Quasigroups and Related Systems **20** (2012), 139 – 156

Bipolar fuzzy Lie superalgebras

Muhammad Akram, Wenjuan Chen and Yunqiang Yin

Abstract. We introduce the notion of bipolar fuzzy Lie sub-superalgebras (resp. bipolar fuzzy ideals) and present some of their properties. First we investigate the properties of bipolar fuzzy Lie sub-superalgebras and bipolar fuzzy ideals under homomorphisms of Lie superalgebras. Next we study bipolar fuzzy bracket product, solvable bipolar fuzzy ideals and nilpotent bipolar fuzzy ideals of Lie superalgebras.

1. Introduction

The concept of fuzzy set was first initiated by Zadeh [16] in 1965 and since then, fuzzy set has become an important tool in studying scientific subjects, in particular, it can be applied in a wide variety of disciplines such as computer science, medical science, management science, social science, engineering and so on. There are a number of generalizations of Zadeh's fuzzy set theory so far reported in the literature viz., interval-valued fuzzy theory, intuitionistic fuzzy theory, L-fuzzy theory, probabilistic fuzzy theory and so on. In 1994, Zhang [17, 18] initiated the concept of bipolar fuzzy sets as a generalization of fuzzy sets. Bipolar fuzzy sets are an extension of fuzzy sets whose membership degree range is $[-1, 1]$. In a bipolar fuzzy set, the membership degree 0 of an element means that the element is irrelevant to the corresponding property, the membership degree $(0, 1]$ of an element indicates that the element somewhat satisfies the property, and the membership degree $[-1, 0)$ of an element indicates that the element somewhat satisfies the implicit counter-property. Although bipolar fuzzy sets and intuitionistic fuzzy sets look similar to each other, they are essentially different sets [15]. In many domains, it is important to be able to deal with bipolar information. It is noted that positive information represents what is granted to be possible, while negative information represents what is considered to be impossible. This domain has recently motivated new research in several directions. In particular, fuzzy and possibilistic formalisms for bipolar information have been proposed [12], because when we deal with spatial information in image processing or in spatial reasoning applications, this bipolarity also occurs. For instance, when we assess the position of an object in a space, we may have positive information expressed as a set of possible places and negative information expressed as a set of impossible places.

2010 Mathematics Subject Classification: 04A72, 17B99
Keywords: Lie superalgebra, bipolar fuzzy Lie sub-superalgebra, bipolar fuzzy ideal, solvable bipolar fuzzy ideal, nilpotent bipolar fuzzy ideal.

As another example, let us consider the spatial relations. Human beings consider "left" and "right" as opposite directions. But this does not mean that one of them is the negation of the other. The semantics of “opposite" captures a notion of symmetry rather than a strict complementation. In particular, there may be positions which are considered neither to the right nor to the left of some reference object, thus leaving some room for indetermination. This corresponds to the idea that the union of positive and negative information does not cover the whole space.

The theory of Lie superalgebras was constructed by V.G. Kac [14] in 1977 as a generalization of the theory of Lie algebras. This theory had played an important role in both mathematics and physics. In particular, Lie superalgebras are important in theoretical physics where they are used to describe the mathematics of supersymmetry [11]. Furthermore, Lie superalgebras had found many applications in computer science such as unimodal polynomials [13].

Recently, Chen [7, 8, 9, 10] have considered Lie superalgebras in fuzzy settings, intuitionistic fuzzy settings, interval-valued fuzzy settings and investigated their several properties. Akram introduced the notion of cofuzzy Lie superalgebras over a cofuzzy field in [4]. Now, it is natural to consider Lie superalgebras in bipolar fuzzy settings. In this paper, we introduce the notion of bipolar fuzzy Lie sub-superalgebras (resp. bipolar fuzzy ideals) and investigate the properties of bipolar fuzzy Lie sub-superalgebras and bipolar fuzzy ideals under homomorphisms of Lie superalgebras. We also introduce the concept of bipolar fuzzy bracket product and study solvable bipolar fuzzy ideals and nilpotent bipolar fuzzy ideals of Lie superalgebras and present the corresponding theorems parallel to Lie superalgebras. We have used standard definitions and terminologies in this paper. For notations, terminologies and applications not mentioned in the paper, the readers are referred to [2–6, 15, 17].

2. Preliminaries

In this section, we review some elementary aspects that are necessary for this paper.

Definition 2.1. [14] Suppose that V is a vector space and $V_{\bar{0}}, V_{\bar{1}}$ are its (vector) subspaces. Let $V = V_{\bar{0}} \oplus V_{\bar{1}}$ be the direct sum of the subspaces. Then V (with this decomposition) is called a $\mathbb{Z}_2$-*graded vector space* if each element v of a $\mathbb{Z}_2$-graded vector space has a unique expression of the form $v = v_{\bar{0}} + v_{\bar{1}}$ $(v_{\bar{0}} \in V_{\bar{0}},\ v_{\bar{1}} \in V_{\bar{1}})$. The subspaces $V_{\bar{0}}$ and $V_{\bar{1}}$ are called the even part and odd part of V, respectively. In particular, if v is an element of either $V_{\bar{0}}$ or $V_{\bar{1}}$, v is said to be homogeneous.

Definition 2.2. [14] A $\mathbb{Z}_2$-graded vector space $\mathbb{L} = \mathbb{L}_{\bar{0}} \oplus \mathbb{L}_{\bar{1}}$ with a Lie bracket

$$[\ ,\ ] : \mathbb{L} \times \mathbb{L} \xrightarrow{\text{bilinear}} \mathbb{L}$$

is called a *Lie superalgebra*, if it satisfies the following conditions:

(1) $[\mathbb{L}_i, \mathbb{L}_j] \subseteq \mathbb{L}_{i+j}$ for $i,\, j \in \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$,

(2) $[x, y] = -(-1)^{|x||y|}[y, x]$ (antisymmetry),

(3) $[x, [y, z]] = [[x, y], z] + (-1)^{|x||y|}[[x, z], y]$(Jacobi identity),

where for any homogeneous element $a \in \mathbb{L}_i$, $i = \bar{0}, \bar{1}$. The subspaces $\mathbb{L}_{\bar{0}}$ and $\mathbb{L}_{\bar{1}}$ are called the even and odd parts of $\mathbb{L}$, respectively. Therefore, a Lie algebra is a Lie superalgebra with trivial odd part.

Definition 2.3. [14] If $\varphi : \mathbb{L}_1 \to \mathbb{L}_2$ is a linear map between Lie superalgebras $\mathbb{L}_1$ $=\mathbb{L}_{1\bar{0}} \oplus \mathbb{L}_{1\bar{1}}$ and $\mathbb{L}_2 = \mathbb{L}_{2\bar{0}} \oplus \mathbb{L}_{2\bar{1}}$ such that

(4) $\varphi(\mathbb{L}_{1i}) \subseteq \mathbb{L}_{2i}$ $(i \in \mathbb{Z}_2)$ (preserving the grading),

(5) $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ (preserving the Lie bracket).

Then φ is called a *homomorphism* of Lie superalgebras.

Throughout this paper, we denote V a vector space, $\mathbb{L}$ a Lie superalgebra over field F.

Let μ be a *fuzzy subset* on V, i.e., a map $\mu : V \to [0, 1]$. In this paper, the notations $x \vee y = \max\{x, y\}$ and $x \wedge y = \min\{x, y\}$.

Definition 2.4. [17] Let X be a nonempty set. A *bipolar fuzzy set* B in X is an object having the form

$$B = \{(x,\, \mu_B^P(x),\, \mu_B^N(x)) \,|\, x \in X\}$$

where $\mu_B^P : X \to [0,\, 1]$ and $\mu_B^N : X \to [-1,\, 0]$ are mappings. For the sake of simplicity, we shall use the symbol $B = (\mu_B^P,\, \mu_B^N)$ for the bipolar fuzzy set $B = \{(x,\, \mu_B^P(x),\, \mu_B^N(x)) \,|\, x \in X\}$.

Definition 2.5. [15] For every two bipolar fuzzy sets $A = (\mu_A^P, \mu_A^N)$ and $B = (\mu_B^P, \mu_B^N)$ in X, we define

- $(A \bigcap B)(x) = (\min(\mu_A^P(x), \mu_B^P(x)), \max(\mu_A^N(x), \mu_B^N(x)))$,
- $(A \bigcup B)(x) = (\max(\mu_A^P(x), \mu_B^P(x)), \min(\mu_A^N(x), \mu_B^N(x)))$.

In order to point out the differences between intuitionistic fuzzy Lie sub-superalgebras and bipolar fuzzy Lie sub-superalgebras, we omit the similar proofs in this paper.

Lemma 2.6. *$A = (\mu_A^P, \mu_A^N)$ is a bipolar fuzzy subspace of V if and only if μ_A^P and μ_A^N are fuzzy subspaces of V.* □

Lemma 2.7. *Let $A = (\mu_A^P, \mu_A^N)$ and $B = (\mu_B^P, \mu_B^N)$ be bipolar fuzzy subspaces of V. Then $A + B$ is also a bipolar fuzzy subspace of V.* □

Lemma 2.8. *Let $A = (\mu_A^P, \mu_A^N)$ and $B = (\mu_B^P, \mu_B^N)$ be bipolar fuzzy subspaces of V. Then $A \cap B$ is also a bipolar fuzzy subspace of V.* □

Lemma 2.9. *Let $A = (\mu_A^P, \mu_A^N)$ be a bipolar fuzzy subspace of $V^{'}$ and ϕ be a mapping from vector space V to $V^{'}$. Then the inverse image $\phi^{-1}(A)$ is also a bipolar fuzzy subspace of V.* □

Lemma 2.10. *Let $A = (\mu_A^P, \mu_A^N)$ be a bipolar fuzzy subspace of V and f be a mapping from V to $V^{'}$. Then the image $\phi(A)$ is also a bipolar fuzzy subspace of V'.* □

3. Bipolar fuzzy Lie sub-superalgebras

Definition 3.1. Let $V = V_{\bar{0}} \oplus V_{\bar{1}}$ be a $\mathbb{Z}_2$-graded vector space. Suppose that $A_{\bar{0}} = (\mu_{A_{\bar{0}}}^P, \mu_{A_{\bar{0}}}^N)$ and $A_{\bar{1}} = (\mu_{A_{\bar{1}}}^P, \mu_{A_{\bar{1}}}^N)$ are bipolar fuzzy vector subspaces of $V_{\bar{0}}$, $V_{\bar{1}}$, respectively. We define $A'_{\bar{0}} = (\mu_{A'_{\bar{0}}}^P, \mu_{A'_{\bar{0}}}^N)$ where

$$\mu_{A'_{\bar{0}}}^P(x) = \begin{cases} \mu_{A_{\bar{0}}}^P(x) & x \in V_{\bar{0}} \\ 0 & x \notin V_{\bar{0}} \end{cases}, \quad \mu_{A'_{\bar{0}}}^N(x) = \begin{cases} \mu_{A_{\bar{0}}}^N(x) & x \in V_{\bar{0}} \\ 0 & x \notin V_{\bar{0}} \end{cases}$$

and define $A'_{\bar{1}} = (\mu_{A'_{\bar{1}}}^P, \mu_{A'_{\bar{1}}}^N)$ where

$$\mu_{A'_{\bar{1}}}^P(x) = \begin{cases} \mu_{A_{\bar{1}}}^P(x) & x \in V_{\bar{1}} \\ 0 & x \notin V_{\bar{1}} \end{cases}, \quad \mu_{A'_{\bar{1}}}^N(x) = \begin{cases} \mu_{A_{\bar{1}}}^N(x) & x \in V_{\bar{1}} \\ 0 & x \notin V_{\bar{1}} \end{cases}$$

Then $A'_{\bar{0}} = (\mu_{A'_{\bar{0}}}^P, \mu_{A'_{\bar{0}}}^N)$ and $A'_{\bar{1}} = (\mu_{A'_{\bar{1}}}^P, \mu_{A'_{\bar{1}}}^N)$ are the bipolar fuzzy vector subspaces of V. Moreover, we have $A'_{\bar{0}} \cap A'_{\bar{1}} = (\mu_{A'_{\bar{0}} \cap A'_{\bar{1}}}^P, \mu_{A'_{\bar{0}} \cap A'_{\bar{1}}}^N)$, where

$$\mu_{A'_{\bar{0}} \cap A'_{\bar{1}}}^P(x) = \mu_{A'_{\bar{0}}}^P(x) \wedge \mu_{A'_{\bar{1}}}^P(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases},$$

$$\mu_{A'_{\bar{0}} \cap A'_{\bar{1}}}^N(x) = \mu_{A'_{\bar{0}}}^N(x) \vee \mu_{A'_{\bar{1}}}^N(x) = \begin{cases} -1 & x = 0 \\ 0 & x \neq 0 \end{cases}.$$

So $A'_{\bar{0}} + A'_{\bar{1}}$ is the direct sum and denoted by $A_{\bar{0}} \oplus A_{\bar{1}}$. If $A = (\mu_A^P, \mu_A^N)$ is an bipolar fuzzy vector subspace of V and $A = A_{\bar{0}} \oplus A_{\bar{1}}$, then $A = (\mu_A^P, \mu_A^N)$ is called a *$\mathbb{Z}_2$-graded bipolar fuzzy vector subspace* of V.

Definition 3.2. Let $A = (\mu_A^P, \mu_A^N)$ be an bipolar fuzzy set of $\mathbb{L}$. Then $A = (\mu_A^P, \mu_A^N)$ is called a *bipolar fuzzy Lie sub-superalgebra* of $\mathbb{L}$, if it satisfies the following conditions:

(1) $A = (\mu_A^P, \mu_A^N)$ is a $\mathbb{Z}_2$-graded bipolar fuzzy vector subspace,

(2) $\mu_A^P([x, y]) \geq \mu_A^P(x) \wedge \mu_A^P(y)$ and $\mu_A^N([x, y]) \leq \mu_A^N(x) \vee \mu_A^N(y)$.

If the condition (2) is replaced by

(3) $\mu_A^P([x,y]) \geq \mu_A^P(x) \vee \mu_A^P(y)$ and $\mu_A^N([x,y]) \leq \mu_A^N(x) \wedge \mu_A^N(y)$,

then $A = (\mu_A^P, \mu_A^N)$ is called a *bipolar fuzzy ideal* of $\mathbb{L}$.

Example 3.3. Let $N = N_{\bar{0}} \oplus N_{\bar{1}}$, where $N_{\bar{0}} = \langle e \rangle, N_{\bar{1}} = \langle a_1, \cdots, a_n, b_1, \cdots, b_n \rangle$ and $[a_i, b_i] = e, i = 1, 2, \cdots n$, the remaining brackets being zero. Then N is Lie superalgebra. Define $A_{\bar{0}} = (\mu_{A_{\bar{0}}}^P, \mu_{A_{\bar{0}}}^N)$ where

$$\mu_{A_{\bar{0}}}^P(x) = \begin{cases} 0.7 & x \in N_{\bar{0}} \setminus \{0\} \\ 1 & x = 0 \end{cases}, \quad \mu_{A_{\bar{0}}}^N(x) = \begin{cases} -0.2 & x \in N_{\bar{0}} \setminus \{0\} \\ -1 & x = 0 \end{cases}.$$

Define $A_{\bar{1}} = (\mu_{A_{\bar{1}}}^P, \mu_{A_{\bar{1}}}^N)$ where

$$\mu_{A_{\bar{1}}}^P(x) = \begin{cases} 0.5 & x \in N_{\bar{1}} \setminus \{0\} \\ 1 & x = 0 \end{cases}, \quad \mu_{A_{\bar{1}}}^N(x) = \begin{cases} -0.4 & x \in N_{\bar{1}} \setminus \{0\} \\ -1 & x = 0 \end{cases}.$$

Define $A = (\mu_A^P, \mu_A^N)$ by $A = A_{\bar{0}} \oplus A_{\bar{1}}$. Then $A = (\mu_A^P, \mu_A^N)$ is an bipolar fuzzy ideal of N. □

Definition 3.4. For any $t \in [0,1]$ and fuzzy subset μ^P of $\mathbb{L}$, the set $U(\mu^P, t) = \{x \in \mathbb{L} | \mu^P(x) \geqslant t\}$ (resp. $L(\mu^P, t) = \{x \in \mathbb{L} | \mu^P(x) \leqslant t\}$) is called an *upper* (resp. *lower*) *t-level cut* of μ^P.

The proofs of the following theorems are omitted.

Theorem 3.5. *If $A = (\mu_A^P, \mu_A^N)$ is an bipolar fuzzy Lie sub-superalgebra (resp. bipolar fuzzy ideal) of $\mathbb{L}$, then the sets $U(\mu_A^P, t)$ and $L(\mu_A^N, t)$ are Lie sub-superalgebras (resp. ideals) of $\mathbb{L}$ for every $t \in Im\mu_A^P \cap Im\mu_A^N$.* □

Theorem 3.6. *If $A = (\mu_A^P, \mu_A^N)$ is an bipolar fuzzy set of $\mathbb{L}$ such that all non-empty level sets $U(\mu_A^P, t)$ and $L(\mu_A^N, t)$ are Lie sub-superalgebras (resp. ideals) of $\mathbb{L}$, then $A = (\mu_A^P, \mu_A^N)$ is an bipolar fuzzy Lie sub-superalgebra (resp. bipolar fuzzy ideal) of $\mathbb{L}$.* □

Theorem 3.7. *If $A = (\mu_A^P, \mu_A^N)$ and $B = (\mu_B^P, \mu_B^N)$ are bipolar fuzzy Lie sub-superalgebras (resp. bipolar fuzzy ideals) of $\mathbb{L}$, then so is $A + B = (\mu_{A+B}^P, \mu_{A+B}^N)$.* □

Theorem 3.8. *If $A = (\mu_A^P, \mu_A^N)$ and $B = (\mu_B^P, \mu_B^N)$ are bipolar fuzzy Lie sub-superalgebras (resp. bipolar fuzzy ideals) of $\mathbb{L}$, then so is $A \cap B = (\mu_{A\cap B}^P, \mu_{A\cap B}^N)$.* □

Proposition 3.9. *Let $\varphi : \mathbb{L} \to \mathbb{L}'$ be a Lie homomorphism. If $A = (\mu_A, \mu_A^N)$ is a bipolar fuzzy Lie sub-superalgebra (resp. bipolar fuzzy ideal) of $\mathbb{L}'$, then the bipolar fuzzy set $\varphi^{-1}(A)$ of $\mathbb{L}$ is also a bipolar fuzzy Lie sub-superalgebra (resp. bipolar fuzzy ideal).*

Proof. Since φ preserves the grading, we have $\varphi(x) = \varphi(x_{\bar{0}}+x_{\bar{1}}) = \varphi(x_{\bar{0}})+\varphi(x_{\bar{1}}) \in \mathbb{L}'_{\bar{0}} \oplus \mathbb{L}'_{\bar{1}}$, for $x = x_{\bar{0}} + x_{\bar{1}} \in \mathbb{L}$. We define $\varphi^{-1}(A)_{\bar{0}} = (\mu^P_{\varphi^{-1}(A)_{\bar{0}}}, \mu^N_{\varphi^{-1}(A)_{\bar{0}}})$ where $\mu^P_{\varphi^{-1}(A)_{\bar{0}}} = \varphi^{-1}(\mu^P_{A_{\bar{0}}})$, $\mu^N_{\varphi^{-1}(A)_{\bar{0}}} = \varphi^{-1}(\mu^N_{A_{\bar{0}}})$ and $\varphi^{-1}(A)_{\bar{1}} = (\mu^P_{\varphi^{-1}(A)_{\bar{1}}}, \mu^N_{\varphi^{-1}(A)_{\bar{1}}})$ where $\mu^P_{\varphi^{-1}(A)_{\bar{1}}} = \varphi^{-1}(\mu^P_{A_{\bar{1}}})$, $\mu^N_{\varphi^{-1}(A)_{\bar{1}}} = \varphi^{-1}(\mu^N_{A_{\bar{1}}})$. By Lemma 2.9, we have that they are bipolar fuzzy subspaces of $\mathbb{L}_{\bar{0}}, \mathbb{L}_{\bar{1}}$, respectively.

Then we define $\varphi^{-1}(A)'_{\bar{0}} = (\mu^P_{\varphi^{-1}(A)'_{\bar{0}}}, \mu^N_{\varphi^{-1}(A)'_{\bar{0}}})$, where $\mu^P_{\varphi^{-1}(A)'_{\bar{0}}} = \varphi^{-1}(\mu^P_{A'_{\bar{0}}})$, $\mu^N_{\varphi^{-1}(A)'_{\bar{0}}} = \varphi^{-1}(\mu^N_{A'_{\bar{0}}})$, and $\varphi^{-1}(A)'_{\bar{1}} = (\mu^P_{\varphi^{-1}(A)'_{\bar{1}}}, \mu^N_{\varphi^{-1}(A)'_{\bar{1}}})$, where $\mu^P_{\varphi^{-1}(A)'_{\bar{1}}} = \varphi^{-1}(\mu^P_{A'_{\bar{1}}})$, $\mu^N_{\varphi^{-1}(A)'_{\bar{1}}} = \varphi^{-1}(\mu^N_{A'_{\bar{1}}})$.

Clearly,

$$\mu^P_{\varphi^{-1}(A)'_{\bar{0}}}(x) = \begin{cases} \mu^P_{\varphi^{-1}(A)_{\bar{0}}}(x) & x \in \mathbb{L}_{\bar{0}} \\ 0 & x \notin \mathbb{L}_{\bar{0}} \end{cases}, \ \mu^N_{\varphi^{-1}(A)'_{\bar{0}}}(x) = \begin{cases} \mu^N_{\varphi^{-1}(A)'_{\bar{0}}}(x) & x \in \mathbb{L}_{\bar{0}} \\ 0 & x \notin \mathbb{L}_{\bar{0}} \end{cases}$$

and

$$\mu^P_{\varphi^{-1}(A)'_{\bar{1}}}(x) = \begin{cases} \mu^P_{\varphi^{-1}(A)'_{\bar{1}}}(x) & x \in \mathbb{L}_{\bar{1}} \\ 0 & x \notin \mathbb{L}_{\bar{1}} \end{cases}, \ \mu^N_{\varphi^{-1}(A)'_{\bar{1}}}(x) = \begin{cases} \mu^N_{\varphi^{-1}(A)'_{\bar{1}}}(x) & x \in \mathbb{L}_{\bar{1}} \\ 0 & x \notin \mathbb{L}_{\bar{1}} \end{cases}$$

These show that $\varphi^{-1}(A)'_{\bar{0}}$ and $\varphi^{-1}(A)'_{\bar{1}}$ are the extensions of $\varphi^{-1}(A)_{\bar{0}}$ and $\varphi^{-1}(A)_{\bar{1}}$.

For $0 \neq x \in \mathbb{L}$, we have

$$\begin{aligned} \mu^P_{\varphi^{-1}(A)'_{\bar{0}}}(x) \wedge \mu^P_{\varphi^{-1}(A)'_{\bar{1}}}(x) &= \varphi^{-1}(\mu^P_{A'_{\bar{0}}})(x) \wedge \varphi^{-1}(\mu^P_{A'_{\bar{1}}})(x) \\ &= \mu^P_{A'_{\bar{0}}}(\varphi(x)) \wedge \mu^P_{A'_{\bar{1}}}(\varphi(x)) = 0 \end{aligned}$$

and

$$\begin{aligned} \mu^N_{\varphi^{-1}(A)'_{\bar{0}}}(x) \vee \mu^N_{\varphi^{-1}(A)'_{\bar{1}}}(x) &= \varphi^{-1}(\mu^N_{A'_{\bar{0}}})(x) \vee \varphi^{-1}(\mu^N_{A'_{\bar{1}}})(x) \\ &= \mu^N_{A'_{\bar{0}}}(\varphi(x)) \vee \mu^N_{A'_{\bar{1}}}(\varphi(x)) = 0. \end{aligned}$$

For $x \in \mathbb{L}$ we have

$$\begin{aligned} \mu^P_{\varphi^{-1}(A)'_{\bar{0}}+\varphi^{-1}(A)'_{\bar{1}}}(x) &= \sup_{x=a+b} \{\mu^P_{\varphi^{-1}(A)'_{\bar{0}}}(a) \wedge \mu^P_{\varphi^{-1}(A)'_{\bar{1}}}(b)\} \\ &= \sup_{x=a+b} \{\varphi^{-1}(\mu^P_{A'_{\bar{0}}})(a) \wedge \varphi^{-1}(\mu^P_{A'_{\bar{1}}})(b)\} \\ &= \sup_{x=a+b} \{\mu^P_{A'_{\bar{0}}}(\varphi(a)) \wedge \mu^P_{A'_{\bar{1}}}(\varphi(b))\} \\ &= \sup_{\varphi(x)=\varphi(a)+\varphi(b)} \{\mu^P_{A'_{\bar{0}}}(\varphi(a)) \wedge \mu^P_{A'_{\bar{1}}}(\varphi(b))\} \\ &= \mu^P_{A'_{\bar{0}}+A'_{\bar{1}}}(\varphi(x)) = \mu^P_A(\varphi(x)) = \mu^P_{\varphi^{-1}(A)}(x) \end{aligned}$$

and

$$\mu^N_{\varphi^{-1}(A)'_{\bar{0}}+\varphi^{-1}(A)'_{\bar{1}}}(x) = \inf_{x=a+b} \{\mu^N_{\varphi^{-1}(A)'_{\bar{0}}}(a) \vee \mu^N_{\varphi^{-1}(A)'_{\bar{1}}}(b)\}$$

$$\begin{aligned}
&= \inf_{x=a+b}\{\varphi^{-1}(\mu^N_{A'_{\bar{0}}})(a) \vee \varphi^{-1}(\mu^N_{A'_{\bar{1}}})(b)\}\\
&= \inf_{x=a+b}\{\mu^N_{A'_{\bar{0}}}(\varphi(a)) \vee \mu^N_{A'_{\bar{1}}}(\varphi(b))\}\\
&= \inf_{\varphi(x)=\varphi(a)+\varphi(b)}\{\mu^N_{A'_{\bar{0}}}(\varphi(a)) \vee \mu^N_{A'_{\bar{1}}}(\varphi(b))\}\\
&= \mu^N_{A'_{\bar{0}}+A'_{\bar{1}}}(\varphi(x)) = \mu^N_A(\varphi(x)) = \mu^N_{\varphi^{-1}(A)}(x).
\end{aligned}$$

So, $\varphi^{-1}(A) = \varphi^{-1}(A)_{\bar{0}} \oplus \varphi^{-1}(A)_{\bar{1}}$ is a $\mathbb{Z}_2$-graded bipolar fuzzy vector subspace of $\mathbb{L}$.

Let $x, y \in \mathbb{L}$. Then

(1) $\mu^P_{\varphi^{-1}(A)}([x,y]) = \mu^P_A(\varphi([x,y])) = \mu^P_A([\varphi(x),\varphi(y)]) \geq \mu^P_A(\varphi(x)) \wedge \mu^P_A(\varphi(y)) = \mu^P_{\varphi^{-1}(A)}(x) \wedge \mu^P_{\varphi^{-1}(A)}(y)$, and $\mu^N_{\varphi^{-1}(A)}([x,y]) = \mu^N_A(\varphi([x,y])) = \mu^N_A([\varphi(x),\varphi(y)]) \leq \mu^N_A(\varphi(x)) \vee \mu^N_A(\varphi(y)) = \mu^N_{\varphi^{-1}(A)}(x) \vee \mu^N_{\varphi^{-1}(A)}(y)$, thus $\varphi^{-1}(A)$ is a bipolar fuzzy Lie sub-superalgebra.

(2) $\mu^P_{\varphi^{-1}(A)}([x,y]) = \mu^P_A(\varphi([x,y])) = \mu^P_A([\varphi(x),\varphi(y)]) \geq \mu^P_A(\varphi(x)) \vee \mu^P_A(\varphi(y)) = \mu^P_{\varphi^{-1}(A)}(x) \vee \mu^P_{\varphi^{-1}(A)}(y)$, and $\mu^N_{\varphi^{-1}(A)}([x,y]) = \mu^N_A(\varphi([x,y])) = \mu^N_A([\varphi(x),\varphi(y)]) \leq \mu^N_A(\varphi(x)) \wedge \mu^N_A(\varphi(y)) = \mu^N_{\varphi^{-1}(A)}(x) \wedge \mu^N_{\varphi^{-1}(A)}(y)$, thus $\varphi^{-1}(A)$ is a bipolar fuzzy ideal. □

Proposition 3.10. *Let $\varphi : \mathbb{L} \to \mathbb{L}'$ be a Lie homomorphism. If $A = (\mu^P_A, \mu^N_A)$ is a bipolar fuzzy Lie sub-superalgebra of $\mathbb{L}$, then the bipolar fuzzy set $\varphi(A)$ is also a bipolar fuzzy Lie sub-superalgebra of $\mathbb{L}'$.*

Proof. Since $A = (\mu^P_A, \mu^N_A)$ is a bipolar fuzzy Lie sub-superalgebra of $\mathbb{L}$, we have $A = A_{\bar{0}} \oplus A_{\bar{1}}$ where $A_{\bar{0}} = (\mu_{A_{\bar{0}}}, \mu^N_{A_{\bar{0}}}), A_{\bar{1}} = (\mu_{A_{\bar{1}}}, \mu^N_{A_{\bar{1}}})$ are bipolar fuzzy vector subspaces of $\mathbb{L}_{\bar{0}}$ and $\mathbb{L}_{\bar{1}}$, respectively. We define $\varphi(A)_{\bar{0}} = (\mu^P_{\varphi(A)_{\bar{0}}}, \mu^N_{\varphi(A)_{\bar{0}}})$, where $\mu^P_{\varphi(A)_{\bar{0}}} = \varphi(\mu^P_{A_{\bar{0}}})$, $\mu^N_{\varphi(A)_{\bar{0}}} = \varphi(\mu^N_{A_{\bar{0}}})$, $\varphi(A)_{\bar{1}} = (\mu^P_{\varphi(A)_{\bar{1}}}, \mu^N_{\varphi(A)_{\bar{1}}})$, where $\mu^P_{\varphi(A)_{\bar{1}}} = \varphi(\mu^P_{A_{\bar{1}}})$, $\mu^N_{\varphi(A)_{\bar{1}}} = \varphi(\mu^N_{A_{\bar{1}}})$. By Lemma 2.10, $\varphi(A)_{\bar{0}}$ and $\varphi(A)_{\bar{1}}$ are bipolar fuzzy subspaces of $\mathbb{L}_{\bar{0}}$, $\mathbb{L}_{\bar{1}}$, respectively. And extend them to $\varphi(A)'_{\bar{0}}, \varphi(A)'_{\bar{1}}$, we define $\varphi(A)'_{\bar{0}} = (\mu^P_{\varphi(A)'_{\bar{0}}}, \mu^N_{\varphi(A)'_{\bar{0}}})$ where $\mu^P_{\varphi(A)'_{\bar{0}}} = \varphi(\mu^P_{A'_{\bar{0}}}), \mu^N_{\varphi(A)'_{\bar{0}}} = \varphi(\mu^N_{A'_{\bar{0}}})$ and $\varphi(A)'_{\bar{1}} = (\mu^P_{\varphi(A)'_{\bar{1}}}, \mu^N_{\varphi(A)'_{\bar{1}}})$ where $\mu^P_{\varphi(A)'_{\bar{1}}} = \varphi(\mu^P_{A'_{\bar{1}}}), \mu^N_{\varphi(A)'_{\bar{1}}} = \varphi(\mu^N_{A'_{\bar{1}}})$. Clearly,

$$\mu^P_{\varphi(A)'_{\bar{0}}}(x) = \begin{cases} \mu^P_{\varphi(A)_{\bar{0}}}(x) & x \in \mathbb{L}_{\bar{0}} \\ 0 & x \notin \mathbb{L}_{\bar{0}} \end{cases}, \quad \mu^N_{\varphi(A)'_{\bar{0}}}(x) = \begin{cases} \mu^N_{\varphi(A)_{\bar{0}}}(x) & x \in \mathbb{L}_{\bar{0}} \\ 0 & x \notin \mathbb{L}_{\bar{0}} \end{cases},$$

$$\mu^P_{\varphi(A)'_{\bar{1}}}(x) = \begin{cases} \mu^P_{\varphi(A)_{\bar{1}}}(x) & x \in \mathbb{L}_{\bar{1}} \\ 0 & x \notin \mathbb{L}_{\bar{1}} \end{cases}, \quad \mu^N_{\varphi(A)'_{\bar{1}}}(x) = \begin{cases} \mu^N_{\varphi(A)_{\bar{1}}}(x) & x \in \mathbb{L}_{\bar{1}} \\ 0 & x \notin \mathbb{L}_{\bar{1}} \end{cases}.$$

For $0 \neq x \in \mathbb{L}'$ we have

$$\begin{aligned}
\mu^P_{\varphi(A)'_{\bar{0}}}(x) \wedge \mu^P_{\varphi(A)'_{\bar{1}}}(x) &= \varphi(\mu^P_{A'_{\bar{0}}})(x) \wedge \varphi(\mu^P_{A'_{\bar{1}}})(x) = \sup_{x=\varphi(a)}\{\mu^P_{A'_{\bar{0}}}(a)\} \wedge \sup_{x=\varphi(a)}\{\mu^P_{A'_{\bar{1}}}(a)\}\\
&= \sup_{x=\varphi(a)}\{\mu^P_{A'_{\bar{0}}}(a) \wedge \mu^P_{A'_{\bar{1}}}(a)\} = 0,
\end{aligned}$$

$$\begin{aligned}\mu^N_{\varphi(A)'_{\bar0}}(x) \vee \mu^N_{\varphi(A)'_{\bar1}}(x) = \varphi(\mu^N_{A'_{\bar0}})(x) \vee \varphi(\mu^N_{A'_{\bar1}})(x) &= \inf_{x=\varphi(a)}\{\mu^N_{A'_{\bar0}}(a)\} \vee \inf_{x=\varphi(a)}\{\mu^N_{A'_{\bar1}}(a)\}\\ &= \inf_{x=\varphi(a)}\{\mu^N_{A'_{\bar0}}(a) \vee \mu^N_{A'_{\bar1}}(a)\} = 0.\end{aligned}$$

Let $y \in \mathbb{L}'$. Then

$$\begin{aligned}\mu^P_{\varphi(A)'_{\bar0}+\varphi(A)'_{\bar1}}(y) &= \sup_{y=a+b}\{\mu^P_{\varphi(A)'_{\bar0}}(a) \wedge \mu^P_{\varphi(A)'_{\bar1}}(b)\} = \sup_{y=a+b}\{\varphi(\mu^P_{A'_{\bar0}})(a) \wedge \varphi(\mu^P_{A'_{\bar1}})(b)\}\\ &= \sup_{y=a+b}\{\sup_{a=\varphi(m)}\{\mu^P_{A'_{\bar0}}(m)\} \wedge \sup_{b=\varphi(n)}\{\mu^P_{A'_{\bar1}}(n)\}\}\\ &= \sup_{y=\varphi(x)}\{\sup_{x=m+n}\{\mu^P_{A'_{\bar0}}(m) \wedge \mu^P_{A'_{\bar1}}(n)\}\}\\ &= \sup_{y=\varphi(x)}\{(\mu^P_{A'_{\bar0}+A'_{\bar1}})(x)\} = \sup_{y=\varphi(x)}\{\mu^P_A(x)\} = \mu^P_{\varphi(A)}(y),\end{aligned}$$

$$\begin{aligned}\mu^N_{\varphi(A)'_{\bar0}+\varphi(A)'_{\bar1}}(y) &= \inf_{y=a+b}\{\mu^N_{\varphi(A)'_{\bar0}}(a) \vee \mu^N_{\varphi(A)'_{\bar1}}(b)\} = \inf_{y=a+b}\{\varphi(\mu^N_{A'_{\bar0}})(a) \vee \varphi(\mu^N_{A'_{\bar1}})(b)\}\\ &= \inf_{y=a+b}\{\inf_{a=\varphi(m)}\{\mu^N_{A'_{\bar0}}(m)\} \vee \inf_{b=\varphi(n)}\{\mu^N_{A'_{\bar1}}(n)\}\}\\ &= \inf_{y=\varphi(x)}\{\inf_{x=m+n}\{\mu^N_{A'_{\bar0}}(m) \vee \mu^N_{A'_{\bar1}}(n)\}\}\\ &= \inf_{y=\varphi(x)}\{(\mu^N_{A'_{\bar0}+A'_{\bar1}})(x)\} = \inf_{y=\varphi(x)}\{\mu^N_A(x)\} = \mu^N_{\varphi(A)}(y).\end{aligned}$$

So $\varphi(A) = \varphi(A)_{\bar0} \oplus \varphi(A)_{\bar1}$ is a $\mathbb{Z}_2$-graded bipolar fuzzy vector subspace.

Let $x, y \in \mathbb{L}'$. It is enough to show $\mu^P_{\varphi(A)}([x,y]) \geq \mu^P_{\varphi(A)}(x) \wedge \mu^P_{\varphi(A)}(y)$ and $\mu^N_{\varphi(A)}([x,y]) \leq \mu^N_{\varphi(A)}(x) \vee \mu^N_{\varphi(A)}(y)$. If $\mu^P_{\varphi(A)}([x,y]) < \mu^P_{\varphi(A)}(x) \wedge \mu^P_{\varphi(A)}(y)$, we have $\mu^P_{\varphi(A)}([x,y]) < \mu^P_{\varphi(A)}(x)$ and $\mu^P_{\varphi(A)}([x,y]) < \mu^P_{\varphi(A)}(y)$. We choose a number $t \in [0,1]$ such that $\mu^P_{\varphi(A)}([x,y]) < t < \mu^P_{\varphi(A)}(x)$ and $\mu^P_{\varphi(A)}([x,y]) < t < \mu^P_{\varphi(A)}(y)$. Then there exist $a \in \varphi^{-1}(x), b \in \varphi^{-1}(y)$ such that $\mu^P_A(a) > t$, $\mu^P_A(b) > t$. Since $\varphi([a,b]) = [\varphi(a), \varphi(b)] = [x,y]$, we have $\mu^P_{\varphi(A)}([x,y]) = \sup\limits_{[x,y]=\varphi([a,b])}\{\mu^P_A([a,b])\} \geq \mu^P_A([a,b]) \geqslant \mu^P_A(a) \wedge \mu^P_A(b) > t > \mu^P_{\varphi(A)}([x,y])$. This is a contradiction.

Suppose that $\mu^N_{\varphi(A)}([x,y]) > \mu^N_{\varphi(A)}(x) \vee \mu^N_{\varphi(A)}(y)$, we have $\mu^N_{\varphi(A)}([x,y]) > \mu^N_{\varphi(A)}(x)$ and $\mu^N_{\varphi(A)}([x,y]) > \mu^N_{\varphi(A)}(y)$. We choose $t \in [-1,0]$ such that $\varphi(\mu^N)([x,y]) > t > \mu^N_{\varphi(A)}(x)$ and $\mu^N_{\varphi(A)}([x,y]) > t > \mu^N_{\varphi(A)}(y)$. Then there exist $a \in \varphi^{-1}(x), b \in \varphi^{-1}(y)$ such that $\mu^N_A(a) < t, \mu^N_A(b) < t$. Since $\varphi([a,b]) = [\varphi(a), \varphi(b)] = [x,y]$, we have $\mu^N_{\varphi(A)}([x,y]) = \inf\limits_{[x,y]=\varphi([a,b])}\{\mu^N_A([a,b])\} \leqslant \mu^N_A([a,b]) \leq \mu^N_A(a) \vee \mu^N_A(b) < t < \mu^N_{\varphi(A)}([x,y])$. This is a contradiction.

Therefore, $\varphi(A)$ is a bipolar fuzzy Lie sub-superalgebra of $\mathbb{L}'$. □

We state the following results without proofs.

Proposition 3.11. *Let $\varphi : \mathbb{L} \to \mathbb{L}'$ be a surjective Lie homomorphism. If $A = (\mu^P_A, \mu^N_A)$ is a bipolar fuzzy ideal of $\mathbb{L}$, then $\varphi(A)$ is also a bipolar fuzzy ideal of $\mathbb{L}'$.* □

Theorem 3.12. *Let $\varphi : \mathbb{L} \to \mathbb{L}'$ be a surjective Lie homomorphism. Then for any bipolar fuzzy ideals $A = (\mu^P_A, \mu^N_A)$ and $B = (\mu_B, \mu^N_B)$ of $\mathbb{L}$ we have $\varphi(A + B) = \varphi(A) + \varphi(B)$.* □

4. Bipolar fuzzy bracket product

Definition 4.1. For any bipolar fuzzy sets $A = (\mu^P_A, \mu^N_A)$ and $B = (\mu^P_B, \mu^N_B)$ of $\mathbb{L}$, we define the *bipolar fuzzy bracket product* $[A, B] = (\mu^P_{[A,B]}, \mu^N_{[A,B]})$ putting

$$\mu^P_{[A,B]}(x) = \begin{cases} \sup\limits_{x=\sum\limits_{i\in N}\alpha_i[x_i,y_i]} \{\min\limits_{i\in N}\{\mu^P_A(x_i) \wedge \mu^P_B(y_i)\}\} & \text{where } \alpha_i \in F,\ x_i, y_i \in \mathbb{L} \\ 0 & \text{if } x \text{ is not expressed as } x = \sum\limits_{i\in N} \alpha_i[x_i, y_i] \end{cases}$$

and

$$\mu^N_{[A,B]}(x) = \begin{cases} \inf\limits_{x=\sum\limits_{i\in N}\alpha_i[x_i,y_i]} \{\max\limits_{i\in N}\{\mu^N_A(x_i) \vee \mu^N_B(y_i)\}\} & \text{where } \alpha_i \in F,\ x_i, y_i \in \mathbb{L} \\ 0 & \text{if } x \text{ is not expressed as } x = \sum\limits_{i\in N} \alpha_i[x_i, y_i] \end{cases} .$$

Lemma 4.2. *Let $A_1 = (\mu^P_{A_1}, \mu^N_{A_1}), A_2 = (\mu^P_{A_2}, \mu^N_{A_2}), B_1 = (\mu^P_{B_1}, \mu^N_{B_1})$ and $B_2 = (\mu^P_{B_2}, \mu^N_{B_2})$ be bipolar fuzzy sets of $\mathbb{L}$ such that $A_1 \subseteq A_2$, $B_1 \subseteq B_2$. Then $[A_1, B_1] \subseteq [A_2, B_2]$. In particular, if $A = (\mu^P_A, \mu^N_A)$ and $B = (\mu^P_B, \mu^N_B)$ are bipolar fuzzy sets of $\mathbb{L}$, then $[A_1, B] \subseteq [A_2, B]$ and $[A, B_1] \subseteq [A, B_2]$.* □

Lemma 4.3. *Let $A_1 = (\mu^P_{A_1}, \mu^N_{A_1}), A_2 = (\mu^P_{A_2}, \mu^N_{A_2}), B_1 = (\mu^P_{B_1}, \mu^N_{B_1}), B_2 = (\mu^P_{B_2}, \mu^N_{B_2})$ and $A = (\mu^P_A, \mu^N_A), B = (\mu^P_B, \mu^N_B)$ be any bipolar fuzzy vector subspaces of $\mathbb{L}$. Then $[A_1+A_2, B] = [A_1, B]+[A_2, B]$ and $[A, B_1+B_2] = [A, B_1]+[A, B_2]$.* □

Lemma 4.4. *Let $A = (\mu^P_A, \mu^N_A)$ and $B = (\mu^P_B, \mu^N_B)$ be bipolar fuzzy vector subspaces of $\mathbb{L}$. Then for any $\alpha, \beta \in F$, we have $[\alpha A, B] = \alpha[A, B]$ and $[A, \beta B] = \beta[A, B]$.* □

Theorem 4.5. *Let $A_1 = (\mu^P_{A_1}, \mu^N_{A_1}), A_2 = (\mu^P_{A_2}, \mu^N_{A_2}), B_1 = (\mu^P_{B_1}, \mu^N_{B_1}), B_2 = (\mu^P_{B_2}, \mu^N_{B_2})$ and $A = (\mu^P_A, \mu^N_A), B = (\mu^P_B, \mu^N_B)$ be bipolar fuzzy vector subspaces of $\mathbb{L}$. Then for any $\alpha, \beta \in F$, we have*

$$[\alpha A_1 + \beta A_2, B] = \alpha[A_1, B] + \beta[A_2, B],$$

$$[A, \alpha B_1 + \beta B_2] = \alpha[A, B_1] + \beta[A, B_2].$$

Proof. The results follow from Theorem 4.3 and Lemma 4.4. □

Lemma 4.6. *Let $A = (\mu_A^P, \mu_A^N)$ and $B = (\mu_B^P, \mu_B^N)$ be any two bipolar fuzzy vector subspaces of $\mathbb{L}$. Then $[A, B]$ is a bipolar fuzzy vector subspace of $\mathbb{L}$.* □

Let $A = (\mu_A^P, \mu_A^N)$ and $B = (\mu_B^P, \mu_B^N)$ be $\mathbb{Z}_2$-graded bipolar fuzzy vector subspaces of $\mathbb{L}$. Then $A = A_{\bar{0}} \oplus A_{\bar{1}}$, $B = B_{\bar{0}} \oplus B_{\bar{1}}$, where $A_{\bar{0}}, B_{\bar{0}}$ are bipolar fuzzy vector subspaces of $\mathbb{L}_{\bar{0}}$ and $A_{\bar{1}}, B_{\bar{1}}$ are bipolar fuzzy vector subspaces of $\mathbb{L}_{\bar{1}}$.

We define:

- $[A_{\bar{0}}, B_{\bar{0}}] = (\mu^P_{[A_{\bar{0}},B_{\bar{0}}]}, \mu^N_{[A_{\bar{0}},B_{\bar{0}}]})$, where

$$\mu^P_{[A_{\bar{0}},B_{\bar{0}}]}(x) = \sup_{x=\sum\limits_{i\in N} \alpha_i[x_i,y_i]} \{\min_{i\in N}\{\mu^P_{A_{\bar{0}}}(x_i) \wedge \mu^P_{B_{\bar{0}}}(y_i)\}\}$$

and

$$\mu^N_{[A_{\bar{0}},B_{\bar{0}}]}(x) = \inf_{x=\sum\limits_{i\in N} \alpha_i[x_i,y_i]} \{\max_{i\in N}\{\mu^N_{A_{\bar{0}}}(x_i) \vee \mu^N_{B_{\bar{0}}}(y_i)\}\},$$

for $x_i \in \mathbb{L}_{\bar{0}}$ and $y_i \in \mathbb{L}_{\bar{0}}$,

- $[A_{\bar{0}}, B_{\bar{1}}] = (\mu^P_{[A_{\bar{0}},B_{\bar{1}}]}, \mu^N_{[A_{\bar{0}},B_{\bar{1}}]})$, where

$$\mu^P_{[A_{\bar{0}},B_{\bar{1}}]}(x) = \sup_{x=\sum\limits_{i\in N} \alpha_i[x_i,y_i]} \{\min_{i\in N}\{\mu^P_{A_{\bar{0}}}(x_i) \wedge \mu^P_{B_{\bar{1}}}(y_i)\}\}$$

and

$$\mu^N_{[A_{\bar{0}},B_{\bar{1}}]}(x) = \inf_{x=\sum\limits_{i\in N} \alpha_i[x_i,y_i]} \{\max_{i\in N}\{\mu^N_{A_{\bar{0}}}(x_i) \vee \mu^N_{B_{\bar{1}}}(y_i)\}\},$$

for $x_i \in \mathbb{L}_{\bar{0}}$ and $y_i \in \mathbb{L}_{\bar{1}}$,

- $[A_{\bar{1}}, B_{\bar{0}}] = (\mu^P_{[A_{\bar{1}},B_{\bar{0}}]}, \mu^N_{[A_{\bar{1}},B_{\bar{0}}]})$, where

$$\mu^P_{[A_{\bar{1}},B_{\bar{0}}]}(x) = \sup_{x=\sum\limits_{i\in N} \alpha_i[x_i,y_i]} \{\min_{i\in N}\{\mu^P_{A_{\bar{1}}}(x_i) \wedge \mu^P_{B_{\bar{0}}}(y_i)\}\}$$

and

$$\mu^N_{[A_{\bar{1}},B_{\bar{0}}]}(x) = \inf_{x=\sum\limits_{i\in N} \alpha_i[x_i,y_i]} \{\max_{i\in N}\{\mu^N_{A_{\bar{1}}}(x_i) \vee \mu^N_{B_{\bar{0}}}(y_i)\}\},$$

for $x_i \in \mathbb{L}_{\bar{1}}$ and $y_i \in \mathbb{L}_{\bar{0}}$,

- $[A_{\bar{1}}, B_{\bar{1}}] = (\mu^P_{[A_{\bar{1}},B_{\bar{1}}]}, \mu^N_{[A_{\bar{1}},B_{\bar{1}}]})$, where

$$\mu^P_{[A_{\bar{1}},B_{\bar{1}}]}(x) = \sup_{x=\sum\limits_{i\in N} \alpha_i[x_i,y_i]} \{\min_{i\in N}\{\mu^P_{A_{\bar{1}}}(x_i) \wedge \mu^P_{B_{\bar{1}}}(y_i)\}\}$$

and

$$\mu^N_{[A_{\bar{1}},B_{\bar{1}}]}(x) = \inf_{x=\sum\limits_{i\in N} \alpha_i[x_i,y_i]} \{\max_{i\in N}\{\mu^N_{A_{\bar{1}}}(x_i) \vee \mu^N_{B_{\bar{1}}}(y_i)\}\},$$

for $x_i \in \mathbb{L}_{\bar{1}}$ and $y_i \in \mathbb{L}_{\bar{1}}$.

Note that $[A_{\bar{0}}, B_{\bar{0}}], [A_{\bar{1}}, B_{\bar{1}}]$ are bipolar fuzzy sets of $\mathbb{L}_{\bar{0}}$ and $[A_{\bar{0}}, B_{\bar{1}}], [A_{\bar{1}}, B_{\bar{0}}]$ are bipolar fuzzy sets of $\mathbb{L}_{\bar{1}}$.

Lemma 4.7. *Let $A = (\mu_A^P, \mu_A^N)$ and $B = (\mu_B^P, \mu_B^N)$ be any two $\mathbb{Z}_2$-graded bipolar fuzzy vector subspaces of $\mathbb{L}$. Then*

$[A, B]_{\bar{0}} := [A_{\bar{0}}, B_{\bar{0}}] + [A_{\bar{1}}, B_{\bar{1}}]$ *is a bipolar fuzzy vector subspace of* $\mathbb{L}_{\bar{0}}$,

$[A, B]_{\bar{1}} := [A_{\bar{0}}, B_{\bar{1}}] + [A_{\bar{1}}, B_{\bar{0}}]$ *is a bipolar fuzzy vector subspace of* $\mathbb{L}_{\bar{1}}$ *and*

$[A, B]$ *is a $\mathbb{Z}_2$-graded bipolar fuzzy vector subspace of* $\mathbb{L}$.

Proof. Since $[A_{\bar{0}}, B_{\bar{0}}]$ and $[A_{\bar{1}}, B_{\bar{1}}]$ are bipolar fuzzy vector subspaces of $\mathbb{L}_{\bar{0}}$ by Lemma 5.5, we can get that $[A, B]_{\bar{0}} := [A_{\bar{0}}, B_{\bar{0}}] + [A_{\bar{1}}, B_{\bar{1}}]$ is a bipolar fuzzy vector subspace of $\mathbb{L}_{\bar{0}}$ by Lemma 2.6. Similarly, $[A, B]_{\bar{1}} := [A_{\bar{0}}, B_{\bar{1}}] + [A_{\bar{1}}, B_{\bar{0}}]$ is a bipolar fuzzy vector subspace of $\mathbb{L}_{\bar{1}}$. We define $[A, B]'_{\bar{0}} := [A'_{\bar{0}}, B'_{\bar{0}}] + [A'_1, B'_{\bar{1}}]$ and $[A, B]'_{\bar{1}} := [A'_{\bar{0}}, B'_{\bar{1}}] + [A'_1, B'_{\bar{0}}]$.

Let $x \in \mathbb{L}_{\bar{0}}$. We have

$$
\begin{aligned}
\mu^P_{[A,B]'_{\bar{0}}}(x) &= (\mu^P_{[A'_{\bar{0}},B'_{\bar{0}}]+[A'_{\bar{1}},B'_{\bar{1}}]})(x)\\
&= \sup_{x=a+b}\{\mu^P_{[A'_{\bar{0}},B'_{\bar{0}}]}(a) \wedge \mu^P_{[A'_{\bar{1}},B'_{\bar{1}}]}(b)\}\\
&= \sup_{x=a+b}\{\sup_{a=\sum\limits_{i\in N}\alpha_i[k_i,l_i]}\{\min_{i\in N}\{\mu^P_{A'_{\bar{0}}}(k_i) \wedge \mu^P_{B'_{\bar{0}}}(l_i)\}\} \wedge\\
&\qquad\qquad \wedge \sup_{b=\sum\limits_{i\in N}\beta_i[m_i,n_i]}\{\min_{i\in N}\{\mu^P_{A'_{\bar{1}}}(m_i) \wedge \mu^P_{B'_{\bar{1}}}(n_i)\}\}\\
&= \sup_{x=a+b}\{\sup_{a=\sum\limits_{i\in N}\alpha_i[k_i,l_i]}\{\min_{i\in N}\{\mu^P_{A_{\bar{0}}}(k_i) \wedge \mu^P_{B_{\bar{0}}}(l_i)\}\} \wedge\\
&\qquad\qquad \wedge \sup_{b=\sum\limits_{i\in N}\beta_i[m_i,n_i]}\{\min_{i\in N}\{\mu^P_{A_{\bar{1}}}(m_i) \wedge \mu^P_{B_{\bar{1}}}(n_i)\}\}\\
&= \sup_{x=a+b}\{\mu^P_{[A_{\bar{0}},B_{\bar{0}}]}(a) \wedge \mu^P_{[A_{\bar{1}},B_{\bar{1}}]}(b)\} = (\mu^P_{[A_{\bar{0}},B_{\bar{0}}]+[A_{\bar{1}},B_{\bar{1}}]})(x) = \mu^P_{[A,B]_{\bar{0}}}(x)
\end{aligned}
$$

and

$$
\begin{aligned}
\mu^N_{[A,B]'_{\bar{0}}}(x) &= (\mu^N_{[A'_{\bar{0}},B'_{\bar{0}}]+[A'_{\bar{1}},B'_{\bar{1}}]})(x) = \inf_{x=a+b}\{\mu^N_{[A'_{\bar{0}},B'_{\bar{0}}]}(a) \vee \mu^N_{[A'_{\bar{1}},B'_{\bar{1}}]}(b)\}\\
&= \inf_{x=a+b}\{\inf_{a=\sum\limits_{i\in N}\alpha_i[k_i,l_i]}\{\max_{i\in N}\{\mu^N_{A'_{\bar{0}}}(k_i) \vee \mu^N_{B'_{\bar{0}}}(l_i)\}\} \vee\\
&\qquad\qquad \vee \inf_{b=\sum\limits_{i\in N}\beta_i[m_i,n_i]}\{\max_{i\in N}\{\mu^N_{A'_{\bar{1}}}(m_i) \vee \mu^N_{B'_{\bar{1}}}(n_i)\}\}
\end{aligned}
$$

$$= \inf_{x=a+b}\{ \inf_{a=\sum\limits_{i\in N}\alpha_i[k_i,l_i]}\{\max_{i\in N}\{\mu^N_{A_{\bar 0}}(k_i)\vee\mu^N_{B_{\bar 0}}(l_i)\}\}\vee$$

$$\vee \inf_{b=\sum\limits_{i\in N}\beta_i[m_i,n_i]}\{\max_{i\in N}\{\mu^N_{A_{\bar 1}}(m_i)\vee\mu^N_{B_{\bar 1}}(n_i)\}\}$$

$$= \inf_{x=a+b}\{\mu^N_{[A_{\bar 0},B_{\bar 0}]}(a)\vee\mu^N_{[A_{\bar 1},B_{\bar 1}]}(b)\} = (\mu^N_{[A_{\bar 0},B_{\bar 0}]+[A_{\bar 1},B_{\bar 1}]})(x) = \mu^N_{[A,B]_{\bar 0}}(x).$$

Now let $x\notin\mathbb{L}_{\bar 0}$. Then $\mu^P_{[A,B]'_{\bar 0}}(x)=0$ and $\mu^N_{[A,B]'_{\bar 0}}(x)=-1$. Similarly, for $x\in\mathbb{L}_{\bar 1}$, we have $\mu^P_{[A,B]'_{\bar 1}}(x)=\mu^P_{[A,B]_{\bar 1}}(x)$ and $\mu^N_{[A,B]'_{\bar 1}}(x)=\mu^N_{[A,B]_{\bar 1}}(x)$. For $x\notin\mathbb{L}_{\bar 1}$, we have $\mu^P_{[A,B]'_{\bar 1}}(x)=0$ and $\mu^N_{[A,B]'_{\bar 1}}(x)=-1$. Thus $[A,B]'_{\bar 0}$ and $[A,B]'_{\bar 1}$ are the extensions of $[A,B]_{\bar 0}$ and $[A,B]_{\bar 1}$.

Clearly, $[A,B]'_{\bar 0}\cap[A,B]'_{\bar 1}=(\mu^P_{[A,B]'_{\bar 0}\cap[A,B]'_{\bar 1}},\mu^N_{[A,B]'_{\bar 0}\cap[A,B]'_{\bar 1}})$, where

$$\mu^P_{[A,B]'_{\bar 0}\cap[A,B]'_{\bar 1}}(x)=\mu^P_{[A,B]'_{\bar 0}}(x)\wedge\mu^P_{[A,B]'_{\bar 1}}(x)=\begin{cases}1 & x=0\\ 0 & x\neq 0\end{cases},$$

$$\mu^N_{[A,B]'_{\bar 0}\cap[A,B]'_{\bar 1}}(x)=\mu^N_{[A,B]'_{\bar 0}}(x)\vee\mu^N_{[A,B]'_{\bar 1}}(x)=\begin{cases}-1 & x=0\\ \ \ 0 & x\neq 0\end{cases}.$$

For $x\in\mathbb{L}$ we have

$$\begin{aligned}[A,B](x)&=[A'_{\bar 0}+A'_{\bar 1},B'_{\bar 0}+B'_{\bar 1}](x)=([A'_{\bar 0},B'_{\bar 0}]+[A'_{\bar 1},B'_{\bar 1}]+[A'_{\bar 0},B'_{\bar 1}]+[A'_{\bar 1},B'_{\bar 0}])(x)\\&=([A,B]'_{\bar 0}+[A,B]'_{\bar 1})(x).\end{aligned}$$

Hence $[A,B]=[A,B]_{\bar 0}\oplus[A,B]_{\bar 1}$ is a $\mathbb{Z}_2$-graded bipolar fuzzy vector subspace. □

Lemma 4.8. *Let $A=(\mu^P_A,\mu^N_A)$ and $B=(\mu^P_B,\mu^N_B)$ be any two $\mathbb{Z}_2$-graded bipolar fuzzy vector subspaces of $\mathbb{L}$. Then $[A,B]=[B,A]$.* □

The following theorem is our main theorem in this section. The proof is base on Lemma 4.8. The left is similar to intuitionistic fuzzy ideal of Lie superalgebras. For more details see [10].

Theorem 4.9. *Let $A=(\mu^P_A,\mu^N_A)$ and $B=(\mu^P_B,\mu^N_B)$ be any two bipolar fuzzy ideals of $\mathbb{L}$. Then $[A,B]$ is also a bipolar fuzzy ideal of $\mathbb{L}$.* □

5. Solvable and nilpotent bipolar fuzzy ideals

Definition 5.1. Let $A=(\mu^P_A,\mu^N_A)$ be a bipolar fuzzy ideal of $\mathbb{L}$. Define inductively a sequence of bipolar fuzzy ideals of $\mathbb{L}$ by $A^{(0)}=A$, $A^{(1)}=[A^{(0)},A^{(0)}]$, $A^{(2)}=[A^{(1)},A^{(1)}],\cdots,A^{(n)}=[A^{(n-1)},A^{(n-1)}]$, then $A^{(n)}$ is called the *nth derived bipolar fuzzy ideal* of $\mathbb{L}$. In which, $A^{(i+1)}=(\mu^P_{A^{(i+1)}},\mu^N_{A^{(i+1)}})$, where

$$\mu^P_{A^{(i+1)}}(x)=\begin{cases}\sup\limits_{x=\sum\limits_{j\in N}\alpha_j[x_j,y_j]}\{\min\limits_{j\in N}\{\mu^P_{A^{(i)}}(x_j)\wedge\mu^P_{A^{(i)}}(y_j)\}\} \text{ where } \alpha_j\in F,\ x_j,y_j\in\mathbb{L}\\ 0 \qquad\qquad \text{if } x \text{ is not expressed as } x=\sum\limits_{j\in N}\alpha_j[x_j,y_j]\end{cases}$$

and

$$\mu^N_{A^{(i+1)}}(x)=\begin{cases}\inf\limits_{x=\sum\limits_{j\in N}\alpha_j[x_j,y_j]}\{\max\limits_{j\in N}\{\mu^N_{A^{(i)}}(x_j)\vee\mu^N_{A^{(i)}}(y_j)\}\} \text{ where } \alpha_j\in F,\ x_j,y_j\in\mathbb{L}\\ 0 \qquad\qquad \text{if } x \text{ is not expressed as } x=\sum\limits_{j\in N}\alpha_j[x_j,y_j].\end{cases}$$

.

From the definition, we can get $\mu^P_{A^{(0)}}\supseteq\mu^P_{A^{(1)}}\supseteq\mu^P_{A^{(2)}}\supseteq\cdots\supseteq\mu^P_{A^{(n)}}\supseteq\cdots$ and $\mu^N_{A^{(0)}}\subseteq\mu^N_{A^{(1)}}\subseteq\mu^N_{A^{(2)}}\subseteq\cdots\subseteq\mu^N_{A^{(n)}}\subseteq\cdots$.

Definition 5.2. Let $A^{(n)}$ be as above. Define: $\eta^{(n)}=\sup\{\mu^P_{A^{(n)}}(x):0\neq x\in\mathbb{L}\}$ and $\kappa^{(n)}=\inf\{\mu^N_{A^{(n)}}(x):0\neq x\in\mathbb{L}\}$. Then it is clear that $\eta^{(0)}\geqslant\eta^{(1)}\geqslant\eta^{(2)}\geqslant\cdots\geqslant\eta^{(n)}\geqslant\cdots$ and $\kappa^{(0)}\leqslant\kappa^{(1)}\leqslant\kappa^{(1)}\leqslant\cdots\leqslant\kappa^{(n)}\leqslant\cdots$.

Definition 5.3. An bipolar fuzzy ideal $A=(\mu^P_A,\mu^N_A)$ of $\mathbb{L}$ is called *solvable*, if there is a positive integer n such that $\eta^{(n)}=0$ and $\kappa^{(n)}=0$. So, it is a solvable bipolar fuzzy ideal, then there is positive integer n such that $\mu^P_{A^{(n)}}=1_0$ and $\mu^N_{A^{(n)}}=(-1)_0$.

Example 5.4. For the Lie superalgebra L from Example 3.3 we define $A_{\bar 0}=(\mu^P_{A_{\bar 0}},\mu^N_{A_{\bar 0}})$, where $\mu^P_{A_{\bar 0}}(x)=1,\mu^N_{A_{\bar 0}}(x)=-1$ for all $x\in N_{\bar 0}$. Then it is a bipolar fuzzy subspace of $N_{\bar 0}$. Let $x\in N_{\bar 1}$. Then $x=k_1a_1+k_2a_2+k_3b_1+k_4b_2$, for $k_i\neq 0$ and $i=1,2,3,4$. We define $A_{\bar 1}=(\mu^P_{A_{\bar 1}},\mu^N_{A_{\bar 1}})$ where $\mu^P_{A_{\bar 1}}(x)=\mu^P_{A_{\bar 1}}(a_1)\wedge\mu^P_{A_{\bar 1}}(a_2)\wedge\mu^P_{A_{\bar 1}}(b_1)\wedge\mu^P_{A_{\bar 1}}(b_2)$, in which $\mu^P_{A_{\bar 1}}(a_1)=0.2$, $\mu^P_{A_{\bar 1}}(a_2)=1$, $\mu^P_{A_{\bar 1}}(b_1)=0.1$, $\mu^P_{A_{\bar 1}}(b_2)=1$, $\mu^P_{A_{\bar 1}}(0)=1$, and $\mu^N_{A_{\bar 1}}(x)=\mu^N_{A_{\bar 1}}(a_1)\vee\mu^N_{A_{\bar 1}}(a_2)\vee\mu^N_{A_{\bar 1}}(b_1)\vee\mu^N_{A_{\bar 1}}(b_2)$, in which $\mu^N_{A_{\bar 1}}(a_1)=-0.7$, $\mu^N_{A_{\bar 1}}(a_2)=-1$, $\mu^N_{A_{\bar 1}}(b_1)=-0.9$, $\mu^N_{A_{\bar 1}}(b_2)=-1$, $\mu^N_{A_{\bar 1}}(0)=-1$. Then A is a bipolar fuzzy subspace of $N_{\bar 1}$.

Let $x\in N$. Then $x=ke+k_1a_1+k_2a_2+k_3b_1+k_4b_2$ for $k,k_i\neq 0$ and $i=1,2,3,4$. We define $A=(\mu^P_A,\mu^N_A)$ where $\mu^P_A(x)=\mu^P_A(e)\wedge\mu^P_A(a_1)\wedge\mu^P_A(a_2)\wedge\mu^P_A(b_1)\wedge\mu^P_A(b_2)$, in which $\mu^P_A(e)=1,\mu^P_A(a_1)=0.2$, $\mu^P_A(a_2)=1$, $\mu^P_A(b_1)=0.1$, $\mu^P_A(b_2)=1$, $\mu^P_A(0)=1$ and $\mu^N_A(x)=\mu^N_B(e)\vee\mu^N_A(a_1)\vee\mu^N_A(a_2)\vee\mu^N_A(b_1)\vee\mu^N_A(b_2)$, in which $\mu^N_A(e)=-1,\mu^N_A(a_1)=-0.7$, $\mu^N_A(a_2)=-1$, $\mu^N_A(b_1)=-0.9$, $\mu^N_A(b_2)=-1$, $\mu^N_A(0)=-1$. Then $A=A_{\bar 0}\oplus A_{\bar 1}$ is a bipolar fuzzy ideal of N.

Let $A^{(0)}=A$. Note that $[a_i,b_i]=e$ and the other brackets are zero. Then $\mu^P_{A^{(0)}}(x)=0.1$, $\mu^N_{A^{(0)}}(x)=-0.7$. We define $A^{(1)}=[A^{(0)},A^{(0)}]$. If $x\in N_1$, then x can not be expressed as $x=\sum\alpha_i[x_i,y_i]$, $x_i,y_i\in N$, so $\mu^P_{A^{(1)}}(x)=0,\mu^N_{A^{(1)}}(x)=0$. If $x\in N_0$, then x can be expressed as $x=\alpha_1[a_1,b_1]+\alpha_2[a_2,b_2]$, $\alpha_1,\alpha_2\in k$. We calculate

$$\mu^P_{A^{(1)}}(x) = \sup_{x=\sum\limits_{i=1,2}\alpha_i[a_i,b_i]}\{\min_{i=1,2}\{\mu^P_{A^{(0)}}(a_i)\wedge\mu^P_{A^{(0)}}(b_i)\}\} = 0.1,$$
$$\mu^N_{A^{(1)}}(x) = \inf_{x=\sum\limits_{i=1,2}\alpha_i[a_i,b_i]}\{\max_{i=1,2}\{\mu^N_{A^{(0)}}(a_i)\vee\mu^N_{A^{(0)}}(b_i)\}\} = -1.$$

Define $A^{(2)} = [A^{(1)}, A^{(1)}]$, we calculate

$$\mu^P_{A^{(2)}}(x) = \sup_{x=\sum\limits_{i=1,2}\alpha_i[a_i,b_i]}\{\min_{i=1,2}\{\mu^P_{A^{(1)}}(a_i)\wedge\mu^P_{A^{(1)}}(b_i)\}\} = 0,$$
$$\mu^N_{A^{(2)}}(x) = \inf_{x=\sum\limits_{i=1,2}\alpha_i[a_i,b_i]}\{\max_{i=1,2}\{\mu^N_{A^{(1)}}(a_i)\vee\mu^N_{A^{(1)}}(b_i)\}\} = 0.$$

So, $\eta^{(0)} \geqslant \eta^{(1)} \geqslant \eta^{(2)} = 0$ and $\kappa^{(0)} \leqslant \kappa^{(1)} \leqslant \kappa^{(2)} = 0$. These show that A is a solvable bipolar fuzzy ideal of N. □

From the definition of solvable bipolar fuzzy ideals, we can easily get

Lemma 5.5. *Let $A = (\mu^P_A, \mu^N_A)$ be a bipolar fuzzy Lie ideal of $\mathbb{L}$. Then $A = (\mu^P_A, \mu^N_A)$ is a solvable bipolar fuzzy ideal if and only if there is a positive integer n such that $\mu^P_{A^{(m)}} = 1_0, \mu^N_{A^{(m)}} = (-1)_0$ for all $m \geqslant n$.* □

Theorem 5.6. *Homomorphic images of solvable bipolar fuzzy ideals are also solvable bipolar fuzzy Lie ideals.*

Proof. Let $\varphi : \mathbb{L} \to \mathbb{L}'$ be a homomorphism of Lie superalgebra and assume that $A = (\mu^P_A, \mu^N_A)$ is a bipolar fuzzy ideal of $\mathbb{L}$. Let $\varphi(A) = B$, i.e, $\mu^P_B = \mu^P_{\varphi(A)}, \mu^N_B = \mu^N_{\varphi(A)}$. We prove $\mu^P_{\varphi(A^{(n)})} = \mu^P_{B^{(n)}}$ and $\mu^N_{\varphi(A^{(n)})} = \mu^N_{B^{(n)}}$ by induction on n, where n is any positive integer. Indeed, let $y \in \mathbb{L}'$. Consider $n = 1$,

$$\begin{aligned}
\mu^P_{\varphi(A^{(1)})}(y) = \mu^P_{\varphi([A,A])}(y) &= \sup_{y=\varphi(x)}\{\mu^P_{[A,A]}(x)\}\\
&= \sup_{y=\varphi(x)}\{\sup_{x=\sum\limits_{i\in N}\alpha_i[x_i,y_i]}\{\min_{i\in N}(\mu^P_A(x_i)\wedge\mu^P_A(y_i))\}\}\\
&= \sup_{y=\sum\limits_{i\in N}\alpha_i\varphi[x_i,y_i]}\{\min_{i\in N}(\mu^P_A(x_i)\wedge\mu^P_A(y_i))\}\\
&= \sup_{y=\sum\limits_{i\in N}\alpha_i[a_i,b_i]}\{\min_{i\in N}(\mu^P_A(x_i)\wedge\mu^P_A(y_i)) : \varphi(x_i) = a_i, \varphi(y_i) = b_i\}\\
&= \sup_{\sum\limits_{i\in N}\alpha_i[a_i,b_i]=y}\{\min_{i\in N}(\mu^P_B(a_i)\wedge\mu^P_B(b_i))\} = \mu^P_{[B,B]}(y) = \mu^P_{B^{(1)}}(y),
\end{aligned}$$

and

$$\begin{aligned}
\mu^N_{\varphi(A^{(1)})}(y) = \mu^N_{\varphi([A,A])}(y) &= \inf_{y=\varphi(x)}\{\mu^N_{[A,A]}(x)\}\\
&= \inf_{y=\varphi(x)}\{\inf_{x=\sum\limits_{i\in N}\alpha_i[x_i,y_i]}\{\max_{i\in N}(\mu^N_A(x_i)\vee\mu^N_A(y_i))\}\}\\
&= \inf_{y=\sum\limits_{i\in N}\alpha_i\varphi[x_i,y_i]}\{\max_{i\in N}(\mu^N_A(x_i)\vee\mu^N_A(y_i))\}\\
&= \inf_{y=\sum\limits_{i\in N}\alpha_i[a_i,b_i]}\{\max_{i\in N}(\mu^N_A(x_i)\vee\mu^N_A(y_i)) : \varphi(x_i)=a_i, \varphi(y_i)=b_i\}\\
&= \inf_{\sum\limits_{i\in N}\alpha_i[a_i,b_i]=y}\{\max_{i\in N}(\mu^N_B(a_i)\vee\mu^N_B(b_i))\} = \mu^N_{[B,B]}(y) = \mu^N_{B^{(1)}}(y).
\end{aligned}$$

These prove the case of $n=1$. Suppose that the case of $n-1$ is true, then $\mu^P_{\varphi(A^{(n)})} = \mu^P_{\varphi([A^{(n-1)},A^{(n-1)}])} = \mu^P_{[\varphi(A^{(n-1)}),\varphi(A^{(n-1)})]} = \mu^P_{[B^{(n-1)},B^{(n-1)}]} = \mu^P_{B^{(n)}}$ and $\mu^N_{\varphi(A^{(n)})} = \mu^N_{\varphi([A^{(n-1)},A^{(n-1)}])} = \mu^N_{[\varphi(A^{(n-1)}),\varphi(A^{(n-1)})]} = \mu^N_{[B^{(n-1)},B^{(n-1)}]} = \mu^N_{B^{(n)}}$. Let m be a positive integer such that $\mu^P_{A^{(m)}} = 1_0$ and $\mu^N_{A^{(m)}} = (-1)_0$. Then for any $0 \neq y \in \mathbb{L}'$, we get $\mu^P_{B^{(m)}}(y) = \mu^P_{\varphi(A^{(m)})}(y) = \sup\limits_{y=\varphi(x)}\{1_0(x)\} = 0$, $\mu^N_{B^{(m)}}(y) = \varphi(\mu^N_{A^{(m)}})(y) = \inf\limits_{y=\varphi(x)}\{(-1)_0(x)\} = 0$. So $\mu^P_{B^{(m)}} = 1_0$ and $\mu^N_{B^{(m)}} = (-1)_0$. □

Let $A = (\mu^P_A, \mu^N_A)$ be a bipolar fuzzy ideal of $\mathbb{L}$ and I be an ideal of $\mathbb{L}$. We can prove that A/I is a bipolar fuzzy ideal of $\mathbb{L}/I$.

Theorem 5.7. *Let $A = (\mu^P_A, \mu^N_A)$ be an bipolar fuzzy ideal of $\mathbb{L}$ and A/I be a solvable bipolar fuzzy ideal of $\mathbb{L}/I$. If $B = (\mu^P_B, \mu^N_B)$ is a solvable bipolar fuzzy ideal of $\mathbb{L}$ and is also a bipolar fuzzy ideal of $A = (\mu^P_A, \mu^N_A)$ such that $B(I) = A(I)$, then $A = (\mu^P_A, \mu^N_A)$ is solvable.*

Proof. Let φ be the canonical projection from $\mathbb{L}$ to $\mathbb{L}/I$. From the proof of Theorem 5.6, we get $\mu^P_{\varphi(A^{(n)})} = \mu^P_{(A/I)^{(n)}}$ and $\mu^N_{\varphi(A^{(n)})} = \mu^N_{(A/I)^{(n)}}$. Since A/I is solvable, there exists n such that $\mu^P_{(A/I)^{(n)}} = 1_0$ and $\mu^N_{(A/I)^{(n)}} = (-1)_0$.

For $0 \neq \bar{y} \in \mathbb{L}/I$, we have $\sup\limits_{m\in\varphi^{-1}(\bar{y})}\{\mu^P_{A^{(n)}}(m)\} = \mu^P_{\varphi(A^{(n)})}(\bar{y}) = \mu^P_{(A/I)^{(n)}}(\bar{y}) = 0$ and $\inf\limits_{m\in\varphi^{-1}(\bar{y})}\{\mu^N_{A^{(n)}}(m)\} = \mu^N_{\varphi(A^{(n)})}(\bar{y}) = \mu^N_{(A/I)^{(n)}}(\bar{y}) = 0$. Notice that $m \in \mathbb{L}$ and $m \neq 0$, we get $\mu^P_{A^{(n)}}(m) = 0$ and $\mu^N_{A^{(n)}}(m) = 0$.

For $\bar{y} = 0$, we have $\sup\limits_{m\in\varphi^{-1}(0)}\{\mu^P_{A^{(n)}}(m)\} = \mu^P_{\varphi(A^{(n)})}(0) = 1$ and $\inf\limits_{m\in\varphi^{-1}(0)}\{\mu^N_{A^{(n)}}(m)\} = \mu^N_{\varphi(A^{(n)})}(0) = -1$. Since $\varphi^{-1}(0) = I$ and $B(I) = A(I)$, we have $\mu^P_{B^{(n)}}(I) =$

$\mu^P_{A^{(n)}}(I)$ and $\mu^N_{B^{(n)}}(I) = \mu^N_{A^{(n)}}(I)$. For any $x \in I$, B is solvable, then there exists n such that $\mu^P_{B^{(n)}} = 1_0$ and $\mu^N_{B^{(n)}} = (-1)_0$, we have $\mu^P_{A^{(n)}} = 1_0$ and $\mu^N_{A^{(n)}} = (-1)_0$.

Hence for any $x \in \mathbb{L}$, we always have that $\mu^P_{A^{(n)}} = 1_0$ and $\mu^N_{A^{(n)}} = (-1)_0$, which imply that $A = (\mu^P_A, \mu^N_A)$ is solvable. □

Lemma 5.8. *Let $A = (\mu^P_A, \mu^N_A)$ and $B = (\mu^P_B, \mu^N_B)$ be bipolar fuzzy ideals of $\mathbb{L}$. Then $(A \oplus B)^{(n)} = A^{(n)} \oplus B^{(n)}$.*

Proof. Let $0 \neq x \in \mathbb{L}$. Then we have $[A, B] = (\mu^P_{[A,B]}, \mu^P_{[A,B]})$, where

$$\mu^P_{[A,B]}(x) = \sup_{x=\sum\limits_{i\text{ß}N} \alpha_i[x_i,y_i]} \{\underset{x\in N}{\min}(\mu^P_A(x_i) \wedge \mu^P_B(y_i))\} \leq \mu^P_A(x) \wedge \mu^P_B(x) = 0,$$

$$\mu^N_{[A,B]}(x) = \inf_{x=\sum\limits_{i\text{ß}N} \alpha_i[x_i,y_i]} \{\underset{x\in N}{\max}(\mu^N_A(x_i) \vee \mu^N_B(y_i))\} \geq \mu^N_A(x) \vee \mu^N_B(x) = 0.$$

So $\mu^P_{[A,B]} = 1_0$ and $\mu^N_{[A,B]} = (-1)_0$. Consequently, for any positive integer a, b, we have $\mu^P_{[A^{(a)},B^{(b)}]} = 1_0$ and $\mu^N_{[A^{(a)},B^{(b)}]} = (-1)_0$. We prove the lemma by induction on n.

Let $n = 1$. Then

$$(A \oplus B)^{(1)} = [A \oplus B, A \oplus B] = [A, A] \oplus [A, B] \oplus [B, A] \oplus [B, B] = A^{(1)} \oplus B^{(1)}.$$

Suppose that the case of $n - 1$ is true, then

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

So we get $(A \oplus B)^{(n)} = A^{(n)} \oplus B^{(n)}$. □

Theorem 5.9. *Direct sum of any solvable bipolar fuzzy Lie ideals is also a solvable bipolar Lie ideal.*

Proof. Let $A = (\mu^P_A, \mu^N_A)$ and $B = (\mu^P_B, \mu^N_B)$ be solvable bipolar fuzzy ideals. Then there exist positive integers m, n such that $\mu^P_{A^{(m)}} = 1_0, \mu^N_{A^{(m)}} = (-1)_0$ and $\mu^P_{B^{(n)}} = 1_0, \mu^N_{B^{(n)}} = (-1)_0$. Since $(A \oplus B)^{(m+n)} = A^{(m+n)} \oplus B^{(m+n)}$, we have $\mu^P_{(A\oplus B)^{(m+n)}} = \mu^P_{A^{(m+n)}\oplus B^{(m+n)}} = 1_0$ and $\mu^N_{(A\oplus B)^{(m+n)}} = \mu^N_{A^{(m+n)}\oplus B^{(m+n)}} = (-1)_0$. So $A \oplus B$ is a solvable bipolar fuzzy Lie ideal. □

Definition 5.10. Let $A = (\mu^P_A, \mu^N_A)$ be a bipolar fuzzy ideal of $\mathbb{L}$. Define inductively a sequence of bipolar fuzzy ideals of $\mathbb{L}$ by $A^0 = A, \quad A^1 = [A, A^0], \quad A^2 = [A, A^1], \cdots, A^n = [A, A^{n-1}] \cdots$, which is called the *descending central series* of a bipolar fuzzy ideal $A = (\mu^P_A, \mu^N_A)$ of $\mathbb{L}$. We get $\mu^P_{A^0} \supseteq \mu^P_{A^1} \supseteq \mu^P_{A^2} \supseteq \cdots \supseteq \mu^P_{A^n} \supseteq \cdots$ and $\mu^N_{A^0} \subseteq \mu^N_{A^1} \subseteq \mu^N_{A^2} \subseteq \cdots \subseteq \mu^N_{A^n} \subseteq \cdots$

Definition 5.11. For any bipolar fuzzy Lie ideal $A = (\mu^P_A, \mu^N_A)$, define $\eta^n = \sup\{\mu^P_{A^n}(x) : 0 \neq x \in \mathbb{L}\}$ and $\kappa^n = \inf\{\mu^N_{A^n}(x) : 0 \neq x \in \mathbb{L}\}$, for any positive integer n. The bipolar fuzzy ideal is called a *nilpotent bipolar fuzzy ideal*, if there is a positive integer m such that $\eta^m = 0$ and $\kappa^m = 1$, or equivalently, $\mu^P_{A^m} = 1_0$ and $\mu^N_{A^m} = (-1)_0$.

Example 5.12. Let us take the basis h, e, f of $\mathfrak{sl}(1|1)$ as follows

$$h = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}. \tag{1}$$

Then h is an even element, and e and f are odd element. Their bracket products are as follows: $[e, f] = [f, e] = h$, the other brackets $= 0$. Then $\mathfrak{sl}(1|1)$ is a three-dimensional Lie superalgebra.

Define $A_{\bar 0} = (\mu^P_{A_{\bar 0}}, \mu^N_{A_{\bar 0}}) : \mathfrak{sl}(1|1)_{\bar 0} \to [-1, 1]$ where

$$\mu^P_{A_{\bar 0}}(x) = \begin{cases} 0.6 & x = h \\ 1 & \text{otherwise} \end{cases}, \mu^N_{A_{\bar 0}}(x) = \begin{cases} -0.4 & x = h \\ -1 & \text{otherwise} \end{cases}$$

Define $A_{\bar 1} = (\mu^P_{A_{\bar 1}}, \mu^N_{A_{\bar 1}}) : \mathfrak{sl}(1|1)_{\bar 1} \to [-1, 1]$ where

$$\mu^P_{A_{\bar 1}}(x) = \begin{cases} 0.3 & x = e \\ 0.5 & x = f \\ 1 & \text{otherwise} \end{cases}, \mu^N_{A_{\bar 1}}(x) = \begin{cases} -0.7 & x = e \\ -0.5 & x = f \\ -1 & \text{otherwise} \end{cases}$$

Define $A = (\mu^P_A, \mu^N_A) : \mathfrak{sl}(1|1) \to [-1, 1]$ where $\mu^P_A(x) = \mu^P_{A_{\bar 0}}(x_{\bar 0}) \wedge \mu^P_{A_{\bar 1}}(x_{\bar 1})$ and $\mu^N_A(x) = \mu^N_{A_{\bar 0}}(x_{\bar 0}) \vee \mu^N_{A_{\bar 1}}(x_{\bar 1})$. Then A is a bipolar fuzzy ideal of $\mathfrak{sl}(1|1)$.

Let $A^0 = A$. We define $A^1 = [A, A^0]$, then if $x \in \mathfrak{sl}(1|1)_{\bar 1}$, x can not be expressed as $x = \sum \alpha_i [x_i, y_i]$, $x_i, y_i \in \mathfrak{sl}(1|1)$ then $\mu^P_{A^1}(x) = 0, \mu^N_{A^1}(x) = 0$. If $x \in \mathfrak{sl}(1|1)_{\bar 0}$, $x = \alpha[e, f]$, $\alpha \in F$, then $\mu^P_{A^1}(x) = \sup\{\mu^P_A(e) \wedge \mu^P_{A^0}(f)\} = 0.3$ and $\mu^N_{A^1}(x) = \inf\{\mu^N_A(e) \vee \mu^N_{A^0}(f)\} = -0.5$.

Define $A^2 = [A, A^1]$, we calculate if $x \in \mathfrak{sl}(1|1)_{\bar 1}$, $\mu^P_{A^2}(x) = 0, \mu^N_{A^2}(x) = 0$. If $x \in \mathfrak{sl}(1|1)_{\bar 0}$, $\mu^P_{A^2}(x) = \sup\{\mu^P_A(e) \wedge \mu^P_{A^1}(f)\} = 0$ and $\mu^N_{A^2}(x) = \inf\{\mu^N_A(e) \vee \mu^N_{A^1}(f)\} = 0$. Then we get $\eta^0 \geqslant \eta^1 \geqslant \eta^2 = 0$ and $\kappa^0 \leq \kappa^1 \leqslant \kappa^2 = 0$. So A is a nilpotent bipolar fuzzy Lie ideal of $\mathfrak{sl}(1|1)$. □

Theorem 5.13. *Homomorphic images of nilpotent bipolar fuzzy ideals are also nilpotent bipolar fuzzy Lie ideals. Direct sum of nilpotent bipolar fuzzy ideals is also a nilpotent bipolar fuzzy ideal.* □

Theorem 5.14. *If $A = (\mu^P_A, \mu^N_A)$ is a nilpotent bipolar fuzzy ideal of $\mathbb{L}$, then it is solvable.* □

References

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

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

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

[4] **M. Akram**, *Co-fuzzy Lie superalgebras over a co-fuzzy field*, World Applied Sciences Journal **7** (2009), 25 – 32.

[5] **M. Akram**, *Bipolar fuzzy graphs*, Information Sciences **181** (2011), 5548 – 5564.

[6] **M. Akram and W.A. Dudek**, *Regular bipolar fuzzy graphs*, Neural Computing & Appl. **21** (2012), $S197 - S205$.

[7] **W.J. Chen**, *Fuzzy quotient Lie superalgebras*, J. Shandong Univ., Nat. Sci. **43** (2008), 25 – 27.

[8] **W.J. Chen**, *Intuitionistic fuzzy quotient Lie superalgebras*, Internat. J. Fuzzy Systems **12** (2010), 330 – 339.

[9] **W.J. Chen and M. Akram**, *Interval-valued fuzzy structures on Lie superalgebras*, J. Fuzzy Math. **19** (2011), 951 – 968.

[10] **W.J. Chen and S. H. Zhang**, *Intuitionistic fuzzy Lie sub-superalgebras and intuitionistic fuzzy ideals*, Computers Math. Appl. **58** (2009), 1645 – 1661.

[11] **L. Corwin, Y. Nêman, and S. Sternberg**, *Graded Lie algebras in mathematics and physics* (*Bose-Fermi symmetry*), Reviews of Modern Physics **47** (1975), 573 – 603.

[12] **D. Dubois, S. Kaci and H. Prade**, *Bipolarity in Reasoning and Decision, an Introduction*, Int. Con. on Inf. Pro. Man. Unc. IPMU'04, (2004), 959 – 966.

[13] **J.W.B Hughes and J. Van der Jeugt**, *Unimodal polynomials associated with Lie algebras and superalgebras*, J. Computational Appl. Math. **37** (1991), 481 – 88.

[14] **V.G. Kac**, *Lie superalgebras*, Advances Math. **26** (1977), 8 – 96.

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

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

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

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

Received June 6, 2012

M. Akram
Punjab University College of Information Technology, University of the Punjab,
Old Campus, Lahore-54000, Pakistan
E-mail: m.akram@pucit.edu.pk

W. Chen
School of Mathematics, University of Jinan, Jinan, Shandong, 250022, P.R. China
E-mail: wjchenmath@gmail.com
Y. Yin
School of Mathematics and Information Sciences, East China Institute of Technology, Fuzhou,
Jiangxi 344000, China
E-mail: yunqiangyin@gmail.com

Quasigroups and Related Systems **20** (2012), 157 − 168

Recursively r-differentiable quasigroups within S-systems and MDS-codes

Galina B. Belyavskaya

Abstract. We study recursively r-differentiable binary quasigroups and such quasigroups with an additional property (strongly recursively r-differentiable quasigroups). These quasigroups we find in S-systems of quasigroups and give a lower bound of the parameters of idempotent 2-recursive MDS-codes that respect to strongly recursively r-differentiable quasigroups. Some illustrative examples are given.

1. Introduction

In the article [7], the notion of a recursively r-differentiable k-ary quasigroup which arise in the connect complete k-recursive codes is introduced. The minimum Hamming distance of these codes achieves the Singleton bound.

Let $Q = \{a_1, a_2, \dots, a_q\}$ be a finite set. Any subset $K \subseteq Q^n$ is called a *code of length* n or an n-*code* over the alphabet Q. An n-code is called an $[n,k]_Q$-*code* if $\mid K \mid = q^k$. An $[n,k,d]_Q$-code is an $[n,k]_Q$-code with the minimum Hamming distance d between code words. An $[n,k,d]_Q$-code is an MDS-*code* if $d = n-k+1$ ($d \leqslant n-k+1$ is the Singleton bound).

A code K is a *complete k-recursive code* if there exists a function $f : Q^k \to Q$ ($k \leqslant n$) such that K is the set of all words $u(\overline{0,n-1}) = (u(0),\dots,u(n-1))$ satisfying the condition $u(i+k) = f(u(i),\dots,u(i+k-1))$ for $i \in \overline{0,n-k-1}$, where $u(0),\dots,u(k-1)$ are arbitrary elements of Q.

This code is a error-correcting code and is denoted by $K(n,f)$. Any subcode $K_1 \subseteq K$ of a complete k-recursive code is called k-*recursive*.

A complete k-recursive code $K(n,f)$ is called *idempotent* if the function f is idempotent, that is $f(x,x,\dots,x) = x$.

Let $n^r(k,q)$ ($n^{ir}(k,q)$) denote the maximal number n such that there exists a complete k-recursive MDS-code (a complete idempotent k-recursive MDS-code) over an alphabet of q elements.

By Theorem 6 of [7], the equality $n^r(2,q) = q+1$ holds for any primary number (prime power) $q = p^\alpha \geqslant 3$ and by Corollary 4 of [7],

$$n^r(2,q) \geqslant \min\{p_1^{\alpha_1}+1, p_2^{\alpha_2}+1, \dots, p_t^{\alpha_t}+1\}$$

2010 Mathematics Subject Classification: 20N05, 94B60, 05B15

Keywords: quasigroup, S-system of quasigroups, orthogonal operations, balanced incomplete block design, recursively r-differentiable quasigroup, recursive MDS-code

if $q = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ is the canonical decomposition of the number q.

According to Proposition 10 from [7], $n^{ir}(2,q) \geqslant q-1$ for any primary $q \geqslant 3$. By Proposition 11 from [7], $n^{ir}(2,p) \geqslant p$ if p is a prime number.

For binary function f a code $K(n,f)$ the system of check functions has the form $f^{(t)}(x,y) = f(f^{(t-2)}(x,y), f^{(t-1)}(x,y))$ for $t \geqslant 2$, where $f^{(0)}(x,y) = f(x,y)$ and $f^{(1)}(x,y) = f(y, f^{(0)}(x,y))$.

In [7] it is proved that r-differentiable quasigroups correspond to complete recursive codes and various methods of constructions of binary recursively 1-differentiable quasigroups are suggested. Moreover, in [7] it is proved that for any $q \in N$, excepting $1, 2, 6$ and possibly $14, 18, 26, 42$, there exist recursively 1-differentiable quasigroups of order q, that is $n^r(2,q) \geqslant 4$.

A quasigroup operation f is called *recursively r-differentiable* if all its *recursive derivatives* $f^{(1)}, f^{(2)}, \dots, f^{(r)}$ are quasigroups. By Theorem 4 of [7], a quasigroup (Q,f) is recursively r-differentiable if and only if the code $K(r+3,f)$ is an MDS-code. In this case the code words are $(x, y, f^{(0)}(x,y), f^{(1)}(x,y), \dots f^{(r)}(x,y))$, $(x,y) \in Q^2$.

A. Abashin in [1] consider special linear recursive MDS-codes with k=2 or 3. V. Izbash and P. Syrbu in [9] prove that for any k-ary ($k \geqslant 2$) operation f the equality $f^{(r)} = f\theta^r$ holds, where $\theta : Q^k \to Q^k$, $\theta(x_1^k) = (x_2, x_3, \dots, x_k, f(x_1^k))$ for all $(x_1^k) \in Q^k$. (Note that this result for $k = 2$ was announced in [4]). They also establish a connection between recursive differentiability of a binary group and the Fibonacci sequence.

In this article we establish properties of binary recursively r-differentiable quasigroups, introduce the notion of a strongly recursively r-differentiab-le quasigroup, and find such idempotent quasigroups in S-systems of quasigroups. A lower bound of $n_s^{ir}(2,q)$ for complete idempotent strongly 2-recursive MDS-codes with primary q is found and illustrative examples are given.

2. Preliminaries

Let Q be a finite or infinite set, Λ_Q be the set of all binary operations defined on Q. On the set Λ_Q it can be defined the *Mann's right* (*left*) *multiplication* $A \cdot B$ ($A \circ B$) of operations $A, B \in \Lambda_Q$ in the following way:

$$(A \cdot B)(x,y) = A(x, B(x,y)) = A(F,B)(x,y),$$

$$(A \circ B)(x,y) = A(B(x,y), y) = A(B,E)(x,y),$$

where $E(x,y) = y$, $F(x,y) = x$ are the right and the left identity operations.

For any operations $A, B \in \Lambda_Q$ the equality $(A \circ B)^* = A^* \cdot B^*$ holds, where $A^*(x,y) = A(y,x)$ (Lemma 4.5 in [2]).

The set $\Lambda_r(\cdot)$ (the set $\Lambda_l(\circ)$) of all invertible from the right (from the left) operations given on a set Q forms the group $\Lambda_r(\cdot)$ (the group $\Lambda_l(\circ)$) under the right (under the left) multiplication of operations.

The operation E, F are the identity elements of the group $\Lambda_r(\cdot)$ and $\Lambda_l(\circ)$, respectively, and $A^{-1} \cdot A = A \cdot A^{-1} = E$, ${}^{-1}\!A \circ A = A \circ {}^{-1}\!A = F$, where

$$A^{-1}(x,y) = z \Leftrightarrow A(x,z) = y, \quad {}^{-1}\!A(x,y) = z \Leftrightarrow A(z,y) = x.$$

Every pair (A,B) of operations of the set Λ_Q defines a mapping θ of the set Q^2 into Q^2 in the following way:

$$\theta(x,y) = (A(x,y), B(x,y)), \quad x,y \in Q.$$

And conversely, any mapping θ of the set Q^2 into Q^2 uniquely defines the pair of operations $A,B \in \Lambda_Q$: if $\theta(a,b) = (c,d)$, then $c = A(a,b)$, $d = B(a,b)$, and $(A,B) = (C,D)$ if and only if $A = C$, $B = D$.

If θ is a permutation on a set Q^2, then operations A,B defined by θ are *orthogonal* (shortly, $A \perp B$), that is the system of equations $\{A(x,y) = a,\ B(x,y) = b\}$ has a unique solution for any $a,b \in Q$. And conversely, an orthogonal pair of operations, given on a set Q, corresponds to the permutation θ on the set Q^2.

If $A,B,C \in \Lambda_Q$, then the new binary operation D can be defined by the following superposition:

$$D(x,y) = A(B(x,y), C(x,y))$$

or shortly, $D = A(B,C) = A\theta$, where $\theta = (B,C)$, that is $D(x,y) = A\theta(x,y)$.

The identity operations F, E of Λ_Q define the identity permutation $(F,E) = \overline{\varepsilon}$ on Q^2. The equality $(A,B)\theta = (A\theta, B\theta)$ holds [2, 3].

3. Recursively r-differentiable quasigroups

Let (Q,A) be a finite quasigroup given on a set Q. Then, the sequence of operations $A^{(0)}, A^{(1)}, \ldots, A^{(t)}, \ldots$ for A is defined in the following way:

$$A^{(0)}(x,y) = A(x,y), \quad A^{(1)}(x,y) = A(y, A^{(0)}(x,y)),$$
$$A^{(t)}(x,y) = A(A^{(t-2)}(x,y), A^{(t-1)}(x,y))$$

for $t \geqslant 2$. This sequence can be written shortly as:

$$A^{(0)} = A(F,E), \quad A^{(1)} = A(E, A^{(0)}), \quad A^{(t)} = A(A^{(t-2)}, A^{(t-1)}),\ t \geqslant 2.$$

According to [7], the operation $A^{(r)}$ of this sequence is called the *r-th recursive derivative* of a quasigroup (Q,A).

By definition, a quasigroup (Q,A) is *recursively r-differentiable* if all its recursive derivatives $A^{(1)}, A^{(2)}, \ldots, A^{(r)}$ are quasigroup operations. In this case, the system of operations $\Sigma = \{F, E, A, A^{(1)}, A^{(2)}, \ldots, A^{(r)}\}$ is orthogonal (Proposition 7 of [7]).

By Theorem 4 of [7], a quasigroup (Q, A) is recursively r-differentiable if and only if the 2-recursive code $K(r+3, A)$ is an MDS-code.

First we establish some properties of finite binary recursively r-differentiable quasigroups.

Theorem 1. *Let $A^{(i)}$ be the i-th recursive derivative of a quasigroup (Q, A) and $\theta = (E, A)$, then $A^{(i)} = A\theta^i$, $\theta^i = (A^{(i-2)}, A^{(i-1)})$, $\theta^2 \neq (F, E)$.*

Proof. Note that the mapping $\theta = (E, A)$ of Q^2 into Q^2 is a permutation since A is a quasigroup operation. By the definition,

$$A^{(1)}(x, y) = A(y, A(x, y)) = A(E, A)(x, y) = A\theta(x, y),$$
$$A^{(2)} = A(A, A(E, A)) = A(A, A\theta) = A\theta^2,$$

since $(E, A)^2 = (E, A)(E, A) = (A, A(E, A)) = (A, A\theta)$ whence $(E, A)^2 \neq (F, E)$ as $A \neq F$.

Let $A^{(k)} = A\theta^k$ for all k, $1 \leqslant k \leqslant i-1$, then by the induction we have $A^{(i)} = A(A^{(i-2)}, A^{(i-1)}) = A(A\theta^{i-2}, A\theta^{i-1}) = A(A, A\theta)\theta^{i-2} = A\theta^2\theta^{i-2} = A\theta^i$. From these equalities the second equality of the theorem follows.

Note that, in the general case, the equality $A\theta_1 = A\theta_2$, where θ_1, θ_2 are two permutations not necessarily implies $\theta_1 = \theta_2$. □

The result of Theorem 1 for binary quasigroups was announced in [4] and was generalized for k-ary quasigroups in [9].

Let $A^*(x, y) = A(y, x)$, then $A^* = ({}^{-1}(A^{-1}))^{-1} = {}^{-1}(({}^{-1}A)^{-1})$ (see [3]).

Corollary 1. *If $A^{(1)}, A^{(2)}, \ldots, A^{(t)}, \ldots$ are the sequence of the recursive derivatives of a quasigroup (Q, A), then for $i \geqslant 1$ we have*

$$A^{(i)} = (A^{(i-1)} \cdot A^*)^* = (A^{(i-1)})^* \circ A,$$

where $(\cdot)$ and $(\circ)$ are the right and left multiplication of the operations given on the set Q.

Proof. Indeed, by Theorem 1,

$$A^{(i)} = A\theta^i = A^{(i-1)}(E, A) = (A^{(i-1)})^* \circ A = (A^{(i-1)} \cdot A^*)^*,$$

since $A(E, B) = A^* \circ B$ and $(A \circ B)^* = A^* \cdot B^*$. □

Proposition 1. *Let a quasigroup (Q, A) be recursively r-differentiable. Then,*

$A^{(i)} \perp {}^{-1}(A^{-1})$ for any $i = 0, 1, 2, \ldots, r-1$, $r \geqslant 1$.

If $A^{(r+1)} = F$, $r \geqslant 0$, then $A^{(r)} = {}^{-1}(A^{-1})$ and $A^{(r+2)} = E$.

If $A^{(r+2)} = E$, $r \geqslant 0$, then $A^{(r+1)} = F$.

Proof. By the criterion of orthogonality of two quasigroups (cf. [2]), $A \perp B$ if and only if $A \cdot B^{-1}$ is a quasigroup operation. But by Corollary 1, the operations $A^{(i+1)} = (A^{(i)} \cdot A^*)^*$ by $i \geqslant 0$ are quasigroup operations, and therefore the operation $(A^{(i+1)})^* = A^{(i)} \cdot A^*$ is a quasigroup operation. Taking into account that $A^* = ({}^{-1}(A^{-1}))^{-1}$, we have $A^{(i)} \perp {}^{-1}(A^{-1})$ for any $i = 0, 1, 2, \dots, r-1$.

Let $A^{(r+1)} = F$, then by Corollary 1, $A^{(r+1)} = (A^{(r)})^* \circ A = F$ for $r \geqslant 0$, so $(A^{(r)})^* = {}^{-1}A$ since $\Lambda_l(\circ)$ is a group with the identity F and the quasigroup ${}^{-1}A$ is inverse for A in this group. Thus, $A^{(r)} = {}^{-1}(A^{-1})$. In this case we have $A^{(r+2)} = A(A^{(r)}, A^{(r+1)}) = A(A^{(r)}, F) = A^*(F, A^{(r)}) = A^* \cdot A^{(r)} = A^* \cdot {}^{-1}(A^{-1}) = E$ because $A^* = ({}^{-1}(A^{-1}))^{-1}$, $\Lambda_r(\cdot)$ is a group with the identity E and A^* is the inverse quasigroup for ${}^{-1}(A^{-1})$ in this group.

Let $A^{(r+2)} = E$, $r \geqslant 0$, then $(A^{(r+2)})^* = F$ and according to Corollary 1, $A^{(r+3)} = (A^{(r+2)})^* \circ A = F \circ A = A$ since $\Lambda_l(\circ)$ is a group with the identity F. But then

$$A^{(r+3)} = A(A^{(r+1)}, A^{(r+2)})) = A(A^{(r+1)}, E) = A \circ A^{(r+1)} = A$$

and so $A^{(r+1)} = F$. □

Definition 1. A quasigroup (Q, A) is called *strongly recursively r-differentiable* if it is r-differentiable and $A^{(r+1)} = F$ (or $A^{(r+2)} = E$). A quasigroup (Q, A) is *strongly recursively 0-differentiable* if $A^{(1)} = F$.

Note that a quasigroup not always is strongly recursively 0-differentiable, although any quasigroup is recursively 0-differentiable. In contrast to recursively r-differentiable quasigroups, a strongly recursively r-differentiable quasigroup is not strongly recursively r_1-differentiable if $r_1 < r$.

Recall that a quasigroup (Q, A) is called *semisymmetric* if in (Q, A) the identity $A(x, A(y, x)) = y$ holds.

Corollary 2. *Let (Q, A) be a strongly recursively r-differentiable quasigroup, then $A^{(r)} = {}^{-1}(A^{-1})$, $A^{(r+2)} = E$ for any $r \geqslant 0$. A quasigroup (Q, A) is strongly recursively 0-differentiable (1-differentiable) if and only if it is semisymmetric ($A^{(1)} = {}^{-1}(A^{-1})$ respectively).*

Proof. The first statement follows from Proposition 1. It is easy to see that a quasigroup (Q, A) is semisymmetric if and only if $A^* = A^{-1}$ (or $A = {}^{-1}(A^{-1})$), so for a semisymmetric quasigroup $A^{(1)} = A^* \circ {}^{-1}(A^{-1}) = A^{-1} \circ {}^{-1}(A^{-1}) = F$. If $A^{(1)} = F$, then by Proposition 1, $A = A^{(0)} = {}^{-1}(A^{-1})$, that is (Q, A) is semisymmetric.

Let $A^{(1)} = {}^{-1}(A^{-1})$, then $A^{(2)} = (A^{(1)})^* \circ A = ({}^{-1}(A^{-1}))^* \circ A = {}^{-1}A \circ A = F$. If $A^{(2)} = F$, then, by Proposition 1, $A^{(1)} = {}^{-1}(A^{-1})$. □

Proposition 2. *A recursively r-differentiable quasigroup (Q, A) is strongly recursively r-differentiable if and only if the permutation $\theta = (E, A)$ has order $r + 3$.*

Proof. Let the permutation $\theta = (E, A)$ have order $r + 3$, that is $\theta^{r+3} = (F, E)$, then by Theorem 1, $(A^{(r+1)}, A^{(r+2)}) = (F, E)$ and so $A^{(r+1)} = F$.

Conversely, suppose that a quasigroup (Q, A) is strongly recursively r-differentiable, then r is the least number such that $A^{(r+1)} = F$. By Proposition 1, $A^{(r+2)} = E$, so $\theta^{r+3} = (A^{(r+1)}, A^{(r+2)}) = (F, E)$. □

Proposition 3. *The direct product of strongly recursively r-differentiable quasigroups is a strongly recursively r-differentiable quasigroup.*

Proof. Suppose that (Q, A) and (P, B), $|Q| = q_1$, $|P| = q_2$, are strongly recursively r-differentiable quasigroups. Then, the direct product $A \times B$ of these quasigroups is an r-differentiable quasigroup since

$$(A \times B)^{(i)} = A^{(i)} \times B^{(i)},\ i \in N$$

(see the proof of Proposition 9 of [7]). Furthermore, from $A^{(r+1)} = F_Q$ and $B^{(r+1)} = F_P$ it follows that $(A \times B)^{(r+1)} = A^{(r+1)} \times B^{(r+1)} = F_Q \times F_P$. But $F_Q \times F_P$ is the left identity operation under the left multiplication of operations given on the set $Q \times P$, so by the definition, the operation $A \times B$ given on the set $Q \times P$ is a strongly recursively r-differentiable quasigroup of order $q_1 q_2$. □

4. Strongly recursively r-differentiable quasigroups

In the theory of binary quasigroups the notion of a Stein system (shortly, an S-system) is known. This system can be defined in the following way [2].

Definition 2. [2] A system $Q(\Sigma)$ of operations given on a finite set Q is called an *S-system* if

1) Σ contains the operation F, E, the rest operations are quasigroup operations;
2) if $A, B \in \Sigma'$, where $\Sigma' = \Sigma \backslash F$, then $A \cdot B \in \Sigma'$;
3) if $A \in \Sigma$, then $A^* \in \Sigma$.

In this case, $\Sigma'(\cdot)$, $\Sigma''(\circ)$, where $\Sigma' = \Sigma \backslash F$ and $\Sigma'' = \Sigma \backslash E$, are isomorphic groups.

We recall some necessary information about S-systems. Let s be the number of operations in an S-system $Q(\Sigma)$, n be the order of the set Q. Then, by Theorem 4.3 of [2], the number $s - 1$ divides $n - 1$ and $k = (n-1)/(s-1) \geqslant s$ or $k = 1$.

The number k is called *the index of an S-system* $Q(\Sigma)$. In the case $k = 1$ we say that $Q(\Sigma)$ is a *complete* S-system.

Complete S-systems are described by V. Belousov in [2]. Incomplete S-systems are described by G. Belyavskaya and A. Cheban in [5, 6].

All operations of an S-system $Q(\Sigma)$ are orthogonal and by Theorem 4.2 [2], are idempotent if $s \geqslant 4$, that is $A(x, x) = x$ for all $x \in Q$ and $A \in \Sigma$.

If $Q(\Sigma)$ is an S-system, then according to Theorem 4.1 [2], for any $A, B, C \in \Sigma$ the operation $C(A, B)$:

$$C(A, B)(x, y) = C(A(x, y), B(x, y))$$

belongs to Σ and the set Δ of all mappings $\theta = (B, C)$, where $B, C \in \Sigma$, $B \neq C$, is a group.

Recall that an algebra $(Q, +, \cdot)$ with two operations is called a *near-field* if $(Q, +)$ is an abelian group with the identity 0, $(Q', \cdot)$ is a group, where $Q' = Q \backslash \{0\}$ and the right distributive law: $(x + y)z = xz + yz$ holds [10].

By Theorem 4.6 of [2], any complete S-system $Q(\Sigma)$ is a system over some near-field $Q(+, \cdot)$, that is any its operation has the form

$$A_a(x, y) = a(y - x) + x$$

for a fixed element $a \in Q$.

Thus, for a complete S-system $Q(\Sigma)$ containing s quasigroups of order q we have $s = q = p^\alpha$ for some primary number since any near-field has such order, and for any prime power there exists a near-field of this order [10]. If a near-field is a field, then the quasigroups are linear over the group $(Q, +)$ and have the form

$$A_a(x, y) = (1 - a)x + ay.$$

All S-systems that are not complete are described in the article [5] by means of near-fields (by means of complete S-systems) and balanced incomplete block designs $BIB(v, b, r, k, 1)$.

A *balanced incomplete block design* $BIB(v, b, r, k, 1)$ is an arrangement of v elements by b blocks such that

every block contains exactly k different elements;
every element appears in exactly r different blocks;
every pair of different elements appears in exactly one block.

The parameters r and k of a $BIB(v, b, r, k, 1)$ define the number v and b [11].

By Theorem 1 of [5], an S-system with operations of order q, of index k containing s operations exists if and only if there exists a $BIB(q, b, , k, p^\alpha, 1)$ with a prime p. In this case,

$$q = ks - k + 1, \quad b = ((ks - k + 1)/s)k, \quad s = p^\alpha.$$

Below S-systems will be used to finding of strongly recursively r-differentiable idempotent quasigroups. Since we consider only recursively r-differentiable quasigroups sometimes the word "recursively" will be omitted.

Theorem 2. *A quasigroup (Q, A) of an S-system $Q(\Sigma)$ is (strongly) recursively r-differentiable if and only if r is the least number such that $A^{(r+1)} = F$ (the permutation $\theta = (E, A)$ has order $r + 3$).*

Proof. If a quasigroup (Q, A) of an S-system $Q(\Sigma)$ is strongly r-differentiable, then by the definition, $A^{(r+1)} = F$ and $A^{(1)}, A^{(2)}, \ldots, A^{(r)}$ are quasigroups.

For the proof of the converse statement we first note that from the properties of S-systems $Q(\Sigma)$ pointed above it follows that all recursive derivatives of any quasigroup (Q, A), where $A \in \Sigma$, are in Σ. So, they can be quasigroup operations or the identity operations F, E.

Let a quasigroup operation A be in Σ, r be the least number such that $A^{(r+1)} = F$, then the recursive derivatives $A^{(i)}$, $1 \leqslant i \leqslant r$, of A either all are quasigroup operations or $A^{(i_0)} = E$ for some $i_0 \leqslant r$, and all operations $A^{(i)}$, $i < i_0$, are quasigroup operations.

In the first case, A is a strongly r-differentiable quasigroup. In the second case, the quasigroup A is $(i_0 - 1)$-differentiable. On the other hand, by Proposition 1, we have $A^{(i_0-1)} = F$ since $A^{(i_0)} = E$. But $A^{(i_0-1)}$ is a quasigroup, that is we obtain the contradiction.

Let the permutation $\theta = (E, A)$ have order $r+3$, then $\theta^{(r+3)} = (A^{(r+1)}, A^{(r+2)}) = (F, E)$ whence $A^{(r+1)} = F$, $A^{(r+2)} = E$, moreover, this number r is the least one with such property. In this case, as has been shown above, the quasigroup (Q, A) is strongly r-differentiable. The converse follows from Proposition 2. □

Theorem 3. *Let $Q(\Sigma)$ be an S-system containing $p^\alpha \geqslant 3$ operations, A be a quasigroup operation of Σ, and the permutations $\theta_A = (E, A)$ have order $r+3$ for some $r \geqslant 0$. Then*

$$(r+3) \mid p^\alpha(p^\alpha - 1).$$

Proof. Let $\Sigma = \{F, E, A_1, A_2, \dots A_{s-2}\}$ be an S-system containing $s = p^\alpha$ operations of order $q = p^\alpha$ if the system Σ is complete, and of order $q = ks - k + 1$ if Σ is an S-system of index k.

By Theorem 4.1 of [2], the set $\triangle$ of all mappings $\theta = (B, C)$, $B, C \in \Sigma$, $B \neq C$, of any S-system is a group. The order of the group $\triangle$ is $s(s-1) = p^\alpha(p^\alpha - 1)$.

The permutation $\theta_A = (E, A) \in \triangle$ for any operation A of Σ, $A \neq E$.

If for $A \in \Sigma$ the permutation θ_A has order $r+3$, then $\theta_A^{r+3} = (F, E)$. Thus $(r+3) \mid p^\alpha(p^\alpha - 1)$. □

Theorem 4. *Let $p^\alpha \geqslant 5$ be an odd prime power, $Q(\Sigma)$ be an S-system containing p^α operations. Then in Σ there exists a quasigroup operation A such that the permutation $\theta_A = (E, A)$ has order $r+3$ for some $r+3 = p^{\alpha_1}$, $\alpha_1 \leqslant \alpha$, and A is a strongly recursively idempotent r-differentiable quasigroup operation of order $q = p^\alpha$. If there exists a $BIB(q, b, k, p^\alpha, 1)$, then A has order $q = kp^\alpha - k + 1$.*

Proof. Let $p^\alpha \geqslant 5$ be an odd prime power, $Q(\Sigma)$ be an S-system containing $s = p^\alpha$ operations. Then by Theorem 4.1 of [2] the set $\triangle$ of all mappings $\theta = (B, C)$, $B, C \in \Sigma$, $B \neq C$ is a group. Moreover, from the proof of Theorem 4.6 in [2] it follows that this group is twice transitive on Σ and contains a strongly transitive on Σ invariant abelian subgroup $\triangle_0$. It is obvious that the group $\triangle_0$ has order $s = p^\alpha$.

Let $\overline{\theta}_C$ be the permutation of $\triangle_0$ such that $F\overline{\theta}_C = C$. Then $F\overline{\theta}_E = E$ and $\overline{\theta}_E = (E, A) = \theta_A$ for a unique operation A of Σ. Moreover, $A \neq F$. Indeed, if $A = F$, then $\overline{\theta}_E^2 = (E, F)(E, F) = (F, E)$, so $p^\alpha = 2^\alpha$ and the subgroup $\triangle_0$ has even order.

Suppose that the permutation $\overline{\theta}_E$ has order $r+3$. Then $r+3=p^{\alpha_1}$ for $\alpha_1 \leqslant \alpha$ since $(r+3) \mid p^\alpha$. Hence, $\overline{\theta}_E^{r+3}=\theta_A^{r+3}=(F,E)$. By Theorem 2, (Q,A) is strongly r-differentiable quasigroup of order $q=p^\alpha$ if the S-system $Q(\Sigma)$ is complete, and has order $q=kp^\alpha-k+1$ if it is incomplete with index k. Recall that by Theorem 4.2 of [2] any operation of an S-system is idempotent if $s \geqslant 4$.

According to Corollary 2, $A^r={}^{-1}(A^{-1})$, $A^{(r+1)}=F$, $A^{(r+2)}=E$. Thus, we have the subsystem

$\Sigma_1=\{A, A^{(1)}, A^{(2)}, \dots, A^{(r)}={}^{-1}(A^{-1}), A^{(r+1)}=F, A^{(r+2)}=E\} \subset \Sigma$
for $r=p^{\alpha_1}-3$. □

Corollary 3. *For any prime p, $p \geqslant 5$, there exists a strongly recursively $(p-3)$-differentiable idempotent quasigroup of order $q=p$ (of order $q=kp-k+1$ if there exists a $BIB(q,b,k,p,1)$).*

Proof. In this case the subgroup $\triangle_0$ of the group $\triangle$ of an S-system has odd order p, that is, $\triangle_0$ is a cyclic group and so the permutation $\overline{\theta}_E=(E,A)$ of $\triangle_0$ has order p. Now the statements of the corollary follow from Theorem 4 by $q=p$. □

Proposition 4. *For any prime power p^α, $p \geqslant 5$, there exists a strongly recursively idempotent $(p-3)$-differentiable quasigroup of order $q=p^\alpha$ (respectively, of order $q=(kp-k+1)^\alpha$ if there exists a $BIB(q,b,k,p,1)$).*

Proof. By Corollary 3 there exists a strongly $(p-3)$-differentiable quasigroup of order p. Using Proposition 3 and taking the direct product of α copies of this quasigroup, we get a strongly $(p-3)$-differentiable idempotent quasigroup of order p^α. It is obvious that the direct product of idempotent quasigroups is an idempotent quasigroup. □

Remark. Note that the direct product of two strongly recursively r-differentiable idempotent quasigroups of order $p_1^{\alpha_1}$ and $p_2^{\alpha_2}$, $p_1 \neq p_2$, over near-fields of the respective orders already is not a quasigroup over some near-field since has order $p_1^{\alpha_1}p_2^{\alpha_2}$ which is not a prime power.

Corollary 4. *There exist strongly recursively 2-differentiable idempotent quasigroups of order $q=21,25,41,45,61$; strongly recursively 4-differentiable idempotent quasigroups of order $q=49,91$ and strongly recursively 8-differentiable idempotent quasigroups of order $q=121$.*

Proof. These statements follow from Corollary 3 and the existence of the following designs:

$BIB(21,21,5,5,1)$ (N7), $BIB(25,30,6,5,1)$ (N11),

$BIB(41,82,10,5,1)$ (N42), $BIB(45,99,11,5,1)$ (N51),

$BIB(61,183,15,5,1)$ (N108) (for these designs we have $(2=5-3)$-differentiable idempotent quasigroups of order $q=21,25,41,45,61$ respectively.

The designs $BIB(49,56,8,7,1)$ (N24) and $BIB(91,195,15,7,1)$ (N111) give a strongly $(4=7-3)$-differentiable idempotent quasigroups of order $q=49,91$.

The design $BIB(121, 132, 12, 11, 1)$ (N68) corresponds to a strongly ($8 = 11–3$) -differentiable idempotent quasigroup of order $q = 121$.

All these BIB-designs exist (near with each design we point its number in Table of Application I of [11]. □

Definition 3. An MDS-code $K(n, A)$ is said to be *strongly recursive* if the quasigroup (Q, A) is strongly recursively $(n - 3)$-differentiable.

Corollary 5. *For any prime power p^α, $p \geqslant 5$, there exists an idempotent strongly 2-recursive code $K(p, A)$, where A is a quasigroup of order p^α.*

Proof. By Theorem 4 of [7], a quasigroup A is r-differentiable if and only if the code $K(r + 3, A)$ is an MDS-code. Next use Corollary 3 for $r = p - 3$ and Proposition 4. □

Denote by $K_s^i(n, A)$ the idempotent strongly 2-recursive MDS-code corresponding to a quasigroup (Q, A) and let $n_s^{ir}(2, q)$ denote the maximal number n such that there exists a (complete) idempotent strongly 2-recursive MDS-code $K_s^i(n, A)$ over an alphabet of q elements.

From Corollary 5 it follows

Corollary 6. *$n_s^{ir}(2, p^\alpha) \geqslant p$ for any prime p, $p \geqslant 5$ and $\alpha \in N$.* □

Corollary 7. *If there exist strongly recursively r-differentiable quasigroups of order q_1 and q_2, then*

$$n_s^{ir}(2, q_1 q_2) \geqslant r + 3.$$

Proof. That follows from Proposition 3 and Theorem 4 of [7]. □

Below, we give some illustrative examples of strongly recursively r-differentiable idempotent quasigroups over fields.

Example 1. Consider the following quasigroup operation A_2 of the S-system of quasigroups over the field $GF(5)$: $A_2(x, y) = 2(y - x) + x = 4x + 2y$. The recursive derivatives of this quasigroup are:

$A_2^{(1)}(x, y) = A_2(y, A_2(x, y)) = 4y + 2(4x + 2y) = 3x + 3y$;
$A_2^{(2)}(x, y) = A_2(A_2(x, y), A_2^{(1)}(x, y)) = 4(4x + 2y) + 2(3x + 3y) = 2x + 4y$;
$A_2^{(3)}(x, y) = A_2(A_2^{(1)}(x, y), A_2^{(2)})(x, y) = 4(3x + 3y) + 2(2x + 4y) = x$.

Hence, A_2 is a strongly 2-differentiable quasigroup operation of the S-system over the field $GF(5)$, and the orthogonal system $\Sigma = \{F, E, A_2, A_2^{(1)}, A_2^{(2)}\}$ corresponds to the code $K_s^i(5, A_2)$.

Example 2. Consider the quasigroup operation of the same form over the field $GF(7)$:

$A_2(x, y) = 2(y - x) + x = 6x + 2y$; $A_2^{(1)}(x, y) = 5x + 3y$; $A_2^{(2)}(x, y) = 4x + 4y$;
$A_2^{(3)}(x, y) = 3x + 5y$; $A_2^{(4)}(x, y) = 2x + 6y$; $A_2^{(5)}(x, y) = x$.

Thus, this quasigroup is strongly $(7-3=4)$-differentiable. The orthogonal system $\Sigma = \{F, E, A_2, A_2^{(1)}, A_2^{(2)}, A_2^{(3)}, A_2^{(4)}\}$ corresponds to the code $K_s^i(7, A_2)$.

Note that for a quasigroup operation A over $GF(7)$ the group Δ (see the proof of Theorem 3) has order $7 \cdot 6$, so a permutation $\theta = (E, A)$ for $A \in \Sigma$ can have only order 3 or 7 ($(E, A)^2 \neq (F, E)$ if A is a quasigroup operation).

For the quasigroup operation $A_3(x, y) = 3(y-x)+x = 5x+3y$ over $GF(7)$ the permutation $\theta = (E, A_3)$ has order 3 since $A_3^{(1)}(x, y) = A_3(y, A_3(x, y)) = 5y + 3(5x+3y) = x$. In this case, the quasigroup operation A_3 is strongly 0-differential, $\theta \in \Delta \backslash \Delta_0$ since $\mid \Delta_0 \mid = 7$.

The subsystem $\Sigma_1 = \{F, E, A_3\}$ of the complete S-system over $GF(7)$ corresponds to the code $K_s^i(3, A_3)$.

Example 3. Among of quasigroups over the field $GF(11)$ necessarily there are strongly $(11-3=8)$-differentiable quasigroups (by Corollary 3) and a priori can be strongly $(5-3=2)$- or $(10-3=7)$-differentiable quasigroups since the group Δ has order $11 \cdot 10$. Show that all these cases are possible.

The quasigroup operation $A_2(x, y) = 2(y-x)+x = 10x+2y$ is strongly 8-differentiable with the following recursive derivatives:

$A_2^{(1)}(x, y) = 9x+3y$; $A_2^{(2)}(x, y) = 8x+4y$; $A_2^{(3)}(x, y) = 7x+5y$;

$A_2^{(4)}(x, y) = 6x+6y$; $A_2^{(5)}(x, y) = 5x+7y$; $A_2^{(6)}(x, y) = 4x+8y$;

$A_2^{(7)}(x, y) = 3x+9y$; $A_2^{(8)}(x, y) = 2x+10y$; $A_2^{(9)}(x, y) = x$.

The system $\Sigma = \{F, E, A_2, A_2^{(1)}, A_2^{(2)}, \ldots, A_2^{(8)}\}$ corresponds to $K_s^i(11, A_2)$.

The commutative quasigroup operation $A_6(x, y) = 6(y-x)+x = 6x+6y$ over the field $GF(11)$ is strongly 2-differentiable: $A_6^{(1)}(x, y) = 3x+9y$; $A_6^{(2)}(x, y) = 10x+2y$; $A_6^{(3)}(x, y) = x$, corresponds to the subsystem $\Sigma_1 = \{F, E, A_6, A_6^{(1)}, A_6^{(2)}\}$ and to the code $K_s^i(5, A_6)$. The permutation $\theta = (E, A_6)$ has order 5 and is in the subset $\Delta \backslash \Delta_0$.

Finally, consider the quasigroup operation $A_9(x, y) = 9(y-x)+x = 3x+9y$ over $GF(11)$:

$A_9^{(1)}(x, y) = 5x+7y$; $A_9^{(2)}(x, y) = 10x+2y$; $A_9^{(3)}(x, y) = 6x+6y$;

$A_9^{(4)}(x, y) = 7x+5y$; $A_9^{(5)}(x, y) = 4x+8y$; $A_9^{(6)}(x, y) = 2x+10y$;

$A_9^{(7)}(x, y) = 8x+4y$; $A_9^{(8)}(x, y) = x$.

Thus, the quasigroup operation A_9 is strongly 7-differentiable and corresponds to the subsystem Σ_1 of 10 (from 11) operations and to the code $K_s^i(10, A_9)$.

Note that the direct product of the strongly 2-differentiable quasigroups $A_2 = 4x+2y$ over $GF(5)$ (Example 1) and $A_6(x, y) = 6x+6y$ over the field $GF(11)$ (Example 3) is a strongly 2-differentiable quasigroup of order 55 and corresponds to the code $K_s^i(5, A_2 \times A_6)$ by Proposition 3 and Theorem 4 of [7].

References

[1] **A.S. Abashin**, *Linear recursive MDS-codes of dimention* 2 *and* 3, (Russian), Discret. Mat. **12** (1998), 140 – 153.

[2] **V.D. Belousov**, *Systems of quasigroups with generalized identities*, (Russian), Uspehi Matem. Nauk **20(121)** (1965), 75 – 146.

[3] **V.D. Belousov**, *Systems of orthogonal operations*, (Russian), Mat. Sbornik **77(119)** (1968), 38 – 58.

[4] **G.B. Belyavskaya**, *On r-differentiable quasigroups*, Abstracts Int. Conf. Pure Applied Math., Kiev 2002, 11 – 12.

[5] **G.B. Belyavskaya and A.M. Cheban**, *S-systems of arbitrary index, I*, (Russian), Mat. Issled. **7** (1972), vyp.1, 27 – 43.

[6] **G.B. Belyavskaya and A.M. Cheban**, *S-systems of arbitrary index, II*, Mat. Issled. **7** (1972), vyp.2, 3 – 13.

[7] **E. Couselo, S. Gonsalez, V. Markov and A. Nechaev**, *Recursive MDS-codes and recursive differentiable quasigroup*, Discrete Math. Appl. **8** (1998), 217 – 245.

[8] **E. Couselo, S. Gonzzlez, V. Markov and A. Nechaev**, *Parameters of recursive MDS-codes*, Discrete Math. Appl. **10** (2000), 443 – 453.

[9] **V.I. Izbash and P. Syrbu**. *Recursively differentiable quasigroups and complete recursive codes*, Comm. Math. Univ. Carolinae **45** (2004), 257 – 263.

[10] **M. Hall**, *The theory of groups*, The Macmillian Company, New York, 1959.

[11] **M. Hall**, *Combinatorial Theory*, Blaisdell Publishing Company, Toronto-London, 1967.

Received March 1, 2012

Institute of Mathematics and Computer Science Academy of Sciences of Moldova
str. Academiei 5, MD-2028 Chisinau, Moldova
E-mail: gbel1@rambler.ru

Quasigroups and Related Systems **20** (2012), 169 – 176

A characterization of binary invertible algebras of various types of linearity

Sergey S. Davidov

Abstract. In this paper we define the left (right) linear over a group binary invertible algebras and invertible algebras of mixed type of linearity and characterize the classes of such algebras by the second-order formula, namely by the $\forall\exists(\forall)-$ identities.

1. Introduction

Linear quasigroups introduced by V.D. Belousov in 1967 in connection with an investigation of balanced identities in quasigroups [2] play a special role in the study of quasigroups isotopic to groups [5, 4, 6, 10, 11].

A binary algebra $(Q;\Sigma)$ is called *invertible*, if $(Q;A)$ is a quasigroup for any operation $A\in\Sigma$.

Below we introduce the notions of left (right) linear invertible algebras and invertible algebras of mixed type of linearity and characterize the classes of such algebras by the second order formulae, namely by the $\forall\exists(\forall)-$ identities.

For details about $\forall\exists(\forall)-$ identities see [9, 12].

2. Left and right linear invertible algebras

We denote by $L_{A,a}$ and $R_{A,a}$ the left and right translations of the binary algebra $(Q;\Sigma)$: $L_{A,a}$: $x\mapsto A(a,x)$, $R_{A,a}: x\mapsto A(x,a)$. If the algebra $(Q;\Sigma)$ is an invertible algebra then the translations $L_{A,a}$ and $R_{A,a}$ are bijections for all $a\in Q$ and all $A\in\Sigma$.

It is well known (see [2]) that the quasigroups A^{-1}, ${}^{-1}A$, ${}^{-1}\big(A^{-1}\big)$, $\big({}^{-1}A\big)^{-1}$, A^{*}, where $A^{*}(x,y)=A(y,x)$, are associated with the quasigroup A.

Similarly, the invertible algebras:

$$\big(Q;\Sigma^{-1}\big)\,,\ \big(Q;{}^{-1}\Sigma\big)\,,\ \big(Q;{}^{-1}(\Sigma^{-1})\big)\,,\ \big(Q;({}^{-1}\Sigma)^{-1}\big)\,,\ \big(Q;\Sigma^{*}\big)\,,$$

where

$$\Sigma^{-1}=\{A^{-1}|\ A\in\Sigma\},\ \ {}^{-1}\Sigma=\{\,{}^{-1}A|\ A\in\Sigma\},\ \ {}^{-1}(\Sigma^{-1})=\{\,{}^{-1}(A^{-1})|\ A\in\Sigma\},$$

2010 Mathematics Subject Classification: 20N05
Keywords: quasigroup, invertible algebra, linear algebra, second-order formula.

$$({}^{-1}\Sigma)^{-1} = \{({}^{-1}A)^{-1} |\ A \in \Sigma\}, \quad \Sigma^{*} = \{A^{*} |\ A \in \Sigma\}$$

are associated with the invertible algebra (Q, Σ). Each of these algebras is called the *parastrophy* of the algebra $(Q; \Sigma)$.

Definition 2.1. An invertible algebra $(Q; \Sigma)$ is called *left* (*right*) *linear over a group* $(Q; +)$, if every operation $A \in \Sigma$ has the form:

$$A(x, y) = \varphi_A x + \beta_A y \quad (A(x, y) = \alpha_A x + \psi_A y)\,,$$

where β_A (respectively α_A) is a permutation of the set Q, and φ_A (respectively ψ_A) is an automorphism of the group $(Q; +)$.

An invertible algebra is called *left* (*right*) *linear* if it is left (right) linear over some group $(Q; +)$.

Theorem 2.2. *A binary invertible algebra* $(Q; \Sigma)$ *is left linear if and only if for all* $X, Y \in \Sigma$ *the following formula*

$$X\left(Y\left(x, Y^{-1}(u, y)\right), z\right) = X\left(Y\left(x, Y^{-1}(u, u)\right), X^{-1}\left(u, X(y, z)\right)\right) \tag{1}$$

is valid in the algebra $(Q; \Sigma \cup \Sigma^{-1})$.

Proof. Let $(Q; \Sigma)$ be an invertible left linear algebra. Then for every $X \in \Sigma$ we have

$$X\,(x, y) = \varphi_X x + \beta_X y, \tag{2}$$

where $\varphi_X \in Aut(Q; +)$ and $\beta_X \in S_Q$. We prove that equality (1) is valid in the algebra $(Q; \Sigma \cup \Sigma^{-1})$ for all $X, Y \in \Sigma$.

Observe that from (2) we obtain

$$X^{-1}(x, y) = \beta_X^{-1}\left(-\varphi_X x + y\right). \tag{3}$$

Thus, according to (2) and (3) we get:

$$\begin{aligned} X(Y(x, Y^{-1}(u, y)), z) &= \varphi_X(\varphi_Y x + \beta_Y Y^{-1}(u, y)) + \beta_X z \\ &= \varphi_X(\varphi_Y x + \beta_Y \beta_Y^{-1}(-\varphi_Y u + y)) + \beta_X z \\ &= \varphi_X \varphi_Y x - \varphi_X \varphi_Y u + \varphi_X y + \beta_X z, \end{aligned}$$

$$\begin{aligned} X(Y(x,Y^{-1}(u, u)),X^{-1}(u,X(y, z))) &= \varphi_X Y(x, Y^{-1}(u, u)) + \beta_X X^{-1}(u, X(y, z)) \\ &= \varphi_X(\varphi_Y x - \varphi_Y u + u) - \varphi_X u + \varphi_X y + \beta_X z \\ &= \varphi_X \varphi_Y x - \varphi_X \varphi_Y u + \varphi_X u - \varphi_X u + \varphi_X y + \beta_X z \\ &= \varphi_X \varphi_Y x - \varphi_X \varphi_Y u + \varphi_X y + \beta_X z. \end{aligned}$$

Hence, the right and left sides of (1) are the same.

Conversely, let (1) holds in $(Q;\Sigma\cup\Sigma^{-1})$ for all $X,Y\in\Sigma$. Then for $u=p$ and $X=A$, $Y=B$, where $A,B\in\Sigma$, we have

$$A(B(x,B^{-1}(p,y)),z)=A(B(x,B^{-1}(p,p)),A^{-1}(p,A(y,z))).$$

From this, by putting $A_1(x,y)=A(x,y)$, $A_2(x,y)=B(x,B^{-1}(p,y))$, $A_3(x,y)=A(B(x,B^{-1}(p,p)),y)$ and $A_4(x,y)=A^{-1}(p,A(x,y))$ we obtain

$$A_1(A_2(x,y),z)=A_3(x,A_4(y,z)),$$

which by Belousov‘s theorem on four quasigroups (see [3]) shows that operations A_1,A_2,A_3,A_4 are isotopic to the same group $(Q;*)$. Hence, the operations A and B are also isotopic to $(Q;*)$. Since the operations A and B are arbitrary, we obtain that all operations from Σ are isotopic to this group.

For every $X\in\Sigma$, let us define the operation:

$$x\underset{X}{+}y=X(R^{-1}_{X,a}x,L^{-1}_{X,b}y),\tag{4}$$

where a,b are some fixed elements from Q. The operation $\underset{X}{+}$ is a loop operation with the identity element $0_X=X(b,a)$. Obviously, $(Q;\underset{X}{+})$ is a loop isotopic to the group $(Q;*)$. Hence, by Albert‘s theorem, it is a group. Hence every $X\in\Sigma$ each $(Q;\underset{X}{+})$ is a group. So, (1) (where $X=A$, $Y=B$) can be rewritten in the form:

$$A(B(x,L_{B^{-1},u}y),z)=A(R_{B,B^{-1}(u,u)}x,L_{A^{-1},u}A(y,z)),$$

$$R_{A,a}(R_{B,a}x\underset{B}{+}L_{B,b}L_{B^{-1},u}y)\underset{A}{+}L_{A,b}z=R_{A,a}R_{B,B^{-1}(u,u)}x\underset{A}{+}L_{A,b}L_{A^{-1},u}(R_{A,a}y\underset{A}{+}L_{A,b}z).$$

Taking $z=L^{-1}_{A,b}0_A$ in the last equality, we have

$$R_{A,a}(R_{B,a}x\underset{B}{+}L_{B,b}L_{B^{-1},u}y)=R_{A,a}R_{B,B^{-1}(u,u)}x\underset{A}{+}L_{A,b}L_{A^{-1},u}R_{A,a}y,$$

$$R_{A,a}(x\underset{B}{+}y)=\alpha_{A,B}x\underset{A}{+}\beta_{A,B}y,\tag{5}$$

where $\alpha_{A,B}=R_{A,a}R_{B,B^{-1}(u,u)}R^{-1}_{B,a}$, $\beta_{A,B}=L_{A,b}L_{A^{-1},u}R_{A,a}L^{-1}_{B^{-1},u}L^{-1}_{B,b}$ are permutations of the set Q. Since the operations A and B are arbitrary we can take $A=B$ in (5). Hence

$$R_{A,a}(x\underset{A}{+}y)=\alpha_{A,A}x\underset{A}{+}\beta_{A,A}y.\tag{6}$$

From (5) and (6) we have

$$\alpha^{-1}_{A,B}x\underset{B}{+}\beta^{-1}_{A,B}y=\alpha^{-1}_{A,A}x\underset{A}{+}\beta^{-1}_{A,A}y,$$

$$x\underset{A}{+}y=\gamma_{A,B}x\underset{B}{+}\delta_{A,B}y,\tag{7}$$

where $\gamma_{A,B} = \alpha^{-1}_{A,B}\alpha_{A,A}$ and $\delta_{A,B} = \beta^{-1}_{A,B}\beta_{A,A}$ are permutations of the set Q. Hence, according to (7), we get

$$R_{A,a}(x \underset{B}{+} y) = \gamma_{A,B}\alpha_{A,B}x \underset{B}{+} \delta_{A,B}\beta_{A,B}y,$$

i.e., $R_{A,a}$ is a quasiautomorphism of the group $(Q; \underset{B}{+})$. Since A is arbitrary we have that $R_{A,a}$ is a quasiautomorfism of the group $(Q; \underset{B}{+})$ for all operations $A \in \Sigma$.

According to (4) we have

$$A(x, y) = R_{A,a}x \underset{A}{+} L_{A,b}y.$$

This, according to (7), gives:

$$A(x, y) = \theta^1_{A,B}x \underset{B}{+} \theta^2_{A,B}y, \tag{8}$$

where $\theta^1_{A,B} = \gamma_{A,B}R_{A,a}$ and $\theta^2_{A,B} = \delta_{A,B}L_{A,b}$ are permutations of the set Q. Thus, we can represent every operation from Σ by the operation $\underset{B}{+}$.

Let $+ = \underset{B}{+}$. We prove that $\theta^1_{A,B}$ is a quasiautomorphism of the group $(Q; +)$. To do it we take $z = (\theta^2_{A,B})^{-1}0_B,\ X = A,\ Y = B$ in (1) and rewrite this equality in the form:

$$\theta^1_{A,B}(R_{B,a}x+L_{B,b}L_{B^{-1},u}y)+\theta^2_{A,B}z= \theta^1_{A,B}R_{B,B^{-1}(u,u)}x+\theta^2_{A,B}L_{A^{-1},u}(\theta^1_{A,B}y+\theta^2_{A,B}z),$$

$$\theta^1_{A,B}(R_{B,a}x + L_{B,b}L_{B^{-1},u}y) = \theta^1_{A,B}R_{B,B^{-1}(u,u)}x + \theta^2_{A,B}L_{A^{-1},u}\theta^1_{A,B}y.$$

The last equality shows that $\theta^1_{A,B}$ is a quasiautomorphism of the group $(Q; +)$. According to [2, Lemma 2.5] we have

$$\theta^1_{A,B}x = \varphi_A x + s_A,$$

where φ_A is an automorphism of the group $(Q, +)$ and s_A is some element of the set Q. Hence, it follows from (8) that

$$A(x, y) = \varphi_A x + \beta_A y, \tag{9}$$

where $\beta_A y = s_A + \theta^2_{A,B}y$. Since A is an arbitrary operation we obtain that all operations from Σ can be represented in the form (9), i.e., the algebra $(Q; \Sigma)$ is left linear. □

Similarly, we can prove the following theorem.

Theorem 2.3. *A binary invertible algebra $(Q; \Sigma)$ is a right linear algebra if and only if for all $X, Y \in \Sigma$ the following formula*

$$X(x, Y(^{-1}Y(y, u), z)) = X(^{-1}X(X(x, y), u), Y(^{-1}Y(u, u), z)), \tag{10}$$

is valid in the algebra $(Q; \Sigma \cup {}^{-1}\Sigma)$. □

Proposition 2.4. *A left and right linear invertible algebra is linear.* □

Corollary 2.5. *The class of all invertible linear algebras is characterized by the second order formulaes* (1) *and* (10). □

A linear invertible algebra over an abelian group is called an *invertible T-algebra* (see [7]). The class of medial invertible algebras is a special subclass of invertible T-algebras. An invertible algebra $(Q;\Sigma)$ is called a *left* (*right*) *T-algebra*, briefly a *LT-algebra* (*RT-algebra*) if $(Q;\Sigma)$ is a left (right) linear algebra over an abelian group. It follows from Proposition 2.4, that if an invertible algebra is a LT-algebra and RT-algebra, then it is a T-algebra.

Using the same arguments as in the proof of Theorem 1 from [6] and applying our Theorems 2.2 and 2.3 we obtain

Theorem 2.6. *A binary invertible algebra $(Q;\Sigma)$ is a LT-algebra if and oly if for all $X,Y\in\Sigma$ the following formulaes*

$$X(Y(x,Y^{-1}(u,y)),z)=X(Y(x,Y^{-1}(u,u)),X^{-1}(u,X(y,z))),$$

$$X({}^{-1}X(x,u),X^{-1}(u,y))=X({}^{-1}X(y,u),X^{-1}(u,x)), \tag{11}$$

are valid in the algebra $(Q;\Sigma\cup\Sigma^{-1}\cup{}^{-1}\Sigma)$. □

Theorem 2.7. *A binary invertible algebra $(Q;\Sigma)$ is a RT-algebra if and only if for all $X,Y\in\Sigma$ the following formulaes*

$$X(x,Y({}^{-1}Y(y,u),z))=X({}^{-1}X(X(x,y),u),Y({}^{-1}Y(u,u),z)),$$

$$X({}^{-1}X(x,u),X^{-1}(u,y))=X({}^{-1}X(y,u),X^{-1}(u,x))$$

are valid in the algebra $(Q;\Sigma\cup\Sigma^{-1}\cup{}^{-1}\Sigma)$.

Corollary 2.8. *The class of all invertible T-algebras is characterized by the second order formulaes* (1), (10) *and* (11). □

3. Invertible algebras of mixed type of linearity

Definition 3.1. An invertible algebra $(Q;\Sigma)$ is called an *invertible algebra of mixed type of linearity of the first* (*second*) *kind* over a group $(Q;+)$, if every operation $A\in\Sigma$ has the form

$$A(x,y)=\varphi_Ax+c_A+\overline{\psi}_Ay \quad (A(x,y)=\overline{\varphi}_Ax+c_A+\psi_Ay),$$

where $\varphi_A,\psi_A\in Aut(Q;+)$, $\overline{\psi}_A,\overline{\varphi}_A$ are antiautomorphisms of $(Q;+)$, and c_A is a fixed element from Q.

Theorem 3.2. *An invertible algebra $(Q;\Sigma)$ is of mixed type of linearity of the first kind if and only if for all $X, Y \in \Sigma$ the following second order formulaes*

$$X(Y(x, Y^{-1}(u, y)), z) = X(Y(x, Y^{-1}(u, u)), X^{-1}(u, X(y, z))), \tag{12}$$

$$X(x, {}^{-1}Y(Y(y, Y^{-1}(u, v)), u)) = X({}^{-1}X(X(x, {}^{-1}Y(v, u)), u), y) \tag{13}$$

are valid in the algebra $(Q; \Sigma \cup \Sigma^{-1} \cup {}^{-1}\Sigma)$.

Proof. Let $(Q;\Sigma)$ be an invertible algebra of mixed type of linearity of the first kind, then for every $X \in \Sigma$ we have

$$\begin{aligned} X(x, y) &= \varphi_X x + c_X + \overline{\psi}_X y, \\ {}^{-1}X(x, y) &= \varphi_X^{-1}(x - \overline{\psi}_X y - c_X), \\ X^{-1}(x, y) &= \overline{\psi}_X^{-1}(-c_X - \varphi_X x + y), \end{aligned}$$

where $\varphi_X \in Aut(Q;+)$, $\overline{\psi}_X$ is an antiautomorphism of $(Q;+)$ and $c_X \in Q$.

Using the above identities we can prove that the left and right sides of (12) and (13) are the same.

Conversely, let (12) and (13) be valid in the algebra $(Q; \Sigma \cup \Sigma^{-1} \cup {}^{-1}\Sigma)$ for all $X, Y \in \Sigma$. We prove that an algebra $(Q;\Sigma)$ is an algebra of mixed type of linearity of the first kind.

As in the proof of Theorem 2.2 we can see that from (12) we obtain

$$A(x, y) = \theta^1_{A,B} x + \theta^2_{A,B} y, \tag{14}$$

for any operation $A \in \Sigma$, where $\theta^1_{A,B}$ is a quasiautomorfism of the group $(Q;+)$.

Thus,

$$\theta^1_{A,B} x = \varphi_A x + t_A, \tag{15}$$

where $\varphi_A \in Aut(Q;+)$ and t_A is some element of the set Q [2, Lemma 2.5].

To prove that $\theta^2_{A,B}$ is an antiquasiautomorphism of the group $(Q;+)$ observe that (13) for $X = A$, $Y = B$ and fixed $u \in Q$ gives

$$A(x, R_{^{-1}B,u} B(y, L_{B^{-1},u} v)) = A(R_{^{-1}A,u} A(x, R_{^{-1}B,u} v), y),$$

$$\theta^1_{A,B} x + \theta^2_{A,B} R_{^{-1}B,u}(R_{B,a} y + L_{B,b} L_{B^{-1},u} v) = \theta^1_{A,B} R_{^{-1}A,u}(\theta^1_{A,B} x + \theta^2_{A,B} R_{^{-1}B,u} v) + \theta^2_{A,B} y.$$

Taking $x = (\theta^1_{A,B})^{-1}0$ in the last equality, we obtain

$$\theta^2_{A,B} R_{^{-1}B,u}(y + v) = \theta^1_{A,B} R_{^{-1}A,u} \theta^2_{A,B} R_{^{-1}B,u} L^{-1}_{B^{-1},u} L^{-1}_{B,b} v + \theta^2_{A,B} R^{-1}_{B,a} y.$$

Thus, the triplet

$$(\theta^1_{A,B} R_{^{-1}A,u} \theta^2_{A,B} R_{^{-1}B,u} L^{-1}_{B^{-1},u} L^{-1}_{B,b},\ \theta^2_{A,B} R^{-1}_{B,a},\ \theta^2_{A,B} R_{^{-1}B,u})$$

is an antiautotopy of the group $(Q;+)$. Since any component of an antiautotopy of a group is an antiquasiautomorphism (see [1]), then $\theta^2_{A,B}R^{-1}_{B,a}$ is an antiquasiautomorphism of the group $(Q;+)$. Similarly as in the proof of Theorem 2.2 we can see that $R^{-1}_{B,a}$ is a quasiautomorphism of the group $(Q;+)$. Therefore $\theta^2_{A,B}$ is an antiquasiautomorphism of the group $(Q;+)$.

Thus,

$$\theta^2_{A,B}x = s_A + \overline{\psi}_A x, \tag{16}$$

where $\overline{\psi}_A$ is an antiautomorphism of $(Q;+)$, and s_A is an element of the set Q.

Hence, from (14), (15) and (16) we get

$$A(x,y) = \varphi_A x + c_A + \overline{\psi}_A x, \tag{17}$$

where $c_A = t_A + s_A$. □

Theorem 3.3. *An invertible algebra $(Q;\Sigma)$ is an invertible algebra of mixed type of linearity of the second kind if and only if for all $X,Y\in\Sigma$ the following formulaes*

$$X(x, Y({}^{-1}Y(y,u),z)) = X({}^{-1}X(X(x,y),u), Y({}^{-1}Y(u,u),z)), \tag{18}$$

$$X(Y^{-1}(u, Y({}^{-1}Y(x,u),y)),v) = X(y, X^{-1}(u, X(Y^{-1}(u,x),v))), \tag{19}$$

are valid in the algebra $(Q;\Sigma\cup\Sigma^{-1}\cup{}^{-1}\Sigma)$.

Proof. The proof is similar to the proof of Theorem 3.2. □

Note, that the equalities (1), (10), (11), (12), (13), (18) and (19) are the identities of the second order (in the sense of Yu.M. Movsisyan [11]).

References

[1] **V.D. Belousov**, *Systems of quasigroups with generalised identities*, Uspekhi Mat. Nauk. **20** (1965), 75 – 146.

[2] **V.D. Belousov**, *Balanced identities on quasigroups*, (Russian) Mat. Sb. **70** (1966), 55 – 97.

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

[4] **G.B. Belyavskaya and A.H. Tabarov**, *Nuclei and the centre of linear quasigroups* (Russian), Izvestya AN Repub. Moldova, Matematika **6** (1991), no. 3, 37 – 42.

[5] **G.B. Belyavskaya and A.H. Tabarov**, *Characterizations of linear and alinear quasigroups*, (Russian), Diskretnaya Mat. **4** (1992), 42 – 47.

[6] **G.B. Belyavskaya and A.H. Tabarov**, *One-sided T-quasigroups and irreducible balanced identities*, Quasigroups and Related Systems **1** (1994), 8 – 21.

[7] **S.S. Davidov**, *A characterization of binary invertible algebras linear over a group*, Quasigroups and Related Systems **19** (2011), 207 – 222.

[8] **T. Kepka and P. Nemec**, *T-quasigroups. Part I*, Acta Univ. Carolinae Math. et Phis. **12** (1971), no.1, 39 – 49.

[9] **Yu.M. Movsisyan**, *Biprimitive classes of second order algebras*, (Russian), Mat. Issled. **9** (1974), 70 – 82.

[10] **Yu.M. Movsisyan**, *Hyperidentities and hyprvarieties in algebras*, (Russian), Yerevan State University Press, Yerevan (1990).

[11] **Yu.M. Movsisyan**, *Hyperidenetities and hyprvarieties*, Sci. Math. Japonicae **54** (2001), 595 – 640.

[12] **A.H. Tabarov**, *Homomorphisms and endomorphisms of linear and alinear quasigroups*, Discrete Math. Appl. **17** (2007), 253 – 260.

Received January 27, 2012

Department of Mathematics and Mechanics
Yerevan State University
1 Alex Manoogian
Yerevan 0025
Armenia
e-mail: davidov@ysu.am

Quasigroups and Related Systems **20** (2012), 177 – 182

Generalized IP-loops

Ivan I. Deriyenko

Abstract. Some generalization of the inverse identities for loops are presented and it is proved that loops of order $n < 7$ satisfy one of these generalized identities. Included examples presented method of computation of these identities. Some universal relations between left, right and middle translations are described.

1. Introduction

Let $Q = \{1, 2, \ldots, n\}$ be a finite set, S_n - the set of all permutations of Q. The multiplication (composition) of permutations $\varphi, \psi \in S_n$ is defined as $\varphi\psi(x) = \varphi(\psi(x))$. All permutations will be written in the form of cycles, cycles will be separated by dots, e.g.

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 6 & 1 & 5 & 2 & 3 \end{pmatrix} = (1\,4)(2\,7\,3\,6)(5) = (1\,4.\,2\,7\,3\,6.\,5.).$$

By a *cyclic type* of permutation φ we mean the sequence $\{l_1, l_2, \ldots, l_n\}$, where l_i denotes the number of cycles of the length i. In this case we will write

$$C(\varphi) = \{l_1, l_2, \ldots, l_n\} \quad \text{and} \quad P(\varphi) = \{x_1^{l_1}, x_2^{l_2}, \ldots, x_n^{l_n}\}.$$

For example, forthe above permutation φ we have $C(\varphi) = \{1, 1, 0, 1, 0, 0, 0\}$ and $P(\varphi) = \{x_1^1, x_2^1, x_3^0, x_4^1, x_5^0, x_6^0, x_7^0\}$.

Let $Q(\cdot)$ be a quasigroup with the multiplication denoted by juxtaposition. Then $L_a(x) = a \cdot x$ is called a *left translation*, $R_a(x) = x \cdot a$ is called a *right translation*. By a *middle translation* (shortly: *track*) we mean a permutation φ_a such that $x \cdot \varphi_a(x) = a$ for every $x \in Q$. The permutation φ_a^{-1} is denoted by λ_a, i.e., $\lambda_a(x) \cdot x = a$ for every $x \in Q$. Moreover, for all $i, j \in Q$, $i \neq j$, we define *left spins* $L_{ij} = L_i L_j^{-1}$, *right spins* $R_{ij} = R_i R_j^{-1}$ and *middle spins* $\varphi_{ij} = \varphi_i \varphi_j^{-1}$.

The "matrices" $L = [L_{ij}]$, $R = [R_{ij}]$ and $\Phi = [\varphi_{ij}]$ are called the *left* (*right*, *middle*) *spectrum* of a quasigroup $Q(\cdot)$, respectively. By the *indicator of the spectrum* L (cf. [5]) we mean the polynomial $L^* = \sum_{i=1}^n P(\overline{L}_i)$, where $\overline{L}_i$ is the ith row of L and $P(\overline{L}_i) = \sum_{j=1,\, i \neq j}^n P(L_{ij})$.

2010 Mathematics Subject Classification: 20N05
Keywords: Quasigroup, isotopy, parastrophe.

The indicators R^*, Φ^* of R and Φ are defined analogously.

As it is well known (cf. [6]), two permutations $\varphi, \psi \in S_n$ are *conjugated* if there exists a permutation $\rho \in S_n$ such that $\rho\varphi\rho^{-1} = \psi$.

Theorem 1.1. (Theorem 5.1.3. in [6]) *Two permutations are conjugate if and only if they have the same cyclic type.* □

We will use the following notation: $L'_{ij} = L_i^{-1}L_j$, $R'_{ij} = R_i^{-1}R_j$, $\varphi'_{ij} = \varphi_i^{-1}\varphi_j$.

2. IP-identities

As it is well known (cf. for example [1]), IP-loops satisfy the following two identities:

$$x^{-1} \cdot (x \cdot y) = y, \qquad (y \cdot x) \cdot x^{-1} = y. \tag{1}$$

In any IP-loop we also have:

$$(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}. \tag{2}$$

Let $Q(\cdot)$ be a quasigroup, $\alpha, \beta, \gamma, \rho, \sigma, \tau$ – fixed permutations of Q. Consider the following identities:

$$\alpha(x) \cdot \beta(x \cdot y) = \gamma(y) \tag{3}$$

$$\beta(y \cdot x) \cdot \alpha(x) = \gamma(y) \tag{4}$$

$$\alpha(x) \cdot \beta(y \cdot x) = \gamma(y) \tag{5}$$

$$\beta(x \cdot y) \cdot \alpha(x) = \gamma(y) \tag{6}$$

$$\rho(x \cdot y) = \sigma(y) \cdot \tau(x). \tag{7}$$

Identities (3) – (6) generalize (1), (7) is a generalization of (2).

Theorem 2.1. *If* (3) *and* (5) (*or* (4) *and* (6)) *hold for some* α, β, γ, *then* (7) *holds for some* ρ, σ, τ.

Proof. Let (3) and (5) be satisfied, i.e., let

$$\alpha_1(x) \cdot \beta_1(x \cdot y) = \gamma_1(y) \tag{8}$$

$$\alpha_2(x) \cdot \beta_2(y \cdot x) = \gamma_2(y) \tag{9}$$

for some $\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2$. Multiplying the second identity by β_1 and $\alpha_1(\alpha_2(x))$ we obtain

$$\alpha_1(\alpha_2(x)) \cdot \beta_1(\alpha_2(x) \cdot \beta_2(y \cdot x)) = \alpha_1(\alpha_2(x)) \cdot \beta_1(\gamma_2(y)),$$

which for $\alpha_2(x) = u$ and $\beta_2(y \cdot x) = v$ gives

$$\alpha_1(u) \cdot \beta_1(u \cdot v) = \alpha_1(u) \cdot \beta_1(\gamma_2(y)).$$

From this, applying (8), we get

$$\alpha_1(u)\cdot\beta_1(\gamma_2(y))=\gamma_1(v).$$

So,

$$\gamma_1(\beta_2(y\cdot x))=\alpha_1(\alpha_2(x))\cdot\beta_1(\gamma_2(y)).$$

This shows that (7) is satisfied for $\rho=\gamma_1\beta_2$, $\sigma=\alpha_1\alpha_2$, $\tau=\beta_1\gamma_2$.

Analogously we can show that (4) and (6)) imply (7). □

Theorem 2.2. *In any quasigroup:*

- (3) *holds if and only if* $R_i=\beta^{-1}\varphi_{\gamma(i)}\alpha$,
- (4) *holds if and only if* $L_i=\beta^{-1}\varphi^{-1}_{\gamma(i)}\alpha$,
- (5) *holds if and only if* $L_i=\beta^{-1}\varphi_{\gamma(i)}\alpha$,
- (6) *holds if and only if* $R_i=\beta^{-1}\varphi^{-1}_{\gamma(i)}\alpha$,
- (7) *holds if and only if* $L_i=\rho^{-1}R_{\tau(i)}\sigma$

for all $i\in Q$.

Proof. We prove only the first equivalence. The proof of other equivalences is very similar.

Let (3) holds. Then for $y=i$ we have

$$\alpha(x)\cdot\beta R_i(x)=\gamma(i)=\alpha(x)\cdot\varphi_{\gamma(i)}\alpha(x),$$

which means that $\beta R_i=\varphi_{\gamma(i)}\alpha$, whence we obtain $R_i=\beta^{-1}\varphi_{\gamma(i)}\alpha$.

The converse statement is obvious. □

Theorem 2.3. *In a quasigroup* $Q(\cdot)$ *we have:*

(*a*) $R^*=\Phi^*$ *if* (3) *or* (6) *holds,*

(*b*) $L^*=\Phi^*$ *if* (4) *or* (5) *holds,*

(*c*) $L^*=R^*$ *if* (7) *holds.*

Proof. Let (3) holds. Then $R_i=\beta^{-1}\varphi_{\gamma(i)}\alpha$, whence $R_{ij}=\beta^{-1}\varphi_{\gamma(i)\gamma(j)}\beta$. This, by Theorem 2.2, gives $R'_{ij}=\beta^{-1}\varphi_{\gamma(i)\gamma(j)}\beta$. So, $R^*=\Phi^*$.

In other cases the proof is similar. □

Corollary 2.4. *If in a quasigroup* $Q(\cdot)$ *for every* $i\in Q$

(*a*) $R_i=\beta^{-1}\varphi_{\gamma(i)}\alpha$ *or* $R_i=\beta^{-1}\varphi^{-1}_{\gamma(i)}\alpha$, *then* $R^*=\Phi^*$,

(*b*) $L_i=\beta^{-1}\varphi_{\gamma(i)}\alpha$ *or* $L_i=\beta^{-1}\varphi^{-1}_{\gamma(i)}\alpha$, *then* $L^*=\Phi^*$,

(*c*) $L_i=\rho^{-1}R_{\tau(i)}\sigma$, *then* $L^*=R^*$. □

Theorem 2.5. *Relations* $L_i=\beta^{-1}\varphi_{\gamma(i)}\alpha$, $L_i=\beta^{-1}\varphi^{-1}_{\gamma(i)}\alpha$, $R_i=\beta^{-1}\varphi_{\gamma(i)}\alpha$, $R_i=\beta^{-1}\varphi^{-1}_{\gamma(i)}\alpha$ *and* $L_i=\rho^{-1}R_{\tau(i)}\sigma$ *are universal, i.e., they are saved by isotopy.*

Proof. Assume that quasigroups $Q(\circ)$ and $Q(\cdot)$ are isotopic, i.e.,

$$\delta(x \circ y) = \mu(x) \cdot \eta(y)$$

for some permutations δ, μ, η of Q.

Translations L_i, R_i, φ_i of $Q(\cdot)$ and translations L°_i, R°_i, φ°_i of $Q(\circ)$ are connected by formulas:

$$L_i = \delta L^\circ_{\mu^{-1}(i)}\eta^{-1}, \qquad R_i = \delta R^\circ_{\eta^{-1}(i)}\mu^{-1}, \qquad \varphi_i = \eta\varphi^\circ_{\delta^{-1}(i)}\mu^{-1}$$

(for details see [5]). Hence, if the formula $L_i = \beta^{-1}\varphi_{\gamma(i)}\alpha$ is satisfied in $Q(\cdot)$, then in $Q(\circ)$ it has the form

$$\delta L^\circ_{\mu^{-1}(i)}\eta^{-1} = \beta^{-1}(\eta\varphi^\circ_{\delta^{-1}\gamma(i)}\mu^{-1})\alpha\,.$$

Thus

$$L^\circ_{\mu^{-1}(i)} = \delta^{-1}\beta^{-1}\eta\varphi^\circ_{\delta^{-1}\gamma(i)}\mu^{-1}\alpha\eta\,,$$

which for $j = \mu^{-1}(i)$ gives

$$L^\circ_j = (\delta^{-1}\beta^{-1}\eta)\varphi^\circ_{\delta^{-1}\gamma\mu(i)}(\mu^{-1}\alpha\eta)\,.$$

So, the formula $L_i = \beta^{-1}\varphi_{\gamma(i)}\alpha$ is universal.

In other cases the proof is analogous. □

3. Examples

We will use universal relations mentioned in Theorem 2.5 to determine conditions under which identities (3) – (7) are satisfied by quasigroups belonging to the isotopy classes of quasigroups listed in the book [2]. We omit classes of quasigroups isotopic to groups since groups satisfy each of these identities for some permutations.

1. The first class is represented by the loop No. 2.1.1:

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

$L_1 = \varphi_1 = (1.2.3.4.5.)$	$R_1 = (1.2.3.4.5.)$
$L_2 = \varphi_2 = (12.345.)$	$R_2 = (12.354.)$
$L_3 = \varphi_3 = (13.254.)$	$R_3 = (13.245.)$
$L_4 = \varphi_4 = (14.235.)$	$R_4 = (14.253.)$
$L_5 = \varphi_5 = (15.243.)$	$R_5 = (15.234.)$

In this loop $L_i = \varphi_i$ for all i, so from the first universal relation $L_i = \beta^{-1}\varphi_{\gamma(i)}\alpha$ we see that this is possible for $\alpha = \beta = \gamma = \varepsilon$, which, by Theorem 2.2, means that this loop satisfies the identity:

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

This universal relation is possible also for other α and β. Indeed, for $\gamma(1)=1$, from Theorem 2.2 and (3), we obtain $\alpha(x)\cdot\beta(x)=1$, which for this loop implies $\alpha=\beta$. Hence for $\gamma(2)=3$ we have $L_2=\alpha^{-1}\varphi_3\alpha$. This is possible only for $\alpha=(1.23.45.)$. Then $\gamma=\alpha$. So, the identity

$$\alpha(x)\cdot\alpha(y\cdot x)=\alpha(y), \tag{10}$$

where $\alpha=(1.23.45.)$ also is possible in this loop.

Now we check connections between R_i and φ_i. For this we use indicators R^* and Φ^*. In the case $R^*\neq\Phi^*$ no any connections, in the case $R^*=\Phi^*$ connections are possible.

For this loop we have

$\overline{\Phi}_1=\{\varphi_{12},\varphi_{13},\varphi_{14},\varphi_{15}\}=\{(12.354.),(13.245.),(14.253.),(15.234.)\}$
$\overline{\Phi}_2=\{\varphi_{21},\varphi_{23},\varphi_{24},\varphi_{25}\}=\{(12.345.),(14325.),(15423.),(13524.)\}$
$\overline{\Phi}_3=\{\varphi_{31},\varphi_{32},\varphi_{34},\varphi_{35}\}=\{(13.254.),(15234.),(12435.),(14532.)\}$
$\overline{\Phi}_4=\{\varphi_{41},\varphi_{42},\varphi_{43},\varphi_{45}\}=\{(14.235.),(13245.),(15342.),(12543.)\}$
$\overline{\Phi}_5=\{\varphi_{51},\varphi_{52},\varphi_{53},\varphi_{54}\}=\{(15.243.),(14235.),(12354.),(13452.)\}$

and

$P(\overline{\Phi}_1)=\sum_{j=2}^{5}P(\varphi_{1j})=x_2x_3+x_2x_3+x_2x_3+x_2x_3=4x_2x_3$
$P(\overline{\Phi}_2)=\sum_{j=1,\,j\neq2}^{5}P(\varphi_{2j})=x_2x_3+x_5+x_5+x_5=x_2x_3+3x_5$
$P(\overline{\Phi}_3)=P(\overline{\Phi}_4)=P(\overline{\Phi}_5)=P(\overline{\Phi}_2)=x_2x_3+3x_5$
$\Phi^*=\sum_{i=1}^{5}P(\overline{\Phi}_i)=5x_2x_3+12x_5$

Analogously,

$\overline{R}_1=\{R_{12},R_{13},R_{14},R_{15}\}=\{(12.345.),(13.254.),(14.235.),(15.243.)\}$
$\overline{R}_2=\{R_{21},R_{23},R_{24},R_{25}\}=\{(12.354.),(15324.),(13425.),(14523.)\}$
$\overline{R}_3=\{R_{31},R_{32},R_{34},R_{35}\}=\{(13.245.),(14234.),(15432.),(12534.)\}$
$\overline{R}_4=\{R_{41},R_{42},R_{43},R_{45}\}=\{(14.253.),(15243.),(12345.),(13542.)\}$
$\overline{R}_5=\{R_{51},R_{52},R_{53},R_{54}\}=\{(15.234.),(13245.),(14352.),(12453.)\}$

and

$P(\overline{R}_1)=4x_2x_3,\ P(\overline{R}_2)=P(\overline{R}_3)=P(\overline{R}_4)=P(\overline{R}_5)=x_2x_3+3x_5$
$R^*=5x_2x_3+12x_5$

So, $R^*=\Phi^*$. Thus, the relation $R_i=\beta^{-1}\varphi_{\gamma(i)}\alpha$ or $R_i=\beta^{-1}\varphi_{\gamma(i)}^{-1}\alpha$ is possible (Corollary 2.4). If the first relation holds, then $R_{ij}=\beta^{-1}\varphi_{\gamma(i)\gamma(j)}\beta$. For $i=1$ must be $\gamma(1)=1$ since two conjugated permutations have the same cyclic type (Theorem 1.1). So, $R_{1j}=\beta^{-1}\varphi_{1\gamma(j)}\beta$, which for $\gamma(2)=2$ gives $R_{12}=\beta^{-1}\varphi_{12}\beta$. The last equation has three solutions: $\beta_1=(1.2.3.45.)$, $\beta_2=(1.2.35.4.)$ and $\beta_3=(1.2.34.5.)$. Hence, in view of Theorem 2.3, the identity (3) may be true in this class of quasigroups for $\alpha=\beta=\gamma=\beta_i$. Comparing this fact with (10), where $\alpha=(1.23.45.)$, and the end of the proof of Theorem 2.1 ($\rho=\gamma_1\beta_2$, $\sigma=\alpha_1\alpha_2$, $\tau=\beta_1\gamma_2$), we see that $\alpha_1=\beta_1=\gamma_1=(1.23.45.)$, $\alpha_2=\beta_2=\gamma_2=(1.2.3.45.)$ and

$\rho = \sigma = \tau = (1.23.4.5.)$. So, in this loop we have

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

for $\rho = (1.23.4.5.)$.

2. Using the same method we can see that $L^* = R^* = \Phi^*$ for loops no. 3.1.1, 4.1.1, 5.1.1, 6.1.1 and 7.1.1. For example, for the loop no. 3.1.1 we have $L^* = R^* = \Phi^* = 6(2x_3^2 + 3x_6)$ and $L_i = \beta^{-1}\varphi_{\gamma(i)}\alpha$, where $\alpha = (1.2.3.465.)$, $\beta = \gamma = (1.23.4.5.6.)$. So, in this loop $\alpha(x) \cdot \beta(y \cdot x) = \beta(y)$ for the above α, β. In this loop also $R_i = \beta^{-1}\varphi_{\gamma(i)}\alpha$ for $\alpha = (1.2.3.46.5.)$, $\beta = \gamma = (1.23.4.56.)$, which means that this loop satisfies $\alpha(x) \cdot \beta(x \cdot y) = \beta(y)$ for the above α, β. Hence, it satisfies also $\rho(x \cdot y) = \rho(y) \cdot \rho(x)$ for $\rho = (1.2.3.4.56.)$.

3. For loops no. 8.1.1, 8.2.1, 8.3.1, 9.1.1, 9.2.1, 9.3.1, 10.1.1, 10.2.1, 10.3.1, 11.1.1, 11.2.1, 11.3.1, 12.1.1, 12.2.1 and 12.3.1, one of the following relations take place: $L^* = R^* \neq \Phi^*$, $L^* \neq R^* = \Phi^*$, $R^* \neq L^* = \Phi^*$.

References

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

[2] **J. Dénes and A.D. Keedwell**, *Latin squares and their applications*, Akadémai Kiadó, Budapest, 1974.

[3] **I.I. Deriyenko**, *On middle translations of finite quasigroups*, Quasigroups and Related Systems **16** (2008), 17 – 24.

[4] **I.I. Deriyenko**, *Configurations of conjugated permutations*, Quasigroups and Related Systems **18** (2010), 17 – 24.

[5] **I.I. Deriyenko**, *Indicators of quasigroups*, Quasigroups and Related Systems **19** (2011), 223 – 226.

[6] **M. Hall**, *The theory of groups*, Macmillan, 1959.

Received November 15, 2012

Department of Higher Mathematics and Informatics, Kremenchuk National University,
Pershotravneva 20, 39600, Kremenchuk, Ukraine
E-mail: ivan.deriyenko@gmail.com

D-loops

Ivan I. Deriyenko and Wieslaw A. Dudek

Abstract. D-loops are loops with the antiautomorphic inverse property. The class of such loops is larger than the class of IP-loops. The smallest D-loops which is not an IP-loop has six elements. We prove several basic properties of such loops and present methods of constructions of D-loops from IP-loops. Unfortunately, a loop isotopic to a D-loop may not be a D-loop.

1. Introduction

A loop is a quasigroup $Q(\circ)$ with an identity element always denoted by 1. A loop $Q(\circ)$ has the *inverse property*, i.e., it is an *IP-loop*, if for each its element a there exists in Q a uniquely determined *inverse element* a' such that $a'\circ(a\circ b) = (b\circ a)\circ a'$. This means that in an *IP*-loop for *right* and *left translations*, i.e., for $R_a(x) = x\circ a$, $L_a(x) = a\circ x$, we have

$$R_a^{-1} = R_{a'}, \qquad L_a^{-1} = L_{a'}. \tag{1}$$

It is not difficult to shown that in an IP-loop $Q(\circ)$ for all $a, b \in Q$ hold

$$a\circ a' = a'\circ a = 1, \quad (a')' = a \tag{2}$$

and

$$(a\circ b)' = b'\circ a'\,. \tag{3}$$

On the other hand, in any loop $Q(\circ)$ for each $a \in Q$ there are uniquely determined *left* and *right loop-inverse* elements $a_{_L}^{-1}, a_{_R}^{-1} \in Q$ for which we have $a_{_L}^{-1}\circ a = a\circ a_{_R}^{-1} = 1$. A two-sided loop-inverse element to $a \in Q$ is denoted by a^{-1}. Clearly, $(a^{-1})^{-1} = a$. Hence, an element $a^{-1} \in Q$ is loop-inverse to $a \in Q$ if and only if $a \in Q$ is loop-inverse to a^{-1}. In a loop each inverse element is loop-inverse but a loop-inverse element may not be inverse.

2010 Mathematics Subject Classification: 20N05
Keywords: Quasigroup, loop, D-loop, antiautomorphic inverse property, track.

The main results of this paper were presented at the conference Loops'11 which was held in Trest, Czech Republic, July, 2011.

Example 1.1. Consider the following loop $Q(\circ)$:

$\circ$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	1	6	7	5	4
3	3	1	2	7	6	4	5
4	4	7	6	5	1	3	2
5	5	6	7	1	4	2	3
6	6	4	5	2	3	7	1
7	7	5	4	3	2	1	6

In this loop we have $a_L^{-1} = a_R^{-1}$ for each $a \in Q$. Hence, each element of this loop is loop-inverse. But $a = 5$ is not an inverse element since $4 \circ (5 \circ 6) \neq 6$. The map $h(x) = x_R^{-1}$ is an antiautomorphism of this loop, i.e., it satisfies the identity $h(x \circ y) = h(y) \circ h(x)$. □

Recall that a loop $Q(\circ)$ satisfies the *antiautomorphic inverse property* if for each $x \in Q$ there exists a two-sided loop-inverse element x^{-1} such that $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$ holds for all $x, y \in Q$. A simple example of such loop is an IP-loop. The above example proves that there are also loops with this property which are not IP-loops. Thus, the class of loops with this property is much larger than the class of IP-loops.

This enables us to introduce the following definition.

Definition 1.2. A loop $Q(\circ)$ is called a *D-loop* if it satisfies the *dual automorphic property* for $\varphi(x) = x_R^{-1}$, i.e., if

$$(x \circ y)_R^{-1} = y_R^{-1} \circ x_R^{-1} \tag{4}$$

holds for all $x, y \in Q$.

Theorem 1.3. *A loop $Q(\circ)$ is a D-loop if and only if it satisfies the identity*

$$(x \circ y)_L^{-1} = y_L^{-1} \circ x_L^{-1}. \tag{5}$$

Proof. Suppose that $Q(\circ)$ is a D-loop. Since $x_L^{-1} \circ x = 1$, from (4) it follows

$$1 = 1_R^{-1} = (x_L^{-1} \circ x)_R^{-1} = x_R^{-1} \circ (x_L^{-1})_R^{-1},$$

which together with $1 = x_L^{-1} \circ (x_L^{-1})_R^{-1}$ gives $x_L^{-1} = x_R^{-1}$. Thus (4) implies (5).

Analogously, using $x \circ x_R^{-1} = 1$ and $(x_R^{-1})_L^{-1} \circ x_R = 1$ we can prove that (5) implies (4). □

Corollary 1.4. *For all elements of D-loops we have*

$$a_L^{-1} = a_R^{-1} \quad \textit{and} \quad (a^{-1})^{-1} = a. \qquad \square$$

This means that in the multiplication table of a D-loop $Q(\circ)$ its neutral element is located symmetrically with respect to the main diagonal and the class of all D-loops coincides with the class of loops with the antiautomorphic inverse property but we'll keep the term *D-loop* since it is shorter and more convenient to use.

2. Constructions of D-loops

Below we present several methods of verification when a given loop is a D-loop. To describe these methods we must reminder some definitions from [2], [5] and [6].

Definition 2.1. Let $Q(\cdot)$ be a loop. A permutation φ_a of Q, where $a \in Q$, is called a *right middle translation* or a *right track* (shortly: *track*) of $Q(\cdot)$ if

$$x \cdot \varphi_a(x) = a \tag{6}$$

holds for all $x \in Q$. By a *left middle translation* or a *left track* we mean a permutation λ_a such that

$$\lambda_a(x) \cdot x = a. \tag{7}$$

It is clear that $\lambda_a = \varphi_a^{-1}$ and $\varphi_1(x) = x_R^{-1}$ for all $a, x \in Q$.

The permutation φ_a selects in the multiplication table of a given loop the number of columns in an element a appears. For the loop defined in Example 1.1

$$\varphi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 6 & 1 & 5 & 2 & 3 \end{pmatrix} = (1\,4)(2\,7\,3\,6)(5).$$

Further, permutations will be written in the form of cycles, cycles will be separated by dots. For example, the above permutation φ_4 will be written as $\varphi_4 = (1\,4.\,2\,7\,3\,6.\,5.)$.

It is clear that a loop $Q(\cdot)$, where $Q = \{1, 2, \ldots, n\}$, can be identified with the set $\{\varphi_1, \varphi_2, \ldots, \varphi_n, \}$ of its tracks.

Theorem 2.2. *A loop $Q(\cdot)$ is a D-loop if and only if*

$$\varphi_1 \varphi_a \varphi_1 = \varphi_{a^{-1}}^{-1} \tag{8}$$

for every $a \in Q$, where a^{-1} is (right) inverse to a.

Proof. Let $Q(\cdot)$ be a D-loop. Then $x_R^{-1} = x^{-1}$ for every $x \in Q$ and, according to (6), for all $a, x \in Q$ we have $\varphi_a^{-1}(x) \cdot x = a$. Hence

$$a^{-1} = (\varphi_a^{-1}(x) \cdot x)^{-1} = x^{-1} \cdot (\varphi_a^{-1}(x))^{-1} = \varphi_1(x) \cdot \varphi_1 \varphi_a^{-1}(x).$$

Since also $a^{-1} = \varphi_1(x) \cdot \varphi_{a^{-1}} \varphi_1(x)$, from the above we obtain $\varphi_1 \varphi_a^{-1} = \varphi_{a^{-1}} \varphi_1$, which implies (8).

Conversely, let $x \cdot y = a$. Then $y = \varphi_a(x)$. Hence

$$\begin{aligned} y_R^{-1} \cdot x_R^{-1} &= \varphi_1 \varphi_a(x) \cdot \varphi_1(x) = \varphi_1 \varphi_a \varphi_1(x^{-1}) \cdot x^{-1} \\ &\overset{(8)}{=} \varphi_{a^{-1}}^{-1}(x^{-1}) \cdot x^{-1} = \lambda_{a^{-1}}(x^{-1}) \cdot x^{-1} \overset{(7)}{=} a_R^{-1} = (x \cdot y)_R^{-1}. \end{aligned}$$

This completes the proof. □

Corollary 2.3. *A loop $Q(\cdot)$ is a D-loop if and only if it satisfies one of the following identities:*

(a) $\varphi_1\varphi_a^{-1}\varphi_1 = \varphi_{a^{-1}}$,

(b) $\varphi_1 R_a \varphi_1 = L_{a^{-1}}$,

(c) $\varphi_1 L_a \varphi_1 = R_{a^{-1}}$.

Proof. Indeed, (8) can be written in the form $\varphi_1\varphi_{a^{-1}}\varphi_1 = \varphi_a^{-1}$, which, in view of $\varphi_1\varphi_1 = id_Q$, is equivalent to (a). Moreover, $(x \cdot a)^{-1} = a^{-1} \cdot x^{-1}$ means that $\varphi_1 R_a = L_{a^{-1}}\varphi_1$. The last is equivalent to (b) and (c). □

Example 2.4. Consider the loop $Q(\cdot)$:

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	5	1	6	4	2
4	4	6	5	2	1	3
5	5	3	6	1	2	4
6	6	4	2	5	3	1

We will use Theorem 2.2 to verify that this loop is a D-loop.

We have

$$\varphi_1 = (1.\,2.\,3.\,4\,5.\,6.) \qquad \varphi_4 = (1\,4.\,2\,3\,5\,6.)$$
$$\varphi_2 = (1\,2.\,3\,6.\,4.\,5.) \qquad \varphi_5 = (1\,5.\,2\,6\,4\,3.)$$
$$\varphi_3 = (1\,3.\,2\,4\,6\,5.) \qquad \varphi_6 = (1\,6.\,2\,5\,3\,4.)$$

We have to check the condition (8) for $a = 2, 3, 4, 5, 6$ because $\varphi_1\varphi_1\varphi_1 = \varphi_1^{-1}$ holds in each loop. Permutations φ_1 and φ_2 have disjoint cycles hence $\varphi_1\varphi_2\varphi_1 = \varphi_2 = \varphi_2^{-1}$. In other cases we obtain:

$$\varphi_1\varphi_3\varphi_1 = (1\,3.\,2\,5\,6\,4.) = \varphi_3^{-1} \qquad \varphi_1\varphi_5\varphi_1 = (1\,4.\,2\,6\,5\,3.) = \varphi_4^{-1}$$
$$\varphi_1\varphi_4\varphi_1 = (1\,5.\,2\,3\,4\,6.) = \varphi_5^{-1} \qquad \varphi_1\varphi_6\varphi_1 = (1\,6.\,2\,4\,3\,5.) = \varphi_6^{-1}$$

This shows that $Q(\circ)$ is a D-loop. □

Note that in general loops isotopic to D-loops are not D-loops.

Example 2.5. The following loop

$\circ$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	6	3	4	5
3	3	6	2	5	1	4
4	4	5	1	6	2	3
5	5	3	4	1	6	2
6	6	4	5	2	3	1

is isotopic to a D-loop $Q(\circ)$ from the previous example. This isotopy has the form $\gamma(x\circ y)=\alpha(x)\cdot\beta(y)$, where $\alpha=(1\,4\,2.\,3.\,5.\,6.)$, $\beta=(1\,2\,5\,4\,6.\,3.)$, $\gamma=(1\,6\,4\,3\,5\,2.)$. The loop $Q(\circ)$ is not a D-loop since $3_L^{-1}\neq 3_R^{-1}$. □

Theorem 2.6. *Let $Q(\cdot)$ be an IP-loop and let $a\in Q$ be fixed. If an element $a'\in Q$ is inverse to a in $Q(\cdot)$, then $Q(\circ)$ with the operation*

$$x\circ y=R_{a'}(x)\cdot L_a(y) \tag{9}$$

is a D-loop with the same identity as in $Q(\cdot)$.

Proof. It is clear that $Q(\circ)$ is a quasigroup. Let an element $a'\in Q$ be inverse to a in $Q(\cdot)$. Then

$$x\circ 1=R_{a'}(x)\cdot L_a(1)=(x\cdot a')\cdot a=x.$$

Similarly $1\circ x=x$. Hence $Q(\circ)$ is a loop with the same identity as in $Q(\cdot)$.

Moreover, for every $x\in Q$ there exists $\overline{x}\in Q$ such that

$$1=x\circ\overline{x}=R_{a'}(x)\cdot L_a(\overline{x})=(x\cdot a')\cdot(a\cdot\overline{x}),$$

which gives $a\cdot\overline{x}=(x\cdot a')^{-1}=(a')^{-1}\cdot x^{-1}=a\cdot x^{-1}$. Thus $\overline{x}=x^{-1}$ for every $x\in Q$. Hence

$$\begin{aligned}(x\circ y)^{-1}&=(R_{a'}(x)\cdot L_a(y))^{-1}=((x\cdot a')\cdot(a\cdot y))^{-1}\\&=(a\cdot y)^{-1}\cdot(x\cdot a')^{-1}=(y^{-1}\cdot a^{-1})\cdot((a')^{-1}\cdot x^{-1})\\&=(y^{-1}\cdot a')\cdot(a\cdot x^{-1})=R_{a'}(y^{-1})\cdot L_a(x^{-1})=y^{-1}\circ x^{-1}.\end{aligned}$$

Therefore $Q(\circ)$ is a D-loop. □

Corollary 2.7. *Any IP-loop of order n determines $n-1$ isotopic D-loops.*

Example 2.8. Starting from the following *IP*-loop:

$\cdot$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	1	6	7	5	4
3	3	1	2	7	6	4	5
4	4	7	6	5	1	2	3
5	5	6	7	1	4	3	2
6	6	4	5	3	2	7	1
7	7	5	4	2	3	1	6

and using (9) with $a=2$ we obtain a D-loop:

$\circ$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	1	6	7	5	4
3	3	1	2	5	4	7	6
4	4	5	6	7	1	2	3
5	5	4	7	1	6	3	2
6	6	7	5	3	2	4	1
7	7	6	4	2	3	1	5

which is not an *IP*-loop because $3 \circ (2 \circ 5) \neq 5$. Hence $a = 2$ is not an inverse element in $Q(\circ)$. Putting $x * y = R_3(x) \circ L_2(y)$ we obtain a quasigroup:

$*$	1	2	3	4	5	6	7
1	1	2	3	7	6	4	5
2	2	3	1	6	7	5	4
3	3	1	2	5	4	7	6
4	7	5	6	4	1	2	3
5	6	4	7	1	5	3	2
6	4	7	5	3	2	6	1
7	5	6	4	2	3	1	7

which is isotopic to the initial D-loop $Q(\circ)$ but it is not a D-loop. This means that in Theorem 2.6 the assumption on a can not be ignored. □

Proposition 2.9. *An element $a \in Q$ used in Theorem* 2.6 *has the same inverse element in $Q(\cdot)$ and $Q(\circ)$ defined by* (9) *if and only if*

$$x \cdot a = x \circ a \quad \textit{and} \quad a' \cdot x = a' \circ x \tag{10}$$

for all $x \in Q$.

Proof. Let $a' \in Q$ be inverse to a in $Q(\cdot)$ and $Q(\circ)$. Then $a = (a')'$ and

$$z = (z \circ a') \circ a = (R_{a'}(z) \cdot L_a(a')) \circ a = R_{a'}(z) \circ a,$$

which for $z = x \cdot a$ gives $x \cdot a = x \circ a$.

Similarly,

$$z = a' \circ (a \circ z) = a' \circ (R_{a'}(a) \cdot L_a(z)) = a' \circ L_a(z)$$

for $z = a' \cdot x$ implies $a' \cdot x = a' \circ x$.

Conversely, if $a' \in Q$ is inverse to a in $Q(\cdot)$ and (10) are satisfied, then

$$(x \circ a) \circ a' = (x \cdot a) \circ a' = R_{a'}(x \cdot a) \cdot L_a(a') = ((x \cdot a) \cdot a') \cdot (a \cdot a') = x.$$

Analogously $a' \circ (a \circ x) = a' \cdot (a \circ x) = x$. Hence a' is inverse to a in $Q(\circ)$. □

Corollary 2.10. *An element $a \in Q$ used in Theorem* 2.6 *has the same inverse element in $Q(\cdot)$ and $Q(\circ)$ defined by* (9) *if and only if the multiplication tables of these two loops have the same a–columns and the same a'–rows.*

Proposition 2.11. *An element $a \in Q$ used in Theorem* 2.6 *has the same inverse element in $Q(\cdot)$ and $Q(\circ)$ defined by* (9) *if and only if*

$$L_a L_a = L_{a^2} \quad \textit{and} \quad R_a R_a = R_{a^2} \tag{11}$$

where L_a and R_a are translations in $Q(\cdot)$.

Proof. Let $a \in Q$ has the same inverse a' in $Q(\cdot)$ and $Q(\circ)$. Then for every $x \in Q$ we have

$$\begin{aligned} x = a' \circ (a \circ x) &= R_{a'}(a') \cdot L_a(R_{a'}(a) \cdot L_a(x)) \\ &= R_{a'}(a')L_aL_a(x) = L_{a'\cdot a'}L_aL_a(x) = L_{(a^2)'}L_aL_a(x), \end{aligned}$$

whence, applying (1), we get $L_aL_a = L^{-1}_{(a^2)'} = L_{a^2}$.

Similarly, for every $z \in Q$ we have

$$z \circ a = R_{a'}(z) \cdot L_a(a) = R_{a^2}R_{a'}(z),$$

which for $z = R_a(x)$, by (1), gives

$$R_a(x) \circ a = R_{a^2}R_{a'}R_a(x) = R_{a^2}(x).$$

Hence $R_aR_a = R_{a^2}$. This proves (11).

The converse statement is obvious. □

Below we present a simple method of construction of new loops from given loops. This method is based on *exchange of tracks.* Next, this method will be applied to the construction of *D*-loops.

Let $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$ be tracks of a *D*-loop $Q(\cdot)$ with the identity 1. We say that for $i \neq j \neq 1$ tracks φ_i, φ_j are *decomposable* if there exist two nonempty subsets X, Y of Q such that $Q = X \cup Y$, $X \cap Y = \emptyset$, $1 \in X$ and

$$\begin{cases} \varphi_i = \bar{\varphi}_i\hat{\varphi}_i \\ \varphi_j = \bar{\varphi}_j\hat{\varphi}_j \end{cases} \tag{12}$$

where $\bar{\varphi}_i$, $\bar{\varphi}_j$ are permutations of X, $\hat{\varphi}_i, \hat{\varphi}_j$ are permutations of Y.

Putting

$$\begin{cases} \psi_i = \bar{\varphi}_i\hat{\varphi}_j \\ \psi_j = \bar{\varphi}_j\hat{\varphi}_i \end{cases} \tag{13}$$

and $\psi_k = \varphi_k$ for $k \notin \{i, j\}$ we obtain the new system of tracks which defines on Q the new loop $Q(\circ)$ with the same identity as in $Q(\cdot)$.

Example 2.12. The loop $Q(\cdot)$ defined by

$\cdot$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	3	4	1	6	7	8	5
3	3	4	1	2	7	8	5	6
4	4	1	2	3	8	5	6	7
5	5	8	7	6	1	4	3	2
6	6	5	8	7	2	1	4	3
7	7	6	5	8	3	2	1	4
8	8	7	6	5	4	3	2	1

is a group (so, it is a D-loop) with the following tracks:

$$\begin{array}{lll}
\varphi_1 = (1.24.3.4.5.6.7.8.) & \varphi_2 = (12.34.5876.) & \varphi_3 = (13.2.4.57.68.) \\
\varphi_4 = (14.23.5678.) & \varphi_5 = (15.37.2846.) & \varphi_6 = (16.38.2547.) \\
\varphi_7 = (17.35.2648.) & \varphi_8 = (18.36.2745.) &
\end{array}$$

For $(i,j) \in \{(2,3),(2,4),(3,4),(5,7),(6,8)\}$ tracks φ_i, φ_j are decomposable. In the case $(i,j) = (6,8)$ we have

$$\left\{\begin{array}{lll} \varphi_6 = \bar{\varphi}_6\hat{\varphi}_6, & \text{where} & \bar{\varphi}_6 = (16.38.),\ \hat{\varphi}_6 = (2547.) \\ \varphi_8 = \bar{\varphi}_8\hat{\varphi}_8, & \text{where} & \bar{\varphi}_8 = (18.36.),\ \hat{\varphi}_8 = (2745.) \end{array}\right.$$

whence, according to (13), we obtain

$$\left\{\begin{array}{l} \psi_6 = \bar{\varphi}_6\hat{\varphi}_8 = (16.38.2745.) \\ \psi_8 = \bar{\varphi}_8\hat{\varphi}_6 = (18.36.2547.) \end{array}\right.$$

and $\psi_k = \varphi_k$ for $k = 1,2,3,4,5,7$.

This new system of tracks $\{\psi_1, \psi_2, \ldots, \psi_8\}$ defines the loop $Q(\circ)$:

$\circ$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	3	4	1	$\boxed{8}$	7	$\boxed{6}$	5
3	3	4	1	2	7	8	5	6
4	4	1	2	3	$\boxed{6}$	5	$\boxed{8}$	7
5	5	$\boxed{6}$	7	$\boxed{8}$	1	4	3	2
6	6	5	8	7	2	1	4	3
7	7	$\boxed{8}$	5	$\boxed{6}$	3	2	1	4
8	8	7	6	5	4	3	2	1

where items changed by tracks ψ_6 and ψ_8 are entered in the box. □

This new loop $Q(\circ)$ can be used for the construction of another loop since it has the same pair of decomposable tracks as $Q(\cdot)$. So, for the construction of new loops we can use not only one but also two or more pairs of decomposable tracks. Using different pairs of decomposable tracks we obtain different loops which may not be isotopic. Obtained loops may not be isotopic to the initial loop $Q(\cdot)$, too.

Example 2.13. Direct computations show that this loop

$\cdot$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	5	7	3	8	4	6
3	3	8	6	1	4	2	5	7
4	4	6	1	5	7	3	8	2
5	5	7	4	2	8	1	6	3
6	6	4	8	3	1	7	2	5
7	7	5	2	8	6	4	3	1
8	8	3	7	6	2	5	1	4

is a D-loop. It hasn't got any decomposable pair of tracks. □

Theorem 2.14. *Let $Q(\cdot)$ be a D-loop with the identity* 1*. If φ_i, φ_j, where $i \cdot j = 1$ and $i \neq j$, are decomposable tracks of $Q(\cdot)$, then a loop $Q(\circ)$ obtained from $Q(\cdot)$ by exchange of tracks is a D-loop.*

Proof. Since $Q(\circ)$ is a loop it is sufficient to show that $\psi_1\psi_k\psi_1 = \psi_{k^{-1}}^{-1}$ for every $k \in Q$ (Theorem 2.2). For $k \notin \{i,j\}$ we have $\psi_k = \varphi_k$, so for $k \notin \{i,j\}$ this condition is satisfied by the assumption. For $k = i$ we have

$$\psi_1\psi_i\psi_1 = \varphi_1\bar{\varphi}_i\hat{\varphi}_j\varphi_1 = (\varphi_1\bar{\varphi}_i\varphi_1)(\varphi_1\hat{\varphi}_j\varphi_1) = \bar{\varphi}_j{}^{-1}\hat{\varphi}_i{}^{-1} = \psi_j^{-1} = \psi_{i^{-1}}^{-1}$$

because $\varphi_1^2 = \varepsilon$, $\bar{\varphi}_i\hat{\varphi}_j = \hat{\varphi}_j\bar{\varphi}_i$ and $i \cdot j = 1$.

For $k = j$ the proof is analogous. So, $Q(\circ)$ is a D-loop. □

The assumption $i \cdot j = 1$ is essential. Indeed, in Example 2.12 tracks φ_3, φ_4 are decomposable, $4 \cdot 3 \neq 1$, $4^{-1} = 2$ and $\psi_1\psi_4\psi_1 = \psi_4 \neq \psi_2^{-1}$. So, a loop determined by tracks $\psi_1, \ldots, \psi_8$ is not a D-loop.

The D-loop $Q(\circ)$ constructed in Example 2.12 is not isotopic to the initial group $Q(\cdot)$ since $(7 \circ 7) \circ 2 \neq 7 \circ (7 \circ 2)$. In this loop we also have $7 \circ (7 \circ 2) \neq 2$, so it is not an IP-loop, too.

Example 2.15. The loop $Q(\cdot)$ defined by

·	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	5	7	3	8	4	6
3	3	8	4	1	7	2	6	5
4	4	6	1	3	8	7	5	2
5	5	7	8	2	6	1	3	4
6	6	4	7	8	1	5	2	3
7	7	5	2	6	4	3	8	1
8	8	3	6	5	2	4	1	7

is a D-loop with the following tracks:

$\varphi_1 = (1.2.34.56.78.)$ $\varphi_2 = (12.367.485.)$ $\varphi_3 = (13.4.25768.)$
$\varphi_4 = (14.3.27586.)$ $\varphi_5 = (15.6.23847.)$ $\varphi_6 = (16.5.28374.)$
$\varphi_7 = (17.8.24635.)$ $\varphi_8 = (18.7.26453.)$

For $(i,j) \in \{(3,4),(5,6),(7,8)\}$ tracks φ_i, φ_j are decomposable. Each pair of such tracks gives a D-loop. Obtained loops are isotopic but they are not isotopic to $Q(\cdot)$ since they and $Q(\cdot)$ have different indicators Φ^*. (Isotopic loops have the same indicators – see [7].)

If for the construction of a new loop we use two pairs of decomposable tracks: φ_3, φ_4 and φ_5, φ_6, or φ_3, φ_4 and φ_7, φ_8, or φ_5, φ_6 and φ_7, φ_8, then we obtain three isotopic D-loops. These loops are not isotopic either to $Q(\cdot)$ or to the previous because have different indicators Φ^*.

Also in the case when we use three pairs of decomposable tracks obtained D-loop. It is not isotopic to any of the previous.

So, from this D-loop we obtain three nonisotopic D-loops which also are not isotopic to the initial D-loop $Q(\cdot)$. □

As it is well known with each quasigroup $Q(\cdot)$ we can conjugate five new quasigroups (called *parastrophes* of $Q(\cdot)$) by permuting the variables in the defining equation. Namely, if $Q_0 = Q(\cdot)$ is a fixed quasigroup, then its parastrophes have the form

$$\begin{array}{lccc}
Q(\backslash) & x\backslash z = y & \Longleftrightarrow & x \cdot y = z, \\
Q(/) & z/y = x & \Longleftrightarrow & x \cdot y = z, \\
Q(\ast) & y \ast x = z & \Longleftrightarrow & x \cdot y = z, \\
Q(\bullet) & y \bullet z = x & \Longleftrightarrow & x \cdot y = z, \\
Q(\triangleleft) & z \triangleleft x = y & \Longleftrightarrow & x \cdot y = z.
\end{array}$$

Theorem 2.16. *Parastrophes of a D-loop $Q(\cdot)$ are isomorphic to one of the following quasigroups: $Q(\cdot)$, $Q(\backslash)$, $Q(/)$.*

Proof. Indeed, if $Q(\cdot)$ is a D-loop, φ_1 – its track determined by the identity of $Q(\cdot)$, then, according to the definition of D-loops, we have

$$\varphi_1(x \cdot y) = \varphi_1(y) \cdot \varphi_1(x).$$

Hence

$$\varphi_1(y \ast x) = \varphi_1(z) \Longleftrightarrow \varphi_1(x \cdot y) = \varphi_1(z) \Longleftrightarrow \varphi_1(y) \cdot \varphi_1(x) = \varphi_1(z).$$

So, $\varphi_1(y \ast x) = \varphi_1(y) \cdot \varphi_1(x)$, i.e., $Q(\ast)$ and $Q(\cdot)$ are isomorphic.

Further,

$$\begin{aligned}
\varphi_1(y \bullet z) = \varphi_1(x) \quad & \Longleftrightarrow \varphi_1(x \cdot y) = \varphi_1(z) \Longleftrightarrow \varphi_1(y) \cdot \varphi_1(x) = \varphi_1(z) \\
& \Longleftrightarrow \varphi_1(y)\backslash\varphi_1(z) = \varphi_1(x).
\end{aligned}$$

Thus, $\varphi_1(y \bullet z) = \varphi_1(y\backslash z)$. Consequently, $Q(\bullet) \cong Q(\backslash)$.

Analogously,

$$\begin{aligned}
\varphi_1(z \triangleleft x) = \varphi_1(y) \quad & \Longleftrightarrow \varphi_1(x \cdot y) = \varphi_1(z) \Longleftrightarrow \varphi_1(y) \cdot \varphi_1(x) = \varphi_1(z) \\
& \Longleftrightarrow \varphi_1(z)/\varphi_1(x) = \varphi_1(y),
\end{aligned}$$

whence $\varphi_1(z \triangleleft x) = \varphi_1(z/x)$. So, $Q(\triangleleft) \cong Q(/)$. □

3. Loops isotopic to D-loops

As was mentioned earlier, loops isotopic to D-loops are not D-loops in general, but in some cases principal isotopes of D-loops are D-loops. Below we find conditions under which D-loops are isotopic to groups and conditions under which a principal isotope of a D-loop is a D-loop.

Definition 3.1. Let $Q(\cdot)$, where $Q = \{1, 2, \dots, n\}$, be a quasigroup. By a *spin* of a quasigroup $Q(\cdot)$ we mean a permutation

$$\varphi_{ij} = \varphi_i \varphi_j^{-1} = \varphi_i \lambda_j \, ,$$

where φ_i and λ_j are right and left tracks of $Q(\cdot)$ respectively.

Obviously $\varphi_{ii} = \varepsilon$ for $i \in Q$ and $\varphi_{ij} \neq \varphi_{ik}$ for $j \neq k$, but the situation where $\varphi_{ij} = \varphi_{kl}$ for some $i, j, k, l \in Q$ also is possible (cf. [6]). Hence the collection Φ of all spins of a given quasigroup $Q(\cdot)$ can be divided into disjoint subsets $\Phi_i = \{\varphi_{ij} : j \in Q\}$ (called *spin-basis*) in which all elements are different. Generally, Φ_i are not closed under the composition of permutations but in some cases Φ_i are groups.

In [6] the following result is proved.

Theorem 3.2. *A quasigroup $Q(\cdot)$ is isotopic to some group if and only if its spin-basis Φ_1 is a group.* □

In this case $\Phi_1 = \Phi_i$ for all $i \in Q$.

Theorem 3.3. *In D-loops we have $\Phi = \langle \Phi_1 \rangle = \{\varphi_{1i}\varphi_{1j} : i, j \in Q\}$.*

Proof. Indeed, by Corollary 2.3

$$\varphi_{1i}\varphi_{1j} = \varphi_1 \varphi_i^{-1} \varphi_1 \varphi_j^{-1} = (\varphi_1 \varphi_i^{-1} \varphi_1) \varphi_j^{-1} = \varphi_{i^{-1}} \varphi_j^{-1} = \varphi_{i^{-1}j} \in \Phi$$

and conversely, each $\varphi_{ij} \in \Phi$ can be written in the form $\varphi_{ij} = \varphi_{1i^{-1}}\varphi_{1j}$. □

Corollary 3.4. *A D-loop is isotopic to a group if and only if $\langle \Phi_1 \rangle = \Phi_1$.*

Proof. If a D-loop $Q(\cdot)$ is isotopic to a group, then, by Theorem 3.2, Φ_1 is a group. Hence $\langle \Phi_1 \rangle = \Phi_1$.

Conversely, if $\langle \Phi_1 \rangle = \Phi_1$, then $\varphi_{1i}\varphi_{i1} = \varphi_{11}$ implies $\varphi_{1i}^{-1} = \varphi_{i1} \in \Phi = \langle \Phi_1 \rangle = \Phi_1$ which means that Φ_1 is a group. Thus $Q(\circ)$ is isotopic to some group. □

Corollary 3.5. *A D-loop is isotopic to a group if and only if Φ_1 is closed under a composition of permutations.*

Proof. If a D-loop $Q(\cdot)$ is isotopic to a group, then, by Theorem 3.2, Φ_1 is a group. Hence Φ_1 is closed under a composition of permutations.

Conversely, if Φ_1 is closed under a composition of permutations, then, in view of Theorem 3.3, from $\varphi_{1i}\varphi_{i1} = \varphi_{11}$ it follows $\varphi_{1i}^{-1} = \varphi_{i1} \in \Phi = \langle \Phi_1 \rangle = \Phi_1$, which means that Φ_1 is a group. Thus $Q(\cdot)$ is isotopic to some group. □

Corollary 3.6. *A D-loop $Q(\cdot)$ is isotopic to a group if and only if for all $i, j \in Q$ there exists $k \in Q$ such that $\varphi_i \varphi_1 \varphi_j = \varphi_k$.*

Proof. Indeed, $\varphi_{1j}\varphi_{1i} = \varphi_{1k}$ means that $\varphi_1 \varphi_j^{-1} \varphi_1 \varphi_i^{-1} = \varphi_1 \varphi_k^{-1}$. Thus $\varphi_j^{-1} \varphi_1 \varphi_i^{-1} = \varphi_k^{-1}$. Hence $\varphi_k = \varphi_i \varphi_1 \varphi_j$. □

Theorem 3.7. *If a quasigroup $Q(\cdot)$ is isotopic to a D-loop $Q(\circ)$, then there exists a permutation σ of Q and an element $p \in Q$ and such that*

$$\varphi_p\varphi_i^{-1}\varphi_p = \varphi_{\sigma(i)} \tag{14}$$

for all tracks φ_i of $Q(\cdot)$.

Proof. Let a quasigroup $Q(\cdot)$ be isotopic to a D-loop $Q(\circ)$. Then

$$\gamma(x \cdot y) = \alpha(x) \circ \beta(y) \tag{15}$$

for some permutations α, β, γ of Q. Thus for all $i, x \in Q$ we have

$$\gamma(i) = \gamma(x \cdot \varphi_i(x)) = \alpha(x) \circ \beta\varphi_i(x),$$

where φ_i is a right track of $Q(\cdot)$. Hence

$$\gamma(i) = z \circ \beta\varphi_i\alpha^{-1}(z)$$

for all $i \in Q$ and $z = \alpha(x)$. This together with $\gamma(i) = z \circ \psi_{\gamma(i)}(z)$ gives

$$\beta\varphi_i\alpha^{-1} = \psi_{\gamma(i)},$$

i.e.,

$$\varphi_i = \beta^{-1}\psi_{\gamma(i)}\alpha, \qquad \varphi_i^{-1} = \alpha^{-1}\psi_{\gamma(i)}^{-1}\beta. \tag{16}$$

Thus for $p = \gamma^{-1}(1)$, where 1 is the identity of $Q(\circ)$, we obtain

$$\varphi_p\varphi_i^{-1}\varphi_p = (\beta^{-1}\psi_1\alpha)(\alpha^{-1}\psi_{\gamma(i)}^{-1}\beta)(\beta^{-1}\psi_1\alpha) = \beta^{-1}(\psi_1\psi_{\gamma(i)}^{-1}\psi_1)\alpha.$$

Since $Q(\circ)$ is a D-loop, for $k = \gamma^{-1}\psi_1\gamma(i)$, by Corollary 2.3, we have

$$\beta^{-1}(\psi_1\psi_{\gamma(i)}^{-1}\psi_1)\alpha = \beta^{-1}\psi_{\gamma(i)^{-1}}\alpha = \beta^{-1}\psi_{\psi_1\gamma(i)}\alpha = \beta^{-1}\psi_{\gamma(k)}\alpha = \varphi_k.$$

So, $\varphi_p\varphi_i^{-1}\varphi_p = \varphi_k$, which means that (14) is valid for $\sigma = \gamma^{-1}\psi_1\gamma$. □

The converse statement is more complicated.

Theorem 3.8. *Let a quasigroup $Q(\cdot)$ and a loop $Q(\circ)$ with the identity 1 be isotopic, i.e., let (15) holds. If φ_i are tracks of $Q(\cdot)$, ψ_i – tracks of $Q(\circ)$ and (14) is satisfied for $p = \gamma^{-1}(1)$, $\sigma = \gamma^{-1}\psi_1\gamma$ and all $i \in Q$, then $Q(\circ)$ is a D-loop.*

Proof. Indeed, (15) holds, then for $p = \gamma^{-1}(1)$ and any $i \in Q$, in view of (16), we have

$$\begin{aligned}\psi_1\psi_i^{-1}\psi_1 &= (\beta\varphi_{\gamma^{-1}(1)}\alpha^{-1})(\alpha\varphi_{\gamma^{-1}(i)}^{-1}\beta^{-1})(\beta\varphi_{\gamma^{-1}(1)}\alpha^{-1}) = \beta(\varphi_p\varphi_{\gamma^{-1}(i)}^{-1}\varphi_p)\alpha^{-1}\\ &= \beta\varphi_{\sigma(\gamma(i))}\alpha^{-1} = \beta\varphi_{\gamma^{-1}\varphi_1(i)}\alpha^{-1} = \psi_{\psi_1(i)} = \psi_{i^{-1}},\end{aligned}$$

where i^{-1} is calculated in $Q(\circ)$.

Thus $\psi_1\psi_i^{-1}\psi_1 = \psi_{i^{-1}}$, which means that $Q(\circ)$ is a D-loop. □

Lemma 3.9. *A loop $Q(\circ)$ is a principal isotope of a quasigroup $Q(\cdot)$ if and only if*

$$x \circ y = R_b^{-1}(x) \cdot L_a^{-1}(y),$$

for some $a, b \in Q$ such that $a \cdot b = 1$, where 1 is the identity of $Q(\circ)$ and L_a, R_b are translations of $Q(\cdot)$.

Proof. Indeed, if $Q(\circ)$ is a loop with the identity 1 and $x \circ y = \alpha(x) \cdot \beta(y)$ for some permutations α, β of Q, then for $a = \alpha(1)$, $b = \beta(1)$ we have

$$1 = 1 \circ 1 = \alpha(1) \cdot \beta(1) = a \cdot b,$$
$$x = x \circ 1 = \alpha(x) \cdot \beta(1) = \alpha(x) \cdot b,$$
$$y = 1 \circ y = \alpha(1) \cdot \beta(y) = a \cdot \beta(y).$$

Thus

$$\alpha(x) = R_b^{-1}(x), \qquad \beta(y) = L_a^{-1}(y).$$

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

The converse statement is obvious. □

Corollary 3.10. *A quasigroup $Q(\cdot)$ is a principal isotope of a loop $Q(\circ)$ with the identity 1 if and only if*

$$x \cdot y = R_b(x) \circ L_a(y),$$

for some translations L_a, R_b of $Q(\cdot)$ such that $a \cdot b = 1$. □

Proposition 3.11. *In any principal isotope $Q(\cdot)$ of a D-loop $Q(\circ)$ with the identity 1 we have*

$$\varphi_1 \varphi_i^{-1} \varphi_1 = \varphi_{i^{-1}},$$

where i^{-1} is calculated in $Q(\circ)$.

Proof. It is a consequence of (15) and (16). □

Corollary 3.12. *A principal isotope $Q(\cdot)$ of a D-loop $Q(\circ)$ is a D-loop if and only if $Q(\cdot)$ and $Q(\circ)$ have the same inverse elements.* □

Corollary 3.13. *A principal isotope $Q(\cdot)$ of a D-loop $Q(\circ)$ is a D-loop if and only if $Q(\cdot)$ and $Q(\circ)$ have the same tracks induced by the identity of $Q(\circ)$, i.e., if and only if φ_1 and ψ_1, where 1 he identity of $Q(\circ)$.* □

4. Proper D-loops

A *D*-loop is *proper* if it is not an IP-loop. The smallest *D*-loop has six elements. Below we present a full list of all nonisotopic proper *D*-loops of order 6. They represent (respectively) the classes 8.1.1, 9.1.1, 10.1.1 and 11.1.1 mentioned in the book [4].

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	6	5	3	4
3	3	6	1	2	4	5
4	4	5	2	1	6	3
5	5	3	4	6	1	2
6	6	4	5	3	2	1

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	6	4	5
3	3	1	2	5	6	4
4	4	6	5	1	2	3
5	5	4	6	2	3	1
6	6	5	4	3	1	2

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	6	5	4	3
3	3	5	1	2	6	4
4	4	6	2	1	3	5
5	5	3	4	6	2	1
6	6	4	5	3	1	2

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	5	6	3
3	3	4	2	6	1	5
4	4	5	6	2	3	1
5	5	6	1	3	2	4
6	6	3	5	1	4	2

References

[1] **R. Artzy**, *On automorphic-inverse properties in loops*, Proc. Amer. Math. Soc. **10** (1959), 588 – 591.

[2] **V.D. Belousov**, *On the group associated with a quasigroup*, (Russian), Mat. Issled. **4** (1969), 21 – 39.

[3] **R.H. Bruck**, *What is a loop?*, Studies in modern algebra, New Jersey, 1963.

[4] **J. Dénes and A.D. Keedwell**, *Latin squares and their applications*, Akademiai Kiado, Budapest, 1974.

[5] **I.I. Deriyenko**, *Necessary conditions of the isotopy of finite quasigroups*, (Russian), Mat. Issled. **120** (1991), 51 – 63.

[6] **I.I. Deriyenko**, *On middle translations of finite quasigroups*, Quasigroups and Related Systems **16** (2008), 17 – 24.

[7] **I.I. Deriyenko**, *Indicators of quasigroups*, Quasigroups and Related Systems **19** (2011), 223 – 226.

Received September 23, 2012

I.I. Deriyenko
Department of Higher Mathematics and Informatics, Kremenchuk State Polytechnic University,
20 Pervomayskaya str.,39600 Kremenchuk, Ukraine
E-mail: ivan.deriyenko@gmail.com

W.A. Dudek
Institute of Mathematics and Computer Science, Wroclaw University of Technology,
Wyb. Wyspiańskiego 27, 50-370 Wroclaw, Poland
E-mail: Wieslaw.Dudek@pwr.wroc.pl

Quasigroups and Related Systems **20** (2012), 197 − 202

Prime and weakly prime ideals in semirings

Manish Kant Dubey

Abstract. We study the concept of subtractive prime and weakly prime ideals in a semiring and prove some results analogous to ring theory.

1. Introduction

The notion of a semiring was first introduced by H. S. Vandiver in 1935. After that several authors have generalized and characterized the results in many ways. By a *semiring*, we mean a semigroup $(S, \cdot)$ and a commutative monoid $(S, +, 0)$ in which 0 is the additive identity and $s \cdot 0 = 0 \cdot s = 0$ for all $s \in S$, both are connected by ring-like distributivity. In this paper, all semirings are considered to be semirings with zero.

A nonempty subset I of a semiring S is called an (*left, right*) *ideal* if $a, b \in I$ and $s \in S$ implies $a + b \in I$ and ($sa \in I$, $as \in I$ respectively) $as \in S$ and $sa \in I$. A *subtractive ideal* I of S is an ideal such that if $a, a + b \in I$ then $b \in I$.

For the remaining definition of a semiring we refer [6].

2. Weakly prime ideals

D. D. Anderson and E. Smith [3] have introduced and studied the concept of a weakly prime ideal of an associative ring with unity. After that several authors have focused on the study of this concept to extend the results to commutative ring and commutative semiring theory.

Definition 2.1. A proper ideal P of a semiring S is said to be *prime* if $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$ for any ideals A, B of S.

Definition 2.2. A proper ideal P of a semiring S is said to be *weakly prime* if $\{0\} \neq AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$ for any ideals A and B of S.

It is clear that every prime ideal is weakly prime. If S be a semiring with zero, then $I = \{0\}$ is a weakly prime ideal of S. It is easy to see that in Z_6 an ideal $I = \{0\}$ is weakly prime but not prime.

2010 Mathematics Subject Classification: 16Y60
Keywords: Subtractive ideal, prime ideal, weakly prime ideal.

Definition 2.3. An element s in a semiring S is said to be *nilpotent* if there exists a positive integer n (depending on s), such that $s^n = 0$ for $s \in S$. *Nil* S denote the set of all nilpotent element of S. An ideal I in a semiring S is said to be *nilpotent* if there exists a positive integer n (depending on I), such that $I^n = 0$.

Theorem 2.4. *Let I be a subtractive ideal in a semiring S with $1 \neq 0$. The following statements are equivalent:*

(i) *I is a weakly prime ideal.*

(ii) *If A, B are right (left) ideals of S such that $\{0\} \neq AB \subseteq I$, then $A \subseteq I$ or $B \subseteq I$.*

(iii) *If $a, b \in S$ such that $\{0\} \neq aSb \subseteq I$, then $a \in I$ or $b \in I$.*

Proof. $(i) \Rightarrow (ii)$ Suppose that I is a weakly prime ideal of S and A, B are two right (left) ideals of S such that $\{0\} \neq AB \subseteq I$. Let $\langle A \rangle, \langle B \rangle$ be the ideals generated by A, B respectively. Then $\{0\} \neq \langle A \rangle \langle B \rangle \subseteq I$ implies $\langle A \rangle \subseteq I$ or $\langle B \rangle \subseteq I$ and $A \subseteq \langle A \rangle \subseteq I$ or $B \subseteq \langle B \rangle \subseteq I$. Therefore $A \subseteq I$ or $B \subseteq I$.

$(ii) \Rightarrow (iii)$ Let $\{0\} \neq aSb \subseteq I$. Since S has an identity, therefore $\{0\} \neq (aS)(bS) \subseteq I$ implies $a \in aS \subseteq I$ or $b \in bS \subseteq I$.

$(iii) \Rightarrow (i)$ Suppose that $AB \subseteq I$ for ideals A and B of S, where $A \nsubseteq I$ and $B \nsubseteq I$. Let $a \in A \setminus I$, $b \in B \setminus I$. Also let $a' \in A \cap I$, $b' \in B \cap I$ be chosen arbitrary. Since $a + a', b + b' \notin I$, we must have $\{0\} = (a + a')S(b + b')$. Now if we are letting $a' = 0$ or $b' = 0$ or $a' = 0$ and $b' = 0$ and considering all combinations we get $0 = ab = a'b = a'b' = a'b'$ and hence $AB = \{0\}$. □

Proposition 2.5. *Every ideal of a semiring S is weakly prime if and only if for any ideals A, B in S, we have $AB = A$, $AB = B$, or $AB = 0$.*

Proof. Assume that every ideal of S is weakly prime. Let A, B be ideals of S. Suppose $AB \neq S$. Then AB is weakly prime. If $\{0\} \neq AB \subseteq AB$; then we have $A \subseteq AB$ or $B \subseteq AB$ (since AB is weakly prime ideal of S), that is, $A = AB$ or $B = AB$. If $AB = S$, then we have $A = B = S$ whence $S^2 = S$. Conversely, let I be any proper ideal of S and suppose that $\{0\} \neq AB \subseteq I$ for ideals A and B of S. Then we have either $A = AB \subseteq I$ or $B = AB \subseteq I$. □

Now we can easily prove the following results based on the above proposition. *Let S be a semiring in which every ideal of S is weakly prime. Then for any ideal A of S, we have either $A^2 = A$ or $A^2 = 0$.*

Lemma 2.6. *Let P be a subtractive ideal of semiring S. Let P be a weakly prime ideal but not a prime ideal of semiring S. Suppose $ab = 0$ for some $a, b \notin P$, then we have $aP = Pb = \{0\}$.*

Proof. Suppose $ap_1 \neq 0$, for some $p_1 \in P$. Then $0 \neq a(b + p_1) \in P$. Since P is a weakly prime ideal of S, therefore $a + p_1 \in P$ or $b \in P$, that is, $a \in P$ or $b \in P$, a contradiction. Therefore $aP = \{0\}$. Similarly, we can show that $Pb = \{0\}$ □

Theorem 2.7. *Suppose that P is a subtractive ideal in a semiring S. If P is weakly prime but not prime, then $P^2 = \{0\}$.*

Proof. Suppose that $p_1p_2 \neq 0$ for some $p_1, p_2 \in P$ and $ab = 0$ for some $a, b \notin P$, where P is not a prime ideal of S. Then by Lemma 2.6 we have $(a+p_1)(b+p_2) = p_1p_2 \neq 0$. Hence either $(a+p_1) \in P$ or $(b+p_2) \in P$, and thus either $a \in P$ or $b \in P$, a contradiction. Hence $P^2 = \{0\}$. □

Corollary 2.8. *Let P be a weakly prime ideal of S. If P is not a prime ideal of S, then $P \subseteq Nil\, S$.*

A subtractive ideal in a commutative semiring S satisfying $P^2 = \{0\}$ may not be weakly prime.

Example 2.9. Let $S = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in Z_{12}^{+}\right\}$. Then S is a commutative semiring and $P = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 0 \end{pmatrix}\right\}$ is its ideal such that $P^2 = \{0\}$. In this semiring $\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} \in P$ but $\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \notin P$ and $\begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} \notin P$. Therefore P is not a weakly prime ideal of S.

Theorem 2.10. *Let P be a weakly subtractive prime ideal of a commutative semiring S that is not prime. Then if $z \in Nil\, S$, then either $z \in P$ or $zP = \{0\}$.*

Proof. Let $z \in$*Nil S*. To show that if $zP \neq \{0\}$, then $z \in P$, suppose that $zP \neq \{0\}$. Let n be the least positive integer such that $z^n = 0$. Then for $n \geqslant 2$ and for some $p \in P$ we have $0 \neq z(p + z^{n-1}) = zp \in P$. Hence either $z \in P$ or $(p + z^{n-1}) \in P$. If $z \in P$ then nothing to prove. So let $(p + z^{n-1}) \in P$. Then $z^{n-1} \in P$ and thus $z \in P$. Hence for each $z \in$ *Nil S*, we have either $z \in P$ or $zP = \{0\}$. Again we suppose that $z \notin P$ for some $z \in$ *Nil S*. Then we will show that $zP = \{0\}$. Now let $zp \neq 0$ for some $p \in P$. Let n be the least positive integer such that $z^n = 0$. Since $z \notin P, n \geqslant 2$ and $zP \neq 0$. Hence $z(z^{n-1}+p) = zp \neq 0$. Since $0 \neq z(z^{n-1} + p) \in P$, therefore we have either $z \in P$ or $z^{n-1} \neq 0$ and $z^{n-1} \in P$. Hence in both cases, we have $z \in P$, a contradiction. Thus $zP = \{0\}$. □

3. Prime ideals

The following lemma is obvious.

Lemma 3.1. *Let f be a homomorphism of semiring S_1 onto a semiring S_2. Then each of the following is true:*

- (*i*) *If I is an ideal* (*subtractive ideal*) *in S_1, then $f(I)$ is an ideal* (*subtractive ideal*) *in S_2.*

(*ii*) *If J is an ideal (subtractive ideal) in S_2, then $f^{-1}(J)$ is an ideal (subtractive ideal) in S_1.*

Proposition 3.2. *If $f : S_1 \to S_2$ is a homomorphism of semirings and P is a prime ideal in S_2, then $f^{-1}(P)$ is a prime ideal in S_1.*

Proof. By Lemma $f^{-1}(P)$ is an ideal of S_1. Let $xy \in f^{-1}(P)$. Then $f(xy) \in P$ implies $f(x)f(y) \in P$. Since P is a prime ideal of S_2 therefore it follows that either $f(x) \in P$ or $f(y) \in P$ and thus either $x \in f^{-1}(P)$ or $y \in f^{-1}(P)$. Hence $f^{-1}(P)$ is a prime ideal of S_1. □

Theorem 3.3. *Let I be an arbitrary ideal of a semiring S and $P_1, P_2, \ldots, P_n$ be subtractive prime ideals of S. If $I \nsubseteq P_i$ for all i, then there exists an element $a \in I such$ that $a \notin \bigcup P_i$. Hence, $I \nsubseteq \bigcup P_i$.*

Proof. We will prove it by induction. Clearly the result is true for $n = 1$. Suppose that the theorem holds for $n-1$ subtractive prime ideals. Then, for each i, where $1 \leqslant i \leqslant n$, there exists $x_i \in I$ with $x_i \notin \bigcup_{j \neq i} P_j$. If $x_i \notin P_i$, then $x_i \notin \cup P_j$ and then we are done. Now suppose that $x_i \in P_i$ for all i. Let $a_i = x_1 \cdots x_{i-1}x_{i+1} \cdots x_n$. We claim that $a_i \notin P_i$. Suppose $a_i \in P_i$ and since P_i is prime therefore $x_j \in P_i$ for some $j \neq i$, which is not possible by original choice of x_j. If $j \neq i$, then the element $a_j \in P_i$ because x_i being a factor of a_j. Consider $a = \sum_{j=1}^{n} a_j$. Since each $a_j \in I$ where $1 \leqslant j \leqslant n$, therefore $a \in I$. As $a = a_i + \sum_{j \neq i} a_j$ with $\sum_{j \neq i} a_j \in P_i$ implies that $a \in P_i$; otherwise we would obtain $a_i \in P_i$ (as P_i is a subtractive ideal), which is a contradiction. Thus we get an existence of an element $a = \sum a_j \in I$ and $a \notin P_i$, which proves the theorem. □

Corollary 3.4. *Let I be an arbitrary ideal of a semiring S and $P_1, P_2, \ldots, P_n$ be subtractive prime ideals of S. If $I \subseteq \bigcup P_i$, then $I \subseteq P_i$ for some I.*

Theorem 3.5. *Let I be a subset of a commutative semiring S which is closed under addition and multiplication.*

(*i*) *Let $P_1, \ldots, P_n$ be subtractive ideals in S, at least $n-2$ of which are primes. If $I \subseteq P_1 \cup \ldots \cup P_n$, then I is contained in some P_i.*

(*ii*) *Let J be an ideal of S with $J \subset I$. If there are subtractive prime ideals $P_1, \ldots, P_n$ such that $I \setminus J \subseteq P_1 \cup \ldots \cup P_n$, then $I \subseteq P_i$ for some i.*

Proof. (*i*) The proof is by induction $n \geqslant 2$. If we consider $n = 2$, that is, $I \subseteq P_1 \cup P_2$ implies $I \subseteq P_1$ or $I \subseteq P_2$. In this case P_1 and P_2 need not be prime because if $I \nsubseteq P_2$, then there is $x_1 \in I$ with $x_1 \notin P_2$; since $I \subseteq P_1 \cup P_2$, we must have $x_1 \in P_1$. Similarly, if $I \nsubseteq P_1$, there is $x_2 \in I$ with $x_2 \notin P_1$ and $x_2 \in P_2$. However, if $a = x_1 + x_2$, then $a \notin P_1$ (because if $a \in P_1$ then $x_2 \in P_1$), a contradiction. Similarly, $a \notin P_2$ which contradicts to fact that $I \subseteq P_1 \cup P_2$.

Now assume that $I \subseteq P_1 \cup \ldots \cup P_{n+1}$, where at least $n-1 = (n+1)-2$ of the P_i are prime ideals. Let $M_i = P_1 \cup \ldots \cup P_{i-1} \cup P_{i+1} \ldots \cup P_{n+1}$. Since M_i is union of n ideals at least $(n-1)-1=n-2$ of which are prime. By the hypothesis we can suppose that $I \nsubseteq M_i$ for all i. Thus, for all i, there exist $x_i \in I$ with $x_i \notin M_i$; since $I \subseteq M_i \cup P_i$ therefore we must have $x_i \in P_i$. Now $n \geqslant 3$, so that at least one of the P_i are prime ideals; without loss of generality assume that P_1 is prime. Consider the element $a = x_1 + x_2 x_3 \cdots x_{n+1}$. Since all $x_i \in I$ and I is closed under addition and multiplication and $a \in I$. Now $a \notin P_1$ because if $a \in P_1$ then $x_2 \cdots x_{n+1} \in P_1$ (as P_1 is subtractive). Since P_1 is a prime ideal in S therefore some $x_i \in P_1$. This is a contradiction, for $x_i \notin P_1 \subseteq M_i$. If $i > 1$ and $a \in P_i$, then $x_2 x_3 \cdots x_{n+1} \in P_i$, because P_i is an subtractive ideal and so $x_1 \in P_i$. This cannot be, for $x_1 \notin P_i \subseteq M_1$. Therefore, $a \notin P_i$ for any i, contradicting to fact that $I \subseteq P_1 \cup \ldots \cup P_{n+1}$.

(ii) By hypothesis, we have $I \subseteq J \cup P_1 \cup \ldots \cup P_n$. Therefore (i) gives $I \subseteq J$ or $I \subseteq P_i$. Since J is a proper subset of I therefore $I \nsubseteq J$. Hence we must have $I \subseteq P_i$. □

Let I be an ideal of a commutative semiring S. Then the *radical* of I, denoted by $\sqrt{I}$, is defined as the set

$$\sqrt{I} = \{x \in S : x^n \in I \quad \text{for some positive integer}\, n\}.$$

This is an ideal of S containing I, and it is the intersection of all prime ideals of S containing I [2]. It is easy to see that if an ideal I is subtractive then $\sqrt{I}$ is subtractive.

Definition 3.6. An ideal I of the commutative semiring S is said to be *semiprime* if and only if $I = \sqrt{I}$.

Subtractive semiprime ideals of semirings are characterized by the following theorem.

Theorem 3.7. *An subtractive ideal I of a commutative semiring S is semiprime if and only if the quotient semiring S/I has no nonzero nilpotent elements.*

Proof. Suppose that a subtractive ideal I of a semiring S is semiprime. Let $a+\sqrt{I}$ be a nilpotent element of $S/\sqrt{I}$. Then there exists some positive integer $n \in Z^+$ such that $(a+\sqrt{I})^n = a^n + \sqrt{I} = \sqrt{I}$. As $\sqrt{I}$ is subtractive therefore $a^n \in \sqrt{I}$. Hence, $(a^n)^m = a^{nm} \in I$ for some positive integer m. This shows that $a \in I$. Therefore we have $a + \sqrt{I} = \sqrt{I}$, the zero element of $S/\sqrt{I}$.

Conversely, suppose that S/I has no nonzero nilpotent elements and let $a \in \sqrt{I}$. Then for some positive integer n, we have $a^n \in I$. This implies that $(a+I)^n = I$, that is, $a+I$ is nilpotent in S/I. As $a+I = I$ (by hypothesis), therefore $a \in I$. Thus, we have $\sqrt{I} \subseteq I$. The inclusion $I \subseteq \sqrt{I}$ is obvious. Hence $I = \sqrt{I}$, so I is semiprime. □

References

[1] **P.J. Allen**, *A fundamental theorem of homomorphisms for semirings*, Proc. Amer. Math. Soc. **21** (1969), 412 – 416.

[2] **P.J. Allen and J. Neggers**, *Ideal theory in commutative semirings*, Kyungpook Math. J. **46** (2006), 261 – 271.

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

[4] **S.E. Atani**, *The ideal theory in quotient of commutative semirings*, Glasnik Mat. **42(62)** (2007), 301 – 308.

[5] **D.M. Burton**, *A first course in rings and ideals*, Addition-Wesley Publishing Company, (1970).

[6] **J.S. Golan**, *Semirings and their applications*, Kluwer Academic Publishers, Dordrecht, (1999).

[7] **Y. Hirano, E. Poon, and H. Tsutsui**, *On rings in which every ideal is weakly prime*, Bull. Korean Math. Soc. 47 (2010), 1077 – 1087.

[8] **D.R. LaTorre**, *A note on quotient semirings*, Proc. Amer. Math. Soc. 24 (1970), 463465.

Received March 2, 2012

SAG, DRDO, Metcalfe House Complex
Near civil lines
Delhi-110054
India
E-mail: kantmanish@yahoo.com

Quasigroups and Related Systems **20** (2012), 203 − 209

Congruences on completely inverse AG^{**}-groupoids

Wieslaw A. Dudek and *Roman S. Gigoń*

Abstract. By a completely inverse AG^{**}-groupoid we mean an inverse AG^{**}-groupoid A satisfying the identity $xx^{-1} = x^{-1}x$, where x^{-1} denotes a unique element of A such that $x = (xx^{-1})x$ and $x^{-1} = (x^{-1}x)x^{-1}$. We show that the set of all idempotents of such groupoid forms a semilattice and the Green's relations $\mathcal{H}, \mathcal{L}, \mathcal{R}, \mathcal{D}$ and $\mathcal{J}$ coincide on A. The main result of this note says that any completely inverse AG^{**}-groupoid meets the famous Lallement's Lemma for regular semigroups. Finally, we show that the Green's relation $\mathcal{H}$ is both the least semilattice congruence and the maximum idempotent-separating congruence on any completely inverse AG^{**}-groupoid.

1. Preliminaries

By an *Abel-Grassmann's groupoid* (briefly an *AG-groupoid*) we shall mean any groupoid which satisfies the identity

$$xy \cdot z = zy \cdot x. \tag{1}$$

Such groupoid is also called a *left almost semigroup* (briefly an *LA-semigroup*) or a *left invertive groupoid* (cf. [2], [3] or [5]). This structure is closely related to a commutative semigroup, because if an AG-groupoid contains a right identity, then it becomes a commutative monoid. Moreover, if an AG-groupoid A with a left zero z is finite, then (under certain conditions) $A \setminus \{z\}$ is a commutative group (cf. [6]).

One can easily check that in an arbitrary AG-groupoid A, the so-called *medial law* is valid, that is, the equality

$$ab \cdot cd = ac \cdot bd \tag{2}$$

holds for all $a, b, c, d \in A$.

Recall from [11] that an *AG-band* A is an AG-groupoid satisfying the identity $x^2 = x$. If in addition, $ab = ba$ for all $a, b \in A$, then A is called an *AG-semilattice.*

Let A be an AG-groupoid and $B \subseteq A$. Denote the set of all idempotents of B by E_B, that is, $E_B = \{b \in B : b^2 = b\}$. From (2) follows that if $E_A \neq \emptyset$, then $E_A E_A \subseteq E_A$, therefore, E_A is an AG-band.

2010 Mathematics Subject Classification: 20N02, 06B10
Keywords: completely inverse AG^{**}-groupoid, AG-group, LA-semigroup, congruence, Green's relation.

Further, an AG-groupoid satisfying the identity

$$x \cdot yz = y \cdot xz \tag{3}$$

is said to be an AG^{**}*-groupoid*. Every AG^{**}-groupoid is *paramedial* (cf. [1]), i.e., it satisfies the identity

$$ab \cdot cd = db \cdot ca. \tag{4}$$

Notice that each AG-groupoid with a left identity is an AG^{**}-groupoid (see [1], too). Furthermore, observe that if A is an AG^{**}-groupoid, then (4) implies that if $E_A \neq \emptyset$, then it is an AG-semilattice. Indeed, in this case E_A is an AG-band and $ef = ee \cdot ff = fe \cdot fe = fe$ for all $e, f \in E_A$. Moreover, for $a, b \in A$ and $e \in E_A$, we have

$$e \cdot ab = ee \cdot ab = ea \cdot eb = e(ea \cdot b) = e(ba \cdot e) = ba \cdot ee = ba \cdot e = ea \cdot b,$$

that is,

$$e \cdot ab = ea \cdot b \tag{5}$$

for all $a, b \in A$ and $e \in E_A$. Thus, as a consequence, we obtain

Proposition 1.1. *The set of all idempotents of an* AG^{**}*-groupoid is either empty or a semilattice.*

We say that an AG-groupoid A with a left identity e is an *AG-group* if each of its elements has a *left inverse* a', that is, for every $a \in A$ there exists $a' \in A$ such that $a'a = e$. It is not difficult to see that such element a' is uniquely determined and $aa' = e$. Therefore an AG-group has exactly one idempotent.

Let A be an arbitrary groupoid, $a \in A$. Denote by $V(a)$ the set of all *inverses* of a, that is,

$$V(a) = \{a^* \in A : a = aa^* \cdot a,\ a^* = a^*a \cdot a^*\}.$$

An AG-groupoid A is called *regular* (in [1] it is called *inverse*) if $V(a) \neq \emptyset$ for all $a \in A$. Note that AG-groups are of course regular AG-groupoids, but the class of all regular AG-groupoids is vastly more extensive than the class of all AG-groups. For example, every AG-band A is regular, since $a = aa \cdot a$ for all $a \in A$. In [1] it has been proved that in any regular AG^{**}-groupoid A we have $|V(a)| = 1$ $(a \in A)$, so we call it an *inverse* AG^{**}*-groupoid*. In this case, we denote a unique inverse of $a \in A$ by a^{-1}. Notice that $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in A$. Further, one can prove that in an inverse AG^{**}-groupoid A, we have $aa^{-1} = a^{-1}a$ if and only if $aa^{-1}, a^{-1}a \in E_A$ (cf. [1]).

Many authors studied various congruences on some special classes of AG^{**}-groupoids and described the corresponding quotient algebras as semilattices of some subgroupoids (see for example [1, 5, 7, 8, 9, 10]). Also, in [1, 9] the authors studied congruences on inverse AG^{**}-groupoids satisfying the identity $xx^{-1} =$

$x^{-1}x$. We will be called such groupoids *completely inverse AG^{**}-groupoids.* A simple example of such AG^{**}-groupoid is an AG-group. In the light of Proposition 1.1, the set of all idempotents of any completely inverse AG^{**}-groupoid forms a semilattice.

A nonempty subset B of a groupoid A is called a *left ideal* of A if $AB \subseteq B$. The notion of a *right ideal* is defined dually. Also, B is said to be an *ideal* of A if it is both a left and right ideal of A. It is clear that for every $a \in A$ there exists the least left ideal of A containing the element a. Denote it by $L(a)$. Dually, $R(a)$ is the least right ideal of A containing the element a. Finally, $J(a)$ denotes the least ideal of A containing $a \in A$.

In a similar way as in semigroup theory we define the *Green's equivalences* on an AG-groupoid A by putting:

$$\begin{gathered} a\,\mathcal{L}\,b \iff L(a) = L(b), \\ a\,\mathcal{R}\,b \iff R(a) = R(b), \\ a\,\mathcal{J}\,b \iff J(a) = J(b), \\ \mathcal{H} = \mathcal{L} \cap \mathcal{R}, \quad \mathcal{D} = \mathcal{L} \vee \mathcal{R}. \end{gathered}$$

2. The main results

Let A be a completely inverse AG^{**}-groupoid. Then

$$a = (aa^{-1})a \in Aa$$

for every $a \in A$.

Proposition 2.1. *Let A be a completely inverse AG^{**}-groupoid, $a \in A$. Then:*
(a) $aA = Aa$;
(b) $aA = L(a) = R(a) = J(a)$;
(c) $\mathcal{H} = \mathcal{L} = \mathcal{R} = \mathcal{D} = \mathcal{J}$;
(d) $aA = (aa^{-1})A$;
(e) $aA = a^{-1}A$;
(f) $eA = fA$ *implies* $e = f$ *for all* $e, f \in E_A$.

Proof. (a). Let $b \in A$. Then

$$ab = (aa^{-1})a \cdot b = ba \cdot aa^{-1} = ba \cdot a^{-1}a = aa \cdot a^{-1}b = (a^{-1}b \cdot a)a \in Aa.$$

Thus $aA \subseteq Aa$. Also,

$$ba = b \cdot (aa^{-1})a = aa^{-1} \cdot ba = ab \cdot a^{-1}a = ab \cdot aa^{-1} = a(ab \cdot a^{-1}) \in aA,$$

so $Aa \subseteq aA$. Consequently, $aA = Aa$.

(b). Obviously, it is sufficient to show that $aA = Aa$ is an ideal of A. Let $x = ab \in aA$ and $c \in A$. Then we have $cx = c(ab) = a(cb) \in aA$ and $xc = (ab)c = (cb)a \in Aa = aA$.

(c). It follows from (b).

(d). Let $b \in A$. Then $ab = (aa^{-1})a \cdot b = ba \cdot aa^{-1} \in A(aa^{-1}) = (aa^{-1})A$, that is, $aA \subseteq (aa^{-1})A$. Furthermore, $(aa^{-1})b = (ba^{-1})a \in Aa = aA$. Thus $(aa^{-1})A \subseteq aA$. Consequently, the condition (d) holds.

(e). By (d), $aA = (aa^{-1})A = (a^{-1}a)A = (a^{-1}(a^{-1})^{-1})A = a^{-1}A$.

(f). Let $e, f \in E_A$ and $eA = fA$. Then $e \in fA$, that is, $e = fa$ for some $a \in A$. Hence $fe = f(fa) = (ff)a$ (by Proposition 1.1), and so $fe = e$. Similarly, $ef = f$. Since E_A is a semilattice, $e = f$. □

Corollary 2.2. *Let A be a completely inverse AG^{**}-groupoid. Then each left ideal of A is also a right ideal of A, and vice versa. In particular,*

$$L \cap R = LR$$

for every (left) ideal L and every (right) ideal R.

Proof. Let L be a left ideal of A and $l \in L$. Then $lA = Al \subseteq L$. It follows that

$$L = \bigcup \{lA : l \in L\}.$$

Since each component lA of the above set-theoretic union is a right ideal of A, then L is itself a right ideal of A. Similar arguments show that every right ideal of A is a left ideal.

Clearly, $LR \subseteq L \cap R$. Conversely, if $a \in L \cap R$, then $a = (aa^{-1})a \in LR$. Hence $L \cap R = LR$. □

Let A be a completely inverse AG^{**}-groupoid. Denote by $\mathcal{H}_a$ the equivalence $\mathcal{H}$-class containing the element $a \in A$. We say that $\mathcal{H}_a \leq \mathcal{H}_b$ if and only if $aA \subseteq bA$.

The following theorem is the main result of this paper.

Theorem 2.3. *If ρ is a congruence on a completely inverse AG^{**}-groupoid A and $a\rho \in E_{A/\rho}$ $(a \in A)$, then there exists $e \in E_{a\rho}$ such that $\mathcal{H}_e \leq \mathcal{H}_a$.*

Proof. Let ρ be a congruence on A, $a \in A$ and $a\rho a^2$. We know that there exists $x \in A$ such that $a^2 = a^2x \cdot a^2$, $x = xa^2 \cdot x$ and $a^2x = xa^2 \in E_A$. Notice that

$$a^2x \cdot aa = a(a^2x \cdot a) = a(xa^2 \cdot a) = a(aa^2 \cdot x) = aa^2 \cdot ax = a^2 \cdot a^2x = a^2 \cdot xa^2,$$

i.e., $a^2 = a^2 \cdot xa^2$. Put $e = a \cdot xa$. Then $e\,\rho\,(a^2 \cdot xa^2) = a^2\,\rho\,a$. Hence $e \in a\rho$. Also,

$$e^2 = (a \cdot xa)(a \cdot xa) = a((a \cdot xa) \cdot xa) = a(ax \cdot (xa \cdot a)) = a(ax \cdot a^2x).$$

Further,

$$ax \cdot a^2x = ax \cdot xa^2 = a^2x \cdot xa = xa^2 \cdot xa = (xa^2 \cdot x)a$$

by (5), since $xa^2 \in E_A$. Hence $ax \cdot a^2x = xa$. Consequently,

$$e^2 = a \cdot xa = e \in E_A.$$

Thus, $e \in E_{a\rho}$.

Finally, let $b \in A$. Then $eb = (a \cdot xa)b = (b \cdot xa)a \in Aa = aA$, therefore, $eA \subseteq aA$, so $\mathcal{H}_e \leq \mathcal{H}_a$. □

We say that a congruence ρ on a groupoid A is *idempotent-separating* if $e\rho f$ implies that $e = f$ for all $e, f \in E_A$. Furthermore, ρ is a *semilattice* congruence if A/ρ is a semilattice. Finally, A is said to be a *semilattice A/ρ of AG-groups* if ρ is a semilattice congruence and every ρ-class of A is an AG-group.

Corollary 2.4. *Let A be a completely inverse AG^{**}-groupoid. Then*:

(a) *$\mathcal{H}$ is the least semilattice congruence on A*;

(b) *$\mathcal{H}$ is the maximum idempotent-separating congruence on A*;

(c) *A is a semilattice $A/\mathcal{H} \cong E_A$ of AG-groups $\mathcal{H}_e$ $(e \in E_A)$.*

Proof. (a). Let $aA = bA$ and $c, x \in A$. Then $x \cdot ca = c \cdot xa$. On the other hand,

$$xa \in Aa = aA = bA = Ab,$$

i.e., $xa = yb$, where $b \in A$, so $x \cdot ca = c \cdot yb = y \cdot cb \in A(cb)$. Thus $A(ca) \subseteq A(cb)$. By symmetry, we conclude that $A(ca) = A(cb)$. Moreover, $a = yb$ for some $y \in A$. Hence $ac \cdot x = xc \cdot a = xc \cdot yb = bc \cdot yx \in (bc)A$. Thus $(ac)A \subseteq (bc)A$. In a similar way we can obtain the converse inclusion, so $(ac)A = (bc)A$. Consequently, $\mathcal{H}$ is a congruence (by Proposition 2.1 (b)). In the light of Proposition 2.1 (d), every $\mathcal{H}$-class contains an idempotent of A. This implies that $A/\mathcal{H}$ is a semilattice, that is, $\mathcal{H}$ is a semilattice congruence on A.

Suppose that there is a semilattice congruence ρ on A such that $\mathcal{H} \nsubseteq \rho$. Then the relation $\mathcal{H} \cap \rho$ is a semilattice congruence which is properly contained in $\mathcal{H}$, and so not every $(\mathcal{H} \cap \rho)$-class contains an idempotent of A, since each $\mathcal{H}$-class contains exactly one idempotent (Proposition 2.1 (f)), a contradiction with Theorem 2.3. Consequently, $\mathcal{H}$ must be the least semilattice congruence on A.

(b). By (a) and Proposition 2.1 (f), $\mathcal{H}$ is an idempotent-separating congruence on A. On the other hand, if ρ is an idempotent-separating congruence on A and $(a, b) \in \rho$, then $(a^{-1}, b^{-1}) \in \rho$, so $(aa^{-1}, bb^{-1}) \in \rho$. Hence $aa^{-1} = bb^{-1}$. Let $x \in A$. Then

$$xa = x(aa^{-1} \cdot a) = x(bb^{-1} \cdot a) = bb^{-1} \cdot xa = (xa \cdot b^{-1})b \in Ab.$$

Thus $Aa \subseteq Ab$. By symmetry, we conclude that $Aa = Ab$. Consequently, $a\,\mathcal{H}\,b$ (Proposition 2.1 (b)), that is, $\rho \subseteq \mathcal{H}$, as required.

(c). We show that every $\mathcal{H}$-class of A is an AG-group. In view of the above and Proposition 2.1 $(d),(e)$, each $\mathcal{H}$-class is an AG^{**}-groupoid. Consider an arbitrary $\mathcal{H}$-class $\mathcal{H}_e$ $(e \in E_A)$. Let $a \in \mathcal{H}_e$. Then $aa^{-1} \in \mathcal{H}_e$. Hence $aa^{-1} = e$ and so $ea = a$, that is, e is a left identity of $\mathcal{H}_e$. Since $a^{-1}a = e$ and $a^{-1} \in \mathcal{H}_e$, then $\mathcal{H}_e$ is an AG-group. Obviously, $A/\mathcal{H} \cong E_A$. Consequently, A is a semilattice $A/\mathcal{H} \cong E_A$ of AG-groups $\mathcal{H}_e$ $(e \in E_A)$. □

We say that an ideal K of a groupoid A is the *kernel* of A if K is contained in every ideal of A. If in addition, K is an AG-group, then it is called the *AG-group kernel* of A. Finally, a congruence ρ on A is said to be an *AG-group* congruence if A/ρ is an AG-group.

Corollary 2.5. *Let A be a completely inverse AG^{**}-groupoid. If e is a zero of E_A, then $\mathcal{H}_e = eA$ is the AG-group kernel of A and the map $\varphi : A \to eA$ given by $a\varphi = ea$ $(a \in A)$ is an epimorphism such that $x\varphi = x$ for all $x \in eA$.*

Proof. Obviously, $\mathcal{H}_e \subseteq eA$. Conversely, if $x = ea \in eA$, then

$$xx^{-1} = ea \cdot ea^{-1} = ee \cdot aa^{-1} = e.$$

In a view of Proposition 2.1 (d), $x \in \mathcal{H}_e$. Consequently, $\mathcal{H}_e = eA$. If I is an ideal of A, then clearly $E_I \neq \emptyset$. Let $i \in E_I$. Then $e = ei \in E_I$. Hence $a = ea \in I$ for all $a \in \mathcal{H}_e$, so $\mathcal{H}_e \subseteq I$. Thus $\mathcal{H}_e = eA$ is the AG-group kernel of A. Also, for all $a, b \in A$, $(a\varphi)(b\varphi) = (ea)(eb) = (ee)(ab) = e(ab) = (ab)\varphi$, i.e., φ is a homomorphism of A into eA. Evidently, φ is surjective. Finally, $\varphi_{|eA} = 1_{eA}$ (by Proposition 1.1). □

Corollary 2.6. *Let A be a completely inverse AG^{**}-groupoid. If e is a zero of E_A, then*

$$\sigma = \{(a,b) \in A \times A : ea = eb\}$$

is the least AG-group congruence on A and $A/\sigma \cong \mathcal{H}_e$.

Proof. It is clear that σ is an AG-group congruence on A induced by φ (defined in the previous corollary). If ρ is also an AG-group congruence on A and $a \, \sigma \, b$, then $(e\rho)(a\rho) = (e\rho)(b\rho)$. By cancellation, $a \, \rho \, b$ and so $\sigma \subseteq \rho$. Obviously, $A/\sigma \cong \mathcal{H}_e$. □

Remark 2.7. Let I be an ideal of a completely inverse AG^{**}-groupoid A. The relation $\rho_I = (I \times I) \cup 1_A$ is a congruence on A. If e is a zero of E_A, then $\mathcal{H}_e$ is an ideal of A and $\sigma \cap \rho_{\mathcal{H}_e} = 1_A$. It follows that A is a subdirect product of the group $\mathcal{H}_e$ and the completely inverse AG^{**}-groupoid $A/\mathcal{H}_e$. Note that we may think about $A/\mathcal{H}_e$ as a groupoid $B = (A \setminus \mathcal{H}_e) \cup \{e\}$ with zero e, where all products $ab \in \mathcal{H}_e$ are equal e. In fact, $fg = e$ in A $(f, g \in E_A)$ if and only if $\mathcal{H}_f\mathcal{H}_g \subseteq \{e\} = \mathcal{H}_e$ in B.

Obviously, in any finite completely inverse AG^{**}-groupoid A, the semilattice E_A has a zero.

References

[1] **M. Božinović, P.V. Protić and N. Stevanović**, *Kernel normal system of inverse AG^{**}-groupoids*, Quasigroups and Related Systems **17** (2009), 1 – 8.

[2] **P. Holgate**, *Groupoids satisfying a simple invertive law*, Math. Student **61** (1992), 101 – 104.

[3] **M. Kazim and M. Naseeruddin**, *On almost semigroups*, Alig. Bull. Math. **2** (1972), 1 – 7.

[4] **G. Lallement**, *Congruences et équivalences de Green sur un demi-groupe régulier*, C. R. Acad. Sci. Paris **262A** (1966), 613 – 616.

[5] **Q. Mushtaq and Q. Iqbal**, *Decomposition of a locally associative LA-semigroup*, Semigroup Forum **41** (1990), 155 – 164.

[6] **Q. Mushtaq and M.S. Kamran**, *Finite AG-groupoid with left identity and left zero*, Int. J. Math. Math. Sci. **27** (2001), 387 – 389.

[7] **Q. Mushtaq and M. Khan**, *Decomposition of a locally associative AG^{**}-groupoid*, Adv. Algebra Anal. **1** (2006), 115 – 122.

[8] **Q. Mushtaq and M. Khan**, *Semilattice decomposition of locally associative AG^{**}-groupoids*, Algebra Colloq. **16** (2009), 17 – 22.

[9] **P.V. Protić**, *Congruences on an inverse AG^{**}-groupoid via the natural partial order*, Quasigroups and Related Systems **17** (2009), 283 – 290.

[10] **P.V. Protić and M. Božinović**, *Some congruences on an AG^{**}-groupoid*, Filomat (Niš) **9** (1995), 879 – 886.

[11] **P.V. Protić and N. Stevanović**, *Abel-Grassmann's bands*, Quasigroups and Related Systems **11** (2004), 95 – 101.

Received August 29, 2012

Institute of Mathematics and Computer Science
Wroclaw University of Technology
Wyb. Wyspianskiego 27
50 – 370 Wroclaw
Poland
E-mails: wieslaw.dudek@pwr.wroc.pl, romekgigon@tlen.pl

Construction of subdirectly irreducible SQS-skeins of cardinality $\mathbf{n2^m}$

Enas M. A. Elzayat

Abstract. We give a construction for subdirectly irreducible SQS-skeins of cardinality $n2^m$ having a monolith with a congruence class of cardinality 2^m for each integer $m \geqslant 2$. Moreover, the homomorphic image of the constructed SQS-skein modulo its atom is isomorphic to the initial SQS-skein. Consequently, we will construct an $SK(n2^m)$ with a derived $SL(n2^m)$ such that $SK(n2^m)$ and $SL(n2^m)$ are subdirectly irreducible and have the same congruence lattice. Also, we may construct an $SK(n2^m)$ with a derived $SL(n2^m)$ in which the congruence lattice of $SK(n2^m)$ is a proper sublattice of the congruence lattice of $SK(n2^m)$.

1. Introduction

A *Steiner quadruple* (*triple*) *system* is a pair $(S; B)$ where S is a finite set and B is a collection of 4-subsets (3-subsets) called*blocks* of S such that every 3-subset (2-subset) of S is contained in exactly one block of B (see [8] and [11]). Let $\mathbf{SQS}(m)$ denote a Steiner quadruple system (briefly quadruple system) of cardinality m and $\mathbf{STS}(n)$ denote Steiner triple system (briefly triple system) of cardinality n. It is well-known that $\mathbf{SQS}(m)$ exists iff $m \equiv 2$ or 4 (mod 6) and $\mathbf{STS}(n)$ exists if and only if $n \equiv 1$ or 3 (mod 6) [8] and [11]. Let $(S; B)$ be an **SQS.** If one considers $S_a = S - \{a\}$ for any point $a \in S$ and deletes that point from all blocks which contain it then the resulting system $(S_a; B(a))$ is a triple system, where $B(a) = \{b - \{a\} \forall b \in B, a \in b\}$. Now, $(S_a; B(a))$ is called a *derived triple system* (or briefly **DTS**) of $(S; B)$ (cf. [8] and [11]).

A *sloop* (briefly **SL**) $L = (L; \cdot, 1)$ is a groupoid with a neutral element 1 satisfying the identities:

$$x \cdot y = y \cdot x, \quad 1 \cdot x = x, \quad x \cdot (x \cdot y) = y.$$

A sloop L is called *Boolean* if it satisfies the associative law. The cardinality of the Boolean sloop is equal 2^m.

2010 Mathematics Subject Classification: 05B30, 05B07, 20N05, 08A99
Keywords: Steiner triple system, Steiner loop, sloop, subdirectly irreducible sloop, Steiner quadruple systems, Steiner skein, SQS-skein, subdirectly irreducible SQS-skein.
This paper was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant No. (18-857-D1432).

There is one to one correspondence between **STS**s and Steiner loops (sloops) [8].

An ***SQS-skein*** (briefly an **SK**) $(Q;q)$ is an algebra with a unique ternary operation q satisfying:

$$q(x,y,z)=q(x,z,y)=q(z,x,y),\quad q(x,x,y)=y,\quad q(x,y,q(x,y,z))=z.$$

An **SQS**-skein $(Q;q)$ is called *Boolean* if it satisfies in addition the identity:

$$q(a,x,q(a,y,z))=q(x,y,z).$$

There is one to one correspondence between **SQS**s and **SQS**-skeins (cf. [8] and [11]).

The sloop associated with a derived triple system is also called *derived.* A derived sloop of an **SQS**-skein $(Q;q)$ with respect to $a\in Q$ is the sloop $(Q_a;\cdot,a)$ with the binary operation $\cdot$ defined by $x\cdot y=q(a,x,y)$.

A subsloop N of L (sub-**SQS**-skein of Q) is called *normal* if and only if $N=[1]\theta$ $(N=[a]\theta\ )$ for a congruence θ on L (Q) (cf. [8] and [12]). The associated congruence θ with the normal subsloop (sub-**SQS**-skein) N is given by:

$$\theta=\{(x,y):x\cdot y\quad(\text{or } q(a,y,z))\in N\}.$$

Quackenbush in [12] and similarly Armanious in [1] have proved that the congruences of sloops (**SQS**-skeins) are permutable, regular and uniform. Also, we may say that the congruence lattice of each of sloops and **SQS**-skeins is modular. Moreover, they proved that a maximal subsloop (sub-**SQS**-skein) has the same property as in groups.

Theorem 1. (cf. [1] and [8]) *Every subsloop (sub-SQS-skein) of a finite sloop* $(L;\cdot,1)$ (**SQS**-*skein* $(Q;q)$) *with cardinality* $\frac{1}{2}|L|$ $(\frac{1}{2}|Q|)$ *is normal.* □

A Boolean sloop is a Boolean group. If $(G;+)$ is a Boolean group, then $(G;q(x,y,z)=x+y+z)$ is a Boolean **SQS**-skein [1].

Guelzow [10] and Armanious [2], [3] gave generalized doubling constructions for nilpotent subdirectly irreducible **SQS**-skeins and sloops of cardinality $2n$. In [6] the authors gave recursive construction theorems as $n\to 2n$ for subdiredtly irreducible sloops and **SQS**-skeins. All these constructions supplies us with subdirectly irreducible **SQS**-skeins having a monolith θ satisfying $|[x]\theta|=2$ (the minimal possible order of a proper normal **SQS**-skeins). Also in these constructions, the authors begin with a subdirectly irreducible $\mathbf{SK}(n)$ to construct a subdirectly irreducible $\mathbf{SK}(2n)$ satisfying the property that the cardinality of the congruence class of its monolith is equal 2. Armanious [5] has given another construction of a subdirectly irreducible $\mathbf{SK}(2n)$. He begins with a finite simple $\mathbf{SK}(n)$ to costruct a subdirectly irreducible $\mathbf{SK}(2n)$ having a monolith θ with $|[x]\theta|=n$ (the maximal possible order of a proper normal sub-**SQS**-skein).

In [7] the authors begin with an arbitrary $\mathbf{SL}(n)$ to construct subdirectly irreducible $\mathbf{SL}(n2^m)$ for each possible integers $n\geqslant 4$ and $m\geqslant 2$.

In this article, we begin with an arbitrary $\mathbf{SK}(n)$ for each possible value $n \geqslant 4$ to construct subdirectly irreducible $\mathbf{SK}(n2^m)$ for each integer $m \geqslant 2$. This construction enables us to construct subdirectly irreducible **SQS**-skein having a monolith θ satisfying that its congruence class is $\mathbf{SK}(2^m)$. Moreover, its homomorphic image modulo θ is isomorphic to Q.

We will show that our construction supplies us with construction of an $\mathbf{SK}(n2^m)$ with a derived $\mathbf{SL}(n2^m)$ such that the congruence lattices of $\mathbf{SK}(n2^m)$ and $\mathbf{SL}(n2^m)$ are the same for each possible case. Moreover, we may construct an $\mathbf{SK}(n2^m)$ with a derived $\mathbf{SL}(n2^m)$ such that the congruence lattices of $\mathbf{SK}(n2^m)$ is a proper sublattice of the congruence lattice of $\mathbf{SL}(n2^m)$.

2. Subdirectly irreducible SQS-skeins $Q \times_\alpha B$

Let $Q := (Q; q)$ be an $\mathbf{SK}(n)$ and $B := (B; \bullet, 1)$ be a Boolean $\mathbf{SL}(2^m)$, where $Q = \{x_0, x_1, x_2, \ldots, x_{n-1}\}$ and $B = \{1, a_1, a_2, \ldots, a_{{}_2m_{-1}}\}$. In this section we extend the **SQS**-skein Q to a subdireclty irreducible **SQS**-skein $Q \times_\alpha B$ of cardinality $n2^m$ having Q as a homomorphic image.

We divide the set of elements of the direct product $Q \times B$ into two subsets $\{x_0, x_1\} \times B$ and $\{x_2, \ldots, x_{n-1}\} \times B$. Consider the cyclic permutation $\alpha = (a_1 a_2 \ldots a_{{}_2m_{-1}})$ on the set $\{1, a_1, a_2, \ldots, a_{{}_2m_{-1}}\}$ and the characteristic function χ from the direct product $Q \times B$ to B defined as follows

$$\chi((y_1, i_1), (y_2, i_2), (y_3, i_3)) =$$

$$\begin{cases} i_m \bullet i_n \bullet \alpha^{-1}(i_m \bullet i_n) & \text{for } y_m = y_n = x_0,\ y_k = x_1 \text{ and } \{m, n, k\} = \{1, 2, 3\} \\ i_m \bullet i_n \bullet \alpha(i_m \bullet i_n) & \text{for } y_m = y_n = x_1,\ y_k = x_0 \text{ and } \{m, n, k\} = \{1, 2, 3\} \\ 1 & \text{otherwise.} \end{cases}$$

It is clear that $\chi((y_1, i_1), (y_2, i_2), (y_3, i_3)) = 1$ in two cases:

(i) $y_1 = y_2 = y_3 = x_0$ or $y_1 = y_2 = y_3 = x_1$.

(ii) y_1, y_2 or $y_3 \in Q - \{x_0, x_1\}$.

For this characteristic function we obtain the following result:

Lemma 2. *The characteristic function χ satisfies the properties:*

(i) $\chi((x, a), (y, b), (z, c)) = \chi((x, a), (z, c), (y, b)) = \chi((z, c), (x, a), (y, b))$;

(ii) $\chi((x, a), (x, a), (y, b)) = 1$;

(iii) $\chi((x, a), (y, b), (q(x, y, z), a \bullet b \bullet c \bullet \chi((x, a), (y, b), (z, c)))) =$
$\chi((x, a), (y, b), (z, c))$.

Proof. According to the definition of χ, we may deduce that (i) is valid.

In (ii), if $x = x_0$ and $y = x_1$ then $\chi((x_0, a), (x_0, a), (x_1, b)) = a \bullet a \bullet \alpha^{-1}(a \bullet a) = 1$. If $x = x_1$ and $y = x_0$, then $\chi((x_1, a), (x_1, a), (x_0, b)) = a \bullet a \bullet \alpha(a \bullet a) = 1$. Otherwise if x or$y \neq x_0$ or x_1, then $\chi((x, a), (x, a), (y, b)) = 1$.

To prove the third property, we have only three essential cases:
(1) If $x = y = x_0$ and $z = x_1$ then

$$\begin{aligned}&\chi((x_0, a), (x_0, b), (q(x_0, x_0, x_1), a \bullet b \bullet c \bullet \chi((x_0, a), (x_0, b), (x_1, c))))\\ &= \chi((x_0, a), (x_0, b), (x_1, c \bullet \alpha^{-1}(a \bullet b))) = a \bullet b \bullet \alpha^{-1}(a \bullet b)\\ &= \chi((x_0, a), (x_0, b), (x_1, c)).\end{aligned}$$

(2) If $x = y = x_1$ and $z = x_0$ then

$$\begin{aligned}&\chi((x_1, a), (x_1, b), (q(x_1, x_1, x_0), a \bullet b \bullet c \bullet \chi((x_1, a), (x_1, b), (x_0, c))))\\ &= \chi((x_1, a), (x_1, b), (x_0, c \bullet \alpha(a \bullet b))) = a \bullet b \bullet \alpha(a \bullet b)\\ &= \chi((x_1, a), (x_1, b), (x_0, c)).\end{aligned}$$

Note that
$\chi((x_0, a), (x_0, b), (x_1, c)) = \chi((x_0, a), (x_1, c), (x_0, b)) = \chi((x_1, c), ((x_0, a), (x_0, b))$
and
$\chi((x_1, a), (x_1, b), (x_0, c)) = \chi((x_1, a), (x_0, c), (x_1, b)) = \chi((x_0, c), ((x_1, a), (x_1, b)).$

(3) Otherwise, i.e., when *i)* $x = y = z = x_0$ or $x = y = z = x_1$
ii) x, y or $z \notin \{x_0, x_1\}$,
we have

$$\chi((x, a), (y, b), (q(x, y, z), a \bullet b \bullet c \bullet \chi((x, a), (y, b), (z, c)))) = \chi((x, a), (y, b), (z, c) = 1.$$

This completes the proof of the lemma. □

Lemma 3. *Let* $(Q; q)$ *be an arbitrary* $\mathbf{SK}(n)$*, and* $(B; \bullet, 1)$ *be a Boolean* $\mathbf{SL}(2^m)$ *for* $m \geqslant 2$*. Also let* q' *be a ternary operation on the set* $Q \times B$ *defined by :*

$$q'((x, a), (y, b), (z, c)) := (q(x, y, z), a \bullet b \bullet c \bullet \chi((x, a), (y, b), (z, c))).$$

Then $Q \times_\alpha B = (Q \times B; q')$ *is an* $\mathbf{SK}(n2^m)$ *for each possible number* $n \geqslant 4$*.*

Proof. Let $Q = \{x_0, x_1, x_2, \dots, x_{n-1}\}$ and $B = \{1, a_1, a_2, \dots, a_{2^m-1}\}$. For all $(x, a), (y, b), (z, c) \in Q \times B$, according to Lemma 2 (*i*) and the properties of the operations "q" and " $\bullet$ " we find that:

$$q'((x, a), (y, b), (z, c)) = q'((x, a), (z, c), (y, b)) = q'((z, c), (x, a), (y, b)).$$

By using Lemma 2 (*ii*)

$$q'((x, a), (x, a), (y, b) = (q(x, x, y), a \bullet a \bullet b \bullet \chi((x, a), (x, a), (y, b))) = (y, b).$$

Also, Lemma 2 (*iii*) gives us that

$$\begin{aligned}&q'((x, a), (y, b), (q'((x, a), (y, b), (z, c)))\\ &= q'((x, a), (y, b), (q(x, y, z), a \bullet b \bullet c \bullet \chi((x, a), (y, b), (z, c)) = (z, c).\end{aligned}$$

Hence $Q \times_\alpha B = (Q \times B; q')$ is an $\mathbf{SQS}$-skein. □

In the next theorem we prove that the constucted $Q\times_\alpha B$ is a subdirectly irreducible **SQS**-skein having a monolith θ_1 satisfying that the cardinality of its congruence class equal 2^m.

Theorem 4. *The constructed sloop $Q\times_\alpha B = (Q\times B; q')$ is a subdirectly irreducible* ***SQS****-skein.*

Proof. The projection $\Pi : (x,a) \to x$ from $Q \times B$ into Q is an onto homomorphism and the congrurnce Ker $\Pi := \theta_1$ on $Q \times B$ is given by:

$$\theta_1 = \bigcup\nolimits_{i=0}^{n-1} \left\{(x_i,1), (x_i,a_1), \dots, (x_i,a_{2m-1})\right\}^2,$$

so one can directly see that $[(x_0,1)]\theta_1 = \left\{(x_0,1),(x_0,\alpha_1),\dots,(x_0,a_{2m-1})\right\}$.

Now $\mathbf{C}(Q) \cong \mathbf{C}((Q\times_\alpha B)/\theta_1) \cong [\theta_1 : 1]$. Our proof will now be complete if we show that θ_1 is the unique atom of $\mathbf{C}(Q\times_\alpha B)$.

First, assume that θ_1 is not an atom of $\mathbf{C}(Q\times_\alpha B)$, then we can find an atom γ satisfying that: $\gamma \subset \theta_1$ and $|[(x_i,a_i)]\,\gamma| = r < |[(x_i,a_i)]\,\theta_1| = 2^m$. In the following we get a contradiction by proving $[(x_1,1)]\,\gamma$ is not a normal sub-**SQS**-skein of $Q\times_\alpha B$.

Suppose $[(x_1,1)]\gamma = \left\{(x_1,1),(x_1,a_{s_1}),\dots.,(x_1,a_{s_{r-1}})\right\}$. If $\left\{a_{s_1},a_{s_2},\dots,a_{s_{r-1}}\right\}$ is an increasing successive subsequence of $\left\{a_1,a_2,\dots,a_{2m-1}\right\}$ and if $\alpha(a_{s_i}) = a_{s_{i+1}}$ for all $i = 1,2,\dots,r-1$, then $\alpha(a_{s_{r-1}}) = a_{s_r} \notin \left\{a_{s_1},a_{s_2},\dots,a_{s_{r-1}}\right\}$. If $\left\{a_{s_1},a_{s_2},\dots,a_{s_{r-1}}\right\}$ is an increasing and not successive subsequence selected from $\left\{a_1,a_2,\dots,a_{2m-1}\right\}$ then there exists an element $a_j \in \left\{a_{s_1},a_{s_2},\dots,a_{s_{r-1}}\right\}$ such that $\alpha(a_j) = a_{j+1} \notin \left\{a_{s_1},a_{s_2},\dots,a_{s_{r-1}}\right\}$. For both cases, we can always find an element $(x_1,a_k) \in [(x_1,1)]\,\gamma$ such that $(x_1,\alpha(a_k)) \notin [(x_1,1)]\,\gamma$ ($a_k = a_{s_{r-1}}$ for the first case, and $a_k = a_j$ for the second case).

We can determine the class containing $(x_0,1)$ when we use the fact that $[(x_0,1)]\,\gamma = q'\left([(x_1,1)]\,\gamma,(x_1,1),(x_0,1)\right)$, hence we will find that

$$[(x_0,1)]\,\gamma = \left\{(x_0,1),(x_0,\alpha(a_{s_1})),(x_0,\alpha(a_{s_2})),\dots,\left(x_0,\alpha\left(a_{s_{r-1}}\right)\right)\right\}.$$

By the same way $[(x_2,1)]\,\gamma = q'\left([(x_1,1)]\,\gamma,(x_1,1),(x_2,1)\right)$, and this leads to

$$[(x_2,1)]\,\gamma = \left\{(x_2,1),(x_2,a_{s_1}),(x_2,a_{s_2}),\dots,\left(x_2,a_{s_{r-1}}\right)\right\}.$$

From the other side $[(x_2,1)]\,\gamma = q'\left([(x_0,1)]\,\gamma,(x_0,1),(x_2,1)\right)$, here we will find that

$$[(x_2,1)]\,\gamma = \left\{(x_2,1),(x_2,\alpha(a_{s_1})),(x_2,\alpha(a_{s_2})),\dots,\left(x_2,\alpha\left(a_{s_{r-1}}\right)\right)\right\}.$$

This means that for each $a_k \in \left\{a_{s_1},a_{s_2},\dots,a_{s_{r-1}}\right\}$ $\alpha(a_k) \in \left\{a_{s_1},a_{s_2},\dots,a_{s_{r-1}}\right\}$. This contradicts the assumption that $(x_1,\alpha(a_k)) \notin [(x_1,1)]\,\gamma$. Hence, we may say that there is no atom γ of $\mathbf{C}(Q\times_\alpha B)$ satisfying $\gamma \subset \theta_1$. Therefore, θ_1 is an atom of the lattice $\mathbf{C}(Q\times_\alpha B)$.

Secondly, to prove that θ_1 is the unique atom of $\mathbf{C}(Q \times_\alpha B)$. Assume that δ is another atom of $\mathbf{C}(Q \times_\alpha B)$, then $\theta_1 \cap \delta = 0$. Hence, one can easily see that there is only one element $(x, a_i) \in [(x, a_i)]\delta$ with the first component x (note that $[(x, a_i)]\,\theta_1 = \big\{(x, 1), (x, a_1), \dots, (x, a_i), \dots, (x, a_{2^m-1})\big\}$). For this reason we may say that the class $[(x_0, 1)]\delta$ has at most one pair (x_1, a_i) with first component x_1. So we have two possibilities; either

(i) $[(x_0, 1)]\delta$ contains only one pair (x_1, a_i) with first component x_1, or

(ii) $[(x_0, 1)]\delta$ has not any pairs with first component x_1.

For the first case, let $((x, a), (x_1, a_s)) \in \delta$ such that $x_0 \neq x \neq x_1$, and $a_s \neq a_i$. Then

$$q'((x_0, 1), (x, a), (x_1, a_s)) \in [(x_0, 1)]\delta.$$

In this case $(x_1, a_i) \in [(x_0, 1)]\,\delta$. Thus

$$q'((x_0, 1), (x_1, a_i), q'((x_0, 1), (x, a), (x_1, a_s))) \in [(x_0, 1)]\delta.$$

Hence, $(x, a_i \bullet a \bullet a_s) \in [(x_0, 1)]\,\delta$.

By using the properties of congruences, $((x_0, 1)\,, (x_1, a_i))\,, ((x_1, a_s)\,, (x, a))$ and $((x_1, a_i)\,, (x_1, a_i)) \in \delta$, we shall find that $(q'((x_0, 1), (x_1, a_s), (x_1, a_i)), (x, a)) \in \delta$. This means that

$$q'((x_0, 1), (x, a), q'((x_0, 1), (x_1, a_s), (x_1, a_i))) \in [(x_0, 1)]\delta.$$

So,

$$(x, a \bullet \alpha(a_i \bullet a_s)) \in [(x_0, 1)]\,\delta.$$

Since the class $[(x_0, 1)]\,\delta$ contains at most one element with a first component x, it follows that $\alpha(a_i \bullet a_s) = a_i \bullet a_s$ hence $a_i \bullet a_s = 1$, which contradicts the choice that $a_s \neq a_i$. This implies that $[(x_0, 1)]\,\delta$ is not a normal sub-**SQS**-skein of $Q \times_\alpha B$.

For the second case (ii) when $[(x_0, 1)]\delta$ has not any pair with first component x_1. Let $(x, a) \in [(x_0, 1)]\delta$ such that $x_0 \neq x \neq x_1$, and let (x, b) and (x, c) are two elements in $Q \times B$ such that $a \neq b$. Then

$$q'((x_0, 1), (x, a), q'((x_0, 1), (x_1, c), (x, b))) \in [q'((x_0, 1), (x_1, c), (x, b))]\,\delta.$$

This means that $(x_1, c \bullet a \bullet b) \in [q'((x_0, 1), (x_1, c), (x, b))]\,\delta$. Also,

$$\begin{aligned} q'((x_0, 1), (x_1, c), q'((x_0, 1), (x, a), (x, b))) &\in q'((x_0, 1), (x_1, c), [(x, b)]\delta) \\ &= [q'((x_0, 1), (x_1, c), (x, b))]\,\delta. \end{aligned}$$

Therefore $(x_1, c \bullet \alpha^{-1}(a \bullet b)) \in [q'((x_0, 1), (x_1, c), (x, b))]\,\delta$.

By using the fact that the class $[q'((x_0, 1), (x_1, c), (x, b))]\,\delta$ contains only one element with the first component x_1, we may say that $\alpha^{-1}(a \bullet b) = a \bullet b$, hence $a \bullet b = 1$, which contradicts that $a \neq b$.Thus $[(x_0, 1)]\delta$ is not a normal sub-**SQS**-skein of $Q \times_\alpha B$.This mean that there is no another atom δ, and θ_1 is the unique atom of $\mathbf{C}(Q \times_\alpha B)$. Therefore, $Q \times_\alpha B$ is a subdirectly irreducible **SQS**-skein. □

Note that in the constructed **SQS**-skein $Q \times_\alpha B$, we may choose B a Boolean $\mathbf{SL}(2^m)$ for each $m \geqslant 2$. Therefore, as a consequence of the proof of Theorem 3, we obtain

Corollary 5. *Let B be a Boolean $\mathbf{SL}(2^m)$ for an integer $m \geqslant 2$. Then the congruence class $[(x_0, 1)]\theta_1$ of the monolith θ_1 of the constucted subdirectly irreducible **SQS**-skein $Q \times_\alpha B$ is a Boolean $\mathbf{SK}(2^m)$.* □

Also, Theorem 3 enable us to construct a subdirectly irreducible **SQS**-skein $Q \times_\alpha B$ having a monolith θ_1 satisfying that $(Q \times_\alpha B)/ \theta_1 \cong Q$.

Corollary 6. *Every **SQS**-skein Q is isomorphic to the homomorphic image of the subdirectly irreducible **SQS**-skein $Q \times_\alpha B$ over its monolith, for each Boolean sloop B.* □

Remark: The **SQS**-skein $Q \times_\alpha B$ having $L \times_\alpha B$ as a derived sloop.

Let $(Q; q)$ be an $\mathbf{SK}(n)$ and $(L; *, x_0)$ be a derived $\mathbf{SL}(n)$ of Q with respect to the element x_0 with the same congruence lattice. This means that for $L = Q = \{x_0, x_1, \ldots, x_{n-1}\}$, the binary operation " $*$ " is defined by $x * y = q(x_0, x, y)$.

By using the construction in [7], we construct subdirectly irreducible $\mathbf{SL}(n2^m)$. This means that if we begin with our derived sloop $L := (L; *, x_0)$ of cardinality n and the Boolean sloop $B := (B; \bullet, 1)$ of cardinality 2^m, we get subdirectly irreducible sloop $L{\times_\alpha}B =(L \times B; \circ, (x_0, 1))$, where

$$(x, a) \circ (y, b) := (x * y, a \bullet b \bullet \chi((x, a), (y, b)))$$

and

$$\chi((x, a), (y, b))_L = \begin{cases} a \bullet \alpha^{-1}(a) & \text{for } x = x_0,\ y = x_1, \\ b \bullet \alpha^{-1}(b) & \text{for } x = x_1,\ y = 1, \\ c \bullet \alpha(c) & \text{for } x = x_1 = y \text{ and } a \bullet b = c, \\ 1 & \text{otherwise.} \end{cases}$$

It is easy to see that $\chi((x, a), (y, b))_L = \chi((x_0, 1), (x, a), (y, b))$ (the characteristic function of our construction) for all $x, y \in L = Q$. Hence $(x, a) \circ (y, b) = q'((x_0, 1), (x, a), (y, b))$ for all $(x, a)\,, (y, b) \in L \times B = Q \times B$, this means directly that the constructed sloop $L{\times_\alpha}B$ is a derived sloop of the constructed **SQS**-skein $Q \times_\alpha B$. Therefore, we have the following result:

Corollary 7. *Let L be a derived sloop of the **SQS**-skein Q with respect to the element x_0, then the sloop $L{\times_\alpha}B$ is a derived sloop of the **SQS**-skein $Q \times_\alpha B$ with respect to $(x_0, 1)$.* □

Note that Q is isomorphic to the homomorphic image of $Q \times_\alpha B$ over its monolith (Corollary 5) and also L is isomorphic to the homomorphic image of $L \times_\alpha B$ over its monolith [7]. Hence according to [7], Theorem 4 and Corollary 6, we may say that:

There is always an SQS-skein $Q \times_\alpha B$ with a derived sloop $L \times_\alpha B$, in which both $Q \times_\alpha B$ and $L \times_\alpha B$ are subdirectly irreducible of cardinality $n2^m$ having the same congruence lattice for each possible integers $n \geqslant 4$ and $m \geqslant 2$.

The construction of a semi-Boolean **SQS**-skein (each derived sloop L of Q is Boolean) given in [9] satisfies that $C(Q)$ is a proper sublattice of the congruence lattice of its derived sloop $C(L)$. This means that we may begin with **SQS**-skein Q with a derived sloop L in which the congruence lattice of Q is a proper sublattice of the congruence lattice of L, this leads to $C(L \times_\alpha B)$ is a proper sublattice of $C(Q \times_\alpha B)$.

Consequently, *we may construct SQS-skein $Q \times_\alpha B$ with a derived sloop $L \times_\alpha B$ such that $Q \times_\alpha B$ and $L \times_\alpha B$ are subdirectly irreducible of cardinality $n2^m$ and have the same congruence lattice, if we begin with L derived sloop of Q with the same congruence lattice. Also, we may construct SQS-skein $Q \times_\alpha B$ with a derived sloop $L \times_\alpha B$ in which the congruence lattice of $Q \times_\alpha B$ is a proper sublattice of the congruence lattice of $L \times_\alpha B$, if we begin with L derived sloop of Q such that the congruence lattice of Q is a proper sublattice of the congruence lattice of L.*

References

[1] **M.H. Armanious**, *Algebraische Theorie der Quadrupelsysteme*, Ph.D. Thesis, Fachbereich Mathematik der Technischen Hochschule Darmstadt, 1980.

[2] **M.H. Armanious**, *Construction of nilpotent sloops of class n*, Discrete Math. **171** (1997), 17 – 25.

[3] **M.H. Armanious**, *Nilpotent SQS-skeins with nilpotent derived sloops*, Ars Combin. **56** (2000), 193 – 200.

[4] **M.H. Armanious**, *On subdirectly irreducible Steiner loops of cardinality 2n*, Beitrage zur Algebra und Geometrie **43** (2002), 325 – 331.

[5] **M.H. Armanious**, *On subdirectly irreducible SQS-skeins*, J. Combin. Math. Combin. Comput. **52** (2005), 117 – 130.

[6] **M.H. Armanious and E.M. Elzayat**, *Subdirectly irreducible sloops and SQS-skeins*, Quasigroups and Reelated Systems **15** (2007), 233 – 250.

[7] **E.M. Elzayat and M.H. Armanious**, *Construction for subdirectly irreducible sloops of cardinality $n2^m$*, Quasigroups and Reelated Systems **17** (2009), 151 – 158.

[8] **B. Ganter and H. Werner**, *Co-ordinatizing Steiner systems*, Ann. Discrete Math. **7** (1980), 3 – 24.

[9] **A.J. Guelzow**, *Semi-boolean SQS-skeins*, J. Alg. Comb. **2** (1993), 147 – 153.

[10] **A.J. Guelzow**, *The structure of nilpotent Steiner quadruple systems*, J. Comb. Designs **1** (1993), 301 – 321.

[11] **C.C. Lindner and A. Rosa**, *Steiner quadruple systems*, Discrete Math. **21** (1978), 147 – 181.

[12] **R.W. Quackenbush**, *Varieties of Steiner loops and Steiner quasigroups*, Canadian J. Math. **28** (1978), 1187 – 1198.

Received August 25, 2012

Department of Mathematics, Faculty of Science and Arts, Khulais, King Abdulaziz University,
Kingdom of Saudi Arabia
E-mail: enaselzyat@yahoo.com

Quasigroups and Related Systems **20** (2012), 219 − 232

Clifford congruences on an idempotent-surjective R-semigroup

Roman S. Gigoń

Abstract. In the paper we describe the least Clifford congruence ξ on an idempotent-surjective R-semigroup, and so we generalize the result of LaTorre (1983). In addition, a characterization of all Clifford congruences on such a semigroup (in particular, on a structurally regular semigroup) is given. Furthermore, we find necessary and sufficient conditions for ξ to be idempotent pure or E-unitary. Moreover, using some earlier result, we give a description of all USG-congruences on an idempotent-surjective semigroup, and so we generalize the result of Howie and Lallement for regular semigroups (1966). Finally, in Section 4 we study the subdirect products of an E-unitary semigroup and a Clifford semigroup.

1. Preliminaries

Whenever possible the notation and conventions of Howie [11, 12] are used. Let S be a semigroup and let $A \subseteq S$. Denote by E_A the set of all *idempotents* of A, that is, $E_A = \{a \in A : a^2 = a\}$, and by $Reg(S)$ the set of all *regular elements* of S, i.e., $Reg(S) = \{a \in S : a \in aSa\}$. We say that S is *regular* if $Reg(S) = S$. More generally, in [10] Hall observed that the set $Reg(S)$ of a semigroup S with $E_S \neq \emptyset$ forms a regular subsemigroup of S if and only if the product of any two idempotents of S is regular. In a such case, S is said to be an *R-semigroup*. Finally, if E_S is a subsemigroup of S, then S is called an *E-semigroup*. Clearly, any E-semigroup is an R-semigroup.

Let S be a semigroup, $a \in S$. The set $W(a) = \{x \in S : x = xax\}$ is called the set of *weak inverses* of a, so the elements of $W(a)$ will be called *weak inverse elements* of a. A semigroup S is said to be *E-inversive* if for every $a \in S$ there is $x \in S$ such that $ax \in E_S$ [21]. Clearly, S is E-inversive iff $W(a) \neq \emptyset$ $(a \in S)$, so if S is E-inversive, then for all $a \in S$ there is $x \in S$ such that $ax, xa \in E_S$. For some interesting results concerning E-inversive semigroups, see [18, 4].

A generalization of the concept of regularity will also prove convenient. Define a semigroup S to be *idempotent-surjective* if whenever ρ is a congruence on S and $a\rho$ is an idempotent of S/ρ, then $a\rho$ contains some idempotent of S [2]. The famous Lallement's Lemma says that all regular semigroups are idempotent-surjective. Finally, it is known that idempotent-surjective semigroups are E-inversive.

2010 Mathematics Subject Classification: 20M99, 06B10
Keywords: Clifford congruence, R-semigroup, idempotent-surjective semigroup, E-semigroup, structurally regular semigroup, E-unitary congruence, USG-congruence.

On the other hand, Kopamu defined in [14] a countable family of congruences on a semigroup S, as follows: for each ordered pair of non-negative integers (m, n), he put:

$$\theta_{m,n} = \{(a, b) \in S \times S : (\forall x \in S^m, y \in S^n)\ xay = xby\},$$

and he made the convention that $S^1 = S$ and S^0 denotes the set containing only the empty word. In particular, $\theta_{0,0} = 1_S$. Recall from [14] that if $S/\theta_{m,n}$ is regular for some non-negative integers m, n, then S is *structurally regular*. Kopamu also proved that structurally regular semigroups are idempotent-surjective. Finally, in [8] the author showed that structurally regular semigroups are R-semigroups, and so *every* structurally regular semigroup is an *idempotent-surjective R-semigroup*.

Green's relations on S are denoted by $\mathcal{L}$ ($(a, b) \in \mathcal{L}$ if $Sa \cup \{a\} = Sb \cup \{b\}$), $\mathcal{R}$ ($(a, b) \in \mathcal{R}$ if $aS \cup \{a\} = bS \cup \{b\}$) and $\mathcal{H}$ $(= \mathcal{L} \cap \mathcal{R})$. Denote by $\mathcal{H}_a$ the $\mathcal{H}$-class containing the element a. Notice that Green's Theorem says that in an arbitrary semigroup S either $\mathcal{H}_a\mathcal{H}_a \cap \mathcal{H}_a = \emptyset$ or $\mathcal{H}_a$ is a group.

Recall that a semigroup S is a *semilattice* if $a^2 = a$, $ab = ba$ for all $a, b \in S$. Let $\mathcal{C}$ be some class of semigroups of the same type $\mathcal{T}$ (for example: the class of all groups); call its elements *$\mathcal{C}$-semigroups*. A congruence ρ on a semigroup S is said to be a *$\mathcal{C}$-congruence* if $S/\rho \in \mathcal{C}$. Clearly, the least semilattice congruence η (say) on an arbitrary semigroup S exists. Finally, a semigroup S is a *semilattice S/ρ of groups* if there exists a semilattice congruence ρ on S such that every ρ-class is a group. Since $\mathcal{H} \subseteq \eta$, then a semigroup S is a semilattice S/ρ of groups if and only if $\mathcal{H} = \eta$. Indeed, $\mathcal{H} \subseteq \eta \subseteq \rho$ and evidently $\rho \subseteq \mathcal{H}$. Consequently we have $\mathcal{H} = \eta$. The converse implication follows from Green's Theorem.

Moreover, some preliminaries about group congruences on a semigroup S are needed. A subset A of S is called (respectively) *full*; *reflexive* and *dense* if $E_S \subseteq A$; $(\forall a, b \in S)(ab \in A \Rightarrow ba \in A)$ and $(\forall s \in S)(\exists\, x, y \in S)\ sx, ys \in A$. Also, we define the *closure operator* ω on S by $A\omega = \{s \in S : (\exists\, a \in A)\ as \in A\}$ (where $A \subseteq S$). We shall say that $A \subseteq S$ is *closed* (in S) if $A\omega = A$. Further, a subsemigroup N of a semigroup S is said to be *normal* if it is full, dense, reflexive and closed (if N is normal, then we shall write $N \lhd S$). Finally, if a subsemigroup of S is dense and reflexive, then it is called *quasi-normal*.

By the *kernel* of a congruence ρ on a semigroup S we shall mean the set $\ker(\rho) = \{x \in S : (x, x^2) \in \rho\}$.

Result 1.1. [5] *Let B be a quasi-normal subsemigroup of a semigroup S. Then the relation $\rho_B = \{(a, b) \in S \times S : (\exists\ x, y \in B)\, ax = yb\}$ is a group congruence on S. Also, $B \subseteq B\omega = \ker(\rho_B)$, and if $B \lhd S$, then $B = \ker(\rho_B)$.*

Conversely, if ρ is a group congruence on S, then there is a normal subsemigroup N of S such that $\rho = \rho_N$ (in fact, $N = \ker(\rho)$). Thus there is an inclusion-preserving bijection between the set of all normal subsemigroups of S and the set of all group congruences on S.

Moreover, the least group congruence on an E-inversive E-semigroup is given by

$$\sigma = \{(a, b) \in S \times S : (\exists\, e, f \in E_S)\ ea = bf\}. \qquad \square$$

Remark 1.2. [5] Let B be a quasi-normal subsemigroup of S. Then:

$$(a,b) \in \rho_B \Leftrightarrow (\exists\, x \in S)\ xa, xb \in B.$$

It is easily seen that if S is an E-inversive semigroup (and so E_S is dense), then there exists the least normal subsemigroup of S. In the light of Result 1.1, every E-inversive semigroup possesses the least group congruence σ.

An inverse semigroup in which the idempotents are central is called a *Clifford* semigroup. Recall that a semigroup S is a Clifford semigroup if and only if it is a semilattice of groups [11]. Observe that if $ab = e \in E_S$, then

$$ba = baa^{-1}a = a^{-1}aba = a^{-1}ea \in E_S.$$

Thus $ab = ba$ (since ab and ba belong to the same subgroup of S), so E_S is reflexive. Further, a semigroup S is called *η-simple* if S has no semilattice congruences except the universal relation. It is well known that every η-class of S is η-simple [20].

Recall from [9] that a full quasi-normal subsemigroup of a semigroup is called *seminormal.*

Finally, we have need the following two results.

Theorem 1.3. *Let ρ be an arbitrary semilattice congruence on an idempotent-surjective R-semigroup S, N be a (semi)normal subsemigroup of S and let $a \in S$. Put $N_a = N \cap a\rho$. Then:*

(a) $a\rho$ is an E-inversive R-semigroup;

(b) N_a is a (semi)normal subsemigroup of $a\rho$.

Proof. (a). Let $a \in S$ and $e \in E_{a\eta}$. Suppose by way of contradiction that $a\eta$ is not E-inversive. Then the set A of all non E-inversive elements of $a\eta$ is an ideal of $a\eta$. Clearly, $e \notin A$. Consider an equivalence ρ (say) on $a\eta$ induced by the partition: $\{A, a\eta \setminus A\}$ and suppose that there are elements $s, t \in a\eta \setminus A$ such that $st \in A$. Then $fg \in A$ for some idempotents $f, g \in a\eta \setminus A$. Since S is an R-semigroup, then $x = xfgx, fg = fgxfg$ for some $x \in S$. It follows that $x \in a\eta$, so $x \in W(fg)$ in $a\eta$, which contradicted to $fg \in A$. Hence ρ is a semilattice congruence on an η-simple semigroup $a\eta$, a contradiction. Consequently, $A = \emptyset$ (since $e \notin A$), and so $a\eta$ is an E-inversive R-semigroup.

(b). The second part of the theorem is a direct consequence of the definition of a (semi)normal subsemigroup and the first part of the theorem. □

Lemma 1.4. *Let B be the least seminormal subsemigroup of an idempotent-surjective semigroup S. If ϕ is an epimorphism of S onto a Clifford semigroup T, then $B\phi = E_T$.*

Proof. Put $A = (E_T)\phi^{-1}$. Clearly, A is a full subsemigroup of S. Thus A is dense. Moreover, if $xy \in A$, then $E_T \ni (xy)\phi = x\phi \cdot y\phi = y\phi \cdot x\phi = (yx)\phi$ (since E_T is reflexive), so $yx \in A$. Hence $B \subseteq A$. Thus $B\phi \subseteq ((E_T)\phi^{-1})\phi \subseteq E_T$. Since S is idempotent-surjective and B is full, then $E_T = (E_S)\phi \subseteq B\phi$. Consequently, $B\phi = E_T$. □

2. Clifford congruences

Let ε be a semilattice congruence on an idempotent-surjective R-semigroup S. Denote ε-classes of S by S_α, where α's are elements of some set A, and define on A a binary operation $\circ$, as follows: if $a \in S_\alpha, b \in S_\beta$, then

$$\alpha \circ \beta = \gamma \Leftrightarrow ab \in S_\gamma.$$

Clearly, $(A, \circ)$ is a semilattice (isomorphic to S/ϵ), so

$$S = \bigcup \{S_\alpha : \alpha \in A\}$$

is a semilattice A of E-inversive R-semigroups S_α (Theorem 1.3(a)). For any seminormal subsemigroup I of S, put $I_\alpha = I \cap S_\alpha$ ($\alpha \in A$); see Theorem 1.3(b). Then by Result 1.1 and Remark 1.2, for every α, the relation

$$\rho_{I_\alpha} = \{(a,b) \in S_\alpha \times S_\alpha : (\exists\, x \in S_\alpha)\ xa, xb \in I_\alpha\}$$

is a group congruence on S_α. Put $\rho = \bigcup\{\rho_{I_\alpha} : \alpha \in A\}$. We will show that ρ is a congruence on S. Let $(a,b) \in \rho$, say $(a,b) \in \rho_{I_\alpha}$; $c \in S_\beta$. Then $xa, xb \in I_\alpha$ for some $x \in S_\alpha$. Since I_β is dense, then $cz \in I_\beta$ for some $z \in S_\beta$. Notice that $ac, bc, zx \in S_{\alpha\beta}$. Furthermore, $(xa)(cz) \in I_\alpha I_\beta \subseteq I$. Hence $(zx)(ac) \in I$ (since I is reflexive), therefore, $(zx)(ac) \in I \cap S_{\alpha\beta} = I_{\alpha\beta}$. Similarly, $(zx)(bc) \in I_{\alpha\beta}$. This implies that $(ac, bc) \in \rho$, and so ρ is a right congruence on S. By symmetry of the definition of ρ_{I_α}, we conclude that ρ is also a left congruence on S. Thus ρ is a congruence on S and for all $a \in S$, $a\rho = a\rho_{I_\alpha}$ if $a \in S_\alpha$. Put $G_\alpha = S_\alpha/\rho_{I_\alpha}$. Then $S/\rho = \bigcup\{G_\alpha : \alpha \in A\}$ is a semilattice A of groups G_α.

Applying the above construction (of ρ) to the least semilattice congruence η on S and to the least seminormal subsemigroup B of S, we obtain some semilattice of groups congruence on S, say ξ.

Let S be an idempotent-surjective E-semigroup. Then each η-class of S is an E-semigroup. Define on every S_α the least group congruence σ_α (see Result 1.1). Then the relation ξ^*, induced by this partition of S, is a congruence on S. Indeed, if $a\,\xi^*\,b$, say $(a,b) \in \sigma_\alpha$ in S_α; $c \in S_\beta$, then $ea = bf$, where $e, f \in E_{S_\alpha}$, and so $(bcc^*b^*e)ac = bc(c^* {\cdot} b^*bf {\cdot} c)$ for every $b^* \in W_{S_\alpha}(b)$, $c^* \in W_{S_\beta}(c)$. The expressions in the parentheses belong to E_S. Further, $bcc^*b^*e, c^*b^*bfc \in S_{\alpha\beta}$, $ac, bc \in S_{\alpha\beta}$. Hence ξ^* is a right congruence on S. By symmetry, ξ^* is a left congruence on S. Thus S/ξ^* is a semilattice of groups.

Finally, we will show that ξ is the least Clifford congruence on an idempotent-surjective R-semigroup S. Let ρ be any congruence on S such that S/ρ is a semilattice A of groups, say $S/\rho = \bigcup\{G_\alpha : \alpha \in A\}$; $\rho^\natural$ be the natural homomorphism of S onto S/ρ and φ be the canonical morphism of S/ρ onto A, defined by $(a\rho)\varphi = \alpha$ if $a\rho \in G_\alpha$. The composition map $\Phi = \rho^\natural\varphi$ is a morphism of S onto A, so $\Phi\Phi^{-1}$, where $a(\Phi\Phi^{-1})b$ if and only if $a\rho, b\rho \in G_\alpha$ for some $\alpha \in A$, is a semilattice congruence on S. Thus $\eta \subseteq \Phi\Phi^{-1}$. Suppose that $a\,\xi\,b$. Then $a\,\eta\,b$ and $xa = by$ for some

$x, y \in a\eta \cap B$, where B is the least seminormal subsemigroup of S. Since x, y, a, b lie in the same η-class, then they belong to the same $\Phi\Phi^{-1}$-class, so $x\rho, y\rho, a\rho, b\rho$ lie in G_α ($\alpha \in A$). Since $x, y \in B$, then $x\rho, y\rho \in E_{S/\rho}$ (Lemma 1.4), so $x\rho = y\rho = 1_{G_\alpha}$ (the identity of the group G_α). It follows that

$$a\rho = (x\rho)(a\rho) = (xa)\rho = (by)\rho = (b\rho)(y\rho) = b\rho.$$

Consequently, $\xi \subseteq \rho$, as required.

Observe that if S is an E-semigroup, then $x, y \in E_S$ (by the definition of ξ^*), so obviously $x\rho = y\rho = 1_{G_\alpha} \in E_{S/\rho}$. Thus $\xi^* \subseteq \rho$.

Note that $\xi, \xi^* \subseteq \eta \cap \sigma$ and denote by $B_{a\eta}$ the intersection of $a\eta$ and B ($a \in S$).

We have just shown the following theorem.

Theorem 2.1. *The least Clifford congruence on an idempotent-surjective R-semigroup S is given by*

$$\xi = \{(a, b) \in \eta : (\exists\, x, y \in B_{a\eta})\ xa = by\}. \qquad \square$$

Remark 2.2. In the light of Remark 1.2,

$$\xi = \{(a, b) \in \eta : (\exists\, x \in a\eta)\ xa, xb \in B_{a\eta}\}.$$

Corollary 2.3. *The least Clifford congruence on an idempotent-surjective E-semigroup S is given by*

$$\xi^* = \{(a, b) \in \eta : (\exists\, e, f \in E_{a\eta})\ ea = bf\}. \qquad \square$$

Note also that we have proved the first part of the following theorem which is new for regular semigroups (and it is probably new even for inverse semigroups).

Theorem 2.4. *Let ε be an arbitrary semilattice congruence on an idempotent-surjective R-semigroup S and let A be a seminormal subsemigroup of S. Then the relation*

$$\rho_{A,\varepsilon} = \{(a, b) \in \varepsilon : (\exists\, x, y \in a\varepsilon \cap A)\ xa = by\}$$

is a Clifford congruence on S.

Conversely, if ρ is a Clifford congruence on S, then there exists a semilattice congruence ε on S and a seminormal subsemigroup A of S such that $\rho = \rho_{A,\varepsilon}$.

Proof. Let ρ be a semilattice of groups congruence on S. Since S/ρ is a semilattice of groups, then the least semilattice congruence on S/ρ is $\mathcal{H}^{S/\rho}$. Define a relation ε on S, as follows: $(a, b) \in \varepsilon$ if and only if $(a\rho, b\rho) \in \mathcal{H}^{S/\rho}$. Then $\mathcal{H}^{S/\rho} = \varepsilon/\rho$. It follows that ε is a semilattice congruence on S, since $(S/\rho)/\mathcal{H}^{S/\rho} \cong S/\varepsilon$. Next, put

$$A = \bigcup\{e\rho : e \in E_S\}.$$

Since S is idempotent-surjective and $E_{S/\rho}$ is a subsemigroup of S/ρ, then A is a semigroup. Obviously, A is full. Finally, A is reflexive, since $E_{S/\rho}$ is reflexive.

Consequently, A is a seminormal subsemigroup of S. Further, note that $\rho \subseteq \varepsilon$, and consider an arbitrary ρ-class $e\rho$, where $e \in E_S$. Let $x \in (e\rho)\omega$ in $e\varepsilon$ (in particular, $(x\rho, e\rho) \in \mathcal{H}^{S/\rho}$). Then $ax \in e\rho$ for some $a \in e\rho$. Hence

$$e\rho = (a\rho)(x\rho) = (e\rho)(x\rho) = x\rho,$$

because $(x\rho, e\rho) \in \mathcal{H}^{S/\rho}$. Thus $e\rho$ is closed in $e\varepsilon$. Since $A \cap e\varepsilon = e\rho$ for every $e \in E_S$, then $\rho = \rho_{A,\varepsilon}$, as required. □

A congruence ρ on a semigroup S is called *idempotent pure* if $e\rho \subseteq E_S$ for all $e \in E_S$. Note that if S is idempotent-surjective, then ρ is idempotent pure if and only if $\ker(\rho) = E_S$.

Let $\mathcal{E}$ be the relation on a semigroup S induced by the partition $\{E_S,\, S \setminus E_S\}$. Then $\mathcal{E}^\flat$ is the greatest idempotent pure congruence on S. Put $\tau = \mathcal{E}^\flat$. Then [12]

$$\tau = \{(a,b) \in S \times S : (\forall x, y \in S^{(1)})\ xay \in E_S \Leftrightarrow xby \in E_S\},$$

where $S^{(1)}$ denotes the semigroup obtained from S by adjoining the identity 1.

Recall from [5] that an E-inversive semigroup S is *E-unitary* if and only if E_S is closed in S.

The following result will be useful.

Result 2.5. [5, 7] *Let S be an idempotent-surjective semigroup. Then the following conditions are equivalent*:

(a) *S is E-unitary*;

(b) $\ker(\sigma) = E_S$;

(c) *every idempotent pure congruence on S is E-unitary*;

(d) *there exists an idempotent pure E-unitary congruence on S*;

(e) $\sigma = \tau$. □

The following theorem gives necessary and sufficient conditions for ξ to be idempotent pure. Note that the condition (c) is new even for regular semigroups.

Theorem 2.6. *Let S be an idempotent-surjective R-semigroup. Then the following conditions are equivalent*:

(a) *ξ is idempotent pure*;

(b) *each η-class of S is an E-unitary E-inversive subsemigroup of S*;

(c) $\xi = \eta \cap \tau$.

Proof. (a) $\Longleftrightarrow$ (b). It follows from the construction of ξ and Result 2.5 (see (b)).

(a) $\Longrightarrow$ (c). Let ξ be idempotent pure, that is, $\xi \subseteq \tau$. Then evidently $\xi \subseteq \eta \cap \tau$. Conversely, let $a(\eta \cap \tau)b$. Take any weak inverse x of a in $a\eta$. Then $(xa, xb) \in \tau$, where $xa \in E_{a\eta}$. Since $xb \in a\eta$, then $xb \in E_{a\eta}$. Thus $(a,b) \in \xi$ (by Remark 2.2).

(c) $\Longrightarrow$ (a). This is trivial. □

Corollary 2.7. *Let S be an idempotent-surjective R-semigroup. Then ξ is idempotent pure if and only if S is a semilattice of E-unitary E-inversive semigroups.* □

Moreover, we have the following theorem.

Theorem 2.8. *Let S be an idempotent-surjective R-semigroup. Then the following conditions are equivalent*:

(a) *S is E-unitary*;

(b) *ξ is an idempotent pure E-unitary congruence on S*;

(c) *for every $a \in S$, $a\eta$ is E-unitary and $\sigma_{a\eta} = \sigma_S \cap (a\eta \times a\eta)$.*

Proof. $(a) \Longrightarrow (b)$. If S is E-unitary, then each η-class of S is also E-unitary and so, by Theorem 2.6, ξ is idempotent pure. Hence by Result 2.5, ξ is E-unitary.

$(b) \Longrightarrow (a)$. This follows from Result 2.5.

$(a) \Longrightarrow (c)$. Let $a \in S$. It is clear that $a\eta$ is E-unitary. Also, if $(a, b) \in \sigma$, then $ab^* \in E_S$ for all $b^* \in W(b)$, so if $(a, b) \in \sigma \cap (a\eta \times a\eta)$, then $ab^* \in E_{a\eta}$ for all $b^* \in W(b)$ in $a\eta$. Thus $ab^*b \in E_{a\eta}b$. It follows that $(a, b) \in \sigma_{a\eta}$. Therefore $\sigma \cap (a\eta \times a\eta) \subseteq \sigma_{a\eta}$. The converse inclusion is obvious.

$(c) \Longrightarrow (a)$. Let $e \in E_S$, $x \in a\eta$, where $a \in S$. Choose $f \in E_{a\eta}$ and suppose that $(x, e) \in \sigma_S$. Clearly, $(e, f) \in \sigma_S$. Hence $(x, f) \in \sigma_S \cap (a\eta \times a\eta) = \sigma_{a\eta}$. Thus $x \in E_S$, so S is E-unitary (by Result 2.5). □

The next result gives some equivalent conditions for ξ to be E-unitary, when ξ is idempotent pure.

Corollary 2.9. *Let an idempotent-surjective R-semigroup S be a semilattice of an E-unitary E-inversive semigroups. Then the following conditions are equivalent*:

(a) *S is E-unitary*;

(b) $\xi = \eta \cap \sigma$;

(c) *ξ is E-unitary*;

(d) *for every $a \in S$, $\sigma_{a\eta} = \sigma_S \cap (a\eta \times a\eta)$.*

Proof. $(a) \Longrightarrow (b)$. The main assumption of the corollary implies that ξ is idempotent pure (Corollary 2.7). Hence $\xi = \eta \cap \tau$ (Theorem 2.6). Since S is E-unitary, then $\tau = \sigma$ (Result 2.5). Thus $\xi = \eta \cap \sigma$.

$(b) \Longrightarrow (c)$. The congruences η and σ are both E-unitary. Therefore $\xi = \eta \cap \sigma$ is also E-unitary.

$(c) \Longrightarrow (a)$. The assumptions imply that the congruence ξ is idempotent pure and E-unitary. Thus S is E-unitary (Result 2.5).

$(a) \Longleftrightarrow (d)$. It is a consequence of Theorem 2.8. □

Finally, we have the following corollary.

Corollary 2.10. *In any E-unitary idempotent-surjective semigroup S,*

$$\xi \cap \mathcal{H} = 1_S.$$

If in addition E_S forms a semilattice, then

$$\xi \cap \mathcal{L} = \xi \cap \mathcal{R} = 1_S.$$

Proof. This follows from Theorem 5.5 [5], since $\xi \subseteq \sigma$. □

3. USG-congruences

A semigroup S is said to be a USG-*semigroup* if it is an E-unitary Clifford semigroup. Recall from [13] that if S is a USG-semigroup, then $\sigma \cap \eta = 1_S$.

Remark that if a semigroup is a subdirect product of a group and a semilattice, then it is an E-semigroup.

Theorem 3.1. *In any idempotent-surjective semigroup S, $\sigma \cap \eta = 1_S$ if and only if S is a* USG-*semigroup.*

Proof. Let $\sigma \cap \eta = 1_S$. Then S is a subdirect product of the group S/σ and the semilattice S/η, so S is an idempotent-surjective E-semigroup. In particular, the least Clifford congruence ξ exists on S. Also, $\xi \subseteq \sigma \cap \eta$ and so $\xi = 1_S$. Hence S is a semilattice of groups. Thus $\mathcal{H} = \eta$. Let $(x, e) \in \sigma$ (where $x \in S, e \in E_S$). Then (since $x \in \mathcal{H}_f$ for some $f \in E_S \subseteq e\sigma$) $(x, f) \in \sigma \cap \mathcal{H} = \sigma \cap \eta = 1_S$, so $x = f \in E_S$. Consequently, S is E-unitary. □

If ρ, υ are two congruences on S such that $\rho \subseteq \upsilon$, then the map $\varphi : S/\rho \to S/\upsilon$, $(a\rho)\varphi = a\upsilon$ $(a \in S)$, is a well-defined epimorphism between these semigroups. Denote its kernel $\varphi\varphi^{-1}$ by

$$\upsilon/\rho = \{(a\rho, b\rho) \in S/\rho \times S/\rho : a\,\upsilon\,b\}.$$

Then $(S/\rho)/(\upsilon/\rho) \cong S/\upsilon$. Also, each congruence α on S/ρ is of the form υ/ρ, where $\upsilon \supseteq \rho$ is a congruence on S. Indeed, the relation υ, defined on S by: $a\,\upsilon\,b$ if and only if $(a\rho, b\rho) \in \alpha$, is a congruence on S such that $\rho \subseteq \upsilon$ and $\alpha = \upsilon/\rho$. Finally, let $\rho \subseteq \upsilon_1, \upsilon_2$ (where υ_1, υ_2 are congruences on S). Then $(\upsilon_1/\rho) \cap (\upsilon_2/\rho) = (\upsilon_1 \cap \upsilon_2)/\rho$, and $(\upsilon_1 \cap \upsilon_2)/\rho = 1_{S/\rho}$ implies that $\rho = \upsilon_1 \cap \upsilon_2$.

Note that if a class $\mathcal{C}$ of semigroups is closed under homomorphic images and the least $\mathcal{C}$-congruence $\rho_S^{\mathcal{C}}$ on a semigroup S exists, then the interval $[\rho_S^{\mathcal{C}}, S \times S]$ consists of all $\mathcal{C}$-congruences on S and is a complete sublattice of $\mathcal{C}(S)$.

Theorem 3.2. *Let $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$ be some classes of semigroups; $\rho_A^{\mathcal{C}_1}$, $\rho_A^{\mathcal{C}_2}$ be the least $\mathcal{C}_1$-congruence, $\mathcal{C}_2$-congruence on any semigroup A, respectively, such that $A \in \mathcal{C}_3$ if and only if $\rho_A^{\mathcal{C}_1} \cap \rho_A^{\mathcal{C}_2} = 1_A$. Then the intersection of a $\mathcal{C}_1$-congruence and a $\mathcal{C}_2$-congruence on a semigroup S is a $\mathcal{C}_3$-congruence. Conversely, every $\mathcal{C}_3$-congruence on S can be expressed in this way.*

Proof. Let ρ_i be a $\mathcal{C}_i$-congruence on S (for $i = 1, 2$). Put $\rho = \rho_1 \cap \rho_2$ and observe that ρ_1/ρ is a $\mathcal{C}_1$-congruence, ρ_2/ρ is a $\mathcal{C}_2$-congruence on S/ρ. Since $(\rho_1/\rho) \cap (\rho_2/\rho)$ is the identity relation on S/ρ, then $\rho_{S/\rho}^{\mathcal{C}_1} \cap \rho_{S/\rho}^{\mathcal{C}_2} = 1_{S/\rho}$. Thus $S/\rho \in \mathcal{C}_3$, and so $\rho = \rho_1 \cap \rho_2$ is a $\mathcal{C}_3$-congruence on S.

Conversely, let ρ be any $\mathcal{C}_3$-congruence on S, $\rho_1/\rho = \rho_{S/\rho}^{\mathcal{C}_1}$, $\rho_2/\rho = \rho_{S/\rho}^{\mathcal{C}_2}$, where $\rho \subseteq \rho_1, \rho_2$. Then ρ_i is a $\mathcal{C}_i$-congruence on S (for $i = 1, 2$). Furthermore,

$$(\rho_1 \cap \rho_2)/\rho = \rho_{S/\rho}^{\mathcal{C}_1} \cap \rho_{S/\rho}^{\mathcal{C}_1} = 1_{S/\rho}.$$

Thus $\rho = \rho_1 \cap \rho_2$, as required. □

Remark 3.3. One can modify Theorem 3.2 for any type of a universal algebra.

The following theorem describes all USG-congruences on idempotent-surjective semigroups.

Theorem 3.4. *The intersection of a group congruence ν and a semilattice congruence γ on an idempotent-surjective semigroup S is a* USG*-congruence.*

Conversely, any USG*-congruence ρ on S can be expressed in this way, and ν, γ are uniquely determined by ρ.*

Proof. Note that the class of all idempotent-surjective semigroups is closed under homomorphic images. All assertions of the theorem except a uniqueness follows from Theorems 3.1, 3.2 (see the proof of Theorem 3.2).

Let $\rho = \nu_1 \cap \gamma_1 = \nu_2 \cap \gamma_2$, where ν_i is a group congruence and γ_i is a semilattice congruence on S $(i = 1, 2)$, and let $(a, b) \in \gamma_1$. Since $\gamma_1 \cap \gamma_2$ is a band congruence, then there are $e, f \in E_S$ such that $(a, e) \in \gamma_1 \cap \gamma_2$, $(e, f) \in \nu_1$ and $(f, b) \in \gamma_1 \cap \gamma_2$. In fact, $(e, f) \in \gamma_1 \cap \nu_1 = \gamma_2 \cap \nu_2 \subseteq \gamma_2$. Hence $(a, b) \in \gamma_2$. Thus $\gamma_1 \subseteq \gamma_2$. Similarly, we obtain the opposite inclusion, so $\gamma_1 = \gamma_2$. Put $\gamma_1 = \gamma_2 = \gamma$. Let $(a, b) \in \nu_1$. Then $(aab, abb) \in \nu_1 \cap \gamma \subseteq \nu_2$. Hence $(a, b) \in \nu_2$ (by cancellation), therefore, $\nu_1 \subseteq \nu_2$. By symmetry, $\nu_2 \subseteq \nu_1$. Consequently, $\nu_1 = \nu_2$, as required. □

Corollary 3.5. *The relation $\sigma \cap \eta$ is the least* USG*-congruence on an arbitrary idempotent-surjective semigroup S.* □

Corollary 3.6. *An idempotent-surjective semigroup is a subdirect product of a group and a semilattice if and only if it is a* USG*-semigroup.*

Proof. Let $S \subseteq G \times Y$ be a subdirect product of a group G and a semilattice Y. Then the two projection maps induce on S a group congruence and a semilattice congruence. The intersection of these congruences is the equality relation on S. Thus $\sigma \cap \eta = 1_S$, so S is a USG-semigroup (Theorem 3.1).

The converse implication is clear. □

Lemma 3.7. *Let S be an E-unitary idempotent-surjective semigroup. Then S/ξ is a* USG*-semigroup.*

Proof. Let S be E-unitary. Then every η-class of S is E-unitary, too. In the light of Theorem 2.6, ξ is idempotent pure. Hence ξ is E-unitary (Corollary 2.9). Thus S/ξ is a USG-semigroup. □

One can show without difficulty that the least E-unitary congruence π on an arbitrary E-inversive semigroup exists.

Lemma 3.8. *Let S be an idempotent-surjective R-semigroup. Then the relation*

$$(\xi \vee \pi)/\pi$$

is the least Clifford congruence on S/π.

Proof. Indeed, $S/(\xi \vee \pi)$ is a Clifford semigroup, so $(\xi \vee \pi)/\pi$ is a semilattice of groups congruence on S/π, since $S/(\xi \vee \pi) \cong (S/\pi)/((\xi \vee \pi)/\pi)$. On the other hand, if α is a semilattice of groups congruence on S/π, then $\alpha = \rho/\pi$, where $\pi \subseteq \rho$. Since $(S/\pi)/(\rho/\pi) \cong S/\rho$, then ρ is a Clifford congruence on S, so π, $\xi \subseteq \rho$. Hence $\xi \vee \pi \subseteq \rho$. Thus $(\xi \vee \pi)/\pi \subseteq \rho/\pi = \alpha$, as required. □

Theorem 3.9. *In any idempotent-surjective R-semigroup S,*

$$\sigma \cap \eta = \xi \vee \pi.$$

Proof. We have just seen that $S/(\xi \vee \pi) \cong (S/\pi)/((\xi \vee \pi)/\pi)$. By Lemmas 3.7, 3.8, $(S/\pi)/((\xi \vee \pi)/\pi)$ is an E-unitary semilattice of groups and so $S/(\xi \vee \pi)$ is also an E-unitary semilattice of groups. Thus $\xi \vee \pi$ is a USG-congruence on S. Moreover, $\xi \subseteq \sigma \cap \eta$ and $\pi \subseteq \sigma \cap \eta$. Hence $\xi \vee \pi \subseteq \sigma \cap \eta$. Thus $\xi \vee \pi = \sigma \cap \eta$ (because $\sigma \cap \eta$ is the least USG-congruence on S). □

Corollary 3.10. *In any E-unitary idempotent-surjective semigroup,*

$$\xi = \sigma \cap \eta.$$ □

4. The condition $\pi \cap \xi = 1_S$

In this section we characterize those idempotent-surjective R-semigroups S which are a subdirect product of an E-unitary semigroup and a Clifford semigroup, i.e., those semigroups S for which $\pi \cap \xi$ is the identity relation. Since E-unitary semigroups and Clifford semigroups are both E-semigroups, then S are E-semigroups, too.

In [2] Edwards defined the relation μ on a semigroup S by

$$(a, b) \in \mu \iff \begin{cases} (x \,\mathcal{L}\, ax \text{ or } x \,\mathcal{L}\, bx) \Longrightarrow ax \,\mathcal{H}\, bx, \\ (x \,\mathcal{R}\, xa \text{ or } x \,\mathcal{R}\, xb) \Longrightarrow xa \,\mathcal{H}\, xb, \end{cases}$$

where x is an arbitrary element of $Reg(S)$. Furthermore, he proved in [3] that μ is the maximum *idempotent-separating* congruence on an arbitrary idempotent-surjective semigroup S (that is, $\mu \cap (E_S \times E_S) = 1_S$).

Recall that a semigroup S is:

- *fundamental* if $\mu = 1_S$ [1];
- *η-simple* if $\eta = S \times S$ [20].

Note that if an E-inversive semigroup S is η-simple, then the least Clifford congruence ξ coincides with σ. Indeed, let ρ be a Clifford congruence on S. Since S/ρ is a Clifford semigroup, then the least semilattice congruence on S/ρ is $\mathcal{H}$. Define a relation ε on S, as follows: $(a, b) \in \varepsilon$ if $(a\rho)\mathcal{H}(b\rho)$. Then $\mathcal{H} = \varepsilon/\rho$, so ε is a semilattice congruence on S, since $(S/\rho)/\mathcal{H} \cong S/\varepsilon$. Thus $(a\rho)\mathcal{H}(b\rho)$ for all $a, b \in S$. Consequently, S/ρ is a group.

Recall that π denotes the least E-unitary congruence on an E-inversive semigroup. Clearly, $\pi \subseteq \sigma$ (the least group congruence).

From the last two paragraphs we obtain the following corollary.

Corollary 4.1. *Let S be an η-simple E-inversive semigroup. Then S is E-unitary if and only if $\pi \cap \xi = 1_S$.* □

Proposition 4.2. *Let S be an idempotent-surjective R-semigroup, $\pi \cap \xi = 1_S$. Then S is a semilattice of (η-simple) E-unitary E-inversive semigroups.*

Proof. It is sufficient to show that every η-class of S is E-unitary. Let $a \in S$. Then the restriction of π to $a\eta$ is an E-unitary congruence on $a\eta$ and the restriction of ξ to $a\eta$ is a group congruence on $a\eta$. From the assumption of the proposition follows that the intersection of these two congruences is the identity relation on $a\eta$, so the intersection of the least E-unitary congruence and the least Clifford congruence on $a\eta$ is also the identity relation. In the light of Corollary 4.1, $a\eta$ is E-unitary. □

Theorem 4.3. *Let S be a fundamental idempotent-surjective R-semigroup. Then $\pi \cap \xi = 1_S$ if and only if S is E-unitary.*

Proof. Let $\pi \cap \xi = 1_S$; $e, f \in E_S$. If $(e,f) \in \pi$, then $(e,f) \in \eta$. Hence $(e,f) \in \xi$. Thus $e = f$, so $\pi \subseteq \mu = 1_S$. Consequently, S is E-unitary.

The converse implication is trivial. □

Remark 4.4. The above theorem is valid for any $\mathcal{C}$-congruence ρ (instead of π) contained in η (i.e., if we replace in the theorem π by ρ, then we must replace "E-unitary" with "$\mathcal{C}$-semigroup").

Recall from [7] that (for idempotent-surjective semigroups) every congruence of the interval $[\pi, \sigma]$ is E-unitary. Also, $\ker(\rho) = \ker(\pi)$ for every $\rho \in [\pi, \sigma]$.

We have mentioned above that the class of idempotent-surjective semigroups is closed under homomorphic images. Using Hall's observation, one can prove without difficulty that the class of all idempotent-surjective R-semigroups possess this property. It is also known that the class of all structurally regular semigroups is closed under taking homomorphic images [14].

For regular semigroups S, $\mu \cap \tau = 1_S$. The next theorem gives necessary and sufficient conditions for $\pi \cap \xi$ to be the identity relation on idempotent-surjective R-semigroups S such that $\mu \cap \tau = 1_S$ (in particular, the theorem is valid, too, for structurally regular semigroups having this additional property).

Remark 4.5. Using Lemma 1.2 [17], Janet Mills proved for orthodox semigroups a similar result to the next theorem (see Theorem 3.5 [17]). However, the proof of her lemma is not correct (see [6]). Moreover, in [6] using different methods, the author showed the theorem of Mills (with a very important additional condition). Finally, notice that the implication "$(f) \Rightarrow (g)$" in the following theorem is proved in a different way than the corresponding implication in [6].

Theorem 4.6. *If S is an idempotent-surjective R-semigroup such that $\mu \cap \tau = 1_S$, then the following conditions are equivalent*:

(*a*) $\pi \cap \xi = 1_S$;

(*b*) *S is a semilattice of E-unitary E-inversive semigroups and $\pi \subseteq \mu$*;

(*c*) *S is a semilattice of E-unitary E-inversive semigroups and $\pi \subseteq \mu \cap \sigma \subseteq \sigma$*;

(*d*) *S is a semilattice of E-unitary E-inversive semigroups and the congruence $\mu \cap \sigma$ is E-unitary*;

(*e*) *S is a semilattice of E-unitary E-inversive semigroups and at least one idempotent-separating congruence on S (say ρ) is E-unitary*;

(*f*) *S is a subdirect product of an E-unitary idempotent-surjective semigroup and a Clifford semigroup*;

(*g*) *S is a semilattice of E-unitary E-inversive semigroups and the relation $\mathcal{H} \cap \sigma$ is E-unitary congruence on S.*

Proof. $(a) \Longrightarrow (b)$. This implication follows directly from Proposition 4.2 and from the proof of Theorem 4.3.

$(b) \Longrightarrow (c)$. This is clear, since $\pi \subseteq \sigma$.

$(c) \Longrightarrow (d)$. In that case, $\mu \cap \sigma \in [\pi, \sigma]$, so $\mu \cap \sigma$ is E-unitary.

$(d) \Longrightarrow (e)$. This is evident.

$(e) \Longrightarrow (a)$. In such case, $\pi \subseteq \rho \subseteq \mu$. Hence $\pi \cap \xi \subseteq \mu \cap \xi = \mu \cap (\eta \cap \tau)$ (see Corollary 2.7 and Theorem 2.6). Thus $\pi \cap \xi \subseteq \mu \cap \tau = 1_S$.

$(a) \Longrightarrow (f)$. This is clear.

$(f) \Longrightarrow (g)$. Suppose that S is a subdirect product of an E-unitary idempotent-surjective semigroup A and a Clifford semigroup T. Notice that $(a,t)(\mathcal{H} \cap \sigma)(b,w)$ in S if and only if $(a,b) \in \mathcal{H} \cap \sigma$ in A and $(t,w) \in \mathcal{H} \cap \sigma = \eta \cap \sigma$ in T, i.e., if and only if $a = b$ (Theorem 5.5 [5]) and $(t,w) \in \eta \cap \sigma$ in T. This implies that $\mathcal{H} \cap \sigma$ is a congruence on S. Finally, we will show that the congruence $\mathcal{H} \cap \sigma$ is E-unitary. Let

$$(e,g)(a,t)(\mathcal{H} \cap \sigma)(f,h),$$

where $(e,g),(f,h) \in E_S$, then $ea = f$ and $(gt,h) \in \mathcal{H} \cap \sigma$ in T. It follows that

$$a \in E_A \quad \& \quad t \in \ker(\sigma_T).$$

Hence

$$(t,i) \in \mathcal{H}^T \cap \sigma_T$$

for some $i \in E_T$, since T is a semilattice of groups. Consequently,

$$(a,t)(\mathcal{H} \cap \sigma)(a,i),$$

where $(a,i) \in E_S$, so $\mathcal{H} \cap \sigma$ is E-unitary.

$(g) \Longrightarrow (e)$. This is evident. □

References

[1] **D. Easdown**, *Biorder-preserving coextensions of fundamental semigroups*, Proc. Edinburgh Math. Soc. **31** (1988), 463–467.

[2] **P.M. Edwards**, *Eventually regular semigroups*, Bull. Austral. Math. Soc. **28** (1983), 23–38.

[3] **P.M. Edwards**, *Maximizing a congruence with respect to its partition of idempotents*, Semigroup Forum **39** (1985), 313–317.

[4] **R.S. Gigoń**, *Some results on E-inversive semigroups*, Quasigroups Relat. Systems **20** (2012), 53–60 .

[5] **R.S. Gigoń**, *Congruences and group congruences on a semigroup*, Semigroup Forum (in print), doi:10.1007/s00233-012-9425-z.

[6] **R.S. Gigoń**, *Comment on the paper of Janet E. Mills: "Certain congruences on orthodox semigroups"*, (to appear in Studia Sci. Math. Hungarica).

[7] **R.S. Gigoń**, *On the lattice of congruences on idempotent-regular-surjective semigroups*, (to appear in Communications in Algebra).

[8] **R.S. Gigoń**, *Regular congruences on an idempotent-regular-surjective semigroup*, Bull. Australian Math. Soc. (in print).

[9] **G. Gomes**, *A characterization of the group congruences on a semigroup*, Semigroup Forum **46** (1993), 48–53.

[10] **T.E. Hall**, *On regular semigroups*, J. Algebra **24** (1973), 1–24.

[11] **J.M. Howie**, *An introduction to semigroup theory*, Academic Press, London (1976).

[12] **J.M. Howie**, *Fundamentals of semigroup theory*, Oxford University Press, New York (1995).

[13] **J.M. Howie and G. Lallement**, *Certain fundamental congruences on a regular semigroup*, Proc. Glasgow Math. Soc. **7** (1966), 145–159.

[14] **S.J.L. Kopamu**, *The concept of structural regularity*, Portugaliae Math. **53** (1996), 435–456.

[15] **G. Lallement**, *Congruences et équivalences de Green sur un demi-groupe régulier*, C. R. Acad. Sci. Paris **262A** (1966), 613–616.

[16] **D.R. LaTorre**, *The least semilattice of groups congruence on a regular semigroup*, Semigroup Forum **27** (1983), 319–329.

[17] **J.E. Mills**, *Certain congruences on orthodox semigroups*, Pac. J. Math. **64** (1976), 317–226.

[18] **H. Mitsch and M. Petrich**, *Restricting idempotents in E-inversive semigroups*, Acta Sci. Math. (Szeged) **67** (2001), 555–570.

[19] **M. Petrich**, *Inverse semigroups*, Wiley, New York (1984).

[20] **T. Tamura**, *Note of the greatest semilattice decomposition of semigroups*, Semigroup Forum **4** (1972), 255–261.

[21] **G. Thierrin**, *Demi-groupes inversés et rectangulaires*, Bull. Cl. Sci. Acad. Roy. Belgique **41** (1955), 83–92.

Received August 10, 2012
Revised December 20, 2012

Institute of Mathematics and Computer Science, Wroclaw University of Technology,
Wyb. Wyspiańskiego 27, 50–370 Wrocław, Poland
E-mail: romekgigon@tlen.pl

Quasigroups and Related Systems **20** (2012), 233 − 238

A new characterization of Osborn-Buchsteiner loops

Tèmítọ́pẹ́ Gbọ́láhàn Jaiyéọlá and John Olúsọlá Adéníran

Abstract. In the study of loops of Bol-Moufang types, a question that quickly comes to mind is this. Since a loop is an extra loop if and only if it is a Moufang loop and a CC-loop(or C-loop), then can one generalize this statement by identifying a "new identity" for a loop which generalizes the C-loop identity such that we can say "An Osborn loop is a Buchsteiner loop if and only if it obeys "certain" identity? A somewhat close answer to this question is the unpublished fact by M. K. Kinyon that "An Osborn loop Q with nucleus N is a Buchsteiner loop if and only if Q/N is a Boolean group" where Q/N being a Boolean group somewhat plays the role of the missing identity. It is proved that an Osborn loop is a Buchsteiner loop if and only if it satisfies the identity $(x \cdot xy)(x^\lambda \cdot xz) = x(x \cdot yz)$. The importance of its emergence which was traced from the facts that Buchsteiner loops generalize extra loops while Osborn loops generalize Moufang loops is the fact that not every Osborn-Buchsteiner loop is an extra loop. An LC-loop obeys this identity. An Osborn-Buchsteiner loop (OBL) is shown to be nuclear square and to obey the identity $x^\rho \cdot xx = xx \cdot x^\lambda = x$. Necessary and sufficient condition for a OBL to be central square is established. It is shown that in an OBL, the cross inverse property and commutativity are equivalent, and the properties: 3-power associativity $(xx \cdot x = x \cdot xx)$, self right inverse property $(xx \cdot x^\rho = x)$, self left inverse property $(x^\lambda \cdot xx = x)$ and $x^\rho = x^\lambda$ are equivalent.

1. Introduction

Let L be a nonempty set with a binary operation denoted by juxtaposition. If the system of equations: $ax = b$, $ya = b$ has unique solutions x and y respectively, then $(L, \cdot)$ is called a *quasigroup*. Furthermore, if there exists a unique element $e \in L$ called the *identity* such that for all $x \in L$, $xe = ex = x$, $(L, \cdot)$ is called a *loop*. For each $x \in L$, the elements $x^\rho = xJ_\rho$, $x^\lambda = xJ_\lambda$ such that $xx^\rho = e = x^\lambda x$ are called the *right*, *left inverses* of x respectively. For any $x, y \in L$, we shall take $(xy)(x, y) = yx$, where $(x, y) \in L$ is called the *commutator* of x and y.

The triple $\alpha = (A, B, C)$ of bijections on a loop $(L, \cdot)$ is called an *autotopism* if and only if

$$xA \cdot yB = (xy)C \quad \text{for all } x, y \in L.$$

2010 Mathematics Subject Classification: 20N02, 20NO5

Keywords: Osborn loop, Buchsteiner loop.

The authors dedicate this paper to the 50$^{\text{th}}$ Anniversary of Obafemi Awolowo University

Such triples form a group $AUT(L,\cdot)$ called the *autotopism group* of $(L,\cdot)$. For an overview of the theory of loops, readers may check [10, 19].

Further to reduce of number of brackets we will use dots instead of some brackets. For example, the formula $x((yz)x)$ will be written as $x(yz\cdot x)$.

A loop that satisfies any of the following equivalent identities is called an *Osborn* loop.

$$\begin{aligned} OS_0 &: x(yz\cdot x)=x(yx^{\lambda}\cdot x)\cdot zx, && (1)\\ \mathrm{OS}_1 &: x(yz\cdot x)=[x(yx\cdot x^{\rho})]\cdot zx, && (2)\\ \mathrm{OS}_2 &: x[(x^{\lambda}y)z\cdot x]=y\cdot zx, && (3)\\ \mathrm{OS}_3 &: (x\cdot yz)x=xy\cdot[(x^{\lambda}\cdot xz)\cdot x], && (4)\\ \mathrm{OS}_4 &: [x\cdot y(zx^{\rho})]x=xy\cdot z. && (5)\end{aligned}$$

Kinyon [17] revived the study of Osborn loops in 2005. The most popularly known varieties of Osborn loops are: VD-loops (Basarab [1]), Moufang loops, CC-loops, universal weak inverse property loops and extra loops. Some recent works on Osborn loops are Jaiyéọlá [11, 12], Jaiyéọlá and Adéníran [13, 14, 15], and Jaiyéọlá, Adéníran and Sòlárìn [16].

The *Buchsteiner* law

$$\mathrm{BL} : x\backslash(xy\cdot z)=(y\cdot zx)/x$$

was first introduced by Buchsteiner [2]. Its study in loops is on revival by Csörgő et. al. [3, 4, 5] and Drápal et. al. [6, 7, 8]. Buchsteiner loops are G-loops and extra loops belongs to their class.

Buchsteiner loops generalize extra loops while Osborn loops generalize Moufang loops. A question that quickly comes to mind is this: since a loop is an extra loop if and only if it is a Moufang loop and a CC-loop (or C-loop), then can one generalize this statement by identifying a new identity that describes a new class of loop which generalizes a C-loop such that we can say "An Osborn loop is a Buchsteiner loop if and only if it is a "certain" loop?" A some what close answer to this question is the unpublished fact by M. K. Kinyon that "An Osborn loop Q with nucleus N is a Buchsteiner loop if and only if Q/N is a Boolean group" where Q/N being a Boolean group some what plays the role of the missing loop variety. It will be shown in this study that this new class of loop is described by the identity

$$(x\cdot xy)(x^{\lambda}\cdot xz)=x(x\cdot yz). \qquad (6)$$

LC-loops fall into this class. It must be noted that when Drápal and Jedlička [6] used nuclear identification to obtain some loop identities, the Osborn and our new loop identities did not feature among such identities. We shall refer to an Osborn loop which obeys the Buchsteiner law as an *Osborn-Buchsteiner* loop.

Theorem 1.1. (Proposition 2.5 in [5]) *Let Q be a CC-loop with nucleus $N(Q)$. Then Q is a Buchsteiner loop if and only if $x^2\in N(Q)$ for every $x\in Q$.* □

We got the following unpublished result from Kinyon through personal contact.

Theorem 1.2. (Kinyon, 2009) *Let Q be a loop with nucleus $N = N(Q)$. Any two of the following implies the third.*
1. *Q is an Osborn loop.*
2. *Q is a Buchsteiner loop.*
3. *N is a normal in Q and Q/N is a Boolean group.* □

We can also say that:

Theorem 1.3. *Let Q be an Osborn loop with nucleus $N = N(Q)$. Then Q is a Buchsteiner loop if and only if Q/N is a Boolean group. Hence, Q is an Osborn loop that is nuclear square.* □

Theorem 1.4. (Theorem 11.3 in [5]) *Let Q be a Buchsteiner loop with nucleus $N = N(Q)$. If $|Q| < 32$, then Q is a CC-loop. If $|Q| < 64$, then Q/N has exponent* 2. □

Theorem 1.5. (Theorem 7.14 in [5]) *Let Q be a Buchsteiner loop with nucleus $N = N(Q)$. Then Q/N is an abelian group of exponent* 4. □

Theorem 1.2 is a generalization of Theorem 1.1.

2. Main Results

Theorem 2.1. *An Osborn loop is a Buchsteiner loop if and only if it obeys identity* (6)*. Hence, it is a nuclear square loop and the loop modulo its nucleus is an abelian group of exponent* 2.

Proof. Using the identities OS_1, OS_2 and OS_3 of an Osborn loop $(L, \cdot)$ and the identity BL of a Buchsteiner loop L, it can be shown that

$$(R_xR_{x^\rho}L_x^2, I, R_xT_{(x)}^{-1}L_x) \in AUT(L). \tag{7}$$

This is done as follows. Take $T_{(x)} = R_xL_x^{-1}$. From equation (2),

$$R_zR_xL_x = R_xR_{x^\rho}L_xR_{zx} \Leftrightarrow R_{zx} = L_x^{-1}R_{x^\rho}^{-1}R_x^{-1}R_zR_xL_x.$$

From the Buchsteiner law, $R_{zx} = L_xR_zL_x^{-1}R_x$. So,

$$\begin{gathered}L_xR_zL_x^{-1}R_x = L_x^{-1}R_{x^\rho}^{-1}R_x^{-1}R_zR_xL_x \Leftrightarrow R_xR_{x^\rho}L_x^2R_zL_x^{-1}R_x = R_zR_xL_x \Leftrightarrow\\ yR_xR_{x^\rho}L_x^2R_zL_x^{-1}R_x = yR_zR_xL_x \Leftrightarrow yR_xR_{x^\rho}L_x^2R_zL_x^{-1}R_x = (yz)R_xL_x \Leftrightarrow\\ yR_xR_{x^\rho}L_x^2 \cdot z = (yz)R_xT_{(x)}^{-1}L_x \Leftrightarrow (R_xR_{x^\rho}L_x^2, I, R_xT_{(x)}^{-1}L_x) \in AUT(L).\end{gathered}$$

Thus, if an Osborn loop L is a Buchsteiner loop, then (7) holds. Doing the reverse of the procedure above, it is also true that if in an Osborn loop L holds (7), then

L is a Buchsteiner loop. So, we have shown that an Osborn loop is a Buchsteiner loop if and only if (7) holds.

From equation (3), $(L_{x^\lambda}, R_x^{-1}, L_x^{-1}R_x^{-1}) \in AUT(L)$ while from equation (4), $(L_x, L_xL_{x^\lambda}R_x, L_xR_x) \in AUT(L)$. Thus,

$$(L_xL_{x^\lambda}, L_xL_{x^\lambda}, L_xR_xL_x^{-1}R_x^{-1}) = (L_xL_{x^\lambda}, L_xL_{x^\lambda}, L_xT_{(x)}R_x^{-1}) \in AUT(L).$$

Therefore, in an Osborn loop L, keeping in mind that $L_xL_{x^\lambda}R_xR_{x^\rho} = I$,

$$(L_xL_{x^\lambda}, L_xL_{x^\lambda}, L_xT_{(x)}R_x^{-1})(R_xR_{x^\rho}L_x^2, I, R_xT_{(x)}^{-1}L_x) =$$
$$(L_xL_{x^\lambda}R_xR_{x^\rho}L_x^2, L_xL_{x^\lambda}, L_x^2) = (L_x^2, L_xL_{x^\lambda}, L_x^2) \in AUT(L)$$
$$\Leftrightarrow (x \cdot xy)(x^\lambda \cdot xz) = x(x \cdot yz).$$

Thus, we have shown that an Osborn loop which is also a Buchsteiner loop obeys the identity (6). Assuming the identity (6) is true in the Osborn loop L and doing the reverse of the process above, it will be observed that (7) holds, hence by the earlier fact, L is a Buchsteiner loop. Recall that (7) implies $yR_xR_{x^\rho}L_x^2 \cdot z = (yz)R_xT_{(x)}^{-1}L_x$ for all $y, z \in L$. Substituting $z = e$, we have

$$R_xR_{x^\rho}L_x^2 = R_xT_{(x)}^{-1}L_x \text{ for all } x \in L. \tag{8}$$

So, (7) implies $yR_xR_{x^\rho}L_x^2 \cdot z = (yz)R_xR_{x^\rho}L_x^2$ for all $y, z \in L$. Substituting $y = e$, we see that $x^2z = zR_xR_{x^\rho}L_x^2$ implies $L_{x^2} = R_xR_{x^\rho}L_x^2$ for all $x \in L$. Thus, $(L_{x^2}, I, L_{x^2}) \in AUT(L)$ which means that $x^2 \in N$ for all $x \in L$. That is, L is nuclear square. Thus, by Theorem 1.5, L/N is a Boolean group. □

From Theorem 2.1 we can deduce that in Theorem 1.2 conditions 1. and 2. imply 3. The proof of Theorem 2.1 was carried out without the knowledge of Theorem 1.2.

Corollary 2.2. *Let Q be an Osborn loop with nucleus $N = N(Q)$. The following are equivalent:*

1. *Q is a Buchsteiner loop,*
2. *Q/N is a Boolean group,*
3. *Q obeys (6).*

Hence, Q is an Osborn loop that is nuclear square.

Proof. The proof follows from Theorem 1.3 and Theorem 2.1. □

Lemma 2.3. *Let $(Q, \cdot)$ be an Osborn loop that is nuclear square. Then*

1. $x^\rho \cdot xx = xx \cdot x^\lambda = x$.
2. *The following are equivalent:* $xx \cdot x^\rho = x$, $x^\lambda \cdot xx = x$, $x^\rho = x^\lambda$ *and* $xx \cdot x = x \cdot xx$. *Hence,* $(x^2, x^\rho) = (x^2, x^\lambda) = e$.
3. *L is central square if and only if* $x \cdot (x^\lambda y \cdot x)x = x(x \cdot yx^\rho) \cdot x$.

Proof. 1. By OS_1, $x(yz \cdot x) = [x(yx \cdot x^\rho)] \cdot zx$. Substituting $z = x$, we have $x(yx \cdot x) = [x(yx \cdot x^\rho)] \cdot xx \Rightarrow (yx \cdot x) = (yx \cdot x^\rho)(xx) \Rightarrow x^\rho \cdot xx = x$. Doing a similar thing with OS_3, we get $xx \cdot x^\lambda = x$.

2. Using OS_0 the way OS_1 was used above, we get $yx \cdot x = (yx^\lambda \cdot x)(xx)$. Taking $y = x$, it is easy to see that $xx \cdot x = x \cdot xx$ if and only if $x^\rho = x^\lambda$. In Lemma 3.20 of [16], the equivalence of the first three identities was proved in an Osborn loop. Hence, the equivalence of the four identities follows.

3. In OS_2, $x[(x^\lambda y)z \cdot x] = y \cdot zx$, making $z = x$, we get $R_{x^2} = L_{x^\lambda} R_x^2 L_x$. Doing a similar thing with OS_4, we have $L_{x^2} = R_{x^\rho} L_x^2 R_x$. So, L is central square if and only if $R_{x^2} = L_{x^2} \Leftrightarrow L_{x^2} = R_{x^\rho} L_x^2 R_x = R_{x^\rho} L_x^2 R_x \Leftrightarrow x \cdot (x^\lambda y \cdot x)x = x(x \cdot yx^\rho) \cdot x$. □

Lemma 2.4. *Let $(Q, \cdot)$ be an Osborn-Buchsteiner loop. Then*

1. *the following are equivalent: $xx \cdot x^\rho = x$, $x^\lambda \cdot xx = x$, $x^\rho = x^\lambda$, $xx \cdot x = x \cdot xx$ and $(x \cdot xy)x = x(x \cdot yx)$. Hence, $(x, y) = e$ if and only if $(x, x \cdot xy) = e$ or $(x, x \cdot yx) = e$.*
2. *$(x \cdot yx^\rho)x = xy$.*
3. *L is a cross inverse property loop if and only if L is commutative.*

Proof. 1. The equivalence of the first four identities follows from 1. of Lemma 2.3. From identity (6), $(x \cdot xy)(x^\lambda \cdot xz) = x(x \cdot yz)$, so taking $z = x$, $(x \cdot xy)(x^\lambda \cdot xx) = x(x \cdot yx)$, so $x^\lambda \cdot xx = x \Leftrightarrow (x \cdot xy)x = x(x \cdot yx)$.

2. Recall that from (8), $R_x R_{x^\rho} L_x^2 = R_x T_{(x)}^{-1} L_x$, for all $x \in L$. Putting $T_{(x)} = R_x L_x^{-1}$, we get $R_{x^\rho} L_x R_x = L_x \Leftrightarrow (x \cdot yx^\rho)x = xy$.

3. This follows from 2. above. □

Not all Osborn-Buchsteiner loops are extra loops. A loop is said to be *nuclear square* if the square of each element is nuclear (i.e. in the nucleus). It is well known from Fenyves [9] that extra loops are nuclear square loops. In Table 2 of the last section of [18], the authors established the fact that there exists a non-extra CC-loop that is nuclear square by constructing a power associative CC-loop of order 16 that is nuclear square. Thus, by Theorem 1.1, such a loop is a Buchsteiner loop, hence an Osborn-Buchsteiner loop. This fact can also be corroborated with Theorem 1.4 following the fact that $|Q| < 32$.

Furthermore, in [Page 7, [4]], it was observed that not every Buchsteiner loop Q with nucleus N such that Q/N is a Boolean group has to be a CC-loop. Hence, since Q/N is a Boolean group implies Q is nuclear square, then there exist nuclear square Buchsteiner loops that are not CC-loops.

As shown in Corollary 2.1, Theorem 2.1 is another characterization of Osborn-Buchsterner loops in identity form relative to the group-structural characterization form of Q modulo N being a Boolean group. The importance of this characterization can be linked to the fact that Buchsteiner [2] originally claimed that in a Buchsteiner loop Q, Q/N is a Boolean group, while [5] clarified this statement by showing in Theorem 1.5 that Q/N is actually an abelian group of exponent 4.

Kinyon in personal correspondence went further to show that a Buchsteiner loop Q for which Q/N is a Boolean group must be an Osborn loop. So, a single identity to describe a Osborn-Buchsterner loop Q for which Q/N is a Boolean group is (6).

References

[1] **A.S. Basarab**, *Generalised Moufang G-loops*, Quasigroups and Related Systems **3** (1996), 1 – 6.

[2] **H.H. Buchsteiner**, *O nekotorom Klasse binarnych lup*, Mat. Issled. **39** (1976), 54 – 66.

[3] **P. Csörgő and A. Drápal**, *On loops rich in automorphisms that are abelian modulo the nucleus*, Forum Math. **21** (2009), 477 – 489.

[4] **P. Csörgő and A. Drápal**, *Buchsteiner loops and conjugacy closedness*, Comm. Algebra **38** (2010), 11 – 27.

[5] **P. Csörgő, A. Drápal and M.K. Kinyon**, *Buchsteiner loops*, Internat. J. Algebra Comput. **19** (2009), 1049 – 1088.

[6] **A. Drápal and P. Jedlička**, *On loop identities that can be obtained by a nuclear identification*, European J. Combin. **31**(7) (2010), 1907 – 1923.

[7] **A. Drápal and M. K. Kinyon**, *Buchsteiner loops: associators and constructions*, Submitted. arXiv:0812.0412.

[8] **A. Drápal and K. Kunen**, *Buchsteiner loops of the smallest order*, pre-print.

[9] **F. Fenyves**, *Extra loops II*, Publ. Math. Debrecen, **16** (1969), 187 – 192.

[10] **T.G. Jaiyéọlá**, *A study of new concepts in smarandache quasigroups and loops*, ProQuest Information and Learning(ILQ), Ann Arbor, USA, 2009.

[11] **T.G. Jaiyéọlá**, *On Three Cryptographic Identities in Left Universal Osborn Loops*, J. Discrete Math. Sci. & Cryptography **14**(1) (2011), 33 – 50.

[12] **T.G. Jaiyéọlá** (2012), *Osborn loops and their universality*, Scientific Annals of "Al.I. Cuza" University of Iasi **58** (2012), 437 – 452.

[13] **T.G. Jaiyéọlá and J.O. Adéníran**, *Not every Osborn loop is universal*, Acta Math. Acad. Paedagogiace Nyíregyháziensis **25** (2009), 189 – 190.

[14] **T.G. Jaiyéọlá and J.O. Adéníran**, *New identities in universal Osborn loops*, Quasigroups and Related Systems **17** (2009), 55 – 76.

[15] **T.G. Jaiyéọlá and J.O. Adéníran**, *On another two cryptographic identities in universal Osborn loops*, Surveys in Math. Appl. **5** (2010), 17 – 34.

[16] **T.G. Jaiyéọlá, J.O. Adéníran and A. R. T. Sòlárìn**, *The universality of Osborn loops*, Acta Univ. Apulensis Math.-Inform. **26** (2011), 301 – 320.

[17] **M.K. Kinyon**, *A survey of Osborn loops*, Milehigh conference on loops, quasigroups and non-associative systems, University of Denver, Denver, Colorado, 2005.

[18] **M.K. Kinyon, K. Kunen, J.D. Phillips**, *Diassociativity in conjugacy closed loops*, Commun. Alg. **32** (2004), 767 – 786.

[19] **H.O. Pflugfelder**, *Quasigroups and loops: Introduction*, Sigma series in Pure Math. **7**, Heldermann Verlag, Berlin, 1990.

Received November 26, 2011

T.G.Jaiyéọlá
Department of Mathematics, Faculty of Science, Obafemi Awolowo University, Ilé Ifè 220005, Nigeria. E-mail: jaiyeolatemitope@yahoo.com, tjayeola@oauife.edu.ng
J.O.Adéníran
Department of Mathematics, College of Natural Sciences, Federal University of Agriculture, Abẹ́ókùta 110101, Nigeria. E-mail: ekenedilichineke@yahoo.com, adeniranoj@unaab.edu.ng

Quasigroups and Related Systems **20** (2012), 239 – 249

Left quasi-regular and intra-regular ordered semigroups using fuzzy ideals

Niovi Kehayopulu

Abstract. As a continuation of our paper in [6], we characterize here the ordered semigroups which are both intra-regular and left (right) quasi-regular also the ordered semigroups which are both regular and intra-regular in terms of fuzzy right, fuzzy left and fuzzy bi-ideals using first the first and then the second definitions of fuzzy ideals. As in [6], comparing the proofs of the results using the two definitions, we see that with the second definitions the proofs of the results are drastically simplified.

1. Introduction and prerequisites

In [6], we characterized the ordered semigroups in which $f \wedge h \wedge g \preceq g \circ h \circ f$, $f \wedge h \wedge g \preceq h \circ f \circ g$ and $f \wedge h \wedge g \preceq f \circ h \circ g$ as the ordered semigroups which are intra-regular, both regular and intra-regular, and regular, respectively. It would be interesting to characterize the rest, that is the ordered semigroups in which $f \wedge h \wedge g \preceq f \circ g \circ h$, $f \wedge h \wedge g \preceq h \circ g \circ f$ and $f \wedge h \wedge g \preceq g \circ f \circ h$. In this respect, we characterize the ordered semigroups which are both intra-regular and left (or right) quasi-regular, also the ordered semigroups which are both regular and intra-regular in terms of fuzzy left, fuzzy right and fuzzy bi-ideals. We prove that the property $f \wedge h \wedge g \preceq g \circ f \circ h$ characterizes the ordered semigroups which are both intra-regular and left quasi-regular, and the property $f \wedge h \wedge g \preceq h \circ g \circ f$ the ordered semigroups which are both intra-regular and right quasi-regular. We also prove that the property $f \wedge h \wedge g \preceq f \circ g \circ h$ characterizes the ordered semigroups which are both regular and intra-regular adding an additional characterization to the characterization of the same type of semigroups already considered in [6]. The left (resp. right) quasi-regular ordered semigroups are the ordered semigroups in which the left (resp. right) ideals are idempotent. According to the present paper, if an ordered semigroup $(S, ., \leqslant)$ is intra-regular and the left (resp. right) ideals of S are idempotent, then for every fuzzy right ideal f, every fuzzy left ideal g and every fuzzy subset h of $(S, \cdot)$ we have $f \wedge h \wedge g \preceq g \circ f \circ h$ (resp. $f \wedge h \wedge g \preceq h \circ g \circ f$) which shows that the corresponding results in [5] hold not

2010 Mathematics Subject Classification: 06F05 (08A72).
Keywords: Ordered semigroup, regular, intra-regular, left quasi-regular, left (right) ideal, bi-ideal, fuzzy left (right) ideal, fuzzy bi-ideal.

only for the fuzzy right, left, bi-ideals of $(S,\cdot,\leqslant)$ but for the fuzzy right, left, bi-ideals of $(S,\cdot)$, not only for the bi-ideals h but for any fuzzy subset h of S. Moreover, if an ordered semigroup $(S,\cdot,\leqslant)$ is both regular and intra-regular, then for every fuzzy right ideal f, every fuzzy subset g and every fuzzy bi-ideal h of $(S,\cdot)$ we have $f\wedge h\wedge g\preceq f\circ g\circ h$. We notice that investigations in the existing bibliography are based on the first definitions. Characterizations of semigroups (without order) which are intra-regular and left quasi-regular have been given by Kuroki in [7].

These are the first definitions:

Definition 1.1. Let $(S,\cdot,\leqslant)$ be an ordered groupoid. A fuzzy subset f of S is called a *fuzzy left* (resp. *right*) ideal of $(S,\cdot,\leqslant)$ if
(1) $f(xy)\geqslant f(y)$ (resp. $f(xy)\geqslant f(x)$) for all $x,y\in S$ and
(2) if $x\leqslant y$, then $f(x)\geqslant f(y)$.
In particular, if $(S,\cdot,\leqslant)$ is an ordered semigroup, then a fuzzy subset f of S is called a *fuzzy bi-ideal* of $(S,\cdot,\leqslant)$ if
(1) $f(xyz)\geqslant\min\{f(x),f(z)\}$ for all $x,y\in S$ and
(2) if $x\leqslant y$, then $f(x)\geqslant f(y)$.

These are the second definitions:

Definition 1.2. Let $(S,\cdot,\leqslant)$ be an ordered groupoid. A fuzzy subset f of S is called a *fuzzy left* (resp. *right*) ideal of $(S,\cdot,\leqslant)$ if
(1) $1\circ f\preceq f$ (resp. $f\circ 1\preceq f$) and
(2) if $x\leqslant y$, then $f(x)\geqslant f(y)$.
In particular, if $(S,\cdot,\leqslant)$ is an ordered semigroup, then a fuzzy subset f of S is called a *fuzzy bi-ideal* of $(S,\cdot,\leqslant)$ if
(1) $f\circ 1\circ f\preceq f$ and
(2) if $x\leqslant y$, then $f(x)\geqslant f(y)$.

A fuzzy subset f of $(S,\cdot,\leqslant)$ is said to be a fuzzy left (resp. right) ideal or fuzzy bi-ideal of $(S,\cdot)$ if the following assertions, respectively hold in $(S,\cdot,\leqslant)$: $f(xy)\geqslant f(y)$ (resp. $f(xy)\geqslant f(x)$), $f(xyz)\geqslant\min\{f(x),f(z)\}$ for all $x,y,z\in S$. The fuzzy set $1:S\to[0,1]\mid a\to 1$ is the greatest element in the set of fuzzy subsets of S. We have $1\circ 1\preceq 1$. In particular in intra-regular, also in regular ordered semigroups we have $1\circ 1=1$. If $(S,\cdot,\leqslant)$ is an ordered groupoid, f,g fuzzy subsets of $(S,\cdot)$ and $f\preceq g$ then, for any fuzzy subset h of $(S,\cdot)$, we have $f\circ h\preceq g\circ h$ and $h\circ f\preceq h\circ g$. If the multiplication on S is associative, then the multiplication " $\circ$ " on fuzzy subsets of S is also associative. An ordered semigroup $(S,\cdot,\leqslant)$ is called *regular* if for every $a\in S$ there exists $x\in S$ such that $a\leqslant axa$, equivalently if $A\subseteq(ASA]$ for every $A\subseteq S$. It is called *intra-regular* if for every $a\in S$ there exist $x,y\in S$ such that $a\leqslant xa^2y$, equivalently if $A\subseteq(SA^2S]$ for every $A\subseteq S$. An ordered semigroup $(S,\cdot,\leqslant)$ is regular if and only if for every fuzzy right ideal f and every fuzzy left ideal g of $(S,\cdot,\leqslant)$, we have $f\wedge g=f\circ g$ equivalently $f\wedge g\preceq f\circ g$. It is intra-regular if and only if for every fuzzy right ideal f and every fuzzy left ideal g of $(S,\cdot,\leqslant)$, we have $f\wedge g\preceq g\circ f$.

Moreover, an ordered semigroup S is regular if and only if for every fuzzy subset f of S, we have $f \preceq f \circ 1 \circ f$. It is intra-regular if and only if for every fuzzy subset f of S, we have $f \preceq 1 \circ f^2 \circ 1$. For further information we refer to [6]. The next two lemmas can be proved using only sets, which shows their pointless character.

Lemma 1.1. (cf. also [1]) *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. If S is intra-regular, then for every right ideal X and every left ideal Y of $(S, \cdot)$ we have $X \cap Y \subseteq (YX]$. "Conversely", if for every right ideal X and every left ideal Y of $(S, \cdot, \leqslant)$ we have $X \cap Y \subseteq (YX]$, then S is intra-regular.*

Proof. $\Longrightarrow$. Let X be a right ideal and Y a left ideal of $(S, \cdot)$. Since S is intra-regular, we have

$$X \cap Y \subseteq (S(X \cap Y)^2 S] = (S(X \cap Y)(X \cap Y)S] \subseteq ((SY)(XS)] \subseteq (YX].$$

$\Longleftarrow$. Let $A \subseteq S$. Since $R(A)$, $L(A)$ are right and left ideals of $(S, \cdot, \leqslant)$, respectively, by hypothesis, we have

$$\begin{aligned} A &\subseteq R(A) \cap L(A) \subseteq (L(A)R(A)] = ((A \cup SA](A \cup AS]] \\ &= ((A \cup SA)(A \cup AS)] = (A^2 \cup SA^2 \cup A^2S \cup SA^2S], \end{aligned}$$

$$\begin{aligned} A^2 &\subseteq (A^2 \cup SA^2 \cup A^2S \cup SA^2S](A] \\ &\subseteq (A^3 \cup SA^3 \cup A^2SA \cup SA^2SA] \\ &\subseteq (SA^2 \cup A^2S \cup SA^2S], \end{aligned}$$

$$\begin{aligned} A &\subseteq ((SA^2 \cup A^2S \cup SA^2S] \cup SA^2 \cup A^2S \cup SA^2S] \\ &= ((SA^2 \cup A^2S \cup SA^2S]] = (SA^2 \cup A^2S \cup SA^2S], \end{aligned}$$

$$A^2 \subseteq (SA^2 \cup A^2S \cup SA^2S](A] \subseteq (SA^3 \cup A^2SA \cup SA^2SA],$$
$$SA^2 \subseteq (S](SA^3 \cup A^2SA \cup SA^2SA] \subseteq (SA^3 \cup SA^2SA] \subseteq (SA^2S], ++$$
$$A \subseteq ((SA^2S] \cup A^2S \cup SA^2S] = (A^2S \cup (SA^2S]],$$
$$A^2 \subseteq (A](A^2S \cup (SA^2S]] \subseteq (A^3S \cup A(SA^2S]].$$

Since $A(SA^2S] \subseteq (A](SA^2S] \subseteq (ASA^2S] \subseteq (SA^2S]$, we have

$$A^2 \subseteq (A^3S \cup (SA^2S]] \subseteq (SA^2S \cup (SA^2S]] = ((SA^2S]] = (SA^2S].$$

Then we have $A^2S \subseteq (SA^2S](S] \subseteq (SA^2S]$, and $A \subseteq ((SA^2S]] = (SA^2S]$. □

In a similar way, the following lemma holds.

Lemma 1.2. (cf. also [2]) *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. If S is regular, then for every right ideal X and every left ideal Y of $(S, \cdot)$ we have $X \cap Y = (XY]$. "Conversely", if for every right ideal X and every left ideal Y of $(S, \cdot, \leqslant)$ we have $X \cap Y \subseteq (XY]$, then S is regular.*

2. Main results

The first theorem characterizes the ordered semigroups which are both intra-regular and left quasi-regular in terms of fuzzy ideals. These are the ordered semigroups for which $f \wedge h \wedge g \preceq g \circ f \circ h$. Let us prove this theorem using first the first and then the second definitions.

Definition 2.1. An ordered semigroup S is called *left quasi-regular* if for every $a \in S$ there exist $x, y \in S$ such that $a \leqslant xaya$.

Equivalent Definitions:
1) $a \in (SaSa]$ for every $a \in S$.
2) $A \subseteq (SASA]$ for every $A \subseteq S$.

Recall that this type of ordered semigroups are the ordered semigroups in which the left ideals are idempotent.

Theorem 2.1. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. If $(S, \cdot, \leqslant)$ is intra-regular and left quasi-regular, then for every fuzzy right ideal f, every fuzzy left ideal g and every fuzzy subset h of $(S, \cdot)$, we have*

$$f \wedge h \wedge g \preceq g \circ f \circ h.$$

"Conversely", if for every fuzzy right ideal f, every fuzzy left ideal g and every fuzzy bi-ideal h of $(S, \cdot, \leqslant)$ we have $f \wedge h \wedge g \preceq g \circ f \circ h$, then S is intra-regular and left quasi-regular.

Proof of Theorem 2.1 using the first definitions

We need the following lemmas.

Lemma 2.1. *Let $(S, \cdot, \leqslant)$ be an ordered groupoid. If A is a left (resp. right) ideal of $(S, \cdot, \leqslant)$, then the characteristic function f_A is a fuzzy left (resp. fuzzy right) ideal of $(S, \cdot, \leqslant)$. "Conversely", if A is a nonempty set and f_A a fuzzy left (resp. right) ideal of $(S, \cdot, \leqslant)$, then A is a left (resp. right) ideal of $(S, \cdot, \leqslant)$. In particular, let $(S, \cdot, \leqslant)$ be an ordered semigroup. Then, if B is a bi-ideal of $(S, \cdot, \leqslant)$, then the characteristic function f_B is a fuzzy bi-ideal of $(S, \cdot, \leqslant)$. "Conversely", if B is a nonempty set and f_B a fuzzy bi-ideal of $(S, \cdot, \leqslant)$, then B is a bi-ideal of $(S, \cdot, \leqslant)$.*

Lemma 2.2. *If S is an ordered groupoid (or groupoid) and $\{A_i \mid i \in I\}$ a family of subsets of S, then we have*

$$\bigwedge_{i \in I} f_{A_i} = f_{\bigcap\limits_{i \in I} A_i}.$$

Lemma 2.3. *Let S be an ordered semigroup, n a natural number, $n \geqslant 2$ and $\{A_1, A_2, \ldots\ldots, A_n\}$ a set of nonempty subsets of S. Then we have*

$$f_{A_1} \circ f_{A_2} \circ \ldots\ldots \circ f_{A_n} = f_{(A_1 A_2 \ldots\ldots A_n]}.$$

Lemma 2.4. *If S is an ordered groupoid (or groupoid) and A, B subsets of S, then we have*

$$A \subseteq B \Longleftrightarrow f_A \preceq f_B.$$

Lemma 2.5. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. If S is intra-regular and left quasi-regular, then for every right ideal X and every left ideal Y of $(S, \cdot)$, and every subset B of S we have*

$$X \cap B \cap Y \subseteq (YXB].$$

"Conversely", if for every right ideal X, every left ideal Y and every bi-ideal B of $(S, \cdot, \leqslant)$ we have $X \cap B \cap Y \subseteq (YXB]$, then S is intra-regular and left quasi-regular.

Proof. $\Longrightarrow$. Let X be a right ideal, Y a left ideal of $(S, \cdot)$ and B a subset of S. Then we have

$$\begin{aligned} X \cap B \cap Y &\subseteq (S(X \cap B \cap Y)S(X \cap B \cap Y)] \quad \text{(since } S \text{ is left quasi-regular)} \\ &\subseteq (S(S(X \cap B \cap Y)^2 S]S(X \cap B \cap Y)] \quad \text{(since } S \text{ is intra-regular)} \\ &= (S(S(X \cap B \cap Y)^2 S)S(X \cap B \cap Y)] \\ &\subseteq (S(X \cap B \cap Y)(X \cap B \cap Y)S(X \cap B \cap Y)] \\ &\subseteq ((SY)(XS)B] \subseteq (YXB]. \end{aligned}$$

$\Longleftarrow$. Let X be a right ideal and Y a left ideal of $(S, \cdot, \leqslant)$. Since S is a bi-ideal of $(S, \cdot, \leqslant)$, by hypothesis, we have $X \cap Y = X \cap S \cap Y \subseteq (YXS] \subseteq (YX]$. By Lemma 1.1, S is intra-regular. Let now A be a left ideal of $(S, \cdot, \leqslant)$. Since S is a right ideal, A a bi-ideal and A a left ideal of $(S, \cdot, \leqslant)$, by hypothesis, we have

$$A = S \cap A \cap A \subseteq (A(SA)] \subseteq (A^2] \subseteq (SA] \subseteq (A] = A.$$

Then $(A^2] = A$, so S is left quasi-regular. □

Lemma 2.6. [4; Prop. 5] *Let S be an ordered groupoid, f, g fuzzy subsets of S, and $a \in S$. The following are equivalent:*

(1) $(f \circ g)(a) \neq 0$.

(2) *There exists $(x, y) \in A_a$ such that $f(x) \neq 0$ and $g(y) \neq 0$.* □

Proof of Theorem 2.1

$\Longrightarrow$. Let f be a fuzzy right ideal, g a fuzzy left ideal, h a fuzzy subset of $(S, \cdot)$, and $a \in S$. Since $(S, \cdot, \leqslant)$ is intra-regular, there exist $x, y \in S$ such that $a \leqslant xa^2y$. Since S is left quasi-regular, there exist $s, t \in S$ such that $a \leqslant sata$. Then we have $a \leqslant sata \leqslant s(xa^2y)ta = sxa^2yta$. Since $(sxa^2yt, a) \in A_a$, we have $A_a \neq \emptyset$, and

$$((g \circ f) \circ h)(a) := \bigvee_{(u,v) \in A_a} \min\{(g \circ f)(u), h(v)\} \geqslant \min\{(g \circ f)(sxa^2yt), h(a)\}.$$

Since $(sxa, ayt) \in A_{sxa^2yt}$, we have $A_{sxa^2yt} \neq \emptyset$, and

$$(g \circ f)(sxa^2yt) := \bigvee_{(w,t) \in A_{sxa^2yt}} \min\{g(w), f(t)\} \geqslant \min\{g(sxa), f(ayt)\}.$$

Since g is a fuzzy left ideal of S, $g(sxa) \geqslant g(a)$. Since f is a fuzzy right ideal of S, $f(ayt) \geqslant f(a)$. Therefore we get

$$\begin{aligned}(g \circ f \circ h)(a) &= ((g \circ f) \circ h)(a) \geqslant \min\{\min\{g(sxa), f(ayt)\}, h(a)\}\\ &\geqslant \min\{\min\{g(a), f(a)\}, h(a)\} = \min\{g(a), f(a), h(a)\}\\ &= (f \wedge h \wedge g)(a).\end{aligned}$$

This holds for every $a \in S$, so $f \wedge h \wedge g \preceq g \circ f \circ h$.

For the converse statement we give three proofs. For the first one we use the Lemmas 2.1–2.5. For the second and third proof the Lemmas 2.1, 2.3 and 2.5 and Lemmas 2.1, 2.5 and 2.6, respectively, together with some basic properties of fuzzy sets.

First proof. Let X be a right ideal, Y a left ideal, B a bi-ideal of $(S, \cdot, \leqslant)$. By Lemma 2.1, f_X is a fuzzy right, f_Y a fuzzy left and f_B a fuzzy bi-ideal of $(S, \cdot, \leqslant)$. By hypothesis, we have $f_X \wedge f_B \wedge f_Y \preceq f_Y \circ f_X \circ f_B$. By Lemma 2.2, $f_X \wedge f_B \wedge f_Y = f_{X \cap B \cap Y}$. By Lemma 2.3, $f_Y \circ f_X \circ f_B = f_{(YXB]}$, then $f_{X \cap B \cap Y} \preceq f_{(YXB]}$. By Lemma 2.4, $X \cap B \cap Y \subseteq (YXB]$. By Lemma 2.5, $(S, \cdot, \leqslant)$ is intra-regular and left quasi-regular.

Second proof. Let X be a right ideal, Y a left ideal, B a bi-ideal of $(S, \cdot, \leqslant)$ and $a \in X \cap B \cap Y$. By Lemma 2.5, it is enough to prove that $a \in (YXB]$. As in the first proof, by Lemma 2.1 and hypothesis, we have $f_X \wedge f_B \wedge f_Y \preceq f_Y \circ f_X \circ f_B$. Then

$$(f_Y \circ f_X \circ f_B)(a) \geqslant (f_X \wedge f_B \wedge f_Y)(a) = \min\{f_X(a), f_B(a), f_Y(a)\}.$$

Since $a \in X$, we have $f_X(a) = 1$, since $a \in B$, $f_B(a) = 1$, since $a \in Y$, $f_Y(a) = 1$. Thus we have $(f_Y \circ f_X \circ f_B)(a) \geqslant 1$. Besides, since $f_Y \circ f_X \circ f_B$ is a fuzzy subset of S, we have $(f_Y \circ f_X \circ f_B)(a) \leqslant 1$, then $(f_Y \circ f_X \circ f_B)(a) = 1$. By Lemma 2.3, $f_Y \circ f_X \circ f_B = f_{(YXB]}$, then $f_{(YXB]}(a) = 1$, and $a \in (YXB]$.

Third proof. Let X be a right ideal, Y a left ideal, B a bi-ideal of $(S, \cdot, \leqslant)$ and $a \in X \cap B \cap Y$. As in the second proof, by Lemma 2.1, we have $(f_Y \circ (f_X \circ f_B))(a) = 1 \neq 0$. By Lemma 2.6, there exists $(b, c) \in A_a$ such that $f_Y(b) \neq 0$ and $(f_X \circ f_B)(c) \neq 0$. Since $(f_X \circ f_B)(c) \neq 0$, there exists $(d, e) \in A_c$ such that $f_X(d) \neq 0$ and $f_B(e) \neq 0$. Then $f_Y(b) = f_X(d) = f_B(e) = 1$, $b \in Y$, $d \in X$, $e \in B$, and $a \leqslant bc \leqslant bde \in YXB$, so $a \in (YXB]$. By Lemma 2.5, S is intra-regular and left quasi-regular. □

Proof of Theorem 2.1 using the second definitions

We need the following lemma

Lemma 2.7. [3] *An ordered semigroup $(S, \cdot, \leqslant)$ is left quasi-regular if and only if, for every fuzzy subset f of S, we have*

$$f \preceq 1 \circ f \circ 1 \circ f,$$

equivalently, if the fuzzy left ideals of $(S,\cdot,\leqslant)$ *are idempotent.*

Proof of the theorem.

$\Longrightarrow$. Let f be a fuzzy right, g a fuzzy left and h a fuzzy bi-ideal of $(S,\cdot)$. By Lemma 2.7, we have

$$\begin{aligned} f\wedge h\wedge g &\preceq 1\circ(f\wedge h\wedge g)\circ 1\circ(f\wedge h\wedge g)\ \ \text{(since } S \text{ is left quasi-regular)}\\ &\preceq 1\circ 1\circ(f\wedge h\wedge g)\circ(f\wedge h\wedge g)\circ 1\circ 1\circ(f\wedge h\wedge g)\\ &\qquad\qquad \text{(since } S \text{ is intra-regular)}\\ &\preceq (1\circ g)\circ(f\circ 1)\circ h\preceq g\circ f\circ h. \end{aligned}$$

$\Longleftarrow$. Let f be a fuzzy right ideal and g a fuzzy left ideal of $(S,\cdot,\leqslant)$. Since 1 is a fuzzy bi-ideal of S, by hypothesis, we have

$$f\wedge g=f\wedge 1\wedge g\preceq g\circ(f\circ 1)\preceq g\circ f,$$

so S is intra-regular. Let now g be a fuzzy left ideal of $(S,\cdot,\leqslant)$. Since 1 is a fuzzy right ideal and g at the same time a fuzzy bi-ideal of $(S,\cdot,\leqslant)$, by hypothesis, we have $g=1\wedge g\wedge g\preceq g\circ(1\circ g)\preceq g^2\preceq 1\circ g\preceq g$, so $g^2=g$. By Lemma 2.7, S is left quasi-regular. □

The next theorem characterizes the ordered semigroups which are both intra-regular and right quasi-regular in terms of fuzzy left, right and fuzzy bi-ideals. These are the ordered semigroups for which $f\wedge h\wedge g\preceq h\circ g\circ f$.

Definition 2.2. An ordered semigroup S is called *right quasi-regular* if for every $a\in S$ there exist $x,y\in S$ such that $a\leqslant axay$.

Equivalent Definitions:

1) $a\in(aSaS]$ for every $a\in S$.
2) $A\subseteq(ASAS]$ for every $A\subseteq S$.

Theorem 2.2. *Let* $(S,\cdot,\leqslant)$ *be an ordered semigroup. If* $(S,\cdot,\leqslant)$ *is intra-regular and right quasi-regular, then for every fuzzy right ideal f, every fuzzy left ideal g and every fuzzy subset h of* $(S,\cdot)$, *we have*

$$f\wedge h\wedge g\preceq h\circ g\circ f.$$

"Conversely", if for every fuzzy right ideal f, every fuzzy left ideal g and every fuzzy bi-ideal h of $(S,\cdot,\leqslant)$ *we have* $f\wedge h\wedge g\preceq h\circ g\circ f$, *then* $(S,\cdot,\leqslant)$ *is intra-regular and right quasi-regular.*

Proof of Theorem 2.2 using the first definitions

In addition to Lemmas 2.1–2.4 (or 2.1 and 2.3 or 2.1 and 2.6), we need the following lemma.

Lemma 2.8. *Let $(S,\cdot,\leqslant)$ be an ordered semigroup. If S is intra-regular and right quasi-regular, then for every right ideal X and every left ideal Y of $(S,\cdot)$, and every subset B of S we have*

$$X\cap B\cap Y\subseteq (BYX].$$

"Conversely", if for every right ideal X, every left ideal Y and every bi-ideal B of $(S,\cdot,\leqslant)$ we have $X\cap B\cap Y\subseteq (BYX]$, then S is intra-regular and right quasi-regular.

Proof of Theorem 2.2.

$\Longrightarrow$. Let f be a fuzzy right ideal, g a fuzzy left ideal, h a fuzzy subset of $(S,\cdot)$, and $a\in S$. Since $(S,\cdot,\leqslant)$ is intra-regular, there exist $x,y\in S$ such that $a\leqslant xa^2y$. Since S is right regular, there exist $s,t\in S$ such that $a\leqslant asat$. Then we have $a\leqslant asat\leqslant as(xa^2y)t=asxa^2yt$. Then $(asxa,ayt)\in A_a$, $A_a\neq\emptyset$, and

$$((h\circ g)\circ f)(a):=\bigvee_{(u,v)\in A_a}\min\{(h\circ g)(u),f(v)\}\geqslant\min\{(h\circ g)(asxa),f(ayt)\}.$$

Since $(a,sxa)\in A_{asxa}$, we have $A_{asxa}\neq\emptyset$ and

$$(h\circ g)(asxa):=\bigvee_{(w,t)\in A_{asxa}}\min\{(h(w),g(t)\}\geqslant\min\{h(a),g(sxa)\}.$$

Therefore we get

$$((h\circ g)\circ f)(a)\geqslant\min\{\min\{h(a),g(sxa)\},f(ayt)\}=\min\{h(a),g(sxa),f(ayt)\}.$$

Since g is a fuzzy left ideal of S, we have $g(sxa)\geqslant g(a)$. Since f is a fuzzy right ideal of S, we have $f(ayt)\geqslant f(a)$. Then we get

$$(h\circ g\circ f)(a)=((f\circ g)\circ f)(a)\geqslant\min\{h(a),g(a),f(a)\}=(f\wedge h\wedge g)(a).$$

Thus we obtain $f\wedge h\wedge g\preceq h\circ g\circ f$.

$\Longleftarrow$. Let X be a right ideal, Y a left ideal and B a bi-ideal of $(S,\cdot,\leqslant)$. Since f_X is a fuzzy right, f_Y a fuzzy left and f_B a fuzzy bi-ideal of $(S,\cdot,\leqslant)$, by hypothesis, we have $f_X\wedge f_B\wedge f_Y\preceq f_B\circ f_Y\circ f_X$. Since $f_X\wedge f_B\wedge f_Y=f_{X\cap B\cap Y}$ and $f_B\circ f_Y\circ f_X=f_{(BYX]}$, we have $f_{X\cap B\cap Y}\preceq f_{(BYX]}$. Then $X\cap B\cap Y\subseteq(BYX]$ and, by Lemma 2.8, S is intra-regular and right quasi-regular. □

Proof of Theorem 2.2 using the second definition.

We need the following lemma.

Lemma 2.9. [3] *An ordered semigroup $(S,\cdot,\leqslant)$ is right quasi-regular if and only if, for every fuzzy subset f of S, we have*

$$f\preceq f\circ 1\circ f\circ 1,$$

equivalently, if the fuzzy right ideals of $(S,\cdot,\leqslant)$ *are idempotent.*

Proof of the theorem.

$\Longrightarrow$. Let f be a fuzzy right ideal, g a fuzzy left ideal, h a fuzzy subset of $(S,\cdot)$. By Lemma 2.9, we have

$$\begin{aligned} f\wedge h\wedge g &\preceq (f\wedge h\wedge g)\circ 1\circ (f\wedge h\wedge g)\circ 1 \text{ (since } S \text{ is right quasi-regular)}\\ &\preceq (f\wedge h\wedge g)\circ 1\circ 1\circ (f\wedge h\wedge g)\circ (f\wedge h\wedge g)\circ 1\circ 1\\ &\qquad\qquad \text{(since } S \text{ is intra-regular)}\\ &= (f\wedge h\wedge g)\circ 1\circ (f\wedge h\wedge g)\circ (f\wedge h\wedge g)\circ 1\\ &\preceq h\circ (1\circ g)\circ (f\circ 1)\preceq h\circ g\circ f. \end{aligned}$$

$\Longleftarrow$. Let f be a fuzzy right ideal and g a fuzzy left ideal of $(S,\cdot,\leqslant)$. Since 1 is a fuzzy bi-ideal of $(S,\cdot,\leqslant)$, by hypothesis, we have $f\wedge g = f\wedge 1\wedge g \preceq (1\circ g)\circ f \preceq g\circ f$, so S is intra-regular. Let now f be a fuzzy right ideal of $(S,\cdot,\leqslant)$. Since f is at the same time a fuzzy bi-ideal and 1 a fuzzy left ideal of $(S,\cdot,\leqslant)$, by hypothesis, we have

$$f = f\wedge f\wedge 1 \preceq (f\circ 1)\circ f \preceq f\circ f \preceq f\circ 1 \preceq f,$$

so $f^2 = f$. By Lemma 2.9, S is right quasi-regular. □

The last theorem characterizes the ordered semigroups which are both regular and intra-regular in terms of fuzzy left, right and fuzzy bi-ideals. These are the ordered semigroups for which $f\wedge h\wedge g \preceq f\circ g\circ h$.

Theorem 2.3. *Let* $(S,\cdot,\leqslant)$ *be an ordered semigroup. If* S *is both regular and intra-regular, then for every fuzzy right ideal* f*, every fuzzy subset* g *and every fuzzy bi-ideal* h *of* $(S,\cdot)$ *we have*

$$f\wedge h\wedge g \preceq f\circ g\circ h.$$

"Conversely", if for every fuzzy right ideal f*, every fuzzy left ideal* g *and every fuzzy bi-ideal* h *of* $(S,\cdot,\leqslant)$ *we have* $f\wedge h\wedge g \preceq f\circ g\circ h$*, then* S *is both regular and intra-regular.*

Proof of Theorem 2.3 using the first definitions

In addition to Lemmas 2.1–2.4 (or 2.1 and 2.3 or 2.1 and 2.6), we need the following lemma.

Lemma 2.10. (cf. also [8]) *Let* $(S,\cdot,\leqslant)$ *be an ordered semigroup. If* $(S,\cdot,\leqslant)$ *is both regular and intra-regular, then for every right ideal* X*, every subset* Y *and every bi-ideal* B *of* $(S,\cdot)$*, we have*

$$X\cap B\cap Y \subseteq (XYB].$$

"Conversely", if for every right ideal X*, every left ideal* Y *and every bi-ideal* B *of* $(S,\cdot,\leqslant)$*, we have* $X\cap B\cap Y\subseteq (XYB]$*, then* S *is both regular and intra-regular.*

Proof. Condition "$A \subseteq (ASA^2SA]$ for all $A \subseteq S$" characterizes the ordered semigroups which are both regular and intra-regular. Let now X be a right ideal, Y a subset and B a bi-ideal of $(S,\cdot)$. Then we have

$$\begin{aligned} X\cap B\cap Y &\subseteq ((X\cap B\cap Y)S(X\cap B\cap Y)(X\cap B\cap Y)S(X\cap B\cap Y)] \\ &\subseteq ((XS)Y(BSB)] \subseteq (XYB]. \end{aligned}$$

For the converse statement, suppose X is a right ideal and Y a left ideal of $(S,\cdot,\leqslant)$. Since S is a left ideal and Y a bi-ideal of $(S,\cdot,\leqslant)$, by hypothesis, we have $X\cap Y = X\cap Y\cap S \subseteq (XSY] \subseteq (XY]$ then, by Lemma 1.2, S is regular. Since S is a right ideal and X a bi-ideal of $(S,\cdot,\leqslant)$, by hypothesis, we have $X\cap Y = S\cap X\cap Y \subseteq (SYX] \subseteq (YX]$ then, by Lemma 1.1, S is intra-regular.□

Proof of Theorem 2.3.

$\Longrightarrow$. Let f be a fuzzy right ideal of $(S,\cdot)$, g a fuzzy subset of S, h a fuzzy bi-ideal of $(S,\cdot)$, and $a\in S$. Since S is both regular and intra-regular, there exist $x,y,z\in S$ such that $a\leqslant axa$ and $a\leqslant za^2y$. Then we have $a\leqslant ax(axa)\leqslant ax(za^2y)xa$. As $(axza, ayxa)\in A_a$, we have $A_a\neq\emptyset$, and

$$((f\circ g)\circ h)(a) := \bigvee_{(u,v)\in A_a}\min\{(f\circ g)(u), h(v)\} \geqslant \min\{(f\circ g)(axza), h(ayxa)\}.$$

Since $(axz, a)\in A_{axza}$, we have $A_{axza}\neq\emptyset$, and

$$(f\circ g)(axza) := \bigvee_{(w,t)\in A_{axza}}\min\{f(w), f(t)\} \geqslant \min\{f(axz), g(a)\}.$$

Then we have

$$\begin{aligned} (f\circ g\circ h)(a) &\geqslant \min\{\min\{f(axz), g(a)\}, h(ayxa)\} \\ &= \min\{f(axz), g(a), h(ayxa)\} \\ &\geqslant \min\{f(a), g(a), h(a)\} \\ &= (f\wedge h\wedge g)(a). \end{aligned}$$

Thus we obtain $f\wedge h\wedge g \preceq f\circ g\circ h$.

$\Longleftarrow$. Let X be a right ideal, Y a left ideal and B a bi-ideal of $(S,\cdot,\leqslant)$. Since f_X is a fuzzy right ideal, f_Y a fuzzy left ideal and f_B a fuzzy bi-ideal of $(S,\cdot,\leqslant)$, by hypothesis, we have $f_X\wedge f_B\wedge f_Y \preceq f_X\circ f_Y\circ f_B$. Then $f_{X\cap B\cap Y}\preceq f_{(XYB]}$, and $X\cap B\cap Y\subseteq (XYB]$. By Lemma 2.10, S is both regular and intra-regular. □

Proof of Theorem 2.3 using the second definitions

$\Longrightarrow$. Since S is both regular and intra-regular, for every fuzzy subset f of S, we have $f\preceq f\circ 1\circ f^2\circ 1\circ f$. Indeed: Since S is regular, we have $f\preceq f\circ 1\circ f$ and, since S is intra-regular, $f\preceq 1\circ f^2\circ 1$. Then we have $f\preceq f\circ 1\circ (f\circ 1\circ f)\preceq$

$f \circ 1 \circ (1 \circ f^2 \circ 1) \circ 1 \circ f = f \circ 1 \circ f^2 \circ 1 \circ f$. Let now f be a fuzzy right ideal, g a fuzzy subset and h a fuzzy bi-ideal of $(S, \cdot)$. Then we have

$$\begin{aligned} f \wedge h \wedge g &\preceq (f \wedge h \wedge g) \circ 1 \circ (f \wedge h \wedge g) \circ (f \wedge h \wedge g) \circ 1 \circ (f \wedge h \wedge g) \\ &\preceq (f \circ 1) \circ g \circ (h \circ 1 \circ h) \\ &\preceq f \circ g \circ h. \end{aligned}$$

$\Longleftarrow$. Let f be a fuzzy right ideal and g a fuzzy left ideal of $(S, \cdot, \leqslant)$. Since g is a fuzzy bi-ideal and 1 a fuzzy left ideal of $(S, \cdot, \leqslant)$, by hypothesis, we have $f \wedge g = f \wedge g \wedge 1 \preceq (f \circ 1) \circ g \preceq f \circ g$, so S is regular. Since 1 is a fuzzy right ideal and f a fuzzy bi-ideal of $(S, \cdot, \leqslant)$, by hypothesis, we have $f \wedge g = 1 \wedge f \wedge g \preceq (1 \circ g) \circ f \preceq g \circ f$, and S is intra-regular. □

I would like to thank the managing editor of the journal Professor Wieslaw A. Dudek for editing and communicating the paper and the referee for his time to read the paper very carefully.

References

[1] **N. Kehayopulu**, *On regular, intra-regular ordered semigroups*, Pure Math. Appl. **4**, no. 4 (1993), 447–461.

[2] **N. Kehayopulu**, *On regular ordered semigroups*, Math. Japon. **47**, no. 3 (1997), 549–553.

[3] **N. Kehayopulu**, *Characterization of left quasi-regular and semisimple ordered semigroups in terms of fuzzy sets*, Int. J. Algebra, **6**, no. 15 (2012), 747–755.

[4] **N. Kehayopulu and M. Tsingelis**, *Characterization of some types of ordered semigroups in terms of fuzzy sets*, Lobachevskii J. Math. **29**, no. 1 (2008), 14–20.

[5] **N. Kehayopulu and M. Tsingelis**, *Intra-regular ordered semigroups in terms of fuzzy sets*, Lobachevskii J. Math. **30**, no. 1 (2009), 23–29.

[6] **N. Kehayopulu and M. Tsingelis**, *On fuzzy ordered semigroups*, Quasigroups Related Systems **20** (2012), 61 – 70.

[7] **N. Kuroki**, *Fuzzy generalized bi-ideals in semigroups*, Inform. Sci. **66** (1992), 235–243.

[8] **S. Lajos**, *Solution to a problem by Niovi Kehayopulu*, Pure Math. Appl. **4**, no. 3 (1993), 329–331.

Received March 21, 2012

University of Athens
Department of Mathematics
15784 Panepistimiopolis
Athens, Greece

E-mail: nkehayop@math.uoa.gr

Quasigroups and Related Systems **20** (2012), 251 – 256

On fuzzy ordered semigroups

Niovi Kehayopulu

Abstract. We characterize the ordered semigroups which are both regular and intra-regular, the completely regular, the quasi-semisimple, and the quasi left (right) regular ordered semigroups in terms of fuzzy sets.

1. For an ordered semigroup S and a subset A of S we denote by $(A]$ the subset of S defined by $(A] := \{t \in S \mid t \leqslant a$ for some $a \in A\}$. An ordered semigroup S is called *regular* if for any $a \in S$ there exists $x \in S$ such that $a \leqslant axa$. It is called *left* (resp. *right*) *regular* if for any $a \in S$ there exists $x \in S$ such that $a \leqslant xa^2$ (resp. $a \leqslant a^2x$). It is called *intra-regular* if for any $a \in S$ there exist $x, y \in S$ such that $a \leqslant xa^2y$. So, an ordered semigroup S is regular (left regular, right regular) if and only if $a \in (aSa]$ ($a \in (Sa^2]$, $a \in (a^2S]$) for all $a \in S$. It is intra-regular if and only if $a \in (Sa^2S]$ for all $a \in S$. Using fuzzy sets, we get the following: An ordered semigroup S is regular if and only if for every fuzzy subset f of S, we have $f \preceq f \circ 1 \circ f$. It is left (resp. right) regular if and only if for every fuzzy subset f of S, we have $f \preceq 1 \circ f^2$ (resp. $f \preceq f^2 \circ 1$). It is intra-regular if and only if for every fuzzy subset f of S, we have $f \preceq 1 \circ f^2 \circ 1$ [2]. An ordered semigroup S is called *completely regular* if at the same time is regular, left regular and right regular. As one can easily see, an ordered semigroup S is completely regular if and only if for every $a \in S$ there exists $x \in S$ such that $a \leq a^2xa^2$. That is, if $a \in (a^2Sa^2]$ for all $a \in S$. Our aim is to show that the definitions of regular, left (right) regular and intra-regular ordered semigroups using fuzzy sets play an essential role in studying the structure of ordered semigroups. In this respect, we prove that an ordered semigroup S is both regular and intra-regular if and only if for every fuzzy subset f of S, we have $f \preceq f \circ 1 \circ f^2 \circ 1 \circ f$. An ordered semigroup S is completely regular if and only if for every fuzzy subset f of S, we have $f \preceq f^2 \circ 1 \circ f^2$. We prove them first in the usual way, then using the equivalent definition of regular, left (right) regular and intra-regular ordered semigroups mentioned above. Comparing the two proofs we see that using the characterizations given in [2] the proofs of the results are drastically simplified.

On the other hand, we characterized in [1] the left (right) quasi-regular and the more general class of semisimple ordered semigroups using similar conditions. An ordered semigroup S is called *left* (resp. *right*) *quasi-regular* if for every $a \in S$ there

2010 Mathematics Subject Classification: 06F05 (08A72).

Keywords: Ordered semigroup, regular, intra-regular, completely regular, fuzzy subset, quasi left (right) regular, quasi-regular, quasi-semisimple.

exist $x, y \in S$ such that $a \leqslant axay$ (resp. $a \leqslant xaya$). Equivalently, if $a \in (aSaS]$ (resp. $a \in (SaSa]$) for all $a \in S$. It is called *semisimple* if for every $a \in S$ there exist $x, y, z \in S$ such that $a \leqslant xayaz$. That is, if $a \in (SaSaS]$ for all $a \in S$. We have already seen in [1] that an ordered semigroup S is left (resp. right) quasi-regular if and only if for every fuzzy subset f of S, we have $f \preceq 1 \circ f \circ 1 \circ f$ (resp. $f \preceq f \circ 1 \circ f \circ 1$); it is semisimple if and only if for every fuzzy subset f of S, we have $f \preceq 1 \circ f \circ 1 \circ f \circ 1$.

A semigroup S (without order) is called *quasi-semisimple* if $a \in SaS$ for every $a \in S$. A semigroup S is called *quasi left* (resp. *right*) *regular* if $a \in Sa$ (resp. $a \in aS$) for every $a \in S$. Keeping in mind the terminology of quasi-semisimple and quasi left (resp. right) regular semigroups given above, in the present paper we first introduce the concepts of quasi-semisimple and quasi left (right) regular ordered semigroups. Then, as a continuation of the paper in [1], we characterize the quasi-semisimple, the quasi left (right) regular and the quasi-regular ordered semigroups in terms of fuzzy sets. Each quasi-regular ordered semigroup is a quasi-semisimple ordered semigroup.

As always, denote by 1 the fuzzy subset on S defined by $1(x) = 1$ for every $x \in S$. Recall that if S is regular or intra-regular, then $1 \circ 1 = 1$. If f, g are fuzzy subsets of S such that $f \preceq g$, then for any fuzzy subset h of S we have $f \circ h \preceq g \circ h$ and $h \circ f \preceq h \circ g$. Denote $f^2 := f \circ f$, and by f_a the characteristic function on the set S defined by $f_a(x) = 1$ if $x = a$ and $f_a(x) = 0$ if $x \neq a$ $(a \in S)$. Denote by A_a the subset of $S \times S$ defined by $A_a := \{(x, y) \in S \times S \mid a \leqslant xy\}$.

2. In this section we characterize the ordered semigroups which are both regular and intra-regular and the completely regular ordered semigroups in terms of fuzzy sets. For the following three lemmas we refer to [2].

Lemma 1. *Let $(S, ., \leqslant)$ be an ordered groupoid, f,g fuzzy subsets of S and $a \in S$. The following are equivalent:*

(1) $(f \circ g)(a) \neq 0$.

(2) *There exists $(x, y) \in A_a$ such that $f(x) \neq 0$ and $g(y) \neq 0$.* □

Lemma 2. *Let $(S, ., \leqslant)$ be an ordered groupoid, f a fuzzy subset of S and $a \in S$. The following are equivalent:*

(1) $(f \circ 1)(a) \neq 0$.

(2) *There exists $(x, y) \in A_a$ such that $f(x) \neq 0$.* □

Lemma 3. *Let $(S, ., \leqslant)$ be an ordered groupoid, g a fuzzy subset of S and $a \in S$. The following are equivalent:*

(1) $(1 \circ g)(a) \neq 0$.

(2) *There exists $(x, y) \in A_a$ such that $g(y) \neq 0$.*

Theorem 4. *An ordered semigroup S is both regular and intra-regular if and only if for every fuzzy subset f of S, we have*

$$f \preceq f \circ 1 \circ f^2 \circ 1 \circ f.$$

Proof. $\Longrightarrow$. Let $a \in S$. Since S is regular and intra-regular, there exist $x, y, z \in S$ such that $a \leqslant axa$ and $a \leqslant ya^2z$. Then we have

$$a \leqslant ax(axa) \leqslant ax(ya^2z)xa = (axy)a^2zxa.$$

Since $(axy, a^2zxa) \in A_a$, we have $A_a \neq \emptyset$ and

$$\begin{aligned}(f \circ 1 \circ f^2 \circ 1 \circ f)(a) : &= \bigvee_{(u,v) \in A_a} \min\{(f \circ 1)(u), (f^2 \circ 1 \circ f)(v)\} \\ &\geqslant \min\{(f \circ 1)(axy), (f^2 \circ 1 \circ f)(a^2zxa)\}.\end{aligned}$$

Since $(a, xy) \in A_{axy}$, we have $A_{axy} \neq \emptyset$ and

$$(f \circ 1)(axy) := \bigvee_{(w,t) \in A_{axy}} \min\{f(w), 1(t)\} \geqslant \min\{f(a), 1(xy)\} = f(a).$$

Since $(a^2zx, a) \in A_{a^2zxa}$, we have $A_{a^2zxa} \neq \emptyset$ and

$$(f^2 \circ 1 \circ f)(a^2zxa) : = \bigvee_{(k,h) \in A_{a^2zxa}} \min\{(f^2 \circ 1)(k), f(h)\} \geqslant \min\{(f^2 \circ 1)(a^2zx), f(a)\}.$$

Since $(a^2, zx) \in A_{a^2zx}$, we have $A_{a^2zx} \neq \emptyset$ and

$$(f^2 \circ 1)(a^2zx) : = \bigvee_{(s,g) \in A_{a^2zx}} \min\{f^2(s), 1(g)\} \geqslant \min\{f^2(a^2), 1(zx)\} = f^2(a^2).$$

Since $(a, a) \in A_{a^2}$, we have $A_{a^2} \neq \emptyset$ and

$$(f \circ f)(a^2) : = \bigvee_{(s,g) \in A_{a^2}} \min\{f(s), f(g)\} \geqslant \min\{f(a), f(a)\} = f(a).$$

Thus

$$\begin{aligned}(f \circ 1 \circ f^2 \circ 1 \circ f)(a) &\geqslant \min\{(f \circ 1)(axy), (f^2 \circ 1 \circ f)(a^2zxa)\} \\ &\geqslant \min\{f(a), \min\{(f^2 \circ 1)(a^2zx)\}, f(a)\}\} \\ &\geqslant \min\{f(a), \min\{f^2(a^2), f(a)\}\} \\ &\geqslant \min\{f(a), \min\{f(a), f(a)\}\} \\ &= \min\{f(a), f(a)\} = f(a).\end{aligned}$$

$\Longleftarrow$. Let $a \in S$. Since f_a is a fuzzy set in S, by hypothesis, we have $1 = f_a(a) \leqslant (f_a \circ 1 \circ f_a^2 \circ 1 \circ f_a)(a)$. Since $f_a \circ 1 \circ f_a^2 \circ 1 \circ f_a$ is a fuzzy set in S, we have $(f_a \circ 1 \circ f_a^2 \circ 1 \circ f_a)(a) \leqslant 1$. Thus we have $(f_a \circ 1 \circ f_a^2 \circ 1 \circ f_a)(a) = 1$. By Lemma 1, there exists $(x, y) \in A_a$ such that $(f_a \circ 1)(x) \neq 0$ and $(f_a^2 \circ 1 \circ f_a)(y) \neq 0$. Since $(f_a \circ 1)(x) \neq 0$, by Lemma 2, there exists $(u, v) \in A_x$ such that $f_a(u) \neq 0$. Since $(f_a^2 \circ 1 \circ f_a)(y) \neq 0$, by Lemma 1, there exists $(w, t) \in A_y$ such that $(f_a^2 \circ 1)(w) \neq 0$ and $f_a(t) \neq 0$. Since $(f_a^2 \circ 1)(w) \neq 0$, by Lemma 2, there exists $(k, h) \in A_w$ such that $f_a^2(k) \neq 0$. Since $(f_a \circ f_a)(k) \neq 0$, by Lemma 1, there exists $(s,g) \in A_k$ such that $f_a(s) \neq 0$ and $f_a(g) \neq 0$. Since $f_a(u) \neq 0$, we have $f_a(u) = 1$, and $u = a$. Since $f_a(t) \neq 0$, $t = a$; since $f_a(s) \neq 0$, $s = a$; since $f_a(g) \neq 0$, $g = a$. Thus we have $a \leqslant xy \leqslant (uv)(wt) \leqslant uv(kh)t \leqslant uv(sg)ht = ava^2ha$, from which $a \leqslant a(va^2h)a$ and $a \leqslant (av)a^2(ha)$, where the elements va^2h and av, ha are in S. So S is regular and intra-regular. □

Second proof

$\Longrightarrow$. Let f be a fuzzy set on S. Since S is regular, we have $f \preceq f \circ 1 \circ f$; since S is intra-regular, $f \preceq 1 \circ f^2 \circ 1$. Thus we have

$$f \preceq f \circ 1 \circ (f \circ 1 \circ f) \preceq f \circ 1 \circ (1 \circ f^2 \circ 1) \circ 1 \circ f = f \circ 1 \circ f^2 \circ 1 \circ f.$$

$\Longleftarrow$. Let f be a fuzzy set on S. By hypothesis, we have

$$f \preceq f \circ 1 \circ f^2 \circ 1 \circ f \preceq f \circ 1 \circ f,\ 1 \circ f^2 \circ 1,$$

so S is both regular and intra-regular. □

Theorem 5. *An ordered semigroup S is completely regular if and only if for every fuzzy subset f of S we have*

$$f \preceq f^2 \circ 1 \circ f^2.$$

Proof. $\Longrightarrow$. Let $a \in S$. Since S is completely regular, there exists $x \in S$ such that $a \leqslant a^2xa^2$. Since $(a^2xa, a) \in A_a$, we have $A_a \neq \emptyset$, and

$$(f^2 \circ 1 \circ f^2)(a) := \bigvee_{(u,v) \in A_a} \min\{(f^2 \circ 1 \circ f)(u), f(v)\} \geqslant \min\{(f^2 \circ 1 \circ f)(a^2xa), f(a)\}.$$

Since $(a^2x, a) \in A_{a^2xa}$, we have $A_{a^2xa} \neq \emptyset$, and

$$(f^2 \circ 1 \circ f)(a^2xa) := \bigvee_{(w,t) \in A_{a^2xa}} \min\{(f^2 \circ 1)(w), f(t)\} \geqslant \min\{(f^2 \circ 1)(a^2x), f(a)\}.$$

Since $(a^2, x) \in A_{a^2x}$, we have $A_{a^2x} \neq \emptyset$, and

$$(f^2 \circ 1)(a^2x) := \bigvee_{(k,h) \in A_{a^2x}} \min\{f^2(k), 1(h)\} \geqslant \min\{f^2(a^2), 1(x)\} = f^2(a^2).$$

Since $(a, a) \in A_{a^2}$, we have $A_{a^2} \neq \emptyset$, and

$$(f \circ f)(a^2) := \bigvee_{(s,g) \in A_{a^2}} \min\{f(s), f(g)\} \geqslant \min\{f(a), f(a)\} = f(a).$$

Then

$$\begin{aligned}(f^2 \circ 1 \circ f^2)(a) &\geqslant \min\{(f^2 \circ 1 \circ f)(a^2xa), f(a)\}\\ &\geqslant \min\{\min\{(f^2 \circ 1)(a^2x), f(a)\}, f(a)\}\\ &\geqslant \min\{\min\{f^2(a^2), f(a)\}, f(a)\}\\ &\geqslant \min\{\min\{f(a), f(a)\}, f(a)\} = f(a).\end{aligned}$$

Thus $f \preceq f^2 \circ 1 \circ f^2$.

$\Longleftarrow$. Let $a \in S$. For the characteristic function f_a, by hypothesis, we have $1 = f_a(a) \leqslant (f_a^2 \circ 1 \circ f_a^2)(a)$. Since $f_a^2 \circ 1 \circ f_a^2$ is a fuzzy subset of S, we have $(f_a^2 \circ 1 \circ f_a^2)(a) \leqslant 1$. Thus we have $(f_a^2 \circ 1 \circ f_a^2)(a) = 1$. By Lemma 1, there exists $(x, y) \in A_a$ such that $(f_a^2 \circ 1)(x) \neq 0$ and $f_a^2(y) \neq 0$. Since $(f_a^2 \circ 1)(x) \neq 0$, by Lemma 2, there exists $(u, v) \in A_x$ such that $f_a^2(u) \neq 0$. Since $(f_a \circ f_a)(y) \neq 0$, by Lemma 1, there exists $(w, t) \in A_y$ such that $f_a(w) \neq 0$ and $f_a(t) \neq 0$. Since $(f_a \circ f_a)(u) \neq 0$, by Lemma 1, there exists $(k, h) \in A_u$ such that $f_a(k) \neq 0$ and $f_a(h) \neq 0$. Since $f_a(w) \neq 0$, we have $f_a(w) = 1$, and so $w = a$. Since $f_a(t) \neq 0$, $f_a(k) \neq 0$, $f_a(h) \neq 0$, we have $t = k = h = a$. Thus we have

$$a \leqslant xy \leqslant (uv)y \leqslant uv(wt) \leqslant (kh)vwt = a^2va^2,$$

where $v \in S$, so S is completely regular. □

Second proof

$\Longrightarrow$. Let f be a fuzzy set on S. Since S is completely regular, we have $f \preceq f \circ 1 \circ f$, $f \preceq f^2 \circ 1$ and $f \preceq 1 \circ f^2$. Then we have

$$f \preceq f \circ 1 \circ f \preceq (f^2 \circ 1) \circ 1 \circ (1 \circ f^2) = f^2 \circ 1 \circ f^2.$$

$\Longleftarrow$. Let f be a fuzzy set on S. By hypothesis, we have

$$f \preceq f \circ f \circ 1 \circ f \circ f \preceq f \circ 1 \circ f,\ f^2 \circ 1,\ 1 \circ f^2,$$

so S is regular, left regular and right regular. □

3. In this section, we characterize the quasi-semisimple, the quasi left (right) regular and the quasi-regular ordered semigroups using fuzzy sets.

Definition 6. An ordered semigroup $(S, ., \leqslant)$ is called *quasi-semisimple* if, for every $a \in S$ we have $a \in (SaS]$. That is, for every $a \in S$ there exist $x, y \in S$ such that $a \leqslant xay$.

Theorem 7. *An ordered semigroup $(S, ., \leqslant)$ is quasi-semisimple if and only if for every fuzzy subset f of S, we have $f \preceq 1 \circ f \circ 1$.*

Proof. $\Longrightarrow$. Let f be a fuzzy subset of S and $a \in S$. Since S is quasi-semisimple, there exist $x, y \in S$ such that $a \leqslant xay$. Then $(x, ay) \in A_a$, $A_a \neq \emptyset$ and

$$(1 \circ f \circ 1)(a) := \bigvee_{(u,v) \in A_a} \min\{1(u), (f \circ 1)(v)\} \geqslant \min\{1(x), (f \circ 1)(ay)\} = (f \circ 1)(ay).$$

Since $(a, y) \in A_{ay}$, we have $A_{ay} \neq \emptyset$ and

$$(f \circ 1)(ay) := \bigvee_{(w,t) \in A_{ay}} \min\{f(w), 1(t)\} \geqslant \min\{f(a), 1(y)\} = f(a).$$

Thus we have $(1 \circ f \circ 1)(a) \geqslant (f \circ 1)(ay) \geqslant f(a)$, and so $f \preceq 1 \circ f \circ 1$.

$\Longleftarrow$. Let $a \in S$. Since f_a is a fuzzy subset of S, by hypothesis, we have

$$1 = f_a(a) \leqslant (1 \circ f_a \circ 1)(a).$$

Since $1 \circ f_a \circ 1$ is a fuzzy subset of S, we have $(1 \circ f_a \circ 1)(a) \leqslant 1$. Then we have $(1 \circ f_a \circ 1)(a) = 1$. Since $(1 \circ (f_a \circ 1))(a) \neq 0$, by Lemma 3, there exists $(x, y) \in A_a$ such that $(f_a \circ 1)(y) \neq 0$. Then, by Lemma 2, there exists $(u, v) \in A_y$ such that $f_a(u) \neq 0$. Then $f_a(u) = 1$, and $u = a$. Finally, $a \leqslant xy \leqslant x(uv) = xav \in SaS$, so $a \in (SaS]$, and S is quasi-semisimple. □

Definition 8. An ordered semigroup $(S, ., \leqslant)$ is called *quasi left regular* if, for every $a \in S$ we have $a \in (Sa]$. That is, for every $a \in S$ there exists $x \in S$ such that $a \leqslant xa$. It is called *quasi right regular* if, for every $a \in S$ we have $a \in (aS]$, and *quasi-regular* if it is both left quasi regular and right quasi regular.

Theorem 9. *An ordered semigroup $(S, ., \leqslant)$ is quasi left regular if and only if for every fuzzy subset f of S, we have $f \preceq 1 \circ f$.*

Proof. $\Longrightarrow$. Let f be a fuzzy subset of S and $a \in S$. Since S is quasi left regular, there exists $x \in S$ such that $a \leqslant xa$. Then $(x, a) \in A_a$, $A_a \neq \emptyset$ and

$$(1 \circ f)(a) := \bigvee_{(u,v) \in A_a} \min\{1(u), f(v)\} \geqslant \min\{1(x), f(a)\} = f(a).$$

Thus we have $f \preceq 1 \circ f$.

$\Longleftarrow$. Let $a \in S$. Since f_a and $1 \circ f_a$ are fuzzy subsets of S, by hypothesis, we have $1 = f_a(a) \leqslant (1 \circ f_a)(a) \leqslant 1$, so $(1 \circ f_a)(a) = 1$. Since $(1 \circ f_a)(a) \neq 0$, by Lemma 3, there exists $(x, y) \in A_a$ such that $f_a(y) \neq 0$. Then $f_a(y) \neq 1$, and $y = a$. Thus we have $a \leqslant xy = xa \in Sa$, and $a \in (Sa]$. □

In a similar we prove the following:

Theorem 10. *An ordered semigroup $(S, ., \leqslant)$ is quasi right regular if and only if for every fuzzy subset f of S, we have $f \preceq f \circ 1$.* □

Corollary 11. *A quasi-regular ordered semigroup is quasi-semisimple.*

Proof. Let f be a fuzzy subset of S. Since S is quasi left regular, by Theorem 9, we have $f \preceq 1 \circ f$. Since S is quasi right regular, by Theorem 10, we have $f \preceq f \circ 1$. Then we have $f \preceq 1 \circ f \preceq 1 \circ (f \circ 1) = 1 \circ f \circ 1$. By Theorem 7, S is quasi-semisimple. □

References

[1] **N. Kehayopulu**, *Characterization of left quasi-regular and semisimple ordered semigroups in terms of fuzzy sets*, Int. J. Algebra **6** (2012), 747 – 755.

[2] **N. Kehayopulu and M. Tsingelis**, *Characterization of some types of ordered semigroups in terms of fuzzy sets*, Lobachevskii J. Math. **29** (2008), 14 – 20.

Received May 23, 2012

Quasigroups and Related Systems **20** (2011), 257 – 260

On finite loops whose inner mapping groups are direct products of dihedral groups and abelian groups

Emma Leppälä and Markku Niemenmaa

Abstract. We show that a finite loop, whose inner mapping group is a direct product of a dihedral group and an abelian group, is solvable provided that the components in the direct product have coprime orders.

1. Introduction

Let Q be a groupoid with a neutral element e. If each of the two equations $ax = b$ and $ya = b$ has a unique solution for any $a, b \in Q$, then we say that Q is a loop. The two mappings $L_a(x) = ax$ and $R_a(x) = xa$ are permutations on Q for every $a \in Q$. The permutation group $M(Q) = \langle L_a, R_a : a \in Q\rangle$ is called the *multiplication group of the loop* Q. Clearly, $M(Q)$ is transitive on Q. The stabilizer of the neutral element e is denoted by $I(Q)$ and is called the *inner mapping group* of Q.

A subloop H of Q is *normal* in Q if $x(yH) = (xy)H$, $(Hx)y = H(xy)$ and $xH = Hx$ for every $x, y \in Q$. A loop Q is *solvable* if it has a series $1 = Q_0 \subseteq \cdots \subseteq Q_n = Q$, where Q_{i-1} is a normal subloop of Q_i and Q_i/Q_{i-1} is an abelian group for each i. In 1996 Vesanen [8] managed to show that the solvability of $M(Q)$ (in the group theoretical sense) implies the solvability of Q (in the loop theoretical sense) if Q is a finite loop. After this we were naturally interested in those properties of $I(Q)$ which imply the solvability of $M(Q)$.

In 2000 Csörgő and Niemenmaa [1] considered the case where $I(Q)$ is a nonabelian group of order $2p$ (here p is an odd prime number) and they showed that $M(Q)$ is then a solvable group. In 2002, Drápal [2] investigated the case where $I(Q)$ is a nonabelian group of order pq (p and q are two different prime numbers) and again the solvability of $M(Q)$ followed. Finally, in 2004 Niemenmaa [5] showed that finite loops with dihedral inner mapping groups are solvable. Now we are able to prove the following: *If Q is a finite loop and $I(Q) = S \times L$, where S is dihedral, L is abelian and* $\gcd(|S|, |L|) = 1$, *then $M(Q)$ is solvable.* By the

2010 Mathematics Subject Classification: 20N05, 20D15
Keywords: loop, inner mapping group, solvable loop, solvable group.

result of Vesanen, Q is solvable, too. The result also holds in the case that S is a nonabelian group of order pq, where p and q are two different prime numbers.

Many properties of loops and their multiplication groups can be reduced to the properties of connected transversals in groups. Thus in section two we shall give the needed background material about connected transversals and their connections to loop theory. Section three contains our main results about the solvability of finite loops with given inner mapping groups.

2. Connected transversals

Let G be a group, $H \leq G$ and let A and B be two left transversals to H in G. We say that the two transversals A and B are *H-connected* if $a^{-1}b^{-1}ab \in H$ for every $a \in A$ and $b \in B$. We denote by H_G the core of H in G (the largest normal subgroup of G contained in H). If Q is a loop, then $A = \{L_a : a \in Q\}$ and $B = \{R_a : a \in Q\}$ are $I(Q)$-connected transversals in $M(Q)$ and the core of $I(Q)$ in $M(Q)$ is trivial. Niemenmaa and Kepka proved in 1990 the following [6, Theorem 4.1]

Theorem 2.1. *A group G is isomorphic to the multiplication group of a loop if and only if there exist a subgroup H and H-connected transversals A and B such that $H_G = 1$ and $G = \langle A, B\rangle$.* □

In the following results, which are needed later, we assume that A and B are H-connected transversals in G.

Lemma 2.2. *If $C \subseteq A \cup B$ and $K = \langle H, C\rangle$, then $C \subseteq K_G$.* □

Lemma 2.3. *If $G = \langle A, B\rangle$ and H is cyclic, then $G' \leq H$.* □

Theorem 2.4. *If G is finite and H is abelian or dihedral, then G is solvable.* □

For the proofs, see [6, Lemma 2.5 and Theorem 3.5], [7, Theorem 4.1] and [5, Theorem 3.1].

Next we wish to show that the solvability of G also follows in the case that H is a nonabelian subgroup of order pq (here $p \neq q$ are prime numbers). For the proof we need the following loop theoretical result by Drápal [2, Corollary 4.7].

Theorem 2.5. *If Q is a loop and $I(Q)$ is a nonabelian group of order pq, where $p \neq q$ are prime numbers, then $M(Q)$ is solvable.* □

We also need

Lemma 2.6. *Let $G = AH$ be a finite group, where A is an abelian subgroup, H is a subgroup of order pq and $p \neq q$ are prime numbers. Then G is solvable.* □

For the proof, see [4, Lemma 2.5].

Theorem 2.7. *Let G be a finite group, $H \leq G$ and $|H| = pq$, where $p \neq q$ are prime numbers. If there exist H-connected transversals A and B in G, then G is solvable.*

Proof. If $H_G > 1$, then we consider the group G/H_G and the subgroup H/H_G. Since H/H_G is cyclic, the claim follows from Theorem 2.4. Thus we may assume that $H_G = 1$.

If $G = \langle A, B\rangle$, then we apply Theorems 2.1 and 2.5, and the solvability of G follows. Thus we may assume that $E = \langle A, B\rangle < G$. If we write $K = E \cap H$, then $K < H$ and we have K-connected transversals A and B in E. Then $E' \leq K$ by Lemma 2.3 and K is normal in E. As $G = EH$, we may conclude that $K^G = \langle K^g : g \in G\rangle \leq H$. If $K \neq 1$, then we get a contradiction, as $H_G = 1$. Thus $K = 1$ and it follows that $E = A = B$ is an abelian group. Now $G = EH$ and we can apply Lemma 2.6. □

3. Main results

The following classical result of Wielandt is needed in the proof of our main theorem.

Theorem 3.1. *Let G be a finite group and let G contain a nilpotent Hall π-subgroup H. Then every π-subgroup of G is contained in a conjugate of H.* □

For the proof, see [3, Satz 5.8, p. 285].

Theorem 3.2. *Let G be a finite group and $H = S \times L \leq G$, where S is dihedral, L is abelian and* $\gcd(|S|, |L|) = 1$*. If there exist H-connected transversals A and B in G, then G is solvable.*

Proof. Let G be a minimal counterexample. If $H_G > 1$, then we consider G/H_G and its subgroup H/H_G and by using induction or Theorem 2.4, it follows that G/H_G is solvable, hence G is solvable.

Thus we may assume that $H_G = 1$. If H is not maximal in G, then there exists a subgroup T such that $H < T < G$. By Lemma 2.2, $T_G > 1$ and we may consider G/T_G and its subgroup $HT_G/T_G = T/T_G$. It follows that G/T_G is solvable. Since T is solvable by induction, we conclude that G is solvable.

We thus assume that H is a maximal subgroup of G. Let P be a Sylow p-subgroup of L. As $H_G = 1$, we conclude that P is a Sylow p-subgroup of G. From this it follows that L is a Hall subgroup of G. Clearly, $N_G(P) = H = C_G(P)$ and by using the Burnside normal complement theorem there exists a normal p-complement in G for each p that divides $|L|$. Clearly, this means that $G = KL$, where K is normal in G and $\gcd(|K|, |L|) = 1$.

If $1 \neq a \in A$, then $a = yx$, where $y \in L$ and $x \in K$. Then $aK = yK$ and $(aK)^d = K$, where d divides $|L|$. Thus $a^d \in K$, hence $(a^d)^t = 1$, where t divides $|K|$. It follows that $(a^t)^d = 1$, hence $|a^t|$ divides d. Since L is an abelian Hall subgroup of G, we may apply Theorem 3.1 and it follows that $a^t \in L^g$ for some $g \in G$. As L is abelian, $\langle a^t \rangle$ is normal in $\langle a, H^g \rangle = G$. As $H_G = 1$, we conclude that $a^t = 1$. Now there exist integers m and n such that $md + nt = 1$. Thus $a = a^{md+nt} = (a^d)^m (a^t)^n \in K$.

We may conclude that $A \cup B \subseteq K$. Clearly, $S \leq K$ and thus $K = AS = BS$. By Theorem 2.4, K is a solvable group. As $G = KL$, it follows that G is solvable, too. □

Theorem 3.3. *Let G be a finite group and $H = S \times L \leq G$, where S is a nonabelian group of order pq (here $p \neq q$ are prime numbers), L is abelian and* $\gcd(|S|, |L|) = 1$. *If there exist H-connected transversals A and B in G, then G is solvable.*

Proof. The proof is analogous to the proof of Theorem 3.2. We just have to replace Theorem 2.4 by Theorem 2.7 when needed. □

By combining Theorem 2.1 with Theorems 3.2 and 3.3, and by applying the theorem of Vesanen [8], we have the following

Corollary 3.4. *Let Q be a finite loop. If $I(Q) = S \times L$, where S is either dihedral or nonabelian of order pq, L is abelian and* $\gcd(|S|, |L|) = 1$, *then $M(Q)$ is a solvable group and Q is a solvable loop.* □

Remark 3.5. It would be interesting to know if the results of Theorems 3.2 and 3.3 and Corollary 3.4 also hold in the case that L is nilpotent.

References

[1] **P. Csörgő and M. Niemenmaa**, *Solvability conditions for loops and groups*, J. Algebra **232** (2000), 336 – 342.

[2] **A. Drápal**, *Orbits of inner mapping groups*, Monatsh. Math. **134** (2002), 191 – 206.

[3] **B. Huppert**, *Endliche Gruppen I*, Springer-Verlag, Berlin/Heidelberg, 1967.

[4] **M. Niemenmaa**, *On connected transversals to subgroups whose order is a product of two primes*, Europ. J. Combinatorics **18** (1997), 915 – 919.

[5] **M. Niemenmaa**, *Finite loops with dihedral inner mapping groups are solvable*, J. Algebra **273** (2004), 288 – 294.

[6] **M. Niemenmaa and T. Kepka**, *On multiplication groups of loops*, J. Algebra **135** (1990), 112 – 122.

[7] **M. Niemenmaa and T. Kepka**, *On connected transversals to abelian subgroups*, Bull. Austral. Math. Soc. **49** (1994), 121 – 128.

[8] **A. Vesanen**, *Solvable loops and groups*, J. Algebra **180** (1996), 862 – 876.

Received March 29, 2012

Department of Mathematical Sciences, University of Oulu, Pentti Kaiteran katu 1, PO Box 3000,
90014 University of Oulu, Finland
E-mails: emmalepp@paju.oulu.fi, markku.niemenmaa@oulu.fi

Quasigroups and Related Systems **20** (2012), 261 − 266

New signature scheme based on difficulty of finding roots

Nikolai A. Moldovyan and Victor A. Shcherbacov

Abstract. There are considered two digital signature schemes based on difficulty of finding the wth roots in the finite ground fields $GF(p)$. The first scheme uses the prime value $p = Nt_0t_1t_2+1$, where N is an even number; t_0, t_1, t_2 are prime numbers such that $|t_0| \approx |t_1| \approx |t_2| \approx 80$ bits. The public key is defined as follows $Y = K_1^{w_1}K_2^{w_2}$, where $w_1 = t_0t_1$ and $w_2 = t_0t_2$. The second scheme uses the value $p = Nt_1t_2 + 1$, and the public key composed of two values $Y_1 = K_1^{t_1}K_2^{t_2}$ mod p and $Y_2 = K_3^{t_1}K_4^{t_2}$ mod p, where four numbers K_1, K_2, K_3, and K_4 are the private key.

1. Introduction

There are well known signature schemes based on the difficulty of finding discrete logarithms [1] and factorization [3, 6] problems.

In paper [2] it has been proposed the signature scheme based on difficulty of finding the kth roots in the finite fields $GF(p)$ such that $p = Nk^2 + 1$, where k is sufficiently large prime having the size $| k | \geqslant 160$ bits and N is even number such that the size of p is $| p | \geqslant 1024$ bits.

To provide faster signature generation and verification procedures it is interesting to design signature schemes based on the last problem defined over the elliptic curves (ECs) [5] having the order divisible by the square of large prime k. However generating the EC with required order is an open problem. In the present paper there are considered other approaches to designing signature schemes based on difficulty of finding roots in the finite ground fields. The proposed approaches can be applied with using the ECs.

2. The first signature scheme

2.1. Algorithms for signature generation and verification

For the synthesis of the DS schemes it can be used complexity of finding the roots of large degree modulo prime p in the case of the modulus structure $p = Nt_0t_1t_2 + 1$,

2010 Mathematics Subject Classification: 11G20 11T71
Keywords: cryptography, public key, digital signature, difficult problem, computing roots

where N is even number; t_0, t_1, t_2 are prime numbers such that $|t_0| \approx |t_1| \approx |t_2| \approx$ 80 bits. In such signature schemes the difficulty of finding the wth roots is defined by difficulty of performing large number of checks that are required to find a value that can be represented as the wth power of some number.

It is supposed performing computations in the multiplicative group of the finite ring $(Z_p, +, \cdot)$. The security of the DS scheme using the prime modulus $p = Nt_0t_1t_2 + 1$ is defined by the fact that procedure of finding the qth roots, where q is a prime that divides the group order Ω, can be performed only for Ω/q different elements of the group. For sufficiently large value q probability that a random element a can be represented as x^q is negligible. Let us consider the construction of the DS scheme.

The public key Y is formed using two private keys $K_1 < p$ and $K_2 < p$ that are selected at random. The public key is calculated as follows $Y = K_1^{w_1} K_2^{w_2}$, where $w_1 = t_0t_1$ and $w_2 = t_0t_2$. This is a characteristic feature of the considered signature scheme. The digital signature is a triple e, S_1 and S_2. Suppose a message M is given. The signature generation procedure is performed as follows:

1. Select at random two numbers T_1 and T_2.
2. Calculate the value $R = T_1^{w_1} T_2^{w_2} \pmod p$.
3. Calculate the first signature element e: $e = F(R, M) = RH \pmod{w_1}$, where H is the hash value computed from the message: $H = F_H(M)$.
4. Calculate the second signature element S_1 using the formula $S_1 = T_1 K_1^{-e} \pmod p$.
5. Calculate the third signature element S_2 using the formula $S_2 = T_2 K_2^{-e} \pmod p$.

2.2. The signature verification algorithm

The signature verification algorithm is as follows.

1. Using the given signature (e, S_1, S_2) calculate the value $R' = Y^e S_1^{w_1} S_2^{w_2} \pmod p$.
2. Calculate the value $e' = F(R', M) = R'H \pmod{w_1}$.
3. Compare e' with e. If $e' = e$, then the signature is valid.

Proof that signature verification works. If the digital signature has been formed correctly, i.e., using the true private key in accordance with the specified procedure for the signature generation, then in step 3 of the signature verification procedure it is obtained the equality of the values e and e'. On the basis of the equality $e = e'$ it is concluded that the signature is valid. Correctness of the signature scheme can be shown as follows. Substituting into the formula $R' = Y^e S_1^{w_1} S_2^{w_2} \pmod p$ the values $Y = K_1^{w_1} K_2^{w_2} \pmod p$, $S_1 = T_1 K_1^{-e} \pmod p$, and $S_2 = T_2 K_2^{-e} \pmod p$ we obtain:

$$R' = (K_1^{w_1} K_2^{w_2})^e \, (T_1 K_1^{-e})^{w_1} \, (T_2 K_2^{-e})^{w_2} \pmod p = T_1^{w_1} T_2^{w_2} \pmod p = R,$$

i.e., the value R' obtained at the first step of the signature verification procedure is equal to R, therefore $e' = R'H \pmod{w_1} = RH \pmod{w_1} = e$.

2.3. Possible attacks

Let us consider some attacks on the constructed signature algorithm.

The first type attack. In the first attack it is supposed that a potential attacker can do the following attack, including the generation of random values T_1 and T_2, then calculate value $R = T_1^{w_1} T_2^{w_2} \pmod p$, $e = F(R, M)$ and try to find a pair numbers S_1 and S_1 such that the following equation $S_1^{w_1} S_2^{w_2} = RY^{-e} \pmod p$ holds, where S_1 and S_2 are the unknowns.

In this case the right side of the equation has a random value because a function $F(R, M)$ is a confusion function, for example, a hash function, or function of the form $e = RH \pmod{w_1}$.

If you set one of the unknowns, for example S_2, the equation is transformed into an equation with unknown S_1. In the last equation the right side with negligibly small probability will have a value, at which the last equation is solvable. An exponentiation operation modulo p is performed to verify condition of the solvability. To obtain the case when the solvability condition is satisfied, it is required to perform the described attempt on the average t_1 time. When the length of t_1 equal to 80 bits or more, the computational complexity of forging the signature is so high that it is practically infeasible. Similarly, the signature forgery can be performed with solving some equation relatively unknown S_2, when it is required do t_2 described attempts. If the length of the value t_2 is equal to 80 bits or more, then the computational difficulty of such attempt is sufficiently high and the attack is infeasible.

The second type attack. The second attack model is more sophisticated. In the second variant it is considered the case in which the attacker generates the value $R = Y^u \pmod p$, calculates $e = F(R, M)$, and tries to find a pair of the numbers S_1 and S_2 using the formulas $S_1 = Y^{s_1 w_1} \pmod p$ and $S_2 = Y^{s_2 w_2} \pmod p$.

For this representation of the desired values S_1 and S_2 the expression $Y^u = Y^e Y^{s_1 w_1} Y^{s_2 w_2} \pmod p$ holds, if the following relation holds $u - e = s_1 w_1 + s_2 w_2 \pmod{(p-1)}$, which is a Diophantine equation for the unknown s_1 and s_2.

Because $w_1 = t_0 t_1$ and $w_2 = t_0 t_2$, where t_0, t_1, and t_2 are prime numbers, then this Diophantine equation has a solution in integers only in the case when the right side of the equation is divisible by the number t_0, which is equal to the greatest common divisor of the coefficients for the unknowns s_1 and s_2. The value e is determined by the formula $e = F(R, M)$ and has a random value. The probability that a number t_0 will divide the number $u - e$ (i.e., the probability that a Diophantine equation has solutions) is $1/t_0$.

When the size t_0 is equal to 80 bits, for one case the solvability of the Diophantine equation requires on the average to perform 2^{80} attempts to forge the signature. The difficulty of the last process exceeds 2^{80} exponentiations modulo p.

The third type attack. The most effective method for attacking the signature scheme is based on solving the discrete logarithm problem in the finite field $GF(p)$.

The method is described as follows. It is easy to find a primitive element G, the degree of which run through all nonzero elements of the field $GF(p)$. Then the public key can be represented as:

$$Y = G^z = X_1^{w_1} X_2^{w_2} = G^{x_1 w_1} G^{x_2 w_2} = G^{x_1 w_1 + x_2 w_2} \pmod p,$$

where x_1 and x_2 are the values of the discrete logarithms of the secret key elements X_1 and X_2, respectively. The last relation shows that finding the discrete logarithm z from the public key to the base G allows one to obtain the equation $z = x_1 w_1 + x_2 w_2 = x_1 t_0 t_1 + x_2 t_0 t_2 \pmod{(p-1)}$.

The last equation can be easily solved relatively the unknowns x_1 and x_2. Its solvability follows from the fact of the divisibility of numbers z by t_0. Let $z = z' t_0$. Then we have $z' = x_1 t_1 + x_2 t_2 \pmod{(p-1)/t_0}$

From the last relation, for some integer N we obtain the following equation with two unknowns x_1 and x_2: $z' + N\frac{p-1}{t_0} = x_1 t_1 + x_2 t_2$, from which it follows

$$z' = x_1 t_1 \pmod{t_2} \Rightarrow x_1 = \frac{z'}{t_1} \pmod{t_2}$$

Similarly, one can obtain a formula for calculating the second unknown x_2: $x_2 = \frac{z'}{t_2} \pmod{t_1}$. Thus, the DS scheme proposed in this section requires to use a prime p, whose size is not less than 1024 bits. In the last case the discrete logarithm problem can be considered as practically infeasible one, since its difficulty estimation is 2^{80} multiplications $\mod p$ [4]. Thus, the proposed signature scheme provides security $\geqslant 2^{80}$ for values p having size $\geqslant$ 1024 bits.

3. The second signature scheme

3.1. Algorithms for generation and verification signatures

Let us consider another variant of the construction of the DS scheme based on difficulty of finding the roots of large degree, which is characterized in using the two-element public-key. In the construction it is used a prime modulus p having the following structure $p = Nt_1t_2 + 1$, where N is an even number; t_1 and t_2 are prime numbers such that $|t1| \approx |t_2| \geqslant 80$ bits. In contrast to the DS scheme described previously, the public key Y is formed in the form of two numbers, which are calculated using the formulas $Y_1 = K_1^{t_1} K_2^{t_2} \mod p$ and $Y_2 = K_3^{t_1} K_4^{t_2} \mod p$, where four numbers $K_1 < p$, $K_2 < p$, $K_3 < p$, and $K_4 < p$ are the private key. The digital signature is a triple e, S_1, and S_2.

Suppose a message M is given. The signature generation procedure is performed as follows:

1. Select at random two numbers T_1 and T_2.
2. Calculate the value $R = T_1^{t_1} T_2^{t_2} \pmod p$.
3. Calculate the first signature element e: $e = F(R, M) = RH \pmod{w_1}$,

where H is the hash value computed from the message: $H = F_H(M)$. The value e is represented as the concatenation of two values e_1 and e_2: $e = e_1||e_2$.

4. Calculate second signature element S_1 using the following formula $S_1 = T_1 K_1^{-e_1} K_3^{-e_2} \pmod p$.
5. Calculate the third signature element S_2 using the following formula $S_2 = T_2 K_2^{-e_1} K_4^{-e_2} \pmod p$.

The signature verification algorithm is as follows.

1. Using the signature (e, S_1, S_2) calculate the value $R' = Y_1^{e_1} Y_2^{e_2} S_1^{t_1} S_2^{t_2} \pmod p$.
2. Calculate the value $e' = F(R', M) = R'H \pmod{t_1}$.
3. Compare e' with e. If $e' = e$, then the signature is valid.

3.2. Proof that signature verification works

If the digital signature has been formed correctly, i.e., using the true private key in accordance with the specified procedure of the signature generation, then in step 3 of the signature verification procedure it is obtained the value e' equal to e. On the basis of the equality $e' = e$ it is concluded about validity of the digital signature. Correctness of the signature scheme can be proved as follows. Substituting into the formula $R' = Y_1^{e_1} Y_2^{e_2} S_1^{t_1} S_2^{t_2} \pmod p$ the values $Y_1 = K_1^{t_1} K_2^{t_2} \pmod p$, $Y_2 = K_3^{t_1} K_4^{t_2} \pmod p$, $S_1 = T_1 K_1^{-e_1} K_3^{-e_2} \pmod p$, and $S_2 = T_2 K_2^{-e_1} K_4^{-e_2} \pmod p$, we obtain:

$$
\begin{aligned}
&R' = Y_1^{e_1} Y_2^{e_2} S_1^{t_1} S_2^{t_2} \pmod p = \\
&(K_1^{t_1} K_2^{t_2})^{e_1} (K_3^{t_1} K_3^{t_2})^{e_2} (T_1 K_1^{-e_1} K_3^{-e_2})^{t_1} (T_2 K_2^{-e_1} K_4^{-e_2})^{t_2} \pmod p = \\
&T_1^{t_1} T_2^{t_2} \pmod p = R
\end{aligned}
$$

i.e., the value R' obtained at the first step of the signature verification algorithm is equal to R, so $e' = R'H \mod t_1 = RH \mod t_1 = e$.

3.3. Security discussion

The variants of the attack presented in Section 2.3 can be also applied against the second DS scheme. Details of the algorithms for forging the signature are different, but the used ideas and approaches are similar to the case of attacking the first signature scheme. The first two variants of the attack dictate the need of the choice of the size of prime powers t_1 and t_2 equal to $|t_1| = |t_2| \geqslant 80$ bits. The third type attack, based on solving the discrete logarithm problem, determine the size of the prime modulus $|p| = 1024$ bits, which provides 80-bit security of the considered signature scheme.

4. Conclusion

The proposed two constructions of the signature algorithms illustrates two new approaches to design of the digital signature schemes based on the difficulty of finding large prime roots in the ground finite fields. The cryptosystems can be broken with solving the discrete logarithm problem in the finite ground field like in the case of the cryptosystem described in [2]. To obtain the 80-bit security of the cryptosystems based on difficulty of finding roots in the finite field GF(p) one should use the 1024-bit value p. The advantage of the proposed approaches against the construction introduced in [4] consists in possibility to construct fast signature schemes based on difficulty of finding roots in the finite groups of the EC points.

Acknowledgement. The first author was supported by Russian Foundation for Basic Research grant # 11-07-00004-a.

References

[1] **N. Koblitz and A.J. Menezes**, *Another look at "Provable Security"*, J. Cryptology **20** (2007), 3 – 38.

[2] **N.A. Moldovyan**, *Digital signature scheme based on a new hard problem*, Computer Sci. J. Moldova **16** (2008), 163 – 182.

[3] **A.A. Moldovyan, D.N. Moldovyan and L.V. Gortinskaya**, *Cryptoschemes based on new signature formation mechanism*, Computer Sci. J. Moldova **14** (2006), 397 – 411.

[4] **A.J. Menezes and P.C. Van Oorschot**, *Handbook of applied cryptography*, CRC Press, Boca Raton, 1997.

[5] **A.J. Menezes and S.A. Vanstone**, *Elliptic curve cryptosystems and their implementation*, J. Cryptology **6** (1993), 209 – 224.

[6] **R.L. Rivest, A. Shamir and L.M. Adleman**, *A method for obtaining digital signatures and public key cryptosystems*, Commun. ACM **21**, (1978), 120 – 126.

Received April 05, 2012

N.A. Moldovyan
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences,
14 Liniya, 39, 199178, St. Petersburg, Russia
E-mail: nmold@mail.ru

V.A. Shcherbacov
Institute of Mathematics and Computer Science of the Academy of Sciences, Academiei 5,
MD-2028, Chisinau, Moldova
E-mail: scerb@math.md

Quasigroups and Related Systems **20** (2012), 267 − 274

Some remarks on Abel-Grassmann's groups

Petar V. Protić

Abstract. Abel-Grassmann's groupoids or shortly AG-groupoids have been considered in quite a number of papers, although under the different names (left-almost semigroups, left invertive groupoids). Abel-Grassmann's groups (AG-groups) is an Abel-Grassmann's groupoid with left identity in which every element has inverse. In this paper we describe AG-groups by equations. Also, we describe congruences on AG-groups.

1. Introduction

Abel-Grassmann's groupoids, abbreviated as AG-groupoids, are also called left almost semigroups (LA-semigroups in short). They are closely related with commutative semigroup because if an AG-groupoid contains right identity then it becomes a commutative monoid. Although the structure is non-associative and non-commutative, nevertheless, it posses many interesting properties which we usually found in associative and commutative algebraic structures. For instance $a^2b^2 = b^2a^2$, for all a, b holds in a commutative semigroup, while this equation also holds for an AG-groupoid with left identity e, moreover $ab = (ba)e$ for any subset $\{a, b\}$ of an AG-groupoid. An idempotent AG-groupoid with left identity is a semilattice [6].

A groupoid $(S, \cdot)$ is called *AG-groupoid*, if it satisfies the *left invertive law*:

$$ab \cdot c = cb \cdot a. \tag{1}$$

Any AG-groupoid satisfies the *medial law*:

$$ab \cdot cd = ac \cdot bd. \tag{2}$$

An AG-groupoid satisfying the identity

$$a \cdot bc = b \cdot ac \tag{3}$$

is called an *AG^{**}-groupoid*. Notice that each AG-groupoid with left identity is an AG^{**}-groupoid [7]. In any AG^{**}-groupoid G holds the *paramedial law*:

$$ab \cdot cd = db \cdot ca. \tag{4}$$

In this paper by G^e we denote the AG-groupoid G with a left identity e.

2010 Mathematics Subject Classification: 20N02
Keywords: Abel-Grassmann's groupoid, AG-groupoid, AG-group, congruence.
Supported by Grant ON 174026 of Ministry of Science through Math. Inst. SANU

2. AG-groups

The element $x \in G^e$ ($y \in G^e$) is a *left* (resp. *right*) *inverse* for $a \in G^e$ if $xa = e$ (resp. $ay = e$), and an element which is both a left and a right inverse is called an *inverse element*. In [5] it has been proved that in G^e left identity and left inverse are uniquely determined and that any left inverse is a right inverse and conversely. Hence, left and right inverses is an inverse and it is unique. An inverse of $a \in G^e$ is denoted by a'. Clearly, for any $a, b \in G^e$, $(a')' = a$, $(ab)' = a'b'$.

Definition 2.1. [5] An AG-groupoid G^e is called an *AG-group* if every $a \in G^e$ has an inverse element a'.

Obviously, any AG-group is an AG^{**}-groupoid. Hence any AG^{**}-group satisfies (1), (2), (3) and (4).

A simple example of an AG-group is an AG-groupoid $der(G, *)$ *derived* from an Abelian group $(G, *)$ i.e., an AG-groupoid with the operation $xy = x^{-1} * y$. In this AG-group we have $x' = x$ for all $x \in G$. But there are AG-groups which are not of this form.

Example 2.2. It is not difficult to see that the groupoid $(G, \cdot)$ defined by the following table

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	c	b	a	e
c	b	c	e	a

is an AG-groupoid. It is not a semigroup since, for example, $ba \cdot a \neq b \cdot aa$. The element e is its left identity, $a = a'$, $b' = c$ and $c' = b$. Hence, $(G, \cdot)$ is an AG-group. Obviously this AG-group is not derived from a group. □

Lemma 2.3. *In an AG-group G^e the equation $xa = b$ has an unique solution for every $a, b \in G^e$.*

Proof. Indeed, since for all $a, b \in G^e$ we have

$$b = eb = aa' \cdot b = ba' \cdot a,$$

the element $x = ba' \in G^e$ is a solution of the equation $xa = b$.

Let x_1 and x_2 be solutions of the equation $xa = b$, then

$$\begin{aligned} x_1 &= ex_1 = a'a \cdot x_1 = x_1a \cdot a' = ba' \\ &= x_2a \cdot a' = a'a \cdot x_2 = ex_2 = x_2. \end{aligned}$$

Hence, the equation $xa = b$ has an unique solution. □

Theorem 2.4. *On any AG-group G^e we can define an Abelian group $ret(G^e)$ by putting $x \circ y = xe \cdot y$.*

Proof. If G^e is an AG-group, then by (1) the operation $x \circ y = xe \cdot y$ is commutative and e is its neutral element. Moreover, for all $x, y, z \in G^e$ we have

$$(x \circ y) \circ z = (xe \cdot y)e \cdot z \overset{(1)}{=} ze \cdot (xe \cdot y) \overset{(1)}{=} ze \cdot (ye \cdot x) \overset{(4)}{=} xe \cdot (ye \cdot z) = x \circ (y \circ z).$$

So, $(G^e, \circ)$ is a commutative monoid.

Consider the equation $b = x \circ a = xe \cdot a$. By Lemma 2.3 the equation $za = b$ has a unique solution $z_0 \in G^e$. The equation $xe = z_0$ also has a unique solution. Thus for every $a, b \in G^e$ there exists x such that $x \circ a = b$. Hence $ret(G^e) = (G^e, \circ)$ is an Abelian group. In this group $a^{-1} = a'e$, where a' is an inverse element in an AG-group G^e. □

Remark 2.5. For an AG-groupoid G^e derived from an Abelian group $(G, *)$ we have $ret(G^e) = der(G, *)$. So, $ret(der(G, *)) = (G, *)$ and $der(ret(G^e)) = G^e$. Example 2.2 show that the last equality is not true for AG-groups which are not derived from an Abelian group.

From results obtained in [6] it follows that $der(ret(G^e)) = G^e$ holds only for AG-groups satisfying the identity $x^2 = e$.

Theorem 2.6. *Let H, K be two AG-subgroups of an AG-groupoid G. If e_H, e_K are left identities of H and K respectively, then*

$$H \cap K \neq \emptyset \iff e_H = e_K.$$

Proof. Let $H \cap K \neq \emptyset$ and let $a \in H \cap K$, then $aa'_H = a'_H a = e_H$, $aa'_K = a'_K a = e_K$ for some $a'_H \in H$, $a'_K \in K$. Thus

$$e_H e_K = a'_H a \cdot e_K = e_K a \cdot a'_H = aa'_H = e_H.$$

By symmetry, $e_K e_H = e_K$. Now, by (1) and (2), we obtain

$$e_H e_K = aa'_H \cdot e_K = e_K a'_H \cdot a = e_K a'_H \cdot e_K a = e_K e_H \cdot a'_H a = e_K e_H,$$

and so $e_H = e_K$.

The converse statement is trivial. □

3. Congruences on AG-groups

In this section we shall characterize all congruences on an arbitrary AG-group by its normal AG-subgroups.

Lemma 3.1. *If ρ is a congruence on an AG-group G^e, then for all $a, b \in G^e$ we have*

$$a \rho b \iff a' \rho b'.$$

Proof. Indeed, if $a\rho\, b$, then $(b'a)\rho\,(b'b)$, and so $(b'a)\rho\, e$. Therefore, $(b'a\cdot a')\rho\,(ea')$. On the other hand, $b'a\cdot a' = a'a\cdot b' = eb' = b'$. Hence, $b'\rho\, a'$.

The converse implication is obvious, since $(a')' = a$ for every $a \in G^e$. □

Definition 3.2. A nonempty subset K of an AG-group G^e is called

- *self conjugate* if $x\cdot Kx' \subseteq K$ for all $x \in G^e$,
- *inverse closed* if $x' \in K$ for all $x \in K$,
- an *AG-subgroup* if it is an inverse closed subgroupoid of G^e,
- a *normal AG-subgroup* if it is a self conjugate AG-subgroup of G^e.

Obviously, any AG-subgroup of G^e is a subgroup of the group $ret(G^e)$. The converse is not true in general. For example, it is not difficult to see that for an AG-group G^e defined in Example 2.2, $H = \{e, b\}$ is a subgroup of $ret(G^e)$, but it is not an AG-subgroup of G^e.

Lemma 3.3. *Let ρ be a congruence relation defined on an AG-group G^e. Then*

$$\ker\rho = \{x \in G^e : x\,\rho\, e\}$$

is a normal AG-subgroup of G^e.

Proof. Let ρ be a congruence on G^e. Obviously, $e \in \ker\rho$. Moreover, if $a, b \in \ker\rho$, then $a\rho e$, $b\rho e$ and so $ab\,\rho\, e$. Hence, $ab \in \ker\rho$. Thus $\ker\rho$ is a subgroupoid of G^e. It is inverse closed since for every $x \in \ker\rho$ we have $x\rho e$, which by Lemma 3.1 implies $x'\rho\, e$, whence $x' \in \ker\rho$. Hence, $\ker\rho$ is an AG-subgroup of G^e.

Now let $x \in G^e$. Then for every $y \in x\cdot \ker\rho\, x'$ there exists $a \in \ker\rho$ such that $y = a\cdot ax'$. Thus $(x\cdot ax')\rho(x\cdot ex')$, i.e., $(x\cdot ax')\rho e$, which means that $y = x\cdot ax' \in \ker\rho$. So, $\ker\rho$ is a normal AG-subgroup of G^e. □

Theorem 3.4. *Let K be a normal AG-subgroup of an AG-group G^e. Then the relation ρ_K defined by*

$$a\rho_K b \iff a \in Kb \;\wedge\; b \in Ka$$

is the unique congruence on G^e for which $\ker\rho_K = K$.

Proof. Let K be a normal AG-subgroup of G^e. Clearly, the relation ρ_K is reflexive and symmetric. If $a\rho_K b$, $b\rho_K c$, then obviously $a \in Kb$, $b \in Kc$. From this, applying (1) and (4) we obtain

$$a \in Kb \subseteq K\cdot Kc = KK\cdot Kc = cK\cdot KK = cK\cdot K = KK\cdot c = Kc.$$

Dually, $c \in Ka$, whence $a\rho_K c$ and so ρ is a transitive relation. Therefore, ρ is an equivalence on G^e.

Now let $a\rho_K b$ and $c\rho_K d$. Then $ac \in Kb \cdot Kd = KK \cdot bd = K \cdot bd$ and dually $bd \in K \cdot ac$. Hence $(ab)\rho_K(cd)$. Thus ρ_K is a congruence on G^e.

If $a \in \ker \rho_K$, then $a\rho_K e$. Consequently $a \in Ke$ and $e \in Ka$. From the above $ea' \in Ka \cdot a'$, whence $a' \in a'a \cdot K = eK = K$. Now, since K is inverse closed, we have $a \in K$. Hence $\ker \rho_K \subseteq K$. Conversely, if $a \in K$ then $e, a' \in K$ and so

$$e = a'a \in Ka, \quad a \in K = KK = eK \cdot K = KK \cdot e = Ke,$$

whence $a\rho_K e$ and $a \in \ker \rho_K$. Hence $K \subseteq \ker \rho_K$ and so $K = \ker \rho_K$.

To prove that ρ_K is an unique congruence on G^e with the kernel K consider an arbitrary congruence λ on G^e and assume that its kernel also is K. Then for $a\lambda b$ we have $ab'\lambda\, bb'$ and $aa'\lambda\, ba'$. So, $ab', ba' \in \ker \lambda = K$. Thus $ab' \cdot b \in Kb$ and so $a = bb' \cdot a = ab' \cdot b \in Kb$. Analogously we obtain $b = ba' \cdot a \in Ka$. This proves that $a\rho_K b$. Thus $\lambda \subseteq \rho_K$.

Conversely, if $a\rho_K b$, then $a \in Kb$, $b \in Ka$, and consequently

$$ab' \in Kb \cdot b' = b'b \cdot K = eK = K = \ker \lambda,$$

whence $ab'\lambda e$. This implies $(ab' \cdot b)\lambda eb$, i.e., $(ab' \cdot b)\lambda b$. But $ab' \cdot b = bb' \cdot a = a$, so $a\lambda b$. Hence $\rho_K \subseteq \lambda$. Thus $\rho_K = \lambda$. This means that ρ_K is an unique congruence on G^e with kernel K. □

Corollary 3.5. *For any congruence λ on an AG-group G^e we have $\rho_{\ker \lambda} = \lambda$.*

Proof. Indeed, by Lemma 3.3, $\ker \lambda$ is a normal AG-subgroup of G^e, and in a view of Theorem 3.4 we have $\ker \rho_{\ker \lambda} = \ker \lambda$. This implies $\rho_{\ker \lambda} = \lambda$. □

As a consequence of results proved in [3] we obtain the following proposition which will be used later.

Proposition 3.6. *The lattice of congruences on an AG-group is modular.* □

4. Congruences on AG**-groupoids

An AG^{**}-groupoid G in which for every $x \in G$ there exists uniquely determined element $x^{-1} \in G$ such that

$$x = xx^{-1} \cdot x, \quad x^{-1} = x^{-1}x \cdot x^{-1} \tag{5}$$

and

$$xx^{-1} = x^{-1}x \tag{6}$$

is called *completely inverse.*

Obviously any AG-group is a completely inverse AG^{**}-groupoid. Moreover, in this case $x^{-1} = x'$.

One can prove (cf. [1]) that an AG^{**}-groupoid (satisfying (5)) satisfies (6) if and only if xx^{-1} and $x^{-1}x$ are idempotents. Thus a completely inverse AG^{**}-groupoid containing only one idempotent is an AG-group (cf. [3]).

Let E_G denote the set of idempotents of a completely inverse AG^{**}-groupoid G. Then E_G is a semilattice (cf. [1]) and the relation $\leqslant$ defined on G by

$$a \leqslant b \Longleftrightarrow a \in E_G b$$

is the *natural partial order* on G.

The following result can be deduced from [9].

Lemma 4.1. *In any completely inverse AG^{**}-groupoid G, the relation $\leqslant$ is a compatible partial order on G. Also, $a \leqslant b$ implies $a^{-1} \leqslant b^{-1}$ for all $a, b \in G$.* □

Definition 4.2. For any nonempty subset B of a completely inverse AG^{**}-groupoid G, the set

$$B\omega = \{a \in G : \exists\ (b \in B)\ b \leqslant a\}$$

is called the *closure of B in G*.

If $B = B\omega$, then we shall say that B is *closed in G*. Clearly, $B\omega$ is closed in G.

It is clear that a subgroupoid B of a completely inverse AG^{**}-groupoid G is itself a completely inverse AG^{**}-groupoid if and only if $b \in B$ implies $b^{-1} \in B$ for every $b \in B$. A subgroupoid with this property is called a *completely inverse AG^{**}-subgroupoid* of G.

Definition 4.3. A nonempty subset B of a completely inverse AG^{**}-groupoid G is called:

- *full* if $E_G \subseteq B$,
- *symmetric* if $xy \in B$ implies $yx \in B$ for all $x, y \in G$,
- *normal* if it is full, closed and symmetric.

Denote the set of AG-group congruences on an arbitrary completely inverse AG^{**}-groupoid G by $\mathcal{GC}(G)$, and denote by σ the least such a congruence on G. Then $\mathcal{GC}(G) = [\sigma, G \times G]$ is a complete sublattice of the lattice $\mathcal{C}(G)$ of all congruences on G. Notice that $\mathcal{GC}(G) \cong \mathcal{C}(G/\sigma)$ and so the lattice $\mathcal{GC}(G)$ is modular (by Proposition 3.6). Furthermore, let $\mathcal{N}(G)$ be the set of all normal completely inverse AG^{**}-subgroupoids of G. Obviously, $E_G\omega \subseteq N$ for every normal completely inverse AG^{**}-subgroupoid N of G. If $\emptyset \neq \mathcal{F} \subseteq \mathcal{N}(G)$, then $\bigcap \mathcal{F} \in \mathcal{N}(G)$. Consequently, $\mathcal{N}(G)$ is a complete lattice.

The following theorem describes the AG-groups congruences on a completely inverse AG^{**}-groupoid in the terms of its normal completely inverse AG^{**}-subgroupoids.

Theorem 4.4. *Let N be a normal completely inverse AG^{**}-subgroupoid of a completely inverse AG^{**}-groupoid G. Then the relation*

$$\rho_N = \{(a,b) \in G \times G : ab^{-1} \in N\}$$

is the unique AG-group congruence ρ on G for which $\ker(\rho) = N$.

Proof. Clearly, ρ_N is reflexive. Further, if $ab^{-1} \in N$, then $b^{-1}a \in N$, so $ba^{-1} \in N$, therefore, ρ_N is symmetric. Also, if $ab^{-1}, bc^{-1} \in N$, then $ab^{-1} \cdot c^{-1}b \in N$. Hence $ac^{-1} \cdot b^{-1}b \in N$, so $b^{-1}b \cdot ac^{-1} \in N$, that is, $b^{-1}b \cdot ac^{-1} = n$ for some $n \in N$ and so $n \leqslant ac^{-1}$. Thus $ac^{-1} \in N\omega = N$. Consequently, ρ_N is an equivalence relation on G. Moreover, let $(a,b) \in \rho_N$ and $c \in G$. Then

$$ac \cdot (bc)^{-1} = ac \cdot b^{-1}c^{-1} = ab^{-1} \cdot cc^{-1} \in NE_G \subseteq NN \subseteq N$$

and similarly $ca \cdot (cb)^{-1} \in N$, therefore, ρ_N is a congruence on G. Furthermore, since $ef^{-1} = ef \in E_G \subseteq N$ for all $e, f \in E_G$, then S/ρ_N is an AG-group. Finally, if $a \in N\omega$, then $ea \in N$ for some $e \in E_G$. Hence $ae = ae^{-1} \in N$ and so $(a,e) \in \rho_N$. Thus we have $a \in \ker(\rho)$. Conversely, if $a \in \ker(\rho)$, then $aa \cdot a^{-1} = a^{-1}a \cdot a \in N$. Hence $a \in N\omega = N$. Consequently, $\ker(\rho_N) = N$. It is easy to see that an arbitrary AG-group congruence on G is uniquely determined by its kernel, so ρ_N is a unique AG-group congruence with $\ker(\rho_N) = N$. □

Theorem 4.5. *If ρ is a group congruence on a completely inverse AG^{**}-groupoid G, then* $\ker(\rho) \in \mathcal{N}(G)$ *and* $\rho = \rho_{\ker(\rho)}$.

Proof. Indeed, $N = \ker(\rho)$ is a normal completely inverse AG^{**}-subgroupoid of G, so that $\rho = \rho_N$. □

Corollary 4.6. *The map $\varphi : \mathcal{N}(G) \to \mathcal{GC}(G)$ given by $\varphi(N) = \rho_N$, where G is a completely inverse AG^{**}-groupoid, is a complete lattice isomorphism of $\mathcal{N}(G)$ onto $\mathcal{GC}(G)$. In particular, the lattice $\mathcal{N}(G)$ is modular.* □

More interesting facts concerning certain fundamental congruences on a completely inverse AG^{**}-groupoid one can find in [2] and [3]. In [3] are determined, for example, the maximum idempotent-separating congruence, the least AG-group and the least E-unitary congruence. In particular, the congruences on completely inverse AG^{**}-groupoids are described by their kernel and trace.

Acknowledgements. The author is very grateful to Professor Wieslaw A. Dudek and his Ph.D. student Roman S. Gigoń for their valuable comments and suggestions for improving this paper. Special thanks to R. S. Gigoń for Theorem 4.4.

References

[1] **M. Božinović, P.V. Protić and N. Stevanović**, *Kernel normal system of inverse AG^{**}-groupoids*, Quasigroups and Related Systems **17** (2008), $1-8$.

[2] **W.A. Dudek and R.S. Gigoń**, *Congruences on completely inverse AG^{**}-groupoids*, Quasigroups and Related Systems **20** (2012), $203-209$.

[3] **W.A. Dudek and R.S. Gigoń**, *Completely inverse AG^{**}-groupoids*, Semigroup Forum (in print).

[4] **P. Holgate**, *Groupoids satisfying a simple invertible law*, Math. Stud. **61** (1992), $101-106$.

[5] **M.S. Kamaran**, *Conditions for LA-semigroups to resemble associative structures*, Ph.D. Thesis, Quaid-i-Azam Universiti, Islamabad, 1993.

[6] **Mushtaq**, *Abelian groups defined by LA-semigroups*, Studia Sci. Math. Hungar. **18** (1983), $427-428$.

[7] **Q. Mushtaq and M.S. Kamaran**, *On left almost groups*, Proc. Pak. Acad. of Sciences, **33** (1996), $1-2$.

[8] **Q. Mushtaq and M. Khan**, *Ideals in AG-band and AG^{*}-groupoids*, Quasigroup and Related Systems **14** (2006), $207-215$.

[9] **P.V. Protić**, *Congruences on an inverse AG^{**}-groupoid via the natural partial order*, Quasigroups and Related Systems **17** (2009), $283-290$.

[10] **P.V. Protić and M. Božinović**, *Some congruences on an AG^{**}-groupoid*, Filomat (Niš) **9** (1995), $879-886$.

Received September 6, 2012
Revised December 4, 2012

P.V.Protić
University of Niš, Faculty of Civil Engineering, Aleksandra Medvedeva 14,
18000 Niš, Serbia
E-mail: pvprotic@yahoo.com

Quasigroups and Related Systems **20** (2012), 275 − 281

Polyadic groups and automorphisms of cyclic extensions

Mohammad Shahryari

Abstract. We show that for any n-ary group (G,f), the group $Aut(G,f)$ can be embedded in $Aut(\mathbb{Z}_{n-1} \ltimes G)$ and so we can obtain a class of interesting automorphisms of cyclic extensions.

1. Introduction

Our notations in this article are standard and can be find in [2], for example.

Let (G,f) be an n-ary group. We know that, there is a binary operation "$\cdot$" on G, such that $(G,\cdot)$ is an ordinary group, and further, there is a $\theta \in Aut(G,\cdot)$ with an element $b \in G$, such that

(i) $\theta(b) = b$, and $\theta^{n-1}(x) = bxb^{-1}$ for all $x \in G$,

(ii) $f(x_1^n) = x_1\theta(x_2)\cdots\theta^{n-1}(x_n)b$.

So, some times, we denote (G,f) by the notation $der_{\theta,b}(G,\cdot)$. If $b = e$, the identity element of $(G,\cdot)$, then we use the notation $der_\theta(G,\cdot)$.

We associate another binary group to (G,f) which is called the *universal covering group* or *Post's cover* of (G,f). Let a be an arbitrary element of G and suppose $G_a^* = \mathbb{Z}_{n-1} \times G$. Define a binary operation on this set by

$$(i,x) * (j,y) = (i+j+1, f_*(x, \overset{(i)}{a}, y, \overset{(j)}{a}, \overline{a}, \overset{(i,j)}{a})).$$

Here of course, $i+j+1$ is computed modulo $n-1$, and $(i,j) = n-i-j-3$ modulo $n-1$. The symbol f_* indicates that f applies one or two times depending on the values of i and j and $\overline{a}$ denotes the skew element of a. It is proved that (see [4]), G_a^* is a binary group and the subset

$$R = \{(n-2,x) : x \in G\}$$

is a normal subgroup such that $G_a^*/R \cong \mathbb{Z}_{n-1}$. Further, if we identify G by the subset

$$\{(0,x) : x \in G\},$$

2010 Mathematics Subject Classification: 20N15
Keywords: Polyadic group, covering group, semi-direct product, cyclic extensions.

then G is a coset of R and it generates G_a^*. We also have

$$f(x_1^n) = x_1 * x_2 * \cdots * x_n.$$

It is not hard to see that for all $a, b \in G$, we have $G_a^* \cong G_b^*$, so for simplicity, we always, assume that $a = e$, the identity element of $(G, \cdot)$.

Through this article, we assume that $(G, f) = der_\theta(G, \cdot)$. So, we have $\theta^{n-1} = id$ and

$$f(x_1^n) = x_1\theta(x_2)\cdots\theta^{n-2}(x_{n-1})x_n.$$

We also assume that e is the identity element of $(G, \cdot)$. We will prove first the following theorem on the structure of the Post's cover.

Theorem 1.1. *$(der_\theta(G, \cdot))_e^* \cong \mathbb{Z}_{n-1} \ltimes G$, where $\mathbb{Z}_{n-1}$ acts on $(G, \cdot)$ by $i.x = \theta^i(x)$.*

Note that, we used a special case of this theorem in [6], to investigate representations of polyadic groups. The main idea of this article is almost the same as in [6]. Our second goal is to obtain an embedding from $Aut(G, f)$ to $Aut(G_e^*)$. The method we employ is the same as in [6]. For any $i \in \mathbb{Z}_{n-1}$ and $u \in G$, suppose $\delta(i, u) = \theta(u)\theta^2(u)\ldots\theta^i(u)$. We prove

Theorem 1.2. *Let $\Lambda \in Aut(G, f)$ and define $\Lambda^* : G_e^* \to G_e^*$ by*

$$\Lambda^*(i, x) = (i, \Lambda(x)\delta(i, u)),$$

where $u = \Lambda(e)$. Then the map $\Lambda \mapsto \Lambda^*$ is an embedding.

In [3], the structure of automorphisms of (G, f) is determined. If $\Lambda \in Aut(G, f)$, then we have $\Lambda = R_u\varphi$, where u is an idempotent element, i.e. $f(\overset{(n)}{u}) = u$, R_u is the right translation by u and φ is an ordinary automorphism of $(G, \cdot)$ with the property $[\varphi, \theta] = I_u$, (the bracket denotes the commutator $\varphi\theta\varphi^{-1}\theta^{-1}$ and I_u is the inner automorphism corresponding to u). The converse is also true; if u and φ satisfy above conditions, the $\Lambda = R_u\varphi$ is an automorphism of the polyadic group (G, f). We will use this fact frequently through this article. The interested reader should see [3] for a full description of homomorphisms between polyadic groups.

Combining Theorems 1.1 and 1.2, we obtain an embedding of $Aut(G, f)$ into $Aut(\mathbb{Z}_{n-1} \ltimes G)$. More precisely, we prove the following.

Theorem 1.3. *Let $\hat{G} = A \ltimes G$, with $A = \langle a \rangle$ cyclic of order $n - 1$ and let $\theta(x) = axa^{-1}$. Then for any $\varphi \in Aut(G)$ and $u \in G$, the hypotheses $[\varphi, \theta] = I_u$ and $(au)^{n-1} = 1$ imply that the map*

$$(a^i, x) \mapsto (a^i, u^{-1}\varphi(x)u(au)^i a^{-i})$$

is an automorphism of $\hat{G}$ and these automorphisms are mutually distinct.

2. Proofs

Proof of Theorem 1.1. Note that in G_e^*, we have

$$\begin{aligned}(i,x)*(j,y) &= (i+j+1, f_*(x, \overset{(i)}{e}, y, \overset{(j)}{e}, \overline{e}, \overset{(i,j)}{e}))\\ &= (i+j+1, x\theta(e)\cdots\theta^{i}(e)\theta^{i+1}(y)\theta^{i+2}(e)\\ &\qquad\qquad \cdots\theta^{i+j+2}(e)\theta^{i+j+3}(\overline{e})\cdots\theta^{n-2}(e))\\ &= (i+j+1, x\theta^{i+1}(y)\theta^{i+j+3}(\overline{e})),\end{aligned}$$

but, since $\overline{e} = e$, so

$$(i,x)*(j,y) = (i+j+1, x\theta^{i+1}(y)) = (i,x)(1,e)(j,y),$$

where the right hand side product is done in $\mathbb{Z}_{n-1} \ltimes G$. Note that in general, if $(A,\cdot)$ is a group and $a \in A$, then we can define a new binary operation on A by $x \circ y = xay$ and together with this new operation, A is a group too, and so we denote it by $A_a = (A, \circ)$. We have $A \cong A_a$ and the isomorphism is given by $\varphi(x) = a^{-1}x$. Now, by this notation, we have

$$(der_\theta(G,\cdot))_e^* = G_e^* = (\mathbb{Z}_{n-1} \ltimes G)_{(1,e)},$$

and hence $(der_\theta(G,\cdot))_e^* \cong \mathbb{Z}_{n-1} \ltimes G.$ □

Now, let $\Lambda \in Aut(G,f)$ and $u = \Lambda(e)$. Define $\Lambda_e^* : G_e^* \to G_u^*$ by $\Lambda_e^*(i,x) = (i, \Lambda(x))$.

Lemma 2.1. *Λ_e^* is an isomorphism.*

Proof. Note that

$$\Lambda_e^*((i,x)*(j,y)) = \Lambda_e^*(i+j+1, x\theta^{i+1}(y)) = (i+j+1, \Lambda(x\theta^{i+1}(y))).$$

On the other hand,

$$\begin{aligned}\Lambda_e^*(i,x)*\Lambda_e^*(j,y) &= (i,\Lambda(x))*(j,\Lambda(y))\\ &= (i+j+1, f_*(\Lambda(x), \overset{(i)}{u}, \Lambda(y), \overset{(j)}{u}, \overline{u}, \overset{(i,j)}{u})).\end{aligned}$$

But $f(\overline{u}, \overset{(n-1)}{u}) = u$, so $\Lambda(f(v, \overset{(n-1)}{e})) = \Lambda(e)$, where $\Lambda(v) = \overline{u}$. Therefore $f(v, \overset{(n-1)}{e}) = e$ and so $v = e$ and hence $\overline{u} = \Lambda(e) = u$. Now, we have

$$\begin{aligned}\Lambda_e^*(i,x)*\Lambda_e^*(j,y) &= (i+j+1, \Lambda(f_*(x, \overset{(i)}{e}, y, \overset{(j)}{e}, e, \overset{(i,j)}{e}))) = (i+j+1, \Lambda(x\theta^{i+1}(y)))\\ &= \Lambda_e^*((i,x)*(j,y)).\end{aligned}$$

This shows that Λ_e^* is an isomorphism. □

An element $u \in G$ is said to be *idempotent* if $f(\overset{(n)}{u}) = u$. For an arbitrary element $u \in G$, we remember that the *right translation map* R_u is defined by $R_u(x) = xu$. In [3], it is proved that every element of $Aut(G,f)$ can be uniquely represented as $R_u\varphi$ with u an idempotent and $\varphi \in Aut(G,\cdot)$ satisfies $[\varphi,\theta] = I_u$, where I_u is the inner automorphism of G, corresponding to u. The converse is also true and so we have a complete description of automorphisms of $Aut(G,f)$ in terms of automorphisms of $(G,\cdot)$ and idempotents. Now, for any idempotent u and $i \in \mathbb{Z}_{n-1}$, define

$$\delta(i,u) = \theta(u)\theta^2(u)\cdots\theta^i(u).$$

Note that for the case $i = 0$, we have $\delta(0,u) = \delta(n-1,u) = e$. If $\Lambda \in Aut(G,f)$ and $u = \Lambda(e)$, then we define a map $q_u : G_u^* \to G_e^*$ by $q_u(i,x) = (i, x\delta(i,u))$.

Lemma 2.2. *The map q_u is an isomorphism.*

Proof. We first assume that $i,j \neq 0$. Note that in G_u^*, we have

$$\begin{aligned}(i,x) * (j,y) &= (i+j+1, f_*(x, \overset{(i)}{u}, y, \overset{(j)}{u}, \overline{u}, \overset{(i,j)}{u}))\\ &= (i+j+1, \Lambda(f_*(\Lambda^{-1}(x), \overset{(i)}{e}, \Lambda^{-1}(y), \overset{(j)}{e}, e, \overset{(i,j)}{e})))\\ &= (i+j+1, \Lambda(\Lambda^{-1}(x)\theta^{i+1}(\Lambda^{-1}(y)))).\end{aligned}$$

Now, as we said before, $\Lambda = R_u\varphi$ such that $\varphi \in Aut(G)$ and $[\varphi,\theta] = I_u$. Therefore

$$\begin{aligned}(i,x) * (j,y) &= (i+j+1, R_u\varphi(\varphi^{-1}R_u^{-1}(x)\theta^{i+1}(\varphi^{-1}R_u^{-1}(y))))\\ &= (i+j+1, R_u((xu^{-1})\varphi\theta^{i+1}\varphi(yu^{-1}))).\end{aligned}$$

Since $[\varphi,\theta] = I_u$, so we have $\varphi\theta^{i+1}\varphi^{-1} = (I_u\theta)^{i+1}$. But

$$\begin{aligned}(I_u\theta)^{i+1}(z) &= u\theta(u)\cdots\theta^i(u)\theta^{i+1}(z)\theta(u)^{-1}\cdots\theta(u)^{-1}u^{-1}\\ &= u\delta(i,u)\theta^{i+1}(z)\delta(i,u)^{-1}u^{-1}.\end{aligned}$$

Hence, we have

$$\begin{aligned}(i,x) * (j,y) &= (i+j+1, R_u(xu^{-1}u\delta(i,u)\theta^{i+1}(yu^{-1})\delta(i,u)^{-1}u^{-1}))\\ &= (i+j+1, x\delta(i,u)\theta^{i+1}(yu^{-1})\delta(i,u)^{-1}).\end{aligned}$$

Now, we are ready to show that q_u is a homomorphism. First, note that

$$\begin{aligned}q_u((i,x) * (j,y)) &= q_u(i+j+1, x\delta(i,u)\theta^{i+1}(yu^{-1})\delta(i,u)^{-1})\\ &= (i+j+1, x\delta(i,u)\theta^{i+1}(yu^{-1})\delta(i,u)^{-1}\delta(i+j+1,u)).\end{aligned}$$

On the other hand

$$\begin{aligned}q_u(i,x) * q_u(j,y) &= (i, x\delta(i,u)) * (j, y\delta(j,u))\\ &= (i+j+1, x\delta(i,u)\theta^{i+1}(y\delta(j,u)))\\ &= (i+j+1, x\delta(i,u)\theta^{i+1}(y)\theta^{i+1}(\delta(j,u))).\end{aligned}$$

Hence, q_u is a homomorphism, if and only if we have

$$\theta^{i+1}(\delta(j,u)) = \theta^{i+1}(u^{-1})\delta(i,u)^{-1}\delta(i+j+1,u).$$

But, we have,

$$\theta^{i+1}(u^{-1})\delta(i,u)^{-1}\delta(i+j+1,u) = \theta^{i+2}(u)\cdots\theta^{i+j+1}(u) = \theta^{i+1}(\delta(j,u)).$$

The case $i = 0$ can be verified similarly, so q_u is a homomorphism. It is easy to see that also q_u is a bijection and so we proved the lemma. □

Combining two isomorphisms q_u and Λ^*_e, we obtain an automorphism $\Lambda^* = q_u \circ \Lambda^*_e \in Aut(G^*_e)$. Note that, we have

$$\Lambda^*(i,x) = (i, \Lambda(x)\delta(i,u)) = (0,\Lambda(x)) * (0,u)^i.$$

Lemma 2.3. *The map $\Lambda \mapsto \Lambda^*$ is an embedding from $Aut(G,f)$ into $Aut(G^*_e)$.*

Proof. Let $\Lambda_1, \Lambda_2 \in Aut(G,f)$ and $u = \Lambda_1(e)$ and $v = \Lambda_2(e)$. Suppose also $w = \Lambda_1(v) = (\Lambda_1 \circ \Lambda_2)(e)$. We have

$$(\Lambda_1 \circ \Lambda_2)^*(i,x) = (i, \Lambda_1(\Lambda_2(x))\delta(i,w)).$$

On the other hand

$$\Lambda^*_1(\Lambda^*_2(i,x)) = \Lambda^*_1(i,\Lambda_2(x)\delta(i,v)) = (i, \Lambda_1(\Lambda_2(x)\delta(i,v))\delta(i,u)).$$

But we have

$$\begin{aligned}\Lambda_1(\Lambda_2(x)\delta(i,v)) &= \Lambda_1(\Lambda_2(x)\theta(v)\cdots\theta^i(v)\theta^{i+1}(e)\cdots\theta^{n-2}(e)e)\\ &= \Lambda_1(f(\Lambda_2(x), \overset{(i)}{v}, \overset{(n-i-2)}{e}, e))\\ &= f(\Lambda_1(\Lambda_2(x)), \overset{(i)}{w}, \overset{(n-i-2)}{u}, \Lambda_1(e))\\ &= \Lambda_1(\Lambda_2(x))\delta(i,w)\theta^{i+1}(u)\cdots\theta^{n-2}(u)\Lambda_1(e).\end{aligned}$$

Note that we have

$$\theta^{i+1}\cdots\theta^{n-2}\Lambda_1(e)\delta(i,u) = \theta^{i+1}(u)\cdots\theta^{n-2}(u)u\theta(u)\cdots\theta^i(u) = e,$$

because,

$$\theta(u)\cdots\theta^i(u)\theta^{i+1}(u)\cdots\theta^{n-2}(u)\Lambda_1(e) = u^{-1}\Lambda_1(f(\overset{(n)}{e})) = u^{-1}\Lambda_1(e) = e.$$

Therefore we obtain

$$\Lambda^*_1(\Lambda^*_2(i,x)) = (i, \Lambda_1(\Lambda_2(x))\delta(i,w)),$$

and this shows that the map $\Lambda \mapsto \Lambda^*$ is a homomorphism. Now suppose $\Lambda^* = id$. Then $\Lambda(x)\delta(i,u) = x$ for all x and i, so if we put $x = e$, then $\delta(i,u) = u^{-1}$ for all i. Assuming $i = 1$, we get $\theta(u) = u^{-1}$ and so assuming $i = 2$, we obtain $u^{-1}u = u^{-1}$, hence $u = e$ and consequently $\Lambda = id$. This completes the proof of the lemma. □

Remember that we proved

$$G_e^* = (\mathbb{Z}_{n-1} \ltimes G)_{(1,e)} \cong \mathbb{Z}_{n-1} \ltimes G,$$

and this isomorphism is given by $\varphi(i,x) = (1,e)^{-1}(i,x)$. So,

$$\varphi(i,x) = (n-2,e)(i,x) = (n+i-2, \theta^{n-2}(x)) = (i-1, \theta^{n-2}(x)).$$

Now, for any $\Lambda \in Aut(G,f)$, define

$$\alpha(\Lambda) = \varphi^{-1} \circ \Lambda^* \circ \varphi.$$

Therefore $\alpha(\Lambda)$ is an automorphism of $\mathbb{Z}_{n-1} \ltimes G$ and the map $\Lambda \mapsto \alpha(\Lambda)$ is an embedding. We have

$$\begin{aligned} \alpha(\Lambda)(i,x) &= \varphi^{-1}(i-1, \Lambda(\theta^{-1}(x))\delta(i-1,u)) \\ &= (1,e)(i-1, \Lambda(\theta^{-1}(x))\delta(i-1,u)) \\ &= (i, (\theta\Lambda\theta^{-1})(x)\theta(u^{-1})\delta(i,u)). \end{aligned}$$

Since $\Lambda = R_u\varphi$, so $(\theta\Lambda\theta^{-1})(x) = (\theta\varphi\theta^{-1})(x)\theta(u)$. Hence

$$\alpha(\Lambda)(i,x) = (i, (\theta\varphi\theta^{-1})(x)\delta(i,u)).$$

On the other hand $\theta\varphi\theta^{-1} = I_u^{-1}\varphi$ and hence

$$\alpha(\Lambda)(i,x) = (i, u^{-1}\varphi(x)u\delta(i,u)).$$

Summarizing, we obtain the following corollary:

Corollary 2.4. *There is an embedding* $\alpha : Aut(G,f) \to Aut(\mathbb{Z}_{n-1} \ltimes G)$*, such that*

$$\alpha(\Lambda)(i,x) = (i, u^{-1}\varphi(x)u\delta(i,u)).$$

Now, we are ready to prove Theorem 1.3.

Proof of Theorem 1.3. Suppose $\hat{G} = A \ltimes G$ where $A = \langle a \rangle$ is a cyclic of order $n-1$. Define an automorphism of G by $\theta(x) = axa^{-1}$, so $\theta^{n-1} = id$. Let

$$(G,f) = der_\theta(G,\cdot).$$

So, there is an embedding $\alpha : Aut(G,f) \to Aut(\hat{G})$ such that

$$\alpha(\Lambda)(a^i,x) = (a^i, u^{-1}\varphi(x)u\delta(i,u)).$$

Since u is an idempotent, so $f(\overset{(n)}{u}) = u$, and therefore

$$u\theta(u)\cdots\theta^{n-1}(u) = u,$$

which implies that

$$aua^{-1}a^2ua^{-2}\cdots a^{n-2}ua^{-(n-2)}u = e.$$

Hence $(au)^{n-1} = 1$. Similarly, $\delta(i,u) = (au)^i a^{-i}$, so for any $\varphi \in Aut(G)$ and for any $u \in G$, the hypotheses

$$(au)^{n-1} = 1, \quad [\varphi, \theta] = I_u$$

imply that the map

$$(a^i, x) \mapsto (a^i, u^{-1}\varphi(x)u(au)^i a^{-i})$$

is an automorphism of $\hat{G}$. Clearly this is an embedding and hence the theorem is proved. □

Example 2.5. Let $E = GF(q)$ be the Galois field of order q and $m \geqslant 1$. Let $G = (E^m, +)$ and suppose $\alpha : E^m \to E^m$ is a linear map of order $n-1$. Then $A = \langle\alpha\rangle$ acts naturally on G, so $\hat{G} = A \ltimes G \cong \mathbb{Z}_{n-1} \ltimes E^m$. In this case $\theta = \alpha^{-1}$ and for any $u \in \ker(1 + \alpha + \cdots + \alpha^{n-2})$ and any

$$\varphi \in C_{GL_m(q)}(\alpha)$$

we have $[\theta, \varphi] = 1 = I_u$. Note that we have $u \in \ker(1 + \alpha + \cdots + \alpha^{n-2})$, iff $u = \alpha(v) - v$ for some $v \in E^m$. This shows that for any such v and φ, the map

$$(\alpha^i, x) \mapsto (\alpha^i, \varphi(x) + (\alpha^{i-1} - \alpha^{-1})(v))$$

is an automorphism of $\mathbb{Z}_{n-1} \ltimes E^m$.

References

[1] **W.A. Dudek and K. Glazek**, *Around the Hosszú-Gluskin Theorem for n-ary groups*, Discrete Math. **308** (2008), 4861 – 4876.

[2] **W.A. Dudek and M. Shahryari**, *Representation theory of polyadic groups*, Algebras and Representation Theory **15** (2012), 29 – 51.

[3] **H. Khodabandeh and M. Shahryari**, *On the Automorphisms and representations of polyadic groups*, Commun. Algebra **40** (2012), 2199 – 2212.

[4] **J. Michalski**, *Covering k-groups of n-groups*, Archivum Math. (Brno) **17** (1981), 207 – 226.

[5] **E.L. Post**, *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1940), 208 – 350.

[6] **M. Shahryari**, *Representations of finite polyadic groups*, Commun. Algebra **40** (2012), 1625 – 1631.

Received June 7, 2012

Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Tabriz,
Tabriz, Iran
E-mail: mshahryari@tabrizu.ac.ir