Quasigroups and Related Systems **24** (2016), 141 – 150

m-polar fuzzy Lie ideals of Lie algebras

Muhammad Akram and Adeel Farooq

Abstract. We introduce the notion of an m-polar fuzzy Lie ideal of a Lie algebra and investigate some properties of nilpotency of m-polar fuzzy Lie ideals. We introduce the concept of m-polar fuzzy adjoint representation of Lie algebras and discuss the relationship between this representation and nilpotent m-polar fuzzy Lie ideals. We also define Killing form in the m-polar fuzzy case and study some of its properties.

1. Introduction

The concept of Lie groups was first introduced by Sophus Lie in nineteenth century through his studies in geometry and integration methods for differential equations. The importance of Lie algebras in mathematics and physics have become increasingly evident in recent years. In applied mathematics, Lie theory remains a powerful tool for studying differential equations, special functions and perturbation theory. It is noted that Lie theory has applications not only in mathematics and physics but also in diverse fields such as continuum mechanics, cosmology and life sciences. A Lie algebra has nowadays even been applied by electrical engineers in solving problems in mobile robot control [8].

In 1965, Zadeh [15] introduced the concept of fuzzy subset of a set. A fuzzy set on a given set X is a mapping $A: X \to [0,1]$. In 1994, Zhang [16] extended the idea of a fuzzy set and defined the notion of bipolar fuzzy set on a given set X as a mapping $A: X \to [-1,1]$, where the membership degree 0 of an element x means that the element x is irrelevant to the corresponding property, the membership degree in $(0,1]$ of an element x indicates that the element satisfies the property, and the membership degree in $[-1,0)$ of an element x indicates that the element somewhat satisfies the implicit counter-property. In 2014, Chen *et al.* [7] introduced the notion of m-polar fuzzy sets as a generalization of bipolar fuzzy set and showed that bipolar fuzzy sets and 2-polar fuzzy sets are cryptomorphic mathematical notions and that we can obtain concisely one from the corresponding one in [7]. The idea behind this is that “multipolar information" (not just bipolar information which correspond to two-valued logic) exists because data for a real world problems are sometimes from n agents ($n \geqslant 2$). For example, the exact degree of telecommunication safety of mankind is a point in $[0,1]^n (n \approx 7 \times 10^9)$ because different person has been monitored different times. There are many

2010 Mathematics Subject Classification: 04A72, 17B99

Keywords: m-polar fuzzy Lie ideal, nilpotent Lie ideal, adjoint representation, Killing form.

examples such as truth degrees of a logic formula which are based on n logic implication operators ($n \geqslant 2$), similarity degrees of two logic formula which are based on n logic implication operators ($n \geqslant 2$), ordering results of a magazine, ordering results of a university and inclusion degrees (accuracy measures, rough measures, approximation qualities, fuzziness measures, and decision preformation evaluations) of a rough set.

The notions of fuzzy ideals and fuzzy subalgebras of Lie algebras over a field were considered first in [13] by Yehia. Since then, the concepts and results of Lie algebras have been broadened to the fuzzy setting frames [1-6, 10, 13]. In this paper, we introduce the notion of an m-polar fuzzy Lie ideal of a Lie algebra and investigate some properties of nilpotency of m-polar fuzzy Lie ideals. We introduce the concept of m-polar fuzzy adjoint representation of Lie algebras and discuss the relationship between this representation and nilpotent m-polar fuzzy Lie ideals. We also define Killing form in the m-polar fuzzy case and study some of its properties. The definitions and terminologies that we used in this paper are standard. For other notations, terminologies and applications, the readers are refereed to [8-12, 17].

2. Preliminaries

In this section, we first review some elementary aspects that are necessary for this paper. A *Lie algebra* is a vector space $\mathscr{L}$ over a field $\mathbb{F}$ (equal to $\mathbb{R}$ or $\mathbb{C}$) on which $\mathscr{L} \times \mathscr{L} \to \mathscr{L}$ denoted by $(x, y) \to [x, y]$ is defined satisfying the following axioms:

(L1) $[x, y]$ is bilinear,

(L2) $[x, x] = 0$ for all $x \in \mathscr{L}$,

(L3) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in \mathscr{L}$ (Jacobi identity).

Throughout this paper, $\mathscr{L}$ is a Lie algebra and $\mathbb{F}$ is a field. We note that the multiplication in a Lie algebra is not associative, i.e., it is not true in general that $[[x, y], z] = [x, [y, z]]$. But it is *anticommutative*, i.e., $[x, y] = -[y, x]$. A subspace H of $\mathscr{L}$ closed under $[\cdot, \cdot]$ will be called a *Lie subalgebra.*

A *fuzzy set* $\mu : \mathscr{L} \to [0, 1]$ is called a *fuzzy Lie ideal* [1] of $\mathscr{L}$ if

(a) $\mu(x + y) \geqslant \min\{\mu(x), \mu(y)\}$,

(b) $\mu(\alpha x) \geqslant \mu(x)$,

(c) $\mu([x, y]) \geqslant \mu(x)$

hold for all $x, y \in \mathscr{L}$ and $\alpha \in \mathbb{F}$. The addition and the commutator [,] of $\mathscr{L}$ are extended by Zadeh's extension principle [15], to two operations on I^L in the following way:

$$(\mu \oplus \lambda)(x) = \sup\{\min\{\mu(y), \lambda(z)\} \mid y, z \in \mathscr{L},\ y + z = x\},$$

$$\ll \mu,\lambda \gg (x) = \sup\{\min\{\mu(y),\lambda(z)\} \,|\, y,z \in \mathscr{L},\ [y,z]=x\},$$

where μ,λ are fuzzy sets on $I^{\mathscr{L}}$ and $x \in \mathscr{L}$. The scalar multiplication αx for $\alpha \in \mathbb{F}$ and $x \in \mathscr{L}$ is extended to an action of the field $\mathbb{F}$ on $I^{\mathscr{L}}$ denoted by $\odot$ as follows for all $\mu \in I^{L}$, $\alpha \in \mathbb{F}$ and $x \in \mathscr{L}$:

$$(\alpha \odot \mu)(x) = \begin{cases} \mu(\alpha^{-1}x) & \text{if } \alpha \neq 0, \\ 1 & \text{if } \alpha = 0,\ x = 0, \\ 0 & \text{if } \alpha = 0,\ x \neq 0. \end{cases}$$

The two operations of the field $\mathbb{F}$ can be extended to two operations on $I^{\mathbb{F}}$ in the same way. The operations are denoted by $\oplus$ and $\circ$ as well [15]. The zeros of $\mathscr{L}$ and $\mathbb{F}$ are denoted by the same symbol 0. Obviously $0 \odot \mu = 1_0$ for every $\mu \in I^{\mathscr{L}}$ and every $\mu \in I^{\mathbb{F}}$, where 1_x is the fuzzy subset taking 1 at x and 0 elsewhere.

Definition 2.1. [7] An *m-polar fuzzy set* (or a $[0,1]^m$-set) on X is a mapping $A : \mathscr{L} \to [0,1]^m$. The set of all m-polar fuzzy sets on $\mathscr{L}$ is denoted by $m(\mathscr{L})$.

Note that $[0,1]^m$(m-power of [0, 1]) is considered a poset with the point-wise order $\leqslant$, where m is an arbitrary ordinal number (we make an appointment that $m = \{n \,|\, n < m\}$ when $m > 0$), $\leqslant$ is defined by $x \leqslant y \Leftrightarrow p_i(x) \leqslant p_i(y)$ for each $i \in m$ ($x, y \in [0,1]^m$), and $p_i : [0,1]^m \to [0,1]$ is the i-th projection mapping ($i \in m$). $\mathbf{0} = (0,0,\ldots,0)$ is the smallest element in $[0,1]^m$ and $\mathbf{1} = (1,1,\ldots,1)$ is the largest element in $[0,1]^m$.

Definition 2.2. Let C be an m-polar fuzzy set on a set $\mathscr{L}$. An *m-polar fuzzy relation* on C is an m-polar fuzzy set D of $\mathscr{L} \times \mathscr{L}$ such that for all $x, y \in X$ and $i = 1,2,3,\ldots,m$ we have $p_i \circ D(xy) \leqslant \inf(p_i \circ C(x), p_i \circ C(y))$.

3. m-polar fuzzy Lie ideals

Definition 3.1. An m-polar fuzzy set C on $\mathscr{L}$ is called an *m-polar fuzzy Lie ideal* if the following conditions are satisfied:

(1) $C(x+y) \geqslant \inf(C(x), C(y))$,

(2) $C(\alpha x) \geqslant C(x)$,

(3) $C([x,y]) \geqslant C(x)$ for all $x, y \in \mathscr{L}$ and $\alpha \in \mathbb{F}$.

That is,

(1) $p_i \circ C(x+y) \geqslant \inf(p_i \circ C(x), p_i \circ C(y))$,

(2) $p_i \circ C(\alpha x) \geqslant p_i \circ C(x)$,

(3) $p_i \circ C([x,y]) \geqslant p_i \circ C(x)$

for all $x, y \in \mathscr{L}$ and $\alpha \in \mathbb{F}$, $i = 1, 2, 3, \ldots, m$.

Example 3.2. Let $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$ be the set of all 3-dimensional real vectors. Then $\mathbb{R}^3$ with the bracket $[\cdot, \cdot]$ defined as the usual cross product, i.e., $[x, y] = x \times y$, forms a real Lie algebra. We also define an m-polar fuzzy set $C : \mathbb{R}^3 \to [0, 1]^m$ by

$$C(x, y, z) = \begin{cases} (0.8, 0.8, \ldots, 0.8) & \text{if } x = y = z = 0, \\ (0.1, 0.1, \ldots, 0.1) & \text{otherwise.} \end{cases}$$

By routine computations, we can verify that the above m-polar fuzzy set C is an m-polar fuzzy Lie ideal of the Lie algebra $\mathbb{R}^3$.

Example 3.3. A subalgbera $sl_2(\mathbb{C})$ of all 2×2 matrices with trace 0 is an ideal of $gl_2(\mathbb{C})$. The basis of $sl_2(\mathbb{C})$ are: $h = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and $e = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The commutators are $[e, f] = h$, $[h, f] = -2f$ and $[h, e] = 2e$.

We define an m-polar fuzzy set $C : gl_2(\mathbb{C}) \to [0, 1]^m$ by

$$C(g) = \begin{cases} (1, 1, \ldots, 1), & g \in sl_n(\mathbb{C}) \\ (0, 0, \ldots, 0), & \text{otherwise.} \end{cases}$$

By routine computations, we see that C is an m-polar fuzzy ideal.

We sate the following theorem without its proof.

Theorem 3.4. Let C be an m-polar fuzzy Lie ideal in a Lie algebra $\mathscr{L}$. Then C is an m-polar fuzzy Lie ideal of $\mathscr{L}$ if and only if the non-empty upper s-level cut $C_{[s]} = \{x \in \mathscr{L} | C(x) \geqslant s\}$ is Lie ideal of $\mathscr{L}$, for all $s = (s_1, s - 2, \ldots, s_m) \in [0, 1]^m$.

Example 3.5. Consider the group algebra $\mathbb{C}[S_3]$, where S_3 is the Symmetric group. Then $\mathbb{C}[S_3]$ assumes the structure of a Lie algebra via the bracket (commutator) operation.

Clearly, the linear span of the elements $\hat{g} = g - g^{-1}$ for $g \in S_3$ is the subalgebra of $\mathbb{C}[S_3]$, which is also known as Plesken Lie algebra and denoted by $\mathscr{L}(S_3)_{\mathbb{C}}$. It is easy to see that $\mathscr{L}(S_3)_{\mathbb{C}} = Span_{\mathbb{C}}\{\widehat{(1, 2, 3)}\}$ and $\widehat{(1, 2, 3)} = (1, 2, 3) - (1, 3, 2)$.

We define an m-polar fuzzy set $C : \mathscr{L}(S_3)_{\mathbb{C}} \to [0, 1]^m$ by

$$C(g) = \begin{cases} (t_1, t_2, \ldots, t_m), & g = \gamma(1, 2, 3) - \gamma(1, 3, 2), \text{ where } \gamma \in \mathbb{C}, g \in \mathbb{C}[S_3] \\ (s_1, s_2, \ldots, s_m), & \text{otherwise, where } s_i < t_i \end{cases}$$

By routine calculations, we have $\{g \in \mathbb{C}[S_3] : C(g) > (s_1, s_2, \ldots, s_m)\} = \mathscr{L}(S_3)_{\mathbb{C}}$. Then we see that $\mathscr{L}(S_3)_{\mathbb{C}}$ can be realized $C_{[s]}$ as an upper s_i-level cut and C is an m-polar fuzzy Lie ideal of $\mathscr{L}(S_3)_{\mathbb{C}}$.

Definition 3.6. Let $C \in I^{\mathscr{L}}$, an m-polar fuzzy subspace of $\mathscr{L}$ generated by C will be denoted by $[C]$. It is the intersection of all m-polar fuzzy subspaces of $\mathscr{L}$ containing C. For all $x \in \mathscr{L}$, we define:

$$[C](x) = \sup\{\inf C(x_i) \,|\, x = \sum \alpha_i x_i, \alpha_i \mathbb{F}, x_i \in \mathscr{L}\}.$$

Definition 3.7. Let $f : \mathscr{L}_1 \to \mathscr{L}_2$ be a homomorphism of Lie algebras which has an extension $f : I^{\mathscr{L}_1} \to I^{\mathscr{L}_2}$ defined by:

$$f(C)(y) = \sup\{C(x), x \in f^{-1}(y)\}.$$

for all $C \in I^{\mathscr{L}_1}$, $y \in \mathscr{L}_2$. Then $f(C)$ is called the *homomorphic image* of C.

Proposition 3.8. *Let $f : \mathscr{L}_1 \to \mathscr{L}_2$ be a homomorphism of Lie algebras and let C be an m-polar fuzzy Lie ideal of $\mathscr{L}_1$. Then*

(i) *$f(C)$ is an m-polar fuzzy Lie ideal of $\mathscr{L}_2$,*

(ii) *$f([C]) \supseteq [f(C)]$.*

Proposition 3.9. *If C and D are m-polar fuzzy Lie ideals in $\mathscr{L}$, then $[C, D]$ is an m-polar fuzzy Lie ideal of $\mathscr{L}$.*

Theorem 3.10. *Let C_1, C_2, D_1, D_2 be m-polar fuzzy Lie ideals in $\mathscr{L}$ such that $C_1 \subseteq C_2$ and $D_1 \subseteq D_2$, then $[C_1, D_1] \subseteq [C_2, D_2]$.*

Proof. Indeed,

$$\begin{aligned} \ll C_1, D_1 \gg (x) &= \sup\{\inf(C_1(a), D_1(b)) \mid a, b \in \mathscr{L}_1, [a, b] = x\} \\ &\geqslant \sup\{\inf(C_2(a), D_2(b)) \mid a, b \in \mathscr{L}_1, [a, b] = x\} \\ &= \ll C_2, D_2 \gg (x). \end{aligned}$$

Hence $[C_1, D_1] \subseteq [C_2, D_2]$. □

Let C be an m-polar fuzzy Lie ideal in $\mathscr{L}$. Putting

$$C^0 = C,\ C^1 = [C, C_0],\ C^2 = [C, C_1],\ \ldots,\ C^n = [C, C^{n-1}]$$

we obtain a descending series of an m-polar fuzzy Lie ideals

$$C^0 \supseteq C^1 \supseteq C^2 \supseteq \ldots \supseteq C^n \supseteq \ldots$$

and a series of m-polar fuzzy sets $D^n = \sup\{C^n(x) \,|\, 0 \neq x \in \mathscr{L}\}$.

Definition 3.11. An m-polar fuzzy Lie ideal C is called *nilpotent* if there exists a positive integer n such that $D^n = \mathbf{0}$.

Theorem 3.12. *A homomorphic image of a nilpotent m-polar fuzzy Lie ideal is a nilpotent m-polar fuzzy Lie ideal.*

Proof. Let $f : \mathscr{L}_1 \to \mathscr{L}_2$ be a homomorphism of Lie algebras and let C be a nilpotent m-polar fuzzy Lie ideal in $\mathscr{L}_1$. Assume that $f(C) = D$. We prove by induction that $f(C^n) \supseteq D^n$ for every natural n. First we claim that $f([C,C]) \supseteq [f(C), f(C)] = [D,D]$. Let $y \in \mathscr{L}_2$, then

$$\begin{aligned}
&f(\ll C, C \gg)(y) = \sup\{\ll C, C \gg)(x) \mid f(x) = y\}\\
&= \sup\{\sup\{\inf(C(a), C(b)) \mid a, b \in \mathscr{L}_1, [a,b] = x, f(x) = y\}\}\\
&= \sup\{\inf(C(a), C(b)) \mid a, b \in \mathscr{L}_1, [a,b] = x, f(x) = y\}\\
&= \sup\{\inf(C(a), C(b)) \mid a, b \in \mathscr{L}_1, [f(a), f(b)] = y\}\\
&= \sup\{\inf(C(a), C(b)) \mid a, b \in \mathscr{L}_1, f(a) = u, f(b)] = v, [u,v] = y\}\\
&\geqslant \sup\{\inf(\sup_{a\in f^{-1}(u)} C(a), \sup_{b\in f^{-1}(v)} C(b)) \mid [u,v] = y\}\\
&= \sup\{\inf(f(C)(u), f(C)(v)) \mid [u,v] = y\} = \ll f(C), f(C) \gg (y),
\end{aligned}$$

Thus

$$f([C,C]) \supseteq f(\ll C, C \gg) \supseteq \ll f(C), f(C) \gg = [f(C), f(C)].$$

For $n > 1$, we get

$$f(C^n) = f([C, C^{n-1}]) \supseteq [f(C), f(C^{n-1})] \supseteq [D, D^{n-1}] = D^n.$$

Let m be a positive integer such that $C^m = \mathbf{0}$. Then for $0 \neq y \in L_2$ we have

$$D^m(y) \leqslant f(\mu^P_{C^n})(y) = f(0)(y) = \sup\{0(a) \,|\, f(a) = y\} = \mathbf{0}.$$

This completes the proof. □

Let C be an m-polar fuzzy Lie ideal in $\mathscr{L}$. Putting

$$C^{(0)} = C,\ C^{(1)} = [C^{(0)}, C^{(0)}],\ C^{(2)} = [C^{(1)}, C^{(1)}], \dots, C^{(n)} = [C^{(n-1)}, C^{(n-1)}]$$

we obtain series

$$C^{(0)} \subseteq C^{(1)} \subseteq C^{(2)} \subseteq \dots \subseteq C^{(n)} \subseteq \dots$$

of m-polar fuzzy Lie ideals and a series of m-polar fuzzy sets $D^{(n)}$ such that

$$D^n = \sup\{C^n(x) \,|\, 0 \neq x \in \mathscr{L}\}.$$

Definition 3.13. An m-polar fuzzy Lie ideal C is called *solvable* if there exists a positive integer n such that $D^{(n)} = \mathbf{0}$.

Theorem 3.14. *A nilpotent m-polar fuzzy Lie ideal is solvable.*

Proof. It is enough to prove that $C^{(n)} \subseteq C^n$ for all positive integers n. We prove it by induction on n and by the use of Theorem 3.10:

$$C^{(1)} = [C,C] = C^1, \qquad C^{(2)} = [C^{(1)}, C^{(1)}] \subseteq [C, C^{(1)}] = C^2.$$

$$C^{(n)} = [C^{(n-1)}, C^{(n-1)}] \subseteq [C, C^{(n-1)}] \subseteq [C, C^{(n-1)}] = C^n.$$

This completes the proof. □

Definition 3.15. Let C and D be two m-polar fuzzy Lie ideals of a Lie algebra $\mathscr{L}$. The sum $C \oplus D$ is called a *direct sum* if $C \cap D = \mathbf{0}$.

Theorem 3.16. *The direct sum of two nilpotent m-polar fuzzy Lie ideals is also a nilpotent m-polar fuzzy Lie ideal.*

Proof. Suppose that C and D are two m-polar fuzzy Lie ideals such that $C \cap D = \mathbf{0}$. We claim that $[C, D] = \mathbf{0}$. Let $x(\neq 0) \in \mathscr{L}$, then

$$\ll C, D \gg (x) = \sup\{\inf(C(a), D(b)) \mid [a, b] = x\} \leqslant \inf(C(x), D(x)) = \mathbf{0}.$$

This proves our claim. Thus we obtain $[C^m, D^n] = \mathbf{0}$ for all positive integers m, n. Now we again claim that $(C \oplus D)^n \subseteq C^n \oplus D^n$ for positive integer n. We prove this claim by induction on n. For $n = 1$,

$$(C \oplus D)^1 = [C \oplus D, C \oplus D] \subseteq [C, C] \oplus [C, D] \oplus [D, C] \oplus [D, D] = C^1 \oplus D^1.$$

Now for $n > 1$,

$$\begin{aligned}(C \oplus D)^n &= [C \oplus D, (C \oplus D)^{n-1}] \subseteq [C \oplus D, C^{n-1} \oplus D^{n-1}] \\ &\subseteq [C, C^{n-1}] \oplus [C, D^{n-1}] \oplus [D, C^{n-1}] \oplus [D, D^{n-1}] = C^n \oplus D^n.\end{aligned}$$

Since there are two positive integers p and q such that $C^p = D^q = \mathbf{0}$, we have $(C \oplus D)^{p+q} \subseteq C^{p+q} \oplus D^{p+q} = \mathbf{0}$. □

In a similar way we can prove the following theorem.

Theorem 3.17. *The direct sum of two solvable m-polar fuzzy Lie ideals is a solvable m-polar fuzzy Lie ideal.*

Definition 3.18. For any $x \in \mathscr{L}$ we define the function $adx : \mathscr{L} \to \mathscr{L}$ putting $adx(y) = [x, y]$. It is clear that this function is a linear homomorphism with respect to y. The set $H(\mathscr{L})$ of all linear homomorphisms from $\mathscr{L}$ into itself is made into a Lie algebra by defining a commutator on it by $[f, g] = f \circ g - g \circ f$. The function $ad : \mathscr{L} \to H(\mathscr{L})$ defined by $ad(x) = adx$ is a Lie homomorphism which is called the *adjoint representation* of $\mathscr{L}$.

The adjoint representation $adx : \mathscr{L} \to \mathscr{L}$ is extended to $a\bar{d}x : I^{\mathscr{L}} \to I^{\mathscr{L}}$ by putting

$$a\bar{d}x(\gamma)(y) = \sup\{\gamma(a) : [x, a] = y\}$$

for all $\gamma \in I^{\mathscr{L}}$ and $y \in \mathscr{L}$.

Theorem 3.19. *Let C be an m-polar fuzzy Lie ideal in a Lie algebra $\mathscr{L}$. Then $C^n \subseteq [C_n]$ for any $n > 0$, where an m-polar fuzzy subset $[C_n]$ is defined by*

$$[C_n](x) = \sup\{C(a) \mid [x_1, [x_2, [\ldots, [x_n, a] \ldots]]] = x, \quad x_1, \ldots, x_n \in \mathscr{L}\}.$$

Proof. It is enough to prove that $\ll C, C^{n-1} \gg \subseteq [C_n]$. We prove it by induction on n. For n=1 and $x \in \mathscr{L}$, we have

$$\begin{aligned}\ll C, C \gg (x) &= \sup\{\inf(C(a), C(b)) \,|\, [a,b] = x\}\\ &\geqslant \sup\{C(b) \,|\, [a,b] = x, a \in \mathscr{L}\} = [C_1](x).\end{aligned}$$

For $n > 1$,

$$\begin{aligned}&\ll C, C^{(n-1)} \gg (x) = \sup\{\inf(C(a), C^{(n-1)}(b)) \,|\, [a,b] = x\}\\ &= \sup\{\inf(C(a), [C(b), C^{(n-2)}(b)]) \,|\, [a,b] = x\}\\ &\geqslant \sup\{\inf(C(a), \sup\{\ll C, C^{(n-2)} \gg (b_i) \,|\, b = \textstyle\sum \alpha_i b_i\}) \,|\, [a,b] = x\}\\ &\geqslant \sup\{\inf(C(a), \sup\{[C_{n-1}](b_i) \,|\, b = \textstyle\sum \alpha_i b_i\}) \,|\, [a,b] = x\}\\ &\geqslant \sup\{\inf(C(a), [C_{n-1}](b_i)) \,|\, \textstyle\sum \alpha_i [a, b_i] = x\}\\ &\geqslant \sup\{\inf(C(a), \sup\{C_{n-1}(c_i) \,|\, b_i = \textstyle\sum \beta_i c_i\}) \,|\, \textstyle\sum \alpha_i [a, b_i] = x\}\\ &\geqslant \sup\{\inf(C(a), C_{n-1}(c_i)) \,|\, \textstyle\sum \gamma_i [a, c_i] = x\}\\ &\geqslant \sup\{\inf(C(a), \sup\{C(d_i)) \,|\, [x_1, [x_2, [\ldots, [x_{n-1}, d_i]\ldots]]] = c_i\} \,|\, \textstyle\sum \gamma_i [a, c_i] = x\}\\ &\geqslant \sup\{\inf(C(a), C(d_i)) \,|\, \textstyle\sum \gamma_i [a, [x_1, [x_2, [\ldots, [x_{n-1}, d_i]\ldots]]]] = x\}\\ &\geqslant \sup\{C_n(d_i) \,|\, \textstyle\sum \gamma_i [a, [x_1, [x_2, [\ldots, [x_{n-1}, d_i]\ldots]]]] = x\} \geqslant [C_n](x).\end{aligned}$$

This complete the proof. □

Theorem 3.20. *If for an m-polar fuzzy Lie ideal C there exists a positive integer n such that*

$$(a\bar{d}x_1 \circ a\bar{d}x_2 \circ \ldots \circ a\bar{d}x_n)(C) = \mathbf{0}.$$

for all $x_1, \ldots, x_n \in \mathscr{L}$, then C is nilpotent.

Proof. For $x_1, \ldots, x_n \in \mathscr{L}$ and $x(\neq 0) \in \mathscr{L}$, we have

$$(a\bar{d}x_1 \circ \cdots \circ a\bar{d}x_n)(C)(x) = \sup\{C(a) \,|\, [x_1, [x_2, [\ldots, [x_n, a]\ldots]]] = x\} = \mathbf{0}.$$

Thus $[C_n] = \mathbf{0}$. From Theorem 3.19, it follows that $C^n = \mathbf{0}$. Hence C is a nilpotent m-polar fuzzy Lie ideal. □

The mapping $K : \mathscr{L} \times \mathscr{L} \to \mathbb{F}$ defined by $K(x,y) = Tr(adx \circ ady)$, where Tr is the *trace* of a linear homomorphism, is a symmetric bilinear form which is called the *Killing form*. It is not difficult to see that this form satisfies the identity $K([x,y],z) = K(x,[y,z])$. The form K can be naturally extended to $\overline{K} : I^{\mathscr{L}\times\mathscr{L}} \to I^{\mathbb{F}}$ defined by putting

$$\overline{K}(C)(\beta) = \sup\{C(x,y) \,|\, Tr((adx \circ ady)) = \beta\}.$$

The Cartesian product of two m-polar fuzzy sets C and D is defined as

$$(C \times D)(x,y) = \inf(C(x), D(y)).$$

Similarly we define

$$\overline{K}(C \times D)(\beta) = \sup\{\inf(C(x), D(y)) \,|\, Tr((adx \circ ady)) = \beta\}.$$

Theorem 3.21. *Let C be an m-polar fuzzy Lie ideal of Lie algebra $\mathscr{L}$. Then $\overline{K}(C \times 1_{(\alpha x)}) = \alpha \odot \overline{K}(C \times 1_x)$ for all $x \in \mathscr{L}$, $\alpha\mathbb{F}$.*

Proof. If $\alpha = 0$, then for $\beta = 0$ we have

$$\begin{aligned}\overline{K}(C \times 1_0)(0) &= \sup\{\inf(C(x), 1_0(y)) \,|\, Tr(adx \circ ady) = 0\} \\ &\geqslant \inf(C(0), 1_0(0)) = \mathbf{0}.\end{aligned}$$

For $\beta \neq 0$ $\;Tr((adx \circ ady) = \beta$ means that $x \neq 0$ and $y \neq 0$. So,

$$\overline{K}(C \times 1_0)(\beta) = \sup\{\inf(C(x), 1_0(y)) \,|\, Tr((adx \circ ady) = \beta\} = \mathbf{0}.$$

If $\alpha \neq 0$, then for arbitrary β we obtain

$$\begin{aligned}\overline{K}(C \times 1_{\alpha x})(\beta) &= \sup\{\inf(C(y), 1_{\alpha x}(z)) \,|\, Tr((ady \circ adz) = \beta\} \\ &= \sup\{\inf(C(y), \alpha \odot 1_x(z)) \,|\, Tr((ady \circ adz) = \beta\} \\ &= \sup\{\inf(C(y), 1_x(\alpha^{-1}z)) \,|\, \alpha Tr((ady \circ ad(\alpha^{-1}z)) = \beta\} \\ &= \sup\{\inf(C(y), 1_x(\alpha^{-1}z)) \,|\, Tr((ady \circ ad(\alpha^{-1}z)) = \alpha^{-1}\beta\} \\ &= \overline{K}(C \times 1_x)(\alpha^{-1}\beta) = \alpha \odot \overline{K}(C \times 1_x)(\beta).\end{aligned}$$

This completes the proof. □

Theorem 3.22. *Let C be an m-polar fuzzy Lie ideal of a Lie algebra $\mathscr{L}$. Then $\overline{K}(C\times 1_{(x+y)}) = \overline{K}(C\times 1_x) \oplus \overline{K}(C\times 1_y)$ and $\overline{K}(C\times 0_{(x+y)}) = \overline{K}(C\times 0_x) \oplus \overline{K}(C\times 0_y)$ for all $x, y \in \mathscr{L}$.*

Proof. Indeed,

$$\begin{aligned}\overline{K}(C \times 1_{(x+y)})(\beta) &= \sup\{\inf(C(z), 1_{x+y}(u)) \,|\, Tr((adz \circ adu) = \beta\} \\ &= \sup\{C(z) \,|\, Tr(adz \circ ad(x+y)) = \beta\} \\ &= \sup\{C(z) \,|\, Tr(adz \circ adx) + Tr(adz \circ ady) = \beta\}\end{aligned}$$

$$\begin{aligned}&= \sup\{\inf(C(z), \inf(1_x(v), 1_y(w))) \,|\, Tr(adz \circ adv) + Tr(adz \circ adw) = \beta\} \\ &= \sup\{\inf(\sup\{\inf(C(z), 1_x(v)) \,|\, Tr(adz \circ adv) = \beta_1\}, \\ &\qquad \sup\{\inf(C(z), 1_y(w)) \,|\, Tr(adz \circ adw) = \beta_2\} \,|\, \beta_1 + \beta_2 = \beta)\} \\ &= \sup\{\inf(\overline{K}(C \times 1_x)(\beta_1),\ \overline{K}(C \times 1_y)(\beta_2)) \,|\, \beta_1 + \beta_2 = \beta\} \\ &= \overline{K}(C \times 1_x) \oplus \overline{K}(C \times 1_y)(\beta).\end{aligned}$$

This completes the proof. □

We conclude that:

Corollary 3.23. *For each m-polar fuzzy Lie ideal C and all $x, y \in \mathscr{L}$, $\alpha, \beta \in \mathbb{F}$ we have*

$$\overline{K}(C \times 1_{(\alpha x + \beta y)}) = \alpha \odot \overline{K}(C \times 1_x) \oplus \beta \odot \overline{K}(C \times 1_y).$$

References

[1] **M. Akram**, *Anti fuzzy Lie ideals of Lie algebras*, Quasigroups and Related Systems **14** (2006), 123 – 132.

[2] **M. Akram**, *Intuitionistic (S, T)-fuzzy Lie ideals of Lie algebras*, Quasigroups and Related Systems **15** (2007), 201 – 218.

[3] **M. Akram**, *Intuitionistic fuzzy Lie ideals of Lie algebras*, J. Fuzzy Math. **16** (2008), 991 – 1008.

[4] **M. Akram**, *Generalized fuzzy Lie subalgebras*, J. Generalized Lie Theory and Appl. **2** (2008), 261 – 268.

[5] **M. Akram**, *Fuzzy Lie ideals of Lie algebras with interval-valued membership function*, Quasigroups and Related Systems **16** (2008), 1 – 12.

[6] **M. Akram and K.P. Shum**, *Intuitionistic fuzzy Lie algebras*, Southeast Asian Bull. Math. **31** (2007), 843 – 855.

[7] **J. Chen, S.G. Li, S. Ma and X. Wang**, *m-polar fuzzy sets: An extention of m-polar fuzzy sets*, The Scientific World J. vol. 2014, pp. 8.

[8] **P. Coelho and U. Nunes**, *Lie algebra application to mobile robot control: a tutorial*, Robotica **21** (2003), 483 – 493.

[9] **J.E. Humphreys**, *Introduction to Lie Algebras and Representation Theory*, Springer, New York 1972.

[10] **C.G. Kim and D.S. Lee**, *Fuzzy Lie ideals and fuzzy Lie subalgebras*, Fuzzy Sets and Systems **94** (1998), 101 – 107.

[11] **M. Kondo** and **W.A. Dudek**, *On the transfer principle in fuzzy theory*, Mathware and Soft Computing, **12** (2005), 41 – 55.

[12] **K.M. Lee**, *Comparison of interval-valued fuzzy sets, intuitionistic fuzzy sets, and bipolar-valued fuzzy sets*, J. Fuzzy Logic Intell. Sys. **14** (2004), 125 – 129.

[13] **S.E. Yehia**, *Fuzzy ideals and fuzzy subalgebras of Lie algebras*, Fuzzy Sets and Systems **80** (1996), 237 – 244.

[14] **S.E. Yehia**, *The adjoint representation of fuzzy Lie algebras*, Fuzzy Sets and Systems **119** (2001), 409 – 417.

[15] **L.A. Zadeh**, *Fuzzy sets*, Information and Control **8** (1965), 338 – 353.

[16] **W.R. Zhang**, *Bipolar fuzzy sets and relations: a computational framework forcognitive modeling and multiagent decision analysis*, Proc. of IEEE conf. (1994), 305–309.

[17] **W.R. Zhang**, *Bipolar fuzzy sets*, Proc. of FUZZ-IEEE (1998), 835 – 840.

Received January 3, 2016

M. Akram
Department of Mathematics, University of the Punjab, New Campus, Lahore, Pakistan
E-mail: m.akram@pucit.edu.pk

A. Farooq
Department of Mathematics, COMSATS Institute of Information Technology, Lahore, Pakistan.
E-mail: adeelfarooq@ciitlahore.edu.pk

Quasigroups and Related Systems **24** (2016), 151 − 156

On locally maximal product-free sets in 2-groups of coclass 1

Chimere S. Anabanti

Abstract. This paper is in two parts: first, we classify the 2-groups of coclass 1 that contain locally maximal product-free sets of size 4, then give a classification of the filled 2-groups of coclass 1.

1. Introduction

Let S be a product-free set in a finite group G. Then S is *locally maximal* in G if S is not properly contained in any other product-free set in G, and S is said to *fill* G if $G^* \subseteq S \sqcup SS$, where $G^* = G \setminus \{1\}$. We call G a *filled group* if every locally maximal product-free set in G fills G.

Street and Whitehead [6] classified the abelian filled groups as one of C_3, C_5 or an elementary abelian 2-group. Recently, Anabanti and Hart [2] classified the filled groups of odd order as well as gave a characterisation of the filled nilpotent groups. In the latter direction, they proved that if G is a filled nilpotent group, then G is one of C_3, C_5 or a 2-group. One of the goals of this paper is the classification of filled 2-groups of coclass 1.

By a 2-*group of coclass* 1, we mean a group of order 2^n and nilpotency class $n-1$ for $n \geqslant 3$, and is one of the following:
(i) $D_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = y^2 = 1, xy = yx^{-1}\rangle$, $n \geqslant 3$ (Dihedral);
(ii) $Q_{2^n} = \langle x, y \,|\, x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, xy = yx^{-1}\rangle$ for $n \geqslant 3$ (Generalised quaternion);
(iii) $QD_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^2 = 1, xy = yx^{2^{n-2}-1}\rangle$, $n \geqslant 4$ (Quasi-dihedral).

In 2006, Giudici and Hart [5] began the classification of groups containing locally maximal product-free sets (LMPFS for short) of small sizes. They classified all finite groups containing LMPFS of sizes 1 and 2, and some of size 3. The classification problem for size 3 was concluded in [1]. Dihedral groups containing LMPFS of size 4 were classified in [2]. Another goal of this paper is to classify groups of forms (ii) and (iii) that contain locally maximal product-free sets of size 4, continuing work in [1] and [5].

2010 Mathematics Subject Classification: 20D60, 20P05, 05E15
Keywords: Locally maximal, sum-free, product-free, 2-groups.

2. Preliminaries

Here, we gather together some useful results.

Lemma 2.1. [5, Lemma 3.1] *Suppose S is a product-free set in a finite group G. Then S is locally maximal if and only if $G = T(S) \cup \sqrt{S}$, where $T(S) = S \cup SS \cup SS^{-1} \cup S^{-1}S$ and $\sqrt{S} = \{x \in G : x^2 \in S\}$.*

Proposition 2.2. [2, Proposition 1.3] *Each product-free set of size $\frac{|G|}{2}$ in a finite group G is the non-trivial coset of a subgroup of index 2. Furthermore such sets are locally maximal and fill G.*

Lemma 2.3. [6, Lemma 1] *Let N be a normal subgroup of a finite group G. If G is filled, then G/N is filled.*

Theorem 2.4. [2, Propositions 2.8 and 4.8]
(a) The only filled dihedral 2-groups are D_4 and D_8.
(b) No generalised quaternion group is filled.

3. Main results

For a subset S of a 2-group of coclass 1, we write $A(S)$ for $S \cap \langle x \rangle$, and $B(S)$ for $S \cap \langle x \rangle y$. Given $a \in \mathbb{N}$, we write $[0, a]$ for $\{0, 1, \ldots, a\}$.

Proposition 3.1. *Let S be a LMPFS of size $m \geqslant 2$ in a generalised quaternion group G. If $x^{2^{n-2}} \notin S$, then $|G| \leqslant 2(|B(S)| + 4|A(S)||B(S)|)$.*

Proof. Let $A = A(S)$ and $B = B(S)$. By Lemma 2.1, $|G| = 2|B(T(S) \cup \sqrt{S})|$; so to bound $|G|$, we count only the possible elements of $B(S \cup SS \cup S^{-1}S \cup SS^{-1} \cup \sqrt{S})$, and double the result. As $x^{2^{n-2}} \notin S$, we have $B(\sqrt{S}) = \emptyset$. But $B(SS) = AB \cup BA$, $B(SS^{-1}) = BA^{-1} \cup AB^{-1}$ and $B(S^{-1}S) = B^{-1}A \cup A^{-1}B$. By the relations in a generalised quaternion group, $AB = BA^{-1}$ and $BA = A^{-1}B$.

Hence, $|B(T(S) \cup \sqrt{S})| \leqslant |B| + 4|A||B|$, and the result follows. □

A little modification to the proof of Proposition 3.1 gives the following:

Lemma 3.2. *If S is a LMPFS of size $m \geqslant 2$ in a generalised quaternion group G such that $A(S) = A(S)^{-1}$ and $x^{2^{n-2}} \notin S$, then $|G| \leqslant 2(|B(S)| + 2|A(S)||B(S)|)$.*

The next result is a complement of Proposition 3.1. We omit the proof since it is a consequence of the definition of the group in question.

Lemma 3.3. *Let G be a generalised quaternion group. If S is a LMPFS in G and contains the unique involution in $A(G)$, then $S \subseteq A(G)$ and S is locally maximal product-free in $A(G)$.*

In the light of Lemma 3.3, we need to study $A(G)$ more carefully. All cyclic groups containing LMPFS of sizes 1, 2 and 3 are known by the classification results in [1] and [5]. However, we cannot lay our hands on any literature that classified cyclic groups containing LMPFS of a given size $m \geqslant 1$; so we proceed in that direction. Our result (Corollary 3.5) addresses the question of Babai and Sós [3, p. 111] as well as Street and Whitehead [6, p. 226] on the minimal sizes of LMPFS in finite groups for the cyclic group case.

Proposition 3.4. *Let S be a LMPFS of size $m \geqslant 1$ in C_n. Then:*

(*i*) $|SS| \leqslant \frac{m(m+1)}{2}$,

(*ii*) $|SS^{-1}| \leqslant m^2 - m + 1$,

(*iii*) *if n is odd, then* $|\sqrt{S}| = m$,

(*iv*) *if n is even, then* $|\sqrt{S}| \leqslant 2m$.

Proof. Suppose $S = \{x_1, x_2, \dots, x_m\}$. For (i), observe that $SS \subseteq \{x_1x_1, \dots, x_1x_m\} \cup \{x_2x_2, \dots, x_2x_m\} \cup \dots \cup \{x_{m-1}x_{m-1}, x_{m-1}x_m\} \cup \{x_mx_m\}$. Hence, $|SS| \leqslant m + (m-1) + \dots + 2 + 1 = \frac{m(m+1)}{2}$. Case (ii) follows from $SS^{-1} \subseteq \{1, x_1x_2^{-1}, \dots, x_1x_{m-1}^{-1}, x_1x_m^{-1}\} \cup \{x_2x_1^{-1}, 1, \dots, x_2x_{m-1}^{-1}, x_2x_m^{-1}\} \cup \dots \cup \{x_mx_1^{-1}, x_mx_2^{-1}, \dots, x_mx_{m-1}^{-1}, 1\}$. For (iii) and (iv), define a homomorphism $\theta : C_n \to C_n$ by $\theta(x) = x^2$ $\forall x \in C_n$. If n is odd, then $\mathrm{Ker}(\theta) = \{1\}$, and if n is even, then $\mathrm{Ker}(\theta) = \{1, u\}$, where u is the unique involution in C_n. By the first isomorphism theorem, the latter case implies that each element of S has at most two square roots while the former case shows that every element of S has exactly one square root. □

Corollary 3.5. *If S is a LMPFS of size m in a cyclic group G, then $|G| \leqslant \frac{3m^2+3m+2}{2}$ or $\frac{3m^2+5m+2}{2}$ according as $|G|$ being odd or even.*

Proof. As G is abelian, $S^{-1}S = SS^{-1}$; hence by Lemma 2.1, $|G| \leqslant |S| + |SS| + |SS^{-1}| + |\sqrt{S}|$. The rest follows from Proposition 3.4. □

The bound in Corollary 3.5 is fairly tight. For instance, it says that the size of a cyclic group that can contain a LMPFS of size 1 is at most 4. Indeed, the singleton consisting of the unique involution in C_4 is an example.

Definition 3.6. Two LMPFS S and T in a group G are said to be *equivalent* if there is an automorphism of$G$ that takes one into the other.

For a finite group G, we write M_k for the set consisting of all locally maximal product-free sets of size $k \geqslant 1$ in G, S for the representatives of each equivalence class of M_k under the action of the automorphism groups of G, and N_k for the respective number of LMPFS in each orbit. Using GAP [4], we present our results in the Table below.

G	$\|M_4\|$	S	N_4
C_8	1	$\{x, x^3, x^5, x^7\}$	1
C_{10}	2	$\{x, x^4, x^6, x^9\}$	2
C_{11}	5	$\{x, x^3, x^8, x^{10}\}$	5
C_{12}	9	$\{x, x^4, x^6, x^{11}\}, \{x, x^4, x^7, x^{10}\}, \{x^2, x^3, x^8, x^9\}, \{x^2, x^3, x^9, x^{10}\}$	$4, 2, 2, 1$
C_{13}	21	$\{x, x^3, x^5, x^{12}\}$, $\{x, x^3, x^{10}, x^{12}\}$, $\{x, x^5, x^8, x^{12}\}$	$12, 6, 3$
C_{14}	27	$\{x, x^3, x^8, x^{10}\}, \{x, x^3, x^8, x^{13}\}$, $\{x, x^4, x^6, x^{13}\}$, $\{x, x^4, x^7, x^{12}\}, \{x, x^6, x^8, x^{13}\}$	$6, 6, 6, 6, 3$
C_{15}	16	$\{x, x^3, x^5, x^7\}, \{x, x^3, x^7, x^{12}\}$	$8, 8$
C_{16}	37	$\{x, x^3, x^{10}, x^{12}\}$, $\{x, x^4, x^6, x^9\}$, $\{x, x^4, x^6, x^{15}\}$, $\{x, x^4, x^9, x^{14}\}$, $\{x, x^6, x^9, x^{14}\}$, $\{x, x^6, x^{10}, x^{14}\}$, $\{x^2, x^6, x^{10}, x^{14}\}$	$8, 4, 8, 4, 4, 8, 1$
C_{17}	48	$\{x, x^3, x^8, x^{13}\}, \{x, x^3, x^8, x^{14}\}, \{x, x^3, x^{11}, x^{13}\}$	$16, 16, 16$
C_{18}	54	$\{x, x^3, x^5, x^{12}\}, \{x, x^3, x^8, x^{14}\}, \{x, x^3, x^9, x^{14}\}, \{x, x^3, x^{12}, x^{14}\}, \{x, x^4, x^9, x^{16}\}, \{x, x^4, x^{10}, x^{17}\}, \{x, x^5, x^8, x^{12}\}, \{x, x^5, x^8, x^{17}\}, \{x, x^6, x^9, x^{16}\}$	$6, 6, 6, 6, 6, 6, 6, 6, 6$
C_{19}	36	$\{x, x^3, x^5, x^{13}\}, \{x, x^4, x^6, x^9\}$	$18, 18$
C_{20}	36	$\{x, x^3, x^{10}, x^{16}\}, \{x, x^3, x^{14}, x^{16}\}, \{x, x^4, x^{11}, x^{18}\}, \{x, x^5, x^{14}, x^{18}\}, \{x, x^6, x^8, x^{11}\}, \{x^2, x^5, x^{15}, x^{16}\}$	$8, 8, 4, 8, 4, 4$
C_{21}	34	$\{x, x^3, x^5, x^{15}\}, \{x, x^4, x^{10}, x^{17}\}, \{x, x^4, x^{14}, x^{16}\}, \{x, x^8, x^{12}, x^{18}\}$	$12, 12, 4, 6$
C_{22}	10	$\{x, x^4, x^{10}, x^{17}\}$	10
C_{24}	4	$\{x, x^6, x^{17}, x^{21}\}$	4

Table: LMPFS of size 4 in cyclic group G for $8 \leqslant |G| \leqslant 34$

In the light of Corollary 3.5 therefore, if a cyclic group G contains a LMPFS S of size 4, then both G and S are contained in Table. Proposition 2.2 clearly tells us that the LMPFS of size 4 in Q_8 are the non-trivial cosets of the subgroups of index 2. So we shall eliminate this from our investigation.

Proposition 3.7. *Let $G = Q_{2^n}$. If $|G| > 8$ and G contains a LMPFS of size 4, then $G = Q_{16}$. Moreover, up to automorphisms of Q_{16}, the only such set is $\{x, x^6, y, x^4y\}$.*

Proof. Let S be a LMPFS of size 4 in G. We conclude from Lemma 3.3 and deductions from Corollary 3.5 that no such S exist if $x^{2^{n-2}} \in S$. So, suppose $x^{2^{n-2}} \notin S$. In Proposition 3.1, if $|B(S)| = 0$ or 4, then $|G| < 16$, contrary to our assumption that $|G| > 8$. If $|B(S)| = 1$ or 3, we get $|G| < 32$; so $|G| = 16$, and by direct computation, no such S exists. Finally, if $|B(S)| = 2$, then $|G| < 64$. It can easily be seen using dynamics of Lemma 2.1 that S cannot be contained in Q_{32}, and hence the only possibility is that $S \subseteq Q_{16}$. Also elements of $A(S)$ cannot have same order, and that if $B(S) = \{x^iy, x^jy\}$, then i and j must have same parity. Thus, the only possibilities for S are $S_1 := \{x, x^6, y, x^4y\}$, $S_2 := \{x, x^6, xy, x^5y\}$, $S_3 := \{x, x^6, x^3y, x^7y\}$, $S_4 := \{x, x^6, x^2y, x^6y\}$, $S_5 := \{x^2, x^7, y, x^4y\}$, $S_6 := \{x^2, x^7, xy, x^5y\}$, $S_7 := \{x^2, x^7, x^3y, x^7y\}$, $S_8 := \{x^2, x^7, x^2y, x^6y\}$, $S_9 := \{x^2, x^3, y, x^4y\}$, $S_{10} := \{x^5, x^6, y, x^4y\}$, $S_{11} := \{x^2, x^3, xy, x^5y\}$, $S_{12} := \{x^2, x^3, x^3y, x^7y\}$, $S_{13} := \{x^2, x^3, x^2y, x^6y\}$, $S_{14} := \{x^5, x^6, xy, x^5y\}$, $S_{15} := \{x^5, x^6, x^3y, x^7y\}$ and $S_{16} := \{x^5, x^6, x^2y, x^6y\}$. The result follows from the fact that the automorphism ϕ_i takes S_1 into S_i for $1 \leqslant i \leqslant 16$, where $\phi_1 : x \mapsto x, y \mapsto y$, $\phi_2 : x \mapsto x, y \mapsto xy$, $\phi_3 : x \mapsto x, y \mapsto x^3y$, $\phi_4 : x \mapsto x, y \mapsto x^2y$, $\phi_5 : x \mapsto x^7, y \mapsto y$, $\phi_6 : x \mapsto x^7, y \mapsto xy$, $\phi_7 : x \mapsto x^7, y \mapsto x^3y$, $\phi_8 : x \mapsto x^7, y \mapsto x^2y$, $\phi_9 : x \mapsto x^3, y \mapsto y$, $\phi_{10} : x \mapsto x^5, y \mapsto y$, $\phi_{11} : x \mapsto x^3, y \mapsto xy$, $\phi_{12} : x \mapsto x^3, y \mapsto x^3y$, $\phi_{13} : x \mapsto x^3, y \mapsto x^2y$, $\phi_{14} : x \mapsto x^5, y \mapsto xy$, $\phi_{15} : x \mapsto x^5, y \mapsto x^3y$ and $\phi_{16} : x \mapsto x^5, y \mapsto x^2y$. □

Proposition 3.8. *Let S be a LMPFS of size $m \geqslant 4$ in a quasi-dihedral group G. If $x^{2^{n-2}} \notin S$, then $|G| \leqslant 2(|B(S)| + 6|A(S)||B(S)|)$.*

Proof. Similar to the proof of Proposition 3.1. □

Lemma 3.9. *No LMPFS of size 4 in a quasi-dihedral group G contains the unique involution in $A(G)$.*

Proof. Let S be a LMPFS of size 4 in a quasi-dihedral group G such that $x^{2^{n-2}} \in S$. First observe that S must contain elements from both $A(G)$ and $B(G)$; so we have the following three cases: (I) $|A(S)| = 1$ and $|B(S)| = 3$; (II) $|A(S)| = 2$ and $|B(S)| = 2$; (III) $|A(S)| = 3$ and $|B(S)| = 1$. As S is product-free in G, it cannot contain elements of the form $\{x^{2l+1}y,\ l \geqslant 0\}$; otherwise $(x^{2l+1}y)^2 = x^{2^{n-2}} \in S$. For Case I, let $S := \{x^{2^{n-2}}, x^{2i}y, x^{2j}y, x^{2k}y\}$ for $0 \leqslant i, j, k \leqslant 2^{n-2}-1$. Then $A(T(S)) = A(S \cup SS \cup S^{-1}S \cup SS^{-1}) = A(S \cup SS)$. But $A(S \cup SS)$ cannot yield an element of the form x^{2l+1}; so we can only rely on $A(\sqrt{S})$ for such element. Observe that $\sqrt{x^{2i}y} = \sqrt{x^{2j}y} = \sqrt{x^{2k}y} = \emptyset$, and from Proposition 3.4(iv), $|A(\sqrt{x^{2^{n-2}}})| \leqslant 2$. In particular, $A(\sqrt{x^{2^{n-2}}}) = \{x^{2^{n-3}}, x^{3(2^{n-3})}\}$. Hence, there is no element of the form x^{2l+1} in $A(T(S) \cup \sqrt{S})$; a fallacy! as the number of such element in $A(QD_{2^n})$ is 2^{n-2}. Thus, no such S exist. For Case II, let $S := \{x^{2^{n-2}}, x^r, x^{2j}y, x^{2k}y\}$. If r is even, then the number of elements of the form x^{2l+1} in $A(\sqrt{S})$, $A(SS)$ and $A(SS^{-1})$ are at most 2, 0 and 0 respectively; so no such S exist. If r is odd, then the number of elements of the form x^{2l+1} in $A(\sqrt{S})$, $A(SS)$ and $A(SS^{-1})$ are at most 0, 1 and 1 respectively; again, no such S exist. Case III is similar. □

The proof of the next result is similar to that of Proposition 3.7 using Proposition 3.8 and Lemma 3.9.

Proposition 3.10. *Up to automorphisms of QD_{16}, the LMPFS of size 4 in QD_{16} are $\{x, x^6, y, x^4y\}$ and $\{x, x^6, x^3y, x^7y\}$. Furthermore, there is no LMPFS of size 4 in QD_{2^n} for $n > 4$.*

We are now in the position to address the second aim of this paper: classification of filled 2-groups of coclass 1.

Theorem 3.11. *The only filled* 2*-group of coclass* 1 *is* D_8.

Proof. By Theorem 2.4, we only show that no quasi-dihedral group is filled. Let $G = QD_{2^n}$, $n \geqslant 4$. Then $N := \langle x^8 \rangle$ is a normal subgroup of G whose quotient is of size 16. Suppose $|G| > 16$. Given $a_1 \in [0,7]$, $x^{a_1}N = x^{a_1+8a_2}N$ for $1 \leqslant a_2 \leqslant |N|-1$. Similarly, given $b_1 \in [0,7]$, $x^{b_1}yN = x^{b_1+8b_2}yN$ for $1 \leqslant b_2 \leqslant |N|-1$. Thus, $G/N = X \sqcup Y$, where $X = \{x^iN|\ 0 \leqslant i \leqslant 7\}$ and $Y = \{x^iyN|\ 0 \leqslant i \leqslant 7\}$. Clearly, $X \cong C_8 \cong A(D_{16})$. On the other hand, each element of Y has order 2 since for i even, $(x^iyN)(x^iyN) = NN = N$, and for i odd, $(x^iyN)(x^iyN) = x^{2^{n-2}}NN = N$. Hence, $G/N \cong D_{16}$. By Theorem 2.4(a) and Lemma 2.3 therefore, G is not a filled group. Now let $|G| = 16$. By Proposition 3.10, $S = \{x, x^6, y, x^4y\}$ is locally maximal in QD_{16}. However, S does not fill QD_{16} since $|A(QD_{16}^*)| = 7 > 6 = |A(S \sqcup SS)|$; so QD_{16} is not filled. □

We conclude this discussion with the following question:

Question 3.12. *Are there infinitely many non-abelian filled groups?*

Acknowledgements

This research is supported by a Birkbeck PhD scholarship. The author is grateful to Professor Sarah Hart for useful comments.

References

[1] **C.S. Anabanti and S.B. Hart**, *Groups containing small locally maximal product-free sets*, Intern. J. Combin. (2016), Article ID 8939182, 5 pages.

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

[3] **L. Babai and V.T. Sós**, *Sidon sets in groups and induced subgraphs of Cayley graphs*, European J. Combin. **6** (1985), 101 – 114.

[4] **The GAP Group**, *GAP – Groups, Algorithms, and Programming, Version 4.7.7*; 2015, (`http://www.gap-system.org`).

[5] **M. Giudici and S. Hart**, *Small maximal sum-free sets*, Electronic J. Combin. **16** (2009), 1 – 17.

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

Received February 15, 2016

Department of Economics, Mathematics and Statistics, Birkbeck, University of London, WC1E 7HX London, United Kingdom
E-mail: c.anabanti@mail.bbk.ac.uk

Department of Mathematics, University of Nigeria, Nsukka, Nigeria
E-mail: chimere.anabanti@unn.edu.ng

Structure of the finite groups with $4p$ elements of maximal order

Bahareh Asadian and Neda Ahanjideh

Abstract. Let G be a finite group and $p > 3$ be a prime number. We determine the structure of the finite group G with $4p$ elements of maximal order. In particular, we show that if G is a finite group with 20 elements of maximal order, then G is a non-abelian 2-group of order 32 with $\exp(G) = 4$, $G \cong C_6 \times \mathbb{S}_3$ or $G \cong \mathbb{S}_5$, where $\mathbb{S}_n$ denotes the symmetric group of degree n, $G \cong C_{44} \rtimes (C_u \times C_l)$, where $u|10$ and $l|2$, $G \cong C_{25} \rtimes C_l$ or $G \cong C_{50} \rtimes C_l$, where $l|4$.

1. Introduction

Throughout this paper, we use the following notations: For a finite group G, we denote by $\pi(G)$ the set of prime divisors of $|G|$ and by $\pi_e(G)$ the set of element orders of G. By $m_i(G)$, we denote the number of elements of order i, where $i \in \pi_e(G)$. Set $\mathrm{nse}(G) := \{m_i(G) : i \in \pi_e(G)\}$.

One of the interesting topics in the group theory is to determine the solvability of a group with the given particular properties. For example, one of the problems which is proposed by Thompson is:

Thompson's Problem. *Let $T(G) = \{(n, m_n) : n \in \pi_e(G) \ \ and \ \ m_n \in \mathrm{nse}(G)\}$, where m_n is the number of elements of order n in G. Suppose that $T(G) = T(S)$. If S is a solvable group, is it true that G is also necessarily solvable?*

Up to now, nobody can solve this problem and it remains as an open problem. In order to approach to this problem, some authors have examined the solvability of a group with a given number of elements of maximal order. For instance, in [2, 9, 10], the authors have examined the structure of the groups which have a given number of the elements of maximal order. Also, in [4], some groups with exactly $4p$ elements of maximal order have been studied. The purpose of this paper is to study the structure of a group containing exactly $4p$ elements of maximal order. Then as an example, we find the structure of finite groups with exactly 20 elements of maximal order.

From now on, we use $\mathrm{Syl}_p(G)$ for the set of the p-Sylow subgroups of G, where $p \in \pi(G)$. Also, G_p denotes a p-Sylow subgroup of G and $n_p(G) = |\mathrm{Syl}_p(G)|$. We denote by ϕ the Euler's totient function. For every $x \in G$, $o(x)$ denotes the order

2010 Mathematics Subject Classification: 20D05, 20D60
Keywords: group, maximal order,Thompson's problem.

of x and $\langle x\rangle$ denotes the generated subgroup by x in G. $C_G(\langle x\rangle)$ and $N_G(\langle x\rangle)$ are used as centralizer and normalizer of $\langle x\rangle$ in G, respectively. Let A and N be finite groups. The action of A on N is Frobenius if and only if $C_N(a) = 1$, for all nonidentity elements $a \in A$. We use $a|n$ when a is a divisor of n and use $|n|_a = a^e$, when $a^e||n$, i.e., $a^e|n$ but $a^{e+1}\nmid n$. By C_n, we denote a cyclic group of order n. Throughout this paper, k denotes the maximal order of elements in G, $M(G)$ is the number of elements of order k and $n, l \in \mathbb{N}$. Also, $Z(G)$ denotes the center of group G. We apply symbol $(*)$ instead of assumption $M(G) = 4p$, where p is a prime number. All unexplained notations are standard and can be found in [7]. In this paper, we will prove that:

Main Theorem. *Suppose that G is a finite group with $M(G) = 4p$, where $p > 3$ is a prime number. Then G is one of the following groups:*

(1) *If $k = 4$, then G is a non-abelian 2-group with $|G| < 16p$ and* $\exp(\mathrm{G}) = 4$*;*

(2) *if $k = 5$,* $\exp(\mathrm{G}) = 5$ *and $p = (5^u - 1)/4$, then either G is a 5-group of order 5^u or $G \cong \mathrm{G}_5 \rtimes C_{2^t}$, where $t \in \{1, 2\}$ and G_5 denotes 5-Sylow subgroup of G;*

(3) *if $k = 6$, then either $G \cong \mathbb{S}_5$, where $\mathbb{S}_5$ denotes the symmetric group of degree 5 or G is a $\{2, 3\}$-group;*

(4) *if $k = 10$, then G is a $\{2, 5\}$-group;*

(5) *if $k = 12$, then G is a $\{2, 3\}$-group;*

(6) *if $4p+1$ is a prime number and $k = 4p+1$, then $G \cong \mathrm{C}_{4\mathrm{p}+1} \rtimes \mathrm{C}_{\mathrm{l}}$, where $l|4p$;*

(7) *if $2p+1$ is a prime number and $k = 4(2p+1)$, then $G \cong \mathrm{C}_{4(2\mathrm{p}+1)} \rtimes (\mathrm{C}_u \times C_l)$, where $u|2p$ and $l|2$;*

(8) *if $4p + 1$ is a prime number and $k = 2(4p + 1)$, then $G \cong \mathrm{C}_{2(4\mathrm{p}+1)} \rtimes \mathrm{C}_u$, where $u|4p$;*

(9) *if $k = 25$, then $G \cong C_{25} \rtimes C_l$, where $l|4$;*

(10) *if $k = 50$, then then $G \cong C_{50} \rtimes C_l$, where $l|4$.*

As a consequent of the main theorem, we will prove that:

Corollary. *Suppose that G is a finite group with $M(G) = 20$. Then G is one of the following groups:*

(1) *If $k = 4$, then G is a non-abelian 2-group of order 32;*

(2) *if $k = 6$, then either $G \cong \mathbb{S}_5$ or $G \cong C_6 \times \mathbb{S}_3$;*

(3) *if $k = 25$, then $G \cong C_{25} \rtimes C_l$, where $l|4$;*

(4) *if $k = 44$, then $G \cong C_{44} \rtimes (C_u \times C_l)$, where $u|10$ and $l|2$;*

(5) *if $k = 50$, then $G \cong C_{50} \rtimes C_l$, where $l|4$.*

2. Preliminary results

Throughout this paper, we assume that $p > 3$ is a prime number. In the following lemmas, we bring some facts which will be used during the proof of the main theorem:

Lemma 2.1. [3, Lemma 2.2] *Suppose that G has exactly n cyclic subgroups of order l, then $m_l(G) = n \cdot \phi(l)$. In particular, if n denotes the number of cyclic subgroups of G of order k, then $M(G) = n \cdot \phi(k)$.*

The following lemma is concluded from Lemma 2.1:

Lemma 2.2. *If $M(G) = 4p$, then the possible values of k and $\phi(k)$ are given in the following table:*

$\phi(k)$	k	Condition
1	2	–
2	3, 4, 6	–
4	5, 10, 12	–
p	null	–
$2p$	$2p+1$, $2(2p+1)$	$2p+1$ is prime
$4p$	25, 50	$p = 5$
$4p$	$4(2p+1)$	$2p+1$ is prime
$4p$	$4p+1$, $2(4p+1)$	$4p+1$ is prime

Lemma 2.3. [2, Lemma 6] *If k is a prime number, then $k|M(G)+1$.*

Corollary 2.4. *Let $M(G) = 4p$. Then $k \neq 2$ and $k \neq 5$ except when $p = 5t+1$, where $t \in \mathbb{N}$. Also, if $2p+1$ is prime, then $k \neq 2p+1$.*

Proof. It follows from Lemma 2.3. □

Lemma 2.5. [2, Lemma 7] *If there exists a prime divisor p of k with $p(p-1) > M(G)$, then G contains a unique normal p-Sylow subgroup $\mathrm{G_p}$ and $|\mathrm{G_p}| = p$.*

Lemma 2.6. *Let G be a finite group such that $[C_G(x) : \langle x \rangle]$ is a prime power number. Then $C_G(x)$ is direct product of its sylow subgroups.*

Proof. The proof is straightforward. □

Lemma 2.7. [2, Lemma 8] *There exists a positive integer α such that $|G|$ divides $M(G)k^\alpha$.*

Lemma 2.8. *For every element $x \in G$ of order k, $[G : N_G(\langle x \rangle)] \cdot \phi(o(x)) \leqslant M(G)$.*

Proof. The proof is straightforward. □

Lemma 2.9. *For every element $x \in G$ of order k, if $\pi_e(C_G(x)) = \pi_e(\langle x \rangle)$, then $[C_G(x) : \langle x \rangle] \cdot \phi(o(x)) \leqslant M(G)$.*

Proof. Fix $1 \leqslant i \leqslant t$ and $1 \leqslant j \leqslant o(x)$, where $t = [C_G(x) : \langle x\rangle]$. Suppose that $\mathcal{A} = \{y_i\langle x\rangle : y_i \in C_G(x)\}$ is the distinct left coset of $\langle x\rangle$ in $C_G(x)$. It is easily seen that if $y_i\langle x\rangle \neq \langle x\rangle$ and $o(x^j) = k$, then $o(y_i x^j) = o(x^j)$. Also, for every element $y_i\langle x\rangle \in \mathcal{A}$, there exist exactly $\phi(x)$ elements $y_i x^j$ of order k. So, we have:

$$[C_G(x) : \langle x\rangle] \cdot \phi(o(x)) = |\{y_i x^j : o(x^j) = k\}|.$$

It is evident that $|\{y_i x^j : o(x^j) = k\}| \leqslant |\{g \in G : o(g) = k\}| = M(G)$. Hence, the lemma follows. □

Lemma 2.10. [9, Lemma 2.5] *Let P be a p-group of order p^t, where t is a positive integer. Suppose that $b \in Z(P)$, where for $u \in \mathbb{N}$, $o(b) = p^u = k$. Then P has at least $(p-1)p^{t-1}$ elements of order k.*

Lemma 2.11. [10, Lemma 4] *Let G be a non-abelian finite group with* $\exp(G) = 4$. *If $x \in G \setminus Z(G)$ is an element of order 2, then G has at least $\frac{|G|-|C_G(x)|}{2} = \frac{|C_G(x)|.([G:C_G(x)]-1)}{2}$ elements of order 4.*

Lemma 2.12. [5] *Let $p \in \pi(G)$ be odd. Let $\mathrm{G}_p \in \mathrm{Syl}_p(G)$ and $n = p^s m$ with* $\gcd(p, m) = 1$. *If G_p is not cyclic and $s > 1$, then the number of elements of order n is always a multiple of p^s.*

Lemma 2.13. [13, Theorem 3] *Let G be a finite group. Then the number of elements whose orders are multiples of n is either zero, or a multiple of the greatest divisor of $|G|$ that is prime to n.*

Lemma 2.14. [1] *Let $L = U_n(q)$, where $n > 3$, $q = p^\alpha$, and let $d = (n, q+1)$. Then $\pi_e(L)$ consists of all divisors of m, where $m = p^\gamma \frac{q^{n_1}-(-1)^{n_1}}{d}$, where γ, $n_1 > 0$ satisfying $p^{\gamma-1} + 1 + n_1 = n$.*

Lemma 2.15. [5] *Let t be a positive integer dividing $|G|$. If $M_t(G) = \{g \in G | g^t = 1\}$, then $t||M_t(G)|$.*

Corollary 2.16. *For a finite group G:*

(*i*) *if $d \in \pi_e(G)$, then $d|\sum_{s|d} m_s$;*

(*ii*) *if $P \in \mathrm{Syl}_p(G)$ is a cyclic group of prime order p and $r \in \pi(G) - \{p\}$, then $m_{rp} = n_p(G)(p-1)(r-1)t$, where t is the number of cyclic subgroups of order r in $C_G(P)$.*

Proof. (*i*) follows from Lemma 2.15. For proving (*ii*), let $P \in \mathrm{Syl}_p(G)$. Since $m_p(P) = p - 1$ and every element of order rp is in $C_G(P^g)$, for some $g \in G$, we deduce that $m_{rp}(G) = m_p(G) \cdot n_p(G) \cdot m_r(C_G(P)) = (p-1) \cdot n_p(G) \cdot (\phi(r) \cdot t) = n_p(G) \cdot (p-1) \cdot (r-1) \cdot t$, where t is the number of the cyclic subgroups of order r in $C_G(P)$. □

Lemma 2.17. *If p is a prime number, then $4p + 1 \neq 3^t$.*

Proof. Suppose on the contrary that $4p+1=3^t$. Then $4|3^t-1$ and hence, t is a even number. Thus $3^2-1|3^t-1=4p$, which is a contradiction. □

Lemma 2.18. [12] *Let G be a non-solvable group. Then G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that $\frac{K}{H}$ is a direct product of isomorphic non-abelian simple groups and $|\frac{G}{K}|||\mathrm{Out}(\frac{K}{H})|$.*

Lemma 2.19. *Let $H \trianglelefteq G$ and let $r \in \pi(H)$. If $p \in \pi(\frac{G}{H})$, $p \notin \pi(H)$ and $pr \notin \pi_e(G)$, then $p||H|_r-1$.*

Proof. By Frattini's argument, $G=HN_G(R)$, where $R \in \mathrm{Syl}_r(H)$. Thus we can see that $\mathrm{G_p}^g \leqslant N_G(R)$ for some $g \in G$. But $pr \notin \pi_e(G)$ and hence, the action of $\mathrm{G_p}^g$ on R is Frobenius. Therefore, $|G|_p||H|_r-1$ and the result follows. □

A finite group G is called a *simple K_n-group*, if G is a simple group with $|\pi(G)|=n$. So, a simple K_3-group is a simple group with $|\pi(G)|=3$. In the following lemma, the simple K_3-groups and their orders are recognized:

Lemma 2.20. [8] *Let G be a simple K_3-group. Then G is isomorphic to one of following simple groups: $A_5(2^2\cdot3\cdot5)$, $A_6(2^3\cdot3^2\cdot5)$, $L_2(7)(2^3\cdot3\cdot7)$, $L_2(8)(2^3\cdot3^2\cdot7)$, $L_2(17)(2^4\cdot3^2\cdot17)$, $L_3(3)(2^4\cdot3^3\cdot13)$, $U_3(3)(2^5\cdot3^3\cdot7)$, $U_4(2)(2^6\cdot3^4\cdot5)$.*

Theorem 2.21. *If G is a non-solvable group with $M(G)=4p$, where p is a prime number, then $p=5$ and $G \cong \mathbb{S}_5$.*

Proof. Since G is a non-solvable group, Lemma 2.18 shows that there exists a chief series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that $\frac{K}{H}$ is a direct product of isomorphic non-abelian simple groups and $|\frac{G}{K}|||\mathrm{Out}(\frac{K}{H})|$. Lemmas 2.2 and 2.7 show that $|\pi(G)| \leqslant 3$ and every finite group such that its order is divisible by exactly two prime numbers is solvable. Thus $|\pi(\frac{K}{H})|=3$ and $p||\frac{K}{H}|$. Therefore, $\frac{K}{H}$ is a simple K_3-group and $p \in \pi(\frac{K}{H})$. Also, by virtu of Lemma 2.20, we can see that for every simple K_3-group S, $3 \in \pi(S)$. Since our assumption forces $p>3$, $k \neq 3$. Therefore, Lemmas 2.2 and 2.7 imply that the non-solvability of G can be occurred when $k \in \{6,12\}$.

We continue the proof in the following cases:

1. If $k=6$, then Lemma 2.7 and the above statements show that $|K/H|=2^\alpha 3^\beta p$, where $\alpha,\beta>0$. Then $\frac{K}{H}$ is a simple K_3-group and hence, Lemma 2.20 shows that one of the following subcases holds:

(i). If $\frac{K}{H} \cong A_5$ or A_6, then $p=5$. Let z be an element of G with $o(z)=6$. By Lemma 2.9, we have $[C_G(z):\langle z\rangle] \leqslant 10$. Since $k=6$, $5 \nmid |C_G(z)|$. If $[C_G(z):\langle z\rangle] \in \{8,9\}$, then Lemma 2.6 implies that $C_G(z)$ is direct product of its sylow subgroups. Hence, it is easy to see that $m_6(C_G(z))>20$. So, we get a contradiction with $M(G)=20$. Therefore, $[C_G(z):\langle z\rangle] \in \{1,2,3,4,6\}$. We have,

$$|G|=6\cdot[C_G(z):\langle z\rangle]\cdot[N_G(\langle z\rangle):C_G(z)]\cdot[G:N_G(\langle z\rangle)].$$

By virtue of Lemma 2.8, we can see that $[G:N_G(\langle z\rangle)] \leqslant 2p=10$.

Since $[N_G(\langle z\rangle) : C_G(\langle z\rangle)]||\mathrm{Aut}(\langle z\rangle)| = 2$, we deduce that $5|[G : N_G(\langle z\rangle)]$. Hence, $|G||2^5 \cdot 3^2 \cdot 5$ and $2^2 \cdot 3 \cdot 5||\frac{K}{H}|$. Therefore, $|H||2^3 \cdot 3$. But $2 \cdot 5, 3 \cdot 5 \notin \pi_e(G)$. So, Lemma 2.19 shows that $5|3^t - 1$ or $5|2^u - 1$, where $t < 2$ and $u \leqslant 3$. Thus, $t = u = 0$ and hence, $|H| = 1$. Thus $K \cong A_5$ or A_6. Since $|\frac{G}{K}|||\mathrm{Out}(K)|$, we deduce that $G \cong \mathbb{S}_5$ or $\mathbb{S}_6$. But $M(\mathbb{S}_5) = 20$ and $M(\mathbb{S}_6) = 240$. Thus $G \cong \mathbb{S}_5$.

(ii). If $\frac{K}{H} \cong L_2(7), L_2(8), L_2(17), L_3(3), U_3(3)$, then there exists $p \in \pi(G)$ such that $p > 6$, which is a contradiction.

(iii). If $\frac{K}{H} \cong U_4(2)$, then Lemma 2.14 implies that $12 \in \pi_e(\frac{K}{H})$ and hence, we arrive at a contradiction.

2. Let $k = 12$. Then applying Lemma 2.7 shows that $\pi(G) = \{2, 3, p\}$. Since every finite group such that its order is divisible by exactly two prime numbers is solvable and $|\pi(G)| = 3$, we deduce that $|\pi(\frac{K}{H})| = 3$ and $p||\frac{K}{H}|$. Since $k = 12$, we deduce that $p \leqslant 11$ and for every $x \in G$ with $o(x) = 12$, $C_G(\langle x\rangle)$ is a $\{2, 3\}$-group. Since $\frac{K}{H}$ is a simple K_3-group, Lemma 2.20 shows that one of the following subcases holds:

(i). If $\frac{K}{H} \cong A_5$ or A_6, then $p = 5$. In the following, we show that this case is impossible with our assumption. It is easy to see that $|C_G(\langle x\rangle)| = 2^u \cdot 3^v$ such that $2 \leqslant u \leqslant 4$ and $1 \leqslant v \leqslant 2$. Applying Lemma 2.8 to this case shows that $[G : N_G(\langle x\rangle)] \in \{1, 2, 3, 4, 5\}$. Note that for every $x \in G$ with $o(x) = 12$, $[N_G(\langle x\rangle) : C_G(\langle x\rangle)]||\mathrm{Aut}(\langle x\rangle)| = 4$. But $5||G|$ and

$$|G| = [G : N_G(\langle x\rangle)] \cdot [N_G(\langle x\rangle) : C_G(\langle x\rangle)] \cdot |C_G(\langle x\rangle)|. \tag{1}$$

Thus $[G : N_G(\langle x\rangle)] = 5$ and $|G||2^6 \cdot 3^2 \cdot 5$. Since $|\mathrm{Aut}(\langle x\rangle)| = 4$, we conclude that $\mathrm{G}_3 \leqslant C_G(\langle x\rangle)$. Set $C = C_G(\langle x\rangle)$. We examine two possibilities for v:

(a). Let $v = 2$. Applying Lemma 2.9 shows that $|C_G(\langle x\rangle)| = 2^2 \cdot 3^2$. Since $\langle x\rangle \leqslant Z(C)$, $12||Z(C)|$. Thus C is abelian and hence,

$$C = C_4 \times (C_3 \times C_3). \tag{2}$$

Therefore, $m_{12}(C) = 16$. If there exists $y \in G$ of order 12 such that $9 \nmid |C_G(y)|$, then obviously $y \notin C$ and (1) leads us to see that $3|[G : N_G(\langle y\rangle)] = 5$, which is a contradiction. This shows that for every $y \in G$ of order 12, $|C_G(y)|_3 = 9$, so for some $g \in G$,

$$\mathrm{G}_3^g \leqslant C_G(y). \tag{3}$$

Also, (2) shows that $C \leqslant C_G(\mathrm{G}_3)$. So, $C_G(\mathrm{G}_3)$ contains at least 16 elements of order 12. Thus for every $g \in G$ with $C_G(\mathrm{G}_3) \neq C_G(\mathrm{G}_3^g)$, $C_G(\mathrm{G}_3) \cap C_G(\mathrm{G}_3^g)$ contains at least 12 elements of order 12. Let y be an element of order 12 in $C_G(\mathrm{G}_3) \cap C_G(\mathrm{G}_3^g)$, then $\mathrm{G}_3, \mathrm{G}_3^g \trianglelefteq C_G(y)$. Thus $\mathrm{G}_3 = \mathrm{G}_3^g$ and hence $\mathrm{G}_3 \trianglelefteq G$. Therefore, (3) shows that for every $y \in G$ of order 12, $y \in C_G(\mathrm{G}_3) = \mathrm{G}_3 \times \mathrm{G}_2(C_G(\mathrm{G}_3))$. Hence $20 = m_{12}(G) = m_{12}(C_G(\mathrm{G}_3)) = m_3(\mathrm{G}_3) \cdot m_4(\mathrm{G}_2(C_G(\mathrm{G}_3))) = 8 \cdot m_4(\mathrm{G}_2(C_G(\mathrm{G}_3)))$, which is a contradiction.

(b). Let $v = 1$. Then $K/H \cong A_5$ and $|C_G(\langle x\rangle)| = 2^u \cdot 3$. Since $[N_G(\langle x\rangle) : C_G(\langle x\rangle)]$ divides 4 and $[G : N_G(\langle x\rangle)] = 5$, $|G|_3 = 3$. Also, Lemma 2.9 forces $u \leqslant 4$. Thus

$|G||2^6 \cdot 3 \cdot 5$ and hence, $n_3(G) = 2^\alpha \cdot 5^\beta$, where $\beta \in \{0, 1\}$. On the other hand, $n_3(K/H) = 10|n_3(G)$. But Corollary 2.16(ii) shows that $m_{12}(G) = n_3(G) \cdot \phi(3) \cdot t = 20$, where $t = m_4(C_G(\mathrm{G}_3)) \geqslant 2$, which is impossible.

(ii). If $\frac{K}{H} \cong L_3(3)$ or $L_2(17)$, then there exists $p \in \pi(\frac{K}{H})$ such that $p > 11$, which is contradiction.

(iii). If $\frac{K}{H} \cong U_4(2)$ or $U_3(3)$, then $p = 5$ or 7, respectively. Applying Lemma 2.14 and GAP program [6] imply that $12 \in \pi_e(\frac{K}{H})$. Since $m_{12}(U_3(3)) = 1008$ and $m_{12}(U_4(2)) = 4320$, we arrive at a contradiction;

(iv). If $\frac{K}{H} \cong L_2(7)$ or $L_2(8)$, then $p = 7$ and $|G| = 7 \cdot 2^u \cdot 3^v$, where $1 \leqslant u \leqslant 7$ and $1 \leqslant v \leqslant 2$. If $v = 2$, then we can see at once that either $K/H \cong L_2(8)$ or $|H|_3 = 3$. If $|H|_3 = 3$, then since $21 \notin \pi_e(G)$, Lemma 2.19 shows that $7|3 - 1$, which is a contradiction. Thus let $K/H \cong L_2(8)$. Then since for every $y \in G$ of order 12, y is central in $C_G(y)$, we deduce that $y \in C_G(\mathrm{G}_3)$. Thus we can see at once that $C_G(\mathrm{G}_3)$ contains at least 16 elements of order 12. So, for every $g \in G$ with $C_G(\mathrm{G}_3) \neq C_G(\mathrm{G}_3^g)$, $C_G(\mathrm{G}_3) \cap C_G(\mathrm{G}_3^g)$ contains at least 12 elements of order 12. Let y be an element of order 12 in $C_G(\mathrm{G}_3) \cap C_G(\mathrm{G}_3^g)$. Then $\mathrm{G}_3, \mathrm{G}_3^g \leqslant C_G(y)$. On the other hand, applying the argument in Subcase (i) shows that $|C_G(y)| \leq 3^2 \cdot 2^3$. Thus $\mathrm{G}_3 \times \langle y^3 \rangle$, $\mathrm{G}_3^g \times \langle y^3 \rangle \trianglelefteq C_G(y)$ and hence, $\mathrm{G}_3, \mathrm{G}_3^g \trianglelefteq C_G(y)$. Thus $\mathrm{G}_3 = \mathrm{G}_3^g$ which is a contradiction. Therefore, $C_G(\mathrm{G}_3) \trianglelefteq G$ and hence, $\mathrm{G}_3 \trianglelefteq G$. Thus the same argument as that of used in (2) shows that for every $y \in G$ of order 12, $y \in C_G(\mathrm{G}_3) = \mathrm{G}_3 \times \mathrm{G}_2(C_G(\mathrm{G}_3))$ and hence, $28 = m_{12}(G) = m_3(\mathrm{G}_3) \cdot m_4(\mathrm{G}_2(C_G(\mathrm{G}_3))) = 8 \cdot m_4(\mathrm{G}_2(C_G(\mathrm{G}_3)))$, which is impossible. Thus $v = 1$ and hence, $K/H \cong L_2(7)$ and $m_{12}(G) = 2 \cdot n_3(G) \cdot t = 28$, where $t = m_4(C_G(\mathrm{G}_3)) \geqslant 2$. But $n_3(L_2(7)) = 28|n_3(G)$, which is impossible. □

3. Proof of the main theorem

In this section, we prove the main theorem by considering the eight values for k obtained in Lemma 2.2:

1) $k = 3$. By virtue of Lemma 2.7, we have $|G||4 \cdot 3^\alpha \cdot p$, where $\alpha > 0$. But $k = 3$ and according to our assumption $p > 3$. Thus $|G||2^2 \cdot 3^\alpha$. Since $k = 3$, two possibilities can be occurred for $|G|$:

(i). If $|G| = 3^u$, where $u \in \mathbb{N}$, then since $k = 3$, $\exp(G) = 3$ and hence, $|G| - 1 = M(G)$. Thus $3^u - 1 = 4p$, which is a contradiction with Lemma 2.17.

(ii). If $2 \in \pi(G)$, then $|G| = 2^{\alpha_1} \cdot 3^{\alpha_2}$ such that $0 \leqslant \alpha_1 \leqslant 2$ and $\alpha_2 > 0$. Thus G is solvable. Let N be a normal minimal subgroup of G. Then N is t-elementary abelian, where $t \in \{2, 3\}$. Since $6 \notin \pi_e(G)$, we deduce that for $u \in \{2, 3\} - \{t\}$, the action of G_u on N is Frobenius. Thus if $t = 2$, then G_3 is cyclic and since $k = 3$, we deduce that by Corollary 2.16(ii), $2 \cdot n_3(G) = 4p$. This forces $n_3(G) = 2p||G|_2$, which is a contradiction. Now let $t = 3$. Then G_2 is a cyclic group or a quaternion group. But $4 \notin \pi_e(G)$ and hence, $|\mathrm{G}_2| = 2$. This guarantees that $\mathrm{G}_3 \trianglelefteq G$. Thus $m_3(G) = m_3(\mathrm{G}_3)$ and hence, applying the previous argument leads us to get a contradiction.

2) $k = 4$. Applying Lemma 2.7 shows that either $p = 3$ and $\pi(G) = \{2, 3\}$ or G is a 2-group. According to our assumption, $p > 3$ and hence, G is a 2-group. Let $|G| = 2^\alpha$, where $\alpha \in \mathbb{N}$. Then by $(*)$, we can see $|G| > 4p + 1$. If G is an abelian group such that $|G| = 2^\alpha$, then $\{x \in G : o(x)|2\} \leqslant G$ and hence, $1+m_2(G) = 2^u$ and $1+m_2(G)+m_4(G) = |G|$ gives that $2^u+4p = 2^\alpha$. This forces $2^u(2^{\alpha-u} - 1) = 4p$ and hence, $u = 2$. Thus $m_2(G) = 3$ and hence, $G \cong C_4 \times C_4$ or $C_2 \times C_4$. So, $m_4(G) \leqslant 12$, which is a contradiction. If G is a non-abelian 2-group, then we claim that there exists an element y in G such that $y \notin Z(G)$ and $o(y) = 2$. If not, then $Z(G)$ contains all elements of order 2 in G. If $2^{\alpha-3} \leqslant p$, then since our assumption shows that $|Z(G)| \geq |G| - 4p$, we have $|G/Z(G)| \leqslant 2$. Thus G is abelian, which is a contradiction. If $2^{\alpha-3} > p$, then Lemma 2.10 shows that there is no element of order 4 in $Z(G)$, so $|G| = |Z(G)| + M(G)$ and hence, $2^\alpha = 2^m + M(G)$, where $|Z(G)| = 2^m$. Thus $m = 2$ and $p = 2^{\alpha-2} - 1 > 2^{\alpha-3} > p$, which is a contradiction. So, there exists $y \in G \setminus Z(G)$ with $o(y) = 2$. Therefore, Lemma 2.11 and $(*)$ show that $\frac{|G|}{4} \leq \frac{|G|-|C_G(x)|}{2} \leqslant 4p$ and hence, we can conclude that $|G| < 16p$.

3) $k = 5$ and $p = 5t+1$. Then by virtue of Lemma 2.7, $|G||2^2 \cdot p \cdot 5^\alpha$, where $\alpha > 0$. Since $p = 5t + 1$ is a prime number which is greater than 5, $p \notin \pi(G)$. If G is a 5-group, then $\exp(G) = 5$, so $4p = |G| - 1 = 5^u - 1$ and hence, $p = (5^u - 1)/4$. If G is a $\{2, 5\}$-group, then G is solvable. Let N be a normal minimal subgroup of G. In the following, we examine two possibilities for order of N:

(i). If $|N|=2^t$, where $t\in\mathbb{N}$, then the action of G_5on N is Frobenius. Hence G_5 is cyclic. Since $25 \notin \pi_e(G)$, $|\mathrm{G}_5| = 5$. Corollary 2.16(ii) shows that $m_5(G) = n_5(G)\cdot 4$ $= 4p$ which follows that $p = n_5(G)||G|$. Hence, we arrive at a contradiction.

(ii). If $|N| = 5^u$, then $|\mathrm{G}_2| \in \{2, 4\}$. Thus $\mathrm{G}_5 \trianglelefteq G$ and hence, $G \cong \mathrm{G}_5 \rtimes C_{2^t}$, where $t \in \{1, 2\}$. Therefore, $5^u - 1 = |\mathrm{G}_5| - 1 = 4p$ and hence, $p = (5^u - 1)/4$, as claimed.

4) $k = 6$. By virtue of Lemma 2.7, we deduce that $|G||2^{\alpha_1} \cdot 3^{\alpha_2} \cdot p$, where for $i \in \{1, 2\}$, $\alpha_i > 0$. If $\pi(G) = \{2, 3, p\}$, then since $k = 6$, $p \leqslant 5$. But $p \neq 3$ and hence, $p = 5$, thus by Lemma 2.8, there is no element such as z in G with $o(z) = 6$ such that $[G : N_G(\langle z\rangle)] \in \{15, 20\}$. We claim that there exists z' in G such that $o(z') = 6$ and $5|[G : N_G(\langle z'\rangle)]$. If not, then since $|\mathrm{Aut}(\langle z'\rangle)| = 2$, it is concluded that $5||C_G(\langle z'\rangle)|$. So, G contains an element of order 30, which is contradiction with $k = 6$. Thus $5|[G : N_G(\langle z'\rangle)]$ and hence, Lemma 2.8 shows that $[G : N_G(\langle z'\rangle)] \in \{5, 10\}$. Since $[G : N_G(\langle z'\rangle)]|10$ and $[N_G(\langle z'\rangle) : C_G(\langle z'\rangle)]|2$, we deduce that $\mathrm{G}_3 \leqslant C_G(\langle z'\rangle)$. By our assumption, we can conclude $\exp(\mathrm{G}_3) = 3$ and hence, $|C_G(\langle z'\rangle)|_3 \leqslant 20$. So, we have $|\mathrm{G}_3| \in \{3, 9\}$. First let G be a solvable group and let H be a $\{3, 5\}$-Hall subgroup of G. Therefore, $n_3(H) = 3s + 1|5$ and hence, $s = 0$. So, $5||N_H(\mathrm{G}_3)|$ and hence, $5||N_G(\mathrm{G}_3)|$. But, $[N_G(\mathrm{G}_3) : C_G(\mathrm{G}_3)]||\mathrm{Aut}(\mathrm{G}_3)|$ and $\mathrm{Aut}(\mathrm{G}_3) \cong C_2$ or $GL_2(3)$. Therefore, $5||C_G(\mathrm{G}_3)|$ and hence, G contains an element of order 15, which is a contradiction with $k = 6$. Hence, G is a $\{2, 3\}$-group. Also, if G is a non-solvable group, then Theorem 2.21 shows that $G \cong \mathbb{S}_5$.

5) $k = 10$. In this case, Lemma 2.7 shows that $10||G|$ and $|G||2^{\alpha_1} \cdot 5^{\alpha_2} \cdot p^{\alpha_3}$, where for $i \in \{1,2\}$, $\alpha_i > 0$ and $\alpha_3 \in \{0,1\}$. If $p \neq 5$ and $\pi(G) = \{2,5,p\}$, then since $k = 10$, $p < 10$. Since $3 < p$, $p = 7$. Hence, Lemma 2.8 forces $[G : N_G(\langle z\rangle)] \leqslant 7$, where z is an element in G with $o(z) = 10$. We claim that 7 divides $[G : N_G(\langle z\rangle)]$. If not, then since $[N_G(\langle z\rangle) : C_G(\langle z\rangle)]|4$, (1) shows that $7||C_G(\langle z\rangle)|$, which is a contradiction with $k = 10$. Hence, $[G : N_G(\langle z\rangle)] = 7$, so (1) implies that $\mathrm{G}_5 \leqslant C_G(\langle z\rangle)$. Thus $\exp(\mathrm{G}_5) = 5$ and hence, $|C_G(\langle z\rangle)|_5 \leqslant 28$. Thus $|\mathrm{G}_5| \in \{5, 25\}$. By virtue of Theorem 2.21, G is solvable. Let H be a $\{5,7\}$-Hall subgroup of G. Therefore, $n_5(H) = 5v + 1|7$ and hence, $v = 0$. So, $7||N_H(\mathrm{G}_5)|$ and hence, $7||N_G(\mathrm{G}_5)|$. But $[N_G(\mathrm{G}_5) : C_G(\mathrm{G}_5)]||\mathrm{Aut}(\mathrm{G}_5)|$. Since $\mathrm{Aut}(\mathrm{G}_5) \cong C_4$ or $GL_2(5)$, $7||C_G(\mathrm{G}_5)|$, by (1). Hence, G contains an element of order 35, which is a contradiction with $k = 10$. Therefore, G is a $\{2,5\}$-group.

6) $k = 12$. Then applying Lemma 2.7 shows that $|G||2^{\alpha_1} \cdot 3^{\alpha_2} \cdot .p^{\alpha_3}$, where for $i \in \{1,2\}$, $\alpha_i > 0$ and $\alpha_3 \in \{0,1\}$. By our assumption, we have $p \neq 3$. If $\pi(G) = \{2,3,p\}$, then since $k = 12$, we deduce that $p \leqslant 11$. If $p = 5$, then repeating the argument given in the proof of Case (2-i) of Theorem 2.21 shows that $|G|_3 = 3$ and $n_3(G) \in \{1, 5, 10, 40, 160\}$. But Corollary 2.16($ii$) shows that $m_{12}(G) = n_3(G) \cdot \phi(3) \cdot t = 20$, where $t = m_4(C_G(\mathrm{G}_3)) \geq 2$ and also, $n_3(G) = 3s+1 \neq 5$. Thus $n_3(G) \notin \{5, 10, 40, 160\}$ and hence, $n_3(G) = 1$. Also, $15 \notin \pi_e(G)$. So, the action of G_5 on G_3 is Frobenius and hence, $|\mathrm{G}_5| = 5|3 - 1$, which is a contradiction. If $p = 7$, then repeating the argument given in the proof of Case (2-iv) of Theorem 2.21 shows that $|G|_3 = 3$ and $|G|_7 = 7$. Let N be a normal minimal subgroup of G. If $|N| = 7$, then since $14 \notin \pi_e(G)$, the action of G_2 on N is Frobenius and hence, $|\mathrm{G}_2||7 - 1$. Thus $|\mathrm{G}_2| = 2$, which is a contradiction. Also, since $21 \notin \pi_e(G)$ and $7 \nmid 3 - 1$, we can see that $3 \nmid |N|$. Thus $n_3(G) \neq 1$. But $28 = m_{12}(G) = 2 \cdot n_3(G) \cdot m_4(C_G(\mathrm{G}_3))$. Therefore, $n_3(G) = 7$ and $m_4(C_G(\mathrm{G}_3)) = 2$. Also, this allows us to assume that $\mathrm{G}_2 \leqslant N_G(\mathrm{G}_3)$. If $|N| = 2^t$, then since $14 \notin \pi_e(G)$, the action of G_7 on N is Frobenius and hence, G_2 is abelian and $7|2^t - 1$. Also, applying Lemmas 2.10 and 2.11 guarantee that $4 \leqslant |\mathrm{G}_2(C_G(\mathrm{G}_3))| \leqslant 8$. On the other hand, $|N_G(\mathrm{G}_3)|/|C_G(\mathrm{G}_3)|||\mathrm{Aut}(C_3)| = 2$ and $\mathrm{G}_2 \leqslant N_G(\mathrm{G}_3)$. So, $8 \leqslant |\mathrm{G}_2| \leqslant 16$. Therefore, $t = 3$ and hence, we can see at once that N is a 2-elementary abelian group of order 8 and $C_G(N) = N$. Thus $|\mathrm{G}_2| = 16$, because, $4 \in \pi_e(G)$. On the other hand, $12 \in \pi_e(G)$ and hence, we can see that $C_6 \lesssim N_G(N)/C_G(N) \cong GL_3(2)$, which is a contradiction, because $6 \notin \pi_e(GL_3(2))$. If $p = 11$, then Lemma 2.8 forces $[G : N_G(\langle z\rangle)] \leqslant 11$, where z is an element in G with $o(z) = 12$. We claim that $11|[G : N_G(\langle z\rangle)]$. If not, then since $[N_G(\langle z\rangle) : C_G(\langle z\rangle)]|4$, (1) shows that $11||C_G(\langle z\rangle)|$, which is a contradiction with $k = 12$. Hence, $[G : N_G(\langle z\rangle)] = 11$ and so, (1) implies that $\mathrm{G}_3 \leqslant C_G(\langle z\rangle)$. Thus $\exp(\mathrm{G}_3) = 3$ and hence, $|C_G(\langle z\rangle)|_3 \times 2 \leqslant 44$. Therefore, $|\mathrm{G}_3| \in \{3, 9\}$. By virtue of Theorem 2.21, G is solvable. Let H be a $\{3,11\}$-Hall subgroup of G. Therefore, $n_3(H) = 3v + 1|11$ and hence, $v = 0$. So, $11||N_H(\mathrm{G}_3)|$ and hence, $11||N_G(\mathrm{G}_3)|$. But $[N_G(\mathrm{G}_3) : C_G(\mathrm{G}_3)]||\mathrm{Aut}(\mathrm{G}_3)|$ and $\mathrm{Aut}(\mathrm{G}_3) \cong C_2$ or $GL_2(3)$, thus $11||C_G(\mathrm{G}_3)|$, by (1). Hence, G contains an element of order 33, which is a contradiction with $k = 12$. Therefore, G is a $\{2,3\}$-group.

7) Let $2p + 1$ be a prime number and $k \in \{2(2p + 1), 4(2p + 1)\}$ or let $4p + 1$ be a prime number and $k \in \{4p+1, 2(4p+1)\}$. In the following, we examine the structure of G for every value of k:

(i). If $k = 4p+1$, then since $(4p+1)4p > 4p$, Lemma 2.5 implies that $n_{4p+1} = 1$ and $|\mathrm{G}_{4p+1}| = 4p+1$ and hence, G_{4p+1} is a cyclic normal subgroup of G. Since by Lemma 2.9, $|C_G(\mathrm{G}_{4p+1})| = 4p+1$, we have $G/C_G(\mathrm{G}_{4p+1}) \hookrightarrow \mathrm{Aut}(\mathrm{G}_{4p+1}) \cong C_{4p}$ and hence, $G \cong C_{4p+1} \rtimes C_l$, where $l|4p$.

(ii). If $k = 2(2p+1)$, then by virtue of Lemma 2.7, we deduce that $|G||2^{\alpha_1} \cdot p \cdot (2p+1)^{\alpha_2}$, where for $i \in \{1,2\}$, $\alpha_i > 0$. Since $(2p+1)2p > 4p$, Lemma 2.5 implies that $\mathrm{G}_{2p+1} \trianglelefteq G$ and $|\mathrm{G}_{2p+1}| = 2p+1$. Hence, G_{2p+1} is a cyclic subgroup of G. Thus Corollary 2.16(ii) shows that $m_{2(2p+1)}(G) = n_{2p+1}(G) \cdot 2p \cdot t$, where $t = m_2(C_G(\mathrm{G}_{2p+1}))$ and hence, $m_{2(2p+1)}(G) = 2p \cdot t = 4p$ which shows that $t = 2$. It is a contradiction with Corollary 2.16(i).

(iii). If $k = 4(2p+1)$ and x is an element G of order k, then by Lemmas 2.8 and 2.9, we can see that $C_G(x) = \langle x \rangle$ and $[G : N_G(\langle x \rangle)] = 1$. Thus $\langle x \rangle \trianglelefteq G$ and $G/\langle x \rangle \hookrightarrow \mathrm{Aut}(\langle x \rangle) \cong C_{2p} \times C_2$. Therefore, $G \cong C_{4(2p+1)} \rtimes (C_u \times C_l)$, where $u|2p$ and $l|2$.

(iv). If $k = 2(4p+1)$ and x is an element G of order k, then by Lemmas 2.8 and 2.9, we can see that $C_G(x) = \langle x \rangle$ and $[G : N_G(\langle x \rangle)] = 1$. Thus $\langle x \rangle \trianglelefteq G$ and $G/\langle x \rangle \hookrightarrow \mathrm{Aut}(\langle x \rangle) \cong C_{4p}$. Therefore, $G \cong C_{2(4p+1)} \rtimes C_l$, where $l|4p$.

8) Let $k = 25$ and let x be an element of order 25 in G. According to Lemma 2.2, in this case $p = 5$. Hence, Lemma 2.7 shows that $|G||2^2 \cdot 5^\alpha$, where $\alpha > 0$. It follows by Lemmas 2.8 and 2.9 that $C_G(x) = \langle x \rangle$ and $\langle x \rangle$ is a normal subgroup of G. Therefore, $G/\langle x \rangle \lesssim \mathrm{Aut}(C_{25}) \cong C_{20}$. If $5^3||G|$, then since $25 \in \pi_e(G)$ and $\mathrm{G}_5 \trianglelefteq G$, we deduce that $m_{25}(G) = m_{25}(\mathrm{G}_5)$. Since there is not any group of order 125 with the unique cyclic subgroup of order 25, we deduce that $|\mathrm{G}_5| = 25$. Thus $\frac{G}{C_G(x)} \lesssim C_4$ and hence, $G \cong C_{25} \rtimes C_l$, where $l|4$.

9) $k = 50$. Let $x \in G$ such that $o(x) = 50$. By virtue of Lemma 2.2, $p = 5$. Similar to the previous argument, we have $\langle x \rangle = C_G(x)$. Since $k = 50$, $5^2||G|$ and hence, we conclude that $5^2 \leqslant |G|_5$. We claim that $|G|_5 = 5^2$. If not, then $|\mathrm{G}_5| = 5^s$, where $s \geqslant 3$. Then it is evident that G_5 can not be a cyclic group and hence, Lemma 2.12 shows that $5^2|M(G) = 20$, which is impossible. So, we deduce that $|\mathrm{G}_5| = 5^2$ and hence, $\frac{G}{C_G(x)} \lesssim C_4$. Thus $G \cong C_{50} \rtimes C_l$, where $l|4$. □

In the following, as a consequent of the main theorem, we examine the structure of finite group G with $M(G) = 20$:

Corollary 3.1. *Let G be a finite group with $M(G) = 20$. Then G is one of the following groups:*

(1) *If $k = 4$, then G is a non-abelian 2-group of order 32;*

(2) *if $k = 6$, then either $G \cong \mathbb{S}_5$ or $G \cong C_6 \times \mathbb{S}_3$;*

(3) *if $k = 25$, then $G \cong C_{25} \rtimes C_l$, where $l|4$;*

(4) *if $k = 44$, then $G \cong C_{44} \rtimes (C_u \times C_l)$, where $u|10$ and $l|2$;*

(5) *if $k = 50$, then $G \cong C_{50} \rtimes C_l$, where $l|4$.*

Proof. In Lemma 2.1 and Lemma 2.2, the possible values for k, are recognized. On the other hand, according to Lemma 2.3, $k \neq 2, 5, 11$. Also, Theorem 2.21 implies that $k \neq 3$.

In the following, the other values of k are examined:

(1). Let $k = 4$. According to case (2) of the proof of the main theorem, G is a non-abelian 2-group with $|G| < 16 \cdot 5 = 80$. According to the classification of non-abelian groups of order 64, there is no group of order 64 with $\exp(G) = 4$ and $M(G) = 20$. So, G is a non-abelian 2-group of order 32.

(2). If $k = 6$ and G is a non-solvable group, then $G \cong \mathbb{S}_5$, by Theorem 2.21. In the following, we examine the structure of G, when G is a solvable group and $k = 6$. According to our main theorem, G is a $\{2, 3\}$-group. We have $|C_G(x)| = 2^u \cdot 3^v$, where $u, v \leqslant 2$ and $x \in G$ such that $o(x) = 6$. Since $M(G) = 20$, then Lemma 2.8 shows that $[G : N_G(\langle x\rangle)] \in \{1, 2, 3, 4, 6, 8, 9\}$. If there exists an element y of order 6 in G such that $[G : N_G(\langle y\rangle)] \in \{3, 6, 8, 9\}$, then our assumption, $M(G) = 20$, guarantees the existence of another element z of order 6 in G such that $[G : N_G(\langle z\rangle)] \in \{1, 2, 4\}$. In fact, without loss of generality, we can assume that G always has an element x such that $[G : N_G(\langle x\rangle)] \in \{1, 2, 4\}$. Also, $[N_G(\langle x\rangle) : C_G(\langle x\rangle)]||\mathrm{Aut}(\langle x\rangle)| = 2$. So, (1) forces $|G||2^5 \cdot 3^2$.

Since $[G : N_G(\langle x\rangle)]|4$ and $[N_G(\langle x\rangle) : C_G(\langle x\rangle)]|2$, we deduce that $\mathrm{G}_3 \leqslant C_G(\langle x\rangle)$. Applying the third Sylow's theorem implies that $n_3(G) \in \{1, 4, 16\}$. In the following, we examine two possibilities for v:

(i). If $v = 1$, then $|G|_3 = 3$. Therefore, Corollary 2.16(ii) forces $m_6(G) = n_3(G) \cdot 2t$, where $t = m_2(C_G(\mathrm{G}_3))$. Thus $m_6(G) \in \{2t, 8t, 32t\}$. If $m_6(G) = 2t$, then $t = 10$, which is a contradiction with Corollary 2.16(i). If $m_6(G) \in \{8t, 32t\}$, then we get a contradiction with $M(G) = 20$.

(ii). If $v = 2$, then $|\mathrm{G}_3| = 9$. So, G_3 is a 3-elementary abelian group. Set $C := C_G(\langle x\rangle)$. If C is abelian, then we can see that $C = C_3 \times C_3 \times C_2 \times C_2$ and hence, $m_6(C) = 8 \cdot 3 = 24$, which is a contradiction with $(*)$. Thus C is not abelian and hence, $C \cong C_6 \times \mathbb{S}_3$, where $\mathbb{S}_3$ denotes the symmetric group of degree 3. Therefore, $m_6(C) = m_6(C_6) \cdot |\mathbb{S}_3| + m_3(C_6) \cdot m_2(\mathbb{S}_3) + m_2(C_6) \cdot m_3(\mathbb{S}_3) = 20$ and hence, C is normal in G. This forces $\langle x\rangle = Z(C)$ to be normal in G. Thus $[G : N_G(\langle x\rangle)] = 1$ and hence, (1) guarantees $|G||72$. If $|G| = 72$, then $\pi_e(G) \subseteq \{1, 2, 3, 4, 6\}$. Thus by Lemma 2.13, $9|m_2 + m_4 + m_6 = m_2 + m_4 + 20$ and $8|m_3 + m_6 = m_3 + 20$. So, there exist the natural numbers s, t such that $s, t \geqslant 3$, $m_2 + m_4 + 20 = 9t$ and $m_3 + 20 = 8s$. Therefore, $1 + m_2 + m_3 + m_4 + m_6 = 72$ forces $8s + 9t = 91$. Thus considering the different values of s and t shows that $s = 8$ and $t = 3$. So, $m_3 = 64 - 20 = 44$. But $n_3(G) = 3u + 1|8$ and hence $n_3(G) \leq 4$. This shows that $44 = m_3(G) \leqslant n_3(G).(|\mathrm{G}_3| - 1) \leqslant 4 \cdot 8 = 32$, which is a contradiction. Thus $|G| = 36$ and hence, $G = C \cong C_6 \times \mathbb{S}_3$.

(3). If $k = 10$, then Lemma 2.7 shows that $|G||2^{\alpha_1} \cdot 5^{\alpha_2}$, where for $i \in \{1, 2\}$, $\alpha_i > 0$. Let $x \in G$ such that $o(x) = 10$. Then $|C_G(\langle x\rangle)| = 2^u \cdot 5^v$. According to $(*)$, we can see that $u \leqslant 2$ and $v = 1$. Since $[G : N_G(\langle x\rangle)]||G|$, Lemma 2.8 shows that $[G : N_G(\langle x\rangle)] \in \{1, 2, 4, 5\}$. Note that if $[G : N_G(\langle x\rangle)] \in \{4, 5\}$, then there exists $y \in G$ such that $[G : N_G(\langle y\rangle)] \in \{1, 2\}$. So, without loss of generality, we can assume that $[G : N_G(\langle x\rangle)]|2$ and hence, (1) shows that $|G||2^5 \cdot 5^2$. Since $[N_G(\langle x\rangle) : C_G(\langle x\rangle)]|2$, we deduce that $\mathrm{G}_5 \leqslant C_G(\langle x\rangle)$. If $\mathrm{G}_5 \ntrianglelefteq G$, then $|G : N_G(\mathrm{G}_5)| \geqslant 6$. Thus Corollary 2.16$(ii)$ shows that $m_{10}(G) = n_5(G) \cdot \phi(10) \cdot t \geqslant 6 \cdot 4 \cdot t = 24t$, where $t = m_2(C_G(\mathrm{G}_5))$. Obviously, this is a contradiction with $(*)$. If $\mathrm{G}_5 \trianglelefteq G$, then Corollary 2.16$(ii)$ shows that $m_{10}(G) = 4t = 20$, where $t = m_2(C_G(\mathrm{G}_5)) = 5$. Since $C_G(\mathrm{G}_5) = \mathrm{G}_5 \times \mathrm{G}_2(C_G(\mathrm{G}_5))$, we deduce that $|\mathrm{G}_2(C_G(\mathrm{G}_5))| - 1 = t = 5$, which is impossible.

(4). If $k = 12$, then by applying the argument in Case (2), Subcase (i) of the proof of Theorem 2.21, we get a contradiction.

(5). If $k = 22$, then the main theorem leads us to get a contradiction and if $k=44$, then the main theorem shows that $G \cong C_{44} \rtimes (C_u \times C_l)$, where $u|10$ and $l|2$.

(6). If $k \in \{25, 50\}$, then the main theorem completes the proof. □

References

[1] **A.A. Buturlakin**, *Spectra of finite linear and unitary groups*, Algebra and Logic **47(2)** (2008), 91 – 99.

[2] **G.Y. Chen and W. Shi**, *Finite groups with* 30 *elements of maximal order*, Appl. Categorical Structures **16(1)** (2008), 239 – 247.

[3] **Y. Cheng**, *Finite groups based on the numbers of elements of maximal order*, (Chinese), Chin. Ann. Math. **14** (1993), 561 – 567.

[4] **X.L. Du and Y.Y. Jiang**, *On finite groups with exact* 4p *elements of maximal order are solvable*, (Chinese), Chin. Ann. Math., **25A(5)** (2004), 607 – 612..

[5] **G. Frobenius**, *Verallgemeinerung des sylowschen satze*, Berliner sitz (1895), 981 – 993.

[6] **The GAP group**, *GAP- Groups, Algorithms, and Programming*, Version 4.3, Aachen, Andrews, 2002, (http://www.gap-system.org).

[7] **D. Gorenstein**, *Finite groups*, New York, 1968.

[8] **M. Herzog**, *On fnite simple groups of order divisible by three primes only*, J. Algebra **10** (1968), 383 – 388.

[9] **Y. Jiang**, *A theorem of finite groups with* 18p *elements having maximal order*, Algebra Coll., **15** (2008), 317 – 329.

[10] **Q. Jiang and C. Shao**, *Finite groups with* 24 *elements of maximal order*, Frontiers Math. in China **5** (2010), 665 – 678.

[11] **G.A. Miller**, *Addition to a theorem due to Frobenius*, Bull. Amer. Math. Soc. **11** (1904), 6 – 7.

[12] **H. Xu, G. Chen and Y. Yan**, *A new characterization of simple K_3-groups by their orders and large degrees of their irreducible character*, Commun. Algebra **42** (2014), 5374 – 5380.

[13] **L. Zhang and X. Liu**, *Characterization of the projective general linear groups $PGL_2(q)$ by their orders and patterns*, Intern. J. Algebra Computation **19** (2009), 873 – 889.

Received December 1, 2015

Department of Pure Mathematics, Faculty of Mathematical Sciences, Shahrekord University,
P.O. Box 115, Shahrekord, Iran
E-mails: asadian.bahare@stu.sku.ac.ir, ahanjideh.neda@sci.sku.ac.ir

Quasigroups and Related Systems **24** (2016), 169 − 177

Some results on multigroups

Johnson Aderemi Awolola and Adeku Musa Ibrahim

Abstract. The theory of multisets is an extension of the set theory. In this paper, we have studied some new results on multigroups following [11].

1. Introduction

A mathematical structure known as multiset (mset, for short) is obtained if the restriction of distinctness on the nature of the objects forming a set is relaxed. Unlike classical set theory which assumes that mathematical objects occur without repetition. However, the situation in science and in ordinary life is not like that. It is observed that there is enormous repetition in the physical world. For example, consideration of repeated roots of polynomial equation, repeated observations in statistical sample, repeated hydrogen atoms in a water molecule H_2O, etc., do play a significant role. The challenging task of formulating sufficiently rich mathematics of multiset started receiving serious attention from beginning of the 1970s. An updated exposition on both historical and mathematical perspective of the development of theory of multisets can be found in [3, 4, 5, 8, 9, 10, 13, 14, 15].

The theory of groups is an important algebraic structure in modern mathematics. Several authors have studied the algebraic structure of set theories dealing with uncertainties such as the concept of group in fuzzy sets [12], soft sets [1], smooth sets [6], rough sets [2] etc.

2. Preliminaries

In this section, we present fundamental definitions of multisets that will be used in the subsequent sections of this paper.

Definition 2.1. Let X be a set. A *multiset* (mset) A drawn from X is represented by a count function C_A defined as $C_A : X \to \mathcal{D} = \{0, 1, 2, \ldots\}$. For each $x \in X$, $C_A(x)$ denotes the number of occurrences of the element x in the mset A. The representation of the mset A drawn from $X = \{x_1, x_2, \ldots, x_n\}$ will be as $A = [x_1, x_2, \ldots, x_n]_{m_1, m_2, \ldots, m_n}$ such that x_i appears m_i times, $i = 1, 2, \ldots, n$ in the mset A.

2010 Mathematics Subject Classification: 20E10, 94D05
Keywords: Multiset, multigroup, multigroup homomorphism.

Definition 2.2. A domain X is defined as a set of elements from which msets are constructed. For any positive integer n, the mset space $[X]^n$ is the set of all msets whose elements are in X such that no element in the mset occurs more than n times. The set $[X]^\infty$ is the set of all msets over a domain X such that there is no limit on the number of times an element in an mset occurs.

Definition 2.3. Let $A_1, A_2, A_i \in [X]^n$, $i \in I$. Then

(i) $A_1 \subseteq A_2 \Leftrightarrow C_{A_1}(x) \leqslant C_{A_2}(x)$, $\forall\ x \in X$.

(ii) $A_1 = A_2 \Leftrightarrow C_{A_1}(x) = C_{A_2}(x)$, $\forall\ x \in X$.

(iii) $\bigcap_{i\in I} A_i = \bigwedge_{i\in I} C_{A_i}(x)$, $\forall\ x \in X$ (where $\bigwedge$ is the minimum operation).

(iv) $\bigcup_{i\in I} A_i = \bigvee_{i\in I} C_{A_i}(x)$, $\forall\ x \in X$ (where $\bigvee$ is the maximum operation).

(v) $A_i^c = n - C_{A_i}(x)$, $\forall x \in X$, $n \in \mathbb{Z}^+$.

Definition 2.4. Let X and Y be two nonempty sets and $f : X \to Y$ be a mapping. Then the *image* $f(A)$ of an mset $A \in [X]^n$ is defined as

$$C_{f(A)}(y) = \begin{cases} \bigvee_{f(x)=y} C_A(x), & f^{-1}(y) \neq \emptyset, \\ 0, & f^{-1}(y) = \emptyset. \end{cases}$$

Definition 2.5. Let X and Y be two nonempty sets and $f : X \to Y$ be a mapping. Then the *inverse image* $f^{-1}(B)$ of an mset $B \in [Y]^n$ is defined as $C_{f^{-1}B}(x) = C_B\left(f(x)\right)$.

3. Multigroup

In this section, we briefly give the definition of multigroup, some remarks and present some existing results given by [11], and $MS(X)$ is denoted as the set all msets over X (which is assumed to be an initial universal set unless it is stated otherwise).

Definition 3.1. 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) $C_A(xy) \geqslant [C_A(x) \wedge C_A(y)]$, $\forall\ x, y \in X$,

(ii) $C_A(x^{-1}) \geqslant C_A(x)$, $\forall\ x \in X$.

We denote the set of all multigroups over X by $MG(X)$.

Example 3.2. Let the subset $X = \{1, -1, i, -i\}$ of complex numbers be a group and $A = [1, -1, i, -i]_{3,2,2,2}$ be a multiset over X. Then, as it is not difficult to verify, A is a multigroup over X.

Definition 3.3. Let $A, B \in MG(X)$, we have the following definitions:

(i) $C_{A\circ B}(x) = \bigvee \{C_A(y) \wedge C_B(z) : y, z \in X, yz = x\}$
$= \max [\min \{C_A(y), C_B(z)\} : y, z \in X, yz = x]$,

(ii) $C_{A^{-1}}(x) = C_A(x^{-1})$.

We call $A \circ B$ the product of A and B, and A^{-1} the inverse of A.

Definition 3.4. (cf. [11]) Let $A \in MG(X)$. Then A is called an *abelian multigroup* over X if $C_A(xy) = C_A(yx)$, $\forall\ x, y \in X$. The set of all abelian multigroups is denoted by $AMG(X)$.

Definition 3.5. (cf. [11]) Let $A, B \in MG(X)$. Then A is said to be a *submultigroup* of B if $A \subseteq B$.

Definition 3.6. (cf. [11]) Let $H \in MG(X)$. For any $x \in X$, xH and Hx defined by $C_{xH}(y) = C_H(x^{-1}y)$ and $C_{Hx}(y) = C_H(yx^{-1})$, $\forall\ y \in X$ are respectively called the *left* and *right mcosets* of H in X.

The following results have been given by [11] as related to this paper except for Remark 3.25 and 3.25.

Proposition 3.7. *Let $A \in MG(X)$. Then*

(i) $C_A(x^n) \geqslant C_A(x),\ \ \forall\ x \in X$,

(ii) $C_A(x^{-1}) = C_A(x),\ \forall\ x \in X$,

(iii) $C_A(e) \geqslant C_A(x),\ \ \forall\ x \in X$.

Proposition 3.8. *Let $A, B, C, A_i \in MG(X)$, then the following hold:*

(i) $C_{A\circ B}(x) = \bigvee_{y\in X} \left[C_A(y) \wedge C_B(y^{-1}x)\right] = \bigvee_{y\in X} \left[C_A\left(xy^{-1}\right) \wedge C_B(y)\right],\ \forall x \in X$,

(ii) $A^{-1} = A$,

(iii) $\left(A^{-1}\right)^{-1} = A$,

(iv) $A \subseteq B \Longrightarrow A^{-1} \subseteq B^{-1}$,

(v) $\left(\bigcup_{i\in I} A_i\right)^{-1} = \bigcup_{i\in I} \left(A^{-1}\right)$,

(vi) $\left(\bigcap_{i\in I} A_i\right)^{-1} = \bigcap_{i\in I} \left(A^{-1}\right)$,

(vii) $(A \circ B)^{-1} = B^{-1} \circ A^{-1}$,

$(viii)$ $(A \circ B) \circ C = A \circ (B \circ C)$.

Proposition 3.9. *Let $A, B \in AMG(X)$. Then $A \circ B = B \circ A$.*

Proposition 3.10. *If $A, B \in MG(X)$, then $C_{A\circ B}(x^{-1}) = C_{A\circ B}(x)$.*

Proposition 3.11. *Let $A \in [X]^n$. Then $A \in MG(X)$ if and only if $A \circ A \leqslant A$ and $A^{-1} = A$.*

Proposition 3.12. *Let $A \in [X]^n$. Then $A \in MG(X)$ if and only if $C_A\left(xy^{-1}\right) \geqslant [C_A(x) \wedge C_A(y)]$, $\forall\ x, y \in X$.*

Proposition 3.13. *Let $A, B \in MG(X)$. Then $A \cap B \in MG(X)$.*

Remark 3.14. If $\{A_i\}_{i\in I}$ is a family of multigroups over X, then their intersection $\bigcap_{i\in I} A_i$ is a multigroup over X.

Remark 3.15. If $\{A_i\}_{i\in I}$ is a family of multigroups over X, then their union $\bigcup_{i\in I} A_i$ need not be a multigroup over X.

Proposition 3.16. *Let $A \in MG(X)$. Then the non-empty sets of the form*

$$A_n = \{x \in X : C_A(x) \geqslant n,\ n \in \mathbb{N}\}$$

are subgroups of X.

Proposition 3.17. *Let $A \in MG(X)$. Then the non-empty sets defined as*

$$A^* = \{x \in X : C_A(x) > 0\} \text{ and } A_* = \{x \in X : C_A(x) = C_A(e)\}$$

are subgroups of X.

Proposition 3.18. *Let $A \in MS(X)$. Then the following assertions are equivalent:*

(*a*) $C_A(xy) = C_A(yx)$, $\forall\ x, y \in X$,

(*b*) $C_A\left(xyx^{-1}\right) = C_A(y)$, $\forall\ x, y \in X$,

(*c*) $C_A\left(xyx^{-1}\right) \geqslant C_A(y)$, $\forall\ x, y \in X$,

(*d*) $C_A\left(xyx^{-1}\right) \leqslant C_A(y)$, $\forall\ x, y \in X$.

Proposition 3.19. *Let $A \in AMG(X)$. Then A_*, A^* and A_n, $n \in \mathbb{N}$ are normal subgroups of X.*

Proposition 3.20. *Let $H \in MG(X)$, then $xH = yH$ if and only if $x^{-1}y \in H_*$.*

Remark 3.21. If $H \in AMG(X)$, then $xH = Hx$, $\forall\ x \in X$.

Proposition 3.22. *Let X and Y be two groups and $f : X \to Y$ be a homomorphism. If $A \in MG(X)$, then $f(A) \in MG(Y)$.*

Remark 3.23. Let X and Y be two groups and $f : X \to Y$ be a homomorphism. If $A_i \in MG(X)$, $i \in I$, then $f\left(\cap_{i\in I} A_i\right) \in MG(Y)$.

Proposition 3.24. *Let X and Y be two groups and $f : X \to Y$ be a homomorphism. If $B \in MG(Y)$, then $f^{-1}(B) \in MG(X)$.*

Remark 3.25. Let X and Y be two groups and $f : X \to Y$ be a homomorphism. If $B_i \in MG(Y)$, $i \in I$, then $f^{-1}\left(\bigcap_{i\in I} B_i\right) \in MG(X)$.

We now present some results to broaden the theoretical aspect of multigroup theory.

Proposition 3.26. *Let $A \in MG(X)$. Then*

(i) $C_A(xy)^{-1} \geqslant C_A(x) \wedge C_A(y)$, $\forall\ x, y \in X$,

(ii) $C_A(xy)^n \geqslant C_A(xy)$, $\forall\ x, y \in X$.

Proof. The proofs are straightforward. □

Proposition 3.27. *Let $A \in MG(X)$. If $C_A(x) < C_A(y)$ for some $x, y \in X$, then $C_A(xy) = C_A(x) = C_A(yx)$.*

Proof. Given that $C_A(x) < C_A(y)$ for some $x, y \in X$. Since $A \in MG(X)$, then $C_A(xy) \geqslant C_A(x) \wedge C_A(y) = C_A(x)$. Now, $C_A(x) = C_A\left(xyy^{-1}\right) \geqslant C_A(xy) \wedge C_A(y) = C_A(xy)$, since $C_A(x) < C_A(y)$, $C_A(xy) < C_A(y)$. Therefore, $C_A(xy) = C_A(x)$. Similarly, $C_A(yx) = C_A(x)$. □

Proposition 3.28. *Let $A \in MG(X)$. Then $C_A(xy^{-1}) = C_A(e)$ implies $C_A(x) = C_A(y)$.*

Proof. Given $A \in MG(X)$ and $C_A(xy^{-1}) = C_A(e)\ \ \forall\ x, y \in X$. Then

$$C_A(x)=C_A(x(y^{-1}y))=C_A((xy^{-1})y)\geqslant C_A(xy^{-1})\wedge C_A(y)=C_A(e)\wedge C_A(y)=C_A(y),$$

i.e., $C_A(x) \geqslant C_A(y)$.

Also, $C_A(y) = C_A(y^{-1}) = C_A(ey^{-1}) = C_A((x^{-1}x)y^{-1}) \geqslant C_A(x^{-1}) \wedge C_A(xy^{-1}) = C_A(x) \wedge C_A(e) = C_A(x)$, i.e., $C_A(y) \geqslant C_A(x)$. Hence, $C_A(x) = C_A(y)$. □

Proposition 3.29. *Let $A, B, C, D \in MG(X)$. If $A \subseteq B$ and $C \subseteq D$, then $A \circ C \subseteq B \circ D$.*

Proof. Since $A \subseteq B$ and $C \subseteq D$, it follows that $C_A(x) \geqslant C_B(x)$, $\forall\ x \in X$ and $C_C(x) \leqslant C_D(x)$, $\forall\ x \in X$. So,

$$\begin{aligned} C_{(A\circ C)}(x) &= \bigvee \{C_A(y) \wedge C_C(z) : y, z \in X, yz = x\} \\ &\leqslant \bigvee \{C_B(y) \wedge C_D(z) : y, z \in X, yz = x\} = C_{(B\circ D)}(x). \end{aligned}$$

Hence, $A \circ C \subseteq B \circ D$. □

Proposition 3.30. *Let $A, B \in MG(X)$ and $A \subseteq B$ or $B \subseteq A$. Then $A \cup B \in MG(X)$.*

Proof. The proof is straightforward. □

Remark 3.31. Let $A \in MG(X)$, then A^c need not be a multigroup over X. Indeed, if $X = (V_4, +) = \{0, a, b, c\}$ is the Klein's 4-group, then for $A = [0, a]_{2,1}$ we have $A^c = [0, a]_{2,3} \neq MG(X)$ because $\exists\ C_A(a) > C_A(0)$.

Proposition 3.32. *If $A \in MG(X)$, then $A^c \in MG(X)$ if and only if $C_A(x) = C_A(e)$, $\forall\ x \in X$.*

Proposition 3.33. *Let $A \in MG(X)$ and $x \in X$. Then $C_A(xy) = C_A(y)\ \forall\ y \in X$ if and only if $C_A(x) = C_A(e)$.*

Proof. Let $C_A(xy) = C_A(y)$, $\forall y \in X$. Then $C_A(x) = C_A(xe) = C_A(e)$.

Conversely, let $C_A(x) = C_A(e)$. Since $C_A(e) \geqslant C_A(y)\ \forall y \in X$, we have $C_A(x) \geqslant C_A(y)$. Thus, $C_A(xy) \geqslant C_A(x) \wedge C_A(y) = C_A(e) \wedge C_A(y) = C_A(y)$, i.e., $C_A(xy) \geqslant C_A(y)$, $\forall y \in X$.

But $C_A(y) = C_A(x^{-1}xy) \geqslant C_A(x) \wedge C_A(xy)$ and $C_A(x) \geqslant C_A(xy)$, $\forall y \in X$, imply $C_A(x) \wedge C_A(xy) = C_A(xy) \leqslant C_A(y)$, $\forall y \in X$. So, $C_A(y) \geqslant C_A(xy)$, $\forall y \in X$. Hence, $C_A(xy) = C_A(y)\ \ \forall y \in X$. □

Proposition 3.34. *If $A \in MG(X)$ and $H \leqslant X$, then $A|_H \in MG(H)$.*

Proof. Let $x, y \in H$. Then $xy^{-1} \in H$. Since $A \in MG(X)$, then $C_A(xy^{-1}) \geqslant C_A(x) \wedge C_A(y)\ \ \forall x, y \in X$. Moreover,$C_{A|_H}(xy^{-1}) \geqslant C_{A|H}(x) \wedge C_{A|H}(y)\ \ \forall x, y \in X$. Hence, $A|_H \in MG(H)$. □

4. Multigroup homomorphism

Proposition 4.1. *Let $f : X \longrightarrow Y$ be an epimorphism and $B \in MS(Y)$. If $f^{-1}(B) \in MG(X)$, then $B \in MG(Y)$.*

Proof. Let $x, y \in Y$ then $\exists\ a, b \in X$ such that $f(a) = x$ and $f(b) = y$. It follows that

$$\begin{aligned} C_B(xy) = C_B(f(a)f(b)) = C_B(f(ab)) = C_{f^{-1}(B)}(ab) &\geqslant C_{f^{-1}(B)}(a) \wedge C_{f^{-1}(B)}(b) \\ &= C_B(f(a)) \wedge C_B(f(b)) = C_B(x) \wedge C_B(y). \end{aligned}$$

Again,

$$\begin{aligned} C_B(x^{-1}) &= C_B(f(a)^{-1}) = C_B(f(a^{-1})) = C_{(f^{-1}(B))}(a^{-1}) = C_{f^{-1}(B)}(a) \\ &= C_B(f(a)) = C_B(x). \end{aligned}$$

Therefore, $B \in MG(Y)$. □

Proposition 4.2. *Let X be a group and $f : X \longrightarrow X$ is an automorphism. If $A \in MG(X)$, then $f(A) = A$ if and only if $f^{-1}(A) = A$.*

Proof. Let $x \in X$. Then $f(x) = x$. Now, $C_{(f^{-1}(A))}(x) = C_A(f(x)) = C_A(x)$ implies $f^{-1}(A) = A$.

Conversely, let $f^{-1}(A) = A$. Since f is an automorphism, then

$$\begin{aligned} C_{f(A)}(x) &= \bigvee \{C_A(x') : x' \in X,\ f(x') = f(x) = x\} \\ &= C_A(f(x)) = C_{(f^{-1}(A))}(x) = C_A(x). \end{aligned}$$

Hence, the proof. □

Proposition 4.3. *Let $f : X \to Y$ be a homomorphism of groups, $A \in MG(X)$ and $B \in MG(Y)$. If A is a constant on $Kerf$, then $f^{-1}(f(A)) = A$.*

Proof. Let $f(x) = y$. Then

$$C_{f^{-1}(f(A))}(x) = C_{f(A)}f(x) = C_{f(A)}(y) = \bigvee\{C_A(x) : x \in X,\ f(x) = y\}.$$

Since $f(x^{-1}z) = f(x^{-1})f(z) = (f(x))^{-1}f(z) = y^{-1}y = e'$, $\forall z \in X$ such that $f(z) = y$, which implies $x^{-1}z \in Kerf$. Also, since A is constant on $Kerf$, then $C_A(x^{-1}z) = C_A(e)$. Therefore, $C_A(x) = C_A(z)\ \ \forall\ z \in X$ such that $f(z) = y$ by Proposition 3.28 . Hence, the proof. □

Proposition 4.4. *Let $H \in AMG(X)$. Then the map $f : X \to X/H$ defined by $f(x) = xH$ is a homomorphism $Kerf = \{x \in X : C_H(x) = C_H(e)\}$, where e is the identity of X.*

Proof. Let $x, y \in X$. Then $f(xy) = (xy)H = xHyH = f(x)f(y)$. Hence, f is a homomorphism. Further,

$$\begin{aligned} Kerf &= \{x \in X : f(x) = eH\} = \{x \in X : xH = eH\} \\ &= \big\{x \in X : C_H(x^{-1}y) = C_H(y)\ \forall y \in X\big\} \\ &= \big\{x \in X : C_H(x^{-1}) = C_H(e)\big\} = \{x \in X : C_H(x) = C_H(e)\} = H_*, \end{aligned}$$

which completes the proof. □

Remark 4.5. By Propositions 4.4 and 3.19, $Ker\, f$ is a normal subgroup of X.

Proposition 4.6. (First Isomorphism Theorem) *Let $f : X \to Y$ be an epimorphism of groups and $H \in AMG(X)$, then $X/H_* \cong Y$, where $H_* = Kerf$.*

Proof. Define $\Theta : X/H_* \to Y$ by $\theta(xH_*) = f(x)\ \ \forall x \in X$. Let $xH = yH$ such that $C_H(x^{-1}y) = C_H(e)$. Since $x^{-1}y \in H_*$, then $f(x^{-1}y) = f(e) \Longrightarrow f(x) = f(y)$. Hence, Θ is well-defined. Obviously it is an epimorphism. Moreover, $f(x) = f(y)$ implies $f(x)^{-1}f(y) = f(e)$. So, $f(x^{-1})f(y) = f(x^{-1}y) = f(e)$, i.e., $x^{-1}y \in H_*$ and consequantly, $C_H(x^{-1}y) = C_H(e)$. Thus, $xH = yH$, which shows Θ is an isomorphism. □

Proposition 4.7. (Second Isomorphism Theorem) *If $H, N \in AMG(X)$ such that $C_H(e) = C_N(e)$, then $H_*N_*/N \cong H_*/H \cap N$.*

Proof. Clearly, for any $x \in H_*N_*$, $x = hn$ where $h \in H_*$ and $n \in N_*$. Define $\varphi : H_*N_*/N \to H_*/H \cap N$ by $\varphi(xN) = h(H \cap N)$.

If $xN = yN$, where $y = h_1n_1$, $h_1 \in H_*$ and $n_1 \in N_*$, then

$$C_N(x^{-1}y) = C_N((hn)^{-1}h_1n_1) = C_N(n^{-1}h^{-1}h_1n_1) = C_N(h^{-1}h_1n^{-1}n_1) = C_N(e).$$

Hence, $C_N(h^{-1}h_1) = C_N(n^{-1}n_1) = C_N(e)$. Thus,

$$C_{H\cap N}(h^{-1}h_1) = C_H(h^{-1}h_1) \wedge C_N(h^{-1}h_1) = C_H(e) \wedge C_N(e) = C_{H\cap N}(e),$$

i.e., $h(H \cap N) = h_1(H \cap N)$. Hence, φ is well-defined.

If $xN, yN \in H_*N_*\ N$, then $xy = hnh_1n_1$. Since $H \in AMG(X)$, then $C_H(nh_1n_1) = C_H(h_1)$ gives $nh_1n_1 \in H_*$. Hence,

$\varphi(xNyN) = \varphi(xyN) = h(nh_1n1)(H \cap N) = h(H \cap N)nh_1n_1(H \cap N)$ and

$$\begin{aligned} C_{H\cap N}(h_1^{-1}(nh_1n_1)) &\geqslant C_H(h_1^{-1}nh_1n_1) \wedge C_N(h_1^{-1}nh_1n_1) \\ &= C_H(h_1^{-1}(nh_1n_1)) \wedge C_N(n(h_1^{-1}h_1n_1)) \\ &= C_H(e) \wedge C_N(e) \\ &= C_{H\cap N}(e). \end{aligned}$$

Hence, $nh_1n_1(H \cap N) = h_1(H \cap N)$, i.e., $\varphi(xNyN) = h(H \cap N)h_1(H \cap N) = \varphi(xN)\varphi(yN)$, which shows that φ is a homomorphism.

φ is also an epimorphism, since for $h(H \cap N) \in H_*/H \cap N$ and $n \in N_*$, we have $x = hn \in H_*N_*$ and $\varphi(xN) = h(H \cap N)$.

Moreover, if $x, y \in H_*N_*$, where $x = hn$ and $y = h_1n_1$, $h, h_1 \in H_*$ and $n, n_1 \in N_*$ and $h(H \cap N) = h_1(H \cap N)$, then $C_{H\cap N}(h^{-1}h_1) = C_{H\cap N}(e)$, i.e., $C_H(h^{-1}h_1) \wedge C_N(h^{-1}h_1) = C_H(e) \wedge C_N(e)$. But $C_H(e) = C_N(e)$ and $C_H(h^{-1}h_1) = C_H(e)$, so $C_N(h^{-1}h_1) = C_N(e)$. Therefore,

$$\begin{aligned} C_N(x^{-1}y) &= C_N((hn)^{-1}h_1n_1) \\ &= C_N(n^{-1}h^{-1}h_1n_1) = C_N(h^{-1}h_1n^{-1}n_1) \\ &\geqslant C_N(h^{-1}h_1) \wedge C_N(n^{-1}n_1) = C_N(e) \wedge C_N(e) = C_N(e). \end{aligned}$$

Thus, $C_N(x^{-1}y) = C_N(e)$, and consequently, $xN = yN$.

Hence, $H_*N_*/N \cong H_*/H \cap N$. □

Proposition 4.8. (Third Isomorphism Theorem) *Let $H, N \in AMG(X)$ with $H \subseteq N$ and $C_H(e) = C_N(e)$. Then $X/N \cong (X/H)/(N_*/H)$.*

Proof. Define $f : X/H \to X/N$ by $f(xH) = xN\ \ \forall x \in X$ such that $C_H(x^{-1}y) = C_H(e) = C_N(e)\ \ \forall xH = yH$. Because $H \subseteq N$, we have $C_N(x^{-1}y) \geqslant C_H(x^{-1}y) = C_N(e)$ and so $C_N(x^{-1}y) = C_N(e)$, i.e., $xN = yN$, which means that f is well-defined. Obviously f is an epimorphism.

Moreover,

$$\begin{aligned} Kerf &= \{xH \in X/H : f(xH) = eN\} \\ &= \{xH \in X/Hx : N = eN\} \\ &= \{xH \in X/H : C_N(x) = C_N(e)\} \\ &= \{xH \in X/H : x \in N_*\} = N_*/H. \end{aligned}$$

Thus, $Kerf = N_*/H$ and $X/N \cong (X/H)/(N_*/H)$. □

References

[1] **H. Aktas and N. Cagman**, *Soft sets and soft groups*, Inform. Sci. **177** (2007), 2726 – 2735.

[2] **R. Biswas and S. Nanda**, *Rough groups and rough subgroups*, Bull. Polish Acad. Sci. Math. **42** (1994), 251 – 254.

[3] **W. Blizard**, *The development of multiset theory*, Modern Logic **1** (1991), 319 – 352.

[4] **K. Chakraborty**, *On bags and fuzzy bags*, Adv. Soft Comput. Techn. Appl. **25** (2000), 201 – 2012.

[5] **C.S. Claude, G. Paũn, G. Rozenberg and A. Salomaa (eds.)**, *Multiset processing mathematics,computer science and molecular computing points of view*, Lecture Notes Comput. Sci. **2235** (2001).

[6] **M. Demirci**, *Smooth groups*, Fuzzy Sets Systems **117** (2001), 431 – 437.

[7] **M. Dresher and O. Ore**, *Theory of multigroups*, American J. Math. **60** (1938), 705 – 733.

[8] **J.L. Hickman**, *A note on the concept of multiset*, Bull. Australian Math. Soc. **22** (1980), 211 – 217.

[9] **D.E. Knuth**, *The art of computer programming*, vol. 2, Adison-Wesley, 1981.

[10] **J. Lake**, *Sets, fuzzy sets, multisets and functions*, J. London Math. Soc. **12** (1976), 323 – 326.

[11] **S.K. Nazmul, P. Majumdar and S. K. Samanta**, *On multisets and multigroups*, Annals Fuzzy Math. Inform. **6** (2013), 643 – 656.

[12] **A. Rosenfeld**, *Fuzzy groups*, J. Math. Anal. Appl. **35** (1971), 512 – 517.

[13] **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.

[14] **D. Singh, A.M. Ibrahim, T. Yohanna and J.N. Singh**, *A systematization of fundamentals of multisets*, Lecturas Matematicas **29** (2008), 33 – 48.

[15] **R.R. Yager**, *On the theory of bags*, Int. J. General Systems **13** (1986), 23 – 27.

Received April 16, 2016

Department of Mathematics/Statistics/Computer Science, University of Agriculture, Makurdi, Nigeria
E-mail: remsonjay@yahoo.com

and

Department of Mathematics, Ahmadu Bello University, Zaria, Nigeria
E-mail: amibrahim@abu.edu.ng

Quasigroups and Related Systems **24** (2016), 179 – 185

On quasi n-absorbing elements of multiplicative lattices

Ece Yetkin Celikel

Abstract. A proper element q of a lattice L is said to be a quasi n-absorbing element if whenever $a^n b \leqslant q$ implies that either $a^n \leqslant q$ or $a^{n-1}b \leqslant q$. We investigate properties of this new type of elements and obtain some relations among prime, 2-absorbing, n-absorbing elements in multiplicative lattices.

1. Introduction

In this paper we define and study quasi n-absorbing elements in multiplicative lattices. A *multiplicative lattice* is a complete lattice L with the least element 0 and compact greatest element 1, on which there is defined a commutative, associative, completely join distributive product for which 1 is a multiplicative identity. Notice that $L(R)$ the set of all ideals of a commutative ring R is a special example for multiplicative lattices which is principally generated, compactly generated and modular. However, there are several examples of non-modular multiplicative lattices (see [1]). Weakly prime ideals [3] were generalized to multiplicative lattices by introducing weakly prime elements [7]. While 2-absorbing, weakly 2-absorbing and n-absorbing ideals in commutative rings were introduced in [5], [6], and [4], 2-absorbing and weakly 2-absorbing elements in multiplicative lattices were studied in [10].

We begin by recalling some background material which will be needed. An element a of L is said to be *compact* if whenever $a \leqslant \bigvee_{\alpha \in I} a_\alpha$ implies $a \leqslant \bigvee_{\alpha \in I_0} a_\alpha$ for some finite subset I_0 of I. By a *C-lattice* we mean a (not necessarily modular) multiplicative lattice which is generated under joins by a multiplicatively closed subset C of compact elements of L. We note that in a C-lattice, a finite product of compact elements is again compact. Throughout this paper L and L_* denotes a multiplicative lattice and the set of compact elements of the lattice L, respectively. An element a of L is said to be *proper* if $a < 1$. A proper element p of L is said to be *prime* (resp. *weakly prime*) if $ab \leqslant p$ (resp. $0 \neq ab \leqslant p$) implies either $a \leqslant p$ or $b \leqslant p$. If 0 is prime, then L is said to be a *domain*. A proper element m of L is said to be *maximal* if $m < x \leqslant 1$ implies $x = 1$. The *Jacobson radical* of a lattice L is

2010 Mathematics Subject Classification: 13A15

Keywords: 2-absorbing element, n-absorbing element, multiplicative lattice, quasi n-absorbing element.

defined as $J(L) = \bigwedge\{m \mid m$ is a maximal element of $L\}$. L is said to be *quasi-local* if it contains a unique maximal element. If $L = \{0, 1\}$, then L is called a field. For $a \in L$, we define a *radical* of a as $\sqrt{a} = \bigwedge\{p \in L \mid p$ is prime and $a \leqslant p\}$. Note that in a C-lattice L,

$$\sqrt{a} = \bigwedge\{p \in L \mid p \text{ is prime and } a \leqslant p\} = \bigvee\{x \in L_* \mid x^n \leqslant a \text{ for some } n \in Z^+\}$$

by (Theorem 3.6 of [12]). Elements of the set $Nil(L) = \sqrt{0}$ are called *nilpotent.* For any prime element $p \in L$ by L_p we denote the localization $F = \{x \in C \mid x \nleqslant p\}$. For details on C-lattices and their localizations see [9] and [11]. An element $e \in L$ is said to be *principal* [8], if it satisfies the identities (i) $a \wedge be = ((a : e) \wedge b)e$ and (ii) $(ae \vee b) : e = (b : e) \vee a$. Elements satisfying the identity (i) are called *meet principal*, elements satisfying (ii) are called *join principal.* Note that any finite product of meet (join) principal elements of L is again meet (join) principal [8, Lemma 3.3 and Lemma 3.4]. If every element of L is principal, then L is called a *principal element lattice* [2].

Recall from [10] that a proper element q of L is called 2-*absorbing* (resp. *weakly* 2-*absorbing*) if whenever $a, b, c \in L$ with $abc \leqslant q$ (resp. $0 \neq abc \leqslant q$), then either $ab \leqslant q$ or $ac \leqslant q$ or $bc \leqslant q$. We say that (a, b, c) is a *triple zero element* of q if $abc = 0$, $ab \nleqslant q$, $ac \nleqslant q$ and $bc \nleqslant q$. Observe that if q is a weakly 2-absorbing element which is not a 2-absorbing, then there exist a triple zero of q. A proper element $q \in L$ is n-*absorbing* (resp. *weakly* n-*absorbing*) if $a_1a_2 \cdots a_{n+1} \leqslant q$ (resp. $0 \neq a_1a_2 \cdots a_{n+1} \leqslant q$) for some $a_1a_2 \cdots a_{n+1} \in L_*$ then $a_1a_2 \cdots a_{k-1}a_{k+1} \cdots a_{n+1} \leqslant q$ for some $k = 1, \ldots, n + 1$.

2. Quasi n-absorbing elements

Let L be a multiplicative lattice and n be a positive integer.

Definition 2.1. A proper element q of L is called:
- *quasi* n-*absorbing* if $a^n b \leqslant q$ for some $a, b \in L_*$ implies $a^n \leqslant q$ or $a^{n-1}b \leqslant q$,
- *weakly quasi* n-*absorbing* if $0 \neq a^n b \leqslant q$ for some $a, b \in L_*$ implies $a^n \leqslant q$ or $a^{n-1}b \leqslant q$.

Theorem 2.2. *Let q be a proper element of L and $n \geqslant 1$. Then:*

(1) *q is a prime element if and only if it is quasi* 1*-absorbing,*

(2) *q is a weakly prime element if and only if it is weakly quasi* 1*-absorbing,*

(3) *if q is n-absorbing, then it is quasi n-absorbing,*

(4) *if q is quasi n-absorbing, then it is weakly quasi n-absorbing,*

(5) *if q is quasi n-absorbing, then it is quasi m-absorbing for all $m \geqslant n$,*

(6) *if q is weakly quasi n-absorbing, then it is weakly quasi m-absorbing for all $m \geqslant n$.*

Proof. (1), (2), (3) and (4) are obvious. To prove (5) suppose that q is a quasi n-absorbing element of L, and $a, b \in L_*$ with $a^m b \leqslant q$ for some $m \geqslant n$. Hence

$a^n(a^{m-n}b) \leqslant q$. Since q is a quasi n-absorbing element, we have either $a^n \leqslant q$ or $a^{n-1}(a^{m-n}b) \leqslant q$. So, either $a^m \leqslant q$ or $a^{m-1}b \leqslant q$. This shows that q is a quasi m-absorbing element of L.

(6) can be proved analogously. □

Corollary 2.3. *Let q be a proper element of L.*

(1) *If q is prime, then it is quasi n-absorbing for all $n \geqslant 1$.*

(2) *If q is weakly prime, then it is weakly quasi n-absorbing all $n \geqslant 1$.*

(3) *If q is 2-absorbing, then it is a quasi n-absorbing for all $n \geqslant 2$.*

(4) *If q is weakly 2-absorbing, then it is weakly quasi n-absorbing for all $n \geqslant 2$.*

The converses of these relations are not true in general.

Example 2.4. Consider the lattice of ideals of the ring of integers $L = L(\mathbb{Z})$. Note that the element $30\mathbb{Z}$ of L is a quasi 2-absorbing element, and so quasi n-absorbing element for all $n \geqslant 2$ by Corollary 2.3, but it is not a 2-absorbing element of L by Theorem 2.6 in [7].

Proposition 2.5. *For a proper element q of L the following statements are equivalent.*

(1) *q is a quasi n-absorbing element of L.*

(2) *$(q : a^n) = (q : a^{n-1})$ where $a \in L_*$, $a^n \nleqslant q$.*

In paticular, 0 is a quasi n-absorbing element of L if and only if for each $a \in L_*$ we have $a^n = 0$ or $ann(a^n) = ann(a^{n-1})$.

Proof. It follows directly from Definition 2.1. □

Notice that if q is a weakly quasi n-absorbing element which is not quasi n-absorbing, then there are some elements $a, b \in L_*$ such that $a^n b = 0$, $a^n \nleqslant q$ and $a^{n-1}b \nleqslant q$. We call the pair of elements (a, b) with this property – a *quasi n-zero element* of q. Notice that a zero divisor element of L is a quasi 1-zero element of 0_L, and (a, a, b) is a triple zero element of q if and only if (a, b) is a quasi 2-zero element of q.

Theorem 2.6. *Let q be a weakly quasi n-absorbing element of L. If (a, b) is a quasi n-zero element of q for some $a, b \in L_*$, then $a^n \in ann(q)$ and $b^n \in ann(q)$.*

Proof. Suppose that $a^n \notin ann(q)$. Hence $a^n q_1 \neq 0$ for some $q_1 \in L_*$ where $q_1 \leqslant q$. It follows $0 \neq a^n(b \vee q_1) \leqslant q$. Since $a^n \nleqslant q$, and q is weakly quasi n-absorbing, we conclude that $a^{n-1}(b \vee q_1) \leqslant q$. So $a^{n-1}b \leqslant q$, a contradiction. Thus $a^n q = 0$, and so $a^n \in ann(q)$. Similarly we conclude that $b^n \in ann(q)$. □

Theorem 2.7. *If $\{p_\lambda\}_{\lambda\in\Lambda}$ is a family of (weakly) prime elements of L, then $\bigwedge\limits_{\lambda\in\Lambda} p_\lambda$ is a (weakly) quasi m-absorbing element for all $m \geqslant 2$.*

Proof. Let $\{p_\lambda\}_{\lambda\in\Lambda}$ be a family of prime elements of L. By Corollary 2.3 (3) it is sufficient to prove that $\bigwedge\limits_{\lambda\in\Lambda} p_\lambda$ is a quasi 2-absorbing element of L.

Let $a, b \in L_*$ with $a^2b \leqslant \bigwedge\limits_{\lambda\in\Lambda} p_\lambda$. Since $a^2b \leqslant p_i$ for all prime elements p_i, we have $a \leqslant p_i$ or $b \leqslant p_i$. Thus $ab \leqslant p_i$ for all $i = 1, \dots, n$ and so $ab \leqslant \bigwedge\limits_{\lambda\in\Lambda} p_\lambda$, which completes the proof for prime elements.

For weakly prime elements the proof is similar. □

Corollary 2.8. *Let q be a proper element of L. Then $\sqrt{q}$, $Nil(L)$ and $J(L)$ are quasi n-absorbing elements of L for all $n \geqslant 2$.*

Proof. It is clear from Theorem 2.7. □

Theorem 2.9. *If $\{q_\lambda\}_{\lambda\in\Lambda}$ is a family of (weakly) quasi m-absorbing elements of a totally ordered lattice L, then for each positive integer m $\bigwedge\limits_{\lambda\in\Lambda} q_\lambda$ is a (weakly) quasi m-absorbing element of L.*

Proof. Assume that $\{q_\lambda\}_{\lambda\in\Lambda}$ is an ascending chain of quasi m-absorbing elements and $a^m \nleqslant \bigwedge\limits_{\lambda\in\Lambda} q_\lambda$ and $a^{m-1}b \nleqslant \bigwedge\limits_{\lambda\in\Lambda} q_\lambda$. We show that $a^mb \nleqslant \bigwedge\limits_{\lambda\in\Lambda} q_\lambda$. Hence $a^m \nleqslant q_j$ and $a^{m-1}b \nleqslant q_k$ for some $j, k = 1, \dots, n$.

Put $t = \min\{j, k\}$. Then $a^m \nleq q_t$ and $a^{m-1}b \nleq q_t$. Since q_t is a quasi m-absorbing element, it follows $a^mb \nleq q_t$. Thus $a^mb \nleqslant \bigwedge\limits_{\lambda\in\Lambda} q_\lambda$, we are done.

For weakly prime elements the proof is similar. □

Theorem 2.10. *Let for all $i = 1, 2, \dots, n$, elements $q_1, \dots, q_n \in L$ are (weakly) quasi m_i-absorbing, respectively. Then $\bigwedge\limits_{i=1}^{n} q_i$ is a (weakly) quasi m-absorbing element of L for $m = \max\{m_1, \dots, m_n\} + 1$.*

Proof. Suppose that $q_1, \dots, q_n$ are quasi m_i-absorbing, respectively. Let $a, b \in L_*$ be such that $a^mb \leqslant \bigwedge\limits_{i=1}^{n} q_i$. Hence $a^{m_i} \leqslant q_i$ or $a^{m_i-1}b \leqslant q_i$ for all $i = 1, .., n$. Now assume that $a^m \nleqslant \bigwedge\limits_{i=1}^{n} q_i$. Without loss generality we can suppose that $a^{m_i} \leqslant q_i$ for all $1 \leqslant i \leqslant j$, and $a^{m_i} \nleqslant q_i$ for all $j + 1 \leqslant i \leqslant n$. Hence we have $a^{m_i-1}b \leqslant q_i$ for all $j + 1 \leqslant i \leqslant n$. Then we get clearly $a^{m-1}b \leqslant q_i$ for $m = \max\{m_1, \dots, m_n\} + 1$ and for all $1 \leqslant i \leqslant n$. Thus $a^{m-1}b \leqslant \bigwedge\limits_{i=1}^{n} q_i$, so we are done.

For weakly prime elements the proof is similar. □

If $x \in L$, the interval $[x, 1]$ is denoted be L/x. The elemets of $\overline{a}$ and L/x is again a multiplicative lattice with $\overline{a} \circ \overline{b} = ab \vee x$ for all $\overline{a}, \overline{b} \in L/x$.

Theorem 2.11. *Let x and q be proper elements of L with $x \leqslant q$. If q is a (weakly) quasi n-absorbing element of L, then $\overline{q}$ is a (weakly) quasi n-absorbing element of L/x.*

Proof. Suppose that $\overline{a} = a \vee x$, $\overline{b} = b \vee x \in L$ with $\overline{a}^n\overline{b} \leqslant \overline{q}$, where q is a quasi n-absorbing element of L. Then $a^n b \vee x \leqslant q$, and so $a^n b \leqslant q$. Since q is quasi 2-absorbing, we get either $a^n \leqslant q$ or $a^{n-1}b \leqslant q$. Thus $\overline{a}^n = (a \vee x)^n \leqslant \overline{q}$ or $\overline{a}^{n-1}\overline{b} = (a \vee x)^{n-1}(b \vee x) \leqslant \overline{q}$, as needed.

For weakly prime elements the proof is similar. □

Recall that any C-lattice can be localized at a multiplicatively closed set. Let L be a C-lattice and S a multiplicatively closed subset of L_*. Then for $a \in L$, $a_S = \bigvee\{x \in L_* \,|\, xs \leqslant a \text{ for some } s \in S\}$ and $L_S = \{a_S \,|\, a \in L\}$. L_S is again a multiplicative lattice under the same order as L with the product $a_S \circ b_s = (a_S b_S)_S$ where the right hand side is evaluated in L.

If $p \in L$ is prime and $S = \{x \in L_* \,|\, x \nleqslant p\}$, then L_S is denoted by L_p. [9]

Theorem 2.12. *Let m be a maximal element of L and q be a proper element of L. If q is a (weakly) quasi n-absorbing element of L, then q_m is a (weakly) quasi n-absorbing element of L_m.*

Proof. Let $a, b \in L_*$ such that $a_m^n b_m \leqslant q_m$. Hence $ua^n b \leqslant q$ for some $u \nleqslant m$. It implies that $a^n \leqslant q$ or $a^{n-1}(ub) \leqslant q$. Since $u_m = 1_m$, we get $a_m^n \leqslant q_m$ or $a_m^{n-1}b_m \leqslant q_m$, we are done. □

Theorem 2.13. *Let L be a principal element lattice. Then the following statements are equivalent.*

(1) *Every proper element of L is a quasi n-absorbing element of L.*

(2) *For every a, $b \in L_*$, $a^n = ca^n b$ or $a^{n-1}b = da^n b$ for some c, $d \in L$.*

(3) *For all $a_1, a_2, \ldots, a_{n+1} \in L_*$, $(a_1 \wedge a_2 \wedge \ldots \wedge a_n)^n \leqslant ca_1a_2 \cdots a_{n+1}$ or $(a_1 \wedge a_2 \wedge \ldots \wedge a_n)^{n-1}a_{n+1} \leqslant da_1a_2 \cdots a_{n+1}$ for some c, $d \in L$.*

Proof. (1) ⇔ (2). Suppose that every proper element of L is a quasi n-absorbing element of L. Hence $a^n b \leqslant (a^n b)$ implies that $a^n \leqslant (a^n b)$ or $a^{n-1}b \leqslant (a^n b)$. Since L is a principal element lattice, there is some element $c \in L$ with $a^n = ca^n b$ or there is some element $d \in L$ with $a^{n-1}b = da^n b$. The converse is clear.

(2) ⇒ (3). Put $a = a_1 \wedge a_2 \wedge \ldots \wedge a_n$ and $b = a_{n+1}$. Hence the result follows from (2).

(3) ⇒ (2). For all $a, b \in L_*$, we can write $a^n = (\underbrace{a \wedge a \wedge \ldots \wedge a}_{n \text{ times}}) \leqslant ca^n b$ or $a^{n-1}b = (\underbrace{a \wedge a \wedge \ldots \wedge a}_{n-1 \text{ times}})b \leqslant da^n b$. □

Theorem 2.14. *Let $L = L_1 \times L_2$ where L_1 and L_2 are C-lattices. Then:*

(1) *q_1 is a quasi n-absorbing element of L_1 if and only if $(q_1, 1_{L_2})$ is a quasi n-absorbing element of L,*

(2) *q_2 is a quasi n-absorbing element of L_2 if and only if $(1_{L_1}, q_2)$ is a quasi n-absorbing element of L.*

Proof. (1). Suppose that q_1 is a quasi n-absorbing element of L_1.

Let $(a_1, a_2)^n(b_1, b_2) \leqslant (q_1, 1_{L_2})$ for some a_1, $b_1 \in L_{1_*}$ and a_2, $b_2 \in L_{2_*}$. Then $a_1^n b_1 \leqslant q_1$ implies that either $a_1^n \leqslant q_1$ or $a_1^{n-1}b_1 \leqslant q_1$. It follows either $(a_1, a_2)^n \leqslant (q_1, 1_{L_2})$ or $(a_1, a_2)^{n-1}(b_1, b_2) \leqslant (q_1, 1_{L_2})$. Thus $(q_1, 1_{L_2})$ is a quasi n-absorbing element of L. Conversely suppose that $(q_1, 1_{L_2})$ is a quasi n-absorbing element of L and $a^n b \leqslant q_1$ for some $a, b \in L_{1_*}$. Hence $(a, 1_{L_2})^n(b, 1_{L_2}) \leqslant (q_1, 1_{L_2})$ which implies that either $(a, 1_{L_2})^n \leqslant (q_1, 1_{L_2})$ or $(a, 1_{L_2})^{n-1}(b, 1_{L_2}) \leqslant (q_1, 1_{L_2})$. So $a_1^n \leqslant q_1$ or $a_1^{n-1}b_1 \leqslant q_1$, as needed.

(2). It can be verified similar to (1). □

Theorem 2.15. *Let $L = L_1 \times \cdots \times L_k$ where all L_i are C-lattices. If q_i is a quasi n_i-absorbing element of L_i for all $i = 1, \ldots, k$, then $(q_1, \ldots, q_k)$ is a quasi m-absorbing element of L where $m = \max\{n_1, \ldots, n_k\} + 1$.*

Proof. Suppose that $(a_1, \ldots, a_k)^m(b_1, \ldots, b_k) \leqslant (q_1, \ldots, q_k)$ for some $(a_1, \ldots, a_k)$, $(b_1, \ldots, b_k) \in L_*$ and $m = \max\{n_1, \ldots, n_k\} + 1$. Hence $a_i^m b_i = a_i^{n_i}(a_i^{m-n_i}b_i) \leqslant q_i$ for all $i = 1, \ldots, k$. Since each q_i is a quasi n_i-absorbing element, we have either $a_i^{n_i} \leqslant q_i$ or $a_i^{m-1}b_i = a_i^{n_i-1}(a_i^{m-n_i}b_i) \leqslant q_i$ for all $i = 1, .., k$. If $a_i^{n_i} \leqslant q_i$ for all $i = 1, \ldots, k$, then $(a_1, \ldots, a_k)^m \leqslant (q_1, \ldots, q_k)$. Without loss generality, suppose that $a_i^{n_i} \leqslant q_i$ for all $1 \leqslant i \leqslant j$ and $a_i^{m-1}b_i \leqslant q_i$ for all $j + 1 \leqslant i \leqslant k$, for some $j = 1, \ldots, k$. Thus $(a_1, \ldots, a_k)^{m-1}(b_1, \ldots, b_k) \leqslant (q_1, \ldots, q_k)$, so we are done. □

Definition 2.16. A proper element q of L is said to be a *strongly quasi n-absorbing* element of L if whenever $a, b \in L$ (not necessarily compact) with $a^n b \leqslant q$ implies that either $a^n \leqslant q$ or $a^{n-1}b \leqslant q$.

It is clearly seen that every strongly quasi n-absorbing element of L is quasi n-absorbing.

Theorem 2.17. *Let L be a principal element lattice. The following statements are equivalent.*

(1) *Every proper element of L is a strongly quasi n-absorbing element of L.*

(2) *For all $a, b \in L$, $a^n = a^n b$ or $a^{n-1}b = a^n b$.*

(3) *$(a_1 \wedge a_2 \wedge \ldots \wedge a_n)^n \leqslant a_1a_2 \cdots a_{n+1}$ or $(a_1 \wedge a_2 \wedge \ldots \wedge a_n)^{n-1}a_{n+1} \leqslant a_1a_2 \cdots a_{n+1}$ for all $a_1, a_2, \ldots, a_{n+1} \in L$.*

Proof. This can be easily shown using the similar argument in Theorem 2.13. □

Theorem 2.18. *Let q be a proper element of L. Then:*

(1) *If $a^n b \leqslant q \leqslant a \wedge b$, where $a, b \in L$, implies that $a^n \leqslant q$ or $a^{n-1}b \leqslant q$, then q is a strongly quasi n-absorbing element of L.*

(2) *If $a_1a_2 \cdots a_{n+1} \leqslant q \leqslant a_1 \wedge a_2 \wedge \ldots \wedge a_{n+1}$, where $a_1, a_2, \ldots, a_{n+1} \in L$, implies that $a_1 \cdots a_{i-1}a_{i+1} \cdots a_{n+1} \leqslant q$, for some $1 \leqslant i \leqslant n + 1$, then q is a strongly quasi n-absorbing element of L.*

Proof. (1). Let $x, y \in L$ with $x^n y \leqslant q$. We show that $x^n \leqslant q$ or $x^{n-1}y \leqslant q$. Now put $a = x \vee q$ and $b = y \vee q$. Hence we conclude $a^n b \leqslant q \leqslant a \wedge b$, and so $a^n \leqslant q$ or $a^{n-1}b \leqslant q$ by (1). It follows $x^n \leqslant q$ or $x^{n-1}y \leqslant q$.

(2). It can be easily verified similar to (1). □

References

[1] **F. Alarcon and D.D. Anderson**, *Commutative semirings and their lattices of ideals*, Houston J. Math. **20** (1994), 571 – 590.

[2] **D.D. Anderson and C. Jayaram**, *Principal element lattices*, Czechoslovak Math. J. **46** (1996), 99 – 109.

[3] **D.D. Anderson and E. Smith**, *Weakly prime ideals*, Houston J. Math. **29** (2003), 831 – 840.

[4] **D.F. Anderson and A. Badawi**, *On n-absorbing ideals of commutative rings*, Commun. Algebra **39** (2011), 1646 – 1672.

[5] **A. Badawi**, *On* 2*-absorbing ideals of commutative rings*, Bull. Austral. Math. Soc. **75** (2007), 417 – 429.

[6] **A. Badawi and A.Y. Darani**, *On weakly* 2*-absorbing ideals of commutative rings*, Houston J. Math. **39** (2013), 441 – 452.

[7] **F. Callialp, C. Jayaram and U. Tekir**, *Weakly prime elements in multiplicative lattices*, Commun. Algebra **40** (2012), 2825 – 2840.

[8] **R.P. Dilworth**, *Abstract commutative ideal theory*, Pacific J. Math. **12** (1962), 481 – 498.

[9] **C. Jayaram and E.W Johnson**, *s-prime elements in multiplicative lattices*, Periodica Math. Hungarica **31** (1995), 201 – 208.

[10] **C. Jayaram, U. Tekir and E. Yetkin**, 2*-absorbing and weakly* 2*-absorbing elements in multiplicative lattices*, Commun. Algebra **42** (2014), 2338 – 2353.

[11] **J.A. Johnson and G.R. Sherette**, *Structural properties of a new class of CM-lattices*, Canadian J. Math. **38** (1986), 552 – 562.

[12] **N.K. Thakare, C.S. Manjarekar and S. Maeda**, *Abstract spectral theory II, Minimal characters and minimal spectrums of multiplicative lattices*, Acta. Sci. Math. (Szeged). **52** (1988), 53 – 67.

Received March 07, 2016

Department of Mathematics, Gaziantep University, 27310 Gaziantep, Turkey
E-mail: yetkin@gantep.edu.tr

Quasigroups and Related Systems **24** (2016), 187 − 196

A note on left loops with WA-property

Natalia N. Didurik and *Ivan A. Florja*

Abstract. We study properties of WA-quasigroups with a left identity element, i.e., quasigroups satisfying two identities: $xx \cdot yz = xy \cdot xz$ and $xy \cdot zz = xz \cdot yz$.

1. Introduction

We start from some definitions and examples. Other basic facts about quasigroups and loops can be found in [2] and [13].

Definition 1.1. (cf. [5, 8]) A groupoid $(Q, \cdot)$ is called a *quasigroup* if, on the set Q, there exist operations "\" and "/" such that in the algebra $(Q, \cdot, \backslash, /)$ identities

$$x \cdot (x \backslash y) = y, \tag{1}$$

$$(y/x) \cdot x = y, \tag{2}$$

$$x \backslash (x \cdot y) = y, \tag{3}$$

$$(y \cdot x)/x = y, \tag{4}$$

are fulfilled.

Definition 1.2. (cf. [11, 12]) A quasigroup $(Q, \cdot)$ with the identities

$$xx \cdot yz = xy \cdot xz \quad \text{and} \quad xy \cdot zz = xz \cdot yz \tag{5}$$

is called a *WA-quasigroup* or a *semi-medial quasigroup* (shortly: *SM-quasigroup*) (cf. [14, 15]).

Identities (5) are not equivalent.

Example 1.3. This quasigroup satisfies only the first of these identities.

$*$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	2	5	4
2	2	4	0	5	1	3
3	4	2	5	0	3	1
4	3	5	1	4	0	2
5	5	3	4	1	2	0

2010 Mathematics Subject Classification: 20N05
Keywords: loop, left loop, WA-property

Lemma 1.4. *In any WA-quasigroup* $(Q, \cdot)$ *the following identities are true:*

$$x^2\backslash(yz) = (x\backslash y)(x\backslash z), \tag{6}$$

$$(yz)/x^2 = (y/x)(z/x), \tag{7}$$

$$x(y\backslash z) = (xy)\backslash(x^2 z), \tag{8}$$

$$(y/z)x = (yx^2)/(zx), \tag{9}$$

where $xy = z \Leftrightarrow x\backslash z = y \Leftrightarrow z/y = x$.

Proof. (6). It is clear that there exists an element z' such that $x^2\backslash yz' = (x\backslash y)(x\backslash z)$. We must prove that $z' = z$. From the definition of the operation $\backslash$ we have

$$yz' = x^2((x\backslash y)(x\backslash z)) \overset{(5)}{=} x(x\backslash y) \cdot x(x\backslash z) \overset{(1)}{=} yz.$$

Therefore, $z' = z$.

(7). It is clear that there exists an element z' such that $yz'/x^2 = (y/x)(z/x)$. We must prove that $z' = z$. From the definition of the operation $/$ we have

$$yz' = (y/x)(z/x) \cdot x^2 \overset{(5)}{=} (y/x)x \cdot (z/x)x \overset{(2)}{=} yz.$$

Therefore, $z' = z$.

(8). It is clear that there exists an element z' such that $x(y\backslash z) = (xy)\backslash(x^2 z')$. We must prove that $z' = z$. We have

$$x^2 z' = (xy) \cdot x(y\backslash z) \overset{(5)}{=} x^2 \cdot y(y\backslash z) \overset{(1)}{=} x^2 z.$$

Therefore, $z' = z$.

(9). It is clear that there exists an element y' such that $(y/z)x = (y'x^2)/(zx)$. We must prove that $y' = y$. As in previous cases

$$y'x^2 = (y/z)x \cdot (zx) \overset{(5)}{=} (y/z)z \cdot x^2 \overset{(2)}{=} yx^2.$$

Therefore, $y' = y$. □

Definition 1.5. (cf. [2]) Let λ and ρ be two maps $Q \to Q$. A quasigroup $(Q, \cdot)$ is called an *LIP-quasigroup* if it satisfies the identity

$$\lambda x \cdot (x \cdot y) = y,$$

and an *RIP-quasigroup* if it satisfies the identity

$$(x \cdot y) \cdot \rho y = x.$$

A quasigroup which is simultaneously an LIP- and RIP-quasigroup is called an *IP-quasigroup.*

Definition 1.6. (cf. [9]) A quasigroup $(Q,\cdot)$ is called a *left Bol quasigroup*, if it satisfies the identity

$$x(y\cdot xz)=R_{e_x}^{-1}(x\cdot yx)\cdot z.$$

It is called a *right Bol quasigroup*, if it satisfies the identity

$$(yx\cdot z)x=yL_{f_x}^{-1}(xz\cdot x),$$

where $xe_x=x=f_xx$.

Definition 1.7. (cf. [2]) A quasigroup $(Q,\cdot)$ is called a *Moufang quasigroup*, if in $(Q,\cdot)$ the following identities are true

$$(xy\cdot z)y=x(y(e_yz\cdot y)),\tag{10}$$

$$y(x\cdot yz)=((y\cdot xf_y)y)z\tag{11}$$

where $ye_y=y=f_yy$.

In his PhD thesis (see also [4]) I.A. Florja proved that in quasigroups the identities (10) and (11) are equivalent, so Moufang quasigroups can be defined as quasigroups satisfying one of these identities.

We will need the following two lemmas. The first was proved by I.A. Florja in his PhD thesis, the second is proved in the Belousov's book [2].

Lemma 1.8. *A left and right Bol quasigroup is a Moufang quasigroup.*

Lemma 1.9. *A loop isotopic to a Moufang quasigroup is an IP-loop.*

Definition 1.10. A commutative loop $(Q,\cdot)$ with the identity $xx\cdot yz=xy\cdot xz$ is called a *commutative Moufang loop.*

From Definitions 1.2 and 1.10 it follows that any commutative Moufang loop is a WA-quasigroup.

Theorem 1.11. (cf. [7, 12, 15]) *Each loop isotopic to a WA-quasigroup is a commutative Moufang loop.*

2. Properties of left WA-loops

Lemma 2.1. *Any WA-quasigroup with a left identity element is a left Bol quasigroup.*

Proof. If f is a left identity element of a quasigroup $(Q,\cdot)$, then $ff=f$, $L_fx=x$ for all $x\in Q$ and $L_f=\varepsilon$. From Theorem 1.11 it follows that an isotope of the form

$$x\circ y=R_f^{-1}x\cdot L_f^{-1}y=R_f^{-1}x\cdot y\tag{12}$$

of a quasigroup $(Q,\cdot)$ is a commutative Moufang loop. Any commutative Moufang loop $(Q,\circ)$ is an IP-loop, i.e., there exists a permutation I such that

$$Ix\circ(x\circ y)=(y\circ x)\circ Ix=y \tag{13}$$

for all $x,y\in Q$.

Going in the equation (13) to the operation $\cdot$ we have $R_f^{-1}Ix\cdot(R_f^{-1}x\cdot y)=y$, $R_f^{-1}IR_fx\cdot(x\cdot y)=y$. Hence, $I_lx\cdot(x\cdot y)=y$ for

$$I_l=R_f^{-1}IR_f. \tag{14}$$

Thus $(Q,\cdot)$ is an LIP-quasigroup. This, by results of [9], shows that $(Q,\cdot)$ is a left Bol quasigroup. □

Corollary 2.2. *If f is a left identity element of a WA-quasigroup $(Q,\cdot)$, then the translation R_f is an automorphism of $(Q,\cdot)$, and an automorphism of the commutative Moufang loop $(Q,\circ)$ defined by* (12).

Proof. The fact that $R_f\in Aut(Q,\cdot)$ follows from (5) and the equality $ff=f$. Further, using the formula (12), we have: $R_f(x\circ y)=R_fx\circ R_fy$, $R_f(R_f^{-1}x\cdot y)=R_f^{-1}R_fx\cdot R_fy$, $x\cdot R_fy=x\cdot R_fy$. Therefore $R_fI=IR_f$, and (14) takes the form $I_l=I$. □

Lemma 2.3. *Any WA-quasigroup with a right identity element is a right Bol quasigroup.*

Proof. Consider the isotope $(Q,\circ)$ of a WA-quasigroup $(Q,\cdot)$ given by:

$$x\circ y=x\cdot L_e^{-1}y,$$

where e is a right identity of $(Q,\cdot)$. By Theorem 1.11, $(Q,\circ)$ is a commutative Moufang loop. Let 1 be the identity element of $(Q,\circ)$ and I be a permutation of Q such that $x\circ Ix=1$ for all $x\in Q$. Since $(y\circ x)\circ Ix=y$ for all $x,y\in Q$, we have $y=(y\circ x)\circ Ix=(y\cdot L_e^{-1}x)\cdot L_e^{-1}Ix$. Therefore, $(y\cdot x)\cdot L_e^{-1}IL_ex=y$, hence $(y\cdot x)\cdot\rho x=y$ for $\rho=L_e^{-1}IL_e$. So, $(Q,\cdot)$ is an RIP-quasigroup. This, by results of [9] means that $(Q,\cdot)$ is a right Bol quasigroup. □

Lemma 2.4. *Any WA-quasigroup $(Q,\cdot)$ with the left* (*right*) *inverse property is a left* (*right*) *Bol quasigroup.*

Proof. Since a WA-quasigroup with the left inverse property is an LIP-quasigroup, the proof of this lemma is very similar to the proof of Lemma 2.1.

For WA-quasigroups with the right inverse property the proof is analogous. □

Corollary 2.5. *Any WA-quasigroup that is an IP-quasigroup, is a Moufang quasigroup.*

Proof. The proof follows from Lemma 2.4 and Lemma 1.8. □

Definition 2.6. (cf. [2]) The isotope of the form

$$x \circ y = L_a^{-1}(L_a x \cdot y) \tag{15}$$

is called a *right derivative operation of* $(Q, \cdot)$ *generated by* a.

The isotope of the form

$$x \circ y = R_a^{-1}(x \cdot R_a y) \tag{16}$$

is called a *left derivative operation of* $(Q, \cdot)$ *generated by* a.

Theorem 2.7. *Let* $(Q, \cdot)$ *be a WA-quasigroup. Then*

(i) *the right derivative operation* $(Q, \cdot)$ *is a left Bol quasigroup,*

(ii) *the left derivative operation of* $(Q, \cdot)$ *is a right Bol quasigroup.*

Proof. (i). From (15) it follows that a quasigroup $(Q, \circ)$ has a left identity element, namely, $f = e_a$, where $ae_a = a$. Indeed, $e_a \circ y = L_a^{-1}(L_a e_a \cdot y) = L_a^{-1} L_a y = y$. In particular $f \circ f = f$.

We consider the following isotope of a quasigroup $(Q, \circ)$:

$$x + y = (R_f^\circ)^{-1} x \circ y, \tag{17}$$

where $R_f^\circ x = x \circ f$. Then $(Q, +)$ is a loop with the identity element f.

Indeed, $f + y = (R_f^\circ)^{-1} f \circ y = f \circ y = y$, since, if $(R_f^\circ)^{-1} f = z$, then $f = (R_f^\circ) z$, $f = z \circ f$. But, as was mentioned, $f \circ f = f$, therefore, $z = f$. Further we have $x + f = (R_f^\circ)^{-1} x \circ f = R_f^\circ (R_f^\circ)^{-1} x = x$.

Using (15) we can re-write (17) as follows:

$$x + y = L_a^{-1}(L_a (R_f^\circ)^{-1} x \cdot y).$$

Thus the loop $(Q, +)$ is an isotope of a WA-quasigroup $(Q, \cdot)$. By Theorem 1.11 among loop isotopes of a WA-quasigroup $(Q, \cdot)$ there exists a commutative Moufang loop. We recall that any loop isotopic to a Moufang loop is a Mofang loop (cf. [2]). Therefore $(Q, +)$ is a Moufang loop.

Our proof will be complete, if we prove that a quasigroup $(Q, \circ)$ is an LIP-quasigroup.

From $x^{-1} + (x + y) = y$, using (17), we obtain $(R_f^\circ)^{-1} x^{-1} \circ ((R_f^\circ)^{-1} x \circ y) = y$. Now, denoting $(R_f^\circ)^{-1} x^{-1}$ by αx and $(R_f^\circ)^{-1} x$ by βx, we obtain two permutations α, β of the set Q, and the possibility to rewrite the last equation in more useful form $\alpha x \circ (\beta x \circ y) = y$, which is equivalent to $\alpha \beta^{-1} x \circ (x \circ y) = y$.

The last means that $(Q, \circ)$ is an LIP-quasigroup. This completes the proof of (i).

(ii). From (16) it follows that a quasigroup $(Q, \circ)$ has a right identity element $e = f_a$, where $f_a a = a$. Indeed, $x \circ f_a = R_a^{-1}(x \cdot R_a f_a) = R_a^{-1}(x \cdot a) = x$.

We consider the following isotope of the quasigroup (right loop) $(Q,\circ)$:

$$x+y = x\circ (L_e^\circ)^{-1}y, \tag{18}$$

where $L_e^\circ x = e\circ x$. Then $(Q,+)$ is a loop with the identity element e. The proof is similar to the proof in the case (i) and we omit it.

From (18), using (16), we have

$$x+y = R_a^{-1}(x\cdot R_a(L_e^\circ)^{-1}y).$$

Analogously as in (i) we can prove that $(Q,+)$ is a Moufang loop. Next, from $(y+x)+x^{-1} = y$, using (18), we deduce $(y\circ(L_e^\circ)^{-1}x)\circ(L_e^\circ)^{-1}x^{-1} = y$. This shows that $(Q,\circ)$ is an RIP-quasigroup. □

3. Automorphisms of left WA-loops

We start with the following lemma which is a quasigroup folklore.

Lemma 3.1. *In a quasigroup autotopy any two components uniquely define the third.*

Elements of the group $I_h(Q,\cdot) = \{\alpha\in M(Q,\cdot)\,|\,\alpha h = h\}$, where $M(Q,\cdot)$ is the group generated by all left and right translations of a quasigroup $(Q,\cdot)$, are called *inner mappings of* $(Q,\cdot)$ *relative to the element* $h\in Q$ (cf. [2]). Belousov proved (cf. [2]) that the group $I_h(Q,\cdot)$ is generated by all permutations of the form:

$$\begin{aligned} L_{x,y} &= L_{x\circ y}^{-1}L_xL_y\,, &&\text{where}\quad (x\circ y)h = x\cdot yh,\\ R_{x,y} &= R_{x\bullet y}^{-1}R_yR_x\,, &&\text{where}\quad h(x\bullet y) = hx\cdot y,\\ T_x &= L_{\sigma x}^{-1}R_x\,, &&\text{where}\quad \sigma = R_h^{-1}L_h. \end{aligned}$$

Lemma 3.2. *In a WA-quasigroup $(Q,\cdot)$ with the left identity element f inner permutations $L_{x,y}$, $R_{x,y}$, and T_x relative to the element f are automorphisms of $(Q,\cdot)$.*

Proof. In our case $L_{x,y} = L_{x\circ y}^{-1}L_xL_y$, where $x\circ y = R_f^{-1}(x\cdot R_fy) = R_f^{-1}x\cdot y$, by Corollary 2.2. Therefore

$$L_{x,y} = L_{R_f^{-1}x\cdot y}^{-1}L_xL_y. \tag{19}$$

Moreover, $x\cdot y = fx\cdot y = f(x\bullet y) = x\bullet y$ implies

$$R_{x,y} = R_{x\cdot y}^{-1}R_yR_x. \tag{20}$$

Since $\sigma x = R_f^{-1}L_fx = R_f^{-1}x$, we also have $T_x = L_{R_f^{-1}x}^{-1}R_x$. Thus

$$L_{x,y}f = R_{x,y}f = T_xf = f. \tag{21}$$

From (5) it follows that for any fixed $a \in Q$ the following triplets (L_a, L_a, L_{a^2}) and (R_a, R_a, R_{a^2}), their inverse and various component-vise products are autotopies of $(Q, \cdot)$. Therefore

$$\begin{aligned}&(L^{-1}_{R_f^{-1}x\cdot y}, L^{-1}_{R_f^{-1}x\cdot y}, L^{-1}_{(R_f^{-1}x\cdot y)^2})(L_x, L_x, L_{x^2})(L_y, L_y, L_{y^2}) = \\ &(L_{x,y}, L_{x,y}, L^{-1}_{(R_f^{-1}x\cdot y)^2}L_{x^2}L_{y^2}).\end{aligned} \tag{22}$$

This means that

$$L_{x,y}f \cdot L_{x,y}z = L^{-1}_{(R_f^{-1}x\cdot y)^2}L_{x^2}L_{y^2}(f \cdot z), \tag{23}$$

whence, applying (21), we obtain

$$L_{x,y}z = L^{-1}_{(R_f^{-1}x\cdot y)^2}L_{x^2}L_{y^2}z \tag{24}$$

for all $x, y, z \in Q$. This, together with (22), shows that $L_{x,y}$ is an automorphism of the quasigroup $(Q, \cdot)$.

Similarly from

$$(R^{-1}_{x\cdot y}, R^{-1}_{x\cdot y}, R^{-1}_{(x\cdot y)^2})(R_y, R_y, R_{y^2})(R_x, R_x, R_{x^2}) = (R_{x,y}, R_{x,y}, R^{-1}_{(x\cdot y)^2}R_{y^2}R_{x^2}) \tag{25}$$

and

$$(L^{-1}_{R_f^{-1}x}, L^{-1}_{R_f^{-1}x}, L^{-1}_{(R_f^{-1}x)^2})(R_x, R_x, R_{x^2}) = (T_x, T_x, L^{-1}_{(R_f^{-1}x)^2}R_{x^2}) \tag{26}$$

it follows that $R_{x,y}$ and T_x are automorphisms of $(Q, \cdot)$. □

Corollary 3.3. *In any WA-quasigroup with a left identity element we have*

$$L_{x,y} = L_{x^2,y^2}, \quad R_{x,y} = R_{x^2,y^2}, \quad T_x = T_{x^2}.$$

Proof. Putting $y = z$ in (5), we obtain

$$(xy)^2 = x^2 \cdot y^2. \tag{27}$$

From (19) and (24) it follows that the identity $L_{x,y} = L_{x^2,y^2}$ will be proved, if we prove that $(R_f^{-1}x \cdot y)^2 = R_f^{-1}x^2 \cdot y^2$. This follows from (27) and the fact that R_f (and its inverse) are automorphisms of $(Q, \cdot)$ (see Corollary 2.2). Indeed, $(R_f^{-1}x)^2 = R_f^{-1}x \cdot R_f^{-1}x = R_f^{-1}(x \cdot x) = R_f^{-1}x^2$. Since $R_{x,y} = R^{-1}_{(x\cdot y)^2}R_{y^2}R_{x^2}$, by (25), from (20) and (27) we obtain $R_{x,y} = R_{x^2,y^2}$.

The third identity can be proved in a similar way. □

Definition 3.4. (cf. [10, 13]) Let $(Q, \cdot)$ be a groupoid. The element $a \in Q$ is called a *left nuclear element* in $(Q, \cdot)$ if $L_{ax} = L_a L_x$ for all $x \in Q$. The set of all left nuclear elements in $(Q, \cdot)$ is called the *left nucleus* of $(Q, \cdot)$ and is denoted by N_l.

It is well known (cf. [2, 3]) that in a quasigroup the set N_l forms a subgroup.

Theorem 3.5. *In a WA-quasigroup $(Q,\cdot)$ with the left identity element f the inner permutations $L_{x,y}$, $R_{x,y}$, and T_x relative to $a \in Q$ are automorphisms of $(Q,\cdot)$ if and only if $a \in N_l$ and the following identity $xy \cdot a = xf \cdot ya$ is satisfied.*

Proof. In this case $L_{x,y} = L^{-1}_{x\circ y}L_xL_y$, where $x \circ y = R^{-1}_a(x \cdot R_ay)$, $R_{x,y} = R^{-1}_{x\bullet y}R_yR_x$, where $ax \cdot y = a(x \bullet y)$ and $T_x = L^{-1}_{\sigma x}R_x$, where $\sigma x = R^{-1}_a L_f a$.

In a similar way as in the proof of Lemma 3.2 (identities (22), (23), and (24)), we can prove that $L_{x,y}$, $R_{x,y}$, and T_x are automorphisms of $(Q,\cdot)$. Then $L^{-1}_{x\circ y}L_xL_yf = f$, i.e., $L_xL_yf = L_{x\circ y}f$. So, $x \cdot yf = L_{x\circ y}f = R^{-1}_a(x \cdot R_ay)f$, which gives $R^{-1}_f(x \cdot yf) = R^{-1}_a(x \cdot R_ay)$. Since R^{-1}_f is an automorphism of $(Q,\cdot)$ (Corollary 2.2), from the last identity we obtain $R^{-1}_f x \cdot y = R^{-1}_a(x \cdot R_ay)$, and consequently, $xy = R^{-1}_a(R_fx \cdot R_ay)$. Thus, $xy \cdot a = xf \cdot ya$ for all $x, y \in Q$.

Moreover, $R^{-1}_{x\bullet y}R_yR_xf = f$ implies $R_yR_xf = R_{x\bullet y}f$. Hence $xy = x \bullet y$ and $ax \cdot y = a(x \bullet y) = a \cdot xy$ for all $x, y \in Q$. Therefore $a \in N_l$.

The converse statement is obvious. □

Lemma 3.6. *The permutation L_aR_a is an automorphism of a WA-quasigroup $(Q,\cdot)$ with the left identity element element f if and only if $a^2 = f$.*

Proof. Since

$$(L_a, L_a, L_{a^2})(R_a, R_a, R_{a^2}) = (L_aR_a, L_aR_a, L_{a^2}R_{a^2}) \tag{28}$$

is an autotopy of $(Q,\cdot)$, we have

$$L_aR_af \cdot L_aR_ay = L_{a^2}R_{a^2}y \tag{29}$$

for all $y \in Q$. This autotopy is an automorphism if and only if $L_{a^2}R_{a^2} = L_aR_a$. The last equality holds if and only if $L_aR_af = f$, i.e., if and only if $a^2 = f$. □

Corollary 3.7. *Let $(Q,\cdot)$ be a WA-quasigroup with the left identity element f. If $a^2 = f$, then $L_aR_a = L_{a^2}R_{a^2} = R_f$.*

Proof. From (28) and the fact that L_aR_a is an automorphism of $(Q,\cdot)$ it follows $L_aR_a = L_{a^2}R_{a^2}$. From (29), $L_aR_af = f$ and $a^2 = f$ we obtain $L_aR_a = R_f$. □

Lemma 3.8. *The permutation $L_{a^2}R_a$ is an automorphism of a WA-quasigroup $(Q,\cdot)$ with the left identity element f if and only if $a^2 \cdot a = f$.*

Proof. It is clear that

$$(L_{a^2}, L_{a^2}, L_{(a^2)^2})(R_a, R_a, R_{a^2}) = (L_{a^2}R_a, L_{a^2}R_a, L_{(a^2)^2}R_{a^2})$$

is an autotopy of $(Q,\cdot)$. Therefore $L_{a^2}R_af \cdot L_{a^2}R_ay = L_{(a^2)^2}R_{a^2}y$ is true for all $y \in Q$. This autotopy is an automorphism if and only if $L_{(a^2)^2}R_{a^2} = L_{a^2}R_a$, i.e., if and only if $L_{a^2}R_af = f$. The last condition is equivalent to $a^2 \cdot a = f$. □

4. Pseudoautomorphisms and subloops

A bijection θ of a set Q is called a *right pseudoautomorphism* of a quasigroup $(Q,\cdot)$ if there exists at least one element $c\in Q$ such that $(c\cdot\theta x)\cdot\theta y=c\cdot\theta(x\cdot y)$ for all $x,y\in Q$, i.e., if $(L_c\theta,\theta,L_c\theta)$ is an autotopy of a quasigroup $(Q,\cdot)$. The element c is called a *companion* of θ (cf. [2]).

A quasigroup with a right pseudoautomorphism has also a left identity element (cf. [13]).

Lemma 4.1. *In a WA-quasigroup with a left identity element f the translation R_a is a right pseudoautmorphism if and only if the translation L_a is a right pseudoautmorphism and $a^2=f$.*

Proof. Suppose that R_a is a right pseudoautomorphism with the companion k, i.e., a quasigroup $(Q,\cdot)$ has an autotopy (L_kR_a,R_a,L_kR_a). By Lemma 3.6 , L_aR_a, where $a^2=f$, is an automorphism of $(Q,\cdot)$.

Therefore

$$(L_kR_a,R_a,L_kR_a)(L_aR_a,L_aR_a,L_aR_a)^{-1}=(L_kL_a^{-1},L_a^{-1},L_kL_a^{-1})$$

also is an autotopy of $(Q,\cdot)$. The last means that L_a^{-1} is a right pseudoautomorphism of $(Q,\cdot)$. Since the set of all right pseudoatomorphisms of $(Q,\cdot)$ forms a group (cf. [2]), also L_a is a right pseudoautomorphism of $(Q,\cdot)$.

The converse statement is obvious. □

Lemma 4.2. *Let $(H,\cdot)$ be a subquasigroup of a WA-quasigroup $(Q,\cdot)$. Then $(aH,\cdot)$ is a subquasigroup of $(Q,\cdot)$ for any $a=a^2$.*

Proof. By (5), we have $ah_1\cdot ah_2=a^2\cdot h_1h_2=a\cdot h_1h_2\in aH$. Thus the set aH is closed with respect to the quasigroup operation.

The equation $ah_1\cdot x=ah_2$, where $h_1,h_2\in H$, has a unique solution $x\in Q$. Obviously, $x=ax'$ for some $x'\in Q$. Thus, $ah_1\cdot ax'=a\cdot h_1x'=ah_2$. Hence $h_1x'=h_2$, and consequently, $x'\in H$. Therefore $x=ax'\in aH$.

Analogously we prove that the equation $y\cdot ah_1=ah_2$ has a solution in aH. □

Lemma 4.3. *Let $(Q,\cdot)$ be a WA-quasigroup with the left identity element f and $(Q,\circ)$ be a loop defined by* (12). *If $(Q,\cdot)$ satisfies the inverse property, then:*

- (i) *$R_f^2=\varepsilon$, where ε is the identity permutation,*
- (ii) *$I_l=I$, $I_r=IR_f$ for $I_lx\cdot xy=y$, $xy\cdot I_ry=x$, $Ix\circ(x\circ y)=y$,*
- (iii) *I_l and I_r are automorphisms of a quasigroup $(Q,\cdot)$ and a loop $(Q,\circ)$,*
- (iv) *$I_lI_r=R_f$, $I_lI_r=I_rI_l$.*

Proof. (i). Indeed, $I_lf=I_rf=f$. Thus $xf\cdot f=x$ for any $x\in Q$. So, $R_f^2=\varepsilon$.

(ii). Since $x\circ y\overset{(12)}{=}R_f^{-1}x\cdot y=R_fx\cdot y$, by (i), R_f is an automorphism of $(Q,\cdot)$ and the corresponding commutative Moufang loop $(Q,\circ)$ (Theorem 1.11 and Corollary 2.2).

Going now in the equation $I_lx(x\cdot y) = y$ to the loop operation $\circ$ we obtain $R_fI_lx\circ(R_fx\circ y) = y$. Thus $R_fI_lR_f^{-1}x\circ(x\circ y) = y$. Consequently, $I = R_fI_lR_f^{-1}$ and $I_l = R_f^{-1}IR_f = I$, since in $(Q,\circ)$ automorphisms R_f and I commute.

Similarly, going in the equation $(x\cdot y)I_ry = x$ to the loop operation $\circ$ we obtain $R_f(R_fx\circ y)\circ I_ry = x$. Thus, $(x\circ R_fy)\circ I_ry = x$ and $(x\circ y)\circ I_rR_f^{-1}y = x$. Therefore, $I = I_rR_f^{-1}$ and $I_r = IR_f$.

(iii). It is a consequence of (ii) and (iii).

(iv). Since $I = I_l$ and $I_r = IR_f$, we have $I_lI_r = I^2R_f = R_f$. Analogously, $I_rI_l = IR_fI = R_f$. □

References

[1] **A.A. Albert**, *Quasigroups. I,* Trans. Amer. Math. Soc. **54** (1943), 507 – 519.

[2] **V.D. Belousov**, *Foundations of the theory of quasigroups and loops*, (Russian), Nauka, Moscow, 1967.

[3] **V.D. Belousov**, *Elements of qasigroup theory: A special course*, (Russian), Kishinev State Univ., Kishinev, 1981.

[4] **V.D. Belousov and I.A. Florja**: *Quasigroups with the inverse property,* (Russian), Bul. Akad. Ştiinţe RSS Moldoven. 1966, no. 4, 3 – 17.

[5] **G. Birkhoff**, *Lattice theory*, Third edition, AMS Colloquium Publications, Providence, 1967.

[6] **R.H. Bruck**, *A survey of binary systems*, Springer Verlag, 1971.

[7] **A.M. Cheban**, *WA-quasigroups*, (Russian), Bull. Transdniestrian Univ. **7** (1997), 31 – 34.

[8] **T. Evans**, *Homomorphisms of non-associative systems,* J. London Math. Soc. **24** (1949), 254 – 260.

[9] **I.A. Florja**, *Bol quasigroups*, (Russian), Studies in General Algebra, Khishinev, 1965, 136 – 154.

[10] **G.N. Garrison**, *Quasi-groups*, Ann. Math. **41** (1940), 474 – 487.

[11] **T. Kepka**, *Quasigroups which satisfy certain generalized forms of the Abelian identity,* Časopis Pěst. Mat. **100** (1975), 46 – 60.

[12] **T. Kepka**, *A note on WA-quasigroups*, Acta Univ. Carolin. Math. Phys. **19(2)** (1978), 61 – 62.

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

[14] **V.A. Shcherbacov**, *On the structure of left and right F-, SM- and E-quasigroups*, J. Gen. Lie Theory Appl. **3** (2009), 197 – 259.

[15] **K.K. Shchukin**, *Action of a group on a quasigroup*, (Russian), Khishinev State Univ., 1985.

Received August 2, 2016

Faculty of Physics and Mathematics, Shevchenko Transnistria State University, 25 October str., 128, MD-3300 Tiraspol, Moldova
E-mail: natnikkr83@mail.ru

Quasigroups and Related Systems **24** (2016), 197 − 204

On entropicity in n-ary semigroups

Sonia Dog

Abstract. We investigate entropicity and the generalized entropic property in n-ary semigroups derived from binary semigroups satisfying for some fixed $k \geqslant 2$ the identity $x^k = x$.

1. We say that an n-ary semigroup (S, f), where $n > 2$, has the *entropic property* or is *entropic* (*medial* in other terminology), if it satisfies the identity

$$f(f(x_{11}, \dots, x_{1n}), f(x_{21}, \dots, x_{2n}) \dots, f(x_{n1}, \dots, x_{nn})) =$$

$$f(f(x_{11}, \dots, x_{n1}), f(x_{12}, \dots, x_{n2}) \dots, f(x_{1n}, \dots, x_{nn})).$$

If in (S, f) there exist n-ary terms $t_1, t_2, \dots, t_n$ such that (S, f) satisfies the identity

$$f(f(x_{11}, \dots, x_{1n}), f(x_{21}, \dots, x_{2n}) \dots, f(x_{n1}, \dots, x_{nn})) =$$

$$f(t_1(x_{11}, \dots, x_{n1}), t_2(x_{12}, \dots, x_{n2}) \dots, t_n(x_{1n}, \dots, x_{nn})),$$

then we say that (S, f) has the *generalized entropic property.* These two properties, studied by many authors with various names, are not equivalent in general. The entropicity of n-ary semigroups is a generalization of *mediality*:

$$xy \cdot zu = xz \cdot yu,$$

and *semimediality*:

$$xy \cdot zx = xz \cdot yx$$

of binary algebras (cf. for example [17] or [22]).

The entropicity and the generalized entropicity in idempotent n-ary semigroups were studied in [15]. Below we give very simple (almost trivial) proofs of results given in this paper. We also present some generalizations of these results.

2. We start with some comments on entropic n-ary groups ($n > 2$).

In [11] it is proved that an n-ary group (S, f) is entropic if and only if it is *semiabelian*, i.e., if

$$f(x_1, x_2, \dots, x_{n-1}, x_n) = f(x_n, x_2, \dots, x_{n-1}, x_1)$$

for all $x_1, x_2, \dots, x_n \in S$.

2010 Mathematics Subject Classification: 20M15, 08B26
Keywords: n-ary semigroup, n-ary group, generalized entropic property, medial law.

From [5] (Corollary 15) it follows that an n-ary group (S,f) is entropic if and only if for some $a\in S$ and all $x,y\in S$ we have

$$f(x,a,\dots,a,y)=f(y,a,\dots,a,x).$$

Thus, by Gluskin-Hosszú theorem (cf. [12, 13]) any entropic n-ary group (S,f) can be presented in the form

$$f(x_1,x_2,\dots,x_n)=x_1\circ\varphi(x_2)\circ\varphi^2(x_3)\circ\dots\circ\varphi^{n-2}(x_{n-1})\circ x_n\circ b,$$

where $(S,\circ)$ is an abelian group, φ its automorphism such that $\varphi^{n-1}=id$ and $\varphi(b)=b$ for some fixed element $b\in S$ (cf. [7]). Moreove, as it is proved in [24] (see also [10]), $(A,\circ)$, φ and b are uniquely determined.

3. *Mal'cev n-semigroups*, i.e., n-ary semigroups (S,f) satisfying the identities

$$f(x,y,\dots,y)=x \quad\text{ and }\quad f(y,\dots,y,x)=x, \tag{1}$$

studied in [15], are in fact n-ary groups. This follows from Proposition 3.1 in [8]. It also can be deduced from results proved in [25]. Hence, Mal'cev n-semigroups (as n-ary groups) are cancellative, i.e.,

$$f(x_1,\dots,x_{i-1},a,x_{i+1},\dots,x_n)=f(x_1,\dots,x_{i-1},b,x_{i+1},\dots,x_n)\Rightarrow a=b \tag{2}$$

for all $i=1,\dots,n$ and $a,b,x_1,\dots,x_n\in S$.

On the other hand, an n-ary semigroup is cancellative if and only if it satisfies (2) for some $i=2,3,\dots,n-1$ or, equivalently, for $i=1$ and $i=n$ (Lemma 2 in [6]). Hence, in an idempotent i-cancellative n-ary semigroup (S,f) we have

$$f(x,y,\dots,y)=f(x,y,\dots,y,f(y,\dots,y))=f(f(x,y,\dots,y),y,\dots,y),$$

which implies the first identity of (1). Analogously we obtain the second identity. (It is Lemma 3.2 in [15]). Thus an idempotent n-ary semigroup i-cancellative for some $i=2,\dots,n-1$ or for $i=1$ and $i=n$ is an n-ary group satisfying (1). Hence, Proposition 3.3 in [15] is trivial.

As a simple consequence, we obtain Theorem 3.5 from [15]: *a Mal'cev n-semigroup is entropic if and only if it is semiabelian.*

4. By Gluskin-Hosszú theorem, for any ternary Mal'cev semigroup (S,f), as for a ternary group, there exists a group $(S,\cdot)$, its automorphism φ and an element $b\in S$ such that $\varphi(b)=b$ and

$$f(x,y,z)=x\cdot\varphi(y)\cdot\varphi^2(z)\cdot b.$$

Since a ternary Mal'cev semigroup is idempotent, $\varphi(x)\cdot\varphi^2(x)\cdot b=e$. Hence, $\varphi(x)=x^{-1}\cdot b^{-1}$ and $b^{-1}=\varphi(b^{-1})=e$. Therefore, $b=e$ and $\varphi(x)=x^{-1}$. Thus, for any ternary Mal'cev semigroup (S, f) there is an abelian group $(A, +)$ such that

$$f(x, y, z) = x - y + z.$$

From this, as a simple consequence, we obtain all results proved in Section 4 in [15]. Theorem 4.5 in [15] is a special case of Artamonov's Proposition 6 (cf. [2]). It also can be deduced from the description of free n-ary groups presented by Shchuchkin [14, 18, 19] and Sioson [23].

5. We say that an n-ary semigroup (S, f) is *derived* from a semigroup $(S, \cdot)$ if $f(x_1, x_2, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$ for all $x_1, \ldots, x_n \in S$. Obviously, an n-ary semigroup derived from an entropic semigroup is entropic, too. For a *surjective* semigroup, i.e., a semigroup $(S, \cdot)$ with the property $S^2 = S$, we have a stronger result.

Proposition 1. *An n-ary semigroup (S, f) derived from a surjective semigroup $(S, \cdot)$ is entropic if and only if $(S, \cdot)$ is entropic.*

Proof. An entropic n-ary semigroup (S, f) derived from a surjective semigroup $(S, \cdot)$ is semiabelian and each its element can be presented as a multiplication of $n - 1$ elements of S. Thus, for any $x, y, a, b \in S$, we have

$$\begin{aligned} xa \cdot by &= x(a_2a_3 \cdots a_n) \cdot (b_2b_3 \cdots b_n)y = x(a_2a_3 \cdots a_nb_2)b_3 \cdots b_ny \\ &= x(b_2a_3 \cdots a_na_2)b_3 \cdots b_ny = xb_2(a_3a_4 \cdots a_na_2b_3)b_4 \cdots b_ny \\ &= xb_2(b_3a_4 \cdots a_na_2a_3)b_4 \cdots b_ny = xb_2b_3(a_4 \cdots a_na_2a_3b_4)b_5 \cdots b_ny \\ &= \ldots = x(b_2b_3 \cdots b_n) \cdot (a_2a_3 \cdots a_n)y = xb \cdot ay, \end{aligned}$$

which completes the proof. □

We say that a semigroup $(S, \cdot)$ is *k-idempotent* ($k > 1$), if for all $x \in S$ we have $x^k = x$. An n-ary semigroup derived from an n-idempotent semigroup is obviously idempotent, but a $(k+1)$-ary semigroup derived from a k-idempotent semigroup is not idempotent. So, results proved for n-ary semigroups derived from k-idempotent semigroups are a significant generalization of results proved in [15].

Lemma 2. *Any k-idempotent semigroup has at least one idempotent.*

Proof. In a 2-idempotent semigroup each element is idempotent. It is clear. For $k > 2$, we have $a^{k-1} = a^ka^{k-2} = a^{k-1}a^{k-1}$, which means that in a k-idempotent semigroup each element a^{k-1} is idempotent. □

Proposition 3. *A k-idempotent semigroup is entropic if and only if it is semimedial.*

Proof. An entropic semigroup is obviously semimedial. To prove the converse statement observe that in a semimedial semigroup

$$\begin{aligned}(xyzu)^2 &= (xy(zu)x)yzu = (x(zu)yx)yzu = x(z(uyx)yz)u = x(zy(uyx)z)u\\ &= xzy(uy(xz)u) = xzy(u(xz)yu) = (xzyu)^2\end{aligned}$$

and

$$(xzyu)(xyzu) = xzy(u(xy)zu) = xz((yu)zx(yu)) = (xzyu)(xzyu) = (xzyu)^2.$$

Thus, in a k-idempotent semigroup

$$\begin{aligned}xyzu &= (xyzu)^k = (xyzu)^2(xyzu)^{k-2} = (xzyu)^2(xyzu)^{k-2} = \ldots = (xzyu)^k\\ &= xzyu, \qquad \text{if } k \text{ is even.}\end{aligned}$$

For $k = 2t+1$ we have

$$\begin{aligned}xyzu &= (xyzu)^{2t+1} = (xyzu)^2(xyzu)^{2t-1} = \ldots = (xzyu)^{2t}(xyzu)\\ &= (xzyu)^{2t-1}(xzyu)(xyzu) = (xzyu)^{2t-1}(xzyu)^2 = (xzyu)^{2t+1}\\ &= xzyu,\end{aligned}$$

which completes our proof. □

As a consequence, we obtain

Corollary 4. [15, Lemma 6.3] *An n-idempotent semigroup is entropic if and only if it is semimedial.*

Proposition 5. *An n-ary semigroup derived from a k-idempotent semigroup is semiabelian if and only if it is commutative.*

Proof. Let (S, f) be a semiabelian n-ary semigroup derived from a k-idempotent semigroup $(S, \cdot)$. Then for all $x, y \in S$ we have

$$\begin{aligned}xy &= xx^{k-1}y = xx^{k-1}x^{k-1}y = \ldots = xx^{k-1}\ldots x^{k-1}y = f(x, x^{k-1}, \ldots, x^{k-1}y)\\ &= f(y, x^{k-1}, \ldots, x^{k-1}x) = yx^{k-1}\ldots x^{k-1}x = yx,\end{aligned}$$

which means that $(S, \cdot)$ is a commutative semigroup. Consequently, (S, f) is commutative, too.

The converse statement is obvious. □

Corollary 6. [15, Corollary 6.6] *For an n-ary semigroup (S, f) derived from an n-idempotent semigroup $(S, \cdot)$ the following statements are equivalent:*

(a) *(S, f) is semiabelian,*

(b) *$(S, \cdot)$ is commutative,*

(c) *(S, f) is commutative.*

6. Below we present simple proofs of some other results presented in [15]. For this we will use the concept of the covering semigroup.

As is well known (cf. for example [3] or [4]) each n-ary semigroup (S, f) can be isomorphically embedded into some semigroup $(S^*, \cdot)$, called the *covering* or *enveloping semigroup*, in this way that $f(x_1, x_2, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$ for all

$x_1, \ldots, x_n \in S \subseteq S^*$. The construction of such semigroup is very similar to the construction of the covering group for an n-ary group (cf. [16]). Unfortunately, as it was observed in [9], two non-isomorphic n-ary semigroups (groups) may have the same covering semigroup (group).

Proposition 7. [15, Proposition 5.1] *An associative and idempotent n-ary operation f satisfying the identities*

$$f(x, \ldots, x, y) = f(y, x, \ldots, x) = f(x, y, x, \ldots, x)$$

or

$$f(x, \ldots, x, y) = f(y, x, \ldots, x) = f(x, \ldots, x, y, x)$$

is commutative.

Proof. Let (S, f) be an idempotent n-ary semigroup satisfying the above identities. Then in its covering semigroup $(S^*, \cdot)$, for every $x, y \in S$, we have $x^n = x$ and $x^{n-1}y = yx^{n-1} = xyx^{n-2}$. So,

$$xy = x^n y = x \cdot x^{n-1} y = x \cdot yx^{n-1} = xyx^{n-2} \cdot x = yx^{n-1} \cdot x = yx^n = yx$$

for every $x, y \in S$. Hence f is a commutative operation. □

An n-ary semigroup (S, f) is called a *left zero n-semigroup* if it satisfies the identity $f(x_1, \ldots, x_n) = x_1$. If it satisfies the identity $f(x_1, \ldots, x_n) = x_n$, then it is called a *right zero n-semigroup*.

Proposition 8. [15, Proposition 5.3] *Let (S, f) be an n-ary semigroup. If (S, f) satisfies the identity $f(x, \ldots, x, y) = x$, then it is a left zero semigroup. If (S, f) satisfies the identity $f(y, x, \ldots, x) = x$, then it is a right zero semigroup.*

Proof. In the covering semigroup of (S, f) for all $x, y \in S$ we have $x^{n-1}y = x$ and $x^n = x$. Thus $xy = x^n y = x \cdot x^{n-1} y = xx$, and consequently,

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= (x_1 x_2) x_3 x_4 \cdots x_n = (x_1 x_1) x_3 x_4 \cdots x_n = x_1 (x_1 x_3) x_4 \cdots x_n \\ &= x_1 x_1 x_1 x_4 \cdots x_n = \ldots = x_1 \cdots x_1 (x_1 x_n) = x_1 \end{aligned}$$

for all $x_1, \ldots, x_n \in S$. Hence (S, f) is a left zero semigroup.

The second sentence can be proved analogously. □

7. In the case of an n-ary semigroup (S, f) derived from a binary semigroup $(S, \cdot)$, the generalized entropic property has the form

$$\begin{gathered} (x_{11} \cdot \ldots \cdot x_{1n}) \cdot (x_{21} \cdot \ldots \cdot x_{2n}) \cdot \ldots \cdot (x_{n1} \cdot \ldots \cdot x_{nn}) = \\ t_1(x_{11}, \ldots, x_{n1}) \cdot t_2(x_{12}, \ldots, x_{n2}) \cdot \ldots \cdot t_n(x_{1n}, \ldots, x_{nn}), \end{gathered} \tag{3}$$

where $t_1, t_2, \ldots, t_n$ are some n-ary terms of (S, f).

We start with the following two lemmas which are a generalization of results proved in [15] for idempotent n-ary semigroups derived from binary semigroup containing an idempotent element. We do not assume that considered semigroups are idempotent.

Lemma 9. *If an n-ary semigroup (S,f) derived from a binary semigroup $(S,\cdot)$ with an idempotent e satisfies the generalized entropic property* (3)*, then for every $a\in S$ we have*

$$t_1(e,a,e,\ldots,e)\cdot e = eae = e\cdot t_n(a,e,\cdot,e).$$

Proof. The proof is the same as the proof of Lemma 6.4 in [15]. □

Lemma 10. *If an n-ary semigroup (S,f) derived from a binary semigroup $(S,\cdot)$ with an idempotent e satisfies the generalized entropic property* (3)*, then*

$$eabe = ebeae$$

for all $a,b\in S$.

Proof. The proof is the same as the proof of Lemma 6.5 in [15]. □

Theorem 11. *If an n-ary semgroup (S,f) derived from a k-idempotent semigroup $(S,\cdot)$ has the generalized entropic property, then $(S,\cdot)$ is entropic.*

Proof. For any $a\in S$ consider the set

$$S_a=\{a^{k-1}sa^{k-1} : s\in S\}.$$

It is not difficult to see that $(S_a,\cdot)$ is a semigroup and $e=a^{k-1}$ is its neutral element. So, (S_a,f) is an n-ary subsemigroup of (S,f). Moreover, from the generalized entropic property (3), for all $x_1,\ldots,x_n\in S_a$ we have

$$\begin{aligned} x_1\cdot x_2\cdot\ldots\cdot x_n &= (x_1\cdot e\cdot\ldots\cdot e)\cdot(x_2\cdot e\cdot\ldots\cdot e)\cdot\ldots\cdot(x_n\cdot e\cdot\ldots\cdot e)\\ &= t_1(x_1,x_2,\ldots,x_n)\cdot t_2(e,e,\ldots,e)\cdot\ldots\cdot t_n(e,e,\ldots,e)\\ &= t_1(x_1,x_2,\ldots,x_n). \end{aligned}$$

Thus $t_1(x_1,x_2,\ldots,x_n)=x_1\cdot x_2\cdot\ldots\cdot x_n$. Analogously we obtain $t_k(x_1,x_2,\ldots,x_n)=x_1\cdot x_2\cdot\ldots\cdot x_n$ for other terms $t_2,\ldots,t_n$.

So, in this case, (3) has the form

$$\begin{gathered}(x_{11}\cdot\ldots\cdot x_{1n})\cdot(x_{21}\cdot\ldots\cdot x_{2n})\cdot\ldots\cdot(x_{n1}\cdot\ldots\cdot x_{nn})=\\ (x_{11}\cdot\ldots\cdot x_{n1})\cdot(x_{12}\cdot\ldots\cdot x_{n2})\cdot\ldots\cdot(x_{1n}\cdot\ldots\cdot x_{nn}),\end{gathered}$$

which, for $x_{1n}\neq e$, $x_{n1}\neq e$ and $x_{ij}=e$ in other cases, gives the commutativity of $(H_a,\cdot)$. Therefore, for all $a,b,c\in S$ we have

$$a^{k-1}b\cdot ca^{k-1}=a^{k-1}ba^{k-1}\cdot a^{k-1}ca^{k-1}=a^{k-1}ca^{k-1}\cdot a^{k-1}ba^{k-1}=a^{k-1}c\cdot ba^{k-1}.$$

So, $a^{k-1}b\cdot ca^{k-1}=a^{k-1}c\cdot ba^{k-1}$. This implies $ab\cdot ca=ac\cdot ba$. Thus $(S,\cdot)$ is semimedial. Proposition 3 completes the proof. □

Corollary 12. [15, Theorem 6.7] *Let (S, f) be an idempotent n-ary semigroup derived from an n-idempotent semigroup $(S, \cdot)$ and assume that (S, f) has the generalized entropic property. Then $(S, \cdot)$ is entropic.*

Theorem 13. *A k-idempotent semigroup has the generalized entropic property if and only if it is entropic.*

Proof. Let $(S, \cdot)$ be a k-idempotent semigroup satisfying the generalized entropic property. Then there are terms t_1 and t_2 such that

$$xy \cdot zu = t_1(x, z)t_2(y, u)$$

for all $x, y, z, u \in S$. By Lemma 2, the set E_S of all idempotents of a semigroup $(S, \cdot)$ is non-empty. Since $ef \cdot ef = t_1(e, e)t_2(f, f) = ef$ for all $e, f \in E_S$, $(E_S, \cdot)$ is a subsemigroup of $(S, \cdot)$. By [1, Proposition 3.11], $(E_S, \cdot)$ is entropic. This completes the proof for $k = 2$ because in this case $S = E_S$.

For $k > 2$, for every $a \in S$ we have $a = axa$ and $ax = xa$, where $x = a^{k-2}$. So, $(S, \cdot)$ is a completely regular semigroup whose idempotents forms a subsemigroup, i.e., a normal band. Hence, in this case, the proof is identical with the second part of the proof of Theorem 6.8 in [15]. Namely, by [20, Theorem 4.1 and Corollary 4.4], a semigroup $(S, \cdot)$ is a normal band of groups. Thus, by [21, Theorem 3.2], it is a subdirect product of a band B and a semilattice L of groups. Since, by the definition of subdirect product, B and L are homomorphic images of a semigroup $(S, \cdot)$, they satisfy all identities satisfied by $(S, \cdot)$. Hence, they satisfy the generalized entropic property. This means that a band B is entropic (see the case $k = 2$). Every group with the generalized entropic property is commutative [1, Proposition 4.7] and a semilattice of commutative groups is commutative. Thus a semilattice L is commutative and hence entropic. Consequently, $(S, \cdot)$, as a subdirect product of entropic B and L, is entropic. □

Corollary 14. [15, Theorem 6.8] *An n-idempotent semigroup $(S, \cdot)$ has the generalized entropic property if and only if it is entropic.*

References

[1] **K. Adaricheva, A. Pilitowska and D. Stanovský**, *Complex algebras of subalgebras*, (Russian), Algebra Logika **47** (2008), 655 – 686.

[2] **V.A. Artamonov**, *Free n-groups*, Math. Notes **8** (1970), 750 – 754 (tranlation from Mat. Zametki **8** (1970), 499 – 507).

[3] **G. Čupona**, *On associatives*, (Macedonian), Makedon. Akad. Nauk. Umet. Oddel. Prirod.-Mat. Nauk. Prilozi **1** (1969), 9 – 20.

[4] **G. Čupona and N. Celakoski**, *On representation of n-associatives into semigroups*, (Macedonian), Makedon. Akad. Nauk. Umet. Oddel. Prirod.-Mat. Nauk. Prilozi **6** (1974), 23 – 34.

[5] **W.A. Dudek**, *Remarks on n-groups*, Demonstratio Math. **13** (1980), 165 – 181.

[6] **W.A. Dudek**, *Autodistributive n-groups*, Commentationes Math. Annales Soc. Math. Polonae, Prace Matematyczne **23** (1983), $1-11$.

[7] **W.A. Dudek**, *Medial n-groups and skew elements*, Proc. V Universal Algebra Symposium "Universal and Applied Algebra", Turawa 1988, World Scientific, Singapore 1989, $55-80$.

[8] **W.A. Dudek**, *Varieties of polyadic groups*, Filomat **9** (1995), $657-674$.

[9] **W.A. Dudek and K. Glazek**, *Around the Hosszú-Gluskin Theorem for n-ary groups*, Discrete Math. **308** (2008), $4861-4876$.

[10] **W.A. Dudek and J. Michalski**, *On a generalization of Hosszú Theorem*, Demonstratio Math. **15** (1982), $783-805$.

[11] **K. Głazek and B. Gleichgewicht**, *Abelian n-groups*, Coll. Math. Soc. J. Bolyai, **29** Universal Algebra, Esztergom (Hungary), 1977, $321-329$.

[12] **L.M. Gluskin**, *Positional operatives*, (Russian), Mat. Sb. (N.S.) **68(110)** (1965), $444-472$.

[13] **M. Hosszú**, *On the explicit form of n-group operations*, Publ. Math. Debrecen **10** (1963), $88-92$.

[14] **V.M. Kusov and N.A. Shchuchkin**, *Free abelian semicyclic n-ary groups*, (Russian), Chebyshevskii Sb. **12** (2011), no. 2(38), $68-76$.

[15] **E. Lehtonen and A. Pilitowska**, *Entropicity and generalized entropic property in idempotent n-semigroups*, Semigroup Forum **91** (2015), $260-281$.

[16] **E.L. Post**, *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1940), $208-350$.

[17] **V.A. Shcherbacov**, *On the structure of left and right F-, SM- and E-quasigroups*, J. Gen. Lie Theory Appl. **3** (2009), $197-259$.

[18] **N.A. Shchuchkin**, *Free abelian n-ary groups*, (Russian), Chebyshevskiǐ Sb. **12** (2011), $163-170$.

[19] **N.A. Shchuchkin**, *Free semiabelian n-ary groups*, Quasigroups and Related Systems **23** (2015), $309-317$.

[20] **M. Petrich**, *Regular semigroups satisfying certain conditions on idempotents and ideals*, Trans. Am. Math. Soc. **170** (1972), $245-267$.

[21] **M. Petrich**, *Regular semigroups which are subdirect products of a band and a semilattice of groups*, Glasgow Math. J. **14** (1973), $27-49$.

[22] **K.K. Shchukin**, *Action of a group on a quasigroup*, (Russian), Khishinev State Univ., 1985.

[23] **F.M. Sioson**, *On free abelian n-groups II*, Proc. Japan. Acad. **43** (1967), $880-883$.

[24] **E.I. Sokolov**, *The Gluskin-Hosszú theorem for Dörnte n-groups*, (Russian), Mat. Issledovanya **39** (1965), $187-189$.

[25] **V.I. Tyutin**, *About the axiomatics of n-ary groups*, (Russian), Doklady Akad. Nauk BSSR **29** (1985), $691-693$.

Received August 20, 2016

E-mail: sonia.dog@sovamua.com

On the fine structure of quadratical quasigroups

Wieslaw A. Dudek and Robert A. R. Monzo

Abstract. We prove that quadratical quasigroups form a variety $\mathcal{Q}$ of right and left simple groupoids and that the spectrum of $\mathcal{Q}$ is contained in the set of integers equal to 1 plus a multiple of 4. Properties of quadratical quasigroups are described and their inter-relationships are explored. Every element of a quadratical quasigroup is proved to belong to a 4-cycle. These results are applied to find conditions under which the group of additive integers, modulo n, induces quadratical quasigroups.

1. Introduction

This paper builds on the work of Polonijo [3], Volenec [5] and Dudek [1] on quadratical quasigroups. Polonijo [3] and Volenec [5] proved that a quadratical groupoid is a quasigroup. Volenec [5, 6] gave a motivation for studying quadratical quasigroups, in terms of a geometrical representation of the complex numbers C as points of the Euclidean plane. He defined a product $*$ on C that defines a quadratical quasigroup and in which the product of distinct elements x and y is the third vertex of a positively oriented, isosceles right triangle, at which the right angle occurs. Other geometrical motivations for the study of quadratical quasigroups one can find in [7, 8].

Volenec proved in [5] a number of properties of quadratical quasigroups, which are listed in Theorem 2.2 below. These properties tell us a great deal and, indeed, we apply them to prove that quadratical quasigroups form a variety $\mathcal{Q}$ (Theorem 2.30). Inter-relationships amongst the properties of quadratical quasigroups are explored in Section 2.

We begin to amplify our understanding of the fine structure of quadratical quasigroups in Section 3. In so doing, we give further meaning to the *quad* in the word quadratical, in terms of 4-*cycles.* We apply this to prove that the order of a finite quadratical quasigroup is $m = 4t + 1$ for some $t \in \{0, 1, 2, \ldots\}$ (Propositions 3.1 − 3.4), fine tuning Dudek's result that the order of a finite quadratical quasigroup is odd [1, Corollary 1].

In Section 4 we prove results about conditions under which the group of additive integers, modulo n, induces quadratical quasigroups. Results in this section rely heavily on Dudek's Theorem (cf. Theorem 4.1) that proves that every quadratical quasigroup is induced by a commutative group.

2010 Mathematics Subject Classification: 20M15, 20N02
Keywords: quadratical quasigroup, variety, dual groupoid, cycle.

This paper is the first of two by the authors on quadratical quasigroups. The second paper will examine the fine structure of quadratical quasigroups in detail and introduce the concept of a *translatable* quadratical quasigroup. Quadratical quasigroups of many new orders will also be given, along with ideas about possible directions of future research in this area.

2. Properties of quadratical groupoids

Definition 2.1. A groupoid $(Q,\cdot)$ has *property* A if it satisfies the identity

$$xy\cdot x = zx\cdot yz. \tag{A}$$

It is called *right solvable* (*left solvable*) if for any $\{a,b\}\subseteq Q$ there exists a unique $x\in G$ such that $ax=b$ ($xa=b$). It is *left* (*right*) *cancellative* if $xy=xz$ implies $y=z$ ($yx=zx$ implies $y=z$). It is a *quasigroup* if it is left and right solvable.

Note that a right solvable groupoid is left cancellative and a left solvable groupoid is right cancellative.

Volenec [5] defined a *quadratical groupoid* as a right solvable groupoid satisfying property A. He proved that a quadratical groupoid is left solvable and satisfies the following identities:

Theorem 2.2. *A quadratical groupoid satisfies the following identities:*

$$x = x^2 \quad (\textit{idempotency}), \tag{1}$$
$$x\cdot yx = xy\cdot x \quad (\textit{elasticity}), \tag{2}$$
$$x\cdot yx = xy\cdot x = yx\cdot y \quad (\textit{strong elasticity}), \tag{3}$$
$$yx\cdot xy = x \quad (\textit{bookend}), \tag{4}$$
$$x\cdot yz = xy\cdot xz \quad (\textit{left distributivity}), \tag{5}$$
$$xy\cdot z = xz\cdot yz \quad (\textit{right distributivity}), \tag{6}$$
$$xy\cdot zw = xz\cdot yw \quad (\textit{mediality}), \tag{7}$$
$$x(y\cdot yx) = (xy\cdot x)y, \tag{8}$$
$$(xy\cdot y)x = y(x\cdot yx), \tag{9}$$
$$xy = zw \longleftrightarrow yz = wx \quad (\textit{alterability}). \tag{10}$$

Corollary 2.3. [2 and 3, Theorem 5] *A quadratical groupoid is a quasigroup.*

Note that throughout the remainder of this paper we will use the fact that quadratical groupoids are quasigroups and satisfy properties (1) through (10), often without mention. Note also that property (3) allows us to write the term xyx without ambivalence in any quadratical quasigroup.

Definition 2.4. We define $\mathcal{Q}$ to be the collection of quadratical quasigroups.

Theorem 2.5. *A groupoid Q is a quadratical quasigroup if and only if it satisfies* (A), (3), (4) *and* (7).

Proof. $(\Rightarrow)$ This follows from Theorem 2.2 and the definition of a quadratical quasigroup.
$(\Leftarrow)$ First we prove that Q is left cancellative. Suppose that $ax = ay$. Then,

$$x \overset{(4)}{=} ax \cdot xa \overset{ax=ay}{=} ay \cdot xa \overset{(A)}{=} yx \cdot y \overset{(3)}{=} xy \cdot x \overset{(A)}{=} ax \cdot ya \overset{ax=ay}{=} ay \cdot ya \overset{(4)}{=} y.$$

So $x = y$ and Q is left cancellative.

Property A implies $x^2 \cdot x = x^2x^2$ and so left cancellativity implies $x = x^2$. Hence, Q is idempotent. Since Q is medial and idempotent it is therefore (left and right) distributive.

Using left and right distributivity, mediality, idempotency and strong elasticity we have

$$a(b \cdot ba) = ab \cdot (a \cdot ba) = ab \cdot (ba \cdot b) = (a \cdot ba)b = (ab \cdot a)b.$$

Hence,

$$a(b \cdot ba) = (ab \cdot a)b. \tag{11}$$

We now prove that $ax = b$ has a unique solution $x = (b \cdot ba) \cdot (b \cdot ba)(ba \cdot a)$. Indeed,

$$\begin{aligned} ax &\overset{(5)}{=} a(b \cdot ba) \cdot (a(b \cdot ba) \cdot a(ba \cdot a)) \overset{(11),(5),(3)}{=} (aba \cdot b) \cdot (aba \cdot b)(aba \cdot a) \\ &\overset{(5)}{=} (aba)(b \cdot ba) \overset{(7),(1)}{=} ab \cdot ba \overset{(4)}{=} b. \end{aligned}$$

The solution x is unique because Q is left cancellative. We have proved that Q is right solvable and so by definition, Q is a quadratical quasigroup. □

Corollary 2.6. *Q is a quadratical quasigroup if and only if it a medial, idempotent groupoid that satisfies property A.*

Proof. $(\Rightarrow)$ This follows from the definition of a quadratical quasigroup and from Theorem 2.2.
$(\Leftarrow)$ Let Q be a medial, idempotent groupoid that satisfies property A. By Theorem 2.5 we need only show that Q satisfies (3) and (4).

Since Q is idempotent and satisfies property A, for all $\{x, y\} \subseteq Q$,

$$x = x^2 \overset{(7)}{=} x^2x \overset{(A)}{=} yx \cdot xy,$$

so Q satisfies (4). Also, idempotency and mediality imply (5) and so

$$xy \cdot x \overset{(1)}{=} xy \cdot x^2 \overset{(7)}{=} x^2 \cdot yx \overset{(1)}{=} x \cdot yx \overset{(A)}{=} yx \cdot yy \overset{(1)}{=} yx \cdot y,$$

which proves (3). □

Theorem 2.7. *A groupoid satisfying* (4) *and either* (5) *or* (6) *is idempotent*

Proof. From (4) we obtain $x^2x^2 = x$ for any $x \in G$. If Q also satisfies (5), then

$$x^2x = x^2(x^2x^2) \overset{(5)}{=} (x^2x^2)(x^2x^2) = x^2.$$

Also,

$$x = x^2x^2 = (x^2x)(x^2x) \overset{(5)}{=} ((x^2x)x^2)((x^2x)x) = (x^2x^2)(x^2x) = xx^2.$$

Then

$$x^2 = x^2x = (x^2x)(xx^2) \overset{(4)}{=} x.$$

Similarly, in a groupoid satisfying (4) and (6), $x = x^2x$, $x^2 = xx^2$ and $x^2 = xx^2 = (x^2x)(xx^2) = x$, by (4). □

Example 2.8. A groupoid Q of order greater than or equal to 2 and satisfying the identity $xy = zw$ is distributive but not idempotent.

Example 2.9. The following groupoid Q satisfies (4) but not (1), (2), (7), (5), (10). Moreover, it is not left solvable or right solvable.

$\cdot$	x	y	z	w
x	y	z	w	y
y	w	x	w	x
z	y	x	w	y
w	z	z	x	z

Theorem 2.10. *A groupoid Q satisfying* (4), (5), (6) *and* (7) *is cancellative.*

Proof. Suppose that $ax = ay$ for any $\{a, x, y\} \subseteq Q$. By Theorem 2.7, $ax = (ax)^2$. Then, $ax = ax \cdot ax = ax \cdot ay = ay \cdot ax = a \cdot yx = a \cdot xy$. Consequently, $yx \overset{(4)}{=} (a{\cdot}yx)(yx{\cdot}a) = ax{\cdot}(yx{\cdot}a) \overset{(5)}{=} (ax{\cdot}yx)(ax{\cdot}a) \overset{(6)}{=} (ay{\cdot}x)(ay{\cdot}a) \overset{(5)}{=} ay{\cdot}xa = ax{\cdot}xa \overset{(4)}{=} x$. Similarly, $xy = y$. So $y = xy \cdot yx = yx = x$.

Analogously, $xa = ya$ implies $x = y$, so Q is cancellative. □

Theorem 2.11. *A groupoid satisfying* (4), (5), (6) *and* (7) *also satisfies* (3).

Proof. Theorems 2.7 and 2.10 imply that Q is idempotent and cancellative. So $xy{\cdot}x = xy{\cdot}xx = x{\cdot}yx$. Hence, $(xy{\cdot}x)y = (x{\cdot}yx)y \overset{(6)}{=} xy{\cdot}(yx{\cdot}y) \overset{(5)}{=} (xy{\cdot}yx)(xy{\cdot}y) \overset{(4)}{=} y(xy \cdot y) \overset{(5)}{=} (y \cdot xy)y^2 = (y \cdot xy)y$ and, by cancellation, $xy \cdot x = y \cdot xy \overset{(5)}{=} yx \cdot y$. Therefore, Q is strongly elastic, i.e., it satisfies (3). □

Corollary 2.12. *An idempotent medial groupoid satisfying* (4) *is cancellative and strongly elastic.*

Proof. Medial idempotent groupoids are distributive. The corollary follows from Theorems 2.10 and 2.11. □

Theorem 2.13. *A left (or right) cancellative, medial, idempotent groupoid satisfying* (3) *satisfies* (4).

Proof. Mediality and idempotency imply distributivity. Then, $(ca \cdot ac)^2 = ca{\cdot}ac = (ca \cdot a)(ca \cdot c)$. Thus, by (3) we obtain

$$(ca \cdot ac)^2 = ca \cdot ac = (ca \cdot a)(c \cdot ac) = (ca \cdot a)(ca \cdot c) = (ca \cdot a)(ac \cdot a) = (ca \cdot ac)a$$

and so left cancellativity implies $ca \cdot ac = a$. Also, using right cancellativity,

$$(ca \cdot ac)^2 = ca \cdot ac = ca \cdot (ac)^2 = (c \cdot ac)(a \cdot ac) = (a \cdot ca)(a \cdot ac) = a(ca \cdot ac)$$

implies $a = ca \cdot ac$. □

Theorem 2.14. *A groupoid Q is a quadratical quasigroup if and only if it is idempotent, medial and satisfies* (4).

Proof. (⇒) This follows from Theorem 2.2.
(⇐) By Corollary 2.6, we need only show that $xy{\cdot}x = zx{\cdot}yz$. But, since mediality and idempotency imply left distributivity, $zx{\cdot}yz = (zx{\cdot}y)(zx{\cdot}z)$ and, by Corollary 2.12, $zx \cdot yz = (zx \cdot y)(xz \cdot x) = (zx \cdot xz)(yx) = x \cdot yx = xy \cdot x$. □

Definition 2.15. The *dual* of a groupoid $(Q, \cdot)$ is the groupoid $Q^* = (Q, *)$, where $x * y = y \cdot x$.

Corollary 2.16. *The dual of a quadratical quasigroup is a quadratical quasigroup.*

Corollary 2.17. *Any subgroupoid of a quadratical quasigroup is a quadratical quasigroup.*

Note that an idempotent semigroup satisfies (4) if and only if it satisfies the identity $x = xyx$; that is, if and only if it is a rectangular band. A semigroup with property A is cancellative if and only if it is trivial.

Theorem 2.18. *An idempotent groupoid satisfying* (4) *and* (10) *is elastic.*

Proof. Indeed, $x = x^2 = yx \cdot xy$ implies $x \cdot yx = xy \cdot x$. □

Theorem 2.19. *An elastic groupoid satisfying* (4) *is idempotent.*

Proof. $x^2 = xx^2 \cdot x^2x = x^2x \cdot xx^2 = x$. □

Theorem 2.20. *A groupoid Q is a quadratical quasigroup if and only if it satisfies* (2), (4) *and* (7).

Proof. (⇒) This follows from Theorem 2.2.
(⇐) Assume that Q satisfies (2), (4) and (7). By Theorem 2.19, Q is idempotent. By Theorem 2.14 then, Q is quadratical. □

Theorem 2.21. *An idempotent groupoid satisfying* (2) *and* (10) *satisfies* (4).

Proof. $x \cdot yx = xy \cdot x$ implies $yx \cdot xy = x^2 = x$. □

Corollary 2.22. *An idempotent groupoid satisfying* (10) *satisfies* (2) *if and only if it satisfies* (4).

Proof. This follows from Theorems 2.18 and 2.21. □

Theorem 2.23. *A medial groupoid satisfying* (4) *satisfies* (10).

Proof. Suppose that $xy = zw$. Then $zw{\cdot}yx = xy{\cdot}yx = y$ and $wz{\cdot}xy = wz{\cdot}zw = z$. Therefore, $yz = (zw \cdot yx)(wz \cdot xy) = (zw \cdot wz)(yx \cdot xy) = wx$. □

Theorem 2.24. *A groupoid Q is a quadratical quasigroup if and only if it satisfies* (1), (2), (7) *and* (10).

Proof. (⇒) This follows from Theorem 2.2.
(⇐) Suppose that Q satisfies (1), (2), (7) and (10). By Theorem 2.21, it satisfies (4). By Theorem 2.20 it is a quadratical quasigroup. □

Theorem 2.25. *A left* (*or right*) *distributive groupoid satisfying* (3) *and* (10) *has the property A.*

Proof. Since in a left distributive groupoid $y \cdot zx = yz \cdot yx$, $zx \cdot yz = yx \cdot y = xy \cdot x$. Similarly, in a right distributive groupoid. □

Theorem 2.26. *In a quadratical quasigroup $x \cdot yz = xy \cdot z$ if and only if $x = z$.*

Proof. (⇒) Using Theorem 2.2, $x \cdot yz = xy \cdot z$ implies $xy \cdot xz = xz \cdot yz$ implies $yz \cdot xy = (xz)^2 = xz = zx \cdot z$ implies $xz = zx \cdot z$ implies $x = zx$ implies $x = z$.
(⇐) By Theorem 2.2, a quadratical quasigroup is elastic and so $x \cdot yx = xy \cdot x$. □

Definition 2.27. A groupoid is *nowhere commutative* if $xy = yx$ implies $x = y$.

Theorem 2.28. *Quadratical quasigroups are nowhere commutative.*

Proof. Since by Theorem 2.2, quadratical quasigroups are alterable and idempotent, $xy = yx$ implies $y^2 = x^2$ implies $y = x$. □

Theorem 2.29. *A groupoid Q is a quadratical quasigroup if and only if it satisfies* (4), (5) *and* (10).

Proof. (⇒) This follows from Theorem 2.2.
(⇐) By Theorem 2.7, Q is idempotent. Therefore, by Theorem 2.14 we need only show that Q is medial. Observe that by Theorems 2.11 and 2.25, this groupoid has the property A. Hence, $wx{\cdot}w = zw{\cdot}xz = yw{\cdot}xy$ and, using (10), $xz{\cdot}yw = xy{\cdot}zw$. So it is medial. □

As a consequence of the above results we obtain

Theorem 2.30. *The class of all quadratical quasigroups form a variety uniquely defined by*

- (A), (3), (4), (7), *or*
- (1), (4), (7), *or*
- (2), (4), (7), *or*
- (4), (5), (10).

Definition 2.31. A subset I of a groupoid Q is a *right* (*left*) *ideal* of Q if $ig \in I$ ($gi \in I$) for all $i \in I$ and all $g \in Q$. The subset I is called an *ideal* if it is a right ideal and a left ideal. A groupoid Q is *simple* (*right simple; left simple*) if for every ideal (right ideal; left ideal) I of Q, $I = Q$.

Theorem 2.32. *Groupoids satisfying* (4) *are right simple and left simple groupoids.*

Proof. Suppose that I is a right or left ideal of a groupoid Q satisfying (4). Let $i \in I$ and $g \in Q$. Then, $g = ig \cdot gi \in I$ and so $I = Q$. □

Corollary 2.33. *Quadratical quasigroups are right and left simple.*

3. Cycles in quadratical quasigroups

Let Q be a quadratical quasigroup with $a, b \in Q$ and $a \neq b$. Suppose that $C = \{x_1, x_2, \ldots, x_n\} \subseteq Q$ consists of n distinct elements, such that $aba = x_1x_2 = x_2x_3 = x_3x_4 = \ldots = x_{n-1}x_n = x_nx_1$. Then C will be called an (*ordered*) *n-cycle based on aba*. Note that $x_1 \neq aba$, or else $x_1 = x_2 = \ldots = x_n = aba$. Note also that if $C = \{x_1, x_2, x_3, \ldots, x_n\} \subseteq Q$ is an n-cycle based on aba, then so is $C_i = \{x_i, x_{(i+1) mod\, n}, x_{(i+2) mod\, n}, \ldots, x_{(i+n-1) mod\, n}\}$.

Proposition 3.1. *If n-cycles exist in a quadratical quasigroup then $n = 4$.*

Proof. Since $aba = x_nx_1 = x_1x_2 = x_2x_3$, by (10) $x_1 = x_2x_n$ and $x_2 = x_3x_1$. Now $x_3 \cdot x_2x_4 = x_3x_2 \cdot x_3x_4 = x_3x_2 \cdot aba = (x_3 \cdot aba)(x_2 \cdot aba)$. But by (10), $aba \cdot x_2 = x_3 \cdot aba$ and so $x_3 \cdot x_2x_4 = (x_3 \cdot aba)(x_2 \cdot aba) = (aba \cdot x_2)(x_2 \cdot aba) = x_2 = x_3x_1$. Hence, by cancellation, $x_1 = x_2x_4 = x_2x_n$ and so $x_4 = x_n$. □

Proposition 3.2. *Let Q be a quadratical quasigroup with $a, b \in Q$ and $a \neq b$. Then every element $x_1 \neq aba$ of Q is a member of a 4-cycle based on aba.*

Proof. Let $a, b \in Q$ and $a \neq b$. Suppose that $x_1 \neq aba$ for some $x_1 \in Q$. Using right solvability, we can solve the equations $aba = x_1x$, $aba = xy$, $aba = yz$ and $aba = zw$. If we define $x_2 = x$, $x_3 = y$, $x_4 = z$ and $x_5 = w$, then $aba = x_1x_2 = x_2x_3 = x_3x_4 = x_4x_5$. Using (10), $x_4 = x_5x_3$ and $x_5x_1 = x_2x_4 = x_2 \cdot x_5x_3 = x_2x_5 \cdot x_2x_3 = x_2x_5 \cdot aba$. Therefore, by (10), $aba \cdot x_5 = x_1 \cdot x_2x_5 = x_1x_2 \cdot x_1x_5 = aba \cdot x_1x_5$. Hence $x_5 = x_1x_5$ and $x_1 = x_5$. So we have proved that $\{x_1, x_2, x_3, x_4\}$ is a 4-cycle based on aba. □

Proposition 3.3. *Let C and D be two 4-cycles based on aba $(a \neq b)$ in a quadratical quasigroup. Then either $C = D$ or $C \cap D = \emptyset$.*

Proof. Suppose that $C = \{x_1, x_2, x_3, x_4\}$ and $D = \{y_1, y_2, y_3, y_4\}$. If $x_1 = y_1$, then $aba = x_1x_2 = y_1y_2 = x_1y_2$ and so $x_2 = y_2$. Then, $aba = x_2x_3 = y_2x_3 = y_2y_3$ and so $x_3 = y_3$. Finally, $aba = x_3x_4 = y_3x_4 = y_3y_4$ and $x_4 = y_4$. Hence, $C = D$. Similarly, if $x_1 = y_2$, then we can prove that $x_2 = y_3$, $x_3 = y_4$ and $x_4 = y_1$ and $C = D$. Similarly, if $x_1 \in \{y_3, y_4\}$ it is straightforward to prove that $C = D$.

The proofs that $C = D$ if $x_2 \in D$ or $x_3 \in D$ or $x_4 \in D$ are similar. □

Proposition 3.4. *Any finite quadratical quasigroup has order $m = 4t + 1$ for some $t \in \{0, 1, 2, \ldots\}$.*

Proof. A finite quadratical quasigroup consists of the element aba and the union of its disjoint 4-cycles based on aba. By definition, no cycle contains the element aba. The proposition is therefore valid. □

So, later we will assume that $m = 4t + 1$ for some natural t.

4. Existence of quadratical quasigroups

We start with the following theorem proved in [1].

Theorem 4.1. *A groupoid $(G, \cdot)$ is a quadratical quasigroup if and only if there exists a commutative group $(G, +)$ in which for every $a \in G$ the equation $z + z = a$ has a unique solution $z = \frac{1}{2}a \in G$, and two its automorphisms φ, ψ such that for all $x, y \in G$ we have*

$$x \cdot y = \varphi(x) + \psi(y), \tag{12}$$

$$\varphi(x) + \psi(x) = x, \tag{13}$$

$$2\psi\varphi(x) = x. \tag{14}$$

From the proof of this theorem it follows that $\varphi\psi = \psi\varphi$. So, if $\varphi \neq \psi$, then $(G, +)$ induces two quadratical quasigroups: $G = (G, \cdot)$ and its dual $G^* = (G, \circ)$, where $x \circ y = y \cdot x$. Clearly, in any case $G \neq G^*$ since $x \circ y = x \cdot y$ means that $(G, \cdot)$ is commutative which together with the basic identity (A) gives $xy \cdot x = zx \cdot yz = xz \cdot yz = xy \cdot z$. This implies $x = z$, a contradiction. Since, G and G^*, by (12), are isotopic to the same group, they are isotopic too. Moreover, from Theorem 3.3 in [2] it follows that *all parastrophes of a quadratical quasigroup are isotopic.*

Corollary 4.2. *There are no quadratical quasigroups with left (right) neutral element.*

Proof. If e is a left neutral element then $x = e \cdot x = \varphi(e) + \psi(x)$. Since $\psi(x) = x - \varphi(e)$ is an automorphism of a group $(Q, +)$, we have $(x + y) - \varphi(e) = \psi(x + y) = \psi(x) + \psi(y) = (x + y) - 2\varphi(e)$, which implies $\varphi(e) = 0$. Thus $\psi(x) = x$, consequently, by (13), $\varphi(x) = 0$ for every $x \in Q$, a contradiction.

Analogously for quasigroups with a right neutral element. □

Corollary 4.3. *There are no quadratical quasigroups that are loops or groups.*

Corollary 4.4. *If a quadratical quasigroup Q is induced by groups $(Q,+)$ and $(Q,\circ)$, then these groups are isomorphic.*

Proof. Indeed, $x\cdot y=\varphi(x)+\psi(y)=\alpha(x)\circ\beta(y)$. Thus, $\varphi\alpha^{-1}(x)+\psi\beta^{-1}(y)=x\circ y$. So, groups $(Q,+)$ and $(Q,\circ)$ are isotopic. Thus, by Albert's theorem, they are isomorphic. □

Corollary 4.5. *Quadratical quasigroups are isotopic if and only if they are induced by isomorphic groups.*

Proof. Let quadratical quasigroups Q_1 and Q_2 be induced by groups $(Q_1,*_1)$ and $(Q_2,*_2)$, respectivety. If quasigroups Q_1 and Q_2 are isotopic, then groups $(Q_1,*_1)$ and $(Q_2,*_2)$ also are isotopic, and consequently, they are isomorphic. □

Corollary 4.6. *Quadratical quasigroups induced by the same group are isotopic.*

Corollary 4.7. *Quadratical quasigroups of the same prime order are isotopic.*

Theorem 4.8. *A quadratical groupoid induced by the additive group $\mathbb{Z}_m$ has the form*

$$x\cdot y=ax+(1-a)y\,, \tag{15}$$

where $a\in\mathbb{Z}_m$ *and*

$$2a^2-2a+1=0. \tag{16}$$

Proof. First observe that in the additive group $\mathbb{Z}_m$, where $m=4t+1$, for every $b\in\mathbb{Z}_m$ there exists $z\in\mathbb{Z}_m$ such that $z+z=b$. Indeed, if b is even, then obviously $z=\frac{1}{2}b\in\mathbb{Z}_m$. If b is odd, then $1+b$ is even and $z+z=b+4t+1$ for $z=2t+\frac{1+b}{2}\in\mathbb{Z}_m$.

In $\mathbb{Z}_m$ the equation (16) has the form $2a(a-1)+1=0=km$. Let d be a positive common divisor of a and m. Since m is odd, d also is odd and $d|(2a(a-1)+1)$. Consequently, $d|1$. Hence $(a,m)=1$. Analogously we can see that $(a-1,m)=1$. So, for any a satisfying (16) we have $(a,m)=(1-a,m)=1$. Thus the maps $\varphi(x)=ax$ and $\psi(x)=(1-a)x$, where $a\in\mathbb{Z}_m$ satisfies (16), are automorphisms of the additive group $\mathbb{Z}_m$ and satisfy (13), which in this case is equivalent to (15). Since (14) is equivalent to (16), a quasigroup defined by (15) is quadratical. □

Corollary 4.9. *A groupoid induced by $\mathbb{Z}_m$ by* (15) *is quadratical if and only if its dual groupoid with the operation*

$$x\cdot y=(1-a)x+ay \tag{17}$$

is quadratical.

Proof. Indeed, as it is not difficult to see a satisfies (16) if and only if (16) is satisfied by $1-a$. So, a and $1-a$ are roots of the polynomial $w(x)=2x^2-2x+1$. If $a=1-a$, then $w(x)=2(x-a)^2=2x^2-4ax+2a^2$. Hence $2a=1$ and $2a^2=1$. Thus, $1=4a^2=2$. Obtained contradiction shows that $a\neq 1-a$. Thus, (15) and (17) define two different quadratical quasigroups. □

Theorem 4.10. *If $m=4t+1$ is prime, then the additive group $\mathbb{Z}_m$ induces exactly two quadratical groupoids. They have form*

$$x\circ_1 y=a_1x+a_2y \qquad\text{and}\qquad x\circ_2 y=a_2x+a_1y,$$

where $a_1=2t+1+s$, $a_2=2t+1-s$ and $s^2\equiv t(\operatorname{mod} m)$.

Proof. By the Lagrange theorem (cf. [4]), the equation $2a^2-2a+1\equiv 0(\operatorname{mod} m)$ has no more than two solutions in $\mathbb{Z}_m$. $(\mathbb{Z}_m,+,\cdot)$ is a field, so these solutions have the form $a_1=\frac{1}{2}+\sqrt{t}$ and $a_1=\frac{1}{2}-\sqrt{t}$. Since in this field $\frac{1}{2}$ is equal to $2t+1$ and $\sqrt{t}\in\mathbb{Z}_m$ for each $t\in\mathbb{Z}_m$, we have $a_1=2t+1+s$ and $a_2=2t+1-s$, where $s^2\equiv t(\operatorname{mod} m)$. Obviously $a_1\neq a_2$ and $(a_1,m)=(a_2,m)=1$. Theorem 4.8 completes the proof. □

Theorem 4.11. *There are no quadratical quasigroups of order $m=p_1p_2\cdots p_k$, where p_i are different odd primes such that at least one $p_j\equiv 3(\operatorname{mod} 4)$.*

Proof. Indeed, all groups of such order are isomorphic to the additive group $\mathbb{Z}_m$. Since any automorphism of the group $\mathbb{Z}_m$ has the form $\varphi(x)=ax$, by Theorem 4.8, a quadratical quasigroup induced by this group has the form (15), where a satisfies (16).

The equation (16) is equivalent to the equation $4a^2-4a+2=0(\operatorname{mod} m)$, i.e., to the equation $(2a-1)^2+1=0(\operatorname{mod} m)$. In the ring $\mathbb{Z}_m$ the last equation can be written in the form $x^2\equiv(-1)(\operatorname{mod} m)$, where $x=2a-1$. The equation $x^2\equiv(-1)(\operatorname{mod} m)$ has a solution only in the case when each prime divisor p of m has the property $p\equiv 1(\operatorname{mod} 4)$ (cf. [4]). So, if some prime $p_j|m$ and $p_j\equiv 3(\operatorname{mod} 4)$, then this group cannot induce quadratical quasigroups. □

Corollary 4.12. *There are no quadratical quasigroups of order* $21,33,57,69,77,93,105,129,\ldots$

Theorem 4.13. *A commutative group of order $m=p_1p_2\cdots p_n$, where $p_1,\ldots,p_n$ are different primes such that $p_i\equiv 1(\text{mod }4)$, induces 2^n different quadratical quasigroups.*

Proof. Such groups are isomorphic to the additive group $\mathbb{Z}_m$. Quadratical quasigroups defined on this group have the form (15), where a satisfies (16). The number of solutions of the equation $f(x)\equiv 0(\text{mod }m)$ is equal to $T_1T_2\cdots T_n$, where T_i denotes of the number of solutions of the equation $f(x)\equiv 0(\text{mod }p_i)$ (cf. [4]). But for $f(x)=2x^2-2x+1$ the last equation has exactly two solutions (Theorem 4.10). Thus, $f(x)\equiv 0(\text{mod }m)$ has exactly 2^n solutions. Consequently, it defines 2^n quadratical quasigroups. □

Each finite commutative group is isomorphic to a direct product of cyclic groups. For simplicity consider the case when a commutative group G of order $m = 4t+1$ is a direct product of two groups $\mathbb{Z}_{m_1}$ and $\mathbb{Z}_{m_2}$. If $m_1 \neq m_2$, then each automorphism φ of G has the form $\varphi(x,y) = (\varphi_1(x), \varphi(x_2))$, where φ_i is an automorphism of the group $\mathbb{Z}_{m_i}$ because any automorphism saves the order of each element, so $\varphi(\mathbb{Z}_{m_1} \times \{0\}) = \mathbb{Z}_{m_1} \times \{0\}$. Thus, in this case, quadratical quasigroups induced by G are direct products of quadratical quasigroups induced by groups $\mathbb{Z}_{m_i}$.

Theorem 4.14. *The group $\mathbb{Z}_m$ induces a quadratical quasigroup if and only if $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where p_i are different primes such that $p_i \equiv 1(\operatorname{mod} 4)$ for all $i = 1, 2, \ldots, n$.*

Proof. Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where p_i are different primes. Then obviously $\mathbb{Z}_m = \mathbb{Z}_{p_1^{\alpha}} \times \mathbb{Z}_{p_1^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_n^{\alpha_n}}$. Any automorphism of this group has the form $\varphi(x_1, x_2, \ldots, x_n) = a(x_1, x_2, \ldots, x_n) = (ax_1, ax_2, \ldots, ax_n)$. So, the equation (16), i.e., $2a^2 - 2a + 1 \equiv 0(\operatorname{mod} m)$ has a solution if and only if each of equations $2a^2 - 2a + 1 \equiv 0(\operatorname{mod} p_i^{\alpha_i})$ has a solution. The last equation is solved only in the case when $2a^2 - 2a + 1 \equiv 0(\operatorname{mod} p_i)$ is solved (cf. [4]), but it is possible if and only if $p_i \equiv 1(\operatorname{mod} 4)$. □

Corollary 4.15. *If there exists a prime $p|m$ such that $p \equiv 3(\operatorname{mod} 4)$, then there are no quadratical quasigroups induced by the group $\mathbb{Z}_m$.*

Below are listed all quadratical quasigroups of the form $x \cdot y = ax + by(\text{mod } m)$, where $a < b$, defined on the group $\mathbb{Z}_m$ for $m < 400$. Dual quasigroups $x \circ y = bx + ay(\text{mod } m)$ are omitted.

m	a	b
5	2	4
13	3	11
17	7	11
25	4	22
29	9	21
37	16	22
41	5	37
53	12	42
61	6	56
65	24	42
	29	37
73	14	60
85	7	79
	24	62
89	28	62
97	38	60
101	46	56
109	17	93
113	8	106
125	29	97
137	19	119
145	9	137
	67	79
149	53	97
157	65	93
169	50	120
173	47	127
181	10	172
185	22	164
	59	127
193	41	153
197	92	106
205	37	169
	87	119
221	11	211
	24	198
229	54	176
233	45	189
241	89	153
257	121	137
265	12	254
	42	224
269	94	176
277	109	169
281	27	255
289	126	164
293	78	216
305	67	239
	117	189
313	13	301
317	102	216
325	29	297
	154	172
337	95	243
349	107	243
353	156	198
365	14	352
	87	279
373	135	239
377	50	328
	154	224
389	58	332
397	32	366

The case when finite commutative group is isomorphic to a direct product of cyclic groups of the same order is more complicated. Suppose for simplicity that $G=\mathbb{Z}_n\times\mathbb{Z}_n$ for some natural $n>1$. Then G can be considered as a module or a vector space $\mathbb{Z}_n\times\mathbb{Z}_n$ over $\mathbb{Z}_n$. So, automorphisms of this group can be calculated as linear maps of $\mathbb{Z}_n\times\mathbb{Z}_n$. From Theorem 4.1 it follows that the matrices of these maps satisfy the equation $2A(A-I)+I=\theta$, where I and θ are the identity and zero matrices. Obviously, if A satisfies this equation then $B=A-I$ also satisfies this equation and $A+B=I$. Hence $(x,y)*(z,u)=A(x,y)+B(z,u)$ and $(x,y)\circ(z,u)=B(x,y)+A(z,u)$ are dual quasigroups.

Case $m=9$.
Direct computations shows that for $\mathbb{Z}_3\times\mathbb{Z}_3$ we have six such quasigroups (cf. [1]). These quasigroups are defined by maps with the following matrices:

$$A_1=\begin{bmatrix}0&1\\1&1\end{bmatrix},\ A_2=\begin{bmatrix}0&2\\2&1\end{bmatrix},\ A_3=\begin{bmatrix}2&1\\2&2\end{bmatrix}\text{ and } B_i=A_i-I.$$

Case $m=25$.
Using a similar argument we can see that the group $G=\mathbb{Z}_5\times\mathbb{Z}_5$ induces 16 quadratical quasigroups $(G,*_i)$ with the operation

$$(x,y)*_i(z,u)=A_i(x,y)+B_i(z,u)\tag{18}$$

and 16 quasigroups dual to the above. These quasigroups are determined by matrices A_i:

$$\begin{bmatrix}0&a\\b&1\end{bmatrix},\ \begin{bmatrix}2&0\\0&2\end{bmatrix},\ \begin{bmatrix}2&c\\d&4\end{bmatrix},\ \begin{bmatrix}3&1\\1&3\end{bmatrix},\ \begin{bmatrix}3&3\\2&3\end{bmatrix},$$

where $ab=2(\text{mod}\,5)$ and $cd=0(\text{mod}\,5)$.

Case $m=45$.
Commutative groups of order $m=45$ are isomorphic to $\mathbb{Z}_{45}$, $\mathbb{Z}_3\times\mathbb{Z}_{15}$, $\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_5$ or $\mathbb{Z}_9\times\mathbb{Z}_5$. Groups $\mathbb{Z}_3$, $\mathbb{Z}_9$ and $\mathbb{Z}_{45}$ do not induce quadratical quasigroups. Therefore, from the above groups only $\mathbb{Z}_\times\mathbb{Z}_3\times\mathbb{Z}_5$ induces such quasigroups. These quasigroups are a direct product of quadratical quasigroups induced by $\mathbb{Z}_3\times\mathbb{Z}_3$ and $\mathbb{Z}_9$. So, they have the form

$$(x_1,y_1,z_1)*_i(x_2,y_2,z_2)=(A_i(x_1,y_1)+B_i(x_2,y_2),a_iz_1+b_iz_2),$$

where A_i,B_i are as in the above and a_i is equal to 2 or to 4. We have 12 such quasigroups.

Case $m=49$.
By Theorem 4.11 the group $\mathbb{Z}_{49}$ do not induce any quadratical quasigroups. The group $\mathbb{Z}_7\times\mathbb{Z}_7$ induces 21 quadratical quasigroups defined by (18) and 21 duals. These quasigroups are determined by matrices A_i:

$$\begin{bmatrix}0&a\\b&1\end{bmatrix},\ \begin{bmatrix}2&c\\d&6\end{bmatrix},\ \begin{bmatrix}3&e\\f&5\end{bmatrix},\ \begin{bmatrix}4&1\\5&4\end{bmatrix},\ \begin{bmatrix}4&2\\6&4\end{bmatrix},\ \begin{bmatrix}4&3\\4&4\end{bmatrix},$$

where $ab = 3(\bmod 7)$, $cd = 1(\bmod 7)$ and $ef = 4(\bmod 7)$.

Case $m = 65$.
Quadratical quasigroups induced by $\mathbb{Z}_{65} = \mathbb{Z}_5 \times \mathbb{Z}_{13}$ are direct products of quadratical quasigroups induced by $\mathbb{Z}_5$ an $\mathbb{Z}_{13}$. So, they have the form

$$\begin{aligned}
&(x, y) *_1 (z, u) = (2x + 4z, 3y + 11u),\\
&(x, y) *_2 (z, u) = (4x + 2z, 11y + 3u),\\
&(x, y) *_3 (z, u) = (2x + 4z, 11y + 3u),\\
&(x, y) *_4 (z, u) = (4x + 2z, 3y + 11u).
\end{aligned}$$

Obviously $(G, *_1)$ and $(G, *_2)$, also $(G, *_3)$ and $(G, *_4)$, are dual and are isomorphic to quasigroups mentioned in the above table for $\mathbb{Z}_{65}$.

Case $m = 81$.
Commutative groups of order $m = 81$ are isomorphic to one of groups $\mathbb{Z}_{81}$, $\mathbb{Z}_9 \times \mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_{27}$, $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. By Corollary 4.15 groups $\mathbb{Z}_3$, $\mathbb{Z}_9$, $\mathbb{Z}_{27}$, $\mathbb{Z}_{81}$ do not induce quadratical quasigroups. Thus quadratical quasigroups of order 81 can be induced by groups $\mathbb{Z}_9 \times \mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ only. The group $\mathbb{Z}_9 \times \mathbb{Z}_9$ induces 27 quadratical quasigroups defined by (18) and 27 duals. These quasigroups are determined by matrices A_i:

$$\begin{bmatrix} 0 & a \\ b & 1 \end{bmatrix}, \begin{bmatrix} 2 & c \\ d & 8 \end{bmatrix}, \begin{bmatrix} 3 & e \\ f & 7 \end{bmatrix}, \begin{bmatrix} 4 & g \\ h & 6 \end{bmatrix}, \begin{bmatrix} 5 & 1 \\ 2 & 5 \end{bmatrix}, \begin{bmatrix} 5 & 2 \\ 1 & 5 \end{bmatrix}, \begin{bmatrix} 5 & 4 \\ 5 & 5 \end{bmatrix},$$

where $ab = 4(\bmod 9)$, $cd = 2(\bmod 9)$, $ef = 7(\bmod 9)$ and $gh = 1(\bmod 9)$.

Using a computer we can see that the group $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ induces 2106 quadratical quasigroups defined by (18) and 2106 duals. So, this group defines 4212 quadratical quasigroups.

Case $m = 125$.
Commutative groups of order $m = 125$ are isomorphic to one of the groups $\mathbb{Z}_{125}$, $\mathbb{Z}_5 \times \mathbb{Z}_{25}$ or $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. The first group induces only two quadratical quasigroups, the second induces 64. Using a computer we can see that the last group induces 1552 quadratical quasigroups. So in the case $m = 125$ we have 1618 such quasigroups.

It is not difficult to observe that if p is prime and $p \equiv 1(\text{mod } 4)$ then the group $(\mathbb{Z}_p)^k$ induces quadratical quasigroups for every k, but for $p \equiv 3(\text{mod } 4)$ it induces quadratical quasigroups only for even k.

Theorem 4.16. *There are no quadratical quasigroups induced by the additive groups $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.*

Proof. In $\mathbb{Z}$ there are no x such that $x + x = 1$, so, by Theorem 4.1 such a group cannot induce quadratical quasigroups. Automorphisms of the group $(\mathbb{Q}, +)$ have the form $\varphi(x) = ax$ for some $0 \neq a \in \mathbb{Q}$. Obviously $\psi(x) = (1 - a)x$ for $a \neq 1$, also is an automorphism and φ, ψ satisfy (13). Then (14) gives (16), which is equivalent to $(2a-1)^2+1=0$. So, $a=\frac{1}{2}(1+i)$ or $a=\frac{1}{2}(1-i)$. These elements are not in $\mathbb{Q}$. Since for each automorphism φ of $(\mathbb{R},+)$ there is $a\in\mathbb{R}-\{0\}$ such that $\varphi(x)=ax$ for $x\in\mathbb{Q}$, each automorphism of $(\mathbb{R},+)$ defining a quadratical quasigroup satisfies (14), i.e., a satisfies (16). But in this case $a\notin\mathbb{R}$. □

Corollary 4.17. *The smallest quadratical quasigroup of infinite order is defined on the additive group* $\mathbb{Q}[i]=\{u+vi\,|\,u,v\in\mathbb{Q}\}$ *and has the form* $xy=ax+(1-a)y$, *where* $a=\frac{1}{2}(1+i)$ *or* $a=\frac{1}{2}(1-i)$.

References

[1] **W.A. Dudek**, *Quadratical quasigroups*, Quasigroups and Related Systems **4** (1997), 9 − 13.

[2] **W.A. Dudek**, *Parastrophes of quasigroups*, Quasigroups and Related Systems **23** (2015), 221 − 230.

[3] **M. Polonijo**, *A note on Ward quasigroups*, An. Ştiinţ. Univ. Al. I. Cuza Iaşi. Secţ. I a Mat. (N.S.), **32** (1986), no. 2, 5 − 10.

[4] **I.M. Vinogradov**, *Foundations of the theory of numbers*, (Russian), Nauka, Moscow, 1965.

[5] **V. Volenec**, *Quadratical groupoids*, Note di Matematica **13** (1993), no. 1, 107 − 115.

[6] **V. Volenec**, *Squares in quadratical quasigroups*, Quasigroups and Related Systems **7** (2000), 37 − 44.

[7] **V. Volenec and R. Kolar-Šuper**, *Skewsquares in quadratical quasigroups*, Comment. Math. Univ. Carolin. **49** (2008), 397 − 410.

[8] **V. Volenec and R. Kolar-Šuper**, *Parallelograms in quadratical quasigroups*, Quasigroups and Related Systems **18** (2010), 229 − 240.

Received February 23, 2016
Revised September 20, 2016

W.A. Dudek
Faculty of Pure and Applied Mathematics, Wroclaw University of Science and Technology
50-370 Wroclaw, Poland
Email: wieslaw.dudek@pwr.edu.pl

R.A.R. Monzo
Flat 10, Albert Mansions, Crouch Hill, London N8 9RE, United Kingdom
E-mail: bobmonzo@talktalk.net

On $(\mathbf{i},\mathbf{j})$-commutativity in Menger algebras of n-place functions

Wieslaw A. Dudek and *Valentin S. Trokhimenko*

Abstract. We present an abstract characterization of Menger $(2,n)$-semigroups of n-place functions containing the operation $\pi_{ij}\colon f(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n)\mapsto f(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$.

1. Introduction

On the set $\mathcal{F}(A^n,A)$ of all partial n-place functions $f\colon A^n\to A$ $(n\geqslant 2)$ one can consider the following operations:

- the $(n+1)$-ary *Menger's superposition* $\mathcal{O}\colon(f,g_1,\ldots,g_n)\mapsto f[g_1\ldots g_n]$ such that

$$f[g_1\ldots g_n](a_1^n)=f(g_1(a_1^n),g_2(a_1^n),\ldots,g_n(a_1^n)),$$

- the binary *Mann's superpositions* $\underset{1}{\oplus},\underset{2}{\oplus},\ldots,\underset{n}{\oplus}$ defined by

$$(f\underset{i}{\oplus}g)(a_1^n)=f(a_1^{i-1},g(a_1^n),a_{i+1}^n),$$

where a_i^j denotes the sequence $a_i,a_{i+1},\ldots,a_{j-1},a_j$ if $i\leqslant j$, and the empty symbol if $i>j$.

Let Φ be a nonempty subset of $\mathcal{F}(A^n,A)$. If Φ is closed with respect to the Menger superposition, then the algebra $(\Phi,\mathcal{O})$ is called a *Menger algebra of n-place functions*. Since each Mann's superposition is an associative operation, the algebra $(\Phi,\underset{1}{\oplus},\underset{2}{\oplus},\ldots,\underset{n}{\oplus})$ is called a *$(2,n)$-semigroup of n-place functions*. Consequently, the algebra $(\Phi,\mathcal{O},\underset{1}{\oplus},\underset{2}{\oplus},\ldots,\underset{n}{\oplus})$ is called a *Menger $(2,n)$-semigroup of n-place functions*.

One can prove (cf. [3] or [8]) that an abstract $(n+1)$-ary algebra (G,o) is isomorphic to some algebra $(\Phi,\mathcal{O})$ of n-place functions if and only if it satisfies the *superassociative law*:

$$x[y_1\ldots y_n][z_1\ldots z_n]=x[y_1[z_1\ldots z_n]\ldots y_n[z_1\ldots z_n]],\tag{1}$$

2010 Mathematics Subject Classification: 20N15
Keywords: Menger algebra, $(2,n)$-semigroup, n-place function, (i,j)-commutativity.

where $x[y_1 \dots y_n]$ denotes $o(x, y_1, \dots, y_n)$. An $(n+1)$-ary algebra (G, o) satisfying this law is called a *Menger algebra of rank* n. An algebra $(G, \underset{1}{\oplus}, \underset{2}{\oplus}, \dots, \underset{n}{\oplus})$ with n binary associative operations $\underset{1}{\oplus}, \underset{2}{\oplus}, \dots, \underset{n}{\oplus}$ is called a $(2,n)$*-semigroup*. A $(2,n)$-semigroup closed with respect to an $(n+1)$-ary operation o satisfying (1) is called a *Menger* $(2,n)$*-semigroup* and is denoted by $(G, o, \underset{1}{\oplus}, \underset{2}{\oplus}, \dots, \underset{n}{\oplus})$.

For simplicity, all expressions of the form $(\cdots((x \underset{i_1}{\oplus} y_1) \underset{i_2}{\oplus} y_2) \cdots) \underset{i_k}{\oplus} y_k$ will be denoted by $x \overset{i_k}{\underset{i_1}{\oplus}} y_1^k$. In the case when $i = i_k$ and $i \notin \{i_1, \dots, i_{k-1}\}$ for some $k \in \{1, \dots, s\}$, the expression $x_k \overset{i_s}{\underset{i_{k+1}}{\oplus}} x_{k+1}^s$ will be written in the form $\mu_i(\overset{i_s}{\underset{i_1}{\oplus}} x_1^s)$. In any other case $\mu_i(\overset{i_s}{\underset{i_1}{\oplus}} x_1^s)$ is the empty symbol. For example, $\mu_1(\underset{2}{\oplus} x \underset{1}{\oplus} y \underset{3}{\oplus} z) = y \underset{3}{\oplus} z$, $\mu_2(\underset{2}{\oplus} x \underset{1}{\oplus} y \underset{3}{\oplus} z) = x \underset{1}{\oplus} y \underset{3}{\oplus} z$, $\mu_3(\underset{2}{\oplus} x \underset{1}{\oplus} y \underset{3}{\oplus} z) = z$. The symbol $\mu_4(\underset{2}{\oplus} x \underset{1}{\oplus} y \underset{3}{\oplus} z)$ is empty.

It is known (cf. [7] or [8]) that *an algebra* $(G, \underset{1}{\oplus}, \dots, \underset{n}{\oplus})$ *with* n *binary operations is isomorphic to some algebra* $(\Phi, \underset{1}{\oplus}, \dots, \underset{n}{\oplus})$ *of* n*-place functions if and only if for all* $g, x_i, y_j \in G$, $i = 1, \dots, s$, $j = 1, \dots, k$, *it satisfies the implication*

$$\bigwedge_{i=1}^{n} \Big(\mu_i(\overset{i_s}{\underset{i_1}{\oplus}} x_1^s) = \mu_i(\overset{j_k}{\underset{j_1}{\oplus}} y_1^k) \Big) \longrightarrow g \overset{i_s}{\underset{i_1}{\oplus}} x_1^s = g \overset{j_k}{\underset{j_1}{\oplus}} y_1^k, \tag{2}$$

where $i_1, \dots, i_s, j_1, \dots, j_k \in \{1, \dots, n\}$.

Note that the condition (2) implies the associativity of all binary operations $\underset{1}{\oplus}, \underset{2}{\oplus}, \dots, \underset{n}{\oplus}$. Indeed, for two expressions $\underset{i}{\oplus} y \underset{i}{\oplus} z$ and $\underset{i}{\oplus}(y \underset{i}{\oplus} z)$, where $y, z \in G$, we have $\mu_i(\underset{i}{\oplus} y \underset{i}{\oplus} z) = y \underset{i}{\oplus} z = \mu_i(\underset{i}{\oplus}(y \underset{i}{\oplus} z))$. For $k \neq i$ the symbols $\mu_k(\underset{i}{\oplus} y \underset{i}{\oplus} z)$ and $\mu_k(\underset{i}{\oplus}(y \underset{i}{\oplus} z))$ are empty. So, the premise of (2) is satisfied. Therefore for all $x \in G$ we have $x \underset{i}{\oplus} y \underset{i}{\oplus} z = x \underset{i}{\oplus}(y \underset{i}{\oplus} z)$, i.e., $(x \underset{i}{\oplus} y) \underset{i}{\oplus} z = x \underset{i}{\oplus}(y \underset{i}{\oplus} z)$.

An abstract characterization of Menger $(2,n)$-semigroup of n-place functions is more difficult. For such characterization we need to use the implication (2) and several identities. Namely, as it is proved in [6] (cf. also [8]), *an algebra* $(G, o, \underset{1}{\oplus}, \dots, \underset{n}{\oplus})$ *of type* $(n+1, 2, \dots, 2)$ *is isomorphic to some algebra* $(\Phi, \mathcal{O}, \underset{1}{\oplus}, \dots, \underset{n}{\oplus})$ *of* n*-place functions if and only if it satisfies* (1), (2) *and*

$$(x \underset{i}{\oplus} y)[z_1 \dots z_n] = x[z_1 \dots z_{i-1}\, y[z_1 \dots z_n]\, z_{i+1}, \dots, z_n]\,, \tag{3}$$

$$x[y_1 \dots y_n] \underset{i}{\oplus} z = x[(y_1 \underset{i}{\oplus} z) \dots (y_n \underset{i}{\oplus} z)]\,, \tag{4}$$

$$x \overset{i_s}{\underset{i_1}{\oplus}} y_1^s = x[\mu_1(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s)\ \dots\ \mu_n(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s)]\,, \tag{5}$$

where $i=1,2,\dots,n$ *and* $\{i_1,\dots,i_s\}=\{1,\dots,n\}$.

2. Menger $(2,n)$-semigroups

Algebras with one n-ary operation allowing certain permutations of variables were investigated by various authors (cf. for example [2, 9, 10, 12, 13]). Such n-ary algebras also are used to study the properties of some affine geometries (cf. [11]).

In this section we describe algebras on n-place functions allowing an exchange of variables at two fixed places. Namely, on the set $\mathcal{F}(A^n,A)$ we will consider the unary operation π_{ij} defined in the following way:

$$(\pi_{ij}f)(a_1^n)=f(a_1^{i-1},a_j,a_{i+1}^{j-1},a_i,a_{j+1}^n),$$

where $1\leqslant i<j\leqslant n$ are fixed and the left and right hand sides are defined or not defined simultaneously. The operation π_{ij} is called the *operation of* (i,j)-*commutativity.* Functions with the property $\pi_{ij}f=f$ are called (i,j)-*commutative*; functions with the property $\pi_{1n}f=f$ – *semicommutative.* Some n-ary algebras (G,f) in which the operation f is semicommutative are strongly connected with medial (entropic) algebras (cf. [4], [9]) and abelian groups (cf. [1] and [5]).

Let $(G,o,\underset{1}{\oplus},\dots,\underset{n}{\oplus},\pi_{ij})$ be an arbitrary algebra of type $(n+1,\overbrace{2,\dots,2}^{n},1)$, where, for simplicity, the unary operation is denoted by π_{ij}.

Theorem 1. *An algebra* $(G,o,\underset{1}{\oplus},\dots,\underset{n}{\oplus},\pi_{ij})$ *of type* $(n+1,2,\dots,2,1)$ *is isomorphic to the algebra* $(\Phi,\mathcal{O},\underset{1}{\oplus},\dots,\underset{n}{\oplus},\pi_{ij})$ *of partial n-place functions if and only if* $(G,o,\underset{1}{\oplus},\dots,\underset{n}{\oplus})$ *is a Menger* $(2,n)$*-semigroup satisfying the following identities:*

$$(\pi_{ij}\,x)[y_1\dots y_n]=x[y_1^{i-1}\,y_j\,y_{i+1}^{j-1}\,y_i\,y_{j+1}^n],\tag{6}$$

$$\pi_{ij}(x[y_1\dots y_n])=x[\pi_{ij}y_1\dots\pi_{ij}y_n],\tag{7}$$

$$\pi_{ij}(x\underset{k}{\oplus}y)=\begin{cases}(\pi_{ij}x)\underset{k}{\oplus}(\pi_{ij}y), & \textit{if } k\in\{1,\dots,n\}-\{i,j\},\\ (\pi_{ij}x)\underset{j}{\oplus}(\pi_{ij}y), & \textit{if } k=i,\\ (\pi_{ij}x)\underset{i}{\oplus}(\pi_{ij}y), & \textit{if } k=j,\end{cases}\tag{8}$$

$$\pi_{ij}^2x=x.\tag{9}$$

Proof. Let $(\Phi,\mathcal{O},\underset{1}{\oplus},\dots,\underset{n}{\oplus},\pi_{ij})$ be an arbitrary algebra of partial n-place functions $f\colon A^n\to A$. Then obviously $(\Phi,\mathcal{O},\underset{1}{\oplus},\dots,\underset{n}{\oplus})$ is a Menger $(2,n)$-semigroup. To prove that π_{ij} satisfies the conditions (6) – (9) consider $f,g_1,\dots,g_n\in\Phi$ and $a_1,\dots,a_n\in A$. Then

$$\begin{aligned}&(\pi_{ij}f)[g_1\dots g_n](a_1^n)=(\pi_{ij}f)(g_1(a_1^n),\dots,g_n(a_1^n))\\&=f(g_1(a_1^n),\dots,g_{i-1}(a_1^n),g_j(a_1^n),g_{i+1}(a_1^n),\dots,g_{j-1}(a_1^n),g_i(a_1^n),g_{j+1}(a_1^n),\dots,g_n(a_1^n))\\&=f[g_1\dots g_{i-1}g_jg_{i+1}\dots g_{j-1}g_ig_{j+1}\dots g_n](a_1^n)=f[g_1^{i-1}g_jg_{i+1}^{j-1}g_ig_{j+1}^n](a_1^n),\end{aligned}$$

which proves (6).

Similarly, we can see that

$$\begin{aligned}\pi_{ij}(f[g_1\dots g_n])(a_1^n)&=f[g_1\dots g_n](a_1^{i-1},a_j,a_{i+1}^{j-1},a_i,a_{j+1}^n)\\&=f(g_1(a_1^{i-1},a_j,a_{i+1}^{j-1},a_i,a_{j+1}^n),\dots,g_n(a_1^{i-1},a_j,a_{i+1}^{j-1},a_i,a_{j+1}^n))\\&=f(\pi_{ij}g_1(a_1^n),\dots,\pi_{ij}g_n(a_1^n))=f[\pi_{ij}g_1\dots\pi_{ij}g_n](a_1^n).\end{aligned}$$

This proves (7).

To prove (8) we must consider three cases: $k\in\{1,\dots,n\}-\{i,j\}$, $k=i$ and $k=j$. In the first case we have three subcases:

$$1\leqslant k<i<j\leqslant n,\quad 1\leqslant i<k<j\leqslant n,\quad 1\leqslant i<j<k\leqslant n.$$

In the first subcase:

$$\begin{aligned}\pi_{ij}(f\underset{k}{\oplus}g)(a_1^n)&=f\underset{k}{\oplus}g(a_1^{i-1},a_j,a_{i+1}^{j-1},a_i,a_{j+1}^n)\\&=f(a_1^{k-1},g(a_1^{i-1},a_j,a_{i+1}^{j-1},a_i,a_{j+1}^n),a_{k+1}^{i-1},a_j,a_{i+1}^{j-1},a_i,a_{j+1}^n)\\&=\pi_{ij}f(a_1^{k-1},\pi_{ij}g(a_1^n),a_{k+1}^n)=(\pi_{ij}f)\underset{k}{\oplus}(\pi_{ij}g)(a_1^n).\end{aligned}$$

The remaining two subcases can be verified analogously.

In the case $k=i$ we have

$$\begin{aligned}\pi_{ij}(f\underset{i}{\oplus}g)(a_1^n)&=f\underset{i}{\oplus}g(a_1^{i-1},a_j,a_{i+1}^{j-1},a_i,a_{j+1}^n)\\&=f(a_1^{i-1},g(a_1^{i-1},a_j,a_{i+1}^{j-1},a_i,a_{j+1}^n),a_{i+1}^{j-1},a_i,a_{j+1}^n)\\&=\pi_{ij}f(a_1^{j-1},\pi_{ij}g(a_1^n),a_{j+1}^n)=(\pi_{ij}f)\underset{j}{\oplus}(\pi_{ij}g)(a_1^n).\end{aligned}$$

In a similar way we can verify the case $k=j$.

So the condition (8) is valid.

The condition (9) is obvious.

So, the algebra $(\Phi,\mathcal{O},\underset{1}{\oplus},\dots,\underset{n}{\oplus},\pi_{ij})$ satisfies all the conditions mentioned in the theorem.

Conversely, let $(G,o,\underset{1}{\oplus},\dots,\underset{n}{\oplus},\pi_{ij})$ be an arbitrary Menger $(2,n)$-semigroup with the unary operation π_{ij} satisfying the conditions (6) – (9). We will show that there exists an algebra of n-place functions λ_g and the mapping $P\colon g\mapsto\lambda_g$ such that $P\colon G\to\Phi=\{\lambda_g : g\in G\}$ is an isomorphism.

Consider the set $G^* = G \cup \{e_1, \ldots, e_n\}$, where $e_1, \ldots, e_n$ are different elements not belonging to G. For every $g \in G$ we define on G^* an n-place function λ_g putting

$$\lambda_g(x_1^n) = \begin{cases} g[x_1 \ldots x_n], & \text{if } \ x_1, \ldots, x_n \in G, \\ g, & \text{if } \ (x_1, \ldots, x_n) = (e_1, \ldots, e_n), \\ \pi_{ij} g, & \text{if } \ (x_1, \ldots, x_n) = (e_1^{i-1}, e_j, e_{i+1}^{j-1}, e_i, e_{j+1}^n), \\ g \overset{i_s}{\underset{i_1}{\oplus}} y_1^s, & \text{if } \ x_i = \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), \ i = 1, \ldots, n, \\ & \text{for some } y_1, \ldots, y_s \in G, \ \{i_1, \ldots, i_s\} \subset \{1, \ldots, n\}, \\ (\pi_{ij} g) \overset{i_s}{\underset{i_1}{\oplus}} y_1^s, & \text{if } \ x_i = \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_j = \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), \\ & x_k = \mu_k^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), \ k \in \{1, \ldots, n\} - \{i, j\}, \\ & y_1, \ldots, y_s \in G \ \text{ and } \{i_1, \ldots, i_s\} \subset \{1, \ldots, n\}, \end{cases}$$

where by $\mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} x_1^s)$ we denote the element of G^* such that

$$\mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} x_1^s) = \begin{cases} \mu_i(\overset{i_s}{\underset{i_1}{\oplus}} x_1^s) & \text{if } \ i \in \{i_1, \ldots, i_s\}, \\ e_i & \text{if } \ i \notin \{i_1, \ldots, i_s\}. \end{cases}$$

In other cases $\lambda_g(x_1^n)$ is not defined.

Note that, according to (2), in the above definition the value of $g \overset{i_s}{\underset{i_1}{\oplus}} y_1^s$ does not depends on $y_1, \ldots, y_s \in G$.

We shall prove that algebras $(G, o, \underset{1}{\oplus}, \ldots, \underset{n}{\oplus}, \pi_{ij})$ and $(\Phi, \mathcal{O}, \underset{1}{\oplus}, \ldots, \underset{n}{\oplus}, \pi_{ij})$, where $\Phi = \{\lambda_g \mid g \in G\}$, are isomorphic. For this consider the map $P \colon g \mapsto \lambda_g$.

• First we check that such defined P is a homomorphism of (G, o) onto $(\Phi, \mathcal{O})$, i.e., $P(g[g_1 \ldots g_n]) = P(g)[P(g_1) \ldots P(g_n)]$, or equivalently,

$$\lambda_{g[g_1 \ldots g_n]}(x_1^n) = \lambda_g[\lambda_{g_1} \ldots \lambda_{g_n}](x_1^n)$$

for all $g, g_1, \ldots, g_n \in G$ and $x_1, \ldots, x_n \in G^*$.

1) Let $x_1, \ldots, x_n \in G$. Then, in view of (3), we obtain:

$$\begin{aligned} \lambda_{g[g_1 \ldots g_n]}(x_1^n) &= g[g_1 \ldots g_n][x_1 \ldots x_n] = g[g_1[x_1 \ldots x_n] \ldots g_n[x_1 \ldots x_n]] \\ &= \lambda_g(g_1[x_1 \ldots x_n], \ldots, g_n[x_1 \ldots x_n]) = \lambda_g(\lambda_{g_1}(x_1^n), \ldots, \lambda_{g_n}(x_1^n)) \\ &= \lambda_g[\lambda_{g_1} \ldots \lambda_{g_n}](x_1^n). \end{aligned}$$

2) For $(x_1, \ldots, x_n) = (e_1, \ldots, e_n)$, we have

$$\begin{aligned} \lambda_{g[g_1 \ldots g_n]}(e_1^n) &= g[g_1 \ldots g_n] = \lambda_g(g_1^n) \\ &= \lambda_g(\lambda_{g_1}(e_1^n), \ldots, \lambda_{g_n}(e_1^n)) = \lambda_g[\lambda_{g_1} \ldots \lambda_{g_n}](e_1^n). \end{aligned}$$

3) If $(x_1,\ldots,x_n)=(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n)$, then

$$\begin{aligned}\lambda_{g[g_1\ldots g_n]}(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n)&=\pi_{ij}(g[g_1\ldots g_n])=g[\pi_{ij}g_1\ldots\pi_{ij}g_n]\\&=\lambda_g(\lambda_{g_1}(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n),\ldots,\lambda_{g_n}(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n))\\&=\lambda_g[\lambda_{g_1}\ldots\lambda_{g_n}](e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n).\end{aligned}$$

4) Now let $(x_1,\ldots,x_n)=(\mu_1^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),\ldots,\mu_n^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s))$. If $\{i_1,\ldots,i_s\}=\{1,\ldots,n\}$, then, according to (5), this case is reduced to the case when $x_1,\ldots,x_n\in G$. For $\{i_1,\ldots,i_s\}\neq\{1,\ldots,n\}$, we have

$$\begin{aligned}\lambda_{g[g_1\ldots g_n]}(x_1^n)&=g[g_1\ldots g_n]\overset{i_s}{\underset{i_1}{\oplus}}y_1^s=g[g_1\overset{i_s}{\underset{i_1}{\oplus}}y_1^s\ldots g_n\overset{i_s}{\underset{i_1}{\oplus}}y_1^s]\\&=\lambda_g\left(\lambda_{g_1}(x_1^n),\ldots,\lambda_{g_n}(x_1^n)\right)=\lambda_g[\lambda_{g_1}\ldots\lambda_{g_n}](x_1^n).\end{aligned}$$

5) In the case $(x_1,\ldots,x_n)=(x_1^{i-1},\mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),x_{i+1}^{j-1},\mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),x_{j+1}^n)$, where $x_k=\mu_k^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s)$ and $k\in\{1,\ldots,n\}-\{i,j\}$, we obtain

$$\begin{aligned}\lambda_{g[g_1\ldots g_n]}(x_1^{i-1},\mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),x_{i+1}^{j-1},\mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),x_{j+1}^n)&=\pi_{ij}(g[g_1\ldots g_n])\overset{i_s}{\underset{i_1}{\oplus}}y_1^s\\&\overset{(7)}{=}g[\pi_{ij}g_1\ldots\pi_{ij}g_n]\overset{i_s}{\underset{i_1}{\oplus}}y_1^s=g[(\pi_{ij}g_1)\overset{i_s}{\underset{i_1}{\oplus}}y_1^s\ldots(\pi_{ij}g_n)\overset{i_s}{\underset{i_1}{\oplus}}y_1^s]\\&=\lambda_g(\lambda_{g_1}(x_1^n),\ldots,\lambda_{g_n}(x_1^n))\\&=\lambda_g[\lambda_{g_1}\ldots\lambda_{g_n}](x_1^{i-1},\mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),x_{i+1}^{j-1},\mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),x_{j+1}^n).\end{aligned}$$

This completes the proof that P is a homomorphism of (G,o) onto $(\Phi,\mathcal{O})$.

• Now we check that P a homomorphism of a $(2,n)$-semigroup $(G,\underset{1}{\oplus},\ldots,\underset{n}{\oplus})$ onto a $(2,n)$-semigroup $(\Phi,\underset{1}{\oplus},\ldots,\underset{n}{\oplus})$, i.e., $P(g_1\underset{i}{\oplus}g_2)=P(g_1)\underset{i}{\oplus}P(g_2)$, or equivalently,

$$\lambda_{g_1\underset{i}{\oplus}g_2}(x_1^n)=\lambda_{g_1}\underset{i}{\oplus}\lambda_{g_2}(x_1^n)$$

for all $i=1,2,\ldots,n$, $g_1,g_2\in G$ and $x_1,\ldots,x_n\in G^*$. Similarly as in previous case we must verify several cases.

1) If $x_1,\ldots,x_n\in G$, then, applying (3), we obtain

$$\begin{aligned}\lambda_{g_1\underset{i}{\oplus}g_2}(x_1^n)&=(g_1\underset{i}{\oplus}g_2)[x_1\ldots x_n]=g_1[x_1\ldots x_{i-1}\,g_2[x_1\ldots x_n]\,x_{i+1}\ldots x_n]\\&=\lambda_{g_1}\left(x_1^{i-1},\lambda_{g_2}(x_1^n),x_{i+1}^n\right)=\lambda_{g_1}\underset{i}{\oplus}\lambda_{g_2}(x_1^n).\end{aligned}$$

2) For $(x_1,\dots,x_n)=(e_1,\dots,e_n)$ we have $\lambda_{g_1 \underset{i}{\oplus} g_2}(e_1^n)=g_1\underset{i}{\oplus}g_2$. Consequently,

$$\lambda_{g_1}\underset{i}{\oplus}\lambda_{g_2}(e_1^n)=\lambda_{g_1}\left(e_1^{i-1},\lambda_{g_2}(e_1^n),e_{i+1}^n\right)=\lambda_{g_1}\left(e_1^{i-1},g_2,e_{i+1}^n\right)=g_1\underset{i}{\oplus}g_2,$$

because $\mu_i^*(\underset{i}{\oplus}g_2)=g_2$ and $\mu_k^*(\underset{i}{\oplus}g_2)=e_k$ for $k\neq i$, $k=1,\dots,n$.

Thus, $\lambda_{g_1\underset{i}{\oplus}g_2}(e_1^n)=\lambda_{g_1}\underset{i}{\oplus}\lambda_{g_2}(e_1^n)$.

3) In the case $(x_1,\dots,x_n)=(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n)$, for $k=1,\dots,n$, according to (8), we have

$$\lambda_{g_1\underset{k}{\oplus}g_2}(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n)=\pi_{ij}(g_1\underset{k}{\oplus}g_2)=\begin{cases}(\pi_{ij}g_1)\underset{k}{\oplus}(\pi_{ij}g_2), & \text{if } k\notin\{i,j\},\\ (\pi_{ij}g_1)\underset{j}{\oplus}(\pi_{ij}g_2), & \text{if } k=i,\\ (\pi_{ij}g_1)\underset{i}{\oplus}(\pi_{ij}g_2), & \text{if } k=j.\end{cases}$$

For $k\notin\{i,j\}$ we have three possibilities:

$$1\leqslant k<i<j\leqslant n \quad\text{or}\quad 1\leqslant i<k<j\leqslant n \quad\text{or}\quad 1\leqslant i<j<k\leqslant n.$$

In the case $1\leqslant k<i<j\leqslant n$ we get

$$\begin{aligned}&\lambda_{g_1}\underset{k}{\oplus}\lambda_{g_2}(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n)\\ &\qquad=\lambda_{g_1}(e_1^{k-1},\lambda_{g_2}(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n),e_{k+1}^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n)\\ &\qquad=\lambda_{g_1}(e_1^{k-1},\pi_{ij}g_2,e_{k+1}^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n)=(\pi_{ij}g_1)\underset{k}{\oplus}(\pi_{ij}g_2)\\ &\qquad=\lambda_{g_1}\underset{k}{\oplus}\lambda_{g_2}(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n),\end{aligned}$$

since $\mu_k^*(\underset{k}{\oplus}\pi_{ij}g_2)=\pi_{ij}g_2$ and $\mu_s^*(\underset{k}{\oplus}\pi_{ij}g_2)=e_s$ for $s\neq k$, $s=1,\dots,n$.

In the remaining two cases the proof is analogous.

If $k=i$, then

$$\begin{aligned}\lambda_{g_1}\underset{i}{\oplus}\lambda_{g_2}(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n)&=\lambda_{g_1}(e_1^{i-1},\lambda_{g_2}(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n),e_{i+1}^{j-1},e_i,e_{j+1}^n)\\ &=\lambda_{g_1}(e_1^{i-1},\pi_{ij}g_2,e_{i+1}^{j-1},e_i,e_{j+1}^n)=(\pi_{ij}g_1)\underset{j}{\oplus}(\pi_{ij}g_2)\\ &=\lambda_{g_1}\underset{i}{\oplus}\lambda_{g_2}(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n),\end{aligned}$$

since $\mu_j^*(\underset{j}{\oplus}\pi_{ij}g_2)=\pi_{ij}g_2$ and $\mu_s^*(\underset{j}{\oplus}\pi_{ij}g_2)=e_s$ for $s\neq j$, $s=1,\dots,n$.

In the same manner we can verity the case $k=j$.

4) Now let $(x_1,\dots,x_n)=(\mu_1^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),\dots,\mu_n^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s))$. Then, according to the definition, $\lambda_{g_1\underset{i}{\oplus}g_2}(x_1^n)=g_1\underset{i}{\oplus}g_2\overset{i_s}{\underset{i_1}{\oplus}}y_1^s$. On the other side, we have $\mu_i^*(\underset{i}{\oplus}g_2\overset{i_s}{\underset{i_1}{\oplus}}y_1^s)=$

$g_2 \overset{i_s}{\underset{i_1}{\oplus}} y_1^s = \lambda_{g_2}(x_1^n)$ and $\mu_k^*(\underset{i}{\oplus} g_2 \overset{i_s}{\underset{i_1}{\oplus}} y_1^s) = \mu_k^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s) = x_k$ for all $k \neq i$, $k = 1, \ldots, n$. Hence

$$\lambda_{g_1} \underset{i}{\oplus} \lambda_{g_2}(x_1^n) = \lambda_{g_1}\left(x_1^{i-1}, \lambda_{g_2}(x_1^n), x_{i+1}^n\right) = g_1 \underset{i}{\oplus} g_2 \overset{i_s}{\underset{i_1}{\oplus}} y_1^s.$$

Thus $\lambda_{g_1 \underset{i}{\oplus} g_2}(\mu_1^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), \ldots, \mu_n^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s)) = \lambda_{g_1} \underset{i}{\oplus} \lambda_{g_2}(\mu_1^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), \ldots, \mu_n^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s))$.

5) In the case when $(x_1, \ldots, x_n) = (x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n)$, where $x_k = \mu_k^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s)$ for $k \in \{1, \ldots, n\} - \{i, j\}$, we get

$$\lambda_{g_1 \underset{k}{\oplus} g_2}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n)$$

$$= \pi_{ij}(g_1 \underset{k}{\oplus} g_2) \overset{i_s}{\underset{i_1}{\oplus}} y_1^s = \begin{cases} (\pi_{ij} g_1) \underset{k}{\oplus} (\pi_{ij} g_2) \overset{i_s}{\underset{i_1}{\oplus}} y_1^s, & \text{if } k \in \{1, \ldots, n\} - \{i, j\}, \\ (\pi_{ij} g_1) \underset{j}{\oplus} (\pi_{ij} g_2) \overset{i_s}{\underset{i_1}{\oplus}} y_1^s, & \text{if } k = i, \\ (\pi_{ij} g_1) \underset{i}{\oplus} (\pi_{ij} g_2) \overset{i_s}{\underset{i_1}{\oplus}} y_1^s, & \text{if } k = j. \end{cases}$$

For $k \in \{1, \ldots, n\} - \{i, j\}$ we get three cases:

$$1 \leqslant k < i < j \leqslant n, \quad 1 \leqslant i < k < j \leqslant n, \quad 1 \leqslant i < j < k \leqslant n.$$

We verify only the last case. Other cases can be verified analogously.

To prove this case let $x_1, \ldots, x_n, y_1, \ldots, y_s \in G^*$ and $1 \leqslant i < j < k \leqslant n$. Then

$$\lambda_{g_1} \underset{k}{\oplus} \lambda_{g_2}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n)$$

$$= \lambda_{g_1}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^{k-1}, \lambda_{g_2}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n), x_{k+1}^n)$$

$$= \lambda_{g_1}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^{k-1}, (\pi_{ij} g_2) \overset{i_s}{\underset{i_1}{\oplus}} y_1^s, x_{k+1}^n)$$

$$= (\pi_{ij} g_1) \underset{k}{\oplus} (\pi_{ij} g_2) \overset{i_s}{\underset{i_1}{\oplus}} y_1^s,$$

since $\mu_k^*(\underset{k}{\oplus} (\pi_{ij} g_2) \overset{i_s}{\underset{i_1}{\oplus}} y_1^s) = (\pi_{ij} g_2) \overset{i_s}{\underset{i_1}{\oplus}} y_1^s$ and $\mu_s^*(\underset{k}{\oplus} (\pi_{ij} g_2) \overset{i_s}{\underset{i_1}{\oplus}} y_1^s) = \mu_s^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s)$ for $s \neq k$, $s = 1, \ldots, n$. Thus,

$$\lambda_{g_1 \underset{k}{\oplus} g_2}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n) = \lambda_{g_1} \underset{k}{\oplus} \lambda_{g_2}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n).$$

So in this case $P(g_1 \underset{k}{\oplus} g_2) = P(g_1) \underset{k}{\oplus} P(g_2)$.

In the case $k = i$, we get

$$\lambda_{g_1} \underset{i}{\oplus} \lambda_{g_2}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n)$$

$$= \lambda_{g_1}(x_1^{i-1}, \lambda_{g_2}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n)$$

$$= \lambda_{g_1}(x_1^{i-1}, (\pi_{ij}g_2)\overset{i_s}{\underset{i_1}{\oplus}} y_1^s, x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n) = (\pi_{ij}g_1)\underset{j}{\oplus}(\pi_{ij}g_2)\overset{i_s}{\underset{i_1}{\oplus}} y_1^s,$$

since $\mu_j^*(\underset{j}{\oplus}(\pi_{ij}g_2)\overset{i_s}{\underset{i_1}{\oplus}} y_1^s) = (\pi_{ij}g_2)\overset{i_s}{\underset{i_1}{\oplus}} y_1^s$ and $\mu_s^*(\underset{j}{\oplus}(\pi_{ij}g_2)\overset{i_s}{\underset{i_1}{\oplus}} y_1^s) = \mu_s^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s)$ for $s \neq j$, $s = 1, \ldots, n$. Thus,

$$\lambda_{g_1\underset{i}{\oplus}g_2}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n) = \lambda_{g_1}\underset{i}{\oplus}\lambda_{g_2}(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n).$$

So, $P(g_1 \underset{i}{\oplus} g_2) = P(g_1) \underset{i}{\oplus} P(g_2)$.

For $k = j$ the proof is very similar.

In this way we have proved that P a homomorphism of a $(2,n)$-semigroup $(G, \underset{1}{\oplus}, \ldots, \underset{n}{\oplus})$ onto a $(2,n)$-semigroup $(\Phi, \underset{1}{\oplus}, \ldots, \underset{n}{\oplus})$.

• This homomorphism also saves the operation π_{ij}, i.e., $P(\pi_{ij}g) = \pi_{ij}P(g)$ or, in other words, $\lambda_{\pi_{ij}g}(x_1^n) = \pi_{ij}\lambda_g(x_1^n)$ for all $g \in G$ and $x_1, \ldots, x_n \in G^*$.

1) If $x_1, \ldots, x_n \in G$, then

$$\begin{aligned}\lambda_{\pi_{ij}g}(x_1^n) = (\pi_{ij}g)[x_1 \ldots x_n] &\overset{(6)}{=} g[x_1^{i-1}x_j x_{i+1}^{j-1} x_i x_{j+1}^n] \\ &= \lambda_g(x_1^{i-1}, x_j, x_{i+1}^{j-1}, x_i, x_{j+1}^n) = \pi_{ij}\lambda_g(x_1^n).\end{aligned}$$

2) For $(x_1, \ldots, x_n) = (e_1, \ldots, e_n)$ we have

$$\lambda_{\pi_{ij}g}(e_1^n) = \pi_{ij}g = \lambda_g(e_1^{i-1}, e_j, e_{i+1}^{j-1}, e_i, e_{j+1}^n) = \pi_{ij}\lambda_g(e_1^n).$$

3) In the case $(x_1, \ldots, x_n) = (e_1^{i-1}, e_j, e_{i+1}^{j-1}, e_i, e_{j+1}^n)$, we obtain

$$\begin{aligned}\lambda_{\pi_{ij}g}(e_1^{i-1}, e_j, e_{i+1}^{j-1}, e_i, e_{j+1}^n) = \pi_{ij}(\pi_{ij}g) = \pi_{ij}^2 g &\overset{(9)}{=} g \\ &= \lambda_g(e_1^n) = \pi_{ij}\lambda_g(e_1^{i-1}, e_j, e_{i+1}^{j-1}, e_i, e_{j+1}^n).\end{aligned}$$

4) Now, if $(x_1, \ldots, x_n) = (\mu_1^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), \ldots, \mu_n^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s))$, then

$$\begin{aligned}\lambda_{\pi_{ij}g}(\mu_1^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), \ldots, \mu_n^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s)) &= (\pi_{ij}g)\overset{i_s}{\underset{i_1}{\oplus}} y_1^s \\ &= \lambda_g(x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n) \\ &= \pi_{ij}\lambda_g(x_1^{i-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n) \\ &= \pi_{ij}\lambda_g(\mu_1^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), \ldots, \mu_n^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s)).\end{aligned}$$

5) In the last case when $(x_1, \ldots, x_n) = (x_1^{i-1}, \mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{i+1}^{j-1}, \mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s), x_{j+1}^n)$, where $x_k = \mu_k^*(\overset{i_s}{\underset{i_1}{\oplus}} y_1^s)$ and $k \in \{1, \ldots, n\} - \{i, j\}$, we get

$$\begin{aligned}&\lambda_{\pi_{ij}g}(x_1^{i-1},\mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),x_{i+1}^{j-1},\mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),x_{j+1}^n)=(\pi_{ij}^2g)\overset{i_s}{\underset{i_1}{\oplus}}y_1^s=g\overset{i_s}{\underset{i_1}{\oplus}}y_1^s\\&=\lambda_g(\mu_1^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),\ldots,\mu_n^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s))=\pi_{ij}\lambda_g(x_1^{i-1},\mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),x_{i+1}^{j-1},\mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),x_{j+1}^n).\end{aligned}$$

This completes the proof that $P\colon g\mapsto\lambda_g$ is an epimorphism of $(G,\underset{1}{\oplus},\ldots,\underset{n}{\oplus},\pi_{ij})$ onto $(\Phi,\underset{1}{\oplus},\ldots,\underset{n}{\oplus},\pi_{ij})$. Since $P(g_1)=P(g_2)$ implies $\lambda_{g_1}(e_1^n)=\lambda_{g_2}(e_1^n)$, which gives $g_1=g_2$, we see that $P\colon g\mapsto\lambda_g$ is an isomorphism. □

From the above theorem we can deduce the following two corollaries.

Corollary 1. *An algebra (G,o,π_{ij}) of type $(n+1,1)$ is isomorphic to an algebra $(\Phi,\mathcal{O},\pi_{ij})$ of partial n-place functions if and only if it satisfies* (1), (6), (7) *and* (9).

Proof. From the first part of the proof of Theorem 1 it follows that $(\Phi,\mathcal{O},\pi_{ij})$ is a Menger algebra with the operation π_{ij} satisfying the conditions (6), (7) and (9).

To prove the converse statement consider an arbitrary algebra (G,o,π_{ij}) of type $(n+1,1)$ satisfying all the conditions mentioned in the corollary and define on the set $G^*=G\cup\{e_1,\ldots,e_n\}$, where $e_1,\ldots,e_n$ are different elements not belonging to G, the function λ_g putting:

$$\lambda_g(x_1^n)=\begin{cases}g[x_1\ldots x_n], & \text{if } x_1,\ldots,x_n\in G,\\ g, & \text{if } (x_1,\ldots,x_n)=(e_1,\ldots,e_n),\\ \pi_{ij}g, & \text{if } (x_1,\ldots,x_n)=(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n).\end{cases}$$

In other cases $\lambda_g(x_1^n)$ is not defined.

Then in the same way as in the second part of the proof of Theorem 1, we can prove that the algebras (G,o,π_{ij}) and $(\Phi,\mathcal{O},\pi_{ij})$, where $\Phi=\{\lambda_g\,|\,g\in G\}$, are isomorphic. This isomorphism has the form $P\colon g\mapsto\lambda_g$. □

Corollary 2. *An algebra $(G,\underset{1}{\oplus},\ldots,\underset{n}{\oplus},\pi_{ij})$ of type $(2,\ldots,2,1)$ is isomorphic to the algebra $(\Phi,\underset{1}{\oplus},\ldots,\underset{n}{\oplus},\pi_{ij})$ of partial n-place functions if and only if it satisfies the identities* (8), (9), *and the implication* (2).

Proof. Clearly, the algebra $(\Phi,\underset{1}{\oplus},\ldots,\underset{n}{\oplus},\pi_{ij})$ of partial n-place functions satisfies (2), (8) and (9).

Conversely, if an algebra $(G,\underset{1}{\oplus},\ldots,\underset{n}{\oplus},\pi_{ij})$ of type $(2,\ldots,2,1)$ satisfies the conditions (2), (8) and (9), then for each element $g\in G$ we define on the set $G^*=G\cup\{e_1,\ldots,e_n\}$, where $e_1,\ldots,e_n$ are different elements not belonging to G, the n-place function $\lambda_g\colon(G^*)^n\to G^*$ putting

$$\lambda_g(x_1^n)=\begin{cases} g, & \text{if } (x_1,\ldots,x_n)=(e_1,\ldots,e_n),\\ \pi_{ij}g, & \text{if } (x_1,\ldots,x_n)=(e_1^{i-1},e_j,e_{i+1}^{j-1},e_i,e_{j+1}^n),\\ g\overset{i_s}{\underset{i_1}{\oplus}}y_1^s, & \text{if } x_i=\mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),\ i=1,\ldots,n,\\ & \text{for some } y_1,\ldots,y_s\in G,\\ & \{i_1,\ldots,i_s\}\subset\{1,\ldots,n\},\\ (\pi_{ij}g)\overset{i_s}{\underset{i_1}{\oplus}}y_1^s, & \text{if } x_i=\mu_j^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),\ x_j=\mu_i^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),\\ & x_k=\mu_k^*(\overset{i_s}{\underset{i_1}{\oplus}}y_1^s),\ k\in\{1,\ldots,n\}-\{i,j\},\\ & \text{where } y_1,\ldots,y_s\in G,\ \{i_1,\ldots,i_s\}\subset\{1,\ldots,n\}. \end{cases}$$

In other cases $\lambda_g(x_1^n)$ is not defined.

In the same way as in the second part of the proof of Theorem 1, we can see that $P\colon g\mapsto\lambda_g$ is an isomorphism between $(G,\underset{1}{\oplus},\ldots,\underset{n}{\oplus},\pi_{ij})$ and $(\Phi,\underset{1}{\oplus},\ldots,\underset{n}{\oplus},\pi_{ij})$, where $\Phi=\{\lambda_g\,|\,g\in G\}$. □

From Theorem 1 we deduce the following characterizations of algebras of (i,j)-commutative functions.

Corollary 3. *An algebra $(G,o,\underset{1}{\oplus},\ldots,\underset{n}{\oplus})$ of type $(n+1,2,\ldots,2)$ is isomorphic to the algebra $(\Phi,\mathcal{O},\underset{1}{\oplus},\ldots,\underset{n}{\oplus})$ of partial (i,j)-commutative n-place functions if and only if it satisfies the condition* (1), (2), (3), (4), (5) *and*

$$x[y_1\ldots y_n]=x[y_1^{i-1}\,y_j\,y_{i+1}^{j-1}\,y_i\,y_{j+1}^n],\tag{10}$$

$$x\underset{k}{\oplus}y=\begin{cases} x\underset{j}{\oplus}y, & \textit{if } k=i,\\ x\underset{i}{\oplus}y, & \textit{if } k=j.\end{cases}\tag{11}$$

Corollary 4. *An $(n+1)$-ary algebra (G,o) is isomorphic to the algebra $(\Phi,\mathcal{O})$ of partial (i,j)-commutative n-place functions if and only if it satisfies the conditions* (1) *and* (10).

Corollary 5. *An algebra $(G,\underset{1}{\oplus},\ldots,\underset{n}{\oplus})$ of type $(2,\ldots,2)$ is isomorphic to the algebra $(\Phi,\underset{1}{\oplus},\ldots,\underset{n}{\oplus})$ of partial (i,j)-commutative n-place functions if and only if it satisfies the condition* (11) *and the implication* (2).

References

[1] **J.R. Cho**, *Representations of certain medial algebras*, J. Korean Math. Soc. **27** (1990), 69 – 76.

[2] **S.S. Davidov**, *On regular medial division algebras*, Quasigroups and Related Systems **21** (2013), 155 – 164.

[3] **R.M. Dicker**, *The substitutive law*, Proc. London Math. Soc. **13** (1963), 493 – 510.

[4] **W.A. Dudek**, *Remarks on n-groups*, Demonstratio Math. 13 (1980), 165 – 180.

[5] **W.A. Dudek**, *Medial n-groups and skew elements*, Proc. V Universal Algebra Symposium, Turawa 1988, World Sci. Publ., Singapore 1989, 55 – 80.

[6] **W.A. Dudek and V.S. Trokhimenko**, *Representations of Menger* $(2,n)$*-semigroups by multiplace functions*, Commun. Algebra **34** (2006), 259 – 274.

[7] **W.A. Dudek and V.S. Trokhimenko**, *Representations of* $(2,n)$*-semigroups by multiplace functions*, Studia Sci. Math. Hungar. **44** (2007), 131 – 146.

[8] **W.A. Dudek and V.S. Trokhimenko**, *Algebras of multiplace functions*, Walter de Gruyter GmbH & Co. KG, Berlin/Boston, 2012.

[9] **K. Glazek and B. Gleichgewicht**, *Abelian n-groups*, Coll. Math. Soc. J. Bolyai, 29 Universal Algebra, Esztergom (Hungary), 1977, 321 – 329.

[10] **L.M. Gluskin**, *Positional operatives*, (Russian), Mat. Sb. (N.S.) **68(110)** (1965), 444 – 472.

[11] **Yu.I. Kulazhenko**, *Geometry of semiabelian n-ary groups*, Quasigroups and Related Systems **19** (2011), 265 – 278.

[12] **I.A. Mal'cev**, *Iterative Post algebras*, (Russian), Library Dep. Algebra and Math. Logic Novosibirsk State Univ., Novosibirsk, 1976.

[13] **V.S. Trokhimenko**, *Characteristics of some algebras of functions of many-valued logic*, Cybernetics **23** (1987), 362 – 368 (translation from Kibernetika (Kiev) 1987, 63 – 68).

[14] **V.S. Trokhimenko**, *A characterization of iterative function algebras*, Algebra Universalis **31** (1994), 542 – 550.

Received April 26, 2016

W.A. Dudek
Faculty of Pure and Applied Mathematics
Wroclaw University of Science and Technology
50-370 Wroclaw
Poland
Email: wieslaw.dudek@pwr.edu.pl

V.S. Trokhimenko
Department of Mathematics
Pedagogical University
21100 Vinnitsa
Ukraine
Email: vtrokhim@gmail.com

Quasigroups and Related Systems **24** (2016), 231 − 246

Soft set theoretical approach to residuated lattices

Young Bae Jun and *Xiaohong Zhang*

Abstract. Molodtsov's soft set theory is applied to residuated lattices. The notion of (filteristic) residuated lattices is introduced, and their properties are investigated. Divisible int-soft filters and strong int-soft filters are defined, and several properties are investigated. Characterizations of a divisible and strong int-soft filter are discussed. Conditions for an int-soft filter to be divisible are established. Relations between a divisible int-soft filter and a strong int-soft filter are considered.

1. Introduction

Various problems in system identification involve characteristics which are essentially non-probabilistic in nature [13]. In response to this situation Zadeh [14] introduced *fuzzy set theory* as an alternative to probability theory. Uncertainty is an attribute of information. In order to suggest a more general framework, the approach to uncertainty is outlined by Zadeh [15]. To solve complicated problem in economics, engineering, and environment, we cannot successfully use classical methods because of various uncertainties typical for those problems. There are three theories: theory of probability, theory of fuzzy sets, and the interval mathematics which we can consider as mathematical tools for dealing with uncertainties. But all these theories have their own difficulties. Uncertainties cannot be handled using traditional mathematical tools but may be dealt with using a wide range of existing theories such as probability theory, theory of (intuitionistic) fuzzy sets, theory of vague sets, theory of interval mathematics, and theory of rough sets. However, all of these theories have their own difficulties which are pointed out in [9]. Maji et al. [8] and Molodtsov [9] suggested that one reason for these difficulties may be due to the inadequacy of the parametrization tool of the theory. To overcome these difficulties, Molodtsov [9] introduced the concept of soft set as a new mathematical tool for dealing with uncertainties that is free from the difficulties that have troubled the usual theoretical approaches. Molodtsov pointed out several directions for the applications of soft sets. At present, works on the soft set theory are progressing rapidly. Maji et al. [8] and Çağman et al. [2] described the application of soft set theory to a decision making problem. Maji et al. [7] also studied several operations on the theory of soft sets. Jun and

2010 Mathematics Subject Classification: 03G10, 06B10, 03G25, 06D72.

Keywords: residuated lattice, (filteristic) residuated lattice, (divisible, strong) filter, int-soft filter, divisible int-soft filter, strong int-soft filter.

Park [5] applied the notion of soft sets to BCK/BCI-algebras. In order to deal with fuzzy and uncertain informations, non-classical logic has become a formal and useful tool. As the semantical systems of non-classical logic systems, various logical algebras have been proposed. Residuated lattices are important algebraic structures which are basic of MTL-algebras, BL-algebras, MV-algebras, Gödel algebras, R_0-algebras, lattice implication algebras, etc. The filter theory plays an important role in studying logical systems and the related algebraic structures, and various filters have been proposed in the literature. Zhang et al. [16] introduced the notions of IMTL-filters (NM-filters, MV-filters) of residuated lattices, and presented their characterizations. Ma and Hu [6] introduced divisible filters, strong filters and n-contractive filters in residuated lattices.

In this paper, we apply the notion of soft set theory by Molodtsov to residuated lattices. We introduce the notion of (filteristic) residuated lattices, and investigate their properties. We also define divisible int-soft filters and strong int-soft filters, and investigate related properties. We discuss characterizations of a divisible and strong int-soft filter, and provide conditions for an int-soft filter to be divisible. We establish relations between a divisible int-soft filter and a strong int-soft filter.

2. Preliminaries

We display basic notions on residuated lattices and soft sets which are used in this paper.

Definition 2.1. A *residuated lattice* is an algebra $\mathcal{L} := (L, \vee, \wedge, \otimes, \to, 0, 1)$ of type $(2, 2, 2, 2, 0, 0)$ such that

(L1) $(L, \vee, \wedge, 0, 1)$ is a bounded lattice,

(L2) $(L, \otimes, 1)$ is a commutative monoid,

(L3) $\otimes$ and $\to$ form an adjoint pair, that is,

$$(\forall x, y, z \in L)\, (x \leqslant y \to z \;\Leftrightarrow\; x \otimes y \leqslant z)\,.$$

In a residuated lattice $\mathcal{L}$, the ordering $\leqslant$ and negation $\neg$ are defined as follows:

$$(\forall x, y \in L)\, (x \leqslant y \;\Leftrightarrow\; x \wedge y = x \;\Leftrightarrow\; x \vee y = y \;\Leftrightarrow\; x \to y = 1)$$

and $\neg x = x \to 0$ for all $x \in L$.

Proposition 2.2 ([1, 3, 4, 6, 11, 12])**.** *In a residuated lattice $\mathcal{L}$, the following properties are valid.*

$$1 \to x = x,\; x \to 1 = 1,\; x \to x = 1,\; 0 \to x = 1,\; x \to (y \to x) = 1, \tag{2.1}$$

$$x \to (y \to z) = (x \otimes y) \to z = y \to (x \to z), \tag{2.2}$$

$$x \leqslant y \;\Rightarrow\; z \to x \leqslant z \to y,\; y \to z \leqslant x \to z, \tag{2.3}$$

$$x \leqslant y \;\Rightarrow\; x \otimes z \leqslant y \otimes z, \tag{2.4}$$

$$z \to y \leqslant (x \to z) \to (x \to y),\; z \to y \leqslant (y \to x) \to (z \to x), \tag{2.5}$$

$$(x \to y) \otimes (y \to z) \leq x \to z. \tag{2.6}$$

$$x \otimes y \leqslant x \otimes (x \to y) \leqslant x \wedge y \leqslant x \wedge (x \to y) \leqslant x, \tag{2.7}$$

$$x \to (y \wedge z) = (x \to y) \wedge (x \to z),\ (x \vee y) \to z = (x \to z) \wedge (y \to z), \tag{2.8}$$

$$x \to y \leqslant (x \otimes z) \to (y \otimes z), \tag{2.9}$$

$$\neg\neg(x \to y) \leqslant \neg\neg x \to \neg\neg y. \tag{2.10}$$

$$\neg x = \neg\neg\neg x,\ x \leqslant \neg\neg x,\ \neg 1 = 0,\ \neg 0 = 1, \tag{2.11}$$

$$x \to (x \wedge y) = x \to y. \tag{2.12}$$

Definition 2.3 ([10]). A nonempty subset F of a residuated lattice $\mathcal{L}$ is called a *filter* of $\mathcal{L}$ if it satisfies the conditions:

$$(\forall x, y \in L)\,(x, y \in F \ \Rightarrow\ x \otimes y \in F)\,, \tag{2.13}$$

$$(\forall x, y \in L)\,(x \in F,\ x \leqslant y \ \Rightarrow\ y \in F)\,. \tag{2.14}$$

Proposition 2.4 ([10]). *A nonempty subset F of a residuated lattice $\mathcal{L}$ is a filter of $\mathcal{L}$ if and only if it satisfies:*

$$1 \in F, \tag{2.15}$$

$$(\forall x \in F)\,(\forall y \in L)\,(x \to y \in F \ \Rightarrow\ y \in F)\,. \tag{2.16}$$

Definition 2.5 ([17]). A soft set $\left(\tilde{f}, L\right)$ over U in a residuated lattice $\mathcal{L}$ is called an *int-soft filter* of $\mathcal{L}$ over U if it satisfies:

$$(\forall x, y \in L)\left(\tilde{f}(x \otimes y) \supseteq \tilde{f}(x) \cap \tilde{f}(y)\right), \tag{2.17}$$

$$(\forall x, y \in L)\left(x \leqslant y \ \Rightarrow\ \tilde{f}(x) \subseteq \tilde{f}(y)\right). \tag{2.18}$$

Theorem 2.6 ([17]). *A soft set $\left(\tilde{f}, L\right)$ over U in a residuated lattice $\mathcal{L}$ is an int-soft filter of $\mathcal{L}$ over U if and only if the following assertions are valid:*

$$(\forall x \in L)\left(\tilde{f}(1) \supseteq \tilde{f}(x)\right), \tag{2.19}$$

$$(\forall x, y \in L)\left(\tilde{f}(y) \supseteq \tilde{f}(x \to y) \cap \tilde{f}(x)\right). \tag{2.20}$$

3. (Filteristic) soft residuated lattices

In what follows let $\mathcal{L}$ and A be a residuated lattice and a nonempty set, respectively.

Definition 3.1. Let $(\tilde{f}, A)$ be a soft set over $\mathcal{L}$. Then $(\tilde{f}, A)$ is called a *soft residuated lattice* over $\mathcal{L}$ if $\tilde{f}(x)$ is a sub-residuated lattices of $\mathcal{L}$ for all $x \in A$ with $\tilde{f}(x) \neq \emptyset$. If $\tilde{f}(x)$ is a filter of $\mathcal{L}$ for all $x \in A$ with $\tilde{f}(x) \neq \emptyset$, then $(\tilde{f}, A)$ is called a *filteristic soft residuated lattice* over $\mathcal{L}$.

Example 3.2. Let $L = \{0, a, b, 1\}$ be a chain with the operations $\otimes$ and $\rightarrow$ given by tables

$\otimes$	0	a	b	1
0	0	0	0	0
a	0	0	a	a
b	0	a	b	b
1	0	a	b	1

$\rightarrow$	0	a	b	1
0	1	1	1	1
a	a	1	1	1
b	0	a	1	1
1	0	a	b	1

Then $\mathcal{L} := (L, \vee, \wedge, \otimes, \rightarrow, 0, 1)$ is a residuated lattice. For $A = \mathbb{N}$, define two soft sets $(\tilde{f}, A)$ and $(\tilde{g}, A)$ over $U = L$ in $\mathcal{L}$ by

$$\tilde{f} : A \rightarrow \mathcal{P}(L), \quad x \mapsto \begin{cases} L & \text{if } x \in \{a \in \mathbb{N} \mid a \leqslant 10\}, \\ \{b, 1\} & \text{otherwise,} \end{cases}$$

and

$$\tilde{g} : A \rightarrow \mathcal{P}(L), \quad x \mapsto \begin{cases} L & \text{if } x \in \{a \in \mathbb{N} \mid a \leqslant 10\}, \\ \{b, 1\} & \text{if } x \in \{a \in \mathbb{N} \mid 10 < a \leqslant 30\}, \\ \{1\} & \text{if } x \in \{a \in \mathbb{N} \mid 30 < a \leqslant 60\}, \\ \emptyset & \text{otherwise,} \end{cases}$$

respectively. Then $(\tilde{f}, A)$ is a soft residuated lattices over $\mathcal{L}$ and $(\tilde{g}, A)$ is a filteristic soft residuated lattice over $\mathcal{L}$.

Theorem 3.3. *Let $(\tilde{f}, A)$ be a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$. If B is a subset of A, then $(\tilde{f}|_B, B)$ is a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$.*

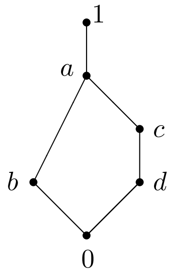
Proof. Straightforward. □

The following example shows that there exists a soft set $(\tilde{f}, A)$ over $\mathcal{L}$ such that

(i) $(\tilde{f}, A)$ is not a soft residuated lattice over $\mathcal{L}$.

(ii) there exists a subset B of A such that $(\tilde{f}|_B, B)$ is a soft residuated lattice over $\mathcal{L}$.

Example 3.4. Consider a residuated lattice $L := \{0, a, b, c, d, 1\}$ with the following Hasse diagram and Cayley tables.



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

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

Let $(\tilde{f}, A)$ be a soft set over $\mathcal{L}$, where $A = \mathbb{N}$ and

$$\tilde{f} : A \to \mathcal{P}(L), \quad x \mapsto \begin{cases} L & \text{if } x \in \{a \in \mathbb{N} \mid a \leqslant 10\}, \\ \{a, 1\} & \text{if } x \in \{a \in \mathbb{N} \mid 10 < a \leqslant 20\}, \\ \{b, 1\} & \text{if } x \in \{a \in \mathbb{N} \mid 20 < a \leqslant 30\}, \\ \{c, 1\} & \text{if } x \in \{a \in \mathbb{N} \mid 30 < a \leqslant 40\}, \\ \{d, 1\} & \text{if } x \in \{a \in \mathbb{N} \mid 40 < a \leqslant 50\}, \\ \{c, d, 1\} & \text{otherwise.} \end{cases}$$

Then $(\tilde{f}, A)$ is not a soft residuated lattice over $\mathcal{L}$. But if we take

$$B := \{a \in \mathbb{N} \mid a \leqslant 50\},$$

then $(\tilde{f}|_B, B)$ is a soft residuated lattice over $\mathcal{L}$.

Theorem 3.5. *Let $(\tilde{f}, A)$ and $(\tilde{g}, B)$ be two soft residuated lattices (resp., filteristic soft residuated lattices) over $\mathcal{L}$. If $A \cap B \neq \emptyset$, then the intersection $(\tilde{f}, A)\tilde{\cap}(\tilde{g}, B)$ is a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$.*

Proof. Note that $(\tilde{f}, A)\tilde{\cap}(\tilde{g}, B) = (\tilde{h}, C)$, where $C = A \cap B$ and $\tilde{h}(x) = \tilde{f}(x)$ or $\tilde{g}(x)$ for all $x \in C$. Note that $\tilde{h} : C \to \mathcal{P}(L)$ is a mapping, and therefore $(\tilde{h}, C)$ is a soft set over $\mathcal{L}$. Since $(\tilde{f}, A)$ and $(\tilde{g}, B)$ are soft residuated lattices (resp., filteristic soft residuated lattices) over $\mathcal{L}$, it follows that $\tilde{h}(x) = \tilde{f}(x)$ is a sub-residuated lattice (resp., filter) of L, or $\tilde{h}(x) = \tilde{g}(x)$ is a sub-residuated lattice (resp., filter) of $\mathcal{L}$ for all $x \in C$. Hence $(\tilde{h}, C) = (\tilde{f}, A)\tilde{\cap}(\tilde{g}, B)$ is a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$. □

Corollary 3.6. *Let $(\tilde{f}, A)$ and $(\tilde{g}, A)$ be two soft residuated lattices (resp., filteristic soft residuated lattices) over $\mathcal{L}$. Then their intersection $(\tilde{f}, A)\tilde{\cap}(\tilde{g}, A)$ is a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$.*

Proof. Straightforward. □

Theorem 3.7. *Let $(\tilde{f}, A)$ and $(\tilde{g}, A)$ be two soft residuated lattices (resp., filteristic soft residuated lattices) over $\mathcal{L}$. If A and B are disjoint, then the union $(\tilde{f}, A)\tilde{\cup}(\tilde{g}, A)$ is a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$.*

Proof. Note that $(\tilde{f}, A)\tilde{\cup}(\tilde{g}, B) = (\tilde{h}, C)$, where $C = A \cup B$ and for every $e \in C$,

$$\tilde{h}(e) = \begin{cases} \tilde{f}(e) & \text{if } e \in A \setminus B, \\ \tilde{g}(e) & \text{if } e \in B \setminus A, \\ \tilde{f}(e) \cup \tilde{g}(e) & \text{if } e \in A \cap B. \end{cases}$$

Since $A \cap B = \emptyset$, either $x \in A \setminus B$ or $x \in B \setminus A$ for all $x \in C$. If $x \in A \setminus B$, then $\tilde{h}(x) = \tilde{f}(x)$ is a sub-residuated lattice (resp., filter) of $\mathcal{L}$ since $(\tilde{f}, A)$ is a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$. If $x \in B \setminus A$, then $\tilde{h}(x) = \tilde{g}(x)$ is a sub-residuated lattice (resp., filter) of $\mathcal{L}$ since $(\tilde{g}, B)$ is a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$. Hence $(\tilde{h}, C) = (\tilde{f}, A)\tilde{\cup}(\tilde{g}, A)$ is a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$. □

Theorem 3.8. *If $(\tilde{f}, A)$ and $(\tilde{g}, B)$ are soft residuated lattices (resp., filteristic soft residuated lattices) over $\mathcal{L}$, then $(\tilde{f}, A)\tilde{\wedge}(\tilde{g}, B)$ is a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$.*

Proof. Note that $(\tilde{f}, A)\tilde{\wedge}(\tilde{g}, B) = (\tilde{h}, A \times B)$, where $\tilde{h}(x, y) = \tilde{f}(x) \cap \tilde{g}(y)$ for all $(x, y) \in A \times B$. Since $\tilde{f}(x)$ and $\tilde{g}(y)$ are sub-residuated lattices (resp., filters) of $\mathcal{L}$, the intersection $\tilde{f}(x) \cap \tilde{g}(y)$ is also a sub-residuated lattice (resp., filter) of $\mathcal{L}$. Hence $\tilde{h}(x, y)$ is a sub-residuated lattice (resp., filter) of $\mathcal{L}$ for all $(x, y) \in A \times B$, and therefore $(\tilde{f}, A)\tilde{\wedge}(\tilde{g}, B) = (\tilde{h}, A \times B)$ is a soft residuated lattice (resp., filteristic soft residuated lattice) over $\mathcal{L}$. □

4. Divisible and strong int-soft filters

Definition 4.1 ([6]). A filter F of $\mathcal{L}$ is said to be *divisible* if it satisfies:

$$(\forall x, y \in L)\,((x \wedge y) \to [x \otimes (x \to y)] \in F)\,. \tag{4.21}$$

Definition 4.2. An int-soft filter $\left(\tilde{f}, L\right)$ of $\mathcal{L}$ over U is said to be *divisible* if it satisfies:

$$(\forall x, y \in L)\left(\tilde{f}\big((x \wedge y) \to [x \otimes (x \to y)]\big) = \tilde{f}(1)\right). \tag{4.22}$$

Example 4.3. Consider the residuated lattice $\mathcal{L} := (L, \vee, \wedge, \otimes, \to, 0, 1)$ which is given in Example 3.2. Define a soft set $\left(\tilde{f}, L\right)$ over $U = \mathbb{Z}$ in $\mathcal{L}$ by $\tilde{f}(1) = 2\mathbb{Z}$ and $\tilde{f}(x) = 2\mathbb{N}$ for all $x (\neq 1) \in L$. It is routine to verify that $\left(\tilde{f}, L\right)$ is a divisible int-soft filter of $\mathcal{L}$ over $U = \mathbb{Z}$.

Example 4.4. Consider a residuated lattice $L = [0, 1]$ in which two operations "$\otimes$" and "$\to$" are defined as follows:

$$x \otimes y = \begin{cases} 0 & \text{if } x + y \leqslant \frac{1}{2}, \\ x \wedge y & \text{otherwise.} \end{cases}$$

$$x \to y = \begin{cases} 1 & \text{if } x \leqslant y, \\ \left(\frac{1}{2} - x\right) \vee y & \text{otherwise.} \end{cases}$$

The soft set $\left(\tilde{f}, L\right)$ over $U = \mathbb{N}$ in $\mathcal{L}$ given by $\tilde{f}(1) = 3\mathbb{N}$ and $\tilde{f}(x) = 6\mathbb{N}$ for all $x(\neq 1) \in L$ is an int-soft filter of $\mathcal{L}$. But it is not divisible since

$$\tilde{f}((0.3 \wedge 0.2) \to (0.3 \otimes (0.3 \to 0.2)) = \tilde{f}(0.3) \neq \tilde{f}(1).$$

Proposition 4.5. *Every divisible int-soft filter $\left(\tilde{f}, L\right)$ of $\mathcal{L}$ over U satisfies the following identity.*

$$\tilde{f}(((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (y \wedge z))) = \tilde{f}(1) \tag{4.23}$$

for all $x, y, z \in L$.

Proof. Let $x, y, z \in L$. If we let $x := x \otimes y$ and $y := x \otimes z$ in (4.22), then

$$\tilde{f}(((x \otimes y) \wedge (x \otimes z)) \to ((x \otimes y) \otimes ((x \otimes y) \to (x \otimes z)))) = \tilde{f}(1). \tag{4.24}$$

Using (2.2) and (2.7), we have

$$\begin{aligned}(x \otimes y) \otimes ((x \otimes y) \to (x \otimes z)) &= x \otimes y \otimes (y \to (x \to (x \otimes z))) \\ &\leqslant x \otimes (y \wedge (x \to (x \otimes z))),\end{aligned}$$

which implies from (2.3)

$$\begin{aligned}&((x \otimes y) \wedge (x \otimes z)) \to ((x \otimes y) \otimes ((x \otimes y) \to (x \otimes z))) \\ &\leqslant ((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (y \wedge (x \to (x \otimes z)))).\end{aligned}$$

It follows from (4.24) and (2.18) that

$$\begin{aligned}\tilde{f}(1) &= \tilde{f}(((x \otimes y) \wedge (x \otimes z)) \to ((x \otimes y) \otimes ((x \otimes y) \to (x \otimes z)))) \\ &\subseteq \tilde{f}(((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (y \wedge (x \to (x \otimes z)))))\end{aligned}$$

and so that

$$\tilde{f}(((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (y \wedge (x \to (x \otimes z))))) = \tilde{f}(1). \tag{4.25}$$

On the other hand, if we take $x := x \to (x \otimes z)$ in (4.22) then

$$\begin{aligned}\tilde{f}(1) &= \tilde{f}((y \wedge (x \to (x \otimes z))) \to ((x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y))) \\ &\subseteq \tilde{f}((x \otimes (y \wedge (x \to (x \otimes z)))) \to \\ &\qquad (x \otimes ((x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y)))) \\ &= \tilde{f}((x \otimes (y \wedge (x \to (x \otimes z)))) \to \\ &\qquad (x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y)))\end{aligned}$$

by using (2.9), (2.18) and the commutativity and associativity of $\otimes$. Hence

$$\begin{aligned}\tilde{f}(1) = \tilde{f}((x \otimes (y \wedge (x \to (x \otimes z)))) \to \\ (x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y))).\end{aligned} \tag{4.26}$$

Using (2.6), we obtain

$$\begin{aligned}&(((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (y \wedge (x \to (x \otimes z)))))\otimes \\ &\quad ((x \otimes (y \wedge (x \to (x \otimes z)))) \to (x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y))) \\ &\leqslant ((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y)).\end{aligned}$$

It follows from (2.18), (2.17), (4.25) and (4.26) that

$$\begin{aligned}&\tilde{f}(((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y))) \\ &\supseteq \tilde{f}((((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (y \wedge (x \to (x \otimes z)))))\otimes \\ &\quad ((x \otimes (y \wedge (x \to (x \otimes z)))) \to (x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y)))) \\ &\supseteq \tilde{f}((((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (y \wedge (x \to (x \otimes z))))))\cap \\ &\qquad\qquad \tilde{f}(((x \otimes (y \wedge (x \to (x \otimes z)))) \to \\ &\qquad\qquad\qquad (x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y)))) \\ &= \tilde{f}(1)\end{aligned}$$

Thus

$$\tilde{f}(((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y))) = \tilde{f}(1). \tag{4.27}$$

Since

$$x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y)) \leqslant x \otimes z \otimes (z \to y) \leqslant x \otimes (y \wedge z),$$

we get

$$\begin{aligned}&((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y))) \\ &\leqslant ((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (y \wedge z)).\end{aligned}$$

It follows that

$$\begin{aligned}&\tilde{f}(((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (y \wedge z))) \\ &\supseteq \tilde{f}(((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (x \to (x \otimes z)) \otimes ((x \to (x \otimes z)) \to y)))) \\ &= \tilde{f}(1)\end{aligned}$$

and that $\tilde{f}(((x \otimes y) \wedge (x \otimes z)) \to (x \otimes (y \wedge z))) = \tilde{f}(1)$. □

We consider characterizations of a divisible int-soft filter.

Theorem 4.6. *An int-soft filter $\left(\tilde{f}, L\right)$ of $\mathcal{L}$ over U is divisible if and only if the following assertion is valid:*

$$\tilde{f}\big([x \to (y \wedge z)] \to [(x \to y) \otimes ((x \wedge y) \to z)]\big) = \tilde{f}(1) \tag{4.28}$$

for all $x, y, z \in L$.

Proof. Assume that $\left(\tilde{f}, L\right)$ is a divisible int-soft filter of $\mathcal{L}$ over U. If we take $x := x \to y$ and $y := x \to z$ in (4.22) and use (2.8) and (2.2), then

$$\begin{aligned}\tilde{f}(1) &= \tilde{f}\left([(x \to y) \wedge (x \to z)] \to [(x \to y) \otimes ((x \to y) \to (x \to z))]\right)\\ &= \tilde{f}\left([x \to (y \wedge z)] \to [(x \to y) \otimes ((x \otimes (x \to y)) \to z)]\right).\end{aligned}$$

Using (2.5) and (2.9), we have

$$\begin{aligned}&(x \wedge y) \to [x \otimes (x \to y)] \leqslant [(x \otimes (x \to y)) \to z] \to [(x \wedge y) \to z]\\ &\leqslant [(x \to y) \otimes ((x \otimes (x \to y)) \to z)] \to [(x \to y) \otimes ((x \wedge y) \to z)]\end{aligned}$$

for all $x, y, z \in L$. Since $\left(\tilde{f}, L\right)$ is a divisible int-soft filter of $\mathcal{L}$ over U, it follows from (4.22) and (2.18) that

$$\begin{aligned}\tilde{f}(1) &= \tilde{f}((x \wedge y) \to [x \otimes (x \to y)])\\ &\subseteq \tilde{f}([(x \to y) \otimes ((x \otimes (x \to y)) \to z)] \to [(x \to y) \otimes ((x \wedge y) \to z)])\end{aligned}$$

and so from (2.19) that

$$\tilde{f}([(x \to y) \otimes ((x \otimes (x \to y)) \to z)] \to [(x \to y) \otimes ((x \wedge y) \to z)]) = \tilde{f}(1)$$

for all $x, y, z \in L$. Using (2.6), we get

$$\begin{aligned}&\Big([x \to (y \wedge z)] \to [(x \to y) \otimes ((x \otimes (x \to y)) \to z)]\Big) \otimes\\ &\qquad\qquad \Big([(x \to y) \otimes ((x \otimes (x \to y)) \to z)] \to [(x \to y) \otimes ((x \wedge y) \to z)]\Big)\\ &\leqslant [x \to (y \wedge z)] \to [(x \to y) \otimes ((x \wedge y) \to z)],\end{aligned}$$

and so

$$\begin{aligned}&\tilde{f}\Big([x \to (y \wedge z)] \to [(x \to y) \otimes ((x \wedge y) \to z)]\Big)\\ &\supseteq \tilde{f}\Big(([x \to (y \wedge z)] \to [(x \to y) \otimes ((x \otimes (x \to y)) \to z)]) \otimes\\ &\qquad\qquad ([(x \to y) \otimes ((x \otimes (x \to y)) \to z)] \to [(x \to y) \otimes ((x \wedge y) \to z)])\Big)\\ &\supseteq \tilde{f}\big([x \to (y \wedge z)] \to [(x \to y) \otimes ((x \otimes (x \to y)) \to z)]\big) \cap\\ &\qquad\qquad \tilde{f}\big([(x \to y) \otimes ((x \otimes (x \to y)) \to z)] \to [(x \to y) \otimes ((x \wedge y) \to z)]\big)\\ &= \tilde{f}(1).\end{aligned}$$

Therefore

$$\tilde{f}\Big([x \to (y \wedge z)] \to [(x \to y) \otimes ((x \wedge y) \to z)]\Big) = \tilde{f}(1)$$

for all $x, y, z \in L$.

Conversely, let $\left(\tilde{f}, L\right)$ be an int-soft filter that satisfies the condition (4.28). If we take $x := 1$ in (4.28) and use (2.1), then we obtain (4.22). □

Theorem 4.7. *An int-soft filter $\left(\tilde{f}, L\right)$ of $\mathcal{L}$ over U is divisible if and only if it satisfies:*

$$\tilde{f}\left([y \otimes (y \to x)] \to [x \otimes (x \to y)]\right) = \tilde{f}(1) \tag{4.29}$$

for all $x, y \in L$.

Proof. Suppose that $\left(\tilde{f}, L\right)$ is a divisible int-soft filter of $\mathcal{L}$ over U. Note that

$$(x \wedge y) \to [x \otimes (x \to y)] \leq [y \otimes (y \to x)] \to [x \otimes (x \to y)]$$

for all $x, y \in L$. It follows from (4.22) and (2.18) that

$$\tilde{f}(1) = \tilde{f}\left((x \wedge y) \to [x \otimes (x \to y)]\right) \subseteq \tilde{f}\left([y \otimes (y \to x)] \to [x \otimes (x \to y)]\right)$$

and that $\tilde{f}\left([y \otimes (y \to x)] \to [x \otimes (x \to y)]\right) = \tilde{f}(1)$.

Conversely, let $\left(\tilde{f}, L\right)$ be an int-soft filter of $\mathcal{L}$ over U that satisfies the condition (4.29). Since $y \to x = y \to (y \wedge x)$ for all $x, y \in L$, the condition (4.29) implies that

$$\tilde{f}\left([y \otimes (y \to (x \wedge y))] \to [x \otimes (x \to (x \wedge y))]\right) = \tilde{f}(1). \tag{4.30}$$

If we take $y := x \wedge z$ in (4.30), then

$$\begin{aligned}\tilde{f}(1) &= \tilde{f}\left([(x \wedge z) \otimes ((x \wedge z) \to (x \wedge (x \wedge z)))] \to [x \otimes (x \to (x \wedge (x \wedge z)))]\right)\\ &= \tilde{f}\left((x \wedge z) \to [x \otimes (x \to z)]\right).\end{aligned}$$

Therefore $\left(\tilde{f}, L\right)$ is a divisible int-soft filter of $\mathcal{L}$ over U. □

We discuss conditions for an int-soft filter to be divisible.

Theorem 4.8. *If an int-soft filter $\left(\tilde{f}, L\right)$ of $\mathcal{L}$ over U satisfies the following assertion:*

$$\tilde{f}((x \wedge y) \to (x \otimes y)) = \tilde{f}(1) \tag{4.31}$$

for all $x, y \in L$, then $\left(\tilde{f}, L\right)$ is divisible.

Proof. Note that $x \otimes y \leqslant x \otimes (x \to y)$ for all $x, y \in L$. It follows from (2.3) that

$$(x \wedge y) \to (x \otimes y)] \leqslant (x \wedge y) \to (x \otimes (x \to y)).$$

Hence, by (4.31) and (2.18), we have

$$\tilde{f}(1) = \tilde{f}((x \wedge y) \to (x \otimes y)) \subseteq \tilde{f}((x \wedge y) \to (x \otimes (x \to y))),$$

and so $\tilde{f}((x \wedge y) \to (x \otimes (x \to y))) = \tilde{f}(1)$ for all $x, y \in L$. Therefore $\left(\tilde{f}, L\right)$ is a divisible int-soft filter of $\mathcal{L}$ over U. □

Theorem 4.9. *If an int-soft filter* $\left(\tilde{f}, L\right)$ *of* $\mathcal{L}$ *over* U *satisfies the following assertion:*

$$\tilde{f}((x \wedge (x \to y)) \to y) = \tilde{f}(1) \tag{4.32}$$

for all $x, y \in L$ *then* $\left(\tilde{f}, L\right)$ *is divisible.*

Proof. If we take $y := x \otimes y$ in (4.32), then

$$\tilde{f}(1) = \tilde{f}((x \wedge (x \to (x \otimes y))) \to (x \otimes y)) \subseteq \tilde{f}((x \wedge y) \to (x \otimes y))$$

and so $\tilde{f}((x \wedge y) \to (x \otimes y)) = \tilde{f}(1)$ for all $x, y \in L$. It follows from Theorem 4.8 that $\left(\tilde{f}, L\right)$ is a divisible int-soft filter of $\mathcal{L}$ over U. □

Theorem 4.10. *If an int-soft filter* $\left(\tilde{f}, L\right)$ *of* $\mathcal{L}$ *over* U *satisfies the following assertion:*

$$\tilde{f}(x \to z) \supseteq \tilde{f}((x \otimes y) \to z) \cap \tilde{f}(x \to y) \tag{4.33}$$

for all $x, y, z \in L$*, then* $\left(\tilde{f}, L\right)$ *is divisible.*

Proof. If we take $x := x \wedge (x \to y)$, $y := x$ and $z := y$ in (4.33), then

$$\begin{aligned}
&\tilde{f}((x \wedge (x \to y)) \to y) \\
&\supseteq \tilde{f}(((x \wedge (x \to y)) \otimes x) \to y) \cap \tilde{f}((x \wedge (x \to y)) \to x) \\
&= \tilde{f}(1).
\end{aligned}$$

Thus $\tilde{f}((x \wedge (x \to y)) \to y) = \tilde{f}(1)$ for all $x, y \in L$, and so $\left(\tilde{f}, L\right)$ is a divisible int-soft filter of $\mathcal{L}$ over U by Theorem 4.9. □

Theorem 4.11. *If an int-soft filter* $\tilde{f}$ *of* $\mathcal{L}$ *over* U *satisfies the following assertion:*

$$\tilde{f}(x \to (x \otimes x)) = \tilde{f}(1) \tag{4.34}$$

for all $x \in L$*, then* $\left(\tilde{f}, L\right)$ *is divisible.*

Proof. Let $\left(\tilde{f}, L\right)$ be an int-soft filter of $\mathcal{L}$ over U that satisfies the condition (4.34). Using (2.9) and the commutativity of $\otimes$, we have

$$x \to y \leqslant (x \otimes x) \to (x \otimes y),$$

and so

$$(x \to (x \otimes x)) \otimes (x \to y) \leqslant (x \to (x \otimes x)) \otimes ((x \otimes x) \to (x \otimes y))$$

for all $x, y \in L$ by (2.4) and the commutativity of $\otimes$. It follows from (2.6), (2.4) and the commutativity of $\otimes$ that

$$\begin{aligned} &((x \to (x \otimes x)) \otimes (x \to y)) \otimes ((x \otimes y) \to z) \\ &\leqslant ((x \to (x \otimes x)) \otimes ((x \otimes x) \to (x \otimes y))) \otimes ((x \otimes y) \to z) \\ &\leqslant (x \to (x \otimes y)) \otimes ((x \otimes y) \to z) \\ &\leqslant x \to z \end{aligned}$$

and so from (2.17), (2.18), (2.19) and (4.34) that

$$\begin{aligned} \tilde{f}(x \to z) &\supseteq \tilde{f}(((x \to (x \otimes x)) \otimes (x \to y)) \otimes ((x \otimes y) \to z)) \\ &\supseteq \tilde{f}((x \to (x \otimes x)) \otimes (x \to y)) \cap \tilde{f}((x \otimes y) \to z) \\ &\supseteq \tilde{f}(x \to (x \otimes x)) \cap \tilde{f}(x \to y) \cap \tilde{f}((x \otimes y) \to z) \\ &= \tilde{f}(1) \cap \tilde{f}(x \to y) \cap \tilde{f}((x \otimes y) \to z) \\ &= \tilde{f}((x \otimes y) \to z) \cap \tilde{f}(x \to y) \end{aligned}$$

for all $x, y, z \in L$. Therefore $\left(\tilde{f}, L\right)$ is a divisible int-soft fillter of $\mathcal{L}$ over U by Theorem 4.10. □

Definition 4.12 ([6]). A filter F of $\mathcal{L}$ is said to be *strong* if it satisfies:

$$\neg\neg(\neg\neg x \to x) \in F \tag{4.35}$$

for all $x \in L$.

Definition 4.13. An int-soft filter $\left(\tilde{f}, L\right)$ of $\mathcal{L}$ over U is said to be *strong* if it satisfies:

$$\tilde{f}\big(\neg\neg(\neg\neg x \to x)\big) = \tilde{f}(1) \tag{4.36}$$

for all $x \in L$.

Example 4.14. Consider the residuated lattice $\mathcal{L} := (L, \vee, \wedge, \otimes, \to, 0, 1)$ which is given in Example 3.4. Define a soft set $\left(\tilde{f}, L\right)$ over $U = \mathbb{Z}$ in $\mathcal{L}$ by $\tilde{f}(1) = 3\mathbb{Z}$ and $\tilde{f}(x) = 6\mathbb{N}$ for all $x (\neq 1) \in L$. It is routine to check that $\left(\tilde{f}, L\right)$ is a strong int-soft filter of $\mathcal{L}$ over $U = \mathbb{Z}$.

We provide characterizations of a strong int-soft filter.

Theorem 4.15. *Given a soft set* $\left(\tilde{f}, L\right)$ *over* U *in* $\mathcal{L}$*, the following assertions are equivalent.*

(i) $\left(\tilde{f}, L\right)$ *is a strong int-soft filter of* $\mathcal{L}$ *over* U*.*

(ii) $\left(\tilde{f}, L\right)$ *is an int-soft filter of* $\mathcal{L}$ *over* U *that satisfies*

$$(\forall x, y \in L)\left(\tilde{f}((y \to \neg\neg x) \to \neg\neg(y \to x) = \tilde{f}(1)\right). \tag{4.37}$$

(iii) $\left(\tilde{f}, L\right)$ *is an int-soft filter of* $\mathcal{L}$ *over* U *that satisfies*

$$(\forall x, y \in L)\left(\tilde{f}((\neg x \to y) \to \neg\neg(\neg y \to x)) = \tilde{f}(1)\right). \tag{4.38}$$

Proof. Assume that $\left(\tilde{f}, L\right)$ is a strong int-soft filter of $\mathcal{L}$ over U. Then $\left(\tilde{f}, L\right)$ is an int-soft filter of $\mathcal{L}$ over U. Note that

$$\begin{aligned}\neg\neg(\neg\neg x \to x) &\leqslant \neg\neg((y \to \neg\neg x) \to (y \to x))\\ &\leqslant \neg\neg((y \to \neg\neg x) \to \neg\neg(y \to x))\\ &= (y \to \neg\neg x) \to \neg\neg(y \to x)\end{aligned}$$

and

$$\begin{aligned}\neg\neg(\neg\neg x \to x) &\leqslant \neg\neg(((\neg x \to y) \otimes \neg y) \to x)\\ &= \neg\neg((\neg x \to y) \to (\neg y \to x))\\ &\leqslant \neg\neg((\neg x \to y) \to \neg\neg(\neg y \to x))\\ &= (\neg x \to y) \to \neg\neg(\neg y \to x)\end{aligned}$$

for all $x, y \in L$. If follows from (4.36) and (2.18) that

$$\tilde{f}(1) = \tilde{f}(\neg\neg(\neg\neg x \to x)) \subseteq \tilde{f}((y \to \neg\neg x) \to \neg\neg(y \to x)) \tag{4.39}$$

and

$$\tilde{f}(1) = \tilde{f}(\neg\neg(\neg\neg x \to x)) \subseteq \tilde{f}((\neg x \to y) \to \neg\neg(\neg y \to x)). \tag{4.40}$$

Combining (2.19), (4.39) and (4.40), we have $\tilde{f}((y \to \neg\neg x) \to \neg\neg(y \to x)) = \tilde{f}(1)$ and $\tilde{f}((\neg x \to y) \to \neg\neg(\neg y \to x)) = \tilde{f}(1)$ for all $x, y \in L$. Therefore (ii) and (iii) are valid. Let $\left(\tilde{f}, L\right)$ be an int-soft filter of $\mathcal{L}$ over U that satisfies the condition (4.37). If we take $y := \neg\neg x$ in (4.37) and use (2.1), then we can induce the condition (4.36) and so $\left(\tilde{f}, L\right)$ is a strong int-soft filter of $\mathcal{L}$ over U. Let $\left(\tilde{f}, L\right)$ be an int-soft filter of $\mathcal{L}$ over U that satisfies the condition (4.38). Taking $y := \neg x$ in (4.38) and using (2.1) induces the condition (4.36). Hence $\left(\tilde{f}, L\right)$ is a strong int-soft filter of $\mathcal{L}$ over U. □

We investigate relationship between a divisible int-soft filter and a strong int-soft filter.

Theorem 4.16. *Every divisible int-soft filter is a strong int-soft filter.*

Proof. Let $\left(\tilde{f}, L\right)$ be a divisible int-soft filter of $\mathcal{L}$ over U. If we put $x := \neg\neg x$ and $y := x$ in (4.22), then we have

$$\tilde{f}((\neg\neg x \wedge x) \to (\neg\neg x \otimes (\neg\neg x \to x))) = \tilde{f}(1). \tag{4.41}$$

Using (2.5) and (2.4), we get

$$\begin{aligned}(\neg\neg x \wedge x) \to (\neg\neg x \otimes (\neg\neg x \to x)) &\leqslant \neg(\neg\neg x \otimes (\neg\neg x \to x)) \to \neg(\neg\neg x \wedge x)\\ &\leqslant (\neg\neg x \otimes \neg(\neg\neg x \otimes (\neg\neg x \to x))) \to (\neg\neg x \otimes \neg(\neg\neg x \wedge x))\\ &\leqslant \neg(\neg\neg x \otimes \neg(\neg\neg x \wedge x)) \to \neg(\neg\neg x \otimes \neg(\neg\neg x \otimes (\neg\neg x \to x)))\end{aligned}$$

for all $x \in L$. It follows from (4.41) and (2.18) that

$$\begin{aligned}\tilde{f}(1) &= \tilde{f}((\neg\neg x \wedge x) \to (\neg\neg \otimes (\neg\neg x \to x)))\\ &\subseteq \tilde{f}(\neg(\neg\neg x \otimes \neg(\neg\neg x \wedge x)) \to \neg(\neg\neg x \otimes \neg(\neg\neg x \otimes (\neg\neg x \to x)))).\end{aligned} \tag{4.42}$$

Combining (4.42) with (2.19), we have

$$\tilde{f}(\neg(\neg\neg x \otimes \neg(\neg\neg x \wedge x)) \to \neg(\neg\neg x \otimes \neg(\neg\neg x \otimes (\neg\neg x \to x)))) = \tilde{f}(1) \tag{4.43}$$

for all $x \in L$. Using (2.2), (2.10), (2.12) and (2.11), we get

$$\begin{aligned}\neg(\neg\neg x \otimes \neg(\neg\neg x \wedge x)) &= \neg\neg x \to \neg\neg(\neg\neg x \wedge x)\\ &\geq \neg\neg(x \to (\neg\neg x \wedge x))\\ &= \neg\neg(x \to (x \wedge \neg\neg x))\\ &= \neg\neg(x \to \neg\neg x) = \neg\neg 1 = 1\end{aligned}$$

and so $\neg(\neg\neg x \otimes \neg(\neg\neg x \wedge x)) = 1$ for all $x \in L$. It follows from (4.43) and (2.20) that

$$\begin{aligned}&\tilde{f}(\neg(\neg\neg x \otimes \neg(\neg\neg x \otimes (\neg\neg x \to x))))\\ &\supseteq \tilde{f}(\neg(\neg\neg x \otimes \neg(\neg\neg x \wedge x)) \to \neg(\neg\neg x \otimes \neg(\neg\neg x \otimes (\neg\neg x \to x)))) \cap\\ &\qquad\qquad \tilde{f}(\neg(\neg\neg x \otimes \neg(\neg\neg x \wedge x)))\\ &= \tilde{f}(1)\end{aligned}$$

and so that

$$\begin{aligned}\tilde{f}(1) &= \tilde{f}(\neg(\neg\neg x \otimes \neg(\neg\neg x \otimes (\neg\neg x \to x))))\\ &= \tilde{f}(\neg(\neg\neg x \otimes (\neg\neg x \to \neg(\neg\neg x \to x)))).\end{aligned} \tag{4.44}$$

Taking $x := \neg\neg x$ and $y := \neg(\neg\neg x \to x)$ in (4.22) induces

$$\begin{aligned}\tilde{f}(1) &= \tilde{f}((\neg\neg x \wedge \neg(\neg\neg x \to x)) \to (\neg\neg x \otimes (\neg\neg x \to \neg(\neg\neg x \to x))))\\ &\subseteq \tilde{f}(\neg(\neg\neg x \otimes (\neg\neg x \to \neg(\neg\neg x \to x))) \to \neg(\neg\neg x \wedge \neg(\neg\neg x \to x)))\end{aligned}$$

by using (2.3) and (2.18). Thus

$$\tilde{f}(\neg(\neg\neg x \otimes (\neg\neg x \to \neg(\neg\neg x \to x))) \to \neg(\neg\neg x \wedge \neg(\neg\neg x \to x))) = \tilde{f}(1). \quad (4.45)$$

Since $\neg(\neg\neg x \to x) \leqslant \neg\neg x$ for all $x \in L$, it follows from (2.19), (2.20), (4.44) and (4.45) that

$$\tilde{f}(1) = \tilde{f}(\neg(\neg\neg x \wedge \neg(\neg\neg x \to x))) = \tilde{f}(\neg\neg(\neg\neg x \to x))$$

for all $x \in L$. Therefore $\left(\tilde{f}, L\right)$ is a strong int-soft filter of $\mathcal{L}$ over U. □

Corollary 4.17. *If an int-soft filter* $\left(\tilde{f}, L\right)$ *of* $\mathcal{L}$ *over* U *satisfies one of conditions* (4.28)*,* (4.29)*,* (4.31)*,* (4.32)*,* (4.33) *and* (4.34)*, then* $\tilde{f}$ *is a strong int-soft filter of* $\mathcal{L}$ *over* U*.*

The following example shows that the converse of Theorem 4.16 may not be true in general.

Example 4.18. The strong int-soft filter $\tilde{f}$ of $\mathcal{L}$ over U which is given in Example 4.14 is not a divisible int-soft filter of $\mathcal{L}$ over U since

$$\tilde{f}((a \wedge c) \to (a \otimes (a \to c))) = \tilde{f}(a) \neq \tilde{f}(1).$$

5 Conclusions

We have considered the soft set theoretical approach to residuated lattices. We have discussed (filteristic) soft residuated lattices We have defined divisible int-soft filters and strong int-soft filters, and have investigated related properties. We have discussed characterizations of a divisible and strong int-soft filter, and have provided conditions for an int-soft filter to be divisible. We have establish relations between a divisible int-soft filter and a strong int-soft filter. In a forthcoming paper, we will study the int-soft version of n-contractive filters in residuated lattices, and apply the results to the another type filters in residuated lattices.

Acknoweledgments. This work was supported by National Natural Science Foundation of China (Grant No. 61573240, 61473239).

References

[1] **R. Belohlavek**, *Some properties of residuated lattices,* Czechoslovak Math. J. **53(123)** (2003), 161 – 171.

[2] **N. Çağman and S. Enginoğlu**, *Soft set theory and uni-int decision making,* Eur. J. Oper. Res. **207** (2010), 848 – 855.

[3] **F. Esteva and L. Godo**, *Monoidal t-norm based logic, towards a logic for left-continuous t-norms,* Fuzzy Sets and Systems **124** (2001), 271 – 288.

[4] **P. Hájek**, *Metamathematics of Fuzzy Logic,* Kluwer Academic Press, Dordrecht, 1998.

[5] **Y.B. Jun and C.H. Park**, *Applications of soft sets in ideal theory of BCK/BCI-algebras,* Inform. Sci. **178** (2008), 2466 – 2475.

[6] **Z.M. Ma and B.Q. Hu**, *Characterizations and new subclasses of $\mathcal{I}$-filters in residuated lattices,* Fuzzy Sets and Systems **247** (2014), 92 – 107.

[7] **P.K. Maji, R. Biswas and A.R. Roy**, *Soft set theory,* Comput. Math. Appl. **45** (2003), 555 – 562.

[8] **P.K. Maji, A.R. Roy and R. Biswas**, *An application of soft sets in a decision making problem,* Comput. Math. Appl. **44** (2002), 1077 – 1083.

[9] **D. Molodtsov**, *Soft set theory - First results,* Comput. Math. Appl. **37** (1999), 19 – 31.

[10] **J.G. Shen and X.H. Zhang**, *Filters of residuated lattices.* Chin. Quart. J. Math. **21** (2006), 443 – 447.

[11] **E. Turunen**, *BL-algebras of basic fuzzy logic,* Mathware Soft Comput. **6** (1999), 49 – 61.

[12] **E. Turunen**, *Boolean deductive systems of BL-algebras,* Arch. Math. Logic **40** (2001), 467 – 473.

[13] **L.A. Zadeh**, *From circuit theory to system theory,* Proc. Inst. Radio Eng. **50** (1962), 856 – 865.

[14] **L.A. Zadeh**, *Fuzzy sets,* Information and Control **8** (1965), 338–353.

[15] **L.A. Zadeh**, *Toward a generalized theory of uncertainty (GTU) – an outline,* Inform. Sci. **172** (2005), 1 – 40.

[16] **X.H. Zhang, H. Zhou and X. Mao**, *$IMTL(MV)$-filters and fuzzy $IMTL(MV)$-filters of residuated lattices,* J. Intell. Fuzzy Systems **26** (2014), 589 – 596.

[17] **Y.Q. Zhu and Y. Xu**, *On filter theory of residuated lattices,* Inform. Sci. **180** (2010), 3614 – 3632.

Rceived March 2, 2016

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

X.H. Zhang
Department of Mathematics, College of Arts and Sciences, Shanghai Maritime University,
Shanghai 201306, P.R. China
E-mail: zxhonghz@263.net

On the paper "On dual ordered semigroups"

Niovi Kehayopulu

Abstract. This is about the paper by Thawhat Changphas and Nawamin Phaipong in Quasigroups and Related Systems 22 (2014), 193–200.

This paper is actually the introduction and the main part from section 2 (the first decomposition theorem) of the paper by St. Schwarz [3]. The authors considered an ordered semigroup $(S, \cdot, \leq)$ instead of the semigroup $(S, \cdot)$ considered by Schwarz. The order plays a very little role in Lemma 1.1(1), Lemma 1.1(4), Lemma 2.7 and Lemma 2.15(3),(4) (the Lemma 2.8 and Corollaries 2.9 and 2.10 are immediate consequences of Lemma 2.7), but the proofs of Lemma 1.1(1) and Lemma 1.1(4) are wrong. In addition, the Lemma 1.1(4) does not need any proof since it is an immediate consequence of Lemma 1.1(1). This is a copy of the proof of the Lemma 1.1(1) in [1]: *If* $x \in l(A)$ *and* $S \ni y \leq x$*, then* $yA \subseteq xA = 0$*, and hence* $y \in l(A)$. As we see, according to this proof, we first have $yA \subseteq xA$ (there is no the proof in the paper) and then, based on it, we have $y \in l(A)$. But to prove that $x \in l(A)$ and $S \ni y \leq x$ implies $yA \subseteq xA$ (that actually implies $yA = xA$), we first have to prove that $y \in l(A)$. Then our argument is finished and we do not go back to use the $yA \subseteq xA$ to prove that $y \in l(A)$ (which has been already proved before the proof of the $yA \subseteq xA$). So when the authors say "If $x \in l(A)$ and $S \ni y \leq x$ implies $yA \subseteq xA$", they cannot mean anything else than the "$y \leq x$ implies $yA \subseteq xA$", and this is not true in general. The same problem occurs in the proof of Lemma 1.1(4) of the paper in [1]. It might be mentioned here that $y \leq x$ implies $yA \subseteq (xA]$.

Let us prove that if M is a right (resp. left) ideal of an ordered semigroup S, then $y \leq x$ does not imply $My \subseteq Mx$ (resp. $yM \subseteq xM$) in general. This shows the mistake in Lemma 1.1(1) as well, as the right and the left ideals of an ordered semigroup S are nonempty subsets of S.

Example. [2] Consider the ordered semigroup $S = \{a, b, c, d, f\}$ defined by the multiplication and the covering relation given below:

2010 Mathematics Subject Classification: 06F05, 20M10
Keywords: dual semigroup; dual ordered semigroup; left (right) ideal.

$\cdot$	a	b	c	d	f
a	a	b	a	a	a
b	a	b	a	a	a
c	a	b	c	a	a
d	a	b	a	a	d
f	a	b	a	a	f

$$\prec = \{a,b),(c,a),(d,a)\}.$$

The set $M = \{a,c,d\}$ is a left ideal of S, $c \leq a$ but $cM \nsubseteq aM$. The set $M = \{a,b,c,d\}$ is a right ideal of S, $c \leq a$ but $Mc \nsubseteq Ma$. □

This is the corrected form of Lemma 1.1(1) and its proof:

Lemma 1.1(1). *If $(S,.,\leq)$ is an ordered semigroup with zero and A a nonempty subset of S, then the set $l(A)$ is a left ideal and the set $r(A)$ is a right ideal of S.*

Proof. The set $l(A)$ is a left ideal of the semigroup $(S,.)$ [3]. Let now $x \in l(A)$ and $S \ni y \leq x$. Then $y \in l(A)$, that is, $yA = \{0\}$. Indeed: if $z \in A$, then $yz \leq xz \in xA = \{0\}$, so $yz = 0$. Since $yA \subseteq \{0\}$ and $yA \neq \emptyset$, we have $yA = \{0\}$. □

References

[1] **T. Changphas and N. Phaipong**, *On dual ordered semigroups*, Quasigroups and Related Systems **22** (2014), 193 – 200.

[2] **N. Kehayopulu**, *On regular, intra-regular ordered semigroups*, Pure Math. Appl. (PU.M.A.) **4** (1993), 447 – 461.

[3] **S. Schwarz**, *On dual semigroups*, Czechoslovak Math. J. **10** (85) (1960), 201 – 230.

Received May 12, 2016

University of Athens
Department of Mathematics
15784 Panepistimiopolis
Athens, Greece
E-mail: nkehayop@math.uoa.gr

Quasigroups and Related Systems **24** (2016), 249 − 268

Cryptcodes Based on Quasigroups in Gaussian channel

Daniela Mechkaroska, Aleksandra Popovska-Mitrovikj, Verica Bakeva

Abstract. Cryptcodes based on quasigroups transformation, known as Random Codes Based on Quasigroups (RCBQ) are error-correcting codes defined by using a cryptographic algorithm during the encoding/decoding process. Therefore, they allow not only correction of certain amount of errors in the input data, but they also provide an information security, all built in one algorithm. Standard and Cut-Decoding algorithms for these codes are defined elsewhere. Also, performances of these codes are investigated elsewhere, when a transmission through a binary symmetric channel is used. In this paper, we investigate the performances of RCBQ for transmission through Gaussian channel. We analyze the influence of the code parameters on the performances of RCBQ for code (72,288) with rate 1/4. We present and compare several experimental results obtained with different coding/decoding algorithms for these codes.

1. Introduction

Random Codes Based on Quasigroups (RCBQ) considered in this paper are cryptcodes. In order to provide an information security cryptcodes include an application of some of the known ciphers on codewords, before sending them through an insecure channel ([11, 12]). Usually, in the design of these codes two algorithms are used, one for error-correcting and another for obtaining information security. In the paper [4] authors give one algorithm where a block cipher and an error-correcting code are combined. But, the main application of their design is for cryptographic purposes, although it can be used as an error-correcting code.

RCBQs are proposed in [2] and they are defined by using a cryptographic algorithm during the encoding/decoding process. They allow not only correction of certain amount of errors in the input data, but they also provide an information security, all built in one algorithm. Therefore, these codes are interesting for further investigation. The influence of the code parameters on the performances of these codes are investigated in [6]. In [5] authors compare the performances of RCBQ with Reed-Solomon and Reed-Muller codes. From the results for packet-error and bit-error probabilities given there, authors concluded that RCBQ outperforms Reed-Muller and Reed-Solomon codes significantly for $p \geqslant 0.05$ in binary

2010 Mathematics Subject Classification: 94B35, 94B60, 68P30, 20N05.
Keywords: quasigroup, random code, error-correcting code, cryptcoding, packet-error probability, bit-error probability.

symmetric channel. But, the time efficiency of RCBQ is much lower than time efficiency of these two popular codes. In order to improve the decoding speed and other performances of RCBQ, in [7, 9] authors proposed new coding/decoding algorithms. In all papers for RCBQs, transmission through a binary symmetric channel is considered. Here, we investigate performances of these codes for transmission through Gaussian channel where the noise is a random variable with normal $N(0, N_0)$ distribution. In this channel, the probability of bit-error (see [10]) is given by

$$P_b = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N_0}}\right), \tag{1}$$

where E_b is a power constraint.

RCBQs are designed using algorithm for encryption/decryption from the implementation of TASC (Totally Asynchronous Stream Ciphers) by quasigroup string transformation ([1]). These cryptographic algorithms use the alphabet Q and a quasigroup operation $*$ on Q together with its parastrophe " $\backslash$ ". The notions of quasigroups and quasigroup string transformations are given in the previous papers for these codes ([5], [6]). Here, we are using the same terminology and notations as there. Note that in this paper we consider only ability of RCBQ for corrections of errors in the transmitted data. The provided information security is guaranteed from the used quasigroup string transformation E given in [3].

The rest of this paper is organized as follows. In Section 2, we will briefly repeat the coding/decoding algorithms of RSBQ. In Section 3 we explain how the experiments are made. The influence of the code parameters on the performances of RCBQ with Standard algorithm is investigated in Section 4. In Section 5, we present experimental results obtained with Cut-Decoding algorithm and we compare these results with the best results for Standard algorithm. In order to improve the performances of Cut-Decoding algorithm for transmission through Gaussian channel, in Section 6, we define two combinations of the proposed methods for decreasing the number of unsuccessful decodings. At the end, we give some conclusions.

2. Description of RCBQ

Description of coding with Standard and Cut-Decoding algorithms

Let $M = m_1 m_2 \dots m_l$ be a block of $N_{block} = 4l$ bits where $m_i \in Q$ and Q is an alphabet of 4-bit symbols (nibbles). First, we add a redundancy as zero symbols and produce message

$$L = L^{(1)} L^{(2)} ... L^{(s)} = L_1 L_2 ... L_m,$$

of $N = 4m$ bits ($m = rs$), where $L_i \in Q$, $L^{(i)}$ are sub-blocks of r symbols from Q. After erasing the redundant zeros from each $L^{(i)}$, the message L will produce the original message M. In this way we obtain (N_{block}, N) code with rate $R = N_{block}/N$. The codeword is produced after applying the encryption algorithm of TASC (given in Figure 1) on the message L. For this aim, a key $k = k_1k_2...k_n \in Q^n$ should be chosen. The obtained codeword of M is

$$C = C_1C_2...C_m,$$

where $C_i \in Q$.

Encryption	**Decryption**
Input: Key $k = k_1k_2\dots k_n$ and $L = L_1L_2\dots L_m$ **Output**: codeword $C = C_1C_2...C_m$	**Input**: The pair $(a_1a_2\dots a_r, k_1k_2\dots k_n)$ **Output**: The pair $(c_1c_2\dots c_r, K_1K_2\dots K_n)$

```
For $j = 1$ to $m$
    $X \leftarrow L_j$;
    $T \leftarrow 0$;
    For $i = 1$ to $n$
        $X \leftarrow k_i * X$;
        $T \leftarrow T \oplus X$;
        $k_i \leftarrow X$;
    $k_n \leftarrow T$
Output: $C_j \leftarrow X$
```

```
For $i = 1$ to $n$
    $K_i \leftarrow k_i$;
For $j = 0$ to $r - 1$
    $X, T \leftarrow a_{j+1}$;
    $temp \leftarrow K_n$;
    For $i = n$ to 2
        $X \leftarrow temp \setminus X$;
        $T \leftarrow T \oplus X$;
        $temp \leftarrow K_{i-1}$;
        $K_{i-1} \leftarrow X$;
    $X \leftarrow temp \setminus X$;
    $K_n \leftarrow T$;
    $c_{j+1} \leftarrow X$;
Output: $(c_1c_2\dots c_r, K_1K_2\dots K_n)$
```

Figure 1: Algorithms for encryption and decryption

In Cut-Decoding algorithm, instead of using (N_{block}, N) code with rate R, we use together two $(N_{block}, N/2)$ codes with rate $2R$ for coding/decoding the same message of N_{block} bits. Namely, for coding we apply two times the encryption algorithm, given in Figure 1, on the same redundant message L using different parameters (different keys or quasigroups). In this way we obtain the codeword of the message as concatenation of the two codewords of $N/2$ bits.

Description of decoding with Standard and Cut-Decoding algorithm

After transmission through a noise channel (for our experiments we use Gaussian channel), the codeword C will be received as message $D = D^{(1)}\, D^{(2)} \dots D^{(s)} = D_1D_2\dots D_m$ where $D^{(i)}$ are blocks of r symbols from Q and $D_i \in Q$. The decoding process consists of four steps: (i) procedure for generating the sets with predefined Hamming distance, (ii) inverse coding algorithm, (iii) procedure for generating decoding candidate sets and (iv) decoding rule.

Let B_{max} be a given integer which denotes the asumed maximum number of errors occur in a block during transmission. The probability that at most t bits in D^i are not correctly transmitted is

$$P(P_b;t) = \sum_{k=0}^{t} \binom{4r}{k} P_b^k (1-P_b)^{4r-k},$$

where P_b is probability of bit-error in a Gaussian channel. Then $P(P_b; B_{max})$ is the probability that at most B_{max} errors occur in a block during transmission. We generate the sets $H_i = \{\alpha | \alpha \in Q^r, \quad H(D^{(i)}, \alpha) \leqslant B_{max}\}$, for $i = 1, 2, \ldots, s$, where $H(D^{(i)}, \alpha)$ is the Hamming distance between $D^{(i)}$ and α.

The decoding candidate sets S_0, S_1, S_2,...,S_s, are defined iteratively. Let $S_0 = (k_1 \ldots k_n; \lambda)$, where λ is the empty sequence. Let S_{i-1} be defined for $i \geqslant 1$. Then S_i is the set of all pairs $(\delta, w_1 w_2 \ldots w_{4ri})$ obtained by using the sets S_{i-1} and H_i as follows (w_j are bits). For each element $\alpha \in H_i$ and each $(\beta, w_1 w_2 \ldots w_{4r(i-1)}) \in S_{i-1}$, we apply the inverse coding algorithm (i.e., algorithm for decryption given in Figure 1) with input (α, β). If the output is the pair (γ, δ) and if both sequences γ and $L^{(i)}$ have the redundant zeros in the same positions, then the pair $(\delta, w_1 w_2 \ldots w_{4r(i-1)} c_1 c_2 \ldots c_r) \equiv (\delta, w_1 w_2 \ldots w_{4ri})$ $(c_i \in Q)$ is an element of S_i.

The decoding of the received message D is given by the following rule: If the set S_s contains only one element

$$(d_1 \ldots d_n, w_1 \ldots w_{4rs}),$$

then $L = w_1 \ldots w_{4rs}$ is the decoded (redundant) message and we say that we have a *successful decoding*. In the case when the set S_s contains more than one element then the decoding of D is unsuccessful and we say a *more-candidate-error* appears. In the case when $S_j = \emptyset$ for some $j \in \{1, \ldots, s\}$, the process will be stopped and we say that a *null-error* appears.

In Cut-Decoding algorithm, after transmitting through a noise channel, we divide the outgoing message $D = D^{(1)} D^{(2)} \ldots D^{(s)}$ in two messages $D_1 = D^{(1)} D^{(2)} \ldots D^{(s/2)}$ and $D_2 = D^{(s/2+1)}\ D^{(s/2+2)} \ldots D^{(s)}$ with equal lengths and we decode them parallel with the corresponding parameters. In this decoding algorithm we make modification in the procedure for generating decoding candidate sets. Let $S_i^{(1)}$ and $S_i^{(2)}$ be the decoding candidate sets obtained in the i^{th} iteration of the two parallel decoding processes, $i = 1, \ldots, s$. Then, before the next iteration we eliminate from $S_i^{(1)}$ all elements whose second part does not match with the second part of an element in $S_i^{(2)}$, and vice versa. In the $(i+1)^{th}$ iteration the both processes use the corresponding reduced sets $S_i^{(1)}$ and $S_i^{(2)}$. With Cut-Decoding algorithm the decoding speed is improved and the values of the packet-error probability (PER) and the bit-error probability (BER) for code $(72, 288)$ are smaller.

3. Experiments

The experiments with the random codes based on quasigroup are made on a high performance claster on Faculty of Computer Science and Engineering, UKIM - Skopje. The cluster has 24 GB RAM, a processor with 2.266 GHz and 12 physical cores (24 logical cores) are used.

The experiments are made in the following way:

- Firstly, we extend the message obtained from the source using a pattern for adding redundant zero nibbles. We made experiments with 6 different patterns.
- The extended message is coded using an algorithm for coding (Standard or Cut-Decoding) and blocks of 4 nibbles.
- On the coded message we make $BPSK$ modulation ($0 \to -1$ and $1 \to 1$).
- The signal is transmitted through Gaussian channel and due to the noises, the received output signal can be different from the input signal.
- Then, we make demodulation on the output signal in the following way:
    1) if the received signal is greater than 0, then the receiver assumes that bit 1 was transmitted;
    2) if the received signal is less than 0, then the receiver assumes that bit 0 was transmitted.
- The demodulated message is decoded with the corresponding (previously defined) decoding algorithm.
- We compare the decoded message with the input message and compute BER and PER for different values of SNR in the interval from -3 to 10.

The packet-error probability PER is computed as a ratio of the number of incorrectly decoded packets (messages) and the number of all packets. The incorrectly decoded packets appear in the following cases:

1. If the last decoding candidate set S_s has only one element, then the message in that element (the decoded message) is compared with the input message. If both are equal then we have a correct decoding. If the decoded message differs in at least one bit then we have an uncorrected error.
2. Packet errors appear in other cases of unsuccessful decoding (*more-candidate errors* and *null-errors*).

The bit-error probability BER is computed as a ratio of the number of incorrectly decoded bits and the number of all bits. The incorrectly decoded bits appear in the following cases:

1. When the decoding is successful, we compare the decoded and the input message computing Hamming distance between them. It gives the number of incorrectly decoded bits.

2. When *a null-error* appears, i.e., $S_i = \emptyset$ for some $0 \leqslant j \leqslant s$, we take all elements from the set S_{i-1} and we find their maximal common prefix substring. If this string has k bits and the length of the input message is $4l$ bits then we compare this substring with the first k bits of the input message. If they differ in t bits then the number of incorrectly decoded bits is $4l - k + t$.

3. If *a more-candidate-error* appears we take all elements from the set S_s and we find their maximal common prefix substring. The number of incorrectly decoded bits is computed as previously.

4. Experimental results for Standard algorithm

In this section we present and analyze the results obtained using Standard coding/decoding algorithm for RCBQ. We investigate the influence of the code parameters on the code performances.

The influence of the pattern on the code performances

In order to check the influence of the pattern on the code performances, we made experiments with 6 different patterns for redundant zero nibbles for code $(72, 288)$ with rate $R = 1/4$. This means that the alphabet

$$Q = \{0, 1, 2, 3, 4, 5, 6, 8, 9, \mathrm{a}, \mathrm{b}, \mathrm{c}, \ \mathrm{d}, \mathrm{e}, \mathrm{f}\}.$$

In these experiments we have used the quasigroup $(Q, *)$ and its parastrophe $(Q, \backslash)$ given in Table 1, the initial key $k = 0123456789$ and 6 patterns given in Table 2. In the patterns, we denote the message (information) symbol with 1 and the redundant zero symbol with 0. The experiments for different values of SNR in the interval from -3 to 10 dB are made. In this section we present the experimental results for bit-error probability (BER) and packet-error probability (PER).

Firstly, we made experiments for $B_{max} = 3$ with 13888 messages. The obtained results for BER are given in Table 3 and presented in Figure 2, while the appropriate values of PER are presented in Table 4 and Figure 3.

The experimental results for BER are compared with a probability P_b for bit-error in Gaussian channel. It is obvious that the values of BER and PER increase as the values of SNR decrease (smaller values of SNR mean larger noise). Therefore, we made experiments starting from $SNR = 10$ and decreasing the values of SNR by 1. We stoppped with experiments when we get $BER > P_b$. In this case the codes does not have sense since the bit-error probability obtained using the code is greater than the bit-error probability P_b without coding. All experimental results for BER obtained using pattern 1 and pattern 5 were greater

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

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

Table 1: Quasigroup of order 16 used in the experiments and corresponding parastrophe

pattern 1	**pattern 2**	**pattern 3**	**pattern 4**	**pattern 5**	**pattern 6**
1000 1000	1100 1100	1100 1100	1100 1100	1100 1000	1100 1100
1000 1000	0000 1100	1000 0000	1100 0000	0000 1100	1000 0000
1000 1000	1100 0000	1100 1000	0000 1100	1000 0000	1100 1100
1000 1000	1100 1100	1000 0000	1100 1100	1100 1000	1000 0000
1000 1000	0000 1100	1100 1100	0000 0000	0000 1100	1100 1100
1000 1000	1100 0000	1000 0000	1100 1100	1000 0000	1000 0000
1000 1000	1100 0000	1100 1000	1100 0000	1100 1000	1000 1000
1000 1000	0000 0000	1000 0000	0000 0000	0000 1100	1000 0000
1000 1000	0000 0000	0000 0000	0000 0000	1000 0000	0000 0000

Table 2: Patterns for redundant zero nibbles

than P_b and therefore these results are not present in the following tables and figures.

From all experimental results given in the tables and figures we can see that when the value of SNR increases, the bit-error and packet-error probabilities decrease.

SNR	**pattern 2**	**pattern 3**	**pattern 4**	**pattern 6**
1	0.08637	0.08737	0.10262	0.08838
2	0.02054	0.02075	0.02418	0.02057
3	0.00387	0.00408	0.00398	0.00321
4	0.00055	0.00046	0.00030	0.00016
5	0	0	0.00007	0
6	0	0	0	0.00004
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Table 3: Experimental results for BER for different patterns and $B_{max} = 3$

From Figure 2 and Figure 3 we can notice that none of the considered patterns

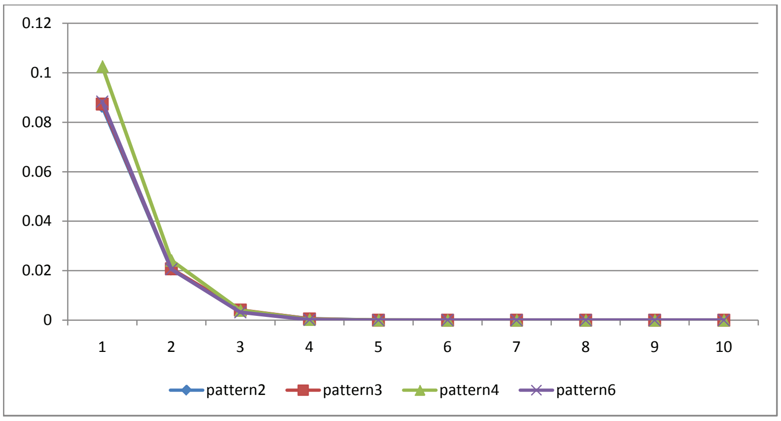


Figure 2: Experimental results for BER for different patterns and $B_{max} = 3$

SNR	pattern 2	pattern 3	pattern 4	pattern 6
1	0.176915	0.17519	0.171659	0.175403
2	0.043707	0.04435	0.040971	0.043131
3	0.007488	0.00801	0.007056	0.007272
4	0.001008	0.00086	0.000648	0.000432
5	0	0	0.00007	0
6	0	0	0	0.00007
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Table 4: Experimental results for PER for different patterns and $B_{max} = 3$

stands out as the best or as the worst, i.e., for all patterns the values of BER (PER) are very close. In these experiments we did not obtain any unsuccessful decoding with *more-candidate-error*. So, all unsuccessful decodings are *null-errors*, whose number decreases when SNR increases.

Further on, we made experiments with the same parameters, but for $B_{max} = 4$. The decoding process in these experiments is much slower than for $B_{max} = 3$ since the number of elements in the sets S_i are greater. The obtained results for BER are presented in Table 5 and Figure 4, and the results for PER in Table 6 and Figure 5.

From Figure 4, we can see that pattern 6 is the worst pattern for this value of B_{max}, while the other patterns give almost equal values of BER (the differences are in the fourth decimal). Only for smaller values of SNR pattern 3 gives better results than pattern 2 and pattern 4.

As we concluded before, for $B_{max} = 3$, *more-candidate-error* does not appear with none of the patterns. But, from the experiment for $B_{max} = 4$ we can conclude the following:

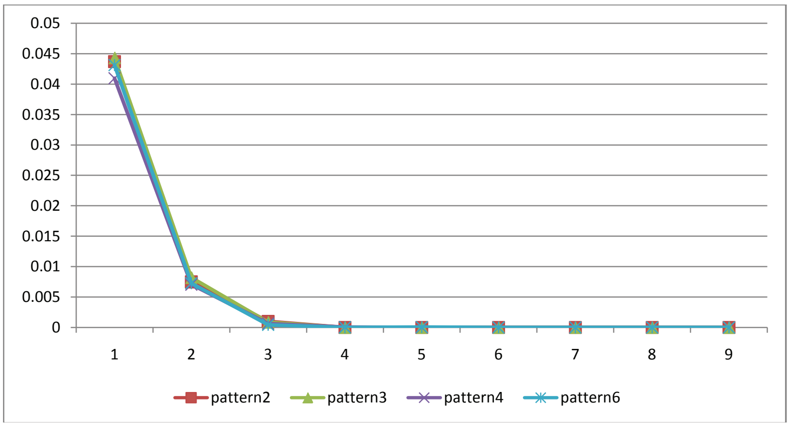


Figure 3: Experimental results for PER for different patterns and $B_{max} = 3$

SNR	pattern 2	pattern 3	pattern 4	pattern 6
0	0.10582	0.08343	0.09630	0.94627
1	0.02411	0.01928	0.02336	0.24562
2	0.00361	0.00400	0.00424	0.04602
3	0.00049	0.00068	0.00047	0.00788
4	0.00024	0.00042	0.00014	0.00202
5	0.00004	0.00066	0.00016	0.00136
6	0.00032	0.00054	0.00016	0.00374
7	0.00025	0.00046	0.00011	0.00354
8	0.00025	0.00053	0.00004	0.00372
9	0.00025	0.00053	0.00004	0.00372
10	0.00025	0.00053	0.00004	0.00372

Table 5: Experimental results for BER for different patterns and $B_{max} = 4$

SNR	pattern 2	pattern 3	pattern 4	pattern 6
0	0.10750	0.10829	0.10808	0.10707
1	0.02448	0.02520	0.02635	0.02758
2	0.00367	0.00554	0.00482	0.00511
3	0.00050	0.00137	0.00065	0.00086
4	0.00029	0.00101	0.00014	0.00029
5	0.00007	0.00144	0.00004	0.00014
6	0.00036	0.00115	0.00029	0.00043
7	0.00029	0.00108	0.00022	0.00043
8	0.00029	0.00122	0.00001	0.00043
9	0.00029	0.00122	0.00001	0.00043
10	0.00029	0.00122	0.00001	0.00043

Table 6: Experimental results for PER for different patterns and $B_{max} = 4$

- for $SNR \leqslant 3$, we obtain more *null-errors* than *more-candidate-errors*;
- for $SNR > 3$, we do not have *null-errors*, but we have *more-candidate-errors*.

In order to reduce the number of unsuccessful decodings with *more-candidate-error*, we use the heuristic introduced in [7] in the experiments with $B_{max} = 4$.

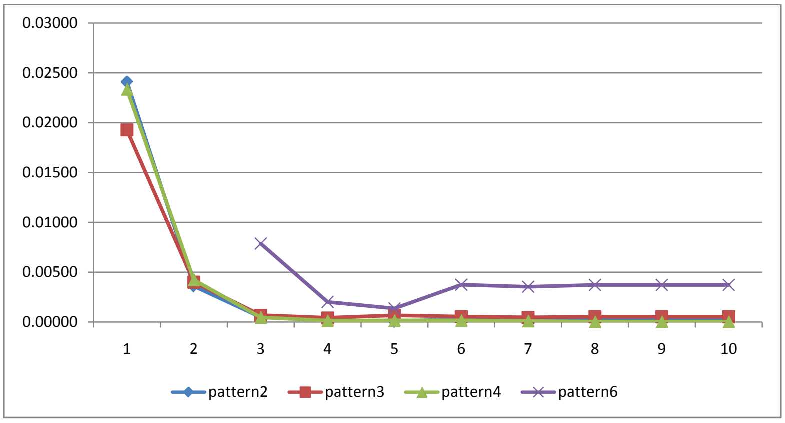


Figure 4: Experimental results for BER for different patterns and $B_{max} = 4$

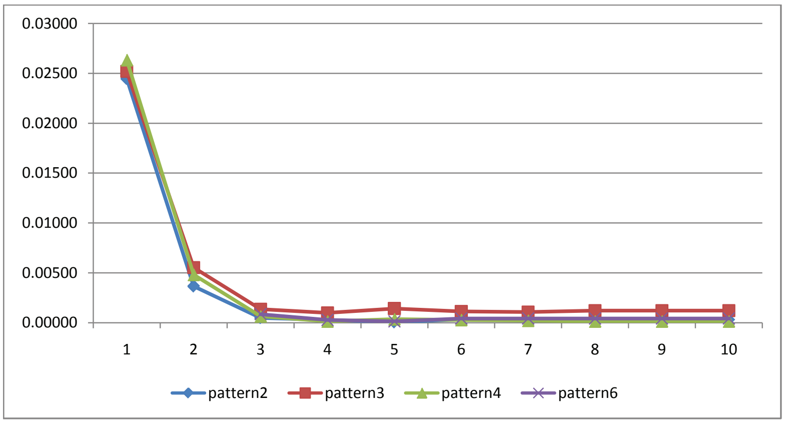


Figure 5: Experimental results for PER for different patterns and $B_{max} = 4$

According to this heuristic, in the case of *more-candidate-error* we randomly select a message from the last decoding candidate set and it is taken as decoded message. The results for BER and PER obtained using the heuristic are presented in Table 7 and Table 8 (Figure 6 and Figure 7), correspondingly. From the results, we can conclude that using this heuristic, the values of BER and PER are slightly better.

From the previous experiments, we can conclude that the chosen pattern has a great influence on the code performances. For some patterns (for example, **pattern 1** and **pattern 5** given in Table 2) the coding does not have a sense.

SNR	pattern 2	pattern 3	pattern 4	pattern 6
0	0.10582	0.08301	0.09609	0.94627
0.5	0.05395	0.04187	0.04913	0.48607
1	0.02397	0.01919	0.02336	0.24562
1.5	0.01169	0.00923	0.00960	0.08374
2	0.00361	0.00368	0.00424	0.04602
3	0.00042	0.00052	0.00047	0.00788
4	0.00011	0.00028	0.00014	0.00202
5	0.00004	0.00031	0.00016	0.00136
6	0.00025	0.00025	0.00016	0.00374
7	0.00018	0.00032	0.00011	0.00354
8	0.00018	0.00035	0.00004	0.00372
9	0.00018	0.00035	0.00004	0.00372
10	0.00018	0.00035	0.00004	0.00372

Table 7: Experimental results for BER for $B_{max} = 4$ using the heuristic for decreasing of *more-candidate-errors*

SNR	pattern 2	pattern 3	pattern 4	pattern 6
0	0.10750	0.10829	0.10808	0.10707
1	0.02434	0.02506	0.02635	0.02758
2	0.00367	0.00490	0.00482	0.00511
3	0.00043	0.00058	0.00065	0.00086
4	0.00014	0.00058	0.00014	0.00029
5	0.00007	0.00065	0.00036	0.00014
6	0.00029	0.00043	0.00029	0.00043
7	0.00022	0.00058	0.00022	0.00043
8	0.00022	0.00065	0.00014	0.00043
9	0.00022	0.00065	0.00014	0.00043
10	0.00022	0.00065	0.00014	0.00043

Table 8: Experimental results for PER for $B_{max} = 4$ using the heuristic for decreasing of *more-candidate-errors*

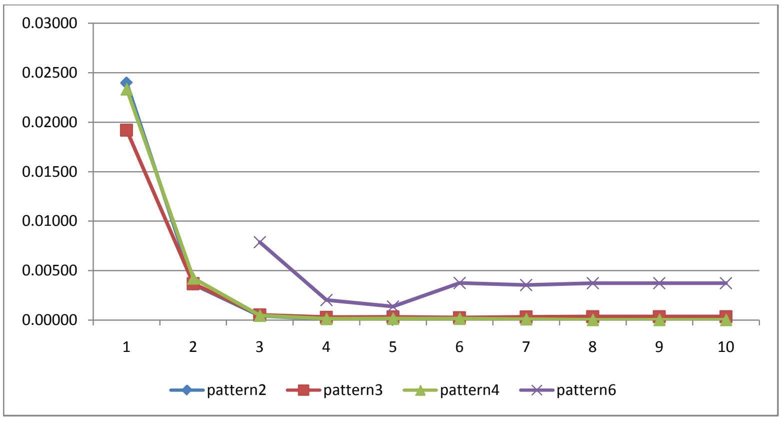


Figure 6: Experimental results for BER for $B_{max} = 4$ using the heuristic for decreasing of *more-candidate-errors*

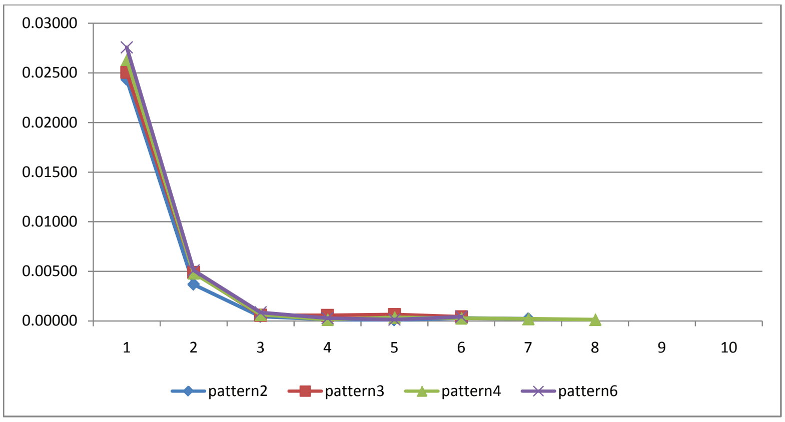


Figure 7: Experimental results for PER for $B_{max} = 4$ using the heuristic for decreasing of *more-candidate-errors*

Influence of the key length to the code performances

In order to check the influence of the key length to the code performances, we have made experiments using keys with different lengths. The results obtained for key lengths of 5, 10 and 15 nibbles are represented in Table 9, Figure 8 (for BER) and Table 10, Figure 9 (for PER).

SNR	key length 5	key length 10	key length 15
1	0.02838	0.01928	0.02090
2	0.01135	0.00400	0.00401
3	0.01026	0.00068	0.00091
4	0.00899	0.00042	0.00041
5	0.00952	0.00066	0.00032
6	0.00910	0.00054	0.00081
7	0.00931	0.00046	0.00067
8	0.00922	0.00053	0.00067
9	0.00927	0.00053	0.00066
10	0.00929	0.00053	0.00066

Table 9: Experimental results for BER for key lengths of 5, 10 and 15 nibbles

Analyzing the presented results we can see that results obtained using keys with length 10 and 15 are almost identical. Also, in these cases, the decoding speeds are same. In the experiments with a key of length 5, the worse results for BER and PER are obtained. For this key length and $SNR \geqslant 3$, the bit-error probability is about 15 to 20 times greater than the corresponding probability obtained with the key length 10, and it is up to 29 times greater than the probability obtained with the key length 15.

From the experiments we can conclude that the key length also has a great influence on the performances of these codes.

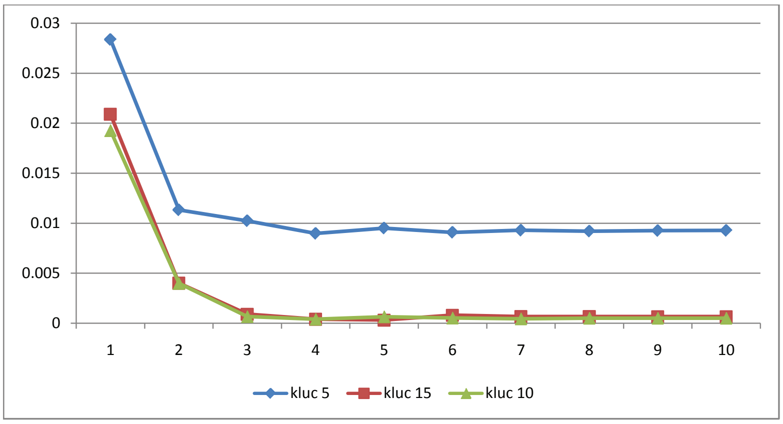


Figure 8: Experimental results for BER for key lengths of 5, 10 and 15 nibbles

SNR	key length 5	key length 10	key length 15
1	0.03816	0.02520	0.02772
2	0.01533	0.00554	0.00583
3	0.01360	0.00137	0.00151
4	0.01202	0.00101	0.00093
5	0.01245	0.00144	0.00079
6	0.01216	0.00115	0.00144
7	0.01252	0.00108	0.00129
8	0.01245	0.00122	0.00129
9	0.01245	0.00122	0.00129
10	0.01250	0.00122	0.00129

Table 10: Experimental results for PER for key lengths of 5, 10 and 15 nibbles

Influence of the chosen quasigroup to the code performances

In order to check the influence of the choice of a quasigroup on the code performances, we have made experiments with a cyclic quasigroup of order 16 using a key of 10 nibbles. Firstly, the experiments were made by using the third pattern. But, in these experiments we obtained a great number of messages in the decoding candidate sets. So, the decoding process was very slow and it did not finish in reasonable time.

Therefore, we made experiments using the first pattern and $B_{max} = 4$. The decoding was faster than in the previous case, but not enough. Also, we obtained a great number of *more-candidate-errors*. For example, for $SNR = 1$, the probability for this type of error is 0.98.

From these experiments, we can conclude that the choice of the quasigroup has an enormous influence on the performances of these codes.

From all experimental results obtained with Standard algorithm for coding/decoding messages transmitted through a Gaussian channel, we can conclude that the best results are obtained using the third pattern, the key length equal to 10

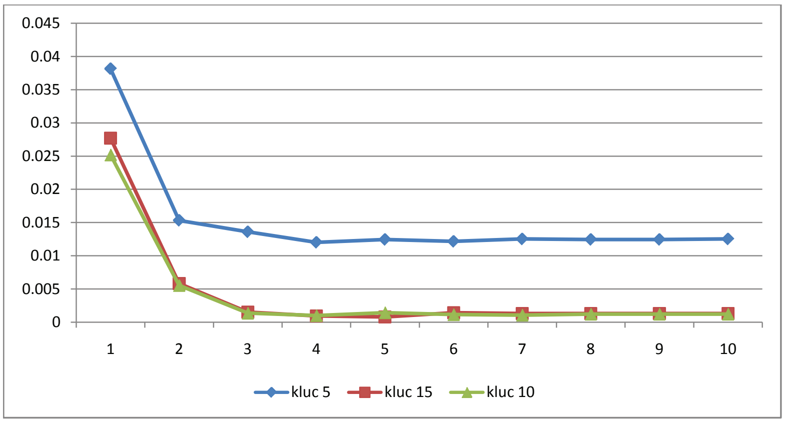


Figure 9: Experimental results for PER for key lengths of 5, 10 and 15 nibbles

(or 15), the quasigroup given in Table 1 and $B_{max} = 4$.

5. Experimental results for Cut-Decoding algorithm

In the experiments made with Cut-Decoding algorithm, in both processes of coding/decoding we used a same quasigroup and different keys. The best results are obtained for the following parameters:

- redundancy pattern: 1100 1110 1100 1100 1110 1100 1100 1100 0000;
- two different keys with length 5: $k_1 = 01234$ and $k_2 = 56789$;
- the quasigroup given in Table 1;
- $B_{max} = 4$.

Also, experiments with keys of 10 nibbles were made, but the results were similar.

Let PER_c be the packet-error probability and BER_c the bit-error probability obtained with Cut-Decoding algorithm. We will compare these probabilities with PER_s and BER_s obtained with Standard algorithm using the best parameters (pattern 3, quasigroup given in Table 1 and key $k = 0123456789$). In Table 11 and Figure 10, BER_s and BER_c for different values of SNR are given, and in Table 12 and Figure 11 - the corresponding results for PER_s and PER_c. In the tables we present the results for $SNR \geqslant 0$, since the decoding does not have sense ($BER > P_b$) for smaller values of SNR.

SNR	BER_s	BER_c
0	0.08343	0.07153
1	0.01928	0.01831
2	0.00400	0.00249
3	0.00068	0.00073
4	0.00042	0.00052
5	0.00066	0.00047
6	0.00054	0.00060
7	0.00046	0.00049
8	0.00053	0.00046
9	0.00053	0.00046
10	0.00053	0.00046

Table 11: Comparison of experimental results for BER for both algorithms

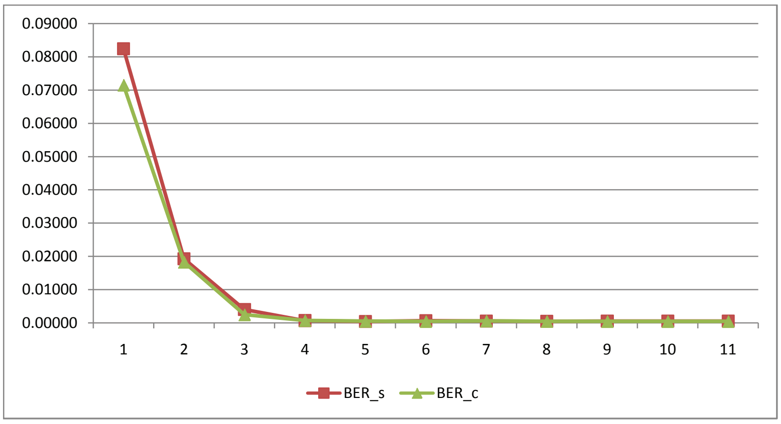


Figure 10: Comparison of BERs

From the results given in Table 11 and Table 12, we can conclude that for both algorithms the results for PER and BER are approximately equal (they differ in the third or higher decimal). But the decoding process with Cut-Decoding algorithm is about 4 times faster than with Standard algorithm.

SNR	PER_s	PER_c
0	0.10829	0.10001
1	0.02520	0.02722
2	0.00554	0.00410
3	0.00137	0.00230
4	0.00101	0.00252
5	0.00144	0.00230
6	0.00115	0.00252
7	0.00108	0.00238
8	0.00122	0.00223
9	0.00122	0.00223
10	0.00122	0.00223

Table 12: Comparison of experimental results for PER for both algorithms

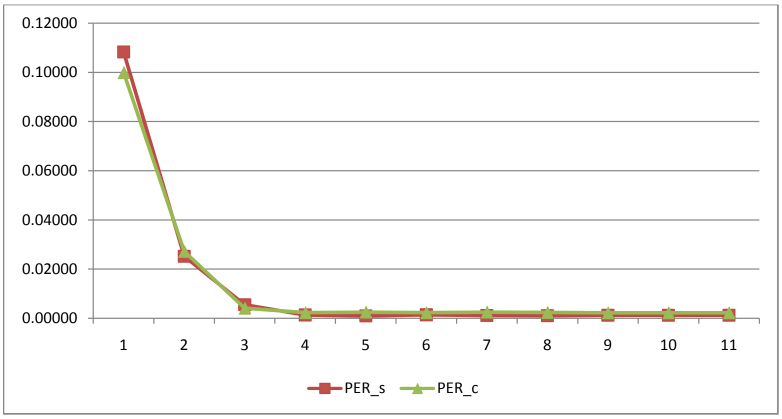


Figure 11: Comparison of PERs

Methods for decreasing of number of unsuccessful decodings with Cut-Decoding algorithm

In order to reduce the number of unsuccessful decodings with *null-error* and *more-candidate-error*, several modifications of Cut-Decoding algorithm are defined (in [7]). To improve the performances of Cut-Decoding algorithm (for transmission through Gaussian channel) we use the following two combinations of the proposed modifications.

In the both combinations with backtracking, if the decoding ends with *null-error*, then the last two iterations are canceled and the first of them is reprocessed with $B_{max} + 2 = 6$ (the next iterations use the previous value of B_{max}). If the decoding ends with *more-candidate-error*, then the last two iterations of the decoding process are canceled and the penultimate iteration is reprocessed with $B_{max} - 1 = 3$. In the decoding of a message only one backtracking is made, except when after the backtracking for *null-error*, *more-candidate-error* appears. In Combination 1, we make one more backtracking for *more-candidate-error* if both decoding candidate sets are non-empty. In Combination 2, we make one more backtracking for *more-candidate-error*, if at least one of decoding candidate sets is non-empty.

The bit-error and packet-error probabilities obtained with Combination 1 are denoted by BER_{c-back} and PER_{c-back}. The bit-error and packet-error probabilities obtained with Combination 2 are denoted by $BER_{c-back-2}$ and $PER_{c-back-2}$.

In Table 13 and Figure 12, we compare the values of packet-error probabilities PER_s, PER_c, PER_{c-back} and $PER_{c-back-2}$ and in Table 14 and Figure 13 - corresponding bit-error probabilities BER, BER_c, BER_{c-back} and $BER_{c-back-2}$.

SNR	PER_s	PER_c	PER_{c-back}	$PER_{c-back-2}$
0	0.10829	0.10001	0.07431	0.07496
1	0.02520	0.02722	0.01944	0.01743
2	0.00554	0.00410	0.00259	0.00331
3	0.00137	0.00230	0.00043	0.00036
4	0.00101	0.00252	0.00014	0.00014
5	0.00144	0.00230	0.00014	0.00007
6	0.00115	0.00252	0.00022	0.00014
7	0.00108	0.00238	0.00029	0.00029
8	0.00122	0.00238	0.00029	0.00029
9	0.00122	0.00223	0.00029	0.00029
10	0.00122	0.00223	0.00029	0.00029

Table 13: Comparison of experimental results for PER

SNR	BER_s	BER_c	BER_{c-back}	$BER_{c-back-2}$
0	0.08343	0.07153	0.04701	0.04815
1	0.01928	0.01830	0.01163	0.01137
2	0.00400	0.00249	0.00146	0.00227
3	0.00068	0.00073	0.00018	0.00013
4	0.00042	0.00052	0.00009	0.00010
5	0.00066	0.00047	0.00005	0.00003
6	0.00054	0.00060	0.00007	0.00006
7	0.00046	0.00049	0.00010	0.00010
8	0.00053	0.00046	0.00010	0.00010
9	0.00053	0.00046	0.00010	0.00010
10	0.00053	0.00046	0.00010	0.00010

Table 14: Comparison of experimental results for BER

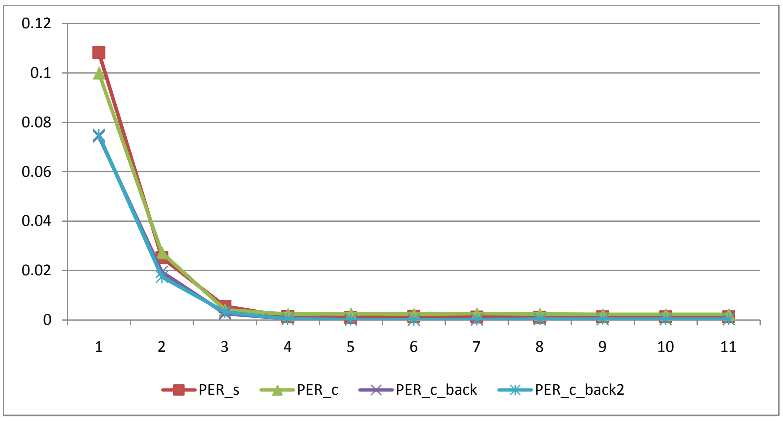


Figure 12: Comparison of PERs

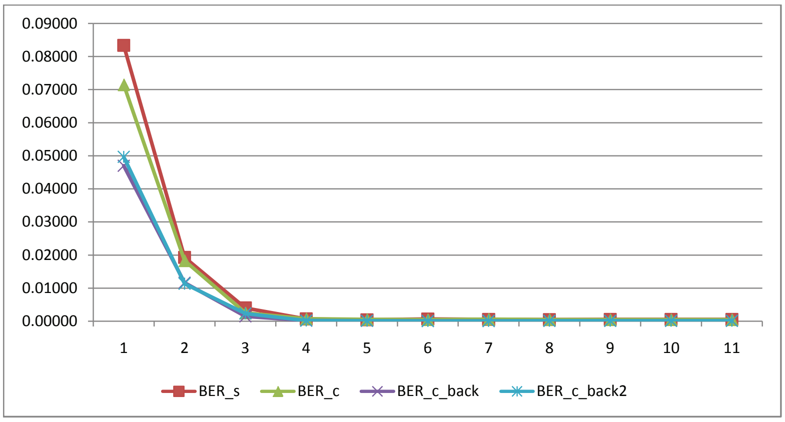


Figure 13: Comparison of BERs

Analyzing the results we can see that Cut-Decoding algorithm with the both proposed combinations for backtracking gives better (and almost identical) results than Cut-Decoding algorithm without backtracking and Standard algorithm.

Also, we calculate the percentage of the eliminated unsuccessful decodings by using the both combinations for backtracking. These results are given in Table 15.

We can notice that the obtained percentages of the eliminated unsuccessful decodings are same with both proposed combinations for backtracking, i.e, we have the same number of eliminated unsuccessful decodings. But, for $SNR \leqslant 2$, the first combination gives better elimination of *null-errors* and the second one -

SNR	% of elimination 1$^{\text{st}}$ combination	% of elimination 2$^{\text{st}}$ combination
0	22.75%	22.85%
1	35.19%	35.19%
2	35.09%	35.09%
3	84.38%	84.38%
4	80.00%	80.00%
5	90.63%	90.63%
6	91.43%	91.43%
7	87.88%	87.88%
8	87.10%	87.10%
9	83.87%	83.87%
10	87.10%	87.10%

Table 15: Percent of eliminated unsuccessful decodings

better elimination of *more-candidate-errors*.

Conclusions

From the experiments made for investigation of the performances of RCBQ for transmission through Gaussian channel, we can conclude that all parameters (a pattern for adding redundancy, a key length and a chosen quasigroup) have influence to the performances of these codes. Also, the pattern and the quasigroup have a great influence to the decoding speed. Namely, with inappropriate choice of these parameters, the decoding process does not finish in real time and the packet-error and bit-error probabilities are very large. Two combinations with backtracking of Cut-Decoding algorithm are proposed and they give a good percentage of eliminated unsuccessful decodings.

These conclusions for influence of parameters on the performances of RCBQ for transmission through Gaussian channel are very similar with corresponding conclusions for transmission through a binary symmetric channel (see, [6, 7, 8, 9]).

Acknowledgment

This research was partially supported by Faculty of Computer Science and Engineering at the University "Ss Cyril and Methodius" in Skopje.

References

[1] **D. Gligoroski, S. Markovski and Lj. Kocarev**. *Totally asynchronous stream ciphers + Redundancy = Cryptcoding*, S. Aissi, H.R. Arabnia (Eds.): Proc. Internat. Confer. Security and Management, SAM 2007, Las Vegas, CSREA Press (2007), pp. 446 – 451.

[2] **D. Gligoroski, S. Markovski and Lj. Kocarev**, *Error-correcting codes based on quasigroups*, Proc. 16th Intern. Confer. Computer Communications and Networks (2007), pp. 165 – 172.

[3] **S. Markovski, D. Gligoroski and V. Bakeva**, *Quasigrouop string processing: Part* 1, Contributions, Sec. Math. Tech. Sci., MANU, **20** (1999), 13 – 28.

[4] **C.N. Mathur, K. Narayan and K.P. Subbalakshmi**, *High Diffusion Cipher: Encryption and Error Correction in a Single Cryptographic Primitive*, Lecture Notes Comput. Sci. **3989** (2006), 309 – 324.

[5] **A. Popovska-Mitrovikj, V. Bakeva and S. Markovski**, *On random error correcting codes based on quasigroups*, Quasigroups and Related Systems **19** (2011), 301 – 316.

[6] **A. Popovska-Mitrovikj, S. Markovski and V. Bakeva**, *Performances of error-correcting codes based on quasigroups*, D.Davcev, J.M.Gomez (Eds.): ICT-Innovations 2009, Springer (2009), pp. 377 – 389.

[7] **A. Popovska-Mitrovikj, S. Markovski anf V. Bakeva**, *Increasing the decoding speed of random codes based on quasigroups*, S. Markovski, M. Gusev (Eds.): ICT Innovations 2012, Web proceedings, ISSN 1857-7288, pp. 93 – 102.

[8] **A. Popovska-Mitrovikj, S. Markovski and V. Bakeva**, *Some New Results for Random Codes Based on Quasigroups*, Proc. 10th Conf. Informatics and Information Technology with International Participants, Bitola (2013), pp. 178 – 181.

[9] **A. Popovska-Mitrovikj, S. Markovski and V. Bakeva**, 4-*Sets-Cut-Decoding algorithms for random codes based on quasigroups*, Intern. J. Electronics Commun. **69** (2015), 1417 – 1428.

[10] **J.G. Proakis and M. Salehi**, *Digital Communications*, Fifth Edition, McGrawHill Higher Education (2008)

[11] **H. Tzonelih and T.R.N. Rao**, *Secret error-correcting codes*, Lecture Notes Comput. Sci. **403** (1990), 540 – 563.

[12] **N. Zivic and C. Ruland**, *Parallel Joint Channel Coding and Cryptography*, Intern. J. Electrical and Electronics Engineering, **4(2)** (2010), 140 – 144.

Received March 19, 2016

University "Ss Cyril and Methodius" - Skopje,
Faculty of Computer Science and Engineering,
P.O. Box 393, Republic of Macedonia
E-mails: daniela-mec@hotmail.com, aleksandra.popovska.mitrovikj@finki.ukim.mk,
verica.bakeva@finki.ukim.mk

Centralizers on semiprime MA-semirings

Sara Shafiq and *Muhammad Aslam*

Abstract. Let T_1, T_2 be left centralizers on 2-torsion free non-commutative semiprime MA-semiring S such that $[T_2(x), T_1(x)]T_2(x) + T_2(x)[T_2(x), T_1(x)] = 0$ holds for all $x \in S$, then $[T_1(x), T_2(x)] = 0$.

1. Introduction

By a *semiring* we mean a nonempty set S in which two binary operations '$+$' (addition) and '$\cdot$' (multiplication) are defined in this way that $(S, \cdot)$ is a semigroup and $(S, +)$ is a commmutative semigroup with an absorbing zero 0 (i.e., $a + 0 = 0 + a = a$, $a0 = 0 = 0a$, for all $a \in S$) and both right and left distributive laws holds in S. A semiring S is called an *inverse semiring* [4] if for every $a \in S$ there exists an element $a' \in S$ such that $a + a' + a = a$ and $a' + a + a' = a'$, where a' is called the *pseudo inverse* of a. Throughout this paper S will denote MA-semiring which is an inverse semiring that satisfies the Bandlet's and Petrich's condition A_2, i.e., $a + a'$ is in center $Z(S)$ of S. For example, commutative inverse semirings and distributive lattices are MA-semirings. For more examples (non-commutative) we refer reader to [2]. According to [2], a *commutator* $[., .]$ is defined as $[x, y] = xy + y'x$. We will make use the following commutator identities:

$$[x, yz] = [x, y]z + y[x, z], \quad [xy, z] = [x, z]y + x[y, z], \quad [xy, x] = x[y, x],$$
$$[x, xy] = x[x, y], \quad [xy, y] = [x, y]y, \quad [y, xy] = [y, x]y$$

(see [2], for their proofs). One can see that these fundamental identities including jacobian identity are useful tools to explore and extend various Lie type results of rings in the structure of inverse semirings (see [2] and [3]).

A semiring S is *prime* if $aSb = (0)$ implies $a = 0$ or $b = 0$ and it is *semiprime* if $aSa = 0$ implies $a = 0$. S is *n-torsion free* if $nx = 0$, $x \in S$ implies $x = 0$. Following [7], an additive mapping $T : S \to S$ is called a *left* (*right*) *centralizer* if for all $x, y \in S$, $T(xy) = T(x)y$ (resp. $T(xy) = xT(y)$) and T is a *centralizer* if it is both right and left centralizer.

Motivated by the work of Zalar [7] on centralizers, J. Vukman investigated the identities satisfied by centralizers on semiprime rings.

In this paper, we explore these identities and extend J. Vukman's results [6] to MA-semirings.

2010 Mathematics Subject Classification: 16N60, 16W25.
Keywords: Semiprime inverse semiring, left centralizer, right centralizer, centralizer, 2-torsion free semiring, MA-semiring.

2. Main results

To prove our results we need the following lemma (Lemm 1.1 in [5]).

Lemma 2.1. *Let S be an inverse semiring. Then $a+b=0$ implies $a=b'$, for all $a,b\in S$.*

Theorem 2.2. *Let S be a 2-torsion free non-commutative semiprime MA-semiring and T_1,T_2 be left centralizers on S. If*

$$[T_2(x),T_1(x)]T_2(x)+T_2(x)[T_2(x),T_1(x)]=0 \tag{1}$$

holds for all $x\in S$, then $[T_2(x),T_1(x)]=0$.

Proof. Linearize (1), we get

$$\begin{aligned}&[T_2(x),T_1(x)]T_2(y)+T_2(y)[T_2(x),T_1(x)]+[T_2(y),T_1(y)]T_2(x)+\\ &\quad T_2(x)[T_2(y),T_1(y)]+[T_2(y),T_1(x)]T_2(x)+T_2(x)[T_2(y),T_1(x)]+\\ &\quad [T_2(x),T_1(y)]T_2(x)+T_2(x)[T_2(x),T_1(y)]+[T_2(x),T_1(y)]T_2(y)+\\ &\quad T_2(y)[T_2(x),T_1(y)]+[T_2(y),T_1(x)]T_2(y)+T_2(y)[T_2(y),T_1(x)]=0.\end{aligned} \tag{2}$$

Replacing x by x' in (2), and using the fact that $T_i(x')=T_i'(x)=(T_i(x))'$, $i=1,2$, we have

$$\begin{aligned}&[T_2(x),T_1(x)]T_2(y)+T_2(y)[T_2(x),T_1(x)]+[T_2(y),T_1(y)]T_2(x')+\\ &\quad T_2(x')[T_2(y),T_1(y)]+[T_2(y),T_1(x)]T_2(x)+T_2(x)[T_2(y),T_1(x)]+\\ &\quad [T_2(x),T_1(y)]T_2(x)+T_2(x)[T_2(x),T_1(y)]+[T_2(x'),T_1(y)]T_2(y)+\\ &\quad T_2(y)[T_2(x'),T_1(y)]+[T_2(y),T_1(x')]T_2(y)+T_2(y)[T_2(y),T_1(x')]=0.\end{aligned} \tag{3}$$

Multiplying (2) by 2 and adding the result in (3), we have

$$\begin{aligned}&3[T_2(x),T_1(x)]T_2(y)+3T_2(y)[T_2(x),T_1(x)]+[T_2(y),T_1(y)]T_2(x'+2x)+\\ &\quad T_2(x'+2x)[T_2(y),T_1(y)]+3[T_2(y),T_1(x)]T_2(x)+3T_2(x)[T_2(y),T_1(x)]+\\ &\quad 3[T_2(x),T_1(y)]T_2(x)+3T_2(x)[T_2(x),T_1(y)]+[T_2(x'+2x),T_1(y)]T_2(y)+\\ &T_2(y)[T_2(x'+2x),T_1(y)]+[T_2(y),T_1(x'+2x)]T_2(y)+T_2(y)[T_2(y),T_1(x'+2x)]=0.\end{aligned}$$

Using (2) and the fact that S is a 2-torsion free inverse semiring, we get

$$\begin{aligned}&[T_2(x),T_1(x)]T_2(y)+T_2(y)[T_2(x),T_1(x)]+[T_2(y),T_1(x)]T_2(x)+\\ &\quad T_2(x)[T_2(y),T_1(x)]+[T_2(x),T_1(y)]T_2(x)+T_2(x)[T_2(x),T_1(y)]=0.\end{aligned} \tag{4}$$

Replacing y by xy in (4) and then using (1) we obtain

$$\begin{aligned} &T_2(x)y[T_2(x),T_1(x)]+2[T_2(x),T_1(x)]yT_2(x)+T_2(x)[y,T_1(x)]T_2(x)+\\ &\quad(T_2(x))^2[y,T_1(x)]+T_1(x)[T_2(x),y]T_2(x)+T_2(x)[T_2(x),T_1(x)]y+\\ &\quad T_2(x)T_1(x)[T_2(x),y]=0. \qquad (5)\end{aligned}$$

Replacing y by $yT_2(x)$ in last equation, we get

$$\begin{aligned} &T_2(x)yT_2(x)[T_2(x),T_1(x)]+T_2(x)y[T_2(x),T_1(x)]T_2(x)+\\ &\quad 2[T_2(x),T_1(x)]y(T_2(x))^2+T_2(x)[y,T_1(x)](T_2(x))^2+\\ &\quad (T_2(x))^2y[T_2(x),T_1(x)]+(T_2(x))^2[y,T_1(x)]T_2(x)+\\ &\quad T_1(x)[T_2(x),y](T_2(x))^2+T_2(x)[T_2(x),T_1(x)]yT_2(x)+\\ &\quad T_2(x)T_1(x)[T_2(x),y]T_2(x)=0. \qquad (6)\end{aligned}$$

Using (5) in (6), we get

$$T_2(x)yT_2(x)[T_2(x),T_1(x)]+(T_2(x))^2y[T_2(x),T_1(x)]=0 \qquad (7)$$

Replacing y by $T_1(x)y$ in (7), we have

$$T_2(x)T_1(x)yT_2(x)[T_2(x),T_1(x)]+(T_2(x))^2T_1(x)y[T_2(x),T_1(x)]=0. \qquad (8)$$

Pre-multiplying (7) by $T_1(x)$, we have

$$T_1(x)T_2(x)yT_2(x)[T_2(x),T_1(x)]+T_1(x)(T_2(x))^2y[T_2(x),T_1(x)]=0. \qquad (9)$$

Adding pseudo inverse of (9) in (8) and then using (1), we obtain

$$[T_2(x),T_1(x)]yT_2(x)[T_2(x),T_1(x)]=0, \qquad (10)$$

which implies

$$T_2(x)[T_2(x),T_1(x)]=0. \qquad (11)$$

From (1), we get

$$[T_2(x),T_1(x)]T_2(x)=0. \qquad (12)$$

As (4) obtained from (1), from (12) we get

$$[T_2(y),T_1(x)]T_2(x)+[T_2(x),T_1(y)]T_2(x)+[T_2(x),T_1(x)]T_2(y)=0. \qquad (13)$$

Replacing y by xy in (13) and then using (12), we get

$$[T_2(x),T_1(x)](2y+y')T_2(x)+T_2(x)yT_1(x)T_2(x)+T_1(x)y'(T_2(x))^2=0$$

or

$$[T_2(x),T_1(x)]yT_2(x)+T_2(x)yT_1(x)T_2(x)+T_1(x)y'(T_2(x))^2=0. \qquad (14)$$

Post-multiplying (14) by $T_1(x)$

$$[T_2(x), T_1(x)]yT_2(x)T_1(x) + T_2(x)yT_1(x)T_2(x)T_1(x) + T_1(x)y'(T_2(x))^2T_1(x) = 0. \tag{15}$$

Replacing y by $yT_1(x)$ in (14), we get

$$[T_2(x), T_1(x)]yT_1(x)T_2(x) + T_2(x)y(T_1(x))^2T_2(x) + T_1(x)y'T_1(x)(T_2(x))^2 = 0. \tag{16}$$

Adding pseudo inverse of (16) in (15) and then using (1), we have

$$[T_2(x), T_1(x)]y[T_2(x), T_1(x)] + T_2(x)yT_1(x)[T_2(x), T_1(x)] + T_1(x)y[(T_2)^2, T_1(x)] = 0$$

or

$$[T_2(x), T_1(x)]y[T_2(x), T_1(x)] + T_2(x)yT_1(x)[T_2(x), T_1(x)] = 0. \tag{17}$$

Replacing y by $zT_2(x)y$ in (17), we have

$$[T_2(x), T_1(x)]zT_2(x)y[T_2(x), T_1(x)] + T_2(x)zT_2(x)yT_1(x)[T_2(x), T_1(x)]. \tag{18}$$

Pre-multiplying (17) by $T_2(x)z$

$$T_2(x)z[T_2(x), T_1(x)]y[T_2(x), T_1(x)] + T_2(x)zT_2(x)yT_1(x)[T_2(x), T_1(x)]. \tag{19}$$

Applying Lemma 2.1 to (19) and using it in (18), we get

$$F(x, z)y[T_2(x), T_1(x)] = 0, \tag{20}$$

where $F(x, z) = [T_2(x), T_1(x)]zT_2(x) + T_2(x)z'[T_2(x), T_1(x)]$.
Replacing y by $yT_2(x)z$ in (20)

$$F(x, z)yT_2(x)z[T_2(x), T_1(x)] = 0. \tag{21}$$

Post-multiplying (20) by $zT_2(x)$

$$F(x, z)y[T_2(x), T_1(x)]zT_2(x) = 0. \tag{22}$$

Adding pseudo inverse of (21) in (22), we get

$$F(x, z)yF(x, z) = 0.$$

Semiprimness of S implies

$$F(x, z) = [T_2(x), T_1(x)]zT_2(x) + T_2(x)z'[T_2(x), T_1(x)] = 0. \tag{23}$$

Applying Lemma 2.1 to (23), we get

$$[T_2(x), T_1(x)]zT_2(x) = T_2(x)z[T_2(x), T_1(x)]. \tag{24}$$

Replacing z by $yT_1(x)$ in last equation, we have

$$[T_2(x),T_1(x)]yT_1(x)T_2(x)=T_2(x)yT_1(x)[T_2(x),T_1(x)]. \tag{25}$$

Using (25) to (17), we get

$$[T_2(x),T_1(x)]yT_2(x)T_1(x)+[T_2(x),T_1(x)](y+y')(T_1(x)\acute{)}T_2(x)=0$$

or

$$[T_2(x),T_1(x)]yT_2(x)T_1(x)+[T_2(x),T_1(x)]y(T_1(x)+T_1(x'))T_2(x)=0,$$

since $T_1(x)+T_1(x')\in Z(S)$, so we have

$$[T_2(x),T_1(x)]yT_2(x)T_1(x)+[T_2(x),T_1(x)]yT_2(x)(T_1(x)+T_1(x'))=0$$

or

$$[T_2(x),T_1(x)]yT_2(x)T_1(x)=0. \tag{26}$$

Replacing y by $yT_1(x)$ in above equation

$$[T_2(x),T_1(x)]yT_1(x)T_2(x)T_1(x)=0. \tag{27}$$

Post-multiplying (26) by $T_1(x)$

$$[T_2(x),T_1(x)]yT_2(x)(T_1(x))^2=0. \tag{28}$$

Adding pseudo inverse of (27) in (28), we have

$$[T_2(x),T_1(x)]y[T_2(x),T_1(x)]T_1(x)=0.$$

Replacing y by $T_1(x)y$ and using semiprimeness of S, we have

$$[T_2(x),T_1(x)]T_1(x)=0. \tag{29}$$

Replacing z by $T_1(x)y$ in (24) and using (29), we have

$$T_2(x)T_1(x)y[T_2(x),T_1(x)]=0. \tag{30}$$

As (14) obtained from (12), from (11), we obtain

$$T_2(x)y[T_2(x),T_1(x)]+T_2(x)T_1(x)y'T_2(x)+(T_2(x))^2yT_1(x)=0. \tag{31}$$

By (24), we have

$$T_2(x)T_1(x)(y+y')T_2(x)+(T_1(x))'T_2(x))yT_2(x)+(T_2(x))^2yT_1(x)=0$$

or

$$T_2(x)(T_1(x)+T_1(x'))yT_2(x)+(T_1(x))'T_2(x))yT_2(x)+(T_2(x))^2yT_1(x)=0$$

or

$$(T_1(x) + T_1(x'))T_2(x)yT_2(x) + (T_1(x))'T_2(x))yT_2(x) + (T_2(x))^2yT_1(x) = 0$$

$$(T_1(x))'T_2(x)yT_2(x) + (T_2(x))^2yT_1(x) = 0. \tag{32}$$

Replacing y by $yT_1(x)$ in last equation

$$(T_1(x))'T_2(x)yT_1(x)T_2(x) + (T_2(x))^2y(T_1(x))^2 = 0. \tag{33}$$

Post-multiplying (32) by $T_1(x)$

$$(T_1(x))'T_2(x)yT_2(x)T_1(x) + (T_2(x))^2y(T_1(x))^2 = 0. \tag{34}$$

Applying Lemma 2.1 to (34) and using the result in (33) we get

$$T_1(x)T_2(x)y[T_2(x), T_1(x)] = 0. \tag{35}$$

Adding pseudo inverse of (35) in (30) we get

$$[T_2(x), T_1(x)]y[T_2(x), T_1(x)].$$

This implies

$$[T_2(x), T_1(x)] = 0,$$

which completes the proof. □

Theorem 2.3. *Let S be 2-torsion free non-commutative semiprime MA-semiring. If T_1 and T_2 are left centralizers on S satisfying*

$$[[T_2(x), T_1(x)], T_2(x)] = 0 \tag{36}$$

for all $x \in S$. then $[T_2(x), T_1(x)] = 0$.

Proof. As (4) obtained from (1), from (36), we get

$$[[T_2(x), T_1(x)], T_2(y)] + [[T_2(x), T_1(y)], T_2(x)] + [[T_2(y), T_1(x)], T_2(x)] = 0. \tag{37}$$

Replacing y by xy in last equation and using (36), we obtain

$$\begin{aligned}T_2(x)[[T_2(x), T_1(x)], y] + 3[T_2(x), T_1(x)][y, T_2(x)]+ \\ T_1(x)[[T_2(x), y], T_2(x)] + T_2(x)[[y, T_1(x)], T_2(x)] = 0.\end{aligned} \tag{38}$$

Replacing y by $yT_2(x)$ in last equation, we get

$$\begin{aligned}T_2(x)[[T_2(x), T_1(x)], y]T_2(x) + T_2(x)y[[T_2(x), T_1(x)], T_2(x)]+ \\ 3[T_2(x), T_1(x)][y, T_2(x)]T_2(x) + T_1(x)[y[T_2(x), T_2(x)], T_2(x)]+ \\ T_1(x)[[T_2(x), y]T_2(x), T_2(x)] + T_2(x)[y[T_2(x), T_1(x)], T_2(x)]+ \\ T_2(x)[[y, T_1(x)], T_2(x)]T_2(x) = 0.\end{aligned} \tag{39}$$

Now as $T_2(x)+T_2(x')\in Z(S)$, so we have

$$\begin{aligned}&T_1(x)[y[T_2(x),T_2(x)],T_2(x)]+T_1(x)[[T_2(x),y]T_2(x),T_2(x)]\\&=T_1(x)[y(T_2(x){+}T_2(x'))T_2(x),T_2(x)]{+}T_1(x)[(T_2(x)yT_2(x){+}y'T_2(x)T_2(x)),T_2(x)]\\&=T_1(x)[(T_2(x)+T_2(x')+T_2(x))yT_2(x)+y'T_2(x)T_2(x),T_2(x)]\\&=T_1(x)[[T_2(x),y]T_2(x),T_2(x)].\end{aligned}\tag{40}$$

From (40), (39) and (38), we obtain

$$T_2(x)[y,T_2(x)][T_2(x),T_1(x)]=0$$

or

$$T_2(x)yT_2(x)[T_2(x),T_1(x)]+(T_2(x))^2y'[T_2(x),T_1(x)]=0.\tag{41}$$

Replacing y by $T_1(x)y$ in last equation, we obtain

$$T_2(x)T_1(x)yT_2(x)[T_2(x),T_1(x)]+(T_2(x))^2T_1(x)y'[T_2(x),T_1(x)]=0.\tag{42}$$

Pre-multiplying (41) by $T_1(x)$, we get

$$T_1(x)T_2(x)yT_2(x)[T_2(x),T_1(x)]+T_1(x)(T_2(x))^2y'[T_2(x),T_1(x)]=0.\tag{43}$$

Adding pseudo inverse of (43) in (42)

$$\begin{aligned}&[T_2(x),T_1(x)]yT_2(x)[T_2(x),T_1(x)]+T_2(x)[T_2(x),T_1(x)]y'[T_2(x),T_1(x)]+\\&[T_2(x),T_1(x)]T_2(x)y'[T_2(x),T_1(x)]=0.\end{aligned}\tag{44}$$

Applying Lemma 2.1 in (36) and using the result in the last equation, we have

$$[T_2(x),T_1(x)]yT_2(x)[T_2(x),T_1(x)]+2T_2(x)[T_2(x),T_1(x)]y'[T_2(x),T_1(x)]=0.\tag{45}$$

Pre-multiplying (45) by $T_2(x)$, we have

$$\begin{aligned}&2(T_2(x))^2[T_2(x),T_1(x)]y'[T_2(x),T_1(x)]+\\&T_2(x)[T_2(x),T_1(x)]yT_2(x)[T_2(x),T_1(x)]=0.\end{aligned}\tag{46}$$

Replacing y by $[T_2(x),T_1(x)]y$ in (41), we have

$$\begin{aligned}&T_2(x)[T_2(x),T_1(x)]yT_2(x)[T_2(x),T_1(x)]+\\&(T_2(x))^2[T_2(x),T_1(x)]y'[T_2(x),T_1(x)]=0.\end{aligned}\tag{47}$$

Applying Lemma 2.1 to (46) and using the result in (47), we have

$$T_2(x)[T_2(x),T_1(x)]yT_2(x)[T_2(x),T_1(x)]=0,\tag{48}$$

and semiprimness of S implies

$$T_2(x)[T_2(x),T_1(x)]=0,\tag{49}$$

and from (36) and Lemma 2.1, we obtain

$$[T_2(x),T_1(x)]T_2(x),\tag{50}$$

which gives $[T_2(x),T_1(x)]=0$, as in the proof of Theorem 2.2. □

References

[1] **H.J. Bandlet and M. Petrich**, *Subdirect products of rings and distrbutive lattics*, Proc. Edin. Math. Soc. **25** (1982), 135 – 171.

[2] **M.A. Javed, M. Aslam and M. Hussain**, *On Condition* (A_2) *of Bandlet and petrich for inverse semirings*, Int. Math. Forum **7** (2012), 2903 – 2914.

[3] **M.A. Javed and M. Aslam**, *Some commutativity conditions in prime MA-semirings*, Ars Combin. **114** (2014), 373 – 384.

[4] **P.H. Karvellas**, *Inversive semirings*, J. Aust. Math. Soc. **18** (1974), 277 – 288.

[5] **S. Sara, M. Aslam and M.A. Javed**, *On centralizer of semiprime inverse semiring*, Discussiones Math. General Algebra and Appl. **36** (2016), 71 – 84.

[6] **J. Vukman**, *Centralizers on prime and semiprime rings*, Comment Math., Univ. Carolin. **38** (1997), 231 – 240.

[7] **B. Zalar**, *On centralizers of semiprime rings*, Comment. Math. Univ. Carolin. **32** (1991), 609 – 614.

Received August 28, 2015
Revised November 24, 2015

GC University Lahore, Pakistan, 54000,
E-mails: saro_c18@yahoo.com, aslam298@hotmail.com.

Gyrogroups and the Cauchy property

Teerapong Suksumran and Abraham A. Ungar

Abstract. A gyrogroup is a nonassociative group-like structure. In this article, we extend the Cauchy property from groups to gyrogroups. The (weak) Cauchy property for finite gyrogroups states that if p is a prime dividing the order of a gyrogroup G, then G contains an element of order p. An application of a result in loop theory shows that gyrogroups of odd order as well as solvable gyrogroups satisfy the Cauchy property. Although gyrogroups of even order need not satisfy the Cauchy property, we prove that every gyrogroup of even order contains an element of order two. As an application, we prove that every group of order nq, where $n \in \mathbb{N}$ and q is a prime with $n < q$, contains a unique characteristic subgroup of order q.

1. Introduction

Gyrogroups abound as an integral part of group theory. In fact, (i) every gyrogroup is extendable to a group, called the *gyrosemidirect product group* [23, Section 2.6]; (ii) every gyrogroup is a twisted subgroup of some group [6, 7, 11]; and (iii) a certain group with an automorphism of order two gives rise to a gyrogroup [6, 7, 12, 17]. Further, any group may be viewed as a gyrogroup with trivial gyroautomorphisms. It turns out that gyrogroups share remarkable analogies with groups. Several well-known results in group theory can be naturally extended to the case of gyrogroups such as the Lagrange theorem [18], the fundamental isomorphism theorems, the Cayley theorem [19], the orbit-stabilizer theorem, the class equation, and the Burnside lemma [16]. Moreover, some gyrocommutative gyrogroups admit scalar multiplication, turning themselves into gyrovector spaces, just as some abelian groups admit scalar multiplication, turning themselves into vector spaces. Remarkably, gyrovector spaces form the algebraic setting for analytic hyperbolic geometry, just as vector spaces form the algebraic setting for analytic Euclidean geometry, as evidenced, for instance, from [20, 21, 22, 23, 24, 25, 26, 27]. Thus, like the group notion, the notion of gyrogroups plays a universal computational role.

It is known in the literature that every group satisfies the *Cauchy property*, that is, if p is a prime dividing the order of a group Γ, then Γ contains an element of order p. This is the familiar Cauchy theorem in abstract algebra. Cauchy's

2010 Mathematics Subject Classification: 20N05, 20E34, 20E07
Keywords: Cauchy's theorem, gyrogroup, Bol loop.

Part of this work was done when the first author was a visiting researcher at the Department of Mathematics, North Dakota State University, Fargo, ND, USA.

theorem leads to a better understanding of the structure of a finite group. For instance, using Cauchy's theorem, one can prove that every group of order $2p$, where p is a prime, is isomorphic to the cyclic group or the dihedral group of order $2p$ [8]. Furthermore, the celebrated Sylow theorems are built on Cauchy's theorem, see for instance [4, p. 140] and [3, Section 9.2].

In [18] the authors extend the Cauchy property to the case of gyrogroups and prove that gyrogroups of order pq and nongyrocommutative gyrogroups of order pqr satisfy the (strong) Cauchy property, where p, q and r are primes. Unfortunately, there is no hope of extending Cauchy's theorem to all finite gyrogroups as Nagy proves the existence of a simple right Bol loop of exponent two and of order 96 [13, Corollary 3.7]. See also [2]. This loop gives rise to a gyrocommutative gyrogroup of order 96 in which every nonidentity element has order two. However, some classes of finite gyrogroups do satisfy the Cauchy property. As in the group case, the Cauchy property leads to a better understanding of the structure of a finite gyrogroup. For example, any gyrogroup of order pq, where p and q are distinct primes, is generated by two elements; one has order p and the other has order q [18, Theorem 6.10]. We will see shortly that any gyrogroup of order pq, where p and q are primes with $p < q$, contains a unique subgyrogroup of order q.

2. Preliminaries

For the basic theory of gyrogroups, the reader is referred to [15, 18, 19, 23]. For basic knowledge of loop theory, the reader is referred to [10, 14]. Subgyrogroups, gyrogroup homomorphisms, normal subgyrogroups, and quotient gyrogroups are studied in detail in [15, 18, 19].

Let G be a gyrogroup and let a be an element of G. For $m \in \mathbb{Z}$, define recursively the following notation

$$0a = 0, \quad ma = a \oplus ((m-1)a),\, m \geq 1, \quad ma = (-m)(\ominus a),\, m < 0. \tag{1}$$

It can be shown that $(ma) \oplus (ka) = (m+k)a$ and $(mk)a = m(ka)$ for all $m, k \in \mathbb{Z}$. Hence, the *cyclic subgyrogroup generated by* a, written $\langle a \rangle$, forms a cyclic group with generator a under the gyrogroup operation. In fact,

$$\langle a \rangle = \{ma \colon m \in \mathbb{Z}\}. \tag{2}$$

Further, the gyroautomorphism $\mathrm{gyr}\,[ma, ka]$ descends to the identity automorphism for all $m, k \in \mathbb{Z}$. The *order* of a, denoted by $|a|$, is defined to be the cardinality of $\langle a \rangle$ if $\langle a \rangle$ is finite. In this case, we will write $|a| < \infty$. If $\langle a \rangle$ is infinite, the order of a is defined to be infinity, and we will write $|a| = \infty$. As in the theory of groups, if $|a| < \infty$, then $|a|$ is the smallest positive integer such that $|a|a = 0$. If $|a| = \infty$, then $|ma| = \infty$ for all $m \in \mathbb{Z} \setminus \{0\}$. Furthermore, if G is a finite gyrogroup, then $|G|$ is divisible by $|a|$, see [18, Proposition 6.1].

As a consequence of the left cancellation law, the *left gyrotranslation by* a, defined by $L_a \colon x \mapsto a \oplus x$, $x \in G$, is a permutation of G for all $a \in G$. Because gyrogroups are *left power alternative* [18, p. 288], that is, $L_a^m = L_{ma}$ for all $a \in G$, $m \in \mathbb{Z}$, the gyrogroup-theoretic order of a and the group-theoretic order of L_a coincide.

3. Main results

Throughout the remainder of the article, all gyrogroups are finite and G denotes an arbitrary finite gyrogroup unless explicitly mentioned otherwise.

Definition 3.1. A gyrogroup G has the *weak Cauchy property* if for every prime p dividing the order of G, G contains an element of order p.

Definition 3.2. A gyrogroup G has the *strong Cauchy property* if every subgyrogroup of G has the weak Cauchy property.

It is clear that any gyrogroup that satisfies the strong Cauchy property will automatically satisfy the weak Cauchy property as well. The Cauchy property is an invariant property of finite gyrogroups in the sense that if G and H are isomorphic gyrogroups, then G has the weak (resp. strong) Cauchy property if and only if H has the weak (resp. strong) Cauchy property [18, Corollary 6.6]. Therefore, the Cauchy property becomes important in classification of finite gyrogroups because not every gyrogroup has the Cauchy property. Further, the Cauchy property is a good example to see how information about a gyrogroup G can be obtained from information on its normal subgyrogroup N and on its quotient gyrogroup G/N, as shown in the following theorem.

Theorem 3.3 (Corollary 6.8, [18]). *Let N be a normal subgyrogroup of G. If N and G/N have the weak (resp. strong) Cauchy property, then so has G.*

Using Theorem 3.3, one can show that finite solvable gyrogroups satisfy the strong Cauchy property. A (finite or infinite) gyrogroup G is *solvable* if there exists a series $\{0\} = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n = G$ of subgyrogroups of G such that $G_i \trianglelefteq G_{i+1}$ and the quotient gyrogroup G_{i+1}/G_i is an abelian group for all i with $0 \le i \le n-1$ (cf. [1, p. 116]).

Theorem 3.4 (Proposition 46, [15]). *Every solvable gyrogroup has the strong Cauchy property.*

Proof. The proof of the theorem can be done by induction on the number of subgyrogroups in a subnormal series using Theorem 3.3. □

Recall that a loop $(L, \cdot)$ is a *left Bol loop* if it satisfies the *left Bol identity*:

$$a \cdot (b \cdot (a \cdot c)) = (a \cdot (b \cdot a)) \cdot c \tag{3}$$

for all $a, b, c \in L$. A loop $(L, \cdot)$ has the A_ℓ*-property* if the left inner mapping

$$\ell(a, b) := L_{a \cdot b}^{-1} \circ L_a \circ L_b$$

generated by a and b defines an automorphism of L for all $a, b \in L$. Here, L_a denotes the *left multiplication map* by a defined by $L_a \colon x \mapsto a \cdot x$, $x \in L$. It is known in the literature that every gyrogroup forms a left Bol loop with the A_ℓ-property, where the gyroautomorphisms correspond to left inner mappings, and vice versa. In particular, the left loop property and the left Bol identity are equivalent, see for instance [10, Theorem 6.4].

By Glauberman's result [9], Foguel et al. prove that Cauchy's theorem holds for finite left Bol loops of *odd* order. More specifically, if L is a left Bol loop of odd order and if p is a prime dividing the order of L, then there exists an element a of L such that $|L_a| = p$ [5, Theorem 6.2]. With this result in hand, one can prove that gyrogroups of *odd* order satisfy the weak Cauchy property.

Theorem 3.5 (Cauchy's theorem). *Let G be a gyrogroup of odd order. If p is a prime dividing $|G|$, then G has an element of order p. In other words, G has the week Cauchy property.*

Proof. As noted above, G is a left Bol loop of odd order. Hence, by Theorem 6.2 of [5], there is an element a of G such that $|L_a| = p$. Since $|a|$ equals $|L_a|$, the theorem follows. □

Corollary 3.6. *Every gyrogroup of odd order has the strong Cauchy property.*

Proof. Let G be a gyrogroup of odd order and let H be a subgyrogroup of G. By Lagrange's theorem for gyrogroups [18, Theorem 5.7], $|H|$ divides $|G|$ and so H is a gyrogroup of odd order. It follows that H has the week Cauchy property, which completes the proof. □

We have seen in Corollary 3.6 that any gyrogroup of odd order has the strong Cauchy property. Unfortunately, there is an example of a gyrogroup of *even* order that fails to satisfy the weak Cauchy property. In fact, by Corollary 3.7 of [13], there exists a simple *right* Bol loop of exponent two and of order 96, say $(L_N, \cdot)$. The *dual loop* of L_N, denoted by $\hat{L}_N$, consists of the underlying set L_N with the dual operation

$$a * b := b \cdot a$$

for all $a, b \in L_N$. It is straightforward to check that $\hat{L}_N$ is a left Bol loop, that L_N and $\hat{L}_N$ share the same identity, and that if $a \in L_N$, then the inverse of a in L_N and the inverse of a in $\hat{L}_N$ are identical. Note that $a = a^{-1}$ for all $a \in \hat{L}_N$ since $\hat{L}_N$ is of exponent two. Hence,

$$(a * b)^{-1} = a * b = a^{-1} * b^{-1}$$

for all $a, b \in \hat{L}_N$. This shows that $\hat{L}_N$ is a *left* Bol loop satisfying the automorphic inverse property. Hence, $\hat{L}_N$ is a gyrocommutative gyrogroup by Theorem 6.6 of [10] and Theorem 3.2 of [23]. Since $a * a = 1$ for all $a \in \hat{L}_N$, every nonidentity element of $\hat{L}_N$ has order two. From this it is clear that $\hat{L}_N$ does not satisfy the weak Cauchy property. Nevertheless, any gyrogroup of *even* order does contain an element of order two, as shown in the following theorem.

Theorem 3.7. *If G is a gyrogroup of even order, then G contains an element of order two.*

Proof. We first show that $\{\{a, \ominus a\} \colon a \in G\}$ forms a *disjoint* partition of G. For each $a \in G$, set $C_a = \{a, \ominus a\}$. Clearly, $C_a \neq \emptyset$ for all $a \in G$ and $\bigcup_{a \in G} C_a = G$. We claim that $C_a \cap C_b \neq \emptyset$ implies $C_a = C_b$. In fact, if $x \in C_a \cap C_b$, then there are four possibilities:

(1) $x = a$ and $x = b$;

(2) $x = a$ and $x = \ominus b$;

(3) $x = \ominus a$ and $x = b$;

(4) $x = \ominus a$ and $x = \ominus b$.

Each of (1)–(4) implies that $C_a = C_b$ since $\ominus(\ominus x) = x$. Note that $|C_a| = 1$ or 2. Note also that $|C_a| = 1$ if and only if $a = \ominus a$.

Set $m = |\{a \in G \colon |C_a| = 2\}|$ and $n = |\{a \in G \colon |C_a| = 1\}|$. Then $|G| = 2m + n$. Since 2 divides $|G|$, we have $2 \mid n$. Thus, $n \geq 2$ and so there must be a nonidentity element c of G such that $c = \ominus c$. Hence, $|c| = 2$. □

As a consequence of Theorem 3.7, every gyrocommutative gyrogroup of even order contains the nontrivial subgyrogroup of elements of order two together with the gyrogroup identity.

Lemma 3.8. *Let G be a (finite or infinite) gyrocommutative gyrogroup. Then*

$$L^2_{a \oplus b} = L_a \circ L^2_b \circ L_a$$

for all $a, b \in G$.

Proof. Note that $L_a^{-1} = L_{\ominus a}$ for all $a \in G$. By (2.126) of [23], $\operatorname{gyr}[a, b] = \operatorname{gyr}[\ominus a, \ominus b]$. By (12) of [19] and Theorem 3.2 of [23],

$$L^{-1}_{a \oplus b} \circ L_a \circ L_b = L^{-1}_{\ominus a \ominus b} \circ L_{\ominus a} \circ L_{\ominus b} = L_{\ominus(\ominus a \ominus b)} \circ L_a^{-1} \circ L_b^{-1} = L_{a \oplus b} \circ L_a^{-1} \circ L_b^{-1},$$

which implies $L^2_{a \oplus b} = L_a \circ L^2_b \circ L_a$. □

Theorem 3.9. *If G is a (finite or infinite) gyrocommutative gyrogroup, then*

$$G_2 := \{a \in G \colon 2a = 0\}$$

forms a subgyrogroup of G.

Proof. Clearly, $0 \in G_2$. Let $a, b \in G_2$. Then $a \oplus a = 2a = 0$, which implies $a = \ominus a$. Hence, $\ominus a \in G_2$. As in the proof of Proposition 3.10 of [18], $L_a^m = L_{ma}$ for all $a \in G$, $m \in \mathbb{Z}$. Hence, by Lemma 3.8,

$$L_{2(a\oplus b)} = L_{a\oplus b}^2 = L_a \circ L_b^2 \circ L_a = L_a \circ L_{2b} \circ L_a = L_{2a} = \mathrm{id}_G.$$

It follows that $2(a \oplus b) = 0$ and so $a \oplus b \in G_2$. By the subgyrogroup criterion [19, Proposition 14], $G_2 \leqslant G$. □

If G is a finite gyrocommutative gyrogroup of *odd* order, then G_2 given in Theorem 3.9 is the trivial subgyrogroup of G. In fact, if a is a nonidentity element of G, then $|a|$ divides $|G|$ by Proposition 6.1 of [18]. This implies $|a|$ is odd and hence $2a \neq 0$. In contrast, if G is a finite gyrocommutative gyrogroup of *even* order, then G_2 is nontrivial since Theorem 3.7 ensures the existence of a nonidentity element of G of order two.

4. Applications of Cauchy's theorem

Let H be a subgyrogroup of a gyrogroup G. For each $a \in G$, the *right coset of H by a*, denoted by $H \oplus a$, is defined as $H \oplus a = \{h \oplus a \colon h \in H\}$. As a consequence of the right cancellation law in a gyrogroup [23, Eq. (2.64)], the right gyrotranslation by a, R_a, is a bijection from G to itself. Hence, the restriction of R_a to H is a bijection from H to $H \oplus a$ and so H and $H \oplus a$ have the same size. The following theorem shows that the *right* cosets of a cyclic subgyrogroup of G forms a *disjoint* partition of G. In contrast, the *left* cosets of a cyclic subgyrogroup of G need not partition G.

Theorem 4.1. *Let G be a (finite or infinite) gyrogroup and let $a \in G$. The collection of right cosets of the cyclic subgyrogroup $\langle a\rangle$ in G is a disjoint partition of G.*

Proof. Note that if $x \in G$, then $\langle a\rangle \oplus x \neq \emptyset$. In fact, $x = 0 \oplus x \in \langle a\rangle \oplus x$. This implies that $G = \bigcup\limits_{x\in G} \langle a\rangle \oplus x$. Suppose that $x, y \in G$ are such that $\langle a\rangle \oplus x \cap \langle a\rangle \oplus y$ is not empty, namely $b \in \langle a\rangle \oplus x \cap \langle a\rangle \oplus y$. Then $b = ma \oplus x = na \oplus y$ for some $m, n \in \mathbb{Z}$. To complete the proof, we show that $\langle a\rangle \oplus x = \langle a\rangle \oplus y$. Let $z \in \langle a\rangle \oplus x$. Then $z = ka \oplus x$. We compute

$$\begin{aligned} z &= ka \oplus x \\ &= ((k-m)a \oplus ma) \oplus x \\ &= (k-m)a \oplus (ma \oplus \mathrm{gyr}\,[ma, (k-m)a]x) \\ &= (k-m)a \oplus (ma \oplus x) \\ &= (k-m)a \oplus (na \oplus y) \\ &= ((k-m)a \oplus na) \oplus \mathrm{gyr}\,[(k-m)a, na]y \\ &= (k-m+n)a \oplus y, \end{aligned}$$

which implies $z \in \langle a \rangle \oplus y$. We have the second equation from Proposition 3.7 of [18]; the third equation from the right gyroassociative law; the forth equation from Proposition 3.10 of [18]; the sixth equation from the left gyroassociative law; the last equation from Propositions 3.7 and 3.10 of [18]. This proves $\langle a \rangle \oplus x \subseteq \langle a \rangle \oplus y$. Similarly, $z = k'a \oplus y$ for some $k' \in \mathbb{Z}$ implies $z = (k' - n + m)a \oplus x$, and we have the reverse inclusion $\langle a \rangle \oplus y \subseteq \langle a \rangle \oplus x$. □

Lemma 4.2. *Let G be a gyrogroup and let a be an element of G of finite order. If $n \in \mathbb{Z}$ and $na = 0$, then n is divisible by $|a|$.*

Proof. If $n = 0$, the statement is trivial. We may therefore assume that $n \neq 0$. Set $|a| = m$. Using the division algorithm, we write $n = mk + r$ for some $k, r \in \mathbb{Z}$ such that $0 \leq r < m$. From Proposition 3.7 of [18], we have

$$0 = na = (mk + r)a = k(ma) \oplus ra = 0 \oplus ra = ra.$$

By the minimality of m, $r = 0$. Hence, $n = mk$ and so $m \mid n$. □

Lemma 4.3. *Let q be a prime and let n be a positive integer such that $n < q$. Let G be a gyrogroup of order nq. If a is an element of G of order q, then for all $x \in G$, $|x| = q$ implies $x \in \langle a \rangle$.*

Proof. Let $a \in G$ with $|a| = q$. Suppose that $x \in G$ and $|x| = q$. We prove that there must be distinct integers $i, j \in \{0, 1, \ldots, q-1\}$ such that $\langle a \rangle \oplus ix \cap \langle a \rangle \oplus jx \neq \emptyset$. Note that $|\langle a \rangle \oplus b| = |\langle a \rangle| = q$ for all $b \in G$ by the remark above. Suppose to the contrary that for all $i, j \in \{0, 1, \ldots, q-1\}$, if $i \neq j$, then $\langle a \rangle \oplus ix \cap \langle a \rangle \oplus jx = \emptyset$. Hence, $\left| \bigcup_{i=0}^{q-1} \langle a \rangle \oplus ix \right| = \sum_{i=0}^{q-1} |\langle a \rangle \oplus ix| = \sum_{i=0}^{q-1} q = q^2$, which is impossible, since $\bigcup_{i=0}^{q-1} \langle a \rangle \oplus ix \subseteq G$ and so $\left| \bigcup_{i=0}^{q-1} \langle a \rangle \oplus ix \right| \leq |G| = nq < q^2$. Hence, there are integers i, j with $0 \leq i \neq j < q$ for which $\langle a \rangle \oplus ix \cap \langle a \rangle \oplus jx \neq \emptyset$. There is no loss in assuming that $i < j$. By Theorem 4.1, $\langle a \rangle \oplus ix = \langle a \rangle \oplus jx$. This implies $jx = c \oplus ix$ for some $c \in \langle a \rangle$. By the right cancellation law,

$$c = (c \oplus ix) \boxplus (\ominus ix) = jx \boxplus (\ominus ix) = jx \oplus \operatorname{gyr}[jx, ix](\ominus ix) = jx \ominus ix = (j - i)x.$$

By Corollary 3.15 (2) of [18], $|(j-i)x| = \dfrac{|x|}{\gcd(|x|, j-i)} = q$ for $0 < j - i < q$. Since $c \in \langle a \rangle$, $\langle c \rangle \leqslant \langle a \rangle$. Since $|c| = q = |a|$, $\langle c \rangle = \langle a \rangle$. Similarly, $\langle (j-i)x \rangle = \langle x \rangle$. Therefore, $\langle x \rangle = \langle a \rangle$ and hence $x \in \langle a \rangle$. □

Theorem 4.4. *Let q be a prime and let n be a positive integer such that $n < q$. Let G be a gyrogroup of order nq. Define*

$$G_q = \{a \in G \colon qa = 0\}. \tag{4}$$

Then G_q is either the trivial subgyrogroup or the unique subgyrogroup of G order q.

Proof. If $G_q = \{0\}$, then we are done. We may therefore assume that $G_q \neq \{0\}$. Hence, $qa = 0$ for some $a \in G \setminus \{0\}$. By Lemma 4.2, $|a|$ divides q. Since q is a prime and $a \neq 0$, $|a| = q$. It follows that $\langle a \rangle$ is a subgyrogroup of G of order q. If K is a subgyrogroup of G of order q, then $K = \langle b \rangle$ for some $b \in K$ by Theorem 6.2 of [18]. Since $|b| = q$, Lemma 4.3 implies $b \in \langle a \rangle$. Hence, $K = \langle b \rangle = \langle a \rangle$. This proves existence and uniqueness of the subgyrogroup of G of order q.

Next, we prove that $G_q = \langle a \rangle$. Let $x \in \langle a \rangle$. Then either $x = 0$ or $|x| = q$. In either case, $qx = 0$. Hence, $x \in G_q$. This proves $\langle a \rangle \subseteq G_q$. Let $x \in G_q$. Then $qx = 0$. If $x = 0$, then $x \in \langle a \rangle$. We may therefore assume that $x \neq 0$. By Lemma 4.2, $|x|$ divides q and so $|x| = q$. By Lemma 4.3, $x \in \langle a \rangle$ and we have the reverse inclusion $G_q \subseteq \langle a \rangle$. □

A subgyrogroup H of a gyrogroup G is called an *L-subgyrogroup* of G if

$$\operatorname{gyr}[a, h](H) = H$$

for all $a \in G$, $h \in H$. One of the main aspects of L-subgyrogroups is that they partition G into left cosets of equal size [19, Theorem 20].

Theorem 4.5. *If G_q given in Theorem 4.4 is nontrivial, then it is an L-subgyrogroup of G of index n.*

Proof. Assume that $G_q \neq \{0\}$. Let $a, b \in G$. Since $\operatorname{gyr}[a, b]$ is a gyrogroup automorphism of G, $\operatorname{gyr}[a, b](G_q)$ forms a subgyrogroup of G of order q. By the uniqueness of G_q, $\operatorname{gyr}[a, b](G_q) = G_q$. By definition, $G_q \leqslant_L G$. As $G_q \leqslant_L G$, the index formula holds and hence $[G\colon G_q] = |G|/|G_q| = n$. □

Theorem 4.6. *If G is a gyrogroup of order pq, where p and q are primes with $p < q$, then G contains the unique subgyrogroup of order q.*

Proof. By Cauchy's theorem for gyrogroups of order pq [18, Theorem 6.9], G has an element of order q. So, $G_q \neq \{0\}$ and the theorem follows directly from Theorem 4.4. □

Theorem 4.7. *Let G be a gyrogroup of order pq, where p and q are primes with $p < q$. If the unique subgyrogroup of G of order q is normal in G, then G is solvable.*

Proof. Let N be the unique subgyrogroup of G of order q and assume that $N \trianglelefteq G$. By Theorem 6.2 of [18], N is a cyclic group of order q and hence is an abelian group. Since $N \trianglelefteq G$, G/N has the quotient gyrogroup structure and $|G/N| = [G\colon N] = p$. Hence, G/N is an abelian group as well. Therefore, the series $\{0\} \leqslant N \leqslant G$ fulfills the condition of a solvable gyrogroup. □

Let Γ be a group. A subgroup Ξ of Γ is said to be *characteristic* in Γ if Ξ is invariant under the automorphisms of Γ, that is, if $\tau(\Xi) = \Xi$ for all τ in $\operatorname{Aut}(\Gamma)$. Since group-theoretic conjugation $\kappa_g\colon x \mapsto gxg^{-1}$, $x \in \Gamma$, defines a group automorphism of Γ for all $g \in \Gamma$, every characteristic subgroup of Γ is normal in Γ. From this point of view, characteristic subgroups are sometimes called *strongly normal* subgroups.

In light of Theorem 4.4, not only the structure of a finite gyrogroup, but also the structure of a finite group, is revealed, as shown in the following theorem.

Theorem 4.8. *Let q be a prime and let n be a positive integer such that $n < q$. Every group of order nq contains the unique characteristic subgroup of order q.*

Proof. Let Γ be a group of order nq. By Cauchy's theorem for groups, Γ has an element of order q. By Theorem 4.4, Γ has the unique subgroup of order q, say Ξ. If τ is a group automorphism of Γ, then $\tau(\Xi)$ is indeed a subgroup of Γ of order q. Hence, $\tau(\Xi) = \Xi$. This proves that Ξ is characteristic in Γ. □

Note that if the integer n in Theorem 4.8 becomes a prime, we recover the well-known result in abstract algebra that any group of order pq, where p and q are primes with $p < q$, contains the unique normal subgroup of order q. This result arises as an application of the Sylow theorems, see for instance [4, p. 143]. Further, it is not difficult to see that Theorem 4.8 can be obtained as a consequence of the Sylow theorems as well.

Acknowledgment. The first author would like to thank the Department of Mathematics, North Dakota State University and his host. This research was supported by Chiang Mai University.

References

[1] **M. Aschbacher**, *On Bol loops of exponent 2*, J. Algebra **288** (2005), 99 – 136.

[2] **B. Baumeister and A. Stein**, *Self-invariant 1-factorizations of complete graphs and finite Bol loops of exponent 2*, Beiträge Algebra Geom. **51** (2010), 117 – 135.

[3] **N. Carter**, *Visual group theory*, Classroom Resource Materials, MAA, 2009.

[4] **D.S. Dummit and R.M. Foote**, *Abstract algebra*, 3 ed., John Wiley & Sons, Hoboken, NJ, 2004.

[5] **T. Foguel, M.K. Kinyon, and J.D. Phillips**, *On twisted subgroups and Bol loops of odd order*, Rocky Mountain J. Math. **36** (2006), 183 – 212.

[6] **T. Foguel and A.A. Ungar**, *Involutory decomposition of groups into twisted subgroups and subgroups*, J. Group Theory **3** (2000), 27 – 46.

[7] **T. Foguel and A.A. Ungar**, *Gyrogroups and the decomposition of groups into twisted subgroups and subgroups*, Pacific J. Math. **197** (2001), 1 – 11.

[8] **J.A. Gallian**, *The classification of groups of order 2p*, Math. Mag. **74** (2001), 60 – 61.

[9] **G. Glauberman**, *On loops of odd order*, J. Algebra **1** (1964), 374 – 396.

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

[11] **R. Lal and A.C. Yadav**, *Twisted automorphisms and twisted right gyrogroups*, Comm. Algebra **43** (2015), 3442 – 3458.

[12] **J. Lawson**, *Clifford algebras, Möbius transformations, Vahlen matrices, and B-loops*, Comment. Math. Univ. Carolin. **51** (2010), no. 2, 319 – 331.

[13] **G.P. Nagy**, *A class of finite simple Bol loops of exponent 2*, Trans. Amer. Math. Soc. **361** (2009), 5331 – 5343.

[14] **H.O. Pflugfelder**, *Quasigroups and loops: An introduction*, Sigma Series in Pure Mathematics 7, Heldermann Verlag, Berlin, 1991.

[15] **T. Suksumran**, *Essays in mathematics and its applications: In honor of Vladimir Arnold*, T. M. Rassias and P. M. Pardalos (eds.), pp. 369 – 437, Springer, 2016.

[16] **T. Suksumran**, *Gyrogroup actions: A generalization of group actions*, J. Algebra **454** (2016), 70 – 91.

[17] **T. Suksumran**, *Involutive groups, unique 2-divisibility, and related gyrogroup structures*, J. Algebra Appl. **16** (2017), no. 5, 1750114 (22 pages).

[18] **T. Suksumran and K. Wiboonton**, *Lagrange's theorem for gyrogroups and the Cauchy property*, Quasigroups Related Systems **22** (2014), 283 – 294.

[19] **T. Suksumran and K. Wiboonton**, *Isomorphism theorems for gyrogroups and L-subgyrogroups*, J. Geom. Symmetry Phys. **37** (2015), 67 – 83.

[20] **A.A. Ungar**, *Hyperbolic trigonometry in the Einstein relativistic velocity model of hyperbolic geometry*, Comput. Math. Appl. **40** (2000), 313 – 332.

[21] **A.A. Ungar**, *Beyond the Einstein addition law and its gyroscopic Thomas Precession: The theory of gyrogroups and gyrovector spaces*, Fundamental Theories of Physics, vol. 117, Kluwer Academic, Dordrecht, 2001.

[22] **A.A. Ungar**, *Einstein's velocity addition law and its hyperbolic geometry*, Comput. Math. Appl. **53** (2007), 1228 – 1250.

[23] **A.A. Ungar**, *Analytic hyperbolic geometry and Albert Einstein's Special Theory of Relativity*, World Scientific, Hackensack, NJ, 2008.

[24] **A.A. Ungar**, *A gyrovector space approach to hyperbolic geometry*, Synthesis Lectures on Math. Statistics #4, Morgan & Claypool, San Rafael, CA, 2009.

[25] **A.A. Ungar**, *Barycentric calculus in Euclidean and hyperbolic geometry: A comparative introduction*, World Scientific, Hackensack, NJ, 2010.

[26] **A.A. Ungar**, *Hyperbolic triangle centers: The special relativistic approach*, Springer-Verlag, New York, 2010.

[27] **A.A. Ungar**, *Analytic hyperbolic geometry in N dimensions: An introduction*, CRC Press, Boca Raton, FL, 2015.

Received August 3, 2016

T. Suksumran
Department of Mathematics, Faculty of Science, Chiang Mai University, Chiang Mai 50200, Thailand
E-mail: teerapong.suksumran@cmu.ac.th

A. A. Ungar
Department of Mathematics, North Dakota State University, Fargo, ND 58105, USA
E-mail: abraham.ungar@ndsu.edu