_{\mathfrak{g}}^{r}(S)$.
Definition 2.6. (cf. [6]) Given a $g b$-triple system $\mathfrak{g}$, the center $Z(\mathfrak{g})$ and the derived algebra of $\mathfrak{g}$ are defined respectively by

$$
Z(\mathfrak{g})=\left\{x \in \mathfrak{g}:[\mathfrak{g}, x, \mathfrak{g}]_{\mathfrak{g}}=0\right\}
$$

and

$$
[\mathfrak{g}, \mathfrak{g}, \mathfrak{g}]=\left\{\left[a_{1}, a_{2}, a_{3}\right]_{\mathfrak{g}}, a_{1}, a_{2}, a_{3} \in \mathfrak{g}\right\} .
$$

$\mathfrak{g}$ is said to be perfect if $[\mathfrak{g}, \mathfrak{g}, \mathfrak{g}]_{\mathfrak{g}}=\mathfrak{g}$, and abelian if $[\mathfrak{g}, \mathfrak{g}, \mathfrak{g}]_{\mathfrak{g}}=0$.
Definition 2.7. The full center $Z_{f}(\mathfrak{g})$ of a $g b$-triple system $\mathfrak{g}$ is defined by

$$
Z_{f}(\mathfrak{g})=Z(\mathfrak{g}) \cap\left\{x \in \mathfrak{g}:[\mathfrak{g}, \mathfrak{g}, x]_{\mathfrak{g}}=0 \text { and }[x, \mathfrak{g}, \mathfrak{g}]_{\mathfrak{g}}=0\right\}
$$

The following result is straightforward.
Proposition 2.8. A gb-triple system $\mathfrak{g}$ is abelian if and only if $Z_{f}(\mathfrak{g})=\mathfrak{g}$.
Note that $Z(\mathfrak{g})$ is an ideal of $\mathfrak{g}$ while $Z_{f}(\mathfrak{g})$ and $[\mathfrak{g}, \mathfrak{g}, \mathfrak{g}]_{\mathfrak{g}}$ are 3 -sided ideals of $\mathfrak{g}$. Let $\mathfrak{I}$ be a 3 -sided ideal of a $g b$-triple system $\mathfrak{g}$. Then the quotient space $\mathfrak{g} / \mathfrak{I}$ has a natural $g b$-triple system structure given by the bracket

$$
\begin{equation*}
[x+\mathfrak{I}, y+\mathfrak{I}, z+\mathfrak{I}]_{\mathfrak{g} / \mathfrak{I}}=[x, y, z]+\mathfrak{I} . \tag{2.2}
\end{equation*}
$$

Notice that if $x+\mathfrak{I}=x^{\prime}+\mathfrak{I}, y+\mathfrak{I}=y^{\prime}+\mathfrak{I}$ and $z+\mathfrak{I}=z^{\prime}+\mathfrak{I}$, then

$$
\begin{aligned}
{[x, y, z]_{\mathfrak{g}}=} & {\left[x^{\prime}+\left(x-x^{\prime}\right), y^{\prime}+\left(y-y^{\prime}\right), z^{\prime}+\left(z-z^{\prime}\right)\right]_{\mathfrak{g}} } \\
= & {\left[x^{\prime}, y^{\prime}, z^{\prime}\right]_{\mathfrak{g}}+\left[x^{\prime}+\left(x-x^{\prime}\right), y-y^{\prime}, z^{\prime}+\left(z-z^{\prime}\right)\right]_{\mathfrak{g}} } \\
& +\left[\left(x-x^{\prime}\right), y^{\prime}, z^{\prime}+\left(z-z^{\prime}\right)\right]_{\mathfrak{g}}+\left[x^{\prime}, y^{\prime},\left(z-z^{\prime}\right)\right]_{\mathfrak{g}}
\end{aligned}
$$

and thus $[x, y, z]_{\mathfrak{g}}+\mathfrak{I}=\left[x^{\prime}, y^{\prime}, z^{\prime}\right]_{\mathfrak{g}}+\mathfrak{I}$ since $x-x^{\prime} \in \mathfrak{I}, y-y^{\prime} \in \mathfrak{I}$ and $z-z^{\prime} \in \mathfrak{I}$ as $\mathfrak{I}$ is a 3 -sided ideal. That the bracket (2.2) satisfies the identity (2.1) follows by definition.

Definition 2.9. $\mathfrak{g} / \mathfrak{I}$ endowed with the bracket (2.2) is called quotient gb-triple system of $\mathfrak{g}$ by $\mathfrak{I}$.

Recall that if $V$ is a vector space endowed with a trilinear operation $\sigma: V \times$ $V \times V \longrightarrow V$, then a map $d: V \longrightarrow V$ is called a derivation with respect to $\sigma$ if

$$
\begin{equation*}
d(\sigma(x, y, z))=\sigma(d(x), y, z)+\sigma(x, d(y), z)+\sigma(x, y, d(z)) \tag{2.3}
\end{equation*}
$$

Remark 2.10. Let $\mathfrak{g}$ be a $g b$-triple system. Then by [7, Remark 3.9], the Lie algebra $\operatorname{Der}(\mathfrak{g})$ of derivations of $\mathfrak{g}$ has a $g b$-triple system structure when endowed with the bracket

$$
\left\{d_{1}, d_{2}, d_{3}\right\}=\left[d_{2},\left[d_{1}, d_{3}\right]_{\operatorname{Der}(\mathfrak{g})}\right]_{\operatorname{Der}(\mathfrak{g})} .
$$

Remark 2.11. For every derivation $d$ of $\mathfrak{g}$ and $x, y, y^{\prime}, z \in \mathfrak{g}$, it follows by (2.3) and by setting $\sigma=[-,-,-]_{\mathfrak{g}}$ that

$$
\left[x, y+d\left(y^{\prime}\right), z\right]_{\mathfrak{g}}=[x, y, z]_{\mathfrak{g}}-\left[d(x), y^{\prime}, z\right]_{\mathfrak{g}}-\left[x, y^{\prime}, d(z)\right]_{\mathfrak{g}}+d\left(\left[x, y^{\prime}, z\right]_{\mathfrak{g}}\right)
$$

So if $\mathfrak{I}$ is an ideal of $\mathfrak{g}$, then $\mathfrak{I}+d(\mathfrak{I})$ is also an ideal of $\mathfrak{g}$.

## 3. The Frattini subalgebra of $g b$-triple systems

This section is devoted to the introduction of the Frattini subalgebra and Frattini ideal of $g b$-triple systems.

Definition 3.1. A maximal subalgebra $\mathfrak{m}$ of a $g b$-triple system $\mathfrak{g}$ is a proper subalgebra of $\mathfrak{g}$ such that no proper subalgebra $S$ strictly contains $\mathfrak{m}$.

Remark 3.2. Let $\mathfrak{m}$ be a maximal left ideal of a $g b$-triple system $\mathfrak{g}$. Then as $\mathfrak{m}$ is a left ideal of $\mathfrak{g}, \mathfrak{m} \subseteq \mathfrak{N}_{\mathfrak{g}}^{r}(\mathfrak{m})$. Now since $\mathfrak{m}$ is maximal, then $\mathfrak{N}_{\mathfrak{g}}^{r}(\mathfrak{m})=\mathfrak{m}$ or $\mathfrak{N}_{\mathfrak{g}}^{r}(\mathfrak{m})=\mathfrak{g}$.
Definition 3.3. The intersection of all maximal subalgebras of a $g b$-triple system $\mathfrak{g}$ is the subalgebra $F(\mathfrak{g})$ of $\mathfrak{g}$ called the Frattini subalgebra.

Definition 3.4. The largest ideal of a $g b$-triple system $\mathfrak{g}$ contained in $F(\mathfrak{g})$ is denoted $\phi(\mathfrak{g})$ and called the Frattini ideal of $\mathfrak{g}$.

Proposition 3.5. Let $\mathfrak{g}$ be a non perfect gb-triple system. Then $F(\mathfrak{g}) \subseteq[\mathfrak{g}, \mathfrak{g}, \mathfrak{g}]_{\mathfrak{g}}$. In particular, $F(\mathfrak{g})=0$ if $\mathfrak{g}$ is abelian.

Proof. By contradiction, let $x \in F(\mathfrak{g})$ with $x \notin[\mathfrak{g}, \mathfrak{g}, \mathfrak{g}]_{\mathfrak{g}}$. Any subalgebra $S$ of $\mathfrak{g}$ with dimension $\operatorname{dim} \mathfrak{g}-1$ containing $[\mathfrak{g}, \mathfrak{g}, \mathfrak{g}]_{\mathfrak{g}}$ and with $x \notin S$ is a maximal subalgebra of $\mathfrak{g}$. A contradiction with $x \in F(\mathfrak{g})$.

Following the proofs of [2, Propositions 2.1, 2.2, 2.4], it is easy to show that the following statements which hold for Leibniz 3-algebras also hold for $g b$-triple systems.

Proposition 3.6. Let $\mathfrak{g}$ be a gb-triple system and $\mathfrak{I}$ an ideal of $\mathfrak{g}$. Then there are proper subalgebras Sand $S^{\prime}$ of $\mathfrak{g}$ such
(1) $\mathfrak{g}=\mathfrak{I}+S$ iff $\mathfrak{I}$ is not contained in $F(\mathfrak{g})$.
(2) $\mathfrak{g}=\mathfrak{I}+S^{\prime}$ iff $\mathfrak{I}$ is not contained in $\phi(\mathfrak{g})$.

Proposition 3.7. Let $\mathfrak{g}$ be a gb-triple system, $\mathfrak{I}$ an ideal of $\mathfrak{g}$ and $S$ a subalgebra of $\mathfrak{g}$. Then the following statements hold:
(1) If $S+F(\mathfrak{g})=\mathfrak{g}$, then $S=\mathfrak{g}$.
(2) If $S+\phi(\mathfrak{g})=\mathfrak{g}$, then $S=\mathfrak{g}$.
(3) If $\mathfrak{I} \subseteq F(S)$, then $\mathfrak{I} \subseteq F(\mathfrak{g})$.
(4) If $\mathfrak{I} \subseteq \phi(S)$, then $\mathfrak{I} \subseteq \phi(\mathfrak{g})$.
(5) If $F(S)$ is an ideal of $\mathfrak{g}$, then $F(S) \subseteq F(\mathfrak{g})$.
(6) If $\phi(S)$ is an ideal of $\mathfrak{g}$, then $\phi(S) \subseteq \phi(\mathfrak{g})$.
(7) $(F(\mathfrak{g})+\mathfrak{I}) / \mathfrak{I} \subseteq F(\mathfrak{g} / \mathfrak{I})$.
(8) $(\phi(\mathfrak{g})+\mathfrak{I}) / \mathfrak{I} \subseteq \phi(\mathfrak{g} / \mathfrak{I})$.
(9) If $\mathfrak{I} \subseteq F(\mathfrak{g})$, then $F(\mathfrak{g}) / \mathfrak{I}=F(\mathfrak{g} / \mathfrak{I})$.
(10) If $\mathfrak{I} \subseteq \phi(\mathfrak{g})$, then $\phi(\mathfrak{g}) / \mathfrak{I}=\phi(\mathfrak{g} / \mathfrak{I})$.
(11) If $F(\mathfrak{g} / \mathfrak{I})=0$, then $F(\mathfrak{g}) \subseteq \mathfrak{I}$.
(12) If $\phi(\mathfrak{g} / \mathfrak{I})=0$, then $\phi(\mathfrak{g}) \subseteq \mathfrak{I}$.
(13) If $S$ is minimal with respect to $\mathfrak{g}=\mathfrak{I}+S$, then $\mathfrak{I} \cap S \subseteq \mathfrak{g}$.
(14) If $\mathfrak{I}$ is abelian and $\mathfrak{I} \cap \phi(\mathfrak{g})=0$, then $\mathfrak{g}=\mathfrak{I}+K$ for some subalgebra $K$ of $\mathfrak{g}$.

Proof. The proof is similar to the case of Lie 3-algebras (see [2]).

## 4. Nilpotency of $g b$-triple systems

### 4.1. Definition and Examples

Definition 4.1. The lower central series of a $g b$-triple system $\mathfrak{g}$ is the sequence of subalgebras defined by $\mathfrak{g}^{(s+1)}=\left[\mathfrak{g}, \mathfrak{g}^{(s)}, \mathfrak{g}\right]$ with $\mathfrak{g}^{(1)}=\mathfrak{g}$.

A $g b$-triple system $\mathfrak{g}$ is nilpotent if this sequence terminates, i.e., $\mathfrak{g}^{(s)}=0$ for some positive integer $s$. The smallest of such values $s$ is called class of nilpotency of $\mathfrak{g}$.

Remark 4.2. Let $\mathfrak{g}$ be a nontrivial nilpotent $g b$-triple system of class $s$. Then the following holds.
(1) $\mathfrak{g}$ has a non trivial center. Indeed, since there is some positive integer $s$ such that $\mathfrak{g}^{(s)}=0$ i.e. $\left[\mathfrak{g}, \mathfrak{g}^{(s-1)}, \mathfrak{g}\right]_{\mathfrak{g}}=0$, it follows that $\mathfrak{g}^{(s-1)} \subseteq Z(\mathfrak{g})$.
(2) $\mathfrak{g}$ is abelian if and only if its class is $s=2$.

Proposition 4.3. Let $\mathfrak{g}$ be a gb-triple system. Then $\mathfrak{g}$ is nilpotent if and only if $\mathfrak{g} / Z_{f}(\mathfrak{g})$ is nilpotent
Proof. If $\mathfrak{g}$ is nilpotent of class $s$, then $\left[\mathfrak{g}, \mathfrak{g}^{(s-1)}, \mathfrak{g}\right]_{\mathfrak{g}}=\mathfrak{g}^{(s)}=0$. Using (2.2), it is easy to show that $\left(\mathfrak{g} / Z_{f}(\mathfrak{g})\right)^{(s)}=\mathfrak{g}^{(s)} / Z_{f}(\mathfrak{g})=Z_{f}(\mathfrak{g})$. Therefore $\mathfrak{g} / Z_{f}(\mathfrak{g})$ is nilpotent. Conversely, if $\mathfrak{g} / Z_{f}(\mathfrak{g})$ is nilpotent of class $s$, then $\mathfrak{g}^{(s)} / Z_{f}(\mathfrak{g})=$ $\left(\mathfrak{g} / Z_{f}(\mathfrak{g})\right)^{(s)}=Z_{f}(\mathfrak{g})$. This implies that $\mathfrak{g}^{(s)} \subseteq Z_{f}(\mathfrak{g})$. So $\mathfrak{g}^{(s+1)}=\left[\mathfrak{g}, \mathfrak{g}^{(s)}, \mathfrak{g}\right]_{\mathfrak{g}} \subseteq$ $\left[\mathfrak{g}, Z_{f}(\mathfrak{g}), \mathfrak{g}\right]_{\mathfrak{g}}=0$. Hence $\mathfrak{g}$ is nilpotent.

It is worth mentioning that the above definition of nilpotency appears to extend the definition of nilpotency for both left and right Leibniz algebras [11].

The following theorem classifies a subfamily of two dimensional nilpotent complex $g b$-triple systems.

Theorem 4.4. Up to isomorphisms, there are three two-dimensional nilpotent complex gb-triple systems with one dimensional derived algebra.

Proof. Among the seven two-dimensional complex $g b$-triple systems with one dimensional derived algebra established in the proof of [6, Theorem 11], only the following are nilpotent, all with class of nilotency $s=3$.

$$
\begin{aligned}
& \mathfrak{g}_{2}:\left[a_{i}, a_{j}, a_{k}\right]_{\mathfrak{g}}= \begin{cases}\alpha a_{1}, & \text { if } i, j, k=2 \\
0, & \text { else }\end{cases} \\
& \mathfrak{g}_{3}:\left[a_{i}, a_{j}, a_{k}\right]_{\mathfrak{g}}= \begin{cases}a_{1}, & \text { if } i=1, j, k=2 \\
-a_{1}, & \text { if } i, j=2, k=1 \\
0, & \text { else }\end{cases} \\
& \mathfrak{g}_{6}:\left[a_{i}, a_{j}, a_{k}\right]_{\mathfrak{g}}= \begin{cases}a_{1}, & \text { if } i=1, j, k=2 \\
-a_{1}, & \text { if } i, j=2, k=1 \\
\alpha a_{1}, & \text { if } i, j, k=2 \\
0, & \text { else }\end{cases}
\end{aligned}
$$

with $\alpha \neq 0$.
It was shown in [3] that every maximal subalgebra $\mathfrak{m}$ of a nilpotent 3-Lie algebra $L$ is an ideal of $L$. The following example shows that this statement does not hold for $g b$-triple systems, and Corollary 4.7 shows that the result holds if $\mathfrak{m}$ is a maximal left ideal (or right ideal).

Example 4.5. Consider the nilpotent $g b$-triple system $\mathfrak{g}_{3}$ above with basis $\left\{a_{1}, a_{2}\right\}$. The one-dimensional subspace with basis $\left\{a_{2}\right\}$ is a maximal subalgebra of $\mathfrak{g}_{3}$, but not an ideal of $\mathfrak{g}_{3}$ since $\left[a_{1}, a_{2}, a_{2}\right]_{\mathfrak{g}}=a_{1} \notin<a_{2}>$.

As in Lie algebras, we say that a $g b$-triple system $\mathfrak{g}$ satisfies the right normalizer condition if there is no proper subalgebra $S$ of $\mathfrak{g}$ such that $\mathfrak{N}_{\mathfrak{g}}^{r}(S)=S$. The following result which holds for groups and Leibniz algebras also holds $g b$-triple systems, and the proof is similar.

Proposition 4.6. Nilpotent gb-triple systems satisfy the right normalizer condition.

Corollary 4.7. If $\mathfrak{m}$ is a maximal left or rihgt ideal of a nilpotent gb-triple system $\mathfrak{g}$, then $\mathfrak{m}$ is an ideal of $\mathfrak{g}$.

Proof. Since $\mathfrak{g}$ is nilpotent, it follows from Proposition 4.6 that $\mathfrak{m} \neq \mathfrak{N}_{\mathfrak{g}}^{r}(\mathfrak{m})$. So by Remark 3.2, $\mathfrak{N}_{\mathfrak{g}}^{r}(\mathfrak{m})=\mathfrak{g}$. Hence $\mathfrak{m}$ is an ideal of $\mathfrak{g}$.

### 4.2. Engel's Theorem for $g b$-triple systems

Definition 4.8. (cf. [17]) A Leibniz algebra (sometimes called a Loday algebra, named after Jean-Louis Loday) is a $\mathfrak{K}$ vector space $L$ with a bilinear product $[-,-]$ satisfying the Leibniz identity

$$
\begin{equation*}
[x,[y, z]]=[[x, y] z]+[y,[x, z]] \tag{4.1}
\end{equation*}
$$

A Leibniz algebra $L$ is nilpotent if $L^{<s>}=0$ for some positive integer $s$, where $L^{<1>}=L$ and $L^{<s+1>}=\left[L, L^{<s>}\right]$. A 2-sided ideal of $L$ is a subalgebra $I$ of $L$ satisfying $[I, L] \subseteq L$ and $[L, I] \subseteq L$.

Proposition 4.9. Every Leibniz algebra L has a gb-triple system structure given by the bracket

$$
\{x, y, z\}=[[x, z], y] .
$$

Proof. To check that $\{-,-,-\}$ satisfies the identity (2.1), let $x, y, a, b, c \in L$; we have on one hand

$$
\begin{aligned}
\{x, y,\{a, b, c\}\}+\{\{a, x, c\}, y, b\} & =[[x,\{a, b, c\}], y]+[[\{a, x, c\}, b], y] \\
& =[[x,[[a, c], b]], y]+[[[a, c], x], b], y] \\
& =[[[a, c],[x, b]], y] .
\end{aligned}
$$

On the other hand

$$
\begin{aligned}
\{a,\{x, y, b\}, c\}-\{x,\{a, y, c\}, b\} & =[[a, c],\{x, y, b\}]-[[x, b],\{a, y, c\}] \\
& =[[a, c],[[x, b], y]]-[[x, b],[[a, c], y]]
\end{aligned}
$$

The equality holds by the identity (4.1).
Now recall that for a $g b$-triple system $\mathfrak{g}, \mathfrak{g}^{\otimes 2}$ is a Leibniz algebra (see [6, Proposition 2.1]) when endowed with the bracket

$$
\left[a_{1} \otimes a_{2}, b_{1} \otimes b_{2}\right]_{\mathfrak{g}^{\otimes 2}}=\left[a_{1}, b_{1}, a_{2}\right]_{\mathfrak{g}} \otimes b_{2}+b_{1} \otimes\left[a_{1}, b_{2}, a_{2}\right]_{\mathfrak{g}}
$$

Lemma 4.10. Let $k$ be a positive integer such that $k \geqslant 2$. Then for all $a_{1}, b_{1}, a_{2}, b_{2}$, $\ldots, a_{k}, b_{k}, g_{1}, g_{2} \in \mathfrak{g}$ we have

$$
\begin{aligned}
& {\left[a_{1} \otimes b_{1},\left[a_{2} \otimes b_{2},\left[\ldots,\left[a_{k} \otimes b_{k}, g_{1} \otimes g_{2}\right]_{\mathfrak{g}^{\otimes 2}}\right]_{\mathfrak{g}^{\otimes 2}}\right]_{\mathfrak{g}^{\otimes 2}}\right]_{\mathfrak{g}^{\otimes 2}}} \\
& =\left[a_{1},\left[a_{2},\left[\ldots\left[a_{k}, g_{1}, b_{k}\right]_{\mathfrak{g}} \ldots\right]_{\mathfrak{g}}, b_{2}\right]_{\mathfrak{g}}, b_{1}\right]_{\mathfrak{g}} \otimes g_{2} \\
& +g_{1} \otimes\left[a_{1},\left[a_{2},\left[\ldots\left[a_{k}, g_{2}, b_{k}\right]_{\mathfrak{g}} \ldots\right]_{\mathfrak{g}}, b_{2}\right]_{\mathfrak{g}}, b_{1}\right]_{\mathfrak{g}} \\
& +\sum_{i=1}^{k-1}\left[a_{1},\left[a_{2}, \ldots,\left[\widehat{a_{i}}, \ldots\left[a_{k}, g_{1}, b_{k}\right]_{\mathfrak{g}} \ldots, \widehat{b_{i}}\right]_{\mathfrak{g}}, \ldots b_{2}\right]_{\mathfrak{g}}, b_{1}\right]_{\mathfrak{g}} \otimes\left[a_{i}, g_{2}, b_{i}\right]_{\mathfrak{g}} \\
& +\sum_{i=1}^{k-1}\left[a_{i}, g_{1}, b_{i}\right]_{\mathfrak{g}} \otimes\left[a_{1},\left[a_{2}, \ldots,\left[\widehat{a_{i}}, \ldots\left[a_{k}, g_{2}, b_{k}\right]_{\mathfrak{g}} \ldots, \widehat{b_{i}}\right]_{\mathfrak{g}}, \ldots b_{2}\right]_{\mathfrak{g}}, b_{1}\right]_{\mathfrak{g}},
\end{aligned}
$$

where $\widehat{g}$ means that the variable $g$ is deleted.
Proof. The proof follows by induction and by the formula (2.1) in $[6$, Proposition 2.1].

Corollary 4.11. If $\mathfrak{g}$ is a nilpotent gb-triple system of class $s$, then $\mathfrak{g}^{\otimes 2}$ is a nilpotent Leibniz algebra of class $s+1$.

Proof. The proof follows directly by Lemma 4.10.
Recall also that the map $A_{g_{1} \otimes g_{2}}: \mathfrak{g} \longrightarrow \mathfrak{g}$ defined by $A_{g_{1} \otimes g_{2}}(z)=\left[g_{1}, z, g_{2}\right]_{\mathfrak{g}}$ is a derivation of $\mathfrak{g}$, and the subspace $\mathfrak{A}(\mathfrak{g})=\left\{A_{g_{1} \otimes g_{2}} \mid g_{1}, g_{2} \in \mathfrak{g}\right\}$ is a Lie algebra (see [6, Proposition 2.1]) with respect to the product

$$
\left[A_{a_{1} \otimes a_{2}}, A_{b_{1} \otimes b_{2}}\right]_{\mathfrak{A}(\mathfrak{g})}=A_{a_{1} \otimes a_{2}} \circ A_{b_{1} \otimes b_{2}}-A_{b_{1} \otimes b_{2}} \circ A_{a_{1} \otimes a_{2}}
$$

Proposition 4.12. Let $\mathfrak{g}$ be a gb-triple system, $K=\left\{g_{1} \otimes g_{2} \in \mathfrak{g}^{\otimes 2} \mid A_{g_{1} \otimes g_{2}}=0\right\}$. If $\mathfrak{h}:=\mathfrak{g}^{\otimes 2} / K$ is a nilpotent Leibniz algebra of class $s$, then $\mathfrak{g}^{\otimes 2}$ is a nilpotent Leibniz algebra of class $s+1$.

Proof. From the proof of [6, Proposition 2.4], we have

$$
A_{\left[a_{1} \otimes a_{2}, b_{1} \otimes b_{2}\right]_{\mathfrak{g} \otimes 2}}=\left[A_{a_{1} \otimes a_{2}}, A_{b_{1} \otimes b_{2}}\right]_{\mathfrak{A}(\mathfrak{g})}
$$

for all $a_{1}, a_{2}, b_{1}, b_{2} \in \mathfrak{g}$. It follows that $K$ is a 2-sided ideal of $\mathfrak{g}^{\otimes 2}$. Since $\mathfrak{h}$ is nilpotent of class $s, a d_{\mathfrak{h}}^{(s)}(\mathfrak{h})=\left\{\left[h_{1},\left[h_{2},\left[\ldots,\left[h_{s}, h\right]_{\mathfrak{h}}\right]_{\mathfrak{h}}\right]_{\mathfrak{h}}\right]_{\mathfrak{h}}, h_{1}, h_{2}, \ldots, h_{s}, h \in \mathfrak{h}\right\}=$ $K$. This implies that $a d_{\mathfrak{g}^{\otimes 2}}^{(s)}\left(\mathfrak{g}^{\otimes 2}\right) \subseteq K$. Now for all $g_{1} \otimes g_{2} \in K$ and $a \otimes b \in \mathfrak{g}^{\otimes 2}$, we have

$$
\begin{aligned}
a d_{g_{1} \otimes g_{2}}(a \otimes b) & =\left[g_{1} \otimes g_{2}, a \otimes b\right]_{\mathfrak{g} \otimes 2} \\
& =\left[g_{1}, a, g_{2}\right]_{\mathfrak{g}} \otimes b+a \otimes\left[g_{1}, b, g_{2}\right]_{\mathfrak{g}} \\
& =A_{g_{1} \otimes g_{2}}(a) \otimes b+a \otimes A_{g_{1} \otimes g_{2}}(b)=0 .
\end{aligned}
$$

So $\left[K, \mathfrak{g}^{\otimes 2}\right]_{\mathfrak{g}}{ }^{\otimes 2}=a d_{K}\left(\mathfrak{g}^{\otimes 2}\right)=0$. Therefore

$$
a d_{\mathfrak{g}^{\otimes 2}}^{(s+1)}\left(\mathfrak{g}^{\otimes 2}\right)=\left[a d_{\mathfrak{g}^{\otimes 2}}^{(s)}\left(\mathfrak{g}^{\otimes 2}\right), \mathfrak{g}^{\otimes 2}\right]_{\mathfrak{g}^{\otimes 2}} \subseteq\left[K, \mathfrak{g}^{\otimes 2}\right]_{\mathfrak{g}^{\otimes 2}}=0
$$

Hence $\mathfrak{g}^{\otimes 2}$ is nilpotent of class $s+1$.
The following theorem is known as Engel's Theorem. It was extended to Leibniz algebras in [1].

Theorem 4.13. (cf. [13]) A Lie algebra L is nilpotent if and only if $a d_{x}$ is nilpotent for any $x \in L$, where $a d_{x}(y):=[x, y]$.

Note that the Leibniz algebras version of Theorem 4.13 could be used to prove Proposition 4.12.

The following is a Engel-like Theorem for $g b$-triple system.
Theorem 4.14. A gb-triple system $\mathfrak{g}$ is nilpotent if and only if $A_{g_{1} \otimes g_{2}}$ is nilpotent for every $g_{1}, g_{2} \in \mathfrak{g}$.

Proof. Assume that $\mathfrak{g}$ is nilpotent. Then $\mathfrak{g}^{(s)}=0$ for some positive integer $s$. So for every $g, a_{1}, \ldots, a_{s-1}, b_{1}, \ldots, b_{s-1} \in \mathfrak{g}$,

$$
\left[a_{1},\left[a_{2},\left[\ldots,\left[a_{s-1}, g, b_{s-1}\right]_{g} \ldots\right]_{g}, b_{2}\right]_{g}, b_{1}\right]_{g}=0
$$

that is

$$
A_{a_{1} \otimes b_{1}} \circ A_{a_{2} \otimes b_{2}} \circ \ldots \circ A_{a_{s-1} \otimes b_{s-1}}(g)=0 .
$$

In particular,

$$
(\underbrace{A_{g_{1} \otimes g_{2}} \circ A_{g_{1} \otimes g_{2}} \circ \ldots \circ A_{g_{1} \otimes g_{2}}}_{(\mathrm{s}-1) \text {-times }})(g)=0 \quad \text { for every } \quad g_{1}, g_{2} \in \mathfrak{g} .
$$

So for every $g_{1}, g_{2} \in \mathfrak{g}, A_{g_{1} \otimes g_{2}}$ is nilpotent.
Conversely, assume that $A_{g_{1} \otimes g_{2}}$ is nilpotent for every $g_{1}, g_{2} \in \mathfrak{g}$. So the Lie algebra $\mathfrak{A}(\mathfrak{g})=\left\{A_{g_{1} \otimes g_{2}} \mid g_{1}, g_{2} \in \mathfrak{g}\right\}$ is a Lie algebra of nilpotent linear maps. Moreover, by the proof of [6, Proposition 3.6], $\mathfrak{A}(\mathfrak{g})$ is an ideal of $\operatorname{Der}(\mathfrak{g})$, and thus a closed subset of $\operatorname{End}(\mathfrak{g})$. It follows by [9, Theorem 3.5] that the associative subalgebra generated by $\mathfrak{A}(\mathfrak{g})$ is nilpotent. So there exists a positive integer $s$ such that

$$
\left(A_{a_{1} \otimes b_{1}} \circ A_{a_{2} \otimes b_{2}} \circ \ldots \circ A_{a_{s} \otimes b_{s}}\right)(g)=0 \quad \text { for all } g, a_{1}, \ldots, a_{s}, b_{1}, \ldots, b_{s} \in \mathfrak{g}
$$

This implies that

$$
\left[a_{1},\left[a_{2},\left[\ldots,\left[a_{s}, g, b_{s}\right]_{g} \ldots\right]_{g}, b_{2}\right]_{g}, b_{1}\right]_{g}=0 \quad \text { for all } g, a_{1}, \ldots, a_{s}, b_{1}, \ldots, b_{s} \in \mathfrak{g} .
$$

Hence $\mathfrak{g}^{(s+1)}=0$. Therefore $\mathfrak{g}$ is nilpotent.
Corollary 4.15. Let $\mathfrak{g}$ be a gb-triple system. Then if $\mathfrak{g}$ is nilpotent, so is any subalgebra $S$ of $\mathfrak{g}$.

Proof. Let $S$ be a subalgebra of $\mathfrak{g}$. If $S$ is not nilpotent, then by Theorem 4.14 there exists $g_{1}, g_{2} \in S$ such that the restriction $A_{g_{1} \otimes g_{2}}^{(s)} \mid S \neq 0$ for all positive integer $s$. But this implies that $A_{g_{1} \otimes g_{2}}^{(s)} \neq 0$ for all positive integer $s$. So $A_{g_{1} \otimes g_{2}}$ is not nilpotent, and thus $\mathfrak{g}$ is not nilpotent by Theorem 4.14.

Corollary 4.16. If $L$ is nilpotent as a Leibniz algebra, then $L$ is also nilpotent as a gb-triple system.

Proof. For all $g_{1}, g_{2} \in \mathfrak{g}, A_{g_{1} \otimes g_{2}}=a d_{\left[g_{1}, g_{2}\right]}$ by Proposition 4.9. The result now follows by applying both Engel's theorems for Leibniz and $g b$-triple systems.

### 4.3. Nilpotent ideals of $g b$-triple systems

For an ideal $\mathfrak{I}$ of a $g b$-triple system $\mathfrak{g}$, consider the series defined by $\mathfrak{I}^{(0)}=\mathfrak{g}$, and $\mathfrak{I}^{(s+1)}=\left[\mathfrak{I}, \mathfrak{I}^{(s)}, \mathfrak{g}\right]$ with $\mathfrak{I}^{(1)}=\mathfrak{I}$ where $s$ is a positive integer, $s \geqslant 1$.

Proposition 4.17. $\mathfrak{I}^{(s)}$ is an ideal of $\mathfrak{g}$ for every integer $s \geqslant 0$.

Proof. The cases $s=0,1$ are trivial. By induction, assume that for $s \geqslant 2, \mathfrak{I}^{(s-1)}$ is an ideal of $\mathfrak{g}$ and let $x, y, z \in \mathfrak{g}, b \in \mathfrak{I}$ and $a \in \mathfrak{I}^{(s-1)}$. Then it follows from the identity (2.1) that

$$
\left[x,[b, a, z]_{\mathfrak{g}}, y\right]_{\mathfrak{g}}=\left[b, a,[x, z, y]_{\mathfrak{g}}\right]_{\mathfrak{g}}+[\underbrace{[x, b, y]_{\mathfrak{g}}}_{\in \mathfrak{I}}, a, z]_{\mathfrak{g}}+[b, \underbrace{[x, a, y]_{\mathfrak{g}}}_{\in \mathfrak{I}^{(s-1)}}, z]_{\mathfrak{g}} \in \mathfrak{I}^{(s)} .
$$

So $\mathfrak{I}^{(s)}$ is an ideal of $\mathfrak{g}$.
Proposition 4.18. Let $\mathfrak{I}_{1}$ and $\mathfrak{I}_{2}$ be two ideals of $\mathfrak{g}$ such that $\mathfrak{I}_{1} \subseteq \mathfrak{I}_{2}$. Then

$$
\mathfrak{I}_{1}^{(s)} \subseteq \mathfrak{I}_{2}^{(s)}
$$

for all integer $s \geqslant 0$.
Proof. The cases $s=0,1$ are trivial. By induction, assume that the result is true for $s \geqslant 2$. Then $\mathfrak{I}_{1}^{(s+1)}=\left[\mathfrak{I}_{1}, \mathfrak{I}_{1}^{(s)}, \mathfrak{g}\right]_{g} \subseteq\left[\mathfrak{I}_{2}, \mathfrak{I}_{2}^{(s)}, \mathfrak{g}\right]_{g}=\mathfrak{I}_{2}^{(s+1)}$.

Definition 4.19. An ideal $\mathfrak{I}$ of $\mathfrak{g}$ is nilpotent if $\mathfrak{I}^{(s)}=0$ for some positive integer $s$. The smallest of such values $s$ is called class of nilpotency of $\mathfrak{I}$.

The following lemma provides the fitting decomposition of a $g b$-triple system relative to a derivation in $\mathfrak{A}(\mathfrak{g})$.

Lemma 4.20. Let $\mathfrak{g}$ be a finite dimensional $g b$-tiple system and $g_{1}, g_{2} \in \mathfrak{g}$. Then

$$
\mathfrak{g}=\mathfrak{g}_{0} \oplus \mathfrak{g}_{1}
$$

with $\mathfrak{g}_{0}=\left\{x \in \mathfrak{g} \mid A_{g_{1} \otimes g_{2}}^{(s)}(x)=0\right.$ for some integer $\left.s>0\right\}$ and $A_{g_{1} \otimes g_{2}}(\mathfrak{g})=\mathfrak{g}$
Proof. Apply the Fitting Lemma [15, Chapter 2] on the linear transformation $A_{g_{1} \otimes g_{2}}$.

The spaces $\mathfrak{g}_{0}$ and $\mathfrak{g}_{1}$ are called the Fitting null and one-components of $\mathfrak{g}$ with respect to $A_{g_{1} \otimes g_{2}}$.

The following theorem was proved in [4] for Lie algebras and in [18] for $n$-Lie algebras.

Theorem 4.21. Let $\mathfrak{g}$ be a gb-triple system. If $\mathfrak{I}_{1}$ and $\mathfrak{I}_{2}$ are 3 -sided ideals of $\mathfrak{g}$ such that $\mathfrak{I}_{1} \subseteq \phi(\mathfrak{g}) \cap \mathfrak{I}_{2}$ and $\mathfrak{I}_{2} / \mathfrak{I}_{1}$ is nilpotent, then $\mathfrak{I}_{2}$ is nilpotent.

Proof. We proceed by contradiction. Assume that $\mathfrak{I}_{2}$ is not nilpotent. Then by Theorem 4.14, there exists $g_{1}, g_{2} \in \mathfrak{I}_{2}$ such that $A_{g_{1} \otimes g_{2}}^{(s)}(x) \neq 0$ for all positive integer $s$. By Lemma 4.20 let $\mathfrak{g}_{0}$ and $\mathfrak{g}_{1}$ be the Fitting null and one-components of $\mathfrak{g}$ with respect to $A_{g_{1} \otimes g_{2}}$. Since $\mathfrak{I}_{2}$ is a 3 -sided ideal, it follows that $\mathfrak{g}_{1} \subseteq \mathfrak{I}_{2}$. Also, since $\mathfrak{I}_{2} / \mathfrak{I}_{1}$ is nilpotent we have $\mathfrak{I}_{2}^{(k)} \subseteq \Im_{1}$ for some positive integer $k$. It follows by definition of $\mathfrak{g}_{1}$ that $\mathfrak{g}_{1}=A_{g_{1} \otimes g_{2}}^{(k)}\left(\mathfrak{g}_{1}\right) \subseteq \mathfrak{I}_{2}^{(k)} \subseteq \mathfrak{I}_{1}$. Therefore $\mathfrak{g}_{1} \subseteq \phi(\mathfrak{g})$. So
$\mathfrak{g}=\mathfrak{g}_{0}+\phi(\mathfrak{g})$. Now since by [6, Proposition 2.6] $A_{g_{1} \otimes g_{2}}$ is a derivation of $\mathfrak{g}, \mathfrak{g}_{0}$ is a subalgebra of $\mathfrak{g}$. So there is a maximal subalgebra $\mathfrak{m}$ that contains $\mathfrak{g}_{0}$. Since by definition $\phi(\mathfrak{g}) \subseteq \mathfrak{m}$, it follows that $\mathfrak{m}=\mathfrak{g}$. This contradicts the maximality of $\mathfrak{m}$. Therefore $\mathfrak{I}_{2}$ is nilpotent.

Corollary 4.22. Every 3 -sided ideal of a gb-tiple system $\mathfrak{g}$ contained in the Frattini ideal $\phi(\mathfrak{g})$ is nilpotent. In particular, if $\phi(\mathfrak{g})$ is a 3-sided ideal, then $\phi(\mathfrak{g})$ is a nilpotent ideal of $\mathfrak{g}$.

Proof. Let $\mathfrak{I}$ be a 3 -sided ideal of $\mathfrak{g}$ such that $\mathfrak{I} \subseteq \phi(\mathfrak{g})$. The result follows from Theorem 4.21 by setting $\mathfrak{I}_{1}=\mathfrak{I}_{2}=\mathfrak{I}$. In particular, take $\mathfrak{I}=\phi(\mathfrak{g})$ to show that $\phi(\mathfrak{g})$ is nilpotent.

Corollary 4.23. Let $\mathfrak{g}$ be a gb-triple system for which $\phi(\mathfrak{g})$ is a 3-sided ideal. Then $\mathfrak{g} / \phi(\mathfrak{g})$ is nilpotent if and only if $\mathfrak{g}$ is nilpotent.

Proof. The first implication follows from Theorem 4.21 by setting $\mathfrak{I}_{1}=\phi(\mathfrak{g})$ and $\mathfrak{I}_{2}=\mathfrak{g}$. Conversely, if $\mathfrak{g}$ is nilpotent, then $\mathfrak{g}^{(s)}=0$ for some positive integer $s$. So $(\mathfrak{g} / \phi(\mathfrak{g}))^{(s)}=\mathfrak{g}^{(s)} / \phi(\mathfrak{g})=\phi(\mathfrak{g})$.

## 5. Invariance of the nilradical under derivations

The following Lemma which was proved (see [9, Lemma 3.3]) for Leibniz 3-algebras also holds for $g b$-triple systems, and the proof is identical.

Lemma 5.1. For every derivation d of $\mathfrak{g}$ and every positive integer $s$,

$$
\begin{equation*}
d^{s}\left([x, y, z]_{g}\right)=\sum_{i+j+k=s} \frac{s!}{i!j!k!}\left[d^{i}(x), d^{j}(y), d^{k}(z)\right]_{g} . \tag{5.1}
\end{equation*}
$$

Analogues of the following results were established in [16] for Leibniz 3-algebras.
Proposition 5.2. Let $\mathfrak{I}$ be an ideal of a gb-triple system $\mathfrak{g}$ and d a derivation of $\mathfrak{g}$. Then

$$
\begin{equation*}
(d(\mathfrak{I}))^{(s)} \subseteq d^{s}\left(\mathfrak{I}^{(s)}\right) \tag{5.2}
\end{equation*}
$$

for all positive integer s.
Proof. Notice that the assertion is trivial for $s=1$. Now assume by induction that the result holds for any positive integer $s$, then

$$
(d(\mathfrak{I}))^{(s+1)}=\left[d(\mathfrak{I}),(d(\mathfrak{I}))^{(s)}, \mathfrak{g}\right]_{\mathfrak{g}} \subseteq\left[d(\mathfrak{I}),\left(d^{s}\left(\mathfrak{I}^{(s)}\right), \mathfrak{g}\right]_{\mathfrak{g}} \subseteq d^{s+1}\left(\mathfrak{I}^{(s+1)}\right)\right. \text { by }
$$

Proposition 5.3. Let $\mathfrak{I}$ be an ideal of a gb-triple system $\mathfrak{g}$ and $d$ a derivation of $\mathfrak{g}$. Then for all $s \geqslant 2$,

$$
\begin{equation*}
(\mathfrak{I}+d(\mathfrak{I}))^{(s)} \subseteq \mathfrak{I}+(d(\mathfrak{I}))^{(s)}+\sum_{i=1}^{s-1} d^{i}\left(\mathfrak{I}^{(s)}\right) \tag{5.3}
\end{equation*}
$$

Proof. We verify the assertion for $s=2$.

$$
\begin{aligned}
(\mathfrak{I}+d(\mathfrak{I}))^{(2)} & =[\mathfrak{I}+d(\mathfrak{I}), \mathfrak{I}+d(\mathfrak{I}), \mathfrak{g}]_{\mathfrak{g}} \\
& \subseteq \mathfrak{I}+[\mathfrak{I}, d(\mathfrak{I}), \mathfrak{g}]_{\mathfrak{g}}+[d(\mathfrak{I}), d(\mathfrak{I}), \mathfrak{g}]_{\mathfrak{g}} \\
& \subseteq \mathfrak{I}+d\left(\mathfrak{I}^{(2)}\right)+(d(\mathfrak{I}))^{(2)} \text { by }(5.1) .
\end{aligned}
$$

Now assume by induction that the result holds for any positive integer $s$, then

$$
\begin{aligned}
(\mathfrak{I}+d(\mathfrak{I}))^{(s+1)}= & {\left[\mathfrak{I}+d(\mathfrak{I}),(\mathfrak{I}+d(\mathfrak{I}))^{(s)}, \mathfrak{g}\right]_{\mathfrak{g}} } \\
\subseteq & {\left[\mathfrak{I}+d(\mathfrak{I}), \mathfrak{I}+(d(\mathfrak{I}))^{(s)}+\sum_{i=1}^{s-1} d^{i}\left(\mathfrak{I}^{(s)}\right), \mathfrak{g}\right]_{\mathfrak{g}} } \\
\subseteq & \mathfrak{I}+\left[\mathfrak{I},(d(\mathfrak{I}))^{(s)}, \mathfrak{g}\right]_{\mathfrak{g}}+\sum_{i=1}^{s-1}\left[\mathfrak{I}, d^{i}\left(\mathfrak{I}^{(s)}\right), \mathfrak{g}\right]_{\mathfrak{g}} \\
& +\left[d(\mathfrak{I}),(d(\mathfrak{I}))^{(s)}, \mathfrak{g}\right]_{\mathfrak{g}}+\sum_{i=1}^{s-1}\left[d(\mathfrak{I}), d^{i}\left(\mathfrak{I}^{(s)}\right), \mathfrak{g}\right]_{\mathfrak{g}} \\
\subseteq & \mathfrak{I}+\underbrace{d^{s}\left(\mathfrak{I}^{(s+1))}\right.}+\sum_{i=1}^{s-1} \underbrace{d^{i}\left(\mathfrak{I}^{(s+1)}\right)}_{\text {by }(5.1)}+(d(\mathfrak{I}))^{(s+1)} \\
& +\sum_{i=1}^{s-1} d^{i+1}\left(\mathfrak{I}^{(s+1)}\right) \text { byd }(5.1) \\
\subseteq & \mathfrak{I}+2 \sum_{i=1}^{s} d^{i}\left(\mathfrak{I}^{(s+1)}\right)+(d(\mathfrak{I}))^{(s+1)} \\
\subseteq & \mathfrak{I}+\sum_{i=1}^{s} d^{i}\left(\mathfrak{I}^{(s+1)}\right)+(d(\mathfrak{I}))^{(s+1)} .
\end{aligned}
$$

For the remainder of this paper, we assume that all ideals are also right ideals. We call them 2-sided (right) ideals.

Lemma 5.4. If $\mathfrak{I}_{1}$ and $\mathfrak{I}_{2}$ are 2-sided (right) ideals of a gb-triple system $\mathfrak{g}$, then

$$
\left(\mathfrak{I}_{1}+\mathfrak{I}_{2}\right)^{(s)} \subseteq \sum_{\substack{i+j=s, 0 \leqslant i, j \leqslant s}} \mathfrak{I}_{1}^{(i)} \bigcap \mathfrak{I}_{2}^{(j)}
$$

Proof. By definition, $\left(\mathfrak{I}_{1}+\mathfrak{I}_{2}\right)^{(1)}=\mathfrak{I}_{1}+\mathfrak{I}_{2}=\mathfrak{I}_{1}^{(1)} \bigcap \mathfrak{I}_{2}^{(0)}+\mathfrak{I}_{1}^{(0)} \bigcap \mathfrak{I}_{2}^{(1)}$ since $\mathfrak{I}_{1}^{(0)}=$ $\mathfrak{I}_{2}^{(0)}=\mathfrak{g}$. By induction, assume the result holds for $\left(\mathfrak{I}_{1}+\mathfrak{I}_{2}\right)^{(s-1)}$. Then

$$
\begin{aligned}
\left(\mathfrak{I}_{1}+\mathfrak{I}_{2}\right)^{(s)}= & {\left[\mathfrak{I}_{1}+\mathfrak{I}_{2},\left(\mathfrak{I}_{1}+\mathfrak{I}_{2}\right)^{(s-1)}, \mathfrak{g}\right]_{\mathfrak{g}} } \\
= & {\left[\mathfrak{I}_{1},\left(\mathfrak{I}_{1}+\mathfrak{I}_{2}\right)^{(s-1)}, \mathfrak{g}\right]_{\mathfrak{g}}+\left[\mathfrak{I}_{2},\left(\mathfrak{I}_{1}+\mathfrak{I}_{2}\right)^{(s-1)}, \mathfrak{g}\right]_{\mathfrak{g}} } \\
\subseteq & {\left[\mathfrak{I}_{1}, \mathfrak{I}_{1}^{(s-1)}, \mathfrak{g}\right]_{\mathfrak{g}}+\sum_{r=1}^{s-2}\left[\mathfrak{I}_{1}, \mathfrak{I}_{1}^{(s-r-1)} \bigcap \mathfrak{I}_{2}^{(r)}, \mathfrak{g}\right]_{\mathfrak{g}}+\left[\mathfrak{I}_{1}, \mathfrak{I}_{2}^{(s-1)}, \mathfrak{g}\right]_{\mathfrak{g}} } \\
& +\left[\mathfrak{I}_{2}, \mathfrak{I}_{1}^{(s-1)}, \mathfrak{g}\right]_{\mathfrak{g}}+\sum_{r=1}^{s-2}\left[\mathfrak{I}_{2}, \mathfrak{I}_{1}^{(s-r-1)} \cap \mathfrak{I}_{2}^{(r)}, \mathfrak{g}\right]_{\mathfrak{g}}+\left[\mathfrak{I}_{2}, \mathfrak{I}_{2}^{(s-1)}, \mathfrak{g}\right]_{\mathfrak{g}} \\
\subseteq & \sum_{\substack{i+j=s, 0 \leqslant i, j \leqslant s}} \mathfrak{I}_{1}^{(i)} \bigcap \mathfrak{I}_{2}^{(j)}
\end{aligned}
$$

because

$$
\begin{gathered}
{\left[\mathfrak{I}_{1}, \mathfrak{I}_{1}^{(s-r-1)} \bigcap \mathfrak{I}_{2}^{(r)}, \mathfrak{g}\right]_{\mathfrak{g}} \subseteq \mathfrak{I}_{1}^{(s-r)} \bigcap \mathfrak{I}_{2}^{(r)}} \\
{\left[\mathfrak{I}_{2}, \mathfrak{I}_{1}^{(s-r-1)} \bigcap \mathfrak{I}_{2}^{(r)}, \mathfrak{g}\right]_{\mathfrak{g}} \subseteq \mathfrak{I}_{1}^{(s-r-1)} \bigcap \mathfrak{I}_{2}^{(r+1)}}
\end{gathered}
$$

and

$$
\left[\mathfrak{I}_{1}, \mathfrak{I}_{2}^{(s)}, \mathfrak{g}\right]_{\mathfrak{g}} \subseteq \mathfrak{I}_{1}^{(1)} \bigcap \mathfrak{I}_{2}^{(s)}, \quad\left[\mathfrak{I}_{2}, \mathfrak{I}_{1}^{(s)}, \mathfrak{g}\right]_{\mathfrak{g}} \subseteq \mathfrak{I}_{1}^{(s)} \bigcap \mathfrak{I}_{2}^{(1)}
$$

as $\mathfrak{I}_{1}^{(s-r-1)}, \mathfrak{I}_{2}^{(r)}, \mathfrak{I}_{1}^{(s)}, \mathfrak{I}_{2}^{(s)}$ are ideals and $\mathfrak{I}_{1}, \mathfrak{I}_{2}$ are right ideals.
Proposition 5.5. If $\mathfrak{I}_{1}$ and $\mathfrak{I}_{2}$ are nilpotent 2-sided (right) ideals of $\mathfrak{g}$, then $\mathfrak{I}_{1}+\mathfrak{I}_{2}$ is also a nilpotent 2 -sided (right) ideal of $\mathfrak{g}$.

Proof. This follows by definition and using Lemma 5.4. More precisely one shows that if $\mathfrak{I}_{1}$ is nilpotent of class $s_{1}$ and $\mathfrak{I}_{2}$ is nilpotent of class $s_{2}$, then $\mathfrak{I}_{1}+\mathfrak{I}_{2}$ is nilpotent of class $s_{1}+s_{2}$.

As a consequence of Proposition 5.5, the sum of all nilpotent 2-sided (right) ideals of $\mathfrak{g}$ is also nilpotent and contains all nilpotent 2 -sided (right) ideals of $\mathfrak{g}$. It is the unique maximal nilpotent 2 -sided (right) ideal called nilradical 2 -sided (right) ideal of $\mathfrak{g}$ and denoted $\mathfrak{N}$.

The following result shows that $\mathfrak{N}$ is invariant under derivations of $\mathfrak{g}$.
Corollary 5.6. For every derivation d of $\mathfrak{g}$, we have $d(\mathfrak{N}) \subseteq \mathfrak{N}$.
Proof. Since $\mathfrak{N}$ is nilpotent, $\mathfrak{N}^{(s)}=0$ for some positive integer $s$. Then by (5.2) and (5.3), it follows that $(\mathfrak{N}+d(\mathfrak{N}))^{(s)} \subseteq \mathfrak{N}+(d(\mathfrak{N}))^{(s)} \subseteq \mathfrak{N}+d^{s}\left(\mathfrak{N}^{(s)}\right) \subseteq \mathfrak{N}$. Now by Proposition 4.18, $(\mathfrak{N}+d(\mathfrak{N}))^{(2 s)} \subseteq \mathfrak{N}^{(s)}=0$. Thus $\mathfrak{N}+d(\mathfrak{N})$ is nilpotent. Therefore $\mathfrak{N}+d(\mathfrak{N}) \subseteq \mathfrak{N}$ as $\mathfrak{N}$ is maximal. Hence $d(\mathfrak{N}) \subseteq \mathfrak{N}$.

## References

[1] Sh.A. Ayupov, B.A. Omirov, On Leibniz algebras, Algebra and Operator Theory, Proc. Colloq. in Tashkent, 1997, Kluwer Acad. Publ. 1 - 13.
[2] R.P. Bai, L.Y. Chen, D.J. Meng, The Frattini subalgebra of n-Lie algebras, Acta. Math. Sinica 23 (2007), $847-856$.
[3] R.P. Bai, L. Lili, L. Zhenheng, Elementary and $\phi$-free Lie triple systems, Acta. Math. Sinica 32 (2012), $2322-2328$.
[4] D. Barnes, On the cohomology of soluble Lie algebras, Math. Zeit. 101 (1967), 343-349.
[5] D. Barnes, Some theorems on Leibniz algebras, Commun. Algebra 39 (2011), 2463-2472.
[6] G.R. Biyogmam, Introduction to gb-triple systems, ISRN Algebra, 2014, Article ID $738154,5 \mathrm{pp}$.
[7] G.R. Biyogmam, Lie central triple racks, Int. Electron. J. Algebra 17 (2015), 58-65.
[8] M.R. Bremner, J. Sánchez-Ortega, Leibniz triple systems, Commun. Contemp. Math. 14 (2013), $189-207$.
[9] L.M. Camacho, J.M. Casas, J.R. Gómez, M. Ladra, B.A. Omirov, On nilpotent Leibniz $n$-algebras, J. Algebra Appl. 11 (2012), Article 1250062, 17 pp.
[10] J.M. Casas, J. Loday, T. Pirashvili, Leibniz n-algebras, Forum Math. 14 (2002), 189 - 207.
[11] A. Fialowski, A.Kh. Khudoyberdiyev, B.A. Omirov, A characterization of nilpotent Leibniz algebras, Algebras and Representation Theory 16 (2013), 14891505.
[12] V.T. Filippov, $n$-Lie algebras, Sibirsh. Mat. Zh., 26 (1985), 126 - 140.
[13] T. Hawkins, Emergence of the theory of Lie groups, Sources and Studies in the History of Math. and Phys. Sci., Springer-Verlag, Berlin, New York, 2000.
[14] N. Jacobson, Lie and Jordan triple systems, Amer. J. Math. 71 (1949), 149-170.
[15] N. Jacobson, Lie algebras, Wiley, New York, 1962.
[16] F. Gago, M. Ladra, B.A. Omirov, R.M. Turdibaev, Some radicals, Frattini and Cartan subalgebras of Leibniz n-algebras, Linear and Multilinear Algebra 61 (2013), 1510 - 1527.
[17] J.L. Loday, Une version non commutative des algèbres de Lie: Les algèbres de Leibniz, L'Enseignement Math. 39 (1993), 269 - 293.
[18] M.P. Williams, Frattini theory for n-Lie algebras, Algebra Discrete Math. 2 (2009), $108-115$.

# Semi-prime and meet weak closure operations in lower $B C K$-semilattices 

Hashem Bordbar, Mohammad Mehdi Zahedi and Young Bae Jun


#### Abstract

The notion of semi-prime (resp., meet) weak closure operation is introduced, and related properties are investigated. Characterizations of a semi-prime (resp. meet) closure operation are discussed. Examples which show that the notion of semi-prime weak closure operation is independent to the notion of meet weak closure operation.


## 1. Introduction

Semi-prime closure operations on ideals of $B C K$-algebras are introduced in the paper [2], and a finite type of closure operations on ideals of $B C K$-algebras are discussed in [1]. As a general form of closure operations on ideals of $B C K$-algebras, Bordbar et al. [3] introduced the notion of weak closure operations on ideals of $B C K$-algebras. Regarding weak closure operation, they defined finite type and (strong) quasi-primeness, and investigated related properties. They also discussed positive implicative (resp., commutative and implicative) weak closure operations, and provided several examples to illustrate notions and properties.

In this paper, we introduce the notion of semi-prime (resp., meet) weak closure operation in lower $B C K$-semilattices, and investigate their properties. We discuss characterizations of a semi-prime (resp. meet) closure operation. We provide examples to show that the notion of semi-prime weak closure operation is independent to the notion of meet weak closure operation.

## 2. Preliminaries

A $B C K / B C I$-algebra is an important class of logical algebras introduced by K . Iséki and was extensively investigated by several researchers. We refer the reader to the books $[5,6]$ for further information regarding $B C K / B C I$-algebras.

Suppose that $X$ is a $B C K$-algebra. Define a binary relation $\leqslant$ on $X$ as follows:
$x \leqslant y$ if and only if $x * y=0$
2000 Mathematics Subject Classification: 06F35, 03G25.
Keywords: non-zeromeet element, meet ideal, relative annihilator, semi-prime (resp., meet) weak closure operation.
for any $x, y \in X$. Then $(X, \leqslant)$ is a partially ordered set (see [5]), and we say that $\leqslant$ is the $B C K$-ordering on $X$.

A partially ordered set $(X, \leqslant)$ is called a lower (resp., upper) semilattice if any two elements in $X$ have the greatest lower bound (resp., least upper bound). If $(X, \leqslant)$ is both a lower semilattice and an upper semilattice, we call it a lattice (see [5]).

A $B C K$-algebra $X$ is called a lower $B C K$-semilattice (see [6]) if $X$ is a lower semilattice with respect to the $B C K$-order.

In what follows, let $X$ be a lower $B C K$-semilattice and $\mathcal{I}(X)$ a set of all ideals of $X$ unless otherwise specified.
Definition 1 ([3]). An element $x$ of $X$ is called a zeromeet element of $X$ if the condition

$$
(\exists y \in X \backslash\{0\})(x \wedge y=0)
$$

is valid. Otherwise, $x$ is called a non-zeromeet element of $X$.
For a subset $A$ of a $B C K$-algebra $X$, denote by $\langle A\rangle$ the generated ideal by $A$. If $A=\{a\}$, then $\langle A\rangle$ is denoted by $\langle a\rangle$.

Denote by $Z(X)$ the set of all zeromeet elements of $X$, that is,

$$
Z(X)=\{x \in X \mid x \wedge y=0 \text { for some nonzero element } y \in X\}
$$

Definition 2 ([4]). For any nonempty subsets $A$ and $B$ of $X$, we define a set

$$
(A: \wedge B):=\{x \in X \mid x \wedge B \subseteq A\}
$$

which is called the relative annihilator of $B$ with respect to $A$.
Lemma 1 ([4]). If $A$ and $B$ are ideals of $X$, then the relative annihilator $\left(A:_{\wedge} B\right)$ of $B$ with respect to $A$ is an ideal of $X$.

Definition 3 ([3]). A mapping $c l: \mathcal{I}(X) \rightarrow \mathcal{I}(X)$ is called a weak closure operation on $\mathcal{I}(X)$ if the following conditions are valid.

$$
\begin{align*}
& (\forall A \in \mathcal{I}(X))(A \subseteq \operatorname{cl}(A)),  \tag{1}\\
& (\forall A, B \in \mathcal{I}(X))(A \subseteq B \Rightarrow \operatorname{cl}(A) \subseteq \operatorname{cl}(B)) . \tag{2}
\end{align*}
$$

In what follows, we use $A^{c l}$ instead of $\operatorname{cl}(A)$.

## 3. Semi-prime and meet weak closure operations

Definition 4. For any nonempty subsets $A$ and $B$ of $X$, we denote

$$
A \wedge B:=\langle\{a \wedge b \mid a \in A, b \in B\}\rangle
$$

which is called the meet ideal of $X$ generated by $A$ and $B$. In this case, we say that the operation " $\wedge$ " is a meet operation. If $A=\{a\}$, then $\{a\} \wedge B$ is denoted by $a \wedge B$. Also, if $B=\{b\}$, then $A \wedge\{b\}$ is denoted by $A \wedge b$.

Theorem 1. If $A$ and $B$ are ideals of $X$, then so is the meet set

$$
A \wedge B=\{a \wedge b \mid a \in A, b \in B\}
$$

based on $A$ and $B$.
Proof. Obviously, $0 \in A \wedge B$. Let $x \in A \wedge B$ and $y * x \in A \wedge B$ for $x, y \in X$. Then $x=a \wedge b$ and $y * x=a^{\prime} \wedge b^{\prime}$ where $a, a^{\prime} \in A$ and $b, b^{\prime} \in B$. Since $a \wedge b \leqslant a$ and $A$ is an ideal, we have $x=a \wedge b \in A$. Similarly, we have

$$
y * x=a^{\prime} \wedge b^{\prime} \leqslant a^{\prime} \in A
$$

Since $A$ is an ideal of $X$, it follows that $y \in A$. By the similar way, we get $y \in B$. Therefore,

$$
y=y \wedge y \in\{a \wedge b \mid a \in A, b \in B\}=A \wedge B
$$

and $A \wedge B$ is an ideal of $X$.
Obviously, $A \wedge B=B \wedge A$ for any nonempty subsets $A$ and $B$ of $X$. If $A$ and $B$ are ideals of $X$, then

$$
A \wedge B=\{a \wedge b \mid a \in A, b \in B\}
$$

Given ideals $A$ and $B$ of $X$, we consider two ideals

$$
A \wedge B^{c l} \text { and }(A \wedge B)^{c l}
$$

and investigate their relations where " $c l$ " is a weak closure operation on $\mathcal{I}(X)$.
The following example shows that there exist ideals $A$ and $B$ of $X$ such that

$$
A \wedge B^{c l} \nsubseteq(A \wedge B)^{c l}
$$

Example 1. Consider a lower $B C K$-semilattice $X=\{0,1,2,3,4\}$ with the following Cayley table.

| $*$ | 0 | 1 | 2 | 3 | 4 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 0 |
| 2 | 2 | 2 | 0 | 0 | 0 |
| 3 | 3 | 3 | 3 | 0 | 0 |
| 4 | 4 | 4 | 4 | 3 | 0 |

Note that $X$ has five ideals: $A_{0}=\{0\}, A_{1}=\{0,1\}, A_{2}=\{0,2\}, A_{3}=\{0,1,2\}$ and $A_{4}=X$. Define a map $c l: \mathcal{I}(X) \rightarrow \mathcal{I}(X)$ by $A_{0}^{c l}=A_{0}, A_{1}^{c l}=A_{3}, A_{2}^{c l}=A_{3}$, $A_{3}^{c l}=A_{4}$ and $A_{4}^{c l}=A_{4}$. Then " $c l$ " is a weak closure operation on $\mathcal{I}(X)$, and

$$
A_{1} \wedge A_{2}^{c l}=A_{1} \wedge A_{3}^{c l}=A_{1} \nsubseteq A_{0}=A_{0}^{c l}=\left(A_{1} \wedge A_{2}\right)^{c l}
$$

Proposition 1. For any element $a$ of $X$, we have

$$
\begin{equation*}
\langle a\rangle=a \wedge X \tag{3}
\end{equation*}
$$

Proof. Suppose that $p \in a \wedge X$. Then there exist $b_{1}, b_{2}, \ldots, b_{n} \in\{a \wedge x \mid x \in X\}$ such that $\left(\ldots\left(\left(p * b_{1}\right) * b_{2}\right) * \ldots\right) * b_{n}=0$. Let $b_{i}=a \wedge a_{i}$ where $a_{i} \in X$ for $i=1,2, \ldots, n$. Since $b_{1} \leqslant a$, it follows from (a2) that

$$
\begin{equation*}
(p * a) * b_{2} \leqslant\left(p * b_{1}\right) * b_{2} \tag{4}
\end{equation*}
$$

Since $b_{2} \leqslant a$, we have

$$
\begin{equation*}
(p * a) * a \leqslant(p * a) * b_{2} . \tag{5}
\end{equation*}
$$

By (4) and (5), we have

$$
(p * a) * a \leqslant\left(p * b_{1}\right) * b_{2} .
$$

Continuing this way, we get

$$
p * a^{n}=(\ldots((p * a) * a) * \ldots) * a \leqslant\left(\ldots\left(\left(p * b_{1}\right) * b_{2}\right) * \ldots\right) * b_{n}=0 .
$$

Hence $p * a^{n}=0$, that is, $p \in\langle a\rangle$. Therefore $a \wedge X \subseteq\langle a\rangle$.
Conversely, suppose that $p \in\langle a\rangle$. Then there exists $n \in \mathbb{N}$ such that $p * a^{n}=0$, that is, $(\ldots((p * a) * a) * \ldots) * a=0$. Since $a=a \wedge a$, we conclude that

$$
(\ldots((p *(a \wedge a)) *(a \wedge a)) * \ldots) *(a \wedge a)=0
$$

Also $a \wedge a \in\{a \wedge x \mid x \in X\}$, and so $p \in\langle\{a \wedge x \mid x \in X\}\rangle=a \wedge X$. Therefore $a \wedge X=\langle a\rangle$.
Definition 5. A weak closure operation "cl" on $\mathcal{I}(X)$ is said to be semi-prime if

$$
\begin{equation*}
(\forall A, B \in \mathcal{I}(X))\left(A \wedge B^{c l} \subseteq(A \wedge B)^{c l}\right) \tag{6}
\end{equation*}
$$

Example 2. Consider a lower $B C K$-semilattice $X=\{0,1,2,3,4\}$ with the following Cayley table.

| $*$ | 0 | 1 | 2 | 3 | 4 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 |
| 2 | 2 | 2 | 0 | 0 | 0 |
| 3 | 3 | 3 | 3 | 0 | 0 |
| 4 | 4 | 4 | 4 | 4 | 0 |

Note that $X$ has five ideals $A_{0}=\{0\}, A_{1}=\{0,1\}, A_{2}=\{0,1,2\}, A_{3}=\{0,1,2,3\}$ and $A_{4}=X$. Define a map $c l: \mathcal{I}(X) \rightarrow \mathcal{I}(X)$ by $A_{0}^{c l}=A_{0}, A_{1}^{c l}=A_{2}, A_{2}^{c l}=A_{2}$, $A_{3}^{c l}=A_{4}$ and $A_{4}^{c l}=A_{4}$. It is routine to check that "cl" is a semi-prime weak closure operation on $\mathcal{I}(X)$.

Proposition 2. If "cl" is a semi-prime weak closure operation on $\mathcal{I}(X)$, then

$$
\begin{equation*}
(\forall a \in X)(\forall A \in \mathcal{I}(X))\left(a \wedge A^{c l} \subseteq(a \wedge A)^{c l}\right) \tag{7}
\end{equation*}
$$

Proof. Suppose that " $c l$ " is a semi-prime weak closure operation on $\mathcal{I}(X)$. Then

$$
a \wedge A^{c l} \subseteq\langle a\rangle \wedge A^{c l} \subseteq(\langle a\rangle \wedge A)^{c l}=(a \wedge A)^{c l}
$$

for any $a \in X$ and $A \in \mathcal{I}(X)$ by using Proposition 1 .
In Proposition 2, if " $c l$ " is a weak closure operation on $\mathcal{I}(X)$ which is not semiprime, then (7) is not true in general, that is, there exist $a \in X$ and $A \in \mathcal{I}(X)$ such that $a \wedge A^{c l} \nsubseteq(a \wedge A)^{c l}$ as seen in the following example.

Example 3. Consider a lower $B C K$-semilattice $X=\{0,1,2,3,4\}$ with the following Cayley table.

| $*$ | 0 | 1 | 2 | 3 | 4 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 |
| 2 | 2 | 2 | 0 | 2 | 2 |
| 3 | 3 | 3 | 3 | 0 | 3 |
| 4 | 4 | 4 | 4 | 4 | 0 |

Then $Z(X)=\{0\}$ and $X$ has nine ideals: $A_{0}=\{0\}, A_{1}=\{0,1\}, A_{2}=\{0,1,3\}$, $A_{3}=\{0,1,2\}, A_{4}=\{0,1,4\}, A_{5}=\{0,1,2,3\}, A_{6}=\{0,1,3,4\}, A_{7}=\{0,1,2,4\}$ and $A_{8}=X$. Let $c l: \mathcal{I}(X) \rightarrow \mathcal{I}(X)$ be a function defined by $A_{4}^{c l}=A_{6}, A_{7}^{c l}=A_{8}$ and $A_{i}^{c l}=A_{i}$ for $i=1,2,3,5,6,8$. Then " $c l$ " is a weak closure operation on $\mathcal{I}(X)$. But it is not semi-prime since

$$
A_{4}^{c l} \wedge A_{2}=A_{6} \wedge A_{2}=A_{2} \nsubseteq A_{1}=A_{1}^{c l}=\left(A_{4} \wedge A_{2}\right)^{c l}
$$

On the other hand, we have

$$
3 \wedge A_{4}^{c l}=3 \wedge A_{6}=A_{2} \nsubseteq A_{1}=A_{1}^{c l}=\left(3 \wedge A_{4}\right)^{c l}
$$

for a non-zeromeet element 3 of $X$.
We provide conditions for a weak closure operation to be semi-prime.
Theorem 2. If a weak closure operation "cl" on $\mathcal{I}(X)$ satisfies the condition (7), then it is semi-prime.

Proof. We first show that

$$
\begin{equation*}
\left(\left\langle b_{1}\right\rangle+\left\langle b_{2}\right\rangle\right) \wedge A \subseteq\left\langle b_{1}\right\rangle \wedge A+\left\langle b_{2}\right\rangle \wedge A \tag{8}
\end{equation*}
$$

for all $A \in \mathcal{I}(X)$ and $b_{1}, b_{2} \in X$. If $z \in\left(\left\langle b_{1}\right\rangle+\left\langle b_{2}\right\rangle\right) \wedge A$, then there exist $x \in\left\langle b_{1}\right\rangle+\left\langle b_{2}\right\rangle$ and $a \in A$ such that $z=x \wedge a$. Since $x \in\left\langle b_{1}\right\rangle+\left\langle b_{2}\right\rangle=\left\langle\left\langle b_{1}\right\rangle \cup\left\langle b_{2}\right\rangle\right\rangle$, we have

$$
\begin{equation*}
\left(\ldots\left(\left(x * s_{1}\right) * s_{2}\right) * \ldots\right) * s_{n}=0 \tag{9}
\end{equation*}
$$

for some $s_{i} \in\left\langle b_{1}\right\rangle \cup\left\langle b_{2}\right\rangle, 1 \leqslant i \leqslant n$. Since $s_{i} \in\left\langle b_{1}\right\rangle$ or $s_{i} \in\left\langle b_{2}\right\rangle$ for $i \in\{1,2, \ldots, n\}$, it follows from (9) that $x \in\left\langle b_{1}\right\rangle$ or $x \in\left\langle b_{2}\right\rangle$. Hence

$$
z=x \wedge a \in\left\langle b_{1}\right\rangle \wedge A \text { or } z=x \wedge a \in\left\langle b_{2}\right\rangle \wedge A
$$

and thus $z \in\left\langle b_{1}\right\rangle \wedge A+\left\langle b_{2}\right\rangle \wedge A$. Therefore (8) is valid. Let $B$ be an ideal of $X$. Then $B=\sum_{b \in B}\langle b\rangle$ and $\langle b\rangle \wedge A^{c l}=b \wedge X \wedge A^{c l}=b \wedge A^{c l}$ by Proposition 1. It follows from (8) and (7) that

$$
B \wedge A^{c l}=\left(\sum_{b \in B}\langle b\rangle\right) \wedge A^{c l} \subseteq \sum_{b \in B}\left(\langle b\rangle \wedge A^{c l}\right)=\sum_{b \in B}\left(b \wedge A^{c l}\right) \subseteq \sum_{b \in B}(b \wedge A)^{c l}
$$

Since $b \in B=\sum_{b \in B}\langle b\rangle$, we have $b \wedge A \subseteq \sum_{b \in B}\langle b\rangle \wedge A$ and so

$$
(b \wedge A)^{c l} \subseteq\left(\sum_{b \in B}\langle b\rangle \wedge A\right)^{c l}
$$

Hence $\sum_{b \in B}(b \wedge A)^{c l} \subseteq\left(\sum_{b \in B}\langle b\rangle \wedge A\right)^{c l}=(B \wedge A)^{c l}$. Therefore $B \wedge A^{c l} \subseteq(B \wedge A)^{c l}$ and " $c l$ " is a semi-prime weak closure operation on $\mathcal{I}(X)$.
Definition 6. A weak closure operation " $c l$ " on $\mathcal{I}(X)$ is said to be meet if it satisfies:

$$
\begin{equation*}
(\forall A \in \mathcal{I}(X))(\forall a \in X \backslash Z(X))\left((a \wedge A)^{c l}=a \wedge A^{c l}\right) \tag{10}
\end{equation*}
$$

Example 4. Consider a lower $B C K$-semilattice $X=\{0,1,2,3,4\}$ with the following Cayley table.

| $*$ | 0 | 1 | 2 | 3 | 4 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 0 |
| 2 | 2 | 2 | 0 | 0 | 0 |
| 3 | 3 | 2 | 1 | 0 | 0 |
| 4 | 4 | 4 | 4 | 4 | 0 |

Note that $X$ has five ideals $A_{0}=\{0\}, A_{1}=\{0,1\}, A_{2}=\{0,2\}, A_{3}=\{0,1,2,3\}$ and $A_{4}=X$. Let $c l: \mathcal{I}(X) \rightarrow \mathcal{I}(X)$ be a function defined by $A_{0}^{c l}=A_{0}, A_{1}^{c l}=A_{3}$, $A_{2}^{c l}=A_{3}, A_{3}^{c l}=A_{3}$ and $A_{4}^{c l}=A_{4}$. By routine calculations, we know that " $c l$ " is a meet weak closure operation on $\mathcal{I}(X)$.

The following example shows that there exists a weak closure operation that is not meet.

Example 5. Consider a lower $B C K$-semilattice $X=\{0,1,2,3,4\}$ with the following Cayley table.

| $*$ | 0 | 1 | 2 | 3 | 4 |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 0 |
| 2 | 2 | 2 | 0 | 0 | 2 |
| 3 | 3 | 2 | 1 | 0 | 2 |
| 4 | 4 | 4 | 4 | 4 | 0 |

Recall that $X$ has six ideals: $A_{0}=\{0\}, A_{1}=\{0,1\}, A_{2}=\{0,2\}, A_{3}=\{0,1,2,3\}$, $A_{4}=\{0,1,4\}$ and $A_{5}=X$. Let $c l: \mathcal{I}(X) \rightarrow \mathcal{I}(X)$ be a function defined by $A_{0}^{c l}=A_{0}, A_{1}^{c l}=A_{3}, A_{2}^{c l}=A_{4}, A_{3}^{c l}=A_{3}, A_{4}^{c l}=A_{4}$ and $A_{5}^{c l}=A_{5}$. Then " $c l$ " is a weak closure operation on $\mathcal{I}(X)$, but it is not meet since

$$
3 \wedge A_{1}^{c l}=3 \wedge A_{3}=A_{1} \neq A_{3}=A_{1}^{c l}=\left(3 \wedge A_{1}\right)^{c l}
$$

for a non-zeromeet element 3 of $X$.
We consider relations between $\left(z \wedge A:_{\wedge} z\right)$ and $A$ for any ideal $A$ and $z \in$ $X \backslash Z(X)$. We can easily prove that $A \subseteq(z \wedge A: \wedge z)$. But the reverse inclusion is not true in general as seen in the following example.

Example 6. Consider a lower $B C K$-semilattice $X=\{0,1,2,3,4\}$ with the following Cayley table.

| $*$ | 0 | 1 | 2 | 3 | 4 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 |
| 2 | 2 | 2 | 0 | 2 | 2 |
| 3 | 3 | 3 | 3 | 0 | 3 |
| 4 | 4 | 4 | 4 | 4 | 0 |

For a non-zeromeet element 2 and an ideal $A=\{0,1,2\}$ of $X$, we have

$$
(2 \wedge\{0,1,2\}: \wedge 2)=X \nsubseteq A
$$

In the following proposition, we discuss conditions for the inclusion ( $z \wedge A:_{\wedge}$ $z) \subseteq A$ to be true. We first consider the following condition:

$$
\begin{equation*}
(\forall a, b \in X)(\forall z \in X \backslash Z(X))((a * b) \wedge z \leq(a \wedge z) *(b \wedge z)) \tag{11}
\end{equation*}
$$

The following examples show that the inequality (11) does not hold in general.
Example 7. Consider a lower $B C K$-semilattice $X=\{0,1,2,3,4\}$ with the following Cayley table.

| $*$ | 0 | 1 | 2 | 3 |
| :--- | :--- | :--- | :--- | :--- |
| 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 |
| 2 | 2 | 1 | 0 | 1 |
| 3 | 3 | 3 | 3 | 0 |

Note that 1 is a non-zeromeet element of $X$ and

$$
(2 * 3) \wedge 1=1 \not \leq 0=(2 \wedge 1) *(3 \wedge 1),
$$

which shows that the inequality (11) is not true.
Proposition 3. If $X$ satisfies the condition (11), then $\left(z \wedge A:_{\wedge} z\right) \subseteq A$ and hence $\left(z \wedge A:_{\wedge} z\right)=A$ for every $A \in \mathcal{I}(X)$ and $z \in X \backslash Z(X)$.
Proof. Suppose that $a \in(z \wedge A: \wedge z)$. Then $a \wedge z \in z \wedge A$, and so there exist $a_{1}, a_{2}, \ldots, a_{n} \in A$ such that

$$
\left(\ldots\left((a \wedge z) *\left(a_{1} \wedge z\right)\right) *\left(a_{2} \wedge z\right)\right) * \ldots *\left(a_{n} \wedge z\right)=0
$$

It follows from the condition (11) that

$$
\begin{aligned}
& \left(\ldots\left(\left(a * a_{1}\right) * a_{2}\right) * \ldots * a_{n}\right) \wedge z \\
& \leqslant\left(\ldots\left((a \wedge z) *\left(a_{1} \wedge z\right)\right) *\left(a_{2} \wedge z\right)\right) * \ldots *\left(a_{n} \wedge z\right)=0
\end{aligned}
$$

and so that $\left(\ldots\left(\left(a * a_{1}\right) * a_{2}\right) * \ldots * a_{n}\right) \wedge z=0$. Since $z \in X \backslash Z(X)$, it follows that

$$
\left(\ldots\left(\left(a * a_{1}\right) * a_{2}\right) * \ldots\right) * a_{n}=0 .
$$

Hence $a \in A$, and therefore $\left(z \wedge A:_{\wedge} z\right) \subseteq A$.
The following example illustrates Proposition 3.
Example 8. Consider a lower $B C K$-semilattice $X=\{0,1,2,3,4\}$ with the following Cayley table.

| $*$ | 0 | 1 | 2 | 3 | 4 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 0 |
| 2 | 2 | 2 | 0 | 2 | 0 |
| 3 | 3 | 3 | 3 | 0 | 0 |
| 4 | 4 | 4 | 4 | 4 | 0 |

Note that 4 is the only non-zeromeet element of $X$ and there are nine ideals: $A_{0}=\{0\}, A_{1}=\{0,1\}, A_{2}=\{0,2\}, A_{3}=\{0,3\}, A_{4}=\{0,1,2\}, A_{5}=\{0,1,3\}$, $A_{6}=\{0,2,3\}, A_{7}=\{0,1,2,3\}$ and $A_{8}=X$. We know that

$$
\left(4 \wedge A_{i}: \wedge 4\right)=\left(A_{i}: \wedge 4\right)=A_{i}
$$

for $i=0,1,2, \ldots, 8$.

We consider a characterization of a meet weak closure operation.
Theorem 3. Let $X$ satisfy the condition (11) and let "cl" be a weak closure operation on $\mathcal{I}(X)$. Then "cl" is meet if and only if it satisfies the following properties:

$$
\begin{equation*}
\langle a\rangle^{c l}=\langle a\rangle \text { and } A^{c l}=\left((a \wedge A)^{c l}:_{\wedge} a\right) \tag{12}
\end{equation*}
$$

for any $a \in X \backslash Z(X)$ and any ideal $A$ of $X$.
Proof. Suppose that " $c l$ " is a meet weak closure operation on $\mathcal{I}(X)$. Let $a$ be a non-zeromeet element and $A$ be an ideal of $X$. Then, by Propositions 1 and 3 , we have

$$
\langle a\rangle^{c l}=(a \wedge X)^{c l}=a \wedge X^{c l}=a \wedge X=\langle a\rangle
$$

and

$$
\left((a \wedge A)^{c l}: \wedge a\right)=\left(a \wedge A^{c l}: \wedge a\right)=A^{c l}
$$

respectively.
Conversely, suppose that the condition (12) is valid. For a non-zeromeet element $a$ and an ideal $A$ of $X$, we have

$$
a \wedge A^{c l}=a \wedge\left((a \wedge A)^{c l}: \wedge a\right) \subseteq(a \wedge A)^{c l}
$$

If $z \in(a \wedge A)^{c l}$, then $z \in\langle a\rangle^{c l}=\langle a\rangle$ since $a \wedge A \subseteq\langle a\rangle$. Thus

$$
z \in\langle a\rangle^{c l}=\langle a\rangle=a \wedge X
$$

and so $z=a \wedge b$ for some $b \in X$. Hence $a \wedge b \in(a \wedge A)^{c l}$, i.e., $b \in\left((a \wedge A)^{c l}:_{\wedge}\right.$ $a)=A^{c l}$. Therefore $z=a \wedge b \in a \wedge A^{c l}$ and the proof is complete.

The notion of semi-prime weak closure operation is independent to the notion of meet weak closure operation as seen in the following examples.

Example 9. Consider a lower $B C K$-semilattice $X=\{0,1,2,3,4\}$ with the following Cayley table.

| $*$ | 0 | 1 | 2 | 3 | 4 |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 |
| 2 | 2 | 1 | 0 | 2 | 0 |
| 3 | 3 | 3 | 3 | 0 | 0 |
| 4 | 4 | 4 | 4 | 4 | 0 |

Note that $Z(X)=\{0,1,2,3\}$ and $X$ has five ideals: $A_{0}=\{0\}, A_{1}=\{0,1,2\}$, $A_{2}=\{0,3\}, A_{3}=\{0,1,2,3\}$ and $A_{4}=X$. Let " $c l: \mathcal{I}(X) \rightarrow \mathcal{I}(X)$ " be a mapping defined by $A_{0}^{c l}=A_{1}, A_{1}^{c l}=A_{3}, A_{2}^{c l}=A_{3}, A_{3}^{c l}=A_{3}$ and $A_{4}^{c l}=A_{4}$. Then "cl" is a meet weak closure operation on $\mathcal{I}(X)$. But it not semi-prime since

$$
A_{1}^{c l} \wedge A_{2}=A_{3} \wedge A_{2}=A_{2} \nsubseteq A_{1}=A_{0}^{c l}=\left(A_{1} \wedge A_{2}\right)^{c l} .
$$

Example 10. Consider a lower $B C K$-semilattice $X=\{0,1,2,3,4\}$ with the following Cayley table.

| $*$ | 0 | 1 | 2 | 3 | 4 |
| :--- | :--- | :--- | :--- | :--- | :--- |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 |
| 2 | 2 | 2 | 0 | 0 | 2 |
| 3 | 3 | 3 | 2 | 0 | 3 |
| 4 | 4 | 4 | 4 | 4 | 0 |

Then $Z(X)=\{0\}$ and $X$ has five ideals: $A_{0}=\{0\}, A_{1}=\{0,1\}, A_{2}=\{0,1,2,3\}$, $A_{3}=\{0,1,4\}$ and $A_{4}=X$. Let "cl: $\mathcal{I}(X) \rightarrow \mathcal{I}(X)$ " be a mapping defined by $A_{0}^{c l}=A_{1}, A_{1}^{c l}=A_{4}, A_{2}^{c l}=A_{4}, A_{3}^{c l}=A_{4}$ and $A_{4}^{c l}=A_{4}$. Then " $c l$ " is a semi-prime weak closure operation on $\mathcal{I}(X)$. But it is not meet since

$$
4 \wedge A_{2}^{c l}=4 \wedge A_{4}=A_{3} \neq A_{4}=\left(4 \wedge A_{2}\right)^{c l}
$$

## References

[1] H. Bordbar and M.M. Zahedi, A finite type of closure operations on BCKalgebra, Appl. Math. Inf. Sci. Lett. 4 (2016), no. 2, 1 - 9.
[2] H. Bordbar and M.M. Zahedi, Semi-prime closure operations on BCK-algebra, Commun. Korean Math. Soc. 30 (2015), 385 - 402.
[3] H. Bordbar, M.M. Zahedi, S.S. Ahn and Y.B. Jun, Weak closure operations on ideals of BCK-algebras, J. Comput. Anal. Appl. 23 (2017), 51-64.
[4] H. Bordbar, M.M. Zahedi and Y.B. Jun, Relative annihilators in lower BCKsemilattices, Math. Sci. Letters 6 (2017), $149-155$.
[5] Y. Huang, BCI-algebra, Science Press, Beijing 2006.
[6] J. Meng and Y.B. Jun, BCK-algebras, Kyung Moon Sa Co., Seoul 1994.
Received May 13, 2016
H.Bordbar

Faculty of Mathematics, Statistics and Computer Science, Shahid Bahonar University, Kerman, Iran
E-mail: bordbar.amirh@gmail.com
M.M.Zahedi

Department of Mathematics, Graduate University of Advanced Technology, Mahan-Kerman, Iran E-mail: zahedi_mm@kgut.ac.ir
Y.B.Jun

Department of Mathematics Education, Gyeongsang National University, Jinju 52828, Korea
E-mail: skywine@gmail.com

# Covering semigroups of topological $n$-ary semigroups 

Wieslaw A. Dudek and Vladimir V. Mukhin


#### Abstract

We construct a topology on the covering (enveloping) semigroup of an $n$-ary topological semigroup, and study the properties of the constructed topology. Conditions under which this covering semigroup is a topological semigroup are obtained too.


## 1. Introduction

An $n$-ary semigroup ( $G,[]$ ) with a topology $\tau$ is called a topological $n$-ary semigroup if ( $G, \tau$ ) is a topological space such that the $n$-ary operation [] defined on $G$ is continuous (in all variables together). Such $n$-ary semigroups and groups were studied by many authors in various directions. C̆upona [4] proved that each topological $n$-ary group ( $G$, [ ] ) can be embedded into some topological (binary) group called the universal covering group of ( $G,[]$ ). Moreover, on this universal covering group $G^{*}$ of ( $G,[]$ ) one can define a topology $\tau$ such that $G^{*}$, endowed with this topology, is a topological group (cf. [4]). The base of this topology is formed by sets of the form $U_{1} \cdot U_{2} \cdot \ldots \cdot U_{k}$, where $U_{i}, i=1,2, \ldots, k<n$ are open subsets of $G$. Crombez and Six [3] showed that each topological $n$-ary group is homeomorphic to some topological group. Stronger result was obtained by Endres [8]: a topological $n$-ary group and a normal subgroup of index $n-1$ of the corresponding covering group are homeomorphic. On the other hand, any topological $n$-ary group is uniquely determined by some topological group and some its homeomorphism (cf. [14]). Hence topological properties of topological groups may be moved to topological $n$-ary groups and conversely.

In the case of $n$-ary semigroups the situation is more complicated. Similarly as in case of $n$-ary groups, for any topological $n$-ary semigroup can be constructed the covering semigroup. Connections between the topology of this covering semigroup and the topology of its initial an $n$-ary semigroup are described in [10] (see also [7] and [11]). In some cases an $n$-ary semigroup with a locally compact topology can be topologically embedded into a locally compact binary group as an open set (for deteils see [10]). If additionaly, this $n$-ary semigroup is cancellative and commutative, and all its inner translations (shifts), i.e., mappings of the form $\varphi_{i}(x)=\left[a_{1} l\right.$ dots, $\left.a_{i-1}, x, a_{i+1}, \ldots, a_{n}\right]$, where $a_{1}, \ldots, a_{n}$ are fixed elements,

[^2]are both continuous and open, then this $n$-ary semigroupis can be topologically embedded into a locally compact $n$-ary group as an open $n$-ary subsemigroup [12].

In this paper, the construction of a free covering semigroup of a topological $n$-ary semigroup presented in [6] is generalized to an arbitrary covering semigroup. On this covering semigroup is constructed a topology with the following properties: the right and left shifts are continuous mappings (Theorem 2.2); if an $n$-ary operation is continuous in all variables, then this $n$-ary semigroup is an open subspace of the corresponding covering semigroup (Theorem 3.1). In Theorem 3.3 are given sufficient conditions under which a Hausdorff topology of an $n$-ary semigroup can be extended to a Hausdorff topology of its covering semigroup. An explicit description of a base of a topology of an $n$-ary topological semigroup with some open translations is presented in Theorem 3.7.

## 2. Topologies on covering semigroups

Let $(G,[])$ be an $n$-ary semigroup with $n>2$. The symbol $\left[x_{1}, \ldots, x_{s}\right]$ means that $s=k(n-1)+1$ and the operation [] is applied $k$ times to the sequence $x_{1}, \ldots, x_{s}$. Consequently, $[x]$ means $x$.

By $G^{k}$ we denote the Cartesian product of $G$. If $G$ is a subset of a semigroup $(S, \cdot)$, then by $G^{(k)}$ we denote the set $G \cdot G \cdot \ldots \cdot G(k$ times $)$.

A binary semigroup ( $S, \cdot$ ) is a covering (enveloping) semigroup of an $n$-ary semi$\operatorname{group}(G,[])$ if $S$ is generated by the set $G$ and $\left[x_{1}, x_{2}, \ldots, x_{n}\right]=x_{1} \cdot x_{2} \cdot \ldots \cdot x_{n}$ for all $x_{1}, x_{2}, \ldots, x_{n} \in G$. If additionally, the sets $G, G^{(2)}, G^{(3)}, \ldots, G^{(n-1)}$ are disjoint and their union gives $S$, then $(S, \cdot)$ is called the universal covering semigroup. For each $n$-ary semigroup there exists such universal covering semigroup [5].

Below we describe connections between the the topology of an $n$-ary semigroup and the topology of its free covering semigroup. For this we use the construction of free covering semigroup proposed in [5] and the following proposition from [2] (Chapter 1, §3, Proposition 6).

Proposition 2.1. Let $\rho$ be an equivalence relation on a topological space $X$. Then a map $f$ of $X / \rho$ into a topological space $Y$ is continuous if and only if $f \circ \varphi$, where $\varphi$ is a cannonical map of $X$ onto $X / \rho$, is continuous on $X$.

Let $(S, \cdot)$ be a covering semigroup of an $n$-ary semigroup $(G,[])$. Consider the free semigroup $F$ over the set $G$. Then $F=\bigcup_{k=1}^{\infty} G^{k}$ and the operation on $F$ is defined by

$$
\begin{equation*}
\left(x_{1}, \ldots, x_{p}\right) \cdot\left(y_{1}, \ldots, y_{m}\right)=\left(x_{1}, \ldots, x_{p}, y_{1}, \ldots, y_{m}\right) . \tag{1}
\end{equation*}
$$

For any elements $\alpha=\left(x_{1}, x_{2}, \ldots, x_{p}\right), \beta=\left(y_{1}, y_{2}, \ldots, y_{m}\right)$ from $F$ we define the relation $\Omega$ by putting:

$$
\begin{equation*}
\alpha \Omega \beta \Longleftrightarrow x_{1} \cdot x_{2} \cdot \ldots \cdot x_{p}=y_{1} \cdot y_{2} \cdot \ldots \cdot y_{m} . \tag{2}
\end{equation*}
$$

Such defined relation is a congruence on $F$. Thus, the set $\bar{F}=F / \Omega=\{\bar{\alpha}: \alpha \in F\}$, where $\bar{\alpha}=\{\beta \in F: \alpha \Omega \beta\}$, with the operation $\bar{\alpha} * \bar{\beta}=\overline{\alpha \beta}$ is a semigroup. $\varphi: \alpha \mapsto \bar{\alpha}$ is a canonical mapping from $F$ onto $\bar{F}$. Moreover, the mapping $\pi: \bar{\alpha} \mapsto x_{1} \cdot x_{2} \cdot \ldots \cdot x_{p}$ is an isomorphism of semigroups $(\bar{F}, *)$ and $(S, \cdot)$. Because $\pi\left(\varphi\left(G^{i}\right)\right)=G^{(i)}$ for $i=1,2, \ldots, n-1$ and the union of all $\varphi\left(G^{i}\right)$ covers $\bar{F}$, then, in the case when $(S, \cdot)$ is the universal covering semigroup of $(G,[])$, the sets $\varphi\left(G^{i}\right)$ are pairwise disjoint. So, the semigroups $(\bar{F}, *)$ and $(S, \cdot)$ can be identified. Also can be assumed that $\varphi\left(G^{i}\right)=G^{(i)}$ for $i=1,2, \ldots, n-1$.

Let $\tau$ be a topology on $G, \tau_{k}=\tau \times \cdots \times \tau(k$ times $)$ - a topology on $G^{k}$. By $\tau_{F}$ we denote this topology on $F$ which is the union of all topologies $\tau_{k}$. Then, obviously, the operation (1) is continuous in the topology $\tau_{F}$. The quotient topology (with respect to the relation $\Omega$ ) of the topology $\tau_{F}$ is denoted by $\bar{\tau}$. It is the strongest topology on $\bar{F}$ for which the mapping $\varphi$ is continuous.

Theorem 2.2. Let $(G,[])$ be an n-ary semigroup with a free covering semigroup $F$ and $\tau$ be a topology on $G$. Then each left and each right shift on $(\bar{F}, \bar{\tau})$ is a continuous mapping. Each set $\bar{F}_{i}=\varphi\left(G^{i}\right), i=1,2, \ldots, n-1$, is open. If $(S, \cdot)$ is the universal covering semigroup of $(G,[])$, then each set $\bar{F}_{i}$ is open-closed.

Proof. Let $R_{a}$ and $r_{\bar{a}}$ be right shifts in $F$ and $\bar{F}$, respectively. Then $\varphi \circ R_{a}=$ $r_{\bar{a}} \circ \varphi$. Since $\varphi$ and $R_{a}$ are continuous, by Proposition 2.1, $r_{\bar{a}}$ is continuous too. Analogously we can prove the continuity of left shifts.

The second statement of the theorem follows from the fact that the sets $\varphi^{-1}\left(\overline{F_{i}}\right)$ $=\bigcup_{k=0}^{\infty} G^{k(n-1)+i} \in \tau_{F}$ are saturated with respect to the relation $\Omega$.

In the case when $(S, \cdot)$ is a universal covering semigroup of $(G,[])$ the open sets $\overline{F_{i}}, i=1, \ldots, n-1$, form a partition of $\bar{F}$ and, therefore, are open-closed.

We will need also the following result proved in [9].
Proposition 2.3. Let $S$ be a locally compact, $\sigma$-compact Hausdorff topological semigroup and $\theta$ be a closed congruence on $S$. Then $S / \theta$ is a topological semigroup.

## 3. Topologies on universal covering semigroups

An $n$-ary semigroup ( $G,[]$ ) with a topology $\tau$ is called a topological $n$-ary semigroup if $(G, \tau)$ is a topological space such that the $n$-ary operation [ ] is continuous (in all variables together).

Theorem 3.1. If $(G,[], \tau)$ is a topological n-ary semigroup, then topologies $\bar{\tau}$ and $\tau$ coincide on $G$.

Proof. Let $U \in \bar{\tau}, U \subset G$. Then $\varphi^{-1}(U) \in \tau_{F}$. Thus $U=\varphi^{-1}(U) \cap G \in \tau$.
Let now $U \in \tau$ and $\alpha=\left(a_{1}, \ldots, a_{p}\right) \in \varphi^{-1}(U)$. Then, $\bar{a}_{1} * \ldots * \bar{a}_{p} \in U$, where $p=k(n-1)+1$, and consequently, $\left[a_{1}, \ldots, a_{p}\right]=\bar{a}_{1} * \ldots * \bar{a}_{p} \in U$. Since
the operation [ ] is continuous in all variables, in the topology $\tau$ there are the neighborhoods $V_{1}, \ldots, V_{p}$ of points $\bar{a}_{1}, \ldots, \bar{a}_{p}$ such that $\left[x_{1}, \ldots, x_{p}\right] \in U$ for all $x_{i} \in V_{i}, i=1, \ldots, p$. Therefore, $\varphi\left(x_{1}, \ldots, x_{p}\right)=\bar{x}_{1} * \ldots * \bar{x}_{p}=\left[x_{1}, \ldots, x_{p}\right] \in U$. Consequently, $\varphi^{-1}(U) \supset V_{1} \times \ldots \times V_{p} \in \tau_{F}$. So $\varphi^{-1}(U) \in \tau_{F}$. This together with saturation of $\varphi^{-1}(U)$ gives $U \in \bar{\tau}$.

Example 3.2. Consider on the real interval $G=(1,+\infty)$ the ternary operation $\left[x_{1}, x_{2}, x_{3}\right]=x_{1}+x_{2}+x_{3}$ and the topology $\tau$ which is a union on the topology $\tau_{1}$ on $(1,2]$, the discrete topology on $(2,3]$ and the usual topology on $(3,+\infty)$, where the sets $(a, b]$ with $1 \leqslant a \leqslant b \leqslant 2$ form the basis of the topology $\tau_{1}$. Such defined ternary operation is continuous in all variables together and the semigroup $(G,+)$ is the covering semigroup for $(G,[])$. The shift $x \mapsto x+1.5$ is not a continuous map, since the preimage of the open set $\{3\}$ is not an open set. So, on the set $G$ the topologies $\bar{\tau}$ and $\tau$ are different.

Note that the topology $\bar{\tau}$ is the union of the usual topology on $(3,+\infty)$ and the topology on $(1,3]$ with the base of the form $(a, b]$, where $1 \leqslant a \leqslant b \leqslant 3$.

Consider the set $S=G \cup G_{1}$, where $G_{1}=(2,+\infty) \times\{0\}$, with the commutative binary operation $*$ defined for $x, y \in G$ in the following way:

$$
\begin{aligned}
x * y & =(x+y, 0) \\
x *(y, 0) & =(y, 0) * x=x+y \\
(x, 0) *(y, 0) & =(x+y, 0)
\end{aligned}
$$

It is easy to verify that $(S, *)$ a commutative universal covering semigroup of an $n$-ary semigroup ( $G,[]$ ). On $G$ the topology $\bar{\tau}$ coincides with the topology $\tau$, but the restriction of $\bar{\tau}$ to $G_{1}$ gives the topology with the base formed by sets $(a, b] \times\{0\}$ and $(c, d) \times\{0\}$, where $2 \leqslant a \leqslant b \leqslant 4 \leqslant c \leqslant d$.

Theorem 3.3. If in the universal covering semigroup $(S, \cdot)$ of an n-ary semigroup ( $G,[]$ ) with the Hausdorff topology $\tau$ for any $x_{1}, \ldots, x_{i}, y_{1}, \ldots, y_{i} \in G$ such that $x_{1} \cdot \ldots \cdot x_{i} \neq y_{1} \cdot \ldots \cdot y_{i}$, where $1 \leqslant i<n$, there are $z_{i+1}, \ldots, z_{n} \in G$ such that

$$
\begin{aligned}
& x_{1} \cdot \ldots \cdot x_{i} \cdot z_{i+1} \cdot \ldots \cdot z_{n} \neq y_{1} \cdot \ldots \cdot y_{i} \cdot z_{i+1} \cdot \ldots \cdot z_{n} \quad \text { or } \\
& z_{i+1} \cdot \ldots \cdot z_{n} \cdot x_{1} \cdot \ldots \cdot x_{i} \neq z_{i+1} \cdot \ldots \cdot z_{n} \cdot y_{1} \cdot \ldots \cdot y_{i},
\end{aligned}
$$

then the topology $\bar{\tau}$ on $\bar{F}$ is the Hausdorff topology, too.
Proof. Consider the first case when for some $x_{1}, \ldots, x_{i}, y_{1}, \ldots, y_{i}, z_{i+1}, \ldots z_{n} \in G$ we have $\tilde{x}=x_{1} \cdot \ldots \cdot x_{i} \neq y_{1} \cdot \ldots \cdot y_{i}=\tilde{y}$ and $x=x_{1} \cdot \ldots \cdot x_{i} \cdot z_{i+1} \cdot \ldots \cdot z_{n} \neq$ $y_{1} \cdot \ldots \cdot y_{i} \cdot z_{i+1} \cdot \ldots \cdot z_{n}=y . \tau$ is the Hausdorff topology, so there are neighborhoods $U_{x}$ and $U_{y}$ of $x$ and $y$ such that $U_{x} \cap U_{y}=\emptyset$. Since shifts in $(\bar{F}, \bar{\tau})$ are continuous and $x=\tilde{x} \cdot \tilde{z}, y=\tilde{y} \cdot \tilde{z}$ for $\tilde{z}=z_{i+1} \cdot \ldots \cdot z_{n}$, there are neighborhoods $W_{x}$ and $W_{y}$ of points $\tilde{x}$ and $\tilde{y}$ such that $W_{x} \cdot \tilde{z} \subset U_{x}$ and $W_{y} \cdot \tilde{z} \subset U_{y}$. So, $W_{x} \cap W_{y}=\emptyset$. Thus $\bar{\tau}$ is the Hausdorff topology.

The second case can be proved analogously.

Corollary 3.4. If the universal covering semigroup of an n-ary semigroup (G, [ ]) with the Hausdorff topology $\tau$ is left or right cancellative, then the topology $\bar{\tau}$ on $\bar{F}$ is the Hausdorff topology.

Theorem 3.5. If the universal covering semigroup $(S, \cdot)$ of a topological n-ary semigroup $(G,[])$ with the Hausdorff topology $\tau$ has at least one left or right cancellable element, then the congruence $\Omega$ is a closed subset in a topological space $\left(F \times F, \tau_{F} \times \tau_{F}\right)$.

Proof. Suppose that in $\left(F \times F, \tau_{F} \times \tau_{F}\right)$ the sequence $\left(\alpha_{\xi}, \beta_{\xi}\right)_{\xi \in A} \in \Omega$ converges to $(\alpha, \beta)$. This means that in the topological space $\left(F, \tau_{F}\right)$ the sequences $\left(\alpha_{\xi}\right)_{\xi \in A}$ and $\left(\beta_{\xi}\right)_{\xi \in A}$ converge to $\alpha$ and $\beta$, respectively.

Let $\alpha=\left(x_{1}, \ldots, x_{p}\right) \in G^{p}, \beta=\left(y_{1}, \ldots, y_{q}\right) \in G^{q}$. Since $G^{p}, G^{q}$ are disjoint open-closed subsets in $\left(F, \tau_{F}\right)$, there is an index $\xi_{0} \in A$ such that $\alpha_{\xi}=$ $\left(x_{1}^{\xi}, \ldots, x_{p}^{\xi}\right) \in G^{p}$ and $\beta_{\xi}=\left(y_{1}^{\xi}, \ldots, y_{q}^{\xi}\right) \in G^{q}$ for all $\xi>\xi_{0}$. Therefore, for $\xi>\xi_{0}$ we have $x_{1}^{\xi} \cdot \ldots \cdot x_{p}^{\xi}=y_{1}^{\xi} \cdot \ldots \cdot y_{q}^{\xi}$. Consequently,

$$
\begin{equation*}
a^{f} \cdot x_{1}^{\xi} \cdot \ldots \cdot x_{p}^{\xi}=a^{f} \cdot y_{1}^{\xi} \cdot \ldots \cdot y_{q}^{\xi} \tag{3}
\end{equation*}
$$

for any left cancellable element $a \in S$ and all natural $f$.
Obviously, $a=a_{1} \cdot \ldots \cdot a_{k}$ for some $a_{1}, \ldots, a_{k} \in G$ and $k<n$. Moreover, for each natural $f$ such that $f k \geqslant n$ there is a natural $r$ satisfying the condition $r(n-1)+1 \leqslant f k+p<(r+1)(n-1)+1$. Thus $f k+p-s=r(n-1)+1$ for some $0 \leqslant s<k$. Consequently,

$$
\begin{aligned}
& a_{1} \cdot \ldots a_{s} \cdot[a_{s+1}, \ldots, a_{k}, \underbrace{\underbrace{a_{1}, \ldots, a_{k}}_{1}}_{f-1 \text { times }}, \ldots, \underbrace{a_{1}, \ldots, a_{k}}_{\text {times }}, x_{1}^{\xi}, \ldots, x_{p}^{\xi}]= \\
& a_{1} \cdot \ldots a_{s} \cdot[a_{s+1}, \ldots, a_{k}, \underbrace{\underbrace{\xi}_{1}}_{\underbrace{a_{1}, \ldots, a_{k}}_{\text {times }}, \ldots, \underbrace{a_{1}, \ldots, a_{k}}}, \ldots, y_{p}^{\xi}] .
\end{aligned}
$$

By previous results, $\bar{\tau}$ is the Hausdorff topology which on $G$ coincides with $\tau$ and each left shift in $(\bar{F}, \bar{\tau})$ is a continuous mapping. So, if in $(G, \tau)$ the sequence $\left(x_{i}^{\xi}\right)_{\xi \in A}$ converge to $x_{i}$ and $\left(y_{i}^{\xi}\right)_{\xi \in A}$ converge to $y_{i}$, then (3) implies $a \cdot x_{1} \cdot \ldots \cdot x_{p}=$ $a \cdot y_{1} \cdot \ldots \cdot y_{q}$, which, by the cancellativity of $a$, gives $x_{1} \cdot \ldots \cdot x_{p}=y_{1} \cdot \ldots \cdot y_{q}$. Thus $(\alpha, \beta) \in \Omega$ and $\Omega$ is a closed subset of $\left(F \times F, \tau_{F} \times \tau_{F}\right)$.

For a right cancellable element the proof is similar.
Theorem 3.6. If the universal covering semigroup ( $S, \cdot$ ) of a topological n-ary semigroup $(G,[])$ with the locally compact and $\sigma$-compact Hausdorff topology $\tau$ has at least one left or right cancellable element, then $(\bar{F}, *)$ is a topological semigroup with respect to the topology $\bar{\tau}$.

Proof. Note that the topology $\tau_{F}$ on $F$ is a locally compact, $\sigma$-compact, and the congruence $\Omega$ is a closed subset of $F$. Then, by Proposition 2.3, $(\bar{F}, *, \bar{\tau})$ is a topological semigroup.

Theorem 3.7. Let in a topological n-ary semigroup $(G,[], \tau)$ for certain $1 \leqslant p<n$ all translations $x \mapsto\left[c_{1}, \ldots, c_{p}, x, c_{p+1} \ldots, c_{n-1}\right]$ be continuous. If the universal covering semigroup $(S, \cdot)$ of $(G,[])$ is cancellative, then $(\bar{F}, *, \bar{\tau})$ is a topological semigroup, $G$ is an open-closed subset in $\bar{F}$ and the family

$$
\mathcal{B}=\left\{A_{1} \cdot \ldots \cdot A_{k}: A_{1}, \ldots, A_{k} \in \tau, k=1, \ldots, n-1\right\}
$$

forms the base of the topology $\bar{\tau}$.
Proof. Let $A_{1}, \ldots, A_{k}$ be open sets in $\tau$. We will show that the set $A_{1} \cdot \ldots \cdot A_{k}$ is open in $\bar{\tau}$.

Let $a \in G, a_{1} \in A_{1}, \ldots, a_{k} \in A_{k}$. Then

$$
\left[\begin{array}{l}
(l) \\
a
\end{array}, a_{1}, \ldots, a_{i-1}, A_{i}, a_{i+1}, \ldots, a_{k}, \stackrel{(n-k-l)}{a}\right] \subset\left[\begin{array}{l}
(l) \\
a
\end{array}, A_{1}, \ldots, A_{k}, \stackrel{(n-k-l)}{a}\right]
$$

for all $k+l \leqslant n, i \leqslant k$ and $l+i=p+1$, where $\stackrel{(s)}{a}$ means the sequence $a, \ldots, a(s$ times). By hypothesis, the set $\left[\begin{array}{c}(l) \\ a\end{array}, a_{1}, \ldots, a_{i-1}, A_{i}, a_{i+1}, \ldots, a_{k}, \stackrel{n-k-l)}{a}\right]$ is open in $G$. Since

$$
\left[\stackrel{(l)}{a}, A_{1}, \ldots, A_{k}, \stackrel{(n-k-l)}{a}\right]=\bigcup_{\substack{i=1 \\ a_{j} \in A_{j}}}^{k}\left[\stackrel{(l)}{a}, a_{1}, \ldots, a_{i-1}, A_{i}, a_{i+1}, \ldots, a_{k}, \stackrel{(n-k-l)}{a}\right]
$$

the set $\left[\begin{array}{l}(l) \\ a\end{array}, A_{1}, \ldots, A_{k}, \stackrel{(n-k-l)}{a}\right]$ also is open in $G$.
As was noted earlier, $(\bar{F}, *)$ as a semigroup isomorphic to $(S, \cdot)$, can be identified with $(S, \cdot)$ and treated as a cancellative semigroup.

Consider the translation $\lambda: \bar{F} \rightarrow \bar{F}$ defined by $\lambda(x)=a^{p} x a^{n-p-1}$. We have

$$
\begin{equation*}
\lambda^{-1}\left(\left[\frac{p)}{a}, A_{1} \cdot \ldots \cdot A_{k}, \stackrel{(n-p-1)}{a}\right]\right)=A_{1} \cdot \ldots \cdot A_{k} \tag{4}
\end{equation*}
$$

Indeed, if $x \in \lambda^{-1}\left(\left[\stackrel{(p)}{a}, A_{1} \cdot \ldots \cdot A_{k}, \stackrel{(n-p-1)}{a}\right]\right)$, then

$$
\lambda(x)=a^{p} x a^{n-p-1} \in\left[\stackrel{(p)}{a}, A_{1} \cdot \ldots \cdot A_{k}, \stackrel{(n-p-1)}{a}\right]=a^{p} \cdot A_{1} \cdot \ldots \cdot A_{k} \cdot a^{n-p-1}=a^{p} y a^{n-p-1}
$$

for some $y \in A_{1} \cdot \ldots \cdot A_{k}$, which, by cancellativity, implies $x=y$. So, $x \in A_{1} \cdot \ldots \cdot A_{k}$.
On the other hand, if $x \in A_{1} \cdot \ldots \cdot A_{k}$, then

$$
a^{p} x a^{n-p-1} \in a^{p} \cdot A_{1} \cdot \ldots \cdot A_{k} \cdot a^{n-p-1}=\left[\stackrel{(p)}{a}, A_{1} \cdot \ldots \cdot A_{k}, \stackrel{(n-p-1)}{a}\right] .
$$

Thus $x \in \lambda^{-1}\left(\left[\stackrel{(p)}{a}, A_{1} \cdot \ldots \cdot A_{k}, \stackrel{(n-p-1)}{a}\right]\right)$. This completes the proof of (4).
The set $\left[\stackrel{(p)}{a}, A_{1} \cdot \ldots \cdot A_{k}, \stackrel{(n-p-1)}{a}\right]$ is open in $G$, hence, by Theorem 3.1, it is open in $(\bar{F}, \bar{\tau})$. By Theorem 2.2, the mapping $\lambda$ is continuous and therefore $A_{1} \cdot \ldots \cdot A_{k}=$ $\lambda^{-1}\left(\left[{ }_{a}^{(p)}, A_{1} \ldots \cdot A_{k}, \stackrel{(n-p-1)}{a}\right]\right) \in \bar{\tau}$.

If $U \subset G^{(k)}, U \in \bar{\tau}$ and $a_{1}, \ldots, a_{k} \in G$ such that $a_{1} \ldots a_{k} \in U$, then $W=\varphi^{-1}(U) \in \bar{\tau}$, where $\varphi(x)=a_{1} \cdot \ldots \cdot a_{k} \cdot x$ is a left shift in $\bar{F}$. Consequently $W \in \tau$, because $W \subset G$. So, for any $a \in G$, the set

$$
\left[\stackrel{(n-k+p)}{a}, a_{1}, \ldots, a_{k-1}, W, \stackrel{(n-p-1)}{a}\right]=\left[\stackrel{(p-1)}{a},\left[\stackrel{(n-k+1)}{a}, a_{1}, \ldots, a_{k-1}\right], W, \stackrel{n-p-1)}{a}\right]
$$

is an open subset of $G$.
Since in $(G, \tau)$ the $n$-ary operation [] is continuous in all variables, there exist the family of open neighborhoods $U_{1}, \ldots, U_{k}$ of the points $a_{1}, \ldots, a_{k}$, respectively, such that

$$
\left[\stackrel{(n-k+p)}{a}, U_{1}, \ldots, U_{k}, \stackrel{(n-p-1)}{a}\right] \subset\left[\stackrel{(n-k+p)}{a}, a_{1}, \ldots, a_{k-1}, W, \stackrel{(n-p-1)}{a}\right]
$$

Thus, in $\bar{F}$, we have

$$
a^{n-k+p} \cdot U_{1} \cdot \ldots \cdot U_{k} \cdot a^{n-p-1} \subset a^{n-k+p} \cdot a_{1} \cdot \ldots \cdot a_{k-1} \cdot W \cdot a^{n-p-1}
$$

Because $a_{1} \cdot \ldots \cdot a_{k-1} \cdot W \subset U$, the last implies

$$
a^{n-k+p} \cdot U_{1} \cdot \ldots \cdot U_{k} \cdot a^{n-p-1} \subset a^{n-k+p} \cdot U \cdot a^{n-p-1}
$$

This, in view of the cancellativity, gives $U_{1} \cdot \ldots \cdot U_{k} \subset U$.
By virtue of the arbitrariness of the point $a_{1} \cdot \ldots \cdot a_{k} \in U$, we conclude that the family $\mathcal{B}$ is a base of the topology $\bar{\tau}$ on $\bar{F}$.

Now we will show that the binary operation defined in $\bar{F}$ is continuous in the topology $\bar{\tau}$. Let $g=s \cdot t$ for some $s=a_{1} \cdot \ldots \cdot a_{i}, t=b_{1} \cdot \ldots \cdot b_{j}$, where $a_{1}, \ldots, a_{i}, b_{1}, \ldots, b_{j} \in G$ and $1 \leqslant i, j<n$. If $C \in \mathcal{B}$ and $g \in C$, then $C=C_{1} \cdot \ldots \cdot C_{k}$ for some $k<n$ and $\emptyset \neq C_{i} \in \tau$. Let $g=c_{1} \cdot \ldots \cdot c_{k}$ for some $c_{i} \in C_{i}$. If $i+j<n$, then $s \cdot t=a_{1} \cdot \ldots \cdot a_{i} \cdot b_{1} \cdot \ldots \cdot b_{j}=c_{1} \cdot \ldots \cdot c_{k}$. Thus $i+j=k$.

From the cancellativity of the binary operation in $\bar{F}$ and the continuity of the $n$-ary operation [], we conclude that there exist open neighborhoods $A_{1}, \ldots, A_{i}$ of the points $a_{1}, \ldots, a_{i}$, respectively, and open neighborhoods $B_{1}, \ldots, B_{j}$ of the points $b_{1}, \ldots, b_{j}$ such that $A_{1} \cdot \ldots \cdot A_{i} \cdot B_{1} \cdot \ldots \cdot B_{j} \subset C_{1} \cdot \ldots \cdot C_{k}=C$. Since $A=A_{1} \cdot \ldots \cdot A_{i}$ and $B=B_{1} \cdot \ldots \cdot B_{j}$ are open neighborhoods of the points $s, t$, respectively, the last inclusion implies $A \cdot B \subset C$.

In the case $i+j \geqslant n$ we have $c_{1} \cdot \ldots \cdot c_{k}=a_{1} \cdot \ldots \cdot a_{i} \cdot b_{1} \cdot \ldots \cdot b_{j}=a \cdot b_{n-i+1} \cdot \ldots \cdot b_{j}$ for $a=\left[a_{1}, \ldots, a_{i}, b_{1}, \ldots, b_{n-i}\right]$. So, as above, we conclude that $k=i+j-n$ and there are open neighborhoods $D, B_{n-i+1}, \ldots, B_{j}$ of the points $a, b_{n-i+1}, \ldots, b_{j}$, respectively, such that $D \cdot B_{n-i+1} \cdot \ldots \cdot B_{j} \subset C_{1} \cdot \ldots \cdot C_{k}=C$. Since the $n$-ary operation [] is continuous, then there are open neighborhoods $A_{1}, \ldots, A_{i}$ of the points $a_{1}, \ldots, a_{i}$ and open neighborhoods $B_{1}, \ldots, B_{n-i}$ of the points $b_{1}, \ldots, b_{n-i}$ such that $\left[A_{1}, \ldots, A_{i}, B_{1}, \ldots, B_{n-i}\right] \subset D$. Thus, for $A=A_{1} \cdot \ldots \cdot A_{i}, B=B_{1} \cdot \ldots \cdot B_{j}$ we have $A, B, \in \mathcal{B}, A \cdot B \subset C$ and $s \in A, t \in B$. This proves that the binary multiplication defined in $\bar{F}$ is continuous in the topology $\bar{\tau}$.

Corollary 3.8. If $(G,[], \tau)$ is a topological n-ary group, then its universal covering group $(\bar{F}, *)$ is a topological group with the topology $\bar{\tau}$.

The proof follows immediately from the preceding theorem and the results of [4], where is proved that the operation of taking inverse element is continous if the family $\mathcal{B}$ is a base of the corresponding topology.

## References

[1] H. Boujouf, The topology in the n-ary semigroups, definable by the deflection systems, (Russian), Voprosy Algebry 10 (1996), 187 - 189.
[2] N. Bourbaki, Topologie générale. Structures topologiques, Hermann, Pais, 1965.
[3] G. Crombez, G. Six, On topological n-groups, Abh. Math. Sem. Univ. Hamburg 41 (1974), 115 - 124.
[4] G. Čupona, On topological n-group, Bull. Soc. Math. Phys. R. S. Macedoine 22 (1971), 5 - 10.
[5] G. Čupona, N. Celakoski, On representation of $n$-associatives into semigroups, Makedon. Akad. Nauk. Umet. Oddel. Prirod. Mat. Nauk. Prilozi 6 (1974), $23-34$.
[6] W.A. Dudek, V.V. Mukhin, On topological n-ary semigroups, Quasigroups and Related Systems 3 (1996), $73-88$.
[7] W.A. Dudek, V.V. Mukhin, Free covering semigroups of topological $n$-ary semigroups, Quasigroups and Related Systems 22 (2014), $67-70$.
[8] N. Endres, On topological n-groups and their corresponding groups, Discuss. Math. Algebra Stochastic Methods 15 (1995), 163 - 169.
[9] J.D. Lawson, B.L. Madison, On congruences and cones, Math. Zeitshrift 120 (1971), $18-24$.
[10] V.V. Mukhin, On topological n-semigroups, Quasigroups and Related Systems 4 (1997), $39-49$.
[11] V.V. Mukhin, Topological covering semigroups of topological n-ary semigroups, (Russian), Proc. Confer. Theoretical and applied aspects of mathematics, science and education, Akhangelsk (2014), $248-252$.
[12] V.V. Mukhin, Kh. Buzhuf, On the embedding of n-ary abelian topological semigroups into n-ary topological groups, (Russian) Problems in Algebra 9 (1996), $157-160$.
[13] M.S. Pop, On the boundary in topological n-semigroups, Mathematica ( Cluj ) $22(45)(1980), 127-130$.
[14] M. Žižović, A topological analogue of the Hosszú-Gluskin theorem, (Serbo-Croatian) Mat. Vesnik 13(28) (1976), no. 2, 233 - 235.

Received January 03, 2017
W.A. Dudek

Faculty of Pure and Applied Mathematics, Wroclaw University of Science and Technology, Wroclaw, Poland
E-mail: wieslaw.dudek@pwr.edu.pl
V.V. Mukhin

Vologda Institute of Law and Economics of the Federal Penal Service of Russia, Vologda, Russia
E-mail: mukhinv1945@yandex.ru

# Identities in right Hom-alternative superalgebras 

## A. Nourou Issa


#### Abstract

Some fundamental identities characterizing right Hom-alternative superalgebras are found. These identities are the $\mathbb{Z}_{2}$-graded Hom-versions of well-known identities in right alternative algebras


## 1. Introduction

A right alternative algebra is an algebra satisfying the right alternative identity:

$$
(x y) y=x(y y) .
$$

If, moreover, it satisfies the left alternative identity $(x x) y=x(x y)$, then it is called an alternative algebra. Alternative algebras were studied ([28]) in connection with some problems related to projective planes (see also [17]). The 8-dimensional Cayley algebra is an example of an alternative algebra that is not associative. For fundamentals on alternative algebras, one may refer to [5], [19], [27].

As a generalization of alternative algebras, right alternative algebras were first studied in [1], where an example of a five-dimensional right alternative algebra that is not left alternative is constructed. For further studies on right alternative algebras one may refer, e.g., to [11], [21], [22] (see also [27] and references therein).

A $\mathbb{Z}_{2}$-graded generalization of Lie theory is considered in [4] and [16] with the introduction of the $\mathbb{Z}_{2}$-graded version of Lie algebras (now called Lie superalgebras). Next, the $\mathbb{Z}_{2}$-gradation of algebras is extended to other types of algebras in [10], [20] and [26].

Another generalization of usual algebras is the one of Hom-type generalization of algebras with the introduction of Hom-Lie algebras in [8] (see also [12], [13]). The defining identity of a Hom-Lie algebra is a twisted version of the usual Jacobi identity by a linear map, and the corresponding twisted associative algebra, called Hom-associative algebra, is introduced in [15]. Since then, various Hom-type algebras were defined and studied (see, e.g., [15], [14], [2], [23], [24], [9], [7], [3]). Observe that, in general, the twisting map in a Hom-algebra is neither injective nor surjective (see, e.g., [6] for a study on this topic). A $\mathbb{Z}_{2}$-graded generalization of Hom-Lie algebras is defined in [2].

In [25] the Hom-versions of some well-known identities in right alternative algebras ([11], [21], [22]) are found. The purpose of this short paper is to discuss

Keywords: right alternative superalgebra, Hom-algebra, right Hom-alternative superalgebra.
the $\mathbb{Z}_{2}$-graded versions of the identities found in [25]. Other identities are also proposed. These Hom-super identities could be useful as a working tool in further investigations related to Hom-alternative superalgebras.

In Section 2 we recall some useful notions on Hom-superalgebras and prove some general identities that hold in any Hom-superalgebra. In Section 3 we define the $\mathbb{Z}_{2}$-graded Hom-version of the function $g(w, x, y, z)$ (that is first defined in [11] for right alternative algebras, and its Hom-version is defined in [25]) and we prove that it is identically zero. Next, using essentially the identity $g(w, x, y, z)=0$ along with the Hom-Teichmüller identity, we prove some fundamental identities characterizing right Hom-alternative superalgebras. As a consequence, we obtained the $\mathbb{Z}_{2}$-graded Hom-version of the right Bol identity.

All vector spaces and algebras are considered over a ground field of characteristic not 2 .

## 2. Definitions and some general results

Let $\mathbb{Z}_{2}=\{0,1\}$ be the field of integers modulo 2 . A vector space $A$ is said to be $\mathbb{Z}_{2}$-graded if $A=A_{0} \oplus A_{1}$ (then $A$ is also called a superspace).

Definition 2.1. A triple $(A, \cdot, \alpha)$ is called a (binary) Hom-superalgebra (i.e., a $\mathbb{Z}_{2}$-graded binary Hom-algebra), if $A$ is a superspace, "." a binary operation on $A$ such that $A_{i} \cdot A_{j} \subseteq A_{i+j}, i, j \in \mathbb{Z}_{2}$, and $\alpha$ a linear self-map of $A$ such that $\alpha\left(A_{i}\right) \subseteq A_{i}$ (and then $\alpha$ is said to be even). The subspaces $A_{0}$ and $A_{1}$ are called respectively the even and odd parts of the Hom-superalgebra $A$; so are also called the elements from $A_{0}$ and $A_{1}$ respectively.

All elements in $A$ are assumed to be homogeneous, i.e., either even or odd. For a given homogeneous element $x \in A_{i}(i=0,1)$, by $\bar{x}=i$ we denote its parity. Since $\alpha$ is even, $\overline{\alpha(x)}=\bar{x}$ (we shall use this fact in the sequel without any further comment). In order to reduce the number of braces, we use juxtaposition whenever applicable and so, e.g., $x y \cdot z$ means $(x \cdot y) \cdot z$. Moreover, for simplicity and where there is no danger of confusion, we write $x y$ in place of $x \cdot y$.

In a Hom-superalgebra $(A, \cdot, \alpha)$, the supercommutator and the super Jordan product of any two elements $x, y \in A$ are defined respectively as

$$
[x, y]:=x y-(-1)^{\bar{x}} \bar{y} y x \quad \text { and } \quad x \circ y:=x y+(-1)^{\bar{x}} \bar{y} y x .
$$

For any $x, y, z \in A$, the Hom-associator $(x, y, z)$ is defined as

$$
(x, y, z):=x y \cdot \alpha(z)-\alpha(x) \cdot y z
$$

Definition 2.2. ([2]). A Hom-superalgebra $(A, \cdot, \alpha)$ is called a Hom-Lie superalgebra if it is super anticommutative and satisfies the super Hom-Jacobi identity, i.e.,

$$
x y=-(-1)^{\overline{x y}} y x, \quad \text { and }
$$

$$
x y \cdot \alpha(z)+(-1)^{\bar{x}(\bar{y}+\bar{z})} y z \cdot \alpha(x)+(-1)^{\bar{z}(\bar{x}+\bar{y})} z x \cdot \alpha(y)=0
$$

for all $x, y, z \in A$. A Hom-superalgebra $(A, \cdot, \alpha)$ is said to be Hom-Lie admissible, if $(A,[],, \alpha)$ is a Hom-Lie superalgebra.

Definition 2.3. A Hom-superalgebra $A$ is said to be right Hom-alternative if

$$
\begin{equation*}
\left.(x, y, z)=-(-1)^{\bar{y} \bar{z}}(x, z, y) \quad \text { (right superalternativity }\right) \tag{2.1}
\end{equation*}
$$

for all $x, y, z \in A$. If the left superalternativity $(x, y, z)=-(-1)^{\bar{x}} \bar{y}(y, x, z)$ holds in $A$, then $A$ is said to be Hom-alternative i.e., $-(-1)^{\bar{x}} \bar{y}(y, x, z)=(x, y, z)=$ $-(-1)^{\bar{y} \bar{z}}(x, z, y)$ (superalternativity).

If $A$ has zero odd part, then (2.1) reads as $(x, y, z)=-(x, z, y)$ which is the linearized form of the right Hom-alternativity $x y \cdot \alpha(y)=\alpha(x) \cdot y y$.

The following trilinear function is introduced in [2]:

$$
S(x, y, z):=(x, y, z)+(-1)^{\bar{x}(\bar{y}+\bar{z})}(y, z, x)+(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y)
$$

(this definition differs from the one in [2] by the factor $(-1)^{\bar{x} \bar{z}}$ ).
Consider in a Hom-superalgebra $A$ the following multilinear function

$$
\begin{aligned}
f(w, x, y, z):= & (w x, \alpha(y), \alpha(z))-(\alpha(w), x y, \alpha(z))+(\alpha(w), \alpha(x), y z) \\
& -\alpha^{2}(w)(x, y, z)-(w, x, y) \alpha^{2}(z) .
\end{aligned}
$$

The following identities hold in any Hom-superalgebra.
Proposition 2.4. Let $(A, \cdot, \alpha)$ be a Hom-superalgebra. Then

- $f(w, x, y, z)=0$,
- $[x y, \alpha(z)]-\alpha(x)[y, z]-(-1)^{\bar{y} \bar{z}}[x, z] \alpha(y)=$

$$
\begin{equation*}
(x, y, z)-(-1)^{\bar{y} \bar{z}}(x, z, y)+(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y) \tag{2.3}
\end{equation*}
$$

- $[x y, \alpha(z)]-[x, y] \alpha(z)+(-1)^{\bar{y} \bar{z}}[x z, \alpha(y)]-(-1)^{\bar{y} \bar{z}}[x, z] \alpha(y)=$

$$
\begin{equation*}
(-1)^{\bar{x} \bar{y}}(y, x, z)+(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y) \tag{2.4}
\end{equation*}
$$

- $[x y, \alpha(z)]+(-1)^{\bar{x}(\bar{y}+\bar{z})}[y z, \alpha(x)]+(-1)^{\bar{z}(\bar{x}+\bar{y})}[z x, \alpha(y)]=S(x, y, z)$,
- $(x \circ y) \circ \alpha(z)-(-1)^{\bar{y} \bar{z}}(x \circ z) \circ \alpha(y)=$

$$
\begin{equation*}
S(x, y, z)-(-1)^{\bar{x}} \bar{y} S(y, x, z)-2(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y)+[\alpha(x),[y, z]] \tag{2.6}
\end{equation*}
$$

for all $w, x, y, z$ in $A$.
Proof. The identity (2.2) follows by direct expansion of associators in $f(w, x, y, z)$. Next we have
$[x y, \alpha(z)]-\alpha(x)[y, z]-(-1)^{\bar{y} \bar{z}}[x, z] \alpha(y)=x y \cdot \alpha(z)-(-1)^{\bar{z}(\bar{x}+\bar{y})} \alpha(z) \cdot x y$

$$
\begin{aligned}
& -\alpha(x)\left(y z-(-1)^{\bar{y} \bar{z}} z y\right)-(-1)^{\bar{y}} \bar{z}\left(x z-(-1)^{\bar{y}} \bar{z} z x\right) \alpha(y)=\{x y \cdot \alpha(z)-\alpha(x) \cdot y z\} \\
& -(-1)^{\bar{y} \bar{z}}\{x z \cdot \alpha(y)-\alpha(x) \cdot z y\}+(-1)^{\bar{z}(\bar{x}+\bar{y})}\{z x \cdot \alpha(y)-\alpha(z) \cdot x y\} \\
& =(x, y, z)-(-1)^{\bar{y} \bar{z}}(x, z, y)+(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y)
\end{aligned}
$$

and so we get (2.3). As for (2.4), we compute

$$
\begin{aligned}
& {[x y, \alpha(z)]-[x, y] \alpha(z)+(-1)^{\bar{y}} \bar{z}[x z, \alpha(y)]-(-1)^{\bar{y} \bar{z}}[x, z] \alpha(y)=x y \cdot \alpha(z)} \\
& -(-1)^{\bar{z}(\bar{x}+\bar{y})} \alpha(z) \cdot x y-\left(x y-(-1)^{\bar{x} \bar{y}} y x\right) \alpha(z)+(-1)^{\bar{y} \bar{z}}\left(x z \cdot \alpha(y)-(-1)^{\bar{y}(\bar{x}+\bar{z})} \alpha(y) \cdot x z\right) \\
& -(-1)^{\bar{y} \bar{z}}\left(x z-(-1)^{\bar{x} \bar{z}} z x\right) \alpha(y)=(-1)^{\bar{x}} \bar{y}(y x \cdot \alpha(z)-\alpha(y) \cdot x z) \\
& +(-1)^{\bar{z}(\bar{x}+\bar{y})}(z x \cdot \alpha(y)-\alpha(z) \cdot x y)=(-1)^{\bar{x} \bar{y}}(y, x, z)+(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y),
\end{aligned}
$$

which gives (2.4).
The identity (2.5) follows by expansion of associators in the right-hand side and next rearrangement of terms.

Starting from the right-hand side of (2.6), we have

$$
\begin{aligned}
& S(x, y, z)-(-1)^{\bar{x}} \bar{y} S(y, x, z)-2(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y)+[\alpha(x),[y, z]] \\
& =(x, y, z)-(-1)^{\bar{x} y+\bar{x}+\bar{y} \bar{z}}(z, y, x)+(-1)^{\bar{x}(\bar{y}+\bar{z})}(y, z, x) \\
& -(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y)+(-1)^{\bar{x}} \bar{y}(y, x, z)-(-1)^{\bar{y} \bar{z}}(x, z, y)+[\alpha(x),[y, z]] \\
& =(x \circ y) \cdot \alpha(z)+(-1)^{\bar{z}(\bar{x}+\bar{y})} \alpha(z) \cdot(x \circ y)-(-1)^{\bar{y} \bar{z}}(x \circ z) \cdot \alpha(y)-(-1)^{\bar{x} \bar{y}} \alpha(y) \cdot(x \circ z)
\end{aligned}
$$

(developing associators and commutators and next rearranging terms)

$$
=(x \circ y) \circ \alpha(z)-(-1)^{\bar{y} \bar{z}}(x \circ z) \circ \alpha(y)
$$

and so we get (2.6).
The identity (2.2) is usually called the Hom-Teichmüller identity ([24], [25]). Note that, up to $(-1)^{\bar{y} \bar{z}}$, the identity (2.4) is symmetric with respect to $y$ and $z$.

Upon the additional requirement of right superalternativity or alternativity on $(A, \cdot, \alpha)$, the following corollaries hold.

Corollary 2.5. If $(A, \cdot, \alpha)$ is a right Hom-alternative superalgebra, then

- $(x \circ y) \circ \alpha(z)-(-1)^{\bar{y} \bar{z}}(x \circ z) \circ \alpha(y)=2(x, y, z)+[\alpha(x),[y, z]]$,
- $[x, y] \alpha(z)-\alpha(x)[y, z]-(-1)^{\bar{y} \bar{z}}[x z, \alpha(y)]=2(x, y, z)-(-1)^{\bar{x} \bar{y}}(y, x, z)$,
- $S(x, y, z)+(-1)^{\bar{y} \bar{z}} S(x, z, y)=0$,
- $[x \circ y, \alpha(z)]+(-1)^{\bar{x}(\bar{y}+\bar{z})}[y \circ z, \alpha(x)]+(-1)^{\bar{z}(\bar{x}+\bar{y})}[z \circ x, \alpha(y)]=0$,
- $[[x, y], \alpha(z)]+(-1)^{\bar{x}(\bar{y}+\bar{z})}[[y, z], \alpha(x)]+(-1)^{\bar{z}(\bar{x}+\bar{y})}[[z, x], \alpha(y)]=2 S(x, y, z)$
for all $x, y, z$ in $A$. In particular, $(A, \cdot, \alpha)$ is Hom-Lie admissible if and only if $S(x, y, z)=0$.

Proof. The application of the right superalternativity (2.1) to the right-hand side of (2.6) gives (2.7). Subtracting memberwise (2.4) from (2.3) and next using
(2.1), we get (2.8). The identity (2.9) follows by direct expansion of $S(x, y, z)$ and $S(x, z, y)$ in terms of associators and the use of (2.1). In order to prove (2.10), one starts from (2.9) by replacing $S(x, y, z)$ and $S(x, z, y)$ with their respective expressions from (2.5). Next, rearranging terms with the definition of the super Jordan product in mind, one gets (2.10).

In (2.3) let permute $x$ and $y$ and next multiply by $(-1)^{\bar{x} \bar{y}}$ to get

$$
\begin{align*}
& {\left[(-1)^{\bar{x} \bar{y}} y x, \alpha(z)\right]-(-1)^{\bar{x}} \bar{y} \alpha(y)[x, z]-(-1)^{\bar{x}(\bar{y}+\bar{z})}[y, z] \alpha(x)} \\
& =(-1)^{\bar{x} \bar{y}}(y, x, z)-(-1)^{\bar{x}(\bar{y}+\bar{z})}(y, z, x)+(-1)^{\bar{x} \bar{y}+\bar{z}(\bar{x}+\bar{y})}(z, y, x) . \tag{2.12}
\end{align*}
$$

Now, subtracting memberwise (2.12) from (2.3), we get

$$
\begin{aligned}
& {[x y, \alpha(z)]-\alpha(x)[y, z]-(-1)^{\bar{y} \bar{z}}[x, z] \alpha(y)-\left[(-1)^{\bar{x} \bar{y}} y x, \alpha(z)\right]-(-1)^{\bar{x} \bar{y}} \alpha(y)[x, z] } \\
&-(-1)^{\bar{x}} \bar{y}[y, z] \alpha(x)=(x, y, z)-(-1)^{\bar{y} \bar{z}}(x, z, y)+(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y) \\
&-(-1)^{\bar{x}} \bar{y}(y, x, z)+(-1)^{\bar{x}(\bar{y}+\bar{z})}(y, z, x)-(-1)^{\bar{x}} \bar{y}+\bar{z}(\bar{x}+\bar{y}) \\
& \text { i.e., } \\
& \quad\{[x y, y, x) \\
& \quad+\left\{-(-1)^{\bar{y} \bar{z}}[x, z] \alpha(y)+(-1)^{\bar{x} \bar{y}} \alpha(y)[x, z]\right\} \\
& \quad=\left\{(x, y, z)-(-1)^{\bar{y} \bar{z}}(x, z, y)\right\}+\left\{-(-1)^{\bar{x}} \bar{y}(y, x, z)+(-1)^{\bar{x}(\bar{y}+\bar{z})}(y, z, x)\right\} \\
& \quad+\left\{(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y)-(-1)^{\bar{x} \bar{y}+\bar{z}(\bar{x}+\bar{y})}(z, y, x)\right\}
\end{aligned}
$$

and so, by the definition of the supercommutator and the right superalternativity (2.1), we come to (2.11).

The last assertion is obvious.
Corollary 2.6. If $(A, \cdot, \alpha)$ is a right Hom-alternative superalgebra, then
$[x \circ y, \alpha(z)]=(-1)^{\bar{y} \bar{z}}[x, z] \circ \alpha(y)+\alpha(x) \circ[y, z]+2(x, y, z)+2(-1)^{\bar{x}} \bar{y}(y, x, z)$
for all $x, y, z$ in $A$. Moreover, if $(A, \cdot, \alpha)$ is Hom-alternative, then

$$
\begin{equation*}
[x \circ y, \alpha(z)]=(-1)^{\bar{y} \bar{z}}[x, z] \circ \alpha(y)+\alpha(x) \circ[y, z] \tag{2.14}
\end{equation*}
$$

Proof. Adding (2.3) and (2.12) and next rearranging terms, we obtain

$$
\begin{aligned}
& {[x \circ y, \alpha(z)]-\alpha(x) \circ[y, z]-(-1)^{\bar{y} \bar{z}}[x, z] \circ \alpha(y)} \\
& =\left\{(x, y, z)-(-1)^{\bar{y} \bar{z}}(x, z, y)\right\}+\left\{(-1)^{\bar{x} \bar{y}}(y, x, z)-(-1)^{\bar{x}(\bar{y}+\bar{z})}(y, z, x)\right\} \\
& +\left\{(-1)^{\bar{x} \bar{y}+\bar{z}(\bar{x}+\bar{y})}(z, y, x)+(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y)\right\} \\
& =2(x, y, z)+2(-1)^{\bar{x} \bar{y}}(y, x, z) \text { (by the right superalternativity) }
\end{aligned}
$$

which proves (2.13).
The identity (2.14) follows from (2.13) by the left superalternativity.
Remark. If $(A, \cdot, \alpha)$ has zero odd part, then the identities (2.2) - (2.14) reduce to their ungraded counterparts in Hom-algebras.

## 3. Main results

Throughout this section, unless stated otherwise, $(A, \cdot, \alpha)$ denotes a right Homalternative superalgebra and we will prove some fundamental identities characterizing right Hom-alternative superalgebras.

First, we define on $(A, \cdot, \alpha)$ the following multilinear function

$$
\begin{aligned}
g(x, w, y, z):= & (-1)^{\bar{w}(\bar{y}+\bar{z})}(\alpha(x), \alpha(w), y z)+(-1)^{\bar{w} \bar{z}}(\alpha(x), \alpha(y), w z) \\
& -(-1)^{\bar{w} \bar{z}+\bar{w} \bar{y}+\bar{y} \bar{z}}(x, w, z) \alpha^{2}(y)-(x, y, z) \alpha^{2}(w) .
\end{aligned}
$$

One observes that if $A$ has zero odd part and $\alpha=I d$, then the function $g(x, w, y, z)$ is precisely the one defined in [11]. As a tool in the proof of part of the results below, we show that $g(x, w, y, z)$ is identically zero.

Lemma 3.1. For all $w, x, y, z$ in $A$, the following identity holds:

$$
\begin{equation*}
g(x, w, y, z)=0 \tag{3.1}
\end{equation*}
$$

Proof. By (2.2) and right superalternativity (2.1), we have

$$
\begin{aligned}
0 & =(-1)^{\bar{w}(\bar{y}+\bar{z})} f(x, w, y, z)-(-1)^{\bar{y} \bar{z}} f(x, z, y, w)+(-1)^{\bar{w} \bar{z}+\bar{w} \bar{y}+\bar{y} \bar{z}} f(x, w, z, y) \\
& +(-1)^{\bar{w}} \bar{z} f(x, y, w, z)-(-1)^{\bar{y}(\bar{w}+\bar{z})} f(x, z, w, y)+f(x, y, z, w) \\
& =(-1)^{\bar{w}(\bar{y}+\bar{z})}\{(x w, \alpha(y), \alpha(z))-(\alpha(x), w y, \alpha(z))+(\alpha(x), \alpha(w), y z) \\
& \left.-\alpha^{2}(x)(w, y, z)-(x, w, y) \alpha^{2}(z)\right\} \\
& -(-1)^{\bar{y} \bar{z}}\{(x z, \alpha(y), \alpha(w))-(\alpha(x), z y, \alpha(w))+(\alpha(x), \alpha(z), y w) \\
& \left.-\alpha^{2}(x)(z, y, w)-(x, z, y) \alpha^{2}(w)\right\} \\
& +(-1)^{\bar{w} \bar{z}+\bar{w} \bar{y}+\bar{y} \bar{z}}\{(x w, \alpha(z), \alpha(y))-(\alpha(x), w z, \alpha(y))+(\alpha(x), \alpha(w), z y) \\
& \left.-\alpha^{2}(x)(w, z, y)-(x, w, z) \alpha^{2}(y)\right\} \\
& +(-1)^{\bar{w} \bar{z}}\{(x y, \alpha(w), \alpha(z))-(\alpha(x), y w, \alpha(z))+(\alpha(x), \alpha(y), w z) \\
& \left.-\alpha^{2}(x)(y, w, z)-(x, y, w) \alpha^{2}(z)\right\} \\
& -(-1)^{\bar{y}(\bar{w}+\bar{z})}\{(x z, \alpha(w), \alpha(y))-(\alpha(x), z w, \alpha(y))+(\alpha(x), \alpha(z), w y) \\
& \left.-\alpha^{2}(x)(z, w, y)-(x, z, w) \alpha^{2}(y)\right\} \\
& +\{(x y, \alpha(z), \alpha(w))-(\alpha(x), y z, \alpha(w))+(\alpha(x), \alpha(y), z w) \\
& \left.-\alpha^{2}(x)(y, z, w)-(x, y, z) \alpha^{2}(w)\right\} \\
& =2\left[(-1)^{\bar{w}(\bar{y}+\bar{z})}(\alpha(x), \alpha(w), y z)+(-1)^{\bar{w}} \bar{z}(\alpha(x), \alpha(y), w z)\right. \\
& -(-1)^{\left.\bar{w} \bar{z}+\bar{w} \bar{y}+\bar{y} \bar{z}(x, w, z) \alpha^{2}(y)-(x, y, z) \alpha^{2}(w)\right](\text { after rearranging terms })} \\
& =2 g(x, w, y, z)
\end{aligned}
$$

and so we get (3.1).
We can now prove the following

Theorem 3.2. In $(A, \cdot, \alpha)$, the identities
$(w x, \alpha(y), \alpha(z))+(\alpha(w), \alpha(x),[y, z])=(-1)^{\bar{x}(\bar{y}+\bar{z})}(w, y, z) \alpha^{2}(x)+\alpha^{2}(w)(x, y, z)$,
$(\alpha(x), \alpha(z), y \circ w)=(\alpha(x), z \circ y, \alpha(w))+(-1)^{\bar{w} \bar{y}}(\alpha(x), z \circ w, \alpha(y))$
hold for all $w, x, y, z$ in $A$.
Proof. We have

$$
\begin{aligned}
0 & =f(w, x, y, z)-g(w, z, x, y)(\text { by }(2.2) \text { and }(3.1)) \\
& =(w x, \alpha(y), \alpha(z))-(\alpha(w), x y, \alpha(z))+(\alpha(w), \alpha(x), y z)-\alpha^{2}(w)(x, y, z) \\
& -(w, x, y) \alpha^{2}(z)-(-1)^{\bar{z}(\bar{x}+\bar{y})}(\alpha(w), \alpha(z), x y)-(-1)^{\bar{y} \bar{z}}(\alpha(w), \alpha(x), z y) \\
& +(-1)^{\bar{x}(\bar{y}+\bar{z})+\bar{y} \bar{z}}(w, z, y) \alpha^{2}(x)+(w, x, y) \alpha^{2}(z) \\
& =(w x, \alpha(y), \alpha(z))+(\alpha(w), \alpha(x),[y, z]) \\
& -(-1)^{\bar{x}(\bar{y}+\bar{z})}(w, y, z) \alpha^{2}(x)-\alpha^{2}(w)(x, y, z), \quad \text { (by right superalternativity) }
\end{aligned}
$$

which yields (3.2). As for (3.3), we proceed as follows.

$$
\begin{aligned}
0 & =(-1)^{\bar{w}} \bar{y} f(x, z, w, y)+f(x, z, y, w)(\text { by }(2.2)) \\
& =\left\{(-1)^{\bar{w}} \bar{y}(x z, \alpha(w), \alpha(y))-(-1)^{\bar{w} \bar{y}}(\alpha(x), z w, \alpha(y))+(-1)^{\bar{w} \bar{y}}(\alpha(x), \alpha(z), w y)\right. \\
& \left.-(-1)^{\bar{w} \bar{y}} \alpha^{2}(x)(z, w, y)-(-1)^{\bar{w} \bar{y}}(x, z, w) \alpha^{2}(y)\right\} \\
& +\{(x z, \alpha(y), \alpha(w))-(\alpha(x), z y, \alpha(w))+(\alpha(x), \alpha(z), y w) \\
& \left.-\alpha^{2}(x)(z, y, w)-(x, z, y) \alpha^{2}(w)\right\} \\
& =-(-1)^{\bar{w} \bar{y}}(\alpha(x), z w, \alpha(y))-(\alpha(x), z y, \alpha(w))+(\alpha(x), \alpha(z), y w) \\
& +(-1)^{\bar{w} \bar{y}}(\alpha(x), \alpha(z), w y)+(-1)^{\bar{w}(\bar{y}+\bar{z})}(x, w, z) \alpha^{2}(y)+(-1)^{\bar{y} \bar{z}}(x, y, z) \alpha^{2}(w) \\
& +\left[(-1)^{\bar{w} \bar{y}}(x z, \alpha(w), \alpha(y))+(x z, \alpha(y), \alpha(w))-(-1)^{\bar{w} \bar{y}} \alpha^{2}(x)(z, w, y)-\alpha^{2}(x)(z, y, w)\right] \\
& =(\alpha(x), z w, \alpha(y))-(\alpha(x), z y, \alpha(w))+(\alpha(x), \alpha(z), y w)+(-1)^{\bar{w} \bar{y}}(\alpha(x), \alpha(z), w y) \\
& +(-1)^{\bar{w}(\bar{y}+\bar{z})}(x, w, z) \alpha^{2}(y)+(-1)^{\bar{y} \bar{z}}(x, y, z) \alpha^{2}(w)
\end{aligned}
$$

(since, by right superalternativity, the expression in bracket above is zero)

$$
\begin{aligned}
& =-(-1)^{\bar{w}} \bar{y}(\alpha(x), z w, \alpha(y))-(\alpha(x), z y, \alpha(w))+(\alpha(x), \alpha(z), y w) \\
& +(-1)^{\bar{w}} \bar{y}(\alpha(x), \alpha(z), w y)+(-1)^{\bar{w}(\bar{y}+\bar{z})+\bar{y} \bar{z}}(\alpha(x), \alpha(w), y z) \\
& +(-1)^{\bar{z}(\bar{w}+\bar{y})}(\alpha(x), \alpha(y), w z) \quad(\text { by }(3.1)) \\
& =-(-1)^{\bar{w}} \bar{y}(\alpha(x), z w, \alpha(y))-(\alpha(x), z y, \alpha(w))+(\alpha(x), \alpha(z), y \circ w) \\
& -(-1)^{\bar{y} \bar{z}}(\alpha(x), y z, \alpha(w))-(-1)^{\bar{w}(\bar{y}+\bar{z})}(\alpha(x), w z, \alpha(y)),
\end{aligned}
$$

which leads to (3.3).
In order to prove the identity (3.5) below, we first prove that the following identity holds in $(A, \cdot, \alpha)$.

Lemma 3.3. The identity

```
\((-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}\left[(\alpha(x), y z, \alpha(w))+(-1)^{\bar{w} \bar{z}}(\alpha(x), y w, \alpha(z))+(x, y, z) \alpha^{2}(w)\right.\)
\(\left.+(-1)^{\bar{w}} \bar{z}(x, y, w) \alpha^{2}(z)\right] \cdot \alpha^{3}(t)+\left[(\alpha(x), t z, \alpha(w))+(-1)^{\bar{w}} \bar{z}(\alpha(x), t w, \alpha(z))\right.\)
\(\left.+(x, t, z) \alpha^{2}(w)+(-1)^{\bar{w} \bar{z}}(x, t, w) \alpha^{2}(z)\right] \cdot \alpha^{3}(y)\)
\(=(-1)^{\bar{y}(\bar{t}+\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(y), \alpha(t) \cdot(z \circ w)\right)+(-1)^{\bar{y}(\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(t), \alpha(y) \cdot(z \circ w)\right)\)
```

holds for all $t, w, x, y, z$ in $A$.
Proof. Starting from the left-hand side of (3.4), we have

$$
\begin{aligned}
& (-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}\left[(\alpha(x), y z, \alpha(w))+(-1)^{\bar{w} \bar{z}}(\alpha(x), y w, \alpha(z))+(x, y, z) \alpha^{2}(w)\right. \\
& \left.+(-1)^{\bar{w} \bar{z}}(x, y, w) \alpha^{2}(z)\right] \cdot \alpha^{3}(t)+\left[(\alpha(x), t z, \alpha(w))+(-1)^{\bar{w} \bar{z}}(\alpha(x), t w, \alpha(z))\right. \\
& \left.+(x, t, z) \alpha^{2}(w)+(-1)^{\bar{w} \bar{z}}(x, t, w) \alpha^{2}(z)\right] \cdot \alpha^{3}(y) \\
& =(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}(\alpha(x), y z, \alpha(w)) \alpha^{3}(t) \\
& +(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}+\bar{w} \bar{z}}(\alpha(x), y w, \alpha(z)) \alpha^{3}(t) \\
& +(\alpha(x), t z, \alpha(w)) \alpha^{3}(y)+(-1)^{\bar{w} \bar{z}}(\alpha(x), t w, \alpha(z)) \alpha^{3}(y) \\
& -(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}+\bar{w}(\bar{y}+\bar{z})}\left[(-1)^{\bar{y}(\bar{w}+\bar{z})+\bar{w} \bar{z}}(x, z, y) \alpha^{2}(w)+(x, w, y) \alpha^{2}(z)\right] \cdot \alpha^{3}(t) \\
& -(-1)^{\bar{w}(\bar{t}+\bar{z})}\left[(-1)^{\bar{t}(\bar{w}+\bar{z})+\bar{w} \bar{z}}(x, z, t) \alpha^{2}(w)+(x, w, t) \alpha^{2}(z)\right] \cdot \alpha^{3}(y) \\
& \text { (by right superalternativity) } \\
& =(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}(\alpha(x), y z, \alpha(w)) \alpha^{3}(t) \\
& +(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}+\bar{w} \bar{z}}(\alpha(x), y w, \alpha(z)) \alpha^{3}(t)+(\alpha(x), t z, \alpha(w)) \alpha^{3}(y) \\
& +(-1)^{\bar{w} \bar{z}}(\alpha(x), t w, \alpha(z)) \alpha^{3}(y) \\
& -(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}\left[(-1)^{\bar{z}(\bar{w}+\bar{y})+\bar{w}(\bar{y}+\bar{z})}(\alpha(x), \alpha(z), w y)\right. \\
& \left.+(-1)^{\bar{y} \bar{z}+\bar{w}(\bar{y}+\bar{z})}(\alpha(x), \alpha(w), z y)\right] \cdot \alpha^{3}(t)-\left[(-1)^{\bar{z}(\bar{t}+\bar{w})+\bar{w}(\bar{t}+\bar{z})}(\alpha(x), \alpha(z), w t)\right. \\
& \left.+(-1)^{\bar{t} \bar{z}+\bar{w}(\bar{t}+\bar{z})}(\alpha(x), \alpha(w), z t)\right] \cdot \alpha^{3}(y) \quad(b y(3.1)) \\
& =(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}(\alpha(x), y z, \alpha(w)) \alpha^{3}(t) \\
& +(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}+\bar{w} \bar{z}}(\alpha(x), y w, \alpha(z)) \alpha^{3}(t)+(\alpha(x), t z, \alpha(w)) \alpha^{3}(y)
\end{aligned}
$$

$$
\begin{aligned}
& \left.+(-1)^{\bar{y} \bar{z}}(\alpha(x), z y, \alpha(w))\right] \cdot \alpha^{3}(t)+\left[(-1)^{\bar{w}(\bar{t}+\bar{z})}(\alpha(x), w t, \alpha(z))\right. \\
& \left.+(-1)^{\bar{t} \bar{z}}(\alpha(x), z t, \alpha(w))\right] \cdot \alpha^{3}(y) \quad \text { (by right superalternativity) } \\
& =(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}\left[(\alpha(x), y z, \alpha(w))+(-1)^{\bar{w} \bar{z}}(\alpha(x), y w, \alpha(z))\right. \\
& \left.+(-1)^{\bar{w}(\bar{y}+\bar{z})}(\alpha(x), w y, \alpha(z))+(-1)^{\bar{y} \bar{z}}(\alpha(x), z y, \alpha(w))\right] \cdot \alpha^{3}(t) \\
& +\left[(\alpha(x), t z, \alpha(w))+(-1)^{\bar{w} \bar{z}}(\alpha(x), t w, \alpha(z))+(-1)^{\bar{w}(\bar{t}+\bar{z})}(\alpha(x), w t, \alpha(z))\right. \\
& \left.+(-1)^{\bar{t} \bar{z}}(\alpha(x), z t, \alpha(w))\right] \cdot \alpha^{3}(y)=(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}\left[(-1)^{\bar{w} \bar{z}}(\alpha(x), \alpha(y), w z)\right. \\
& +(\alpha(x), \alpha(y), z w)] \cdot \alpha^{3}(t)+\left[(-1)^{\bar{w} \bar{z}}(\alpha(x), \alpha(t), w z)+(\alpha(x), \alpha(t), z w)\right] \cdot \alpha^{3}(y) \\
& \text { (applying (3.3) to each of the expressions in brackets above) }
\end{aligned}
$$

$$
\begin{aligned}
& =\left\{(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}(\alpha(x), \alpha(y), z w) \alpha^{3}(t)+(\alpha(x), \alpha(t), z w) \alpha^{3}(y)\right\} \\
& +\left\{(-1)^{\left.\bar{w} \bar{z}+(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}(\alpha(x), \alpha(y), w z) \alpha^{3}(t)+(-1)^{\bar{w}} \bar{z}(\alpha(x), \alpha(t), w z) \alpha^{3}(y)\right\}} \begin{array}{l}
=(-1)^{\bar{y}(\bar{t}+\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(y), \alpha(t) \cdot z w\right)+(-1)^{\bar{y}(\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(t), \alpha(y) \cdot z w\right) \\
+(-1)^{\bar{w} \bar{z}}\left[(-1)^{\bar{y}(\bar{t}+\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(y), \alpha(t) \cdot w z\right)+(-1)^{\bar{y}(\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(t), \alpha(y) \cdot w z\right)\right] \\
\text { (applying (3.1) to each of the expressions in }\{\cdots\} \text { above) and so we get (3.4). }
\end{array}\right. \text {. }
\end{aligned}
$$

We are now in position to prove the following

## Theorem 3.4. The identity

$$
\begin{align*}
& (-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}\left[(x, y, z) \alpha^{2}(w)+(-1)^{\bar{w} \bar{z}}(x, y, w) \alpha^{2}(z)\right] \cdot \alpha^{3}(t) \\
& +\left[(x, t, z) \alpha^{2}(w)+(-1)^{\bar{w}} \bar{z}(x, t, w) \alpha^{2}(z)\right] \cdot \alpha^{3}(y) \\
& -(-1)^{\bar{t}(\bar{y}+\bar{z})+\bar{y}(\bar{w}+\bar{z})} \alpha((x, y, z)) \alpha^{2}(t w)-(-1)^{(\bar{t}+\bar{z})(\bar{w}+\bar{y})+\bar{w} \bar{y}} \alpha((x, y, w)) \alpha^{2}(t z) \\
& -(-1)^{\bar{w} \bar{y}} \alpha((x, t, z)) \alpha^{2}(y w)-(-1)^{\bar{z}(\bar{w}+\bar{y})} \alpha((x, t, w)) \alpha^{2}(y z)=0 \tag{3.5}
\end{align*}
$$

holds for all $t, w, x, y, z$ in $A$.
Proof. Relying essentially on (3.1) and (3.4), we compute

$$
\begin{aligned}
& 0=g(\alpha(x), \alpha(y), t z, \alpha(w))+(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}} g(\alpha(x), \alpha(t), y z, \alpha(w)) \\
& +(-1)^{\bar{w} \bar{z}} g(\alpha(x), \alpha(y), t w, \alpha(z))+(-1)^{(\bar{t}+\bar{z})(\bar{w}+\bar{y})+\bar{t} \bar{z}+\bar{w} \bar{y}} g(\alpha(x), \alpha(t), y w, \alpha(z)) \\
& =(-1)^{\bar{y}(\bar{t}+\bar{w}+\bar{z})}\left[\left(\alpha^{2}(x), \alpha^{2}(y), t z \cdot \alpha(w)\right)+(-1)^{\bar{w} \bar{z}}\left(\alpha^{2}(x), \alpha^{2}(y), t w \cdot \alpha(z)\right)\right] \\
& +(-1)^{\bar{y}(\bar{w}+\bar{z})}\left[\left(\alpha^{2}(x), \alpha^{2}(t), y z \cdot \alpha(w)\right)+(-1)^{\bar{w} \bar{z}}\left(\alpha^{2}(x), \alpha^{2}(t), y w \cdot \alpha(z)\right)\right] \\
& +(-1)^{\bar{y}(\bar{w}+\bar{z})+\bar{t}(\bar{y}+\bar{z})}\left[\left(\alpha^{2}(x), \alpha(y z), \alpha(t w)\right)+(-1)^{\bar{y}+\bar{z})(\bar{t}+\bar{w})}\left(\alpha^{2}(x), \alpha(t w), \alpha(y z)\right)\right] \\
& -(-1)^{\bar{t}(\bar{y}+\bar{z})+\bar{y}(\bar{w}+\bar{z})}(\alpha(x), \alpha(y), \alpha(z)) \alpha^{2}(t w) \\
& -(-1)^{(\bar{t}+\bar{z})(\bar{w}+\bar{y})+\bar{w} \bar{y}}(\alpha(x), \alpha(y), \alpha(w)) \alpha^{2}(t z) \\
& -(-1)^{\bar{y} \bar{w}}(\alpha(x), \alpha(t), \alpha(z)) \alpha^{2}(y w)-(-1)^{\bar{z}(\bar{w}+\bar{y})}(\alpha(x), \alpha(t), \alpha(w)) \alpha^{2}(y z) \\
& -(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}(\alpha(x), y z, \alpha(w)) \alpha^{3}(t) \\
& -(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}+\bar{w} \bar{z}}(\alpha(x), y w, \alpha(z)) \alpha^{3}(t) \\
& -(\alpha(x), t z, \alpha(w)) \alpha^{3}(y)-(-1)^{\bar{w} \bar{z}}(\alpha(x), t w, \alpha(z)) \alpha^{3}(y)(\text { after rearranging terms }) \\
& =(-1)^{\bar{y}(\bar{t}+\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(y), \alpha(t) \cdot z w+(-1)^{\bar{w} \bar{z}} \alpha(t) \cdot w z\right) \\
& +(-1)^{\bar{y}(\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(t), \alpha(y) \cdot z w+(-1)^{\bar{w} \bar{z}} \alpha(y) \cdot w z\right) \\
& +\left[(-1)^{\bar{y}(\bar{w}+\bar{z})+\bar{t}(\bar{y}+\bar{z})}\left(\alpha^{2}(x), \alpha(y z), \alpha(t w)\right)+(-1)^{(\bar{y}+\bar{z})(\bar{t}+\bar{w})}\left(\alpha^{2}(x), \alpha(t w), \alpha(y z)\right)\right] \\
& -(-1)^{\bar{t}(\bar{y}+\bar{z})+\bar{y}(\bar{w}+\bar{z})}(\alpha(x), \alpha(y), \alpha(z)) \alpha^{2}(t w) \\
& -(-1)^{(\bar{t}+\bar{z})(\bar{w}+\bar{y})+\bar{w} \bar{y}}(\alpha(x), \alpha(y), \alpha(w)) \alpha^{2}(t z) \\
& -(-1)^{\bar{y} \bar{w}}(\alpha(x), \alpha(t), \alpha(z)) \alpha^{2}(y w)-(-1)^{\bar{z}(\bar{w}+\bar{y})}(\alpha(x), \alpha(t), \alpha(w)) \alpha^{2}(y z) \\
& -(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}(\alpha(x), y z, \alpha(w)) \alpha^{3}(t) \\
& -(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}+\bar{w} \bar{z}}(\alpha(x), y w, \alpha(z)){\alpha^{3}(t)}^{2}
\end{aligned}
$$

$-(\alpha(x), t z, \alpha(w)) \alpha^{3}(y)-(-1)^{\bar{w} \bar{z}}(\alpha(x), t w, \alpha(z)) \alpha^{3}(y)$
(by right superalternativity)

$$
\begin{aligned}
& =(-1)^{\bar{y}(\bar{t}+\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(y), \alpha(t) \cdot(z \circ w)\right)+(-1)^{\bar{y}(\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(t), \alpha(y) \cdot(z \circ w)\right) \\
& +(-1)^{\bar{y}(\bar{w}+\bar{z})+\bar{t}(\bar{y}+\bar{z})}\left[\left(\alpha^{2}(x), \alpha(y) \alpha(z), \alpha(t) \alpha(w)\right)\right. \\
& \left.+(-1)^{(\bar{t}+\bar{w})(\bar{y}+\bar{z})}\left(\alpha^{2}(x), \alpha(t) \alpha(w), \alpha(y) \alpha(z)\right)\right] \\
& -(-1)^{\bar{t}(\bar{y}+\bar{z})+\bar{y}(\bar{w}+\bar{z})} \alpha((x, y, z)) \alpha^{2}(t w)-(-1)^{(\bar{t}+\bar{z})(\bar{w}+\bar{y})+\bar{w} \bar{y}} \alpha((x, y, w)) \alpha^{2}(t z) \\
& -(-1)^{\bar{y} \bar{w}} \alpha((x, t, z)) \alpha^{2}(y w)-(-1)^{\bar{z}(\bar{w}+\bar{y})} \alpha((x, t, w)) \alpha^{2}(y z) \\
& -(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}(\alpha(x), y z, \alpha(w)) \alpha^{3}(t) \\
& -(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}+\bar{w} \bar{z}}(\alpha(x), y w, \alpha(z)) \alpha^{3}(t)-(\alpha(x), t z, \alpha(w)) \alpha^{3}(y) \\
& -(-1)^{\bar{w} \bar{z}}(\alpha(x), t w, \alpha(z)) \alpha^{3}(y)
\end{aligned}
$$

(by linearity of the associator and multiplicativity)

$$
\begin{aligned}
& =\left\{(-1)^{\bar{y}(\bar{t}+\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(y), \alpha(t) \cdot(z \circ w)\right)+(-1)^{\bar{y}(\bar{w}+\bar{z})}\left(\alpha^{2}(x), \alpha^{2}(t), \alpha(y) \cdot(z \circ w)\right)\right. \\
& -(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}(\alpha(x), y z, \alpha(w)) \alpha^{3}(t) \\
& -(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}+\bar{w} \bar{z}}(\alpha(x), y w, \alpha(z)) \alpha^{3}(t) \\
& \left.-(\alpha(x), t z, \alpha(w)) \alpha^{3}(y)-(-1)^{\bar{w} \bar{z}}(\alpha(x), t w, \alpha(z)) \alpha^{3}(y)\right\} \\
& -(-1)^{\bar{t}(\bar{y}+\bar{z})+\bar{y}(\bar{w}+\bar{z})} \alpha((x, y, z)) \alpha^{2}(t w)-(-1)^{(\bar{t}+\bar{z})(\bar{w}+\bar{y})+\bar{w} \bar{y}} \alpha((x, y, w)) \alpha^{2}(t z) \\
& -(-1)^{\bar{y} \bar{w}} \alpha((x, t, z)) \alpha^{2}(y w)-(-1)^{\bar{z}(\bar{w}+\bar{y})} \alpha((x, t, w)) \alpha^{2}(y z) \\
& =\left\{(-1)^{(\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}}(x, y, z) \alpha^{2}(w) \alpha^{3}(t)\right. \\
& +(-1)^{\bar{t}+\bar{y})(\bar{w}+\bar{z})+\bar{t} \bar{y}+\bar{w} \bar{z}}(x, y, w) \alpha^{2}(z) \cdot \alpha^{3}(t) \\
& \left.+(x, t, z) \alpha^{2}(w) \cdot \alpha^{3}(y)+(-1)^{\bar{w} \bar{z}}(x, t, w) \alpha^{2}(z) \cdot \alpha^{3}(y)\right\} \\
& -(-1)^{\bar{t}(\bar{y}+\bar{z})+\bar{y}(\bar{w}+\bar{z})} \alpha((x, y, z)) \alpha^{2}(t w)-(-1)^{(\bar{t}+\bar{z})(\bar{w}+\bar{y})+\bar{w} \bar{y}} \alpha((x, y, w)) \alpha^{2}(t z) \\
& -(-1)^{\bar{y} \bar{w}} \alpha((x, t, z)) \alpha^{2}(y w)-(-1)^{\bar{z}(\bar{w}+\bar{y})} \alpha((x, t, w)) \alpha^{2}(y z)
\end{aligned}
$$

(applying (3.4) to the expression in $\{\cdots\}$ above), which is (3.5).
Remark. It is easily seen that the identities (3.1) - (3.5) are the $\mathbb{Z}_{2}$-graded generalization of identities

$$
\begin{align*}
& (\alpha(x), \alpha(w), y z)+(\alpha(x), \alpha(y), w z)-(x, w, z) \alpha^{2}(y)-(x, y, z) \alpha^{2}(w)=0,  \tag{3.6}\\
& (w x, \alpha(y), \alpha(z))+(\alpha(w), \alpha(x),[y, z])=\alpha^{2}(w)(x, y, z)+(w, y, z) \alpha^{2}(x),  \tag{3.7}\\
& \left(\alpha(x), y^{2}, \alpha(z)\right)=(\alpha(x), \alpha(y), y z+z y)  \tag{3.8}\\
& \left(\alpha^{2}(x), \alpha^{2}(y), \alpha(y) \cdot z^{2}\right)=(\alpha(x), y z, \alpha(z)) \alpha^{3}(y)+(x, y, z) \alpha^{2}(z) \cdot \alpha^{3}(y),  \tag{3.9}\\
& (x, y, z) \alpha^{2}(y) \cdot \alpha^{3}(z)=(x, y, z) \alpha^{2}(z y) \tag{3.10}
\end{align*}
$$

respectively, all of which could be found in [25].
As it could be seen below, some $\mathbb{Z}_{2}$-graded Moufang-type identities hold in right Hom-alternative superalgebras.

Theorem 3.5. In $(A, \cdot, \alpha)$ the identity

$$
\begin{align*}
& (x y \cdot \alpha(z)) \alpha^{2}(w)+(-1)^{\bar{y}} \bar{z}+\bar{w} \bar{y}+\bar{w} \bar{z}(x w \cdot \alpha(z)) \alpha^{2}(y) \\
& =\alpha^{2}(x)(y z \cdot \alpha(w))+(-1)^{\bar{y} \bar{z}+\bar{w} \bar{y}+\bar{w} \bar{z}} \alpha^{2}(x)(w z \cdot \alpha(y)) \tag{3.11}
\end{align*}
$$

holds for all $w, x, y, z$ in $A$.
Proof. In $(A, \cdot, \alpha)$, we have $(-1)^{\bar{w}(\bar{y}+\bar{z})}(\alpha(x), \alpha(w), y z)+(-1)^{\bar{w} \bar{z}}(\alpha(x), \alpha(y), w z)$ $=(-1)^{\bar{y} \bar{z}+\bar{w} \bar{y}+\bar{w} \bar{z}}(x, w, z) \alpha^{2}(y)+(x, y, z) \alpha^{2}(w) \quad($ by $(3.1))$
i.e., by the right superalternativity,

$$
\begin{align*}
& -(\alpha(x), y z, \alpha(w))-(-1)^{\bar{y} \bar{z}+\bar{w} \bar{y}+\bar{w} \bar{z}}(\alpha(x), w z, \alpha(y)) \\
& =(-1)^{\bar{y} \bar{z}+\bar{w} \bar{y}+\bar{w} \bar{z}}(x, w, z) \alpha^{2}(y)+(x, y, z) \alpha^{2}(w) . \tag{3.12}
\end{align*}
$$

Therefore one gets (3.11) if expand associators in (3.12).
Remark. The ungraded version of (3.11) is proved in [25]. For $\alpha=I d$ in (3.11), one gets
and if, moreover, $A$ has zero odd part and $y=w$, one gets the right Bol identity $(x y \cdot z) y=x(y z \cdot y)$ formerly called the "right Moufang identity" (see, e.g., [17] and [27]). Consistent with this observation, (3.11) may be called the "right super Hom-Bol identity".

Remark. In case when $(A, \cdot, \alpha)$ is Hom-alternative, then (3.12) yields

$$
\begin{align*}
& (-1)^{\bar{x}(\bar{y}+\bar{z})}(y z, \alpha(x), \alpha(w))+(-1)^{\bar{x}(\bar{w}+\bar{z})+\bar{w}(\bar{y}+\bar{z})+\bar{y} \bar{z}}(w z, \alpha(x), \alpha(y)) \\
& =(-1)^{\bar{z}(\bar{x}+\bar{y})}(z, x, y) \alpha^{2}(w)+(-1)^{\bar{z}(\bar{x}+\bar{y})+\bar{w} \bar{y}}(z, x, w) \alpha^{2}(y) . \tag{3.13}
\end{align*}
$$

If, moreover, $A$ has zero odd part and $\alpha=I d$, then (3.13) reads as

$$
(y z, x, w)+(w z, x, y)=(z, x, y) w+(z, x, w) y
$$

which is the linearized form of the middle Moufang identity ([27])

$$
(y z, x, y)-(z, x, y) y=0 .
$$

In this sense, the identity (3.12) is (in part) close to the middle Moufang identity.
In [18] (identity (9)) the following identity is proved to hold in right alternative algebras:

$$
(x, z, y \circ w)=2(x, z, w) y-2(x, y, z) w+(x,[z, y], w)+(x,[z, w], y)
$$

Its $\mathbb{Z}_{2}$-graded Hom-version is given by
Theorem 3.6. In $(A, \cdot, \alpha)$ the identity

$$
\begin{align*}
& (\alpha(x), \alpha(z), y \circ w)=2(-1)^{\bar{w} \bar{y}}(x, z, w) \alpha^{2}(y)-2(-1)^{\bar{y}} \bar{z}(x, y, z) \alpha^{2}(w) \\
& +(\alpha(x),[z, y], \alpha(w))+(-1)^{\bar{w}} \bar{y}(\alpha(x),[z, w], \alpha(y)) \tag{3.14}
\end{align*}
$$

holds for all $w, x, y, z$ in $A$.
Proof. We have

$$
\begin{aligned}
& (\alpha(x), \alpha(z), y \circ w)=(\alpha(x), z \circ y, \alpha(w))+(-1)^{\bar{w} \bar{y}}(\alpha(x), z \circ w, \alpha(y)) \text { (see (3.3)) } \\
& =(\alpha(x), z y, \alpha(w))+(-1)^{\bar{y} \bar{z}}(\alpha(x), y z, \alpha(w))+(-1)^{\bar{w} \bar{y}}(\alpha(x), z w, \alpha(y)) \\
& +(-1)^{\bar{w}(\bar{y}+\bar{z})}(\alpha(x), w z, \alpha(y)) \\
& =(\alpha(x),[z, y], \alpha(w))+2(-1)^{\bar{y} \bar{z}}(\alpha(x), y z, \alpha(w))+(-1)^{\bar{w} \bar{y}}(\alpha(x),[z, w], \alpha(y)) \\
& +2(-1)^{\bar{w}(\bar{y}+\bar{z})}(\alpha(x), w z, \alpha(y)) \\
& =(\alpha(x),[z, y], \alpha(w))+(-1)^{\bar{w}} \bar{y}(\alpha(x),[z, w], \alpha(y)) \\
& +2\left\{(-1)^{\bar{y} \bar{z}}(\alpha(x), y z, \alpha(w))+(-1)^{\bar{w}(\bar{y}+\bar{z})}(\alpha(x), w z, \alpha(y))\right\} \\
& =(\alpha(x),[z, y], \alpha(w))+(-1)^{\bar{w} \bar{y}}(\alpha(x),[z, w], \alpha(y)) \\
& -2(-1)^{\bar{y}} \bar{z}\left\{(-1)^{\bar{y}} \bar{z}+\bar{w} \bar{y}+\bar{w} \bar{z}(x, w, z) \alpha^{2}(y)+(x, y, z) \alpha^{2}(w)\right\} \quad \text { (by (3.1)) } \\
& =(\alpha(x),[z, y], \alpha(w))+(-1)^{\bar{w} \bar{y}}(\alpha(x),[z, w], \alpha(y)) \\
& +2(-1)^{\bar{w}} \bar{y}(x, z, w) \alpha^{2}(y)-2(-1)^{\bar{y} \bar{z}}(x, y, z) \alpha^{2}(w)
\end{aligned}
$$

(by the right superalternativity) and so we get (3.14).

## References

[1] A.A. Albert, On right alternative algebras, Ann. Math. 50 (1949), 318 - 328.
[2] F. Ammar and A. Makhlouf, Hom-Lie superalgebras and Hom-Lie admissible superalgebras, J. Algebra 324 (2010), 1513-1528.
[3] S. Attan and A.N. Issa, Hom-Bol algebras, Quasigroups and Related Systems 21 (2013), $131-146$.
[4] F.A. Berezin and G.I. Kats, Lie groups with commuting and anticommuting parameters, (Russian), Mat. Sb. 82(124) (1970), $343-359$.
[5] R.H. Bruck and E. Kleinfeld, The structure of alternative division rings, Proc. Amer. Math. Soc. 2 (1951), 878-890.
[6] Y. Frégier, A. Gohr and S.D. Silvestrov, Unital algebras of Hom-associative type and surjective or injective twistings, J. Gen. Lie Theory Appl. 3 (2009), no. 4, $285-295$.
[7] D. Gaparayi and A.N. Issa, A twisted generalization of Lie-Yamaguti algebras, Int. J. Algebra 6 (2012), no. 7, $339-352$.
[8] J.T. Hartwig, D. Larsson and S.D. Silvestrov, Deformations of Lie algebras using $\sigma$-derivations, J. Algebra 295 (2006), 314 - 361.
[9] A.N. Issa, Hom-Akivis algebras, Comment. Math. Univ. Carolin. 52 (2011), no. 4, 485-500.
[10] V.G. Kac, Classification of simple $\mathbb{Z}$-graded Lie superalgebras and simple Jordan superalgebras, Commun. Algebra 5 (1977), 1375 - 1400.
[11] E. Kleinfeld, Right alternative rings, Proc. Amer. Math. Soc. 4 (1953), 939 - 944.
[12] D. Larsson and S. Silvestrov, Quasi-Hom-Lie algebras, central extensions and 2-cycle-like identities, J. Algebra 288 (2005), 321 - 344.
[13] D. Larsson and S. Silvestrov, Quasi-Lie algebras, Contemp. Math. 391 (2005), 241-248.
[14] A. Makhlouf, Hom-alternative algebras and Hom-Jordan algebras, Int. Electron. J. Alg. 8 (2010), $177-190$.
[15] A. Makhlouf and S.D. Silvestrov, Hom-algebra structures, J. Gen. Lie Theory Appl. 2 (2008), no. 2, $51-64$.
[16] W. Milnor and I.C. Moore, On the structure of Hopf algebras, Ann. Math. 81 (1965), 211 - 264.
[17] R. Moufang, Zur Struktur von Alternative Korpern, Math. Ann. 110 (1935), 416 430.
[18] S.V. Pchelintsev, Free ( $-1,1$ )-algebra with two generators, (Russian), Algebra i Logika 13 (1974), 425 - 449.
[19] R.D. Schafer, An introduction to nonassociative algebras, Dover Pub., New York, 1995.
[20] I.P. Shestakov, Prime Mal'tsev superalgebras, (Russian), Mat. Sb. 182 (1991), $1357-1366$.
[21] L.A. Skornyakov, Right alternative division rings, (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 15 (1952), 177 - 184.
[22] A. Thedy, Right alternative rings, J. Algebra 37 (1975), 1 - 43.
[23] D. Yau, Hom-Novikov algebras, J. Phys. A 44 (2011), 085202.
[24] D. Yau, Hom-Maltsev, Hom-alternative, and Hom-Jordan algebras, Int. Electron. J. Algebra 11 (2012), 177 - 217.
[25] D. Yau, Right Hom-alternative algebras, ArXiv:1010.3407v1 [math. RA], 17 Oct 2010.
[26] E.I. Zel'manov and I.P. Shestakov, Prime alternative superalgebras and nilpotency of the radical of a free alternative algebra, (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 54 (1990), $676-693$.
[27] K.A. Zhevlakov, A.M. Slin'ko, I.P. Shestakov and A.I. Shirshov, Rings that are nearly associative, Academic Press, New York, 1982.
[28] M. Zorn, Theorie der alternativen Ringe, Abh. Math. Sem. Univ. Hamburg 8 (1930), 123 - 147.

Received December 11, 2016 Département de Mathématiques, Université d'Abomey-Calavi, 01 BP 4521, Cotonou 01, Bénin
E-mail: woraniss@yahoo.fr

# Enumeration of exponent three IP loops 

Majid Ali Khan, Shahabuddin Muhammad, Nazeeruddin Mohammad,

Asif Ali


#### Abstract

Inverse Property Loops (IP Loops) are important algebraic structures that fall between loops and groups. Enumerating isomorphism classes of higher order IP loops is an arduous task due to enormous number of isomorphism copies. This paper describes a systematic approach to efficiently eliminate isomorphic copies, which reduces the time to enumerate isomorphism classes. Using the proposed approach, we count and enumerate exponent 3 IP loops of order 15. To the best of our knowledge, this count is reported for the first time in the literature. Further, we also computationally verify and enumerate the existing results for exponent 3 IP loops of order up to 13 . The results show that even after applying stringent condition of exponent 3, a good number of isomorphism classes exist. However, when associativity property is applied, the total number of isomorphism classes reduces drastically. This provides an insight that instead of exponent 3 property, associativity is mainly responsible for the low population of isomorphism classes in groups.


## 1. Introduction

A quasigroup is a groupoid $G$ with a binary operation $*$ such that $x * a=y$ and $b * x=y$ have unique solutions for each $x, y \in G$. A quasigroup is a loop if and only if it contains an identity element $e$ such that $x * e=x=e * x$ for each $x \in G$. A loop $L$ is called an inverse property (IP) loop if it has a two sided inverse $x^{-1}$ such that $x^{-1} *(x * y)=y=(y * x) * x^{-1}$ for each $x, y \in L$. A Steiner loop is an IP loop of exponent $2\left(x * x=e\right.$ or $x^{2}=e$ for all $\left.x \in L\right)$. Also, extensively studied Moufang loops are IP loops satisfying $x *(z *(y * z))=((x * z) * y) * z$.

IP loops form an important class since they represent a generalization of Steiner loops, Moufang loops, and groups. Further, IP loops represent those groupoids whose power sets are exactly the semi-associative relation algebras [19].

The smallest IP loop which is not a group is of order 7. But the number of IP loops increases quickly with the increase in the order of the loop as there are 10,341 IP loops available for $n=13$. The IP loops having order greater than 13 are not reported in the literature because of the huge search space. On the other hand, the number of groups does not necessarily increase with the increase in their

[^3]order. For example, the number of groups for any given prime order is always one. Enumeration of very highly structured loops like Moufang loops is possible up to comparatively high orders [30], where as less structured loops such as nilpotent loops have not been enumerated so far for higher orders [8].

The IP loops of exponent 3 satisfy the following property: $(x * x) * x=x *(x * x)$ $=e$ for all $x \in L$ (i.e., $x^{2}=x^{-1}$ ). For any order n, the IP loops of exponent 3 exists when either $n \equiv 1(\bmod 6)$ or $n \equiv 3(\bmod 6)$ [31]. Figure 1 shows an example exponent 3 IP loop of order 15 .

| $*$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathrm{e}=0$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 1 | 1 | 2 | 0 | 5 | 7 | 4 | 9 | 3 | 11 | 8 | 14 | 13 | 6 | 10 | 12 |
| 2 | 2 | 0 | 1 | 7 | 5 | 3 | 12 | 4 | 9 | 6 | 13 | 8 | 14 | 11 | 10 |
| 3 | 3 | 6 | 8 | 4 | 0 | 10 | 2 | 13 | 1 | 12 | 11 | 14 | 7 | 5 | 9 |
| 4 | 4 | 8 | 6 | 0 | 3 | 13 | 1 | 12 | 2 | 14 | 5 | 10 | 9 | 7 | 11 |
| 5 | 5 | 11 | 10 | 2 | 1 | 6 | 0 | 9 | 14 | 4 | 12 | 7 | 13 | 8 | 3 |
| 6 | 6 | 4 | 3 | 14 | 9 | 0 | 5 | 11 | 13 | 7 | 2 | 1 | 10 | 12 | 8 |
| 7 | 7 | 10 | 12 | 1 | 2 | 14 | 13 | 8 | 0 | 11 | 6 | 3 | 5 | 9 | 4 |
| 8 | 8 | 3 | 4 | 11 | 14 | 12 | 10 | 0 | 7 | 13 | 1 | 9 | 2 | 6 | 5 |
| 9 | 9 | 14 | 13 | 6 | 12 | 1 | 11 | 2 | 5 | 10 | 0 | 4 | 8 | 3 | 7 |
| 10 | 10 | 5 | 7 | 13 | 11 | 8 | 3 | 14 | 12 | 0 | 9 | 6 | 4 | 2 | 1 |
| 11 | 11 | 13 | 5 | 10 | 8 | 9 | 14 | 1 | 6 | 3 | 7 | 12 | 0 | 4 | 2 |
| 12 | 12 | 7 | 14 | 9 | 13 | 2 | 8 | 10 | 4 | 5 | 3 | 0 | 11 | 1 | 6 |
| 13 | 13 | 9 | 11 | 12 | 10 | 7 | 4 | 6 | 3 | 2 | 8 | 5 | 1 | 14 | 0 |
| 14 | 14 | 12 | 9 | 8 | 6 | 11 | 7 | 5 | 10 | 1 | 4 | 2 | 3 | 0 | 13 |


| x | $\mathrm{x}^{2}$ | $\mathrm{x}^{-1}$ |
| :---: | :---: | :---: |
| 0 | 0 | 0 |
| 1 | 2 | 2 |
| 2 | 1 | 1 |
| 3 | 4 | 4 |
| 4 | 3 | 3 |
| 5 | 6 | 6 |
| 6 | 5 | 5 |
| 7 | 8 | 8 |
| 8 | 7 | 7 |
| 9 | 10 | 10 |
| 10 | 9 | 9 |
| 11 | 12 | 12 |
| 12 | 11 | 11 |
| 13 | 14 | 14 |
| 14 | 13 | 13 |

Figure 1: IP loop of exponent 3 with order 15
The class of elementary abelian p-groups is very small; for example, the total number of abelian 3 -groups having order up to 1000 is only seven. It is generally believed that the exponent property ( $x^{p}=e$ ) is responsible for such a low population of abelian 3 -groups. However, we have observed that the number of IP loops of exponent 3 exists in a large quantity; there are 27,765 such IP loops of order less than or equal to 15 . This provides us the notion that the exponent property is not keeping the population of groups so small. Rather, we demonstrate that it is the associative property that is reducing the number of groups.

This paper advances counting the history of loops and presents for the first time the count of IP loops of exponent 3 having order 15 . The presented results are obtained through enumeration and hence are available for inspection. In this paper, our contributions are as follows:

- We have enumerated, for the first time, the IP loops of exponent 3 having order 15.
- We have compared the associativity and exponent properties in IP loops and concluded that associativity is more stringent than exponent property.
- We have computationally verified and enumerated existing IP loops of exponent 3 having order up to 13 .

The rest of the paper is organized as follows. Section 2 describes the history of counting Latin squares and loops. The proposed systematic approach to count isomorphism classes of IP Loops is discussed in Section 3. Results and the related discussions are presented in Section 4.

| Key milestones in Latin Square <br> (LS) counting | Historical study details |
| :--- | :--- |
| Reduced LS up to $\mathrm{N}=5$ | Euler (1782) [10] <br> Cayley (1890) [7] <br> MacMahon (1915) [18] used a different <br> method to count, but obtained a wrong an- <br> swer |
| Reduced LS up to $\mathrm{N}=6$ | Frolov (1890) [12] <br> Tarry (1900) [32] <br> Jacob(1930) [15]-incorrectly |
| Main classes, isotopy classes, <br> and reduced LS up to N $=6$ | Schonhardt (1930) [29] |
| Isotopy classes up to N=6 | Fisher and Yates (1934) [11] |
| Main classes and <br> isotopy classes for $\mathrm{N}=7$ | Norton (1939)[24] -incorrectly <br> Sade (1951) [26] <br> Saxena (1951) [28] using MacMahon's ap- <br> proach |
| Main classes for N=8 | Arlazarov et al (1978) [3]-incorrectly <br> Kolesova et al (1990) [17] |
| Isotopy classes <br> up to N=8 | Brown (1968) [6]-incorrectly <br> Kolesova et al (1990) [17] |
| Reduced LS for N=8 | Wells (1967) [33] |
| Reduced LS for N=9 | Bammel and Rothstein (1975) |
| Reduced LS for N=10 | McKay and Rogoyski (1995) [21] |
| Reduced LS for N=11 | McKay and Wanless (2005) [22] |
| Main classes and isotopy classes <br> for N=9, 10 | McKay, Meynert and Myrvold (2007) [20] |
| Main classes and isotopy classes <br> for $\mathrm{N}=11$ | Hulpke, Kaski and Östergård (2011) [14] |

Table 1: History of counting Latin Squares

## 2. Related work

Earliest history of counting Latin Squares (LS) goes back to at least 1782 as the number of reduced LS of order 5 was known to Euler [10] and Cayley [7]. However, as noted by McKay et al [20], the counting has been constantly troubled by published errors. The history of counting reduced Latin squares and Loops is summarized in Tables 1 and 2. These tables show the main achievements and the related studies.

| Key milestones in Isomor- <br> phism classes of Loops and <br> Quasigroups counting | Historical study details |
| :--- | :--- |
| Loops up to $\mathrm{N}=6$ | Schonhardt (1930) [29], Albert (1944) [1] and <br> Sade (1970) [27] |
| Loops up to $\mathrm{N}=7$ | Brant and Mullen (1985) [5] |
| Loops for $\mathrm{N}=8$ | QSCGZ (2001) [25], Guerin (2001) [20] |
| Loops up to $\mathrm{N}=10$ | McKay, Meynert and Myrvold (2007) [20] |
| Quasigroups up to $\mathrm{N}=6$ | Bower (2000) [20] |
| Quasigroups up to $\mathrm{N}=10$ | McKay, Meynert and Myrvold (2007) [20] |
| Quasigroups and Loops of <br> $\mathrm{N}=11$ | Hulpke, Kaski and Östergård (2011) [14] |
| Inverse Property Loops up <br> to $\mathrm{N}=13$ | Slaney and Ali (2008) [2] |

Table 2: History of counting loops and quasigroups
Although researchers had interest in Latin squares, there has been considerable delay in achieving consecutive milestones. This was because of sheer computational complexity of the problem. These historical results were obtained through deduced mathematical formulas [23, 13], applying algorithmic approaches [27, 33, 4] or formulating them as constraint programming problems [2, 9]. In this paper we used constraint programming approach to further explore IP loops. We obtained for the first time the IP loops of exponent 3 of order up to 15. The algorithmic strategies applied to overcome the computational complexity to obtain these results are discussed in the following sections.

## 3. Enumerating isomorphism classes of IP loops

In order to count the number of IP loops of any order, we model the system as finite domain constraint satisfaction problem (CSPs), where the range of the binary operation $*$ is a CSP variable whose domain consists of elements of the algebra. Then the constraints related to Latin square, loop, and IP loop properties are ap-
plied on CSP variables. Constraint solver explores the state space in order to find all possible solutions that satisfy the specified constraints. For higher orders (even for order greater than 10) the state space becomes too large to perform exhaustive search for all IP loops. Therefore, we added more constraints for symmetry breaking which resulted into reduced state space. The constraints used for symmetry breaking along with other constraints are given in Table 3.

The solutions generated by constraint solver have enormous number of isomorphic copies. These redundant isomorphic copies need to be eliminated in order to get the count of isomorphism classes. The following subsection describes the techniques used to eliminate isomorphic copies from these solutions.

| No. | Name | Constraint |
| :---: | :--- | :--- |
| 1 | Latin square | $\forall r o w: \forall i, j \in$ row, $x_{i}=x_{j} \Rightarrow i=j$ <br> $\forall c o l: \forall i, j \in \operatorname{col}, y_{i}=y_{j} \Rightarrow i=j$ |
| 2 | Loop | $\forall x: e * x=x=x * e$ |
| 3 | IP loop | $\forall x, y \in L: x^{-1} *(x * y)=(y * x) * x^{-1}=y$ |
| 4 | Basic symmetry <br> breaking in IP loop | $\left\|x-x^{-1}\right\| \leq 1$ |
| 5 | Odd and even sym- <br> metry breaking | Odd/Even symmetry breaking con- <br> straints of $[2]$ |
| 6 | Isomorphism | $*_{1}$ Isom. $*_{2} \Leftrightarrow \forall i, j \in *_{1}, f\left(i *_{1} j\right)=$ <br> $f(i) *_{2} f(j)$ |
| 7 | Exponent 3 | $\forall x:(x * x) * x=e=x *(x * x)$ |
| 8 | Group | $\forall x, y, z:(x * y) * z=x *(y * z)$ |

Table 3: Constraints for exponent 3 IP loops and symmetry breaking

### 3.1. Valid mapping generation

Given two IP Loops $\left(L_{1}, *\right)$ and $\left(L_{2}\right.$, .), finding whether these loops are isomorphic to each other boils down to checking if there exists a bijective function $f: L_{1} \rightarrow L_{2}$ such that for all $u$ and $v$ in $L_{1}: f(u * v)=f(u) . f(v)$. In our case, $L_{1}(n \times n)$ is isomorphic to $L_{2}(n \times n)$ if $\forall i, j \leq n, f\left(L_{1}[i][j]\right)=L_{2}[f(i)][f(j)]$. Here $f$ is any permutation of $1 \ldots n$ elements. Finding isomorphism in this way, by applying the above formula for all permutations of $f$ is extremely time consuming and involves huge number of possibilities for even slightly large $n$. However, we observed that there are many permutations (mappings) of $f$ which do not satisfy the isomorphic relation $f\left(m_{1}[i][j]\right)=m_{2}[f(i)][f(j)]$ for all values of $i, j \leq n$ because of constraints shown in Table 3. We consider these mappings as invalid and discard them. We use constraint solver to find all valid mappings which satisfy isomorphic relationship between two IP Loops. Figure 2 represents valid mapping generation process.

The constraint solver models the system by specifying the relevant constraints


Figure 2: Schematic diagram of valid mappings generator
from Table 3. After the constraints are embedded in the model, the constraint solver searches the state space to find those permutations that satisfy these constraints. All such permutations are called "valid mappings". If the set $S$ represents all the permutations of $f$ and the set $S_{v}$ represents all the valid maps then $S_{v} \subseteq S$. The obtained valid mappings are then used to find isomorphism classes.

Figure 3 shows an example of invalid mapping $f(45)$. This mapping, if applied to a valid IP loop structure (shown on left) will produce an algebraic structure (shown on right) which does not satisfy the basic symmetry breaking constraint (i.e., $\left|x-x^{-1}\right| \leq 1$ ). For example, in the algebraic structure on the right side, for $x=3 ; x^{-1}=5$ and thus $\left|x-x^{-1}\right|>1$.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 1 | 2 | 0 | 5 | 7 | 4 | 9 | 3 | 11 | 8 | 14 | 13 | 6 | 10 | 12 |
| 2 | 0 | 1 | 7 | 5 | 3 | 12 | 4 | 9 | 6 | 13 | 8 | 14 | 11 | 10 |
| 3 | 6 | 8 | 4 | 0 | 10 | 2 | 13 | 1 | 12 | 11 | 14 | 7 | 5 | 9 |
| 4 | 8 | 6 | 0 | 3 | 13 | 1 | 12 | 2 | 14 | 5 | 10 | 9 | 7 | 11 |
| 5 | 11 | 10 | 2 | 1 | 6 | 0 | 9 | 14 | 4 | 12 | 7 | 13 | 8 | 3 |
| 6 | 4 | 3 | 14 | 9 | 0 | 5 | 11 | 13 | 7 | 2 | 1 | 10 | 12 | 8 |
| 7 | 10 | 12 | 1 | 2 | 14 | 13 | 8 | 0 | 11 | 6 | 3 | 5 | 9 | 4 |
| 8 | 3 | 4 | 11 | 14 | 12 | 10 | 0 | 7 | 13 | 1 | 9 | 2 | 6 | 5 |
| 9 | 14 | 13 | 6 | 12 | 1 | 11 | 2 | 5 | 10 | 0 | 4 | 8 | 3 | 7 |
| 10 | 5 | 7 | 13 | 11 | 8 | 3 | 14 | 12 | 0 | 9 | 6 | 4 | 2 | 1 |
| 11 | 13 | 5 | 10 | 8 | 9 | 14 | 1 | 6 | 3 | 7 | 12 | 0 | 4 | 2 |
| 12 | 7 | 14 | 9 | 13 | 2 | 8 | 10 | 4 | 5 | 3 | 0 | 11 | 1 | 6 |
| 13 | 9 | 11 | 12 | 10 | 7 | 4 | 6 | 3 | 2 | 8 | 5 | 1 | 14 | 0 |
| 14 | 12 | 9 | 8 | 6 | 11 | 7 | 5 | 10 | 1 | 4 | 2 | 3 | 0 | 13 |$|$



Figure 3: Example of an invalid mapping which produces an algebraic structure (on the right) that does not satisfy the basic symmetry breaking constraint $\left(\left|x-x^{-1}\right| \leq 1\right)$

Detecting isomorphism classes using valid mappings drastically increases the efficiency because $S_{v}$ is usually much smaller than $S$. For example, for IP loop of order 15 , the possible number of mappings $(|S|)$ is approximately 87 billion but there are only 509,086 valid mappings (i.e., $\left|S_{v}\right|$ is $0.0005 \%$ of $|S|$ ). This results in much faster isomorphic detection.

Table 4 shows the reduced number of valid mappings and their impact on
the time taken to identify isomorphism classes for three different problems. In all the three cases, we observed considerable improvement in time when detecting isomorphism. This improvement is even more significant for higher order IP loops. For example, for IP loop of order 11, the time taken to identify isomorphism classes is reduced by a factor of 500 when valid mappings were used.

|  | H 0 0 0 0 0 0 0 0 0 0 | 苞 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | $\bar{\square}$ | cs |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| Latin Square (Order 5) | 161280 | 1411 | 120 | 120 | 138 | 138 | 2 |
| $\begin{aligned} & \text { IP Loop } \\ & \text { (Order 11) } \\ & \hline \end{aligned}$ | 6464 | 49 | 3628800 | 3654 | 5085 | 10 | 5 |
| IP Loop of exponent 3 (Order 13) | 22000 | 64 | $\approx \underset{10^{6}}{ }=$ | 34804 | $\underset{864000}{\approx}$ | 571 | 185 |

Table 4: Time reductions obtained using valid mappings and tree-based approaches

### 3.2. Tree representation of isomorphism classes

In order to identify a new isomorphism class, we need to check a newly found solution against all the previously found isomorphism classes using all valid mappings. This results in a large number of computations, and even with the reduced set of mappings the computational time was too high. After careful examination of isomorphism classes we discovered that these classes have similar structure (elements), and with proper organization of isomorphism classes several computations can be eliminated. So we devised a scheme that represents isomorphism classes using a tree-based structure to reduce redundant computations.

The tree structure is built such that each branch of the tree represents one isomorphism class. All new isomorphism classes are added to the existing tree. As long as two isomorphism classes have the same element values, they are represented by a single branch in the tree. If element values differ at any depth in a branch, a new offshoot is created to represent all the subsequent values.

This representation reduces the memory needed to maintain isomorphism classes, especially when the number of isomorphism classes are high. In addition to memory saving, the tree-based approach drastically improves the speed in detecting isomorphism classes in two ways. First, by eliminating redundant computations since one node in the tree represents elements of many isomorphism classes. Second, by discarding all the siblings of a node whenever it satisfies the isomorphism constraint.

The last column in Table 4 (i.e., Time with $\left|S_{v}\right|$ and Tree) shows the results obtained by using tree representation on different problems. As anticipated, the reduction in time depends on the number of isomorphism classes. For example the time taken to detect isomorphism classes with tree representation was reduced by a factor of 2 when the number of isomorphism classes was 45 , whereas the time taken was reduced by a factor of 45 when the number of isomorphism classes was 6808.


Figure 4: Proposed distributed system to identify isomorphism classes

### 3.3. Distributed system

With the help of reduced mappings and tree representation, isomorphism classes of IP loops up to order 13 can be enumerated in reasonable time using a single desktop machine. However for higher orders, even after reducing the set of mappings and the number of comparisons, the number of isomorphic copies are still too high to be managed by a standalone system. To cope up with this problem, we developed a distributed system for identifying isomorphism classes as shown in Figure 4. The distributed system takes a single input file containing solutions provided by the
constraint solver and breaks it up into several files each containing a manageable subset of the solutions. Each node (i.e., a processor) in the distributed system selects one of the input files for exclusive use and produces the isomorphism classes using valid mappings and tree representation as described in previous sections. The output is written into an intermediate file for further processing. These output files can still contains isomorphic copies as the nodes are unaware of the isomorphism classes found by each other. Therefore, another node exhaustively searches all the intermediate files to produce the final set of isomorphism classes.

| Order | Total <br> solutions | Isomorphism classes |  | $\left\|S_{v}\right\|(\|S\|)$ | Time <br> (sec) |
| :---: | :---: | :---: | :---: | :---: | :---: |
|  |  | non- <br> associative | associative <br> (groups) |  |  |
| $\mathbf{5}$ | 0 | 0 | 0 | $0(24)$ | $<1$ |
| $\mathbf{7}$ | 2 | 1 | 0 | $48(720)$ | $<1$ |
| $\mathbf{9}$ | 10 | 1 | 1 | 276 <br> $(40,320)$ | $<1$ |
| $\mathbf{1 1}$ | 0 | 0 | 0 | 2402 <br> $(3,628,800)$ | $<1$ |
| $\mathbf{1 3}$ | 22,000 | 64 | 0 | 43804 <br> $(\approx 479$ <br> million) | 210 |
| $\mathbf{1 5}$ | $71,149,968$ | 27,698 | 0 | 509086 <br> $(\approx 87$ <br> billion) | $\approx 934,725$ <br> (for hours total <br> solutions) |

Table 5: IP loops of exponent 3

## 4. Results and discussions

We modeled the system as finite domain CSPs and used a generic constraint solver JaCoP to generate IP loops. We were able to verify the results up to IP loops of order 11 using JaCoP. However, we encountered severe memory and latency issues for higher orders. Therefore, we tried another leading constraint solver Google's or-tools and were able to resolve the memory and latency issues. We modeled all IP loop constraints in or-tools and enumerated IP loops of higher order. The valid mappings and tree representation were used to speed up the process of finding isomorphism classes.

The results for IP loops of exponent 3 are shown in Table 5 . We have verified the known results till order 13 and produced new results for order 15. For IP
loops of exponent 3 having order 13, or-tools constraint solver produced 22,000 solutions. It took 210 seconds on a general desktop to find all the 64 isomorphism classes.

For IP loops of exponent 3 having order 15, constraint solver produced roughly 71 million solutions. It took about 28 hours to get these results. 27,698 isomorphism classes were found by using the distributed system described in Section 3.3. It was executed on 71 different processors on 20 general desktop computers. It took about 4 days to find the complete set of isomorphism classes.

Generating IP loops of higher orders gave us new perspective about the algebraic structures and their properties. As shown in the Table 5, the number of non-associative isomorphism classes has a reasonable size for higher orders. However, their size plummets to very small number as soon as associativity property is added to the structure. This clearly indicates that it is the associativity property that is seldom present in algebraic structures thus drastically reducing the number of isomorphism classes.

| Size of automorphism <br> group | Number of exponent 3 <br> IP loops |
| :---: | :---: |
| 1 | 25899 |
| 2 | 1385 |
| 3 | 171 |
| 4 | 140 |
| 6 | 50 |
| 8 | 22 |
| 12 | 10 |
| 16 | 2 |
| 21 | 3 |
| 24 | 13 |
| 168 | 1 |
| 192 | 1 |
| 1344 | 1 |

Table 6: Size of automorphism group of exponent 3 IP loops of order 15
We have also computed the size of automorphism groups of exponent 3 IP loops of order 15 which is shown in Table 6. The IP loop with largest automorphism group is shown in Figure 5.

Another interesting thing to note is the count of $3 \times 3$ Latin subsquares in exponent 3 IP loops due to their role in a conjecture by van Rees [16]. Table 7 shows the count of $3 \times 3$ Latin subsquares in exponent 3 IP loops and Figure 6 shows two exponent 3 IP loops of order 15 which have the highest count of $3 \times 3$ Latin subsquares. Both these loops have 91 such Latin subsquares.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 1 | 2 | 0 | 5 | 6 | 4 | 3 | 9 | 10 | 8 | 7 | 13 | 14 | 12 | 11 |
| 2 | 0 | 1 | 6 | 5 | 3 | 4 | 10 | 9 | 7 | 8 | 14 | 13 | 11 | 12 |
| 3 | 6 | 5 | 4 | 0 | 1 | 2 | 11 | 12 | 14 | 13 | 8 | 7 | 9 | 10 |
| 4 | 5 | 6 | 0 | 3 | 2 | 1 | 12 | 11 | 13 | 14 | 7 | 8 | 10 | 9 |
| 5 | 3 | 4 | 2 | 1 | 6 | 0 | 14 | 13 | 12 | 11 | 9 | 10 | 7 | 8 |
| 6 | 4 | 3 | 1 | 2 | 0 | 5 | 13 | 14 | 11 | 12 | 10 | 9 | 8 | 7 |
| 7 | 10 | 9 | 12 | 11 | 13 | 14 | 8 | 0 | 1 | 2 | 3 | 4 | 6 | 5 |
| 8 | 9 | 10 | 11 | 12 | 14 | 13 | 0 | 7 | 2 | 1 | 4 | 3 | 5 | 6 |
| 9 | 7 | 8 | 13 | 14 | 11 | 12 | 2 | 1 | 10 | 0 | 6 | 5 | 4 | 3 |
| 10 | 8 | 7 | 14 | 13 | 12 | 11 | 1 | 2 | 0 | 9 | 5 | 6 | 3 | 4 |
| 11 | 14 | 13 | 7 | 8 | 10 | 9 | 4 | 3 | 5 | 6 | 12 | 0 | 1 | 2 |
| 12 | 13 | 14 | 8 | 7 | 9 | 10 | 3 | 4 | 6 | 5 | 0 | 11 | 2 | 1 |
| 13 | 11 | 12 | 10 | 9 | 8 | 7 | 5 | 6 | 3 | 4 | 2 | 1 | 14 | 0 |
| 14 | 12 | 11 | 9 | 10 | 7 | 8 | 6 | 5 | 4 | 3 | 1 | 2 | 0 | 13 |

Figure 5: IP loop of exponent 3 with order 15 having the largest automorphism group (size=1344)

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 2 | 0 | 5 | 7 | 9 | 11 | 12 | 10 | 3 | 13 | 14 | 4 | 8 | 6 |
| 2 | 0 | 1 | 9 | 12 | 3 | 14 | 4 | 13 | 5 | 8 | 6 | 7 | 10 | 11 |
| 3 | 11 | 8 | 4 | 0 | 14 | 2 | 9 | 6 | 13 | 1 | 10 | 5 | 7 | 12 |
| 4 | 10 | 6 | 0 | 3 | 12 | 8 | 13 | 2 | 7 | 11 | 1 | 14 | 9 | 5 |
| 5 | 13 | 12 | 7 | 1 | 6 | 0 | 11 | 14 | 8 | 2 | 3 | 10 | 4 | 9 |
| 6 | 4 | 10 | 11 | 13 | 0 | 5 | 3 | 9 | 14 | 12 | 7 | 2 | 1 | 8 |
| 7 | 14 | 9 | 1 | 5 | 10 | 13 | 8 | 0 | 11 | 4 | 2 | 6 | 12 | 3 |
| 8 | 3 | 11 | 14 | 10 | 4 | 12 | 0 | 7 | 2 | 5 | 9 | 13 | 6 | 1 |
| 9 | 7 | 14 | 12 | 2 | 11 | 1 | 6 | 3 | 10 | 0 | 13 | 8 | 5 | 4 |
| 10 | 6 | 4 | 8 | 14 | 13 | 7 | 1 | 12 | 0 | 9 | 5 | 3 | 11 | 2 |
| 11 | 8 | 3 | 13 | 6 | 1 | 9 | 14 | 5 | 4 | 7 | 12 | 0 | 2 | 10 |
| 12 | 5 | 13 | 2 | 9 | 8 | 4 | 10 | 1 | 6 | 14 | 0 | 11 | 3 | 7 |
| 13 | 12 | 5 | 6 | 11 | 7 | 10 | 2 | 4 | 1 | 3 | 8 | 9 | 14 | 0 |
| 14 | 9 | 7 | 10 | 8 | 2 | 3 | 5 | 11 | 12 | 6 | 4 | 1 | 0 | 13 |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 1 | 2 | 0 | 5 | 7 | 9 | 11 | 12 | 10 | 4 | 13 | 14 | 3 | 6 | 8 |
| 2 | 0 | 1 | 12 | 9 | 3 | 13 | 4 | 14 | 5 | 8 | 6 | 7 | 10 | 11 |
| 3 | 10 | 8 | 4 | 0 | 13 | 2 | 5 | 11 | 12 | 6 | 1 | 14 | 9 | 7 |
| 4 | 11 | 6 | 0 | 3 | 7 | 10 | 14 | 2 | 13 | 1 | 8 | 9 | 5 | 12 |
| 5 | 14 | 12 | 9 | 1 | 6 | 0 | 11 | 3 | 8 | 2 | 13 | 10 | 7 | 4 |
| 6 | 4 | 10 | 8 | 14 | 0 | 5 | 13 | 9 | 3 | 12 | 7 | 2 | 11 | 1 |
| 7 | 13 | 9 | 1 | 12 | 10 | 4 | 8 | 0 | 11 | 14 | 2 | 6 | 3 | 5 |
| 8 | 3 | 11 | 13 | 6 | 14 | 12 | 0 | 7 | 2 | 5 | 9 | 4 | 1 | 10 |
| 9 | 7 | 14 | 2 | 5 | 11 | 1 | 6 | 13 | 10 | 0 | 4 | 8 | 12 | 3 |
| 10 | 6 | 3 | 14 | 11 | 4 | 7 | 1 | 12 | 0 | 9 | 5 | 13 | 8 | 2 |
| 11 | 8 | 4 | 10 | 13 | 1 | 9 | 3 | 5 | 14 | 7 | 12 | 0 | 2 | 6 |
| 12 | 5 | 13 | 7 | 2 | 8 | 14 | 10 | 1 | 6 | 3 | 0 | 11 | 4 | 9 |
| 13 | 12 | 7 | 11 | 8 | 2 | 3 | 9 | 6 | 1 | 4 | 10 | 5 | 14 | 0 |
| 14 | 9 | 5 | 6 | 10 | 12 | 8 | 2 | 4 | 7 | 11 | 3 | 1 | 0 | 13 |

Figure 6: IP loops of exponent 3 with order 15 having the highest count of $3 \times 3$ Latin subsquares

| Count of $3 \times 3$ <br> Latin subsquares | Number of exponent 3 IP loops | Count of $3 \times 3$ <br> Latin subsquares | Number of exponent 3 IP loops |
| :---: | :---: | :---: | :---: |
| 7 | 992 | 34 | 44 |
| 9 | 856 | 35 | 34 |
| 10 | 2083 | 36 | 25 |
| 11 | 457 | 37 | 59 |
| 12 | 1996 | 38 | 20 |
| 13 | 2676 | 39 | 10 |
| 14 | 1046 | 40 | 19 |
| 15 | 2430 | 41 | 14 |
| 16 | 2440 | 42 | 4 |
| 17 | 1279 | 43 | 32 |
| 18 | 2022 | 45 | 5 |
| 19 | 1977 | 46 | 5 |
| 20 | 988 | 47 | 2 |
| 21 | 1397 | 48 | 3 |
| 22 | 1090 | 49 | 14 |
| 23 | 619 | 50 | 2 |
| 24 | 705 | 51 | 4 |
| 25 | 626 | 52 | 3 |
| 26 | 332 | 53 | 1 |
| 27 | 422 | 55 | 13 |
| 28 | 293 | 58 | 1 |
| 29 | 175 | 61 | 1 |
| 30 | 159 | 67 | 1 |
| 31 | 177 | 73 | 1 |
| 32 | 62 | 91 | 2 |
| 33 | 80 |  |  |

Table 7: Number of exponent 3 IP loops of order 15 grouped by count of $3 \times 3$ Latin subsquares

## References

[1] A.A. Albert, Quasigroups. II, Trans. American Mathematical Society 55 (1944), 401-409.
[2] A. Ali and J. Slayney, Counting loops with the inverse property, Quasigroups and Related Systems 16 (2008), 13-16.
[3] V.L. Arlazarov, A.M. Baraev, Y.Y. Gol'fand and I.A. Faradzev, Construction with the aid of a computer of all latin squares of order 8, Algorithmic Investigations in Combinatoric 187 (1978), 129 - 141.
[4] S.E. Bammel and J. Rothstein, The number of $9 \times 9$ latin squares, Discrete Math. 11 (1975), $83-95$.
[5] L.J. Brant and G.L. Mullen, A note on isomorphism classes of reduced latin squares of order 7 , Utilitas Mathematica 27 (1985), $261-263$.
[6] J.W. Brown, Enumeration of latin squares with application to order 8, J. Combinatorial Theory 5 (1972), $177-184$.
[7] A. Cayley, On latin squares, Oxford Camb. Dublin Messenger of Math. 19 (1890), 85-239.
[8] D. Daly and P. Vojtechovsky, Enumeration of nilpotent loops via cohomology, J. Algebra 322 (2009), $4080-4098$.
[9] G. Dequen and O. Dubois, The non-existence of a $(3,1,2)$-conjugate orthogonal Latin square of order 10, In: Principles and Practice of Constraint Programming (CP), 108-201.
[10] L. Euler, Recherches sur une nouvelle espéce de quarrés magiques combinatorial aspects of relations, Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen de Vlissingen 9 (1782), $85-239$.
[11] R.A. Fisher and F. Yates, The $6 \times 6$ latin squares, Proc. Cambridge Philos. Soc. 30 (1934), 492 - 507.
[12] M. Frolov, Sur les permutations carrées, J. de Math. spéc IV (1890), 8-11, 25-30.
[13] I. Gessel, Counting latin rectangles, Bull. Amer. Math. Soc. 16 (1987), $79-83$.
[14] A. Hulpke, P. Kaski and P.R.J. Östergård, The number of Latin squares of order 11, Math. Comp. 80 (2011), 1197 - 1219.
[15] S.M. Jacob, The enumeration of the latin rectangle of depth three by means of a formula of reduction, with other theorems relating to non-clashing substitutions and latin squares, Proc. London Math. Soc. 31 (1930), $329-354$.
[16] M. Kinyon and I.M. Wanless, Loops with exponent three in all isotopes, Internat. J. Algebra Comput., 25 (2015), 1159 - 1177.
[17] G. Kolesova, C.W.H. Lam, and L. Thiel, On the number of $8 \times 8$ latin squares, J. Combin. Theory Ser. A 54 (1990), $143-148$.
[18] P.A. MacMahon, Combinatory Analysis, Cambridge University Press 1 (1915).
[19] R. Maddux, Some varieties containing relation algebras, Trans. Amer. Math. Soc. 272 (1982), 501 - 526.
[20] B.D. McKay, A. Meynert, and W. Myrvold, Small latin squares, quasigroups, and loops, J. Combinatorial Designs 15 (2007), 98 - 119.
[21] B.D. McKay and E. Rogoyski, Latin squares of order 10, Electron. J. Combin. 2 (1995), R3, $1-4$.
[22] B.D. McKay and I.M. Wanless, On the number of latin squares, Ann. Combin. 9 (2005), $335-344$.
[23] J.R. Nechvatal, Asymptotic Enumeration of Generalised Latin Rectangles, Util. Math. 20 (1981), 273 - 292.
[24] H.W. Norton, The $7 \times 7$ squares, Ann. Eugenics 9 (1939), $269-307$.
[25] QSCGZ. (pseudonym), Anonymous electronic posting to Loopforum, (2001). http://groups.yahoo.com/group/loopforum.
[26] A. Sade, An omission in norton's list of $7 \times 7$ squares, Ann. Math. Stat. 22 (1951), 306-307.
[27] A. Sade, Morphismes de quasigroupes: Tables, Revista da Faculdade de Ciências de Lisboa, 2: A - Ciências Matemáticas 13 (1970/71), 149 - 172.
[28] P.N. Saxena, A simplified method of enumerating latin squares by MacMahon's differential operators; ii. the $7 \times 7$ latin squares, J. Indian Soc. Agric. Statistics $\mathbf{3}$ (1951), $24-79$.
[29] E. Schönhardt, Über lateinische quadrate und unionen, J. für die reine und angewandte Mathematik 163 (1930), 183 - 230.
[30] M.C. Slattery and A.L. Zenisek, Moufang loops of order 243, Comment. Math. Univ. Carolin. 53 (2012), $423-428$.
[31] J. Slayney and A. Ali, Generating loops with the inverse property, Proc. of ESARM, (2008), $55-66$.
[32] G. Tarry, Le probléme des 36 officiers, Ass. Franc. Paris 29 (1900), $170-203$.
[33] M.B. Wells, The number of latin squares of order eight, J. Combinatorial Theory 3 (1967), 98 - 99.

Received October 30, 2016
College of Computer Engineering and Science
Prince Mohammad Bin Fahd University
Al-Khobar, 31952
KSA
e-mail: makhan@pmu.edu.sa, smuhammad@pmu.edu.sa, nmohammad@pmu.edu.sa
Faculty of Mathematics Department
Quaid-e-Azam University
Islamabad
Pakistan
e-mail: dr_asif_ali@hotmail.com

# On bi-bases of a semigroup 

Pisit Kummoon and Thawhat Changphas


#### Abstract

Based on the results of bi-ideals generated by a non-empty subset of a semigroup $S$, we introduce the concept which is called bi-bases of the semigroup $S$. Using the quasi-order defined by the principal bi-ideals of $S$, we give a characterization when a non-empty subset of $S$ is a bi-base of $S$.


## 1. Preliminaries

Let $S$ be a semigroup. A subset $A$ of the semigroup $S$ is called a two-sided base (or simply base) of $S$ if it satisfies the following two conditions:
(i) $S=A \cup S A \cup A S \cup S A S$;
(ii) if $B$ is a subset of $A$ such that $S=B \cup S B \cup B S \cup S B S$, then $B=A$.

This notion was first introduced and studied by I. Fabrici [3]. In fact, using the quasi-order defined by principal two-sided ideals of $S$, the author gave a characterization when a non-empty subset of $S$ is a base of $S$. Moreover, the structure of semigroups containing two-sided bases was described. Indeed, using the concepts of left ideals and right ideals generated by a non-empty set, the concepts of left bases and right bases of a semigroup were introduced by T. Tamura before the concept of two-sided bases (see [7]). In [2], I. Fabrici studied the structure of a semigroup containing one-sided bases. In [4], I. Fabrici and T. Kepka showed that there is a relation between bases and maximal ideals of a semigroup. The results obtaind by I. Fabrici [3] have been extended to ordered semigroups by T. Changphas and P. Summaprab (see [1]). As in the line of I. Fabrici ([3], [2]) mentioned before, the main purpose of this paper is to introduce the concept which is called bi-bases of a semigroup. We also define the quasi-order using principal bi-ideals of $S$, and give a characterization when a non-empty subset of $S$ is a bi-base of $S$.

Let $S$ be a semigroup, and $A, B$ non-empty subsets of $S$. The set product $A B$ of $A$ and $B$ is defined to be the set of all elements $a b$ with $a$ in $A$ and $b$ in $B$. That is

$$
A B=\{a b \mid a \in A, b \in B\}
$$

For $a \in S$, we write $B a$ for $B\{a\}$, and similarly for $a B$.

A subsemigroup $B$ of a semigroup $S$ is called a bi-ideal ([5], [6]) of $S$ if

$$
B S B \subseteq B
$$

This notion generalizes the notion of one-sided ideals and two-sided ideals of a semigroup.

Let $S$ be a semigroup, and $B_{i}$ a bi-ideal of $S$ for each $i$ in an indexed set $I$. It is known that if $\bigcap_{i \in I} B_{i} \neq \emptyset$, then $\bigcap_{i \in I} B_{i}$ is a bi-ideal of $S$. Moreover, for a non-empty subset $A$ of $S$, the intersection of all bi-ideals of $S$ containing $A$, denoted by $(A)_{b}$, is the smallest bi-ideal of $S$ containing $A$. And it is of the form

$$
(A)_{b}=A \cup A A \cup A S A
$$

In particular, for $A=\{a\}$, we write $(\{a\})_{b}$ by $(a)_{b}$ (see [6]).

## 2. Main Results

We begin this section with the following definition of bi-bases of a semigroup.
Definition 2.1. Let $S$ be a semigroup. A subset $B$ of $S$ is called a bi-base of $S$ if it satisfies the following two conditions:
(i) $S=(B)_{b}$ (i.e. $S=B \cup B B \cup B S B$ );
(ii) if $A$ is a subset of $B$ such that $S=(A)_{b}$, then $A=B$.

Example 2.2. Let $S=\{r, s, t, u\}$ be a semigroup with the binary operation defined by:

| $\cdot$ | $r$ | $s$ | $t$ | $u$ |
| :--- | :--- | :--- | :--- | :--- |
| $r$ | $r$ | $s$ | $r$ | $r$ |
| $s$ | $s$ | $r$ | $s$ | $s$ |
| $t$ | $r$ | $s$ | $t$ | $u$ |
| $u$ | $r$ | $s$ | $u$ | $t$ |

We have that the bi-bases of $S$ are: $B_{1}=\{t\}$ and $B_{2}=\{u\}$.
Example 2.3. Let $S=\{p, q, r, s\}$ be a semigroup with the binary operation defined by:

| $\cdot$ | $p$ | $q$ | $r$ | $s$ |
| :--- | :--- | :--- | :--- | :--- |
| $p$ | $p$ | $p$ | $p$ | $p$ |
| $q$ | $p$ | $p$ | $p$ | $p$ |
| $r$ | $p$ | $p$ | $q$ | $q$ |
| $s$ | $p$ | $p$ | $q$ | $q$ |

It is a routine matter to check that $S$ has only one bi-base: $B=\{r, s\}$.

Example 2.4. Let $S=\{a, b, c, d, x, y\}$ be a semigroup with the binary operation defined by:

| $\cdot$ | $a$ | $b$ | $c$ | $d$ | $x$ | $y$ |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $a$ | $a$ | $b$ | $c$ | $d$ | $x$ | $y$ |
| $b$ | $b$ | $c$ | $a$ | $y$ | $d$ | $x$ |
| $c$ | $c$ | $a$ | $d$ | $x$ | $y$ | $d$ |
| $d$ | $d$ | $x$ | $y$ | $a$ | $b$ | $c$ |
| $x$ | $x$ | $y$ | $d$ | $c$ | $a$ | $b$ |
| $y$ | $y$ | $d$ | $x$ | $b$ | $c$ | $a$ |

We have that the singleton sets consisting of an element of $S$ are bi-bases of $S$.
First, we have the following useful lemma:
Lemma 2.5. Let $B$ be a bi-base of a semigroup $S$, and $a, b \in B$. If $a \in b b \cup b S b$, then $a=b$.

Proof. Assume that $a \in b b \cup b S b$, and suppose that $a \neq b$. We consider

$$
A=B \backslash\{a\}
$$

Then $A \subset B$. Since $a \neq b, b \in A$. We will show that $(A)_{b}=S$. Clearly, $(A)_{b} \subseteq S$. Let $x \in S$. Then, by $(B)_{b}=S$, we have $x \in B \cup B B \cup B S B$. There are three cases to consider:
Case 1: $x \in B$.
Subcase 1.1: $x \neq a$. Then $x \in B \backslash\{a\}=A \subseteq(A)_{b}$.
Subcase 1.2: $x=a$. By assumption,

$$
x=a \in b b \cup b S b \subseteq A A \cup A S A \subseteq(A)_{b} .
$$

Case 2: $x \in B B$. Then $x=b_{1} b_{2}$ for some $b_{1}, b_{2} \in B$.
Subcase 2.1: $b_{1}=a$ and $b_{2}=a$. By assumption,

$$
\begin{aligned}
x=b_{1} b_{2} & \in(b b \cup b S b)(b b \cup b S b)=b b b b \cup b b b S b \cup b S b b b \cup b S b b S b \\
& \subseteq A A A A \cup A A A S A \cup A S A A A \cup A S A A S A \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 2.2: $b_{1} \neq a$ and $b_{2}=a$. By assumption and $A=B \backslash\{a\}$, we have

$$
\begin{aligned}
x=b_{1} b_{2} & \in(B \backslash\{a\})(b b \cup b S b)=(B \backslash\{a\}) b b \cup(B \backslash\{a\}) b S b \\
& \subseteq A A A \cup A A S A \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 2.3: $b_{1}=a$ and $b_{2} \neq a$. By assumption and $A=B \backslash\{a\}$, we have

$$
\begin{aligned}
x=b_{1} b_{2} & \in(b b \cup b S b)(B \backslash\{a\})=b b(B \backslash\{a\}) \cup b S b(B \backslash\{a\}) \\
& \subseteq A A A \cup A S A A \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 2.4: $b_{1} \neq a$ and $b_{2} \neq a$. From $A=B \backslash\{a\}$,

$$
x=b_{1} b_{2} \in(B \backslash\{a\})(B \backslash\{a\})=A A \subseteq(A)_{b}
$$

Case 3: $x \in B S B$. Then $x=b_{3} s b_{4}$ for some $b_{3}, b_{4} \in B$ and $s \in S$.
Subcase 3.1: $b_{3}=a$ and $b_{4}=a$. By assumption,

$$
\begin{aligned}
x=b_{3} s b_{4} & \in(b b \cup b S b) S(b b \cup b S b)=b b S b b \cup b b S b S b \cup b S b S b b \cup b S b S b S b \\
& \subseteq A A S A A \cup A A S A S A \cup A S A S A A \cup A S A S A S A \\
& \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 3.2: $b_{3} \neq a$ and $b_{4}=a$. By assumption and $A=B \backslash\{a\}$, we have

$$
\begin{aligned}
x=b_{3} s b_{3} & \in(B \backslash\{a\}) S(b b \cup b S b)=(B \backslash\{a\}) S b b \cup(B \backslash\{a\}) S b S b \\
& \subseteq A S A A \cup A S A S A \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 3.3: $b_{3}=a$ and $b_{4} \neq a$. By assumption and $A=B \backslash\{a\}$, we have

$$
\begin{aligned}
x=b_{3} s b_{4} & \in(b b \cup b S b) S(B \backslash\{a\})=b b S(B \backslash\{a\}) \cup b S b S(B \backslash\{a\}) \\
& \subseteq A A S A \cup A S A S A \subseteq A S A \subseteq(A)_{b}
\end{aligned}
$$

Subcase 3.4: $b_{3} \neq a$ and $b_{4} \neq a$. From $A=B \backslash\{a\}$, hence

$$
x=b_{3} s b_{4} \in(B \backslash\{a\}) S(B \backslash\{a\})=A S A \subseteq(A)_{b}
$$

Hence, $(A)_{b}=S$. And this is a contradiction. Thus $a=b$.
Lemma 2.6. Let $B$ be a bi-base of a semigroup $S$. Let $a, b, c \in B$. If $a \in c b \cup c S b$, then $a=b$ or $a=c$.

Proof. Assume that $a \in c b \cup c S b$, and suppose that $a \neq b$ and $a \neq c$. We set

$$
A=B \backslash\{a\}
$$

Then $A \subset B$. Since $a \neq b$ and $a \neq c$, we have $b, c \in A$. We will show that $(A)_{b}=S$. Clearly, $(A)_{b} \subseteq S$. Let $x \in S$. By $(B)_{b}=S, x \in B \cup B B \cup B S B$.

We consider three cases:
Case 1: $x \in B$.
Subcase 1.1: $x \neq a$. Then $x \in B \backslash\{a\}=A \subseteq(A)_{b}$.
SUBCASE 1.2: $x=a$. By assumption, $x=a \in c b \cup c S b \subseteq A A \cup A S A \subseteq(A)_{b}$.
Case 2: $x \in B B$. Then $x=b_{1} b_{2}$ for some $b_{1}, b_{2} \in B$.
Subcase 2.1: $b_{1}=a$ and $b_{2}=a$. By assumption,

$$
\begin{aligned}
x=b_{1} b_{2} & \in(c b \cup c S b)(c b \cup c S b)=c b c b \cup c b c S b \cup c S b c b \cup c S b c S b \\
& \subseteq A A A A \cup A A A S A \cup A S A A A \cup A S A A S A \\
& \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 2.2: $b_{1} \neq a$ and $b_{2}=a$. By assumption and $A=B \backslash\{a\}$, we have

$$
\begin{aligned}
x=b_{1} b_{2} & \in(B \backslash\{a\})(c b \cup c S b)=(B \backslash\{a\}) c b \cup(B \backslash\{a\}) c S b \\
& \subseteq A A A \cup A A S A \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 2.3: $b_{1}=a$ and $b_{2} \neq a$. By assumption and $A=B \backslash\{a\}$, we have

$$
\begin{aligned}
x=b_{1} b_{2} & \in(c b \cup c S b)(B \backslash\{a\})=c b(B \backslash\{a\}) \cup c S b(B \backslash\{a\}) \\
& \subseteq A A A \cup A S A A \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 2.4: $b_{1} \neq a$ and $b_{2} \neq a$. From $A=B \backslash\{a\}$, hence

$$
x=b_{1} b_{2} \in(B \backslash\{a\})(B \backslash\{a\})=A A \subseteq(A)_{b}
$$

Case 3: $x \in B S B$. Then $x=b_{3} s b_{4}$ for some $b_{3}, b_{4} \in B$ and $s \in S$.
Subcase 3.1: $b_{3}=a$ and $b_{4}=a$. By assumption we have

$$
\begin{aligned}
x=b_{3} s b_{4} & \in(c b \cup c S b) S(c b \cup c S b)=c b S c b \cup c b S c S b \cup c S b S c b \cup c S b S c S b \\
& \subseteq A A S A A \cup A A S A S A \cup A S A S A A \cup A S A S A S A \\
& \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 3.2: $b_{3} \neq a$ and $b_{4}=a$. By assumption and $A=B \backslash\{a\}$, we have

$$
\begin{aligned}
x=b_{3} s b_{3} & \in(B \backslash\{a\}) S(c b \cup c S b)=(B \backslash\{a\}) S c b \cup(B \backslash\{a\}) S c S b \\
& \subseteq A S A A \cup A S A S A \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 3.3: $b_{3}=a$ and $b_{4} \neq a$. By assumption and $A=B \backslash\{a\}$, we have

$$
\begin{aligned}
x=b_{3} s b_{4} & \in(c b \cup c S b) S(B \backslash\{a\})=c b S(B \backslash\{a\}) \cup c S b S(B \backslash\{a\}) \\
& \subseteq A A S A \cup A S A S A \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Subcase 3.4: $b_{3} \neq a$ and $b_{4} \neq a$. From $A=B \backslash\{a\}$, hence

$$
x=b_{3} s b_{4} \in(B \backslash\{a\}) S(B \backslash\{a\})=A S A \subseteq(A)_{b}
$$

Hence $(A)_{b}=S$. This is a contradiction, and thus $a=b$.
To give a characterization when a non-empty subset of a semigroup is a bi-base of the semigroup we need the quasi-order defined as follows:
Definition 2.7. Let $S$ be a semigroup. Define a quasi-order on $S$ by, for any $a, b \in S$,

$$
a \leqslant_{b} b: \Leftrightarrow(a)_{b} \subseteq(b)_{b}
$$

The following example shows that the relation $\leqslant_{b}$ defined above is not, in general, a partial order.

Example 2.8. From Example 2.4, we have that $(a)_{b} \subseteq(b)_{b}$ (i.e., $a \leqslant_{b} b$ ) and $(b)_{b} \subseteq(a)_{b}$ (i.e., $b \leqslant_{b} a$ ), but $a \neq b$. Thus, $\leqslant_{b}$ is not a partial order on $S$.

Lemma 2.9. Let $B$ be a bi-base of a semigroup $S$. If $a, b \in B$ such that $a \neq b$, then neither $a \leqslant_{b} b$, nor $b \leqslant_{b} a$.

Proof. Assume that $a, b \in B$ such that $a \neq b$. Suppose that $a \leqslant_{b} b$; then

$$
a \in(a)_{b} \subseteq(b)_{b}
$$

By assumption we have $a \neq b$, so $a \in b b \cup b S b$. By Lamma 2.5, $a=b$. This is a contradiction. The case $b \leqslant_{b} a$ can be proved similarly.

Lemma 2.10. Let $B$ be a bi-base of a semigroup $S$. Let $a, b, c \in B$ and $s \in S$ :
(1) If $a \in b c \cup b c b c \cup b c S b c$, then $a=b$ or $a=c$.
(2) If $a \in b s c \cup b s c b s c \cup b s c S b s c$, then $a=b$ or $a=c$.

Proof. (1). Assume that $a \in b c \cup b c b c \cup b c S b c$, and suppose that $a \neq b$ and $a \neq c$. Let

$$
A=B \backslash\{a\}
$$

Then $A \subset B$. Since $a \neq b$ and $a \neq c$, we have $b, c \in A$. We will show that $(B)_{b} \subseteq(A)_{b}$, if suffices to show that $B \subseteq(A)_{b}$. Let $x \in B$. If $x \neq a$, then $x \in A$, and so $x \in(A)_{b}$. If $x=a$, then by assumption we have

$$
x=a \in b c \cup b c b c \cup b c S b c \subseteq A A \cup A A A A \cup A A S A A \subseteq A S A \subseteq(A)_{b}
$$

Thus, $B \subseteq(A)_{b}$. This implies $(B)_{b} \subseteq(A)_{b}$. Since $B$ is a bi-base of $S$,

$$
S=(B)_{b} \subseteq(A)_{b} \subseteq S
$$

Therefore $S=(A)_{b}$. This is a contradiction.
(2). Assume that $a \in b s c \cup b s c b s c \cup b s c S b s c$, and suppose that $a \neq b$ and $a \neq c$. Let

$$
A=B \backslash\{a\} .
$$

Then $A \subset B$. Since $a \neq b$ and $a \neq c$, we have $b, c \in A$. We will show that $(B)_{b} \subseteq(A)_{b}$, if suffices to show that $B \subseteq(A)_{b}$. Let $x \in B$. If $x \neq a$, then $x \in A$, and so $x \in(A)_{b}$. If $x=a$, then by assumption we have

$$
\begin{aligned}
x=a \in b s c \cup b s c b s c \cup b s c S b s c & \subseteq A S A \cup A S A A S A \cup A S A S A S A \\
& \subseteq A S A \subseteq(A)_{b} .
\end{aligned}
$$

Thus, $B \subseteq(A)_{b}$. This implies $(B)_{b} \subseteq(A)_{b}$. Since $B$ is a bi-base of $S$,

$$
S=(B)_{b} \subseteq(A)_{b} \subseteq S
$$

Therefore, $S=(A)_{b}$. This is a contradiction.

Lemma 2.11. Let $B$ be a bi-base of a semigroup $S$.
(1) For any $a, b, c \in B$, if $a \neq b$ and $a \neq c$, then $a \not \Varangle_{b} b c$.
(2) For any $a, b, c \in B$ and $s \in S$, if $a \neq b$ and $a \neq c$, then $a \not{ }_{\nless} b s c$.

Proof. (1). For any $a, b, c \in B$, let $a \neq b$ and $a \neq c$. Suppose that $a \leqslant_{b} b c$, we have

$$
a \in(a)_{b} \subseteq(b c)_{b}=b c \cup b c b c \cup b c S b c
$$

By Lamma 2.10 (1), it follows that $a=b$ or $a=c$. This contradicts to assumption.
(2). For any $a, b, c \in B$ and $s \in S$, let $a \neq b$ and $a \neq c$. Suppose that $a \leqslant_{b} b s c$, we have $a \in(a)_{b} \subseteq(b s c)_{b}=b s c \cup b s c b s c \cup b s c S b s c$. By Lamma 2.10 (2), it follows that $a=b$ or $a=c$. This contradicts to assumption.

We now prove the main result of this paper.
Theorem 2.12. A non-empty subset $B$ of a semigroup $S$ is a bi-base of $S$ if and only if $B$ satisfies the following conditions:
(1) For any $x \in S$,
(1.a) there exists $b \in B$ such that $x \leqslant_{b} b$; or
(1.b) there exist $b_{1}, b_{2} \in B$ such that $x \leqslant_{b} b_{1} b_{2}$; or
(1.c) there exist $b_{3}, b_{4} \in B, s \in S$ such that $x \leqslant_{b} b_{3} s b_{4}$.
(2) For any $a, b, c \in B$, if $a \neq b$ and $a \neq c$, then $a \nless b b c$.
(3) For any $a, b, c \in B$ and $s \in S$, if $a \neq b$ and $a \neq c$, then $a \not{ }_{\star} b s c$.

Proof. Assume first that $B$ is a bi-base of $S$; then $S=(B)_{b}$. To show that (1) holds, let $x \in S$. Then $x \in B \cup B B \cup B S B$.

We consider three cases:
Case 1: $x \in B$. Then $x=b$ for some $b \in B$. This implies $(x)_{b} \subseteq(b)_{b}$. Hence $x \leqslant{ }_{b} b$.

Case 2: $x \in B B$. Then $x=b_{1} b_{2}$ for some $b_{1}, b_{2} \in B$. This implies $(x)_{b} \subseteq$ $\left(b_{1} b_{2}\right)_{b}$. Hence $x \leqslant_{b} b_{1} b_{2}$.

Case 3: $x \in B S B$. Then $x=b_{3} s b_{4}$ for some $b_{3}, b_{4} \in B, s \in S$. This implies $(x)_{b} \subseteq\left(b_{3} s b_{4}\right)_{b}$. Hence $x \leqslant_{b} b_{3} s b_{4}$.

The validity of (2) and (3) follow, respectively, from Lemma 2.11 (1), and Lemma 2.11 (2).

Conversely, assume that the conditions (1), (2) and (3) hold. We will show that $B$ is a bi-base of $S$. Clearly, $(B)_{b} \subseteq S$. By (1), $S \subseteq(B)_{b}$, and $S=(B)_{b}$. It remains to show that $B$ is a minimal subset of $S$ with the property $S=(B)_{b}$.

Suppose that $S=(A)_{b}$ for some $A \subset B$. Since $A \subset B$, there exists $b \in B \backslash A$. Since $b \in B \subseteq S=(A)_{b}$ and $b \notin A$, it follows that $b \in A A \cup A S A$.

There are two cases to consider:

CASE 1: $b \in A A$. Then $b=a_{1} a_{2}$ for some $a_{1}, a_{2} \in A$. We have $a_{1}, a_{2} \in B$. Since $b \notin A$, so $b \neq a_{1}$ and $b \neq a_{2}$. Since $b=a_{1} a_{2}$, so $(b)_{b} \subseteq\left(a_{1} a_{2}\right)_{b}$. Hence $b \leqslant b a_{1} a_{2}$. This contradicts to (2).

Case 2: $b \in A S A$. Then $b=a_{3} s a_{4}$ for some $a_{3}, a_{4} \in A$ and $s \in S$. Since $b \notin A$, we have $b \neq a_{3}$ and $b \neq a_{4}$. Since $A \subset B, a_{3}, a_{4} \in B$. Since $b=a_{3} s a_{4}$, so $(b)_{b} \subseteq\left(a_{3} s a_{4}\right)_{b}$. Hence, $b \leqslant_{b} a_{3} s a_{4}$. This contradicts to (3).

Therefore, $B$ is a bi-base of $S$ as required, and the proof is completed.
In Example 2.2, we have that $\{u\}$ is a bi-base of $S$ where as it is not a subsemigroup of $S$. So, we find a condition in order that a bi-base is a subsemigroup.

Theorem 2.13. Let $B$ be a bi-base of a semigroup $S$. Then $B$ is a subsemigroup of $S$ if and only if $B$ satisfies the following conditions: For any $b, c \in B, b c=b$ or $b c=c$.

Proof. By Lemma 2.6, and $B$ is a subsemigroup of $S$ implies for any $b, c \in B$, $b c=b$ or $b c=c$. The opposit direction is clear.

Question. It was proved in [3] (Theorem 3) that for any two two-sided bases of a semigroup have the same cardinality. This is hold true for an ordered semigroup (see [1], Theorem 2.10). Here, we ask for bi-bases of a semigroup. Indeed, is it true that for any two bi-bases of a semigroup have the same cardinality?

## References

[1] T. Changphas and P. Summaprab, On two-sided bases of an ordered semigroup, Quasigroups and Related Systems 22 (2014), $59-66$.
[2] I. Fabrici, One-sided bases of semigroups, Matematický casopis, 22 (1972), no. 4, 286--290.
[3] I. Fabrici, Two-sided bases of semigroups, Matematický c̆asopis, 3 (2009), 181 --188.
[4] I. Fabrici and T. Kepka, On bases and maximal ideals in semigroups, Math. Slovaca, 31 (1981), 115 - 120.
[5] R.A. Good and D.R. Hughes, Associated groups for a semigroup, Bull. Amer. Math. Soc., 58 (1952), $624-625$.
[6] O. Steinfeld, Quasi-ideals in rings and semigroups, With a foreword by L. Rédei. Disquisitiones Mathematicae Hungaricae [Hungarian Mathematics Investigations], 10. Akadémiai Kiadó, Budapest, 1978.
[7] T. Tamura, One-sided bases and translations of a semigroup, Math. Japan. 3 (1955), $137-141$.

Received April 19, 2017
Department of Mathematics, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
Centre of Excellence in Mathematics, CHE, Si Ayuttaya Rd., Bangkok 10400, Thailand
E-mail: thacha@kku.ac.th

# Deniable-encryption protocols based on commutative ciphers 

Nicolai A. Moldovyan, Alexei V. Shcherbacov and Mikhail A. Eremeev


#### Abstract

There are considered three new deniable encryption protocols representing practical interest. The sender-deniable and sender\&receiver-deniable ones have been designed on the base of combining commutative encryption function (Vernam cipher) with probabilistic public key encryption (RSA algorithm), subexponential resistance to coercive attack being obtained. To get exponential deniability it is proposed to use the ElGamal-like probabilistic algorithm based on computational difficulty of discrete logarithm on elliptic curves instead of the RSA one. The third DE protocol is based on the Pohlig-Hellman exponentiation cipher and represents a planahead shared-key bi-deniable scheme satisfying criterion of computational indistinguishability from probabilistic encryption protocol. Each of the proposed deniable encryption schemes is a three-pass protocol.


## 1. Introduction

### 1.1. Deniable encryption

Encryption is usually used to provide confidentiality of the messages sent via insecure public channels, when a potential adversary can intercepts the send messages. In the case of intercepting the sent ciphertext he is unable to read the message until disclosing the decryption key. The widely used private-key (AES, IDEA, RC5, Serpent et. al.) and public-key (RSA, ElGamal et. al.) encryption algorithms [22] provide computational infeasibility of disclosing the key while performing cryptanalysis of the ciphertext. In some particular applications of the cryptographic protocols it is required to provide security against potential coercive attacks. The main feature of the model of the coercive adversary (coercer) consists in his having power to force sender or/and receiver to open both the source message and the decryption key [2]. After he gets the private key he can check that with the opened key the intercepted ciphertext is decrypted into the opened message.

The notion of deniable encryption (DE) relates to cryptoschemes that are resistant to coercive attacks. Deniability is provided with possibility to decrypt the

[^4]ciphertext intercepted by the coercer in different ways. The sender or/and the receiver open a fake message instead of the secret one and the coercive adversary is not able to disclose their lie. Practical application of the DE algorithms and protocols is connected with providing data secrecy, secure communications via public channels. They are also applicable for preventing vote buying in the internet-voting systems $[1,12]$ and for providing secure multiparty computations [9]. There are distinguished sender-deniable [4, 8, 19], receiver-deniable [13, 25], and bi-deniable $[20,21]$, schemes in which coercer attacks the sender of secret message, the receiver, and the both parties of the communication protocol, respectively.

One should also mention the issue about time at which the attacked parties have to decide on the fake message. In the plan-ahead DE protocols the fake message is selected at time of encryption. There are known practical public-key DE schemes $[16,17]$ and shared-key DE ones [18] in which the fake message is fixed and selected before or during the encryption process. From theoretic point of view the flexible DE protocols represent significant interest, in which the fake massage can be selected arbitrary at time of the coercive attack.

Significant part of the papers devoted to the design and analysis of flexible DE protocols consider the case of the sender-deniable public-key encryption protocols $[1,4,8]$. A possible general scheme of such protocols is as follows. The secret message $M$ is encrypted with public-encryption algorithm $E$ and public key $P$ using a random value $r: C=E_{P}(M, r)$, where $C$ is the produced cryptogram (ciphertext). While being coerced the sender (receiver) opens to adversary the fake message $M^{\prime}$ and another random value $r^{\prime}$ (fake opening) such that $E_{P}\left(M^{\prime}, r^{\prime}\right)=C$, where $r^{\prime} \neq r$. The value $r$ contains some trapdoor information unavailable to coercer, which is used by receiver to decide on the pair ( $M^{\prime}, r^{\prime}$ ) containing real message. Papers $[3,11,21]$ considered some problems connected with construction of the flexible public key DE protocols having super-polynomial security. Recent paper [24] gave the first construction of sender-deniable encryption schemes with super-polynomial security, where a coercive adversary has negligible advantage in distinguishing real and fake messages.

Present paper proposes a novel design of the DE protocols based on combining the probabilistic public encryption with the commutative encryption function implemented with Vernam algorithm. The paper introduces a computationally efficient sender-deniable encryption protocol as well as sender\&receiver deniable one in which using respective fake key the ciphertext can be decrypted in arbitrary fake message selected after performing the protocol, namely, at time of coercive attack. The both protocols have super-polynomial security that is defined by subexponential security of the RSA public encryption algorithm put into the base of the protocols. The proposed protocols are based on combining the probabilistic public encryption with commutative encryption implemented with the Vernam cipher. The proposed design can be implemented with using the ElGamal-like public encryption on elliptic curves, providing exponential resistance to coercive attack. As compared with the known flexible public key DE protocols the proposed ones
have the following merits: i) simplicity of the design, ii) sufficiently high performance, iii) comparatively low overhead in terms of the ciphertext size, and iv) using only one XOR operation to generate a fake opening at time of attack.

### 1.2. Commutative encryption

Encryption function $E$ is called commutative if it satisfies the following condition

$$
E_{K}\left[E_{Q}(M)\right]=E_{Q}\left[E_{K}(M)\right]
$$

where $K$ and $Q$ are encryption keys and $M$ is some plaintext, for arbitrary keys $K$ and $Q \neq K$. The property of commutativity of some encryption function is exploited in Shamir's no key protocol (also called Shamir's three-pass protocol [14]) described as follows. Suppose Alice wishes to send the secret message $M$ to Bob, using a public channel and no shared key. For this purpose they can use the following protocol that provides privacy, but not authentication:

1. Alice chooses a random key $K$ and encrypts the message $M$ using a commutative encryption function $E: C_{1}=E_{K}(M)$, where $C_{1}$ is the produced ciphertext. Then she sends the ciphertext $C_{1}$ to Bob.
2. Bob chooses a random key $Q$ and encrypts the message the ciphertext $C_{1}$ using the function $E$ as follows: $C_{2}=E_{Q}\left(C_{1}\right)$, where $C_{2}$ is the produced ciphertext. Then he sends the ciphertext $C_{2}$ to Alice.
3. Alice decrypts the ciphertext $C_{2}$ obtaining the ciphertext $C_{3}: C_{3}=$ $E_{K}^{-1}\left(C_{2}\right)$. Then she sends the ciphertext $C_{3}$ to Bob.

Having received the ciphertext $C_{3}$ Bob computes the value $M^{\prime}=E_{Q}^{-1}\left(C_{3}\right)$. Due to commutativity of the encryption function the values $M^{\prime}$ and $M$ are equal, i.e., the protocol works correctly. Indeed, one has the following:

$$
\begin{aligned}
& M^{\prime}=E_{Q}^{-1}\left(C_{3}\right)=E_{Q}^{-1}\left[E_{K}^{-1}\left(C_{2}\right)\right]=E_{Q}^{-1}\left[E_{K}^{-1}\left[E_{Q}\left(C_{1}\right)\right]\right]= \\
& E_{Q}^{-1}\left[E_{K}^{-1}\left[E_{Q}\left(E_{K}(M)\right)\right]\right]=E_{Q}^{-1}\left[E_{K}^{-1}\left[E_{K}\left(E_{Q}(M)\right)\right]\right]=E_{Q}^{-1}\left[E_{Q}(M)\right]=M
\end{aligned}
$$

The described three-pass protocol provides security to passive attacks (potential adversary only intercepts the values sent via public channel), if the used commutative encryption function $E$ is secure to the know-input-text attack.

Indeed, if the function $E$ is not secure to such attack, then the passive adversary (after his intercepting the ciphertexts $C_{1}, C_{2}$, and $C_{3}$ ) is able to compute Bob's local key $Q$ from the equation $C_{2}=E_{Q}\left(C_{1}\right)$ and then the secret message $M=$ $E_{Q}^{-1}\left(C_{3}\right)$.

The Vernam cipher represents the simplest commutative cipher. It consists in simple adding the key to the message $M$ in accordance with the formula

$$
C=M \oplus K
$$

where $K$ is the single-use random chosen key such that $|K|=|M|$ (the bit-length of some value $x$ is denoted as $|x|$ ) and $\oplus$ is the bit-wise modulo 2 addition operation
(the XOR operation). Unfortunately it cannot be used in frame of the Shamir's three-pass protocol, since it is not secure to the known-plaintext attack.

The appropriate commutative encryption function is provided by the exponen-tiation-encryption method proposed by Pohlig and Hellman in [7].

The last method is described as follows. Suppose $p$ is a 2464 -bit prime such that number $(p-1)$ contains a large prime divisor $q$, for example, $p=2 q+1$.

To select an encryption/decryption key $(e, d)$ one needs to generate a random 256-bit number $e$ that is mutually prime with $(p-1)$ and then to compute $d=$ $e^{-1} \bmod p-1$. The encryption procedure is described with the formula

$$
C=M^{-e} \bmod p
$$

Decryption of the ciphertext $C$ is performed as computing the value

$$
M=C^{-d} \bmod p
$$

The Pohlig-Hellman algorithm is secure against the known plaintext (ciphertext) attack and can be used in Shamir's no-key protocol.

In the present paper it is also proposed bi-deniable shared-key protocol based on commutative encryption implemented with the Pohlig-Hellman exponentiation cipher. Justifying the bi-deniability of the proposed protocol is performed on the base of the criterion of computational indistinguishability [18] from the probabilistic three-pass protocol applied for encrypting a fake message.

## 2. Sender\&reciever-deniable three pass protocol

In frame of the protocol described below the RSA cryptoscheme [23] is used for performing the public encryption with receiver's (Bob's) public key ( $n, e$ ) that is generated simultaneously with his private key $d$ as follows. Bob selects two strong [6] primes $p$ and $q$ having large size (for example, 1232 bits). The value $n$ is computed as product of the primes: $n=p q$. Then it is selected a random number $e$ that is relatively prime to Euler phi function $\varphi(n)=(p-1)(q-1)$ and has comparatively small size (for example, 32 bits ) to provide faster encryption. The private key $d$ is computed as follows $d=e^{-1} \bmod \varphi(n)$. Probabilistic encryption of some message $M<\left(n\right.$ div $\left.2^{257}\right)$ is performed with the public key as computing the ciphertext $C=(M \| \rho)^{e} \bmod n$, where $\|$ is the concatenation operation; $\rho$ is a random chosen bit string having size exacly equal to 256 bits. Decryption of the ciphertext $C$ is performed using the private key as follows $M=\left(C^{d} \bmod n\right) \operatorname{div} 2^{256}$. The random value $\rho$ is an internal randomization parameter actual in frame of the operation of probabilistic public encryption. The protocols described below do not use any information contained in the value $\rho$ destination of which consist only in randomizing the ciphertext. The parameter $\rho$ takes on different values at each step of the probabilistic RSA encryption and they are not to be saved in computer or hardware memory.

The proposed sender-deniable public encryption protocol is described as follows.

1. To send the secret message $M\left(|M|<\mid n_{B}\right.$ div $2^{257} \mid$, where $\left(n_{B}, e_{B}\right)$ is Bob's public key) Alice generates a random bit string $K$ such that $|K|=|M|$ and computes the value $C=M \oplus K$ and the ciphertext

$$
C_{1}=(C \| \rho)^{e_{B}} \bmod n_{B}=((M \oplus K) \| \rho)^{e_{B}} \bmod n_{B} .
$$

Then she sends the value $C_{1}$ to Bob .
2. Using his private key $d_{B}$ Bob decrypts the ciphertext $C_{1}: C \| \rho=C_{1}^{d_{B}} \bmod$ $n_{B}$, generates a random bit string $Q$ such that $|Q|=|C|$ and computes the ciphertext

$$
C_{2}=C \oplus Q=M \oplus K \oplus Q
$$

Then he sends the value $C_{2}$ to Alice.
3. Alice computes the ciphertext

$$
C_{3}=\left(\left(C_{2} \oplus K\right) \| \rho\right)^{e_{B}} \bmod n_{B}=((M \oplus Q) \| \rho)^{e_{B}} \bmod n_{B}
$$

and sends the value $C_{3}$ to Bob.
Bob decrypts the ciphertext $C_{3}:(M \oplus Q) \| \rho=\left(C_{3}\right)^{d_{B}} \bmod n_{B}$ and discloses the secret message $M$ as follows: $M=(M \oplus Q) \oplus Q$.

If some coercive adversary intercepts the ciphertexts $C_{1}, C_{2}$, and $C_{3}$ and then forces Alice to open the secret message and her local key, then she chooses some fake message $M^{\prime}$ such that $\left|M^{\prime}\right|=|M|$, computes the fake local key $K^{\prime}=M \oplus K \oplus$ $M^{\prime}$, and opens the values $M^{\prime}$ and $K^{\prime}$ as the values had been used at step 1 of the protocol. From the ciphertext $C_{2}$ coercer can compute the value $Q^{\prime}=C_{2} \oplus M^{\prime} \oplus K^{\prime}$ for which the following inequality holds $M^{\prime} \oplus Q^{\prime} \neq M \oplus Q$. However the coercer has no computational possibility to disclose Alice's lie due to the probabilistic encryption performed at step 3 which gives different pseudo-random ciphertexts while encrypting the same input value arbitrary number of times.

Thus, the coercer is unable to demonstrate inequality $M^{\prime} \oplus Q^{\prime} \neq M \oplus Q$ performing public encryption of its left part, using Bob's public key, therefore the described protocol is sender-deniable one. However the protocol is not a receiverdeniable one, since while being coerced Bob should open both his local key $Q$ and his private key $d_{B}$. Using the value $d_{B}$ the coercer is able to disclose Bob's lie, if Bob will open fake key $Q^{\prime} \neq Q$.

The described protocol can be modified into sender- and receiver-deniable one with using Alice's public key $\left(n_{A}, e_{A}\right)$ at step 2 of the protocol. The modified protocol looks as follows:

1. To send the secret message $M\left(|M|<\left|n \operatorname{div} 2^{257}\right|\right.$, where $n=\min \left\{n_{A}, n_{B}\right\}$,) Alice generates a random bit string $K$ such that $|K|=|M|$ and computes the value $C=M \oplus K$ and the ciphertext

$$
C_{1}=(C \| \rho)^{e_{B}} \bmod n_{B}=((M \oplus K) \| \rho)^{e_{B}} \bmod n_{B} .
$$

Then she sends the ciphertext $C_{1}$ to Bob.
2. Using his private key $d_{B}$ Bob decrypts the ciphertext $C_{1}: C \| \rho=C_{1}^{d_{B}} \bmod$ $n_{B}$, generates a random bit string $Q$ such that $|Q|=|C|$ and computes the value $C_{2}^{\prime}=C \oplus Q=M \oplus K \oplus Q$ and the ciphertext

$$
C_{2}=\left(C_{2}^{\prime} \| \rho\right)^{e_{A}} \bmod n_{A}=((M \oplus K \oplus Q) \| \rho)^{e_{A}} \bmod n_{A}
$$

Then he sends the ciphertext $C_{2}$ to Alice.
3. Alice computes the values $C_{2}^{\prime} \| \rho=C_{2}^{d_{A}} \bmod n_{A}$ and

$$
C_{3}=\left(C^{\prime \prime} \| \rho\right)^{e_{B}} \bmod n_{B}=((M \oplus Q) \| \rho)^{e_{B}} \bmod n_{B}
$$

and sends the value $C_{3}$ to Bob.
Bob decrypts the ciphertext $C_{3}:(M \oplus Q) \| \rho=\left(C_{3}\right)^{d_{B}} \bmod n_{B}$ and discloses the secret message $M$ as follows: $M=(M \oplus Q) \oplus Q$.

Like the initial version, the modified version of the protocol resists the senderside coercive attack. Besides, it is also a receiver-deniable protocol. Indeed, if some coercive adversary intercepts the ciphertexts $C_{1}, C_{2}$, and $C_{3}$ and then forces Bob to open the secret message and his local key, then Bob chooses some fake message $M^{\prime}$ such that $\left|M^{\prime}\right|=|M|$, computes the fake local key $Q^{\prime}=M \oplus Q \oplus M^{\prime}$, and opens the values $M^{\prime}$ and $Q^{\prime}$ as the real values used during execution of the protocol. The coercer can compute the value $C=M \oplus K=M^{\prime} \oplus K^{\prime}$, where $K^{\prime}$ is fake Alice's local key, from the ciphertext $C_{1}$ and the value $C^{\prime \prime}=M^{\prime} \oplus Q^{\prime}$ from the ciphertext $C_{2}$. For two different messages $M^{\prime}$ and $M$ the following inequality holds $M^{\prime} \oplus K^{\prime} \oplus Q^{\prime} \neq M \oplus K \oplus Q$. However, due to using probabilistic public encryption, the coercer has no computational possibility to disclose Bob's lie performing many times the encryption of the left part of the inequality with Aice's public key. The coercer is also unable to compute the value $M \oplus K \oplus Q$ performing decryption of the ciphertext $C_{2}$, since he does not know the Alice's private key.

It should be noted that the last protocol is not fully bi-deniable, since it does not resist simultaneous coercive attack on both the sender and the receiver. Indeed, while being simultaneously coerced Alice and Bob should open both their local keys $K$ and $Q$ and their private keys $d_{A}$ and $d_{B}$. Using the values $d_{A}$ and $d_{B}$ the coercer is able to disclose Alice's and/or Bob's lie, if Alice and/or Bob will open fake keys $K^{\prime} \neq K$ and/or $Q^{\prime} \neq Q$.

The described three-pass protocols are sufficiently practical since only four and six modulo exponentiation operations are performed during the first and second described protocols, respectively. The both protocols provide security defined by computational difficulty of the factoring $n$ problem (about $2^{128}$ modulo multiplications in the case of 2464 -bit modulus $n$ ). The second protocol provides authentication due to using both the Alice's public key and Bob's public key. The first protocol provides authentication of one party of the protocol only, namely, authentication of the receiver of the message.

## 3. Bi-deniable three-pass protocol

For constructing a practical bi-deniable encryption protocol the following design criteria have been used:

1) the protocol should use a key ( 128 to 2048 bits) shared by sender and receiver of secrete message;
2) the base encryption procedure should be implemented as the modulo exponentiation operation in the finite field $G F\left(2^{s}\right)$, where $s=128$ to 2048;
3) the protocol should provide bi-deniability, i.e., it should resist simultaneous coercive attacks on the sender and on the receiver;
4) under coercive attack the parties of the protocol disclose a fake shared key and their local fake keys as secret values; when using the fake keys, decryption of the ciphertexts (sent during the deniable-encryption protocol) should recover a fake message;
5) ciphertexts produced at all steps of the protocol should be computationally indistinguishable from the ciphertexts produced by some probabilistic-encryption protocol in the case when the last protocol is used for encrypting some fake message using the disclosed keys.

Construction of the shared-key bi-deniable encryption protocols is connected with the design of respective probabilistic three-pass protocol, which is associated with the first one. The next subsection introduces appropriate probabilisticencryption protocol.

### 3.1. Associated probabilistic-encryption protocol

Suppose Alice and Bob share a secret key representing an irreducible binary polynomial $\mu(x)$ of the degree $s=128$ to 1024 . To encrypt some secret message $M$ Alice represents the message as sequence of the $s$-bit data blocks $M_{i}: M=$ $\left(M_{1}, M_{2}, M_{i}, M_{z}\right)$. To send securely the message $M$ to Bob she can use the following probabilistic-encryption protocol.

1. Alice generates her local key as pair of values $\left(e_{A}, d_{A}\right)$, where random value $e_{A}$ is mutually prime with the value $2^{s}-1$ and $d_{A}=e_{A}^{-1} \bmod 2^{s}-1$. Then for each value $i=1,2, \ldots, z$ she generates random binary polynomials $\rho_{A}(x)$ of the degree $s-1$ and $\eta_{A}(x)$ of the degree $s$ such that $\eta_{A}(x) \neq \mu(x)$ and, considering each data block as binary polynomial, encrypts the message $M$ in accordance with the formula

$$
\begin{align*}
& C_{A i}=\left\{\eta_{A}(x)\left[\eta_{A}^{-1}(x) M_{i}^{e_{A}} \bmod \mu(x)\right]+\mu(x)\left[\mu^{-1}(x) \rho_{A}(x) \bmod \eta_{A}(x)\right]\right\}  \tag{1}\\
& \bmod \mu(x) \eta_{A}(x) .
\end{align*}
$$

Then Alice sends the ciphertext

$$
C_{A}=\left(C_{A 1}, C_{A 2}, \ldots, C_{A i}, \ldots, C_{A z}\right)
$$

to Bob.
2. Bob generates his local key $\left(e_{B}, d_{B}\right)$, where random value $e_{B}$ is mutually prime with the value $2^{s}-1$ and $d_{B}=e_{B}^{-1} \bmod 2^{s}-1$. Then for each value $i=1,2, \ldots, z$ he computes the value $C_{B i}^{\prime}=C_{A i}^{e_{B}} \bmod \mu(x)=M_{i}^{e_{A} e_{B}} \bmod \mu(x)$, generates random binary polynomials $\rho_{B}(x)$ of the degree $s-1$ and $\eta_{B}(x)$ of the degree $s$ such that $\eta_{B}(x) \neq \mu(x)$ and encrypts each data block $C_{A i} \bmod \mu(x)$ in accordance with the formula

$$
\begin{align*}
& C_{B i}=\left\{\eta_{B}(x)\left[\eta_{B}^{-1}(x) C_{B i}^{\prime} \bmod \mu(x)\right]+\mu(x)\left[\mu^{-1}(x) \rho_{B}(x) \bmod \eta_{B}(x)\right]\right\}  \tag{2}\\
& \bmod \mu(x) \eta_{B}(x)
\end{align*}
$$

where $i=1,2, \ldots, z$. Then Bob sends the ciphertext

$$
C_{B}=\left(C_{B 1}, C_{B 2}, \ldots, C_{B i}, \ldots, C_{B z}\right)
$$

to Alice.
3. For each value $i=1,2, \ldots, z$ Alice computes the value $C_{B i} \bmod \mu(x)=$ $M_{i}^{e_{A} e_{B}} \bmod \mu(x)$, generates random binary polynomials $\rho_{A}^{\prime}(x)$ of the degree $s-1$ and $\eta_{A}^{\prime}(x)$ of the degree $s$ such that $\eta_{A}^{\prime}(x) \neq \mu(x)$ and encrypts each data block $C_{B i} \bmod \mu(x)$ in accordance with the formula

$$
\begin{align*}
& C_{A i}^{\prime}=\left\{\eta_{A}^{\prime}(x)\left[\eta_{A}^{\prime-1}(x) C_{B i}^{d_{A}} \bmod \mu(x)\right]+\mu(x)\left[\mu(x)^{-1} \rho_{A}^{\prime}(x) \bmod \eta_{A}^{\prime}(x)\right]\right\}  \tag{3}\\
& \bmod \mu(x) \eta_{A}^{\prime}(x) .
\end{align*}
$$

Then Alice sends the ciphertext

$$
C_{A}^{\prime}=\left(C_{A 1}^{\prime}, C_{A 2}^{\prime}, \ldots, C_{A i}^{\prime}, \ldots, C_{A z}^{\prime}\right)
$$

to Bob. Bob discloses the secret message $M=\left(M_{1}, M_{2}, \ldots, M_{i}, \ldots, M_{z}\right)$ computing the values $C_{i}^{\prime}=C_{A i}^{\prime} \bmod \mu(x)=M_{i}^{e_{B}} \bmod \mu(x)$ and $M_{i}=C_{i}^{\prime d_{B}} \bmod \mu(x)$ for $i=1,2, \ldots, z$.

In the described protocol for probabilistic encryption the ciphertexts $C_{A}, C_{B}$, and $C_{A}^{\prime}$ sent via public channel have size that is exactly two times larger than the size of the input data blocks $M_{i}$. Security of the protocol is provided due to good confusion and diffusion properties of the exponentiation operation and due to using the modulus $\mu(x)$ as secret key. It is worth to mention that in the case of sufficiently large size of the key $\mu(x)(|\mu(x)| \geqslant 1024$ bits) the protocol resists attacks based on the known shared key, i.e., if the adversary gets the key $\mu(x)$ after the protocol have been performed, then he also will not be able to compute the secret message $M$. However after the key $\mu(x)$ becomes known for potential adversary the protocol will provide secrecy (in possible further use of the protocol) but not authentication.

### 3.2. Bi-deniable encryption scheme

Suppose Alice and Bob share a secret key representing the pair of mutually irreducible binary polynomials $\mu(x)$ and $\eta(x)$ of the degree $s=128$ to 1024. To
encrypt some secret message $T$ Alice represents the message as sequence of the $s$-bit data blocks $T_{i}: T=\left(T_{1}, T_{2}, \ldots, T_{i}, \ldots, T_{z}\right)$. To provide bi-deniability of encrypting the secret message $T$ they can use the following three-pass protocol.

1. Alice generates some fake message $M=\left(M_{1}, M_{2}, \ldots, M_{i}, \ldots, M_{z}\right)$ represented as sequence of $s$-bit data blocks and two local keys $\left(e_{A}, d_{A}\right)$ and $\left(\varepsilon_{A}, \delta_{A}\right)$ such that $d_{A}=e_{A}^{-1} \bmod 2^{s}-1$ and $\delta_{A}=\varepsilon_{A}^{-1} \bmod 2^{s}-1$.

Then for each value $i=1,2, \ldots, z$ she computes the ciphertext block $C_{A i}$ as follows:
1.1. Compute the intermediate ciphertext blocks $C_{A i}^{(M)}$ and $C_{A i}^{(T)}$ :

$$
C_{A i}^{(M)}=M_{i}^{e_{A}} \bmod \mu(x) \text { and } C_{A i}^{(T)}=T_{i}^{\varepsilon_{A}} \bmod \eta(x)
$$

1.2. Compute the ( $2 s$ )-bit ciphertext block $C_{A i}$ as solution of the system of congruences

$$
\left\{\begin{array}{l}
C_{A i} \equiv C_{A i}^{(M)} \bmod \mu(x)  \tag{4}\\
C_{A i} \equiv C_{A i}^{(T)} \bmod \eta(x)
\end{array}\right.
$$

Then Alice sends the ciphertext $C_{A}=\left(C_{A 1}, C_{A 2}, \ldots, C_{A i}, \ldots, C_{A z}\right)$ to Bob.
2. Bob generates two local keys $\left(e_{B}, d_{B}\right)$ and $\left(\varepsilon_{B}, \delta_{B}\right)$ such that $d_{B}=e_{B}^{-1} \bmod$ $2^{s}-1$ and $\delta_{B}=\varepsilon_{B}^{-1} \bmod 2^{s}-1$. Then for each value $i=1,2, \ldots, z$ he computes the ciphertext block $C_{B i}$ as follows:
2.1. Compute the intermediate ciphertext blocks $C_{A i}^{(M)}$ and $C_{A i}^{(T)}$ :

$$
C_{A i}^{(M)}=C_{A i} \bmod \mu(x) \text { and } C_{A i}^{(T)}=C_{A i} \bmod \eta(x)
$$

2.2. Compute the intermediate ciphertext blocks $C_{B i}^{(M)}$ and $C_{B i}^{(T)}$ :

$$
\begin{aligned}
& C_{B i}^{(M)}=\left(C_{A i}^{(M)}\right)^{e_{B}} \bmod \mu(x)=M_{i}^{e_{A} e_{B}} \bmod \mu(x) \text { and } \\
& C_{B i}^{(T)}=\left(C_{A i}^{(T)}\right)^{\varepsilon_{B}} \bmod \eta(x)=T_{i}^{\varepsilon_{A} \varepsilon_{B}} \bmod \eta(x)
\end{aligned}
$$

2.3. Compute the $(2 s)$-bit ciphertext block $C_{B i}$ as solution of the system of congruences

$$
\left\{\begin{array}{l}
C_{B i} \equiv C_{B i}^{(M)} \bmod \mu(x)  \tag{5}\\
C_{B i} \equiv C_{B i}^{(T)} \bmod \eta(x)
\end{array}\right.
$$

Then Bob sends the ciphertext $C_{B}=\left(C_{B 1}, C_{B 2}, \ldots, C_{B i}, \ldots, C_{B z}\right)$ to Alice.
3. Then for each value $i=1,2, \ldots, z$ Alice computes the ciphertext block $C_{A i}^{\prime}$ as follows:
3.1. Compute the intermediate ciphertext blocks $C_{B i}^{(M)}$ and $C_{B i}^{(T)}: C_{B i}^{(M)}=$ $C_{B i} \bmod \mu(x)$ and $C_{B i}^{(T)}=C_{B i} \bmod \eta(x)$.
3.2. Compute the intermediate ciphertext blocks $C_{A i}^{\prime(M)}$ and $C_{A i}^{\prime(T)}: C_{A i}^{(M)}=$ $\left(C_{B i}^{(M)}\right)^{d_{A}} \bmod \mu(x)=M_{i}^{e_{B}} \bmod \mu(x)$ and $C_{A i}^{\prime(T)}=\left(C_{B i}^{(T)}\right)^{\delta_{A}} \bmod \eta(x)=T_{i}^{\varepsilon_{B}} \bmod$ $\eta(x)$.
3.3. Compute the $(2 s)$-bit ciphertext block $C_{A i}^{\prime}$ as solution of the system of congruences

$$
\left\{\begin{array}{l}
C_{A i}^{\prime} \equiv C_{A i}^{\prime(M)} \bmod \mu(x)  \tag{6}\\
C_{A i}^{\prime} \equiv C_{A i}^{\prime(T)} \bmod \eta(x) .
\end{array}\right.
$$

Then Alice sends the ciphertext $C_{A}^{\prime}=\left(C_{A 1}^{\prime}, C_{A 2}^{\prime}, \ldots, C_{A i}^{\prime}, \ldots, C_{A z}^{\prime}\right)$ to Bob.
Bob discloses the secret message $T=\left(T_{1}, T_{2}, \ldots, T_{i}, \ldots, T_{z}\right)$ computing the values $C_{A i}^{\prime(T)}=C_{A i}^{\prime} \bmod \eta(x)=T_{i}^{\varepsilon_{B}} \bmod \eta(x)$ and $T_{i}=\left(C_{A i}^{\prime(T)}\right)^{\delta_{B}} \bmod \eta(x)$ for $i=1,2, \ldots, z$.

Respectively, Bob discloses the fake message $M$ computing the values $C_{A i}^{(M)}=$ $C_{A i}^{\prime} \bmod \mu(x)=M_{i}^{e_{B}} \bmod \mu(x)$ and $M_{i}=\left(C_{A i}^{\prime(M)}\right)^{d_{B}} \bmod \mu(x)$.

When being coerced simultaneously, Alice and Bob open the fake message $M=\left(M_{1}, M_{2}, \ldots, M_{i}, \ldots, M_{z}\right)$, the shared key $\mu(x)$, and their local keys $\left(e_{A}, d_{A}\right)$ and $\left(e_{B}, d_{B}\right)$.

They also declare about using the three-pass probabilistic-encryption protocol described in Subsection 3.1. Distinguishing the bi-deniable encryption protocol from the probabilistic encryption protocol is a computationally difficult problem, therefore the protocol described in Subsection 3.2 provides bi-deniability.

## 4. Disscusion

Different variants of the protocols described in Section 2 can be constructed using different variants of the commutative cipher $E_{K}$ with the single-use key $K$, and/or different public encryption algorithms.

For example, the encryption procedure $E_{K}$ can be defined with formula

$$
C=M * K
$$

where $*$ is one of the following operations: modulo $2^{|M|}$ addition (subtraction), modulo $n$ addition (subtraction), modulo $n$ multiplication. Instead of the RSA public encryption algorithm one can use the ElGamal algorithm [5]. The last modification is interesting from practical point of view since it gives possibility to provide more secure encryption in the case of implementing the ElGamal publicencryption algorithm with using elliptic curves [10]. Indeed, in the last case one can provide exponential security of the deniable encryption and higher performance. Besides the ElGamal algorithm is probabilistic in its nature. Using the Rabin public-encryption algorithm [14] is also possible, but not so attractive.

One can note that the second flexible public key DE protocol from Section 2 resists the coercive attack on the sender or on the receiver, but it does not resist coercive attack performed simultaneously on the both parties. Indeed, resistance to last attack means that the sender and the receiver select the same fake message, however to have such possibility they need some pre-agreed information that
indicates what fake message should be selected. Appropriate modification of the source protocol is possible, however it becomes a plan-ahead DE protocol that has no evident advantages as compared with protocols of such type introduced in $[16,17]$.

As compared with the flexible sender-side DE protocols [1, 8] in which the message is encrypted consecutively bit by bit (each bit is sent in form of the $|n|$ bit pseudorandom number, $|n|>1024$ ) in the proposed protocols the message is transformed as a single data block that provides significantly higher performance. Besides, the proposed protocols provide simple and very fast procedure (performing one XOR operation) for computing the fake random input (sender's local key) connected with the fake message.

The bi-deniable encryption scheme presented in Section 3 uses the PohligHellman modulo-exponentiation cipher represented in a specific form in which the modulus that is the binary polynomial $\mu(x)$ serves as shared key. Therefore such implementation provides sufficiently high security even in the case when binary polynomial $\mu(x)$ has sufficiently small degree ( $128 \leqslant s \leqslant 768$ ). If the modulus $\mu(x)$ has high degree $(s \geqslant 1024)$, the protocol becomes resistant to the knownkey attacks. However, if the shared key is compromised the protocol will not provide authentication, like in the case of the probabilistic-encryption algorithm from Subsection 3.1.

Resistance to the simultaneous coercive attacks on Alice and Bob is provided due to fact that Bob using the fake key is able to disclose correctly the fake message $M$ generated by Alice at the first step of the protocol. Besides, the ciphertexts $C_{A}, C_{B}$, and $C_{A}^{\prime}$ computed at steps 1, 2, and 3, correspondingly, look like the ciphertexts produced during performing the probabilistic-encryption protocol from subsection 3.1, when $M$ serves as input message. In other words the proposed bi-deniable encryption protocol is computationally indistinguishable from the proposed probabilistic encryption protocol for the coercer intercepting the ciphertexts $C_{A}, C_{B}$, and $C_{A}^{\prime}$ sent via communication channel. Indeed, computation of each block $C_{A i}$ of the ciphertex $C_{A}$ in accordance with formula (1) gives solution of the following system relatively unknown $C_{A i}$

$$
\left\{\begin{array}{l}
C_{A i} \equiv M_{i}^{e_{A}} \bmod \mu(x) \\
C_{A i} \equiv \rho_{A}(x) \bmod \eta_{A}(x) .
\end{array}\right.
$$

The first congruence coincide with the first congruence in system (4) and for given value $C_{A i}$ and arbitrary $\eta_{A}(x)$ of the degree $s$ such that $\eta_{A}(x) \neq \mu(x)$ we have one value $\rho_{A}(x)$ that satisfies the second congruence of the last system (namely, $\left.\rho_{A}(x)=C_{A i} \bmod \eta_{A}(x)\right)$.

Computation of each block $C_{B i}$ of the ciphertex $C_{B}$ in accordance with formula (2) gives solution of the following system relatively unknown $C_{B i}$

$$
\left\{\begin{array}{l}
C_{B i} \equiv M_{i}^{e_{A} e_{B}} \bmod \mu(x) \\
C_{B i} \equiv \rho_{B}(x) \bmod \eta_{B}(x)
\end{array}\right.
$$

The first congruence coincide with the first congruence in system (5) and for given value $C_{B i}$ and arbitrary $\eta_{B}(x)$ of the degree $s$ such that $\eta_{B}(x) \neq \mu(x)$ we have one value $\rho_{B}(x)$ that satisfies the second congruence of the last system (namely, $\left.\rho_{B}(x)=C_{B i} \bmod \eta_{B}(x)\right)$.

Computation of each block $C_{A i}^{\prime}$ of the ciphertex $C_{A}$ in accordance with formula (3) gives solution of the following system relatively unknown $C_{A i}^{\prime}$

$$
\left\{\begin{array}{l}
C_{A i}^{\prime} \equiv\left(M_{i}\right)^{e_{B}} \bmod \mu(x) \\
C_{A i}^{\prime} \equiv \rho_{A}^{\prime}(x) \bmod \eta_{A}^{\prime}(x)
\end{array}\right.
$$

The first congruence coincide with the first congruence in system (6) and for given value $C_{A i}^{\prime}$ and arbitrary $\eta_{A}^{\prime}(x)$ of the degree $s$ such that $\eta_{A}^{\prime}(x) \neq \mu(x)$ we have one value $\rho_{A}^{\prime}(x)$ that satisfies the second congruence of the last system (namely, $\left.\rho_{A}^{\prime}(x)=C_{A i}^{\prime} \bmod \eta_{A}^{\prime}(x)\right)$.

Thus, the ciphertexts $C_{A}, C_{B}$, and $C_{A}^{\prime}$ produced during performing the bideniable encryption protocol could be produced while performing the probabilisticencryption protocol. To prove the ciphertexts were produced with the three-pass protocol for simultaneous encryption of two messages $M$ and $T$, the coercer has to disclose the secret message from the ciphertexts, however this seems to be a computationally infeasible problem.

A possible modification of the protocols from Section 3 can be get with using the binary polynomials $\eta_{A}(x), \eta_{B}(x), \eta_{A}^{\prime}(x)$, and $\eta(x)$ having degree $s^{\prime}<s$ (the message $T$ is to be divided into $s^{\prime}$-bit data blocks $T_{i}$ ). In the modified protocols the ciphertext blocks have size $s+s^{\prime}<2 s$ and for smaller values $s^{\prime}$ applying the bi-deniable encryption protocol looks more believably as applying the probabilisticencryption protocol. In the case of probabilistic-encryption protocol one can use sufficiently small values $s^{\prime}=4$ to 64 . In the case of the bi-deniable encryption protocol one has some restriction: $64<s^{\prime}<s$, where $s=128$ to 1024. This restriction is connected with using the value $\eta(x)$ as shared secret key.

Indeed, to provide deniability the value $\eta(x)$ and the local key $\varepsilon_{A}\left(\varepsilon_{A}<2^{s^{\prime}}\right)$ should be sufficiently large, for example, $|\eta(x)|+\left|\varepsilon_{A}\right| \geqslant 128$ bits. For small values $s^{\prime}$ (for example, for $s^{\prime}=4$ to 16) the coercer using the values $\mu(x)$ and $e_{A}$ (that are to be opened in the case of coercive attack) can find easily the secret values $\eta(x)$ and $\varepsilon_{A}$ with help of the exhaustive-search method.

## 5. Conclusion

There have been proposed sender-deniable, sender\&receiver-deniable, probabilistic, and bi-deniable encryption schemes representing three-pass protocols based on using commutative ciphers. The probabilistic-encryption protocol has been designed as protocol associated with the bi-deniable encryption protocol, however it has independent practical interest. To get higher performance of the bi-deniable encryption protocol one can design its modification on the base of commutative
encryption operation implemented as multiplying points of elliptic curves defined over finite fields $G F(p)$ and $G F\left(2^{s}\right)$ [15].

The last remark can be attributed also to the design of two flexible public key DE protocols from section 2 in the case of using the ElGamal public encryption algorithm (that is a probabilistic one) in frame of the protocols. For such protocols, besides higher performance, such variants of the flexible sender-deniable and sender\&receiver-deniable public encryption DE protocols will provide exponential resistance to coercive attacks in the case of implementing the ElGamal-like algorithm on the base of elliptic curves.

Another interesting research problem is connected with using the commutative encryption functions to design no-key DE protocols.

## References

[1] M.T. Barakat, A new sender-side public-key deniable encryption scheme with fast decryption. KSII Transactions on Internet and Information Systems 8 (2014), 3231-3249.
[2] R. Canetti, C. Dwork, M. Naor, R. Ostrovsky, Deniable encryption, Lecture Notes Comp. Sci. 1294 (1997), 394-104.
[3] D. Dachman-Soled, On the impossibility of sender-deniable public key encryption, IACR Cryptology ePrint Archive (2012), 727.
[4] D.Dachman-Soled, On minimal assumptions for sender-deniable public key encryption, Lecture Notes Comp. Sci. 8383 (2014), 574-591.
[5] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Information Theory IT-31 (1985), 469-472.
[6] J. Gordon Strong primes are easy to find, Lecture Notes Comp. Sci. 209 (1985), 216-223.
[7] M.E. Hellman, S.C. Pohlig, Exponentiation cryptographic apparatus and method, U.S. Patent \# 4,424,414. 3 Jan. 1984.
[8] M.H. Ibrahim, A method for obtaining deniable Public-Key Encryption, International J. Network Security 8 (2009), 1-9.
[9] Yu. Ishai, E. Kushilevits, R. Ostrovsky, Efficient non-interactive secure computation, Lecture Notes Comp. Sci. 6632 (2011), 406-425.
[10] N. Koblitz, Elliptic curve cryptosystems, Math. Computat. Advances 48 (1987), 203-209.
[11] D. Markus, D.M. Freeman, Deniable encryption with negligible detection probability; An interactive construction Lecture Notes Comp. Sci. 6632 (2011), 610-626.
[12] B. Meng, A secure Internet voting protocol based on non-interactive deniable authentication protocol and proof protocol that two ciphertexts are encryption of the same plaintext, J. Networks 4 (2009), 370-377.
[13] B. Meng, W.J. Qing, A receiver deniable encryption scheme, Proc. Internat. Symposium on Information (2009), 254-257.
[14] A.J. Menezes, P.C. Oorschot, S.A. Vanstone, Applied cryptography. CRC Press, New York, London, 1996.
[15] A.J. Menezes, S.A. Vanstone, Elliptic curve cryptosystems and their implementation, J. Cryptology 6 (1993), 209-224.
[16] A.A. Moldovyan, N.A. Moldovyan, Practical method for bi-deniable public-key encryption, Quasigroups and Related Systems 22 (2014), 277-282.
[17] A.A. Moldovyan, N.A. Moldovyan, V.A. Shcherbacov, Bi-Deniable publickey encryption protocol secure against active coercive adversary, Bul. Acad. Stii. Republ. Moldova, Matematica 3(76) (2014), $23-29$.
[18] A.A. Moldovyan, D.N. Moldovyan, V.A. Shcherbacov, Stream deiableencryption algorithm satisfying criterion of the computational indistinguishability from probabilistic ciphering, Computer Sci. J. Moldova 24 (2016), 68-82.
[19] N.A. Moldovyan, A.A. Moldovyan, V.A. Shcherbacov, Provably senderdeniable encryption scheme, Computer Sci. J. Moldova 23 (2015), 62-71.
[20] N.A. Moldovyan, A.A. Moldovyan, V.A. Shcherbacov, Generating cubic equations as a method for public encryption, Bul. Acad. Stii. Republ. Moldova, Matematica 3(79) (2015), $60-71$.
[21] A. O'Neil, C. Peikert, B. Waters, Bi-deniable public-key encryption, Lecture Notes Comp. Sci. 6841 (2011), 525-542.
[22] J. Pieprzyk, T. Hardjono, J. Seberry, Fundamentals of Computer Security. Springer-Verlag Berlin Heidelberg 2003.
[23] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public key cryptosystems, Commun. ACM 21 (1978), 120-126.
[24] A. Sahai, B. Waters, How to use indistinguishability obfuscation: Deniable encryption, and more, IACR Cryptology ePrint Archive (2013), 454.
[25] C. Wang, J. Wang, A shared-key and receiver-deniable encryption scheme over lattice, J. Computat. Inform. Systems 8 (2012), 747-753.

Received September 23, 2016
N.A. Moldovyan

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences 14 Liniya 39, St.Petersburg 199178, Russia
Email: nmold@mail.ru
A.V. Shcherbacov

Theoretical Lyceum C. Sibirschi, Lech Kaczynski str. 4, MD-2028 Chişinău, Moldova Email: admin@sibirsky.org
M.A. Eremeev

Mozhaisky Military Space Academy, Zhdanovskaya st. 13, St.Petersburg 197198, Russia
Email: mae1@rambler.ru

# Characterizations of ordered $k$-regular semirings by ordered quasi $k$-ideals 

Pakorn Palakawong na Ayutthaya and Bundit Pibaljommee


#### Abstract

We introduce the notion of ordered quasi $k$-ideals of ordered semirings and use them to characterize ordered $k$-regular semirings.


## 1. Introduction

In 1936, von Neumann [7] defined a ring $S$ to be regular if for any $a \in S$ there exists $x \in S$ such that $a=a x a$. Later, Bourne [3] defined a semiring $S$ to be regular if for any $a \in S$ there exist $x, y \in S$ such that $a+a x a=a y a$. In 1996, Adhikari, Sen and Weinert [1] renamed the Bourne regularity to be $k$-regular and investigated some of its properties. The notion of a quasi-ideal was defined by Steinfeld [11] for semigroups in 1956. Then, in 2004, Shabir, Ali and Batool [10] investigated some properties of quasi-ideals and used quasi-ideals to characterize regular semirings. In 2011, Bhuniya and Jana [2] defined $k$-bi-ideals on semirings and used them to characterize $k$-regular and intra- $k$-regular semirings. Later, Jana [5] introduced the notion of quasi $k$-ideals on semirings and characterized $k$-regular and intra- $k$-regular semirings by their quasi $k$-ideals which were a continuation of [2]. In 2011, Gan and Jiang [4] introduced the notion of ordered semirings, defined their ordered ideals and studied some of their properties. In 2014, Mandal [6] called an ordered semiring $S$ to be regular if for any $a \in S$ there exists $x \in S$ such that $a \leqslant a x a$ and to be $k$-regular if for any $a \in S$ there exist $x, y \in S$ such that $a+a x a \leqslant a y a$. Later, Patchakhieo and Pibaljommee [9] introduced the notion of ordered $k$-regular semirings as a generalization of $k$-regular ordered semirings, defined ordered $k$-ideals on ordered semirings and characterized ordered $k$-regular semirings using their ordered $k$-ideals.

In this paper, we introduce the notion of ordered quasi $k$-ideals of ordered semirings, investigate some of their properties, study connections between them and other ordered $k$-ideals and use them to characterize ordered $k$-regular semirings.

[^5]
## 2. Preliminaries

A semiring is an algebraic structure $(S,+, \cdot)$ such that $(S,+)$ and $(S, \cdot)$ are semigroups which are connected by the distributive law. An ordered semiring is a system $(S,+, \cdot, \leqslant)$ such that $(S,+, \cdot)$ is a semiring, $(S, \leqslant)$ is a partially ordered set and the relation $\leqslant$ is compatible with the operations + and $\cdot$ on $S$. An ordered semiring $S$ is called additively commutative if $a+b=b+a$ for all $a, b \in S$.

In this paper, we assume that $S$ is an additively commutative ordered semiring.
For any nonempty subsets $A, B$ of $S$, we denote $A B=\{a b \in S \mid a \in A, b \in B\}$, $A+B=\{a+b \in S \mid a \in A, b \in B\}$ and $(A]=\{x \in S \mid x \leqslant a$ for some $a \in A\}$.

A nonempty subset $A$ of $S$ such that $A+A \subseteq A$ and $A=(A]$ is called a left ordered ideal (right ordered ideal) of $S$ if $S A \subseteq A(A S \subseteq A)$. We call $A$ an ordered ideal [4] if $A$ is both a left ordered ideal and a right ordered ideal.

Let $A, B$ be nonempty subsets of $S$. We denote some notations as follows.

$$
\begin{aligned}
\Sigma A & =\left\{\sum_{i=1}^{n} a_{i} \in S \mid a_{i} \in A, n \in \mathbb{N}\right\} \\
\Sigma A B & =\left\{\sum_{i=1}^{n} a_{i} b_{i} \in S \mid a_{i} \in A, b_{i} \in B, n \in \mathbb{N}\right\} .
\end{aligned}
$$

In case of $A=\{a\}$ for some $a \in S$, we write $\Sigma a$ instead of $\Sigma\{a\}$.
Let $\emptyset \neq A \subseteq S$. Then $A$ is called an ordered quasi-ideal [8] of $S$ if $A+A \subseteq A$, $A=(A]$ and $(\Sigma S A] \cap(\Sigma A S] \subseteq A$. Obviously, every ordered quasi-ideal is a subsemiring. We call $A$ an ordered bi-ideal (ordered interior ideal) of $S$ if $A^{2} \subseteq A$, $A=(A]$ and $A S A \subseteq A(S A S \subseteq A)$.

The $k$-closure [9] of a nonempty subset $A$ of $S$ is defined by

$$
\bar{A}=\{x \in S \mid x+a \leqslant b \text { for some } a, b \in A\} .
$$

Now, we give some properties on an ordered semiring which will be used later as the following two lemmas such that their proofs are not difficult.

Lemma 2.1. Let $A, B, C$ be nonempty subsets of $S$. Then
(i) $A \subseteq \Sigma A$ and $\Sigma(\Sigma A)=\Sigma A$;
(ii) if $A \subseteq B$ then $\Sigma A \subseteq \Sigma B$;
(iii) $A(\Sigma B) \subseteq(\Sigma A)(\Sigma B) \subseteq \Sigma A B$, $(\Sigma A) B \subseteq(\Sigma A)(\Sigma B) \subseteq \Sigma A B ;$
(iv) $\Sigma(A+B) \subseteq \Sigma A+\Sigma B$;
(v) $\Sigma(A \cup B)=\Sigma A \cup \Sigma B$;
(vi) $\Sigma(A \cap B) \subseteq \Sigma A \cap \Sigma B$;
(vii) $\Sigma(A] \subseteq(\Sigma A]$;
(viii) $A \subseteq(A]$ and $((A]]=(A]$;
(ix) if $A \subseteq B$ then $(A] \subseteq(B]$;
$(x) A(B] \subseteq(A](B] \subseteq(A B]$, $(A] B \subseteq(A](B] \subseteq(A B] ;$
(xi) $A+(B] \subseteq(A]+(B] \subseteq(A+B]$;
(xii) $(A \cup B]=(A] \cup(B]$;
(xiii) $(A \cap B] \subseteq(A] \cap(B]$.

Lemma 2.2. Let $A, B$ be nonempty subsets of $S$. Then
(i) $\Sigma \bar{A} \subseteq \overline{\Sigma A}$;
(ii) if $A+A \subseteq A$, then $A \subseteq \bar{A}$ and $\overline{\bar{A}}=\overline{(A]}=\overline{\overline{(A]}}$;
(iii) if $A \subseteq B$, then $\bar{A} \subseteq \bar{B}$;
(iv) $A \bar{B} \subseteq \overline{A B}$ and $\bar{A} B \subseteq \overline{A B}$;
(v) if $A$ and $B$ are closed under addition, then $\bar{A}+\bar{B} \subseteq \overline{A+B}$;
(vi) $\overline{A \cup B} \supseteq \bar{A} \cup \bar{B}$;
(vii) $\overline{A \cap B} \subseteq \bar{A} \cap \bar{B}$ (the equality holds if $A, B$ are closed under addition, $\bar{A}=A$ and $\bar{B}=B$ and also holds for arbitrary intersection);
(viii) if $A+A \subseteq A$, then $A \subseteq(A] \subseteq(\bar{A}]=\bar{A} \subseteq \overline{(A]}$.

As a consequence of Lemma 2.1 and 2.2, we obtain the following lemma.
Lemma 2.3. Let $A, B$ be nonempty subsets of $S$ such that $A$ and $B$ are closed under addition. Then:
(i) $\overline{A \overline{(B]}} \subseteq \overline{(A B]}$ and $\overline{(A]} B \subseteq \overline{(A B]}$;
(ii) $\overline{(A]} \overline{(B]} \subseteq \overline{(\Sigma A B]}$;
(iii) $\Sigma A \overline{(B]} \subseteq \overline{(\Sigma A \overline{(B)]}} \subseteq \overline{(\Sigma \overline{(A]} \overline{(B])}} \subseteq \overline{(\Sigma A B]}$,
$\overline{\Sigma \overline{(A]} B \subseteq \overline{(\Sigma \overline{(A]} B]} \subseteq \overline{(\overline{(A]} \overline{(B])}} \subseteq \overline{(\Sigma A B]} ; ; \text { } ; \overline{(A+B)}}$
(iv) $\overline{(\overline{(A]}+\overline{(B]}]} \subseteq \overline{(A+B]}$.

It is not difficult to prove that if a nonempty subset $A$ of $S$ is closed under addition then $(A], \bar{A}$ and $\overline{(A]}$ are also closed.

Now, we recall the notions of some types of ordered $k$-ideals which occur in [9] as follows. A left ordered $k$-ideal (resp. right ordered $k$-ideal, ordered $k$-ideal, ordered $k$-bi-ideal, ordered $k$-interior ideal) $A$ of $S$ is a left ordered ideal (resp. right ordered ideal, ordered ideal, ordered bi-ideal, ordered interior ideal) of $S$ satisfying the condition if $x \in S$ such that $x+a \in A$ for some $a \in A$ then $x \in A$.

It is easy to prove that the following lemma is true on ordered semirings.
Lemma 2.4. Let $\emptyset \neq A \subseteq S$. Then the following statements hold:
(i) $\overline{(\Sigma S A]}$ is a left ordered $k$-ideal of $S$;
(ii) $\overline{(\Sigma A S]}$ is a right ordered $k$-ideal of $S$;
(iii) $\overline{(\Sigma S A S]}$ is an ordered $k$-ideal of $S$.

As a spacial case of Lemma 2.4, if $A=\{a\}$ then we obtain that $\overline{(S a]}, \overline{(a S]}$ and $\overline{(\Sigma S a S]}$ is a left ordered $k$-ideal, right ordered $k$-ideal and ordered $k$-ideal of $S$, respectively.

By $L_{k}(A), R_{k}(A), J_{k}(A)$ and $B_{k}(A)$ we denote the smallest left ordered $k$ ideal, right ordered $k$-ideal, ordered $k$-ideal and ordered $k$-bi-ideal of $S$ containing $A$, respectively.

Theorem 2.5. (cf. [9]) For any $\emptyset \neq A \subseteq S$ we have:
(i) $L_{k}(A)=\overline{(\Sigma A+\Sigma S A]}$;
(ii) $R_{k}(A)=\overline{(\Sigma A+\Sigma A S]}$;
(iii) $J_{k}(A)=\overline{(\Sigma A+\Sigma S A+\Sigma A S+\Sigma S A S]}$.

It is not difficult to prove that a subsemiring $B$ of $S$ is an ordered $k$-bi-ideal of $S$ if and only if $B S B \subseteq B$ and $B=\bar{B}$.

Theorem 2.6. $B_{k}(A)=\overline{\left(\Sigma A+\Sigma A^{2}+\Sigma A S A\right]}$ for any $\emptyset \neq A \subseteq S$.
Proof. Let $\emptyset \neq A \subseteq S$ and $B=\overline{\left(\Sigma A+\Sigma A^{2}+\Sigma A S A\right]}$. Firstly, we show that $B$ is an ordered $k$-bi-ideal of $S$. Since $\Sigma A+\Sigma A^{2}+\Sigma A S A$ is closed under addition, $B$ is also closed. By Lemma 2.3(ii) and Lemma 2.1(i), we obtain

$$
\begin{aligned}
B^{2} & =\overline{\left(\Sigma A+\Sigma A^{2}+\Sigma A S A\right]} \overline{\left(\Sigma A+\Sigma A^{2}+\Sigma A S A\right]} \\
& \subseteq \overline{\left(\Sigma\left(\Sigma A+\Sigma A^{2}+\Sigma A S\right)\left(\Sigma A+\Sigma A^{2}+\Sigma S A\right)\right]} \\
& \subseteq \overline{\left(\Sigma\left(\Sigma A^{2}+\Sigma A^{3}+\Sigma A S A+\Sigma A^{4}+\Sigma A^{2} S A+\Sigma A S A+\Sigma A S A^{2}+\Sigma A S S A\right)\right]} \\
& \subseteq \overline{\left(\Sigma A^{2}+\Sigma A S A\right]} \subseteq B .
\end{aligned}
$$

Using Lemma 2.3(i,ii), we have

$$
\begin{aligned}
B S B & =\overline{\left(\Sigma A+\Sigma A^{2}+\Sigma A S A\right]} S \overline{\left(\Sigma A+\Sigma A^{2}+\Sigma A S A\right]} \\
& \subseteq \overline{(\Sigma A+\Sigma A S+\Sigma A S A]} \overline{\left(\Sigma S A+\Sigma S A^{2}+\Sigma S A S A\right]} \\
& \subseteq \overline{(\Sigma A+\Sigma A S] \overline{(\Sigma S A]} \subseteq \overline{(\Sigma(\Sigma A+\Sigma A S)(\Sigma S A)]} \subseteq \overline{(\Sigma A S A]}} .
\end{aligned}
$$

Let $x \in \overline{(\Sigma A S A]}$. Then $x+(z+x) \leqslant z+x+x$ for every $z \in \Sigma A+\Sigma A^{2}$ and so $x \in \overline{\Sigma A+\Sigma A^{2}+\overline{(\Sigma A S A]}}$, since $z+x, z+x+x \in \Sigma A+\Sigma A^{2}+\overline{(\Sigma A S A]}$. Thus $\overline{(\Sigma A S A]} \subseteq \overline{\Sigma A+\Sigma A^{2}+\overline{(\Sigma A S A]}}$. Using Lemma 2.2(viii) and Lemma 2.3(iv), we
 Lemma 2.2(ii), we get $\overline{\bar{B}}=B$. This means that $B$ is an ordered $k$-bi-ideal of $S$.

Secondly, we show that $A \subseteq B$. Let $x \in \Sigma A$. Then $x+(x+w) \leqslant x+x+w$ for every $w \in \Sigma A^{2}+\Sigma A S A$ and so $x \in \overline{\Sigma A+\Sigma A^{2}+\Sigma A S A}$, since $x+w, x+$ $x+w \in \Sigma A+\Sigma A^{2}+\Sigma A S A$. It follows that $A \subseteq \Sigma A \subseteq \overline{\Sigma A+\Sigma A^{2}+\Sigma A S A} \subseteq$ $\overline{\left(\Sigma A+\Sigma A^{2}+\Sigma A S A\right]}=B$.

Finally, let $C$ be an ordered $k$-bi-ideal of $S$ containing $A$. Then

$$
B=\overline{\left(\Sigma A+\Sigma A^{2}+\Sigma A S A\right]} \subseteq \overline{\left(\Sigma C+\Sigma C^{2}+\Sigma C S C\right]} \subseteq \overline{(\Sigma C]}=C
$$

Therefore, $B$ is the smallest ordered $k$-bi-ideal of $S$ containing $A$.

## 3. Ordered quasi $k$-ideals

Here, we give the notion of ordered quasi $k$-ideals of ordered semirings, study their properties and investigate connections between them and other ordered $k$-ideals.

Definition 3.1. Let $\emptyset \neq Q \subseteq S$ such that $Q+Q \subseteq Q$. Then $Q$ is called an ordered quasi $k$-ideal of $S$ if
(i) $\overline{\overline{(\Sigma S Q]}} \cap \overline{(\Sigma Q S]} \subseteq Q$;
(ii) if $x \leqslant y$ for some $y \in Q$ then $x \in Q$ (i.e., $Q=(Q])$;
(iii) if $x+a \in Q$ for some $a \in Q$ then $x \in Q$.

It is easy to see that every ordered quasi $k$-ideal $Q$ of $S$ is a subsemiring because $Q^{2} \subseteq S Q \cap Q S \subseteq Q$.

Theorem 3.2. Let $\emptyset \neq Q \subseteq S$ and $Q+Q \subseteq Q$. Then $Q$ is an ordered quasi $k$-ideal of $S$ if and only if $\overline{(\Sigma S Q]} \cap \overline{(\Sigma Q S]} \subseteq Q$ and $Q=\bar{Q}$.

Proof. Let $Q$ be an ordered quasi $k$-ideal of $S$. Clearly, $Q \subseteq \bar{Q}$. Let $x \in \bar{Q}$. Then $x+y \leqslant z$ for some $y, z \in Q$ and so $x+y \in(Q]=Q$. Thus, $x \in Q$. Hence, $Q=\bar{Q}$.

Conversely, we consider $Q \subseteq(Q] \subseteq \bar{Q}=Q$. Thus, $Q=(Q]$. Let $x \in S$ such that $x+y \in Q=(Q]$ for some $y \in Q$. So, $x+y \leqslant q$ for some $q \in Q$. Hence, $x \in \bar{Q}=Q$.

Note that every left ordered $k$-ideal (right ordered $k$-ideal, ordered $k$-ideal) of $S$ is an ordered quasi $k$-ideal. The converse is not true as the following example shows.

Example 3.3. Let $S=\{a, b, c\}$. Define a binary operation + on $S$ by $b+b=b$ and $a+x=x+a=x, c+x=x+c=c$ for all $x \in S$. Define a binary operation - on $S$ by for any $y \in S, x y=a$ if $x=a$ and $x y=b$, otherwise. Define a binary relation $\leq$ on $S$ by $\leqslant:=\{(a, a),(b, b),(c, c),(a, b)\}$. Now, $(S,+, \cdot, \leqslant)$ is an additively commutative ordered semiring. Let $Q=\{a\}$. Clearly, $Q+Q \subseteq Q$ and $Q=(Q]$. We have $\overline{(\Sigma S Q]} \cap \overline{(\Sigma Q S]}=\overline{(\Sigma\{a, b\}]} \cap \overline{(\Sigma\{a\}]}=\{a, b\} \cap\{a\}=\{a\}=Q$ and $\bar{Q}=Q$. This shows that $Q$ is an ordered quasi $k$-ideal. Since $S Q=\{a, b\} \nsubseteq Q$, this follows that $Q$ is not a left ordered $k$-ideal of $S$.

Also every ordered quasi $k$-ideal of $S$ is an ordered $k$-bi-ideal, but not conversely.

Example 3.4. Let $S=\{a, b, c, d, e\}$. Define a binary operation + on $S$ by $a+x=$ $x+a=x$ for all $x \in S, b+b=b, e+e=e$ and $x+y=d$ otherwise. Define a binary operation - on $S$ by for any $y \in S, x y=y x=a$ if $x \in\{a, b\}$ and $x y=b$ otherwise. Define a binary relation $\leqslant$ on $S$ by

$$
\leqslant:=\{(a, a),(b, b),(c, c),(d, d),(e, e),(a, b),(a, c),(a, e),(a, d),(b, d),(c, d),(e, d)\}
$$

Now, $(S,+, \cdot, \leqslant)$ is an additively commutative ordered semiring. Let $B=\{a, e\}$. It is easy to show that $B$ is an ordered $k$-bi-ideal of $S$, but not an ordered quasi $k$-ideal, since $\overline{(\Sigma S B]} \cap \overline{(\Sigma B S]}=\{a, b\} \nsubseteq B$.

Theorem 3.5. The intersection of a right ordered $k$-ideal and a left ordered $k$-ideal of $S$ is an ordered quasi $k$-ideal.

Proof. Let $R$ and $L$ be a right and a left ordered $k$-ideal of $S$, respectively. Then

$$
\overline{(\Sigma(R \cap L) S]} \cap \overline{(\Sigma S(R \cap L)]} \subseteq \overline{(\Sigma R S]} \cap \overline{(\Sigma S L]} \subseteq \overline{(\Sigma R]} \cap \overline{(\Sigma L]}=R \cap L
$$

We consider $\overline{R \cap L}=\bar{R} \cap \bar{L}=R \cap L$. By Theorem 3.2, we obtain $R \cap L$ is an ordered quasi $k$-ideal of $S$.

The converse of Theorem 3.5 is not true as the following example shows.
Example 3.6. Let $S=\{a, b, c, d, e, f, g, h\}$. Define binary operations + and $\cdot$ by the following tables:

| + | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $a$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ |
| $b$ | $b$ | $a$ | $e$ | $f$ | $c$ | $d$ | $h$ | $g$ |
| $c$ | $c$ | $e$ | $a$ | $g$ | $b$ | $h$ | $d$ | $f$ |
| $d$ | $d$ | $f$ | $g$ | $a$ | $h$ | $b$ | $c$ | $e$ |
| $e$ | $e$ | $c$ | $b$ | $h$ | $a$ | $g$ | $f$ | $d$ |
| $f$ | $f$ | $d$ | $h$ | $b$ | $g$ | $a$ | $e$ | $c$ |
| $g$ | $g$ | $h$ | $d$ | $c$ | $f$ | $e$ | $a$ | $b$ |
| $h$ | $h$ | $g$ | $f$ | $e$ | $d$ | $c$ | $b$ | $a$ |


| $\cdot$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $a$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ | $g$ | $a$ | $h$ | $b$ | $g$ | $h$ |
| $c$ | $a$ | $d$ | $a$ | $a$ | $d$ | $d$ | $a$ | $d$ |
| $d$ | $a$ | $d$ | $a$ | $a$ | $d$ | $d$ | $a$ | $d$ |
| $e$ | $a$ | $f$ | $g$ | $a$ | $e$ | $f$ | $g$ | $e$ |
| $f$ | $a$ | $f$ | $g$ | $a$ | $e$ | $f$ | $g$ | $e$ |
| $g$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ |
| $h$ | $a$ | $b$ | $g$ | $a$ | $h$ | $b$ | $g$ | $h$ |

Define a binary relation $\leqslant$ on $S$ by $\leqslant:=\{(x, x) \mid x \in S\}$.
Then $(S,+, \cdot, \leqslant)$ is an additively commutative ordered semiring. Let $Q=$ $\{a, c\}$. Clearly, $Q+Q \subseteq Q$ and $Q=(Q]$. We consider

$$
\overline{(\Sigma S Q]} \cap \overline{(\Sigma Q S]}=\overline{\{a, g\}} \cap \overline{\{a, d\}}=\{a, g\} \cap\{a, d\}=\{a\} \subseteq Q .
$$

It is easy to see that $\bar{Q}=Q$. By Theorem 3.2, $Q$ is an ordered quasi $k$-ideal of $S$. If $Q=R \cap L$ for some a right ordered $k$-ideal $R$ and a left ordered $k$-ideal $L$ of $S$, then $c \in R \cap L$. We have $g=c+c b \in R$ and $g=b c \in L$. Then $g \in R \cap L=Q$, but $g \notin Q$. This give a contradiction.

As a consequence of Lemma 2.4 and Theorem 3.5, we have that $\overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}$ is an ordered quasi $k$-ideals of $S$ for any $\emptyset \neq A \subseteq S$.

For $\emptyset \neq A \subseteq S$, we denote $Q_{k}(A)$ as the smallest ordered quasi $k$-ideal of $S$ containing $A$. Now, we give the construction of $Q_{k}(A)$ as follows.

Theorem 3.7. Let $\emptyset \neq A \subseteq S$. Then $Q_{k}(A)=\overline{(\Sigma A+\overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}]}$.

Proof. Let $\emptyset \neq A \subseteq S$ and $Q=\overline{(\Sigma A+\overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}]}$. Firstly, we show that $Q$ is an ordered quasi $k$-ideal. It is easy to show that $Q$ is closed under addition. Using Lemma $2.3(i)$ and (iv), we obtain

$$
\begin{aligned}
\overline{(\Sigma S Q]} \cap \overline{(\Sigma Q S]} & \subseteq \overline{(\Sigma S Q]}=\overline{(\Sigma S \overline{(\Sigma A+\overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}]}]} \subseteq \overline{(\Sigma \overline{(\Sigma A+\overline{(\Sigma S A]}]})} \\
& \subseteq \overline{(\Sigma S \overline{(\Sigma A+\Sigma S A]}} \subseteq \overline{(\Sigma \overline{(\Sigma S A+\Sigma S S A]}]} \subseteq \overline{(\overline{(\Sigma(\Sigma S A)]}]} \subseteq \overline{(\Sigma S A]}
\end{aligned}
$$

Similarly, we have $\overline{(\Sigma S Q]} \cap \overline{(\Sigma Q S]} \subseteq \overline{(\Sigma A S]}$. So, $\overline{(\Sigma S Q]} \cap \overline{(\Sigma Q S]} \subseteq \overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}$. If $q \in \overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}$ then $q+a^{\prime}+q \leqslant a^{\prime}+q+q \in \Sigma A+\overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}$ for every $a^{\prime} \in \Sigma A$. So, $\overline{(\Sigma S A]} \cap \overline{(\Sigma A S]} \subseteq \overline{\Sigma A+\overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}}$. By Lemma 2.2(ii), we get

$$
\overline{(\Sigma S Q]} \cap \overline{(\Sigma Q S]} \subseteq \overline{(\Sigma S A]} \cap \overline{(\Sigma A S]} \subseteq \overline{\Sigma A+\overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}} \subseteq Q
$$

Using Lemma 2.2(viii), $\bar{Q}=Q$. By Theorem 3.2, $Q$ is an ordered quasi $k$-ideal.
Secondly, we show that $A \subseteq Q$. If $a \in \Sigma A$ then $a+a+w \leqslant a+a+w$ and $a+a+w \in \Sigma A+\overline{(\Sigma S A]} \cap \overline{(\Sigma \overline{A S}]}$, for every $w \in \overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}$. This implies

Finally, let $K$ be an ordered quasi $k$-ideal of $S$ such that $A \subseteq K$. Then

$$
Q=\overline{(\Sigma A+\overline{(\Sigma S A]} \cap \overline{(\Sigma A S])}} \subseteq \overline{(\Sigma K+\overline{(\Sigma S K]} \cap \overline{(\Sigma K S]}]} \subseteq \overline{(K+K]} \subseteq \overline{(K]}=K
$$

Therefore, $Q$ is the smallest ordered quasi $k$-ideal of $S$ containing $A$.
As a spacial case of Theorem 3.7, if $A=\{a\}$ for some $a \in S$ then we obtain $Q_{k}(a)=\overline{(\Sigma a+\overline{(S a]} \cap \overline{(a S]}]}$.

Note that a nonempty intersection of a family of ordered quasi $k$-ideals of $S$ is an ordered quasi $k$-ideal of $S$.

An element $e$ of $S$ is called an identity of $S$ if $e a=a=a e$ for all $a \in S$.
Corollary 3.8. Let $\emptyset \neq A \subseteq S$. If $S$ has an identity then
(i) $L_{k}(A)=\overline{(\Sigma S A]}$;
(ii) $R_{k}(A)=\overline{(\Sigma A S]}$;
(iii) $J_{k}(A)=\overline{(\Sigma S A S]}$;
(iv) $B_{k}(A)=\overline{(\Sigma A S A]} ;$
(v) $Q_{k}(A)=\overline{(\Sigma S A]} \cap \overline{(\Sigma A S]}$.

As a spacial case of Corollary 3.8, if $A=\{a\}$ then we have $L_{k}(a)=\overline{(S a]}$, $R_{k}(a)=\overline{(a S]}, J_{k}(a)=\overline{(\Sigma S a S]}, Q_{k}(a)=\overline{(S a]} \cap \overline{(a S]}$ and $B_{k}(a)=\overline{(a S a]}$.

If $S$ has an identity element, then the converse of Theorem 3.5 is true.

Theorem 3.9. If $S$ has an identity, then ordered quasi $k$-ideals and ordered $k$-biideals coincide.

Proof. Assume that $S$ has an identity. Let $B$ be an ordered $k$-bi-ideal of $S$ and let $x \in \overline{(\Sigma S B]} \cap \overline{(\Sigma B S]}$. Using Lemma 2.3(i), (iii), we obtain

$$
x \in B_{k}(x)=\overline{(x S x]} \subseteq \overline{(\overline{(\Sigma B S]} S \overline{(\Sigma S B]}]} \subseteq \overline{(\Sigma B S S S B]} \subseteq \overline{(\Sigma B S B]} \subseteq \overline{(\Sigma B]}=B
$$

This shows that $B$ is an ordered quasi $k$-ideal of $S$.
Theorem 3.10. If $S$ has an identity, then every ordered quasi $k$-ideal of $S$ can be written in the form $Q=R \cap L$ for some a right ordered $k$-ideal $R$ and a left ordered $k$-ideal $L$ of $S$.
Proof. Let $Q$ be an ordered quasi $k$-ideal of $S$. Clearly, $Q \subseteq R_{k}(Q) \cap L_{k}(Q)$. By Corollary 3.8, we have $R_{k}(Q)=\overline{(\Sigma Q S]}$ and $L_{k}(Q)=\overline{(\Sigma \bar{Q} S]}$. Hence, $R_{k}(Q) \cap$ $L_{k}(Q)=\overline{(\Sigma Q S]} \cap \overline{(\Sigma Q S]} \subseteq Q$. Therefore, $Q=R_{k}(Q) \cap L_{k}(Q)$.

## 4. Ordered $k$-regular semirings

First, we review the notion of a $k$-regular ordered semiring given by Mandal [6] and the notion of an ordered $k$-regular semiring defined by Patchakhieo and Pibaljommee [9] which is a generalization of Mandal $k$-regularity as follows.

Definition 4.1. An element $a$ of $S$ is called regular (resp. $k$-regular, ordered $k$ regular) if $a \leqslant a x a$ (resp. $a+a x a \leqslant a y a, a \in \overline{(a S a]})$ for some $x, y \in S$. We call $S$ regular (resp. $k$-regular, ordered $k$-regular) if every element of $S$ is regular (resp. $k$-regular, ordered $k$-regular).

Obviously, $S$ is ordered $k$-regular if and only if $A \subseteq \overline{(\Sigma A S A]}$ for each $A \subseteq S$.
Theorem 4.2. (cf. [9]) An ordered semiring $S$ is ordered $k$-regular if and only if $R \cap L=\overline{(R L]}$ for every right ordered $k$-ideal $R$ and left ordered $k$-ideal $L$ of $S$.

Corollary 4.3. An ordered semiring $S$ is ordered $k$-regular if and only if $A \subseteq$ $\overline{\left(R_{k}(A) L_{k}(A)\right]}$ for each $A \subseteq S$.

Remark 4.4. If $S$ is ordered $k$-regular then ordered $k$-ideals and ordered $k$-interior ideals coincide.

Proof. Let $J$ be an ordered $k$-ideal of $S$. Then $S J S \subseteq S J \subseteq J S \subseteq J$ and so $J$ is an ordered $k$-interior ideal. Conversely, let $I$ be an ordered $k$-interior ideal of $S$. If $x \in I S$, then $x \in \overline{(x S x]} \subseteq \overline{(I S S I S]} \subseteq \overline{(I S I S]} \subseteq \overline{(I I]} \subseteq \overline{(I]}=I$. So, $I S \subseteq I$ Similarly, we obtain $S I \subseteq I$. Therefore, $I$ is an ordered $k$-ideal of $S$.

Now, we show that if $S$ is ordered $k$-regular, then the converse of Theorem 3.5 is true.

Theorem 4.5. If $S$ is ordered $k$-regular, then their ordered quasi $k$-ideals coincide with their ordered $k$-bi-ideals.

Proof. Assume that $S$ is ordered $k$-regular. Let $B$ be an ordered $k$-bi-ideal of $S$ and let $x \in \overline{(\Sigma S B]} \cap \overline{(\Sigma B S]}$. Using Lemma 2.3(i), (iii) and by assumption, we get

$$
x \in \overline{(x S x]} \subseteq \overline{(\overline{(\Sigma B S]} S \overline{S(\Sigma S B]}]} \subseteq \overline{(\Sigma B S S S B]} \subseteq \overline{(\Sigma B S B]} \subseteq \overline{(\Sigma B]}=B
$$

This shows that $B$ is an ordered quasi $k$-ideal of $S$.
Theorem 4.6. If $S$ is ordered $k$-regular, then every ordered quasi $k$-ideal of $S$ can be written in the form $Q=R \cap L$ for some a right ordered $k$-ideal $R$ and a left ordered $k$-ideal $L$ of $S$.

Proof. Let $Q$ be an ordered quasi $k$-ideal. Clearly, $Q \subseteq R_{k}(Q) \cap L_{k}(Q)$. If $x \in \Sigma Q$ then $x \in \overline{(x S x]} \subseteq \overline{(x S]} \subseteq \overline{((\Sigma Q) S]} \subseteq \overline{(\Sigma Q S]}$. Thus $\Sigma Q \subseteq \overline{(\Sigma Q S]}$. We consider $\overline{\left.\overline{(\Sigma Q S]} \subseteq \overline{(\Sigma Q+\overline{\Sigma Q S]}} \subseteq \overline{(\overline{(\Sigma Q S]}+\Sigma Q S]} \subseteq \overline{(\Sigma Q S]} \text {. This means that } R_{k}(Q)=\overline{(\Sigma Q)}=\overline{\Sigma Q S}\right)}$ $\overline{(\Sigma Q+\Sigma Q S]}=\overline{(\Sigma Q S]}$. Similarly, we can show that $L_{k}(Q)=\overline{(\Sigma S Q]}$. It follows that $R_{k}(Q) \cap L_{k}(Q)=\overline{(\Sigma Q S]} \cap \overline{(\Sigma S Q]} \subseteq Q$. Therefore, $Q=R_{k}(Q) \cap L_{k}(Q)$.

Here, we use ordered quasi $k$-ideals to characterize ordered $k$-regular semirings.
Theorem 4.7. The following statements are equivalent:
(i) $S$ is ordered $k$-regular;
(ii) $B=\overline{(B S B]}$ for every ordered $k$-bi-ideal of $S$;
(iii) $Q=\overline{(Q S Q]}$ for every ordered quasi $k$-ideal of $S$.

Proof. $(i) \Rightarrow(i i)$ : Let $S$ be ordered $k$-regular and $B$ be an ordered $k$-bi-ideal of $S$. Clearly, $\overline{(B S B]} \subseteq \overline{(B]}=B$. If $x \in B$ then $x \in \overline{(x S x]} \subseteq \overline{(B S B]}$. So, $B=\overline{(B S B]}$.
$(i i) \Rightarrow(i i i)$ : It is clear, since every ordered quasi $k$-ideal is an ordered $k$-biideal.
(iii) $\Rightarrow(i)$ : Assume that (iii) holds. Let $A \subseteq S$. Then

$$
A \subseteq Q_{k}(A)=\overline{\left(Q_{k}(A) S Q_{k}(A)\right]} \subseteq \overline{\left(R_{k}(A) S L_{k}(A)\right]} \subseteq \overline{\left(R_{k}(A) L_{k}(A)\right]}
$$

By Corollary 4.3, we obtain that $S$ is ordered $k$-regular.
Theorem 4.8. An ordered semiring $S$ is ordered $k$-regular if and only if for every ordered $k$-bi-ideal B, ordered $k$-ideal $J$ and left ordered $k$-ideal $L$ of $S$ we have $B \cap J \cap L \subseteq \overline{(B J L]}$.
Proof. Assume that $S$ is ordered $k$-regular. Let $B, J$ and $L$ be an ordered $k$ -bi-ideal, an ordered $k$-ideal and a left ordered $k$-ideal of $S$, respectively. Let $x \in B \cap J \cap L$. By assumption, we get $x \in \overline{(x S x]} \subseteq \overline{(\overline{(x S x]} S x]} \subseteq \overline{(x S x S x)} \subseteq$ $\overline{(B S J S L]} \subseteq \overline{(B S L]}$. Hence, $B \cap J \cap L \subseteq \overline{(B J L]}$.

Conversely, let $R$ and $L$ be a right ordered $k$-ideal and a left ordered $k$-ideal of $S$, respectively. We obtain $R \cap L=R \cap S \cap L=\overline{(R S L]} \subseteq \overline{(R L]}$. On the other hand, we know that $\overline{(R L]} \subseteq R \cap L$. So, $\overline{(R L]}=R \cap L$. By Theorem 4.2, $S$ is ordered $k$-regular.

Theorem 4.9. The following statements are equivalent:
(i) $S$ is ordered $k$-regular;
(ii) $Q \cap I=\overline{(Q I Q]}$ for every ordered quasi $k$-ideal $Q$ and ordered $k$-interior ideal $I$ of $S$;
(iii) $Q \cap J=\overline{(Q J Q]}$ for every ordered quasi $k$-ideal $Q$ and ordered $k$-ideal $J$ of $S$
(iv) $Q \cap L \subseteq \overline{(Q L]}$ for every ordered quasi $k$-ideal $Q$ and left ordered $k$-ideal $L$ of $S$;
(v) $R \cap Q \subseteq \overline{(R Q]}$ for every right ordered $k$-ideal $R$ and ordered quasi $k$-ideal $Q$ of $S$;
(vi) $R \cap Q \cap L \subseteq \overline{(R Q L]}$ for every right ordered $k$-ideal $R$, ordered quasi $k$-ideal $Q$ and left ordered $k$-ideal $L$ of $S$.

Proof. Let $Q, I, J, R$ and $L$ be an ordered quasi $k$-ideal, an ordered $k$-interior ideal, an ordered $k$-ideal, a right ordered $k$-ideal and a left ordered $k$-ideal of $S$, respectively.
$(i) \Rightarrow(i i)$ : Assume that $S$ is ordered $k$-regular and let $x \in Q \cap I$. By assumption, we obtain $x \in \overline{(x S x]} \subseteq \overline{(\overline{(x S x]} S x]} \subseteq \overline{(x S x S x]} \subseteq \overline{(Q S I S Q]} \subseteq \overline{(Q I Q]}$. For the opposite inclusion, we consider $\overline{(Q I Q]} \subseteq \overline{(Q S Q]} \subseteq \overline{(Q]}=Q$ and $\overline{(Q I Q]} \subseteq \overline{(S I S]} \subseteq$ $\overline{(I]}=I$. Therefore, $Q \cap I=\overline{(Q I Q]}$.
(ii) $\Rightarrow(i i i)$ : It is obvious.
$(i i i) \Rightarrow(i)$ : Assume that (iii) holds. By assumption, we get $Q=Q \cap S=$ $\overline{(Q S Q]}$. By Theorem 4.7, $S$ is ordered $k$-regular.
$(i) \Rightarrow(i v):$ If $x \in Q \cap L$, then $x \in \overline{(x S x]} \subseteq \overline{(Q S L]} \subseteq \overline{(Q L]}$.
$(i v) \Rightarrow(i)$ : Assume that $(i v)$ holds. Then we obtain $R \cap L \subseteq \overline{(R L]}$, since every right ordered $k$-ideal is an ordered quasi $k$-ideal. Clearly, $\overline{(R L]} \subseteq R \cap L$. So, $R \cap L=\overline{(R L]}$. By Theorem 4.2, $S$ is ordered $k$-regular.
$(i) \Rightarrow(v)$ : If $x \in R \cap Q$, then $x \in \overline{(x S x]} \subseteq \overline{(R S Q]} \subseteq \overline{(R Q]}$.
$(v) \Rightarrow(i)$ : It can be proved in a similar way of $(i v) \Rightarrow(i)$.
$(i) \Rightarrow(v i)$ : Assume that $S$ is ordered $k$-regular and let $x \in R \cap Q \cap L$. Then $x \in \overline{(x S x]} \subseteq \overline{(\overline{(x S x]} S x]} \subseteq \overline{(x S x S x]} \subseteq \overline{(R S Q S L]} \subseteq \overline{(R Q L]}$.
$(v i) \Rightarrow(i)$ : Assume that (vi) holds. We get $R \cap L=R \cap S \cap L \subseteq \overline{(R S L]} \subseteq \overline{(R L]}$. Clearly, $\overline{(R L]} \subseteq R \cap L$. So, $R \cap L=\overline{(R L]}$. By Theorem 4.2, $S$ is ordered $k$ regular.

Definition 4.10. An ordered semiring $S$ is said to be an ordered $k$-duo-semiring if every one-sided (left or right) ordered $k$-ideal of $S$ is an ordered $k$-ideal of $S$.

It is clear that every multiplicatively commutative ordered semiring is an ordered $k$-duo-semiring, but the converse is not true as the following example shows.

Example 4.11. Let $S=\{a, b, c, d, e\}$. Define a binary operation + on $S$ by $a+x=x+a=x$ for all $x \in S$ and $x+y=c$ otherwise. Define a binary operation - on $S$ by $a x=x a=a$ for all $x \in S, b b=b d=d d=e$ and $x y=c$ otherwise. Define a binary relation $\leqslant$ on $S$ by

$$
\leqslant:=\{(a, a),(b, b),(c, c),(d, d),(e, e),(e, c)\} .
$$

Then $(S,+, \cdot, \leqslant)$ is an ordered semiring which is not multiplicatively commutative, since $b d \neq d b$. We have $\{a\}$ and $S$ are only ordered one-sided $k$-ideals of $S$. Obviously, all of them are ordered ideals of $S$. This shows that $S$ is an ordered $k$-duo-semiring.

Theorem 4.12. The following statements are equivalent:
(i) $S$ is an ordered $k$-duo-semiring;
(ii) $R_{k}(A)=L_{k}(A)$ for each $A \subseteq S$;
(iii) $R_{k}(a)=L_{k}(a)$ for each $a \in S$.

Proof. $(i) \Rightarrow(i i)$ and $(i i) \Rightarrow(i i i)$ are obvious.
(iii) $\Rightarrow(i)$ : Assume that (iii) holds and let $R$ be a right ordered $k$-ideal of $S$. Let $x \in R, s \in S$. By assumption, we obtain $s x \in S L_{k}(x) \subseteq L_{k}(x)=R_{k}(x) \subseteq$ $R_{k}(R)=R$. This shows that $R$ is a left ordered $k$-ideal of $S$. Similarly, we can show that if $L$ is a left ordered $k$-ideal of $S$ then $L$ is a right ordered $k$-ideal of $S$. Therefore, $S$ is an ordered $k$-duo-semiring.

As a consequence of Theorem 4.5, 4.6 and Definition 4.10, we obtain the following corollary.

Corollary 4.13. If an ordered $k$-duo-semiring $S$ is ordered $k$-regular, then its ordered $k$-ideals, ordered $k$-interior ideals, ordered quasi $k$-ideals and its ordered $k$-bi-ideals coincide.

Theorem 4.14. Let $S$ be an ordered $k$-duo-semiring. Then the following statements are equivalent:
(i) $S$ is ordered $k$-regular;
(ii) $B_{1} \cap B_{2}=\overline{\left(B_{1} B_{2}\right]}$ for every ordered $k$-bi-ideals $B_{1}$ and $B_{2}$ of $S$;
(iii) $Q_{1} \cap Q_{2}=\overline{\left(Q_{1} Q_{2}\right]}$ for every ordered quasi $k$-ideals $Q_{1}$ and $Q_{2}$ of $S$;
(iv) $J_{1} \cap J_{2}=\overline{\left(J_{1} J_{2}\right]}$ for every ordered $k$-ideal $J_{1}$ and $J_{2}$ of $S$.

Proof. $(i) \Rightarrow(i i)$ : Let $B_{1}, B_{2}$ be ordered $k$-bi-ideals of $S$. By Corollary 4.13, $B_{1}$ and $B_{2}$ are ordered $k$-ideals of $S$. By Theorem 4.2, we obtain $B_{1} \cap B_{2}=\overline{\left(B_{1} B_{2}\right]}$. (ii) $\Rightarrow(i i i)$ and (iii) $\Rightarrow(i v)$ are obvious.
$(v i) \Rightarrow(i)$ : Assume that $(i v)$ holds. Let $A \subseteq S$. Since $S$ is an ordered $k$-duosemiring, $J_{k}(A)=L_{k}(A)=R_{k}(A)$. By assumption, we obtain

$$
A \subseteq J_{k}(A)=J_{k}(A) \cap J_{k}(A)=\overline{\left(J_{k}(A) J_{k}(A)\right]}=\overline{\left(R_{k}(A) L_{k}(A)\right]} .
$$

By Corollary 4.3, we get $S$ is ordered $k$-regular.

## References

[1] M. R. Adhikari, M. K. Sen and H. J. Weinert, On $k$-regular semirings, Bull. Calcutta Math. Soc. 88 (1996), $141-144$.
[2] A. K. Bhuniya and K. Jana, Bi-ideals in $k$-regular and intra $k$-regular semirings, Discuss. Math. Gen. Algebra Appl. 31 (2011), $5-23$.
[3] S. Bourne, The Jacobson radical of a semiring, Proc. Nati. Acad. Sci. USA 31 (1951), $163-170$.
[4] A. P. Gan and Y. L. Jiang, On ordered ideals in ordered semirings, J. Math. Res. Exposition 31 (2011), 989 - 996.
[5] K. Jana, Quasi $k$-ideals in $k$-regular and intra $k$-regular semirings, Pure. Math. Appl. 22 (2011), $65-74$.
[6] D. Mandal, Fuzzy ideals and fuzzy interior ideals in ordered semirings, Fuzzy Inf. Eng. 6 (2014), 101 - 114.
[7] J. von Neumann, On regular rings, Proc. Natl. Acad. Sci. USA 22 (1936), 707 713.
[8] P. Palakawong na Ayuthaya and B. Pibaljommee, Characterizations of regular ordered semirings by ordered quasi-ideals, Int. J. Math. Math. Sci. (2016), Article ID 4272451.
[9] S. Patchakhieo and B. Pibaljommee, Characterizations of ordered $k$-regular semirings by ordered $k$-ideals, Asian-Eur. J. Math. 10 (2017), Article ID 1750020.
[10] M. Shabir, A. Ali and S. Batool, A note on quasi-ideals in semirings, Southeast. Asian. Bull. Math. 27 (2004), $923-928$.
[11] O. Steinfeld, Über die quasiideale von halbgruppen. Publ. Math. Debrecan. 4 (1956), 262 - 275.
[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.

# Prime ordered $k$-bi-ideals in ordered semirings 

Permpoon Senarat and Bundit Pibaljommee


#### Abstract

Various types of ordered $k$-bi-ideals of ordered semirings are investigated. Several characterizations of ordered $k$-bi-idempotent semirings are presented.


## 1. Introduction

The notion of a semiring was introduced by Vandiver [8] as a generalization of a ring. Gan and Jiang [2] investigated an ordered semiring with zero and introduced several notions, for example, ordered ideals, minimal ideals and maximal ideals of an ordered semiring. Han, Kim and Neggers [3] investigated properties orders in a semiring. Henriksen [4] defined more restrict class of ideals in semiring known as $k$-ideals. Several characterizations of $k$-ideals of a semiring were obtained by Sen and Adhikari in [6, 7]. In [1], Akram and Dudek studied properties of intuinistic fuzzy left $k$-ideals of semirings. An ordered $k$-ideal in an ordered semiring was characterized by Patchakhieo and Pibaljommee [5].

In this paper, we introduce the notion of an ordered $k$-bi-ideal, a prime ordered $k$-bi-ideal, a strongly prime ordered $k$-bi-ideal, an irreducible and a strongly irreducible ordered $k$-bi-ideals of an ordered semiring. We introduce the concept of an ordered $k$-bi-idempotent semiring and characterize it using prime, strongly prime, irreducible and strongly irreducible ordered $k$-bi-ideals.

## 2. Preliminaries

A semiring is a triplet $(S,+, \cdot)$ consisting of a nonempty set $S$ and two operations + (addition) and $\cdot($ multiplication) such that $(S,+)$ is a commutative semigroup, $(S, \cdot)$ is a semigroup and $a \cdot(b+c)=a \cdot b+a \cdot c$ and $(a+b) \cdot c=a \cdot c+b \cdot c$ for all $a, b, c \in S$.

A semiring $(S,+, \cdot)$ is called a commutative if $(S, \cdot)$ is a commutative semigroup. An element $0 \in S$ is called a zero element if $a+0=0+a=a$ and $a \cdot 0=0=0 \cdot a$.

A nonempty subset $A$ of a semiring $(S,+, \cdot)$ is called a left (right) ideal of $S$ if $x+y \in A$ for all $x, y \in A$ and $S A \subseteq A(A S \subseteq A)$. We call $A$ an ideal of $S$ if it is both a left and a right ideal of $S$. A subsemiring $B$ of a semiring $S$ is called a bi-ideal of $S$ if $B S B \subseteq B$.

[^6]Let $(S, \leqslant)$ be a partially ordered set. Then $(S,+, \cdot, \leqslant)$ is called an ordered semiring if $(S,+, \cdot)$ is a semiring and the relation $\leqslant$ is compatible with the operations + and $\cdot$, i.e., if $a \leqslant b$, then $a+x \leqslant b+x, x+a \leqslant x+b, a x \leqslant b x$ and $x a \leqslant x b$ for all $a, b, x \in S$.

Let $(S,+, \cdot, \leqslant)$ be an ordered semiring. For nonempty subsets $A, B$ of $S$ and $a \in S$, we denote

$$
\begin{aligned}
(A] & =\{x \in S \mid x \leqslant a \text { for some } a \in A\} \\
A B & =\{x y \in S \mid x \in A, y \in B\} \\
\Sigma A & =\left\{\sum_{i \in I} a_{i} \in S \mid a_{i} \in A \text { and } I \text { is a finite subset of } \mathbb{N}\right\} \\
\Sigma A B & =\left\{\sum_{i \in I} a_{i} b_{i} \in S \mid a_{i} \in A, b_{i} \in B \text { and } I \text { is a finite subset of } \mathbb{N}\right\} \text { and } \\
\mathbb{N} a & =\{n a \in S \mid n \in \mathbb{N}\} .
\end{aligned}
$$

Instead of writing an ordered semiring $(S,+, \cdot, \leqslant)$, we simply denote $S$ as an ordered semiring.

A left (right) ideal $A$ of an ordered semiring $S$ is called a left (right) ordered ideal of $S$ if for any $x \leqslant a$ for some $a \in A$ implies $x \in A$. We call $A$ an ordered ideal if it is both a left and a right ordered ideal of $S$.

A left (right) ordered ideal of $A$ of a semiring $S$ is called a left (right) ordered $k$-ideal of $S$ if $x+a=b$ for some $a, b \in A$ implies $x \in A$. We call $A$ an ordered $k$-ideal of $S$ if it is both a left and a right ordered $k$-ideal of $S$.

The $k$-closure of a nonempty subset $A$ of an ordered semiring $S$ is defined by

$$
\bar{A}=\{x \in S \mid \exists a, b \in A, x+a \leqslant b\} .
$$

Now, we recall the results concerning to the $k$-closure given in [5].
Lemma 2.1. Let $S$ be an ordered semiring and $A, B$ be nonempty subsets of $S$.
(i) $(\bar{A}] \subseteq \overline{(A]}$.
(ii) If $A \subseteq B$, then $\bar{A} \subseteq \bar{B}$.
(iii) $\overline{(A]} B \subseteq \overline{(A B]}$ and $\overline{A(B]} \subseteq \overline{(A B]}$.

Lemma 2.2. Let $A$ be a nonempty subset of an ordered semiring $S$. If $A$ is closed under addition, then $(A]$ and $\overline{(A]}$ are also closed.

Lemma 2.3. Let $S$ be an ordered semiring and $A, B$ be nonempty subsets of $S$ with $A+A \subseteq A$ and $B+B \subseteq B$. Then
(i) $A \subseteq(A] \subseteq \bar{A} \subseteq \overline{(A]}$;
(ii) $\overline{(A]}=\overline{\overline{(A]}}$;
(iii) $A+B \subseteq \bar{A}+\bar{B} \subseteq \overline{A+B}$;
(iv) $\overline{(A]}+\overline{(B]} \subseteq \overline{\overline{(A]}+\overline{(B)}} \subseteq \overline{(A+B]}$;
(v) $\bar{A} \bar{B} \subseteq \overline{(A]} \overline{(B]} \subseteq \overline{(\Sigma A B]}$;
(vi) $A(\Sigma B) \subseteq \Sigma A B$ and $(\Sigma A) B \subseteq \Sigma A B$.

Lemma 2.4. Let $S$ be an ordered semiring and $A$ be a nonempty subset of $S$ with $A+A \subseteq A$. Then $\overline{(\overline{(A]}]}=\overline{(A]}$.

Theorem 2.5. Let $S$ be an ordered semiring and $A$ be a left ideal (resp. right ideal, ideal). Then the following conditions are equivalent:
( $i$ ) $A$ is a left ordered $k$-ideal (resp. right ordered $k$ - ideal, ordered $k$-ideal) of $S$;
(ii) if $x \in S, x+a \leqslant b$ for some $a, b \in A$, then $x \in A$;
(iii) $\bar{A}=A$.

Theorem 2.6. Let $S$ be an ordered semiring and $A$ be a nonempty subset of $S$. If $A$ is a left ideal (resp. right ideal, ideal), then $\overline{(A]}$ is the smallest left ordered $k$-ideal (resp. right ordered $k$-ideal, ordered $k$-ideal) containing $A$.

From Theorem 2.6, we have $A$ is an ordered $k$-ideal if and only if $\overline{(A]}=A$.
Theorem 2.7. Let $S$ be an ordered semiring. If the intersection of a family of left ordered $k$-ideals (resp. right ordered $k$-ideal, ordered $k$-ideal) is not empty, then it is a left ordered $k$-ideal (resp. right ordered $k$-ideal, ordered $k$-ideal).

For a nonempty subset $A$ of an ordered semiring $S$, we denote by $L_{k}(A), R_{k}(A)$ and $M_{k}(A)$ the smallest left ordered $k$-ideal, the smallest right ordered $k$-ideal and the smallest ordered $k$-ideal of $S$ containing $A$, respectively. For any $a \in S$, we denote $L_{k}(a)=L_{k}(\{a\}), R_{k}(a)=R_{k}(\{a\})$ and $M_{k}(a)=M_{k}(\{a\})$.

Theorem 2.8. Let $S$ be an ordered semiring and $a \in S$. Then
(i) $L_{k}(A)=\overline{(\Sigma A+\Sigma S A]}$;
(ii) $R_{k}(A)=\overline{(\Sigma A+\Sigma A S]}$;
(iii) $M_{k}(a)=\overline{(\Sigma A+\Sigma S A+\Sigma A S+\Sigma S A S]}$.

Corollary 2.9. Let $S$ be an ordered semiring and $a \in S$. Then
(i) $L_{k}(a)=\overline{(\mathbb{N} a+S a]}$;
(ii) $R_{k}(a)=\overline{(\mathbb{N} a+a S]}$;
(iii) $M_{k}(a)=\overline{(\mathbb{N} a+S a+S a+\Sigma S a S]}$.

## 3. Prime ordered $k$-bi-ideals

First, we begin with the definition of an ordered $k$-bi-ideal of an ordered semiring and give some concepts in ordered semirings that we need in this section.

Definition 3.1. An ordered subsemiring $B$ of an ordered semiring $S$ is said to be an ordered $k$-bi-ideal of $S$ if
(i) $B S B \subseteq B$;
(ii) if $x \in S, a+x=b$ for some $a, b \in B$, then $x \in B$;
(iii) if $x \in S, x \leqslant b$ for some $b \in B$, then $x \in B$.

We note that every right ordered $k$-ideal or left ordered $k$-ideal is an ordered $k$-bi-ideal of $S$.
Example 3.2. Let $S=\{A, B, C, D, E, F\}$, where $A=\left[\begin{array}{c}\emptyset \\ \emptyset \\ \emptyset \\ \emptyset\end{array}\right], B=\left[\begin{array}{cc}\{1\} & \emptyset \\ \emptyset & \emptyset\end{array}\right]$, $C=\left[\begin{array}{cc}\{1\} & \{1\} \\ \emptyset & \emptyset\end{array}\right], D=\left[\begin{array}{cc}\{1\} & \emptyset \\ \{1\} & \emptyset\end{array}\right], E=\left[\begin{array}{cc}\{1\} & \{1\} \\ \{1\} & \emptyset\end{array}\right], F=\left[\begin{array}{ll}\{1\} & \{1\} \\ \{1\} & \{1\}\end{array}\right]$.
We defined operations + and $\cdot$ on $S$ by letting $U=\left[\begin{array}{ll}a_{1} & a_{2} \\ a_{3} & a_{4}\end{array}\right], V=\left[\begin{array}{ll}b_{1} & b_{2} \\ b_{3} & b_{4}\end{array}\right]$

$$
\begin{aligned}
U+V & =\left[\begin{array}{l}
a_{1} \cup b_{1} a_{2} \cup b_{2} \\
a_{3} \cup b_{3} a_{4} \cup b_{4}
\end{array}\right] \quad \text { and } \\
U \cdot V & =\left[\begin{array}{l}
\left(a_{1} \cap b_{1}\right) \cup\left(a_{2} \cap b_{3}\right)\left(a_{1} \cap b_{2}\right) \cup\left(a_{2} \cap b_{4}\right) \\
\left(a_{3} \cap b_{1}\right) \cup\left(a_{4} \cap b_{3}\right)\left(a_{3} \cap b_{2}\right) \cup\left(a_{4} \cap b_{4}\right)
\end{array}\right] .
\end{aligned}
$$

The tables of both operations are shown as follows.

| + | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $A$ | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ |
| $B$ | $B$ | $B$ | $C$ | $D$ | $E$ | $F$ |
| $C$ | $C$ | $C$ | $C$ | $E$ | $E$ | $F$ |
| $D$ | $D$ | $D$ | $E$ | $D$ | $E$ | $F$ |
| $E$ | $E$ | $E$ | $E$ | $E$ | $E$ | $F$ |
| $F$ | $F$ | $F$ | $F$ | $F$ | $F$ | $F$ |


| $\cdot$ | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $A$ | $A$ | $A$ | $A$ | $A$ | $A$ | $A$ |
| $B$ | $A$ | $B$ | $B$ | $D$ | $D$ | $D$ |
| $C$ | $A$ | $C$ | $C$ | $F$ | $F$ | $F$ |
| $D$ | $A$ | $B$ | $B$ | $D$ | $D$ | $D$ |
| $E$ | $A$ | $C$ | $C$ | $F$ | $F$ | $F$ |
| $F$ | $A$ | $C$ | $C$ | $F$ | $F$ | $F$ |

We defined a partially ordered relation $\leqslant$ on $L$ by

$$
U \leqslant V \text { if and only if } a_{1} \subseteq b_{1}, a_{2} \subseteq b_{2}, a_{3} \subseteq b_{3} \text { and } a_{4} \subseteq b_{4} .
$$

Then $A \leqslant B \leqslant C \leqslant E \leqslant F$ and $A \leqslant B \leqslant D \leqslant E \leqslant F$.
We can see that $(S,+, \cdot, \leqslant)$ is an ordered semiring and $T=\{A\}$ is its ordered $k$-ideal, $Y=\{A, B, C\}$ is a left ordered $k$-ideal but not a right ordered $k$-ideal, $Z=\{A, B, D\}$ is a right ordered $k$-ideal but not a left ordered $k$-ideal and $X=$ $\{A, B\}$ is an ordered $k$-bi-ideal but not a left or a right ordered $k$-ideal.

Theorem 3.3. Let $B$ be a bi-ideal of an ordered semiring S. Then the following statements are equivalent.
(i) $B$ is an ordered $k$-bi-ideal of $S$.
(ii) If $a+x \leqslant b$ for some $a, b \in B$, then $x \in B$.
(iii) $\bar{B}=B$.

Proof. $(i) \Rightarrow(i i)$ : Let $B$ be an ordered $k$-bi-ideal of $S$. If $x+a \leqslant b$ for some $a, b \in B$ and $x \in S$. Then $x+a \in B$. It follows that there exists $p \in B$ such that $x+a=p$. By assumption, $x \in B$.
(ii) $\Rightarrow($ iii $)$ : Let $x \in \bar{B}$. Then there exist $a, b \in B$ such that $x+a \leqslant b$. By assumption, we have $x \in B$. Thus, $\bar{B}=B$.
(iii) $\Rightarrow(i)$ : Assume that $\bar{B}=B$. Let $x \in S$ such that $x+a=b$ for some $a, b \in B$. Then $x \in \bar{B}$. By assumption, we have $x \in B$. By Lemma 2.3(i), $(B] \subseteq \bar{B}=B$. Altogether, $B$ is an ordered $k$-bi-ideal of $S$.

Theorem 3.4. Let $B$ be a bi-ideal of an ordered semiring $S$. Then $\overline{(B]}$ is the smallest ordered $k$-bi-ideal of $S$ containing $B$.
Proof. It is clear that $B \subseteq \overline{(B]}$. By Lemma $2.2, \overline{(B]}$ is closed under addition. By Lemma $2.1($ iii $)$ and Lemma 2.4, we have $\overline{(B)} \overline{(B]} \subseteq \overline{(\overline{(B]} B]} \subseteq \overline{(\overline{(B B]}]} \subseteq \overline{(\overline{(B]]})}=$ $\overline{(B]}$. By Lemma $2.1(i i i), \overline{(B]} \overline{S(B]} \subseteq \overline{(\Sigma B S B]} \subseteq \overline{(B]}$. Thus, $\overline{(B]}$ is a bi-ideal of $S$. By Lemma 2.3(ii), we have $\overline{(B]}=\overline{(B]}$. By Theorem 3.3, $\overline{(B]}$ is an ordered $k$-biideal of $S$. Let $K$ be an ordered $k$-bi-ideal of $S$ containing $B$. Then $(B] \subseteq(K]=K$ and $\overline{(B]} \subseteq \bar{K}=K$. Then $\overline{(B]}$ is the smallest ordered $k$-bi-ideal of $S$ containing $B$.

Corollary 3.5. A bi-ideal $B$ of an ordered semiring $S$ is an ordered $k$-bi-ideal if and only if $\overline{(B]}=B$.

Theorem 3.6. If intersection of a family of ordered $k$-bi-ideals of an ordered semiring $S$ is not empty, then it is an ordered $k$-bi-ideal of $S$.
Definition 3.7. An ordered $k$-bi-ideal $B$ of $S$ is called a semiprime ordered $k$-biideal if $\overline{\left(\Sigma A^{2}\right]} \subseteq B$ implies $A \subseteq B$ for any ordered $k$-bi-ideal $A$ of $S$.

Definition 3.8. An ordered $k$-bi-ideal $B$ of $S$ is called a prime ordered $k$-bi-ideal if $\overline{(\Sigma A C]} \subseteq B$ implies $A \subseteq B$ or $C \subseteq B$ for any ordered $k$-bi-ideal $A, C$ of $S$.

Definition 3.9. An ordered $k$-bi-ideal $B$ of $S$ is called a strongly prime ordered $k$ -bi-ideal if $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]} \subseteq B$ implies $A \subseteq B$ or $C \subseteq B$ for any ordered $k$-bi-ideal $A, C$ of $S$.

Obviously, every strongly prime ordered $k$-bi-ideal of $S$ is a prime ordered $k$ -bi-ideal and every prime ordered $k$-bi-ideal of $S$ is a semiprime ordered $k$-bi-ideal.

The following example shows that every prime ordered $k$-bi-ideal need not to be a strongly prime ordered $k$-bi-ideal.

Example 3.10. Let $S=\{a, b, c\}$. We define operations + and $\cdot$ on $S$ as the following tables.

| + | $a$ | $b$ | $c$ |
| :---: | :---: | :---: | :---: |
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $b$ | $c$ |
| $c$ | $c$ | $c$ | $c$ |

and

| $\cdot$ | $a$ | $b$ | $c$ |
| :---: | :---: | :---: | :---: |
| $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ | $b$ |
| $c$ | $a$ | $c$ | $c$ |

We defined a partially ordered relation $\leqslant$ on $S$ by $\leqslant:=\{(a, a),(b, b),(c, c),(a, b)\}$.
We can show that $(S,+, \cdot, \leqslant)$ is an ordered semiring and $\{a\},\{a, b\},\{a, c\}$ and $S$ are all ordered $k$-bi-ideals of $S$. Now, we have $\{a\}$ is prime but not strongly prime, since $\overline{(\Sigma\{a, b\}\{a, c\}]} \cap \overline{(\Sigma\{a, c\}\{a, b\}]}=\{a\}$ but $\{a, b\} \nsubseteq\{a\}$ and $\{a, c\} \nsubseteq\{a\}$.

Example 3.11. Let $S=\{a, b, c, d, e, f\}$. We define operations + and $\cdot$ on $S$ as the following tables.

| + | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |  |
| :---: | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| $a$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |  |
| $b$ | $b$ | $b$ | $c$ | $d$ | $e$ | $f$ |  |
| $c$ | $c$ | $c$ | $c$ | $e$ | $e$ | $f$ | and |
| $d$ | $d$ | $d$ | $e$ | $d$ | $e$ | $f$ |  |
| $e$ | $e$ | $e$ | $e$ | $e$ | $e$ | $f$ |  |
| $f$ | $f$ | $f$ | $f$ | $f$ | $f$ | $f$ |  |


| $\cdot$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $a$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $a$ | $a$ | $b$ | $b$ | $c$ |
| $c$ | $a$ | $b$ | $c$ | $b$ | $c$ | $c$ |
| $d$ | $a$ | $a$ | $a$ | $d$ | $d$ | $f$ |
| $e$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
| $f$ | $a$ | $d$ | $f$ | $d$ | $f$ | $f$ |

We defined a partially ordered relation $\leqslant$ on $S$ by

$$
\begin{aligned}
\leqslant:=\{ & (a, a),(b, b),(c, c),(d, d),(e, e),(f, f),(a, b),(a, c),(a, d),(a, e), \\
& (b, c),(b, d),(b, e),(c, e),(d, e)\} .
\end{aligned}
$$

The sets $T=\{a\}, X=\{a, b\}, Y=\{a, b, c\}, Z=\{a, b, d\}$ and $S$ are all ordered $k$-bi-ideals of $S$. We find that $Y, Z$ and $S$ are strongly prime ordered $k$-bi-ideals, $X$ is a semiprime ordered $k$-bi-ideal but not prime and $T$ is not a semiprime ordered $k$-bi-ideal.

Definition 3.12. An ordered $k$-bi-ideal $B$ of $S$ is called an irreducible ordered $k$-bi-ideal if for any ordered $k$-bi-ideal $A$ and $C$ of $S, A \cap C=B$ implies $A=B$ or $C=B$.

Definition 3.13. An ordered $k$-bi-ideal $B$ of $S$ is called a strongly irreducible ordered $k$-bi-ideal if for any ordered $k$-bi-ideal $A$ and $C$ of $S, A \cap C \subseteq B$ implies $A \subseteq B$ or $C \subseteq B$.

It is clear that every strongly irreducible ordered $k$-bi-ideal of $S$ is an irreducible ordered $k$-bi-ideal of $S$.

Theorem 3.14. If intersection of any family of prime ordered $k$-bi-ideals (or semiprime ordered $k$-bi-ideals) of $S$ is not empty, then it is a semiprime ordered $k$-bi-ideal.

Proof. Let $\left\{K_{i} \mid i \in I\right\}$ be a family of prime ordered $k$-bi-ideals of $S$. Assume that $\bigcap_{i \in I} K_{i} \neq \emptyset$. For any ordered $k$-bi-ideal $B$ of $S, \overline{\left(\Sigma B^{2}\right]} \subseteq \bigcap_{i \in I} K_{i}$ implies $\overline{\left(\Sigma B^{2}\right]} \subseteq K_{i}$ for all $i \in I$. Since $K_{i}$ are prime ordered $k$-bi-ideals, $B \subseteq K_{i}$ for all $i \in I$. Hence, $B \subseteq \bigcap_{i \in I} K_{i}$. Thus, $\bigcap_{i \in I} K_{i}$ is semiprime.

Theorem 3.15. If $B$ is a strongly irreducible and semiprime ordered $k$-bi-ideal of an ordered semiring $S$, then $B$ is a strongly prime ordered $k$-bi-ideal of $S$.

Proof. Let $B$ be a strongly irreducible and semiprime ordered $k$-bi-ideal of $S$. Let $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]} \subseteq B$ for any ordered $k$-bi-ideals $A$ and $C$ of $S$. Since $\overline{\left(\Sigma(A \cap C)^{2}\right]} \subseteq$ $\overline{(\Sigma A C]}$ and $\overline{\left(\Sigma(A \cap C)^{2}\right]} \subseteq \overline{(\Sigma C A]}$. We have $\overline{\left(\Sigma(A \cap C)^{2}\right]} \subseteq \overline{(\Sigma A C]} \cap \overline{(\Sigma C A]}$. Since $A \cap C$ is an ordered $k$-bi-ideal and $B$ is a semiprime ordered $k$-bi-ideal, $A \cap C \subseteq B$. Since $B$ is a strongly irreducible ordered $k$-bi-ideal, $A \subseteq B$ or $C \subseteq B$. Thus, $B$ is a strongly prime ordered $k$-bi-ideal of $S$.

Theorem 3.16. If $B$ is an ordered $k$-bi-ideal of an ordered semiring $S$ and $a \in S$ such that $a \notin B$, then there exists an irreducible ordered $k$-bi-ideal I of $S$ such that $B \subseteq I$ and $a \notin I$.

Proof. Let $\mathcal{K}$ be the set of all ordered $k$-bi-ideals of $S$ containing $B$ but not containing $a$. Then $\mathcal{K}$ is a nonempty set, since $B \in \mathcal{K}$. Clearly, $\mathcal{K}$ is a partially ordered set under the inclusion of sets. Let $\mathcal{H}$ be a chain subset of $\mathcal{K}$. Then $\cup \mathcal{H} \in \mathcal{K}$. By Zorn's Lemma, there exists a maximal element in $\mathcal{K}$. Let $I$ be a maximal element in $\mathcal{K}$. Let $A$ and $C$ be any two ordered $k$-bi-ideals of $S$ such that $A \cap C=I$. Suppose that $I \subset A$ and $I \subset C$. Since $I$ is a maximal element in $\mathcal{K}$, we have $a \in A$ and $a \in C$. Then $a \in A \cap C=I$ which is a contradiction. Thus, $C=I$ or $A=I$. Therefore, $I$ is an irreducible ordered $k$-bi-ideal.

Theorem 3.17. A prime ordered $k$-bi-ideal $B$ of an ordered semiring $S$ is a prime one sided ordered $k$-ideal of $S$.

Proof. Let $B$ be a prime ordered $k$-bi-ideal of $S$. Suppose $B$ is not a one sided ordered $k$-ideal of $S$. It follows $\overline{(B S]} \nsubseteq B$ and $\overline{(B S]} \nsubseteq B$. Then $\overline{(\Sigma B S]} \nsubseteq B$ and $\overline{(\Sigma S B]} \nsubseteq B$. Since $B$ is a prime ordered $k$-bi-ideal, $\overline{(\Sigma \overline{(\Sigma B S]} \overline{(\Sigma S B]}]} \nsubseteq B$. By Lemma 2.3(v),

$$
\begin{aligned}
\overline{(\Sigma \overline{(\Sigma B S]} \overline{(\Sigma S B]}]} & \subseteq \overline{\Sigma \overline{\Sigma(\Sigma B S)(\Sigma S B)]}]} \subseteq \overline{\Sigma \overline{\Sigma(\Sigma B S S B)]}]} \\
& \subseteq \overline{\Sigma \overline{(\Sigma B S S B)]}]} \subseteq \overline{\Sigma \overline{(\Sigma B)]}]} \subseteq \overline{(\Sigma B]}=B
\end{aligned}
$$

This is a contradiction. Therefore, $\overline{(\Sigma B S]} \subseteq B$ or $\overline{(\Sigma S B]} \subseteq B$. Thus, $B$ is a prime one sided ordered $k$-ideal of $S$.

Theorem 3.18. Let $B$ be an ordered $k$-bi-ideal of an ordered semiring $S$. Then $B$ is prime if and only if for a right ordered $k$-ideal $R$ and a left ordered $k$-ideal $L$ of $S, \overline{(\Sigma R L]} \subseteq B$ implies $R \subseteq B$ or $L \subseteq B$.

Proof. Assume that $B$ is a prime ordered $k$-bi-ideal of $S$. Let $R$ be a right ordered $k$-ideal and $L$ be a left ordered $k$-ideal of $S$ such that $\overline{(\Sigma R L]} \subseteq B$. Since $R$ and $L$ are ordered $k$-bi-ideals of $S, R \subseteq B$ or $L \subseteq B$. Conversely, let $A$ and $C$ be any two ordered $k$-bi-ideals of $S$ such that $\overline{(\Sigma A C]} \subseteq B$. Suppose that $C \nsubseteq \underline{B}$. Let $a \in A$ and $c \in C \backslash B$. Then $\overline{(\mathbb{N} a+a S]} \subseteq A$ and $\overline{(\mathbb{N} c+S c]} \subseteq C$. We have $\overline{(\Sigma \overline{(\mathbb{N} a+a S]} \overline{(\mathbb{N} c+S c]}]} \subseteq \overline{(\Sigma A C]} \subseteq B$. By assumption, $\overline{(\mathbb{N} a+a S]} \subseteq B$ or $\overline{(\mathbb{N} c+S c]} \subseteq B$. But $\overline{(\mathbb{N} c+S c]} \nsubseteq B$ implies that $\overline{(\mathbb{N} a+a S]} \subseteq B$. Then $\bar{a} \in B$. Thus, $A \subseteq B$ and $B$ is a prime ordered $k$-bi-ideal of $S$.

## 4. Fully ordered $k$-bi-idempotent semirings

In this section, we assume that $S$ is an ordered semiring with zero.
Definition 4.1. An ordered semiring $S$ is said to be fully ordered $k$-bi-idempotent if $\overline{\left(\Sigma B^{2}\right]}=B$ for any ordered $k$-bi-ideal $B$ of $S$.

Example 4.2. The ordered semiring $S$ defined in Example 3.2 is fully ordered $k$-bi-idempotent. The ordered semiring $S$ defined in Example 3.11 is not fully ordered $k$-bi-idempotent, since $\overline{\left(\Sigma X^{2}\right]}=T \neq X$.

Theorem 4.3. Let $S$ be an ordered semiring. Then the following statements are equivalent.
(i) $S$ is fully ordered $k$-bi-idempotent.
(ii) $A \cap C=\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]}$ for any ordered $k$-bi-ideal $A$ and $C$ of $S$.
(iii) Each ordered $k$-bi-ideal of $S$ is semiprime.

Proof. $(i) \Rightarrow(i i)$ : Assume that $\overline{\left(\Sigma B^{2}\right]}=B$ for any ordered $k$-bi-ideal $B$ of $S$. Let $A$ and $C$ be any two ordered $k$-bi-ideals of $S$. By Theorem 3.6, $A \cap C$ is an ordered $k$-bi-ideal of $S$. By assumption, $A \cap C=\overline{\left(\Sigma(A \cap C)^{2}\right]}=\overline{(\Sigma(A \cap C)(A \cap C)]} \subseteq$ $\overline{(\Sigma A C]}$. Similarly, we get $A \cap C \subseteq \overline{(\Sigma C A]}$. Therefore, $A \cap C \subseteq \overline{(\Sigma A C]} \cap \overline{(\Sigma C A]}$. Since $\Sigma A C$ is closed under addition, by Lemma $2.2, \overline{(\Sigma A C]}$ is also closed under addition. By Lemma 2.3(vi),

$$
(\Sigma A C)(\Sigma A C) \subseteq \Sigma A C A C \subseteq \Sigma A S A C \subseteq \Sigma A C
$$

Then $\Sigma A C$ is an ordered subsemiring of $S$. By Lemma 2.3(vi),

$$
(\Sigma A C) S(\Sigma A C) \subseteq(\Sigma A C S)(\Sigma A C) \subseteq \Sigma A C S A C \subseteq \Sigma A S S A C \subseteq \Sigma A S A C \subseteq \Sigma A C
$$

Thus, $\Sigma A C$ is a bi-ideal of $S$. By Theorem $3.4, \overline{(\Sigma A C]}$ is an ordered $k$-bi-ideal of $S$. Similarly, $\overline{(\Sigma C A]}$ is an ordered $k$-bi-ideal. By Theorem 3.6, $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]}$ is an ordered $k$-bi-ideal of $S$. By assumption, Lemma $2.3(v),(v i)$ and Lemma 2.4, we have

$$
\begin{aligned}
\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]} & =\overline{(\Sigma(\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]})(\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]})]} \\
& \subseteq \overline{(\Sigma \overline{(\Sigma A C]} \overline{(\Sigma C A]}]} \subseteq \overline{(\Sigma \overline{(\Sigma A C C A]}]} \subseteq \overline{(\Sigma \overline{(\Sigma A S A]}]} \subseteq A .
\end{aligned}
$$

Similarly, we can show that $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]} \subseteq C$. Thus, $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]} \subseteq A \cap C$. Hence, $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]}=A \cap C$.
$(i i) \Rightarrow(i i i)$ : Let $B$ be an ordered $k$-bi-ideal of $S$. Suppose that $\overline{\left(\Sigma A^{2}\right]} \subseteq B$ for any ordered $k$-bi-ideal $A$ of $S$. By assumption, we have $A=A \cap A=\overline{(\Sigma A A]} \cap$ $\overline{(\Sigma A A]}=\overline{(\Sigma A A]} \subseteq B$. Hence, $B$ is semiprime.
(iii) $\Rightarrow(i)$ : Let $B$ be an ordered $k$-bi-ideal of $S$. Since $\overline{\left(\Sigma B^{2}\right]}$ is an ordered $k$-bi-ideal, by assumption, $\overline{\left(\Sigma B^{2}\right]}$ is semiprime. Since $\overline{\left(\Sigma B^{2}\right]} \subseteq \overline{\left(\Sigma B^{2}\right]}, B \subseteq \overline{\left(\Sigma B^{2}\right]}$. Clearly, $\overline{\left(\Sigma B^{2}\right]} \subseteq B$. This shows that $S$ is ordered $k$-bi-idempotent.

Theorem 4.4. Let $S$ be a fully ordered $k$-bi-idempotent semiring and $B$ be an ordered $k$-bi-ideal of $S$. Then $B$ is strongly irreducible if and only if $B$ is strongly prime.

Proof. Assume that $B$ is strongly irreducible. Let $A$ and $C$ be any two ordered $k$ -bi-ideals of $S$ such that $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]} \subseteq B$. By Theorem 4.3, $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]}=$ $A \cap C$. Hence, $A \cap C \subseteq B$. By assumption, we have $A \subseteq B$ or $C \subseteq B$. Thus, $B$ is a strongly prime ordered $k$-bi-ideal of $S$. Conversely, assume that $B$ is strongly prime. Let $A$ and $C$ be any two ordered $k$-bi-ideals of $S$ such that $A \cap C \subseteq B$. By Theorem 4.3, $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]}=A \cap C \subseteq B$. By assumption, we have $A \subseteq B$ or $C \subseteq B$. Thus, $B$ is a strongly irreducible ordered $k$-bi-ideal of $S$.

Theorem 4.5. Every ordered $k$-bi-ideal of an ordered semiring $S$ is a strongly prime ordered $k$-bi-ideal if and only if $S$ is a fully ordered $k$-bi-idempotent semiring and the set of all ordered $k$-bi-ideals of $S$ is totally ordered.

Proof. Assume that every ordered $k$-bi-ideal of $S$ is strongly prime. Then every ordered $k$-bi-ideal of $S$ is semiprime. By Theorem 4.3, $S$ is a fully ordered $k$ -bi-idempotent semiring. Let $A$ and $C$ be any two ordered $k$-bi-ideals of $S$. By Theorem 3.6, $A \cap C$ is an ordered $k$-bi-ideal of $S$. By assumption, $A \cap C$ is a strongly prime ordered $k$-bi-ideal of $S$. By Theorem 4.3, $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]}=A \cap C$. Then $A \subseteq A \cap C$ or $C \subseteq A \cap C$. Therefore, $A=A \cap C$ or $C=A \cap C$. Thus, $A \subseteq C$ or $C \subseteq A$. Conversely, assume that $S$ is a fully ordered $k$-bi-idempotent semiring and the set of all ordered $k$-bi-ideals of $S$ is a totally ordered set. Let $B$ be any ordered $k$-bi-ideal of $S$. Let $A$ and $C$ be any two ordered $k$-bi-ideals of $S$ such that $\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]} \subseteq B$. By Theorem 4.3, $A \cap C=\overline{(\Sigma A C]} \cap \overline{(\Sigma C A]} \subseteq B$. By assumption, $A \subseteq C$ or $C \subseteq A$. Hence, $A \cap C=A$ or $A \cap C=C$. Thus, $A \subseteq B$ or $C \subseteq B$. Therefore, $B$ is a strongly prime ordered $k$-bi-ideal of $S$.

Since every strongly prime ordered $k$-bi-ideal is a prime ordered $k$-bi-ideal and by Theorem 4.3 and 4.5 , we have the following corollary.

Corollary 4.6. Let the set of all ordered $k$-bi-ideals of $S$ be a totally ordered set under inclusion of sets. Then every ordered $k$-bi-ideal of $S$ is strongly prime if and only if every ordered $k$-bi-ideal of $S$ is prime.

Theorem 4.7. If the set of all ordered $k$-bi-ideals of an ordered semiring $S$ is a totally ordered set under inclusion of sets, then $S$ is a fully ordered $k$-bi-idempotent if and only if each ordered $k$-bi-ideal of $S$ is prime.
Proof. Assume that $S$ is a fully ordered $k$-bi-idempotent semiring. Let $B$ be any ordered $k$-bi-ideal of $S$ and $A, C$ be any two ordered $k$-bi-ideals of $S$ such that $\overline{(\Sigma A C]} \subseteq B$. By assumption, we have $A \subseteq C$ or $C \subseteq A$. Without loss of generality, suppose that $A \subseteq C$. Then $A=\overline{(\Sigma A A]} \subseteq \overline{(\Sigma A C]} \subseteq B$. Hence, $B$ is a prime ordered $k$-bi-ideal of $S$. Conversely, assume that every ordered $k$-bi-ideal of $S$ is prime. Then every ordered $k$-bi-ideal of $S$ is semiprime. By Theorem 4.3, $S$ is a fully ordered $k$-bi-idempotent semiring.

Theorem 4.8. If $S$ is a fully ordered $k$-bi-idempotent semiring and $B$ is a strongly irreducible ordered $k$-bi-ideal of $S$, then $B$ is a prime ordered $k$-bi-ideal.

Proof. Let $B$ be a strongly irreducible ordered $k$-bi-ideal of a fully ordered $k$-biidempotent semiring $S$. Let $A$ and $C$ be any two ordered $k$-bi-ideals of $S$ such that $\overline{(\Sigma A C]} \subseteq B$. Since $A \cap C$ is also an ordered $k$-bi-ideal of $S$. By assumption, $\overline{\overline{\left(\Sigma(A \cap C)^{2}\right]}}=A \cap C$. Consider $A \cap C=\overline{\left(\Sigma(A \cap C)^{2}\right]}=\overline{(\Sigma(A \cap C)(A \cap C)]} \subseteq$ $\overline{(\Sigma(A C]} \subseteq B$. Since $B$ is a strongly irreducible ordered $k$-bi-ideal of $S, A \subseteq B$ or $C \subseteq B$. Hence, $B$ is a prime ordered $k$-bi-ideal of $S$.

## 5. Right ordered $k$-weakly regular semirings

First, we recall the definition of a right ordered $k$-weakly regular semiring and some of its properties given by Patchakhieo and Pibaljommee [5] which we need to use in this section. Then we give characterizations of right ordered $k$-weakly regular semirings using ordered $k$-bi-ideals.

An ordered semiring $S$ is said to be a right ordered $k$-weakly regular semiring if $a \in \overline{\left(\Sigma(a S)^{2}\right]}$ for all $a \in S$.

Theorem 5.1. Let $S$ be an ordered semiring. Then the following statements are equivalent.
(i) $S$ is a right ordered $k$-weakly regular.
(ii) $\overline{\left(\Sigma A^{2}\right]}=A$ for every right ordered $k$-ideal $A$ of $S$.
(iii) $A \cap I=\overline{(\Sigma A I]}$ for every right ordered $k$-ideal $A$ of $S$ and every ordered $k$-ideal I of $S$.

Theorem 5.2. An ordered semiring $S$ is right ordered $k$-weakly regular if and only if $B \cap I \subseteq \overline{(\Sigma B I]}$ for any ordered $k$-bi-ideal $B$ and ordered $k$-ideal $I$ of $S$.

Proof. Let $S$ be a right ordered $k$-weakly regular semiring, $B$ be an ordered $k$-biideal and $I$ be an ordered $k$-ideal of $S$. Let $a \in B \cap I$. By Lemma 2.1(iii), Lemma $2.3(v)$ and Lemma 2.4, we have

$$
\begin{aligned}
& a \in \overline{\left(\Sigma(a S)^{2}\right]}=\overline{(\Sigma(a S)(a S)]} \subseteq \overline{(\Sigma(a S) \overline{(\Sigma(a S)(a S)]} S]} \subseteq \overline{(\Sigma \overline{((a S)(\Sigma(a S)(a S)) S]}]} \\
& \subseteq \overline{(\Sigma \overline{(\Sigma(a S a)(S a S S)]}]} \subseteq \overline{(\overline{(\Sigma(B S B)(S I S)]}]} \subseteq \overline{(\overline{(\Sigma B I]}]}=\overline{(\Sigma B I]} .
\end{aligned}
$$

Therefore, $B \cap I \subseteq \overline{(\Sigma B I]}$.
Conversely, assume that $B \cap I \subseteq \overline{(\Sigma B I]}$ for any ordered $k$-bi-ideal $B$ and ordered $k$-ideal $I$ of $S$. Let $R$ be a right ordered $k$-ideal of $S$. Then $R$ is an ordered $k$ -bi-ideal of $S$. By assumption, Lemma 2.8, Lemma 2.1(iii), Lemma 2.3(vi) and Lemma 2.4, we have

$$
\begin{aligned}
R & =R \cap M_{k}(R) \\
& \subseteq \overline{\left(\Sigma R M_{k}(R)\right]}=\overline{(\Sigma R \overline{(\Sigma R+\Sigma R S+\Sigma S R+\Sigma S R S]}]} \\
& \subseteq \overline{\left(\Sigma \overline{\left(\Sigma R^{2}+\Sigma R^{2} S+\Sigma R S R+\Sigma R S R S\right]}\right]} \\
& \subseteq \overline{\left(\Sigma R^{2}+\Sigma R^{2}+\Sigma R^{2}+\Sigma R^{2}\right]} \\
& =\overline{\left(\Sigma R^{2}\right]} .
\end{aligned}
$$

Then $R=\overline{\left(\Sigma R^{2}\right]}$. Thus, by Theorem 5.1, $S$ is a right ordered $k$-weakly regular semiring.

Theorem 5.3. An ordered semiring $S$ is right ordered $k$-weakly regular if and only if $B \cap I \cap R \subseteq \overline{(\Sigma B I R]}$ for any ordered $k$-bi-ideal $B$, ordered $k$-ideal $I$ and right ordered $k$-ideal $R$ of $S$.

Proof. Let $S$ be a right ordered $k$-weakly regular semiring, $B$ be an ordered $k$ -bi-ideal, $I$ be an ordered $k$-ideal and $R$ be a right ordered $k$-ideal of $S$. Let $a \in B \cap I \cap R$. By assumption, Lemma 2.1(iii), Lemma 2.3(vi) and Lemma 2.4, we have

$$
\begin{aligned}
a \in \overline{\left(\Sigma(a S)^{2}\right]} & =\overline{(\Sigma(a S)(a S)]} \subseteq \overline{(\Sigma(a S) \overline{(\Sigma(a S)(a S)]} S]} \\
& \subseteq \overline{(\Sigma \overline{(\Sigma a(S a S)(a S)]}]} \subseteq \overline{(\overline{(\Sigma B I R]}]}=\overline{(\Sigma B I R]}
\end{aligned}
$$

Therefore, $B \cap I \cap R \subseteq \overline{(\Sigma B I R]}$.
Conversely, assume that $B \cap I \cap R \subseteq \overline{(\Sigma B I R]}$ for any ordered $k$-bi-ideal $B$, ordered $k$-ideal $I$ and right ordered $k$-ideal $R$ of $S$. Since $R$ is an ordered $k$-biideal of $S$ and $S$ is also an ordered $k$-ideal of $S$. By assumption, $R=R \cap S \cap R \subseteq$ $\overline{(\Sigma R S R]} \subseteq \overline{\left(\Sigma R^{2}\right]}$. Therefore, $R=\overline{\left(\Sigma R^{2}\right]}$. By Theorem 5.1, $S$ is right ordered $k$-weakly regular.

## References

[1] M. Akram and W.A. Dudek, Intuitionistic fuzzy left $k$-ideals of semirings, Soft Comput. 12 (2008), 881 - 890.
[2] A.P. Gan and Y.L. Jiang, On ordered ideals in ordered semirings, J. Math. Res. Exposition 31 (2011), 989 - 996.
[3] J.S. Han, H.S. Kim and J. Neggers, Semiring orders in semirings, Appl. Math. Inform. Sci. 6 (2012), $99-102$.
[4] M. Henriksen, Ideals in semirings with commutative addition, Amer. Math. Soc. Notices 6 (1958), 321.
[5] S. Patchakhieo and B. Pibaljommee, Characterizations of ordered $k$-regular semirings by ordered $k$-ideals, Asian-Eur. J. Math. 10 (2017), 1750020.
[6] M.K. Sen and M.R. Adhikari, On $k$-ideals of semirings, Int. J. Math. Math.Sci. 15 (1992), 347 - 350.
[7] M.K. Sen and M.R. Adhikari, On maximal $k$-ideals of semirings, Proc. Amer. Math. Soc. 118 (1993), $699-720$.
[8] H.S. Vandiver, On some simple types of semirings, Amer. Math. Monthly 46 (1939), $22-26$.

Department of Mathematics, Faculty of Science,
Khon Kaen University Khon Kaen 4002, Thailand
Centre of Excellence in Mathematics
CHE, Si Ayuttaya Rd. Bangkok 10400, Thailand
E-mails: lamb2283@gmail.com, banpib@kku.ac.th

# On orthogonal systems of ternary quasigroups admitting nontrivial paratopies 

Parascovia Syrbu and Dina Ceban


#### Abstract

In the present work we describe all orthogonal systems consisting of three ternary quasigroup operations and of all (three) ternary selectors, admitting at least one nontrivial paratopy. In [11] we proved that there exist precisely 48 orthogonal systems of the considered form, admitting at least one paratopy, which components are three quasigroup operations, or two quasigroup operations and a selector. Now we show that there exist precisely 105 such systems, admitting at least one nontrivial paratopy which components are two selectors and a quasigroup operation, or three selectors.


## 1. Introduction

An $n$-ary groupoid $(Q, A)$ is called an $n$-ary quasigroup if in the equality

$$
A\left(x_{1}, x_{2}, \ldots, x_{n}\right)=x_{n+1}
$$

any element of the set $\left\{x_{1}, x_{2}, \ldots, x_{n+1}\right\}$ is uniquely determined by the other $n$ elements. If $(Q, A)$ is an $n$-ary quasigroup and $\sigma \in S_{n}$, then the operation ${ }^{\sigma} A$ defined by the equivalence:

$$
{ }^{\sigma} A\left(x_{\sigma 1}, x_{\sigma 2}, \ldots, x_{\sigma n}\right)=x_{\sigma(n+1)} \Leftrightarrow A\left(x_{1}, x_{2}, \ldots, x_{n}\right)=x_{n+1},
$$

for every $x_{1}, x_{2}, \ldots, x_{n}, x_{n+1} \in Q$, is called a $\sigma$-parastrophe (or, simply, a parastrophe) of $(Q, A)$. The operation ${ }^{\sigma} A$ is called a principal parastrophe of $A$ if $\sigma(n+1)=n+1$. The main notions and general properties of $n$-ary quasigroups may be found in [3]. Following [3], we will denote by $\pi_{i}$ the transposition $(i, n+1)$, where $i \in\{1,2, \ldots, n\}$, so ${ }^{(i, n+1)} A={ }^{\pi_{i}} A$.

The $n$-ary operations $A_{1}, A_{2}, \ldots, A_{n}$, defined on a set $Q$, are called orthogonal if, for every $a_{1}, a_{2}, \ldots, a_{n} \in Q$, the system of equations

$$
\left\{A_{i}\left(x_{1}, x_{2}, \ldots, x_{n}\right)=a_{i}\right\}_{i=\overline{1, n}}
$$

has a unique solution in $Q$. A system of $n$-ary operations $A_{1}, A_{2}, \ldots, A_{s}$, defined on a set $Q$, where $s \geqslant n$, is called orthogonal if every $n$ operations of this

[^7]system are orthogonal. For every mapping $\theta: Q^{n} \rightarrow Q^{n}$ there exist, and are unique, $n n$-ary operations $A_{1}, A_{2}, \ldots, A_{n}$, defined on $Q$, such that $\theta\left(\left(x_{1}^{n}\right)\right)=$ $\left(A_{1}\left(x_{1}^{n}\right), A_{2}\left(x_{1}^{n}\right), \ldots, A_{n}\left(x_{1}^{n}\right)\right)$, for every $\left(x_{1}^{n}\right) \in Q^{n}$, where by $\left(x_{1}^{n}\right)$ we denote $\left(x_{1}, \ldots, x_{n}\right)$. Moreover, the mapping $\theta$ is a bijection if and only if the operations $A_{1}, A_{2}, \ldots, A_{n}$ are orthogonal. The operations $E_{1}, E_{2}, \ldots, E_{n}$, defined on $Q$, where $E_{i}\left(x_{1}^{n}\right)=x_{i}$, for every $x_{1}, x_{2}, \ldots, x_{n} \in Q, i=1,2, \ldots, n$, are called $n$-ary selectors. An $n$-ary operation $A$ is a quasigroup operation if and only if the system $\left\{A, E_{1}, E_{2}, \ldots, E_{n}\right\}$ is orthogonal. Orthogonal systems of $n$-ary operations (quasigroups) are considered in [1], [5], [7], [10]. Algebraic transformations of orthogonal systems of operations, that keep the orthogonality, have been defined and considered in [2] and [6].

If $\Sigma=\left\{A_{1}, A_{2}, \ldots, A_{n}, E_{1}, E_{2}, \ldots E_{n}\right\}$ is an orthogonal system, then we will denote the system $\left\{A_{1} \theta, A_{2} \theta, \ldots, A_{n} \theta, E_{1} \theta, E_{2} \theta, \ldots, E_{n} \theta\right\}$ by $\Sigma \theta$. Any bijection $\theta: Q^{n} \rightarrow Q^{n}$ is called a paratopy of $\Sigma$ if $\Sigma \theta=\Sigma$ (cf. [2]).
V. Belousov proved in [2] that there exist precisely nine orthogonal systems of the form $\Sigma=\{A, B, F, E\}$, where $A$ and $B$ are binary quasigroups defined on a set $Q$ and $F, E$ are the binary selectors on $Q$, which admit at least one nontrivial paratopy. He also shown that many paratopies of $\Sigma$ imply identities of length five with two variables (called minimal identities) in one of two quasigroups of $\Sigma$. Later, (see [4]) V. Belousov obtained a classification of such identities. It is known that minimal identities in quasigroups imply the orthogonality of some pairs of their parastrophes.

It is shown in [11] and in the present paper that there exists precisely 153 orthogonal systems, consisting of three ternary quasigroups and the ternary selectors, which admit at least one nontrivial paratopy. Moreover, the paratopies of these systems imply 67 identities. In [8] each of these identities is reduced to one of the following four types:

$$
\begin{aligned}
\text { I. }{ }^{\alpha} A\left({ }^{\beta} A,{ }^{\gamma} A,{ }^{\delta} A\right) & =E_{1}, \\
\text { II. }{ }^{\alpha} A\left({ }^{\beta} A,{ }^{\gamma} A, E_{1}\right) & =E_{2}, \\
\text { III. }{ }^{\alpha} A\left({ }^{\beta} A, E_{1}, E_{2}\right) & ={ }^{\gamma} A\left({ }^{\delta} A, E_{1}, E_{3}\right), \\
\text { IV. }{ }^{\alpha} A\left({ }^{\beta} A, E_{1}, E_{2}\right) & ={ }^{\gamma} A\left({ }^{\delta} A, E_{1}, E_{2}\right),
\end{aligned}
$$

where $A$ is a ternary quasigroup operation and $\alpha, \beta, \gamma, \delta \in S_{4}$. It is known that some of the obtained identities imply the orthogonality of parastrophes of the corresponding quasigroups ([3], [10], [11]).

Let $\Sigma=\left\{A_{1}, A_{2}, A_{3}, E_{1}, E_{2}, E_{3}\right\}$, where $A_{1}, A_{2}, A_{3}$ are ternary quasigroups defined on a set $Q$ and $E_{1}, E_{2}, E_{3}$ are the ternary selectors on $Q$, be an orthogonal system and let $\theta: Q^{3} \rightarrow Q^{3}, \theta=\left(B_{1}, B_{2}, B_{3}\right)$, be a mapping, where $B_{1}, B_{2}, B_{3}$ are ternary operations on $Q$. If $\theta$ is a paratopy of $\Sigma$, then $\Sigma \theta=$ $\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta, E_{1} \theta, E_{2} \theta, E_{3} \theta\right\}=\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta, B_{1}, B_{2}, B_{3}\right\}=\Sigma$, which imply $\left\{B_{1}, B_{2}, B_{3}\right\} \subset \Sigma$, i.e. all paratopies of $\Sigma$ are triplets of operations from $\Sigma$. We study the necessary and sufficient conditions when a triplet of operations from $\Sigma$ defines a paratopy of $\Sigma$. As the ternary selectors $E_{1}, E_{2}, E_{3}$ are fixed, we consider the tuples containing all possible distributions of the ternary selectors in their positions. In [11] we examined the paratopies which components are three quasigroup
operations, or two quasigroup operations and a ternary selector.
In the present article we continue the investigation of the paratopies of $\Sigma$, and prove that there exist 105 such orthogonal systems, that admit at least one nontrivial paratopy consisting of a ternary quasigroup and two ternary selectors, or of three ternary selectors.

## 2. Paratopies consisting of two ternary selectors and a ternary quasigroup operation

It is proved in this section that there exist precisely 87 orthogonal systems $\Sigma=$ $\left\{A_{1}, A_{2}, A_{3}, E_{1}, E_{2}, E_{3}\right\}$, consisting of three ternary quasigroup operations $A_{1}, A_{2}$, $A_{3}$ and three ternary selectors $E_{1}, E_{2}, E_{3}$, admitting at least one paratopy, which components are two ternary selectors and a ternary quasigroup operation.

Lemma 2.1. The triplet $\left(E_{1}, E_{2}, A_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(E_{1}, E_{2}, A_{1}\right), A_{3}={ }^{\pi_{3}} A_{1}$ and $A_{1}\left(E_{1}, E_{2}, A_{1}\left(E_{1}, E_{2}, A_{1}\right)\right)={ }^{\pi_{3}} A_{1}$;
2. $A_{3}=A_{1}\left(E_{1}, E_{2}, A_{1}\right), A_{2}={ }^{\pi_{3}} A_{1}$ and $A_{1}\left(E_{1}, E_{2}, A_{1}\left(E_{1}, E_{2}, A_{1}\right)\right)={ }^{\pi_{3}} A_{1}$;
3. $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{1}, E_{2}, A_{3}\right)={ }^{\pi_{3}} A_{3}\left(E_{1}, E_{2}, A_{2}\right)$.

Proof. Let the triplet $\left(E_{1}, E_{2}, A_{1}\right)$ be a paratopy of the system $\Sigma$. As $E_{1} \theta=$ $E_{1}, E_{2} \theta=E_{2}, E_{3} \theta=A_{1}$, we obtain $\Sigma \theta=\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta, E_{1}, E_{2}, A_{1}\right\}$, that is $\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta\right\}=\left\{E_{3}, A_{2}, A_{3}\right\}$.

1. If $A_{1} \theta=A_{2}, A_{2} \theta=A_{3}, A_{3} \theta=E_{3}$, then $\theta^{2}=\left(E_{1}, E_{2}, A_{2}\right), \theta^{3}=\left(E_{1}, E_{2}, A_{3}\right)$, $\theta^{4}=\varepsilon$. From $A_{1} \theta=A_{2}$ it follows

$$
\begin{equation*}
A_{2}=A_{1}\left(E_{1}, E_{2}, A_{1}\right) \tag{1}
\end{equation*}
$$

Also, $A_{1} \theta=A_{2}$ implies $A_{1} \theta^{3}=E_{3}$, i.e. $A_{1}\left(E_{1}, E_{2}, A_{3}\right)=E_{3}$, so

$$
\begin{equation*}
A_{3}={ }^{\pi_{3}} A_{1} \tag{2}
\end{equation*}
$$

Moreover, from $A_{1} \theta=A_{2}$ it follows $A_{1} \theta^{2}=A_{3}$, i.e. $A_{1}\left(E_{1}, E_{2}, A_{2}\right)=A_{3}$. Using (1) and (2) in the last equality, we get

$$
\begin{equation*}
A_{1}\left(E_{1}, E_{2}, A_{1}\left(E_{1}, E_{2}, A_{1}\right)\right)={ }^{\pi_{3}} A_{1} \tag{3}
\end{equation*}
$$

Conversely, if (1), (2) and (3) hold, then (1) implies $A_{1} \theta=A_{2}$. From (2) it follows $A_{3} \theta={ }^{\pi_{3}} A_{1}\left(E_{1}, E_{2}, A_{1}\right)$, hence $A_{3} \theta=E_{3}$. Using (1) and (2) in (3), we get $A_{1}\left(E_{1}, E_{2}, A_{2}\right)=A_{3}$, hence $A_{2}={ }^{\pi_{3}} A_{1}\left(E_{1}, E_{2}, A_{3}\right)$, which implies $A_{2} \theta={ }^{\pi_{3}} A_{1}$. Using (2) in the last equality, we obtain $A_{2} \theta=A_{3}$.
2. If $A_{1} \theta=A_{2}, A_{2} \theta=E_{3}, A_{3} \theta=A_{3}$, then $A_{3} \theta=A_{3}$, i.e. $A_{3}\left(E_{1}, E_{2}, A_{1}\right)=A_{3}$, implies $A_{1}=E_{3}$, which is a contradiction as $A_{1}$ is a quasigroup.
3. If $A_{1} \theta=A_{3}, A_{2} \theta=A_{2}, A_{3} \theta=E_{3}$, then $A_{2} \theta=A_{2}$, i.e. $A_{2}\left(E_{1}, E_{2}, A_{1}\right)=A_{2}$, implies $A_{1}=E_{3}$, which is a contradiction as $A_{1}$ is a quasigroup.
4. If $A_{1} \theta=A_{3}, A_{2} \theta=E_{3}, A_{3} \theta=A_{2}$, then $\theta^{2}=\left(E_{1}, E_{2}, A_{3}\right), \theta^{3}=\left(E_{1}, E_{2}, A_{2}\right)$, $\theta^{4}=\varepsilon$. From $A_{1} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{3}=A_{1}\left(E_{1}, E_{2}, A_{1}\right) \tag{4}
\end{equation*}
$$

Also, $A_{1} \theta=A_{3}$ implies $A_{1} \theta^{3}=E_{3}$, i.e. $A_{1}\left(E_{1}, E_{2}, A_{2}\right)=E_{3}$, so

$$
\begin{equation*}
A_{2}={ }^{\pi_{3}} A_{1} \tag{5}
\end{equation*}
$$

Moreover, from $A_{1} \theta=A_{3}$ it follows $A_{1} \theta^{2}=A_{2}$, i.e. $A_{1}\left(E_{1}, E_{2}, A_{3}\right)=A_{2}$. Using (4) and (5) in the last equality, we get

$$
\begin{equation*}
A_{1}\left(E_{1}, E_{2}, A_{1}\left(E_{1}, E_{2}, A_{1}\right)\right)={ }^{\pi_{3}} A_{1} . \tag{6}
\end{equation*}
$$

Conversely, if (4), (5) and (6) hold, then (4) implies $A_{1} \theta=A_{3}$. From (5) it follows $A_{2} \theta={ }^{\pi_{3}} A_{1}\left(E_{1}, E_{2}, A_{1}\right)$, hence $A_{2} \theta=E_{3}$. Using (4) and (5) in (6), we get $A_{1}\left(E_{1}, E_{2}, A_{3}\right)=A_{2}$, hence $A_{3}={ }^{\pi_{3}} A_{1}\left(E_{1}, E_{2}, A_{2}\right)$, which implies $A_{3} \theta={ }^{\pi_{3}} A_{1}$. Using (5) in the last equality, we obtain $A_{3} \theta=A_{2}$.
5. If $A_{1} \theta=E_{3}, A_{2} \theta=A_{2}, A_{3} \theta=A_{3}$, then $A_{2} \theta=A_{2}$, i.e. $A_{2}\left(E_{1}, E_{2}, A_{1}\right)=A_{2}$, implies $A_{1}=E_{3}$, which is a contradiction as $A_{1}$ is a quasigroup.
6. If $A_{1} \theta=E_{3}, A_{2} \theta=A_{3}, A_{3} \theta=A_{2}$, then $A_{2} \theta=A_{3}$ implies

$$
\begin{equation*}
A_{1}={ }^{\pi_{3}} A_{2}\left(E_{1}, E_{2}, A_{3}\right) \tag{7}
\end{equation*}
$$

From $A_{3} \theta=A_{2}$ it follows

$$
\begin{equation*}
A_{1}={ }^{\pi_{3}} A_{3}\left(E_{1}, E_{2}, A_{2}\right) \tag{8}
\end{equation*}
$$

Conversely, if (7) and (8) hold, then (8) implies $A_{3} \theta=A_{2}$. From (7) it follows $A_{2} \theta=A_{3}$ and $A_{1} \theta={ }^{\pi_{3}} A_{2}\left(E_{1}, E_{2}, A_{2}\right)$, so $A_{1} \theta=E_{3}$.

Lemma 2.2. The triplet $\left(E_{2}, E_{1}, A_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(E_{2}, E_{1}, A_{1}\right), A_{3}={ }^{(12) \pi_{3}} A_{1}$ and $A_{1}\left(E_{1}, E_{2}, A_{1}\left(E_{2}, E_{1}, A_{1}\right)\right)={ }^{(12) \pi_{3}} A_{1}$;
2. $A_{3}=A_{1}\left(E_{2}, E_{1}, A_{1}\right), A_{2}={ }^{(12) \pi_{3}} A_{1}$ and $A_{1}\left(E_{1}, E_{2}, A_{1}\left(E_{2}, E_{1}, A_{1}\right)\right)={ }^{(12) \pi_{3}} A_{1}$;
3. $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{2}, E_{1}, A_{2}\right)={ }^{\pi_{3}} A_{3}\left(E_{2}, E_{1}, A_{3}\right)$;
4. $A_{1}\left(E_{2}, E_{1}, A_{1}\right)=E_{3}, A_{2}\left(E_{2}, E_{1}, A_{1}\right)=A_{3}$.

Proof. Let the triplet $\left(E_{2}, E_{1}, A_{1}\right)$ be a paratopy of the system $\Sigma$. As $E_{1} \theta=$ $E_{2}, E_{2} \theta=E_{1}, E_{3} \theta=A_{1}$, we obtain $\Sigma \theta=\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta, E_{2}, E_{1}, A_{1}\right\}$, so there are six possible cases:

1. If $A_{1} \theta=A_{2}, A_{2} \theta=A_{3}, A_{3} \theta=E_{3}$, then $\theta^{2}=\left(E_{1}, E_{2}, A_{2}\right), \theta^{3}=\left(E_{2}, E_{1}, A_{3}\right)$, $\theta^{4}=\varepsilon$. From $A_{1} \theta=A_{2}$ it follows

$$
\begin{equation*}
A_{2}=A_{1}\left(E_{2}, E_{1}, A_{1}\right) \tag{9}
\end{equation*}
$$

Also, $A_{1} \theta=A_{2}$ implies $A_{1} \theta^{3}=E_{3}$, that is $A_{1}\left(E_{2}, E_{1}, A_{3}\right)=E_{3}$, so

$$
\begin{equation*}
A_{3}={ }^{(12) \pi_{3}} A_{1} . \tag{10}
\end{equation*}
$$

Moreover, $A_{1} \theta=A_{2}$ implies $A_{1} \theta^{2}=A_{3}$, i.e. $A_{1}\left(E_{1}, E_{2}, A_{2}\right)=A_{3}$. Using (9) and (10) in the last equality we get

$$
\begin{equation*}
A_{1}\left(E_{1}, E_{2}, A_{1}\left(E_{2}, E_{1}, A_{1}\right)\right)={ }^{(12) \pi_{3}} A_{1} \tag{11}
\end{equation*}
$$

Conversely, if (9), (10) and (11) hold, then from (9) it follows $A_{1} \theta=A_{2}$ and (10) implies $A_{3} \theta={ }^{\pi_{3}} A_{1}\left(E_{1}, E_{2}, A_{1}\right)$, so $A_{3} \theta=E_{3}$. Using (9) and (10) in (11) we get $A_{1}\left(E_{1}, E_{2}, A_{2}\right)=A_{3}$, which implies $A_{2}={ }^{\pi_{3}} A_{1}\left(E_{1}, E_{2}, A_{3}\right)$, hence $A_{2} \theta=$ ${ }^{\pi_{3}} A_{1}\left(E_{2}, E_{1}, E_{3}\right)$. Using (10) in the last equality, we obtain $A_{2} \theta=A_{3}$.
2. If $A_{1} \theta=A_{2}, A_{2} \theta=E_{3}, A_{3} \theta=A_{3}$, then $\theta^{2}=\left(E_{1}, E_{2}, A_{2}\right)$. From $A_{3} \theta=A_{3}$ it follows $A_{3} \theta^{2}=A_{3}$, i.e. $A_{3}\left(E_{1}, E_{2}, A_{2}\right)=A_{3}$, so $A_{2}=E_{3}$, which is a contradiction, as $A_{2}$ is a quasigroup operation.
3. If $A_{1} \theta=A_{3}, A_{2} \theta=A_{2}, A_{3} \theta=E_{3}$, then $\theta^{2}=\left(E_{1}, E_{2}, A_{3}\right)$. From $A_{2} \theta=A_{2}$ it follows $A_{2} \theta^{2}=A_{2}$, i.e. $A_{2}\left(E_{1}, E_{2}, A_{3}\right)=A_{2}$, so $A_{3}=E_{3}$, which is a contradiction, as $A_{3}$ is a quasigroup operation.
4. If $A_{1} \theta=A_{3}, A_{2} \theta=E_{3}, A_{3} \theta=A_{2}$, then $\theta^{2}=\left(E_{1}, E_{2}, A_{3}\right), \theta^{3}=\left(E_{2}, E_{1}, A_{2}\right)$, $\theta^{4}=\varepsilon$. From $A_{1} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{3}=A_{1}\left(E_{2}, E_{1}, A_{1}\right) \tag{12}
\end{equation*}
$$

Also, $A_{1} \theta=A_{3}$ implies $A_{1} \theta^{3}=E_{3}$, i.e. $A_{1}\left(E_{2}, E_{1}, A_{2}\right)=E_{3}$, so

$$
\begin{equation*}
A_{2}={ }^{(12) \pi_{3}} A_{1} . \tag{13}
\end{equation*}
$$

Moreover, $A_{1} \theta=A_{3}$ implies $A_{1} \theta^{2}=A_{2}$, i.e. $A_{1}\left(E_{1}, E_{2}, A_{3}\right)=A_{2}$. Using (12) and (13) in the last equality we get

$$
\begin{equation*}
A_{1}\left(E_{1}, E_{2}, A_{1}\left(E_{2}, E_{1}, A_{1}\right)\right)={ }^{(12) \pi_{3}} A_{1} \tag{14}
\end{equation*}
$$

Conversely, if (12), (13) and (14) hold, then from (12) it follows $A_{1} \theta=A_{3}$ and (13) implies $A_{2} \theta={ }^{\pi_{3}} A_{1}\left(E_{1}, E_{2}, A_{1}\right)$, so $A_{2} \theta=E_{3}$. Using (12) and (13) in (14) we get $A_{1}\left(E_{1}, E_{2}, A_{3}\right)=A_{2}$, which implies $A_{3}={ }^{\pi_{3}} A_{1}\left(E_{1}, E_{2}, A_{2}\right)$, therefore $A_{3} \theta=$ ${ }^{\pi_{3}} A_{1}\left(E_{2}, E_{1}, E_{3}\right)$. Using (13) in the last equality, we obtain $A_{3} \theta=A_{2}$.
5. If $A_{1} \theta=E_{3}, A_{2} \theta=A_{2}, A_{3} \theta=A_{3}$, then $\theta^{2}=\varepsilon$. From $A_{2} \theta=A_{2}$ it follows that

$$
\begin{equation*}
A_{1}={ }^{\pi_{3}} A_{2}\left(E_{2}, E_{1}, A_{2}\right) \tag{15}
\end{equation*}
$$

From $A_{3} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{1}={ }^{\pi_{3}} A_{3}\left(E_{2}, E_{1}, A_{3}\right) . \tag{16}
\end{equation*}
$$

Conversely, if (15) and (16) hold, then (15) implies $A_{2} \theta=A_{2}$ and (16) implies $A_{3} \theta=A_{3}$. Also, from (16) we get $A_{1} \theta={ }^{\pi_{3}} A_{3}\left(E_{1}, E_{2}, A_{3}\right)$, so $A_{1} \theta=E_{3}$.
6. If $A_{1} \theta=E_{3}, A_{2} \theta=A_{3}, A_{3} \theta=A_{2}$, then $\theta^{2}=\varepsilon$. From $A_{1} \theta=E_{3}$ it follows

$$
\begin{equation*}
A_{1}\left(E_{2}, E_{1}, A_{1}\right)=E_{3} \tag{17}
\end{equation*}
$$

and $A_{2} \theta=A_{3}$ can be written in the form

$$
\begin{equation*}
A_{3}=A_{2}\left(E_{2}, E_{1}, A_{1}\right) \tag{18}
\end{equation*}
$$

Conversely, if (17) and (18) hold, then (17) implies $A_{1} \theta=E_{3}$ and (18) implies $A_{2} \theta=A_{3}$. Also, from (18) it follows $A_{3} \theta=A_{2}\left(E_{1}, E_{2}, E_{3}\right)$, i.e. $A_{3} \theta=A_{2}$.

Lemma 2.3. The triplet $\left(E_{1}, A_{1}, E_{2}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(E_{1}, A_{1}, E_{2}\right), A_{3}={ }^{(23) \pi_{3}} A_{1}$ and

$$
A_{1}\left(E_{1},(23) \pi_{3} A_{1}, A_{1}\left(E_{1}, A_{1}, E_{2}\right)\right)=E_{3}
$$

2. $A_{1}={ }^{\pi_{2}} A_{3}\left(E_{1}, A_{3}, E_{2}\right), A_{2}={ }^{\pi_{3}} A_{3}\left(E_{1}, E_{3}, A_{3}\right)$ and $A_{3}\left(E_{1},^{\pi_{3}} A_{3}\left(E_{1}, E_{3}, A_{3}\right),{ }^{\pi_{2}} A_{3}\left(E_{1}, A_{3}, E_{2}\right)\right)=A_{3} ;$
3. $A_{1}={ }^{\pi_{2}} A_{2}\left(E_{1}, A_{2}, E_{2}\right), A_{3}={ }^{\pi_{3}} A_{2}\left(E_{1}, E_{3}, A_{2}\right)$ and $A_{2}\left(E_{1},{ }^{\pi_{3}} A_{2}\left(E_{1}, E_{3}, A_{2}\right),{ }^{\pi_{2}} A_{2}\left(E_{1}, A_{2}, E_{2}\right)\right)=A_{2} ;$
4. $A_{2}={ }^{(23) \pi_{3}} A_{1}, A_{3}=A_{1}\left(E_{1}, A_{1}, E_{2}\right) \quad$ and
$A_{1}\left(E_{1},{ }^{(23) \pi_{3}} A_{1}, A_{1}\left(E_{1}, A_{1}, E_{2}\right)\right)=E_{3} ;$
5. $A_{1}={ }^{(23) \pi_{2}} A_{1}={ }^{\pi_{2}} A_{2}\left(E_{1}, A_{2}, E_{2}\right)=\pi^{\pi_{2}} A_{3}\left(E_{1}, A_{3}, E_{2}\right)$.

Proof. Let the triplet $\left(E_{1}, A_{1}, E_{2}\right)$ be a paratopy of the system $\Sigma$. As $E_{1} \theta=$ $E_{1}, E_{2} \theta=A_{1}, E_{3} \theta=E_{2}$, we obtain $\Sigma \theta=\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta, E_{3}, A_{2}, A_{3}\right\}$, that is $\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta\right\}=\left\{E_{3}, A_{2}, A_{3}\right\}$.

1. If $A_{1} \theta=A_{2}, A_{2} \theta=A_{3}, A_{3} \theta=E_{3}$, then $\theta^{2}=\left(E_{1}, A_{2}, A_{1}\right), \theta^{3}=\left(E_{1}, A_{3}, A_{2}\right)$, $\theta^{4}=\left(E_{1}, E_{3}, A_{3}\right), \theta^{5}=\varepsilon$. From $A_{1} \theta=A_{2}$ it follows

$$
\begin{equation*}
A_{2}=A_{1}\left(E_{1}, A_{1}, E_{2}\right) \tag{19}
\end{equation*}
$$

Also, $A_{1} \theta=A_{2}$ implies $A_{1} \theta^{4}=E_{2}$, i.e. $A_{1}\left(E_{1}, E_{3}, A_{3}\right)=E_{2}$, so

$$
\begin{equation*}
A_{3}={ }^{(23) \pi_{3}} A_{1} . \tag{20}
\end{equation*}
$$

Moreover, $A_{1} \theta=A_{2}$ implies $A_{1} \theta^{3}=E_{3}$, i.e. $A_{1}\left(E_{1}, A_{3}, A_{2}\right)=E_{3}$. Using (19) and (20) in the last equality, we get

$$
\begin{equation*}
A_{1}\left(E_{1},{ }^{(23) \pi_{3}} A_{1}, A_{1}\left(E_{1}, A_{1}, E_{2}\right)\right)=E_{3} \tag{21}
\end{equation*}
$$

Conversely, if (19), (20) and (21) hold, then (19) implies $A_{1} \theta=A_{2}$ and (20) implies $A_{3} \theta={ }^{\pi_{3}} A_{1}\left(E_{1}, E_{2}, A_{1}\right)$, so $A_{3} \theta=E_{3}$. Using (19) and (20) in (21), we get $A_{1}\left(E_{1}, A_{3}, A_{2}\right)=E_{3}$, which implies $A_{2}={ }^{\pi_{3}} A_{1}\left(E_{1}, A_{3}, E_{3}\right)$, hence $A_{2} \theta=$ ${ }^{\pi_{3}} A_{1}\left(E_{1}, E_{3}, E_{2}\right)$. Using (20) in the last equality, we obtain $A_{2} \theta=A_{3}$.
2. If $A_{1} \theta=A_{2}, A_{2} \theta=E_{3}, A_{3} \theta=A_{3}$, then $\theta^{2}=\left(E_{1}, A_{2}, A_{1}\right), \theta^{3}=\left(E_{1}, E_{3}, A_{2}\right)$, $\theta^{4}=\varepsilon$. From $A_{3} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{1}={ }^{\pi_{2}} A_{3}\left(E_{1}, A_{3}, E_{2}\right) \tag{22}
\end{equation*}
$$

Also, from $A_{3} \theta=A_{3}$ it follows $A_{3} \theta^{3}=A_{3}$, i.e. $A_{3}\left(E_{1}, E_{3}, A_{2}\right)=A_{3}$, so

$$
\begin{equation*}
A_{2}={ }^{\pi_{3}} A_{3}\left(E_{1}, E_{3}, A_{3}\right) \tag{23}
\end{equation*}
$$

Moreover, $A_{3} \theta=A_{3}$ implies $A_{3} \theta^{2}=A_{3}$, i.e. $A_{3}\left(E_{1}, A_{2}, A_{1}\right)=A_{3}$, Using (22) and (23) in the last equality, we obtain

$$
\begin{equation*}
A_{3}\left(E_{1},{ }^{\pi_{3}} A_{3}\left(E_{1}, E_{3}, A_{3}\right),{ }^{\pi_{2}} A_{3}\left(E_{1}, A_{3}, E_{2}\right)\right)=A_{3} \tag{24}
\end{equation*}
$$

Conversely, if (22), (23) and (24) hold, then (22) implies $A_{3} \theta=A_{3}$ and (23) implies $A_{2} \theta={ }^{\pi_{3}} A_{3}\left(E_{1}, E_{2}, A_{3}\right)$, so $A_{2} \theta=E_{3}$. Using (22) and (23) in (24), we get $A_{3}\left(E_{1}, A_{2}, A_{1}\right)=A_{3}$, which implies $A_{1}={ }^{\pi_{3}} A_{3}\left(E_{1}, A_{2}, A_{3}\right)$, hence $A_{1} \theta=$ ${ }^{\pi_{3}} A_{3}\left(E_{1}, E_{3}, A_{3}\right)$. Using (23) in the last equality, we get $A_{1} \theta=A_{2}$.
3. If $A_{1} \theta=A_{3}, A_{2} \theta=A_{2}, A_{3} \theta=E_{3}$, then $\theta^{2}=\left(E_{1}, A_{3}, A_{1}\right), \theta^{3}=\left(E_{1}, E_{3}, A_{3}\right)$, $\theta^{4}=\varepsilon$. From $A_{2} \theta=A_{2}$ it follows

$$
\begin{equation*}
A_{1}={ }^{\pi_{2}} A_{2}\left(E_{1}, A_{2}, E_{2}\right) \tag{25}
\end{equation*}
$$

Also, from $A_{2} \theta=A_{2}$ it follows $A_{2} \theta^{3}=A_{2}$, i.e. $A_{2}\left(E_{1}, E_{3}, A_{3}\right)=A_{2}$, so

$$
\begin{equation*}
A_{3}={ }^{\pi_{3}} A_{2}\left(E_{1}, E_{3}, A_{2}\right) \tag{26}
\end{equation*}
$$

Moreover, $A_{2} \theta=A_{2}$ implies $A_{2} \theta^{2}=A_{2}$, i.e. $A_{3}\left(E_{1}, A_{3}, A_{1}\right)=A_{2}$. Using (25) and (26) in the last equality, we obtain

$$
\begin{equation*}
A_{2}\left(E_{1},{ }^{\pi_{3}} A_{2}\left(E_{1}, E_{3}, A_{2}\right),{ }^{\pi_{2}} A_{2}\left(E_{1}, A_{2}, E_{2}\right)\right)=A_{2} \tag{27}
\end{equation*}
$$

Conversely, if (25), (26) and (27) hold, then (25) implies $A_{2} \theta=A_{2}$ and (26) implies $A_{3} \theta={ }^{\pi_{3}} A_{2}\left(E_{1}, E_{2}, A_{2}\right)$, so $A_{3} \theta=E_{3}$. Using (25) and (26) in (27), we get $A_{2}\left(E_{1}, A_{3}, A_{1}\right)=A_{2}$, which implies $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{1}, A_{3}, A_{2}\right)$, hence $A_{1} \theta=$ ${ }^{\pi_{3}} A_{2}\left(E_{1}, E_{3}, A_{2}\right)$. Using (26) in the last equality, we get $A_{1} \theta=A_{3}$.
4. If $A_{1} \theta=A_{3}, A_{2} \theta=E_{3}, A_{3} \theta=A_{2}$, then $\theta^{2}=\left(E_{1}, A_{3}, A_{1}\right), \theta^{3}=\left(E_{1}, A_{2}, A_{3}\right)$, $\theta^{4}=\left(E_{1}, E_{3}, A_{2}\right), \theta^{5}=\varepsilon$. From $A_{1} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{3}=A_{1}\left(E_{1}, A_{1}, E_{2}\right) \tag{28}
\end{equation*}
$$

Also, $A_{1} \theta=A_{3}$ implies $A_{1} \theta^{4}=E_{2}$, i.e. $A_{1}\left(E_{1}, E_{3}, A_{2}\right)=E_{2}$, so

$$
\begin{equation*}
A_{2}={ }^{(23) \pi_{3}} A_{1} \tag{29}
\end{equation*}
$$

Moreover, $A_{1} \theta=A_{3}$ implies $A_{1} \theta^{3}=E_{3}$, i.e. $A_{1}\left(E_{1}, A_{2}, A_{3}\right)=E_{3}$. Using (28) and (29) in the last equality, we obtain

$$
\begin{equation*}
A_{1}\left(E_{1},{ }^{(23) \pi_{3}} A_{1}, A_{1}\left(E_{1}, A_{1}, E_{2}\right)\right)=E_{3} \tag{30}
\end{equation*}
$$

Conversely, if (28), (29) and (30) hold, then (28) implies $A_{1} \theta=A_{3}$ and (29) implies $A_{2} \theta={ }^{\pi_{3}} A_{1}\left(E_{1}, E_{2}, A_{1}\right)$, so $A_{2} \theta=E_{3}$. Using (28) and (29) in (30), we get $A_{1}\left(E_{1}, A_{2}, A_{3}\right)=E_{3}$, which implies $A_{3}={ }^{\pi_{3}} A_{1}\left(E_{1}, A_{2}, E_{3}\right)$, hence $A_{3} \theta=$ ${ }^{\pi_{3}} A_{1}\left(E_{1}, E_{3}, E_{2}\right)$. Using (29) in the last equality, we get $A_{3} \theta=A_{2}$.
5. If $A_{1} \theta=E_{3}, A_{2} \theta=A_{2}, A_{3} \theta=A_{3}$, from $A_{1} \theta=E_{3}$ it follows

$$
\begin{equation*}
A_{1}={ }^{(23) \pi_{1}} A_{1} \tag{31}
\end{equation*}
$$

The equality $A_{2} \theta=A_{2}$ implies

$$
\begin{equation*}
A_{1}={ }^{\pi_{2}} A_{2}\left(E_{1}, A_{2}, E_{2}\right) \tag{32}
\end{equation*}
$$

From $A_{3} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{1}={ }^{\pi_{2}} A_{3}\left(E_{1}, A_{3}, E_{2}\right) \tag{33}
\end{equation*}
$$

Conversely, if (31), (32) and (33) hold, then (31) implies $A_{1} \theta=E_{3}$, from (32) it follows $A_{2} \theta=A_{2}$ and (33) implies $A_{3} \theta=A_{3}$.
6. If $A_{1} \theta=E_{3}, A_{2} \theta=A_{3}, A_{3} \theta=A_{2}$, then $\theta^{2}=\left(E_{1}, E_{3}, A_{1}\right), \theta^{3}=\varepsilon$. Remark that $A_{2}=A_{2} \theta^{3}=A_{3} \theta^{2}=A_{2} \theta=A_{3}$, which is a contradiction, as $\Sigma$ is an orthogonal system.

Lemma 2.4. The triplet $\left(E_{2}, A_{1}, E_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{1}={ }^{(132) \pi_{2}} A_{3}, A_{2}=A_{3}\left(E_{3}, E_{1}, A_{3}\right)$ and
${ }^{(132) \pi_{2}} A_{3}\left(E_{2},{ }^{(132) \pi_{2}} A_{3}, E_{1}\right)=A_{3}\left(E_{3}, E_{1}, A_{3}\right)$;
2. $A_{1}={ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{1}\right), A_{2}={ }^{\pi_{3}} A_{3}\left(E_{3}, E_{1}, A_{3}\right)$ and
${ }^{\pi_{2}} A_{3}\left({ }^{\pi_{3}} A_{3}\left(E_{3}, E_{1}, A_{3}\right), A_{3},{ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{1}\right)\right)=E_{3} ;$
3. $A_{1}={ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{1}\right), A_{3}={ }^{\pi_{3}} A_{2}\left(E_{3}, E_{1}, A_{2}\right)$ and ${ }^{\pi_{2}} A_{2}\left({ }^{\pi_{3}} A_{2}\left(E_{3}, E_{1}, A_{2}\right), A_{2},{ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{1}\right)\right)=E_{3} ;$
4. $A_{1}={ }^{(132) \pi_{2}} A_{2}, A_{3}=A_{2}\left(E_{3}, E_{1}, A_{2}\right)$ and
$A_{2}\left(A_{2}, E_{3}, A_{2}\left(E_{3}, E_{1}, A_{2}\right)\right)={ }^{(132) \pi_{2}} A_{2}$;
5. $A_{1}=\pi^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{1}\right)={ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{1}\right)$ and $A_{1}={ }^{(132) \pi_{2}} A_{1}$;
6. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{2}\right), A_{3}=A_{2}\left(E_{3}, E_{1},{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{2}\right)\right)$ and
$A_{1}={ }^{(132) \pi_{2}} A_{1}$.
Proof. Let the triplet $\left(E_{2}, A_{1}, E_{1}\right)$ be a paratopy of the system $\Sigma$. As $E_{1} \theta=$ $E_{2}, E_{2} \theta=A_{1}, E_{3} \theta=E_{1}$, we obtain $\Sigma \theta=\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta, E_{2}, A_{1}, E_{1}\right\}$, that is $\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta\right\}=\left\{E_{3}, A_{2}, A_{3}\right\}$.
7. If $A_{1} \theta=A_{2}, A_{2} \theta=A_{3}, A_{3} \theta=E_{3}$, then $\theta^{2}=\left(A_{1}, A_{2}, E_{2}\right), \theta^{3}=\left(A_{2}, A_{3}, A_{1}\right)$, $\theta^{4}=\left(A_{3}, E_{3}, A_{2}\right), \theta^{5}=\left(E_{3}, E_{1}, A_{3}\right), \theta^{6}=\varepsilon$. From $A_{3} \theta=E_{3}$ it follows

$$
\begin{equation*}
A_{1}={ }^{(132) \pi_{2}} A_{3} . \tag{34}
\end{equation*}
$$

The equality $A_{2} \theta=A_{3}$ implies $A_{2} \theta^{6}=A_{3} \theta^{5}$, so

$$
\begin{equation*}
A_{2}=A_{3}\left(E_{3}, E_{1}, A_{3}\right) \tag{35}
\end{equation*}
$$

Using (34) and (35) in $A_{1} \theta=A_{2}$, we get

$$
\begin{equation*}
{ }^{(132) \pi_{2}} A_{3}\left(E_{2},{ }^{(132) \pi_{2}} A_{3}, E_{1}\right)=A_{3}\left(E_{3}, E_{1}, A_{3}\right) \tag{36}
\end{equation*}
$$

Conversely, if (34), (35) and (36) hold, then from (34) it follows $A_{3} \theta=E_{3}$. The equality (35) implies $A_{2} \theta=A_{3}$. Using (34) and (35) in (36), we obtain $A_{1}\left(E_{2}, A_{1}, E_{1}\right)=A_{2}$, which implies $A_{1} \theta=A_{2}$.
2. If $A_{1} \theta=A_{2}, A_{2} \theta=E_{3}, A_{3} \theta=A_{3}$, then $\theta^{2}=\left(A_{1}, A_{2}, E_{2}\right), \theta^{3}=\left(A_{2}, E_{3}, A_{1}\right)$, $\theta^{4}=\left(E_{3}, E_{1}, A_{2}\right), \theta^{5}=\varepsilon$. From $A_{3} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{1}={ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{1}\right) \tag{37}
\end{equation*}
$$

Also, $A_{3} \theta=A_{3}$ implies $A_{3} \theta^{4}=A_{3}$, i.e. $A_{3}\left(E_{3}, E_{1}, A_{2}\right)=A_{3}$, so

$$
\begin{equation*}
A_{2}={ }^{\pi_{3}} A_{3}\left(E_{3}, E_{1}, A_{3}\right) \tag{38}
\end{equation*}
$$

The equality $A_{1} \theta=A_{2}$ implies $A_{1} \theta^{2}=E_{3}$. From (37) and $A_{1} \theta^{2}=E_{3}$, we get ${ }^{\pi_{2}} A_{3}\left(A_{2}, A_{3}, A_{1}\right)=E_{3}$ so, using (37) and (38) in the last equality, we obtain

$$
\begin{equation*}
{ }^{\pi_{2}} A_{3}\left({ }^{\pi_{3}} A_{3}\left(E_{3}, E_{1}, A_{3}\right), A_{3},{ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{1}\right)\right)=E_{3} \tag{39}
\end{equation*}
$$

Conversely, if (37), (38) and (39) hold, then from (37) it follows $A_{3} \theta=A_{3}$. The equality (38) implies $A_{2} \theta={ }^{\pi_{3}} A_{3}\left(E_{1}, E_{2}, A_{3}\right)$, so $A_{2} \theta=E_{3}$. Using (37) and (38) in (39), we get ${ }^{\pi_{2}} A_{3}\left(A_{2}, A_{3}, A_{1}\right)=E_{3}$, which implies $A_{1}={ }^{\pi_{3}} A_{3}\left(A_{2}, E_{3}, A_{3}\right)$, so $A_{1} \theta={ }^{\pi_{3}} A_{3}\left(E_{3}, E_{1}, A_{3}\right)$. Using (38) in the last equality, we obtain $A_{1} \theta=A_{2}$.
3. If $A_{1} \theta=A_{3}, A_{2} \theta=A_{2}, A_{3} \theta=E_{3}$, then $\theta^{2}=\left(A_{1}, A_{3}, E_{2}\right), \theta^{3}=\left(A_{3}, E_{3}, A_{1}\right)$, $\theta^{4}=\left(E_{3}, E_{1}, A_{3}\right), \theta^{5}=\varepsilon$. From $A_{2} \theta=A_{2}$ it follows

$$
\begin{equation*}
A_{1}={ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{1}\right) \tag{40}
\end{equation*}
$$

Also, $A_{2} \theta=A_{2}$ implies $A_{2} \theta^{4}=A_{2}$, i.e. $A_{2}\left(E_{3}, E_{1}, A_{3}\right)=A_{2}$, so

$$
\begin{equation*}
A_{3}={ }^{\pi_{3}} A_{2}\left(E_{3}, E_{1}, A_{2}\right) \tag{41}
\end{equation*}
$$

The equality $A_{1} \theta=A_{3}$ implies $A_{1} \theta^{2}=E_{3}$ so, using (40) in $A_{1} \theta^{2}=E_{3}$, we get ${ }^{\pi_{2}} A_{2}\left(A_{3}, A_{2}, A_{1}\right)=E_{3}$. Now, from (40), (41) and the last equality, we obtain

$$
\begin{equation*}
{ }^{\pi_{2}} A_{2}\left({ }^{\pi_{3}} A_{2}\left(E_{3}, E_{1}, A_{2}\right), A_{2},{ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{1}\right)\right)=E_{3} . \tag{42}
\end{equation*}
$$

Conversely, if (40), (41) and (42) hold, then from (40) it follows $A_{2} \theta=A_{2}$. The equality (41) implies $A_{3} \theta={ }^{\pi_{3}} A_{2}\left(E_{1}, E_{2}, A_{2}\right)$, so $A_{3} \theta=E_{3}$. Using (40) and (41) in (42), we get ${ }^{\pi_{2}} A_{2}\left(A_{3}, A_{2}, A_{1}\right)=E_{3}$, which implies $A_{1}={ }^{\pi_{3}} A_{2}\left(A_{3}, E_{3}, A_{2}\right)$, so $A_{1} \theta={ }^{\pi_{3}} A_{2}\left(E_{3}, E_{1}, A_{2}\right)$. Using (41) in the last equality, we obtain $A_{1} \theta=A_{3}$.
4. If $A_{1} \theta=A_{3}, A_{2} \theta=E_{3}, A_{3} \theta=A_{2}$, then $\theta^{2}=\left(A_{1}, A_{3}, E_{2}\right), \theta^{3}=\left(A_{3}, A_{2}, A_{1}\right)$, $\theta^{4}=\left(A_{2}, E_{3}, A_{3}\right), \theta^{5}=\left(E_{3}, E_{1}, A_{2}\right), \theta^{6}=\varepsilon$. From $A_{2} \theta=E_{3}$ it follows

$$
\begin{equation*}
A_{1}={ }^{(132) \pi_{2}} A_{2} \tag{43}
\end{equation*}
$$

The equality $A_{3} \theta=A_{2}$ implies $A_{3} \theta^{6}=A_{2} \theta^{5}$, so

$$
\begin{equation*}
A_{3}=A_{2}\left(E_{3}, E_{1}, A_{2}\right) \tag{44}
\end{equation*}
$$

From $A_{1} \theta=A_{3}$ it follows $A_{1} \theta^{6}=A_{2} \theta^{4}$, i.e. $A_{1}=A_{2}\left(A_{2}, E_{3}, A_{3}\right)$, using (43) and (44) in the last equality, we get

$$
\begin{equation*}
A_{2}\left(A_{2}, E_{3}, A_{2}\left(E_{3}, E_{1}, A_{2}\right)\right)=^{(132) \pi_{2}} A_{2} \tag{45}
\end{equation*}
$$

Conversely, if (43), (44) and (45) hold, then from (43) it follows $A_{2} \theta=E_{3}$. The equality (44) implies $A_{3} \theta=A_{2}$. Using (43) and (44) in (45), we obtain $A_{1}=$ $A_{2}\left(A_{2}, E_{3}, A_{3}\right)$, which implies $A_{1} \theta=A_{2}\left(E_{3}, E_{1}, A_{2}\right)$ and using (44) in the last equality, we get $A_{1} \theta=A_{3}$.
5. If $A_{1} \theta=E_{3}, A_{2} \theta=A_{2}, A_{3} \theta=A_{3}$, then from $A_{1} \theta=E_{2}$ it follows

$$
\begin{equation*}
A_{1}={ }^{(132) \pi_{2}} A_{1} \tag{46}
\end{equation*}
$$

The equality $A_{2} \theta=A_{2}$ implies

$$
\begin{equation*}
A_{1}={ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{1}\right) \tag{47}
\end{equation*}
$$

From $A_{3} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{1}={ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{1}\right) \tag{48}
\end{equation*}
$$

Conversely, if (46), (47) and (48) hold, then from (46) and (47) it follows $A_{1} \theta=E_{3}$ and $A_{2} \theta=A_{2}$, respectively, and (48) implies $A_{3} \theta=A_{3}$.
6. If $A_{1} \theta=E_{3}, A_{2} \theta=A_{3}, A_{3} \theta=A_{2}$, then $\theta^{2}=\left(A_{1}, E_{3}, E_{2}\right), \theta^{3}=\left(E_{3}, E_{1}, A_{1}\right)$, $\theta^{4}=\varepsilon$. From $A_{1} \theta=E_{3}$ it follows

$$
\begin{equation*}
A_{1}={ }^{(132) \pi_{2}} A_{1} \tag{49}
\end{equation*}
$$

From $A_{2} \theta=A_{3}$ it follows $A_{2} \theta^{2}=A_{2}$, i.e. $A_{2}\left(A_{1}, E_{3}, E_{2}\right)=A_{2}$, so

$$
\begin{equation*}
A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{2}\right) \tag{50}
\end{equation*}
$$

The equality $A_{3} \theta=A_{2}$ implies $A_{3} \theta^{4}=A_{2} \theta^{3}$, so $A_{3}=A_{2}\left(E_{3}, E_{1}, A_{1}\right)$. Using (50) in the last equality, we get

$$
\begin{equation*}
A_{3}=A_{2}\left(E_{3}, E_{1},{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{2}\right)\right) \tag{51}
\end{equation*}
$$

Conversely, if (49), (50) and (51) hold, then (49) implies $A_{1} \theta=E_{3}$, therefore $\theta^{2}=$ $\left(A_{1}, E_{3}, E_{2}\right), \theta^{3}=\left(E_{3}, E_{1}, A_{1}\right)$ and $\theta^{4}=\varepsilon$. From (50) it follows $A_{2}\left(A_{1}, E_{3}, E_{2}\right)=$ $A_{2}$, so $A_{2} \theta^{2}=A_{2}$, which implies $A_{2} \theta^{3}=A_{2} \theta$. Using (50) in (51), we obtain $A_{3}=A_{2}\left(E_{3}, E_{1}, A_{1}\right)$, so $A_{3}=A_{2} \theta^{3}$. From $A_{2} \theta^{3}=A_{2} \theta$. and $A_{3}=A_{2} \theta^{3}$ it follows $A_{2} \theta=A_{3}$. The equality $A_{3}=A_{2} \theta^{3}$ also implies $A_{3} \theta=A_{2}$.
Lemma 2.5. The triplet $\left(A_{1}, E_{1}, E_{2}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{3}={ }^{(132) \pi_{1}} A_{1}, A_{2}=A_{1}\left(A_{1}, E_{1}, E_{2}\right)$ and $A_{1}\left(E_{3},{ }^{(132) \pi_{1}} A_{1}, A_{1}\left(A_{1}, E_{1}, E_{2}\right)\right)=E_{2}$;
2. $A_{1}={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{1}, E_{2}\right), A_{2}={ }^{\pi_{3}} A_{3}\left(E_{2}, E_{3}, A_{3}\right)$ and $A_{3}\left(E_{3},{ }^{\pi_{3}} A_{3}\left(E_{2}, E_{3}, A_{3}\right),{ }^{\pi_{1}} A_{3}\left(A_{3}, E_{1}, E_{2}\right)\right)=A_{3} ;$
3. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{1}, E_{2}\right), A_{3}={ }^{\pi_{3}} A_{2}\left(E_{2}, E_{3}, A_{2}\right)$ and $A_{2}\left(E_{3},{ }^{\pi_{3}} A_{2}\left(E_{2}, E_{3}, A_{2}\right),{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{1}, E_{2}\right)\right)=A_{2} ;$
4. $A_{2}={ }^{(132) \pi_{3}} A_{1}, A_{3}=A_{1}\left(A_{1}, E_{1}, E_{2}\right)$ and $A_{1}\left(E_{3},{ }^{(132) \pi_{3}} A_{1}, A_{1}\left(A_{1}, E_{1}, E_{2}\right)\right)=E_{2} ;$
5. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{1}, E_{2}\right)={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{1}, E_{2}\right)$ and $A_{1}={ }^{(123) \pi_{1}} A_{1}$;
6. $A_{1}={ }^{\pi_{2}} A_{2}\left(E_{3}, A_{2}, E_{1}\right), A_{3}=A_{2}\left({ }^{\left(\pi_{2}\right.} A_{2}\left(E_{3}, A_{2}, E_{1}\right), E_{1}, E_{2}\right)$ and $A_{1}={ }^{(123) \pi_{1}} A_{1}$.

The proof is analogous to that of Lemma 2.4.
Lemma 2.6. The triplet $\left(A_{1}, E_{2}, E_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(A_{1}, E_{2}, E_{1}\right), A_{3}={ }^{(13) \pi_{3}} A_{1}$ and $A_{1}\left({ }^{(13) \pi_{3}} A_{1}, E_{2}, A_{1}\left(A_{1}, E_{2}, E_{1}\right)\right)=E_{1} ;$
2. $A_{1}={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{2}, E_{1}\right), A_{2}={ }^{\pi_{3}} A_{3}\left(E_{3}, E_{2}, A_{3}\right)$ and $A_{3}\left({ }^{\pi_{3}} A_{3}\left(E_{3}, E_{2}, A_{3}\right), E_{2},{ }^{\pi_{1}} A_{3}\left(A_{3}, E_{2}, E_{1}\right)\right)=A_{3} ;$
3. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{2}, E_{1}\right), A_{3}={ }^{\pi_{3}} A_{2}\left(E_{3}, E_{2}, A_{2}\right)$ and $A_{2}\left({ }^{\pi_{3}} A_{2}\left(E_{3}, E_{2}, A_{2}\right), E_{2},{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{2}, E_{1}\right)\right)=A_{2} ;$
4. $A_{1}={ }^{(13) \pi_{1}} A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{2}, E_{1}\right)={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{2}, E_{1}\right)$;
5. $A_{3}=A_{1}\left(A_{1}, E_{2}, E_{1}\right), A_{2}={ }^{(13) \pi_{3}} A_{1}$ and $A_{1}\left({ }^{(13) \pi_{3}} A_{1}, E_{2}, A_{1}\left(A_{1}, E_{2}, E_{1}\right)\right)=E_{3}$.

The proof is analogous to that of Lemma 2.3.
Lemma 2.7. The triplet $\left(E_{1}, E_{3}, A_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(E_{1}, E_{3}, A_{1}\right), A_{3}={ }^{(23) \pi_{2}} A_{1}$ and $A_{1}\left(E_{1}, A_{1}\left(E_{1}, E_{3}, A_{1}\right),{ }^{(23) \pi_{2}} A_{1}\right)=E_{2} ;$
2. $A_{1}={ }^{\pi_{3}} A_{3}\left(E_{1}, E_{3}, A_{3}\right), A_{2}={ }^{\pi_{2}} A_{3}\left(E_{1}, A_{3}, E_{2}\right)$ and $A_{3}\left(E_{1},{ }^{\pi_{3}} A_{3}\left(E_{1}, E_{3}, A_{3}\right),{ }^{\pi_{2}} A_{3}\left(E_{1}, A_{3}, E_{2}\right)\right)=A_{3} ;$
3. $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{1}, E_{3}, A_{2}\right), A_{3}={ }^{\pi_{2}} A_{2}\left(E_{1}, A_{2}, E_{2}\right)$ and $A_{2}\left(E_{1},{ }^{\pi_{3}} A_{2}\left(E_{1}, E_{3}, A_{2}\right),{ }^{\pi_{2}} A_{2}\left(E_{1}, A_{2}, E_{2}\right)\right)=A_{2} ;$
4. $A_{3}=A_{1}\left(E_{1}, E_{3}, A_{1}\right), A_{2}={ }^{(23) \pi_{2}} A_{1}$ and $A_{1}\left(E_{1}, A_{1}\left(E_{1}, E_{3}, A_{1}\right),{ }^{(23) \pi_{2}} A_{1}\right)=E_{2} ;$
5. $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{1}, E_{3}, A_{2}\right)={ }^{\pi_{3}} A_{3}\left(E_{1}, E_{3}, A_{3}\right)$ and $A_{1}={ }^{(23) \pi_{3}} A_{1}$.

The proof is analogous to that of Lemma 2.3.
Lemma 2.8. The triplet $\left(E_{3}, E_{1}, A_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{1}={ }^{(123) \pi_{3}} A_{3}, A_{2}=A_{3}\left(E_{2}, A_{3}, E_{1}\right)$ and
$A_{3}\left(A_{3}, A_{3}\left(E_{2}, A_{3}, E_{1}\right), E_{2}\right)={ }^{(123) \pi_{3}} A_{3} ;$
2. $A_{1}={ }^{\pi_{3}} A_{3}\left(E_{3}, E_{1}, A_{3}\right), A_{2}={ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{1}\right)$ and $A_{3}\left({ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{1}\right),{ }^{\pi_{3}} A_{3}\left(E_{3}, E_{1}, A_{3}\right), E_{2}\right)=A_{3}$
3. $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{3}, E_{1}, A_{2}\right), A_{3}={ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{1}\right)$ and $A_{2}\left({ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{1}\right),{ }^{\pi_{3}} A_{2}\left(E_{3}, E_{1}, A_{2}\right), E_{2}\right)=A_{2} ;$
4. $A_{1}={ }^{(123) \pi_{3}} A_{2}, A_{3}=A_{2}\left(E_{2}, A_{2}, E_{1}\right)$ and $A_{2}\left(A_{2}, A_{2}\left(E_{2}, A_{2}, E_{1}\right), E_{2}\right)={ }^{(123) \pi_{3}} A_{2} ;$
5. $A_{1}\left(E_{3}, E_{1}, A_{1}\right)=E_{2}, A_{1}={ }^{\pi_{3}} A_{2}\left(E_{3}, E_{1}, A_{2}\right)={ }^{\pi_{3}} A_{3}\left(E_{3}, E_{1}, A_{3}\right)$;
6. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{2}\right), A_{3}=A_{2}\left(E_{2},{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{2}\right), E_{1}\right)$ and $A_{1}={ }^{(123) \pi_{3}} A_{1}$.

The proof is analogous to that of Lemma 2.4.

Lemma 2.9. The triplet $\left(E_{1}, A_{1}, E_{3}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(E_{1}, A_{1}, E_{3}\right), A_{3}={ }^{\pi_{2}} A_{1}$ and $A_{1}\left(E_{1}, A_{1}\left(E_{1}, A_{1}, E_{3}\right), E_{3}\right)={ }^{\pi_{2}} A_{1} ;$
2. $A_{3}=A_{1}\left(E_{1}, A_{1}, E_{3}\right), A_{2}={ }^{\pi_{2}} A_{1} \quad$ and $A_{1}\left(E_{1}, A_{1}\left(E_{1}, A_{1}, E_{3}\right), E_{3}\right)={ }^{\pi_{2}} A_{1} ;$
3. $A_{1}={ }^{\pi_{2}} A_{2}\left(E_{1}, A_{3}, E_{3}\right)={ }^{\pi_{2}} A_{3}\left(E_{1}, A_{2}, E_{3}\right)$.

The proof is analogous to that of Lemma 2.1.
Lemma 2.10. The triplet $\left(E_{3}, A_{1}, E_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{3}={ }^{(13) \pi_{2}} A_{1}, A_{2}=A_{1}\left(E_{3}, A_{1}, E_{1}\right)$ and $A_{1}\left(E_{1}, A_{1}\left(E_{3}, A_{1}, E_{1}\right), E_{3}\right)={ }^{(13) \pi_{2}} A_{1} ;$
2. $A_{3}=A_{1}\left(E_{3}, A_{1}, E_{1}\right), A_{2}={ }^{(13) \pi_{2}} A_{1}$ and $A_{1}\left(E_{1}, A_{1}\left(E_{3}, A_{1}, E_{1}\right), E_{3}\right)={ }^{(13) \pi_{2}} A_{1} ;$
3. $A_{1}=\pi_{2} A_{2}\left(E_{3}, A_{2}, E_{1}\right)={ }^{\pi_{2}} A_{3}\left(E_{3}, A_{3}, E_{1}\right)$;
4. $A_{1}\left(E_{3}, A_{1}, E_{1}\right)=E_{2}, A_{3}=A_{2}\left(E_{3}, A_{1}, E_{1}\right)$.

The proof is analogous to that of Lemma 2.2.
Lemma 2.11. The triplet $\left(A_{1}, E_{1}, E_{3}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(A_{1}, E_{1}, E_{3}\right), A_{3}={ }^{(12) \pi_{2}} A_{1}$ and $A_{1}\left({ }^{(12) \pi_{2}} A_{1}, A_{1}\left(A_{1}, E_{1}, E_{3}\right), E_{3}\right)=E_{2} ;$
2. $A_{1}={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{1}, E_{3}\right), A_{2}={ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{3}\right)$ and $A_{3}\left({ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{3}\right),{ }^{\pi_{1}} A_{3}\left(A_{3}, E_{1}, E_{3}\right), E_{3}\right)=A_{3} ;$
3. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{1}, E_{3}\right), A_{3}={ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{3}\right)$ and $A_{2}\left({ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{3}\right),{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{1}, E_{3}\right), E_{3}\right)=A_{2} ;$
4. $A_{3}=A_{1}\left(A_{1}, E_{1}, E_{3}\right), A_{2}={ }^{(12) \pi_{2}} A_{1}$ and $A_{1}\left({ }^{(12) \pi_{2}} A_{1}, A_{1}\left(A_{1}, E_{1}, E_{3}\right), E_{3}\right)=E_{2} ;$
5. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{1}, E_{3}\right)={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{1}, E_{3}\right)$ and $A_{1}={ }^{(12) \pi_{1}} A_{1}$.

The proof is analogous to that of Lemma 2.3.
Lemma 2.12. The triplet $\left(A_{1}, E_{3}, E_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(A_{1}, E_{3}, E_{1}\right), A_{3}={ }^{(123) \pi_{2}} A_{1}$ and $A_{1}\left(E_{2}, A_{1}\left(A_{1}, E_{3}, E_{1}\right),{ }^{(123) \pi_{2}} A_{1}\right)=E_{3} ;$
2. $A_{1}={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{3}, E_{1}\right), A_{2}={ }^{\pi_{2}} A_{3}\left(E_{3}, A_{3}, E_{2}\right)$ and $A_{3}\left(E_{2},{ }^{\pi_{1}} A_{3}\left(A_{3}, E_{3}, E_{1}\right),{ }^{\pi_{2}} A_{3}\left(E_{3}, A_{3}, E_{2}\right)\right)=A_{3} ;$
3. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{1}\right), A_{3}={ }^{\pi_{2}} A_{2}\left(E_{3}, A_{2}, E_{2}\right)$ and $A_{2}\left(E_{2},{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{1}\right),{ }^{\pi_{2}} A_{2}\left(E_{3}, A_{2}, E_{2}\right)\right)=A_{2} ;$
4. $A_{2}={ }^{(123) \pi_{2}} A_{1}, A_{3}=A_{1}\left(A_{1}, E_{3}, E_{1}\right)$ and $A_{1}\left(E_{2}, A_{1}\left(A_{1}, E_{3}, E_{1}\right),{ }^{(123) \pi_{2}} A_{1}\right)=E_{3} ;$
5. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{1}\right)={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{3}, E_{1}\right)$ and $A_{1}={ }^{(132) \pi_{1}} A_{1}$;
6. $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{2}, E_{1}, A_{2}\right), A_{3}=A_{2}\left(E_{3},{ }^{\pi_{3}} A_{2}\left(E_{2}, E_{1}, A_{2}\right), E_{2}\right)$ and
$A_{1}={ }^{(132)}{ }^{\pi_{1}} A_{1}$.
The proof is similar to the proof of Lemma 2.4.
Lemma 2.13. The triplet $\left(E_{2}, E_{3}, A_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:
7. $A_{2}=A_{1}\left(E_{2}, E_{3}, A_{1}\right), A_{3}={ }^{(123) \pi_{1}} A_{1}$ and $A_{1}\left(A_{1}\left(E_{2}, E_{3}, A_{1}\right),{ }^{(123) \pi_{1}} A_{1}, E_{1}\right)=E_{2} ;$
8. $A_{1}={ }^{\pi_{3}} A_{3}\left(E_{2}, E_{3}, A_{3}\right), A_{2}={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{1}, E_{2}\right) \quad$ and $A_{3}\left({ }^{\pi_{3}} A_{3}\left(E_{2}, E_{3}, A_{3}\right),{ }^{\pi_{1}} A_{3}\left(A_{3}, E_{1}, E_{2}\right), E_{1}\right)=A_{3} ;$
9. $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{2}, E_{3}, A_{2}\right), A_{3}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{1}, E_{2}\right)$ and $A_{2}\left({ }^{\pi_{3}} A_{2}\left(E_{2}, E_{3}, A_{2}\right),{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{1}, E_{2}\right), E_{1}\right)=A_{2} ;$
10. $A_{3}=A_{1}\left(E_{2}, E_{3}, A_{1}\right), A_{2}=(123) \pi_{1} A_{1}$ and $A_{1}\left(A_{1}\left(E_{2}, E_{3}, A_{1}\right),{ }^{(123) \pi_{1}} A_{1}, E_{1}\right)=E_{2} ;$
11. $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{2}, E_{3}, A_{2}\right)={ }^{\pi_{3}} A_{3}\left(E_{2}, E_{3}, A_{3}\right) \quad$ and $\quad A_{1}={ }^{(132) \pi_{3}} A_{1}$;
12. $A_{1}={ }^{\pi_{2}} A_{2}\left(E_{3}, A_{2}, E_{1}\right), A_{3}=A_{2}\left(E_{2}, E_{3},{ }^{\pi_{2}} A_{2}\left(E_{3}, A_{2}, E_{1}\right)\right)$ and $A_{1}={ }^{(132) \pi_{3}} A_{1}$.

The proof is similar to the proof of Lemma ??.
Lemma 2.14. The triplet $\left(E_{3}, E_{2}, A_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(E_{3}, E_{2}, A_{1}\right), A_{3}={ }^{(123) \pi_{1}} A_{1}$ and $A_{1}\left(A_{1}\left(E_{3}, E_{2}, A_{1}\right), E_{2},{ }^{(123) \pi_{1}} A_{1}\right)=E_{1} ;$
2. $A_{1}={ }^{\pi_{3}} A_{3}\left(E_{3}, E_{2}, A_{3}\right), A_{2}={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{2}, E_{1}\right)$ and $A_{3}\left({ }^{\pi_{3}} A_{3}\left(E_{3}, E_{2}, A_{3}\right), E_{2},{ }^{\pi_{1}} A_{3}\left(A_{3}, E_{2}, E_{1}\right)\right)=A_{3} ;$
3. $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{3}, E_{2}, A_{2}\right), A_{3}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{2}, E_{1}\right)$ and $A_{2}\left({ }^{\pi_{3}} A_{2}\left(E_{3}, E_{2}, A_{2}\right), E_{2},{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{2}, E_{1}\right)\right)=A_{2} ;$
4. $A_{1}={ }^{(123) \pi_{3}} A_{2}, A_{3}=A_{2}\left(A_{2}, E_{2}, E_{1}\right)$ and $A_{2}\left(A_{2}\left(A_{2}, E_{2}, E_{1}\right)\right)=^{(123) \pi_{3}} A_{2}$;
5. $A_{1}\left(E_{3}, E_{2}, A_{1}\right)=E_{1}, A_{1}=^{\pi_{3}} A_{2}\left(E_{3}, E_{2}, A_{2}\right)={ }^{\pi_{3}} A_{3}\left(E_{3}, E_{2}, A_{3}\right)$.

The proof is similar to the proof of Lemma 2.3.
Lemma 2.15. The triplet $\left(E_{2}, A_{1}, E_{3}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(E_{2}, A_{1}, E_{3}\right), A_{3}={ }^{(12) \pi_{1}} A_{1} \quad$ and $A_{1}\left(A_{1}\left(E_{2}, A_{1}, E_{3}\right),{ }^{(12) \pi_{1}} A_{1}, E_{3}\right)=E_{1}$;
2. $A_{1}={ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{3}\right), A_{2}={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{1}, E_{3}\right)$ and $A_{3}\left({ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{3}\right),{ }^{\pi_{1}} A_{3}\left(A_{3}, E_{1}, E_{3}\right), E_{3}\right)=A_{3}$
3. $A_{1}={ }^{\pi_{1}} A_{2}\left(E_{2}, A_{2}, E_{3}\right), A_{3}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{1}, E_{3}\right) \quad$ and $A_{2}\left({ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{3}\right),{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{1}, E_{3}\right), E_{3}\right)=A_{2} ;$
4. $A_{3}=A_{1}\left(E_{2}, A_{1}, E_{3}\right), A_{2}={ }^{(12) \pi_{1}} A_{1}$ and $A_{1}\left(A_{1}\left(E_{2}, A_{1}, E_{3}\right),{ }^{(12) \pi_{1}} A_{1}, E_{3}\right)=E_{1} ;$
5. $A_{1}={ }^{\pi_{2}} A_{2}\left(E_{2}, A_{2}, E_{3}\right)={ }^{\pi_{2}} A_{3}\left(E_{2}, A_{3}, E_{3}\right) \quad$ and $\quad A_{1}={ }^{(12) \pi_{2}} A_{1}$.

The proof is similar to the proof of Lemma 2.3.

Lemma 2.16. The triplet $\left(E_{3}, A_{1}, E_{2}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{3}={ }^{(132) \pi_{1}} A_{1}, A_{2}=A_{1}\left(E_{3}, A_{1}, E_{2}\right)$ and
$A_{1}\left(A_{1}\left(E_{3}, A_{1}, E_{2}\right), E_{1},{ }^{(132) \pi_{1}} A_{1}\right)=E_{3} ;$
2. $A_{1}={ }^{\pi_{2}} A_{3}\left(E_{3}, A_{3}, E_{2}\right), A_{2}={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{3}, E_{1}\right)$ and $A_{3}\left({ }^{\pi_{2}} A_{3}\left(E_{3}, A_{3}, E_{2}\right), E_{1},{ }^{\pi_{1}} A_{3}\left(A_{3}, E_{3}, E_{1}\right)\right)=A_{3} ;$
3. $A_{1}={ }^{\pi_{2}} A_{2}\left(E_{3}, A_{2}, E_{2}\right), A_{3}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{1}\right)$ and
$A_{2}\left({ }^{\pi_{2}} A_{2}\left(E_{3}, A_{2}, E_{2}\right), E_{1},{ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{1}\right)\right)=A_{2} ;$
4. $A_{2}={ }^{(132) \pi_{1}} A_{1}, A_{3}=A_{1}\left(E_{3}, A_{1}, E_{2}\right)$ and
$A_{1}\left(A_{1}\left(E_{3}, A_{1}, E_{2}\right), E_{1},{ }^{(132) \pi_{1}} A_{1}\right)=E_{3} ;$
5. $A_{1}={ }^{\pi_{2}} A_{2}\left(E_{3}, A_{2}, E_{2}\right)={ }^{\pi_{2}} A_{3}\left(E_{3}, A_{3}, E_{2}\right)$ and $A_{1}={ }^{(132) \pi_{2}} A_{1}$;
6. $A_{1}={ }^{\pi_{3}} A_{2}\left(E_{2}, E_{1}, A_{2}\right), A_{3}=A_{2}\left({ }^{\pi_{3}} A_{2}\left(E_{2}, E_{1}, A_{2}\right), E_{3}, E_{1}\right)$ and $A_{1}={ }^{(132) \pi_{2}} A_{1}$.

The proof is similar to the proof of Lemma 2.4.
Lemma 2.17. The triplet $\left(A_{1}, E_{2}, E_{3}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{2}=A_{1}\left(A_{1}, E_{2}, E_{3}\right), A_{3}={ }^{\pi_{1}} A_{1}$ and $A_{1}\left(A_{1}\left(A_{1}, E_{2}, E_{3}\right), E_{2}, E_{3}\right)={ }^{\pi_{1}} A_{1} ;$
2. $A_{3}=A_{1}\left(A_{1}, E_{2}, E_{3}\right), A_{2}={ }^{\pi_{1}} A_{1}$ and $A_{1}\left(A_{1}\left(A_{1}, E_{2}, E_{3}\right), E_{2}, E_{3}\right)={ }^{\pi_{1}} A_{1} ;$
3. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{3}, E_{2}, E_{3}\right)={ }^{\pi_{1}} A_{3}\left(A_{2}, E_{2}, E_{3}\right)$.

The proof is similar to the proof of Lemma 2.1.
Lemma 2.18. The triplet $\left(A_{1}, E_{3}, E_{2}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{3}={ }^{(23) \pi_{1}} A_{1}, A_{2}=A_{1}\left(A_{1}, E_{3}, E_{2}\right)$ and
$A_{1}\left(A_{1}\left(A_{1}, E_{3}, E_{2}\right), E_{2}, E_{3}\right)={ }^{(23) \pi_{1}} A_{1} ;$
2. $A_{3}=A_{1}\left(A_{1}, E_{3}, E_{2}\right), A_{2}={ }^{(23) \pi_{1}} A_{1}$ and $A_{1}\left(A_{1}\left(A_{1}, E_{3}, E_{2}\right), E_{2}, E_{3}\right)={ }^{(23) \pi_{1}} A_{1} ;$
3. $A_{1}={ }^{\pi_{1}} A_{2}\left(A_{2}, E_{3}, E_{2}\right)={ }^{\pi_{1}} A_{3}\left(A_{3}, E_{3}, E_{2}\right)$;
4. $A_{3}=A_{2}\left(A_{1}, E_{3}, E_{2}\right)$ and $A_{1}\left(A_{1}, E_{3}, E_{2}\right)=E_{1}$.

The proof is similar to the proof of Lemma 2.2.
From Lemmas 2.1-2.18 we get the following theorem.
Theorem 1. There exist precisely 87 orthogonal systems consisting of three ternary quasigroup operations and the ternary selectors, that admit at least one nontrivial paratopy, which components are two ternary selectors and a ternary quasigroup operation.

## 3. Paratopies consisting of three ternary selectors

In the third section it is shown that there exist precisely 18 orthogonal systems $\Sigma=\left\{A_{1}, A_{2}, A_{3}, E_{1}, E_{2}, E_{3}\right\}$, consisting of three ternary quasigroup operations $A_{1}, A_{2}, A_{3}$ and the ternary selectors, which admit at least one nontrivial paratopy, which components are three ternary selectors.

Lemma 3.1. The triplet $\left(E_{1}, E_{3}, E_{2}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{1}={ }^{(23)} A_{1}, A_{2}={ }^{(23)} A_{2}, A_{3}={ }^{(23)} A_{3}$;
2. $A_{3}={ }^{(23)} A_{2}, A_{1}={ }^{(23)} A_{1}$;
3. $A_{2}={ }^{(23)} A_{1}, A_{3}={ }^{(23)} A_{3}$;
4. $A_{3}={ }^{(23)} A_{1}, A_{2}={ }^{(23)} A_{2}$.

Proof. Let the triplet $\left(E_{1}, E_{3}, E_{2}\right)$ be a paratopy of the system $\Sigma$. As $E_{1} \theta=$ $E_{1}, E_{2} \theta=E_{3}, E_{3} \theta=E_{2}$, we obtain $\Sigma \theta=\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta, E_{1}, E_{2}, E_{3}\right\}$, that is $\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta\right\}=\left\{A_{1}, A_{2}, A_{3}\right\}$.

1. If $A_{1} \theta=A_{1}, A_{2} \theta=A_{2}, A_{3} \theta=A_{3}$, then $A_{1} \theta=A_{1}$ implies

$$
\begin{equation*}
A_{1}={ }^{(23)} A_{1} \tag{52}
\end{equation*}
$$

From $A_{2} \theta=A_{2}$ it follows

$$
\begin{equation*}
A_{2}={ }^{(23)} A_{2} \tag{53}
\end{equation*}
$$

The equality $A_{3} \theta=A_{3}$ implies

$$
\begin{equation*}
A_{3}={ }^{(23)} A_{3} . \tag{54}
\end{equation*}
$$

Conversely, if (52), (53) and (54) hold, then (52) implies $A_{1} \theta=A_{1}$, from (53) it follows $A_{2} \theta=A_{2}$ and (54) implies $A_{3} \theta=A_{3}$.
2. If $A_{1} \theta=A_{1}, A_{2} \theta=A_{3}, A_{3} \theta=A_{2}$, then $A_{1} \theta=A_{1}$ implies

$$
\begin{equation*}
A_{1}={ }^{(23)} A_{1} \tag{55}
\end{equation*}
$$

From $A_{2} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{3}={ }^{(23)} A_{2} \tag{56}
\end{equation*}
$$

Conversely, if (55) and (56) hold, then (55) implies $A_{1} \theta=A_{1}$ and from (56) it follows $A_{2} \theta=A_{3}$. Also, (56) implies $A_{3} \theta=A_{2}$.
3. If $A_{1} \theta=A_{2}, A_{2} \theta=A_{1}, A_{3} \theta=A_{3}$, then $A_{1} \theta=A_{2}$ implies

$$
\begin{equation*}
A_{2}={ }^{(23)} A_{1} \tag{57}
\end{equation*}
$$

From $A_{3} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{3}={ }^{(23)} A_{3} \tag{58}
\end{equation*}
$$

Conversely, if (57) and (58) hold, then (57) implies $A_{1} \theta=A_{2}$ and from (58) it follows $A_{3} \theta=A_{3}$. Also, (57) implies $A_{2} \theta=A_{1}$.
4. If $A_{1} \theta=A_{2}, A_{2} \theta=A_{3}, A_{3} \theta=A_{1}$, then $\theta^{2}=\varepsilon$. The equalities $A_{1} \theta=A_{2}$ and $A_{2} \theta=A_{3}$ imply $A_{1}=A_{1} \theta^{2}=A_{2} \theta=A_{3}$, which is a contradiction, as $\Sigma$ is an orthogonal system of quasigroups.
5. If $A_{1} \theta=A_{3}, A_{2} \theta=A_{2}, A_{3} \theta=A_{1}$, then $A_{2} \theta=A_{2}$ implies

$$
\begin{equation*}
A_{2}={ }^{(23)} A_{2} \tag{59}
\end{equation*}
$$

From $A_{1} \theta=A_{3}$ it follows

$$
\begin{equation*}
A_{3}={ }^{(23)} A_{1} \tag{60}
\end{equation*}
$$

Conversely, if (59) and (60) hold, then (59) implies $A_{2} \theta=A_{2}$ and from (60) it follows $A_{1} \theta=A_{3}$. Also, (59) implies $A_{3} \theta=A_{1}$.
6. If $A_{1} \theta=A_{3}, A_{2} \theta=A_{1}, A_{3} \theta=A_{2}$, then $\theta^{2}=\varepsilon$. The equalities $A_{1} \theta=A_{3}$ and $A_{3} \theta=A_{2}$ imply $A_{1}=A_{1} \theta^{2}=A_{3} \theta=A_{2}$, which is a contradiction, as $\Sigma$ is an orthogonal system of quasigroups.

Lemma 3.2. The triplet $\left(E_{2}, E_{1}, E_{3}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{1}={ }^{(12)} A_{1}, A_{2}={ }^{(12)} A_{2}, A_{3}={ }^{(12)} A_{3}$;
2. $A_{3}={ }^{(12)} A_{2}, A_{1}={ }^{(12)} A_{1}$;
3. $A_{2}={ }^{(12)} A_{1}, A_{3}={ }^{(12)} A_{3}$;
4. $A_{3}={ }^{(12)} A_{1}, A_{2}={ }^{(12)} A_{2}$.

The proof is similar to the proof of Lemma 3.1.
Lemma 3.3. The triplet $\left(E_{3}, E_{2}, E_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{1}={ }^{(13)} A_{1}, A_{2}={ }^{(13)} A_{2}, A_{3}={ }^{(13)} A_{3}$;
2. $A_{3}={ }^{(13)} A_{2}, A_{1}={ }^{(13)} A_{1}$;
3. $A_{2}={ }^{(13)} A_{1}, A_{3}={ }^{(13)} A_{3}$;
4. $A_{3}={ }^{(13)} A_{1}, A_{2}={ }^{(13)} A_{2}$.

The proof is similar to the proof of Lemma 3.1.
Lemma 3.4. The triplet $\left(E_{2}, E_{3}, E_{1}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{1}={ }^{(132)} A_{1}, A_{2}={ }^{(132)} A_{2}, \quad A_{3}={ }^{(132)} A_{3}$;
2. $A_{2}={ }^{(132)} A_{1}, A_{3}={ }^{(123)} A_{1}$;
3. $A_{3}={ }^{(132)} A_{1}, A_{2}={ }^{(123)} A_{1}$.

Proof. Let the triplet $\left(E_{2}, E_{3}, E_{1}\right)$ be a paratopy of the system $\Sigma$. As $E_{1} \theta=$ $E_{2}, E_{2} \theta=E_{3}, E_{3} \theta=E_{1}$, we obtain $\Sigma \theta=\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta, E_{1}, E_{2}, E_{3}\right\}$, that is $\left\{A_{1} \theta, A_{2} \theta, A_{3} \theta\right\}=\left\{A_{1}, A_{2}, A_{3}\right\}$.

1. If $A_{1} \theta=A_{1}, A_{2} \theta=A_{2}, A_{3} \theta=A_{3}$, then then $A_{1} \theta=A_{1}$ implies

$$
\begin{equation*}
A_{1}={ }^{(132)} A_{1} \tag{61}
\end{equation*}
$$

From $A_{2} \theta=A_{2}$ it follows

$$
\begin{equation*}
A_{2}={ }^{(132)} A_{2} \tag{62}
\end{equation*}
$$

The equality $A_{3} \theta=A_{3}$ implies

$$
\begin{equation*}
A_{3}={ }^{(132)} A_{3} \tag{63}
\end{equation*}
$$

Conversely, if (61), (62) and (63) hold, then (61) implies $A_{1} \theta=A_{1}$, from (61) it follows $A_{2} \theta=A_{2}$ and (61) implies $A_{3} \theta=A_{3}$.
2. If $A_{1} \theta=A_{1}, A_{2} \theta=A_{3}, A_{3} \theta=A_{2}$, then $\theta^{2}=\left(E_{3}, E_{1}, E_{2}\right), \theta^{3}=\varepsilon$. The equalities $A_{2} \theta=A_{3}$ and $A_{3} \theta=A_{2}$ imply $A_{2}=A_{2} \theta^{3}=A_{3} \theta^{2}=A_{2} \theta=A_{3}$, which is a contradiction, as $\Sigma$ is an orthogonal system of quasigroup.
3. If $A_{1} \theta=A_{2}, A_{2} \theta=A_{1}, A_{3} \theta=A_{3}$, then $\theta^{2}=\left(E_{3}, E_{1}, E_{2}\right), \theta^{3}=\varepsilon$. The equalities $A_{1} \theta=A_{2}$ and $A_{2} \theta=A_{1}$ imply $A_{1}=A_{1} \theta^{3}=A_{2} \theta^{2}=A_{1} \theta=A_{2}$, which is a contradiction, as $\Sigma$ is an orthogonal system of quasigroup.
4. If $A_{1} \theta=A_{2}, A_{2} \theta=A_{3}, A_{3} \theta=A_{1}$, then $A_{1} \theta=A_{2}$ implies

$$
\begin{equation*}
A_{2}={ }^{(132)} A_{1} \tag{64}
\end{equation*}
$$

From $A_{2} \theta=A_{3}$ it follows $A_{3}={ }^{(132)} A_{2}$. Using (64) in the last equality, we get

$$
\begin{equation*}
A_{3}={ }^{(123)} A_{1} \tag{65}
\end{equation*}
$$

Conversely, if (64) and (65) hold, then (64) implies $A_{1} \theta=A_{2}$ and from (65) it follows $A_{3} \theta=A_{1}$. Also, (64) implies $A_{2} \theta={ }^{(123)} A_{1}$. Using (65) in the last equality, we get $A_{2} \theta=A_{3}$.
5. If $A_{1} \theta=A_{3}, A_{2} \theta=A_{1}, A_{3} \theta=A_{2}$, then $A_{1} \theta=A_{3}$ implies

$$
\begin{equation*}
A_{3}={ }^{(132)} A_{1} \tag{66}
\end{equation*}
$$

From $A_{3} \theta=A_{2}$ it follows $A_{2}={ }^{(132)} A_{3}$. Using (66) in the last equality, we get

$$
\begin{equation*}
A_{2}={ }^{(123)} A_{1} \tag{67}
\end{equation*}
$$

Conversely, if (66) and (67) hold, then (66) implies $A_{1} \theta=A_{3}$ and from (67) it follows $A_{2} \theta=A_{1}$. Also, (66) implies $A_{3} \theta={ }^{(123)} A_{1}$. Using (67) in the last equality, we get $A_{3} \theta=A_{2}$.
6. If $A_{1} \theta=A_{3}, A_{2} \theta=A_{2}, A_{3} \theta=A_{1}$, then $\theta^{2}=\left(E_{3}, E_{1}, E_{2}\right), \theta^{3}=\varepsilon$. The equalities $A_{1} \theta=A_{3}$ and $A_{3} \theta=A_{1}$ imply $A_{1}=A_{1} \theta^{3}=A_{3} \theta^{2}=A_{1} \theta=A_{3}$, which is a contradiction, as $\Sigma$ is an orthogonal system of quasigroup.

Lemma 3.5. The triplet $\left(E_{3}, E_{1}, E_{2}\right)$ is a paratopy of the system $\Sigma$ if and only if one of the following conditions holds:

1. $A_{1}={ }^{(123)} A_{1}, A_{2}={ }^{(123)} A_{2}, A_{3}={ }^{(123)} A_{3}$;
2. $A_{2}={ }^{(123)} A_{1}, A_{3}={ }^{(132)} A_{1}$;
3. $A_{3}={ }^{(123)} A_{1}, A_{2}={ }^{(132)} A_{1}$.

The proof is similar to the proof of Lemma 3.4.
From Lemmas 3.1-3.5 we obtain the following theorem.
Theorem 2. There exist precisely 18 orthogonal systems, consisting of three ternary quasigroup operations and the ternary selectors, that admit at least one nontrivial paratopy, which components are three ternary selectors.

## References

[1] A. Bektenov, T. Yakubov, Systems of orthogonal n-ary operations, (Russian), Izvestiya AN Mold.SSR, Ser. fiz.-mat. nauk 3 (1974), 7 - 14.
[2] V.D. Belousov, Systems of orthogonal operations, (Russian), Matem. Sbornik 77 (119), 1968, $33-52$.
[3] V.D. Belousov, n-Ary quasigroups, (Russian), Chisinau, Shtiintsa, 1972.
[4] V.D. Belousov, Parastrofic-orthogonal quasigroups, Quasigroups and Related Systems 14 (2005), $3-51$.
[5] V.D. Belousov, T. Yakubov, On orthogonal n-ary operations, (Russian), Vopr. Kibernetiki, 16(1975), 3-17.
[6] G.B. Belyavskaya, Secret-sharing schemes and orthogonal systems of $k$-ary operations, Quasigroups and Related Systems, 17 (2009), 161 - 176.
[7] G.B. Belyavskaya, G.L. Mullen, Orthogonal hypercubes and n-ary operations, Quasigroups and Related Systems 13 (2005), $73-86$.
[8] D. Ceban, On some identities in ternary quasigroups, Studia Univ. Moldaviae, Seria Ştiinţe exacte şi economice, 92 (2016), no. 2, $40-45$.
[9] T. Evans, Latin cubes orthogonal to their transposes - a ternary analogue of Stein quasigroups, Aequationes Math. 9 (1973), 296 - 97.
[10] P. Syrbu On orthogonal and self-orthogonal n-ary operations, (Russian), Mat. Issled., 66 (1987), 121 - 129.
[11] P. Syrbu, D. Ceban, On paratopies of orthogonal systems of ternary quasigroups. I, Bul. Acad. Ştiinţe Repub. Mold. Mat. 80, (2016), no. 1, 91 - 117.

Received October 31, 2016
Faculty of Mathematics and Informatics
Moldova State University
A. Mateevici str., 27

MD2009 Chisinau
Republic of Moldova
E-mails: psyrbu@mail.md, cebandina@mail.ru

# A note on a class of gyrogroups 

Marius Tărnăuceanu


#### Abstract

We give a necessary and sufficient condition for a gyrogroup to be gyrocommutative. We also prove that under a suitable assumption two finite groups central by a 2-Engel group are isomorphic if and only if their associated gyrogroups are isomorphic.


## 1. Introduction

Gyrogroups are suitable generalization of groups, whose origin is described in [7, 8]. They share remarkable analogies with groups. In fact, every group forms a gyrogroup under the same operation. Many of classical theorems in group theory also hold for gyrogroups, including the Lagrange theorem [4], the fundamental isomorphism theorems [5], and the Cayley theorem [5] (for all these theorems see also [3]). Gyrogroup actions and related results, such as the orbit-stabilizer theorem, the orbit decomposition theorem, and the Burnside lemma have been studied in [6].

The present note deals with a connection between groups and gyrogroups, namely with the gyrogroup associated to any group central by a 2-Engel group (see [1]). We determine conditions for such a gyrogroup to be gyrocommutative and for such two gyrogroups to be isomorphic. An interesting conservative functor between a subcategory of groups and the category of gyrogroups is constructed, as well.

Recall that a groupoid $(G, \odot)$ is called a gyrogroup if its binary operation satisfies the following axioms:

1. There is an element $e \in G$ such that $e \odot a=a$ for all $a \in G$.
2. For every $a \in G$, there is an element $a^{\prime} \in G$ such that $a^{\prime} \odot a=e$.
3. For all $a, b \in G$, there is an automorphism $\operatorname{gyr}[a, b] \in \operatorname{Aut}(G, \odot)$ such that

$$
a \odot(b \odot c)=(a \odot b) \odot \operatorname{gyr}[a, b](c) \quad \text { (left gyroassociative law) }
$$

for all $c \in G$.
4. For all $a, b \in G, \operatorname{gyr}[a \odot b, b]=\operatorname{gyr}[a, b] . \quad$ (left loop property)

Moreover, if

$$
a \odot b=\operatorname{gyr}[a, b](b \odot a) \quad \text { (gyrocommutative law) }
$$

for all $a, b \in G$, then $(G, \odot)$ is called a gyrocommutative gyrogroup.

[^8]We remark that the axioms in the above definition imply the right counterparts. In particular, any gyrogroup has a unique two-sided identity $e$, and an element $a$ of the gyrogroup has a unique two-sided inverse $a^{\prime}$. Given two elements $a, b$ of a gyrogroup $G$, the map gyr $[a, b]$ is called the gyroautomorphism generated by a and $b$. By Theorem 2.10 of [7], the gyroautomorphisms are completely determined by the gyrator identity

$$
\operatorname{gyr}[a, b](c)=(a \odot b)^{\prime} \odot[a \odot(b \odot c)]
$$

for all $a, b, c \in G$. Obviously, every group forms a gyrogroup under the same operation by defining the gyroautomorphisms to be the identity automorphism, but the converse is not in general true. From this point of view, gyrogroups suitably generalize groups.

Recall also that gyrogroup homomorphism is a map between gyrogroups that preserves the gyrogroup operations. A bijective gyrogroup homomorphism is called a gyrogroup isomorphism. We say that two gyrogroups $G_{1}$ and $G_{2}$ are isomorphic, written $G_{1} \cong G_{2}$, if there exists a gyrogroup isomorphism from $G_{1}$ to $G_{2}$. Given a gyrogroup $G$, a gyrogroup isomorphism from $G$ to itself is called a gyrogroup automorphism of $G$.

One of the most interesting purely algebraic classes of gyrogroups is introduced in [1], as follows. Define on a group $(G, \cdot)$ the binary operation

$$
a \odot b=a^{2} b a^{-1}, \forall a, b \in G
$$

Then, by Theorem 3.7 of [1], we have:
Theorem 1. $(G, \odot)$ is a gyrogroup if and only if $(G, \cdot)$ is central by a 2-Engel group.

In what follows we will call $(G, \odot)$ the gyrogroup associated to a given group $(G, \cdot)$, which is assumed to be central by a 2-Engel group. Note that in this case the gyroautomorphism generated by two elements $a$ and $b$ of $G$ is given by

$$
\operatorname{gyr}[a, b]=\varphi_{\left[a, b^{-1}\right]},
$$

where $\varphi_{\left[a, b^{-1}\right]}$ is the inner automorphism of $G$ induced by the commutator $\left[a, b^{-1}\right]$ of $a$ and $b^{-1}$.

We are now in a position to characterize the gyrocommutativity of $(G, \odot)$.
Theorem 2. $(G, \odot)$ is gyrocommutative if and only if the inner automorphism group of $(G, \cdot)$ is of exponent 3 .

Clearly, if $(G, \cdot)$ is commutative, then the binary operations • and $\odot$ coincide, and $(G, \odot)$ is gyrocommutative. Note that there is also a non- commutative group, which is central by a 2 -Engel group, such that its associated gyrogroup is gyrocommutative (e.g. the group of upper triangular matrices over $\mathbb{F}_{3}$ with diagonal $(1,1,1)$ ).

Next, let $\left(G_{1}, \cdot\right)$ and $\left(G_{2}, \cdot\right)$ be two finite groups central by a 2-Engel group, and let $\left(G_{1}, \odot\right)$ and $\left(G_{2}, \odot\right)$ be their associated gyrogroups. Clearly, if $\left(G_{1}, \cdot\right) \cong\left(G_{2}, \cdot\right)$,
then a group isomorphism from $G_{1}$ to $G_{2}$ is also a gyrogroup isomorphism from $\left(G_{1}, \odot\right)$ to $\left(G_{2}, \odot\right)$, that is, $\left(G_{1}, \odot\right) \cong\left(G_{2}, \odot\right)$. A sufficient condition for the converse to be true is given in the following theorem.
Theorem 3. If $3 \nmid\left|G_{1}\right|$, then $\left(G_{1}, \cdot\right) \cong\left(G_{2}, \cdot\right)$ if and only if $\left(G_{1}, \odot\right) \cong\left(G_{2}, \odot\right)$.
From Theorem 3 we obtain the following corollary.
Corollary 4. Let $(G, \cdot)$ be a group central by a 2-Engel group such that $3 \nmid|G|$. Then the group of all gyrogroup automorphisms of $(G, \odot)$ coincides with the group of all automorphisms of $(G, \cdot)$.

Finally, we observe that there is an interesting conservative functor $F$ between the category $\mathcal{C}$ of finite groups central by a 2-Engel group whose order is not divisible by 3 and the category of gyrogroups, which associates to each object $(G, \cdot)$ in $\mathcal{C}$ the gyrogroup $(G, \odot)$ and to each homomorphism $f$ in $\mathcal{C}$ the gyrogroup homomorphism $F(f)=f$.

Much of our notation is standard and will usually not be repeated here. Elementary notions and results on groups can be found in [2].

## 2. Proofs of the main results

Proof of Theorem 2. In our case the gyrocommutative law becomes

$$
a^{2} b a^{-1}=\varphi_{\left[a, b^{-1}\right]}\left(b^{2} a b^{-1}\right), \quad \forall a, b \in G
$$

which means

$$
b^{3} a=a b^{3}, \quad \forall a, b \in G
$$

i.e.,

$$
b^{3} \in Z(G), \quad \forall b \in G
$$

Obviously, this condition is equivalent to $\exp (\operatorname{Inn}(G))=3$ in view of the group isomorphism $G / Z(G) \cong \operatorname{Inn}(G)$.
Proof of Theorem 3. Assume that $\left(G_{1}, \odot\right) \cong\left(G_{2}, \odot\right)$ and let $f: G_{1} \longrightarrow G_{2}$ be a gyrogroup isomorphism. Then $f$ is a bijection and

$$
\begin{equation*}
f\left(a^{2} b a^{-1}\right)=f(a)^{2} f(b) f(a)^{-1}, \quad \forall a, b \in G . \tag{1}
\end{equation*}
$$

If $e_{i}$ is the identity of $G_{i}, i=1,2$, we infer that $f\left(e_{1}\right)=e_{2}$, by taking $a=b=e_{1}$ in (1). Also, by taking $b=a$ and $b=a^{-1}$ in (1), respectively, one obtain

$$
f\left(a^{2}\right)=f(a)^{2} \text { and } f\left(a^{-1}\right)=f(a)^{-1}, \quad \forall a \in G_{1} .
$$

Next, let us write (1) with $a^{-1} b a$ and $a^{-1} b^{-1}$ instead of $b$, respectively. Then

$$
\begin{equation*}
f(a b)=f(a)^{2} f\left(a^{-1} b a\right) f(a)^{-1} \tag{2}
\end{equation*}
$$

and

$$
\begin{equation*}
f\left(a b a^{-1}\right)=f(a) f(b a) f(a)^{-2} \tag{3}
\end{equation*}
$$

Replace $a$ with $a^{-1}$ in (3). Then $f\left(a^{-1} b a\right)=f(a)^{-1} f\left(b a^{-1}\right) f(a)^{2}$, which together with (2) leads to

$$
f(a b)=f(a) f\left(b a^{-1}\right) f(a)
$$

By writing this equality with $b a$ instead of $b$, we find

$$
f(a b a)=f(a) f(b) f(a), \quad \forall a, b \in G_{1} .
$$

Finally, replacing in this identity $b$ with $a^{2} b a^{-1}$, we obtain

$$
\begin{equation*}
f\left(a^{3} b\right)=f(a)^{3} f(b), \quad \forall a, b \in G_{1}, \tag{5}
\end{equation*}
$$

and taking $b=e_{1}$ in (5) gives

$$
\begin{equation*}
f\left(a^{3}\right)=f(a)^{3}, \quad \forall a \in G_{1} . \tag{6}
\end{equation*}
$$

We are now in a position to prove that $f$ is a group homomorphism.
Let $x, y \in G_{1}$. Since $3 \nmid\left|G_{1}\right|$, we have $3 \nmid o(x)$ and consequently $\operatorname{gcd}(3, o(x))=1$, i.e., $1=3 \alpha+o(x) \beta$ for some integers $\alpha$ and $\beta$. It follows that

$$
x=x^{3 \alpha+o(x) \beta}=x^{3 \alpha} x^{o(x) \beta}=x^{3 \alpha} .
$$

Then (5) and (6) lead to

$$
f(x y)=f\left(x^{3 \alpha} y\right)=f\left(\left(x^{\alpha}\right)^{3} y\right)=f\left(x^{\alpha}\right)^{3} f(y)=f\left(x^{3 \alpha}\right) f(y)=f(x) f(y)
$$

as desired. Hence $f$ is a group isomorphism, completing the proof.

## References

[1] T. Foguel and A.A. Ungar, Gyrogroups and the decomposition of groups into twisted subgroups and subgroups, Pacific J. Math. 197 (2001), 1 - 11.
[2] B. Hupert, Endliche Gruppen, I, II, Springer Verlag, Berlin, 1967, 1968.
[3] T. Suksumran, The algebra of gyrogroups: Cayley's theorem, Lagrange's theorem, and Isomorphism theorems, in Essays in Math. and Appl.: In Honor of V. Arnold, eds. T.M. Rassias and P.M. Pardalos (Springer, 2016), pp. 369-437.
[4] T. Suksumran and K. Wiboonton, Lagrange's theorem for gyrogroups and the Cauchy property, Quasigroups Related Systems 22 (2014), 283 - 294.
[5] T. Suksumran and K. Wiboonton, Isomorphism theorems for gyrogroups and L-subgyrogroups, J. Geom. Symmetry Phys. 37 (2015), $67-83$.
[6] T. Suksumran, Gyrogroup actions: A generalization of group actions, J. Algebra 454 (2016), 70 - 91.
[7] A.A. Ungar, Analytic hyperbolic geometry and Albert Einstein's Special Theory of Relativity, World Scientific, Hackensack, NJ, 2008.
[8] A.A. Ungar, A gyrovector space approach to hyperbolic geometry, Synthesis Lectures on Mathematics and Statistics 4, Morgan and Claypool, San Rafael, 2009.

# On nuclei and conuclei of $S$-quantales 

Xia Zhang and Tingyu Li


#### Abstract

S\)-quantales have been proved to be injectives in the category of $S$-posets with $S$ submultiplicative order-preserving mappings as morphisms. In this work, algebraic investigations on $S$-quantales are presented. A representation theorem of an $S$-quantale according to nuclei is obtained, quotients of an $S$-quantale with respect to nuclei and congruences are completely studied. Simultaneously, the relationship between $S$-subquantales and conuclei of an $S$-quantale is established.


## 1. Preliminary

Various quantale-like structures (quantales, locales, quantale modules, quantale algebras, unital quantales etc.) have been studied for decades and they have useful applications in algebra, logic and computer science ([3], [6], [11], [12]). In [11], algebraic properties and applications of quantales are well studied. The idea was then extended to groupoid quantales [7], involutive quantales [9], [5], sup-lattices [10], quantale mudules [4], [14], [13], and quantale algebras [15], [8], etc. Recently, Zhang and Laan in [16] introduced a new kind of quantale-like structure, named $S$-quantales. It has been shown that $S$-quantles play an important role in the theory of injectivity on the category of $S$-posets with $S$-submultiplicative orderpreserving mappings as morphisms. In fact, injectives in this category are exactly $S$-quantales. The purpose of this paper is to make a contribution on algebraic investigations of $S$-quantales. Lets us first recall some basic definitions.

In this work, $S$ is always a pomonoid, i.e., a monoid $S$ equipped with a partial order $\leqslant$ such that $s s^{\prime} \leqslant t t^{\prime}$ whenever $s \leqslant t, s^{\prime} \leqslant t^{\prime}$ in $S$. A poset $(A, \leqslant)$ together with a mapping $A \times S \rightarrow A$ (under which a pair ( $a, s$ ) maps to an element of $A$ denoted by $a s$ ) is called a right $S$-poset, denoted by $A_{S}$, if for any $a, b \in A, s, t \in S$,

1. $a(s t)=(a s) t$,
2. $a 1=a$,
3. $a \leqslant b, s \leqslant t$ imply that $a s \leqslant b t$.

A left $S$-poset can be defined similarly. In this paper we only consider right $S$-posets, therefore we will omit the word "right".

[^9]Let $A_{S}$ and $B_{S}$ be $S$-posets. A mapping $f: A_{S} \rightarrow B_{S}$ is said to be $S$ submultiplicative if $f(a) s \leqslant f(a s)$ for any $a \in A_{S}, s \in S$. We call $f$ an $S$-poset homomorphism if it preserves both $S$-actions and orders.

An $S$-poset $A_{S}$ is said to be an $S$-quantale ([16]) if
(1) the poset $A$ is a complete lattice;
(2) $(\bigvee M) s=\bigvee\{m s \mid m \in M\}$ for each subset $M$ of $A$ and each $s \in S$.

An $S$-quantale homomorphism is a mapping between $S$-quantales which preserves both $S$-actions and arbitrary joins. An $S$-subquantale of an $S$-quantale $A_{S}$ is indeed the relative subposet of $A_{S}$ which closed under $S$-actions and arbitrary joins.

We begin with properties of $S$-quantale homomorphisms and mappings between $S$-quantales with right adjoints. Then a representation theorem of quotients for $S$-quantales by nuclei is presented. The important topic of relations between the lattices of nuclei and congruences of an $S$-quantale is fully investigated. Dually, the connection on $S$-subquantales and conuclei is studied.

## 2. Mappings and homomorphisms

Let $f: P \rightarrow Q$ be a join-preserving mapping of posets. By the adjoint functor theorem ([1]), $f$ has a unique right adjoint $f_{*}: Q \rightarrow P$, fulfilling

$$
\begin{equation*}
f(x) \leqslant y \Longleftrightarrow x \leqslant f_{*}(y), \tag{1}
\end{equation*}
$$

for any $x \in P, y \in Q$, and hence

$$
\begin{equation*}
f\left(f_{*}(y)\right) \leqslant y, \quad x \leqslant f_{*}(f(x)) \tag{2}
\end{equation*}
$$

Given an $S$-quantale $Q_{S}$, and any $s \in S$, the mapping $s_{-}: Q_{S} \rightarrow Q_{S}$ defined by $s(a)=a s$ for each $a \in Q_{S}$, preserves all joins, and thus has a unique right adjoint, denoted by $s_{*}$, satisfying

$$
\begin{equation*}
s(a) \leqslant b \Longleftrightarrow a \leqslant s_{*}(b) \tag{3}
\end{equation*}
$$

and

$$
\begin{equation*}
s\left(s_{*}(a)\right) \leqslant a, a \leqslant s_{*}(s(a)), \tag{4}
\end{equation*}
$$

for each $a, b \in Q_{S}$. It holds evidently that $s_{*}(a) s \leqslant a, \forall a \in Q_{S}$.
Proposition 2.1. Let $Q_{S}$ be an $S$-quantale. Then for any $b \in Q_{S}, s, t \in S$, the following statements hold.

1. $s_{*}\left(t_{*}(b)\right)=(s t)_{*}(b)$,
2. $s_{*}(b) s=b \Longleftrightarrow\left(\exists a \in Q_{S}\right) a s=b$,
3. $s_{*}(b s)=b \Longleftrightarrow\left(\exists a \in Q_{S}\right) b=s_{*}(a)$.

Proof. We note that for any $x, b \in Q_{S}, s, t \in S$,

$$
x \leqslant s_{*}\left(t_{*}(b)\right) \Longleftrightarrow x s \leqslant t_{*}(b) \Longleftrightarrow x s t \leqslant b \Longleftrightarrow x \leqslant(s t)_{*}(b)
$$

by (3), so we obtain 1.2 and 3 can be proved similarly.
Proposition 2.2. Let $f: P_{S} \rightarrow Q_{S}$ be an $S$-quantale homomorphism. Then

$$
f_{*}\left(s_{*}(a)\right)=s_{*}\left(f_{*}(a)\right)
$$

for any $a \in Q_{S}, s \in S$.
Proof. By (1) and $f$ preserving $S$-actions, we have

$$
\begin{aligned}
f_{*}\left(s_{*}(a)\right) \leqslant s_{*}\left(f_{*}(a)\right) & \Longleftrightarrow f_{*}\left(s_{*}(a)\right) s \leqslant f_{*}(a) \Longleftrightarrow f\left(f_{*}\left(s_{*}(a)\right) s\right) \leqslant a \\
& \Longleftrightarrow f\left(f_{*}\left(s_{*}(a)\right) s \leqslant a \Longleftrightarrow f\left(f_{*}\left(s_{*}(a)\right) \leqslant s_{*}(a),\right.\right.
\end{aligned}
$$

for each $a \in Q_{S}$. But the final inequality natural follows by (2), we soon get that $f_{*}\left(s_{*}(a)\right) \leqslant s_{*}\left(f_{*}(a)\right)$. One may dually gain that $s_{*}\left(f_{*}(a)\right) \leqslant f_{*}\left(s_{*}(a)\right)$.

Recall that for a poset $P$, a monotone mapping $j$ on $P$ is said to be a closure operator if it is both increasing and idempotent.

Definition 2.3. Let $Q_{S}$ be an $S$-quantale, $j$ a closure operator on $Q_{S}$. We call $j$ a nucleus if it is $S$-submultiplicative, i.e.,

$$
j(a) s \leqslant j(a s)
$$

for each $a \in Q_{S}, s \in S$.
Lemma 2.4. Let $Q_{S}$ be an $S$-quantale, $j$ a nucleus on $Q_{S}$. Then

$$
j\left(s_{*}(a)\right) \leqslant s_{*}(j(a))
$$

for all $a \in Q_{S}, s \in S$.
Proof. Keep in mind that $s_{*}(a) s \leqslant a, \forall a \in Q_{S}, s \in S$, we immediately get that $j\left(s_{*}(a)\right) s \leqslant j\left(s_{*}(a) s\right) \leqslant j(a)$, and thus $j\left(s_{*}(a)\right) \leqslant s_{*}(j(a))$ by (3).

Lemma 2.5. Let $f: P_{S} \rightarrow Q_{S}$ be an $S$-quantale homomorphism. Then $f_{*}: Q_{S} \rightarrow$ $P_{S}$ is $S$-submultiplicative.

Proof. By $(2), f\left(f_{*}(a)\right) \leqslant a, \forall a \in Q_{S}$, it follows that $f\left(f_{*}(a) s\right)=f\left(f_{*}(a)\right) s \leqslant a s$, and hence $f_{*}(a) s \leqslant f_{*}(a s)$ by (1).

Lemma 2.6. Let $f: P_{S} \rightarrow Q_{S}$ be an $S$-quantale homomorphism. Then $f_{*} f$ is a nucleus on $P_{S}$.

Proof. If $a \leqslant b$ for $a, b \in P_{S}$, then $f(a) \leqslant f(b)$, and thus $f_{*} f(a) \leqslant f_{*} f(b)$ by the fact that $f_{*}$ preserves arbitrary meets.

Directly applying (2), we hence obtain that $a \leqslant f_{*} f(a)$ and

$$
f_{*} f(a) \leqslant f_{*} f\left(f_{*} f(a)\right)=f_{*}\left(f f_{*}\right)(f(a)) \leqslant f_{*}(f(a))
$$

for any $a \in P_{S}$. So $f_{*} f$ is a closure operator.
In addition, Lemma 2.5 provides that

$$
\left(f_{*} f\right)(a) s=\left(f_{*}(f(a)) s \leqslant f_{*}(f(a) s)=\left(f_{*} f\right)(a s),\right.
$$

for any $a \in Q_{S}, s \in S$. Consequently, $f_{*} f$ is a nucleus as desired.

## 3. Nuclei and a representation theorem

For an $S$-quantale $Q_{S}$, we write $\operatorname{Nuc}\left(Q_{S}\right)$ for the set of all nuclei on $Q_{S} . \operatorname{Nuc}\left(Q_{S}\right)$ will therefore become a complete lattice if it is equipped with the pointwise order. The following properties of nuclei can be easily gained.

Lemma 3.1. (cf. [16]) Let $Q_{S}$ be an $S$-quantale, $j$ a nucleus on $Q_{S}$. Then for any $a \in Q_{S}, s \in S, j(a s)=j(j(a) s)$.

Lemma 3.2. Let $Q_{S}$ be an $S$-quantale, $j$ a nucleus on $Q_{S}$. Then

$$
j\left(\bigvee_{i \in I} j\left(a_{i}\right)\right)=j\left(\bigvee_{i \in I} a_{i}\right), \quad \forall a_{i} \in Q_{S}, i \in I
$$

Proof. Follows from the property of $j$ being a closure operator.
Lemma 3.3. Let $Q_{S}$ be an $S$-quantale, $j, \widetilde{j} \in \operatorname{Nuc}\left(Q_{S}\right)$. Then the following statements hold.

1. $j \leqslant \widetilde{j} \Longleftrightarrow \widetilde{j} j=\widetilde{j}$;
2. $j \leqslant \widetilde{j} \Longleftrightarrow \forall x, y \in Q_{S}, j(x)=j(y) \Rightarrow \widetilde{j}(x)=\widetilde{j}(y)$.

Given a nucleus $j$ on an $S$-quantale $Q_{S}$. Write

$$
Q_{j}=\left\{a \in Q_{S} \mid j(a)=a\right\} .
$$

Then $Q_{j}$ becomes an $S$-quantale with the $S$-action defined by

$$
a \circ s=j(a s), \quad a \in A, \quad s \in S,
$$

and the order inherited from $Q_{S}$, where the joins are given by

$$
\bigvee^{j} D=j(\bigvee D)
$$

for any $D \subseteq Q_{j}$ (cf. [16]).
Proposition 3.4. Let $Q_{S}$ be an $S$-quantale, $P_{S} \subseteq Q_{S}$ an $S$-subquantale. Then $P_{S}=Q_{j}$ for some nucleus $j$ iff $P_{S}$ is closed under meets and $s_{*}(a) \in P_{S}$ whenever $a \in P_{S}$.

Proof. Suppose that $P_{S}=Q_{j}$ for some nucleus $j$ on $Q_{S}$. It is routine to check that $\wedge A \in P_{S}$ for any $A \subseteq P_{S}$. Note that for any $a \in P_{S}, j\left(s_{*}(a)\right) \leqslant s_{*}(j(a))=s_{*}(a)$ by Lemma 2.4 , one gets that $s_{*}(a) \in P_{S}$, as well.

On the contrary, define a mapping $j$ on $Q_{S}$ by

$$
j(x)=\bigwedge\left\{a \in P_{S} \mid x \leqslant a\right\}, \forall x \in Q_{S}
$$

Straightforward verification shows that $j$ is a closure operator.
For any $x \in Q_{S}, s \in S, a \in P_{S}$, since $x s \leqslant a \Leftrightarrow x \leqslant s_{*}(a)$ by (3), and $s_{*}(a) \in P_{S}$ by the assumption, it follows that

$$
j(x s) \leqslant a \Rightarrow x s \leqslant j(x s) \leqslant a \Rightarrow j(x) \leqslant s_{*}(a) \Rightarrow j(x) s \leqslant a,
$$

and results in $j(x) s \leqslant j(x s)$. Therefore, $j$ is a nucleus on $Q_{S}$.
By the definition of $j$ and the fact that $P_{S}$ being closed under meets, we finally achieve that $P_{S}=Q_{j}$.

Let $Q_{S}$ be an $S$-quantale, $\mathcal{P}(Q)$ the power set of $Q$. Define an $S$-action on $\mathcal{P}(Q)$ by

$$
I \cdot s=\{a s \mid a \in I, s \in S\}, \forall I \subseteq Q
$$

Then $\left(\mathcal{P}(Q)_{S}, \cdot, \subseteq\right)$ becomes an $S$-quantale. The following theorem provides a representation of an $S$-quantale according to quotients w.r.t. nuclei.
Theorem 3.5. (Representation Theorem) Let $Q_{S}$ be an $S$-quantale. Then there exists a nucleus $j$ on $\mathcal{P}(Q)_{S}$ such that $Q_{S} \cong \mathcal{P}(Q)_{j}$.

Proof. Define a mapping $j$ on $\mathcal{P}(Q)_{S}$ by

$$
j(I)=(\bigvee I) \downarrow, \forall I \in \mathcal{P}(Q)_{S}
$$

Clearly, $j$ is a closure operator. Suppose that $I \subseteq Q_{S}$ and $x \in j(I)$. Then $x s \leqslant(\bigvee I) s=\bigvee(I s)$ for all $s \in S$, gives that $x s \in j(I s)$. Thus $j(I) \cdot s \subseteq j(I s)$.

We note that for any $I \subseteq Q_{S}, j(I)=I$ iff $I=a \downarrow$ for some $a \in Q_{S}$. Therefore,

$$
\mathcal{P}(Q)_{j}=\left\{I \in \mathcal{P}(Q)_{S} \mid I=j(I)\right\}=\left\{I \subseteq Q_{S} \mid I=a \downarrow \text { for some } a \in Q_{S}\right\} .
$$

Now define a mapping $\sigma: Q_{S} \rightarrow \mathcal{P}(Q)_{j}$ by

$$
\sigma(a)=a \downarrow, \forall a \in Q_{S}
$$

Then $\sigma$ is certainly bijective. We remain to show that $\sigma$ is a homomorphism. By virtue of

$$
\sigma\left(\bigvee_{i \in I} a_{i}\right)=\left(\bigvee_{i \in I} a_{i}\right) \downarrow=\left(\bigvee\left(\bigcup_{i \in I} a_{i} \downarrow\right)\right) \downarrow=j\left(\bigcup_{i \in I} a_{i} \downarrow\right)=\bigvee_{i \in I}^{j} \sigma\left(a_{i}\right)
$$

for any $a_{i} \in Q_{S}, i \in I$, and

$$
\begin{aligned}
\sigma(a) \circ s & =j(\sigma(a) \cdot s)=j(a \downarrow \cdot s)=(\bigvee(a \downarrow \cdot s)) \downarrow \\
& =(\bigvee\{x s \mid x \leqslant a\}) \downarrow=(a s) \downarrow=\sigma(a s),
\end{aligned}
$$

for each $a \in Q_{S}, s \in S$, we finally achieve that $\sigma$ is an isomorphism between $S$-quantales $Q_{S}$ and $\mathcal{P}(Q)_{j}$.

## 4. Quotients of $S$-quantales

Let $Q_{S}$ be an $S$-quantale. A congruence $\rho$ on $Q_{S}$ is an equivalence relation on $Q_{S}$ which is compatible both with $S$-actions and joins, and has the further property that $Q / \rho$ equipped with a partial order becomes an $S$-quantale, and the canonical mapping $\pi: Q_{S} \rightarrow(Q / \rho)_{S}$ is an $S$-quantale homomorphism. Similar to the case of $S$-posets ([2]), a simple way for $Q / \rho$ being an $S$-quantale is that $Q / \rho$ accompanies an order " $\sqsubseteq$ " defined by a $\rho$-chain, that is,

$$
[a]_{\rho} \sqsubseteq[b]_{\rho} \Longleftrightarrow a \underset{\rho}{\leqslant} b, \forall a, b \in Q_{S},
$$

where $a \underset{\rho}{\leqslant} b$ is given by a sequence

$$
a \leqslant a_{1} \rho a_{1}^{\prime} \leqslant a_{2} \rho a_{2}^{\prime} \leqslant \ldots \leqslant a_{n} \rho a_{n}^{\prime} \leqslant b,
$$

for $a_{i}, a_{i}^{\prime} \in Q_{S}, i=1,2 . ., n$. We see at once that in the $S$-quantale $(Q / \rho, \sqsubseteq)$,

$$
\bigvee_{i \in I}\left[a_{i}\right]_{\rho}=\left[\bigvee_{i \in I} a_{i}\right]_{\rho}, \forall a_{i} \in Q_{S}
$$

Let us denote by Con $\left(Q_{S}\right)$ the set of all congruences on $Q_{S}$. Then Con $\left(Q_{S}\right)$ is a complete lattice with the inclusion as order.

This section is devoted to presenting the intrinsic relationship between the posets $\operatorname{Nuc}\left(Q_{S}\right)$ and $\operatorname{Con}\left(Q_{S}\right)$, respectively. We begin with the following results.

Lemma 4.1. Let $Q_{S}$ be an $S$-quantale, $\rho \in \operatorname{Con}\left(Q_{S}\right), \pi: Q_{S} \rightarrow(Q / \rho)_{S}$ be the canonical mapping. Then $\pi=\pi \pi_{*} \pi$.
Proof. By Lemma 2.6, $\pi_{*} \pi$ is a nucleus on $Q_{S}$. So for any $a \in Q_{S}$, one has that $a \leqslant \pi_{*} \pi(a)$, and hence $\pi(a) \leqslant \pi \pi_{*} \pi(a)$. However, (1) indicates that $\pi \pi_{*} \pi(a) \leqslant$ $\pi(a)$. Consequently, we get that $\pi(a)=\pi \pi_{*} \pi(a)$.

Let us write $\pi_{*} \pi$ in Lemma 4.1 as $j_{\rho}$. As usual, $\pi$ is a homomorphism on $Q_{S}$ such that $\rho=\operatorname{ker} \pi$.
Lemma 4.2. Let $Q_{S}$ be an $S$-quantale, $\rho \in \operatorname{Con}\left(Q_{S}\right), \pi: Q_{S} \rightarrow(Q / \rho)_{S}$ be the canonical mapping. Then $\operatorname{ker} j_{\rho}=\operatorname{ker} \pi$.

Proof. Follows by Lemma 4.1.
Lemma 4.3. Let $Q_{S}$ be an $S$-quantale, $j$ a nucleus on $Q_{S}$. Then $\mathrm{ker} j$ is a congruence on $Q_{S}$.
Proof. From Lemma 3.1, we have $j(a s)=j(j(a) s), \forall a \in Q_{S}, s \in S$. Thus for any $(a, b) \in \operatorname{ker} j, s \in S$,

$$
j(a s)=j(j(a) s)=j(j(b) s)=j(b s),
$$

that is, $(a s, b s) \in \operatorname{ker} j$. Moreover, derived from Lemma 3.2, we obtain that

$$
j\left(\bigvee_{i \in I} a_{i}\right)=j\left(\bigvee_{i \in I} j\left(a_{i}\right)\right)=j\left(\bigvee_{i \in I} j\left(b_{i}\right)\right)=j\left(\bigvee_{i \in I} b_{i}\right)
$$

for any $\left(a_{i}, b_{i}\right) \in \operatorname{ker} j, i \in I$. Therefore, $\left(\bigvee_{i \in I} a_{i}, \bigvee_{i \in I} b_{i}\right) \in \operatorname{ker} j$ as needed.

Now we are ready to characterize the concrete relationship between nuclei and congruences of an $S$-quantale.
Theorem 4.4. Let $Q_{S}$ be an $S$-quantale. Then there exists an isomorphism $\varphi$ : $\operatorname{Nuc}\left(Q_{S}\right) \rightarrow \operatorname{Con}\left(Q_{S}\right)$ as posets. Moreover, for each $j \in \operatorname{Nuc}\left(Q_{S}\right), Q_{j} \cong(Q / \varphi(j))_{S}$ as $S$-quantales.
Proof. Define a mapping $\varphi: \operatorname{Nuc}\left(Q_{S}\right) \rightarrow \operatorname{Con}\left(Q_{S}\right)$ by

$$
\varphi(j)=\operatorname{ker} j
$$

for each $j \in \operatorname{Nuc}\left(Q_{S}\right)$. Then by Lemma 4.3, ker $j$ is a congruence on $Q_{S}$. From Lemma 3.3(2), we obtain that $\varphi$ is an order embedding.

Suppose that $\rho \in \operatorname{Con}\left(Q_{S}\right)$, and $\pi: Q_{S} \rightarrow(Q / \rho)_{S}$ is the canonical mapping. Then by Lemma 4.2, we have

$$
\varphi\left(j_{\rho}\right)=\operatorname{ker} j_{\rho}=\operatorname{ker} \pi=\rho
$$

We hence conclude that $\operatorname{Nuc}\left(Q_{S}\right)$ is isomorphic to $\operatorname{Con}\left(Q_{S}\right)$ as posets.
For each $j \in \operatorname{Nuc}\left(Q_{S}\right)$, define $f:(Q / \operatorname{ker} j)_{S} \rightarrow Q_{j}$ and $g: Q_{j} \rightarrow(Q / \operatorname{ker} j)_{S}$ as

$$
f\left([a]_{\mathrm{ker} j}\right)=j(a),
$$

for each $[a]_{\operatorname{ker} j} \in(Q / \operatorname{ker} j)_{S}$, and

$$
g(a)=[a]_{\mathrm{ker} j}
$$

for any $a \in Q_{j}$. We need to show that $f$ and $g$ are invertible $S$-quantale homomorphisms.

Obviously, $f$ is well-defined. For any $a \in Q_{S}, s \in S$, since $j(j(a) s)=j(a s)$ by Lemma 3.1, we obtain that

$$
f\left([a]_{\mathrm{ker} j} s\right)=f\left([a s]_{\mathrm{ker} j}\right)=j(a s)=j(j(a) s)=j(a) \circ s=f\left([a]_{\mathrm{ker} j}\right) \circ s
$$

Moreover, Lemma 3.2 yields that
$f\left(\bigvee_{i \in I}\left[a_{i}\right]_{\mathrm{ker} j}\right)=f\left(\left[\bigvee_{i \in I} a_{i}\right]_{\mathrm{ker} j}\right)=j\left(\bigvee_{i \in I} a_{i}\right)=j\left(\bigvee_{i \in I} j\left(a_{i}\right)\right)=\bigvee_{i \in I} j\left(a_{i}\right)=\bigvee_{i \in I}\left(f\left[a_{i}\right]_{\mathrm{ker} j}\right)$,
for each $\left[a_{i}\right]_{\operatorname{ker} j} \in(Q / \operatorname{ker} j)_{S}, i \in I$. Therefore, $f$ is an $S$-quantale homomorphism. It is clear that $g$ is an $S$-poset homomorphism. Furthermore, the equalities
$g\left(\bigvee_{i \in I} a_{i}\right)=g\left(j\left(\bigvee_{i \in I} a_{i}\right)\right)=\left[j\left(\bigvee_{i \in I} a_{i}\right)\right]_{\mathrm{ker} j}=\left[\bigvee_{i \in I} a_{i}\right]_{\mathrm{ker} j}=\bigvee_{i \in I}\left[a_{i}\right]_{\mathrm{ker} j}=\bigvee_{i \in I} g\left(a_{i}\right)$,
for any $a_{i} \in Q_{j}, i \in I$ indicate that $g$ is an $S$-quantale homomorphism. We then achieve our aim by the final step, that is, for all $a \in Q_{j}$,

$$
f(g(a))=f\left([a]_{\mathrm{ker} j}\right)=j(a)=a
$$

and

$$
g\left(f\left([a]_{\text {ker } j}\right)\right)=g(j(a))=[j(a)]_{\text {ker } j}=[a]_{\text {ker } j},
$$

for any $a \in Q_{S}$.

## 5. Conuclei and $S$-subquantales

In this section, we introduce the notion of conuclei on an $S$-quantale $Q_{S}$, and discuss the relationship between conuclei and $S$-subquantales of $Q_{S}$.

Definition 5.1. Let $Q_{S}$ be an $S$-quantale. We call a coclosure operator $g$ on $Q_{S}$ a conucleus if it is $S$-submultiplicative.

Dually to Theorem 3.5 , which represented quotients of an $S$-quantale by nuclei, the following theorem establishes the relation between conuclei and $S$-subquantales of an $S$-quantale.

Theorem 5.2. Let $Q_{S}$ be an $S$-quantale, $g$ a conucleus on $Q_{S}$. Then

$$
Q_{g}=\left\{a \in Q_{S} \mid g(a)=a\right\}
$$

is an $S$-subsquantale of $Q_{S}$. Moreover, for any $S$-subquantale $P_{S}$ of $Q_{S}$, there is a conucleus $g$ on $Q_{S}$, such that $P_{S}=Q_{g}$.

Proof. Firstly, we have

$$
\bigvee A=\bigvee\{g(a) \mid a \in A\} \leqslant g(\bigvee\{a \mid a \in A\})=g(\bigvee A)
$$

for any $A \subseteq Q_{g}$, and

$$
a s=g(a) s \leqslant g(a s) \leqslant a s,
$$

for each $a \in Q_{g}, s \in S$. It turns out that $Q_{g}$ is an $S$-subquantale of $Q_{S}$.
Next, suppose that $P_{S}$ is an $S$-subquantale of $Q_{S}$. Define a mapping $g$ on $Q_{S}$ as

$$
g(b)=\bigvee\left\{a \in P_{S} \mid a \leqslant b\right\}, \forall b \in Q_{S} .
$$

Straightforward proving shows that $g$ is order-preserving and $g(b) \leqslant b, \forall b \in Q_{S}$. Recall that $P_{S}$ is join closed, $g(b) \in P_{S}$, and hence

$$
g(b) \leqslant \bigvee\left\{a \in P_{S} \mid a \leqslant g(b)\right\}=g(g(b)) .
$$

So $g$ is a coclosure operator. Together with the inequalities

$$
\begin{aligned}
g(b) s=\bigvee\left\{a \in P_{S} \mid a \leqslant b\right\} \cdot s & =\bigvee\left\{a s \in P_{S} \mid a \leqslant b\right\} \\
& \leqslant \bigvee\left\{a \in P_{S} \mid a \leqslant b s\right\}=g(b s),
\end{aligned}
$$

for any $b \in Q_{S}, s \in S$, we consequently obtain that $g$ is a conucleus on $Q_{S}$.
By the definition of $g$, we immediately get that $b \leqslant g(b), \forall b \in P_{S}$. So $P_{S} \subseteq Q_{g}$. Another inclusion is clear. Therefore, $P_{S}=Q_{g}$ as required.

Given an $S$-quantale $Q_{S}$, write $\operatorname{CoNuc}\left(Q_{S}\right)$ as the poset of all conuclei on $Q_{S}$ equipped with pointwise order, and $\operatorname{Sub}\left(Q_{S}\right)$ the poset of all $S$-subquantales of $Q_{S}$ with inclusion as order, respectively. Theorem 5.3 describes the potential connection between the posets $\operatorname{Sub}\left(Q_{S}\right)$ and $\operatorname{CoNuc}\left(Q_{S}\right)$.

Theorem 5.3. Let $Q_{S}$ be a fixed $S$-quantale. Then there is an isomorphism $k: \operatorname{Sub}\left(Q_{S}\right) \rightarrow \operatorname{CoNuc}\left(Q_{S}\right)$ as posets, such that for any $M_{S} \in \operatorname{Sub}\left(Q_{S}\right)$ we have $M_{S}=Q_{k\left(M_{S}\right)}$.
Proof. Define mappings $h: \operatorname{CoNuc}\left(Q_{S}\right) \rightarrow \operatorname{Sub}\left(Q_{S}\right)$ and $k: \operatorname{Sub}\left(Q_{S}\right) \rightarrow \operatorname{CoNuc}\left(Q_{S}\right)$ as

$$
h(g)=Q_{g}, \forall g \in \operatorname{CoNuc}\left(Q_{S}\right)
$$

and

$$
k\left(M_{S}\right)=g_{M_{S}}, \forall M_{S} \in \operatorname{Sub}\left(Q_{S}\right)
$$

respectively, where $g_{M_{S}}$ is given by

$$
g_{M_{S}}(a)=\bigvee\left\{m \in M_{S} \mid m \leqslant a\right\}=\bigvee\left\{M_{S} \cap a \downarrow\right\}, \forall a \in Q_{S}
$$

It is routine to check that $g_{M_{S}}$ is a coclosure operator. In addition, for any $s \in S$, $a \in Q_{S}$, the inequalities

$$
\begin{aligned}
g_{M_{S}}(a) s & =\left(\bigvee\left\{m \in M_{S} \mid m \leqslant a\right\}\right) s=\bigvee\left\{m s \in M_{S} \mid m \leqslant a\right\} \\
& \leqslant \bigvee\left\{m \in M_{S} \mid m \leqslant a s\right\}=g_{M_{S}}(a s)
\end{aligned}
$$

show that $g_{M_{S}}$ is $S$-submultiplicative, and hence a conucleus. $k$ being orderpreserving is clear.

By Theorem 5.2, $h$ is well-defined. Assume that $m, n \in \operatorname{CoNuc}\left(Q_{S}\right)$ with $m \leqslant n$. Then $a=m(a) \leqslant n(a) \leqslant a$, for any $a \in Q_{m}$, indicate that $a \in Q_{n}$. Thus $h$ is order-preserving.

We next show that $h k=i d_{\operatorname{Sub}\left(Q_{S}\right)}$, i.e., $Q_{g_{M_{S}}}=M_{S}, \forall M_{S} \in \operatorname{Sub}\left(Q_{S}\right)$. This follows by the fact that

$$
g_{M_{S}}(x)=\bigvee\left(M_{S} \cap x \downarrow\right)=x
$$

for any $x \in M_{S}$, and conversely, $Q_{g_{M_{S}}} \subseteq M_{S}$ by the reason that $M_{S}$ is closed under joins.

It remains to prove that $k h=i d_{\operatorname{CoNuc}\left(Q_{S}\right)}$, i.e., $g_{Q_{f}}=f, \forall f \in \operatorname{CoNuc}\left(Q_{S}\right)$. Suppose that $a \in Q_{S}$. Then

$$
f(a) \leqslant a \leqslant \bigvee\left(Q_{f} \cap a \downarrow\right)=g_{Q_{f}}(a)
$$

Conversely, for any $x \in Q_{f} \cap a \downarrow, x=f(x) \leqslant f(a)$ give rise to that $f(a)$ is an upper bound of $Q_{f} \cap a \downarrow$. Therefore, we achieve that $g_{Q_{f}}(a)=f(a)$ and finally, $\operatorname{Sub}\left(Q_{S}\right) \cong \operatorname{CoNuc}\left(Q_{S}\right)$ as needed.

## References

[1] J. Adámek, H. Herrlich H and G.E. Strecker, Abstract and Concrete Categories: The Joy of Cats, John Wiley and Sons, New York, 1990.
[2] S. Bulam-Fleming and V. Laan, Lazard's theorem for S-posets, Math. Nachr. 278 (2005), 1743 - 1755.
[3] P.T. Jonestone, Stone spaces, Cambridge university press, 1982.
[4] J. Paseka, A note on nuclei of quantale modules, Cah. Topol. Geom. Differ. Categ. 43 (2002), 19 - 34.
[5] J. Paseka, Multiplier algebras of involutive quantales, Contributions to general algebra, Heyn, Klagenfurt, 14, (2004), 109-118.
[6] D. Kruml and J. Paseka, Algebraic and categorical aspects of quantales, In Handbook of Algebra, Vol. 5, (Hazewinkel M.) Elsevier, 2008, 323 - 362.
[7] A. Palmigiano, R. Re, Relational representation of groupoid quantales, Order 30 (2013), $65-83$.
[8] F.F. Pan and S.W. Han, Free Q-algebras, Fuzzy Sets and Systems 247 (2014), 138-150.
[9] J.W. Pelletier and J. Rosický, Simple involutive quantales, J. Algebra 195 (1997), $367-386$.
[10] P. Resende, Sup-lattice 2-forms and quantales, J. Algebra 276 (2004), 143 - 167.
[11] K.I. Rosenthal, Quantales and their applications, Pitman Research Notes in Math. 234, Harlow, Essex, 1990.
[12] C. Russo, Quantale modules, Lambert Academic publishing, Saarbrücken, 2009.
[13] C. Russo, Quantale modules and their operators, with applications, J. Logic Comput. 20 (2010), 917 - 946.
[14] S.A. Solovyov, On the category of $Q$-Mod, Algebra Universalis 58 (2008), $35-58$.
[15] S.A. Solovyov, A note on nuclei of quantale algebras, Bull. Sect. Logic Univ. Lodz 40 (2011), 91 - 112.
[16] X. Zhang and V. Laan, On injective hulls of $S$-posets, Semigroup Forum 91 (2015), $62-70$.

Received October 10, 2016
School of Mathematical Sciences
South China Normal University
Guangzhou 510631
China
E-mails: xzhang@m.scnu.edu.cn, litingyuhao@126.com


[^0]:    2010 Mathematics Subject Classification: 20N05, 08A40, 08B10.
    Keywords: quasigroup, isotopy, simplicity, Latin square, commutators, polynomially completeness, multiplicative group, highly non-associative
    Research supported by DST-RFBR Indo-Russian joint project

[^1]:    2010 Mathematics Subject Classification: 03E72, 06D72, 11E57, 19A22
    Keywords: Multiset, multigroup, order of an element of a multigroup.

[^2]:    2010 Mathematics Subject Classification: 20N15, 22A15, 22A30
    Keywords: topological $n$-ary semigroup, topological semigroup, free covering semigroup.

[^3]:    2010 Mathematics Subject Classification: 20N05, 05B15
    Keywords: 3 IP Loops, Groups, Isomorphism Classes, Associativity, Symmetry Breaking.
    This work was partially supported by Prince Mohammad Bin Fahd University (PMU).

[^4]:    2010 Mathematics Subject Classification: 94A60, 11 S 05.
    Keywords: cryptography, public encryption, commutative encryption, deniable encryption, shared key, probabilistic encryption
    The work was supported by Russian Science Foundation, research project 17-11-01252

[^5]:    2010 Mathematics Subject Classification: 16Y60, 06F25.
    Keywords: ordered semiring, ordered quasi $k$-ideal, ordered $k$-regular.
    This work has been supported by Faculty of Science and The Research Fund for Supporting Lecturer to Admit High Potential Student to Study and Research on His Expert Program
    Year 2017, Graduate School, Khon Kaen University, Khon Kaen, Thailand.

[^6]:    2010 Mathematics Subject Classification: 20N20, 20N25, 06F05.
    Keywords: ordered semiring, ordered $k$-bi-ideal, prime right ordered $k$-bi-ideal.

[^7]:    2010 Mathematics Subject Classification: 20N15
    Keywords: ternary quasigroup, orthoghonal system, paratopy

[^8]:    2010 Mathematics Subject Classification: 20F99, 20D99, 20 N05.
    Keywords: gyrogroup, gyrocommutative gyrogroup, gyrogroup isomorphism.

[^9]:    2010 Mathematics Subject Classification: 06F99
    Keywords: $S$-quantale, Nucleus, Conucleus, $S$-poset
    This research is supported by Natural Science Foundation of Guangdong Province, China (No. 2016A030313832), the Science and Technology Program of Guangzhou, China (No. 201607010190).

