Quasigroups and Related Systems **19** (2011), 169 – 172

A note on M-hypersystems and N-hypersystems in Γ-semihypergroups

Saleem Abdullah, Muhammad Aslam and Tariq Anwar

Abstract. In this paper, we have introduced the notions of M-hypersystem and N-hypersystem in Γ-semihypergroups, and some related properties are investigated. We have also proved that left Γ-hyperideal P of a Γ-semihypergroup S is quasi-prime if and only if $S\backslash P$ is an M-hypersystem.

1. Introduction

In 1986, Sen and Saha [3] defined the notion of a Γ-semigroup as a generalization of a semigroup. Recently, Davvaz, Hila and et. al. [1, 2] introduced the notion of Γ-semihypergroup as a generalization of a semigroup, a generalization of a semihypergroup and a generalization of a Γ-semigroup. The notion of a Γ-hyperideal of a Γ-semihypergroup was introduced in [1].

Let S and Γ be two non-empty sets. Then S is called a Γ-*semihypergroup* if every $\gamma \in \Gamma$ is a hyperoperation on S, i.e., $x\gamma y \subseteq S$ for every $x, y \in S$, and for every $\alpha, \beta \in \Gamma$ and $x, y, z \in S$ we have $x\alpha(y\beta z) = (x\alpha y)\beta z$. Let S be a Γ-semihypergroup and $\gamma \in \Gamma$. A non-empty subset A of S is called a *sub-*Γ-*semihypergroup* of S if $x\gamma y \subseteq A$ for every $x, y \in A$. A Γ-semihypergroup S is called *commutative* if for all $x, y \in S$ and $\gamma \in \Gamma$, we have $x\gamma y = y\gamma x$.

Example 1.1. Let $S = [0, 1]$ and $\Gamma = \mathbb{N}$. For every $x, y \in S$ and $\gamma \in \Gamma$, we define $\gamma : S^2 \to P^*(S)$ by $x\gamma y = \left[0, \frac{xy}{\gamma}\right]$. Then γ is hyperoperation. For every $x, y, z \in S$ and $\alpha, \beta \in \Gamma$, we have $(x\alpha y)\beta z = \left[0, \frac{xyz}{\alpha\beta}\right] = x\alpha(y\beta z)$. Thus S is a Γ-semihypergroup. □

Example 1.2. Let $(S, \circ)$ be a semihypergroup and Γ be a non-empty subset of S. We define $x\gamma y = x \circ y$ for every $x, y \in S$ and $\gamma \in \Gamma$. Thus S is a Γ-semihypergroup. □

2010 Mathematics Subject Classification: 20N20, 20M17
Keywords: Γ-semihypergroups, quasi-semiprime, M-hypersystem, N-hypersystem.

Example 1.3. Let $S = (0,1)$, $\Gamma = \{\gamma_n \,|n \in \mathbb{N}\}$ and for every $n \in \mathbb{N}$ we define hyperoperation γ_n on S as follows

$$x\gamma_n y = \left\{ \frac{xy}{2^k} \mid 0 \leqslant k \leqslant n \right\}.$$

Then $x\gamma_n y \subset S$ and for every $m, n \in \mathbb{N}$ and $x, y, z \in S$

$$(x\gamma_n y)\gamma_m z = \left\{ \frac{xyz}{2^k} \mid 0 \leqslant k \leqslant n+m \right\} = x\gamma_n (y\gamma_m z).$$

So, S is a Γ-semihypergroup. □

A Γ-semihypergroup S is called *regular* if for all $a \in S$ and $\alpha, \beta \in \Gamma$ there exists $x \in S$ such that $a \in a\alpha x\beta a$.

A non-empty subset A of S is a *left* (*right*) Γ-*hyperideal* of S if $A\Gamma S \subseteq A$ ($S\Gamma A \subseteq A$). A Γ-*hyperideal* is both a left and right Γ-hyperideal.

A left Γ-hyperideal P is *quasi-prime* if for any left Γ-hyperideals A and B such that $A\Gamma B \subseteq P$ it follows $A \subseteq P$ or $B \subseteq P$.

A left Γ-hyperideal P is *quasi-prime* P is *quasi-semiprime* if any left Γ-hyperideal A from $A\Gamma A \subseteq P$ it follows $A \subseteq P$.

2. M-hypersystem and N-hypersystem

A Γ-semihypergroup S is called *fully* Γ-*hyperidempotent* if every Γ-hyperideal is idempotent.

Proposition 2.1. *If S is Γ-semihypergroup and A, B are Γ-hyperideal of S, then the following are equivalent:*

(*a*) *S is fully Γ-hyperidempotent,*

(*b*) $A \cap B = \langle A\Gamma B\rangle$,

(*c*) *the set of all Γ-hyperideals of S form a semilattice $(L_S, \wedge)$, where $A \wedge B = \langle A\Gamma B\rangle$.*

Proof. (*a*) $\Rightarrow$ (*b*) Always hold $A\Gamma B \subseteq A \cap B$, for any Γ-hyperideals A and B of S. Hence $\langle A\Gamma B\rangle \subseteq A \cap B$.

Converse let $x \in A \cap B$. If $\langle x\rangle$ denote the principle left Γ-hyperideal generated by x, then $x \in \langle x\rangle = \langle x\rangle\Gamma\langle x\rangle \subseteq \langle A\Gamma B\rangle$. Thus $x \in \langle A\Gamma B\rangle$. Therefore $A \cap B \subseteq \langle A\Gamma B\rangle$, which proves (*b*).

(*b*) $\Rightarrow$ (*c*) $A \wedge B = \langle A\Gamma B\rangle = A \cap B = B \cap A = \langle B\Gamma A\rangle = B \wedge A$.

(*c*) $\Rightarrow$ (*b*) Let $(L_S, \wedge)$ be a semilattice. Then $A = A \wedge A = \langle A\Gamma A\rangle = A\Gamma A$. Hence S is fully Γ-hyperidempotent. □

Corollary 2.2. *If Γ-semihypergroup S is regular, then $S = S\Gamma S$.* □

A subset M of Γ-semihypergroup S is called an *M-hypersystem* if for all $a, b \in M$, there exist $x \in S$ and $\alpha, \beta \in \Gamma$ such that $a\alpha x\beta b \subseteq M$.

A subset N of Γ-semihypergroup S is called an *N-hypersystem* if for all $a \in N$, there exist $x \in S$ and $\alpha, \beta \in \Gamma$ such that $a\alpha x\beta a \subseteq N$.

Obviously, each M-hypersystem is an N-hypersystem.

Example 2.3. The set $S_i = \left(0, 2^{-i}\right)$, where $i \in \mathbb{N}$, is an M-hypersystem of a Γ-semihypergroup S defined in Example 1.3. The set $T_i = \left(0, 4^{-i}\right)$, where $i \in \mathbb{N}$, is its an N-hypersystem of S. □

Example 2.4. The set $T = [0, t]$, where $t \in [0, 1]$, is an M-hypersystem and an N-hypersystem of a Γ-semihypergroup defined in Example 1.1. □

Theorem 2.5. *Let P be a left Γ-hyperideal of Γ-semihypergroup S. Then the following are equivalent:*

(1) *P is a quasi-prime,*
(2) *$A\Gamma B = \langle A\Gamma B\rangle \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$ for all left Γ-hyperideals,*
(3) *$A \nsubseteq P$ or $B \nsubseteq P \Rightarrow A\Gamma B \nsubseteq P$ for all left Γ-hyperideals,*
(4) *$a \notin P$ or $b \notin P \Rightarrow a\Gamma b \nsubseteq P$ for all $a, b \in S$,*
(5) *$a\Gamma b \subseteq P \Rightarrow a \in P$ or $b \in P$ for all $a, b \in S$.*

Proof. (1) ⇔ (2) ⇔ (3) is straightforward.

(1) ⇔ (4) Let $\langle a\rangle\Gamma\langle b\rangle \subseteq P$. Then by (1) either $\langle a\rangle \subseteq P$ or $\langle b\rangle \subseteq P$, which implies that either $a \in P$ or $b \in P$.

(4) ⇒ (2) Let $A\Gamma B \subseteq P$. If $a \in A$ and $b \in B$, then $\langle a\rangle\Gamma\langle b\rangle \subseteq P$, now by (4) either $a \in P$ or $b \in P$, which implies that either $A \subseteq P$ *or* $B \subseteq P$.

(1) ⇒ (5) Let P be a left Γ-hyperideal of Γ-semihypergroup S and $a\Gamma S\Gamma b \subseteq P$. Then, by (2), (3) and (1), we get $S\Gamma(a\Gamma S\Gamma b) \subseteq S\Gamma P \subseteq P$, that is, $S\Gamma(a\Gamma S\Gamma b) = (S\Gamma a)\Gamma(S\Gamma b)$. Thus, $(S\Gamma a)\Gamma(S\Gamma b) \subseteq P$ implies either $S\Gamma a \subseteq P$ or $S\Gamma b \subseteq P$.

Since $S\Gamma a$ and $S\Gamma b$ are left Γ-hyperideals, for $L(a) = (a \cup S\Gamma a)$ we have

$$\begin{aligned} L(a)\,\Gamma L(a)\,\Gamma L(a) &= (a \cup S\Gamma a)\,\Gamma\,(a \cup S\Gamma a)\,\Gamma\,(a \cup S\Gamma a) \\ &\subseteq a\Gamma a \cup a\Gamma S\Gamma a \cup S\Gamma a\Gamma a \cup \subseteq S\Gamma a\Gamma S\Gamma a\Gamma a \cup S\Gamma a \\ &\subseteq S\Gamma a \subseteq P. \end{aligned}$$

Hence $L(a)\,\Gamma L(a)\,\Gamma L(a) = (L(a)\,\Gamma L(a))\,\Gamma L(a) \subseteq P$. Since P is quasi-prime and $L(a)\,\Gamma L(a)$ is a left Γ-hyperideal of S we have $L(a)\,\Gamma L(a) \subseteq P$

or $L(a) \subseteq P$. If $L(a) \subseteq P$, then $a \in L(a) \subseteq P$. Let $L(a)\Gamma L(a) \subseteq P$. Since P is quasi-prime, $L(a) \subseteq P$. Thus, $a \in L(a) \subseteq P$, i.e., $a \in P$.

(5) $\Rightarrow$ (1) Assume that $A\Gamma B \subseteq P$, wher A and B are left Γ-hyperideals of S such that $A \nsubseteq P$. Then there exist $x \in A$ such that $x \notin P$. Hence $x\Gamma S\Gamma y \subseteq A\Gamma S\Gamma B \subseteq A\Gamma B \subseteq P$ for all $y \in B$. Then, by (5), $y \in P$. □

Proposition 2.6. *A left Γ-hyperideal P of Γ-semihypergroup S is quasi-prime if and only if $S\backslash P$ is an M-hypersystem.*

Proof. Let $S\backslash P$ be an M-hypersystem and $a\Gamma S\Gamma b \subseteq P$ for some $a, b \in S\backslash P$. Then there exist $x \in S$ and $\alpha, \beta \in \Gamma$ such that $a\alpha x\beta b \subseteq S\backslash P$. This implies that $a\alpha x\beta b \nsubseteq P$, which is a contradiction. Hence either $a \in P$ or $b \in P$.

Conversely, if P is quasi-prime and $x, y \in S\backslash P$, then for $z \in S$ and $\alpha, \beta \in \Gamma$ such that $x\alpha z\beta y \nsubseteq S\backslash P$ we haven $x\alpha z\beta y \subseteq P$, i.e., either $x \in P$ or $y \in P$. So, $S\backslash P$ is an M-hypersystem. □

Proposition 2.7. *A left Γ-hyperideal P of Γ-semihypergroup S is quasi-semiprime if and only if $S\backslash P$ is an N-hypersystem.*

Proof. Let $S\backslash P$ be an N-hypersystem and $a\Gamma S\Gamma a \subseteq P$ with $a \notin P$. Then $a\alpha x\beta b \subseteq S\backslash P$ for some $x \in S$ and $\alpha, \beta \in \Gamma$. Thus $a\alpha x\beta a \nsubseteq P$, which is a contradiction. Hence $a \in P$. The converse statement is obvious. □

Theorem 2.8. *Let S be Γ-semihypergroup and P a proper left Γ-hyperideal of S. Then the following are equivalent:*

(1) *P is quasi-prime,*
(2) *$a\Gamma M\Gamma b \subseteq P$ implies $a \in P$ or $b \in P$,*
(3) *$S\backslash P$ is an M-system,*
(4) *$S\backslash P$ is an N-system.* □

References

[1] **S. M. Anvariyeh, S. Mirvakili, and B. Dawaz**, *On Γ-hyperideals in Γ-semihypergroups*, Carpathian J. Math. **26** (2010), 11 – 23.

[2] **D. Heidari, S. O. Dehkordi and B. Davvaz,** *Γ-semihypergroups and their properties,* U.P.B. Sci. Bull., Series A, **72** (2010), 197 – 210.

[3] **M. K. Sen, and N. K. Saha**, *On Γ-semigroup, I*, Bull. Cal. Math. Soc. **78** (1986), 180 – 186.

Received October 19, 2010

Department of Mathematics Quaid-i-Azam University, Islamabad 45320, Pakistan.

Quasigroups and Related Systems **19** (2011), 173 – 182

One relator quotients of the Hecke group $\mathbf{H}(\sqrt{3})$

Muhammad Aslam, Abid Ali and Rehan Ahmad

Abstract. One relator quotients of the modular group Γ and of the groups $H(\sqrt{2})$ and $H(\frac{1+\sqrt{5}}{2})$, have been discussed in [3], [5], [9], [10] and [11]. In this paper we obtain one relator quotients of $H(\sqrt{3})$, by adding an extra relation to the existing ones.

1. Introduction

E. Hecke introduced Hecke groups denoted by $H(\lambda_q)$. These are finitely generated discrete subgroups of $PSL(2,\mathbb{R})$, generated by transformations $R(z) = -1/z$ and $T(z) = -1/(z+\lambda_q)$, of order 2 and q, respectively, where $\lambda_q = 2cos(\pi/q)$, $q \in \mathbb{N}$, $q \geqslant 3$. The modular group $H(\lambda_3) = H(1) = PSL(2,\mathbb{Z})$ is the most interesting, important and a well discussed Hecke group from many aspects as in [3], [5], [6] and [10]. The group for $q = 5$, $H(\lambda_5) = H(\frac{1+\sqrt{5}}{2})$ has been discussed in [4] and [9]. And many similarities to the modular group have been observed. Other two interesting groups of this class are obtained for $q = 4$ and $q = 6$. These are denoted by $H(\sqrt{2})$ and $H(\sqrt{3})$ corresponding to $q = 4$ and $q = 6$, respectively. The group $H(\sqrt{3})$ has been discussed from some aspects in [1] and [11]. One reason for $H(\sqrt{2})$ and $H(\sqrt{3})$ to be the next most important Hecke groups is that these are the only, whose elements can be described completely [11]. One relator quotients of the Hecke groups have been an important aspect of study of Hecke groups for many mathematicians. For example one can refer to [3], [5], [9] and [10]. In [11] one relator quotients of $H(\sqrt{2})$ have been a part of discussion.

In this paper we obtain one relator quotients of the Hecke group $H(\sqrt{3})$. We have mostly used the same notations as were used in [3], [9] and [10].

2010 Mathematics Subject Classification: 11F06, 20H10
Keywords: Hecke group, cyclically reduced word, one relator quotient.

2. One relator quotients of $\mathbf{H}(\sqrt{3})$

$H(\sqrt{3})$ has a presentation $\langle a, b : a^2 = b^6 = 1\rangle$. The effect of adding a new relation to this, is the formation of a new group which is quotient group of $H(\sqrt{3})$.

By adding another relation $w = R(a, b) = 1$ in terms of a and b for a cyclically reduced word $w = ab^{\varepsilon_1}ab^{\varepsilon_2}ab^{\varepsilon_3}...ab^{\varepsilon_n}$, where $1 \leqslant \varepsilon_i \leqslant 5$, we obtain one relator quotient of $H(\sqrt{3})$.

Throughout this paper we denote by k the sum of exponents of a in w and by l the sum of exponents of b in w.

Theorem 2.1. *If $k = 0$ then $1 \leqslant l \leqslant 5$ and if $k = n$ then $n \leqslant l \leqslant 5n$.*

Proof. Immediately follows from the table given at the end. □

As in [9], a word w' is equivalent to w if it can be obtained by cutting some part of w from the beginning and pasting it to the end in the same order and vice versa. Let $N_{k,l}$ be total number of non equivalent cyclically reduced words w with k and l as defined above. Then we have the following theorem.

Theorem 2.2. $N_{n,n} = N_{n,n+1} = N_{n,5n} = N_{n,5n-1} = 1$.

Proof. Immediately follows from the table given at the end. □

To obtain cyclically reduced words for a given pair of integers k and l, we have followed the procedure as followed in [9] and [10]. We illustrate it with an example.

Example 2.3. For $k = 4$ and $l = 11$, we obtain the following non equivalent cyclically reduced words.

$ababab^4ab^5$, $ababab^5ab^4$, $abab^4abab^5$, $abab^2ab^4ab^4$, $abab^4ab^4ab^4$, $abab^4ab^2ab^4$, $abab^3ab^3ab^4$, $abab^3ab^4ab^3$, $abab^4ab^3ab^3$, $ab^2ab^2ab^3ab^4$, $ab^2ab^2ab^4ab^3$, $ab^2ab^3ab^2ab^4$, $ab^2ab^3ab^3ab^3$. □

Let us consider the first word $ababab^4ab^5$, other words $ab^5ababab^4$, ab^4ab^5abab and $abab^4ab^5ab$ are omitted since these are equivalent to it. We add a relation $ababab^4ab^5 = 1$ to the group $\langle a, b : a^2 = b^6 = 1\rangle$. Using all these relations we simplify as

$$a = babab^4ab^5, \quad a = bababab^4ab^5, \quad b = ab^5a$$

and equivalently we have $abab = 1$. Thus we get $\langle a, b : a^2 = b^6 = (ab)^2 = 1\rangle$ which is finite presentation of the triangle group $\Delta(2, 6, 2)$ and is isomorphic to D_6, of order 12. The following table gives the information for different pairs of values for k and l.

k	l	words	quotient group	abstract structure
0	1	b	$\langle a, b : a^2 = b^6 = b = 1\rangle$	C_2
0	2	b^2	$\langle a, b : a^2 = b^6 = b^2 = 1\rangle$	$infinite\ group$
0	3	b^3	$\langle a, b : a^2 = b^6 = b^3 = 1\rangle$	$infinite\ group$
0	4	b^4	$\langle a, b : a^2 = b^6 = b^4 = 1\rangle$	$infinite\ group$
0	5	b^5	$\langle a, b : a^2 = b^6 = b^5 = 1\rangle$	C_2
1	0	a	$\langle a, b : a^2 = b^6 = a = 1\rangle$	C_6
1	1	ab	$\langle a, b : a^2 = b^6 = ab = 1\rangle$	C_2
1	2	ab^2	$\langle a, b : a^2 = b^6 = ab^2 = 1\rangle$	C_2
1	3	ab^3	$\langle a, b : a^2 = b^6 = ab^3 = 1\rangle$	C_6
1	4	ab^4	$\langle a, b : a^2 = b^6 = ab^4 = 1\rangle$	C_2
1	5	ab^5	$\langle a, b : a^2 = b^6 = ab^5 = 1\rangle$	C_2
2	2	$abab$	$\langle a, b : a^2 = b^6 = (ab)^2 = 1\rangle$	D_6
2	3	$abab^2$	$\langle a, b : a^2 = b^6 = abab^2 = 1\rangle$	C_6
2	4	$abab^3$	$\langle a, b : a^2 = b^6 = abab^3 = 1\rangle$	V_4
		ab^2ab^2	$\langle a, b : a^2 = b^6 = ab^2ab^2 = 1\rangle$	$infinite\ group$
2	5	$abab^4$	$\langle a, b : a^2 = b^6 = abab^4 = 1\rangle$	S_3
		ab^2ab^3	$\langle a, b : a^2 = b^6 = ab^2ab^3 = 1\rangle$	C_2
2	6	$abab^5$	$\langle a, b : a^2 = b^6 = abab^5 = 1\rangle$	$V_4 \times C_3$
		ab^2ab^4	$\langle a, b : a^2 = b^6 = ab^2ab^4 = 1\rangle$	$infinite\ group$
		ab^3ab^3	$\langle a, b : a^2 = b^6 = ab^3ab^3 = 1\rangle$	$infinite\ group$
2	7	ab^2ab^5	$\langle a, b : a^2 = b^6 = ab^2ab^5 = 1\rangle$	S_3
		ab^3ab^4	$\langle a, b : a^2 = b^6 = ab^3ab^4 = 1\rangle$	C_2
2	8	ab^3ab^5	$\langle a, b : a^2 = b^6 = ab^3ab^5 = 1\rangle$	V_4
		ab^4ab^4	$\langle a, b : a^2 = b^6 = ab^4ab^4 = 1\rangle$	$infinite\ group$
2	9	ab^4ab^5	$\langle a, b : a^2 = b^6 = ab^4ab^5 = 1\rangle$	C_6
2	10	ab^5ab^5	$\langle a, b : a^2 = b^6 = ab^5ab^5 = 1\rangle$	D_6
3	3	$ababab$	$\langle a, b : a^2 = b^6 = ababab = 1\rangle$	$infinite\ group$

k	l	words	quotient group	abstract structure
3	4	$ababab^2$	$\langle a,b : a^2 = b^6 = ababab^2 = 1\rangle$	C_2
3	5	$ababab^3$	$\langle a,b : a^2 = b^6 = ababab^3 = 1\rangle$	S_3
		$abab^2ab^2$	$\langle a,b : a^2 = b^6 = abab^2ab^2 = 1\rangle$	C_2
3	6	$ababab^4$	$\langle a,b : a^2 = b^6 = ababab^4 = 1\rangle$	$A_4 \times C_2$
		$abab^2ab^3$	$\langle a,b : a^2 = b^6 = abab^2ab^3 = 1\rangle$	C_6
		$abab^3ab^2$	$\langle a,b : a^2 = b^6 = abab^3ab^2 = 1\rangle$	C_6
		$ab^2ab^2ab^2$	$\langle a,b : a^2 = b^6 = ab^2ab^2ab^2 = 1\rangle$	$infinite\ group$
3	7	$ababab^5$	$\langle a,b : a^2 = b^6 = ababab^5 = 1\rangle$	S_3
		$abab^2ab^4$	$\langle a,b : a^2 = b^6 = abab^2ab^4 = 1\rangle$	C_2
		$abab^4ab^2$	$\langle a,b : a^2 = b^6 = abab^4ab^2 = 1\rangle$	C_2
		$abab^3ab^3$	$\langle a,b : a^2 = b^6 = abab^3ab^3 = 1\rangle$	S_3
		$ab^2ab^2ab^3$	$\langle a,b : a^2 = b^6 = ab^2ab^2ab^3 = 1\rangle$	C_2
3	8	$abab^2ab^5$	$\langle a,b : a^2 = b^6 = abab^2ab^5 = 1\rangle$	C_2
		$abab^5ab^2$	$\langle a,b : a^2 = b^6 = abab^5ab^2 = 1\rangle$	C_2
		$abab^3ab^4$	$\langle a,b : a^2 = b^6 = abab^3ab^4 = 1\rangle$	C_2
		$abab^4ab^3$	$\langle a,b : a^2 = b^6 = abab^4ab^3 = 1\rangle$	C_2
		$ab^2ab^2ab^4$	$\langle a,b : a^2 = b^6 = ab^2ab^2ab^4 = 1\rangle$	C_2
		$ab^2ab^3ab^3$	$\langle a,b : a^2 = b^6 = ab^2ab^3ab^3 = 1\rangle$	C_2
3	9	$abab^3ab^5$	$\langle a,b : a^2 = b^6 = abab^3ab^5 = 1\rangle$	$C_9 \sim C_6$
		$abab^5ab^3$	$\langle a,b : a^2 = b^6 = abab^5ab^3 = 1\rangle$	$C_9 \sim C_6$
		$ab^2ab^2ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^2ab^5 = 1\rangle$	$A_4 \times C_2$
		$abab^4ab^4$	$\langle a,b : a^2 = b^6 = abab^4ab^4 = 1\rangle$	$A_4 \times C_2$
		$ab^2ab^3ab^4$	$\langle a,b : a^2 = b^6 = ab^2ab^3ab^4 = 1\rangle$	$C_7 \sim C_6$
		$ab^2ab^4ab^3$	$\langle a,b : a^2 = b^6 = ab^2ab^4ab^3 = 1\rangle$	$C_7 \sim C_6$
		$ab^3ab^3ab^3$	$\langle a,b : a^2 = b^6 = ab^3ab^3ab^3 = 1\rangle$	$infinite\ group$
3	10	$abab^4ab^5$	$\langle a,b : a^2 = b^6 = abab^4ab^5 = 1\rangle$	C_2
		$abab^5ab^4$	$\langle a,b : a^2 = b^6 = abab^5ab^4 = 1\rangle$	C_2
		$ab^2ab^3ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^3ab^5 = 1\rangle$	C_2
		$ab^2ab^5ab^3$	$\langle a,b : a^2 = b^6 = ab^2ab^5ab^3 = 1\rangle$	C_2
		$ab^2ab^4ab^4$	$\langle a,b : a^2 = b^6 = ab^2ab^4ab^4 = 1\rangle$	C_2
		$ab^3ab^3ab^4$	$\langle a,b : a^2 = b^6 = ab^3ab^3ab^4 = 1\rangle$	C_2

k	l	words	quotient group	structure
3	11	$abab^5ab^5$	$\langle a,b : a^2 = b^6 = abab^5ab^5 = 1\rangle$	S_3
		$ab^2ab^4ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^4ab^5 = 1\rangle$	C_2
		$ab^3ab^3ab^5$	$\langle a,b : a^2 = b^6 = ab^3ab^3ab^5 = 1\rangle$	S_3
		$ab^2ab^5ab^4$	$\langle a,b : a^2 = b^6 = ab^2ab^5ab^4 = 1\rangle$	C_2
		$ab^3ab^4ab^4$	$\langle a,b : a^2 = b^6 = ab^3ab^4ab^4 = 1\rangle$	C_2
3	12	$ab^2ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^5ab^5 = 1\rangle$	$A_4 \times C_2$
		$ab^3ab^4ab^5$	$\langle a,b : a^2 = b^6 = ab^3ab^4ab^5 = 1\rangle$	C_6
		$ab^3ab^5ab^4$	$\langle a,b : a^2 = b^6 = ab^3ab^5ab^4 = 1\rangle$	C_6
2		$ab^4ab^4ab^4$	$\langle a,b : a^2 = b^6 = ab^4ab^4ab^4 = 1\rangle$	$infinite\ group$
3	13	$ab^3ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^3ab^5ab^5 = 1\rangle$	S_3
		$ab^4ab^4ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^4ab^5 = 1\rangle$	C_2
3	14	$ab^4ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^5ab^5 = 1\rangle$	C_2
3	15	$ab^5ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^5ab^5ab^5 = 1\rangle$	$\Delta(2,6,3)$
4	4	$abababab$	$\langle a,b : a^2 = b^6 = abababab = 1\rangle$	$\Delta(2,6,4)$
4	5	$abababab^2$	$\langle a,b : a^2 = b^6 = abababab^2 = 1\rangle$	C_2
4	6	$abababab^3$	$\langle a,b : a^2 = b^6 = abababab^3 = 1\rangle$	$D_4 \times C_3$
		$ababab^2ab^2$	$\langle a,b : a^2 = b^6 = ababab^2ab^2 = 1\rangle$	$C_6 \times S_3$
		$abab^2abab^2$	$\langle a,b : a^2 = b^6 = abab^2abab^2 = 1\rangle$	$infinite\ group$
4	7	$abababab^4$	$\langle a,b : a^2 = b^6 = abababab^4 = 1\rangle$	$GL(2,3)$
		$ababab^2ab^3$	$\langle a,b : a^2 = b^6 = ababab^2ab^3 = 1\rangle$	C_2
		$ababab^3ab^2$	$\langle a,b : a^2 = b^6 = ababab^3ab^2 = 1\rangle$	C_2
		$abab^2abab^3$	$\langle a,b : a^2 = b^6 = abab^2abab^3 = 1\rangle$	S_3
		$abab^2ab^2ab^2$	$\langle a,b : a^2 = b^6 = abab^2ab^2ab^2 = 1\rangle$	C_2
4	8	$abababab^5$	$\langle a,b : a^2 = b^6 = abababab^5 = 1\rangle$	D_4
		$ababab^2ab^4$	$\langle a,b : a^2 = b^6 = ababab^2ab^4 = 1\rangle$	D_2
		$ababab^4ab^2$	$\langle a,b : a^2 = b^6 = ababab^4ab^2 = 1\rangle$	$infinite\ group$
		$abab^2abab^4$	$\langle a,b : a^2 = b^6 = abab^2abab^4 = 1\rangle$	$infinite\ group$
		$ababab^3ab^3$	$\langle a,b : a^2 = b^6 = ababab^3ab^3 = 1\rangle$	$GAP4(24,8)$
		$abab^3abab^3$	$\langle a,b : a^2 = b^6 = abab^3abab^3 = 1\rangle$	$infinite\ group$
		$abab^2ab^2ab^3$	$\langle a,b : a^2 = b^6 = abab^2ab^2ab^3 = 1\rangle$	D_2
		$abab^2ab^3ab^2$	$\langle a,b : a^2 = b^6 = abab^2ab^3ab^2 = 1\rangle$	$infinite\ group$
		$abab^3ab^2ab^2$	$\langle a,b : a^2 = b^6 = abab^3ab^2ab^2 = 1\rangle$	D_2
		$ab^2ab^2ab^2ab^2$	$\langle a,b : a^2 = b^6 = ab^2ab^2ab^2ab^2 = 1\rangle$	$infinite\ group$

k	l	words	quotient group	structure
4	9	$ababab^2ab^5$	$\langle a,b : a^2 = b^6 = ababab^2ab^5 = 1\rangle$	$S_3 \times C_3$
		$ababab^5ab^2$	$\langle a,b : a^2 = b^6 = ababab^5ab^2 = 1\rangle$	$S_3 \times C_3$
		$abab^2abab^5$	$\langle a,b : a^2 = b^6 = abab^2abab^5 = 1\rangle$	$GAP4(48,33)$
		$ababab^3ab^4$	$\langle a,b : a^2 = b^6 = ababab^3ab^4 = 1\rangle$	C_6
		$ababab^4ab^3$	$\langle a,b : a^2 = b^6 = ababab^4ab^3 = 1\rangle$	C_6
		$abab^3abab^4$	$\langle a,b : a^2 = b^6 = abab^3abab^4 = 1\rangle$	C_6
		$abab^2ab^2ab^4$	$\langle a,b : a^2 = b^6 = abab^2ab^2ab^4 = 1\rangle$	$S_3 \times C_3$
		$abab^2ab^4ab^2$	$\langle a,b : a^2 = b^6 = abab^2ab^4ab^2 = 1\rangle$	$GAP4(48,33)$
		$abab^4ab^2ab^2$	$\langle a,b : a^2 = b^6 = abab^4ab^2ab^2 = 1\rangle$	$S_3 \times C_3$
		$abab^2ab^3ab^3$	$\langle a,b : a^2 = b^6 = abab^2ab^3ab^3 = 1\rangle$	C_6
		$abab^3ab^2ab^3$	$\langle a,b : a^2 = b^6 = abab^3ab^2ab^3 = 1\rangle$	$infinite\ group$
		$abab^3ab^3ab^2$	$\langle a,b : a^2 = b^6 = abab^3ab^3ab^2 = 1\rangle$	C_6
		$ab^2ab^2ab^2ab^3$	$\langle a,b : a^2 = b^6 = ab^2ab^2ab^2ab^3 = 1\rangle$	C_6
4	10	$ababab^3ab^5$	$\langle a,b : a^2 = b^6 = ababab^3ab^5 = 1\rangle$	D_4
		$ababab^5ab^3$	$\langle a,b : a^2 = b^6 = ababab^5ab^3 = 1\rangle$	D_4
		$abab^3abab^5$	$\langle a,b : a^2 = b^6 = abab^3abab^5 = 1\rangle$	$GAP4(24,8)$
		$ababab^4ab^4$	$\langle a,b : a^2 = b^6 = ababab^4ab^4 = 1\rangle$	$GAP4(96,190)$
		$abab^4abab^4$	$\langle a,b : a^2 = b^6 = abab^4abab^4 = 1\rangle$	$infinite\ group$
		$abab^2ab^3ab^4$	$\langle a,b : a^2 = b^6 = abab^2ab^3ab^4 = 1\rangle$	$infinite\ group$
		$abab^2ab^4ab^3$	$\langle a,b : a^2 = b^6 = abab^2ab^4ab^3 = 1\rangle$	D_6
		$abab^3ab^2ab^4$	$\langle a,b : a^2 = b^6 = abab^3ab^2ab^4 = 1\rangle$	D_2
		$abab^3ab^4ab^2$	$\langle a,b : a^2 = b^6 = abab^3ab^4ab^2 = 1\rangle$	D_6
		$abab^4ab^2ab^3$	$\langle a,b : a^2 = b^6 = abab^4ab^2ab^3 = 1\rangle$	D_2
		$abab^4ab^3ab^2$	$\langle a,b : a^2 = b^6 = abab^4ab^3ab^2 = 1\rangle$	$infinite\ group$
		$ab^2ab^2ab^2ab^4$	$\langle a,b : a^2 = b^6 = ab^2ab^2ab^2ab^4 = 1\rangle$	$infinite\ group$
		$abab^3ab^3ab^3$	$\langle a,b : a^2 = b^6 = abab^3ab^3ab^3 = 1\rangle$	D_4
		$ab^2ab^2ab^3ab^3$	$\langle a,b : a^2 = b^6 = ab^2ab^2ab^3ab^3 = 1\rangle$	D_6
		$ab^2ab^3ab^2ab^3$	$\langle a,b : a^2 = b^6 = ab^2ab^3ab^2ab^3 = 1\rangle$	$infinite\ group$
4	11	$ababab^4ab^5$	$\langle a,b : a^2 = b^6 = ababab^4ab^5 = 1\rangle$	C_2
		$ababab^5ab^4$	$\langle a,b : a^2 = b^6 = ababab^5ab^4 = 1\rangle$	C_2
		$abab^4abab^5$	$\langle a,b : a^2 = b^6 = abab^4abab^5 = 1\rangle$	C_2
		$abab^2ab^3ab^5$	$\langle a,b : a^2 = b^6 = abab^2ab^3ab^5 = 1\rangle$	S_3
		$abab^2ab^5ab^3$	$\langle a,b : a^2 = b^6 = abab^2ab^5ab^3 = 1\rangle$	C_2
		$abab^3ab^2ab^5$	$\langle a,b : a^2 = b^6 = abab^3ab^2ab^5 = 1\rangle$	C_2
		$abab^3ab^5ab^2$	$\langle a,b : a^2 = b^6 = abab^3ab^5ab^2 = 1\rangle$	C_2

k	l	words	quotient group	structure
		$abab^5ab^2ab^3$	$\langle a,b : a^2=b^6=abab^5ab^2ab^3=1\rangle$	C_2
		$abab^5ab^3ab^2$	$\langle a,b : a^2=b^6=abab^5ab^3ab^2=1\rangle$	S_3
		$ab^2ab^2ab^2ab^5$	$\langle a,b : a^2=b^6=ab^2ab^2ab^2ab^5=1\rangle$	$GL(2,3)$
		$abab^2ab^4ab^4$	$\langle a,b : a^2=b^6=abab^2ab^4ab^4=1\rangle$	C_2
		$abab^4ab^2ab^4$	$\langle a,b : a^2=b^6=abab^4ab^2ab^4=1\rangle$	C_2
		$abab^4ab^4ab^2$	$\langle a,b : a^2=b^6=abab^4ab^4ab^2=1\rangle$	C_2
		$abab^3ab^3ab^4$	$\langle a,b : a^2=b^6=abab^3ab^3ab^4=1\rangle$	S_3
		$abab^3ab^4ab^3$	$\langle a,b : a^2=b^6=abab^3ab^4ab^3=1\rangle$	C_2
		$abab^4ab^3ab^3$	$\langle a,b : a^2=b^6=abab^4ab^3ab^3=1\rangle$	S_3
		$ab^2ab^2ab^3ab^4$	$\langle a,b : a^2=b^6=ab^2ab^2ab^3ab^4=1\rangle$	C_2
		$ab^2ab^2ab^4ab^3$	$\langle a,b : a^2=b^6=ab^2ab^2ab^4ab^3=1\rangle$	C_2
		$ab^2ab^3ab^2ab^4$	$\langle a,b : a^2=b^6=ab^2ab^3ab^2ab^4=1\rangle$	S_3
		$ab^2ab^3ab^3ab^3$	$\langle a,b : a^2=b^6=ab^2ab^3ab^3ab^3=1\rangle$	C_2
4	12	$ababab^5ab^5$	$\langle a,b : a^2=b^6=ababab^5ab^5=1\rangle$	$GAP4(72,20)$
		$abab^5abab^5$	$\langle a,b : a^2=b^6=abab^5abab^5=1\rangle$	$infinite\ group$
		$abab^2ab^4ab^5$	$\langle a,b : a^2=b^6=abab^2ab^4ab^5=1\rangle$	$infinite\ group$
		$abab^2ab^5ab^4$	$\langle a,b : a^2=b^6=abab^2ab^5ab^4=1\rangle$	$infinite\ group$
		$abab^4ab^2ab^5$	$\langle a,b : a^2=b^6=abab^4ab^2ab^5=1\rangle$	$GAP4(252,26)$
		$abab^4ab^5ab^2$	$\langle a,b : a^2=b^6=abab^4ab^5ab^2=1\rangle$	$infinite\ group$
		$abab^5ab^2ab^4$	$\langle a,b : a^2=b^6=abab^5ab^2ab^4=1\rangle$	$GAP4(252,26)$
		$abab^5ab^4ab^2$	$\langle a,b : a^2=b^6=abab^5ab^4ab^2=1\rangle$	$infinite\ group$
		$ab^2ab^2ab^3ab^5$	$\langle a,b : a^2=b^6=ab^2ab^2ab^3ab^5=1\rangle$	$(C_7 \sim C_6)\times C_2$
		$ab^2ab^2ab^5ab^3$	$\langle a,b : a^2=b^6=ab^2ab^2ab^5ab^3=1\rangle$	$(C_7 \sim C_6)\times C_2$
		$ab^2ab^3ab^2ab^5$	$\langle a,b : a^2=b^6=ab^2ab^3ab^2ab^5=1\rangle$	$infinite\ group$
4	13	$abab^2ab^5ab^5$	$\langle a,b : a^2=b^6=abab^2ab^5ab^5=1\rangle$	C_2
		$ab^2abab^5ab^5$	$\langle a,b : a^2=b^6=ab^2abab^5ab^5=1\rangle$	C_2
		$abab^5ab^2ab^5$	$\langle a,b : a^2=b^6=abab^5ab^2ab^5=1\rangle$	C_2
		$ab^2ab^2ab^4ab^5$	$\langle a,b : a^2=b^6=ab^2ab^2ab^4ab^5=1\rangle$	C_2
		$ab^2ab^2ab^5ab^4$	$\langle a,b : a^2=b^6=ab^2ab^2ab^5ab^4=1\rangle$	C_2
		$ab^2ab^4ab^2ab^5$	$\langle a,b : a^2=b^6=ab^2ab^4ab^2ab^5=1\rangle$	C_2
		$ab^3ab^3ab^2ab^5$	$\langle a,b : a^2=b^6=ab^3ab^3ab^2ab^5=1\rangle$	S_3
		$ab^3ab^3ab^5ab^3$	$\langle a,b : a^2=b^6=ab^3ab^3ab^5ab^2=1\rangle$	S_3
		$ab^3ab^2ab^3ab^5$	$\langle a,b : a^2=b^6=ab^3ab^2ab^3ab^5=1\rangle$	C_2

k	l	word	quotient group	structure
4	14	$abab^3ab^5ab^5$	$\langle a,b : a^2 = b^6 = abab^3ab^5ab^5 = 1\rangle$	D_4
		$ab^3abab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^3abab^5ab^5 = 1\rangle$	D_4
		$abab^5ab^3ab^5$	$\langle a,b : a^2 = b^6 = abab^5ab^3ab^5 = 1\rangle$	$GAP4(24,8)$
		$ab^2ab^2ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^2ab^5ab^5 = 1\rangle$	$GAP4(96,190)$
		$ab^2ab^5ab^2ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^5ab^2ab^5 = 1\rangle$	$infinite\ group$
		$ab^4ab^4abab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^4abab^5 = 1\rangle$	D_2
		$ab^4ab^4ab^5ab$	$\langle a,b : a^2 = b^6 = ab^4ab^4ab^5ab = 1\rangle$	D_2
		$ab^4abab^4ab^5$	$\langle a,b : a^2 = b^6 = ab^4abab^4ab^5 = 1\rangle$	$infinite\ group$
		$ab^2ab^3ab^4ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^3ab^4ab^5 = 1\rangle$	$infinite\ group$
		$ab^2ab^3ab^5ab^4$	$\langle a,b : a^2 = b^6 = ab^2ab^3ab^5ab^4 = 1\rangle$	D_6
		$ab^2ab^4ab^3ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^4ab^3ab^5 = 1\rangle$	D_2
		$ab^2ab^4ab^5ab^3$	$\langle a,b : a^2 = b^6 = ab^2ab^4ab^5ab^3 = 1\rangle$	D_6
		$ab^2ab^5ab^4ab^3$	$\langle a,b : a^2 = b^6 = ab^2ab^5ab^4ab^3 = 1\rangle$	$infinite\ group$
		$ab^2ab^5ab^3ab^4$	$\langle a,b : a^2 = b^6 = ab^2ab^5ab^3ab^4 = 1\rangle$	D_2
		$ab^3ab^3ab^4ab^4$	$\langle a,b : a^2 = b^6 = ab^3ab^3ab^4ab^4 = 1\rangle$	D_6
		$ab^3ab^4ab^3ab^4$	$\langle a,b : a^2 = b^6 = ab^3ab^4ab^3ab^4 = 1\rangle$	$infinite\ group$
4	15	$ab^3ab^2ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^3ab^2ab^5ab^5 = 1\rangle$	C_6
		$ab^2ab^3ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^3ab^5ab^5 = 1\rangle$	C_6
		$ab^2ab^5ab^3ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^5ab^3ab^5 = 1\rangle$	C_6
		$ab^3ab^3ab^4ab^5$	$\langle a,b : a^2 = b^6 = ab^3ab^3ab^4ab^5 = 1\rangle$	C_6
		$ab^3ab^3ab^5ab^4$	$\langle a,b : a^2 = b^6 = ab^3ab^3ab^5ab^4 = 1\rangle$	C_6
		$ab^3ab^4ab^3ab^5$	$\langle a,b : a^2 = b^6 = ab^3ab^4ab^3ab^5 = 1\rangle$	$infinite\ group$
4	16	$abab^5ab^5ab^5$	$\langle a,b : a^2 = b^6 = abab^5ab^5ab^5 = 1\rangle$	D_4
		$ab^2ab^4ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^4ab^5ab^5 = 1\rangle$	D_2
		$ab^4ab^2ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^2ab^5ab^5 = 1\rangle$	D_2
		$ab^2ab^5ab^4ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^5ab^4ab^5 = 1\rangle$	$infinite\ group$
		$ab^3ab^3ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^3ab^3ab^5ab^5 = 1\rangle$	$GAP4(24,8)$
		$ab^3ab^5ab^3ab^5$	$\langle a,b : a^2 = b^6 = ab^3ab^5ab^3ab^5 = 1\rangle$	$infinite\ group$
		$ab^4ab^4ab^3ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^4ab^3ab^5 = 1\rangle$	D_2
		$ab^4ab^4ab^5ab^3$	$\langle a,b : a^2 = b^6 = ab^4ab^4ab^5ab^3 = 1\rangle$	D_2
		$ab^4ab^3ab^4ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^3ab^4ab^5 = 1\rangle$	$infinite\ group$
		$ab^4ab^4ab^4ab^4$	$\langle a,b : a^2 = b^6 = ab^4ab^4ab^4ab^4 = 1\rangle$	$infinite\ group$

k	l	word	quotient group	structure
4	17	$ab^2ab^5ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^2ab^5ab^5ab^5 = 1\rangle$	$GL(2,3)$
		$ab^3ab^4ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^3ab^4ab^5ab^5 = 1\rangle$	C_2
		$ab^4ab^3ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^3ab^5ab^5 = 1\rangle$	C_2
		$ab^4ab^5ab^3ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^5ab^3ab^5 = 1\rangle$	S_3
		$ab^4ab^4ab^4ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^4ab^4ab^5 = 1\rangle$	C_2
4	18	$ab^3ab^5ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^3ab^5ab^5ab^5 = 1\rangle$	$D_4 \times C_3$
		$ab^4ab^4ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^4ab^5ab^5 = 1\rangle$	$C_6 \times S_3$
		$ab^4ab^5ab^4ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^5ab^4ab^5 = 1\rangle$	$infinite\ group$
4	19	$ab^4ab^5ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^4ab^5ab^5ab^5 = 1\rangle$	C_2
4	20	$ab^5ab^5ab^5ab^5$	$\langle a,b : a^2 = b^6 = ab^5ab^5ab^5ab^5 = 1\rangle$	$\Delta(2,6,4)$

References

[1] **M. Aslam, Q. Mushtaq, T. Maqsood and M. Ashiq,** *Real quadratic irrational numbers and the group* $\langle x,y : x^2 = y^6 = 1\rangle$, Southeast Asian Bull. Math. **27** (2003), 409 – 415.

[2] **İ. N. Cangül and D. Singerman,** *Normal subgroups of Hecke groups and regular maps,* Math. Proc. Camb. Phil. Soc. **123** (1998), 59 – 74.

[3] **M. D. E. Conder,** *Three relator quotients of the modular group,* Quart. J. Math. Oxford **38** (1987), 427 – 447.

[4] **M. Demirci and İ. N. Cangül,** *A class of congruence subgroups of Hecke group* $H(\lambda_5)$*,* Bull. Inst. Math. Acad. Sinicia **1** (2004), 549 – 556.

[5] **G. Havas, M.D.E Conder and M. Newman,** *One relator quotients of the modular group,* Group St Andrews, Bath. **11** August 2009.

[6] **Q. Mushtaq,** *On the word structure of the modular group over finite and real quadratic fields,* Discrete Math. **178** (1998), 155 – 164.

[7] **Q. Mushtaq and M. Aslam,** *Group generated by two elements of order two and six acting on* R *and* $Q(\sqrt{n})$, Discrete Math. **179** (1998), 145 – 154.

[8] **L. A. Parson,** *Normal congruence subgroups of the Hecke groups* $G(2^{(1/2)})$ *and* $G(3^{(1/2)})$, Pacific. J. Math. **70** (1977), 481 – 487.

[9] **Y. T. Ulutas and I. N. Cangül,** *One relator quotients of the Hecke group* $H(\frac{1+\sqrt{5}}{2})$, Bull. Inst. Math. Acad. Sinicia **31** (2003), 59 – 74.

[10] **Y. T. Ulutas and I. N. Cangül,** *One relator quotients of the modular group*, Bull. Inst. Math. Acad. Sinicia **32** (2004), 291 – 296.

[11] **N. Yilmaz and İ. N. Cangül,** *Power subgroups of Hecke groups* $H(\sqrt{n})$, International J. Math. and Math. Sci. **11** (2001), 703 – 708.

Received August 17, 2010

Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan

E-mails: draslamqau@yahoo.com (M.Aslam), aalisandhu@gmail.com (A.Ali), rihan_ahmad3@hotmail.com (R.Ahmad)

Quasigroups and Related Systems **19** (2011), 183 – 192

Parametrization of actions of $\langle \mathbf{u}, \mathbf{v} : \mathbf{u^6} = \mathbf{v^6} = \mathbf{1} \rangle$

Muhammad Aslam and Qaiser Mushtaq

Abstract. Graham Higman proposed the problem of parametrization of actions of the extended modular group $PGL(2, Z)$ on the projective line over F_q. The problem was solved by Q. Mushtaq. In this paper, we take up the problem and parametrize the actions of $\langle u, v, t : u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1 \rangle$ on the projective line over finite Galois fields.

1. Introduction

Graham Higman proposed the problem of parametrization of actions of the extended modular group $PGL(2, Z)$ on the projective line over F_q. The problem was solved by Q. Mushtaq. In this paper, we take up the problem and parametrize the actions of $\langle u, v, t : u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1 \rangle$ on the projective line over finite Galois fields.

It is worthwhile to consider linear fractional transformations x, y satisfying the relations $x^2 = y^m = 1$, with a view to study actions of the group $\langle x, y \rangle$ on real quadratic fields. If $y : z \to \frac{az+b}{cz+d}$ is to act on all real quadratic fields, then a, b, c, d must be rational numbers and can be taken to be integers, so that $\frac{(a+d)^2}{ad-bc}$ is rational. But if $y : z \to \frac{az+b}{cz+d}$ is of order m one must have $\frac{(a+d)^2}{ad-bc} = \omega^2 + \omega^{-2} + 2$, where ω is a primitive mth root of unity. Now $\omega + \omega^{-1}$ is rational, for a primitive mth root ω, only if $m = 1, 2, 3, 4,$ or 6. So these are the only possible orders of y. The group $\langle x, y \rangle$ is cyclic of order two when $m = 1$. When $m = 2$, it is an infinite dihedral group and does not give inspiring information while studying its action on the quadratic numbers. For $m = 3$, the group $\langle x, y \rangle$ is the modular group $PSL(2, Z)$ and its action on real quadratic numbers has been discussed in detail in [2] and [3].

It is well known [1, 5] that the group $G_{2,6}(2, Z)$, where Z is the ring of

2010 Mathematics Subject Classification: 20G40, 20B35
Keywords: Linear-fractional transformation, non-degenerate homomorphism, conjugacy classe, parametrization and projective line.

integers, is generated by the linear-fractional transformations $x : z \longrightarrow \frac{-1}{3z}$ and $y : z \longrightarrow \frac{-1}{3(z+1)}$ which satisfy the relations

$$x^2 = y^6 = 1. \tag{1}$$

Let $v = xyx$, and $u = y$. Then $(z)v = \frac{3z-1}{3z}$ and

$$u^6 = v^6 = 1 \tag{2}$$

So the group $G_{6,6}(2, Z) = \langle u, v \rangle$ is a proper subgroup of the group $G_{2,6}(2, Z)$.

The linear-fractional transformation $t : z \to \frac{1}{3z}$ inverts u and v, that is, $t^2 = (ut)^2 = (vt)^2 = 1$ and so extends the group $G_{6,6}(2, Z)$ to

$$G^*_{6,6}(2, Z) = \langle u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1 \rangle. \tag{3}$$

As u and v have the same orders, there exists an automorphism which interchanges u and v yielding the split extension $G^*_{6,6}(2, Z)$.

Let $PL(F_q)$ denote the projective line over the Galois field F_q , where q is a prime, that is, $PL(F_q) = F_q \cup \{\infty\}$. The group $G^*_{6,6}(2, q)$ is then the group of linear-fractional transformations of the form $z \to \frac{az+b}{cz+d}$, where $a, b, c, d \in F_q$ and $ad - bc \neq 0$, while $G_{6,6}(2, q)$ is its subgroup consisting of all those linear-fractional transformations of the form $z \to \frac{az+b}{cz+d}$, where $a, b, c, d \in F_q$ and $ad - bc$ is a non-zero square in F_q.

Graham Higman proposed the problem of parametrization of actions of $PGL(2, Z)$ on $PL(F_q)$. The problem was solved by Q. Mushtaq in [4]. In this paper, we take up the problem and parametrize the actions of $G^*_{6,6}(2, Z)$ on $PL(F_q)$, except for a few uninteresting ones, by the elements of F_q. We have shown that any non-degenerate homomorphism α from $G_{6,6}(2, Z)$ into $G_{6,6}(2, q)$ can be extended to a non-degenerate homomorphism α from $G^*_{6,6}(2, Z)$ into $G^*_{6,6}(2, q)$. It has been shown also that every element in $G^*_{6,6}(2, q)$, not of order $1, 2$, or 6, is the image of uv under α. It is also proved that the conjugacy classes of $\alpha : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ are in one-to-one correspondence with the conjugacy classes of non-trivial elements of $G^*_{6,6}(2, q)$, under a correspondence which assigns to the homomorphism α the class containing $(uv)\alpha$. Of course, this will mean that we can actually parametrize the actions of $G^*_{6,6}(2, q)$ on $PL(F_q)$, except for a few uninteresting ones, by the elements of F_q.

2. Conjugacy classes

The transformations $u : z \to \frac{-1}{3(z+1)}$, $v : z \to \frac{3z-1}{3z}$ and $t : z \to \frac{1}{3z}$ generate $G^*_{6,6}(2, Z)$, subject to defining relations $u^6 = v^6 = t^2 = (ut)^2 = (vt)^2 = 1$. Thus to choose a homomorphism $\alpha : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ amounts to choosing $\overline{u} = u\alpha, \overline{v} = v\alpha$ and $\overline{t} = t\alpha$, in $G^*_{6,6}(2, q)$ such that

$$\overline{u}^6 = \overline{v}^6 = \overline{t}^2 = (\overline{u}\overline{t})^2 = (\overline{v}\overline{t})^2 = 1. \tag{4}$$

We call α to be a *non-degenerate homomorphism* if neither of the generators u, v of $G^*_{6,6}(2, Z)$ lies in the kernel of α. Two homomorphisms α and β from $G^*_{6,6}(2, Z)$ to $G^*_{6,6}(2, q)$ are called *conjugate* if there exists an inner automorphism ρ of $G^*_{6,6}(2, q)$ such that $\beta = \rho\alpha$. Let δ be the automorphism on $G^*_{6,6}(2, Z)$ defined by $u\delta = tut, v\delta = v$, and $t\delta = t$. Then the homomorphism $\alpha' = \delta\alpha$ is called the *dual homomorphism* of α. This, of course, means that if α maps u, v, t to $\overline{u}$,$\overline{v}$,$\overline{t}$, then α' maps u, v, t to $\overline{t}\overline{u}\overline{t}$, $\overline{v}$, $\overline{t}$ respectively. Since the elements $\overline{u}$,$\overline{v}$,$\overline{t}$ as well as $\overline{t}\overline{u}\overline{t}$, $\overline{v}$, $\overline{t}$ satisfy the relations (4), therefore the solutions of these relations occur in dual pairs. Of course, if α is conjugate to β then α' is conjugate to β'.

2.1. Parametrization

If the natural mapping $GL(2, q) \to G^*_{6,6}(2, q)$ maps a matrix M to the element of g of $G^*_{6,6}(2, q)$, then $\theta = (tr(M))^2 / \det(M)$ is an invariant of the conjugacy class of g. We refer to it as the parameter of g or of the conjugacy class. Of course, every element in F_q is the parameter of some conjugacy class in $G^*_{6,6}(2, q)$. For instance, the class represented by a matrix with characteristic polynomial $z^2 - \theta z + \theta$ if $\theta \neq 0$ or $z^2 - 1$ if $\theta = 0$.

If q is odd, there are two classes with parameter 0. Of course a matrix M in $GL(2, q)$ represents an involution in $G^*_{6,6}(2, q)$ if and only if its trace is zero. This means that the two classes with parameter 0 contain involutions. One of the classes is contained in $G_{6,6}(2, q)$ and the other not. In any case, there are two classes with parameter 4; the class containing the identity element and the class containing the element $z \to z + 1$. Thus apart from these two exceptions, the correspondence between classes and parameters is one-to-one.

If q is odd and g is not an involution, then g belongs to $G_{6,6}(2, q)$ if and only if θ is a square in F_q. On the other hand $g : z \to \frac{az+b}{cz+d}$, where $a, b, c, d \in F_q$, has a fixed point k in the natural representation of $G^*_{6,6}(2, q)$

on $PL(F_q)$ if and only if the discriminant, $a^2+d^2-2ad+4bc$, of the quadratic equation $k^2c + k(d-a) - b = 0$ is a square in F_q. Since the determinant $ad - bc$ is 1 and the trace $a + d$ is r, the discriminant is $(\theta - 4)$. Thus, g has fixed point in the natural representation of $G^*_{6,6}(2, q)$ on $PL(F_q)$ if and only if $(\theta - 4)$ is a square in F_q.

If U and V are two non-singular 2×2 matrices corresponding to the generators $\overline{u}$ and $\overline{v}$ of $G^*_{6,6}(2, q)$ with $\det(UV) = 1$ and trace r, then for a positive integer k

$$\begin{aligned}(UV)^k &= \{\binom{k-1}{0}r^{k-1} - \binom{k-2}{1}r^{k-3} + \ldots\}UV \\ &\quad -\{\binom{k-2}{0}r^{k-2} - \binom{k-3}{1}r^{k-4} + \ldots\}I. \end{aligned} \tag{5}$$

Furthermore, suppose

$$f(r) = \binom{k-1}{0}r^{k-1} - \binom{k-2}{1}r^{k-3} + \ldots \tag{6}$$

The replacement of θ for r^2 in $f(r)$ yields a polynomial $f(\theta) = f_k(\theta)$ in θ. Thus, one can find a minimal polynomial $g_k(\theta)$, which is equal to $f_k(\theta)$ if k is a prime number, otherwise for any positive integer k such that $q \equiv \pm 1(\mathrm{mod\,k})$ by the equation:

$$g_k(\theta) = \frac{f_k(\theta)}{g_{d_1}(\theta)g_{d_2}(\theta)\ldots g_{d_n}(\theta)} \tag{7}$$

where $d_1, d_2, \ldots, d_n$, are the divisors of k such that $1 < d_i < k$, $i = 1, 2, \ldots, n$ and $f_k(\theta)$ is obtained by the equation (3.2).

The degree of the minimal polynomial is obtained as:

$$\deg[g_k(\theta)] = \deg[f_k(\theta)] - \sum \deg[g_{d_i}(\theta)]\,, \tag{8}$$

where $\deg[f_k(\theta)] = \left\{ \begin{array}{ll} \frac{k-1}{2} & \text{if } k \text{ is odd,} \\ \frac{k}{2} & \text{if } k \text{ is even} \end{array} \right\}$. Also, $\deg[g_{p^n}(\theta)] = \frac{p^n}{2} - \frac{p^{n-1}}{2}$, where p is a prime.

Thus:

k	**Minimal equation satisfied by θ**
1	$\theta - 4 = 0$
2	$\theta = 0$

3	$\theta - 1 = 0$
4	$\theta - 2 = 0$
5	$\theta^2 - 3\theta + 1 = 0$
6	$\theta - 3 = 0$
7	$\theta^3 - 5\theta^2 + 6\theta - 1 = 0$
8	$\theta^2 - 4\theta + 2 = 0$
9	$\theta^3 - 6\theta^2 + 9\theta - 1 = 0$
10	$\theta^2 - 5\theta + 5 = 0$
11	$\theta^5 - 9\theta^4 + 28\theta^3 - 35\theta^2 + 15\theta - 1 = 0$
12	$\theta^2 - 4\theta + 1 = 0$
13	$\theta^6 - 11\theta^5 + 45\theta^4 - 84\theta^3 + 70\theta^2 - 21\theta + 1 = 0$
14	$\theta^6 - 120\theta^5 + 55\theta^4 - 120\theta^3 + 126\theta^2 - 56\theta + 7 = 0$
15	$\theta^7 - 13\theta^6 + 66\theta^5 - 165\theta^4 + 210\theta^3 - 126\theta^2 + 28\theta - 1 = 0$
16	$\theta^6 - 12\theta^5 + 54\theta^4 - 112\theta^3 + 106\theta^2 - 40\theta + 4 = 0$
17	$\theta^8 - 15\theta^7 + 91\theta^6 - 286\theta^5 + 495\theta^4 - 462\theta^3 + 210\theta^2 - 36\theta + 1 = 0$
18	$\theta^6 - 12\theta^5 + 54\theta^4 - 112\theta^3 + 105\theta^2 - 36\theta + 3 = 0$
19	$\theta^9 - 17\theta^8 + 120\theta^7 - 455\theta^6 + 1001\theta^5 - 1287\theta^4 + 924\theta^3 - 330\theta^2 + 45\theta - 1 = 0$
20	$\theta^8 - 16\theta^7 + 104\theta^6 - 352\theta^5 + 661\theta^4 - 680\theta^3 + 356\theta^2 - 80\theta + 5 = 0,$

and so on.

Let $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of $GL(2,q)$ corresponding to $\overline{u}$. Then, since $\overline{u}^6 = 1$, U^6 is a scalar matrix, and hence $\det(U)$ is a square in F_q, where $q = \pm 1 (\mathrm{mod}\, 12)$. Thus, replacing U by a suitable scalar multiple, we assume that $\det(U) = 1$.

Since, for any matrix M, such that M^2 and M^3 are not scalar matrices, $M^6 = \lambda I$ if and only if $(tr(M))^2 = 3\det(M)$, we may assume that $tr(U) = a + d = \sqrt{3}$ and $\det(U) = 1$. Thus $U = \begin{bmatrix} a & b \\ c & -a + \sqrt{3} \end{bmatrix}$. Similarly, $V = \begin{bmatrix} e & f \\ g & -e + \sqrt{3} \end{bmatrix}$. Since $\overline{u}^6 = 1$ also implies that the $tr(\overline{u}) = \sqrt{3}$, every element of $GL(2,q)$ of trace equal to $\sqrt{3}$ has upto scalar multiplication, a conjugate of the form $\begin{bmatrix} 0 & -1 \\ 1 & \sqrt{3} \end{bmatrix}$. Therefore U will be of the form $\begin{bmatrix} 0 & -1 \\ 1 & \sqrt{3} \end{bmatrix}$.

Now let $\bar{t}$ be represented by $T = \begin{bmatrix} l & m \\ n & j \end{bmatrix}$. Since $\bar{t}^2 = 1$, the trace of T is zero. So, upto scalar multiplication, the matrix representing $\bar{t}$ will be

of the form $\begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$. Because $(\overline{u}\overline{t})^2 = (\overline{v}\overline{t})^2 = 1$, the $tr(\overline{u}\overline{t}) = tr(\overline{v}\overline{t}) = 0$ and so $b = kc$ and $f = gk$.

Thus the matrices corresponding to generators $\overline{u}$, $\overline{v}$ and $\overline{t}$ of $G^*_{6,6}(2,q)$ will be:

$U = \begin{bmatrix} a & kc \\ c & -a+\sqrt{3} \end{bmatrix}$, $V = \begin{bmatrix} e & gk \\ g & -e+\sqrt{3} \end{bmatrix}$, and $T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$ respectively, where $a, c, e, g, k \in F_q$. Then,

$$1 + a^2 + kc^2 - \sqrt{3}a = 0 \tag{9}$$

and

$$1 + e^2 + kg^2 - \sqrt{3}e = 0, \tag{10}$$

because the determinants of U and V are 1.

This certainly evolves elements satisfying the relations $U^6 = \lambda_1 I, V^6 = \lambda_2 I$, where λ_1 and λ_2 are non-zero scalars and I is the identity matrix. The non-degenerate homomorphism α is determined by $\overline{u}, \overline{v}$ because one-to-one correspondence assigns to α the class containing $\overline{u}\ \overline{v}$. So it is sufficient to check on the conjugacy class of $\overline{u}\ \overline{v}$. The matrix UV has the trace

$$r = 2(ae + kcg) + 3 - \sqrt{3}(a + e). \tag{11}$$

If $tr(UVT) = ks$, then

$$s = 2ag - c(2e - \sqrt{3}) - \sqrt{3}g. \tag{12}$$

So the relationship between (3.7) and (3.8) is

$$r^2 + ks^2 = 3r - 2. \tag{13}$$

We set

$$\theta = r^2. \tag{14}$$

Lemma 1. *Either $\overline{uv}$ is of order 3 or there exists an involution $\overline{t}$ in $G^*_{6,6}(2,q)$ such that $\overline{t}^2 = (\overline{u}\overline{t})^2 = (\overline{v}\overline{t})^2 = 1$.*

Proof. Let U be an element of $GL(2,q)$ which yields the element $\overline{u}$ of $G^*_{6,6}(2,q)$. Since $(\overline{u})^6 = 1$, therefore we can assume that U has the form $\begin{bmatrix} 0 & -1 \\ 1 & -\sqrt{3} \end{bmatrix}$.

Let $V = \begin{bmatrix} a & b \\ c & -a-\sqrt{3} \end{bmatrix}$ and $T = \begin{bmatrix} l & m \\ n & -l \end{bmatrix}$ where $1+a^2+bc-\sqrt{3}a = 0$.

Now suppose that there exists a transformation $\bar{t}$ in $G^*_{6,6}(2, Z)$ such that $\bar{t}^2 = (\overline{u}\bar{t})^2 = (\overline{v}\bar{t})^2 = 1$. Let r be the trace of UV. Then $r = 3+b-c-\sqrt{3}a$. Now

$$UT = \begin{bmatrix} 0 & -1 \\ 1 & -\sqrt{3} \end{bmatrix} \begin{bmatrix} l & m \\ n & -l \end{bmatrix} = \begin{bmatrix} -n & l \\ l-\sqrt{3}n & m-\sqrt{3}l \end{bmatrix}$$

give us $-n+m-\sqrt{3}l = 0$ or $m = n+\sqrt{3}l$.

Also

$$VT = \begin{bmatrix} a & b \\ c & -a+\sqrt{3} \end{bmatrix} \begin{bmatrix} l & m \\ n & -l \end{bmatrix} = \begin{bmatrix} al+bn & am-bl \\ cl-an+\sqrt{3}n & cm+al-\sqrt{3}l \end{bmatrix}$$

yields $2al+bn+cm-\sqrt{3}l = 0$ or $2al+bn+c(n+\sqrt{3}l)-\sqrt{3}l = 0$ or $2al+bn+cn+\sqrt{3}cl-\sqrt{3}l = 0$. Hence

$$(2a+\sqrt{3}c-\sqrt{3})l+(b+c)n = 0. \tag{15}$$

Now for T to be a non-singular matrix, we have $det(T) \neq 0$, that is, $-l^2-mn \neq 0$ or $l^2+mn \neq 0$ or $l^2+n(n+\sqrt{3}l) \neq 0$ or $l^2+n^2+\sqrt{3}nl \neq 0$ or

$$\left(\frac{l}{n}\right)^2+1+\sqrt{3}\left(\frac{l}{n}\right) \neq 0. \tag{16}$$

Thus the necessary and sufficient conditions for the existence of $\bar{t}$ in $G^*_{6,6}(2, q)$ are the equations (15) and (16). Hence $\bar{t}$ exists in $G^*_{6,6}(2, q)$ unless

$$\left(\frac{l}{n}\right)^2+1+\sqrt{3}\left(\frac{l}{n}\right) = 0.$$

Of course, if both $2a+\sqrt{3}c-\sqrt{3}$ and $b+c$ are equal to zero, then the existence of $\bar{t}$ is trivial. If not, then $\frac{l}{n} = \frac{-(b+c)}{2a+\sqrt{3}c-\sqrt{3}}$, and so equation (16) is equivalent to $(b+c)^2+(2a+\sqrt{3}c-\sqrt{3})^2+(2a+\sqrt{3}c-\sqrt{3})(b+c) \neq 0$. Thus there exists $\bar{t}$ in $G^*_{6,6}(2, q)$ such that $\bar{t}^2 = (\overline{u}\bar{t})^2 = (\overline{v}\bar{t})^2 = 1$ unless

$$(b+c)^2+(2a+\sqrt{3}c-\sqrt{3})^2 = \sqrt{3}(2a+\sqrt{3}c-\sqrt{3})(b+c).$$

This yields $(b-c)^2+4bc+4a^2+3c^2+3+4\sqrt{3}ac-4\sqrt{3}a-6c = \sqrt{3}(2ab+\sqrt{3}bc-\sqrt{3}b+2ac+\sqrt{3}c^2-\sqrt{3}c)$.

After simplification we get $r^2 - 3r + 2 = 0$. So, $r^2 = 3r - 2$ and after squaring both sides, we get $\theta^2 - 5\theta + 4 = 0$. This implies that $\theta = 1$ or $\theta = 4$.

By the preceding table, $\theta = 1$ implies that the order of $\overline{uv}$ is 3 and $\theta = 4$ gives the order of $\overline{uv}$ is 1, so neglecting it because $(\overline{u}\,\overline{v}) \neq 1$, the parameter of $\overline{uv}$ is 1 and the order of $\overline{uv}$ is 3. □

Lemma 2. *One and only one of the following holds:*

(*i*) *The pair* $(\overline{u}, \overline{v})$ *is invertible.*

(*ii*) $\overline{u}\,\overline{v}$ *has order* 3 *and* $\overline{u}\,\overline{v} \neq \overline{v}\,\overline{u}$. □

In what follows we shall find a relationship between the parameters of the dual homomorphisms. We first prove the following.

Lemma 3. *Any non trivial element* $\overline{g}$ *of* $G^*_{6,6}(2, q)$ *whose order is not equal to* 2 *or* 6 *is the image of* uv *under some non-degenerate homomorphism* α *of* $G^*_{6,6}(2, , Z)$ *into* $G^*_{6,6}(2, q)$.

Proof. Using Lemma 1, we show that every non-trivial element of $G^*_{6,6}(2, q)$ is a product of two elements of orders 3. So we find elements $\overline{u}, \overline{v}$ and, $\overline{t}$ of $G^*_{6,6}(2, q)$ satisfying the relations (4) with $\overline{u}\,\overline{v}$ in a given conjugacy class.

The class to which we want $\overline{u}\ \overline{v}$ to belong do not consist of involutions because $\overline{g} = \overline{u}\,\overline{v}$ is not of order 2. Thus the traces of the matrices UV and UVT are not equal to zero. Hence $r \neq 0$, and $s \neq 0$, so that we have $\theta = r^2 \neq 0$; and it is sufficient to show that we can choose a, c, e, g, k, in F_q so that r^2 is indeed equal to θ. The solution of θ is therefore arbitrarily in F_q. We can choose r to satisfy $\theta = r^2$, equation (13), yields $ks^2 = 3r - 2 - r^2$. If $r^2 \neq 3r - 2$, we select k as above.

Any quadratic polynomial $\lambda z^2 + \mu z + \nu$, with coefficients in F_q takes at least $(q + 1)/2$ distinct values, as z runs through F_q; since the equation $\lambda z^2 + \mu z + \nu = k$ has at most two roots for fixed k; and there are q elements in F_q, where q is odd. In particular, $a^2 - \sqrt{3}a$ and $-kc^2 - 1$ each taking at least $(q+1)/2$ distinct values as a and c run through F_q. Similarly, $e^2 - \sqrt{3}e$ and $-kg^2 - 1$ each takes at least $(q + 1)/2$ distinct values as e and g run through F_q. Hence we can find a and c so that $a^2 - \sqrt{3}a = -kc^2 - 1$ and e, g so that $e^2 - \sqrt{3}e = -kg^2 - 1$.

Finally, by substituting the values of r, s, a, c, e, g, k in equations (11) and (12) we obtain the values of e and g. These equations are linear equations for e and g with determinant $(2a - \sqrt{3})^2 + 4kc^2 = 4a^2 + 3 - 4\sqrt{3}4kc^2$ $= 4(a^2 + kc^2 - \sqrt{3}a) + 3 = -4 + 3 = -1$. It is non-zero, so that we can

find e and g satisfying equation (10). It is obvious from (13) and (14) that $\theta = 0$ when $r = 0$ and $\theta = 1$ or 4 when $s = 0$. By the preceding table, the possibility that $\theta = 0$ gives rise to the situation where $\overline{u}.\overline{v}$ is of order 2. Similarly, the possibility $\theta = 1$ leads to the situation where $\overline{u}\,\overline{v}$ is of order 3 and $\theta = 4$ yields $\overline{u}\,\overline{v}$ of order 1. □

Theorem 1. *The conjugacy classes of non-degenerate homomorphisms of $G^*_{6,6}(2, Z)$ into $G^*_{6,6}(2, q)$ are in one-to-one correspondence with the non-trivial conjugacy classes of elements of $G^*_{6,6}(2, q)$ under a correspondence which assigns to any non-degenerate homomorphism σ the class containing $(uv)\sigma$.*

Proof. Let $\sigma : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ be a non-degenerate homomorphism such that it maps u, v to $\overline{u}$,$\overline{v}$. Let θ be the parameter of the class represented by $\overline{u}\,\overline{v}$. Now α is determined by $\overline{u}$,$\overline{v}$ and each θ evolves a pair $\overline{u}$,$\overline{v}$, so that σ is associated with θ. We shall call the parameter θ of the class containing $\overline{u}\,\overline{v}$, the parameter of the non-degenerate homomorphism of $G^*_{6,6}(2, Z)$ into $G^*_{6,6}(2, q)$. Now $UT = \begin{bmatrix} ck & -ak \\ -a+\sqrt{3} & -ck \end{bmatrix}$ implies that $\det(UT) = -k(a^2 - \sqrt{3}a + kc^2) = k$ (equation 9). Also, $(UT)V = \begin{bmatrix} kec - akg & k^2gc + ak(e-\sqrt{3}) \\ -ae + e\sqrt{3} - kgc & -akg + kg\sqrt{3} + ck(e-\sqrt{3}) \end{bmatrix}$ implies that $Tr((UT)V) = 2kec - 2akg + \sqrt{3}kg - \sqrt{3}kc = -k(-2ce + 2ag - \sqrt{3}g + \sqrt{3}c) = -ks$. If $\overline{u}, \overline{v}, \overline{t}$ satisfy the relations (4), then so do $\overline{t}\overline{u}\overline{t}, \overline{v}, \overline{t}$. So that the solution of relations (4) occur in dual pairs. Hence replacing the solutions in Lemma 3 by $\overline{t}\overline{u}\overline{t}, \overline{v}, \overline{t}$, we have $\theta = \frac{[Tr((UT)V]^2}{\det(UT)} = \frac{k^2s^2}{k} = ks^2$. We then find a relationship between the parameters of the dual non-degenerate homomorphisms. □

There is an interesting relationship between the parameters of the dual non-degenerate homomorphisms.

Corollary 1. *If $\alpha : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ is a non-degenerate homomorphism, α' is its dual and θ, φ are their respective parameters then $\theta + \varphi = 3r - 2$.*

Proof. Let $\alpha : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ be a non-degenerate homomorphism satisfying the relations $u\alpha = \overline{u}$, $v\alpha = \overline{v}$ and $t\alpha = \overline{t}$. Let α' be the dual of α. As we choose the matrices $U = \begin{bmatrix} a & ck \\ c & -a+\sqrt{3} \end{bmatrix}$, $V = \begin{bmatrix} e & g\ k \\ g & -e+\sqrt{3} \end{bmatrix}$

and $T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$, representing $\overline{u}, \overline{v}$ and $\overline{t}$, respectively such that they satisfy the equations from (9) to (13). Now $(\overline{u}\,\overline{v})^2 = 1$, implies that $Tr(UV) = 0$. Also, we have $\{Tr(UVT)\}/k = s = 0$ if and only if $(\overline{u}\,\overline{v}\overline{t})^2 = 1$. Then $\det(UV) = 1$, thus giving the parameter of $\overline{u}\,\overline{v}$ equal to $r^2 = \theta$. Also since $Tr(UVT) = ks$ and $\det(UVT) = k$ (since $\det(U) = 1$, $\det(V) = 1$ and $\det(T) = k$), we obtain the parameter of $\overline{uv}\overline{t}$ equal to ks^2, which we denote by φ. Thus $\theta + \varphi = r^2 + ks^2$. Substituting the values from equation (13), we therefore obtain $\theta + \varphi = 3r - 2$. Hence if θ is the parameter of the non-degenerate homomorphism α, then $\varphi = 3r - 2 - \theta$ is the parameter of the dual α' of α. □

Theorem 1, of course, means that we can actually parametrize the non-degenerate homomorphisms of $G^*_{6,6}(2, Z)$ to $G^*_{6,6}(2, q)$ except for a few uninteresting ones, by the elements of F_q. Since $G^*_{6,6}(2, q)$ has a natural permutation representation on $PL(F_q)$, any homomorphism $\sigma : G^*_{6,6}(2, Z) \to G^*_{6,6}(2, q)$ gives rise to an action of $G^*_{6,6}(2, Z)$ on $PL(F_q)$.

References

[1] **M. Aslam and Q. Mushtaq**, *Closed paths in the coset diagrams for* $\langle y, t : y^6 = t^6 = 1\rangle$ *acting on real quadratic fields*, Ars Comb. **71** (2004), 267 – 288.

[2] **Q. Mushtaq**, *Coset diagrams for the modular group*, Ph.D. thesis, University of Oxford, 1983.

[3] **Q. Mushtaq**, *Modular group acting on real quadratic fields*, Bull. Austral. Math. Soc. **37** (1988), 303 – 306.

[4] **Q. Mushtaq**, *Parametrization of all homomorphisms from* $PGL(2, Z)$ *into* $PGL(2, q)$, Comm. Algebra **20** (1992), 1023 – 1040.

[5] **Q. Mushtaq and M. Aslam**, *Group generated by two elements of orders two and six acting on* R *and* $Q(\sqrt{n})$, Disc. Math. **179** (1998), 145 – 154.

Received January 03, 2011

Department of Mathematics Quaid-i-Azam University, Islamabad, Pakistan
E-emails: draslamqau@yahoo.com (M.Aslam), qmushtaq@apollo.net.pk (Q.Mushtaq)

Quasigroups and Related Systems **19** (2011), 193 – 206

Classification of loops of generalized Bol-Moufang type

B. Coté, B. Harvill, M. Huhn and A. Kirchman

Abstract. A loop identity $\alpha = \beta$ is of *Bol-Moufang type* if the same 3 variables appear on both sides of the equal sign in the same order, one of the variables appears twice on both sides and the remaining two variables appear once on both sides. One can generalize this definition by allowing different variable orders on either side of the identity, e.g. $((xx)y)z = x(y(xz))$. There are 1215 nontrivial identities of this type. Loop varieties axiomatized by a single identity of this type are said to be of *generalized Bol-Moufang type*. We show that there are 48 such varieties: the 14 varieties of Bol-Moufang type [13], the 6 varieties of commutative Bol-Moufang type, and 28 new varieties.

1. Introduction

The aim of this paper is to find and classify all loops that are a generalization of loops of Bol-Moufang type [3], [4], [8], [13], and [17].

A *quasigroup* is a set Q with a binary operation $*$ such that the equation $a * b = c$ has a unique solution in Q whenever two of a, b, and c are fixed elements of Q.

A *loop* is a quasigroup with a two-sided neutral element, which we will denote as 1. Standard references for loop theory are [1] and [15].

An identity $\alpha = \beta$ is of $Bol - Moufang$ type if it satisfies the following:

1. the only operation in α and β is $*$,
2. the same 3 variables appear in α and β,
3. one of the variables appears twice in α and β,
4. the remaining two variables appear once in α and β,

2010 Mathematics Subject Classification: 20N20, 20M17
Keywords: quasigroup, loop, Bol-Moufang type.
This research was supported by a National Science Foundation grant DMS-0755260 and the Wabash Summer Institute in Mathematics as part of a Research Experience for Undergraduates.

5. the variables appear in the same order in α and β.

We generalize this by dropping the fifth condition, above. An identity $\alpha = \beta$ is of *generalized Bol − Moufang* type if it satisfies the following:

1. the only operation in α and β is $*$,
2. the same 3 variables appear in α and β,
3. one of the variables appears twice in α and β,
4. the remaining two variables appear once in α and β.

This paper presents the classification of all varieties of loops of generalized Bol-Moufang type. Given the classification of loops of Bol-Moufang type [13], we examine those identities in which the variables do not appear in the same order in α and β. We show that these identities are one of 48 varieties: the 14 varieties of Bol-Moufang type [13], the 6 varieties of commutative Bol-Moufang type, and 28 new varieties. As 28 is a perfect number, we name the new varieties *Perfect*.

For our convenience, we let x be the double variable and y and z be the remaining two variables in this classification. Also, we omit $*$ when multiplying two elements together (*e.g.* $x * y = xy$).

Throughout the course of this research, Prover9, an automated theorem prover, and Mace4, a finite model builder, were used [11]. For ease of reading, only several distinguishing proofs and several important counterexamples are found in this paper. Untranslated proofs from Prover9 are not included.

2. Notation and definitions

The following scheme is used to label each identity. This is an extension of the labeling scheme used by Phillips and Vojtěchovský [14].

Variable Order

A	xxyz	G	xxzy
B	xyxz	H	xzxy
C	yxxz	I	zxxy
D	xyzx	J	xzyx
E	yxzx	K	zxyx
F	yzxx	L	zyxx

Multiplication Order

1	$a(b(cd))$
2	$a((bc)c)$
3	$(ab)(cd)$
4	$(a(bc))d$
5	$((ab)c)d$

For example, the identity $(x(yx))z = z((xy)x)$ is called $B4K2$.

The following terminology is used to describe the generalized Bol-Moufang identities. The variable order of α is *normal* if y appears before z, i.e., α of

variable order $A-F$. The remaining variable orders are created by flipping y and z and are thus called *flip* where G is the flip of A, and so on. An identity $\alpha = \beta$ is *normal – normal* if α and β are normal. We define *normal – flip*, *flip – flip*, and *flip – normal* similarly. The *dual* of an identity is the identity created when reading an identity from right to left. For example, the *dual* of $A1B2$, $x(x(yz)) = x((yx)z)$, is $(z(xy))x = ((zy)x)x$, or $E4F5$.

3. Identities of generalized Bol-Moufang type

In order to classify all varieties of loops of generalized Bol-Moufang type, we first count all possible identities of generalized Bol-Moufang type. We then find equivalencies among these identities, systematically examining and eliminating first equivalent commutative identities and then equivalent non-commutative identities. The remainder is the list of unique varieties, the loops of Perfect type.

Theorem 3.1. *There are* 1215 *non-trivial identities of generalized Bol-Moufang type.*

Proof. Note that each normal-flip identity has an equivalent flip-normal identity. For example, $A1H2$ is equivalent to $H2A1$. Likewise, each normal-normal identity has an equivalent flip-flip identity when the substitution $y = z$ is made. It is thus sufficient to count the normal-flip identities and normal-normal identities, i.e. identities where α has the variable order A, B, C, D, E, or F.

Note that α and β can be 1 of 5 possible multiplication orders; each identity of variable order $\alpha = \beta$ thus has 25 possible multiplication orders.

Consider first the normal-flip identities in which β is the flip of α; for example, $A1G3$. There are 25 such identities for A, B, C, D, E, and F. However, for each variable order, ten of the normal-flip identities are equivalent to one of the remaining 15 when the substitution $y = z$ is made. For example, $A1G2$ is equivalent to $A2G1$. Thus, there are 15 identities for the normal-flip identities in which β is the flip of α.

Consider the remaining normal-flip identities and the normal-normal identities. Let A be the variable order for α. Note that AA is Bol-Moufang and has thus been classified [13], and that AG has already been accounted for. There are 10 remaining possible variable pairings with A: AB, AC, AD, AE, AF, AH, AI, AJ, AK, and AL. Likewise, the following are possible variable pairings with B: BA, BC, BD, BE, BF, BG, BI, BJ,

BK, and BL. Note that BA is equivalent to AB and has thus already been counted. Therefore, B has 9 possible variable pairings. Similarly, C has 8 possible variable pairings, D has 7, E has 6, and F has 5.

Multiplying the normal-flip and normal-normal variable orders with the possible 25 multiplication orders and adding the specific case of the normal-flip identities in which β is the flip of α gives the total number of identities: $(10+9+8+7+6+5)*25+(6)*15=1215$ □

4. Commutative identities

First we examine the identities which imply commutativity. Any identity in which letting x, y, or $z=1$ yields $zy=yz$, $xy=yx$, or $xz=zx$ will be commutative.

Theorem 4.1. *There are* 1092 *commutative identities of the generalized Bol-Moufang type.*

Proof. The 840 normal - flip identities are commutative because when $x=1$, they become $yz=zy$.

In addition, 90 normal-normal identities were found to be commutative by letting x, y, or $z=1$: $A1B1$, $A1B2$, $A1B4$, $A1D1$, $A1D2$, $A1D3$, $A1E1$, $A1E3$, $A2B1$, $A2B2$, $A2B4$, $A2D1$, $A2D2$, $A2D3$, $A2E1$, $A2E3$, $A4B1$, $A4B2$, $A4B4$, $A4D1$, $A4D2$, $B1D1$, $B1D2$, $B1D3$, $B1E1$, $B1E3$, $B2D1$, $B2D2$, $B2D3$, $B2E1$, $B2E3$, $B3C3$, $B3C5$, $B3D1$, $B3D2$, $B3D3$, $B3E1$, $B3E3$, $B3E4$, $B3E5$, $B3F4$, $B3F5$, $B5C3$, $B5C5$, $B5E3$, $B5E4$, $B5E5$, $B5F4$, $B5F5$, $C1D1$, $C1D2$, $C1D3$, $C1E1$, $C1E3$, $C3D1$, $C3D2$, $C3D3$, $C3D4$, $C3D5$, $C3E1$, $C3E3$, $C5D3$, $C5D4$, $C5D5$, $D3E3$, $D3E4$, $D3E5$, $D3F4$, $D3F5$, $D4E3$, $D4E4$, $D4E5$, $D4F2$, $D4F4$, $D4F5$, $D5E3$, $D5E4$, $D5E5$, $D5F2$, $D5F4$, $D5F5$, $E2F2$, $E2F4$, $E2F5$, $E4F2$, $E4F4$, $E4F5$, $E5F2$, $E5F4$, $E5F5$.

Example 4.2. For the equation $A4B2$, $(x(xy))z=x((yx)z)$ when setting the variable z as the identity the equation yields $x(xy)=x(yx)$, which is left cancelative. The resulting equation is $xy=yx$, which is commutative.

162 remaining commutative identities were found using Prover9 [11]: $A1B3$, $A1B5$, $A1D4$, $A1D5$, $A1E2$, $A1E4$, $A1E5$, $A2B3$, $A2B5$, $A2D4$, $A2D5$, $A2E2$, $A2E4$, $A2E5$, $A3B1$, $A3B2$, $A3B3$, $A3D1$, $A3D3$, $A3D5$, $A3E3$, $A3E4$, $A3E5$, $A4B3$, $A4B5$, $A4D3$, $A4D4$, $A4D5$, $A4E1$, $A4E2$, $A4E3$, $A4E4$, $A4E5$, $A5B1$, $A5B2$, $A5B3$, $A5D1$, $A5D3$, $A5D5$, $A5E3$, $A5E4$, $A5E5$, $B1C1$, $B1C2$, $B1C3$, $B1C4$, $B1C5$, $B1D4$, $B1D5$, $B1E2$, $B1E4$, $B1E5$, $B1F1$, $B1F2$, $B1F3$,

$B1F4$, $B1F5$, $B2C1$, $B2C2$, $B2C3$, $B2C4$, $B2C5$, $B2D4$, $B2D5$, $B2E2$, $B2E4$, $B2E5$, $B2F1$, $B2F2$, $B2F3$, $B2F4$, $B2F5$, $B3C1$, $B3C2$, $B3C4$, $B3D4$, $B3D5$, $B3E2$, $B3F1$, $B3F2$, $B3F3$, $B4C1$, $B4C3$, $B4C5$, $B4D1$, $B4D3$, $B4D5$, $B4E3$, $B4E4$, $B4E5$, $B4F2$, $B4F4$, $B4F5$, $B5C1$, $B5D1$, $B5D3$, $B5D5$, $B5F2$, $C1D4$, $C1D5$, $C1E2$, $C1E4$, $C1E5$, $C2D1$, $C2D3$, $C2D5$, $C2E3$, $C2E4$, $C2E5$, $C3E2$, $C3E4$, $C3E5$, $C4D1$, $C4D3$, $C4D5$, $C4E3$, $C4E4$, $C4E5$, $C5D1$, $C5D2$, $C5E1$, $C5E2$, $C5E3$, $C5E4$, $C5E5$, $D1E1$, $D1E2$, $D1E3$, $D1E4$, $D1E5$, $D1F1$, $D1F2$, $D1F3$, $D1F4$, $D1F5$, $D2E3$, $D2E4$, $D2E5$, $D2F2$, $D2F4$, $D2F5$, $D3E1$, $D3E2$, $D3F1$, $D3F2$, $D3F3$, $D5E1$, $D5E2$, $D5F1$, $D5F3$, $E1F2$, $E1F4$, $E1F5$, $E3F1$, $E3F2$, $E3F3$, $E3F4$, $E3F5$, $E4F1$, $E4F3$, $E5F1$, $E5F3$.

Thus, since $840+90+162 = 1092$, there are 1092 commutative identities of Bol-Moufang type. □

Theorem 4.3. *Any commutative identity of the generalized Bol-Moufang type can either be commuted to be of the Bol-Moufang type (i.e. the variables appear in the same order in α and β) or is of the commutative Moufang variety.*

Proof. Many commutative identities of the generalized Bol-Moufang type can be commuted to be of the Bol-Moufang type and have thus been classified [13]. Using the following table, we generated a list of the only commutative identities that cannot be commuted to the Bol-Moufang type. Letting α have the variable order of the left-most column and the multiplication order of the top-most row, all possible commutations of α are listed, such that α commutes to some multiplication order of the listed variable orders.

Table 1: Possible Commutations

	1	2	3	4	5
A	D,F,G,J,L	B,D,E,H,J,K,L	F,G,L	B,C,I,K,L	C,I,L
B	D,E,F,G,H,J,K	A,D,E,H,J,K,L	C,D,E,H,I,J,K	A,C,I,K,L	A,C,I,K,L
C	E,F,G,H,I,	F,G,I	B,D,E,H,I,J,K	A,I,L	A,D,E,H,I,K,L
D	B,E,F,G,H,J,K	A,F,G,J,L	B,C,E,H,I,J,K	A,F,G,J,L	A,B,E,H,J,K,L
E	C,F,G,H,I	C,F,G,H,I	B,C,D,H,I,J,K	B,D,F,G,H,J,K	A,B,D,H,J,K,L
F	C,G,I	C,E,G,H,I	A,G,L	B,D,E,G,H,J,K	A,D,G,J,L
G	A,D,F,J,L	B,D,E,F,H,J,K	A,F,L	C,E,F,H,I	C,F,I
H	A,B,D,E,J,K,L	B,D,E,F,G,J,K	B,C,D,E,I,J,K	C,E,F,G,I	C,E,F,G,I
I	A,B,C,K,L	A,C,L	B,C,D,E,H,J,K	C,F,G	C,E,F,G,H
J	A,B,D,E,H,K,L	A,D,F,G,L	B,C,D,E,H,I,K	A,D,F,G,L	B,D,E,F,G,H,K
K	A,B,C,I,L	A,B,C,I,L	B,C,D,E,H,I,J	A,B,D,E,J,H,L	B,D,E,F,G,H,J
L	A,C,I	A,B,C,I,K	A,F,G	A,B,D,E,J,H,K	A,D,F,G,J

Example 4.4. $A3 = (xx)(yz)$, can be commuted into the variable order F, G, or L, namely $(yz)(xx)$, $(xx)(zy)$, or $(zy)(xx)$.

Using this table, we found all generalized Bol-Moufang identities which could not be commuted into the Bol-Moufang type and eliminated any which did not axiomatize a commutative variety. The following identities are commutative but cannot be commuted into the Bol-Moufang type: $A2G5$, $A2I4$, $A3H3$, $A3I3$, $A3J3$, $A3K3$, $A5H2$, $A5J5$, $A5K5$, $B1I2$, $B1L1$, $B2G5$, $B2I4$, $B3G3$, $C2H1$, $C2J1$, $C2K4$, $C2L4$, $C3G3$, $C3L3$, $C4G2$, $C4G2$, $C4J5$, $C4K5$, $D1L1$, $D3G3$, $D3L3$, $D5G5$, $D5I4$, $E3G3$, $E3L3$, $E4I2$, $E4L1$, $E5G5$, $E5I4$, $F1H1$, $F1J1$, $F1K4$, $F1L4$, $F3H3$, $F3I3$, $F3J3$, $F3K3$, and $F4I2$. □

Using Prover9, we found these identities to be equivalent to the commutative Moufang identity, $(xx)(yz) = (xy)(xz)$, and have thus been classified [11]. An example of one of these proofs follows.

Theorem 4.5. *$A2I4$ is of the commutative Moufang variety.*

Proof. Letting $x = 1$ in $A2I4$, $x((xy)z) = (z(xx))y$, gives communtativity, $yz = zy$. Similarly, by setting $y = 1$, we have $x(xz) = z(xx)$. Using these,

$$\begin{aligned} x(z(xy)) &= x((xy)z) && \text{(by commutativity)} \\ &= (z(xx))y && \text{(assumption)} \\ &= (x(xz))y \\ &= ((xz)x)y && \text{(by commutativity)} \end{aligned}$$

Thus, $A2I4$ is commutative Moufang variety. □

Similarly, it can be shown that all commutative identities that do not commute to be of the Bol-Moufang type are of the commutative Moufang variety. Thus, all commutative identities of the generalized Bol-Moufang type have already been classified [13].

5. Non-commutative identities

With 1092 identities that have already been classified, there are 123 remaining non-commutative identities of the generalized Bol-Moufang type. Using the automated theorem prover, Prover9, and the finite model builder, Mace4, we eliminated any identity that was equivalent to another, finding the following 28 Perfect varieties. The first identity listed is used in future structural analysis and was chosen such that its dual is also in the list of 28 varieties. The equivalencies are as follows, with several notable counterexamples and proofs:

Theorem 5.1. *$A4F2$ is not equivalent to any identity.*

Example 5.2. This is a loop that is of the $A4F2$ variety but is not of the $A2C3$ variety.

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	4	5	0	6	7	3
2	2	3	0	1	6	7	4	5
3	3	0	6	7	2	4	5	1
4	4	5	1	2	7	3	0	6
5	5	6	7	4	3	0	1	2
6	6	7	3	0	5	1	2	4
7	7	4	5	6	1	2	3	0

Theorem 5.3. *The following identities are not equivalent to any other identities; $A2C3$, $A2F4$, $A4C2$, $C3F4$, $C4F2$.*

Theorem 5.4. *$A4F5$ and $A1C5$ are equivalent.*

Proof. $A1C5 \to A4F5$

Letting $z = 1$ in $A1A4$, $x(x(yz)) = x(x(yz))$ gives $x(xy) = x(xy)$. By contradiction, we assume $A1 \neq A4$. Then, $x(xy) \neq x(xy)$ which is a contradiction so $A1 = A4$. It remains to show $F5 = A4$. Letting $z = 1$ in $((xy)y)z = y)(y(xz))$ gives $(xy)y = y(yx)$.

$$\begin{aligned} &x(x(yz)) = ((yx)x)z \\ &((xy)y)z) = y(y(xz)) \quad \text{(let } x = y\text{)} \\ &(xy)y = y(yx) \quad \text{(by assumption)} \end{aligned}$$

Similarly, letting $z = 1$ in $((xz)y)y = (y(yx))z$ gives $(xy)y = y(yx)$. By contradiction, assume $F5 \neq A4$.

$$\begin{aligned} &((yz)x)x \neq (x(xy))z \\ &((xz)y)y \neq (y(yx))z \quad \text{(let } x = y\text{)} \\ &(xy)y \neq y(yx) \quad \text{(by assumption)} \end{aligned}$$

But this is a contradiction so $F5 = A4$. So $A4 = F5 = A1$ and $A1 = C5$ by assumption. Therefore $A1C5 \to A4F5$

$A4F5 \to A1C5$

Letting $z = 1$ in $A4A1$, $(x(xy))z = x(x(yz))$ gives $x(xy) = x(xy)$. By contradiction, we assume $A4 \neq A1$. Then, $x(xy) \neq x(xy)$ which is a contradiction so $A4 = A1$. Since $A4 = A1$, it remains to show that $C5 = A1$. Letting $y = 1$ in $A4F5$, $(x(xy))z = ((yz)x)x$, gives $(xx)z = (zx)x$.

$$\begin{array}{ll} (x(xy))z = ((yz)x)x & \\ (x(xz))y = ((zy)x)x & (\text{let } y = z) \\ x(xz) = (zx)x & (\text{let } y = 1) \\ (xx)z = x(xz) & (\text{by assumption}) \end{array}$$

Similarly, in $C5 = A1$,$((yx)x)z = x(x(yz))$, letting $y = 1$ gives $(xx)z = x(xz)$. By contradiction, we assume $C5 \neq A1$. Then $(xx)z \neq x(xz)$, which is a contradiction. Therefore, $C5 = A1$. So $C5 = A1 = A4$ and $A4 = F5$ by assumption. Therefore $A4F5 \to A1C5$.

Therefore, because $A4F5 \to A1C5$ and $A1C5 \to A4F5$, $A4F5$ and $A1C5$ are equivalent. □

Theorem 5.5. *The following sets of loop varieties are equivalent;*

1. $C4F5$ *and* $C5F3$ *are equivalent.*
2. $A1F2$ *and* $C1F5$ *are equivalent.*
3. $A1C2$ *and* $A3C1$ *are equivalent.*
4. $A3F1$, $A3C2$, *and* $C2F3$ *are equivalent.*
5. $A5F1$, $A5C2$, *and* $C4F1$ *are equivalent.*
6. $A5F3$, $A3C4$, *and* $C4F3$ *are equivalent.*
7. $A5F5$, $A3C5$, *and* $C5F5$ *are equivalent.*
8. $B4C4$, $D2F3$, *and* $E1F1$ *are equivalent.*
9. $B5C4$, $D4F3$, *and* $E2F1$ *are equivalent.*
10. $C1F1$, $A4C4$, *and* $A1F3$ *are equivalent.*
11. $A1F5$, $C1F2$, *and* $A4C5$ *are equivalent.*
12. $A1F1$, $C1F3$, *and* $A1C1$ *are equivalent.*
13. $C2E1$, $A5B4$, *and* $A3D2$ *are equivalent.*
14. $C2E2$, $A5B5$, *and* $A3D4$ *are equivalent.*
15. $A3F3$, $A5C4$, *and* $C2F1$ *are equivalent.*
16. $A5C5$, $A3F5$, *and* $C2F2$ *are equivalent.*
17. $A3F2$, $A5F2$, $C2F5$, $C5F1$, *and* $C5F2$ *are equivalent.*
18. $A4F1$, $A5C1$, $A1C4$, $A4C1$ *and* $A4F3$ *are equivalent.*
19. $A4F4$, $A2C1$, $A2C2$, $A3C3$, $A1C3$, $A2F1$, $A2F2$, $A5F4$, $C3F3$, $C3F5$, $C4F4$, *and* $C5F4$ *are equivalent.*
20. $A4C3$, $A2C4$, $A2C5$, $A5C3$, $A1F4$, $A2F3$, $A2F5$, $A3F4$, $C1F4$, $C2F4$, $C3F1$, *and* $C3F2$ *are equivalent.*

21. *A5D4, A5E1, A3E2, A5D2, A5E2, A3E1, A3B4, A3B5, B4C2, B5C2, B4D2, B4D4, B5D2, B5D4, B4E1, B4E2, B5E1, B5E2, B4F1, B4F3, B5F1, B5F3, C2D2, C2D4, C4D2, C4D4, C4E1, C4E2, D2E1, D2E2, D4E1, D4E2, D2F1, D4F1, E1F3, and E2F3 are equivalent.*

Example 5.6. This is a loop that is of the $A4F5$ variety but is not of the $A4F4$ variety.

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	3	2	5	4	9	8	7	6
2	2	3	0	1	6	8	4	9	5	7
3	3	2	1	0	7	9	8	4	6	5
4	4	5	6	7	0	1	2	3	9	8
5	5	4	8	9	1	0	7	6	2	3
6	6	9	4	8	2	7	0	5	3	1
7	7	8	9	4	3	6	5	0	1	2
8	8	7	5	6	9	2	3	1	0	4
9	9	6	7	5	8	3	1	2	4	0

This loop is not of the $A4F4$ variety since $(1 \cdot (1 \cdot 2)) \cdot 4 \neq (2 \cdot (4 \cdot 1)) \cdot 1$.

This demonstrates that there are 28 varieties of the Perfect type which axiomatize the 123 non-commutative identities. It should be noted that 28 is a perfect number. It should also be noted that 6 (also a perfect number) of these identities are not equivalent to any identity of generalized Bol-Moufang type. Three of these 6, $A2C3$, $A2F4$ and $C3F4$, have already been classified as Cheban I, Cheban II and the dual of Cheban I respectively [2].

6. Varieties of loops of Bol-Moufang, commutative and perfect type

The following are the 14 varieties of loops of Bol-Moufang type, the 6 commutative varieties, and the 28 varieties of the Perfect type.

Varieties of Bol-Moufang type

variety	abbrev.	defining identity	its name	ref.
Groups	GR	$x(yz) = (xy)z$	$A1A2$	[14]
Extra	EL	$x(y(zx)) = ((xy)z)x$	$D1D5$	[14]
Moufang	ML	$(xy)(zx) = (x(yz))x$	$D3D4$	[14]
Left Bol	LB	$x(y(xz)) = (x(yx))z$	$B1B4$	[14]
Right Bol	RB	$y((xz)x) = ((yx)z)x$	$E2E5$	[14]
C-loops	CL	$y(x(xz)) = ((yx)x)z$	$C1C5$	[14]
LC-loops	LC	$(xx)(yz) = (x(xy))z$	$A3A4$	[14]
RC-loops	RC	$y((zx)x) = (yz)(xx)$	$F2F3$	[14]
Left Alternative	LA	$x(xy) = (xx)y$	$A4A5$	[14]
Right Alternative	RA	$y(xx) = (yx)x$	$C4C5$	[14]
Flexible Loops	FL	$x(yx) = (xy)x$	$B4B5$	[14]
Middle Nuclear Square	MN	$y((xx)z) = (y(xx))z$	$C2C4$	[14]
Right Nuclear Square	RN	$y(z(xx)) = (yz)(xx)$	$F1F3$	[14]
Left Nuclear Square	LN	$((xx)y)z = (xx)(yz)$	$A5A3$	[14]

Varieties of commutative Bol-Moufang type

variety	abbrev.	defining identity	its name
Comm. Moufang	CM	$(xy)(xz) = (xx)(zy)$	$B3G3$
Abelian Group	AG	$x(yz) = (yx)z$	$A1B2$
Comm. C-loop	CC	$(y(xy))z = x(y(yz))$	$B4C1$
Comm. Alternative	CA	$((xx)y)z = z(x(yx))$	$A5K1$
Comm. Nuclear square	CN	$((xx)y)z = (xx)(zy)$	$A5G3$
Comm. loops	CP	$((yx)x)z = z(x(yx))$	$C5K1$

New varieties (presented below) are primarily named according to the number of Perfect identities that axiomatize them; i.e. *Lonely* for a single identity, *Mate* for two, and *Triad* for three. The six cancellative identities are named 2*can* as they are cancellative and leave two variables. The *Frute* variety is an acronym of the structural properties of $A4F4$, discussed later. $A4C3$ is named because it implies all of the Bol-Moufang varieties, which some may consider crazy. There are historical references to the name as well. Moldova is known for both Valentin Danilovitsch Belousov, who introduced quasigroup and loop theory to much of Eastern Europe, and a musical artist who goes by "Crazy Loop" [16]. $A5D4$ is named Krypton because the variety is axiomatized by 36 identities of the Perfect type and the atomic

number of Krypton is 36.

Varieties of Perfect type

variety	abbrev.	defining identity	its name
Cheban 1	C1	$x((xy)z) = (yx)(xz)$	$A2C3$
Cheban 2	C2	$x((xy)z) = (y(zx))x$	$A2F4$
Lonely I	L1	$(x(xy))z = y((zx)x)$	$A4F2$
Cheban I Dual	CD	$(yx)(xz) = (y(zx))x$	$C3F4$
Lonely II	L2	$(x(xy))z = y((xx)z)$	$A4C2$
Lonely III	L3	$(y(xx))z = y((zx)x)$	$C4F2$
Mate I	M1	$(x(xy))z = ((yz)x)x$	$A4F5$
Mate II	M2	$(y(xx))z = ((yz)x)x$	$C4F5$
Mate III	M3	$x(x(yz)) = y((zx)x)$	$A1F2$
Mate IV	M4	$x(x(yz)) = y((xx)z)$	$A1C2$
Triad I	T1	$(xx)(yz) = y(z(xx))$	$A3F1$
Triad II	T2	$((xx)y)z = y(z(xx))$	$A5F1$
Triad III	T3	$((xx)y)z = (yz)(xx)$	$A5F3$
Triad IV	T4	$((xx)y)z = ((yz)x)x$	$A5F5$
Triad V	T5	$x(x(yz)) = y(z(xx))$	$A1F1$
Triad VI	T6	$(xx)(yz) = (yz)(xx)$	$A3F3$
Triad VII	T7	$((xx)y)z = ((yx)x)z$	$A5C5$
Triad VIII	T8	$(xx)(yz) = y((zx)x)$	$A3F2$
Triad IX	T9	$(x(xy))z = y(z(xx))$	$A4F1$
2can I	2C1	$x(yx) = y(xx)$	$B4C4$
2can II	2C2	$(xy)x = y(xx)$	$B5C4$
2can III	2C3	$x(xz) = z(xx)$	$C1F1$
2can IV	2C4	$x(xz) = (zx)x$	$C1F2$
2can V	2C5	$(xx)z = x(zx)$	$C2E1$
2can VI	2C6	$(xx)z = (xz)x$	$C2E2$
Frute	FR	$(x(xy))z = (y(zx))x$	$A4F4$
Crazy Loop	CR	$(x(xy))z = (yx)(xz)$	$A4C3$
Krypton	KL	$((xx)y)z = (x(yz))x$	$A5D4$

7. Structure of the 28 non-commutative perfect identities

Six Perfect varieties are axiomatized by an identity which is left or right cancellative:

Cancellative identities axiomatizing Perfect varieties

$B4C4$	$(x(yx))z = (y(xx))z$	$x(yx) = y(xx)$
$B5C4$	$((xy)x)z = (y(xx))z$	$(xy)x = y(xx)$
$C1F1$	$y(x(xz)) = y(z(xx))$	$x(xz) = z(xx)$
$C1F2$	$y(x(xz)) = y((zx)x)$	$x(xz) = (zx)x$
$C2E1$	$y((xx)z) = y(x(zx))$	$(xx)z = x(zx)$
$C2E2$	$y((xx)z) = y((xz)x)$	$(xx)z = (xz)x$

For the purpose of this paper, the structures of the six cancellative varieties have not been examined, as they are structurally less interesting.

Cheban I, Cheban II, and the dual of Cheban I, $C3F4$, have not been examined, as they have been already classified [2].

The following chart demonstrates which Perfect varieties imply which Bol-Moufang varieties. **None** of the Bol-Moufang varieties implied the Perfect varieties.

Bol-Moufang varieties implied by Perfect varieties

Groups	($\Leftarrow$) A4C3
Extra	($\Leftarrow$) A4C3
Moufang	($\Leftarrow$) A4C3, A4F4
Left Bol	($\Leftarrow$) A4C3, A4F4
Right Bol	($\Leftarrow$) A4C3, A4F4
C-loops	($\Leftarrow$) A4C3
LC-loops	($\Leftarrow$) A4C3, A4F1, A4F5
RC-loops	($\Leftarrow$) A4C3, A1F2, A3F2
L. Alt.	($\Leftarrow$) A4C3, A3C1, A4F1, A4F4, A4F5
R. Alt.	($\Leftarrow$) A4C3, A1F2, A3F2, A4F4, C4F5
Flexible	($\Leftarrow$) A4C3, A4F4, A5D4
L. Nuclear	($\Leftarrow$) A4C3, A3F2, A4F1, A4F5, A5D4, A5F3, A5F5, C4F5
M. Nuclear	($\Leftarrow$) A4C3, A3F2, A4C2, A4F1, A4F2, A4F5, A5D4, A5F1, C4F2
R. Nuclear	($\Leftarrow$) A4C3, A1F2, A3C1, A3F1, A3F2, A4F1, A5D4, C1F3
3-Power	($\Leftarrow$) A4C3, A1F2, A3C1, A3F1, A3F2, A3F3, A4F1, A4F4, A4F5, A5D4, A5F1, A5F3, B5C4, C1F2, C2E1, C4F5

Theorem 7.1. *$A4C3$ implies groups.*

Proof. Letting $y = y/x$ and $z = 1$ in $A4C3$ gives $x(x(y/x)) = ((y/x))x)x$. Since $y = (y/x)x$, $x(x(y/x)) = yx$. Furthermore, letting $x = y$ and $z = 1$ in $A4C3$ gives $(xy)y = y(yx)$. We prove by contradiction, assuming group, $(xy)z = x(yz)$, is not true.

$$\begin{aligned} &(xy)z \neq x(yz) && \\ &(yx)z \neq y(xz) && (\text{let } y = x) \\ &(((y/x)x)x)z \neq ((y/x)x)(xz) && (\text{let } y = (y/x)x) \end{aligned}$$

$((tx)x)z \neq (tx)(xz)$	(let $t = (y/x)$)
$(x(xt))z \neq (tx)(xz)$	(by assumption)
$(x(x(y/x))z \neq ((y/x)x)(xz)$	(let $t = (y/x)$)
$(x(x(y/x))z \neq y(xz)$	(by assumption)
$x(x(y/x)) \neq yx$	(let $z = 1$)

This is a contradiction. Thus, $A4C3$ implies $(xy)z = x(yz)$, all groups. □

Example 7.2. This is a loop that is of the $C4F2$ variety but is not an extra loop because $1 \cdot (2 \cdot (3 \cdot 1)) \neq ((1 \cdot 2) \cdot 3) \cdot 1$.

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

In addition to the implications, some Perfect varieties satisfied other structural properties. Recall the following definitions:

A loop is *right conjugacy closed* (RCC-loop) if it satisfies $z(yx) = ((zy)/z)(zx)$. A loop is *left conjugacy closed* (LCC-loop) if it satisfies $(xy)z = (xz)(z\backslash(yz))$. A loop is *conjugacy closed* if it is both RCC and LCC. A loop is *Osborn* if it satisfies $x((yz)x) = (x\backslash y)(zx)$. The *center* of a loop L, $Z(L)$, is the set such that $y \in Z(L)$ implies $xy = yx$ for all $x \in L$. A loop L is *nilpotent of class 2* if $L/Z(L)$ is abelian.

Using Prover9, we found that these are the only Perfect varieties to satisfy such conditions:

Theorem 7.3. *$A4C3$ is conjugacy closed and Osborn, $A4F4$ is Osborn, $A4C3$ is nilpotent of class 2.*

$A4F4$ contains the most interesting structural properties of any variety of Perfect type. We call $A4F4$ the *Frute* variety since $A4F4$ is *F*lexible, *R*ight bol and left bol, *U*nity of R. Alt and L. Alt, *T*hree-power associative and *E*ntails both Osborn and Moufang properties. Loops of the Frute variety will be examined further by the authors of this paper and our advisor Dr. J.D. Phillips in a future paper.

Historical Remarks. The classification of varieties of loops of the Bol-Moufang type was initiated by Fenyves and continued by Phillips and Vojtěchovský [6], [7], [13], [14]. In classifying loops of generalized Bol-Moufang

type, we partially respond to Drápal and Jedlička's call to classify all varieties of loops that include all quasigroup binary operations, *, /, and \ of generalized Bol-Moufang type [5].

We would especially like to thank our advisor, Dr. J.D. Phillips, for his invaluable assistance and guidance in our research.

References

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

[2] **A. M. Cheban**, *Loops with identities of length four and of rank three. II*, (Russian), in "General algebra and discrete geometry", Shtiintsa, Kishinev 1980, 117 – 120.

[3] **O. Chein**, *Moufang loops of small order*, Mem. Amer. Math. Soc. **197**, 1978.

[4] **O. Chein and D. A.Robinson**, *An extra law for characterizing Moufang loops*, Proc. Amer. Math. Soc. **33** (1972), 29 – 32.

[5] **A. Drápal and P. Jedlička**, *On loop identities that can be obtained by a nuclear identifictation*, European J. Combin. **31** (2010), 1907 – 1923.

[6] **F. Fenyves**, *Extra Loops I*, Publ. Math. Debrecen **15** (1968), 235 – 238.

[7] **F. Fenyves**, *Extra Loops II. On loops with identities of Bol-Moufang type*, Publ. Math. Debrecen **16** (1969), 187 – 192.

[8] **E. G. Goodaire, S. May and M. Raman**, *The Moufang loops of order less than* 64, Nova Science Publishers, NY 1999.

[9] **F. Lemieux, C. Moore and D. Thérien**, *Polyabelian loops and Boolean completeness*, http://citeseerx.ist.psu.edu/

[10] **K. Kunen**, *The structure of conjugacy closed loops*, Trans. Amer. Math. Soc. **352**, (2000), 2889 – 2911.

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

[12] **R. Moufang**, *Zur Struktur der Alternativkoerpern*, Math. Ann. **110** (1935), 416 – 430.

[13] **J.D. Phillips and P. Vojtěchovský**, *The varieties of loops of Bol-Moufang type*, Algebra Univeralis **54** (2005), 259 – 271.

[14] **J.D. Phillips and P. Vojtěchovský**, *The varieties of quasigroups of Bol-Moufang type: An equational reasoning approach*, J. Algebra **293** (2005), 17 – 33.

[15] **H. O. Pflugfelder**, *Quasigroups and Loops: Introduction*, Sigma Series in Pure Mathematics **7**, Heldermann Verlag Berlin 1990.

[16] **H. O. Pflugfelder**, *Historical notes on loop theory*, Comment. Math. Univ. Carolinae, **7** (2000), 359 – 370.

[17] **D. A. Robinson**, *Bol loops*, Trans. Amer. Math. Soc. **123** (1966), 341 – 354.

Received February 5, 2010
Revised January 16, 2011

Quasigroups and Related Systems **19** (2011), 207 – 222

A characterization of binary invertible algebras linear over a group

Sergey S. Davidov

Abstract. In this paper we define linear over a group and an abelian group binary invertible algebras and characterize the class of such algebras by second-order formulae, namely the $\forall\exists(\forall)$-identities.

1. Introduction

A quasigroup, $(Q;\cdot)$, of the form,

$$xy = \varphi x + a + \psi y,$$

where $(Q;+)$ is a group, φ, ψ are automorphisms (antiautomorphisms) of $(Q;+)$, and a is a fixed element of Q, is called *linear* (*alinear*) *quasigroup* over the group, $(Q;+)$, [2, 6].

All primitive linear (alinear) quasigroups form a variety [6].

A linear quasigroup over an abelian group is called a *T-quasigroup* [10]. An important subclass of the T-quasigroups is the class of medial quasigroups. A quasigroup $(Q;\cdot)$ is called *medial*, if the following identity holds: $xy \cdot uv = xu \cdot yv$. Any medial quasigroup is a T-quasigroup by Toyoda theorem, [3] – [8], with the condition, $\varphi\psi = \psi\varphi$.

Medial quasigroups have been studied by many authors, namely R.H. Bruck [8], T. Kepka, P. Nemec and J. Ježek [9]-[11], D.S. Murdoch [16], A.B. Romanowska and J.D.H. Smith [17], K. Toyoda [21] and others and this class plays a special role in the theory of quasigroups. T-quasigroups were introduced by T. Kepka and P. Nemec [10, 11]. Later G.B. Belyavskaya characterized the class of T-quasigroups by a system of two identities [5, 7].

A binary algebra $(Q;\Sigma)$ is called *invertible*, if $(Q;A)$ is a quasigroup for any operation, $A \in \Sigma$. The invertible algebras first were considered by

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

R. Schauffler in touch with coding theory [19, 20]. Later such algebras were investigated by J. Aczel [1], V.D. Belousov [2, 3], Yu.M. Movsisyan [12] – [15], A. Sade [18] and others.

By analogy with linear (alinear) quasigroups we introduce the notion of a linear (alinear) invertible algebra.

Definition 1.1. An invertible algebra $(Q;\Sigma)$ is called *linear* (*alinear*) over the group $(Q;+)$ if every operation $A \in \Sigma$ has the form:

$$A(x,y) = \varphi_A x + t_A + \psi_A y, \tag{1}$$

where φ_A, ψ_A are automorphisms (antiautomorphisms) of $(Q;+)$ for all $A \in \Sigma$, and t_A are fixed elements of Q.

A linear invertible algebra over an abelian group is called an *invertible T-algebra*.

Let us recall, that the following absolutely closed second-order formulae:

$$\forall X_1, \ldots, X_m \forall x_1, \ldots, x_n \quad (\omega_1 = \omega_2),$$
$$\forall X_1, \ldots, X_k \exists X_{k+1} \ldots, X_m \forall x_1, \ldots, x_n \quad (\omega_1 = \omega_2),$$

where ω_1, ω_2 are words (terms) written in the functional variables $X_1, ..., X_m$, and in the objective variables, $x_1, \ldots, x_n$, are called $\forall(\forall)$-*identity* or *hyper-identity* and $\forall\exists(\forall)$-*identity*. The satisfiability (truth) of these second order formulae in the algebra $(Q;\Sigma)$ is understood in the sense of functional quantifiers, $(\forall X_i)$ and $(\exists X_j)$, meaning: "for every value $X_i = A \in \Sigma$ of the corresponding arity" and "there exists a value $X_j = A \in \Sigma$ of the corresponding arity". It is assumed that such a replacement is possible, that is:

$$\{|X_1|, \ldots, |X_m|\} \subseteq \{|A| \,|\, A \in \Sigma\},$$

where $|S|$ is the arity of S. Generally, hyperidentities are written without a quantifier prefix: $\omega_1 = \omega_2$. For details about such formulae see [12] – [15].

The binary algebra, $(Q;\Sigma)$, is called *medial* (*abelian*) if the following hyperidentity holds:

$$X(Y(x,y),Y(u,v)) = Y(X(x,u),X(y,v)).$$

Yu.M. Movsisyan proved that medial invertible algebras are a special class of invertible T-algebras, namely all automorphisms of the group $(Q;+)$,

which correspond the operations from Σ are permutable:
$\varphi_A \cdot \varphi_B = \varphi_B \cdot \varphi_A$, $\psi_A \cdot \psi_B = \psi_B \cdot \psi_A$, $\varphi_A \cdot \psi_B = \psi_B \varphi_A$ for all $A, B \in \Sigma$.

In the present paper we characterize the class of invertible linear (alinear) algebras and the class of invertible T-algebras by second-order formulae, namely, $\forall\exists(\forall)$-identities. For proofs of these results we use the methods of the papers, [6, 5].

2. Linear and alinear 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 $A \in \Sigma$.

The unique solution of the equality $B(a,x) = a$ ($B(x,a) = a$) is denoted by e_a^B (f_a^B), i.e., e_a^B (f_a^B) is the right (left) local identity of the element a with respect to the operation B.

It is well known [3] that with each quasigroup A the next five quasigroups are connected:

$$A^{-1},\ \ {}^{-1}A,\ \ {}^{-1}(A^{-1}),\ \ ({}^{-1}A)^{-1},\ \ A^*,$$

where $A^*(x,y) = A(y,x)$. These quasigroups are called *inverse quasigroups* or *parastrophies*. Like this, with each invertible algebra $(Q;\Sigma)$ the next five invertible algebras are connected:

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

where

$$\begin{aligned}
\Sigma^{-1} &= \{A^{-1} |\, A \in \Sigma\},\\
{}^{-1}\Sigma &= \{{}^{-1}A |\, A \in \Sigma\},\\
{}^{-1}(\Sigma^{-1}) &= \{{}^{-1}(A^{-1}) |\, A \in \Sigma\},\\
({}^{-1}\Sigma)^{-1} &= \{({}^{-1}A)^{-1} |\, A \in \Sigma\},\\
\Sigma^* &= \{A^* |\, A \in \Sigma\}.
\end{aligned}$$

Each of these invertible algebras are called *parastrophies* of $(Q;\Sigma)$.

Lemma 2.1. *If an invertible algebra $(Q;\Sigma)$ satisfies the following equality:*

$$A(B(x,y),B(u,v)) = A(B(x,u),B(\alpha y,v)), \tag{2}$$

where α is a mapping from Q into Q and A, B are some operations from Σ, then α depends on u, A, B and on their inverse operations and has the form:

$$\alpha y = \alpha_u^{A,B} y = {}^{-1}B\big(A^{-1}(u, A({}^{-1}B(u,u), y), u)), B^{-1}(u,u)\big). \tag{3}$$

Proof. If in (2) $x = f_u^B$ and $v = e_u^B$, we obtain:

$$\begin{gathered} A\big(B(f_u^B, y), B(u, e_u^B)\big) = A\big(B(f_u^B, u), B(\alpha y, e_u^B)\big), \\ A\big(B(f_u^B, y), u\big) = A\big(u, B(\alpha y, e_u^B)\big), \\ A\big(L_{B,f_u^B} y, u\big) = A\big(u, R_{B,e_u^B}\alpha y\big), \\ R_{A,u} L_{B,f_u^B} y = L_{A,u} R_{B,e_u^B} \alpha y, \\ \alpha y = R_{B,e_u^B}^{-1} L_{A,u}^{-1} R_{A,u} L_{B,f_u^B} y. \end{gathered}$$

We have

$$\begin{gathered} \alpha y = R_{B,e_u^B}^{-1} L_{A,u}^{-1} R_{A,u} B\big(f_u^B, y\big) = R_{B,e_u^B}^{-1} L_{A,u}^{-1} A\big(B\big(f_u^B, y\big), u\big) = \\ R_{B,e_u^B}^{-1} A^{-1}\big(u, A\big(B\big(f_u^B, y\big), u\big)\big) = \\ {}^{-1}B\big(A^{-1}\big(u, A\big(B\big({}^{-1}B(u,u), y\big), u\big)\big), {}^{-1}B(u,u)\big), \end{gathered}$$

since $e_u^B = B^{-1}(u,u)$, $f_u^B = {}^{-1}B(u,u)$, $R_{B,y}^{-1} x = {}^{-1}B(x,y)$, $L_{B,y}^{-1} x = B^{-1}(y,x)$. □

Lemma 2.2. *If an invertible algebra $(Q;\Sigma)$ satisfies the following equality:*

$$A(B(x,y), B(u,v)) = A(B(\beta v, y), B(u,x)), \tag{4}$$

where β is a mapping from Q into Q and A, B are some operations from Σ, then β depends on x, A, B and on their inverse operations and has the form:

$$\beta v = \beta_x^{A,B} v = {}^{-1}B\big({}^{-1}A\big(A\big(x, B\big({}^{-1}B(x,x), v\big)\big), x\big), B^{-1}(x,x)\big). \tag{5}$$

Proof. If in (4) $y = e_x^B$ and $u = f_x^B$, then we obtain as in Lemma 2.1. □

Theorem 2.1. *The binary algebra $(Q;\Sigma)$ is an invertible linear algebra iff the following second order formula:*

$$X(Y(x,y), Y(u,v)) = X\big(Y(x,u), Y\big(\alpha_u^{X,Y} y, v\big)\big), \tag{6}$$

where

$$\alpha_u^{X,Y} y = {}^{-1}Y\big(X^{-1}\big(u, X\big(Y\big({}^{-1}Y(u,u), y\big), u\big)\big), Y^{-1}(u,u)\big) \tag{7}$$

is valid in the algebra $(Q;\Sigma \cup \Sigma^{-1} \cup^{-1} \Sigma)$ for all $X, Y \in \Sigma$.

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

$$X(x,y) = \varphi_X x + c_X + \psi_X y\,,$$

where φ_X, ψ_X are automorphisms of the group $(Q;+)$ and $c_X \in Q$. We prove that equality (6) is valid in the algebra $(Q;\Sigma \cup \Sigma^{-1} \cup^{-1} \Sigma)$ for all $X, Y \in \Sigma$, when

$$\alpha_u^{X,Y} y = -\alpha_0^{X,Y} u + \alpha_0^{X,Y} y + u\,,$$

where $\alpha_0^{X,Y} y = \varphi_Y^{-1}\psi_X^{-1}\tilde{L}_{c_Y}^{-1}\tilde{R}_{c_X}\varphi_X\psi_Y y$, $\tilde{L}_{c_Y}x = c_Y + x$, $\tilde{R}_{c_X}x = x + c_X$. Indeed,

$$\begin{aligned} X(Y(x,y),Y(u,v)) &= \varphi_X(\varphi_Y x + c_Y + \psi_Y y) + c_X + \psi_X(\varphi_Y u + c_Y + \psi_Y v) = \\ &= \varphi_X\varphi_Y x + \varphi_X c_Y + \varphi_X\psi_Y y + c_X + \psi_X\varphi_Y u + \psi_X c_Y + \psi_X\psi_Y v\,, \end{aligned}$$

on the other hand, using the expressions for $\alpha_0^{X,Y}$, we obtain

$$\begin{gathered} X\big(Y(x,u),Y\big(\alpha_u^{X,Y}y,v\big)\big) = \varphi_X(\varphi_Y x + c_Y + \psi_Y u) + c_X + \\ +\psi_X\big(\varphi_Y\alpha_u^{X,Y}y + c_Y + \psi_Y v\big) = \varphi_X\varphi_Y x + \varphi_X c_Y + \varphi_X\psi_Y u + c_X + \\ +\psi_X\varphi_Y\big(-\alpha_0^{X,Y}u + \alpha_0^{X,Y}y + u\big) + \psi_X c_Y + \psi_X\psi_Y v = \varphi_X\varphi_Y x + \varphi_X c_Y + \\ +\varphi_X\psi_Y u + c_X - \psi_X\varphi_Y\varphi_Y^{-1}\psi_X^{-1}\tilde{L}_{c_Y}^{-1}\tilde{R}_{c_X}\varphi_X\psi_Y u + \\ +\psi_X\varphi_Y\varphi_Y^{-1}\psi_X^{-1}\tilde{L}_{c_Y}^{-1}\tilde{R}_{c_X}\varphi_X\psi_Y y + \psi_X\varphi_Y u + \psi_X c_Y + \psi_X\psi_Y v = \\ = \varphi_X\varphi_Y x + \varphi_X c_Y + \varphi_X\psi_Y u + c_X - \tilde{L}_{c_Y}^{-1}\tilde{R}_{c_X}\varphi_X\psi_Y u + \tilde{L}_{c_Y}^{-1}\tilde{R}_{c_X}\varphi_X\psi_Y y + \\ +\psi_X\varphi_Y u + \psi_X c_Y + \psi_X\psi_Y v = \varphi_X\varphi_Y x + \varphi_X c_Y + \varphi_X\psi_Y u + c_X - \\ -(-c_Y + \varphi_X\psi_Y u + c_X) - c_Y + \varphi_X\psi_Y y + c_X + \psi_X\varphi_Y u + \psi_X c_Y + \\ +\psi_X\psi_Y v = \varphi_X\varphi_Y x + \varphi_X c_Y + \varphi_X\psi_Y y + c_X - c_X - \varphi_X\psi_Y u + c_Y - \\ -c_Y + \varphi_X\psi_Y y + c_X + \psi_X\varphi_Y u + \psi_X c_Y + \psi_X\psi_Y v = \\ = \varphi_X\varphi_Y x + \varphi_X c_Y + \varphi_X\psi_Y y + c_X + \psi_X\varphi_Y u + \psi_X c_Y + \psi_X\psi_Y v. \end{gathered}$$

Thus, the right and left sides of equality (6) are equal. According to Lemma 2.1 we obtain that $\alpha_u^{X,Y}$ has the form of (7).

Conversely, let formula (6) be valid in the algebra $(Q;\Sigma \cup \Sigma^{-1} \cup^{-1} \Sigma)$ for all $X, Y \in \Sigma$. We prove that the algebra $(Q;\Sigma)$ is an invertible linear algebra. Let us fix (in (6)) the element $u = a$ and the operations $X = A$, $Y = B$, where $A, B \in \Sigma$, then we obtain:

$$\begin{aligned} A(B(x,y),B(a,v)) &= A\big(B(x,a),B\big(\alpha_a^{A,B}y,v\big)\big), \\ A(B(x,y),L_{B,a}v) &= A\big(R_{B,a}x,B\big(\alpha_a^{A,B}y,v\big)\big), \end{aligned}$$

or

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

where $A_1(x,y) = A(x, L_{B,a}y)$, $A_2(x,y) = B(x,y)$, $A_3(x,y) = A(R_{B,a}x, y)$, $A_4(x,y) = B\big(\alpha_a^{A,B}x, y\big)$.

From the last equality, according to Belousov's theorem about four quasigroups which are connected through the associative law [18], all the operations A_i $(i = 1,2,3,4)$ are isotopic to the same group. Hence, the operations, A and B, are isotopic to the same group, and since the operations A and B are arbitrary we obtain that all the operations from Σ are isotopic to the same group $(Q;*)$.

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

$$x \underset{X}{+} y = X\big(R_{X,a}^{-1}x, L_{X,b}^{-1}y\big), \tag{8}$$

where a, b are some elements from Q. These operations are loops with the identity element $0_X = X(b,a)$ [3], and they are isotopic to the group $(Q;*)$. Hence, by Albert's theorem [3], they are groups for every $X \in \Sigma$.

Let us rewrite equality (6) (where $X = A$, $Y = B$), (in terms of the operations $\underset{A}{+}$ and $\underset{B}{+}$) in the following way:

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

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

If we take $u = 0_B$ and $v = L_{A,b}^{-1}0_A$ in the last equality, then we have:

$$R_{A,a}\big(x \underset{B}{+} y\big) \underset{A}{+} L_{A,b}\big(0_B \underset{B}{+} L_{A,b}^{-1}0_A\big) =$$
$$R_{A,a}\big(x \underset{B}{+} L_{B,b}R_{B,a}^{-1}0_B\big) \underset{A}{+} L_{A,b}\big(R_{B,a}\alpha_{R_{B,a}^{-1}0_B}^{A,B} L_{B,b}^{-1}y \underset{B}{+} L_{A,b}^{-1}0_A\big),$$
$$R_{A,a}\big(x \underset{B}{+} y\big) = \alpha_{A,B}x \underset{A}{+} \beta_{A,B}y, \tag{9}$$

where

$$\alpha_{A,B}x = R_{A,a}\big(x \underset{B}{+} L_{B,b}R_{B,a}^{-1}0_B\big),$$
$$\beta_{A,B}y = L_{A,b}\big(R_{B,a}\alpha_{R_{B,a}^{-1}0_B}^{A,B} L_{B,b}^{-1}y \underset{B}{+} L_{A,b}^{-1}0_A\big).$$

Since the operations A and B are arbitrary, we can take $A = B$ in (9), then we obtain:

$$R_{A,a}\big(x \underset{A}{+} y\big) = \alpha_{A,A}x \underset{A}{+} \beta_{A,A}y. \tag{10}$$

From (9) and (10), we have:

$$\begin{aligned} x \underset{A}{+} y &= R_{A,a}\big(\alpha^{-1}_{A,A}x \underset{A}{+} \beta^{-1}_{A,A}y\big),\\ x \underset{A}{+} y &= R_{A,a}\big(\alpha^{-1}_{A,B}x \underset{B}{+} \beta^{-1}_{A,B}y\big),\\ \alpha^{-1}_{A,A}x \underset{A}{+} \beta^{-1}_{A,A}y &= \alpha^{-1}_{A,B}x \underset{B}{+} \beta^{-1}_{A,B}y, \end{aligned}$$

thus, we obtain:

$$x \underset{A}{+} y = \gamma_{A,B}x \underset{B}{+} \delta_{A,B}y, \tag{11}$$

where $\gamma_{A,B} = \alpha^{-1}_{A,B}\alpha_{A,A}$ and $\delta_{A,B} = \beta^{-1}_{A,B}\beta_{A,A}$ are the permutations of the set Q. Hence, from (9), according to (11), we get:

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

i.e., $R_{A,a}$ is a quasiautomorphism of the group $\big(Q; \underset{B}{+}\big)$ and since the operation A is arbitrary, we have that $R_{A,a}$ is the quasiautomorphism of the group $\big(Q; \underset{B}{+}\big)$ for all operations A from Σ. We fix the operation $\underset{B}{+}$ and further will be denote it by $+$.

According to (8), for the operations $A \in \Sigma$ we have:

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

According to (11), from the last equality, we get:

$$A(x, y) = \theta^{A,B}_1 x + \theta^{A,B}_2 y, \tag{12}$$

where $\theta^{A,B}_1 = \gamma_{A,B}R_{A,a}$ and $\theta^{A,B}_2 = \delta_{A,B}L_{A,b}$ are the permutations of Q.

We prove that $\theta^{A,B}_1$ and $\theta^{A,B}_2$ are quasiautomorphisms of the group $(Q; +)$. To do it we take $v = a$, $u = f^B_a$, $X = A$, $Y = B$ in equality (6) and rewrite this equality in terms of the operation $+$:

$$\begin{aligned} &A(B(x, y), a) = A\big(B\big(x, f^B_a\big), B\big(\alpha^{A,B}_{f^B_a}y, a\big)\big),\\ &\theta^{A,B}_1(R_{B,a}x + L_{B,b}y) + \theta^{A,B}_2 a = \theta^{A,B}_1 R_{B,f^B_a}x + \theta^{A,B}_2\big(R_{B,a}\alpha^{A,B}_{f^B_a}y + L_{B,b}a\big),\\ &\theta^{A,B}_1(R_{B,a}x + L_{B,b}y) = \theta^{A,B}_1 R_{B,f^B_a}x + \theta^{A,B}_2\big(R_{B,a}\alpha^{A,B}_{f^B_a}y + L_{B,b}a\big) - \theta^{A,B}_2 a, \end{aligned}$$

$$\theta_1^{A,B}(x+y)=\theta_1^{A,B}R_{B,f_a^B}R_{B,a}^{-1}x+\theta_2^{A,B}\big(R_{B,a}\alpha_{f_a^B}^{A,B}L_{B,b}^{-1}y+L_{B,b}a\big)-\theta_2^{A,B}a,$$
$$\theta_1^{A,B}(x+y)=\sigma_{A,B}x+\mu_{A,B}y,$$

where
$\sigma_{A,B}x=\theta_1^{A,B}R_{B,f_a^B}R_{B,a}^{-1}x$ and $\mu_{A,B}y=\theta_2^{A,B}\big(R_{B,a}\alpha_{f_a^B}^{A,B}L_{B,b}^{-1}y+L_{B,b}a\big)-\theta_2^{A,B}a$ are the permutations of Q and therefore $\theta_1^{A,B}$ is a quasiautomorphism of the group $(Q;+)$.

Now, we take $x=f_b^B$, $u=b$, $X=A$, $Y=B$ in (6) and rewrite this equality in terms of the operation $+$:

$$A\big(B\big(f_b^B,y\big),B(b,v)\big)=A\big(b,B\big(\alpha_b^{A,B}y,v\big)\big),$$
$$\theta_1^{A,B}L_{B,f_b^B}y+\theta_2^{A,B}L_{B,b}v=\theta_1^{A,B}b+\theta_2^{A,B}\big(R_{B,a}\alpha_b^{A,B}y+L_{B,b}v\big),$$
$$\theta_2^{A,B}\big(R_{B,a}\alpha_b^{A,B}y+L_{B,b}v\big)=-\theta_1^{A,B}b+\theta_1^{A,B}L_{B,f_b^B}y+\theta_2^{A,B}L_{B,b}v,$$
$$\theta_2^{A,B}(y+v)=\sigma'_{A,B}y+\mu'_{A,B}v,$$

where $\sigma'_{A,B}y=-\theta_1^{A,B}b+\theta_1^{A,B}L_{B,f_b^B}\big(\alpha_b^{A,B}\big)^{-1}R_{B,a}^{-1}y$ and $\mu'_{A,B}v=\theta_2^{A,B}v$ are the permutations of the set Q and therefore $\theta_2^{A,B}$ is a quasiautomorphism of the group $(Q;+)$.

According to [3, lemma 2.5] we have:

$$\theta_1^{A,B}x=\varphi_Ax+s_A,$$
$$\theta_2^{A,B}x=t_A+\psi_Ay,$$

where φ_A, ψ_A are automorphisms of the group $(Q;+)$ and t_A, s_A are some elements of the set Q. Hence, from (12), it follows that

$$A(x,y)=\varphi_Ax+c_A+\psi_Ay, \tag{13}$$

where $c_A=s_A+t_A$.

Since the operation A is arbitrary, we obtain that all the operations from Σ can be presented in the form of (13) through the operation $+$. □

Theorem 2.2. *The binary algebra $(Q;\Sigma)$ is an invertible alinear algebra iff the following second order formula:*

$$X(Y(x,y),Y(u,v))=X\big(Y\big(\beta_x^{X,Y}v,y\big),Y(u,x)\big), \tag{14}$$

where

$$\beta_x^{X,Y}v={}^{-1}Y\big({}^{-1}X\big(X\big(x,Y\big({}^{-1}Y(x,x),v\big)\big),x\big),Y^{-1}(x,x)\big) \tag{15}$$

is valid in the algebra $(Q;\Sigma\cup\Sigma^{-1}\cup^{-1}\Sigma)$ for all $X,Y\in\Sigma$.

Proof. Let $(Q;\Sigma)$ be an invertible alinear algebra, then for every $X \in \Sigma$

$$X(x,y) = \varphi_X x + c_X + \psi_X y\,,$$

where φ_X, ψ_X are antiautomorphisms of the group $(Q;+)$ and $c_X \in Q$. We prove that equality (14) is valid in the algebra $(Q;\Sigma \cup \Sigma^{-1} \cup^{-1} \Sigma)$ for all $X, Y \in \Sigma$, if:

$$\beta_x^{X,Y} v = x + \beta_0^{X,Y} v - \beta_0^{X,Y} x\,,$$

where $\beta_0^{X,Y} v = \varphi_Y^{-1}\varphi_X^{-1}\tilde{R}_{c_Y}^{-1}\tilde{L}_{c_X}\psi_X\psi_Y v$, $\tilde{R}_{c_Y} x = x + c_Y$, $\tilde{L}_{c_X} x = c_X + x$. Indeed,

$$\begin{aligned} X(Y(x,y),Y(u,v)) &= \varphi_X(\varphi_Y x + c_Y + \psi_Y y) + c_X + \psi_X(\varphi_Y u + c_Y + \psi_Y v) = \\ &= \varphi_X\psi_Y y + \varphi_X c_Y + \varphi_X\varphi_Y x + c_X + \psi_X\psi_Y v + \psi_X c_Y + \psi_X\varphi_Y u\,, \end{aligned}$$

on the other hand, using the expressions for $\beta_0^{X,Y}$, and taking into account that $\varphi_X\varphi_Y$ is an automorphism of the group $(Q;+)$ we obtain:

$$\begin{gathered} X\big(Y\big(\beta_x^{X,Y} v, y\big), Y(u,x)\big) = \varphi_X(\varphi_Y \beta_x^{X,Y} v + c_Y + \psi_Y y) + c_X + \\ +\psi_X\big(\varphi_Y u + c_Y + \psi_Y x\big) = \varphi_X\psi_Y y + \varphi_X c_Y + \varphi_X\varphi_Y \beta_x^{X,Y} v + c_X + \\ +\psi_X\psi_Y x + \psi_X c_Y + \psi_X\varphi_Y u = \varphi_X\psi_Y y + \varphi_X c_Y + \\ +\varphi_X\varphi_Y\big(x + \beta_0^{X,Y} v - \beta_0^{X,Y} x\big) + c_X + \psi_X\psi_Y x + \psi_X c_Y + \psi_X\varphi_Y u = \\ = \varphi_X\psi_Y y + \varphi_X c_Y + \varphi_X\varphi_Y x + \varphi_X\varphi_Y \beta_0^{X,Y} v - \varphi_X\varphi_Y \beta_0^{X,Y} x + c_X + \\ +\psi_X\psi_Y x + \psi_X c_Y + \psi_X\varphi_Y u = \varphi_X\psi_Y y + \varphi_X c_Y + \varphi_X\varphi_Y x + \\ +\varphi_X\varphi_Y\varphi_Y^{-1}\varphi_X^{-1}\tilde{R}_{c_Y}^{-1}\tilde{L}_{c_X}\psi_X\psi_Y v - \varphi_X\varphi_Y\varphi_Y^{-1}\varphi_X^{-1}\tilde{R}_{c_Y}^{-1}\tilde{L}_{c_X}\psi_X\psi_Y x + \\ +c_X + \psi_X\psi_Y x + \psi_X c_Y + \psi_X\varphi_Y u = \varphi_X\psi_Y y + \varphi_X c_Y + \varphi_X\varphi_Y x + c_X + \\ +\psi_X\psi_Y v - c_Y - (c_X + \psi_X\psi_Y x - c_Y) + c_X + \psi_X\psi_Y x + \psi_X c_Y + \psi_X\varphi_Y u = \\ = \varphi_X\psi_Y y + \varphi_X c_Y + \varphi_X\varphi_Y x + c_X + \psi_X\psi_Y v - c_Y + c_Y - \psi_X\psi_Y x - \\ -c_X + c_X + \psi_X\psi_Y x + \psi_X c_Y + \psi_X\varphi_Y u = \\ = \varphi_X\psi_Y y + \varphi_X c_Y + \varphi_X\varphi_Y x + c_X + \psi_X\psi_Y v + \psi_X c_Y + \psi_X\varphi_Y u. \end{gathered}$$

Thus, the right and left sides of equality (14) are equal. According to Lemma 2.2, we get that $\beta_x^{X,Y}$ has the form of (15).

Conversely, let the formula (14) be valid in the algebra $(Q;\Sigma\cup\Sigma^{-1}\cup^{-1}\Sigma)$ for all $X, Y \in \Sigma$. We prove that the algebra $(Q;\Sigma)$ is an invertible alinear algebra. Fixing the element $x = p$ and the operations $X = A$, $Y = B$,

where $A, B \in \Sigma$ in (14), we obtain:

$$A(B(p,y),B(u,v)) = A\big(B\big(\beta_p^{A,B}v,y\big),B(u,p)\big),$$
$$A(L_{B,p}y,B(u,v)) = A\big(B\big(\beta_p^{A,B}v,y\big),R_{B,p}u\big),$$
$$A^*(B(u,v),L_{B,p}y) = A^*\big(R_{B,p}u,B\big(\beta_p^{A,B}v,y\big)\big)$$

or

$$A_1(A_2(u,v),y) = A_3(u,A_4(v,y)),$$

where $A_1(x,y) = A^*(x,L_{B,p}y)$, $A_2(x,y) = B(x,y)$, $A_3(x,y) = A^*(R_{B,p}x,y)$, $A_4(x,y) = B\big(\beta_p^{A,B}x,y\big)$.

From the last equality, according to Belousov's theorem about four quasigroups which are connected with the associative law [18], all the operations A_i $(i = 1,2,3,4)$ are isotopic to the same group. Since the operation B is arbitrary, we obtain that all the operations from Σ are isotopic to the same group $(Q;*)$.

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

$$x \underset{X}{+} y = X\big(R_{X,a}^{-1}x, L_{X,b}^{-1}y\big), \tag{16}$$

where a, b are some elements from Q. These operations are loops with the identity element $0_X = X(b,a)$ [3], and they are isotopic to the group $(Q;*)$. Hence by Albert's theorem [3] they are groups for every $X \in \Sigma$.

Let us rewrite the equality (14) (where $X = A$, $Y = B$) in terms of the operations $\underset{A}{+}$ and $\underset{B}{+}$

$$R_{A,a}\big(R_{B,a}x \underset{B}{+} L_{B,b}y\big) \underset{A}{+} L_{A,b}\big(R_{B,a}u \underset{B}{+} L_{B,b}v\big) =$$
$$R_{A,a}\big(R_{B,a}\beta_x^{A,B}v \underset{B}{+} L_{B,b}y\big) \underset{A}{+} L_{A,b}\big(R_{B,a}u \underset{B}{+} L_{B,b}x\big).$$

If we take $y = a$ and $x = R_{B,a}^{-1}b = d$ in the last equality, we have:

$$R_{A,a}\big(R_{B,a}R_{B,a}^{-1}b \underset{B}{+} L_{B,b}a\big) \underset{A}{+} L_{A,b}\big(R_{B,a}u \underset{B}{+} L_{B,b}v\big) =$$
$$R_{A,a}\big(R_{B,a}\beta_d^{A,B}v \underset{B}{+} L_{B,b}a\big) \underset{A}{+} L_{A,b}\big(R_{B,a}u \underset{B}{+} L_{B,b}d\big),$$
$$R_{A,a}\big(b \underset{B}{+} 0_B\big) \underset{A}{+} L_{A,b}\big(R_{B,a}u \underset{B}{+} L_{B,b}v\big) =$$
$$R_{A,a}\big(R_{B,a}\beta_d^{A,B}v \underset{B}{+} 0_B\big) \underset{A}{+} L_{A,b}B(u,d),$$
$$R_{A,a}b + L_{A,b}\big(R_{B,a}u \underset{B}{+} L_{B,b}v\big) = R_{A,a}R_{B,a}\beta_d^{A,B}v \underset{A}{+} L_{A,b}R_{B,d}u,$$

$$L_{A,b}\big(R_{B,a}u \underset{B}{+} L_{B,b}v\big) = R_{A,a}R_{B,a}\beta_d^{A,B}v \underset{A}{+} L_{A,b}R_{B,d}u,$$

or

$$L_{A,b}\big(u \underset{B}{+} v\big) = \alpha_{A,B}v \underset{A}{+} \beta_{A,B}u \tag{17}$$

where

$$\alpha_{A,B} = R_{A,a}R_{B,a}\beta_d^{A,B}L_{B,b}^{-1} \qquad \text{and} \qquad \beta_{A,B} = L_{A,b}R_{B,d}R_{B,a}^{-1}$$

are permutations of the set Q.

Since the operations A and B are arbitrary, we can take $A = B$ in (17), and get:

$$L_{A,b}\big(u \underset{A}{+} v\big) = \alpha_{A,A}v \underset{A}{+} \beta_{A,A}u. \tag{18}$$

From (17) and (18) we have:

$$\begin{aligned} v \underset{A}{+} u &= L_{A,b}\big(\beta_{A,B}^{-1}u \underset{B}{+} \alpha_{A,B}^{-1}v\big),\\ v \underset{A}{+} u &= L_{A,b}\big(\beta_{A,A}^{-1}u \underset{A}{+} \alpha_{A,A}^{-1}v\big),\\ \beta_{A,B}^{-1}u \underset{B}{+} \alpha_{A,B}^{-1}v &= \beta_{A,A}^{-1}u \underset{A}{+} \alpha_{A,A}^{-1}v, \end{aligned}$$

and thus, we obtain:

$$u \underset{A}{+} v = \gamma_{A,B}u \underset{B}{+} \delta_{A,B}v, \tag{19}$$

where $\gamma_{A,B} = \beta_{A,B}^{-1}\beta_{A,A}$ and $\delta_{A,B} = \alpha_{A,B}^{-1}\alpha_{A,A}$ are the permutations of the set Q.

According to (16), for the operations $A \in \Sigma$, we have:

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

According to (19), from the last equality, we get:

$$A(x,y) = \theta_1^{A,B}x \underset{B}{+} \theta_2^{A,B}y, \tag{20}$$

where $\theta_1^{A,B} = \gamma_{A,B}R_{A,a}$ and the $\theta_2^{A,B} = \delta_{A,B}L_{A,b}$ are the permutations of the set Q. Thus, we can represent every operations from Σ by the operation $\underset{B}{+}$. We fix the operation $\underset{B}{+}$ and further denote it by $+$.

We shall prove that $\theta_1^{A,B}$ and $\theta_2^{A,B}$ are antiquasiautomorphisms of the group $(Q;+)$. To do it we take $x = a$, $u = f_a^B$, $X = A$, $Y = B$, in equality (14) and rewrite this equality in terms of the operation, $+$:

$$A\big(B(a,y),B\big(f_a^B,v\big)\big)=A\big(B\big(\beta_a^{A,B}v,y\big),a\big),$$
$$\theta_1^{A,B}(R_{B,a}a+L_{B,b}y)+\theta_2^{A,B}L_{B,f_a^B}v=\theta_1^{A,B}\big(R_{B,a}\beta_a^{A,B}v+L_{B,b}y\big)+\theta_2^{A,B}a,$$
$$\theta_1^{A,B}(R_{B,a}\beta_a^{A,B}v+L_{B,b}y)=\theta_1^{A,B}\big(R_{B,a}a+L_{B,b}y\big)+\theta_2^{A,B}L_{B,f_a^B}v-\theta_2^{A,B}a,$$
$$\theta_1^{A,B}(v+y)=\theta_1^{A,B}\big(R_{B,a}a+y\big)+\theta_2^{A,B}L_{B,f_a^B}\big(\beta_a^{A,B}\big)^{-1}R_{B,a}^{-1}v-\theta_2^{A,B}a,$$
$$\theta_1^{A,B}(v+y)=\sigma_{A,B}y+\mu_{A,B}v,$$

where
$\sigma_{A,B}y{=}\theta_1^{A,B}\big(R_{B,a}a+y\big)$ and $\mu_{A,B}v{=}\theta_2^{A,B}L_{B,f_a^B}\big(\beta_a^{A,B}\big)^{-1}R_{B,a}^{-1}v-\theta_2^{A,B}a$ are the permutations of the set Q and therefore, $\theta_1^{A,B}$ is an antiquasiautomorphism of the group $(Q;+)$.

If we take $x=a$, $y=e_a^B$, $X=A$, $Y=B$ in the equality (14), we can similarly prove that $\theta_2^{A,B}$ is an antiquasiautomorphism of the group $(Q;+)$.

Thus, we have [2]

$$\theta_1^{A,B}x=\varphi_A x+s_A,$$
$$\theta_2^{A,B}x=t_A+\psi_A y,$$

where φ_A, ψ_A are antiautomorphisms of the group $(Q;+)$ and t_A, s_A are some elements of the set Q. Hence, from (20) we get that:

$$A(x,y)=\varphi_A x+c_A+\psi_A y, \tag{21}$$

where $c_A=s_A+t_A$.

Since the operation A is arbitrary, we obtain that all the operations from Σ can be presented in the form of (21). □

3. Invertible T-algebras

It is known [10, 11] that T-quasigroups are invariant under parastrophies. We have the same result for parastrophies of invertible T-algebras.

Proposition 3.1. *Let $(Q;\Sigma)$ be an invertible T-algebra. Then all parastrophies of the algebra, $(Q;\Sigma)$, are invertible T-algebras.*

Also, as in the case of quasigroups [6], we have the following result:

Proposition 3.2. *If an invertible algebra is linear and alinear then it is T-algebra.*

Lemma 3.1. *If the algebra* $(Q;\Sigma\cup\Sigma^{-1}\cup{}^{-1}\Sigma)$*, where* $(Q;\Sigma)$ *is an invertible* T*-algebra, satisfies equality* (6) *for all* $X,Y\in\Sigma$*, then this equality is also valid in the algebra* $\big(Q;\Sigma\cup^{-1}\Sigma\cup\Sigma^{-1}\cup({}^{-1}\Sigma)^{-1}\cup^{-1}(\Sigma^{-1})\cup\Sigma^*\big)$ *for all* $X,Y\in\Sigma\cup^{-1}\Sigma\cup\Sigma^{-1}\cup({}^{-1}\Sigma)^{-1}\cup^{-1}(\Sigma^{-1})\cup\Sigma^*$.

Proof. We must check equalities for all $A,B\in\Sigma\cup^{-1}\Sigma\cup\Sigma^{-1}\cup({}^{-1}\Sigma)^{-1}\cup^{-1}(\Sigma^{-1})$. For example, let us check the following equality:

$$A\big({}^{-1}B(x,y),{}^{-1}B(u,v)\big)=A\big({}^{-1}B(x,u),{}^{-1}B\big(\alpha_u^{A,{}^{-1}B}y,v\big)\big).$$

In this case, we have:

$$\alpha_u^{A,{}^{-1}B}y=B\big(A^{-1}\big(u,A({}^{-1}B(B(u,u),y),u)\big),({}^{-1}B)^{-1}(u,u)\big).$$

It follows from (1):

$$\begin{aligned}A^{-1}(x,y)&=\psi_A^{-1}(-c_A-\varphi_Ax+y),\\ {}^{-1}B(x,y)&=\varphi_B^{-1}(x-\psi_By-c_B),\\ ({}^{-1}B)^{-1}(x,y)&=\psi_B^{-1}(-c_B-\varphi_By+x).\end{aligned}$$

Let us calculate $\alpha_u^{A,{}^{-1}B}y$:

$$\begin{aligned}\alpha_u^{A,{}^{-1}B}y&=\varphi_B\psi_A^{-1}\big(\varphi_A\varphi_B^{-1}\psi_Bu-\varphi_A\varphi_B^{-1}\psi_By+\psi_Au\big)+u-\varphi_Bu-c_B+c_B\\ &=\varphi_B\psi_A^{-1}\varphi_A\varphi_B^{-1}\psi_Bu-\varphi_B\psi_A^{-1}\varphi_A\varphi_B^{-1}\psi_By+\varphi_Bu+u-\varphi_Bu\\ &=\varphi_B\psi_A^{-1}\varphi_A\varphi_B^{-1}(\psi_Bu-\psi_By)+u.\end{aligned}$$

Therefore

$$\begin{aligned}&A\big({}^{-1}B(x,u),{}^{-1}B\big(\alpha_u^{A,{}^{-1}B}y,v\big)\big)\\ &=A\big(\varphi_B^{-1}(x-\psi_Bu-c_B),\varphi_B^{-1}\big(\alpha_u^{A,{}^{-1}B}y-\psi_Bv-c_B\big)\big)\\ &=\varphi_A\varphi_B^{-1}(x-\psi_Bu-c_B)+\psi_A\varphi_B^{-1}\big(\alpha_u^{A,{}^{-1}B}y-\psi_Bv-c_B\big)+c_A\\ &=\varphi_A\varphi_B^{-1}x-\varphi_A\varphi_B^{-1}\psi_Bu-\varphi_A\varphi_B^{-1}c_B+\psi_A\varphi_B^{-1}\varphi_B\psi_A^{-1}\varphi_A\varphi_B^{-1}\big(\psi_Bu-\psi_By\big)\\ &\qquad+\psi_A\varphi_B^{-1}u-\psi_A\varphi_B^{-1}\psi_Bv-\psi_A\varphi_B^{-1}c_B+c_A\\ &=\varphi_A\varphi_B^{-1}x-\varphi_A\varphi_B^{-1}c_B-\varphi_A\varphi_B^{-1}\psi_By+\psi_A\varphi_B^{-1}u-\psi_A\varphi_B^{-1}\psi_Bv-\psi_A\varphi_B^{-1}c_B+c_A\end{aligned}$$

On the other hand

$$\begin{aligned}&A\big({}^{-1}B(x,u),{}^{-1}B(u,v)\big)=\varphi_A\varphi_B^{-1}(x-\psi_By-c_B)+\psi_A\varphi_B^{-1}(u-\psi_Bv-c_B)+c_A\\ &=\varphi_A\varphi_B^{-1}x-\varphi_A\varphi_B^{-1}\psi_By-\varphi_A\varphi_B^{-1}c_B+\psi_A\varphi_B^{-1}u-\psi_A\varphi_B^{-1}\psi_Bv-\psi_A\varphi_B^{-1}c_B+c_A.\end{aligned}$$

Thus, the right and left sides are equal. Similarly, we can check the other cases. □

Lemma 3.2. *Let $(Q;\Sigma)$ be an invertible T-algebra. If the algebra, $(Q;\Sigma\cup\Sigma^{-1}\cup^{-1}\Sigma)$, satisfies equality (14) for all $X,Y\in\Sigma$, then this equality is valid in the algebra $\big(Q;\Sigma\cup^{-1}\Sigma\cup\Sigma^{-1}\cup({}^{-1}\Sigma)^{-1}\cup^{-1}(\Sigma^{-1})\cup\Sigma^{*}\big)$ for all $X,Y\in\Sigma\cup^{-1}\Sigma\cup\Sigma^{-1}\cup({}^{-1}\Sigma)^{-1}\cup^{-1}(\Sigma^{-1})\cup\Sigma^{*}$.*

Proof. Similarly as Lemma 3.1. □

Theorem 3.1. *$(Q;\Sigma)$ is an invertible T-algebra iff (6) and (14) are valid in the algebra $\big(Q;\Sigma\cup^{-1}\Sigma\cup\Sigma^{-1}\cup({}^{-1}\Sigma)^{-1}\cup^{-1}(\Sigma^{-1})\cup\Sigma^{*}\big)$ for all $X,Y\in\Sigma\cup^{-1}\Sigma\cup\Sigma^{-1}\cup({}^{-1}\Sigma)^{-1}\cup^{-1}(\Sigma^{-1})\cup\Sigma^{*}$.*

Proof. As in the proof of Theorems 2.1 and 2.2, the invertible T-algebra satisfies formulae (6) and (14). The rest follows from Lemmas 3.1 and 3.2. The converse statement is a consequence of Proposition 3.2. □

Corollary 3.1. *Let $(Q;\Sigma)$ be an invertible T-algebra. If $(Q;\Sigma)$ satisfies the following second-order formula:*

$$\forall X_1,X_2\,\forall x_1,x_2,x_3\,\exists x_4$$
$$\big(X_1\big(X_2(x_1,x_2),X_2(x_4,x_3)\big)=X_1\big(X_2(x_1,x_4),X_2(x_2,x_3)\big)\big),\tag{22}$$

then in $(Q;\Sigma)$ the following hyperidentity is valid:

$$X_1\big(X_2(x_1,x_2),X_2(x_4,x_3)\big)=X_1\big(X_2(x_1,x_4),X_2(x_2,x_3)\big).$$

Proof. Let $(Q;\Sigma)$ be an invertible T-algebra. Then it satisfies (6). If we rewrite (6), in terms of the operation $+$, then after cancellations we obtain

$$\psi_X\varphi_Y u+\varphi_X\psi_Y y=\varphi_X\psi_Y u+\psi_X\varphi_Y\alpha_u^{X,Y}y\,,\tag{23}$$

which for $u=0$ gives $\varphi_X\psi_Y=\psi_X\varphi_Y\alpha_0^{X,Y}$. This together with (23) implies

$$u+\alpha_0^{X,Y}y=\alpha_0^{X,Y}u+\alpha_u^{X,Y}y\,,\tag{24}$$

where $\alpha_0^{X,Y}$ is the permutation which corresponds to the identity element of the group, $(Q;+)$.

If (22) is valid in $(Q;\Sigma)$, then for every $X,Y\in\Sigma$ and every $x,y,v\in Q$ there exists an element $h\in Q$ such that the following equality is valid:

$$X(Y(x,y,Y(h,v))=X(Y(x,h),Y(y,v)).$$

Therefore, $\alpha_h^{X,Y}$ is the identity permutation of the set Q.

From the proof of Theorem 2.1, it follows that the loops $x \underset{X}{+} y = X\big(R_{X,a}^{-1}x, L_{X,b}^{-1}y\big)$ are groups for all $a, b \in Q$ and all operations $X \in \Sigma$ and also, we can take any of the groups, $\underset{X}{+}$ $(X \in \Sigma)$ as a group $+$.

Let us choose the elements a, b such that $h = Y(b, a)$ is an identity element of the group $(Q; +)$, then $\alpha_h^{X,Y}$ is the identity permutation of the set Q. Therefore, from (24), we have $\alpha_u^{X,Y} y = y$ since $\alpha_0^{X,Y} = \alpha_h^{X,Y}$ is the identity permutation. Hence $\alpha_u^{X,Y}$ is the identity permutation for all $u \in Q$ and all $X, Y \in \Sigma$. □

Corollary 3.2. *The quasigroup, $(Q; \cdot)$, is a T-quasigroup iff formulae* (6) *and* (14) *are valid in the quasigroup, $(Q; \cdot, /, \backslash)$, for all $X, Y \in \{\cdot, \backslash, /\}$.*

References

[1] **J. Aczel**, *Yorlesungen uber funktionalgleichungen und ihre anwendungem*, Berlin, VEB Deutseh. Verl. Wiss. (1961).

[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, Moskow (1967).

[4] **V.D. Belousov**, *Systems of quasigroups with generalised identities*, Uspekhi Mat. Nauk, **20** (1965), no. 1, 75 – 146.

[5] **G.B. Belyavskaya**, *T-quasigroups and the center of a quasigroup*, (Russian), Math. Issled. **111** (1989), 24 – 43.

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

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

[8] **R.H. Bruck**, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. **55** (1944), 19 – 52.

[9] **J. Ježek, T. Kepka**, *Medial groupoids*, Rozpravy CSAV 93/2, Academia, Praha (1983).

[10] **T. Kepka, P. Némec**, *T-quasigroups. Part I*, Acta Univ. Carolinae Mat. et Phys. **12** (1971), no. 1, 39 – 49.

[11] **T. Kepka, P. Nemec**, *T-quasigroups. Part II*, Acta Univ. Carolinae Mat. et Phys. **12** (1971), no. 2, 31 – 49.

[12] **Yu.M. Movsisyan**, *Introduction to the theory of algebras with hyperidentities*, (Russian), Yerevan State University Press, Yerevan (1986).

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

[14] **Yu.M. Movsisyan**, *Hyperidentities and hypervarieties*, Sci. Math. Japonicae **54** (2001), 595 – 640.

[15] **Yu.M. Movsisyan**, *Hyperidentities in algebras and varieties*, Uspekhi. Mat. Nauk **53** (1998), 61−114; English transl. in Russian Math. Surveys **53** (1998), 57 – 108.

[16] **D.C. Murdoch**, *Structure of abelian quasigroups*, Trans. Amer. Math. Soc. **47** (1941), 134 – 138.

[17] **A.B. Romanowska, J.D.H. Smith**, *Modes*, World Scientific, Singapore (2002).

[18] **A. Sade**, *Theórie des systèmes demosiens de groupoides*, Pacif. J. Math. **10** (1960), 625 – 660.

[19] **R. Schauffler**, *Uber die Bildung von Codewörten*, Arch. Elektr. Uebertragung. **10** (1956), 303 – 314.

[20] **R. Schauffler**, *Die Assoziativität im Ganzen besonders bei quasigruppen*, Math. Zeitschr. **67** (1957), 428 – 435.

[21] **K. Toyoda**, *On axioms of linear functions*, Proc. Imp. Acad. Tokyo **17** (1941), 221 – 227.

Received March 28, 2011

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

Quasigroups and Related Systems **19** (2011), 223 – 226

Indicators of quasigroups

Ivan I. Deriyenko

Abstract. We present some useful conditions which are necessary for isotopy of two quasigroups of the same finite order.

Let $Q = \{1, 2, 3, \ldots, n\}$ be a finite set, S_n – the set of all permutations of Q. The multiplication (composition) of permutations φ and ψ of Q is defined as $\varphi\psi(x) = \varphi(\psi(x))$. All permutations will be written in the form of cycles and cycles will be separated by points, e.g.

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix} = (132.45.6.)$$

By a *cyclic type* of a permutation $\varphi \in S_n$ 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

$$C(\varphi) = \{l_1, l_2, ..., l_n\}.$$

Obviously, $\sum_{i=1}^{n} i \cdot l_i = n$.

Definition 1. By the *indicator* of a permutation φ of type $C(\varphi) = \{l_1, l_2, ..., l_n\}$ we mean the polynomial

$$w(\varphi) = x_1^{l_1} x_2^{l_2} \cdots x_n^{l_n}.$$

For example, for $\varphi = (123.45.6.)$ we have $C(\varphi) = \{1, 1, 1, 0, 0, 0\}$ and $w(\varphi) = x_1 x_2 x_3$; for $\psi = (1.2536.47.80.9.)$, $C(\psi) = \{2, 2, 0, 1, 0, 0, 0, 0, 0, 0\}$ and $w(\psi) = x_1^2 x_2^2 x_4$.

As it is well-known, two permutations $\varphi, \psi \in S_n$ are *conjugate* if there exists a permutation $\rho \in S_n$ such that

$$\rho\varphi\rho^{-1} = \psi.$$

2010 Mathematics Subject Classification: 20N20, 05B15
Keywords: quasigroup, isotopy, autotopy.

Theorem 1. (Theorem 5.1.3 in [4]) *Two permutations are conjugate if and only if they have the same cyclic type.* □

As a consequence we obtain

Corollary 1. *Conjugated permutations have the same indicators.* □

As it is well-known, two quasigroups $Q(\circ)$ and $Q(\cdot)$ are *isotopic* if there are three permutations α, β, γ of Q such that

$$\gamma(x \circ y) = \alpha(x) \cdot \beta(y)\,. \tag{1}$$

In the case $\alpha = \beta = \gamma$ we say that quasigroups are *autotopic*.

A *track* (or a *right middle translation*) of a quasigroup $Q(\cdot)$ is a permutation φ_i of Q satisfying the identity

$$x \cdot \varphi_i(x) = i,$$

where $i \in Q$. Each quasigroup can be identified with the set $\{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ of all its tracks (cf. [2]).

Tracks of $Q(\cdot)$ will be denoted by φ_i, track of $Q(\circ)$ by ψ_1. Similarly, left and right translations of $Q(\cdot)$ will be denoted by L_a and R_a, left and right translations of $Q(\circ)$ by L_a° and R_a°.

Proposition 1. (cf. [2]) *Tracks of isotopic quasigroups satisfying* (1) *are connected by the formula*

$$\varphi_{\gamma(i)} = \beta\psi_i\alpha^{-1}. \tag{2}$$

Similar results hold for left and right translations.

Theorem 2. *Left and right translations of isotopic quasigroups satisfying* (1) *are connected by the conditions*

$$L_{\alpha(a)} = \gamma L_a^\circ \beta^{-1}, \qquad R_{\beta(b)} = \gamma R_b^\circ \alpha^{-1}. \tag{3}$$

Proof. Indeed, putting $x = a$ we obtain $\gamma L_a^\circ(y) = L_{\alpha(a)}\beta(y)$ for every $y \in Q$, which implies $\gamma L_a^\circ \beta^{-1} = L_{\alpha(a)}$. Similarly, putting in (1) $y = b$ we obtain $R_{\beta(b)} = \gamma R_b^\circ \alpha^{-1}$. □

Corollary 2. *For autotopic quasigroups we have*

$$\varphi_{\alpha(i)} = \alpha\psi_i\alpha^{-1}, \qquad L_{\alpha(a)} = \alpha L_a^\circ \alpha^{-1}, \qquad R_{\alpha(b)} = \alpha R_b^\circ \alpha^{-1}. \tag{4}$$

Consider the following three matrices:

$$\Phi = [\varphi_{ij}], \qquad L = [L_{ij}], \qquad R = [R_{ij}],$$

where $\varphi_{ij} = \varphi_i\varphi_j^{-1}$, $L_{ij} = L_iL_j^{-1}$, $R_{ij} = R_iR_j^{-1}$ for all $i, j \in Q$. Obviously, $\varphi_{ii}(x) = L_{ii}(x) = R_{ii}(x) = x$ and $\varphi_{ij}(x) \neq x$, $L_{ij}(x) \neq x$, $R_{ij}(x) \neq x$ for all $i, j, x \in Q$ and $i \neq j$.

Theorem 3. *For isotopic quasigroups $Q(\circ)$ and $Q(\cdot)$ with the isotopy of the form* (1) *we have*

$$\varphi_{\gamma(i)\gamma(j)} = \beta\psi_{ij}\beta^{-1}, \qquad L_{\alpha(i)\alpha(j)} = \gamma L^{\circ}_{ij}\gamma^{-1}, \qquad R_{\beta(i)\beta(j)} = \gamma R^{\circ}_{ij}\gamma^{-1}.$$

Proof. Indeed, using (2) we obtain

$$\varphi_{\gamma(i)\gamma(j)} = \varphi_{\gamma(i)}\varphi^{-1}_{\gamma(j)} = (\beta\psi_i\alpha^{-1})(\beta\psi_j\alpha^{-1})^{-1} = \beta\psi_i\psi_j^{-1}\beta^{-1} = \beta\psi_{ij}\beta^{-1}.$$

In a similar way, using (3), we obtain the other two equations. □

Definition 2. By the *indicator of the matrix* Φ we mean the polynomial

$$w(\Phi) = \sum_{i=1}^{n} w(\Phi_i),$$

where $\Phi_i = \{\varphi_{i1}, \varphi_{i2}, \ldots, \varphi_{in}\}$ and $w(\Phi_i) = \sum\limits_{j=1,\, j\neq i}^{n} w(\varphi_{ij})$.

Indicators of the matrices L and M are defined analogously.

Example 1. Consider two quasigroups defined by the following tables:

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

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

For the quasigroup $Q(\cdot)$ we have:

$$\varphi_1 = (126.354.) \qquad \varphi_2 = (146523.) \qquad \varphi_3 = (1634.2.5.)$$
$$\varphi_4 = (1.2536.4.) \qquad \varphi_5 = (15642.3.) \qquad \varphi_6 = (13245.6.).$$

Thus,

$$\varphi_{11} = (1.2.3.4.5.6.) \qquad \varphi_{12} = (15.24.36.) \qquad \varphi_{13} = (13.26.45.)$$
$$\varphi_{14} = (12.34.56.) \qquad \varphi_{15} = (164.235.) \qquad \varphi_{16} = (146.253.).$$

Consequently,

$$w(\varphi_{11}) = x_1^6, \quad w(\varphi_{12}) = w(\varphi_{13}) = w(\varphi_{14}) = x_2^3, \quad (\varphi_{15}) = w(\varphi_{16}) = x_3^2.$$

Hence $w(\Phi_1) = 3x_2^3 + 2x_3^2$.

By analogous computations we can see that for this quasigroup

$$w(\Phi) = w(L) = w(R) = 6(3x_2^3 + 2x_3^2).$$

For the second quasigroup we obtain:

$$w(\Phi) = (2x_2x_4+6x_2^3+2x_6)+(x_2^3+2x_3^2+2x_6)+2(x_2x_4+x_2^3+3x_6)+2(2x_3^2+3x_6),$$

$$w(L) = w(R) = 2(x_2x_4 + 4x_6) + 2(2x_2x_4 + x_3^2 + 2x_6)\,. \qquad \square$$

As a consequence of our Theorem 3 and Corollary 1 we obtain

Theorem 4. *Isotopic quasigroups have the same indicators of the matrices* Φ*,* L *and* R*.* $\square$

This theorem shows that quasigroups from the above example are not isotopic.

Corollary 3. *For quasigroups of order* n *isotopic to a group we have* $w(\Phi) = nw(\Phi_1)$*.*

Proof. In [2] it is proved that for a quasigroup isotopic to a group all its Φ_i are groups isomorphic to Φ_1. Hence $w(\Phi_i) = w(\Phi_1)$ for every $i \in Q$. $\square$

There are examples proving that the contrary is not true.

References

[1] **I.I. Deriyenko**, *Necessary conditions of the isotopy of finite quasigroups*, (Russian), Mat. Issled. **120** (1991), 51 – 63.

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

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

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

Received December 2, 2011

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

Quasigroups and Related Systems **19** (2011), 227 – 238

On ordered fuzzy Γ-groupoids

Niovi Kehayopulu

Abstract. This paper serves as an example to show the way we pass from fuzzy ordered groupoids (semigroups) to fuzzy ordered Γ-groupoids (semigroups). All the results on fuzzy ordered groupoids (semigroups) can be transferred to fuzzy ordered Γ-groupoids (semigroups) in the way indicated in the present paper.

1. Introduction and prerequisites

The notion of a Γ-ring, a generalization of the notion of associative rings, has been introduced and studied by N. Nobusawa in [10]. Γ-rings have been also studied by W. E. Barnes in [1]. J. Luh studied many properties of simple Γ-rings and primitive Γ-rings in [9]. The concept of a Γ-semigroup has been introduced by M. K. Sen in 1981 as follows: Given a nonempty set Γ, a nonempty set M is called a Γ-semigroup if the following assertions are satisfied: (1) $a\alpha b \in M$ and $\alpha a\beta \in \Gamma$ and (2) $(a\alpha b)\beta c = a(\alpha b\beta)c = a\alpha(b\beta c)$ for all $a, b, c \in M$ and all $\alpha, \beta \in \Gamma$ [12]. In 1986, M. K. Sen and N. K. Saha changed that definition as follows: Given two nonempty sets M and Γ, M is called a Γ-semigroup if (1) $a\alpha b \in M$ and (2) $(a\alpha b)\beta c = a\alpha(b\beta c)$ for all $a, b, c \in M$ and all $\alpha, \beta \in \Gamma$ [13]. One can find that definition of Γ-semigroups in [16], where the notion of radical in Γ-semigroups and the notion of $\Gamma\mathcal{S}$-act over a Γ-semigroup have been introduced, in [14] and [15], where the notions of regular and orthodox Γ-semigroups have been introduced and studied. With that second definition, a semigroup $(S, .)$ can be viewed as a particular case of a Γ-semigroup, considering $\Gamma = \{\gamma\}$ $(\gamma \notin S)$ and defining $a\gamma b := a.b$. Moreover, let M be a Γ-semigroup, take a (fixed) $\gamma \in \Gamma$, and define $a\,.b := a\gamma b$, then $(M, .)$ is a semigroup. Later, in [11], Saha calls a nonempty set M a Γ-semigroup $(\Gamma \neq \emptyset)$ if there is a mapping $M \times \Gamma \times M \to M \mid (a, \gamma, b) \to a\gamma b$ such that $(a\alpha b)\beta c = a\alpha(b\beta c)$

2010 Mathematics Subject Classification: 06F99.
Keywords: Fuzzy Γ-groupoid (semigroup), ordered Γ-groupoid (semigroup), fuzzy subset, fuzzy right (left) ideal, fuzzy ideal, fuzzy quasi-ideal, fuzzy bi-ideal, regular, intra-regular ordered fuzzy Γ-semigroup.

for all $a, b, c \in M$ and all $\alpha, \beta \in \Gamma$, and remarks that the most usual semigroup concepts, in particular regular and inverse Γ-semigroups have their analogous in Γ-semigroups. The uniqueness condition was missing from the definition of a Γ-semigroup given in [12], [13]. If we add the uniqueness condition in the definition of a Γ-semigroup given by Sen and Saha in [13] (that is, considering Γ as a set of binary relations on M) we do not need to define it via mapping. So the definition of a Γ-semigroup given by Sen and Saha in 1986 can be formulated as follows:

For two nonempty sets M and Γ, define $M\Gamma M$ as the set of all elements of the form $m_1\gamma m_2$, where $m_1, m_2 \in M$ and $\gamma \in \Gamma$. That is,

$$M\Gamma M := \{m_1\gamma m_2 \mid m_1, m_2 \in M,\ \gamma \in \Gamma\}.$$

Definition 1. (cf. [2]–[5]) Let M and Γ be two nonempty sets. The set M is called a Γ-*groupoid* if the following assertions are satisfied:

(1) $M\Gamma M \subseteq M$.

(2) If $m_1, m_2, m_3, m_4 \in M$, $\gamma_1, \gamma_2 \in \Gamma$ such that $m_1 = m_3$, $\gamma_1 = \gamma_2$ and $m_2 = m_4$, then $m_1\gamma_1 m_2 = m_3\gamma_2 m_4$.

M is called a Γ-*semigroup* if, in addition, the following assertion holds:

(3) $(m_1\gamma_1 m_2)\gamma_2 m_3 = m_1\gamma_1(m_2\gamma_2 m_3)$

for all $m_1, m_2, m_3 \in M$ and all $\gamma_1, \gamma_2 \in \Gamma$. In other words, Γ is a set of binary operations on M satisfying (3).

According to that "associativity", each of the elements $(m_1\gamma_1 m_2)\gamma_2 m_3$, and $m_1\gamma_1(m_2\gamma_2 m_3)$ is denoted as $m_1\gamma_1 m_2\gamma_2 m_3$.

Using conditions $(1) - (3)$ one can prove that for an element with more than 5 words, for example of the form $m_1\gamma_1 m_2\gamma_2 m_3\gamma_3 m_4$, one can put a parenthesis in any expression beginning with some m_i and ending in some m_j.

There are several examples of Γ-semigroups in the bibliography. However, the example below based on Definition 1 above, shows clearly what a Γ-semigroup is.

Example 2. (cf. [3]) Consider the set $M = \{a, b, c, d\}$, and let $\Gamma = \{\gamma, \mu\}$ be the set of two binary operations on M defined in the tables below:

γ	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

μ	a	b	c	d
a	b	c	d	a
b	c	d	a	b
c	d	a	b	c
d	a	b	c	d

Since $(x\rho y)\omega z = x\rho(y\omega z)$ for all $x, y, z \in M$ and all $\rho, \omega \in \Gamma$, M is a Γ-semigroup.

An *ordered* Γ-*groupoid* (shortly *po*-Γ-*groupoid*) is a Γ-groupoid M together with an order relation $\leqslant$ on M such that $a \leqslant b$ implies $a\gamma c \leqslant b\gamma c$ and $c\gamma a \leqslant c\gamma b$ for all $c \in M$ and all $\gamma \in \Gamma$ (cf. also Sen and Seth [17]).

We have already seen in [2]–[5] that all the results on ordered groupoids or ordered semigroups based on ideals or ideal elements can be transferred to ordered Γ-groupoids or ordered Γ-semigroups. In the same way all the results on groupoids or semigroups (without order) based on ideals can be transferred to Γ-groupoids or Γ-semigroups. In the present paper we show that all the results on fuzzy ordered groupoids or semigroups can be transferred to fuzzy ordered Γ-groupoids or semigroups, respectively. The present paper serves as an example to show the way we pass from fuzzy ordered groupoids or fuzzy ordered semigroups to fuzzy ordered Γ-groupoids or fuzzy ordered Γ-semigroups.

There are two equivalent definitions of fuzzy left ideals, fuzzy right ideals, fuzzy quasi-ideals and fuzzy bi-ideals in ordered semigroups. The first one is in term of the fuzzy subset f itself, the second is based on the multiplication of fuzzy sets. The second one shows how similar is the theory of ordered semigroups based on fuzzy ideals with the theory of ordered semigroups based on ideals or ideal elements and it is very useful for applications. Using that second definition the results on fuzzy ordered semigroups or on fuzzy semigroups (without order) can be drastically simplified (cf. also [2]). In the present paper we examine these equivalent definitions in case of ordered fuzzy Γ-groupoids and ordered fuzzy Γ-semigroups. Characterizations of regular and intra-regular ordered semigroups in terms of fuzzy sets have been given in [7]. In the present paper we also characterize the regular and intra-regular ordered Γ-semigroups in terms of fuzzy sets. In a similar way one can prove that the characterizations of π-regular and intra π-regular ordered semigroups considered in [7] have their analogue for ordered Γ-semigroups.

2. Main results

Following the terminology given by L.A. Zadeh [18], if $(M, ., \leqslant)$ is an ordered Γ-groupoid, we say that f is a fuzzy subset of M (or a fuzzy set in M) if f is a mapping of M into the real closed interval [0,1]. For a subset A of M, the fuzzy subset f_A is defined as follows:

$$f_A : M \to [0,1] \mid x \to f_A(x) := \begin{cases} 1 & if \ \ x \in A \\ 0 & if \ \ x \notin A. \end{cases}$$

For an element a of M, we clearly have

$$f_a : M \to [0,1] \mid x \to f_a(x) := \begin{cases} 1 & if \ \ x = a \\ 0 & if \ \ x \neq a. \end{cases}$$

For an element a of M, denote by A_a the relation on M defined by

$$A_a := \{(y,z) \mid a \leqslant y\gamma z \text{ for some } \gamma \in \Gamma\}.$$

For two fuzzy subsets f and g of M, we define the multiplication of f and g as follows:

$$f \circ g : M \to [0,1] \mid a \to \begin{cases} \sup\limits_{(y,z)\in A_a} \{\min f(y), g(z)\} & \text{if} \ \ A_a \neq \emptyset \\ 0 \quad \text{if} \ \ A_a = \emptyset \end{cases}$$

and in the set of all fuzzy subsets of M we define the order relation as follows:

$$f \preceq g \text{ if and only if } f(x) \leqslant g(x) \text{ for all } x \in M.$$

For two fuzzy subsets f and g of M, let $f \wedge g$ be the fuzzy subset of M defined by:

$$f \wedge g : M \to [0,1] \mid x \to \min\{f(x), g(x)\}.$$

Denote by 1 the fuzzy subset of M defined by

$$1 : M \to [0,1] \mid x \to 1(x) := 1.$$

Denote by f^2 the composition $f \circ f$. If $F(M)$ is the set of fuzzy subsets of M, it is clear that the fuzzy subset 1 of M is the greatest element of the ordered set $(F(M), \preceq)$. In a similar way as in [6] (using the methodology of the present paper) one can prove that if M is an ordered Γ-semigroup and f, g, h fuzzy subsets of M, then $(f \circ g) \circ h = f \circ (g \circ h)$.

Definition 3. Let M be an ordered Γ-groupoid. A fuzzy subset f of M is called a *fuzzy right ideal* of M if

(1) $f(x\gamma y) \geqslant f(x)$ for all $x, y \in M$ and all $\gamma \in \Gamma$,

(2) if $x \leqslant y$, then $f(x) \geqslant f(y)$.

A fuzzy subset f of M is called a *fuzzy left ideal* of M if

(1) $f(x\gamma y) \geqslant f(y)$ for all $x, y \in M$ and all $\gamma \in \Gamma$,

(2) if $x \leqslant y$, then $f(x) \geqslant f(y)$.

Definition 4. Let M be an ordered Γ-groupoid. A fuzzy subset f of M is called a *fuzzy quasi-ideal* of M if

(1) $(f \circ 1) \wedge (1 \circ f) \preceq f$,

(2) if $x \leqslant y$, then $f(x) \geqslant f(y)$.

Definition 5. Let M be an ordered Γ-semigroup. A fuzzy subset f of M is called a *fuzzy bi-ideal* of M if

(1) $f(x\gamma y\mu z) \geqslant \min\{f(x), f(z)\}$ for all $x, y, z \in M$ and all $\gamma, \mu \in \Gamma$,

(2) if $x \leqslant y$, then $f(x) \geqslant f(y)$.

Theorem 6. *Let M be an ordered Γ-groupoid. A fuzzy subset f of M is a fuzzy right ideal of M if and only if*

(1) $f \circ 1 \preceq f$,

(2) *if $x \leqslant y$, then $f(x) \geqslant f(y)$.*

Proof. ($\Longrightarrow$) Let $a \in M$. Then $(f \circ 1)(a) \leqslant f(a)$. In fact: If $A_a = \emptyset$, then $(f \circ 1)(a) := 0 \leqslant f(a)$. Let $A_a \neq \emptyset$. Then

$$(f \circ 1)(a) := \sup_{(y,z)\in A_a} \{\min\{f(y), 1(z)\}\} = \sup_{(y,z)\in A_a} \{f(y)\}.$$

On the other hand, $f(y) \leqslant f(a)$ for every $(y, z) \in A_a$. Indeed: If $(y, z) \in A_a$, then $y, z \in M$ and $a \leqslant y\gamma z$ for some $\gamma \in \Gamma$. Since f is a fuzzy right ideal of M, we have $f(a) \geqslant f(y\gamma z) \geqslant f(y)$. Therefore we have

$$(f \circ 1)(a) = \sup_{(y,z)\in A_a} \{f(y)\} \leqslant f(a).$$

($\Longleftarrow$) Let $x, y \in M$ and $\gamma \in \Gamma$. By hypothesis, we have $(f \circ 1)(x\gamma y) \leqslant f(x\gamma y)$. On the other hand, since $(x, y) \in A_{x\gamma y}$, we have

$$(f \circ 1)(x\gamma y) := \sup_{(u,v)\in A_{x\gamma y}} \{\min\{f(u), 1(v)\}\} \geqslant \min\{f(x), 1(y)\} = f(x).$$

Hence we obtain $f(x\gamma y) \geqslant f(x)$, and f is a fuzzy right ideal of M. □

In a similar way we prove the following theorem

Theorem 7. *Let M be an ordered Γ-groupoid. A fuzzy subset f of M is a fuzzy left ideal of M if and only if*

(1) $1 \circ f \preceq f$,

(2) *if* $x \leqslant y$, *then* $f(x) \geqslant f(y)$. □

Theorem 8. *Let M be an ordered Γ-groupoid. A fuzzy subset f of M is a fuzzy quasi-ideal of M if and only if the following conditions are satisfied:*

(1) *if* $x \leqslant b\gamma s$ *and* $x \leqslant t\mu c$ *for some* $x, b, s, t, c \in M$ *and* $\gamma, \mu \in \Gamma$, *then* $f(x) \geqslant \min\{f(b), f(c)\}$,

(2) *if* $x \leqslant y$, *then* $f(x) \geqslant f(y)$.

Proof. ($\Longrightarrow$) Let $x, b, s, t, c \in M$ and $\gamma, \mu \in \Gamma$ such that $x \leqslant b\gamma s$ and $x \leqslant t\mu c$. Since f is a fuzzy quasi-ideal of M, we have

$$f(x) \geqslant ((f \circ 1) \wedge (1 \circ f))(x) := \min\{(f \circ 1)(x), (1 \circ f)(x)\}.$$

Since $x \leqslant b\gamma s$, we have $(b, s) \in A_x$, then

$$(f \circ 1)(x) := \sup_{(u,v) \in A_x} \{\min\{f(u), 1(v)\}\} \geqslant \min\{f(b), 1(s)\} = f(b).$$

Similarly from $x \leqslant t\mu c$, we get $(1 \circ f)(x) \geqslant f(c)$. Hence we have

$$f(x) \geqslant \min\{(f \circ 1)(x), (1 \circ f)(x)\} \geqslant \min\{f(b), f(c)\}.$$

($\Longleftarrow$) Let $x \in M$. Then $((f \circ 1) \wedge (1 \circ f))(x) \leqslant f(x)$. In fact: We have

$$((f \circ 1) \wedge (1 \circ f))(x) := \min\{(f \circ 1)(x), (1 \circ f)(x)\}.$$

1. If $A_x = \emptyset$, then $(f \circ 1)(x) := 0$ and $(1 \circ f)(x) := 0$. Moreover $\min\{(f \circ 1)(x), (1 \circ f)(x)\} = 0$, and $((f \circ 1) \wedge (1 \circ f))(x) = 0 \leqslant f(x)$.

2. Let $A_x \neq \emptyset$. Then

$$(f \circ 1)(x) := \sup_{(y,s) \in A_x} \{\min\{f(y), 1(s)\}\} \qquad (\star)$$

$$(1 \circ f)(x) := \sup_{(t,z) \in A_x} \{\min\{1(t), f(z)\}\}.$$

2.1. If $f(x) \geqslant (f \circ 1)(x)$, then

$$\begin{aligned} f(x) &\geqslant (f \circ 1)(x) \geqslant \min\{(f \circ 1)(x), (1 \circ f)(x)\} \\ &= ((f \circ 1) \wedge (1 \circ f))(x). \end{aligned}$$

2.2. Let $f(x) < (f \circ 1)(x)$. By $(*)$, there exists $(y, s) \in A_x$ such that $\min\{f(y), 1(s)\} > f(x)$ (otherwise $(f \circ 1)(x) \leqslant f(x)$ which is impossible). Since $\min\{f(y), 1(s)\} = f(y)$, we have

$$f(y) > f(x). \qquad (\star\star)$$

On the other hand, $f(x) \geqslant \min\{1(t), f(z)\}$ for every $(t, z) \in A_x$. Indeed: Let $(t, z) \in A_x$. Since $(y, s) \in A_x$, we have $y, s \in M$ and $x \leqslant y\gamma s$ for some $\gamma \in \Gamma$. Since $(t, z) \in A_x$, we have $t, z \in M$ and $x \leqslant t\mu z$ for some $\mu \in \Gamma$. Since $x, y, s, t, z \in M$ and $\gamma, \mu \in \Gamma$ such that $x \leqslant y\gamma s$ and $x \leqslant t\mu z$, by hypothesis, we have $f(x) \geqslant \min\{f(y), f(z)\}$. If $\min\{f(y), f(z)\} = f(y)$, then $f(x) \geqslant f(y)$ which is impossible by $(**)$. Thus we have $\min\{f(y), f(z)\} = f(z)$, and $f(x) \geqslant f(z) = \min\{1(t), f(z)\}$. Therefore we have

$$\begin{aligned} f(x) &\geqslant \sup_{(t,z)\in A_x} \{\min\{1(t), f(z)\} = (1 \circ f)(x) \\ &\geqslant \min\{(f \circ 1)(x), (1 \circ f)(x)\} = ((f \circ 1) \wedge (1 \circ f))(x), \end{aligned}$$

and the proof is complete. □

By Theorem 8, in a similar way as in [8], one can prove the following theorem.

Theorem 9. *Let M be an ordered Γ-groupoid. A fuzzy subset f of M is a fuzzy quasi-ideal of M if and only if the following conditions are satisfied:*

(1) *if $x \leqslant b\gamma s$ and $x \leqslant t\mu c$ for some $x, b, s, t, c \in M$ and $\gamma, \mu \in \Gamma$, then $f(x) \geqslant \max\{\min\{f(b), f(c)\}, \min\{f(t), f(s)\}\}$,*

(2) *if $x \leqslant y$, then $f(x) \geqslant f(y)$.* □

Theorem 10. *Let M be an ordered Γ-semigroup. A fuzzy subset f of M is a fuzzy bi-ideal of M if and only if the following assertions are satisfied:*

(1) $f \circ 1 \circ f \preceq f$,

(2) *if $x \leqslant y$, then $f(x) \geqslant f(y)$.*

Proof. $(\Longrightarrow)$ Let $a \in S$. Then $(f \circ 1 \circ f)(a) \leqslant f(a)$. In fact: If $A_a = \emptyset$ then $(f \circ 1 \circ f)(a) = ((f \circ 1) \circ f)(a) := 0 \leqslant f(a)$. Let $A_a \neq \emptyset$. Then

$$(f \circ 1 \circ f)(a) := \sup_{(y,z)\in A_a} \{\min\{(f \circ 1)(y), f(z)\}\}.$$

It is enough to prove that

$$\min\{(f \circ 1)(y), f(z)\} \leqslant f(a) \text{ for every } (y,z) \in A_a. \qquad (\star)$$

Let now $(y,z) \in A_a$. If $A_y = \emptyset$, then $(f \circ 1)(y) := 0$, and

$$\min\{(f \circ 1)(y), f(z)\} = 0 \leqslant f(a).$$

Let $A_y \neq \emptyset$. Then

$$(f \circ 1)(y) := \sup_{(s,t) \in A_y} \{\min\{f(s), 1(t)\}.\} \qquad (\star\star)$$

We consider the following two cases:

1. Let $f(a) \geqslant (f \circ 1)(y)$. Then

$$f(a) \geqslant (f \circ 1)(y) \geqslant \min\{(f \circ 1)(y), f(z)\},$$

and condition $(*)$ is satisfied.

2. Let $f(a) < (f \circ 1)(y)$. Then, by $(**)$, there exists $(x,w) \in A_y$ such that $f(a) < \min\{f(x), 1(w)\}$ (otherwise, $f(a) \geqslant (f \circ 1)(y)$ which is impossible). Since $\min\{f(x), 1(w)\} = f(x)$, we have

$$f(a) < f(x).$$

Since $(y,z) \in A_a$, we have $y, z \in M$ and $a \leqslant y\mu z$ for some $\mu \in \Gamma$. Since $(x,w) \in A_y$, we have $x, w \in M$ and $y \leqslant x\gamma w$ for some $\gamma \in \Gamma$. Since $a \leqslant y\mu z \leqslant x\gamma w\mu z$ and f is a fuzzy bi-ideal of S, by the definition of fuzzy bi-ideal, we have

$$f(a) \geqslant f(x\gamma w\mu z) \geqslant \min\{f(x), f(z)\}.$$

If $f(x) \leqslant f(z)$, then $\min\{f(x), f(z)\} = f(x)$, and $f(a) \geqslant f(x)$ which is impossible. Hence we have $f(x) > f(z)$. Then $\min\{f(x), f(z)\} = f(z)$, and $f(a) \geqslant f(z)$. Since $(x,w) \in A_y$, by $(**)$, we have

$$\min\{f(x), 1(w)\} \leqslant \sup_{(s,t) \in A_y} \{\min\{f(s), 1(t)\}\} = (f \circ 1)(y).$$

Then we have $(f \circ 1)(y) \geqslant \min\{f(x), 1(w)\} = f(x) > f(z)$. Consequently $\min\{(f \circ 1)(y), f(z)\} = f(z) \leqslant f(a)$, and condition $(*)$ is satisfied.

($\Longleftarrow$) Let $x, y, z \in M$ and $\gamma, \mu \in \Gamma$. Then $f(x\gamma y\mu z) \geqslant \min\{f(x), f(z)\}$. Indeed: Since $f \circ 1 \circ f \preceq f$ and $x\gamma y\mu z \in M$, we have $(f \circ 1 \circ f)(x\gamma y\mu z) \leqslant f(x\gamma y\mu z)$. Since $x\gamma y\mu z \leqslant (x\gamma y)\mu z$, $\mu \in \Gamma$, we have $(x\gamma y, z) \in A_{x\gamma y\mu z}$. Then

$$\begin{aligned}(f \circ 1 \circ f)(x\gamma y\mu z) &:= \sup_{(u,v)\in A_{x\gamma y\mu z}} \{\min\{(f \circ 1)(u), f(v)\}\} \\ &\geqslant \min\{(f \circ 1)(x\gamma y),\, f(z)\}.\end{aligned}$$

Since $(x, y) \in A_{x\gamma y}$, we have

$$(f \circ 1)(x\gamma y) := \sup_{(z,w)\in A_{x\gamma y}} \{\min\{(f(z), 1(w)\}\} \geqslant \min\{f(x),\, 1(y)\} = f(x).$$

Thus $f(x\gamma y\mu z) \geqslant \min\{(f \circ 1)(x\gamma y), f(z)\} \geqslant \min\{f(x), f(z)\}$. □

Definition 11. An ordered Γ-semigroup M is called *regular* if for every $a \in M$ there exist $x \in M$ and $\gamma, \mu \in \Gamma$ such that $a \leqslant a\gamma x\mu a$.

In a similar way as in [8] we prove the following lemma and the two corollaries below:

Lemma 12. *Let M be an ordered Γ-groupoid, f, g fuzzy subsets of M and $a \in M$. 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 $g(y) \neq 0$.* □

Corollary 13. *Let M be an ordered Γ-groupoid, f a fuzzy subset of M and $a \in M$. The following are equivalent:*

(1) $(f \circ 1)(a) \neq 0$.

(2) *There exists $(x, y) \in A_a$ such that $f(x) \neq 0$.* □

Corollary 14. *Let M be an ordered Γ-groupoid, g a fuzzy subset of M and $a \in M$. 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 15. *An ordered Γ-semigroup M is regular if and only if for every fuzzy subset f of M we have $f \preceq f \circ 1 \circ f$.*

Proof. ($\Longrightarrow$) Let f be a fuzzy subset of M and $a \in M$. Since M is regular, there exist $x \in M$ and $\gamma, \mu \in \Gamma$ such that $a \leqslant a\gamma x\mu a$. Since $a \leqslant (a\gamma x)\mu a$,

where $\mu \in \Gamma$, we have $(a\gamma x, a) \in A_a$. Then we have

$$(f \circ 1 \circ f)(a) := \sup_{(y,z)\in A_a} \{\min\{(f \circ 1)(y), f(z)\}\} \geqslant \min\{(f \circ 1)(a\gamma x), f(a)\}.$$

Since $(a, x) \in A_{a\gamma x}$, we have

$$(f \circ 1)(a\gamma x) := \sup_{(u,v)\in A_{a\gamma x}} \{\min\{f(u), 1(v)\}\} \geqslant \min\{f(a), 1(x)\} = f(a).$$

Hence we have $(f \circ 1 \circ f)(a) \geqslant \min\{(f \circ 1)(a\gamma x), f(a)\} = f(a)$.

($\Longleftarrow$) Let $a \in M$. Since f_a is a fuzzy subset of M, by hypothesis, we have $1 = f_a(a) \leqslant (f_a \circ 1 \circ f_a)(a)$. Since $f_a \circ 1 \circ f_a$ is a fuzzy subset of M, we have $(f_a \circ 1 \circ f_a)(a) \leqslant 1$. Then $((f_a \circ 1) \circ f_a)(a) = (f_a \circ 1 \circ f_a)(a) = 1$. By Lemma 12, there exists $(x, y) \in A_a$ such that $(f_a \circ 1)(x) \neq 0$ and $f_a(y) \neq 0$. If $y \neq a$, then $f_a(y) = 0$ which is impossible. Thus we have $y = a$, $(x, a) \in A_a$, and $a \leqslant x\mu a$ for some $\mu \in \Gamma$. If $A_x = \emptyset$, then $(f_a \circ 1)(x) := 0$ which is impossible. Thus we have $A_x \neq \emptyset$, and

$$(f_a \circ 1)(x) := \sup_{(b,c)\in A_x} \{\min\{f_a(b), 1(c)\}\} = \sup_{(b,c)\in A_x} \{f_a(b)\}.$$

If $b \neq a$ for every $(b, c) \in A_x$, then $f_a(b) = 0$ for every $(b, c) \in A_x$, then $(f_a \circ 1)(x) = 0$ which is impossible. Hence there exists $(b, c) \in A_x$ such that $b = a$. Then $(a, c) \in A_x$, so $x \leqslant a\gamma c$ for some $\gamma \in \Gamma$. Then we obtain $a \leqslant x\mu a \leqslant a\gamma c\mu a$, where $c \in M$ and $\gamma, \mu \in \Gamma$, and M is regular. □

Definition 16. An ordered Γ-semigroup M is called *intra-regular* if for every $a \in M$ there exist $x, y \in M$ and $\gamma, \mu, \rho \in \Gamma$ such that $a \leqslant x\gamma a\mu a\rho y$.

Proposition 17. *Let M be an ordered Γ-groupoid and $a, b \in M$. Then we have $b \leqslant a\gamma a$ for some $\gamma \in \Gamma$ if and only if $f_a^2(b) \neq 0$.*

Proof. ($\Longrightarrow$) Let $b \leqslant a\gamma a$ for some $\gamma \in \Gamma$. Since $(a, a) \in A_b$, we have

$$(f_a \circ f_a)(b) := \sup_{(x,y)\in A_b} \{\min\{f_a(x), f_a(y)\}\} \geqslant \min\{f_a(a), f_a(a)\} = 1.$$

($\Longleftarrow$) Since $f_a^2(b) \neq 0$, by Lemma 12, there exists $(x, y) \in A_b$ such that $f_a(a) \neq 0$ and $f_a(y) \neq 0$. Since $f_a(x) \neq 0$, we have $x = a$. Since $f_a(y) \neq 0$, we have $y = a$. Since $b \leqslant x\gamma y$ for some $\gamma \in \Gamma$, we have $b \leqslant a\gamma a$, where $a \in \Gamma$. □

Theorem 18. *An ordered Γ-semigroup M is intra-regular if and only if for every fuzzy subset f of M we have $f \preceq 1 \circ f^2 \circ 1$.*

Proof. ($\Longrightarrow$) Let f be a fuzzy subset of M and $a \in M$. Since M is intra-regular we have $a \leqslant x\gamma a\mu a\rho y$ for some $x, y \in M$ and $\gamma, \mu, \rho \in \Gamma$. Since $(x\gamma a\mu a, y) \in A_a$, we have

$$\begin{aligned}(1 \circ f^2 \circ 1)(a) &:= \sup_{(u,v)\in A_a} \{\min\{(1 \circ f^2)(u), 1(v)\}\} \\ &\geqslant \min\{(1 \circ f^2)(x\gamma a\mu a), 1(y)\} = (1 \circ f^2)(x\gamma a\mu a).\end{aligned}$$

Since $(x, a\mu a) \in A_{x\gamma a\mu a}$, we have

$$\begin{aligned}(1 \circ f^2)(x\gamma a\mu a) &:= \sup_{(s,t)\in A_{a\gamma\alpha\mu\alpha}} \{\min\{1(s), f^2(t)\}\} \\ &\geqslant \min\{1(x), f^2(a\mu a)\} = f^2(a\mu a).\end{aligned}$$

Since $(a, a) \in A_{a\mu a}$, we have

$$\begin{aligned}f^2(a\mu a) = (f \circ f)(a\mu a) &:= \sup_{(w,z)\in A_{\alpha\mu\alpha}} \{\min\{f(w), f(z)\}\} \\ &\geqslant \{f(a), f(a)\} = f(a).\end{aligned}$$

Hence we have

$$f(a) \leqslant f^2(a\mu a) \leqslant (1 \circ f^2)(x\gamma a\mu a) \leqslant (1 \circ f^2 \circ 1)(a).$$

Since $f(a) \leqslant (1 \circ f^2 \circ 1)(a)$ for every $a \in M$, we have $f \preceq 1 \circ f^2 \circ 1$.

($\Longleftarrow$) Let $a \in M$. Since f_a is a fuzzy subset of M, by hypothesis, we have $f_a \preceq 1 \circ f_a^2 \circ 1$. Then $1 = f_a(a) \leqslant (1 \circ f_a^2 \circ 1)(a)$. Since $1 \circ f_a^2 \circ 1$ is a fuzzy subset of M, we have $(1 \circ f_a^2 \circ 1)(a) \leqslant 1$, so $(1 \circ f_a^2 \circ 1)(a) \neq 0$. Then, by Corollary 13, there exists $(w, y) \in A_a$ such that $(1 \circ f_a^2)(w) \neq 0$. By Corollary 14, there exists $(x, t) \in A_w$ such that $f_a^2(t) \neq 0$. By Proposition 17, we have $t \leqslant a\mu a$, for some $\mu \in \Gamma$. Since $(x, t) \in A_w$, $w \leqslant x\gamma t$ for some $\gamma \in \Gamma$. Since $(w, y) \in A_a$, $a \leqslant w\rho y$ for some $\rho \in \Gamma$. Then we obtain $a \leqslant w\rho y \leqslant x\gamma t\rho y \leqslant x\gamma a\mu a\rho y$, where $\gamma, \mu, \rho \in \Gamma$, and M is intra-regular. □

References

[1] **W. E. Barnes**, *On the Γ-rings of Nobusawa*, Pacific J. Math. **18** (1966), 411 – 422.

[2] **N. Kehayopulu**, *On prime, weakly prime ideals in po-*Γ*-semigroups*, Lobachevskii J. Math. **30** (2009), no. 4, 257 – 262.

[3] **N. Kehayopulu**, *On le-*Γ*-semigroups*, Int. Math. Forum **4** (2009), 1915 – 1922.

[4] **N. Kehayopulu**, *On ordered* Γ*-semigroups*, Sci. Math. Jpn. **71** (2010), 179 – 185.

[5] **N. Kehayopulu**, *On regular duo po-*Γ*-semigroups*, Math. Slovaca, to appear.

[6] **N. Kehayopulu, M. Tsingelis**, *The embedding of an ordered groupoid into a poe-groupoid in terms of fuzzy sets*, Inform. Sci. **152** (2003), 231 – 236.

[7] **N. Kehayopulu, M. Tsingelis**, *Characterization of some types of ordered semigroups in terms of fuzzy sets*, Lobachevskii J. Math. **29** (2008), no. 1, 14 – 20.

[8] **N. Kehayopulu, M. Tsingelis**, *Fuzzy right, left, quasi-ideals, bi-ideals in ordered semigroups*, Lobachevskii J. Math. **30** (2009), no. 1, 17 – 22.

[9] **J. Luh**, *On the theory of simple* Γ*-rings*, Michigan Math. J. **16** (1969), 65–75.

[10] **N. Nobusawa**, *On a generalization of the ring theory*, Osaka J. Math. **1** (1964), 81 – 89.

[11] **N. K. Saha**, *The maximum idempotent-separating congruence on an inverse* Γ*-semigroup*, Kyungpook Math. J. **34** (1994), 59 – 66.

[12] **M. K. Sen**, *On* Γ*-semigroup*, Algebra and its applications (New Delhi, 1981), 301 – 308, Lecture Notes in Pure and Appl. Math. **91**, Dekker, New York, 1984.

[13] **M. K. Sen, N. K. Saha**, *On* Γ*-semigroups I*, Bull. Calcutta Math. Soc. **78** (1986), no. 3, 180 – 186.

[14] **M. K. Sen, N. K. Saha**, *The maximum idempotent-separating congruence on an orthodox* Γ*-semigroup*, J. Pure Math. **7** (1990), 39 – 47.

[15] **M. K. Sen, N. K. Saha**, *Orthodox* Γ*-semigroups*, Internat. J. Math. Math. Sci. **13** (1990), 527 – 534.

[16] **M. K. Sen, A. Seth**, *Radical of* Γ*-semigroup*, Bull. Calcutta Math. Soc. **80** (1988), no. 3, 189 – 196.

[17] **M. K. Sen, A. Seth**, *On po-*Γ*-semigroups*, Bull. Calcutta Math. Soc. **85** (1993), no. 5, 445 – 450.

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

Received May 22, 2011

University of Athens, Department of Mathematics, 15784 Panepistimiopolis, Athens, Greece
E-mail: nkehayop@math.uoa.gr

Quasigroups and Related Systems **19** (2011), 239 – 264

Right product quasigroups and loops

Michael K. Kinyon, Aleksandar Krapež and J. D. Phillips

Abstract. Right groups are direct products of right zero semigroups and groups and they play a significant role in the semilattice decomposition theory of semigroups. Right groups can be characterized as associative right quasigroups (magmas in which left translations are bijective). If we do not assume associativity we get right quasigroups which are not necessarily representable as direct products of right zero semigroups and quasigroups. To obtain such a representation, we need stronger assumptions which lead us to the notion of *right product quasigroup*. If the quasigroup component is a (one-sided) loop, then we have a *right product* (*left, right*) *loop*.

We find a system of identities which axiomatizes right product quasigroups, and use this to find axiom systems for right product (left, right) loops; in fact, we can obtain each of the latter by adjoining just one appropriate axiom to the right product quasigroup axiom system.

We derive other properties of right product quasigroups and loops, and conclude by showing that the axioms for right product quasigroups are independent.

1. Introduction

In the semigroup literature (e.g., [1]), the most commonly used definition of *right group* is a semigroup $(S;\cdot)$ which is right simple (*i.e.*, has no proper right ideals) and left cancellative (*i.e.*, $xy = xz \implies y = z$). The structure of right groups is clarified by the following well-known representation theorem (see [1]):

Theorem 1.1. *A semigroup $(S;\cdot)$ is a right group if and only if it is isomorphic to a direct product of a group and a right zero semigroup.* □

There are several equivalent ways of characterizing right groups. One of particular interest is the following: a right group is a semigroup $(S;\cdot)$ which is also a *right quasigroup*, that is, for each $a, b \in S$, there exists a

2010 Mathematics Subject Classification: Primary: 20N02; Secondary: 20N05, 08A50
Keywords: right quasigroup, right product quasigroup, right product loop, axiomatization, axiom independence, word problem, reproductive equation
The second author was supported by the Ministry of Education and Science of Serbia, grants 174008 and 174026

unique $x \in S$ such that $ax = b$. In a right quasigroup $(S; \cdot)$, one can define an additional operation $\backslash : S \times S \to S$ as follows: $z = x\backslash y$ is the unique solution of the equation $xz = y$. Then the following equations hold.

$$x\backslash xy = y \qquad \text{(Q1)} \qquad\qquad x(x\backslash y) = y \qquad \text{(Q2)}$$

Conversely, if we now think of S as an algebra with two binary operations then we have an equational definition.

Definition 1.2. An algebra $(S; \cdot, \backslash)$ is a *right quasigroup* if it satisfies $(Q1)$ and $(Q2)$. An algebra $(S; \cdot, /)$ is a *left quasigroup* if it satisfies

$$xy/y = x \qquad \text{(Q3)} \qquad\qquad (x/y)y = x \qquad \text{(Q4)}$$

An algebra $(S; \cdot, \backslash, /)$ is a *quasigroup* if it is both a right quasigroup and a left quasigroup.

(We are following the usual convention that juxtaposition binds more tightly than the division operations, which in turn bind more tightly than an explicit use of $\cdot$. This helps avoid excessive parentheses.)

From this point of view, a group is an associative quasigroup with $x\backslash y = x^{-1}y$ and $x/y = xy^{-1}$. If $(S; \cdot, \backslash)$ is a right group viewed as an associative right quasigroup, then its group component has a natural right division operation $/$. This operation can be extended to all of S as follows. We easily show that $x\backslash x = y\backslash y$ for all $x, y \in S$, and then define $e = x\backslash x$, $x^{-1} = x\backslash e$, and $x/y = xy^{-1}$. Note that in the right zero semigroup component of S, we have $xy = x\backslash y = x/y = y$.

If one tries to think of a right quasigroup as a "nonassociative right group", one might ask if there is a representation theorem like Theorem 1.1 which expresses a right quasigroup as a direct product of a quasigroup and a right zero semigroup. This is clearly not the case.

Example 1.3. On the set $S = \{0, 1\}$, define operations $\cdot, \backslash : S \times S \to S$ by $x \cdot 0 = x\backslash 0 = 1$ and $x \cdot 1 = x\backslash 1 = 0$. Then $(S; \cdot, \backslash)$ is a right quasigroup which is neither a quasigroup nor a right zero semigroup, and since $|S| = 2$, $(S; \cdot, \backslash)$ is also not a product of a quasigroup and right zero semigroup. □

For another obstruction to a representation theorem, note that if an algebra which is a direct product of a quasigroup and a right zero semigroup possesses a right neutral element, then the right zero semigroup component is trivial and the algebra is, in fact, a right loop (see below). However, there are right quasigroups with neutral elements which are not right loops.

Example 1.4. Let $\mathbb{N}$ be the set of natural numbers and define

$$x \cdot y = x \backslash y = \begin{cases} y & \text{if } x < y \\ x - y & \text{if } x \geq y \end{cases}$$

Then $(\mathbb{N}; \cdot, \backslash)$ is a right quasigroup, 0 is a neutral element, and $0 \cdot 1 = 1 = 2 \cdot 1$. Since $\cdot$ is not a quasigroup operation, it follows from the preceding discussion that $(\mathbb{N}; \cdot, \backslash)$ is not a direct product of a quasigroup and a right zero semigroup. □

Simply adjoining a right division operation / to a right quasigroup does not fix the problem; for instance, in either Example 1.3 or 1.4, define $x/y = 0$ for all x, y.

In this paper, we will investigate varieties of right quasigroups such that there is indeed a direct product decomposition.

Definition 1.5. A quasigroup $(S; \cdot, \backslash, /)$ is a {*left loop, right loop, loop*} if it satisfies the identity $\{\ x/x = y/y,\ x\backslash x = y\backslash y,\ x\backslash x = y/y\ \}$.

An algebra $(S; \cdot, \backslash, /, e)$ is a *pointed quasigroup* if $(S; \cdot, \backslash, /)$ is a quasigroup. A pointed quasigroup is a {*quasigroup with an idempotent, left loop, right loop, loop*} if the distinguished element e is {an idempotent $(ee = e)$, left neutral $(ex = x)$, right neutral $(xe = x)$, neutral $(ex = xe = x)$}.

Definition 1.6. Let $T = \{\cdot, \backslash, /\}$ be the language of quasigroups and M a further (possibly empty) set of operation symbols disjoint from T. The language $\hat{T} = T \cup M$ is *an extended language of quasigroups.*

The language $T_1 = \{\cdot, \backslash, /, e\}$, obtained from T by the addition of a single constant, is *the language of loops.*

Note that we have two different algebras under the name "loop". They are equivalent and easily transformed one into the other. When we need to distinguish between them we call the algebra $(S; \cdot, \backslash, /)$ satisfying $x\backslash x = y/y$ "the loop in the language of quasigroups" while the algebra $(S; \cdot, \backslash, /, e)$ satisfying identities $ex = xe = x$ is called "the loop in the language of loops". Analogously we do for left and right loops.

Definition 1.7. Let $\mathbb{V}$ be a class of quasigroups. An algebra is a *right product* $\mathbb{V}$*–quasigroup* if it is isomorphic to $Q \times R$, where $Q \in \mathbb{V}$ and R is a right zero semigroup.

In particular, when $\mathbb{V}$ is the class $\{\mathbf{Q}, \mathbf{L\Lambda}, \mathbf{R\Lambda}, \Lambda\}$ of all {*quasigroups, left loops, right loops, loops*} (in the language of quasigroups) then {$\mathbf{RPQ}$, $\mathbf{RPL\Lambda}, \mathbf{RPR\Lambda}, \mathbf{RP\Lambda}$} denote the class of all right product $\mathbb{V}$–quasigroups.

If $\mathbb{V}$ is the class $\{\mathbf{pQ}, \mathbf{Qi}, \mathbf{eQ}, \mathbf{Qe}, \mathbf{Q1}\}$ of all {*pointed quasigroups, quasigroups with an idempotent, left loops, right loops, loops*} (in the language of loops), then $\{\mathbf{RPpQ}, \mathbf{RPQi}, \mathbf{RPeQ}, \mathbf{RPQe}, \mathbf{RPQ1}\}$ denote the class of all right product $\mathbb{V}$–quasigroups.

We wish to view these classes as varieties of algebras. In order to make sense of this, we need to adjust the type of right zero semigroups to match that of (equational) quasigroups. We adopt the convention suggested above.

Convention 1.8. A right zero semigroup is considered to be an algebra in $\hat{T}$ satisfying $x\backslash y = x/y = xy = y$ for all x, y.

This convention agrees with the one used in [7, 8]. Different definitions of $\backslash$ and $/$ in right zero semigroups would affect the form of the axioms for right product quasigroups.

We also denote the class of all (pointed) right zero semigroups by $\mathcal{R}$ ($p\mathcal{R}$). Then, in the language of universal algebra, the variety of all right product $\mathbb{V}$–quasigroups is a product $\mathbb{V} \otimes \mathcal{R}$ of independent varieties $\mathbb{V}$ and $\mathcal{R}$ (see [20]).

Definition 1.9. If t is a term, then $\{\mathrm{head}(t), \mathrm{tail}(t)\}$ is the {first, last} variable of t.

The following is an immediate consequence of Definition 1.7 and Convention 1.8.

Theorem 1.10. *Let u, v be terms in a language extending $\{\cdot, \backslash, /\}$. Then the equality $u = v$ is true in all right product $\mathbb{V}$–quasigroups if and only if* $\mathrm{tail}(u) = \mathrm{tail}(v)$ *and $u = v$ is true in all $\mathbb{V}$–quasigroups.* □

In particular:

Corollary 1.11. *Let s, t, u be terms in a language extending $\{\cdot, \backslash, /\}$. If $s = t$ is true in all $\mathbb{V}$–quasigroups then $s \circ u = t \circ u$ ($\circ \in \{\cdot, \backslash, /\}$) is true in all right product $\mathbb{V}$–quasigroups.* □

We conclude this introduction with a brief discussion of the sequel and some notation conventions. In §2, we will consider the problem of axiomatizing the varieties introduced by the Definition 1.7. In §3 we consider various properties of right product (pointed) quasigroups and loops. Finally, in §4, we verify the independence of the axioms.

We should mention some related work by Tamura *et al* and others. [18, 19, 4, 21]. An "M-groupoid", defined by certain axioms, turns out to

be a direct product of a right zero semigroup and a magma with a neutral element. The axiomatic characterization of these in [18, 19] is of a somewhat different character than ours; besides the fact that they did not need to adjust signatures since they did not consider quasigroups, their axioms are also not entirely equational.

2. Axioms

We now consider the problem of axiomatizing **RPQ**, the class of all right product quasigroups. One approach to axiomatization is the standard method of Knoebel [6], which was used in [7, 8]. It turns out that the resulting axiom system consists of 14 identities, most of which are far from elegant. Another way is via independence of **Q** and $\mathcal{R}$. Using the term $\alpha(x,y) = xy/y$ (see [20, Proposition 0.9]), we get these axioms:

$$xx/x = x$$
$$(xy/y)(uv/v)/(uv/v) = xv/v \qquad (xy \cdot uv)/uv = (xu/u)(yv/v)$$
$$(x\backslash y)(u\backslash v)/(u\backslash v) = (xu/u)\backslash(yv/v) \quad (x/y)(u/v)/(u/v) = (xu/u)/(yv/v)$$

which we also find to be somewhat complicated. Instead, we propose a different scheme, which we call system (A):

$$x\backslash xy = y \tag{A1}$$
$$x \cdot x\backslash y = y \tag{A2}$$
$$x/y \cdot y = xy/y \tag{A3}$$
$$(x/y \cdot y)/z = x/z \tag{A4}$$
$$xy/z \cdot z = x(y/z \cdot z) \tag{A5}$$

We now prove that system (A) axiomatizes the variety of right product quasigroups. It is not difficult to use the results of [5] to prove this, but instead we give a somewhat more enlightening self-contained proof. We start with an easy observation.

Lemma 2.1. *Every right product quasigroup satisfies system* (A).

Proof. The quasigroup axioms (Q3) and (Q4) trivially imply (A3)–(A5), and so quasigroups satisfy (A). For each (Ai), the tails of both sides of the equation coincide. By Theorem 1.10, we have the desired result. □

In an algebra $(S;\cdot,\backslash,/)$ satisfying system (A), define a new term operation $\star : S \times S \to S$ by

$$x \star y = xy/y = x/y \cdot y \tag{$\star$}$$

for all $x, y \in S$. Here the second equality follows from (A3), and we will use it freely without reference in what follows.

Lemma 2.2. *Let $(S;\cdot,\backslash,/)$ be an algebra satisfying system* (A). *Then for all $x, y, z \in S$,*

$$(xy) \star z = x(y \star z) \tag{1}$$
$$(x\backslash y) \star z = x\backslash(y \star z) \tag{2}$$
$$(x/y) \star z = x/(y \star z) \tag{3}$$

Proof. Equation (1) is just (A5) rewritten. Replacing y with $x\backslash y$ and using (A1), we get (2). Finally, for (3), we have

$$\begin{aligned} x/(y \star z) &= (x \star y \star z)/(y \star z) = [(x/y \cdot y) \star z]/(y \star z) \\ &= [(x/y)(y \star z)]/(y \star z) = (x/y) \star y \star z = (x/y) \star z\,, \end{aligned}$$

using (A4) in the first equality, (1) in the third, and the rectangular property of $\star$ in the fifth. □

Lemma 2.3. *Let $(S;\cdot,\backslash,/)$ be an algebra satisfying system* (A). *Then $(S;\star)$ is a rectangular band.*

Proof. Firstly,

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

using (A4). Replacing x with $x/(y \star z)$ in (1), we get

$$[(x/(y \star z))y] \star z = x/(y \star z) \cdot (y \star z) = x \star (y \star z)\,. \tag{5}$$

Thus,

$$x{\star}z = (x{\star}(y{\star}z)){\star}z = ([(x/(y{\star}z))y]{\star}z){\star}z = [(x/(y{\star}z))y]{\star}z = x{\star}(y{\star}z)\,, \tag{6}$$

using (4), (5), (4) again and (5) once more. Together, (4) and (6) show that $(S;\star)$ is a semigroup satisfying $x \star y \star z = x \star z$.

What remains is to show the idempotence of $\star$. Replace x with x/x in (1) and set $y = z = x$, we have

$$(x/x)(x \star x) = (x/x \cdot x) \star x = (x \star x) \star x = x \star x \,,$$

using (4), and so

$$x \star x = (x/x)\backslash(x \star x) = (x/x)\backslash(x/x \cdot x) = x \,,$$

using (A1) in the first and third equalities. □

Let $(S; \cdot, \backslash, /)$ be an algebra satisfying system (A). By Lemma 2.3, $(S; \star)$ is a rectangular band, and so $(S; \star)$ is isomorphic to the direct product of a left zero semigroup and a right zero semigroup [1]. It will be useful to make this explicit. Introduce translation maps in the semigroup $(S; \star)$ as follows

$$\ell_x(y) := x \star y =: (x)r_y \,,$$

so that the left translations $\ell_x : S \to S$ act on the left and the right translations $r_y : S \to S$ act on the right. Let $L = \langle \ell_x | x \in S \rangle$ and $R = \langle r_x | x \in S \rangle$. Then L is a left zero transformation semigroup, that is, $\ell_x \ell_y = \ell_x$, while R is a right zero transformation semigroup, that is, $r_x r_y = r_y$. Since $\ell_x = \ell_{x \star y}$ and $r_y = r_{x \star y}$ for all $x, y \in S$, it follows easily that the map $S \to L \times R; x \mapsto (\ell_x, r_x)$ is an isomorphism of semigroups.

Now we define operations $\cdot$, $\backslash$ and $/$ on R and L. Firstly, we define $\cdot, \backslash, / : R \times R \to R$ by

$$r_x \cdot r_y := r_x \backslash r_y := r_x / r_y := r_y \,.$$

For later reference, we formally record the obvious.

Lemma 2.4. *Let $(S; \cdot, \backslash, /)$ be an algebra satisfying system* (A)*. With the definitions above, $(R; \cdot, \backslash, /)$ is a right zero semigroup.* □

It follows from Lemma 2.1 that $(R; \cdot, \backslash, /)$ is an algebra satisfying system (A).

Lemma 2.5. *Let $(S; \cdot, \backslash, /)$ be an algebra satisfying system* (A)*. The mapping $S \to R; x \mapsto r_x$ is a surjective homomorphism of such algebras.*

Proof. Firstly,

$$(x)r_{yz} = x \star (yz) = x \star [y(z \star z)] = x \star (yz) \star z = x \star z = xr_z = (x)(r_y \cdot r_z) \,,$$

using (1) in the third equality and $(S; \star)$ being a rectangular band in the fourth equality. Similar arguments using (2) and (3) give $r_{y\backslash z} = r_y \backslash r_z$ and $r_{y/z} = r_y / r_z$, respectively. The surjectivity is clear. □

Next, we define $\cdot, \backslash, / : L \times L \to L$ by

$$(\ell_x \cdot \ell_y)(z) = \ell_x(z) \cdot \ell_y(z)$$
$$(\ell_x \backslash \ell_y)(z) = \ell_x(z) \backslash \ell_y(z)$$
$$(\ell_x / \ell_y)(z) = \ell_x(z) / \ell_y(z)$$

for all $x, y, z \in S$.

Lemma 2.6. *Let $(S; \cdot, \backslash, /)$ be an algebra satisfying system* (A). *With the definitions above, $(L; \cdot, \backslash, /)$ is a quasigroup.*

Proof. Equations (Q1) and (Q2) follow immediately from the definitions together with (A1) and (A2). By (A3), it remains to prove, say, (Q3). For all $x, y, z \in S$,

$$((\ell_x \cdot \ell_y)/\ell_y)(z) = (\ell_x(z) \cdot \ell_y(z))/\ell_y(z) = (x \star z) \star (y \star z) = x \star z = \ell_x(z)\,,$$

where we have used the fact that $(S; \star)$ is a rectangular band in the third equality. □

Lemma 2.7. *Let $(S; \cdot, \backslash, /)$ be an algebra satisfying system* (A). *The mapping $S \to L; x \mapsto \ell_x$ is a surjective homomorphism of such algebras.*

Proof. For all $x, y, z \in S$, we compute

$$\begin{aligned}\ell_x(z) \cdot \ell_y(z) &= (x \star z)(y \star z) = (x \star y \star z)(y \star z) = [(x(y \star z))/(y \star z)](y \star z)\\ &= (x(y \star z)) \star y \star z = x(y \star z \star y \star z) = x[y \star z] = (xy) \star z\\ &= \ell_{xy}(z)\,,\end{aligned}$$

where we use rectangularity of $\star$ in the second equality, (1) in the fifth, idempotence of $\star$ in the sixth and (1) in the seventh. Next, if we replace y with $x \backslash y$ and use (A1), we get $\ell_{x\backslash y}(z) = \ell_x(z) \backslash \ell_y(z)$. Finally,

$$\ell_x(z)/\ell_y(z) = (x \star z)/(y \star z) = ((x \star z)/y) \star z = (x/y) \star z = \ell_{x/y}(z)\,,$$

using (3) in the second equality and (A5) in the third. □

We now turn to the main result of this section.

Theorem 2.8. *An algebra $(S; \cdot, \backslash, /)$ is a right product quasigroup if and only if it satisfies* (A).

Proof. The necessity is shown by Lemma 2.1. Conversely, if $(S;\cdot,\backslash,/)$ satisfies (A), then by Lemmas 2.5 and 2.7, the mapping $S \to L \times R; x \mapsto (\ell_x, r_x)$ is a surjective homomorphism. This map is, in fact, bijective, since as already noted, it is an isomorphism of rectangular bands. By Lemmas 2.4 and 2.6, $L \times R$ is a right product quasigroup, and thus so is S. □

Remark 2.9. There are other choices of axioms for right product quasigroups. For instance, another system equivalent to (A) consists of (A1), (A2), (A3) and the equations

$$xx/x = x \quad \text{(B1)} \qquad\qquad (xy \cdot (z/u))/(z/u) = x(yu/u) \quad \text{(B2)}\,.$$

Call this system (B). We omit the proof of the equivalence of systems (A) and (B). One can use the results of [5] to prove the system (B) variant of Theorem 2.8 as follows: (A1) and (A2) trivially imply the equations

$$x(x\backslash y) = x\backslash xy \qquad \text{(A3}'\text{)}$$

$$x\backslash xx = x \quad \text{(B1}'\text{)} \qquad (x\backslash y)\backslash((x\backslash y)\cdot zu) = (x\backslash xz)u \quad \text{(B2}'\text{)}\,.$$

By [5], (A3), (A3′), (B1), (B1′), (B2′) and (B2′) axiomatize the variety of *rectangular quasigroups*, each of which is a direct product of a left zero semigroup, a quasigroup and a right zero semigroup. By (A1) and (A2), the left zero semigroup factor must be trivial, and so a system satisfying system (B) must be a right product quasigroup. □

We conclude this section by considering other varieties of right product quasigroups. Utilizing [9] we get:

Theorem 2.10. *Let $\mathbb{V}$ be a variety of quasigroups axiomatized by additional identities:*

$$s_i = t_i \qquad (\mathrm{V}_i)$$

$(i \in I)$ in an extended language $\hat{T}$ and let z be a variable which does not occur in any s_i, t_i. Then the variety $\boldsymbol{RP}\mathbb{V}$ of right product $\mathbb{V}$–quasigroups can be axiomatized by system (A) *together with (for all $i \in I$):*

$$s_i z = t_i z\,. \qquad (\hat{\mathrm{V}}_i)$$

Proof. Both $\mathbb{V}$–quasigroups and right zero semigroups satisfy system (A) and all $(\hat{\mathrm{V}}_i)$, $i \in I$, and thus so do their direct products i.e., right product $\mathbb{V}$–quasigroups.

Conversely, if an algebra satisfies system (A), it is a right product quasigroup by Theorem 2.8. Since all $(\hat{\mathrm{V}}_i)$ are satisfied, the quasigroup factor has to satisfy them, too. But in quasigroups, the identities $(\hat{\mathrm{V}}_i)$ are equivalent to the identities (V_i) and these define the variety $\mathbb{V}$. □

Theorem 2.11. *Theorem* 2.10 *remains valid if we replace* $(\hat{\mathrm{V}}_i)$ *by any of the following families of identities:*

$$
\begin{aligned}
s_i\backslash z &= t_i\backslash z\\
s_i/z &= t_i/z\\
z/(s_i\backslash z) &= (z/t_i)\backslash z\\
s_i &= (t_i\cdot \operatorname{tail}(s_i))/\operatorname{tail}(s_i)\\
s_i &= (t_i/\operatorname{tail}(s_i))\cdot \operatorname{tail}(s_i)\\
s_i &= t_i \quad (\textit{if } \operatorname{tail}(s_i)=\operatorname{tail}(t_i)).
\end{aligned}
$$

□

Example 2.12. Adding associativity $x\cdot yz = xy\cdot z$ to system (A) gives yet another axiomatization of *right groups*. □

Example 2.13. Right product commutative quasigroups are right product quasigroups satisfying $xy\cdot z = yx\cdot z$. However, commutative right product quasigroups are just commutative quasigroups. □

Obviously:

Corollary 2.14. *If the variety* $\mathbb{V}$ *of quasigroups is defined by the identities* $s_i = t_i$ $(i\in I)$ *such that* $\operatorname{tail}(s_i)=\operatorname{tail}(t_i)$ *for all* $i\in I$*, then the class of all right product quasigroups satisfying identities* $s_i = t_i (i\in I)$ *is the class of all right product* $\mathbb{V}$*–quasigroups.*

If $\operatorname{tail}(s_i)\neq\operatorname{tail}(t_i)$ *for some* $i\in I$*, then the class of all right product quasigroups satisfying identities* $s_i = t_i$ $(i\in I)$ *is just the class of all* $\mathbb{V}$*–quasigroups.* □

Example 2.15. The variety **RPpQ** is defined by adding a constant to the language of quasigroups, not by any extra axioms. □

Example 2.16. The variety **RPQi** of all *right product quasigroups with an idempotent* may be axiomatized by system (A) and $ee = e$. □

Corollary 2.17. *A right product quasigroup is a right product left loop iff it satisfies any (and hence all) of the following axioms:*

$$(x/x)y = y \tag{LL1}$$
$$(x/x)z = (y/y)z \tag{LL2}$$
$$(x \circ y)/(x \circ y) = y/y \tag{LL3}$$

where $\circ$ is any of the operations $\cdot, \backslash, /$.

Proof. In a quasigroup, identities (LL1), (LL2) and (LL3) are equivalent to each other and to $x/x = y/y$, and so a quasigroup satisfying either axiom is a left loop. Conversely, in a left loop with left neutral element e, we have $e = x/x$, and so (LL1), (LL2) and (LL3) hold. Thus a quasigroup satisfies either (and hence all) of (LL1), (LL2), (LL3) if and only if it is a left loop.

On the other hand, (LL1), (LL2) and (LL3) trivially hold in right zero semigroups by Convention 1.8. Putting this together, we have the desired result. □

In the language of loops we have:

Corollary 2.18. *A right product quasigroup is a right product left loop if and only if it satisfies the identity $ex = x$.* □

Similarly:

Corollary 2.19. *A right product quasigroup is a right product right loop if and only if it satisfies any (and hence all) of the following axioms:*

$$x(y\backslash y) \cdot z = xz$$
$$(x\backslash x)z = (y\backslash y)z$$
$$(x \circ y)\backslash(x \circ y) = y\backslash y$$

where $\circ$ is any of the operations $\cdot, \backslash, /$. □

Corollary 2.20. *A right product quasigroup is a right product right loop (in the language of loops) iff it satisfies the identity $xe \cdot y = xy$.* □

Corollary 2.21. *A right product quasigroup is a right product loop if and only if it satisfies any (and hence all) of the following axioms:*

$$\begin{gathered}(x\backslash x)y = y \qquad \text{(L)}\\ x(y/y) = xy/y\\ x(y/y) = (x/y)y\\ (x\backslash x)z = (y/y)z\\ (x\circ y)\backslash(x\circ y) = y/y\\ (x\circ y)/(x\circ y) = y\backslash y\end{gathered}$$

where $\circ$ is any of the operations $\cdot, \backslash, /$. □

Corollary 2.22. *A right product quasigroup is a right product loop (in the language of loops) iff it satisfies both $ex = x$ and $xe \cdot y = xy$.* □

3. Properties of right product (pointed) quasigroups

Calling upon the tools of universal algebra, we now examine some properties of right product quasigroups. We will use the following standard notation.

Definition 3.1.

E_S	–	the subset of all idempotents of S.
$\mathrm{Sub}(S)$	–	the lattice of all subalgebras of S.
$\mathrm{Sub}^0(S)$	–	the lattice of all subalgebras of S with the empty set adjoined as the smallest element (used when two sub–algebras have an empty intersection).
$\mathrm{Con}(S)$	–	the lattice of all congruences of S.
$\mathrm{Eq}(S)$	–	the lattice of all equivalences of S.
$\mathrm{Hom}(S,T)$	–	the set of all homomorphisms from S to T.
$\mathrm{End}(S)$	–	the monoid of all endomorphisms of S.
$\mathrm{Aut}(S)$	–	the group of all automorphisms of S.
$\mathrm{Free}(\mathbb{V}, n)$	–	the free algebra with n generators in the variety $\mathbb{V}$.
$\mathrm{Var}(\mathbb{V})$	–	the lattice of all varieties of a class $\mathbb{V}$ of algebras.

In addition, R_n will denote the unique n-element right zero semigroup – which also happens to be free. However, note that in the language of loops, the free right zero semigroup generated by n elements is R_{n+1}.

3.1. The word problem

Using a well-known result of Evans [3] we have the following corollary of Theorem 1.10:

Corollary 3.2. *The word problem for right product $\mathbb{V}$–quasigroups is solvable if and only if it is solvable for $\mathbb{V}$–quasigroups.* □

In particular:

Corollary 3.3. *The word problem for $\{\boldsymbol{RPQ}, \boldsymbol{RPL}\Lambda, \boldsymbol{RPR}\Lambda, \boldsymbol{RP}\Lambda\}$ is solvable.* □

Likewise:

Corollary 3.4. *The word problem for $\{\boldsymbol{RPpQ}, \boldsymbol{RPQi}, \boldsymbol{RPeQ}, \boldsymbol{RPQe}, \boldsymbol{RPQ1}\}$ is solvable.* □

3.2. Properties of right product quasigroups and loops

The following corollaries are special cases of results in universal algebra (see [20]).

Corollary 3.5. *For all $Q, Q' \in \boldsymbol{Q}$ and $R, N \in \mathcal{R}$:*

1. $E_{Q\times R} = E_Q \times R$,
   in particular:
   - *$Q \times R$ have idempotents if and only if Q have them.*
   - *$E_{Q\times R}$ is subalgebra of $Q \times R$ if and only if E_Q is subalgebra of Q.*
   - *$Q \times R$ is a groupoid of idempotents if and only if Q is.*
2. $\mathrm{Sub}^0(Q \times R) = (\mathrm{Sub}(Q) \times (\mathbf{2}^R \setminus \{\emptyset\})) \cup \{\emptyset\}$.
3. $\mathrm{Con}(Q \times R) = \mathrm{Con}(Q) \times \mathrm{Eq}(R)$.
4. $\mathrm{Hom}(Q \times R,\, Q' \times N) = \mathrm{Hom}(Q, Q') \times N^R$.
5. $\mathrm{End}(Q \times R) = \mathrm{End}(Q) \times R^R$.
6. $\mathrm{Aut}(Q \times R) = \mathrm{Aut}(Q) \times S_{|R|}$. □

Having a distinguished element changes the properties of a variety radically. For example, if $e = (i, j)$ is a distinguished element of the right product pointed quasigroup $Q \times R$ then there is always the smallest subalgebra $< i > \times \{j\}$. So, in case of right product pointed quasigroups, the results analogous to Corollary 3.5 are actually somewhat different in character.

Corollary 3.6. *For all $Q, Q' \in \boldsymbol{pQ}$ and $R, N \in \mathcal{R}$ with a distinguished element j:*

1. $E_{Q \times R} = E_Q \times R$,
   in particular:
   - *$Q \times R$ has idempotents if and only if Q has them.*
   - *$E_{Q \times R}$ is subalgebra of $Q \times R$ if and only if E_Q is subalgebra of Q.*
   - *$Q \times R$ is a groupoid of idempotents if and only if Q is.*
2. $\mathrm{Sub}(Q \times R) = \mathrm{Sub}(Q) \times \{Y \subseteq R \mid j \in Y\} \simeq \mathrm{Sub}(Q) \times \mathbf{2}^{R \setminus \{j\}}$.
3. $\mathrm{Con}(Q \times R) = \mathrm{Con}(Q) \times \mathrm{Eq}(R)$.
4. $\mathrm{Hom}(Q \times R, Q' \times N) = \mathrm{Hom}(Q, Q') \times \{f : R \to N \mid f(j) = j\} \simeq \mathrm{Hom}(Q, Q') \times N^{R \setminus \{j\}}$.
5. $\mathrm{End}(Q \times R) = \mathrm{End}(Q) \times \{f : R \to R \mid f(j) = j\} \simeq \mathrm{End}(Q) \times R^{R \setminus \{j\}}$.
6. $\mathrm{Aut}(Q \times R) = \mathrm{Aut}(Q) \times \{f \in S_R \mid f(j) = j\} \simeq \mathrm{Aut}(Q) \times S_{|R|-1}$. □

Corollary 3.7. *If $\mathbb{V}$ is one of $\boldsymbol{Q}, \boldsymbol{L}\Lambda, \boldsymbol{R}\Lambda, \Lambda$, then*
$$\mathrm{Free}(\boldsymbol{RP}\mathbb{V}, n) \simeq \mathrm{Free}(\mathbb{V}, n) \times R_n. \qquad \square$$

Corollary 3.8. *If $\mathbb{V}$ is one of $\boldsymbol{pQ}, \boldsymbol{Qi}, \boldsymbol{eQ}, \boldsymbol{Qe}, \boldsymbol{Q1}$, then*
$$\mathrm{Free}(\boldsymbol{RP}\mathbb{V}, n) \simeq \mathrm{Free}(\mathbb{V}, n) \times R_{n+1}. \qquad \square$$

Corollary 3.9. *If $\mathbb{V}$ is one of the above varieties of (pointed) quasigroups, then* $\mathrm{Var}(\boldsymbol{RP}\mathbb{V}) \simeq \mathrm{Var}(\mathbb{V}) \times \mathbf{2}$. □

All cases suggested by Corollary 3.5(1) can actually occur. In the examples below, right product quasigroups are in fact quasigroups and thus we display the Cayley tables of the multiplication only.

Example 3.10. Tables 1 give a right product quasigroup with no idempotents (on the left) and an idempotent right product quasigroup (on the right).

$\cdot$	0	1	2
0	1	0	2
1	0	2	1
2	2	1	0

$\cdot$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Table 1: A right product quasigroup with no idempotents and an idempotent right product quasigroup.

Example 3.11. Tables 2 give a right product quasigroup in which E_S is not a subalgebra (on the left) and a right product quasigroup in which E_S is a nontrivial subalgebra (on the right).

$\bullet$	0	1	2	3
0	0	2	1	3
1	3	1	2	0
2	1	3	0	2
3	2	0	3	1

$\bullet$	0	1	2	3	4	5
0	0	2	1	3	5	4
1	2	1	0	5	4	3
2	1	0	2	4	3	5
3	3	5	4	0	2	1
4	5	4	3	2	1	0
5	4	3	5	1	0	2

Table 2: E_S is not closed, E_S is a nontrivial subalgebra.

Moreover, we have the following. These are immediate consequences of well understood properties of quasigroups and semigroups.

Theorem 3.12. *Let $S = Q \times R$ be a right product quasigroup. Then:*

1. *If Q_m $(m \in M)$ is the (possibly empty) family of all maximal subquasigroups of Q then $Q_m \times R$ $(m \in M)$, $Q \times (R \setminus \{r\})$ $(r \in R)$ is the family of all maximal right product subquasigroups of S.*

2. *There are $|R|$ maximal subquasigroups of S. They are all mutually isomorphic and of the form $Q \times \{r\}$ $(r \in R)$.*

From now on we assume $E_S \neq \emptyset$ (i.e., $E_Q \neq \emptyset$).

3. *If E_S is subalgebra then it is the largest subalgebra of idempotents of S.*

4. *There are $|E_S|$ maximal left zero subsemigroups of S. They are all singletons $\{e\}$ $(e \in E_S)$.*

5. *There are $|E_Q|$ maximal right zero subsemigroups of S. They are all mutually isomorphic and of the form $\{i\} \times R$ $(i \in E_Q)$.*

From now on we assume $E_Q = \{i\}$.

6. *$E_S = \{i\} \times R$ is the unique largest subband of S, which happens to be a right zero semigroup.*

7. *If the quasigroup Q is a left loop then the left neutral i of Q is the only idempotent of Q and:*
   - *$E_S = \{a/a \mid a \in S\}$.*
   - *The element $e \in S$ is a left neutral if and only if it is an idempotent.*
   - *The maximal subquasigroups*
   $$Q \times \{r\} = Se = \{x \in S \mid x/x = e\} \quad (e \in E_S, e = (i, r))$$
   are maximal left subloops of S.
   - *For all $e \in E_S$ $S \simeq Se \times E_S$ and the isomorphism is given by $f(x) = (xe/e, x/x)$.*

8. *If the quasigroup Q is a right loop then the right neutral i of Q is the only idempotent of Q and:*
   - *$E_S = \{a\backslash a \mid a \in S\}$.*
   - *S has a right neutral if and only if $|R| = 1$ and then the right neutral is unique. In this case S is a right loop.*
   - *The maximal subquasigroups*
   $$Q \times \{r\} = Se = \{x \in S \mid x\backslash x = e\} \quad (e \in E_S, e = (i, r))$$
   are maximal right subloops of S.
   - *For all $e \in E_S$ $S \simeq Se \times E_S$ and the isomorphism is given by $f(x) = (xe, x\backslash x)$.*

9. *If the quasigroup Q is a loop then:*
   - *The element $e \in S$ is a left neutral if and only if it is an idempotent.*
   - *S has a right neutral if and only if $|R| = 1$ and then the right neutral is unique. In this case S is a loop.*
   - *The maximal subquasigroups*

$$Q \times \{r\} = Se = \{x \in S \mid x \backslash x = x/x = e\} \ \ (e \in E_S, e = (i, r))$$

are maximal subloops of S.

– *For all* $e \in E_S$ $S \simeq Se \times E_S$ *and the isomorphism is given by* $f(x) = (xe, x/x)$. □

Theorem 3.13. *Let* $S = Q \times R$ *be a right product pointed quasigroup with a distinguished element* $e = (i, j)$. *Then:*

1. *If* Q_m $(m \in M)$ *is the (possibly empty) family of all maximal pointed subquasigroups of* Q *then* $Q_m \times R$, $Q \times (R \setminus \{r\})$, *where* $r \in R \setminus \{j\}$, *is the family of all maximal right product pointed subquasigroups of* S.

2. $Se = Q \times \{j\}$ *is the largest pointed subquasigroup of* S.

From now on we assume $E_S \neq \emptyset$ *(i.e.,* $E_Q \neq \emptyset$*).*

3. *If* E_S *is subalgebra then it is the largest subalgebra of idempotents of* S.

4. $Se \cap E_S = \{e\}$ *is the largest pointed left zero subsemigroup of* S *if and only if* $e \in E_S$.

5. $E_S = \{i\} \times R$ *is the largest pointed right zero subsemigroup of* S *if and only if* $i \in E_Q$.

6. $S \simeq Se \times E_S$ *and the isomorphism is given by* $f(x) = (xe/e, ex/x)$.

From now on we assume $E_Q = \{i\}$.

7. $E_S = \{i\} \times R$ *is the unique largest pointed subband of* S, *which happens to be a pointed right zero semigroup.*

8. *If the element* i *is the left neutral of* Q, *it is the only idempotent of* Q *and:*

   – $E_S = \{a/a \mid a \in S\}$.

   – *The element* $a \in S$ *is a left neutral if and only if it is an idempotent.*

   – $Se = \{x \in S \mid x/x = e\}$ *is the largest left subloop of* S.

   – *The isomorphism* $S \simeq Se \times E_S$ *is given by* $f(x) = (xe/e, x/x)$.

9. *If the element i is the right neutral of Q, it is the only idempotent of Q and:*
   - $E_S = \{a\backslash a \mid a \in S\}$.
   - *S has a right neutral if and only if $|R| = 1$ and then the right neutral is e. In this case S is a right loop.*
   - $Se = \{x \in S \mid x\backslash x = e\}$ *is the largest right subloop of S.*
   - *The isomorphism $S \simeq Se \times E_S$ is given by $f(x) = (xe, x\backslash x)$.*
10. *If the element i is the two–sided neutral of Q, it is the only idempotent of Q and:*
   - *The element $a \in S$ is a left neutral if and only if it is an idempotent.*
   - *S has a right neutral if and only if $|R| = 1$ and then the right neutral is e. In this case S is a loop.*
   - $Se = \{x \in S \mid x\backslash x = x/x = e\}$ *is the largest subloop of S.*
   - *The isomorphism $S \simeq Se \times E_S$ is given by $f(x) = (xe, x/x)$.* □

3.3. The equation xa=b

Since a right product quasigroup is a right quasigroup the equation $ax = b$ has the unique solution $x = a\backslash b$. For the equation $xa = b$, the situation is not so clear.

We solve the equation $xa = b$ using the notion of *reproductivity*. The related notion of *reproductive general solution* was defined by E. Schröder [17] for Boolean equations and studied by L. Löwenheim [10, 11] who also introduced the term "reproductive". More recently, S. B. Prešić made significant contributions to the notion of reproductivity [13, 14, 15]. For an introduction to reproductivity, see S. Rudeanu [16].

Definition 3.14. Let $S \neq \emptyset$ and $F : S \longrightarrow S$. The equation $x = F(x)$ is *reproductive* if for all $x \in S$ $F(F(x)) = F(x)$.

The most significant properties of reproductivity are:

Theorem 3.15. *A general solution of the reproductive equation $x = F(x)$ is given by: $x = F(p)$ $(p \in S)$.* □

Theorem 3.16 (S. B. Prešić). *Every consistent equation has an equivalent reproductive equation.* □

We now apply these results to our equation $xa = b$.

Theorem 3.17.

1. *In right product quasigroups, the equation $xa = b$ is consistent if and only if $(b/a)a = b$.*

2. *In right product {left, right} loops, the consistency of $xa = b$ is equivalent to $\{a/a = b/b, a\backslash a = b\backslash b\}$.*

3. *If the equation $xa = b$ consistent, then it is equivalent to the reproductive equation $x = (b/a)x/x$, and thus its general solution is given by $x = (b/a)p/p$ $(p \in S)$. There are exactly $|R|$ distinct solutions.*

4. *If a right product quasigroup $S = Q \times R$ has idempotents, then the general solution of the consistent equation $xa = b$ may be given in the form $x = (b/a)e/e \quad (e \in E_S)$.*

5. *If the quasigroup Q has a unique idempotent, then any idempotent $e \in E_S$ defines the unique solution $x = (b/a)e/e$ of $xa = b$.*

6. *In a right product right loop, the general solution of $xa = b$ may be simplified to $x = (b/a)e \quad (e \in E_S)$.*

Proof. (1) If the equation is consistent then there is at least one solution $x = c$. It follows that $b = ca$ and $(b/a)a = (ca/a)a = ca = b$. If we assume that $(b/a)a = b$ then $x = b/a$ is one solution of the equation $xa = b$, which therefore must be consistent.

(2) Assume S is a right product left loop. If $xa = b$ is consistent then $b/b = xa/xa = a/a$. For the converse assume $S = Q \times R$ for some left loop Q with the left neutral i and a right zero semigroup R. Let $a = (a_1, a_2)$ and $b = (b_1, b_2)$. Then $(i, a_2) = (a_1/a_1, a_2/a_2) = a/a = b/b = (b_1/b_1, b_2/b_2) = (i, b_2)$ i.e., $a_2 = b_2$ which is equivalent to the consistency of $xa = b$.

Now assume S is a right product right loop. If $xa = b$ is consistent then $b\backslash b = xa\backslash xa = a\backslash a$. For the converse assume $S = Q \times R$ for some right loop Q with the right neutral i and a right zero semigroup R. Let $a = (a_1, a_2)$ and $b = (b_1, b_2)$. Then $(i, a_2) = (a_1\backslash a_1, a_2\backslash a_2) = a\backslash a = b\backslash b = (b_1\backslash b_1, b_2\backslash b_2) = (i, b_2)$ i.e., $a_2 = b_2$ which is equivalent to the consistency of $xa = b$.

(3) Let the equation $xa = b$ be consistent. Then $(b/a)x/x = (xa/a)x/x = xx/x = x$. Conversely, if $x = (b/a)x/x$ then $xa = ((b/a)x/x)a =$

$(b/a)a = b$. Therefore, equations $xa = b$ and $x = (b/a)x/x$ are equivalent. The form of the later equation is $x = F(x)$ where $F(x) = (b/a)x/x$. Also, $F(F(x)) = ((b/a) \cdot F(x))/F(x) = ((b/a)((b/a)x/x))/((b/a)x/x) = (b/a)x/x = F(x)$ so equation $x = F(x)$ is reproductive. Its general solution is $x = F(p) = (b/a)p/p (p \in S)$.

Without loss of generality we may assume that S is $Q \times R$ for some quasigroup Q and a right zero semigroup R. Let $a = (a_1, a_2), b = (b_1, b_2), x = (x_1, x_2)$ and $p = (p_1, p_2)$. The consistency of $xa = b$ reduces to $(b_1, b_2) = (b/a)a = ((b_1/a_1)a_1, a_2) = (b_1, a_2)$ i.e., $a_2 = b_2$. In that case, the solutions of $xa = b$ are $x = (b/a)p/p = ((b_1/a_1)p_1/p_1, (b_2/a_2)p_2/p_2) = (b_1/a_1, p_2)$. Evidently, the number of different solutions of $xa = b$ is $|R|$.

(4) Let $S = Q \times R$ and let i be an idempotent of Q. For every $p = (p_1, p_2)$ there is an idempotent $e = (i, p_2)$ of S such that $x = (b/a)p/p = (b_1/a_1, p_2) = ((b_1/a_1)i/i, (b_2/a_2)p_2/p_2) = (b/a)e/e$.

(5) If the idempotent $i \in Q$ is unique then E_S has exactly $|E_S| = |R|$ idempotents, just as many as the equation $xa = b$ has solutions.

(6) Let S be a right product right loop and $e = (i, r)$. Then

$$\begin{aligned} x &= (b/a)e/e = ((b_1/a_1)i/i, (b_2/a_2)r/r) = (b_1/a_1, r) \\ &= ((b_1/a_1)i, (b_2/a_2)r) = (b_1/a_1, b_2/a_2)(i, r) = (b/a)e\,. \end{aligned}$$

The proof is complete. □

3.4. Products of sequences of elements including idempotents

We use $\varrho(a_i, a_{i+1}, \ldots, a_j)$ to denote *the right product* i.e., the product of $a_i, \ldots, a_j$ with brackets associated to the right. More formally, $\varrho(a_i) = a_i$ $(1 \leqslant i \leqslant n)$ and $\varrho(a_i, a_{i+1}, \ldots, a_j) = a_i \cdot \varrho(a_{i+1}, \ldots, a_j)$ $(1 \leqslant i < j \leqslant n)$.

Further, we define $\varrho(\pm a_n) = a_n$ and

$$\varrho(a_i, a_{i+1}, \ldots, a_j, \pm a_n) = \begin{cases} \varrho(a_i, \ldots, a_j); & \text{if } j = n \\ \varrho(a_i, \ldots, a_j, a_n); & \text{if } j < n. \end{cases}$$

In short, a_n should appear in the product $\varrho(a_i, \ldots, a_j, \pm a_n)$, but only once.

The following is an analogue of Theorem 2.4 from [7].

Theorem 3.18. *Let $a_1, \ldots, a_n$ $(n > 0)$ be a sequence of elements of the right product left loop S, such that $a_{p_1}, \ldots, a_{p_m}$ $(1 \leqslant p_1 < \ldots < p_m \leqslant n;$ $0 \leqslant m \leqslant n)$ comprise exactly the idempotents among $a_1, \ldots, a_n$. Then $\varrho(a_1, \ldots, a_n) = \varrho(a_{p_1}, \ldots, a_{p_m}, \pm a_n)$.*

Proof. The proof is by induction on n.
(1) $n = 1$.
If $m = 0$ then $\varrho(a_1) = a_1 = \varrho(\pm a_1)$.
If $m = 1$ then $\varrho(a_1) = a_1 = \varrho(a_1, \pm a_1)$.
(2) $n > 1$.
If $a_1 \in E_S$ (i.e., $1 < p_1$) then $\varrho(a_1, \ldots, a_n) = a_1 \cdot \varrho(a_2, \ldots, a_n) = \varrho(a_2, \ldots, a_n)$ which is equal to $\varrho(a_{p_1}, \ldots, a_{p_m}, \pm a_n)$ by the induction argument.
If $a_1 \notin E_S$ (i.e., $1 = p_1$) then, using induction argument again, we get $\varrho(a_1, \ldots, a_n) = a_1 \cdot \varrho(a_2, \ldots, a_n) = a_{p_1} \cdot \varrho(a_{p_2}, \ldots, a_{p_m}, \pm a_n) = \varrho(a_{p_1}, a_{p_2}, \ldots, a_{p_m}, \pm a_n)$. □

Analogously to $\varrho(\ldots)$, we use $\lambda(a_i, \ldots, a_{j-1}, a_j)$ to denote *the left product* i.e., the product of $a_i, \ldots, a_j$ with brackets associated to the left. Formally, $\lambda(a_i) = a_i$ $(1 \leqslant i \leqslant n)$ and $\lambda(a_i, \ldots, a_{j-1}, a_j) = \lambda(a_i, \ldots, a_{j-1}) \cdot a_j$ $(1 \leqslant i < j \leqslant n)$.

Further, we define $\lambda(\pm a_1, \pm a_n) = a_1$ if $n = 1$, $\lambda(\pm a_1, \pm a_n) = a_1 a_n$ if $n > 1$ and

$$\lambda(\pm a_1, a_i, \ldots, a_j, \pm a_n) = \begin{cases} \lambda(a_i, \ldots, a_j); & \text{if } 1 = i \leqslant j = n \\ \lambda(a_i, \ldots, a_j, a_n); & \text{if } 1 = i \leqslant j < n \\ \lambda(a_1, a_i, \ldots, a_j); & \text{if } 1 < i \leqslant j = n \\ \lambda(a_1, a_i, \ldots, a_j, a_n); & \text{if } 1 < i \leqslant j < n. \end{cases}$$

Therefore, both a_1 and a_n should appear in the product $\lambda(\pm a_1, a_i, \ldots, a_j, \pm a_n)$, but just once each. If $n = 1$ then $a_1 = a_n$ should also appear just once.

Of course, there is an analogue of Theorem 3.18.

Theorem 3.19. *Let $a_1, \ldots, a_n$ $(n > 0)$ be a sequence of elements of the right product right loop S, such that $a_{p_1}, \ldots, a_{p_m}$ $(1 \leqslant p_1 < \ldots < p_m \leqslant n$; $0 \leqslant m \leqslant n)$ and only them among $a_1, \ldots, a_n$ are nonidempotents. Then $\lambda(a_1, \ldots, a_n) = \lambda(\pm a_1, a_{p_1}, \ldots, a_{p_m}, \pm a_n)$.*

Proof. The proof is by induction on n.
(1) $n = 1$.
If $m = 0$ then $\lambda(a_1) = a_1 = \lambda(\pm a_1, \pm a_1)$.
If $m = 1$ then $\lambda(a_1) = a_1 = \lambda(\pm a_1, a_1, \pm a_1)$.
(2) $n > 1$.
(2a) Let $1 = p_1, p_{m-1} = n-1, p_m = n$ (i.e., $a_1, a_{n-1}, a_n \notin E_S$). Then, using induction argument, $\lambda(a_1, \ldots, a_n) = \lambda(a_1, \ldots, a_{n-1}) \cdot a_n = \lambda(\pm a_1, a_{p_1}, \ldots,$

$a_{p_{m-1}}, \pm a_{n-1}) \cdot a_{p_m} = \lambda(a_{p_1}, \ldots, a_{p_{m-1}}) \cdot a_{p_m} = \lambda(a_{p_1}, \ldots, a_{p_{m-1}}, a_{p_m}) = \lambda(\pm a_1, a_{p_1}, \ldots, a_{p_m}, \pm a_n)$.
(2b) Let $1 = p_1, p_m = n-1$ (i.e. $a_1, a_{n-1} \notin E_S; a_n \in E_S$). Then, using induction argument again, we get $\lambda(a_1, \ldots, a_n) = \lambda(a_1, \ldots, a_{n-1}) \cdot a_n = \lambda(\pm a_1, a_{p_1}, \ldots, a_{p_m}, \pm a_{n-1}) \cdot a_n = \lambda(a_{p_1}, \ldots, a_{p_m}) \cdot a_n = \lambda(a_{p_1}, \ldots, a_{p_m}, a_n) = \lambda(\pm a_1, a_{p_1}, \ldots, a_{p_m}, \pm a_n)$.
(2c) Let $1 = p_1, p_{m-1} < n-1, p_m = n$ (i.e., $a_1, a_n \notin E_S; a_{n-1} \in E_S$). Then, by the induction argument and (RL), $\lambda(a_1, \ldots, a_n) = \lambda(a_1, \ldots, a_{n-1}) \cdot a_n = \lambda(\pm a_1, a_{p_1}, \ldots, a_{p_{m-1}}, \pm a_{n-1}) \cdot a_n = \lambda(a_{p_1}, \ldots, a_{p_{m-1}}, a_{n-1}) \cdot a_{p_m} = \lambda(a_{p_1}, \ldots, a_{p_{m-1}}) a_{n-1} \cdot a_{p_m} = \lambda(a_{p_1}, \ldots, a_{p_{m-1}}) \cdot a_{p_m} = \lambda(a_{p_1}, \ldots, a_{p_{m-1}}, a_{p_m}) = \lambda(\pm a_1, a_{p_1}, \ldots, a_{p_m}, \pm a_n)$.
(2d) Let $1 = p_1, p_{m-1} < n$ (i.e., $a_1 \notin E_S; a_{n-1}, a_n \in E_S$). It follows that $\lambda(a_1, \ldots, a_n) = \lambda(a_1, \ldots, a_{n-1}) \cdot a_n = \lambda(\pm a_1, a_{p_1}, \ldots, a_{p_m}, \pm a_{n-1}) \cdot a_n = \lambda(a_{p_1}, \ldots, a_{p_m}, a_{n-1}) \cdot a_n = \lambda(a_{p_1}, \ldots, a_{p_m}) a_{n-1} \cdot a_n = \lambda(a_{p_1}, \ldots, a_{p_m}) \cdot a_n = \lambda(a_{p_1}, \ldots, a_{p_m}, a_n) = \lambda(\pm a_1, a_{p_1}, \ldots, a_{p_m}, \pm a_n)$.

The remaining cases of (2) in which $p_1 \neq 1$, *i.e.*, $a_1 \in E_S$ can be proved analogously. □

In right product {left, right} loops, Theorems 3.18 and 3.19 give us the means to reduce {right, left} products. The result is much stronger in right product loops.

Definition 3.20. Let $(S; \cdot, \backslash, /)$ be a right product quasigroup and $1 \notin S$. By S^1 we denote a triple magma with operations extending $\cdot, \backslash, /$ to $S \cup \{1\}$ in the following way: $x \circ y \quad (\circ \in \{\cdot, \backslash, /\})$ remains as before if $x, y \in S$. If $x = 1$ then $x \circ y = y$ and if $y = 1$ then $x \circ y = x$.

Note that the new, extended operations $\cdot, \backslash, /$ are well defined and that 1 is the neutral element for all three.

Lemma 3.21. *Let $a_1, \ldots, a_n \quad (n > 0)$ be a sequence of elements of a right product loop S such that a_n is an idempotent and $p(a_1, \ldots, a_n)$ some product of $a_1, \ldots, a_n$ (in that order) with an arbitrary (albeit fixed) distribution of brackets. Then $p(a_1, \ldots, a_n) = p(a_1, \ldots, a_{n-1}, 1) \cdot a_n$.*

Proof. First, note that if e is an idempotent then $x \cdot ye = xy \cdot e$ for all $x, y \in S$. Namely, if $e \in E_S$ then there is a $z \in S$ such that $e = z/z$ (for example $z = e$ is one). The identity $x \cdot y(z/z) = xy \cdot (z/z)$ is true in all right product loops as it is true in all loops and all right zero semigroups.

The proof of the lemma is by induction on n.
(1) $n = 1$.

$a_1 = a_n$ is an idempotent, so $p(a_1) = a_1 = 1 \cdot a_1 = p(1) \cdot a_1$.
(2) $n > 1$.
Let $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_k) \cdot r(a_{k+1}, \ldots, a_n)$ for some $k \quad (1 \leqslant k \leqslant n)$. By the induction hypothesis $r(a_{k+1}, \ldots, a_n) = r(a_{k+1}, \ldots, a_{n-1}, 1) \cdot a_n$. So $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_k) \cdot (r(a_{k+1}, \ldots, a_{n-1}, 1) \cdot a_n) = (q(a_1, \ldots, a_k) \cdot r(a_{k+1}, \ldots, a_{n-1}, 1)) \cdot a_n = p(a_1, \ldots, a_{n-1}, 1) \cdot a_n$. □

The following result is an improvement of Theorems 3.18 and 3.19.

Theorem 3.22. *Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n \quad (n > 0)$ be two sequences of elements of the right product loop S (with some of b_k possibly being 1) such that*

$$b_k = \begin{cases} 1; & \text{if } k < n \text{ and } a_k \in E_S \\ a_k; & \text{if } k = n \text{ or } a_k \notin E_S \end{cases}$$

and let $p(a_1, \ldots, a_n)$ be as in Lemma 3.21. Then $p(a_1, \ldots, a_n) = p(b_1, \ldots, b_n)$.

Proof. The proof of the Theorem is by induction on n.
(1) $n = 1$.
There is only one product $p(a_1) = a_1$ and, irrespectively of whether a_1 is idempotent or not, $b_1 = a_1$. Therefore $p(a_1) = p(b_1)$.
(2) $n > 1$.
Let $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_k) \cdot r(a_{k+1}, \ldots, a_n)$ for some k $(1 \leqslant k \leqslant n)$. By the induction hypothesis we have $q(a_1, \ldots, a_k) = q(b_1, \ldots, b_{k-1}, a_k)$ and $r(a_{k+1}, \ldots, a_n) = r(b_{k+1}, \ldots, b_n)$.

If a_k is nonidempotent then $a_k = b_k$ and $p(a_1, \ldots, a_n) = q(b_1, \ldots, b_k) \cdot r(b_{k+1}, \ldots, b_n) = p(b_1, \ldots, b_n)$.

If a_k is idempotent then $b_k = 1$ and by the Lemma 3.21 $p(a_1, \ldots, a_n) = q(b_1, \ldots, b_{k-1}, a_k) \cdot r(b_{k+1}, \ldots, b_n) = (q(b_1, \ldots, a_{k-1}, 1) \cdot a_k) \cdot r(b_{k+1}, \ldots, b_n) = q(b_1, \ldots, b_k) \cdot r(b_{k+1}, \ldots, b_n) = p(b_1, \ldots, b_n)$. □

The following corollary is an analogue of ([7], Theorem 2.4).

Corollary 3.23. *Let $a_1, \ldots, a_n$ be a sequence of elements of the right product loop S, such that at most two of them are nonidempotents. Then all products of $a_1, \ldots, a_n$, in that order, are equal to the following product of at most three of them: First – nonidempotents of $a_1, \ldots, a_{n-1}$ if any (the one with the smaller index first) and then a_n if it is not used already.* □

In right product pointed loops we need not use 1.

Theorem 3.24. *Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ $(n > 0)$ be two sequences of elements of the right product pointed loop S with the distinguished element e such that*

$$b_k = \begin{cases} e; & \text{if } k < n \text{ and } a_k \in E_S \\ a_k; & \text{if } k = n \text{ or } a_k \notin E_S \end{cases}$$

and let $p(a_1, \ldots, a_n)$ be some product of $a_1, \ldots, a_n$. Then $p(a_1, \ldots, a_n) = p(b_1, \ldots, b_n)$. □

4. Independence of axioms

Finally, we consider the independence of the axioms (A) for right product quasigroups.

It is well-known that the quasigroup axioms (Q1)–(Q4) are independent. It follows that axioms (A1) and (A2) are independent. To give just one concrete example, here is a model in which (Q2) = (A2) fails.

Example 4.1. The model $(\mathbb{Z}; \cdot, \backslash, /)$ where $x \cdot y = x + y$, $x/y = x - y$ and $x\backslash y = \max\{y - x, 0\}$ is a left quasigroup satisfying (Q1) but not (Q2), and hence satisfies (A1), (A3), (A4) and (A5), but not (A2). □

As it turns out, the independence of the remaining axioms can be easily shown by models of size 2. These were found using Mace4 [12].

Example 4.2. Table 3 is a model satisfying (A1), (A2), (A4), (A5), but not (A3).

$\cdot$	0	1
0	0	1
1	0	1

$\backslash$	0	1
0	0	1
1	0	1

$/$	0	1
0	1	0
1	1	0

Table 3: (A1), (A2), (A4), (A5), but not (A3).

Example 4.3. Table 4 is a model satisfying (A1), (A2), (A3), (A5), but not (A4). □

Example 4.4. Table 5 is a model satisfying (A1), (A2), (A3), (A4), but not (A5).

$\cdot$	0	1
0	0	1
1	1	0

$\backslash$	0	1
0	0	1
1	1	0

$/$	0	1
0	1	0
1	0	1

Table 4: (A1), (A2), (A3), (A5), but not (A4).

$\cdot$	0	1
0	1	0
1	1	0

$\backslash$	0	1
0	1	0
1	1	0

$/$	0	1
0	1	0
1	1	0

Table 5: (A1), (A2), (A3), (A4), but not (A5).

Acknowledgment. Our investigations were aided by the automated deduction program Prover9 and the finite model builder Mace4, both developed by McCune [12]

References

[1] **A. H. Clifford and G. B. Preston**, *The algebraic theory of semigroups*, Amer. Math. Soc., Providence, (1964)

[2] **Z. Daroóczy and Zs. Páles (eds.)**, *Functional equations – Results and advances*, Kluwer Academic Publishers, Dordrecht, Boston, London, (2002)

[3] **T. Evans**, *The word problem for abstract algebras*, J. London Math. Soc. **26** (1951), 64 – 71.

[4] **N. Graham**, *Note on M–groupoids*, Proc. Amer. Math. Soc. **15** (1964), 525 – 527.

[5] **M. K. Kinyon and J. D. Phillips**, *Rectangular quasigroups and loops*, Comput. Math. Appl. **49** (2005), 1679 – 1685.

[6] **R. A. Knoebel**, *Product of independent algebras with finitely generated identities*, Algebra Universalis **3/2** (1973), 147 – 151.

[7] **A. Krapež**, *Rectangular loops*, Publ. Inst. Math (Belgrade) (N.S.) **68(82)** (2000), 59 – 66.

[8] **A. Krapež**, *Generalized associativity in rectangular quasigroups*, in the book [2], 335 – 349.

[9] **A. Krapež**, *Varieties of rectangular quasigroups*, submitted.

[10] **L. Löwenheim**, *Über das Auflösungsproblem in logischen Klassenkalkul*, Sitzungsber. Berl. Math. Geselschaft **7** (1908), 90 – 94.

[11] **L. Löwenheim**, *Über die Auflösung von Gleichungen im logischen Gebietkalkul*, Math. Ann. **68** (1910), 169 – 207.

[12] **W. W. McCune**, *Prover9, version* 2008 – 06*A*, http://www.cs.unm.edu/ mccune/prover9/

[13] **S. B. Prešić**, *Une classe d'équations matricielles et l'équation fonctionelle* $f^2 = f$, Publ. Inst. Math. (Beograd) **8(22)** (1968), 143 – 148.

[14] **S. B. Prešić**, *Ein Satz über reproductive Lösungen*, Publ. Inst. Math. (Beograd) **14(28)** (1972), 133 – 136.

[15] **S. B. Prešić**, *A generalization of the notion of reproductivity*, Publ. Inst. Math. (Beograd) **67(81)** (2000), 76 – 84.

[16] **S. Rudeanu**, *Lattice Functions and Equations*, Springer–Verlag London Ltd., London, (2001).

[17] **E. Schröder**, *Vorlesungen über die Algebra der Logik*, vol. **1** (1890), vol. **2** (1891), (1905), vol. **3** (1895), reprint: Chelsea, Bronx NY, (1966).

[18] **T. Tamura, R. B. Merkel and J. F. Latimer**, *Note on the direct product of certain groupoids*, Proc. Japan Acad. **37** (1961), 482 – 484.

[19] **T. Tamura, R. B. Merkel and J. F. Latimer**, *The direct product of right singular semigroups and certain groupoids*, Proc. Amer. Math. Soc. **14** (1963), 118 – 123.

[20] **W. Taylor**, *The fine spectrum of the variety*, Alg. Universalis **5** (1975), 263 – 303.

[21] **R. J. Warne**, *The direct product of right zero semigroups and certain groupoids*, Amer. Math. Monthly **74** (1967), 160 – 164.

Received February 15, 2011

M.K.Kinyon
Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, Colorado 80208 USA
E-mail: mkinyon@math.du.edu http://www.math.du.edu/∼mkinyon

A.Krapež
Matematički institut, Kneza Mihaila 36, 11001 Beograd, p.p. 367, Serbia
E-mail: sasa@mi.sanu.ac.rs

J.D.Phillips
Department of Mathematics & Computer Science, Northern Michigan University, Marquette, MI 49855 USA, E-mail: jophilli@nmu.edu http://euclid.nmu.edu/∼jophilli/

Quasigroups and Related Systems **19** (2011), 265 – 278

Geometry of semiabelian n-ary groups

Yurii I. Kulazhenko

Abstract. Semiabelian n-ary groups are characterized by their parallelograms and symmetries of points with respect to the vertices of tetragons.

1. Introduction

If the standard (affine) geometry has a fixed point O, then any point P of this geometry is uniquely determined by the vector $\vec{p}=\overrightarrow{OP}$, and conversely, the vector $\overrightarrow{OP}$ uniquely determines the point P. Any interval $\overline{PQ}$ may be interpreted as the vector $\vec{q}-\vec{p}$ or as the vector $\vec{p}-\vec{q}$. In the second case,

$$\overline{AB}=\overline{CD} \iff \vec{a}-\vec{b}+\vec{d}=\vec{c},$$

or, in the other words

$$\overline{AB}=\overline{CD} \iff f(a,b,d)=c\,,$$

where any vector $\vec{v}$ is treated as an element v of a commutative group $(G,+)$. Then the operation f has the form $f(x,y,z)=x-y+z$. Groups (also non-commutative) with a ternary operation defined in this way were considered by J. Certaine (cf. [3]) as a special case of *ternary heaps* studied earlier by H. Prüfer (cf. [25]). Ternary heaps have interesting applications to projective geometry (cf. [1]), affine geometry (cf. [2]), theory of nets (webs), theory of knots and even to the differential geometry.

On the other hand, affine geometries may be treated as geometries defined by some ternary relations (cf. for example [31]). Such geometries may be defined also by some n-ary ($n>3$) relations (cf. [32]). Basic properties of affine geometries defined by ternary groups were described by Vakarelov (cf. [34]). Rusakov extended these results to the case of affine geometries

2010 Mathematics Subject Classification: 20N20,
Keywords: n-ary group, heap, flock, affine geometry, parallelogram, symmetry.

defined by n-ary groups (cf. [28] and [29]). Later, affine geometries induced by n-ary groups and various properties of n-ary groups connected with affine geometries were studied by many authors (see for example [7], [12], [14], [27]).

2. Preliminaries

We will use the following abbreviated notation: the sequence $x_i, \ldots, x_j$ will be denoted by x_i^j (for $j < i$ it will be the empty symbol). In the case $x_{i+1} = \ldots = x_{i+k} = x$ instead of x_{i+1}^{i+k} we will write $\overset{(k)}{x}$. In this convention the formula $f(x_1, \ldots, x_i, x, x, \ldots, x, x_{i+k+1}, \ldots, x_n)$ will be written in the form $f(x_1^i, \overset{(k)}{x}, x_{i+k+1}^n)$.

If $m = k(n-1)+1$, then the m-ary operation g of the form

$$g(x_1^{k(n-1)+1}) = \underbrace{f(f(\ldots, f(f}_{k}(x_1^n), x_{n+1}^{2n-1}), \ldots), x_{(k-1)(n-1)+2}^{k(n-1)+1})$$

is denoted by $f_{(k)}$. In certain situations, when the arity of g does not play a crucial role, or when it will differ depending on additional assumptions, we write $f_{(.)}$, to mean $f_{(k)}$ for some $k = 1, 2, \ldots$

By an *n-ary group* (G, f) we mean a non-empty set G together with one n-ary operation $f : G^n \to G$ satisfying for all $i = 1, 2, \ldots, n$ the following two conditions:

1^0 *the associative law*:

$$f(f(x_1^n), x_{n+1}^{2n-1}) = f(x_1^{i-1}, f(x_i^{n+i-1}), x_{n+i}^{2n-1})$$

2^0 for all $a_1, a_2, \ldots, a_n, b \in G$ there exits a unique $x_i \in G$ such that

$$f(a_1^{i-1}, x_i, a_{i+1}^n) = b\,.$$

Such n-ary groups may also be considered as algebras with two or more operations (see for example [6]). In particular, an n-ary group may be treated as an algebra with one associative n-ary operation and one unary operation satisfying some identities.

Theorem 2.1. *An algebra $(G, f, ^-)$ with one associative n-ary ($n > 2$) operation f and one unary operation $^- : x \mapsto \overline{x}$ is an n-ary group if and only if the identities*

$$f(\overset{(i-2)}{x}, \overline{x}, \overset{(n-i)}{x}, y) = f(y, \overset{(n-j)}{x}, \overline{x}, \overset{(j-2)}{x}) = y \tag{1}$$

are satisfied for some $i, j \in \{2, \dots, n\}$. □

Theorem 2.2. *An algebra $(G, f, ^{[-2]})$ with one associative n-ary ($n \geqslant 2$) operation f and one unary operation $^{[-2]} : x \mapsto x^{[-2]}$ is an n-ary group if and only if the identities*

$$f(x^{[-2]}, \overset{(n-2)}{x}, f(\overset{(n-1)}{x}, y)) = f(f(y, \overset{(n-1)}{x}), \overset{(n-2)}{x}, x^{[-2]}) = y \tag{2}$$

are satisfied. □

The first theorem is proved in [10], the second in [26]. Useful modifications of Theorem 2.1 one can find in [4, 6, 9].

An element $\overline{x}$ satisfying the identities (1) is called *skew* to x. It is uniquely determined as a solution of the equation $f(\overset{(n-1)}{x}, z) = x$. In general $\overline{x} \neq x$, but there are n-ary groups in which $\overline{x} = x$ for all or only for some x (cf. [5] and [8]). In some n-ary groups we have

$$\overline{f(x_1, x_2, \dots, x_n)} = f(\overline{x}_1, \overline{x}_2, \dots, \overline{x}_n), \tag{3}$$

which means that in some n-ary groups the operation $x \to \overline{x}$ is an endomorphism (cf. [8, 11, 13, 30]). This situation take place in *semiabelian* n-ary groups, i.e., in n-ary groups satisfying the identity

$$f(x_1^n) = f(x_1, x_2^{n-1}, x_n), \tag{4}$$

for example (cf. [13]). The class of all semiabelian n-ary groups coincides with the class of *medial* n-ary groups, i.e., n-ary groups in which

$$f(f(x_{11}^{1n}), f(x_{21}^{2n}), \dots, f(x_{n1}^{nn})) = f(f(x_{11}^{n1}), f(x_{12}^{n2}), \dots, f(x_{1n}^{nn})) \tag{5}$$

holds for all $x_{ij} \in G$ (cf. [13]). This condition means that the value of the operation f applied to the matrix $[x_{ij}]_{n \times n}$ is the same if we apply it to rows (from left) or to columns (from top).

As a simple consequence of results proved in [4] we obtain the following lemma.

Lemma 2.3. *For $n \geqslant 3$ an n-ary group (G, f) is semiabelian if and only if there exists $a \in G$ such that*

$$f(x, \overline{a}, \overset{(n-3)}{a}, y) = f(y, \overline{a}, \overset{(n-3)}{a}, x) \tag{6}$$

holds for all $x, y \in G$. □

In the theory of n-ary groups an important role is played by the Post's coset theorem which says that any n-ary group (G, f) can be embedded (as a coset) into some ordinary group G^* called the *covering group* for (G, f) (cf. [24]). But theory of n-ary groups can not be reduced to the theory of such groups [9]. A nice construction of a covering group is presented in [22].

Theorem 2.4. (Post's coset theorem)
For any n-ary group (G, f) there exists a binary group $(G^*, \cdot)$ such that $G \subset G^*$ and

$$f(x_1^n) = x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_n$$

for all $x_1, x_2, \ldots, x_n \in G$. In this group $\overline{x} = x^{2-n}$. □

3. Geometry of semiabelian n-ary groups

In the affine geometry defined on an n-ary group (G, f) (for details see [27] or [28]) elements of G are called *points*. Four points $a, b, c, d \in G$ define a *parallelogram* if and only if

$$f(f(a, b^{[-2]}, \overset{(n-2)}{b}), \overset{(n-2)}{b}, c) = d.$$

Two points a and c are *symmetric* if and only if there exists a uniquely determined point $x \in G$ such that

$$f(f(a, x^{[-2]}, \overset{(n-2)}{x}), \overset{(n-2)}{x}, c) = x.$$

Since the operation f is associative identities (2) used in Theorem 2.2 can be written in the form

$$f(f(x^{[-2]}, \overset{(n-1)}{x}), \overset{(n-2)}{x}, y) = f(y, \overset{(n-2)}{x}, f(\overset{(n-1)}{x}, x^{[-2]})) = y,$$

which together with Theorem 2.1 implies

$$f(x^{[-2]}, \overset{(n-1)}{x}) = f(\overset{(n-1)}{x}, x^{[-2]}) = \overline{x}\,, \tag{7}$$

where $\overline{x}$ denotes the element skew to x. Thus for $n \geqslant 3$ the above two definitions can be presented in the following more useful form (cf. [7]):

Definition 3.1. Four points a, b, c, d of an n-ary group (G, f), where $n \geqslant 3$, define a *parallelogram* if and only if $f(a, \overline{b}, \overset{(n-3)}{b}, c) = d$.

Definition 3.2. Two elements a and c of an n-ary group (G, f) are *symmetric* if there exists a uniquely determined point $x \in G$ such that

$$f(a, \overline{x}, \overset{(n-3)}{x}, c) = x. \tag{8}$$

Since for symmetric points a and c of G the element x is uniquely determined we can consider the map $S_x : G \to G$ with the property $S_x(a) = c$. This map will be called the *symmetry*.

Definition 3.3. The point x of an n-ary group (G, f) is *self-returning* with respect to the finite sequence of points $a, b, c, \ldots, v \in G$ if

$$S_v(\ldots S_c(S_b(S_a(x)))) = x.$$

From the definition of an n-ary group it follows that in (8) an element c is uniquely determined by elements a and x. Thus, using the same method as in [4] and [10], we can prove that for $n \geqslant 3$ the symmetry S_x has the form:

$$S_x(a) = f(x, \overline{a}, \overset{(n-3)}{a}, x).$$

The point

$$S_a(b) = (a, \overline{b}, \overset{(n-3)}{b}, a)$$

is called *symmetrical* to the point b with respect to the point a. The sequence of k arbitrary elements from G is called a *k-gon* (cf. [29]).

In view of Theorem 2.4 the symmetry of points of an n-ary group can be considered as an *external* symmetry in the corresponding covering group. Namely, *two points a and c of an n-ary group (G, f) are symmetric if there exists a uniquely determined point $x \in G$ such that $ax^{-1}c = x$ in the covering group G^* of (G, f)*. Note that in general x^{-1} is not an element of G.

In this case, the symmetry S_a has the form

$$S_a(x) = ax^{-1}a. \tag{9}$$

Moreover, as a consequence of Lemma 2.3 we obtain

Corollary 3.4. *An n-ary group (G, f) is semiabelian if and only if its covering group we have*

$$ax^{-1}b = bx^{-1}a \tag{10}$$

for all $a, b \in G$ and some fixed $x \in G$. □

Lemma 3.5. *Let $a_1, a_2, a_3, \ldots, a_m$ be arbitrary points of a semiabelian n-ary group (G, f). Then the composition $S_{a_m}(...S_{a_4}(S_{a_3}(S_{a_2}(S_{a_1}(x))))...)$ is equal to*

$$f_{(m)}(x, \underbrace{\overline{a}_1, \overset{(n-3)}{a_1}, a_2}_{2}, \underbrace{\overline{a}_3, \overset{(n-3)}{a_3}, a_4}_{2}, \ldots, \underbrace{\overline{a}_{m-1}, \overset{(n-3)}{a_{m-1}}, a_m}_{2})$$

if m is even, or to

$$f_{(m)}(S_{a_1}(x), \underbrace{\overline{a}_2, \overset{(n-3)}{a_2}, a_3}_{2}, \underbrace{\overline{a}_4, \overset{(n-3)}{a_4}, a_5}_{2}, \ldots, \underbrace{\overline{a}_{m-1}, \overset{(n-3)}{a_{m-1}}, a_m}_{2})$$

if m is odd.

Proof. Indeed, for points $a, b, x \in G$ we have

$$\begin{aligned} S_bS_a(x) = S_b(S_a(x)) &\overset{(9)}{=} b(ax^{-1}a)^{-1}b = ba^{-1}xa^{-1}b \overset{(10)}{=} xa^{-1}ba^{-1}b \\ &\overset{(9)}{=} f_{(2)}(x, \overline{a}, \overset{(n-3)}{a}, b, \overline{a}, \overset{(n-3)}{a}, b). \end{aligned}$$

Similarly,

$$\begin{aligned} S_c(S_bS_a(x)) &\overset{(9)}{=} c(xa^{-1}ba^{-1}b)^{-1}c = cb^{-1}ab^{-1}ax^{-1}c \overset{(10)}{=} ax^{-1}ab^{-1}cb^{-1}c \\ &\overset{(9)}{=} f_{(3)}(a, \overline{x}, \overset{(n-3)}{x}, a, \overline{b}, \overset{(n-3)}{b}, c, \overline{b}, \overset{(n-3)}{b}, c) \\ &= f_{(3)}(S_a(x), \overline{b}, \overset{(n-3)}{b}, c, \overline{b}, \overset{(n-3)}{b}, c). \end{aligned}$$

Consequently,

$$\begin{aligned} S_d(S_c(S_bS_a(x))) &= S_d(S_c(xa^{-1}ba^{-1}b)) = (xa^{-1}ba^{-1}b)c^{-1}dc^{-1}d \\ &= f_{(4)}(x, \overline{a}, \overset{(n-3)}{a}, b, \overline{a}, \overset{(n-3)}{a}, b, \overline{c}, \overset{(n-3)}{c}, d, \overline{c}, \overset{(n-3)}{c}, d) \\ &= f_{(4)}(x, \underbrace{\overline{a}, \overset{(n-3)}{a}, b}_{2}, \underbrace{\overline{c}, \overset{(n-3)}{c}, d}_{2}) \end{aligned}$$

and so on. □

Proposition 3.6. *In any semiabelian n-ary group (G, f) for all elements $a_1, a_2, \ldots, a_m, x \in G$, where m is odd, we have*

$$T_{a_1^m}(T_{a_1^m}(x)) = x\,, \tag{11}$$

where $T_{a_1^m}(x) = S_{a_m}(\ldots S_{a_3}(S_{a_2}(S_{a_1}(x)))...)$.

Proof. According to Lemma 3.5 and (9) for odd m we have

$$T_{a_1^m}(x) = a_1 x^{-1} a_1 a_2^{-1} a_3 a_2^{-1} a_3 a_4^{-1} a_5 a_4^{-1} a_5 \ldots a_{m-1}^{-1} a_m a_{m-1}^{-1} a_m\,,$$

which together with (10) implies (11). □

Corollary 3.7. *Each point of a semiabelian n-ary group is self-returning with respect to double symmetry with respect to the vertex of an arbitrary its polygon with odd number of vertex.* □

These results give the possibility to make new short proofs of the theorems proved in [15 – 21]. Below we give some of them.

Theorem 3.8. *An n-ary group (G, f) is semiabelian if and only if*

$$S_b(S_c(S_d(S_a(x)))) = x \tag{12}$$

for any parallelogram $\langle a, b, c, d\rangle$ of (G, f) and an arbitrary $x \in G$.

Proof. From the above results it follows that points a, b, c, d form a parallelogram of an n-ary group (G, f) if and only if $ab^{-1}c = d$ holds in a covering group of (G, f). This together with (9) reduces (12) to the form

$$bc^{-1}ab^{-1}ca^{-1}x = x.$$

Thus $bc^{-1}a = (b^{-1}ca^{-1})^{-1} = ac^{-1}b$. So, $f(b, \overline{c}, \overset{(n-3)}{c}, a) = f(a, \overline{c}, \overset{(n-3)}{c}, b)$, which by Lemma 2.3 means that (G, f) is semiabelian.

The converse statement is obvious. □

Theorem 3.9. *An n-ary group (G, f) is semiabelian if and only if*

$$S_d(S_c(S_b(S_a(x)))) = x$$

for any parallelogram $\langle a, b, c, d\rangle$ of (G, f) and an arbitrary $x \in G$.

Proof. The proof is analogous to the proof of Theorem 3.8. □

Corollary 3.10. *An n-ary group is semiabelian if and only if each its point is self-returning with respect to the vertex of each its parallelogram.* □

Theorem 3.11. *An n-ary group (G, f) is semiabelian if and only if for any three points $a, b, c \in G$ the tetragon $\langle a, S_b(a), S_c(a), S_d(a)\rangle$, where $d = f(a, \overline{b}, {}^{(n-3)}b, c)$, is a parallelogram.*

Proof. Indeed, in the covering group G^* of (G, f) we have $S_d(a) = ab^{-1}cb^{-1}c$ and $a(S_b(a))^{-1}S_c(a) = ab^{-1}ab^{-1}ca^{-1}c$. Thus $a(S_b(a))^{-1}S_c(a) = S_d(a)$ if and only if $ab^{-1}c = cb^{-1}a$. Corollary 3.4 completes the proof. □

Analogously we can prove the following two theorems.

Theorem 3.12. *An n-ary group is semiabelian if and only if for any three its points a, b, c (at least) one of the following tetragons $\langle a, b, S_c(a), S_c(b)\rangle$, $\langle S_b(a), S_c(a), S_c(b), b\rangle$, $\langle S_{S_c(b)}(a), S_c(b), b, S_c(a)\rangle$ is a parallelogram.* □

Theorem 3.13. *An n-ary group (G, f) is semiabelian if and only if for each $a, b, c \in G$ all points $x \in G$ are self-returning with respect to the vertex of the hexagon $\langle S_b(a), S_c(a), S_c(b), S_a(b), S_a(c), S_b(c)\rangle$.* □

4. Vectors of semiabelian n-ary groups

According to [28] an ordered pair $\langle a, b\rangle$ of points $a, b \in G$ is called a *directed segment* of an n-ary group (G, f).In the set of all directed segments of an n-ary group we introduce the binary relation $=$ by putting

$$\langle a, b\rangle = \langle c, d\rangle \Longleftrightarrow f(a, \overline{b}, {}^{(n-3)}b, c) = d\,,$$

i.e., $\langle a, b\rangle = \langle c, d\rangle$ if and only if $\langle a, b, c, d\rangle$ is a parallelogram of G. Such defined relation is an equivalence and divides the set of all directed segments into disjoint classes $\langle a, b\rangle_=$. The class $\langle a, b\rangle_=$ is called a *vector* and is denoted by $\overrightarrow{ab}$. Hence

$$\overrightarrow{ab} = \overrightarrow{cd} \Longleftrightarrow f(a, \overline{b}, {}^{(n-3)}b, c) = d \Longleftrightarrow ab^{-1}c = d \tag{13}$$

in the covering group of (G, f).

On the set $V(G)$ of all vectors defined on an n-ary group (G, f) one can define the addition $+$ of vectors (cf. [28]). It is not difficult to verify that $(V(G), +)$ is a group. It is Abelian if and only if an n-ary group (G, f) is semiabelian (for details see [28] or [29]).

Lemma 4.1. *In an n-ary group (G, f) for any four points a, b, c, d of G we have*

$$\overrightarrow{a\,b} + \overrightarrow{c\,d} = \overrightarrow{a\,g} = \overrightarrow{h\,d}\,,$$

where $g = f(b, \overline{c}, \overset{(n-3)}{c}, d)$ and $h = f(c, \overline{b}, \overset{(n-3)}{b}, a)$.

Proof. Since in the covering group $g = f(b, \overline{c}, \overset{(n-3)}{c}, d) = bc^{-1}d$, thus

$$f(c, \overline{b}, \overset{(n-3)}{b}, g) = cb^{-1}g = cb^{-1}(bc^{-1}d) = d\,.$$

So, $\langle c, b, g, d\rangle$ is a parallelogram. Hence $\overrightarrow{cd} = \overrightarrow{bg}$. Consequently, $\overrightarrow{ab} + \overrightarrow{cd} = \overrightarrow{ab} + \overrightarrow{bg} = \overrightarrow{ag}$.

The proof of the second identity is analogous. □

Corollary 4.2. *In an n-ary group (G, f) we have*

$$\overrightarrow{ab} + \overrightarrow{cd} = \overrightarrow{a(bc^{-1}d)} \tag{14}$$

for all a, b, c, d of G. □

Theorem 4.3. *An n-ary group (G, f) is semiabelian if and only if*

$$\overrightarrow{ab} + \overrightarrow{cd} = \overrightarrow{ad} + \overrightarrow{cb} \tag{15}$$

for all $a, b, c, d \in G$.

Proof. Indeed, by Lemma 4.1

$$\overrightarrow{ab} + \overrightarrow{cd} = \overrightarrow{ag_1}, \qquad \overrightarrow{ad} + \overrightarrow{cb} = \overrightarrow{ag_2}\,,$$

where $g_1 = f(b, \overline{c}, \overset{(n-3)}{c}, d)$, $g_2 = f(d, \overline{c}, \overset{(n-3)}{c}, b)$. Thus $\overrightarrow{ag_1} = \overrightarrow{ag_2}$ if and only if $\langle a, a, g_1, g_2\rangle$ is a parallelogram, i.e., if and only if $f(a, \overline{a}, \overset{(n-3)}{a}, g_1) = g_2$. The last means that $g_1 = g_2$. This, by Lemma 2.3, means that an n-ary group (G, f) is semiabelian. □

Theorem 4.4. *An n-ary group (G, f) is semiabelian if and only if*

$$\overrightarrow{S_b(a)S_d(c)} = 2\,\overrightarrow{bd} + \overrightarrow{ca} \tag{16}$$

for all $a, b, c, d \in G$.

Proof. Indeed, if an n-ary group (G, f) is semiabelian, then

$$\begin{aligned}\overrightarrow{S_b(a)S_d(c)} &\overset{(9)}{=} \overrightarrow{(ba^{-1}b)(dc^{-1}d)} \overset{(14)}{=} \overrightarrow{(ba^{-1}b)d} + \overrightarrow{cd} \overset{(14)}{=} (\overrightarrow{ba} + \overrightarrow{bd}) + \overrightarrow{cd} \\ &= \overrightarrow{bd} + (\overrightarrow{ba} + \overrightarrow{cd}) \overset{(15)}{=} \overrightarrow{bd} + (\overrightarrow{bd} + \overrightarrow{ca}) = 2\overrightarrow{bd} + \overrightarrow{ca}\,,\end{aligned}$$

which proves (16).

Conversely, if (16) holds for all points $a, b, c, d \in G$, then

$$2\overrightarrow{bd} + \overrightarrow{ca} = \overrightarrow{S_b(a)S_d(c)} = \overrightarrow{ba} + \overrightarrow{bd} + \overrightarrow{cd}\,,$$

which, in view of (14), implies

$$\overrightarrow{b(db^{-1}d)} + \overrightarrow{ca} = \overrightarrow{b(ab^{-1}d)} + \overrightarrow{cd}\,.$$

Thus

$$\overrightarrow{b(db^{-1}dc^{-1}a)} = \overrightarrow{b(ab^{-1}dc^{-1}d)}\,.$$

So, that the tetragon $\langle b, b, (db^{-1}dc^{-1}a), (ab^{-1}dc^{-1}d)\rangle$ is a parallelogram. Hence $bb^{-1}(db^{-1}dc^{-1}a) = ab^{-1}dc^{-1}d$. From this, for $c = d$, we obtain

$$db^{-1}a = ab^{-1}d\,.$$

This by Lemma 2.3 means that an n-ary group (G, f) is semiabelian. □

Using the above method we can give a short proof of the following two theorems proved in [21].

Theorem 4.5. *An n-ary group (G, f) is semiabelian if and only if for each its parallelogram $\langle a, b, c, d\rangle$ and each point $x \in G$ we have*

$$\overrightarrow{x\,a} + \overrightarrow{S_a(x)\,b} + \overrightarrow{S_bS_a(x)\,c} + \overrightarrow{S_cS_bS_a(x)\,d} = \overrightarrow{0}\,. \tag{17}$$

Proof. For any four pints $a, b, c, d \in G$ we have

$$\begin{aligned}&\overrightarrow{x\,a} + \overrightarrow{S_a(x)\,b} + \overrightarrow{S_bS_a(x)\,c} + \overrightarrow{S_cS_bS_a(x)\,d} \\ &\quad\overset{(9)}{=} \overrightarrow{x\,a} + \overrightarrow{(ax^{-1}a)\,b} + \overrightarrow{(ba^{-1}xa^{-1}b)\,c} + \overrightarrow{(cb^{-1}ax^{-1}ab^{-1}c)\,d} \\ &\quad\overset{(14)}{=} \overrightarrow{x\,(xa^{-1}b)} + \overrightarrow{(ba^{-1}xa^{-1}b)\,c} + \overrightarrow{(cb^{-1}ax^{-1}ab^{-1}c)\,d} \\ &\quad\overset{(14)}{=} \overrightarrow{x\,(ab^{-1}c)} + \overrightarrow{(cb^{-1}ax^{-1}ab^{-1}c)\,d} \overset{(14)}{=} \overrightarrow{x\,(xa^{-1}bc^{-1}d)}\,.\end{aligned}$$

So, according to (13),

$$\overrightarrow{x\,(xa^{-1}bc^{-1}d)} = \overrightarrow{0} = \overrightarrow{x\,x} \iff xd^{-1}cb^{-1}a = x \iff d = cb^{-1}a\,.$$

Hence any four points a, b, c, d satisfying (17) form a parallelogram if and only if $d = cb^{-1}a = ab^{-1}c$. Corollary 3.4 completes the proof. □

Theorem 4.6. *An n-ary group (G, f) is semiabelian if and only if*

$$\overrightarrow{x\,a}+\overrightarrow{S_a(x)\,b}+\overrightarrow{S_bS_a(x)\,c}+\overrightarrow{S_cS_bS_a(x)\,d}+\overrightarrow{S_dS_cS_bS_a(x)\,e}+\overrightarrow{S_eS_dS_cS_bS_a(x)\,a} = \overrightarrow{0} \tag{18}$$

for all points $a, b, c, d, x \in G$, where $e = f(d, \overline{c}, {}^{(n-3)}c, b)$.

Proof. Similarly as in the previous proof

$$\begin{aligned}\overrightarrow{xa} + \overrightarrow{S_a(x)\,b} + \overrightarrow{S_bS_a(x)\,c} + \overrightarrow{S_cS_bS_a(x)\,d} + \overrightarrow{S_dS_cS_bS_a(x)\,e} + \overrightarrow{S_eS_dS_cS_bS_a(x)\,a}\\ = \overrightarrow{x\,(xa^{-1}bc^{-1}d)} + \overrightarrow{S_dS_cS_bS_a(x)\,e} + \overrightarrow{S_eS_dS_cS_bS_a(x)\,a}\\ = \overrightarrow{x\,(ab^{-1}cd^{-1}e)} + \overrightarrow{S_eS_dS_cS_bS_a(x)\,a} = \overrightarrow{x\,(xa^{-1}bc^{-1}de^{-1}a)}\,.\end{aligned}$$

Hence

$$\overrightarrow{x\,(xa^{-1}bc^{-1}de^{-1}a)} = \overrightarrow{x\,x} \iff xa^{-1}ed^{-1}cb^{-1}a = x\,.$$

The last means that $a^{-1}e = (d^{-1}cb^{-1}a)^{-1} = a^{-1}bc^{-1}d$, i.e., $e = bc^{-1}d$. But by the assumption $e = dc^{-1}b$. So, (18) holds if and only if $bc^{-1}d = dc^{-1}b$ for all $a, b, c \in G$. □

5. Flocks

Flocks are ternary quasigroups with a *para-associative operation*, i.e., algebras of the form $(G, [\,])$, where $[[x, y, z], u, v] = [x, [u, z, y], v] = [x, y, [z, u, v]]$ for all $x, y, z, u, v \in G$, and for all $a, b \in G$ there are uniquely determined $x, y, z \in G$ such that $[x, a, b] = [a, y, b] = [a, b, z] = c$.

Such flocks are a special case of heaps and semiheaps considered by Vagner [33]. Similar structures are investigated also by Prüfer [25]. Baer (cf. [1]) has investigated a connection linking Brandt groupoids and mixed groups with *idempotent flocks*, i.e., flocks satisfying the identity $[x, x, x] = x$.

As it was observed in [7] flocks and ternary groups have very similar properties. Moreover, the affine geometry induced by n-ary groups ($n > 3$)

can be described by flocks. Namely, if (G, f) is an n-ary group with $n > 3$ then G with the operation

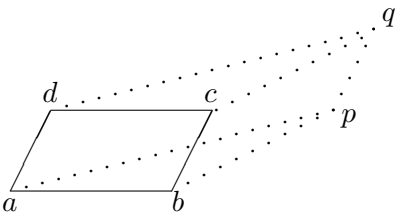
$$[x, y, z] = f(x, \overline{y}, \overset{(n-3)}{y}, z)$$

is a flock. Thus, in the covering group of (G, f) we have $[x, y, z] = xy^{-1}z$. This means that flocks induced by semiabelian n-ary groups are idempotent ternary group.

Theorem 5.1. *Let $\langle a, b, c, d\rangle$ be a parallelogram on an n-ary group (G, f). Then for all $p, q, x, y \in G$*

(1) *$\langle b, p, q, c\rangle$ is a parallelogram if and only if $\langle a, p, q, d\rangle$ is a parallelogram.*
(2) *$\langle d, c, x, y\rangle$ is a parallelogram if and only if $\langle a, b, x, y\rangle$ is a parallelogram.*

The geometrical sense of this theorem is illustrated by the picture:



This theorem is a consequence of Proposition 5.5 proved in [7]. Below we give the equivalent proof based on the above connections.

Proof. Let $\langle a, b, c, d\rangle$ and $\langle b, p, q, c\rangle$ be parallelograms. Then $d = [a, b, c] = ab^{-1}c$ and $c = [b, p, q] = bp^{-1}q$. Thus $[a, p, q] = (ab^{-1}b)p^{-1}q = ab^{-1}(bp^{-1}q) = d$. Hence $\langle a, p, q, d\rangle$ is a parallelogram.

Conversely, if $\langle a, b, c, d\rangle$ and $\langle a, p, q, d\rangle$ are parallelograms, then $ab^{-1}c = d$ and $ap^{-1}q = d$. Thus, $[b, p, q] = (ba^{-1}a)p^{-1}q = ba^{-1}(ap^{-1}q) = ba^{-1}d = c$, which completes the proof of (1). The proof of (2) is analogous. □

Acknowledgements. The author would like to express his warmest thanks to the editor of the journal Professor Wieslaw A. Dudek for his comments and suggestions, especially for the paper [7].

References

[1] **R. Baer**, *Linear algebra and projective geometry*, Academic Press, New York, 1952.

[2] **D. Brănzei**, *Structures affines et opérations ternaires*, An. Şti. Univ. Iaşi, Sect. I a Mat. (N.S.) **23** (1977), 33 – 38.

[3] **J. Certaine**, *The ternary operation* $(abc) = ab^{-1}c$ *of a group*, Bull. Amer. Math. Soc. **49** (1943), 869 – 877.

[4] **W. A. Dudek**, *Remarks on n-groups*, Demonstr. Math. **13** (1980), 165−181.

[5] **W. A. Dudek**, *Medial n-groups and skew elements*, Proc. V Universal Algebra Symposium "Universal and Applied Algebra", Turawa 1988, World Scientific, Singapore 1989, 55 – 80.

[6] **W. A. Dudek**, *Varieties of polyadic groups*, Filomat **9** (1995), 657 – 674.

[7] **W. A. Dudek**, *Ternary quasigroups connected with the affine geometry*, Algebras, Groups and Geometries **16** (1999), 329 – 354.

[8] **W. A. Dudek**, *On some old and new problems in n-ary groups*, Quasigroups and Related Systems **8** (2001), 15 – 36.

[9] **W. A. Dudek, K. Glazek**, *Around the Hosszú-Gluskin Theorem for n-ary groups*, Discrete Math. **308** (2008), 4861 – 4876.

[10] **W. A. Dudek, K. Glazek, B. Gleichgewicht**, *A note on the axioms of n-groups*, Colloquia Math. Soc. J. Bolyai 29 "Universal Algebra", Esztergom (Hungary) 1977, 195 – 202. (North-Holland, Amsterdam 1982.)

[11] **W. A. Dudek, N. A. Shchuchkin**, *Skew endomorphisms on some n-ary groups*, Quasigroups and Related Systems **17** (2009), 205 – 228.

[12] **W. A. Dudek, Z. Stojaković**, *On Rusakov's n-ary rs-groups*, Czechoslovak Math. J. **51(126)** (2001), 275 – 283.

[13] **K. Glazek, B. Gleichgewicht**, *Abelian n-groups*, Colloquia Math. Soc. J. Bolyai 29 "Universal Algebra", Esztergom (Hungary) 1977, 321−329. (North-Holland, Amsterdam 1982.)

[14] **Yu. I. Kulazhenko**, *Geometry of parallelograms*, (Russian), Vopr. Algeb. and Prik. Mat., Izdat. Belorus. Gos. Univ. Transp., Gomel 1995, 65 – 82.

[15] **Yu. I. Kulazhenko**, *Self-returning elements of n-ary groups*, (Russian), Some problems of algebra and appl. math., Gomel, 2002, 66 – 71.

[16] **Yu. I. Kulazhenko**, *Criterions of semiabelity of an n-ary group* $G = \langle X, (\ ), {}^{[-2]} \rangle$ *expressed by self-returning elements*, (Russian), Izv. Gomel. Gos. Univ. **2(41)** (2007), 55 – 58.

[17] **Yu. I. Kulazhenko**, *Symmetry, hexagons and semiabelity of n-ary groups*, (Russian), Izv. Gomel. Gos. Univ. **2(47)** (2008), 99 – 106.

[18] **Yu. I. Kulazhenko**, *Quadrangles, semiabelity and self-returning elements of n-ary groups*, (Russian), Izv. Gomel. Gos. Univ. **6(51)** (2008), 149 – 155.

[19] **Yu. I. Kulazhenko**, *Semiabelity and self-returning points of n-ary groups with respect to verticles of quadrandles*, (Russian), Izv. Gomel. Gos. Univ. **2(53)** (2009), 150 – 156.

[20] **Yu. I. Kulazhenko**, *Self-returning of elements of n-ary groups*, (Russian), Izv. Gomel. Gos. Univ. **3(60)** (2010), 211 – 218.

[21] **Yu. I. Kulazhenko**, *Semi-commutativity criteria and self-coincidence of elements expressed by vectors properties of n-ary groups*, Algebra and Discrete Math. **9** (2010), no.2, 98 – 107.

[22] **J. Michalski**. *Covering k-groups of n-groups*, Arch. Math. (Brno) **17** (1981), 207 – 226.

[23] **A. Yu. Olshanskii**, *Geometry of defining relations in groups*, (Russian), Sovremiennaya Algebra, Nuaka, Moscow, 1989.

[24] **E. L. Post**, *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1940), 208 – 350.

[25] **H. Prüfer**, *Theorie der Abelschen Gruppen*, Math. Z. **20** (1924), 166 – 187.

[26] **S. A. Rusakov**, *A definition of an n-ary group*, (Russian), Doklady AN BSSR **23** (1979), 965 – 967.

[27] **S. A. Rusakov**, *Existence of n-ary rs-groups* (Russian), Voprosy Algebry **6** (1992), 89 – 92.

[28] **S. A. Rusakov**, *Vectors of n-ary groups. Linear operations and their properties* (Russian), in Vopr. Algeb. and Prik. Mat. Izdat. Belorus. Gos. Univ. Transp., Gomel 1995, 10 – 30.

[29] **S. A. Rusakov**, *Some applications of the theory of n-ary groups*, (Russian), Belaruskaya navuka, Minsk, 1998.

[30] **F. M. Sokhatsky**, *On Dudek's problems on the skew operation in polyadic groups*, East Asian Math. J. **19** (2003), 63 – 71.

[31] **W. Szmielew**, *From the affine to Euclidean geometry* (Polish edition), PWN Warszawa, 1981.

[32] **W. Szmielew**, *Theory of n-ary equivalences and its application to geometry*, Dissertationes Math. **191** (1980).

[33] **V. V. Vagner**, *Theory of generalized heaps and generalized groups*, (Russian), Mat. Sbornik **32(74)** (1953), 545 – 632.

[34] **D. Vakarelov**, *Ternary groups*, (Bulgarian), God. Sofij. Univ., Mat. Fak. **61** (1966/67), 71 – 105.

Received February 4, 2011
Received November 14, 2011

Gomel State University, Gomel, Belarus
E-mail: kulazhenko@gsu.by

Quasigroups and Related Systems **19** (2011), 279 – 286

Transversals in loops. 2. Structural theorems

Eugene A. Kuznetsov

Abstract. An investigation of a new notion of a transversal in a loop to its subloop is continued in the present article. This notion generalized a well-known notion of a transversal in a group to its subgroup and can be correctly defined only in the case, when some specific condition (condition A) for a loop and its subloop is fulfilled. The connections between transversals in some loop to its subloop and transversals in multiplicative group of this loop to suitable subgroup are studied in this work.

1. Introduction

In the present work we continue the study of a variant of natural generalization of a notion of transversal in a group to its subgroup [1, 5, 6, 11] at the class of loops, begun in [10]. As the elements of a left (right) transversal in a group to its subgroup are the representatives of every left (right) coset to the subgroup, then a notion of a left (right) transversal in a loop to its subloop can be well defined only in the case when this loop admits a left (right) coset decomposition by its subloop (see Condition A, Definition 2.4, [10]).

In the part 2 the different structural theorems are proved. They demonstrate the correspondence between transversals in a loop to its subloop and transversals in a multiplicative group of this loop to its suitable subgroup. Also, we demonstrate the necessity of Condition A when we generalize a notion of transversal at the class of loops.

Further, we shall use the following notations: $\langle L, \cdot, e\rangle$ is an initial loop with the unit e; $\langle R, \cdot, e\rangle$ is its proper subloop; E is a set of indexes ($1 \in E$) of the left (right) cosets R_i in L to R, where $R_1 = R$.

All necessary definitions and preliminary statements may be found in [10].

2010 Mathematics Subject Classification: 20N05
Keywords: quasigroup, loop, transversal, coset, representation.

2. The Condition A and included subgroups

The following lemma is an explanation of the necessity of the Condition A in the investigation of transversals in loops.

Lemma 2.1. *Let G be a group, H be its proper subgroup. Let K be a subgroup of group G such that $H \subseteq K \subset G$. If $T = \{t_i\}_{i\in E}$ is a left transversal G to H, then:*

1. *$T_1 = T|_K = \{t_j\}_{j\in E_1}$, where $E_1 = \{x \in E \,|\, t_x \in K\}$, is a left transversal K to H,*
2. *$< E_1, \overset{(T_1)}{\cdot}, 1 > \subset < E, \overset{(T)}{\cdot}, 1 >$,*
3. *The left Condition A is fulfilled in the left loop $< E, \overset{(T)}{\cdot}, 1 >$ to its left subloop $< E_1, \overset{(T)}{\cdot}, 1 >$: for every $a, b \in < E, \overset{(T)}{\cdot}, 1 >$ and every $u \in < E_1, \overset{(T)}{\cdot}, 1 >$ there exist $c \in < E, \overset{(T)}{\cdot}, 1 >$ and $u_1 \in < E_1, \overset{(T)}{\cdot}, 1 >$ such that $a \overset{(T)}{\cdot} (b \overset{(T)}{\cdot} u) = c \overset{(T)}{\cdot} u_1$.*

Proof. 1. Let us denote $E_1 = \{x \in E \,|\, t_x \in K\}$. Then the transversal $T_1 = \{t_j\}_{j\in E_1}$ consists of those elements of the transversal T which belong to the subgroup K. Let us take an arbitrary element $g \in K$; since $T = \{t_i\}_{i\in E}$ is a transversal G to H, then $g = t_{i_0} \cdot h$, $t_{i_0} \in T$, $h \in H$. But $g \in K$, $h \in H \subseteq K$, so we obtain that $t_{i_0} \in K$. Then every element $g \in K$ can be represented in the form $g = t_x \cdot h$, where $h \in H$ and

$$x \in E_1 = \{z \in E \,|\, t_z \in K \cap T\}.$$

This representation is unique for every $g \in K$, because it is the same for the transversal T in G to H.

2. Let us consider the set E_1 introduced in 1. Let $t_a, t_b \in K$ (is equal $t_a, t_b \in T_1$), then $K \ni t_a \cdot t_b = (t_c h)$ $h \in H$. As $t_c \in K$, then $t_c \in T_1$ and we obtain: $c \in E_1$. Thus $a \overset{(T_1)}{\cdot} b = c$. But $t_a t_b \in K \subset G$, and $G \ni t_a \cdot t_b = (t_c h)$, $h \in H$, so $a \overset{(T)}{\cdot} b = c$. Therefore

$$(\overset{(T_1)}{\cdot}) \equiv (\overset{(T)}{\cdot})|_{E_1},$$

and finally $< E_1, \overset{(T_1)}{\cdot}, 1 > \subset < E, \overset{(T)}{\cdot}, 1 >$.

3. Let $a, b \in E$ and $x \in E_1$ (is equal $t_a, t_b \in G$ and $t_x \in K$), then

$$\begin{aligned} &t_a \cdot t_b \cdot t_x = t_a t_{b \overset{(T)}{\cdot} x} h' = t_{a \overset{(T)}{\cdot} (b \overset{(T)}{\cdot} x)} h'', \\ &t_a \cdot t_b \cdot t_x = t_{a \overset{(T)}{\cdot} b} h_1 t_x, \quad h_1 \in H, \quad h', h'' \in H. \end{aligned} \tag{1}$$

But $K \ni h_1 t_x = (t_u h'_1)$, $h'_1 \in H$, $u = \hat{t}_u(1) = \hat{t}_u \hat{h}'_1(1) = \hat{h}_1 \hat{t}_x(1) = \hat{h}_1(x)$, $h_1 t_x = (t_{\hat{h}_1(x)} h'_1) \in K$, $t_{\hat{h}_1(x)} \in K$, $\hat{h}_1(x) \in E_1$. So, (1) can be rewritten in the form

$$t_{a \overset{(T)}{\cdot} (b \overset{(T)}{\cdot} x)} h'' = t_{a \overset{(T)}{\cdot} b} t_{\hat{h}_1(x)} h'_1 = t_{(a \overset{(T)}{\cdot} b) \overset{(T)}{\cdot} \hat{h}_1(x)} h''_1.$$

Hence

$$a \overset{(T)}{\cdot} (b \overset{(T)}{\cdot} x) = (a \overset{(T)}{\cdot} b) \overset{(T)}{\cdot} \hat{h}_1(x).$$

Then for the left loop $< E, \overset{(T)}{\cdot}, 1 >$ and its left subloop $< E_1, \overset{(T_1)}{\cdot}, 1 >$ the left Condition A is fulfilled. □

Lemma 2.2. *Let $H \subseteq K \subset G$ be groups and let $T^* = \{t_x\}_{x \in E_0}$ be a left transversal G to K. Then T^* (as a set) can be always supplemented up to some left transversal $T = \{t_x\}_{x \in E}$ of G to H.*

Proof. If $T^* = \{t_x\}_{x \in E_0}$ is the left transversal G to K, then

$$(t_x K) \cap (t_y K) = \varnothing \quad \forall x, y \in E_0, \quad x \neq y.$$

Since $H \subseteq K$, we have $(t_x H) \cap (t_y H) = \varnothing$ for all $x, y \in E_0$, $x \neq y$.

If $K \equiv H$ then everything is proven. Let $H \subset K$ and we shall consider a union

$$S_0 = \bigcup_{x \in E_0} (t_x H).$$

Since

$$S_0 = \bigcup_{x \in E_0} (t_x H) \subset \bigcup_{x \in E_0} (t_x K) = G,$$

then S_0 is a subset in G consisting of a collection of left cosets in G to H. Supplementing S_0 up to G by left cosets in G to H, which consists in $(G - S_0)$, and choosing in every coset an unique representative, we obtain a required left transversal $T = \{t_x\}_{x \in E}$. Moreover, $T^* \subset T$ and $E_0 \subseteq E$. □

Lemma 2.3. *Let the assumptions of Lemma 2.2 be satisfied. Let $T^* = \{t_x\}_{x \in E_0}$ be a left transversal G to K, and $T = \{t_x\}_{x \in E}$ be a such left transversal G to H, for which $T^* \subseteq T$ and $E_0 \subseteq E$. Then $T_1 = T \cap K = \{t_x\}_{x \in E_1}$ is a left transversal K to H and the following statements are true:*

1. *All elements of the subset E_0 form a left transversal the left loop $< E, \overset{(T)}{\cdot}, 1 >$ to its left subloop $< E_1, \overset{(T)}{\cdot}, 1 >$.*
2. *The operations $< E_0, \overset{(T^*)}{\cdot}, 1 >$ and $< E_0, \overset{(E_0)}{\cdot}, 1 >$ are isomorphic (the first operation is a transversal operation that corresponds to the*

left transversal T^* in G to K, the second corresponds to a left transversal E_0 in the left loop $< E, \overset{(T)}{\cdot}, 1 >$ to its left subloop $< E_1, \overset{(T)}{\cdot}, 1 >$).

Proof. According to Lemma 2.1 $T_1 = T \cap K$ is a left transversal K to H.

1. Let g be an arbitrary element of G. Then

$$g = t_x k, \quad t_x \in T^* \subseteq T, \quad k \in K, \quad x \in E_0,$$

and, on the other hand,

$$g = t_y h_1, \quad t_y \in T, \quad h_1 \in H, \quad y \in E.$$

Also $k = t_z h_2,\ t_z \in T_1 \subset T,\ z \in E_1,\ h_2 \in H$. Using the above we obtain

$$t_y h_1 = g = t_x k = t_x t_z h_2 = t_{x \overset{(T)}{\cdot} z} h_2', \quad h_2' \in H,$$

and so

$$y = x \overset{(T)}{\cdot} z. \tag{2}$$

Since $g \in G$ is arbitrary, (2) means that for every $y \in E$ there exist $x \in E_0$ and $z \in E_1$ such that $y = x \overset{(T)}{\cdot} z$. So, it is sufficient to show the uniqueness of the representation (2).

Let us assume, that this representation is not unique, then there exists $y \in E$ such that

$$y = x_1 \overset{(T)}{\cdot} z_1 = x_2 \overset{(T)}{\cdot} z_2, \quad x_1, x_2 \in E_0, \quad z_1, z_2 \in E_1.$$

Then

$$\begin{aligned} t_y = t_{x_1 \overset{(T)}{\cdot} z_1} &= t_{x_1} t_{z_1} h' = t_{x_1}(t_{z_1} h') \in t_{x_1} K, \\ t_y = t_{x_2 \overset{(T)}{\cdot} z_2} &= t_{x_2} t_{z_2} h'' = t_{x_2}(t_{z_2} h'') \in t_{x_2} K, \end{aligned} \tag{3}$$

(where $h', h'' \in H$). Since $T^* = \{t_x\}_{x \in E_0}$ is the left transversal G to K, then $x_1 = x_2$. Thus (3) may be rewritten in the form

$$t_{x_1} t_{z_1} h' = t_y = t_{x_2} t_{z_2} h'',\ t_{z_1} h' = t_{z_2} h''.$$

Since $T_1 = \{t_z\}_{z \in E_1}$ is the left transversal K to H, we have $z_1 = z_2$. Hence the representation (2) is unique, and elements of the set E_0 form a left transversal $< E, \overset{(T)}{\cdot}, 1 >$ to $< E_1, \overset{(T)}{\cdot}, 1 >$.

2. Let $< E_0, \overset{(T^*)}{\cdot}, 1 >$ be a transversal operation corresponding to a left transversal $T^* = \{t_x\}_{x \in E_0}$ the group G to its subgroup K. Then

$$a \overset{(T^*)}{\cdot} b = c \;\Rightarrow\; t_a t_b = t_c k,\; t_a, t_b, t_c \in T^* \subset T, a,\, b,\, c \in E_0,\; k \in K,$$

and $k = t_z h,\; t_z \in T_1 \subset T,\; z \in E_1,\; h \in H$.

From the above we have $t_a t_b = t_c k = t_c t_z h$, i,e., $t_{a \overset{(T)}{\cdot} b} h' = t_{c \overset{(T)}{\cdot} z} h'' h$, $h', h'' \in H$. Thus $a \overset{(T)}{\cdot} b = c \overset{(T)}{\cdot} z$. Since $a, b, c \in E_0$, $z \in E_1$, from 1 we obtain $a \overset{(E_0)}{\cdot} b = c$, (see also (8) from [10]). Consequently, $a \overset{(T^*)}{\cdot} b = c = a \overset{(E_0)}{\cdot} b$, which completes the proof. □

Corollary 2.4. *Let $H \subseteq K \subset G$ be groups. Then there exists a one-to-one correspondence between each left transversal $T^* = \{t_x\}_{x \in E_0}$ of G to K and some left transversal E_0 the left loop $< E, \overset{(E_0)}{\cdot}, 1 >$ to its left subloop $< E_1, \overset{(E_0)}{\cdot}, 1 >$ (where T is a left transversal G to H, $T^* \subset T$, and $T_1 = \{t_z\}_{z \in E_1}$ is a left transversal K to H, $T_1 = T \cap K$) such that corresponding transversal operations $\overset{(T^*)}{\cdot}$ and $\overset{(E_0)}{\cdot}$ are isomorphic.* □

This correspondence can be converted, as it will be shown further in the next paragraph.

Analogous results may be proved for the right transversals and two-sided transversals in loops to its proper subloops.

3. Semidirect products of loops

Let us remind a definition of semidirect product of a left loop $L =< E, \cdot, 1 >$ with two-sided unit 1 and a suitable permutation group H acting on the set E ($H \subseteq St_1(S_E)$) (see [8], [13]).

Definition 3.1. Let the following two conditions be fulfilled for some left loop $L =< E, \cdot, 1 >$ and the permutation group H:

1. $\forall a,\, b \in E :\;\; l_{a,\,b} = (L^{-1}_{a \cdot b} L_a L_b) \in H$,
2. $\forall u \in E$ and $\forall h \in H :\; \varphi(u, h) = (L^{-1}_{h(u)} h\, L_u h^{-1}) \in H$, where L_a is a left translation in $< E, \cdot, 1 >$.

Then the set $E \times H$ with the operation

$$(u, h_1) * (v, h_2) = (u \cdot h_1(v),\; l_{u, h_1(v)} \varphi(v, h_1) h_1 h_2)$$

is a group denoted by $L \leftthreetimes H =< E \times H, *, (1, id) >$ and called a *semidirect product* of L and H. The group H is called a *transassociant* of L.

It is easy to show (see [8, 13]) that for the *left multiplicative group* $LM(L)$ and the *left inner permutation* group $LI(L)$ of L we have

$$LI(L) = St_1(LM(L)) \subset LM(L) \quad \text{and} \quad LM(L) = L \times LI(L).$$

Lemma 3.2. *Let $L =< E, \cdot, 1 >$ be a loop and $R =< E_1, \cdot, 1 >$ be its proper subloop, and the left Condition A be fulfilled. If $T = \{t_x\}_{x \in E_0}$ is a left transversal L to R and $H \subseteq St_1(S_L)$ is a permutation group such that $LI(L) \subseteq H$ and $\varphi(u, h) \in H$ for all $u \in L$ and all $h \in H$, then*

1. *a semidirect product $G = L \leftthreetimes H$ can be defined,*
2. *$K = \{(r, h) \,|\, r \in R,\ h \in H\}$ is a subgroup of the group G and $H \subset K$,*
3. *$T^* = \{(t_x, id) \,|\, t_x \in T_0,\ x \in E_0\}$ is a left transversal the group G to its subgroup K,*
4. *the transversal operations $< E_0, \overset{(T)}{\cdot}, 1 >$ and $< E_0, \overset{(T^*)}{\cdot}, 1 >$ (corresponding to the left transversal T the loop L to its subloop R, and to the left transversal the group G to its subgroup K, respectively) coincide.*

Proof. 1. If the conditions of the Lemma are satisfied, then we can define the semidirect product $G = L \leftthreetimes H = \{(a, h) \,|\, a \in L,\ h \in H\}$, where $H = \{(1, h) \,|\, h \in H\} \subseteq \{(a, h) \,|\, a \in L,\ h \in H\} = G$.

2. Since $R \subseteq L$, then according to the assumptions of our lemma, we have $l_{a,b} \in LI(L) \subseteq H$ for all $a, b \in R$. This implies

$$\varphi(u, h) \in \{\varphi(u, h) \,|\, u \in R,\ h \in H\} \subseteq \{\varphi(u, h) \,|\, u \in L,\ h \in H\} \subseteq H$$

for all $u \in R$ and $h \in H$. Thus, we can define a semidirect product

$$K = R \leftthreetimes H = \{(r, h) \,|\, r \in R,\ h \in H\}.$$

Clearly, $H = \{(1, h) \,|\, h \in H\} \subset K \subseteq \{(a, h) \,|\, a \in L,\ h \in H\} = G$.

3. Let $T = \{t_x\}_{x \in E_0}$ be a left transversal L to R and let

$$T^* = \{(t_x, id) \,|\, t_x \in T,\ x \in E_0\} \subset G.$$

For an arbitrary element $x \in E_0$ we consider the set

$$K_x = (t_x, id) * K = \{(t_x, id) * (r, h) \,|\, r \in R, h \in H\} \subset G. \tag{4}$$

K_x is a left coset in G to K. Indeed, any $g \in G$ can be written in the form $g = (u_0, h_0)$, where $u_0 \in L,\ h_0 \in H$. Since $T = \{t_x\}_{x \in E_0}$ is a left transversal L to R, we have $u_0 = t_{x_0} \cdot r_0$ for some $t_{x_0} \in T_0$ and $r_0 \in R$. Thus for $h_1 = (l^{-1}_{t_{x_0}, r_0} h_0) \in H$ we have

$$(t_{x_0}, id) * (r_0, h_1) = (t_{x_0} \cdot r_0, l_{t_{x_0}, r_0} h_1) = (u_0, h_0) = g,$$

which gives $g \in (t_{x_0}, id) * K$. Since $t_x \cdot R = \{t_x \cdot r | r \in R\}$ is a left coset in L to R, in view of (4), for $x_1 \neq x_2$ we obtain $t_{x_1} \cdot R) \cap (t_{x_2} \cdot R) = \varnothing$. So for $x_1 \neq x_2$ we have

$$\begin{aligned} K_{x_1} \cap K_{x_2} &= ((t_{x_1}, id) * K) \cap ((t_{x_2}, id) * K) \\ &= \{(t_{x_1}, id) * (r, h) \,|\, r \in R, h \in H\} \cap \{(t_{x_2}, id) * (r, h) \,|\, r \in R, h \in H\} \\ &= \{(t_{x_1} \cdot r, l_{t_{x_1}, r} h) \,|\, r \in R, h \in H\} \cap \{(t_{x_2} \cdot r, l_{t_{x_2}, r} h) \,|\, r \in R, h \in H\} = \varnothing. \end{aligned}$$

Hence $K_x = (t_x, id) * K$, $x \in E_0$ is the left cosets in G to K. So, $T^* = \{(t_x, id) \,|\, t_x \in T,\ x \in E_0\}$ is a left transversal G by K.

4. Let us consider the transversal operation $< E_0, \overset{(T^*)}{\cdot}, 1 >$ which corresponds to the left transversal $T^* = \{(t_x, id)\}|_{x \in E_0}$. Then $x \overset{(T^*)}{\cdot} y = z$ iff $(t_x, id) * (t_y, id) = (t_z, id) * (r, h)$, $(r, h \in K)$. Thus $(t_x \overset{(L)}{\cdot} t_y, l_{t_x, t_y}) = (t_z \overset{(L)}{\cdot} r, l_{t_z, r} h)$. Hence $t_x \overset{(L)}{\cdot} t_y = t_z \overset{(L)}{\cdot} r$, $r \in R$, $t_x, t_y, t_z \in T$. Consequently, $x \overset{(T)}{\cdot} y = z$, i.e., $x \overset{(T^*)}{\cdot} y = x \overset{(T)}{\cdot} y$ for all $x, y \in E_0$. □

Corollary 3.3. *If the conditions of Lemma* 3.2 *are satisfied, then for every* $h \in H$ *we have* $\hat{h}(R) \subseteq R$.

Proof. The previous lemma shows that for any two elements (r_1, h_1) and (r_2, h_2) from K holds

$$(r_1, h_1) * (r_2, h_2) = (r_1 \overset{(R)}{\cdot} \hat{h}_1(r_2), l_{r_1, \hat{h}_1(r_2)} \varphi(r_2, h_1) h_1 h_2).$$

Because K is a subgroup of the group G, for all $r_1, r_2 \in R$ and $h \in H$ we have $(r_1 \overset{(R)}{\cdot} \hat{h}(r_2)) \in R$. Hence $\hat{h}(R) \subseteq R$ for all $h \in H$. □

In the case $H = LI(R)$ the inclusion $\hat{h}(R) \subseteq R$ is equivalent to the fact that $l_{a,b}(R) \subseteq R$ for all $a, b \in L$. The last condition is equivalent to the left Condition A for the loop L and its subloop R (Lemma 2.8 in [10]).

References

[1] **R. Baer**, *Nets and groups*, Trans. Amer. Math. Soc. **46** (1939), 110 – 141.

[2] **V. D. Belousov**, *Foundations of quasigroup and loop theory*, (Russian), Moscow, "Nauka", 1967.

[3] **F. Bonetti, G. Lunardon and K. Strambach**, *Cappi di permutazioni*, Rend. Math. **12** (1979), 383 – 395.

[4] **T. Foguel and L. C. Kappe**, *On loops covered by subloops*, Expositiones Matematicae **23** (2005), 255 – 270.

[5] **K. W. Johnson**, *S-rings over loops, right mapping groups and transversals in permutation groups*, Math. Proc. Camb. Phil. Soc. **89** (1981), 433 – 443.

[6] **E. A. Kuznetsov**, *Transversals in groups. 1. Elementary properties*, Quasigroups and Related Systems **1** (1994), 22 – 42.

[7] **E. A. Kuznetsov**, *About some algebraic systems related with projective planes*, Quasigroups and Related Systems **2** (1995), 6 – 33.

[8] **E. A. Kuznetsov**, *Transversals in groups. 3. Semidirect product of a transversal operation and subgroup*, Quasigroups and Related Systems **8** (2001), 37 – 44.

[9] **E. A. Kuznetsov**, *Transversals in loops*, Abstracts Inter. Confer. "Loops-03", Prague 2003, 18 – 20.

[10] **E. A. Kuznetsov**, *Transversals in loops. 1. Elementary properties*, Quasigroups and Related Systems **18** (2010), 11 – 26.

[11] **M. Niemenmaa and T. Kepka**, *On multiplication groups of loops*, J. Algebra **135** (1990), 112 – 122.

[12] **H. Pflugfelder**, *Quasigroups and loops: Introduction*, Sigma Series in Pure Math., 7, Helderman Verlag, New York, 1972.

[13] **L. V. Sabinin and O. I. Mikheev**, *Quasigroups and differential geometry*, in "Quasigroups and loops: Theory and Applications"', Helderman-Verlag, Berlin 1990, 357 – 430.

Received May 13, 2010
Revised February 1, 2011
Institute of Mathematics and Computer Science, Academy of Sciences of Moldova, 5 Academiei str., Chishinau, MD-2028 Moldova
E-mail: kuznet1964@mail.ru

Quasigroups and Related Systems **19** (2011), 287 – 300

Central r-naturally fully ordered groupoids with left identity

Yutaka Matsushita

Abstract. In this paper a generalized version (r-naturally fully ordered groupoid) of a naturally fully ordered groupoid with left identity in the sense that only right solvability is permissible is embedded in a concrete groupoid of all non-negative real numbers. First, the introduction of centrality makes the r-naturally fully ordered groupoid with left identity order-isomorphic to the positive cone of a fully ordered central quasigroup. Second, the left Archimedean property enables this ordered groupoid to be embedded in the concrete groupoid.

1. Introduction

In this paper we will generalize the classical result of Hölder [6] with the embedding of a fully ordered (briefly, f.o.) semigroup in the additive semigroup of all non-negative real numbers in the context of groupoids. The embedding will be carried out in a concrete groupoid (Example 3.1) consisting of all non-negative real numbers. This approach is similar to that of Hartman [5], who considered the embedding of a f.o. loop in the additive group of all real numbers. Our concern lies in an r-naturally f.o. groupoid with left identity, which is a generalized version of a naturally f.o. groupoid with left identity in the sense that only right solvability is guaranteed. First, the analogous concept to centrality [9] for quasigroups is introduced so that an r-naturally f.o. groupoid can be the positive cone of a f.o. central quasigroup with left identity. Second, the left Archimedean property makes the ordered groupoid embeddable in the concrete groupoid.

2010 Mathematics Subject Classification: 06F05, 20N05
Keywords: centrality, naturally ordered, fully ordered groupoid, left Archimedean.

2. Preliminaries

A quasigroup is an algebra $(Q, \cdot, /, \backslash)$ with three binary operations satisfying the following identities:

$$(a \cdot b)/b = a = (a/b) \cdot b \quad \text{and} \quad a\backslash(a \cdot b) = b = a \cdot (a\backslash b).$$

These identities imply that, given $a,\ b \in Q$, the equations $x \cdot b = a$ and $b \cdot x = a$ have unique solutions $x = a/b$ and $x = b\backslash a$, respectively. A loop is a quasigroup Q with an identity element e ($e \cdot a = a = a \cdot e$ for all $a \in Q$). For any $a \in Q$, we denote by R_a and L_a the mappings of Q onto itself defined by the rules $R_a(x) = xa$ and $L_a(x) = ax$, respectively. Moreover, $R_a^{-1}(x) = x/a$, $L_a^{-1}(x) = a\backslash x$. Multiplications expressed implicitly by juxtaposition are meant to bind more strongly than the divisions so as to reduce the number of brackets in quasigroup equalities. For example, $(a \cdot b)/b$ reduces to ab/b.

Every quasigroup $(Q, \cdot, /, \backslash)$ is isotopic to a loop. Indeed, if a binary operation $+$ on Q is defined by

$$a + b = R_{e\backslash e}^{-1}(a) \cdot L_e^{-1}(b) \quad \text{for all } a, b \in Q,$$

then it is seen that $(Q, +, e)$, denoted $B(Q)$, is a loop. Assume here that e is a left identity element for $(Q, \cdot)$ ($ea = a$ for all $a \in Q$). Then $e\backslash a = a$ holds for all $a \in Q$ but $a/e = a$ does not unless $a = e$. Hence

$$a + b = (a/e)b. \tag{1}$$

Using (1),

$$a - b = (a/b)e$$

One outstanding benefit of centering is that it makes the loop $B(Q)$ into an abelian group. According to Corollary 3.7 in [9], a central quasigroup $(Q, \cdot, /, \backslash, e)$ with a left identity element e is characterized by the following identities:

$$((a/e)b/e)c = (a/e)((b/e)c); \tag{2}$$

$$(a/e)b = (b/e)a; \tag{3}$$

$$((a/e)b)e = (ae/e)(be). \tag{4}$$

The first two identities show that $B(Q)$ is an abelian group. Indeed, identities (2) and (3) specify the associativity and commutativity of $B(Q)$, respectively. Identity (4) means that right multiplication by e is an automorphism of $B(Q)$, i.e., $R_e(a + b) = R_e(a) + R_e(b)$.

A quasigroup $(Q, \cdot, /, \backslash)$ with a binary relation $\geqslant$ is called a *f.o. quasigroup* if $(Q, \geqslant)$ is a fully ordered set and the following monotony law holds:

(M) $a \geqslant b \Leftrightarrow ax \geqslant bx \Leftrightarrow xa \geqslant xb$ for all $a, b, x \in Q$.

The law (M) implies that (see [3, Lemma 3.1])

(D) $a \geqslant b \Leftrightarrow a/x \geqslant b/x$, $x\backslash a \geqslant x\backslash b$, $x/b \geqslant x/a$, $b\backslash x \geqslant a\backslash x$.

A *f.o. central quasigroup with left identity* is a f.o. quasigroup with left identity satisfying (2) to (4). In a f.o. central quasigroup Q with left identity, it is clear from (M) and (D) that $(B(Q), \geqslant)$ is a f.o. abelian group. Therefore the positive cone of Q is defined by $Q^+ = \{a \in Q \mid a \geqslant e\}$. A groupoid $(Q, \cdot)$ with a full order $\geqslant$ that satisfies (M) is a *f.o. groupoid*.

3. r-naturally f.o. groupoid and centrality

We follow the terminology of [4] for ordering. An element a of a f. o. groupoid P is *r-positive* or *l-positive* according as $xa \geqslant x$ or $ax \geqslant x$ for all $x \in P$. A f.o. groupoid is called *r-positively ordered* or *l-positively ordered* if all of its elements are r-positive or l-positive, respectively. If a f. o. groupoid contains a left identity element e, then a is l-positive if and only if $a \geqslant e$, whereas a strictly positive element $a > e$ is not always r-positive. However, it will be shown at the end of this section that the introduction of centrality makes an r-positively ordered groupoid equivalent to the positive cone of a f.o. central quasigroup. For this the concept of a naturally ordered groupoid is generalized in such a way that only the existence of a right solution is permissible. A f.o. groupoid P is said to be *r-naturally ordered* if it is r-positively ordered and

$$a > b \text{ implies that } xb = a \text{ for some } x \in P.$$

Note that by (M) the solution x is unique. This condition implies that P has a right division that is "partially" defined on P in the sense that its domain is a subset of P: Set $x = a/b$ with $a > b$. Then $(a/b)b = a$ and $ab/b = a$ are satisfied. Also, P has a partial left division that is always definable on a f.o. groupoid. Since $x = b$ is a unique solution to $ax = ab$ by (M), we can define $x = a\backslash ab$ so that $a\backslash ab = b$ and $a(a\backslash ab) = ab$. Specifically, $e\backslash b = b$. Consequently, P is regarded as a set equipped with three binary operations: the groupoid multiplication and the partial right and left divisions.

Example 3.1. We define a binary operation $\oplus$ on the set $\mathbb{R}^+$ of all non-negative real numbers by

$$a \oplus b = \alpha a + b \quad \text{for some } \alpha \geqslant 1.$$

The set $\mathbb{R}^+$ with this operation and the usual order is an r-naturally f.o. groupoid with a left identity element 0. □

Example 3.2. Let Q be a f.o. central quasigroup with a left identity element e. Assume that $xe \geqslant x$ for all $x \in Q$. Then Q^+ is an r-naturally f.o. groupoid with a left identity element e. □

Throughout the paper, unless otherwise specified, we will use the symbol e to denote a left identity element, and let P be an r-naturally f.o. groupoid with left identity. The trivial case where P has just a single element e will always be excluded. Centrality of P is defined in a similar way to centrality of quasigroups (see [9] for the specific definition of central quasigroups). We now consider the Cartesian product P^2 as a partial algebra $(P^2, \cdot, /, \backslash)$ with componentwise groupoid multiplication and componentwise partial right and left divisions. An equivalence relation W on P is a *congruence* if it is a subalgebra of P^2. The diagonal $\widehat{P} = \{(a, a) \mid a \in P\}$ is a subalgebra of P^2. An r-naturally f.o. groupoid P is defined to be *central* if there exists a congruence W on P^2 having $\widehat{P}$ as a congruence class. In addition we will call this W a *centering congruence*. The equivalence class of $(a, b) \in P^2$ under W is denoted by $(a, b)^W$, i.e., $(a, b)^W = \{(x, y) \in P^2 \mid (x, y)W(a, b)\}$, and the set of equivalence classes by P^2/W.

A partial ternary operation on P is defined by

$$p(a, b, c) = (a/b)c \quad \text{provided that } a \geqslant b.$$

This definition does not entails the identity $p(a, b, b) = a$ in case of $a < b$. Therefore useful methods cannot be used to obtain the following properties of centering congruences. To solve this problem, we provide a new ternary operation p_s on P defined by

$$p_s(a, b, c) = (sa/b)c \quad \text{provided that } sa \geqslant b$$

Indeed, even for $a < b$ by right solvability and (M) we can take $s \in P$ such that $sa \geqslant b$. Then since $p_s(a, b, b) = sa$, it follows that $s\backslash p_s(a, b, b) = a$. Also, $s\backslash p_s(a, a, b) = b$. Using the operation p_s, we obtain similar results to

Propositions 3.1, 3.3, and 3.4 in [9]. The result similar to Proposition 3.1 guarantees the existence of a centering congruence on P^2. The other results are listed in the form in which they will be used in what follows.

Proposition 3.3. *Let P be a central r-naturally f.o. groupoid with left identity and let W be a centering congruence on P^2. Then*

(RR) $(a,b) \in P^2 \Rightarrow (a,a)W(b,b)$;

(RS) $(a,b)W(a',b') \Rightarrow (b,a)W(b',a')$;

(RT) $(a,b)W(a',b')$ and $(b,c)W(b',c') \Rightarrow (a,c)W(a',c')$.

Proof. The proof is much the same as that of [9]. Therefore we prove only (RT) because the operation p_s is necessary in case of $a < b$, $b > c$, $a' < b'$, and $b' > c'$. Assume that $(a,b)W(a',b')$ and $(b,c)W(b',c')$. Take $s \in P$ such that $sa \geqslant b$ and $sa' \geqslant b'$ (which is possible by setting $s = \max(u,v)$ such that $ua \geqslant b$, $va' \geqslant b'$). Then

$$\begin{array}{ll} (s,s)W(s,s) & \text{by (RR)},\\ (a,b)W(a',b') & \text{is given},\\ (b,b)W(b',b') & \text{by (RR)},\\ (b,c)W(b',c') & \text{is given},\\ (s,s)W(s,s) & \text{by (RR)} \end{array}$$

$$\Rightarrow (s\backslash p_s(a,b,b), s\backslash p_s(b,b,c))W(s\backslash p_s(a',b',b'), s\backslash p_s(b',b',c')).$$

Hence we obtain $(a,c)W(a',c')$, as required for (RT). □

Proposition 3.4. *Let P be a central r-naturally f.o. groupoid with left identity and let W be a centering congruence on P^2. Then W is uniquely specified by*

$$\text{if } c \geqslant a, \text{ then } (a,b)W(c,d) \Leftrightarrow d = p(c,a,b). \tag{5}$$

$$\text{if } a \geqslant b, \text{ then } (a,b)W(c,d) \Leftrightarrow c = p(a,b,d). \tag{6}$$

Applying (RS) of W and with the use of (6), we have

$$\text{if } a < b, \text{ then } (a,b)W(c,d) \Leftrightarrow d = p(b,a,c). \tag{7}$$

Lemma 3.5. *If P is an r-naturally f. o. groupoid with left identity, then $a \geqslant e$ for all $a \in P$.*

Proof. By r-positivity we have $aa \geqslant a$ for all $a \in P$, i.e., $aa \geqslant ea$. Hence by (M) we obtain $a \geqslant e$ for all $a \in P$. □

Lemma 3.6. *Let P be a central r-naturally f.o. groupoid with left identity. Then identity* (3) *is satisfied for all elements of P, and if $a \geqslant be$ then*

$$b\backslash a = (a/be)e.$$

Proof. Let $a, b \in P$ be arbitrary positive elements. Both (5) and (7) guarantee the existence of $c \in P$ such that $(e, a)W(b, c)$. Note here that c is uniquely determined. Hence $p(b, e, a) = p(a, e, b)$, or $(b/e)a = (a/e)b$. To prove the latter part, assume that $a \geqslant be$ and let $x \in P$ be such that $bx = a$. Then since $a/be \in P$ by right solvability, it follows from (3) that $(be/e)((a/be)e) = (a/be)(be) = a$. Hence by (M) $x = (a/be)e$. □

Theorem 3.7. *Let P be a central r-naturally f.o. groupoid with left identity and let W be a centering congruence on P^2. Then the quotient P^2/W is a f.o. central quasigroup with left identity, and P is o-isomorphic (order-isomorphic) to the positive cone of P^2/W.*

Proof. Let $P_W = \{(a, b)^W \mid a \geqslant b\}$ and $N_W = \{(a, b)^W \mid a \leqslant b\}$ be the sets of positive and negative elements in P^2/W, respectively. The ordering on P_W and N_W is determined by:

(a) $\geqslant$ on P_W: $(a, b)^W \geqslant (c, d)^W$ if and only if $p(a, b, e) \geqslant p(c, d, e)$,

(b) $\geqslant$ on N_W: $(a, b)^W \geqslant (c, d)^W$ if and only if $p(b, a, e) \leqslant p(d, c, e)$.

Rules (a) and (b) are based on (6) and (7), respectively. Since it is the case that $(a, b)^W > (c, d)^W$ whenever $(a, b)^W \in P_W$ with $a > b$, $(c, d)^W \in N_W$ with $c < d$, (a) and (b) provide a full order on P^2/W. Further, multiplication on P^2/W is defined by

(c) multiplication: $(a, b)^W(c, d)^W = (ac, bd)^W$.

For (c) we may use an element of the form $(s, e)^W$ with $s = p(a, b, e) \geqslant e$ or $(e, t)^W$ with $t = p(b, a, e) \geqslant e$ based on whether each $(a, b)^W$ is positive or negative. We show that P^2/W is right and left solvable. First, the following is clear from (a) and (b): if $a \geqslant b$, then $x = a/b$ is a solution to

$(x,e)^W(b,e)^W = (a,e)^W$ and $(e,x)^W(e,b)^W = (e,a)^W$. Second, if $a \geqslant be$, then by Lemma 3.6 $x = (a/be)e$ is a solution to $(b,e)^W(x,e)^W = (a,e)^W$ and $(e,b)^W(e,x)^W = (e,a)^W$. We consider solutions to the other cases of equations.

Case 1R. $(e,x)^W(b,e)^W = (a,e)^W$ with $a < b$: Since in this case $(a,e)^W = (b,p(b,a,e))^W$ by (5), we have $xe = p(b,a,e)$. Hence $x = b/a$.

Case 1L. $(b,e)^W(e,x)^W = (a,e)^W$ with $a < be$: Since in this case $(a,e)^W = (be,p(be,a,e))^W$ by (5), we have $x = p(be,a,e)$. Hence $x = (be/a)e$.

Case 2R. $(x,e)^W(e,b)^W = (a,e)^W$: Since $(a,e)^W = (p(a,e,b),b)^W$ by (6), we have $xe = p(a,e,b)$. Hence $x = (a/e)b/e$.

Case 2L. $(e,b)^W(x,e)^W = (a,e)^W$: Since $(a,e)^W = (p(a,e,be),be)^W$ by (6), we have $x = p(a,e,be)$. Hence $x = (a/e)(be)$.

A similar method guarantees the existence of a solution to each of the above equations into which $(e,a)^W$ is substituted for $(a,e)^W$. Obviously, $(s,s)^W(= (e,e)^W)$ is a left identity element for multiplication. Therefore the right division on P^2/W is defined as follows:

$$(a_1,a_2)^W/(b_1,b_2)^W = (sa_1/b_1, sa_2/b_2)^W, \tag{8}$$

where $sa_1 \geqslant b_1,\ sa_2 \geqslant b_2$. Indeed, setting $s = b/a$ and $s = b/e$ give the solutions in Cases 1R and 2R, respectively. By making use of Lemma 3.6, the left division is also defined as

$$(b_1,b_2)^W\backslash(a_1,a_2)^W = ((sa_1/b_1e)e, (sa_2/b_2e)e)^W, \tag{9}$$

where $sa_1 \geqslant b_1e,\ sa_2 \geqslant b_2e$. Setting $s = be/a$ and $s = b$ give the solutions in Cases 1L and 2L, respectively. (Note here that by (3) $ba = (a/e)(be)$.)

To show that (M) is satisfied for P^2/W, assume that $(a,e)^W \geqslant (b,e)^W$, so that $a \geqslant b$. Since $ac \geqslant bc$ by (M), $(a,e)^W(c,e)^W \geqslant (b,e)^W(c,e)^W$. The converse is also valid. We next provide three cases to prove $(a,e)^W(e,c)^W \geqslant (b,e)^W(e,c)^W$.

Case 1. $ae,\ be \geqslant c$: Since $(ae/c)e \geqslant (be/c)e$ by (M) and (D), the required inequality follows from (a).

Case 2. $ae,\ be < c$: Since $(c/ae)e \leqslant (c/be)e$ by (M) and (D), we obtain from (b) the required inequality.

Case 3. $ae \geqslant c \geqslant be$: By (6) and (7), $(ae, c)^W = ((ae/c)e, e)^W$ and $(be, c)^W = (e, (c/be)e)^W$. Since $ae/c \geqslant e$ and $c/be \geqslant e$ by (D), we obtain $(a, e)^W(e, c)^W \geqslant (b, e)^W(e, c)^W$.

The converse is also seen to be valid. Similarly, we obtain $(e, a)^W \geqslant (e, b)^W \Leftrightarrow (e, a)^W(c, e)^W \geqslant (e, b)^W(c, e)^W \Leftrightarrow (e, a)^W(e, c)^W \geqslant (e, b)^W(e, c)^W$. We further show that $(a, e)^W \geqslant (e, b)^W \Leftrightarrow (a, e)^W(c, e)^W \geqslant (e, b)^W(c, e)^W$. If $c \geqslant be$, then by (6) $(c, be)^W = ((c/be)e, e)^W$. Since $ac \geqslant c$ and $be \geqslant e$ by (M), it follows from (M) and (D) that $ac = (ac/e)e \geqslant (c/be)e$, and hence by (a) $(ac, e)^W \geqslant (c, be)^W$. If $c < be$, then by definition $(c, be)^W < (e, e)^W \leqslant (ac, e)^W$. The converse is trivial because $(a, e)^W$ is always $\geqslant (e, b)^W$. A similar method gives $(a, e)^W \geqslant (e, b)^W \Leftrightarrow (a, e)^W(e, c)^W \geqslant (e, b)^W(e, c)^W$. Thus P^2/W is a f.o. quasigroup with left identity.

We show that P^2/W is central. According to the proof of Lemma 3.2 in [9], which addresses the case where P is a quasigroup, a relation Ω on $P^2/W \times P^2/W$ is defined by

$$((a_1, a_2)^W, (b_1', b_2')^W)\Omega((a_1', a_2')^W, (b_1, b_2)^W) \Leftrightarrow (a_1, a_3)W(a_1', a_3'), \quad (10)$$

where $(a_2, a_3)W(b_1, b_2)$ and $(a_2', a_3')W(b_1', b_2')$. However, since P is a groupoid, a problem arises, i.e., no solution $a_3 \in P$ exists to $(a_2, a_3)W(b_1, b_2)$, for example, when $b_1 > e, b_2 = e$ and $b_1 > a_2$. Therefore the definition of Ω must be revised. The following lemma is provided for this purpose.

Lemma 3.8. *For any* (a_1, a_2), $(b_1, b_2) \in P^2$, *there exists* $(x_1, x_2) \in P^2$ *such that* $(x_1, x_2)W(a_1, a_2)$ *with* $x_1 \geqslant b_1$, $x_2 \geqslant b_2$.

Proof. Let $x_1 \geqslant a_1$. By (5), $x_2 = p(x_1, a_1, a_2)$ satisfies $(x_1, x_2)W(a_1, a_2)$. Take $s \in P$ such that $sa_1 \geqslant b_1$, $sa_2 \geqslant b_2$. Set $x_1 = sa_1$, so that $x_1 \geqslant b_1$. Then $x_2 = ((sa_1)/a_1)a_2 = sa_2 \geqslant b_2$. □

With the aid of Lemma 3.8, a relation Ω is introduced on $P^2/W \times P^2/W$ by setting $((a_1, a_2)^W, (b_1', b_2')^W)\Omega((a_1', a_2')^W, (b_1, b_2)^W)$ if there exist $(x_1, x_2), (x_1', x_2') \in P^2$ such that

$$(x_1, x_2)W(a_1, a_2),\ x_2 \geqslant b_1 \text{ and } (x_1', x_2')W(a_1', a_2'),\ x_2' \geqslant b_1', \quad (11)$$

and such that the relation

$$((x_1, x_2)^W, (b_1', b_2')^W)\Omega((x_1', x_2')^W, (b_1, b_2)^W) \quad (12)$$

is satisfied in the sense of (10). The inequalities $x_2 \geqslant b_1$ and $x'_2 \geqslant b'_1$ in (11) are needed only to verify the validity of (12) on the basis of (10). Indeed, in view of these inequalities, it is seen from (5) that $(x_2, x_3)W(b_1, b_2)$ and $(x'_2, x'_3)W(b'_1, b'_2)$ have solutions $x_3 = p(x_2, b_1, b_2)$ and $x'_3 = p(x'_2, b'_1, b'_2)$. We will examine whether this definition of Ω is consistent with (10). Assume that (10) is satisfied, i.e.,

$$(a_1, a_3)W(a'_1, a'_3),\ (a_2, a_3)W(b_1, b_2) \text{ and } (a'_2, a'_3)W(b'_1, b'_2).$$

Let $x_3, x'_3 \in P$ be such that $(x_2, x_3)W(b_1, b_2)$ and $(x'_2, x'_3)W(b'_1, b'_2)$. By the transitivity of W we have $(x_2, x_3)W(a_2, a_3)$ and $(x'_2, x'_3)W(a'_2, a'_3)$. Since (11) is satisfied, it follows from (RT) for W that $(x_1, x_3)W(a_1, a_3)$ and $(x'_1, x'_3)W(a'_1, a'_3)$. From the first assumption and transitivity we obtain $(x_1, x_3)W(x'_1, x'_3)$, which implies that (12) is satisfied. Next we examine whether Ω is a subquasigroup of $(P^2/W)^4$. Let $(y_1, y_2), (y'_1, y'_2) \in P^2$ be such that $(y_1, y_2)W(c_1, c_2)$, $y_2 \geqslant d_1$ and $(y'_1, y'_2)W(c'_1, c'_2)$, $y'_2 \geqslant d'_1$, and such that

$$((y_1, y_2)^W, (d'_1, d'_2)^W)\Omega((y'_1, y'_2)^W, (d_1, d_2)^W)$$

is satisfied in the sense of (10), which implies that $((c_1, c_2)^W, (d'_1, d'_2)^W)\Omega$ $((c'_1, c'_2)^W, (d_1, d_2)^W)$. Accordingly we use the proof of Lemma 3.2 [9] to obtain

$$((x_1, x_2)^W(y_1, y_2)^W, (b'_1, b'_2)^W(d'_1, d'_2)^W)$$
$$\Omega\,((x'_1, x'_2)^W(y'_1, y'_2)^W, (b_1, b_2)^W(d_1, d_2)^W).$$

Since $(x_1, x_2)^W(y_1, y_2)^W = (a_1, a_2)^W(c_1, c_2)^W$ and $(x'_1, x'_2)^W(y'_1, y'_2)^W = (a'_1, a'_2)^W(c'_1, c'_2)^W$, we have by (11) and (12)

$$((a_1, a_2)^W(c_1, c_2)^W, (b'_1, b'_2)^W(d'_1, d'_2)^W)$$
$$\Omega\,((a'_1, a'_2)^W(c'_1, c'_2)^W, (b_1, b_2)^W(d_1, d_2)^W).$$

It is clearly seen that the definition of (10) does not depend on the choices of representatives of $(b_1, b_2)^W, (b'_1, b'_2)^W$. Hence we may assume that $b_i \geqslant d_i$, $b'_i \geqslant d'_i$ for $i = 1, 2$. Take $s \in P$ such that $sx_i \geqslant y_i$, $sx'_i \geqslant y'_i$ for $i = 1, 2, 3$. Since

$$((s, s)^W, (e, e)^W)\Omega((s, s)^W, (e, e)^W),$$

it follows that

$$((sx_1, sx_2)^W, (b'_1, b'_2)^W)\Omega((sx'_1, sx'_2)^W, (b_1, b_2)^W).$$

Note here that this is also valid in the context of (10). Hence the proof of Lemma 3.2 [9] is used again to obtain

$$((sx_1, sx_2)^W/(y_1, y_2)^W, (b_1', b_2')^W/(d_1', d_2')^W)$$
$$\Omega\,((sx_1', sx_2')^W/(y_1', y_2')^W, (b_1, b_2)^W/(d_1, d_2)^W).$$

Since $(sx_1, sx_2)^W/(y_1, y_2)^W = (a_1, a_2)^W/(c_1, c_2)^W, (sx_1', sx_2')^W/(y_1', y_2')^W = (a_1', a_2')^W/(c_1', c_2')^W$ by (8), we have by (11) and (12)

$$((a_1, a_2)^W/(c_1, c_2)^W, (b_1', b_2')^W/(d_1', d_2')^W)$$
$$\Omega\,((a_1', a_2')^W/(c_1', c_2')^W, (b_1, b_2)^W/(d_1, d_2)^W).$$

In view of (9), a similar method gives Ω being closed under left division. Using the operations on Ω and p_s, we can prove that Ω satisfies the properties of a centering congruence. Finally, by considering a mapping $P \to P^2/W;\ a \mapsto (a, e)^W$ and by using Lemma 3.5, it is seen that P is o-isomorphic to the positive cone of P^2/W. □

The following corollary corresponds to Corollary 3.7 in [9].

Corollary 3.9. *If P is a central r-naturally f.o. groupoid with left identity, then it satisfies identities* (2), (3), *and* (4). □

A f.o. quasigroup Q with left identity is said to *be generated by P* if it is a quasigroup generated by P on which a full order is introduced such that it is an extension of the full order of P. If, in addition, identities (2) to (4) are satisfied, then Q is the f.o. central quasigroup with left identity generated by P. Henceforth $B(P)$ denotes an algebra $(P, +, e)$ where $+$ is a binary operation defined by (1). Since $a \geqslant e$ for all $a \in P$ (Lemma 3.5), by right solvability we have $a/e \in P$, and thus $B(P)$ is actually a subgroupoid of Q, or $B(Q)$.

Proposition 3.10. *Let P be an r-naturally f.o. groupoid with left identity and let Q be the f.o. central quasigroup with left identity generated by P. Then every element $x \in Q$ is written in the form $x = (a/b)e$ where $a, b \in P$.*

Proof. Let $(A, +, e)$ be the subgroup of $B(Q)$ generated by $B(P)$. Since $B(Q)$ is an abelian group, every element $x \in A$ can be written in the form $x = a - b$, where $a, b \in B(P)$. Using the fact that R_e is an automorphism of $B(Q)$, we can write $xe = (a-b)e = ae - be$. Hence $xe \in A$. Analogously, $x/e \in A$. Since $xy = xe + y,\ x/y = (x - y)/e$, and $y\backslash x = x - ye$, it follows that $xy,\ x/y,\ y\backslash x \in A$ for all $x, y \in A$. Thus A is a subquasigroup of Q

that contains P. This means that $A = Q$ because Q is generated by P. Therefore for every $x \in Q$ we have $x = (a/b)e$, where $a, b \in P$. □

In view of Proposition 3.10, it is easy to see that an extended order on Q from the full order on P is uniquely determined.

Proposition 3.11. *An r-naturally f.o. groupoid P with left identity is central if and only if it is the positive cone of the f.o. central quasigroup Q with left identity generated by P.*

Proof. Assume that $P = Q^+$. Then it is obvious that P is an r-naturally f.o. groupoid with left identity for which (2) to (4) are satisfied. According to [9], define the subtraction mapping $F : P^2 \to Q$ by

$$F(a, a') = a - a'.$$

With the aid of (4), F is a homomorphism with respect to groupoid multiplication and the two partial divisions. We show only the homomorphic property with groupoid multiplication. Since $ab = R_e(a) + b$, it follows that

$$\begin{aligned} F((a, a')(b, b')) &= (R_e(a) + b) - (R_e(a') + b') \\ &= R_e(a - a') + (b - b') \qquad (R_e \text{ is an automorphism}) \\ &= (a - a')(b - b') \qquad (\text{by } (1)) \\ &= F(a, a')F(b, b'). \end{aligned}$$

Hence $\ker F$ is a congruence, and it must have the diagonal $\widehat{P}$ as a congruence class. This means that P is central.

Assume that P is central. By Corollary 3.9, P has the same algebraic properties (i.e., (2) to (4)) as Q, and hence P is embedded o-isomorphically in Q. From Lemma 3.5 we conclude that P is o-isomorphic to Q^+. □

Note that the quotient P^2/W of Theorem 3.7 is o-isomorphic to this Q. Indeed, in view of Proposition 3.10, it can be verified that the mapping $P^2/W \to Q;\ (a, b)^W \mapsto (a/b)e (= a - b)$ is an o-isomorphism.

4. Embedding in the non-negative real numbers

Henceforth assume that a central r-naturally f.o. groupoid P with left identity has no smallest strictly positive element. We will use the fact

that P is o-isomorphic to the positive cone of the f.o. central quasigroup generated by P (Proposition 3.11) to prove the lemmas and theorem in this section.

A relaxed version [7] of the Archimedean property is required for the embedding of P in the non-negative real numbers. Let $a \in P$ be an arbitrary element. We will define the n-th left multiplication of a as $a^n = a \cdot a^{n-1}$ for $n = 2, 3, \ldots$ and $a^1 = a$. An r-naturally f.o. groupoid P is called *left Archimedean* if for every strictly positive elements $a,\ b \in P$ there is a positive integer n such that $a^n > b$.

By (3), we may define the n-th addition of a in the left sided manner: $na = a + (n-1)a$ for $n = 2, 3, \ldots$ and $1 \cdot a = a$. From (1) it is seen that $na = L_{a/e}^{n-1}(a)$ for all $n \geqslant 1$ where $L_{a/e}^0 = L_e$.

Lemma 4.1. *Let P be a central r-naturally f.o. groupoid with left identity. If P is left Archimedean, then $B(P)$ is an Archimedean f.o. monoid.*

Proof. As was stated in Section 2, it is clear that $B(P)$ is a (commutative) monoid. Note that by (M) and (D) of P

$$x \geqslant y \Leftrightarrow (x/e)z \geqslant (y/e)z \text{ and } x \geqslant y \Leftrightarrow (z/e)x \geqslant (z/e)y.$$

Hence $B(P)$ is a f.o. monoid. We show that $B(P)$ is Archimedean. Let $a,\ b \in P$ be strictly positive. Without loss of generality we can assume that $b > a$. Since $a/e > e$ if $a > e$, the left Archimedean property guarantees the existence of $n > 1$ such that $L_{a/e}^{n-1}(a/e) > b$. Since the map $L_{a/e}^{n-1}$ is order preserving, it follows from the r-positivity property that $L_{a/e}^{n-1}((a/e)a) > b$, or $(n+1)a > b$, as required. □

Theorem 4.2. *Let P be a left Archimedean, central r-naturally f.o. groupoid with left identity. Then P is o-isomorphic to a subgroupoid of the groupoid of all non-negative real numbers of Example* 3.1.

Proof. Since $B(P)$ is an Archimedean f.o. monoid by Lemma 4.1, it is seen from Hölder's [6] theorem that there exists an o-isomorphism f of $B(P)$ to a submonoid of the additive f. o. monoid of all non-negative real numbers. Since $ab = ae + b$, $f(ab) = f(ae) + f(b)$. To complete the proof, it suffices to show that $f(ae) = \alpha f(a)$ for some $\alpha \geqslant 1$. For this the following lemma is provided.

Lemma 4.3. *Let $P_e = \{ae \,|\, a \in P\}$. Then P_e is equal to P, and hence $B(P_e) = (P_e, +, e)$ is an Archimedean f.o. monoid.*

Proof. Since it is obvious that $P_e \subset P$, we show only that $P \subset P_e$. Let $x \geqslant e$ be an arbitrary element of P. Then since $x = ae$ where $a = x/e \in P$ by right solvability, we have $x \in P_e$. It is clear from Lemma 4.1 that $B(P_e)$ is an Archimedean f.o. monoid. □

Combining this lemma with Hölder's theorem, we obtain the result that $f(B(P_e))$ is a submonoid of the additive f.o. monoid of all non-negative real numbers. Since $f((a+b)e) = f(ae) + f(be)$ by (4), there is a strictly positive real number α such that $f(ae) = \alpha f(a)$ (e.g. see the proof of Proposition 2.2.1 in [8]). Moreover, since $a \leqslant ae$ for all $a \in P$ by r-positivity, $f(a) \leqslant f(ae) = \alpha f(a)$. Thus $\alpha \geqslant 1$. □

The hypothesis of the following corollaries is that P is a left Archimedean, central r-naturally f.o. groupoid with left identity.

Corollary 4.4. *If $P = \mathbb{R}^+$, then $ab = \alpha a + b$ ($\alpha \geqslant 1$) for all $a, b \in \mathbb{R}^+$.*

Proof. It suffices to show that the o-isomorphism f in the proof of Theorem 4.2 is continuous. Indeed, if so, then since f is additive and continuous on $\mathbb{R}^+$, it is well known [1] that $f(a) = sa$ for some $s \in \mathbb{R}$. Setting $s = 1$, we obtain $f(ab) = \alpha a + b$. To prove continuity, assume that $a > b$. By right solvability $a = xb$ for some $x \in P$. Since P has no smallest strictly positive element, we have $a > x'b > b$ for $x' < x$, and hence $f(a) > f(x'b) > f(b)$. This means that f has no gap in its range. Hence we conclude from Debreu's [2] open gap lemma that f is continuous. □

Corollary 4.5. *If e is a two-sided identity, then P is o-isomorphic to a submonoid of the additive f.o. monoid of all non-negative real numbers.*

Proof. Since $a/e = a$, identities (2) and (3) reduce to $(ab)c = a(bc)$ and $ab = ba$, respectively. Also it is obvious that P satisfies (M) and the Archimedean property. □

Acknowledgment. The author would like to express his sincere gratitude to the reviewer for carefully reading the original manuscript and for many invaluable suggestions that considerably improved the quality of the paper.

References

[1] **J. Aczél**, *Lectures on functional equations and their applications*, Academic Press, New York, 1966.

[2] **G. Debreu**, *Continuity properties of Paretian utility.* International Economic Review **5** (1964), 285 – 293.

[3] **M. Demko**, *Lexicographic product decompositions of partially ordered quasigroups*, Math. Slovaca **51** (2001), 13 – 24.

[4] **L. Fuchs**, *Partially ordered algebraic systems*, Pergamon Press, Oxford, Addison-Wesley, Reading, Mass., 1963.

[5] **P. A. Hartman**, *Integrally closed and complete ordered quasigroups and loops*, Proc. Amer. Math. Soc. **33** (1972), 250 – 256.

[6] **O. Hölder**, *Die axiome der quantität und die lehre vom mass*, Ber. Verh. Sächs. Ges. Wiss. Leipzig Math.-Phys. Cl. **53** (1901), 1 – 64.

[7] **K. Iséki**, *Structure of special ordered loops*, Portugal. Math. **10** (1951), 81−83.

[8] **V. M. Kopytov and N. Y. Medvedev**, *Right-ordered groups*, Plenum, New York, 1996.

[9] **J. D. H. Smith**, *An introduction to quasigroups and their representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.

Received June 2, 2011

Department of Psychological Informatics
Kanazawa Institute of Technology
3-1 Yatsukaho, Hakusan, Ishikawa 924-0838
Japan
E-mail: yutaka@neptune.kanazawa-it.ac.jp

Quasigroups and Related Systems **19** (2011), 301 – 316

On random error correcting codes based on quasigroups

Aleksandra Popovska-Mitrovikj, Verica Bakeva and Smile Markovski

Abstract. Random error-correcting codes based on quasigroups transformations are proposed elsewhere. They are similar to convolution codes and the dependence of the properties of the codes from the used quasigroups are investigated in earlier paper of ours. In this paper we compare the Random error correcting codes based on quasigroups with the well know Reed-Muller and Reed-Solomon codes. The obtained experimental results show that in the case when the bit-error probability of binary symmetric channel is $p > 0.05$ ($p > 0.06$) then the random codes based on quasigroups over perform the Reed-Muller and Reed-Solomon codes for the packet-error probability (for the bit-error probability).

1. Introduction

A new class of codes, Random codes based on quasigroups (RCBQ), are proposed by Gligoroski et al [4]. In RCBQ, similar to recursive convolution codes, the correlation exists between any two bits of a codeword, and they can have infinite length, theoretically. However, in contrast to convolution codes, RCBQ are nonlinear and almost random.

RCBQ have several parameters, and we have investigated the influence of the code parameters to the code performances [8]. Since RCBQ are designed using quasigroup string transformations on messages extended by introduced redundancy, we have investigated how the following parameters affect the codes: the pattern of redundancy, the chosen quasigroups, the number of application of quasigroup transformations. The main goal of this paper is to compare the performances of RCBQ regarding the performances of the Reed-Muller codes (RMC) and Reed-Solomon codes (RSC). For that aim we have chosen an RCBQ with best performances.

2010 Mathematics Subject Classification: 20N05, 68P30, 94B60
Keywords: Quasigroup, quasigroup transformation, error-correcting code, random code, Reed-Muller code, Reed-Solomon code, packet-error and bit-error probability

The paper is organized as follows. The Section 2 contains the definition of quasigroup transformations and the definition of TASC (Totally Asynchronous Stream Ciphers) that is used for code definition. A description of the code, i.e., the algorithms for coding and for decoding, are given in Section 3. In Section 4 the definitions of codes RMC and RSC are given. In Section 5 we show how optimal parameters for RCBQ can be chosen. The comparison results for the performances of RCBQ regarding RMC and RSC are presented in Section 6, which is the section with the main results in this paper. Section 7 contains some conclusions.

2. Quasigroup transformation and TASC

A *quasigroup* $(Q, *)$ is a groupoid, i.e., a set Q with a binary operation $* : Q^2 \longrightarrow Q$, such that for all $u, v \in Q$, there exist unique $x, y \in Q$, satisfying the equalities $u * x = v$ and $y * u = v$. Further on, we assume that the set Q is a finite set.

Given a quasigroup $(Q, *)$, a new operation "$\backslash$", called a *parastrophe*, can be derived from the operation $*$ as follows:

$$x * y = z \iff y = x \setminus z.$$

Then the algebra $(Q, *, \backslash)$ satisfies the identities: $x \setminus (x * y) = y$ and $x * (x \setminus y) = y$, and $(Q, \backslash)$ is also a quasigroup.

Quasigroup string transformations are defined on a finite set Q (i.e., an alphabet Q) endowed with a quasigroup operation $*$, and they are mappings from Q^+ to Q^+, where Q^+ is the set of all nonempty words on Q. Note that $Q^+ = Q \cup Q^2 \cup Q^3 \cup \dots$. Here, we use two types of quasigroup transformations as explained below.

Let $l \in Q$ be a fixed element, called a leader. For every $a_i, b_i \in Q$, e- and d-transformations are defined as follows.

$$e_l(a_1 a_2 \dots a_n) = b_1 b_2 \dots b_n \Leftrightarrow b_{i+1} = b_i * a_{i+1},$$
$$d_l(a_1 a_2 \dots a_n) = b_1 b_2 \dots b_n \Leftrightarrow b_{i+1} = a_i \setminus a_{i+1},$$

for each $i = 0, 1, \dots, n-1$, where $b_0 = a_0 = l$. By using the identities $x \setminus (x * y) = y$ and $x * (x \setminus y) = y$, we have that $d_l(e_l(a_1 a_2 \dots a_n)) = a_1 a_2 \dots a_n$ and $e_l(d_l(a_1 a_2 \dots a_n)) = a_1 a_2 \dots a_n$. This means that e_l and d_l are permutations on Q^n, mutually inverse. Compositions of e- and d-transformations are used in the design of RCBQ.

The concept of TASC was introduced in [3]. That cryptographic concept is the corner stone for the new algorithm for error correction. Here we use a way of implementation of TASC by quasigroup string transformations. We take the alphabet $Q = \{0, 1, \ldots, 9, a, b, c, d, e, f\}$, whose elements are 4-bit words, and we choose a quasigroup $(Q, *)$ (given in Table 1) with good properties according to the investigation in [8]. In fact, by using TASC, we can encrypt and decrypt messages. The TASC algorithm for encryption and decryption that we use for designing of RCBQ is given in Figure 1. TASC uses a key k for the encryption and decryption purposes and the length of the key has influence on the performances of RCBQ (smaller key length produces faster code with worser decoding results).

Encryption	**Decryption**
Input: Key $k = k_1k_2 \ldots k_n$ and message $L = L_1L_2 \ldots L_m$ **Output**: message (codeword) $C = C_1C_2...C_m$	**Input**: The pair $(a_1a_2 \ldots a_s, k_1k_2 \ldots k_n)$ **Output**: The pair $(c_1c_2 \ldots c_s, K_1K_2 \ldots K_n)$
For $j = 1$ to m $X \leftarrow L_j$; $T \leftarrow 0$; For $i = 1$ to n $X \leftarrow k_i * X$; $T \leftarrow T \oplus X$; $k_i \leftarrow X$; $k_n \leftarrow T$ **Output**: $C_j \leftarrow X$	For $i = 1$ to n $K_i \leftarrow k_i$; For $j = 0$ to $s - 1$ $X, T \leftarrow a_{j+1}$; $temp \leftarrow K_n$; For $i = n$ to 2 $X \leftarrow temp \setminus X$; $T \leftarrow T \oplus X$; $temp \leftarrow K_{i-1}$; $K_{i-1} \leftarrow X$; $X \leftarrow temp \setminus X$; $K_n \leftarrow T$; $c_{j+1} \leftarrow X$; **Output**: $(c_1c_2 \ldots c_s, K_1K_2 \ldots K_n)$

Figure 1: TASC algorithm for encryption and decryption

The main characteristic of TASC is that the error propagation is unbounded and it propagates until the end of the stream. However, by adding some redundant information in the stream, the correction of some errors can be done. That is in fact the main idea behind TASC Error Correction. We emphasis here that the pseudo random properties of RCBQ are obtained according to the following theorem.

Theorem 1. [6] *Consider an arbitrary string $\alpha = a_1a_2\dots a_n$ where $a_i \in Q$, and let β be obtained after k applications of an e-transformation. If n is enough large integer then, for each $1 \leqslant t \leqslant k$, the distribution of substrings of β of length t is uniform.* □

Note that for $t > k$ the distribution of substrings of β of length t is not uniform (see [1]).

3. Description of RCBQ

The code design uses the alphabet $Q = \{0, 1, \dots, 9, a, b, c, d, e, f\}$ of nibbles and a quasigroup operation $*$ on Q, together with its parastrophe $\backslash$ (as example, see Table 1).

3.1. Description of coding

Let $M = m_1m_2\dots m_r$ be a block of N_{block} bits, where m_i is a nibble (4-bit letter); hence, $N_{block} = 4r$. We first add redundancy as zero bits and produce block $L = L^{(1)}L^{(2)}\dots L^{(s)} = L_1L_2\dots L_m$ of N bits, where $L^{(i)}$ are 4-nibble words, L_i are nibbles, so $m = 4s, N = 16s$. After erasing the redundant zeros from each $L^{(i)}$ the message L will produce the original message M. On this way we obtain an (N_{block}, N) code with rate $R = N_{block}/N$. The codeword is produced from L after applying the encryption algorithm in TASC given in Figure 1. For that aim, previously, a key $k = k_1k_2\dots k_n$ of length n nibbles should be chosen. The obtained codeword of M is $C = C_1C_2\dots C_m$, where C_i are nibbles.

3.2. Description of decoding

After transmitting through a noise channel (for our experiments we use binary symmetric channel), the codeword C will be transformed to a received message $D = D^{(1)}D^{(2)}\dots D^{(s)} = D_1D_2\dots D_m$, where $D^{(i)}$ are blocks of 4 nibbles and D_j are nibbles. The decoding process consists of four steps: (i) a procedure for generating the sets with predefined Hamming distance, (ii) an inverse coding algorithm, (iii) a procedure for generating decoding candidate sets and (iv) a decoding rule.

Generating sets with predefined Hamming distance: The probability that $\leqslant t$ bits in $D^{(i)}$ are not correct is

$$P(p;t) = \sum_{k=0}^{t} \binom{16}{k} p^k (1-p)^{16-k}.$$

where p is probability of bit-error in a binary symmetric channel. Let B_{max} be an integer such that $1 - P(p; B_{max}) \leqslant q_B$, where q_B $(0 < q_B \leqslant 1)$ is given. Consider the set

$$H_i = \{\alpha | \alpha \in Q^4, \;\; H(D^{(i)}, \alpha) \leqslant B_{max}\},$$

for $i = 1, 2, \ldots, s$, where $H(D^{(i)}, \alpha)$ is the Hamming distance between $D^{(i)}$ and α. Then, with probability at least $1 - q_B$ the block $C^{(i)}$ is an element of the set H_i, for $i = 1, 2, \ldots, s$. The cardinality of the sets H_i is

$$B_{checks} = 1 + \binom{16}{1} + \binom{16}{2} + ... + \binom{16}{B_{max}}$$

and the number B_{checks} determines the complexity of the decoding procedure: for finding the element $C^{(i)}$ in the set H_i, less than or equal to B_{checks} checks have to be made. Clearly, for efficient decoding the number of checks B_{checks} has to be reduced as much as possible.

Inverse coding algorithm: The inverse coding algorithm is the decrypting algorithm of TASC given in Figure 1.

Generating decoding candidate sets: The decoding candidate sets S_0, S_1, S_2,..., S_s are defined iteratively. Let $S_0 = (k_1 \ldots k_n; \lambda)$, where λ is the empty sequence. Let S_{i-1} be defined for $i \geqslant 1$. Then S_i is the set of all pairs $(\delta, w_1 w_2 \ldots w_{16i})$ obtained by using the sets S_{i-1} and H_i as follows (Here, w_j are bits). For each $(\beta, w_1 w_2 \ldots w_{16(i-1)}) \in S_{i-1}$ and each element $\alpha \in H$, we apply the inverse coding algorithm with input (α, β). If the output is the pair (γ, δ) and if both sequences $\gamma = c_1 c_2 \ldots c_{16}$ and $L^{(i)}$ have the redundant nibbles in the same positions, then the pair $(\delta, w_1 w_2 \ldots w_{16(i-1)} c_1 c_2 \ldots c_{16}) \equiv (\delta, w_1 w_2 \ldots w_{16i})$ is an element of S_i.

Decoding rule: The decoding of the received codeword D is given by the following rule: If the set S_s contains only one element $(d_1 \ldots d_n, w_1 \ldots w_{16s})$ then $L = w_1 \ldots w_{16s}$. In this case, we say that we have a *successful decoding*.

In the case when the set S_s contains more than one element, we say that the decoding of D is unsuccessful (and then we say that error of type *more-candidate-error* appears).

In the case when $S_j = \emptyset$ for some $j \in \{1, \ldots, s\}$, the process will be stopped (and then we say that error of type *null-error* appears); we conclude that for some $m \leqslant j$, $D^{(m)}$ contains more than B_{max} errors, resulting with $C_m \notin H$. In this case, whenever it is possible, we may increase the value of B_{max} by 1 and repeat the decoding procedure for the block $D^{(m)}$ again.

Theorem 2. [4] *The packet-error probability of RCBQ is* $q = 1 - (1 - q_B)^s$. □

4. Description of RMC and RSC

RMC are amongst the oldest and most known codes. They were discovered and proposed by D. E. Muller and I. S. Reed in 1954 ([2], [5]). The r^{th} order Reed-Muller code, denoted as $RM(r,m)$, is defined as the set of all polynomials of degree at most r in the ring $F_2[x_0, x_1, \dots x_{m-1}]$. There is a recursive definition of $RM(r,m)$ given as follows.

1. $\mathcal{RM}(0,m) = \{\underbrace{00...0}_{2^m}\ \underbrace{11...1}_{2^m}\}$;
2. $\mathcal{RM}(m,m) = \mathbb{F}_2^{2^m}$;
3. $\mathcal{RM}(r,m) = \{x \| (x \oplus y) \mid x \in \mathcal{RM}(r, m-1), y \in \mathcal{RM}(r-1, m-1)\}$, for $0 < r < m$.

Here, $a \| b$ denotes the concatenation of the words a and b.

For decoding, majority logic decoding is applied.

RMC have many interesting properties that are important for examination. They form an infinite family of codes and larger RMC can be constructed from smaller ones. Unfortunately, RMC become weaker as their length increases. However, they are often used as building blocks in other codes.

The distance of Reed-Muller $RM(r,m)$ code is 2^{m-r} and this code can correct $2^{m-r-1} - 1$ bit errors in the message transmitted through the noise channel.

The RSC were invented in 1960 by I. S. Reed and G. Solomon ([7]). The first application of RSC in mass-production was for the compact discs (1982), where two interleaved RSC are used. Today RSC are used in hard disk drive, DVD, telecommunication, and digital broadcast protocols. These codes are defined over the Galois fields $GF(q)$. The Reed-Solomon code $C_{RS}(n,k)$ of length $n = q - 1$ is defined by the set of polynomials $A(x)$ of degree less than k with coefficients from $GF(q)$. The set of code words for this code is

$$C = \{(c_0, c_1, ..., c_{n-1}) | c_i = A(\alpha^i),\ i = 0, 1, ..., n-1,\ \deg(A(x)) < k\}$$

where α is a primitive element of $GF(q)$. The input message consists of k symbols from $GF(q)$ and they are the coefficients of the polynomials $A(x)$. The decoding is usually realized by using Berlekamp-Massey algorithm.

The Reed-Solomon code $C_{RS}(n,k)$ has minimum distance $n-k+1$ and it can correct $t = \lfloor (n-k)/2 \rfloor$ symbol errors in a code word.

5. Choosing parameters for optimal RCBQ

RCBQ have several parameters, and we have investigated the influence of the code parameters to the code performances [8]. Since RCBQ are designed using quasigroup string transformations on messages extended by introduced redundancy, we have pointed out how 1) the pattern of the redundancy, 2) the length of the key of TASC and 3) the chosen quasigroups, affect the codes.

We have made experiments in the following way. First, we extend input message using different patterns for redundant zero nibbles, and after that we encode the extended message and transmit it through a binary symmetric channel with probability p of bit error. For coding and decoding we use the codes described in Section 3. The outgoing message is decoded and if the decoding process completed successfully (the last set S_s of candidates for decoding has only one element), the decoded message is compared with the input message. If they differ at least one bit, then we say that an uncorrected-error appears. Then we compute the number of incorrectly decoded bits as Hamming distance between the input and the decoded message. Experiments showed that this type of package error occurs rarely.

In our experiments we also calculate the number of incorrectly decoded bits when the decoding process finish with more-candidate-error or null-error. Then, that number is calculated as follows.

When null-error appears, i.e., $S_i = \emptyset$, we take all the elements from the set S_{i-1} and we find their maximal common prefix substring. If this substring has k bits and the length of the sent message is m bits ($k \leqslant m$), then we compare this substring with the first k bits of the sent message. If they differ in s bits, then the number of incorrectly decoded bits is $m-k+s$.

If a more-candidates-error appears we take all the elements from the set S_s and we find their maximal common prefix substring. The number of incorrectly decoded bits is computed as previous.

The total number of incorrectly decoded bits is the sum of all of the previously mentioned numbers of incorrectly decoded bits.

We compute the probability of packet-error as

$$\text{PER} = \#(\textit{incorrectly decoded packets})/\#(\textit{all packets})$$

and the probability of bit-error as

$$\text{BER} = \#(\textit{incorrectly decoded bits in all packets}) \ / \ \#(\textit{bits in all packets}).$$

Experiments are made for different values of bit-error probability p of binary symmetric channel and $B_{max} = 3$ and $B_{max} = 4$. For $B_{max} > 4$, the experiments do not terminate in real time.

Redundancy pattern. We made experiments for different 6 patterns for redundant zero nibbles for (72,288) code with rate R=1/4. In these experiments we have used the quasigroup given in Fig. 1, the initial key $k = 01234$ and the following 6 patterns:

patt.1	**patt.2**	**patt.3**	**patt.4**	**patt.5**	**patt.6**
1000 1000	1100 1100	1100 1100	1100 1100	1100 1000	1100 1100
1000 1000	0000 1100	1000 0000	1100 0000	0000 1100	1000 0000
1000 1000	1100 0000	1100 1000	0000 1100	1000 0000	1100 1100
1000 1000	1100 1100	1000 0000	1100 1100	1100 1000	1000 0000
1000 1000	0000 1100	1100 1100	0000 0000	0000 1100	1100 1100
1000 1000	1100 0000	1000 0000	1100 1100	1000 0000	1000 0000
1000 1000	1100 0000	1100 1000	1100 0000	1100 1000	1000 1000
1000 1000	0000 0000	1000 0000	0000 0000	0000 1100	1000 0000
1000 1000	0000 0000	0000 0000	0000 0000	1000 0000	0000 0000

From the experimental results obtained for all six proposed patterns we conclude that the best results for PER and BER are obtained for the third pattern **patt.3**.

Key length. Theoretical probability of packet-error given in Theorem 2 is determined under the assumption that the code is perfectly random (i.e., the r-tuple are uniformly distributed in each codeword with length N, $r \leqslant N$). Therefore, in that theorem the more-candidates-errors are not provided. In Theorem 1 it is proved that if we apply t quasigroup transformations on a string, we obtain string where n-tuples of letters are uniformly distributed for $n \leqslant t$. In the design of these codes, the length of the key k determines how many times quasigroup transformations will be applied in forming of codeword. Therefore, longer key of the code gives "more random" code. This means that the results of experimental PER will be closer to the theoretical values for PER, i.e., the number of more-candidates-errors will be reduced. So, we made experiments with the third pattern (which give the best results) with key length 10. From the obtained results we saw that in some experiments more-candidates-error are not appeared, and if they appear, their number is very small. We can conclude that when we use a longer key, we can obtain better results for PER with almost the same

$*$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	3	c	2	5	f	7	6	1	0	b	d	e	8	4	9	a
1	0	3	9	d	8	1	7	b	6	5	2	a	c	f	e	4
2	1	0	e	c	4	5	f	9	d	3	6	7	a	8	b	2
3	6	b	f	1	9	4	e	a	3	7	8	0	2	c	d	5
4	4	5	0	7	6	b	9	3	f	2	a	8	d	e	c	1
5	f	a	1	0	e	2	4	c	7	d	3	b	5	9	8	6
6	2	f	a	3	c	8	d	0	b	e	9	4	6	1	5	7
7	e	9	c	a	1	d	8	6	5	f	b	2	4	0	7	3
8	c	7	6	2	a	f	b	5	1	0	4	9	e	d	3	8
9	b	e	4	9	d	3	1	f	8	c	5	6	7	a	2	0
a	9	4	d	8	0	6	5	7	e	1	f	3	b	2	a	c
b	7	8	5	e	2	a	3	4	c	6	0	d	f	b	1	9
c	5	2	b	6	7	9	0	e	a	8	c	f	1	3	4	d
d	a	6	8	4	3	e	c	d	2	9	1	5	0	7	f	b
e	d	1	3	f	b	0	2	8	4	a	7	c	9	5	6	e
f	8	d	7	b	5	c	a	2	9	4	e	1	3	6	0	f

$\backslash$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	8	7	2	0	d	3	6	5	c	e	f	9	1	a	b	4
1	0	5	a	1	f	9	8	6	4	2	b	7	c	3	e	d
2	1	0	f	9	4	5	a	b	d	7	c	e	3	8	2	6
3	b	3	c	8	5	f	0	9	a	4	7	1	d	e	6	2
4	2	f	9	7	0	1	4	3	b	6	a	5	e	c	d	8
5	3	2	5	a	6	c	f	8	e	d	1	b	7	9	4	0
6	7	d	0	3	b	e	c	f	5	a	2	8	4	6	9	1
7	d	4	b	f	c	8	7	e	6	1	3	a	2	5	0	9
8	9	8	3	e	a	7	2	1	f	b	4	6	0	d	c	5
9	f	6	e	5	2	a	b	c	8	3	d	0	9	4	1	7
a	4	9	d	b	1	6	5	7	3	0	e	c	f	2	8	a
b	a	e	4	6	7	2	9	0	1	f	5	d	8	b	3	c
c	6	c	1	d	e	0	3	4	9	5	8	2	a	f	7	b
d	c	a	8	4	3	b	1	d	2	9	0	f	6	7	5	e
e	5	1	6	2	8	d	e	a	7	c	9	4	b	0	f	3
f	e	b	7	c	9	4	d	2	0	8	6	3	5	1	a	f

Table 1: Quasigroup of order 16 and its parastrophe used in the experiments

duration of the decoding process.

Choosing of a quasigroup. Since we work with finite sequences, the randomness of a sequence obtained by quasigroup transformations depends on the used quasigroup. So, we did experiments with several quasigroups, which showed that the choice of the quasigroup does not affect only the values of PER and BER, but they have an enormous influence on the speed of decoding.

First we did experiments with the cyclic group of order 16 and the length of the key 10. Decoding for the third pattern was too slow. So, we did experiment with the first pattern for binary symmetric channel with $p = 0.02$ and $B_{max} = 3$, and we received PER=0.734087 and BER=0.460359 (that is much worse then PER=0.1186, BER=0.0089 obtained by the quasigroup in Table 1). Hence, it is clear that the choice of quasigroup has enormous influence over the performances of the code.

After that we made experiments with quasigroup of order 16 obtained as a direct product of a quasigroup of order 2. Experimental results obtained

with this quasigroup are worse than the results for cyclic group. For the first pattern, $p = 0.02$ and $B_{max} = 3$ we got PER=0.99424 and BER=0.80869.

The cyclic group and the direct product of quasigroups of order 2 are examples of so called fractal quasigroups, they produce biased sequences. The quasigroup in Table 1 is an example of so called non-fractal quasigroups. The results obtained by this quasigroup were quite satisfactory.

From the experiments, we can conclude that the best results for a RCBQ(72,288) were obtained for the third pattern, key length 10, quasigroup given in the Figure 1 (together with its parastrophe) and $B_{max} = 4$. We compare that code with RMC and RSC.

6. Experimental results for comparison

We have made several experiments in order to compare the performances of RCBQ(72,288) of rate 1/4 with Reed-Muller and Reed-Solomon codes of the same rate. (The experiments were made on ordinary PC, 2.6 GHz and 2 Gb RAM.) Because of the construction of RMC, its rate was chosen to be $130/512 \approx 1/4$. We considered transmissions through binary symmetrical channel for several values of probability p of bit-error. In order to obtain relevant statistics, we have made experiments with 13888 packets for RSC, 7692 packets for RMC and 3200 packets for RCBQ. (The experiments for RCBQ are time consuming.) In the experiments we have analyzed the packet-errors and the bit-errors.

For coding with the Reed-Muller code $RM(r, m)$, an input message is divided into blocks of $k = \sum_{i=0}^{r} \binom{m}{i}$ bits, and these blocks are encoded with code words with length $n = 2^m$. In this case, the code rate is $R = k/n$. We need to choose appropriate values for the parameters r and m, such that the code rate will be the closest to $R = 1/4$. Therefore, we made experiments with the code RMC(3,9), the length of the messages is $k = 130$ bits, and the length of the corresponding code words is $n = 512$ bits, i.e., the code rate is $R = 130/512 = 0.2539$.

In our experiments, we have used a shortened version of the RSC(63,27). It is the code RSC(48,12) defined over the Galois field $GF(2^6)$ with a primitive polynomial $p(x) = 1 + X + X^6$ (and it has the same good properties as general RSC). The shortened RSC has the same length of the code words (288 bits) and the same rate (1/4) as the considered RCBQ.

The probability of packet error. The results of the experiments for the PER are given in Table 2 and presented in Figure 2. We can derive the following conclusions.

p	RMC(3,9)	RSC(48,12)	RCBQ(72,288)
0.01	0	0	0.001250
0.02	0	0	0.001250
0.03	0	0.000216	0.003125
0.04	0.000650	0.003312	0.005938
0.05	0.010400	0.028874	0.015938
0.06	0.083073	0.107503	0.035938
0.07	0.260530	0.290251	0.066563
0.08	0.533021	0.505112	0.113125
0.09	0.759750	0.713062	0.188750
0.10	0.914587	0.845694	0.257813
0.11	0.971659	0.933899	0.350000

Table 2: Experimental results obtained for PER.

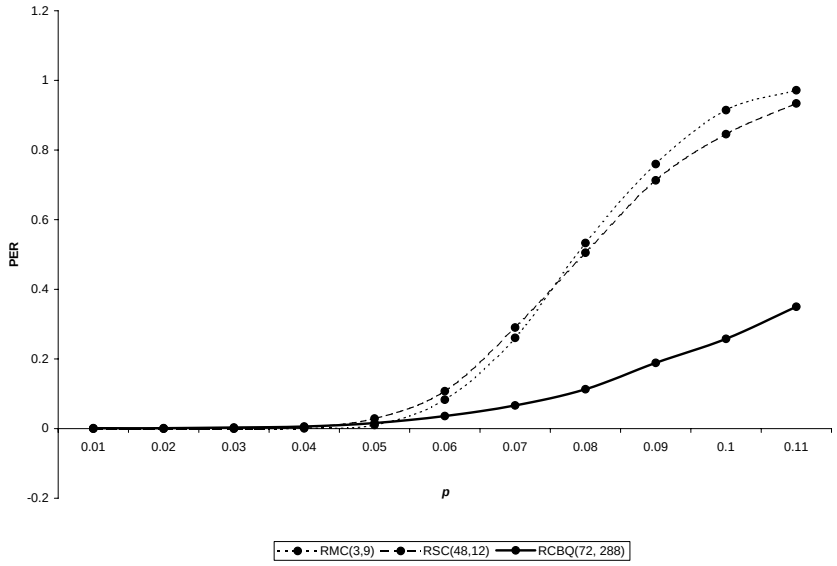


Figure 2: Comparison of PER for all three codes.

The RMC is the best code (with smallest values of PER) for $p \leqslant 0.05$. For $0.05 < p \leqslant 0.07$, RMC is better than RSC, but it is worse than RCBQ. For $p \geqslant 0.08$, RMC has the worst performances. The RSC has better

performances than RMC only for $p \geqslant 0.08$. RCBQ is better than RMC and RSC for $p > 0.05$. It is noticeable that RMC and RSC have similar performances for $p \geqslant 0.06$, while the performances of RCBQ become much better. Maybe the best characteristic for RCBQ appears when $p \geqslant 0.08$, since then RMC and RSC are useless (see Table 2), while RCBQ gives still reliable values.

The rate of growing of these codes is given in Table 3. So, RMC has the highest rate of growing, but it starts with very small PER for small values of p. The similar conclusion holds for RSC, too. The results for RCBQ are much better since the rates of growing are smaller than the suitable rates of RMC and RSC for all considered values of p. Therefore, we conclude that RCBQ is capable to decode for higher values of p.

	RMC(3,9)	RSC(48, 12)	RCBQ(72, 288)
p_1-p_2	PER(p_2)/PER(p_1)	PER(p_2)/PER(p_1)	PER(p_2)/PER(p_1)
0.01 - 0.02	/	/	1.00
0.02 - 0.03	/	/	2.50
0.03 - 0.04	/	15.33	1.90
0.04 - 0.05	16.00	8.72	2.68
0.05 - 0.06	8.00	3.72	2.25
0.06 - 0.07	3.14	2.70	1.85
0.07 - 0.08	2.05	1.74	1.70
0.08 - 0.09	1.43	1.41	1.67
0.09 - 0.10	1.20	1.19	1.37
0.10 - 0.11	1.06	1.10	1.36

Table 3: The rate of growing of PER.

The probability of bit error. The results of the experiments for the BER are given in Table 4 and presented in Figure 3.

It can be seen that we have similar results for BER as for PER, but the differences between the results for RCBQ and those for RMC and RSC are not so significant. The reason for that lies in the constructions of the codes. Namely, for RCBQ, when a bit is incorrectly decoded, then almost all consecutive bits are incorrectly decoded. On the other side, the number of bit-errors in a packet decoded by RMC or RSC are smaller, but they appear in almost all packets when $p \geqslant 0.08$.

Although the code of Reed-Solomon did not give the best results for PER and BER for any value of p, compared with the other two reviewed codes, this code has the best performance in terms of speed of the decoding

process. This is a very important feature in the coding theory. Namely, as a rule, a coding procedure is easily to be done fast and simple, but the problem in designing of codes is to make the decoding process to be time effective (in terms of capabilities for fast detecting and correcting the errors). The speed of decoding is a very important factor since in many real applications the codes work with huge amounts of data.

p	RMC(3,9)	RSC(48, 12)	RCBQ(72, 288)
0.01	0	0	0.000577
0.02	0	0	0.000759
0.03	0	0.000041	0.001359
0.04	0.000181	0.000671	0.003429
0.05	0.002488	0.006082	0.009279
0.06	0.020369	0.023117	0.022396
0.07	0.064838	0.063642	0.040647
0.08	0.135881	0.113436	0.064852
0.09	0.206767	0.166291	0.113572
0.10	0.268919	0.206621	0.156029
0.11	0.320262	0.239463	0.218902

Table 4: Experimental results obtained for BER.

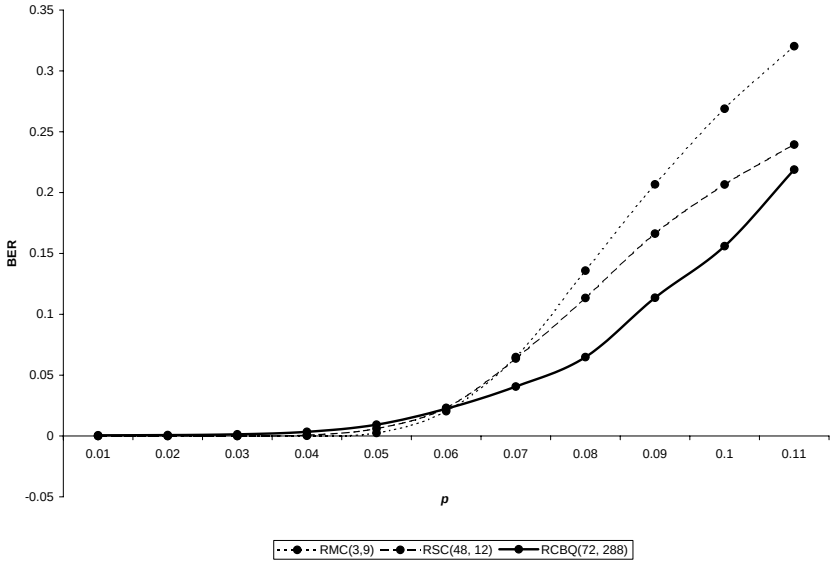


Figure 3: Comparison of BER for all three codes.

In the experiments with these three codes it can be noted that decoding with RCBQ is very complex and it is not time effective, especially for larger values of B_{max}. Thus, decoding of a packet is in average 25 times slower by using $B_{max} = 4$ instead of $B_{max} = 3$. Decoding a packet by using $B_{max} = 5$ could not be finished for a day. Nevertheless, RCBQ can be very useful for decoding messages transmitted through a very noisy channels (with up to 10% noise), especially when the decoding speed is not an important factor (for example, decoding a pictures transmitted from the deep space). The difference of the obtained decoding by using $B_{max} = 3$ and $B_{max} = 4$ can be noticed from Table 5. There, we can see that we have the same values for PER and BER when $B_{max} = 3$ with bit-error $p = 0.05$, and $B_{max} = 4$ with bit-error $p = 0.08$. The values PER_t in Table 5 are the theoretical probabilities according to Theorem 2. The paper [4] contains results for $B_{max} = 5$ and $B_{max} = 6$, obtained by using some auxiliary heuristic algorithms. The same results for PER and BER as above are obtained when $B_{max} = 5$ with bit-error $p \approx 0.115$, and $B_{max} = 6$ with bit-error $p \approx 0.155$.

$B_{max} = 3$			
p	PER_t	PER	BER
0.02	0.004314	0.004752	0.002093
0.03	0.019674	0.018433	0.008493
0.04	0.055435	0.055588	0.026289
0.05	0.118838	0.117584	0.054876
$B_{max} = 4$			
0.03	0.001447	0.003125	0.001359
0.04	0.005541	0.005938	0.003429
0.05	0.015319	0.015938	0.009279
0.06	0.034361	0.035938	0.022396
0.07	0.066467	0.066563	0.040647
0.08	0.114889	0.113125	0.064852

Table 5: Experimental results for $B_{max} = 3$ and $B_{max} = 4$

7. Conclusion

The RMC and the RSC are well known codes that are applied for many practical purposes. The RCBQ are new kind of codes defined by using quasigroups and quasigroup transformations, so RCBQ are based on quite

different principals than those of RMC and RSC. Here we have compared the decoding capacities of these three types of codes in terms on time effectiveness and capabilities for detecting and correcting the errors. For that aims several experiments were produced and relevant statistics were inferred from them. Generally, the RMC and the RSC have better decoding performances in a binary symmetrical channel with bit-error probability $p < 0.05$. In the opposite case, the RCBQ outperforms them significantly. Nevertheless, the time efficiency of the RMC and the RSC is much higher than that of RCBQ. So, the speed of decoding of RCBQ is its disadvantage and it is a challenge for further improvements.

We note that there are interesting results considering RMC and RCBQ when performed in a bounded binary symmetrical channel. A bounded binary symmetrical channel where the maximal number of erroneous bits in every 16 transmitted bits was 5 was considered in [4]. There was shown that RCBQ of rate 3/16 could decode a 32-bit message with 8-10 erroneous bits, while RMC (with the same rate) was not capable to do the decoding. These results suggest further investigations on the performances of RCBQ in different kind of channels.

Another feature of the RCBQ is that they have cryptographic properties. Namely, if the data are encoded with these random codes, then the recipient can decode the original data only if s/he knows exactly which parameters are used in the process of encoding, even if the communication channel is without noise. By the definition and the design of RCBQ, it is clear that if we want to implement the algorithms for decoding we must know the quasigroup and the primary key that is used for encoding the messages and, of course, the pattern for introducing the redundant nibbles into original message. (We could use not only zeros as a redundancy information, it can be any string, even with semantic meaning.) Therefore, the usage of RCBQ for cryptographic purposes is its another advantage over RMC and RSC.

References

[1] **V. Bakeva, V. Dimitrova**, *Some probabilistic properties of quasigroup processed strings useful in cryptanalysis*, M.Gushev, P.Mitreski (Eds.): ICT-Innovations 2010, Springer (2010), 61 – 70.

[2] **M. Bossert**, *Channel coding for telecommunications*, John Wiley and Sons, Ltd (1999).

[3] **D. Gligoroski, S. Markovski, Lj. Kocarev**, *Totally asynchronous stream ciphers + redundancy = cryptcoding*, S. Aissi, H.R. Arabnia (Eds.): Proc.

Internat. Confer. Security and Management, SAM 2007, Las Vegas, CSREA Press (2007), 446 – 451.

[4] **D. Gligoroski, S. Markovski, Lj. Kocarev**, *Error-correcting codes based on quasigroups*, Proc. 16th Intern. Confer. Computer Communications and Networks (2007), 165 – 172.

[5] **D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, J. R. Wall**, *Coding Theory, The Essentials*, Auburn University, Auburn, Alabama (1992).

[6] **S. Markovski, D. Gligoroski, V. Bakeva**, *Quasigroup string processing: Part 1*, Maced. Acad. of Sci. and Arts, Sec. Math. Tech. Scien. **XX** 1-2 (1999), 13 – 28.

[7] **J. C. Moreira, P. G. Farrell**, *Essentials of error-control coding*, John Wiley and Sons, Ltd (2006).

[8] **A. Popovska-Mitrovikj, S. Markovski, V. Bakeva**, *Performances of error-correcting codes based on quasigroups*, ICT-Innovations 2009, Springer (2009), 377 – 389.

Received May 31, 2011

Faculty of Computer Science and Engineering, Ss Cyril and Methodius University,
Rudzer Boshkovikj, 16, P.O.Box 393, Skopje, Republic of Macedonia
E-mails: aleksandra.popovska.mitrovikj@finki.ukim.mk,
verica.bakeva@finki.ukim.mk, smile.markovski@finki.ukim.mk

Quasigroups and Related Systems **19** (2011), 317 – 329

Characterizations of hemirings by interval valued fuzzy ideals

Muhammad Shabir and Tahir Mahmood

Abstract. In this paper we define interval valued fuzzy h-quasi-ideals and interval valued fuzzy h-bi-ideals. We characterize h-hemiregular and h-intra-hemiregular hemirings by the properties of their interval valued fuzzy h-ideals, interval valued fuzzy h-quasi-ideals, and interval valued fuzzy h-bi-ideals.

1. Introduction

Semirings, which are the generalization of associative rings, introduced by H. S. Vandiver in 1934 [12], are very useful for solving problems in different areas of applied mathematics and information sciences, like as, optimization theory, graph theory, theory of discrete event dynamical systems, matrices, determinants, generalized fuzzy computation, automata theory, formal language theory, coding theory, analysis of computer programs, and so on. Hemirings, which are semirings with commutative addition and zero element appears in a natural manner in some applications to the theory of automata and formal languages (see [4]).

Like in rings theory, ideals play important role in the study of hemirings and are useful for many purposes. But they do not coincide with ring ideals. Thus many results of ring theory have no analogues in semirings using only ideals. In order to overcome this deficiency, Henriksen [5] defined a class of ideals in semirings, called k-ideals. These ideals have the property that if the semiring R is a ring then a subset of R is a k-ideal if and only if it is a ring ideal. A more restricted class of ideals in hemirings is defined by Iizuka [6], called h-ideals. La Torre [8] thoroughly studied h-ideals and k-ideals and established some analogues ring results for semirings.

Zadeh [14], in 1965, introduced the concept of fuzzy set. Which proved

2010 Mathematics Subject Classification: 16Y60, 08A72, 03G25, 03E72
Keywords: interval valued fuzzy h-ideals, interval valued fuzzy h-quasi-ideal, interval valued fuzzy h-bi-ideal.

a very useful tool to describe situation in which the data are imprecise or vague. Fuzzy sets handle such situations by attributing a degree to which a certain object belongs to a set. The concept of fuzzy set was further carried out by many researchers to generalize some notions of algebra. In [2] J. Ahsan initiated the study of fuzzy semirings (see also [1]). Fuzzy k-ideals in semirings are studied in [3] by Ghosh and fuzzy h-ideals are studied in [7, 10, 13, 15].

In [9] Ma and Zhan introduced the concept of interval valued fuzzy h-ideals in hemirings and develop some results associated with it. In [11] Sun et al characterized h-hemiregular and h-intra-hemiregular hemirings by the properties of their interval valued fuzzy left and right h-ideals. In this paper we extend this idea and define interval valued fuzzy h-quasi-ideals and interval valued fuzzy h-bi-ideals. We characterize h-hemiregular and h-intra-hemiregular hemirings by the properties of their interval valued fuzzy h-ideals, interval valued fuzzy h-quasi-ideals, and interval valued fuzzy h-bi-ideals.

2. Preliminaries

For basic definitions of ideals see [4]. A left (right) ideal I of a hemiring R is called a *left* (*right*) *h-ideal* if for all $x, z \in R$ and for any $a_1, a_2 \in I$ from $x + a_1 + z = a_2 + z$, it follows $x \in I$ (cf. [8]). A bi-ideal B of a hemiring R is called an *h-bi-ideal* of R if for all $x, z \in R$ and $a_1, a_2 \in B$ from $x + a_1 + z = a_2 + z$, it follows $x \in B$ (cf. [13]).

The *h-closure* $\overline{A}$ of a non-empty subset A of a hemiring R is defined as

$$\overline{A} = \{x \in R \mid x + a + z = b + z \quad \text{for some } a, b \in A, z \in R\}.$$

A quasi-ideal Q of a hemiring R is called an *h-quasi-ideal* of R if $\overline{RQ} \cap \overline{QR} \subseteq Q$ and $x + a_1 + z = a_2 + z$ implies $x \in Q$, for all $x, z \in R$ and $a_1, a_2 \in Q$ (cf. [13]). Every left (right) h-ideal of a hemiring R is an h-quasi-ideal of R and every h-quasi-ideal is an h-bi-ideal of R. However, the converse is not true in general (cf. [13]).

Definition 2.1. A hemiring R is said to be *h-hemiregular* if for each $x \in R$, there exist $a, b, z \in R$ such that $x + xax + z = xbx + z$.

Lemma 2.2. [15] *A hemiring R is h-hemiregular if and only if for any right h-ideal I and any left h-ideal L of R we have $\overline{IL} = I \cap L$.* □

Lemma 2.3. [13] *For a hemiring R the following conditions are equivalent.*

(i) *R is h-hemiregular.*

(ii) *$B = \overline{BRB}$ for every h-bi-ideal B of R.*

(iii) *$Q = \overline{QRQ}$ for every h-quasi-ideal Q of R.* □

Lemma 2.4. [13] *A hemiring R is h-hemiregular if and only if the right and left h-ideals of R are idempotent and for any right h-ideal I and left h-ideal L of R, $\overline{IL}$ is an h-quasi- ideal of R.* □

Definition 2.5. [13] A hemiring R is said to be *h-intra-hemiregular* if for each $x \in R$, there exist $a_i, a_i', b_j, b_j', z \in R$ such that $x + \sum_{i=1}^{m} a_i x^2 a_i' + z = \sum_{j=1}^{n} b_j x^2 b_j' + z$.

Lemma 2.6. [13] *A hemiring R is h-intra-hemiregular if and only if for any right h-ideal I and any left h-ideal L of R we have $I \cap L \subseteq \overline{LI}$.* □

Lemma 2.7. [13] *The following conditions are equivalent for a hemiring R.*

(1) *R is both h-hemiregular and h-intra-hemiregular.*

(2) *$B = \overline{B^2}$ for every h-bi-ideal B of R.*

(3) *$Q = \overline{Q^2}$ for every h-quasi-ideal Q of R.* □

3. Interval valued fuzzy sets

A fuzzy subset f is a function $f : X \to [0, 1]$. Now let $\mathcal{L}$ be the family of all closed subintervals of $[0, 1]$ with minimal element $\tilde{O} = [0, 0]$ and maximal element $\tilde{I} = [1, 1]$ according to the partial order $[\alpha, \alpha'] \leqslant [\beta, \beta']$ if and only if $\alpha \leqslant \beta, \alpha' \leqslant \beta'$ defined on $\mathcal{L}$ for all $[\alpha, \alpha'], [\beta, \beta'] \in \mathcal{L}$. An interval valued fuzzy subset λ of a hemiring R is a function $\lambda : R \to \mathcal{L}$.

We write $\lambda(x) = [\lambda^-(x), \lambda^+(x)] \subseteq [0, 1]$, for all $x \in R$, where λ^-, λ^+ are fuzzy subsets of R such that for each $x \in R$, $0 \leqslant \lambda^-(x) \leqslant \lambda^+(x) \leqslant 1$. For simplicity we write $\lambda = [\lambda^-, \lambda^+]$.

Let $A \subseteq R$. Then the interval valued characteristic function χ_A of A is defined to be a function $\chi_A : R \to \mathcal{L}$ such that for all $x \in R$

$$\chi_A(x) = \begin{cases} \tilde{I} = [1, 1] & \text{if } x \in A, \\ \tilde{O} = [0, 0] & \text{if } x \notin A. \end{cases}$$

Clearly the interval valued characteristic function of any subset of R is also an interval valued fuzzy subset of R. Note that $\chi_R(x) = \tilde{I}$ for all $x \in R$.

For any two interval valued fuzzy subsets λ and μ of a hemiring R we define

$$(\lambda \vee \mu)(x) = [\lambda^-(x) \vee \mu^-(x), \lambda^+(x) \vee \mu^+(x)],$$
$$(\lambda \wedge \mu)(x) = [\lambda^-(x) \wedge \mu^-(x), \lambda^+(x) \wedge \mu^+(x)],$$

where

$\lambda^-(x) \vee \mu^-(x) = \sup\{\lambda^-(x), \mu^-(x)\}, \lambda^-(x) \wedge \mu^-(x) = \inf\{\lambda^-(x), \mu^-(x)\}$,
$\lambda^+(x) \vee \mu^+(x) = \sup\{\lambda^+(x), \mu^+(x)\}, \lambda^+(x) \wedge \mu^+(x) = \inf\{\lambda^+(x), \mu^+(x)\}$.

For any two interval valued fuzzy subsets λ and μ of a hemiring R, $\lambda \leqslant \mu$ if and only if $\lambda(x) \leqslant \mu(x)$, that is $\lambda^-(x) \leqslant \mu^-(x)$ and $\lambda^+(x) \leqslant \mu^+(x)$, for all $x \in R$.

Definition 3.1. [11] Let λ and μ be two interval valued fuzzy subsets in a hemiring R. Then the *h-intrinsic product* of λ and μ is defined by

$$(\lambda \odot \mu)(x) = \sup \left\{ \begin{array}{l} \bigwedge_{i=1}^{m} \left(\lambda^-(a_i) \wedge \mu^-(b_i)\right) \wedge \bigwedge_{j=1}^{n} \left(\lambda^-(a'_j) \wedge \mu^-(b'_j)\right), \\ \bigwedge_{i=1}^{m} \left(\lambda^+(a_i) \wedge \mu^+(b_i)\right) \wedge \bigwedge_{j=1}^{n} \left(\lambda^+(a'_j) \wedge \mu^+(b'_j)\right), \end{array} \right\}$$

for all $x \in R$, if x can be expressed as $x + \Sigma_{i=1}^{m} a_i b_i + z = \Sigma_{j=1}^{n} a'_j b'_j + z$, and $\tilde{O}$ if x cannot be expressed as $x + \Sigma_{i=1}^{m} a_i b_i + z = \Sigma_{j=1}^{n} a'_j b'_j + z$.

An interval valued fuzzy subset λ of a hemiring R is said to be *idempotent* if $\lambda \odot \lambda = \lambda$.

Lemma 3.2. [11] *Let R be a hemiring and $A, B \subseteq R$. Then we have*

(1) $A \subseteq B \longleftrightarrow \chi_A \leqslant \chi_B$,
(2) $\chi_A \wedge \chi_B = \chi_{A \cap B}$,
(3) $\chi_A \odot \chi_B = \chi_{\overline{AB}}$.

Definition 3.3. Let λ be an interval valued fuzzy subset of a hemiring R. Then λ is said to be an *interval valued fuzzy left* (resp. *right*) *h-ideal* of R if and only if for all $x, y \in R$

(i) $\lambda(x + y) \geqslant \lambda(x) \wedge \lambda(y)$,
(ii) $\lambda(xy) \geqslant \lambda(y)$ (resp. $\lambda(xy) \geqslant \lambda(x)$)
(iii) $x + a + y = b + y \longrightarrow \lambda(x) \geqslant \lambda(a) \wedge \lambda(b)$, for all $a, b, x, y \in R$.

An interval valued fuzzy subset $\lambda : R \to \mathcal{L}$ is called an *interval valued fuzzy h-ideal* of hemiring R if it is both, interval valued fuzzy left and right h-ideal of R.

Definition 3.4. An interval valued fuzzy subset λ of a hemiring R is called an *interval valued fuzzy h-bi-ideal* of R if it satisfies (i), (iii) and

(iv) $\lambda(xy) \geqslant \min\{\lambda(x), \lambda(y)\}$,
(v) $\lambda(xyz) \geqslant \min\{\lambda(x), \lambda(z)\}$
for all $x, y, z \in R$.

An interval valued fuzzy subset λ of a hemiring R is called an *interval valued fuzzy h-quasi-ideal* of R if it satisfies (i), (iii) and
(vi) $(\lambda \odot \mathcal{R}) \wedge (\mathcal{R} \odot \lambda) \leqslant \lambda$.

Note that if λ is any interval valued fuzzy left h-ideal (right h-ideal, h-bi-ideal, h-quasi-ideal), then $\lambda(0) \geqslant \lambda(x)$ for all $x \in R$.

Lemma 3.5. *A subset A of a hemiring R is an h-ideal (resp., h-bi-ideal, h-quasi-ideal) of R if and only if χ_A is an interval valued fuzzy h-ideal (resp., h-bi-ideal, h-quasi-ideal) of R.* □

Theorem 3.6. *Every interval valued fuzzy right(left) h-ideal is interval valued fuzzy h-quasi-ideal.* □

Converse of the Theorem 3.6 is not true in general.

Example 3.7. Let $\mathbb{Z}_0 = \mathbb{Z}^+ \cup \{0\}$, $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_0 \right\}$ and $Q = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{Z}_0 \right\}$. Then R is a hemiring under the usual binary operations of addition and multiplication of matrices, and Q is h–quasi-ideal of R but Q is not left (right) h-ideal of R. Then by Lemma 3.5, the characteristic function χ_Q is an interval valued fuzzy h-quasi-ideal of R and by Lemma 3.5, χ_Q is not interval valued fuzzy left (right) h-ideal of R. □

Theorem 3.8. *If λ is an interval valued fuzzy right h-ideal and μ an interval valued fuzzy left h-ideal of a hemiring R, then $\lambda \wedge \mu$ is an interval valued fuzzy h-quasi-ideal of R.*

Proof. Let $x, y \in R$. Then

$$(\lambda \wedge \mu)(x+y) = [\lambda^-(x+y) \wedge \mu^-(x+y), \lambda^+(x+y) \wedge \mu^+(x+y)]$$
$$\geqslant [\lambda^-(x) \wedge \lambda^-(y) \wedge \mu^-(x) \wedge \mu^-(y), \lambda^+(x) \wedge \lambda^+(y) \wedge \mu^+(x) \wedge \mu^+(y)]$$
$$= [\lambda^-(x) \wedge \mu^-(x),\ \lambda^+(x) \wedge \mu^+(x)] \wedge [\lambda^-(y) \wedge \mu^-(y),\ \lambda^+(y) \wedge \mu^+(y)]$$
$$= (\lambda \wedge \mu)(x) \wedge (\lambda \wedge \mu)(y).$$

Now $((\lambda \wedge \mu) \odot \mathcal{R}) \wedge (\mathcal{R} \odot (\lambda \wedge \mu)) \leqslant (\lambda \odot \mathcal{R}) \wedge (\mathcal{R} \odot \mu) \leqslant \lambda \wedge \mu$.

Next let $a, b, x, z \in R$ such that $x + a + z = b + z$. Then

$(\lambda \wedge \mu)(x) = [\lambda^-(x) \wedge \mu^-(x), \lambda^+(x) \wedge \mu^+(x)]$

$$\geqslant [\lambda^-(a) \wedge \lambda^-(b) \wedge \mu^-(a) \wedge \mu^-(b), \lambda^+(a) \wedge \lambda^+(b) \wedge \mu^+(a) \wedge \mu^+(b)]$$
$$= [\lambda^-(a) \wedge \mu^-(a),\ \lambda^+(a) \wedge \mu^+(a)] \wedge [\lambda^-(b) \wedge \mu^-(b),\ \lambda^+(b) \wedge \mu^+(b)]$$
$$= (\lambda \wedge \mu)(a) \wedge (\lambda \wedge \mu)(b).$$

Hence $\lambda \wedge \mu$ is an interval valued fuzzy h-quasi-ideal of R. □

Theorem 3.9. *Any interval valued fuzzy h-quasi-ideal of a hemiring R is an interval valued fuzzy h-bi-ideal of R.*

Proof. Let λ be any interval valued fuzzy h-quasi-ideal of R. Then for all $x, y, z \in R$, for all expressions $xyz + \Sigma_{i=1}^{m} a_i b_i + z' = \Sigma_{j=1}^{n} a'_j b'_j + z'$, we have

$$\lambda(xyz) \geqslant ((\lambda \odot \mathcal{R}) \wedge (\mathcal{R} \odot \lambda))(xyz) = (\lambda \odot \mathcal{R})(xyz) \wedge (\mathcal{R} \odot \lambda)(xyz)$$
$$= \begin{bmatrix} \sup\left\{\left(\bigwedge_{i=1}^{m} \lambda^-(a_i)\right) \wedge \left(\bigwedge_{j=1}^{n} \lambda^-(a'_j)\right), \left(\bigwedge_{i=1}^{m} \lambda^+(a_i)\right) \wedge \left(\bigwedge_{j=1}^{n} \lambda^+(a'_j)\right)\right\} \\ \wedge\ \sup\left\{\left(\bigwedge_{i=1}^{m} \lambda^-(b_i)\right) \wedge \left(\bigwedge_{j=1}^{n} \lambda^-(b'_j)\right), \left(\bigwedge_{i=1}^{m} \lambda^+(b_i)\right) \wedge \left(\bigwedge_{j=1}^{n} \lambda^+(b'_j)\right)\right\} \end{bmatrix}$$
$$\geqslant \{\lambda^-(0) \wedge \lambda^-(x), \lambda^+(0) \wedge \lambda^+(x)\} \wedge \{\lambda^-(0) \wedge \lambda^-(z), \lambda^+(0) \wedge \lambda^+(z)\}$$
(because $xyz+00+0 = x(yz)+0$ and $xyz+00+0 = (xy)z+0$)
$$= \lambda(x) \wedge \lambda(z)$$

Similarly we can show that $\lambda(xy) \geqslant \lambda(x) \wedge \lambda(y)$ for all $x, y \in R$. Hence λ is an interval valued fuzzy h-bi-ideal of R. □

Converse of the Theorem 3.9 is not true in general.

Example 3.10. Let $\mathbb{Z}^+$ and $\mathbb{R}^+$ be the sets of all positive integers and positive real numbers, respectively. And

$$R = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b \in \mathbb{R}^+, c \in \mathbb{Z}^+\right\},$$
$$I = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b \in \mathbb{R}^+, c \in \mathbb{Z}^+, a < b\right\},$$
$$J = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b \in \mathbb{R}^+, c \in \mathbb{Z}^+, b > 3\right\}.$$

Then R is a hemiring under the usual binary operations of addition and multiplication of matrices, and I is right h-ideal and J is left h-ideal of R. Now the product IJ is an h-bi-ideal of R and it is not an h-quasi-ideal of R. Then by Lemma 3.5, the function χ_{IJ} is an interval valued fuzzy h-bi-ideal of R and it is not interval valued fuzzy h-quasi-ideal of R. □

Theorem 3.11. *Let $\lambda = [\lambda^-, \lambda^+]$ be an interval valued fuzzy subset of a hemiring R. Then λ is an interval valued fuzzy h-ideal (h-bi-ideal, h-quasi-ideal) of R if and only if λ^- and λ^+ are fuzzy h-ideals (h-bi-ideals, h-quasi-ideals) of R.* □

Theorem 3.12. [11] *A hemiring R is h-hemiregular if and only if for any interval valued fuzzy right h-ideal λ and interval valued fuzzy left h-ideal μ of R we have $\lambda \odot \mu = \lambda \wedge \mu$.* □

Theorem 3.13. *For a hemiring R the following conditions are equivalent.*

(i) R is h-hemiregular.

(ii) $\lambda \leqslant \lambda \odot \mathcal{R} \odot \lambda$, for every interval valued fuzzy h-bi-ideal of R.

(iii) $\lambda \leqslant \lambda \odot \mathcal{R} \odot \lambda$, for every interval valued fuzzy h-quasi-ideal of R.

Proof. $(i) \Rightarrow (ii)$ Let λ be an interval valued fuzzy h-bi-ideal of R and $x \in R$. Then there exist $a, a', z \in R$ such that $x + xax + z = xa'x + z$. Then for all expressions $x + \Sigma_{i=1}^{m} a_i b_i + z = \Sigma_{j=1}^{n} a'_j b'_j + z$, we have

$$(\lambda \odot \mathcal{R} \odot \lambda)(x)$$

$$= \sup \left\{ \begin{array}{l} \bigwedge\limits_{i=1}^{m} \left((\lambda \odot \mathcal{R})^-(a_i) \wedge \lambda^-(b_i) \right) \wedge \bigwedge\limits_{j=1}^{n} \left((\lambda \odot \mathcal{R})^-(a'_j) \wedge \lambda^-(b'_j) \right), \\ \bigwedge\limits_{i=1}^{m} \left((\lambda \odot \mathcal{R})^+(a_i) \wedge \lambda^+(b_i) \right) \wedge \bigwedge\limits_{j=1}^{n} \left((\lambda \odot \mathcal{R})^+(a'_j) \wedge \lambda^+(b'_j) \right) \end{array} \right\}$$

$$\geqslant \left\{ \begin{array}{l} (\lambda \odot \mathcal{R})^- (xa) \wedge \lambda^- (x) \wedge (\lambda \odot \mathcal{R})^- (xa') \wedge \lambda^- (x), \\ (\lambda \odot \mathcal{R})^+ (xa) \wedge \lambda^+ (x) \wedge (\lambda \odot \mathcal{R})^+ (xa') \wedge \lambda^+ (x) \end{array} \right\}$$

$$= [(\lambda \odot \mathcal{R})^-(xa), (\lambda \odot \mathcal{R})^+(xa)] \wedge [(\lambda \odot \mathcal{R})^-(xa'), (\lambda \odot \mathcal{R})^+(xa')] \wedge [\lambda^-(x), \lambda^+(x)]$$

$$= (\lambda \odot \mathcal{R})(xa) \wedge (\lambda \odot \mathcal{R})(xa') \wedge \lambda(x)$$

$$= \sup \left\{ \bigwedge_{i=1}^{m} \lambda^-(a_i) \wedge \bigwedge_{j=1}^{n} \lambda^-(a'_j), \bigwedge_{i=1}^{m} \lambda^+(a_i) \wedge \bigwedge_{j=1}^{n} \lambda^+(a'_j) \right\} \wedge$$

$$\sup \left\{ \bigwedge_{i=1}^{m} \lambda^-(c_i) \wedge \bigwedge_{j=1}^{n} \lambda^-(c'_j), \bigwedge_{i=1}^{m} \lambda^+(c_i) \wedge \bigwedge_{j=1}^{n} \lambda^+(c'_j) \right\} \wedge \lambda(x)$$

(for all $xa + \Sigma_{i=1}^{m} a_i b_i + z = \Sigma_{j=1}^{n} a'_j b'_j + z$ and $xa' + \Sigma_{i=1}^{m} c_i d_i + z = \Sigma_{j=1}^{n} c'_j d'_j + z$)

$$\geqslant \left\{ \begin{array}{l} [\lambda^- (xax) \wedge \lambda^- (xa'x), \lambda^+ (xax) \wedge \lambda^+ (xa'x)] \wedge \\ [\lambda^- (xax) \wedge \lambda^- (xa'x), \lambda^+ (xax) \wedge \lambda^+ (xa'x)] \wedge \lambda(x) \end{array} \right\}$$

(because $xa + xaxa + za = xa'xa + za$ and $xa' + xaxa' + za' = xa'xa' + za'$)

$\geqslant [\lambda^- (xax), \lambda^+ (xax)] \wedge [\lambda^- (xa'x), \lambda^+ (xa'x)] \wedge \lambda(x) = \lambda(x)$.

Thus $\lambda \leqslant \lambda \odot \mathcal{R} \odot \lambda$.

$(ii) \Rightarrow (iii)$ is straightforward because each interval valued fuzzy h-quasi-ideal is an interval valued fuzzy h-bi-ideal.

$(iii) \Rightarrow (i)$ Let Q be any h-quasi-ideal of a hemiring R. Then by Lemma 3.5, χ_Q is an interval valued fuzzy h-quasi-ideal of R. Then by Lemma 3.2 and the hypothesis $\chi_Q \subseteq \chi_Q \odot \mathcal{R} \odot \chi_Q = \chi_{\overline{QRQ}}$, which implies $Q \subseteq \overline{QRQ}$. Also, as Q is an h-quasi-ideal, so $\overline{QRQ} \subseteq \overline{RQ} \cap \overline{QR} \subseteq Q$. Hence $\overline{QRQ} = Q$. Thus, by Lemma 2.3, R is h-hemiregular hemiring. □

Theorem 3.14. *For a hemiring R, the following conditions are equivalent.*

- (i) *R is h-hemiregular.*
- (ii) *$\lambda \wedge \mu \leqslant \lambda \odot \mu$ for every interval valued fuzzy h-bi-ideal λ and interval valued fuzzy left h-ideal μ of R.*
- (iii) *$\lambda \wedge \mu \leqslant \lambda \odot \mu$ for every interval valued fuzzy h-quasi-ideal λ and interval valued fuzzy left h-ideal μ of R.*
- (iv) *$\lambda \wedge \mu \leqslant \lambda \odot \mu$for every interval valued fuzzy right h-ideal λ and interval valued fuzzy h-bi-ideal μ of R.*
- (v) *$\lambda \wedge \mu \leqslant \lambda \odot \mu$ for every interval valued fuzzy right h-ideal λ and interval valued fuzzy h-quasi-ideal μ of R.*
- (vi) *$\lambda \wedge \mu \wedge \nu \leqslant \lambda \odot \mu \odot \nu$ for every interval valued fuzzy right h-ideal λ, fuzzy h-bi-ideal μ and interval valued fuzzy left h-ideal ν of R.*
- (vii) *$\lambda \wedge \mu \wedge \nu \leqslant \lambda \odot \mu \odot \nu$ for every interval valued fuzzy right h-ideal λ, interval valued fuzzy h-quasi-ideal μ and interval valued fuzzy left h-ideal ν of R.*

Proof. $(i) \Rightarrow (ii)$ Let λ be any *interval valued* fuzzy h-bi-ideal and μ be any *interval valued* fuzzy left h-ideal of R. Since R is h-hemiregular, so for any $a \in R$ there exist $x_1, x_2, z \in R$ such that $a + ax_1a + z = ax_2a + z$. Thus for all expressions $a + \Sigma_{i=1}^{m} a_i b_i + z = \Sigma_{j=1}^{n} a'_j b'_j + z$, we have

$$(\lambda \odot \mu)(a) = \sup \left\{ \begin{array}{l} \bigwedge_{i=1}^{m} \left(\lambda^-(a_i) \wedge \mu^-(b_i)\right) \wedge \bigwedge_{j=1}^{n} \left(\lambda^-(a'_j) \wedge \mu^-(b'_j)\right), \\ \bigwedge_{i=1}^{m} \left(\lambda^+(a_i) \wedge \mu^+(b_i)\right) \wedge \bigwedge_{j=1}^{n} \left(\lambda^+(a'_j) \wedge \mu^+(b'_j)\right) \end{array} \right\}$$

$$\geqslant [\lambda^-(a), \lambda^+(a)] \wedge [\mu^-(x_1a), \mu^+(x_1a)] \wedge [\mu^-(x_2a), \mu^+(x_2a)]$$

(because $a + ax_1a + z = ax_2a + z$)

$$\geqslant [\lambda^-(a), \lambda^+(a)] \wedge [\mu^-(a), \mu^+(a)] \geqslant \lambda(a) \wedge \mu(a) = (\lambda \wedge \mu)(a).$$

So $\lambda \odot \mu \geqslant \lambda \wedge \mu$.

$(ii) \Rightarrow (iii)$ By Theorem 3.9.

$(iii) \Rightarrow (i)$ Let λ be an interval valued fuzzy right h-ideal and μ be an interval valued fuzzy left h-ideal of R. Since every interval valued fuzzy right h-ideal is interval valued fuzzy h-quasi-ideal, so by (iii) we have $\lambda \odot \mu \geqslant \lambda \wedge \mu$. But $\lambda \odot \mu \leqslant \lambda \wedge \mu$. Hence $\lambda \odot \mu = \lambda \wedge \mu$ for every interval valued fuzzy right h-ideal λ of R, and for every interval valued fuzzy left h-ideal μ of R. Thus by Theorem 3.12, R is h-hemiregular.

Similarly we can prove $(i) \Rightarrow (iv) \Rightarrow (v) \Rightarrow (i)$.

$(i) \Rightarrow (vi)$ Let λ be any interval valued fuzzy right h-ideal, μ be an interval valued fuzzy h-bi-ideal and ν be an interval valued fuzzy left h-ideal of R. Since R is h-hemiregular, so for any $a \in R$ there exist $x_1, x_2, z \in R$ such that $a + ax_1a + z = ax_2a + z$. Then for all expressions $a + \Sigma_{i=1}^{m} a_i b_i + z = \Sigma_{j=1}^{n} a'_j b'_j + z$, we have

$$(\lambda \odot \mu \odot \nu)(a) = \sup \left\{ \begin{array}{l} \bigwedge\limits_{i=1}^{m} \left((\lambda \odot \mu)^-(a_i) \wedge \nu^-(b_i) \right) \wedge \bigwedge\limits_{j=1}^{n} \left((\lambda \odot \mu)^-(a'_j) \wedge \nu^-(b'_j) \right), \\ \bigwedge\limits_{i=1}^{m} \left((\lambda \odot \mu)^+(a_i) \wedge \nu^+(b_i) \right) \wedge \bigwedge\limits_{j=1}^{n} \left((\lambda \odot \mu)^+(a'_j) \wedge \nu^+(b'_j) \right) \end{array} \right\}$$

$$\geqslant [(\lambda \odot \mu)^-(a) \wedge \nu^-(x_1at) \wedge \nu^-(x_2a), (\lambda \odot \mu)^+(a) \wedge \nu^+(x_1a) \wedge \nu^+(x_2a)]$$

$$= [(\lambda \odot \mu)^-(a), (\lambda \odot \mu)^+(a)] \wedge [\nu^-(x_1a), \nu^+(x_1a)] \wedge [\nu^-(x_2a), \nu^+(x_2a)]$$

$$= (\lambda \odot \mu)(a) \wedge \nu(x_1a) \wedge \nu(x_2a)$$

$$\geqslant \sup \left\{ \begin{array}{l} \bigwedge\limits_{i=1}^{m} \left(\lambda^-(a_i) \wedge \mu^-(b_i) \right) \wedge \bigwedge\limits_{j=1}^{n} \left(\lambda^-(a'_j) \wedge \mu^-(b'_j) \right), \\ \bigwedge\limits_{i=1}^{m} \left(\lambda^+(a_i) \wedge \mu^+(b_i) \right) \wedge \bigwedge\limits_{j=1}^{n} \left(\lambda^+(a'_j) \wedge \mu^+(b'_j) \right) \end{array} \right\} \wedge \nu(a)$$

(for all expressions $a + \Sigma_{i=1}^{m} a_i b_i + z = \Sigma_{j=1}^{n} a'_j b'_j + z$)

$$\geqslant [\lambda^-(ax_1) \wedge \lambda^-(ax_2) \wedge \mu^-(a), \lambda^+(ax_1) \wedge \lambda^+(ax_2) \wedge \mu^+(a)] \wedge \nu(a)$$

$$= \lambda(ax_1) \wedge \lambda(ax_2) \wedge \mu(a) \wedge \nu(a) \geqslant \lambda(a) \wedge \mu(a) \wedge \nu(a) = (\lambda \wedge \mu \wedge \nu)(a).$$

Thus $\lambda \wedge \mu \wedge \nu \leqslant \lambda \odot \mu \odot \nu$.

$(vi) \Rightarrow (vii)$ Obvious.

$(vii) \Rightarrow (i)$ Let λ be any interval valued fuzzy right h-ideal, and ν be an interval valued fuzzy left h-ideal of R. Then

$$\lambda \wedge \nu = \lambda \wedge \mathcal{R} \wedge \nu \leqslant \lambda \odot \mathcal{R} \odot \nu \leqslant \lambda \odot \nu.]$$

But $\lambda \odot \nu \leqslant \lambda \wedge \nu$ always holds. Hence $\lambda \odot \nu = \lambda \wedge \nu$ for every interval valued fuzzy right h-ideal λ and for every interval valued fuzzy left h-ideal ν of R. Thus by Theorem 3.12, R is h-hemiregular. □

Theorem 3.15. *A hemiring R is h-hemiregular if and only if*

(*i*) *every interval valued fuzzy right and interval valued fuzzy left h-ideal of R are idempotent,*

(*ii*) *for any interval valued fuzzy right h-ideal λ and for any interval valued fuzzy left h-ideal μ of R, $\lambda \odot \mu$ is an interval valued fuzzy h-quasi-ideal of R.*

Proof. Assume R is h-hemiregular and let λ be an interval valued fuzzy left h-ideal of R. Then $\lambda \odot \lambda \leqslant \mathcal{R} \odot \lambda \leqslant \lambda$.

Also as R is h-hemiregular, so for any $a \in R$ there exist $x_1, x_2, z \in R$ such that $a+ax_1a+z = ax_2a+z$. Then for all expressions $a+\Sigma_{i=1}^{m} a_i b_i+z = \Sigma_{j=1}^{n} a'_j b'_j + z$, we have

$$(\lambda \odot \lambda)(a) = \sup \left\{ \begin{matrix} \bigwedge\limits_{i=1}^{m} \left(\lambda^-(a_i) \wedge \lambda^-(b_i)\right) \wedge \bigwedge\limits_{j=1}^{n} \left(\lambda^-(a'_j) \wedge \lambda^-(b'_j)\right), \\ \bigwedge\limits_{i=1}^{m} \left(\lambda^+(a_i) \wedge \lambda^+(b_i)\right) \wedge \bigwedge\limits_{j=1}^{n} \left(\lambda^+(a'_j) \wedge \lambda^+(b'_j)\right) \end{matrix} \right\}$$

$$\geqslant [\lambda^-(a), \lambda^+(a)] \wedge [\lambda^-(x_1a), \lambda^+(x_1a)] \wedge [\lambda^-(x_2a), \lambda^+(x_2a)]$$

(because $a + ax_1a + z = ax_2a + z$)

$$\geqslant [\lambda^-(a), \lambda^+(a)] \wedge [\lambda^-(a), \lambda^+(a)] \geqslant \lambda(a) \wedge \lambda(a) = \lambda(a),$$

that is, $\lambda \odot \lambda \geqslant \lambda$. Thus $\lambda \odot \lambda = \lambda$.

Similarly we can prove for interval valued fuzzy right h-ideal of R. Hence (i) holds. Now let λ be any interval valued fuzzy right h-ideal and μ be any interval valued fuzzy left h-ideal of R, then by Theorem 3.12, $\lambda \odot \mu = \lambda \wedge \mu$. Then by Theorem 3.8, $\lambda \odot \mu$ is interval valued fuzzy h-quasi-ideal of R. Hence (ii) holds.

Conversely, assume that (i) and (ii) holds. Let I be any right h-ideal of R. Then by Lemma 3.5, χ_I is interval valued fuzzy right h-ideal of R. Now by using Lemma 3.2, and hypothesis $\chi_I = \chi_I \odot \chi_I = \chi_{\overline{I^2}}$, which implies $I = I^2$. So I is an idempotent.

Now let I be any right h-ideal and L be any left h-ideal of R. Then by using Lemma 3.2, and hypothesis $\chi_{\overline{IL}} = \chi_I \odot \chi_L$ is an h-quasi-ideal of R. Thus by Lemma 3.5, $\overline{IL}$ is an h-quasi-ideal of R. Hence by Lemma 2.4, R is h-hemiregular. □

Theorem 3.16. *A hemiring R is h-intra-hemiregular if and only if for any interval valued fuzzy left h-ideal λ and any interval valued fuzzy right h-ideal μ of R, $\lambda \wedge \mu \leqslant \lambda \odot \mu$.*

Proof. Assume that R is an h-intra-hemiregular hemiring, λ is an interval valued fuzzy right h-ideal and μ an interval valued fuzzy left h-ideal of R. Now as R is h-intra-hemiregular, so for any $x \in R$, there exists $a_i, a_i', b_j, b_j', z \in R$ such that $x + \sum_{i=1}^{m} a_i x^2 a_i' + z = \sum_{j=1}^{n} b_j x^2 b_j' + z$. Then for all such expressions

$$(\lambda \odot \mu)(x) = \sup \left\{ \begin{array}{l} \bigwedge\limits_{i=1}^{m} \left(\lambda^-(a_i) \wedge \mu^-(b_i)\right) \wedge \bigwedge\limits_{j=1}^{n} \left(\lambda^-(a_j') \wedge \mu^-(b_j')\right), \\ \bigwedge\limits_{i=1}^{m} \left(\lambda^-(a_i) \wedge \mu^-(b_i)\right) \wedge \bigwedge\limits_{j=1}^{n} \left(\lambda^-(a_j') \wedge \mu^-(b_j')\right) \end{array} \right\}$$

$$\geqslant \left\{ \begin{array}{l} \bigwedge\limits_{i=1}^{m} \left(\lambda^-(a_i x) \wedge \mu^-(x a_i')\right) \wedge \bigwedge\limits_{j=1}^{n} \left(\lambda^-(b_j x) \wedge \mu^-(x b_j')\right), \\ \bigwedge\limits_{i=1}^{m} \left(\lambda^+(a_i x) \wedge \mu^+(x a_i')\right) \wedge \bigwedge\limits_{j=1}^{n} \left(\lambda^+(b_j x) \wedge \mu^+(x b_j')\right) \end{array} \right\}$$

(because $x + \sum_{i=1}^{m} (a_i x)(x a_i') + z = \sum_{j=1}^{n} (b_j x)(x b_j') + z$)

$$\geqslant [(\lambda^-(x)) \wedge \mu^-(x), (\lambda^+(x)) \wedge \mu^+(x)] = (\lambda \wedge \mu)(x),$$

which shows $\lambda \wedge \mu \leqslant \lambda \odot \mu$.

Conversely, let I and J be any left and right h-ideals of R, respectively. Then by Lemma 3.5, the characteristic functions χ_I and χ_J are interval valued fuzzy left h-ideal and interval valued fuzzy right h-ideal of R, respectively. Then by hypothesis and Lemma 3.2, we have

$$\chi_{I \cap J} = \chi_I \wedge \chi_J \subseteq \chi_I \odot \chi_J = \chi_{\overline{IJ}},$$

which implies $I \cap J \subseteq \overline{IJ}$. Lemma 2.6 completes the proof. □

Theorem 3.17. *The following conditions are equivalent for a hemiring R.*

(*i*) *R is both h-hemiregular and h-intra-hemiregular.*

(*ii*) *$\lambda = \lambda \odot \lambda$ for every interval valued fuzzy h-bi-ideal λ of R.*

(*iii*) *$\lambda = \lambda \odot \lambda$ for every interval valued fuzzy h-quasi-ideal λ of R.*

Proof. (*i*) ⇒ (*ii*) Let λ be an interval valued fuzzy h-bi-ideal of R and $x \in R$. Then as R is both h-hemiregular and h-intra-hemiregular, so there exist elements $a_1, a_2, p_i, p_i', q_j, q_j', z \in R$ such that

$x + \sum_{j=1}^{n} (x a_2 q_j x)(x q_j' a_1 x) + \sum_{j=1}^{n} (x a_1 q_j x)(x q_j' a_2 x) + \sum_{i=1}^{m} (x a_1 p_i x)(x p_i' a_1 x)$
$+ \sum_{i=1}^{m} (x a_2 p_i x)(x p_i' a_2 x) + z = \sum_{i=1}^{m} (x a_2 p_i x)(x p_i' a_1 x) + \sum_{i=1}^{m} (x a_1 p_i x)(x p_i' a_2 x)$
$+ \sum_{j=1}^{n} (x a_1 q_j x)(x q_j' a_1 x) + \sum_{j=1}^{n} (x a_2 q_j x)(x q_j' a_2 x) + z$ (see Lemma 5.6 [13]).

Now for all expressions $x + \Sigma_{i=1}^{m} a_i b_i + z = \Sigma_{j=1}^{n} a_j' b_j' + z$, we have

$$(\lambda \odot \lambda)(x) = \sup \left\{ \begin{array}{l} \bigwedge\limits_{i=1}^{m} \left(\lambda^-(a_i) \wedge \lambda^-(b_i)\right) \wedge \bigwedge\limits_{j=1}^{n} \left(\lambda^-(a'_j) \wedge \lambda^-(b'_j\right), \\ \bigwedge\limits_{i=1}^{m} \left(\lambda^+(a_i) \wedge \lambda^+(b_i)\right) \wedge \bigwedge\limits_{j=1}^{n} \left(\lambda^+(a'_j) \wedge \lambda^+(b'_j\right) \end{array} \right\}$$

$$\geqslant \left\{ \begin{array}{l} \bigwedge\limits_{j=1}^{n} \left(\lambda^-(xa_2q_jx) \wedge \lambda^-(xq'_ja_1x) \wedge \lambda^-(xa_1q_jx) \wedge \lambda^-(xq'_ja_2x)\right) \wedge \\ \bigwedge\limits_{i=1}^{m} \left(\lambda^-(xa_1p_ix) \wedge \lambda^-(xp'_ia_1x) \wedge \lambda^-(xa_2p_ix) \wedge \lambda^-(xp'_ia_2x)\right), \\ \bigwedge\limits_{j=1}^{n} \left(\lambda^+(xa_2q_jx) \wedge \lambda^+(xq'_ja_1x) \wedge \lambda^+(xa_1q_jx) \wedge \lambda^+(xq'_ja_2x)\right) \wedge \\ \bigwedge\limits_{i=1}^{m} \left(\lambda^+(xa_1p_ix) \wedge \lambda^+(xp'_ia_1x) \wedge \lambda^+(xa_2p_ix) \wedge \lambda^+(xp'_ia_2x)\right) \end{array} \right\}$$

$\geqslant [\lambda^-(x), \lambda^+(x)] = \lambda(x)$.

But as $\lambda \odot \lambda \leqslant \lambda$, so $\lambda \odot \lambda = \lambda$.

$(ii) \Rightarrow (iii)$ is straightforward by Theorem 3.9.

$(iii) \Rightarrow (i)$ Let Q be an h-quasi-ideal of R. Then by Lemma 3.5, χ_Q is an interval valued fuzzy h-quasi-ideal of R. Thus by hypothesis and Lemma 3.2, we have $\chi_Q = \chi_Q \odot \chi_Q = \chi_{\overline{Q^2}}$. This implies $Q = \overline{Q^2}$. Hence, by Lemma 2.7, R is both h-hemiregular and h-intra-hemiregular. □

Theorem 3.18. *The following conditions are equivalent for a hemiring R.*

- (i) *R is both h-hemiregular and h-intra-hemiregular.*
- (ii) *$\lambda \wedge \mu \leqslant \lambda \odot \mu$ for all interval valued fuzzy h-bi-ideals λ and μ of R.*
- (iii) *$\lambda \wedge g \leqslant \lambda \odot \mu$ for every interval valued fuzzy h-bi-ideal λ and every interval valued fuzzy h-quasi-ideals μ of R.*
- (iv) *$\lambda \wedge g \leqslant \lambda \odot \mu$ for every interval valued fuzzy h-quasi-ideal λ and every interval valued fuzzy h-bi-ideals μ of R.*
- (v) *$\lambda \wedge g \leqslant \lambda \odot \mu$ for all interval valued fuzzy h-quasi-ideals λ and μ of R.*

Proof. $(i) \Rightarrow (ii)$ Similarly as in the previous proof.

$(ii) \Rightarrow (iii) \Rightarrow (v)$ and $(ii) \Rightarrow (iv) \Rightarrow (v)$ are straightforward.

$(v) \Rightarrow (i)$ Let λ be an interval valued fuzzy left h-ideals of R and μ be an interval valued fuzzy right h-ideal of R. Then λ and μ are interval valued fuzzy h-quasi-ideals of R. So by hypothesis $\lambda \wedge \mu \leqslant \lambda \odot \mu$. But $\lambda \wedge \mu \geqslant \lambda \odot \mu$ (see [11]). Thus $\lambda \wedge \mu = \lambda \odot \mu$. Hence by Theorem 3.12, R is h-hemiregular. On the other hand by hypothesis we also have $\lambda \wedge \mu \leqslant \lambda \odot \mu$. So by Theorem 3.16, R is h-intra-hemiregular. □

References

[1] **J. Ahsan**, *Semirings characterized by their fuzzy ideals*, J. Fuzzy Math. **6** (1998), 181 – 192.

[2] **J. Ahsan, K. Saifullah and M. F. Khan**, *Fuzzy semirings*, Fuzzy Sets and Syst. **60** (1993), 309 – 320.

[3] **S. Ghosh**, *Fuzzy k-ideals of semirings*, Fuzzy Sets Syst. **95** (1998), 103 – 108.

[4] **J. S. Golan**, *Semirings and their applications*, Kluwer Acad. Publ. 1999.

[5] **M. Henriksen**, *Ideals in semirings with commutative addition*, Amer. Math. Soc. Notices **6** (1958), 321.

[6] **K. Iizuka**, *On Jacobson radical of a semiring*, Tohoku Math. J. **11** (1959), 409 – 421.

[7] **Y. B. Jun, M. A. Özürk and S. Z. Song**, *On fuzzy h-ideals in hemirings*, Inform. Sci. **162** (2004), 211 – 226.

[8] **D. R. La Torre**, *On h-ideals and k-ideals in hemirings*, Publ. Math. Debrecen **12** (1965), 219 – 226.

[9] **X. Ma and J. Zhan**, *On fuzzy h-ideals of hemirings*, J. Syst. Sci. Complexity **20** (2007), 470 – 478.

[10] **M. Shabir, and T. Mahmood**, *Hemirings characterized by the properties of their fuzzy ideals with thresholds*, Quasigroups and Related Systems **18** (2010), 195 – 212.

[11] **G. Sun, Y. Yin and Y. Li**, *Interval valued fuzzy h-ideals of hemirings*, Int. Math. Forum **5** (2010), 545 – 556.

[12] **H. S. Vandiver**, *Note on a simple type of algebra in which cancellation law of addition does not hold*, Bull. Amer. Math. Soc. **40** (1934), 914 – 920.

[13] **Y. Q. Yin and H. Li**, *The charatecrizations of h-hemiregular hemirings and h-intra-hemiregular hemirings*, Inform. Sci. **178** (2008), 3451 – 3464.

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

[15] **J. Zhan and W. A. Dudek**, *Fuzzy h-ideals of hemirings*, Inform. Sci. **177** (2007), 876 – 886.

Received September 15, 2010
Revised December 8, 2010

M.Shabir
Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
E-mail: mshabirbhatti@yahoo.co.uk

T.Mahmood
Department of Mathematics, Faculty of Basic and Applied Sciences, International Islamic University, Islamabad, Pakistan
E-mail: tahirbakhat@yahoo.com

Quasigroups and Related Systems **19** (2011), 331 – 338

Roughness in ternary semigroups

Muhammad Shabir and Noor Rehman

Abstract. In this paper we introduced the notions of rough left (right, lateral) ideal and rough prime ideals in ternary semigroup, and studied some properties of these ideals.

1. Introduction and preliminaries

The notion of rough set introduced by Z. Pawlak in his pioneering paper [7] and that of ternary semigroup by D. H. Lehmer in 1932 [6]. In this paper, we introduce lower and upper approximations with respect to the congruences on a ternary semigroup.

A *ternary semigroup* is an algebraic structure (S, f) such that S is a non-empty set and $f : S^3 \to S$ is a ternary operation satisfying the following associative law:

$$f(f(a,b,c),d,e) = f(a,f(b,c,d),e) = f(a,b,f(c,d,e)).$$

For simplicity we write $f(a,b,c)$ as abc. A non-empty subset T of a ternary semigroup S is said to be a *ternary subsemigroup* of S if $TTT = T^3 \subseteq T$, that is $abc \in T$ for all $a,b,c \in T$.

By a *left* (*right, lateral* (*middle*)) *ideal* of a ternary semigroup S we mean a non-empty subset A of S such that $SSA \subseteq A$ ($ASS \subseteq A$, $SAS \subseteq A$). By a two sided ideal, we mean a subset of S which is both a left and a right ideal of S. If a non-empty subset of S is a left, right and lateral ideal of S, then it is called an *ideal* of S.

A non-empty subset A of a ternary semigroup S is called a *bi-ideal* of S if $AAA \subseteq A$ and $ASASA \subseteq A$ (cf. [2]).

For an equivalence relation ρ on S and a subset A of S we define two subsets

$$\rho_{-}(A) = \{x \in S : [x]_\rho \subseteq A\}, \qquad \rho^{-}(A) = \{x \in S : [x]_\rho \cap A \neq \emptyset\}$$

called *ρ-lower* and *ρ-upper approximations* of A, respectively.

2010 Mathematics Subject Classification: 20N10
Keywords: Ternary semigroup, rough left ideal, rough prime ideal.

Theorem 1.1. *Let ρ and λ be equivalence relations on a certain set S. If A and B are non-empty subsets of S, then*

(1) $\rho_{-}(A) \subseteq A \subseteq \rho^{-}(A)$,
(2) $\rho^{-}(A \cup B) = \rho^{-}(A) \cup \rho^{-}(B)$,
(3) $\rho_{-}(A \cap B) = \rho_{-}(A) \cap \rho_{-}(B)$,
(4) $A \subseteq B$ *implies* $\rho_{-}(A) \subseteq \rho_{-}(B)$,
(5) $A \subseteq B$ *implies* $\rho^{-}(A) \subseteq \rho^{-}(B)$,
(6) $\rho_{-}(A) \cup \rho_{-}(B) \subseteq \rho_{-}(A \cup B)$,
(7) $\rho^{-}(A \cap B) \subseteq \rho^{-}(A) \cap \rho^{-}(B)$,
(8) $\rho \subseteq \lambda$ *implies* $\rho_{-}(A) \supseteq \lambda_{-}(A)$,
(9) $\rho \subseteq \lambda$ *implies* $\rho^{-}(A) \subseteq \lambda^{-}(A)$.

The proof is analogous to the proof presented in [7].

2. Rough ideals in a ternary semigroup

Definition 2.1. A congruence ρ on a ternary semigroup S is called *stable* or *compatible* with the operation if $[a]_{\rho}[b]_{\rho}[c]_{\rho} = [abc]_{\rho}$for all $a, b, c \in S$.

The following example shows that there are congruences which are not stable.

Example 2.2. Let $S = \{a, b, c, d, e\}$ be a semigroup with respect to $*$ and $xyz = (x * y) * z$ for all $x, y, z \in S$. Where $*$ is defined by the table:

$*$	a	b	c	d	e
a	b	b	d	d	d
b	b	b	d	d	d
c	d	d	c	d	c
d	d	d	d	d	d
e	d	d	c	d	c

Then S is a ternary semigroup. Let ρ be a congruence on S such that the $\rho-$congruence classes are the subsets $\{a, b\}, \{c, d\}, \{e\}$.

Then clearly ρ is not stable, since $[a]_{\rho}[c]_{\rho}[a]_{\rho} \neq [aca]_{\rho}$.

Definition 2.3. Let ρ be a congruence on a ternary semigroup S. Then a non-empty subset A of S is called an upper (resp. lower) rough ternary subsemigroup of S if $\rho^{-}(A)$ (resp. $\rho_{-}(A)$) is a ternary subsemigroup of S. A is called an *upper* (resp. *lower*) *rough left* (*right, lateral, two sided*) *ideal* of S if $\rho^{-}(A)$ (resp. $\rho_{-}(A)$) is a left (right, lateral, two sided) ideal of S.

Lemma 2.4. *Let ρ be a congruence relation on a ternary semigroup S. If A, B and C are non-empty subsets of S, then $\bar{\rho}(A)\bar{\rho}(B)\bar{\rho}(C) \subseteq \bar{\rho}(ABC)$.*

Proof. If $d \in \bar{\rho}(t)\bar{\rho}(B)\bar{\rho}(C)$, then $d = abc$ for some $a \in \bar{\rho}(A)$, $b \in \bar{\rho}(B)$, $c \in \bar{\rho}(C)$. Thus there exist elements $x, y, z \in S$ such that $x \in [a]_\rho \cap A$, $y \in [b]_\rho \cap B$, $z \in [c]_\rho \cap C$. This implies that $x \in [a]_\rho$, $y \in [b]_\rho$, $z \in [c]_\rho$ and $x \in A$, $y \in B$, $z \in C$.

Since ρ is a congruence on S, so $xyz \in [abc]_\rho$. Also $xyz \in ABC$. Thus we have $xyz \in [abc]_\rho \cap ABC$. This implies that $abc \in \bar{\rho}(ABC)$. □

The following example shows that the equality in Lemma 2.4 does not hold in general.

Example 2.5. Consider the ternary semigroup S and congruence relation ρ as given in Example 2.2. Let $A = \{a, b\}$, $B = \{b, c\}$, $C = \{d\}$. Then $\bar{\rho}(A) = \{a, b\}$, $\bar{\rho}(B) = \{a, b, c, d\}$, $\bar{\rho}(C) = \{c, d\}$. Thus $\bar{\rho}(A)\bar{\rho}(B)\bar{\rho}(C) = \{d\}$ and $\bar{\rho}(ABC) = \{x \in S : [x]_\rho \cap (ABC) = \{c, d\}$. Therefore, $\bar{\rho}(ABC) \nsubseteq \bar{\rho}(A)\bar{\rho}(B)\bar{\rho}(C)$. □

Lemma 2.6. *Let ρ be a stable congruence on a ternary semigroup S. If A, B, C are non-empty subsets of S, then $\rho_-(A)\,\rho_-(B)\,\rho_-(C) \subseteq \rho_-(ABC)$.*

Proof. The proof is similar to the proof of Lemma 2.4. □

The following example shows that if ρ is not a stable congruence, then Lemma 2.6 does not hold.

Example 2.7. Consider the ternary semigroup S and congruence relation ρ from Example 2.2. For $A = \{a, b\}$, $B = \{c, d\}$, $C = \{e\}$ we have $\rho_-(A) = \{a, b\}$, $\rho_-(B) = \{c, d\}$, $\rho_-(C) = \{e\}$, $\rho_-(A)\,\rho_-(B)\,\rho_-(C) = \{d\}$ and $\rho_-(ABC) = \rho_-(\{d\}) = \emptyset$. So, $\rho_-(A)\,\rho_-(B)\,\rho_-(C) \nsubseteq \rho_-(ABC)$. □

Theorem 2.8. *Let ρ be a congruence on a ternary semigroup S.*

(1) *If A is a ternary subsemigroup of S, then A is an upper rough ternary subsemigroup of S.*

(2) *If A is left (right, lateral, two sided) ideal of S, then A is an upper rough left (right, lateral, two sided) ideal of S.*

Proof. (1) Let A be a ternary subsemigroup of S. Then $A \subseteq \bar{\rho}(A)$ and $\bar{\rho}(A)\,\bar{\rho}(A)\,\bar{\rho}(A) \subseteq \bar{\rho}(AAA) \subseteq \bar{\rho}(A)$, by Lemma 2.4.

(2) Analogously as (1). □

The following examples show that $\rho^{-}(A)$ is a ternary subsemigroup (ideal) of S even if A is not a ternary subsemigroup (ideal) of S.

Example 2.9. Let $S = \{-i, 0, i\}$ be a ternary semigroup. Let ρ be a congruence on S such that the ρ-congruence classes are the subsets $\{-i, i\}, \{0\}$. Then $A = \{i\}$ is not a ternary subsemigroup of S, but $\rho^{-}(A) = \{i, -i\}$ is a ternary subsemigroup. Moreover, $B = \{0, i\}$ is not a left ideal of S, but $\rho^{-}(B) = \{-i, 0, i\}$ is a left ideal. □

Theorem 2.10. *Let ρ be a stable congruence on a ternary semigroup S and let $A \subset S$ be such that $\rho_{-}(A)$ is non-empty.*

(1) *If A is a ternary subsemigroup of S, then $\rho_{-}(A)$ also is a ternary subsemigroup of S.*

(2) *If A is a left (right, lateral, two sided) ideal of S, then $\rho_{-}(A)$ also is a left (right, lateral, two sided) ideal of S.* □

The following example shows that if ρ is a stable congruence on a ternary semigroup S, then $\rho_{-}(A)$ is a ternary subsemigroup of S even if A is not a ternary subsemigroup of S.

Example 2.11. Let $S = \{-i, 0, i\}$ and ρ be as in the previous example. Then $A = \{0, i\}$ is not a ternary subsemigroup of S but $\rho_{-}(A) = \{0\}$ is a ternary subsemigroup of S. □

Definition 2.12. A non-empty subset A of a ternary semigroup S is called a *$\rho-$upper (resp. $\rho-$lower) rough bi-ideal* of S, if $\rho^{-}(A)$ (resp. $\rho_{-}(A)$ is a bi-ideal of S.

Theorem 2.13. *Let ρ be a congruence relation on a ternary semigroup S. If A is a bi-ideal of S, then it is $\rho-$upper rough bi-ideal of S.*

Proof. The proof is similar to the proof of Theorem 2.8. □

Example 2.14. Let S be as in Example 2.2 and let ρ be a congruence relation on S such the $\rho-$congruence classes are the subsets $\{a, b, d\}$,$\{c, e\}$. Then $A = \{a, b\}$ is not a bi-ideal of S but $\rho^{-}(A) = \{a, b, d\}$ is a bi-ideal. □

Theorem 2.15. *Let ρ be a stable congruence on a ternary semigroup S and A a bi-ideal of S. Then $\rho_{-}(A)$ is a bi-ideal of S if it is non-empty.*

Proof. The proof is similar to the proof of Theorem 2.8. □

Theorem 2.16. *Let ρ be a congruence on a ternary semigroup S. If A, B and C are right, lateral and left ideal of S, respectively, then*

(1) $\rho^{-}(ABC) \subseteq \rho^{-}(A) \cap \rho^{-}(B) \cap \rho^{-}(C)$,

(2) $\rho_{-}(ABC) \subseteq \rho_{-}(A) \cap \rho_{-}(B) \cap \rho_{-}(C)$. □

3. Rough prime ideals in ternary semigroups

Definition 3.1. A left (right, lateral) bi-ideal A of a ternary semigroup S is a *prime* left (right, lateral) bi-ideal of S if $xyz \in A$ implies $x \in A$ or $y \in A$ or $z \in A$ for all $x, y, z \in S$.

Theorem 3.2. *Let ρ be a stable congruence on a ternary semigroup S and A a prime ideal of S. Then $\rho_{-}(A) \neq \emptyset$ is a prime ideal of S.*

Proof. Suppose A is a prime ideal of S. Then $\rho_{-}(A)$ is an ideal of S.

Suppose that $\rho_{-}(A)$ is not a prime ideal of S. Then there exist elements $x, y, z \in S$ such that $xyz \in \rho_{-}(A)$ but $x \notin \rho_{-}(A)$, $y \notin \rho_{-}(A)$, and $z \notin \rho_{-}(A)$. Then $[x]_{\rho} \nsubseteq A$, $[y]_{\rho} \nsubseteq A$, $[z]_{\rho} \nsubseteq A$. Thus there exist $x' \in [x]_{\rho}$ but $x' \notin A$, $y' \in [y]_{\rho}$ but $y' \notin A$, $z' \in [z]_{\rho}$ but $z' \notin A$. This implies that $x'y'z' \in [x]_{\rho}[y]_{\rho}[z]_{\rho} \subseteq A$. Since A is a prime ideal of S, we have $x' \in A$ or $y' \in A$ or $z' \in A$. A contradiction. Hence $\rho_{-}(A)$ is a prime ideal of S. □

Theorem 3.3. *Let ρ be a stable congruence on a ternary semigroup S. If A is a prime ideal of S, then A is an upper rough prime ideal of S.*

Proof. Suppose A is a prime ideal of S. Then $\rho^{-}(A)$ is an ideal of S. Let $xyz \in \rho^{-}(A)$ for $x, y, z \in S$. Then $[xyz]_{\rho} \cap A = [x]_{\rho}[y]_{\rho}[z]_{\rho} \cap A \neq \emptyset$. Thus there exist $x' \in [x]_{\rho}$, $y' \in [y]_{\rho}$, $z' \in [z]_{\rho}$ such that $x'y'z' \in A$. Since A is a prime ideal of S, so $x' \in A$ or $y' \in A$ or $z' \in A$. This implies that $[x]_{\rho} \cap A \neq \emptyset$ or $[y]_{\rho} \cap A \neq \emptyset$ or $[z]_{\rho} \cap A \neq \emptyset$ and so $x \in \rho^{-}(A)$ or $y \in \rho^{-}(A)$ or $z \in \rho^{-}(A)$. Thus $\rho^{-}(A)$ is a prime ideal of S. Hence A is an upper rough prime ideal of S. □

Theorem 3.4. *Let ρ be a stable congruence on a ternary semigroup S.*

(1) *If A a prime left (right, lateral) ideal of S, then $\rho_{-}(A) (\neq \emptyset)$ and $\rho^{-}(A)$ are prime left (right, lateral) ideal of S.*

(2) *If A is a prime bi-ideal of S, then it is $\rho-$upper and $\rho-$lower rough prime bi-ideal of S.*

Proof. Proof is similar to the proofs of Theorem 3.2 and Theorem 3.3. □

4. Rough sets and idempotent congruences

A congruence relation ρ on a ternary semigroup S is called an *idempotent congruence* if the quotient ternary semigroup S/ρ is an idempotent ternary semigroup.

Definition 4.1. A subset P of a ternary semigroup S is called *semiprime* if $a^3 \in P$ implies $a \in P$ for all $a \in S$.

Theorem 4.2. *Let ρ be an idempotent stable congruence on a ternary semigroup S. If A is non-empty subset of S, then $\rho^-(A)$ is semiprime.*

Proof. Let $a^3 \in \rho^-(A)$, since ρ is idempotent congruence so $[a]_\rho \cap A = [a]_\rho [a]_\rho [a]_\rho \cap A = \left[a^3\right]_\rho \cap A \neq \emptyset$. Therefore $a \in \rho^-(A)$. So $\rho^-(A)$ is semiprime. □

Theorem 4.3. *Let ρ be an idempotent congruence on a ternary semigroup S. If A, B and C are non-empty subsets of S, then*

(1) $\rho^-(A) \cap \rho^-(B) \cap \rho^-(C) \subseteq \rho^-(ABC)$,

(2) $\rho_-(A) \cap \rho_-(B) \cap \rho_-(C) \subseteq \rho_-(ABC)$.

Proof. (1) Let $d \in \rho^-(A) \cap \rho^-(B) \cap \rho^-(C)$. Then $d \in \rho^-(A)$, $d \in \rho^-(B)$ and $d \in \rho^-(C)$. Then there exist $a, b, c \in S$ such that $a \in [d]_\rho$, $a \in A$, $b \in [d]_\rho$, $b \in B$, $c \in [d]_\rho$, $c \in C$. Since ρ is idempotent, so $abc \in [d]_\rho [d]_\rho [d]_\rho = [d]_\rho$ and since $abc \in ABC$. Therefore $abc \in [d]_\rho \cap ABC$. Thus $d \in \rho^-(ABC)$.

The proof of (2) is similar. □

Theorem 4.4. *Let ρ be an idempotent congruence on a ternary semigroup S. If A, B, C are right, lateral and left ideals of S, respectively, then*

(1) $\rho^-(A) \cap \rho^-(B) \cap \rho^-(C) = \rho^-(ABC)$,

(2) $\rho_-(A) \cap \rho_-(B) \cap \rho_-(C) = \rho_-(ABC)$.

Proof. Follows from Theorem 2.16 and Theorem 4.3. □

5. Rough ideals in a quotient ternary semigroup

Let ρ be a congruence relation on a ternary semigroup S. The lower and upper approximations can be presented as

$$\underline{\rho}(A) = \left\{[x]_\rho \in S/\rho\colon\ [x]_\rho \subseteq A\right\}, \qquad \overline{\rho}(A) = \left\{[x]_\rho \in S/\rho\colon\ [x]_\rho \cap A \neq \emptyset\right\}.$$

Theorem 5.1. *Let ρ be a congruence relation on a ternary semigroup S. If A is a ternary subsemigroup of S, then $\overline{\rho}(A)$ and $\underline{\rho}(A)$ are ternary subsemigroups of S/ρ.*

Proof. Let A be a ternary subsemigroup. Then $\emptyset \neq A \subseteq \overline{\rho}(A)$. For every $[x]_\rho, [y]_\rho, [z]_\rho \in \overline{\rho}(A)$ we have $[x]_\rho \cap A \neq \emptyset$, $[y]_\rho \cap A \neq \emptyset$, $[z]_\rho \cap A \neq \emptyset$. So, there are $a, b, c \in S$ such that $a \in [x]_\rho \cap A$, $b \in [y]_\rho \cap A$, $c \in [z]_\rho \cap A$. Thus $(a, x) \in \rho$, $(b, y) \in \rho$ $(c, z) \in \rho$. As ρ is a congruence on S, we have $(abc, xyz) \in \rho$, this implies that $abc \in [xyz]_\rho$. Then $abc \in [xyz]_\rho \cap A$, so $[xyz]_\rho \in \overline{\rho}(A)$. Hence $\overline{\rho}(A)$ is a ternary subsemigroup of S/ρ.

For $\underline{\rho}(A)$ the proof is similar. □

Theorem 5.2. *Let ρ be a congruence relation on a ternary semigroup S. If A is a left (right, lateral, two sided) ideal of S, then $\overline{\rho}(A)$ is a left (right, lateral, two sided) ideal of S/ρ. Also $\underline{\rho}(A)$ is a left (right, lateral, two sided) ideal of S/ρ, if it is non-empty.*

Proof. Let A be a left ideal of S. Let $[x]_\rho \in \overline{\rho}(A)$, $[y]_\rho$, $[z]_\rho \in S/\rho$, then $[x]_\rho \cap A \neq \emptyset$. Thus there exists $a \in [x]_\rho \cap A$. As A is a left ideal of S, so $zya \in A$. Since $zya \in [z]_\rho [y]_\rho [x]_\rho$, we have $zya \in [z]_\rho [y]_\rho [x]_\rho \cap A$. But $[z]_\rho [y]_\rho [x]_\rho \subseteq [zyx]_\rho$, so $[zyx]_\rho \subseteq \overline{\rho}(A)$. Thus $\overline{\rho}(A)$ is a left ideal of S/ρ.

For $\underline{\rho}(A)$ the proof is analogous. □

Theorem 5.3. *Let ρ be a congruence relation on a ternary semigroup S. If A is a bi-ideal of S, then $\overline{\rho}(A)$ is a bi-ideal of S/ρ. Also $\underline{\rho}(A)$ is a bi-ideal of S/ρ, if it is non-empty.*

Proof. Let A be a bi-ideal of S, so $\overline{\rho}(A)$ is a ternary subsemigroup of S. Let $[x]_\rho, [y]_\rho, [z]_\rho \in \overline{\rho}(A)$ and $[u]_\rho, [v]_\rho \in S/\rho$. Then there exist $a, b, c \in S$ such that $a \in [x]_\rho \cap A$, $b \in [y]_\rho \cap A$, $c \in [z]_\rho \cap A$. Let $u_1 \in [u]_\rho$, $v_1 \in [v]_\rho$. Since A is bi-ideal so $au_1bv_1c \in A$. Now, as $a\rho x$, $u_1\rho u$, $b\rho y$, $v_1\rho v$, $c\rho z$, we have $(au_1bv_1c)\,\rho\,(xuyvz)$. This implies that $au_1bv_1c \in [xuyvz]_\rho$. Thus $[xuyvz]_\rho \cap A \neq \emptyset$. Hence $[xuyvz]_\rho \in \overline{\rho}(A)$. Thus $\overline{\rho}(A)$ is a bi-ideal of S/ρ.

For $\underline{\rho}(A)$ the proof is analogous. □

References

[1] **Z. Bonikowski**, *Algebraic structures of rough sets*, in: W. P Ziarko (Ed.) Rough Sets, Fuzzy Sets and Knowledge Discovery, Springer-Verlag, Berlin, (1995), 242 – 257.

[2] **V. N. Dixit and S. Dewan**, *A note on quasi and bi-ideals in ternary semigroups*, Int. J. Math. Sci. **18** (1995), 501 – 508.

[3] **W. A. Dudek, I. Groździńska**,*On ideals in n−semigroups*, Mat. Bilten (Skopje) **3-4** (1980), 35 – 44.

[4] **T. Iwinski**, *Algebraic approach to rough sets*, Bull Polish Acad. Sci. Math. **36** (1987), 673 – 683.

[5] **S. Kar and B. K. Maity**, *Congruences on ternary semigroups*, J. Chugcheong Math. Soc. **20** (2007), 191 – 200.

[6] **D. H. Lehmer**, **A ternary analogue of abelian groups**, Amer. J. Math. **59** (1932), 329 – 338.

[7] **Z. Pawlak**, *Rough sets*, Int. J. Comp. Sci. **11** (1982), 341 – 356.

[8] **M. Shabir and M. Bano**, *Prime bi-ideals in ternary semigroups*, Quasigroups and Related Systems **16** (2008), 239 – 256.

[9] **F. M. Sioson**, *Ideal theory in ternary semigroups*, Math. Japonica **10** (1965), 63 – 84.

[10] **F. M. Sioson**, *Ideals in* $(m+1)-$*semigroups*, Ann. Math. Pura Appl. **68** (1965), 161 – 200.

Received December 27, 2010
Revised February 8, 2011

Department of Mathematics, Quaid i Azam University, Islamabad, Pakistan.
E-mails: mshabirbhatti@yahoo.co.uk (M.Shabir), noorrehman82@yahoo.com (N.Rehman)

Quasigroups and Related Systems **19** (2011), 339 – 348

Orthodox ternary semigroups

Sheeja G. and Sri Bala S.[*]

Abstract. Using the notion of idempotent pairs we define orthodox ternary semigroups and generalize various properties of binary orthodox semigroups to the case of ternary semigroups. Also right strongly regular ternary semigroups are characterized.

1. Introduction

The study of algebras with one n-ary operation was initiated in 1904 by Kasner (see [4]). An n-ary analog of groups was studied by Dörnte [2], Post [7] and many others. A special case of such algebras are *ternary semigroups*, i.e., algebras with one *ternary operation* $T\times T\times T \longrightarrow T : (x, y, z) \longrightarrow [xyz]$ satisfying the associative law

$$[xy[uvw]] = [x[yuv]w] = [[xyu]vw].$$

Ternary semigroups have been studied by many authors (see for example [6, 5, 11]). The study of ideals and radicals in ternary semigroups was initiated in [11]. Ternary groups are studied in [1] and [5]. The concept of regular ternary semigroups was introduced in [10]. In [3] regular ternary semigroups was characterized by ideals. Santiago and Sri Bala [9] have investigated regular ternary semigroups.

In this paper we generalize the concept of orthodox semigroups to ternary case and characterize such ternary semigroups.

2. Preliminaries

For simplicity a ternary semigroup $(T, [\ ])$ will be denoted by T and the symbol of an inner ternary operation $[\ ]$ will be deleted, i.e., instead of $[[xyz]uw]$ or $[x[yzu]w]$ we will write $[xyzuw]$.

[*]According to the authors request we write their names in the form used in India.

2010 Mathematics Subject Classification: 20N10

Keywords: Regular, idempotent pair, strongly regular, orthodox ternary semigroup.

The second author is supported by University Grants Commission, India.

An element x of a ternary semigroup T is called *regular* if there exists $y \in T$ such that $[xyx] = x$. A ternary semigroup in which each element is regular is called *regular*. An element $x \in T$ is *inverse* to $y \in T$ if $[xyx] = x$ and $[yxy] = y$. Clearly, if x is inverse to y, then y is inverse to x. Thus every regular element has an inverse. The set of all inverses of x in T is denoted by $I(x)$.

Definition 2.1. A pair (a, b) of elements of T is an *idempotent pair* if $[ab[abt]] = [abt]$ and $[[tab]ab] = [tab]$ for all $t \in T$. An idempotent pair (a, b) in which an element a is inverse to b is called a *natural idempotent pair*.

Recall that according to Post [7] two pairs (a, b) and (c, d) are *equivalent* if $[abt] = [cdt]$ and $[tab] = [tcd]$ for all $t \in T$. Equivalent pairs are denoted by $(a, b) \sim (c, d)$. If (a, b) is an idempotent pair, then $([aba], [bab])$ is a natural idempotent pair and $(a, b) \sim ([aba], [bab])$. The equivalence class containing (a, b) will be denoted by $\langle a, b\rangle$. By E_T we denote the set of all equivalence classes of idempotent pairs in T.

Definition 2.2. Two idempotent pairs (a, b) and (c, d) *commute* if $[abcdt] = [cdabt]$ and $[tabcd] = [tcdab]$ for all $t \in T$. A ternary semigroup in which any two idempotent pairs commute is called *strongly regular*.

Proposition 2.3. *In a strongly regular ternary semigroup every element has a unique inverse.*

Proof. Indeed, if x_1 and x_2 are two inverses of x, then $x_1 = [x_1xx_1] = [x_1xx_2xx_1] = [x_1xx_1xx_2] = [x_1xx_2] = [x_1xx_2xx_2] = [x_2xx_1xx_2] = [x_2xx_2] = x_2$ which completes the proof. □

The unique inverse of an element a is denoted by a^{-1}. In the case of ternary groups it coincides with the skew element (see [1] or [2]).

Definition 2.4. A non-empty subset A of a ternary semigroup T is said to be its *left ideal* if $[TTA] \subseteq A$, and a *right ideal* if $[ATT] \subseteq A$. The *left ideal generated by* A has the form $A_l = A \cup [TTA]$, the *right ideal generated by* A has the form $A_r = A \cup [ATT]$.

Definition 2.5. We say that a left (resp. right) ideal L (resp.R) of a ternary semigroup T has an *idempotent representation* if there exists an idempotent pair (a, b) in T such that $L = [Tab]$ (resp.$R = [abT]$). This representation is called *unique* if all idempotent pairs representing L (resp.R) are equivalent.

The following two facts are proved in [8] (see also [9]).

Lemma 2.6. *An element $a \in T$ is regular if and only if the principal left (resp. right) ideal of T generated by a has an idempotent representation.* □

Proposition 2.7. *In a strongly regular ternary semigroup every principal left (resp. right) ideal has a unique idempotent representation.* □

For $a, b \in T$, let $\mathrm{L}_{a,b}, \mathrm{R}_{a,b}$ denote the maps $\mathrm{L}_{a,b} : T \longrightarrow T : x \longrightarrow [abx]$ and $\mathrm{R}_{a,b} : x \longrightarrow [xab]$, $\forall x \in T$. On the set

$$M = \{m(a,b) \,|\, m(a,b) = (\mathrm{L}_{a,b}, \mathrm{R}_{a,b}), a, b \in T\}$$

we introduce a binary product by putting

$$m(a,b)m(c,d) = m([abc], d) = m(a, [bcd]).$$

Then M is a semigroup. This semigroup can be extended to the semigroup $S_T = T \cup M$ as follows. For $A, B \in S_T$ we define

$$AB = \begin{cases} m(a,b) & \text{if} \quad A = a,\ B = b \in T, \\ [abx] & \text{if} \quad A = m(a,b) \in S_T,\ B = x \in T, \\ [xab] & \text{if} \quad A = x \in T,\ B = m(a,b) \in S_T, \\ m([abc], d) & \text{if} \quad A = m(a,b),\ B = m(c,d) \in S_T. \end{cases}$$

The semigroup S_T is a covering semigroup in the sense of Post [7] (see also [1]). The product $[abc]$ in T is equal to (abc) in S_T. The element $m(a,b)$ in S_T is usually denoted by ab. This is called the *standard embedding of the ternary semigroup T* into S_T.

It is shown in [9] that T is a regular (strongly regular) ternary semigroup if and only if S_T is a regular (inverse) semigroup. There is a bijective correspondence between E_T and the set E_{S_T} of idempotents of S_T.

3. Orthodox ternary semigroups

Definition 3.1. An *orthodox ternary semigroup T* is a regular ternary semigroup in which for any two idempotents pairs (a,b) and (c,d) the pair $([abc], d)$ is also an idempotent pair.

For $a, b \in T$ denote by $W(a,b)$ the set of all equivalence classes $\langle u, v\rangle$ such that $(u,v) \in T \times T$ and $[abuvabt] = [abt]$, $[tabuvab] = [tab]$, $[uvabuvt] = [uvt]$, $[tuvabuv] = [tuv]$.

Clearly, $\langle u, v\rangle \in W(a, b)$ if and only if $\langle a, b\rangle \in W(u, v)$. If (a, b) is an idempotent pair, then $\langle a, b\rangle \in W(a, b)$. Moreover, $\langle u, v\rangle \in W(a, b)$ implies $\langle a, b\rangle \in W(u, v)$, but $\langle u, v\rangle \in W(a, b)$ may not imply $W(a, b) = W(u, v)$, in general (see Lemma 4.5).

In the sequel let T denote an orthodox ternary semigroup, unless otherwise specified.

Lemma 3.2. $\{\langle b', a'\rangle \mid a' \in I(a), b' \in I(b)\} \subseteq W(a, b)$ *for any* $a, b \in T$.

Proof. $[abb'a'abt] = [[aa'a]bb'a'abb'bt] = [a[a'abb'a'abb'b]t] = [aa'abb'bt] = [abt]$. Similarly can be proved other equalities. □

Lemma 3.3. *For any* $a, b \in T$, *if* $\langle x, y\rangle \in W(a, b)$, *then* $([abx], y)$ *and* $([xya], b)$ *are idempotent pairs.*

Proof. If $\langle x, y\rangle \in W(a, b)$, then $[abxyabxyt] = [ab[xyabxyt]] = [abxyt]$ for all $t \in T$. Also, $[tabxyabxy] = [tabxy]$. Therefore $([abx], y)$ is an idempotent pair. Similarly $([xya], b)$ is an idempotent pair. □

Corollary 3.4. *If* $a' \in I(a), b' \in I(b)$ *for some* $a, b \in T$, *then* $([abb'], a')$ *and* $([b'a'a], b)$ *are idempotent pairs.* □

Lemma 3.5. $[I(c)I(b)I(a)] \subset I([abc])$, *for all* $a, b, c \in T$.

Proof. By Corollary 3.4 $([b'a'a], b)$ is an idempotent pair. Since T is orthodox $([[b'a'a]bc], c')$ is an idempotent pair. Using Lemma 3.2 we obtain $[abc] = [abb'a'abc]$. Thus $[[abc][c'b'a'][abc]] = [[abb'a'abc][c'b'a'ab][cc'c]] = [ab[b'a'abcc'b'a'abcc'c]] = [[abb'a'abc]c'c] = [abc]$. Similarly $[c'b'a'abcc'b'a'] = [c'b'a']$. □

Theorem 3.6. *For a regular ternary semigroup* T *the following statements are equivalent.*

(1) T *is orthodox;*
(2) *For any* a, b, c, d *in* T, *if* $\langle x, y\rangle \in W(a, b)$ *and* $\langle u, v\rangle \in W(c, d)$, *then* $(\langle [uvx], y\rangle \in W([abc], d)$*;*
(3) *If* (a, b) *is an idempotent pair and* $\langle x, y\rangle \in W(a, b)$, *then* (x, y) *is an idempotent pair.*

Proof. (1) $\Rightarrow$ (2): Let $\langle x, y\rangle \in W(a, b)$ and $\langle u, v\rangle \in W(c, d)$. Then by Lemma 3.3 $([xya], b)$ and $([cdu], v)$ are idempotent pairs. So, $([xyabc], [duv])$ and $([cduvx], [yab])$ are idempotent pairs. Hence for all $t \in T$ we obtain $[abcduvxyabcdt] = [abxyabcduvxyabcduvcdt] = [ab[xyabcduvxyabcduvc]dt]$

$= [abxyabcduvcdt] = [abcdt]$. Analogously $[tabcduvxyabcd] = [tabcd]$ and $[uvxyabcduvxyt] = [uvxyt]$, $[tuvxyabcduvxy] = [tuvxy]$ for all $t \in T$. Hence $\langle [uvx], y\rangle \in W([abc], d)$.

(2) $\Rightarrow$ (3): Let (a, b) be an idempotent pair and let $\langle x, y\rangle \in W(a, b)$. By Lemma 3.3 $([xya], b)$ and $([abx], y)$ are idempotent pairs. Consequently $\langle [xya], b\rangle \in W([xya], b)$ and $\langle [abx], y\rangle \in W([abx], y)$. Then by hypothesis,

$$\langle [[abx]y[xya]], b\rangle \in W([[xya]b[abx]], y) = W([xyabx], y). \tag{1}$$

Since $\langle x, y\rangle \in W(a, b)$ we see that for all $t \in T$ $[xyt] = [xyabxyt] = [xyabxyabxyxyabxyabxyt] = [xyabxyxyabxyt] = [xyxyabxyt] = [xyxyt]$ because $([abx], y)$ is an idempotent pair. Similarly, $[txy] = [txyabxy] = [txyabxyabxyxyabxyabxy] = [txyabxyxyabxyabxy] = [txyxyabxyabxy] = [txyxyabxy] = [txyxy]$ and so (x, y) is an idempotent pair.

(3) $\Rightarrow$ (1): Let (a, b) and (c, d) be two idempotent pairs. Then for $\langle x, y\rangle \in W([abc], d)$ we have $[cdxyabcdxyabt] = [cd[xyabcdxya]bt] = [cdxyabt]$ and $[tcdxyabcdxyab] = [tcdxyab]$ for all $t \in T$. Thus $([cdx], [yab])$ is an idempotent pair. Next $[abcdcdxyababcdt] = [abcdxyabcdt] = [abcdt]$ and $[tabcdcdxyababcd] = [tabcdxyabcd] = [tabcd]$ for all $t \in T$. Also $[cdxyababcdcdxyabt] = [cdxyabcdxyabt] = [cdxyabt]$ and $[tcdxyababcdcdxyab] = [tcdxyabcdxyab] = [tcdxyab]$ for all $t \in T$. This means that $\langle [abc], d\rangle$ belongs to $W([cdx], [yab])$. Hence by our hypothesis $([abc], d)$ is an idempotent pair which proves that T is orthodox. □

Proposition 3.7. *Let (x, y) be an idempotent pair in T. Then $([a'xy], a)$ and $(a, [xya'])$ are idempotent pairs for all $a \in T$ and $a' \in I(a)$.*

Proof. Since T is orthodox $([aa'x], y)$ is an idempotent pair, so $[a'xyaa'xyat] = [[a'aa']xyaa'xyat] = [a'[aa'xyaa'xya]t] = [a'aa'xyat] = [a'xyat]$ $\forall t \in T$. Also $[ta'xyaa'xya] = [ta'xya]$ for all $t \in T$. Thus $([a'xy], a)$ is an idempotent pair. Similarly $(a, [xya'])$ is an idempotent pair. □

Theorem 3.8. *$I(a) = \{[xya'uv] \mid \langle x, y\rangle \in W(a', a), \langle u, v\rangle \in W(a, a')\}$ for all $a \in T$ and $a' \in I(a)$.*

Proof. Let $W(a) = \{[xya'uv] \mid \langle x, y\rangle \in W(a', a), \langle u, v\rangle \in W(a, a')\}$. Then for all $\langle x, y\rangle \in W(a', a)$ and $\langle u, v\rangle \in W(a, a')$ we obtain $[a[xya'uv]a] = [a[a'axya'aa'][aa'uvaa'a]] = [a[a'aa'][aa'a]] = a$. Also $[[xya'uv]a[xya'uv]] = [[xya'][aa'a][[a'aa']uv]] = [xya'uv]$. Thus $W(a) \subseteq I(a)$. Conversely, if $x \in I(a)$, then $\langle x, a\rangle \in W(a', a)$ and $\langle a, x\rangle \in W(a, a')$, by Lemma 3.2. Also $x = [xax] = [xaa'ax]$. Therefore $I(a) \subseteq W(a)$. Hence $I(a) = W(a)$. □

It is clear that if a ternary semigroup T is orthodox, then E_T is a band where the product is defined by $\langle a,b\rangle\ \langle c,d\rangle = \langle [abc],d\rangle = \langle a,[bcd]\rangle$. Thus E_T is a semilattice of rectangular bands, $E_T = \cup_{\alpha\in\Gamma} E_\alpha$. Then $\langle a,a'\rangle \in E_\alpha$ for any $a \in T$, and $a' \in I(a)$, so $W(a,a') = E_\alpha$, by Theorem3.6 (3). For any other $a^* \in I(a)$, $\langle a,a^*\rangle \in W(a,a') = E_\alpha$. Thus $W(a,a') = W(a,a^*)$ for all $a',a^* \in I(a)$. Similarly $W(a',a) = W(a^*,a)$. Hence we have the following lemma.

Lemma 3.9. *For any $a \in T$, if $a',a^* \in I(a)$, then $W(a,a^*) = W(a,a')$ and $W(a^*,a) = W(a',a)$.* □

Theorem 3.10. *A regular ternary semigroup T is orthodox if and only if for all $a,b \in T$ $I(a)\cap I(b) \neq \emptyset$ implies $I(a) = I(b)$.*

Proof. Let T be orthodox and $I(a)\cap I(b) \neq \emptyset$. If $x \in I(a)\cap I(b)$, then $a,b \in I(x)$. Hence, by Lemma 3.9, we have $W(x,a) = W(x,b)$ and $W(a,x) = W(b,x)$. Recalling the definition of $W(a)$ in the proof of Theorem 3.8, we see that $W(a) = \{[uvxpq] \,|\, \langle u,v\rangle \in W(x,a), \langle p,q\rangle \in W(a,x)\}$ and $W(b) = \{[stxwz] \,|\, \langle s,t\rangle \in W(x,b), \langle w,z\rangle \in W(b,x)\}$. Hence $W(a) = W(b)$. By Theorem 3.8, we have $I(a) = W(a) = W(b) = I(b)$.

Conversely assume that for all $a,b \in T$ from $I(a) \cap I(b) \neq \phi$ it follows $I(a) = I(b)$. Let $(a,a'),(b,b')$ be two idempotent pairs of T and let x be an inverse of $[aa'b]$ in T. Then for $y = [bxaa'b]$, $z = [b'bxaa']$ and $w = [xaa'bb']$ we have $[yzy] = [bxaa'bb'bxaa'bxaa'b] = [bxaa'b] = y$, $[zyz] = [b'bxaa'bxaa'bb'bxaa'] = [b'bxaa'] = z$, $[ywy] = [bxaa'bxaa'bb'bxaa'b] = [bxaa'b] = y$ and $[wyw] = [xaa'bb'bxaa'bxaa'bb'] = [xaa'bb'] = w$. Therefore $y \in I(z) \cap I(w)$ and so by hypothesis $I(z) = I(w)$. Thus $[aa'b]$ is in $I(z)$ because, $[[aa'b]z[aa'b]] = [aa'bb'bxaa'aa'b] = [aa'bxaa'b] = [aa'b]$ and $[z[aa'b]z] = [b'bxaa'aa'bb'bxaa'] = [b'b[xaa'bx]aa'] = [b'bxaa'] = z$. Hence by our hypothesis $[aa'b] \in I(w)$. Hence $[aa'bb'aa'bb't] = [[aa'bxaa'b]b'aa'bb't] = [aa'b[xaa'bb']aa'bb't] = [[aa'bwaa'b]b't] = [aa'bb't]$ for all $t \in T$. Similarly $[taa'bb'aa'bb'] = [taa'bb']$. Therefore $([aa'b],b')$ is an idempotent pair which proves that T is orthodox. □

4. Right strongly regular ternary semigroups

Binary right inverse semigroups are characterized in [12]. Below we present similar characterizations for ternary semigroups.

Definition 4.1. A regular ternary semigroup T with zero is called a *right* (resp. *left*) *strongly regular ternary semigroup* if every principal left (resp. right) ideal of T has a unique idempotent representation.

Since T is regular, by Lemma 2.6 every principal left ideal has an idempotent representation $(a)_l = [TTa] = [Ta'a]$. Suppose there are two idempotent pairs (x, y) and (u, v) such that $(a)_l = [TTa] = [Txy] = [Tuv]$. If T is right strongly regular, then (x, y) and (u, v) are equivalent. In other words, $[xyt] = [uvt]$ and $[txy] = [tuv]$ $\forall t \in T$. It can easily be seen that if (a, b) is an idempotent pair in a ternary semigroup T, then $[Tab] = [TT[bab]]$ is a principal left ideal. Thus every principal left ideal of T can be taken to be $[Tab]$ for some idempotent pair (a, b).

Definition 4.2. A ternary semigroup T is called a *right zero ternary semigroup* if $[abc] = c$ for all $a, b, c \in T$.

Theorem 4.3. *The following statements on a regular ternary semigroup T are equivalent:*

(1) *If (a, b), (u, v) are two idempotent pairs of T, then $[abT] \cap [uvT] \neq \emptyset$ and $[abT] \cap [uvT] = [abuvT] = [uvabT]$.*

(2) *If $(a, b), (u, v)$ are idempotent pairs in T, then $[abuvabt] = [uvabt]$ and $[tabuvab] = [tuvab]$ for all $t \in T$.*

(3) *If $\langle u, v\rangle$ and $\langle u_1, v_1\rangle$ belong to $W(a, b)$, then $([uva], b)$ and $([u_1v_1a], b)$ are equivalent idempotent pairs.*

(4) *For any idempotent pair (a, b), $W(a, b)$ is a right zero semigroup.*

(5) *Let (a, b) be an idempotent pair and $x' \in I(x)$. Then $x \in [Tab]$ implies $x' \in [abT]$.*

(6) *T is a right strongly regular ternary semigroup.*

Proof. (1) $\Rightarrow$ (2): Let (a, b), (u, v) be two idempotent pairs of T. Suppose $[abT] \cap [uvT] = [abuvT] = [uvabT]$. Then $[abuvT] \subseteq [uvT]$ and so for any $t \in T$, $[abuvt] = [uvt_1]$ for some $t_1 \in T$. Multiplying on the left by u and v we get $[uvabuvt] = [uvuvt_1] = [uvt_1] = [abuvt]$. So, $[tuvabuv] = [tuvabuvuv] = [tabuvuv] = [tabuv]$. Therefore $[tuvabuv] = [tabuv]$. Since $[uvabT] \subseteq [abT]$. Similarly we get $[abuvabt] = [uvabt]$ and $[tabuvab] = [tuvab]$ for every $t \in T$.

(2) $\Rightarrow$ (3): Suppose (2) holds for all idempotent pairs. If $\langle u, v\rangle \in W(a, b)$ and $\langle u_1, v_1\rangle \in W(a, b)$, then $([uva], b)$ and $([u_1v_1a], b)$ are idempotent pairs. So, $[u_1v_1abt] = [u_1v_1abu_1v_1abt] = [u_1v_1abuvabu_1v_1abt] = [uvabu_1v_1abt] = [uvabt]$ for all $t \in T$. Therefore $[u_1v_1abt] = [uvabt]$ and $[tu_1v_1ab] = [tu_1v_1abu_1v_1ab] = [tu_1v_1abuvabu_1v_1ab] = [tu_1v_1abuvabu_1v_1abab]$

$= [tuvabu_1v_1abab] = [tuvab]$. Hence $[tu_1v_1ab] = [tuvab]$. Thus $([uva], b)$ and $([u_1v_1a], b)$ are equivalent idempotent pairs. This proves (3).

(3) $\Rightarrow$ (4): Let (a, b) be an idempotent pair and $\langle u, v\rangle \in W(a, b)$. Since $\langle a, b\rangle \in W(a, b)$ by hypothesis, $([uva], b) \sim ([aba], b) \sim (a, b)$. Therefore $[uvt] = [uvabuvt] = [abuvt]$ and so, $[uvuvt] = [abuvabuvt] = [abuvt] = [uvt]$. Thus $[uvuvt] = [uvt]$ and $[tuvuv] = [tabuvabuv] = [tabuv] = [tuv]$ for every $t \in T$. Hence (u, v) is an idempotent pair. Let $\langle u_1, v_1\rangle \in W(a, b)$. By hypothesis, $([uva], b)$ and $([u_1v_1a], b)$ are equivalent idempotent pairs. Thus for all $t \in T$ we have $[uvu_1v_1abuvu_1v_1t] = [uvuvabuvu_1v_1t] = [uvabuvu_1v_1t]$ $= [uvu_1v_1t]$. Similarly, $[tuvu_1v_1abuvu_1v_1] = [tuvu_1v_1]$. Also for all $t \in T$, $[abuvu_1v_1abt] = [abuvuvabt] = [abuvabt] = [abt]$. Similarly, $[tabuvu_1v_1ab] = [tab]$. Therefore $\langle [uvu_1], v_1\rangle \in W(a, b)$. Hence for all $t \in T$ will be $[uvu_1v_1t]$ $= [uvu_1v_1abu_1v_1t] = [uvu_1v_1abuvu_1v_1abu_1v_1t] = [uvuvabuvuvabu_1v_1t] =$ $[uvabu_1v_1t] = [u_1v_1abu_1v_1t] = [u_1v_1t]$. Similarly, $[tuvu_1v_1] = [tu_1v_1]$. Therefore $([uvu_1], v_1) \sim (u_1, v_1)$. Hence $W(a, b)$ is a right zero semigroup.

(4) $\Rightarrow$ (3): Let $\langle u, v\rangle$ and $\langle u_1, v_1\rangle$ be in $W(a, b)$. Since $\langle a, b\rangle \in W(a, b)$ and $W(a, b)$ is a right zero semigroup, $([uva], b) \sim (a, b) \sim ([u_1v_1a], b)$.

(4) $\Rightarrow$ (5): Let (a, b) be an idempotent pair and $x \in [Tab]$. Then $x = [xab]$ $\forall x \in T$. Thus for any $x' \in I(x)$, $[x[abx']x] = [[xab]x'x] = [xx'x] =$ x and $[[abx']x[abx']] = [abx'[xab]x'] = [abx'xx'] = [abx']$. Therefore x' and $[abx']$ are inverses of x. Next, we prove that $\langle [abx'], x\rangle \in W(x', x)$. Hence $\forall t \in T$, $[abx'xx'xabx'xt] = [abx'[xab]x'xt] = [abx'xt]$. Similarly $[tabx'xx'xabx'x] = [tabx'x]$ and $[x'xabx'xx'xt] = [x'[xab]x'xt] = [x'xx'xt] =$ $[x'xt]$. Similarly $[tx'xabx'xx'x] = [tx'x]$. Therefore $\langle [abx'], x\rangle \in W(x', x)$. Hence, $([abx'], x)$ is equivalent to (x', x). Therefore $\forall t \in T$, $[abx'xt] = [x'xt]$ and $[tabx'x] = [tx'x]$. For $t = x'$ we have $x' = [x'xx'] = [abx'xx'] = [abx']$, which means that $x' \in [abT]$.

(5) $\Rightarrow$ (6): Since T is regular, by Lemma 2.6 every principal left ideal is of the form $[Tab]$ where (a, b) is an idempotent pair. Suppose (c, d) is an idempotent pair such that $[Tab] = [Tcd]$. Since $(a, b), (c, d)$ are idempotent pairs $([aba], [bab])$ are inverses of one another and $([cdc], [dcd])$ are inverses of one another. Thus $[bab] \in [Tab] = [Tcd]$ and $[dcd] \in [Tcd] = [Tab]$. Therefore $[bab] = [babcd]$ and $[dcd] = [[dcd]ab]$. By hypothesis, $[aba] \in [cdT]$ and $[cdc] \in [abT]$. Therefore $[aba] = [cd[aba]]$ and $[cdc] = [ab[cdc]]$. Thus for all $t \in T$ we have $[abt] = [a[bab]t] = [a[babcd]t] = [abcdt] = [[abcdc]dt] =$ $[cdcdt] = [cdt]$ and $[tab] = [t[aba]b] = [tcdabab] = [tcdab] = [tcd]$. Hence $(a, b) \sim (c, d)$ and T is right inverse.

(6) $\Rightarrow$ (1): Let (a, b) be an idempotent pair and $\langle u, v\rangle \in W(a, b)$. Then

$([uva], b)$ is an idempotent pair and $[Tab] = [Tabuvab] \subseteq [Tuvab] \subset [Tab]$. Therefore $[Tab] = [Tuvab]$. Let $\langle u_1, v_1\rangle \in W(a, b)$. Then $[Tuvab] = [Tab] = [Tu_1v_1ab]$. Thus $([uva], b)$, $([u_1v_1a], b)$ are equivalent idempotent pairs. Thus (6) implies (3). We now show that (1) holds. Let (a, b), (u, v) be idempotent pairs of T. We claim that $([abu], v)$ is an idempotent pair. Let $\langle x, y\rangle \in W([abu], v)$. Then it can easily be seen that $\langle [uvx], y\rangle$ and $\langle [xya], b\rangle$ are both in $W([abu], v)$. By hypothesis (3) we have $([xyababu], v) \sim ([uvxyabu], v)$. Therefore $[xyt] = [xyabuvxyt] = [uvxyabuvxyt] = [uvxyt]$ and so $[xyt] = [xyab[uvxyt]] = [xyabxyt]$. Consequently, $[xyabxyabt] = [xyabt]$. Similarly $[txyabxyab] = [txyab]$. Hence $([xya], b)$ is an idempotent pair. As $\langle [abu], v\rangle \in W([xya], b)$, hence by (4) $([abu], v)$ is an idempotent pair. Next, $[uvabuvuvabuvt] = [uvabuvabuvt] = [uvabuvt]$. Similarly $[tuvabuvuvabuv] = [tuvabuv]$. Hence $([uva], [buv])$ is an idempotent pair. Thus $[Tabuv] = [Tabuvabuv] \subseteq [Tuvabuv] \subset [Tabuv]$. Therefore $[Tabuv] = [Tuvabuv]$. By hypothesis $([abu], v) \sim ([uva], [buv])$ and so for all $t \in T$,$[abuvt] = [uvabuvt]$ and $[tabuv] = [tuvabuv]$. Hence (2) holds. Thus $[abuvT] \subseteq [uvT]$ and $[abuvT] \subset [abT]$. Therefore $[abuvT] \subseteq [abT] \cap [uvT]$ and so $[abt] \cap [uvT] \neq \emptyset$. Also $[abT] \cap [uvT] \subseteq [abuvT]$. Hence $[abT] \cap [uvT] = [abuvT]$. Similarly $[abT] \cap [uvT] = [uvabT]$. Hence (1). □

As a consequence of Theorem 4.3 (2) we obtain

Corollary 4.4. *A right strongly regular ternary semigroup is orthodox.* □

Lemma 4.5. *In a right strongly regular ternary semigroup for any idempotent pair (p, q) from $\langle u, v\rangle \in W(p, q)$ it follows $W(u, v) = W(p, q)$.*

Proof. By Theorem 4.3, $W(p, q)$ is a right zero semigroup. For any $\langle u, v\rangle$ from $W(p, q)$ we have $[uvuvt] = [uvt] = [pquvt]$, $[uvpqt] = [pqt]$, $[tuvuv] = [tuv] = [tpquv]$ and $[tuvpq] = [tpq]$. Suppose $\langle x, y\rangle \in W(u, v)$. Then $[xyxyt] = [xyt] = [uvxyt]$ and $[xyuvt] = [uvt]$. Similarly $[txyxy] = [txy] = [tuvxy]$ and $[txyuv] = [tuv]$, $\forall t \in T$. Therefore $[xypq[xyt]] = [xypq[uvxyt]] = [xyuvxyt] = [xyt]$, $[txypqxy] = [txypquvxy] = [txyuvxy] = [txy]$ and $[pqxypqt] = [pqxyuvpqt] = [pquvpqt] = [pqt]$. Similarly we obtain $[tpqxypq] = [tp[qxyuvp]pq] = [tpq]$ and so $\langle x, y\rangle \in W(p, q)$. Thus $W(u, v) \subseteq W(p, q)$. Analogously $W(p, q) \subseteq W(u, v)$. Hence $W(u, v) = W(p, q)$. □

Lemma 4.6. *Let T be a right strongly regular ternary semigroup. Then $(b', a') \subseteq W(a, b)$ for any $a, b \in T$ $a' \in I(a)$, $b' \in I(b)$.* □

Lemma 4.7. *Let T be a right strongly regular ternary semigroups. Then $[I(b)I(a)T] = \{[uvt] \mid \langle u, v\rangle \in W(a, b), t \in T\}$ for any $a, b \in T$.*

Proof. By Lemma 4.6, $[I(b)I(a)T] \subseteq \{[uvt] \mid \langle u, v\rangle \in W(a, b), t \in T\}$. If $b' \in I(b)$, $a' \in I(a)$ and $\langle u, v\rangle \in W(a, b)$, then $([b'a'a], b)$ and $([uva], b)$ are equivalent idempotent pairs by Theorem 4.3 (3). Hence for $\langle u, v\rangle \in W(a, b)$ we have $[uvt] = [uvabuvt] = [b'a'abuvt] \in [I(b)I(a)T]$. □

Similar results are valid for left strongly regular ternary semigroups.

Acknowledgements. The authors are grateful to Prof. V. Thangaraj and Prof. M. Loganathan for the valuable support. The authors express the gratitude to Prof. W. A. Dudek for his valuable suggestions.

References

[1] **A. Borowiec, W. A. Dudek and S. Duplij**, *Bi-element representations of ternary groups*, Commun. Algebra **34** (2006), 1651 – 1670.

[2] **W. Dörnte**, *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Z. **29** (1928), 1 – 19.

[3] **W. A. Dudek and I. M. Groździńska**, *On ideals in regular n-semigroups*, Mat. Bilten (Skopje) **3/4(29/30)** (1979-1980), 35 – 44.

[4] **E. Kasner**, *An extension of the group concept*, Bull. Amer. Math. Soc. **28** (1967), 261 – 265.

[5] **D. H. Lehmer**, *A ternary analogue of abelian groups*, Amer. J. Math. **54** (1932), 329 – 338.

[6] **J. Łoś**, *On the extending models I*, Fund. Math. **42** (1955), 38 – 54.

[7] **E. L. Post**, *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1920), 208 – 350.

[8] **M. L. Santiago**, *Regular ternary semigroups*, Bull. Calcutta Math. Soc. **82** (1990), 67 – 71.

[9] **M. L. Santiago and Sri Bala S.**, *Ternary semigroups*, Semigroup Forum **81** (2010), 380 – 388.

[10] **F. M. Sioson**, *On regular algebraic systems*, Proc. Japan Acad. **39** (1963), 283 – 286.

[11] **F. M. Sioson**, *Ideal theory in ternary semigroups*, Math. Japonica **10** (1965), 63 – 84.

[12] **P. S. Venkatesan**, *Right (left) inverse semigroups*, J. Algebra **31** (1974), 209 – 217.

Received January 24, 2011

Ramanujan Institute for Advanced Study in Mathematics, University of Madras, Chennai 600 005, India
E-mail: sheejag.dhe@gmail.com (Sheeja), sribalamath@yahoo.co.in (Sri Bala)

Quasigroups and Related Systems **19** (2011), 349 – 352

On n-groupoids in which all transformations are endomorphisms

Valentin S. Trokhimenko

Abstract. For an n-ary groupoid we find the neccesity and sufficient conditions under which all its transformations are endomorphisms.

It is known [1] that a semigroup in which each transformation is an endomorphism, is a left or right zero semigroup. Below we generalize this result to the case of n-ary groupoids.

Let (G, o) be an *n-ary groupoid*, i.e., a nonempty set G with an n-ary operation o. Such groupoid is also called an *n-groupoid* (cf. [2]). An element $0 \in G$ is called a *k-zero*, where $k \in \{1, 2, \ldots, n\}$, of an n-groupoid (G, o), if

$$o(x_1, \ldots, x_{k-1}, 0, x_{k+1}, \ldots, x_n) = 0$$

holds for all $x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n \in G$. An n-groupoid in which each element is a k-zero is called an *n-groupoid of k-zeros* or a *k-zero n-groupoid*. Following [3], an n-groupoid (G, o) in which $o(x_1, \ldots, x_n) \in \{x_1, \ldots, x_n\}$ for any $x_1, \ldots, x_n \in G$ is called *quasitrivial*.

Lemma 1. *An n-groupoid in which each transformation is an endomorphism is quasitrivial.*

Proof. Let φ_x be a transformation of an n-groupoid (G, o) such that $\varphi_x(z) = x$ for every $z \in G$. Since, by the assumption, φ_x is an endomorphism for each $x \in G$, we have

$$x = \varphi_x(o(x, \ldots, x)) = o(\varphi_x(x), \ldots, \varphi_x(x)) = o(x, \ldots, x).$$

So, every element of (G, o) is an idempotent.

2010 Mathematics Subject Classification: 20N15
Keywords: n-ary groupoid, quasi-trivial groupoid, endomorphism.

Suppose that $o(x_1,\dots,x_n) \notin \{x_1,\dots,x_n\}$ for some $x_1,\dots,x_n \in G$. Consider a transformation φ of (G,o) defined by

$$\varphi(z) = \begin{cases} x_1, & \text{if } z \in \{x_1,\dots,x_n\}, \\ z & \text{if } z \notin \{x_1,\dots,x_n\}. \end{cases}$$

Since φ is an endomorphism we have

$$\varphi(o(x_1,\dots,x_n)) = o(\varphi(x_1),\dots,\varphi(x_n)) = o(x_1,\dots,x_1) = x_1.$$

But $o(x_1,\dots,x_n) \notin \{x_1,\dots,x_n\}$, hence

$$\varphi(o(x_1,\dots,x_n)) = o(x_1,\dots,x_n).$$

Thus, $o(x_1,\dots,x_n) = x_1$, which is a contradiction. So, an n-groupoid (G,o) is quasitrivial. □

By E_k we denote the set of all equivalence relations defined on the set $\{1,2,\dots,n\}$ having exactly k equivalence classes, where $1 \leqslant k \leqslant \min(|G|,n)$. Let $E = \bigcup\limits_{k=1}^{m} E_k$, where $m = \min(|G|,n)$. For every $\varepsilon \in E$ by H_ε we denote the set of all such n-tuples $(x_1,\dots,x_n) \in G^n$ for which the equality $x_i = x_j$ holds if and only if $i \equiv j(\varepsilon)$, $i,j \in \{1,2,\dots,n\}$.

Theorem 1. *Each transformation of an n-groupoid (G,o) is its endomorphism if and only if (G,o) is quasitrivial and for any $\varepsilon_1,\varepsilon_2 \in E$, where $\varepsilon_1 \subset \varepsilon_2$, there exist $i \in \{1,2,\dots,n\}$ such that the implication*

$$o(x_1,\dots,x_n) = x_i \longrightarrow o(y_1,\dots,y_n) = y_i \tag{1}$$

is valid for all $(x_1,\dots,x_n) \in H_{\varepsilon_1}$ and $(y_1,\dots,y_n) \in H_{\varepsilon_2}$.

Proof. Let any transformation of an n-groupoid (G,o) be its endomorphism. Then, according to Lemma 1, an n-groupoid (G,o) is quasitrivial. Hence $o(x_1,\dots,x_n) \in \{x_1,\dots,x_n\}$. Consider two equivalence relations $\varepsilon_1,\varepsilon_2 \in E$ such that $\varepsilon_1 \subset \varepsilon_2$ and $(x_1,\dots,x_n) \in H_{\varepsilon_1}$. Suppose that $(y_1,\dots,y_n) \in H_{\varepsilon_2}$ for some $y_1,\dots,y_n \in G$. Since each transformation of (G,o) is an endomorphism, an endomorphism is also the transformation ψ defined by $\psi(x_k) = y_k$ for $x_k \in \{x_1,\dots,x_n\}$ and $\psi(z) = z$ for $z \notin \{x_1,\dots,x_n\}$. Thus,

$$y_i = \psi(x_i) = \psi(o(x_1,\dots,x_n)) = o(\psi(x_1),\dots,\psi(x_n)) = o(y_1,\dots,y_n).$$

So, the condition (1) is satisfied.

Conversely, let (G, o) be an n-groupoid satisfying all conditions of the above theorem. Then, obviously, for arbitrary $x_1, \ldots, x_n \in G$ there exist $\varepsilon_1 \in E$ such that $(x_1, \ldots, x_n) \in H_{\varepsilon_1}$. Since (G, o) is quasitrivial, we have $o(x_1, \ldots, x_n) = x_i$ for some $i \in \{1, 2, \ldots, n\}$. Therefore,

$$\varphi(o(x_1, \ldots, x_n)) = \varphi(x_i) \tag{2}$$

for each transformation φ of (G, o). Let $(\varphi(x_1), \ldots, \varphi(x_n)) \in H_{\varepsilon_2}$, where $\varepsilon_2 \in E$. Then $\varepsilon_1 \subset \varepsilon_2$. Thus, $o(x_1, \ldots, x_n) = x_i$, by (1), implies

$$o(\varphi(x_1), \ldots, \varphi(x_n)) = \varphi(x_i). \tag{3}$$

From (2) and (3) we obtain $\varphi(o(x_1, \ldots, x_n)) = o(\varphi(x_1), \ldots, \varphi(x_n))$. This means that φ is an endomorphism. □

Corollary 1. *If $|G| \geqslant n$, then each transformation of an n-groupoid (G, o) is its endomorphism if and only if (G, o) is a k-zero n-groupoid (for some $k \in \{1, 2, \ldots, n\}$).*

Proof. Let (G, o) be a k-zero n-groupoid. Then $o(x_1, \ldots, x_n) = x_k$ and $\varphi(o(x_1, \ldots, x_n)) = \varphi(x_k)$ for any transformation φ of G. On the other hand $o(\varphi(x_1), \ldots, \varphi(x_n)) = \varphi(x_k)$. So, $\varphi(o(x_1, \ldots, x_n)) = o(\varphi(x_1), \ldots, \varphi(x_n))$, which means that φ is an endomorphism of (G, o).

Conversely, let each transformation of an n-groupoid (G, o) be its endomorphism. Then (G, o) satisfies all conditions of Theorem 1. Because $|G| \geqslant n$ there exists n-tuple $(g_1, \ldots, g_n)$ of pairwise different elements from G. Moreover, in this case $m = \min(|G|, n) = n$, $E_n = \{\triangle\}$ and $(g_1, \ldots, g_n) \in H_\triangle$, where $\triangle$ denotes the identity binary relation on the set $\{1, \ldots, n\}$. By quasitriviality we have $o(g_1, \ldots, g_n) = g_k$ for some $k \in \{1, \ldots, n\}$. Let $(x_1, \ldots, x_n)$ be an arbitrary n-tuple from G^n and let ε be an equivalence relation from E such that $(x_1, \ldots, x_n) \in H_\varepsilon$. Since $\triangle \subset \varepsilon$, from $o(g_1, \ldots, g_n) = g_k$, by (1), we obtain $o(x_1, \ldots, x_n) = x_k$. So, (G, o) is a k-zero n-groupoid. □

Corollary 2. *If all transformations of a binary groupoid are its endomorphisms, then this groupoid is a left or right zero groupoid.*

Proof. For $|G| = 1$ it is obvious. For $|G| \geqslant 2$, by Corollary 1, this groupoid is a k-zero groupoid for some $k \in \{1, 2\}$. So, it is either a left or right zero groupoid. □

Note that each left (right) zero groupoid is a semigroup. Thus Corollary 2 is also valid for semigroups.

Theorem 2. *Each transformation of an n-groupoid (G, o) with $1 \leqslant |G| < n$ is its endomorphism if and only if for arbitrary $\varepsilon_1, \varepsilon_2 \in E$, where $\varepsilon_1 \subset \varepsilon_2$, there exist $i \in \{1, 2, \ldots, n\}$ such that (1) is true for all $(x_1, \ldots, x_n) \in H_{\varepsilon_1}$ and $(y_1, \ldots, y_n) \in H_{\varepsilon_2}$.*

Proof. In view of Theorem 1 it is enough to show that an n-groupoid (G, o) satisfying all conditions of Theorem 2 is quasitrivial.

Since $1 \leqslant |G| < n$, we have $m = \min(|G|, n) = |G|$. Let $x_1, \ldots, x_n \in G$ and $\varepsilon \in E$ be such that $(x_1, \ldots, x_n) \in H_\varepsilon$. Since the set E is finite, it has minimal elements. Clearly, all minimal elements of E belong to E_m. From elements of E_m we can choose ε_0 such that $\varepsilon_0 \subset \varepsilon$. Now let $(g_1, \ldots, g_n) \in H_{\varepsilon_0}$. Then $\{g_1, \ldots, g_n\} = G$ because $|G| = m < n$. Therefore $o(g_1, \ldots, g_n) \in \{g_1, \ldots, g_n\}$, which according to (1), implies $o(x_1, \ldots, x_n) \in \{x_1, \ldots, x_n\}$. So, an n-groupoid (G, o) is quasitrivial. Hence, by Theorem 1, all transformations of this n-groupoid are endomorphisms. So, the necessity of the above conditions is proved.

The proof of the sufficiency of these conditions is based on Lemma 1 and is analogous to the corresponding part of the proof of Theorem 1. □

References

[1] **A.H. Clifford and G.B. Preston**, *The algebraic theory of semigroups*, Amer. Math. Soc., Providence, R. I., vol. 1, 1964.

[2] **W.A. Dudek and V.S. Trokhimenko**, *Algebras of multiplace functions*, Christian Dawn, Kremenchuk, 2010.

[3] **H. Länger**, *Commutative quasitrivial superassociative systems*, Fund. Math. **109** (1980), 79 – 88.

Received October 4, 2011

Department of Mathematics, Pedagogical University, 21100 Vinnitsa, Ukraine
Email: vtrokhim@gmail.com

Quasigroups and Related Systems **19** (2011), 353 – 358

Affine–regular hexagons in the parallelogram space

Vladimir Volenec, Zdenka Kolar–Begović and Ružica Kolar–Šuper

Abstract The concept of the affine–regular hexagon, by means of six parallelograms, is defined and investigated in any parallelogram space and geometrical interpretation in the affine plane is also given.

1. Introduction

Let Q be a given set whose elements are said to be *points*. Let a quaternary relation Par $\subset Q^4$ is defined on the set Q. We shall say that the points a, b, c, d form a *parallelogram* and we shall write Par(a, b, c, d) in the case when $(a, b, c, d) \in Par$.

The pair (Q,Par) is called a *parallelogram space* if the quaternary relation Par $\subset Q^4$ has the following properties:

(P1) For any three points a, b, c there is one and only one point d so that Par(a, b, c, d).

(P2) If (e, f, g, h) is any cyclic permutation of (a, b, c, d) or of (d, c, b, a) then Par(a, b, c, d) implies Par(e, f, g, h).

(P3) From Par(a, b, c, d) and Par(c, d, e, f) it follows Par$(a, b, f, e,)$.

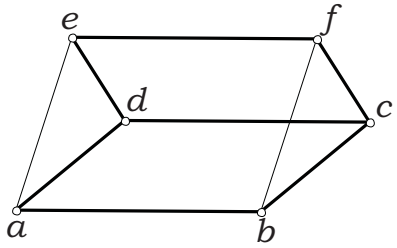


Figure 1.

2010 Mathematics Subject Classification:20N05
Keywords: parallelogram space, affine–regular hexagon

The parallelograms (including degenerated parallelograms) form a parallelogram space in the affine space of any dimension. The property (P3) in the affine plane (space) is illustrated in the Figure 1. Some other properties will be illustrated in the same plane.

2. Midpoint in the parallelogram space

In the parallelogram space the midpoint of the pair of points can be defined. We shall say that b is the *midpoint* of the pair $\{a, c\}$ and we shall write $M(a, b, c)$ if the statement $\mathrm{Par}(a, b, c, b)$ (Figure 2) is valid. From $M(a, b, c)$ obviously follows $M(c, b, a)$ and for any two points a and b there is the unique point c so that the statement $M(a, b, c)$ is valid. There are the examples of the parallelogram space, in which every pair of points does not have to have the unique midpoint.

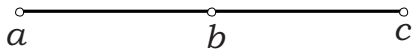


Figure 2.

Theorem 2.1. *Each statement of the three statements* $Par(o, a_1, a_2, a_3)$, $Par(o, a_2, a_3, a_4)$ *and* $M(a_1, o, a_4)$ *is the consequence of the remaining two statements* (*Figure* 3).

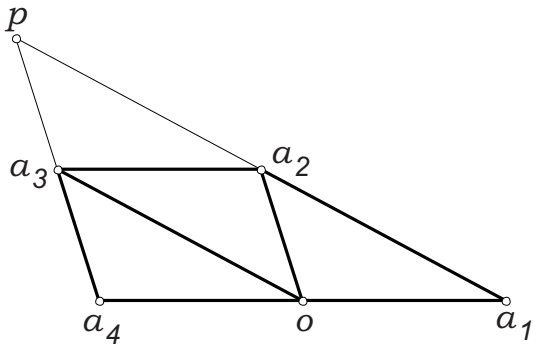


Figure 3.

Proof. The property (P3) by means of the property (P2) gives the implications

$$Par(o,a_1,a_2,a_3), Par(a_2,a_3,a_4,o) \Rightarrow Par(o,a_1,o,a_4)$$
$$Par(a_2,a_3,o,a_1), Par(o,a_1,o,a_4) \Rightarrow Par(a_2,a_3,a_4,o)$$
$$Par(a_2,a_3,a_4,o), Par(a_4,o,a_1,o) \Rightarrow Par(a_2,a_3,o,a_1).$$

But, the statements $\mathrm{Par}(o,a_1,o,a_4)$ and $\mathrm{Par}(a_4,o,a_1,o)$ are equivalent to the statement $M(a_1,o,a_4)$. □

3. Affine regular hexagon in the parallelogram space

We shall say that $(a_1,a_2,a_3,a_4,a_5,a_6)$ is the *affine–regular hexagon* with the vertices a_1,a_2,a_3,a_4,a_5,a_6 and the center o and we write $\mathrm{ARH}_o(a_1,a_2,a_3,a_4,a_5,a_6)$ if the statements

$$Par(o,a_{i-1},a_i,a_{i+1}),\ (i=1,2,3,4,5,6)$$

are valid, where the indexes are taken modulo 6 from the set $\{1,2,3,4,5,6\}$ (Figure 4).

The vertices a_i and a_{i+3} are said to be *opposite vertices* of the considered affine-regular hexagon, and the vertices a_i,a_{i+1},a_{i+2} are said to be *adjacent vertices*.

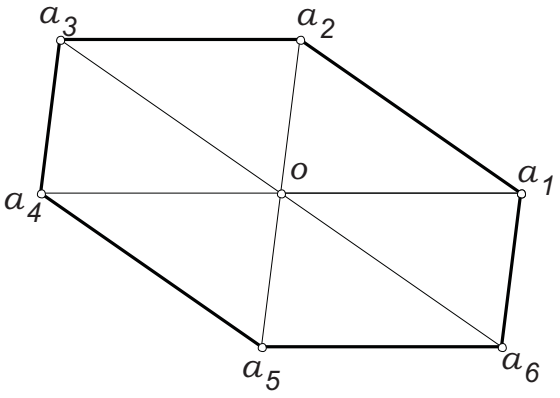


Figure 4.

Corollary 3.1. *The statement* $ARH_o(a_1,a_2,a_3,a_4,a_5,a_6)$ *imply the statement* $ARH_o(a_{i_1},a_{i_2},a_{i_3},a_{i_4},a_{i_5},a_{i_6})$ *where* $(i_1,i_2,i_3,i_4,i_5,i_6)$ *is any cyclic permutation of* $(1,2,3,4,5,6)$ *or of* $(6,5,4,3,2,1)$. □

Theorem 3.2. *If the statement* $ARH_o(a_1, a_2, a_3, a_4, a_5, a_6)$ *is valid then for any* $i \in \{1, 2, 3, 4, 5, 6\}$ *the statements* $Par(a_i, a_{i+1}, a_{i+3}, a_{i+4})$ *and* $M(a_i, o, a_{i+3})$ *are valid where indexes are taken modulo* 6.

Proof. The second statement for the case $i = 1$ is proved by Theorem 2.1 The first statement follows according to (P3) by the implication

$$Par(a_1, a_2, a_3, o), Par(a_3, o, a_5, a_4) \Rightarrow Par(a_1, a_2, a_4, a_5).$$

For the other indexes it is enough to apply cyclic permutations and Corollary 3.1. □

Theorem 3.3. *Affine–regular hexagon is uniquely determined by its center and by any two of its vertices which are not opposite or by any of its three adjacent vertices.*

Proof. Firstly let us prove the last statement. Let the vertices a_1, a_2, a_3 be given. Then according to (P1) there are the points o, a_4, a_5, a_6 so that the following statements

$$Par(a_1, a_2, a_3, o), Par(o, a_2, a_3, a_4), Par(o, a_3, a_4, a_5), Par(o, a_4, a_5, a_6) \quad (1)$$

are valid. From the two first statements (1) according to Theorem 2.1 it follows $M(a_1, o, a_4)$, which together with the fourth statement (1), again according to Theorem 2.1, gives $\mathrm{Par}(o, a_5, a_6, a_1)$. Analogously (increasing all indexes for one) the statement $Par(o, a_6, a_1, a_2)$ could be proved, so we get the statement $\mathrm{ARH}_o(a_1, a_2, a_3, a_4, a_5, a_6)$. Yet, it is necessary to prove that this affine–regular hexagon is uniquely determined by its center and for example by the vertices a_1, a_2 or by the vertices a_1, a_3. These proofs are reduced to the considered case if the vertex a_3 respectively a_2 is determined so that the statement $\mathrm{Par}(o, a_1, a_2, a_3)$ is valid and then we can conclude as in the previous case. □

The points o, a_1, a_2, a_3, a_4 with the properties from Theorem 2.1 determine figure, which will be denoted by the symbol $\mathrm{HARH}_o(a_1, a_2, a_3, a_4)$, "half" of the affine regular hexagon with the center o (Figure 3).

Corollary 3.4. *If the statement* $HARH_o(a_1, a_2, a_3, a_4)$ *is valid, then there are the uniquely determined points* a_5 *and* a_6 *so that the statement* $ARH_o(a_1, a_2, a_3, a_4, a_5, a_6)$ *holds.*

Theorem 3.5. *If the statement*

$$HARH_o(a_1, a_2, a_3, a_4) \tag{2}$$

is valid, then there is a point p such that the statements

$$M(a_1, a_2, p),\ M(a_4, a_3, p) \tag{3}$$

are valid. Conversely, if the statements (3) *are valid, then there is a point o such that the statement* (2) *is valid* (*Figure* 3).

Proof. Let the statement (2) be valid and let p be the point so that the first statement (3) is valid. Then according to (P3) we have the implications

$$Par(p, a_2, a_1, a_2), Par(a_1, a_2, a_3, o) \Rightarrow Par(p, a_2, o, a_3)$$
$$Par(a_4, a_3, a_2, o), Par(a_2, o, a_3, p) \Rightarrow Par(a_4, a_3, p, a_3),$$

so the second statement (3) is valid too. Conversely, let the statements (3) be valid and let o be such a point that the statement $\mathrm{Par}(a_2, p, a_3, o)$ holds. Then we get the implications

$$Par(o, a_3, p, a_2), Par(p, a_2, a_1, a_2) \Rightarrow Par(o, a_3, a_2, a_1)$$
$$Par(o, a_2, p, a_3), Par(p, a_3, a_4, a_3) \Rightarrow Par(o, a_2, a_3, a_4),$$

so the statement (2) is valid. □

Corollary 3.6. *If the statement* (2) *is valid then from the first statement* (3) *the second statement* (3) *follows.* □

Theorem 3.7. *Let $n \in \mathbb{N}$, $n \geqslant 3$. If the statements $HARH_{c_{12}}(b_1, a_1, a_2, b_2)$, $HARH_{c_{23}}(b_2, a_2, a_3, b_3), \ldots, HARH_{c_{n-1,n}}(b_{n-1}, a_{n-1}, a_n, b_n)$ are valid then there is a point c_{n1} so that the statement $HARH_{c_{n1}}(b_n, a_n, a_1, b_1)$ is valid too.* (*The case for $n = 5$ is illustrated in the Figure* 5).

Proof. From $\mathrm{HARH}_{c_{12}}(b_1, a_1, a_2, b_2)$ according to Theorem 3.5 it follows that there is a point o so that the statements $M(b_1, a_1, o)$ and $M(b_2, a_2, o)$ are valid, and then from $\mathrm{HARH}_{c_{23}}(b_2, a_2, a_3, b_3)$ follows the statement $M(b_3, a_3, o)$. Let Corollary 3.6 be applied again and after $(n-1)$–th application of this corollary from $\mathrm{HARH}_{c_{n-1,n}}(b_{n-1}, a_{n-1}, a_n, b_n)$ and $M(b_{n-1}, a_{n-1}, o)$ it follows $M(b_n, a_n, o)$. Finally, from the statements $M(b_n, a_n, o)$, $M(b_1, a_1, o)$ owing to Theorem 3.5 it follows that there is a point c_{n1} so that $\mathrm{HARH}_{c_{n1}}(b_n, a_n, a_1, b_1)$ is valid. □

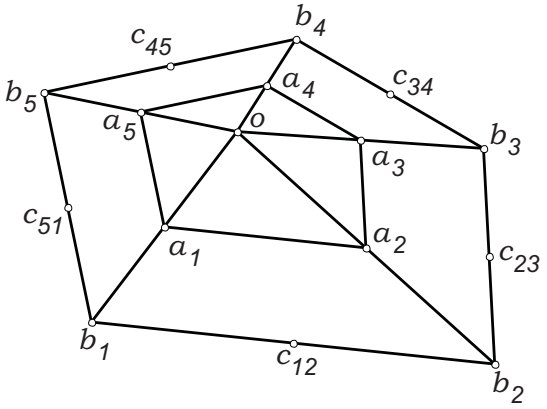


Figure 5.

From Theorem 3.7 by means of Corollary 3.4 we get:

Corollary 3.8. *Let $n \in \mathbb{N}$, $n \geqslant 3$. If the statements $ARH_{c_{12}}(b_1, a_1, a_2, b_2, d_{21}, d_{12})$, $ARH_{c_{23}}(b_2, a_2, a_3, b_3, d_{32}, d_{23}), \ldots, ARH_{c_{n-1,n}}(b_{n-1}, a_{n-1}, a_n, b_n, d_{n,n-1}, d_{n-1,n})$ are valid, then there are the points c_{n1}, d_{n1}, d_{1n} so that the statement $ARH_{c_{n1}}(b_n, a_n, a_1, b_1, d_{1n}, d_{n1})$ is valid too.* □

References

[1] **F. Ostermann, J. Schmidt**, *Begründung der Vektorrechnung aus Parallelogrammeigenschaften*, Math.– phys. Semesterber. **10** (1963), 47–64.

[2] **V. Volenec**, *Parallelogram spaces and their corresponding algebraic and geometric structures*, Math. Communications **2** (1997), 15–20.

Received November 22, 2011

V. Volenec
Department of Mathematics, University of Zagreb, Bijenička c. 30, 10 000 Zagreb, Croatia
E-mail: volenec@math.hr

Z. Kolar–Begović
Department of Mathematics, University of Osijek, Gajev trg 6, 31 000 Osijek, Croatia
E-mail: zkolar@mathos.hr

R. Kolar–Šuper
Faculty of Teacher Education, University of Osijek, Cara Hadrijana bb, 31 000 Osijek, Croatia
E-mail: rkolar@ufos.hr

Quasigroups and Related Systems **19** (2011), 359 – 368

A study of anti-fuzzy quasi-ideals in ordered semigroups

Anwar Zeb and Asghar Khan

Abstract. In this paper, we introduce the concept of anti-fuzzy quasi-ideals in ordered semigroups and investigate the quasi-ideals of ordered semigroups in terms of anti-fuzzy quasi-ideals. We characterize left (resp. right) regular and completely regular ordered semigroups in terms of anti-fuzzy quasi-ideals and semiprime anti-fuzzy quasi-ideals.

1. Introduction

Biswas introduced the concept of an anti-fuzzy subgroup of a group in [3] and studied the basic properties of groups in terms of anti-fuzzy subgroups. Hong and Jun [5] modified Biswas idea and applied it to BCK-algebras. Akram and Dar defined anti-fuzzy left h-ideals of hemirings [2]. Recently Shabir and Nawaz studied anti fuzzy ideals of semigroups [11]. Ahsan et. al in [1] characterize semigroups in terms of fuzzy quasi-ideals. The monograph given by Mordeson and Malik [10] deals with the applications of fuzzy approach to the concepts of automata and formal languages. Fuzzy sets in ordered semigroups were first introduced by Kehayopulu and Tsingelis in [8].

In this paper, we introduce the concept of anti-fuzzy quasi-ideals in ordered semigroups and investigate the basic properties of quasi-ideals of ordered semigroups in terms of anti-fuzzy quasi-ideals. We characterize left (resp. right) regular and completely regular ordered semigroups in terms of anti-fuzzy quasi-ideals. We define semiprime anti-fuzzy quasi-ideals and characterize completely regular ordered semigroups in terms of semiprime anti-fuzzy quasi-ideals.

2010 MSC: 06F05, 06D72, 08A72
Keywords: Fuzzy subset, anti-fuzzy quasi-ideal, simple semigroup, completely regular ordered semigroup.

2. Some basic definitions and results

By an *ordered semigroup* (*po-semigroup*) we mean a *structure* $(S, \cdot, \leqslant)$ in which

$(OS1)$ $(S, \cdot)$ is a *semigroup*,

$(OS2)$ $(S, \leqslant)$ is a *poset*,

$(OS3)$ $(\forall a, b, x \in S)(a \leqslant b \Longrightarrow ax \leqslant bx$ and $xa \leqslant xb)$.

Throughout this paper S will denote an ordered semigroup unless otherwise specified.

For $A, B \subseteq S$, we denote $(A] := \{t \in S \,|\, t \leqslant h$ for some $h \in A\}$ and $AB := \{ab \,|\, a \in A, b \in B\}$. Then $A \subseteq (A]$, $(A](B] \subseteq (AB]$, $((A]] = (A]$ and $((A](B]] \subseteq (AB]$.

A non-empty subset A of S is called a *right* (resp. *left*) *ideal* of S if:

(1) $AS \subseteq A$ (resp. $SA \subseteq A$),

(2) $a \in A$ and $S \ni b \leqslant a$ imply $b \in A$.

If A is both a right and a left ideal of S, then it is called an *ideal* of S.

A non-empty subset Q of S is called a *quasi-ideal* of S if:

(1) $(QS] \cap (SQ] \subseteq Q$,

(2) $a \in Q$ and $S \ni b \leqslant a$ imply $b \in Q$.

A subsemigroup B of S is called a *bi-ideal* of S if:

(1) $BSB \subseteq B$,

(2) $a \in B$ and $S \ni b \leqslant a$ imply $b \in B$.

A fuzzy subset f of S is called a *fuzzy left* (resp. *right*) *ideal* of S if:

(1) $x \leqslant y \Longrightarrow f(x) \geqslant f(y)$,

(2) $f(xy) \geqslant f(y)$ (resp. $f(xy) \geqslant f(x)$) for all $x, y \in S$.

If f is both a fuzzy left and a fuzzy right ideal of S. Then it is called a *fuzzy ideal* of S.

A fuzzy subset f of S is called a *fuzzy subsemigroup* of S if for all $x, y \in S$ $f(xy) \geqslant \min\{f(x), f(y)\}$. A fuzzy subsemigroup f of S is called a *fuzzy bi-ideal* of S if:

(1) $x \leqslant y \Longrightarrow f(x) \geqslant f(y)$,

(2) $f(xyz) \geqslant \min\{f(x), f(z)\}$ for all $x, y \in S$.

For a non-empty *family* of fuzzy subsets $\{f_i\}_{i \in I}$ of S, the fuzzy subsets $\bigwedge\limits_{i \in I} f_i$ and $\bigvee\limits_{i \in I} f_i$ of S are defined as follows:

$$\Big(\bigwedge_{i \in I} f_i\Big)(x) := \inf_{i \in I}\{f_i(x)\}, \qquad \Big(\bigvee_{i \in I} f_i\Big)(x) := \sup_{i \in I}\{f_i(x)\}.$$

For any two fuzzy subsets f and g of S we put

$$(f \circ g)(x) := \begin{cases} \bigvee\limits_{(y,z)\in A_x} \max\{f(y), g(z)\} & \text{if } A_x \neq \emptyset, \\ 0 & \text{if } A_x = \emptyset, \end{cases}$$

where $A_x := \{(y,z) \in S \times S \,|\, x \leqslant yz\}$.

A fuzzy subset f of S is called a *fuzzy quasi-ideal* of S if:

(1) $x \leqslant y \Longrightarrow f(x) \geqslant f(y)$,

(2) $(f \circ 1) \wedge (1 \circ f) \preceq f$,

where $f \preceq g$ means that $f(x) \leqslant g(x)$ for all $x \in S$.

A fuzzy subset f of S is called an *anti-fuzzy subsemigroup* of S if

$$f(xy) \leqslant \max\{f(x), f(y)\}$$

for all $x, y \in S$.

An anti-fuzzy subsemigroup f of S is called an *anti-fuzzy bi-ideal* of S if:

(1) $x \leqslant y$ implies $f(x) \leqslant f(y)$,

(2) $f(xay) \leqslant \max\{f(x), f(y)\}$

for all $x, a, y \in S$.

For fuzzy subsets f and g of S the product $f * g$ is defined as follows:

$$(f * g)(a) = \begin{cases} \bigwedge\limits_{(y,z)\in A_x} \max\{f(y), g(z)\} & \text{if } A_x \neq \emptyset \\ 1 & \text{if } A_x = \emptyset \end{cases}$$

The fuzzy subsets "$\mathcal{S}$" and "$\mathcal{O}$" of S are defined as

$$\mathcal{S}(x) = 1, \qquad \mathcal{O}(x) = 0$$

for all $x \in S$.

Proposition 2.1. *Let $A, B \subseteq S$. Then*

(i) $A \subseteq B$ if and only if $f_{B^c} \preceq f_{A^c}$.

(ii) $f_{A^c} \vee f_{B^c} = f_{A^c \cup B^c} = f_{(A\cap B)^c}$.

(iii) $f_{A^c} * f_{B^c} = f_{(AB]^c}$. □

An ordered semigroup S is called *regular* (see [6]) if for every $a \in S$ there exists $x \in S$ such that $a \leqslant axa$ or equivalently, $(1)(\forall a \in S)(a \in (aSa])$ and $(2)(\forall A \subseteq S)(A \subseteq (ASA])$, and S is called *left* (resp. *right*) *simple* (see [7]) if it has no proper left (resp. right) ideals.

Lemma 2.2. (cf. [7]). *S is left (resp. right) simple if and only if $(Sa] = S$ (resp. $(aS] = S$) for every $a \in S$.* □

An ordered semigroup S is called *left* (resp. *right*) *regular* (see [7]) if for every $a \in S$, there exists $x \in S$ such that $a \leqslant xa^2$ (resp. $a \leqslant a^2x$) or equivalently, $(1)(\forall a \in S)(a \in (Sa^2])$ and $(2)(\forall A \subseteq S)(A \subseteq (SA^2])$. S is called *completely regular* if it is regular, left regular and right regular [7].

If $\emptyset \neq A \subseteq S$, then the set $(A \cup (AS \cap SA)]$ is the quasi-ideal of S generated by A.

Lemma 2.3. (cf. [6]). *S is completely regular if and only if $A \subseteq (A^2SA^2]$ for every $A \subseteq S$. Equivalently, if $a \in (a^2Sa^2]$ for every $a \in S$.* □

3. Anti-fuzzy quasi-ideals

Definition 3.1. A fuzzy subset f of S is called an *anti-fuzzy quasi-ideal*if

(1) $(f * \mathcal{O}) \vee (\mathcal{O} * f) \succeq f$,

(2) $x \leqslant y$ implies $f(x) \leqslant f(y)$ for all $x, y \in S$.

As a consequence of the transfer principle for fuzzy sets (cf. [9] we obtain the following two theorems.

Theorem 3.2. *Let $\emptyset \neq A \subseteq S$. Then A is a quasi-ideal of S if and only if the characteristic function f_{A^c} of the complement of A is an anti-fuzzy quasi-ideal of S.*

Theorem 3.3. *Let f be a fuzzy subset of S. Then each non-empty level $L(f;t)$ is a quasi-ideal if and only if f is an anti-fuzzy quasi-ideal.*

Example 3.4. The set $S = \{a, b, c, d, f\}$ with the multiplication

$\cdot$	a	b	c	d	f
a	a	a	a	a	a
b	a	b	a	d	a
c	a	f	c	c	f
d	a	b	d	d	b
f	a	f	a	c	a

and the order $\leqslant := \{(a,a),(a,b),(a,c),(a,d),(a,f),(b,b),(c,c),(d,d),(f,f)\}$ is an ordered semigroup with the following quasi-ideals:

$\{a\},\{a,b\},\{a,c\},\{a,d\},\{a,f\},\{a,b,d\},\{a,c,d\},\{a,b,f\},\{a,c,f\},S$.

For a fuzzy set f defined by $f(a) = 0.3$, $f(b) = 0.5$, $f(c) = f(f) = 0.8$, $f(d) = 0.6$ we have

$$L(f;t) := \begin{cases} S & \text{if} \quad t \in [0.8, 1), \\ \{a, b, d\} & \text{if} \quad t \in [0.6, 0.8), \\ \{a, b\} & \text{if} \quad t \in [0.5, 0.6), \\ \{a\} & \text{if} \quad t \in [0.3, 0.5), \\ \emptyset & \text{if} \quad t \in [0, 0.3). \end{cases}$$

$L(f;t)$ is a quasi-ideal. By Theorem 3.3, f is an anti-fuzzy quasi-ideal. □

Lemma 3.5. *Every anti-fuzzy quasi-ideal of S is its anti-fuzzy bi-ideal.*

Proof. Let $x, y, z \in S$. Then $xyz = x(yz) = (xy)z$. Hence $(x, yz) \in A_{xyz}$ and $(xy, z) \in A_{xyz}$. Since $A_{xyz} \neq \emptyset$, we have

$$\begin{aligned} f(xyz) &\leqslant [(f * \mathcal{O}) \vee (\mathcal{O} * f)]\,(xyz) \\ &= \max\left[\bigwedge_{(p,q)\in A_{xyz}} \max\{f(p), \mathcal{O}(q)\}, \bigwedge_{(p_1,q_1)\in A_{xyz}} \max\{\mathcal{O}(p_1), f(q_1)\}\right] \\ &\leqslant \max[\max\{f(x), \mathcal{O}(yz)\}, \max\{\mathcal{O}(xy), f(z)\}] \\ &= \max[\max\{f(x), 0\}, \max\{0, f(z)\}] = \max[f(x), f(z)]. \end{aligned}$$

Let $x, y \in S$, then $xy = x(y)$ and hence $(x, y) \in A_{xy}$. Since $A_{xy} \neq \emptyset$, we have

$$\begin{aligned} f(xy) &\leqslant [(f * \mathcal{O}) \vee (\mathcal{O} * f)](xy) \\ &= \max\left[\bigwedge_{(p,q)\in A_{xy}} \max\{f(p), \mathcal{O}(q)\}, \bigwedge_{(p,q)\in A_{xy}} \max\{\mathcal{O}(p), f(q)\}\right] \\ &\leqslant \max[\max\{f(x), \mathcal{O}(y)\}, \max\{\mathcal{O}(x), f(y)\}] \\ &= \max[\max\{f(x), 0\}, \max\{0, f(y)\}] = \max[f(x), f(y)]. \end{aligned}$$

Let $x, y \in S$ be such that $x \leqslant y$. Then $f(x) \leqslant f(y)$, because f is an anti-fuzzy quasi-ideal of S. Thus f is an anti-fuzzy bi-ideal of S. □

The converse of above Lemma is not true, in general.

Example 3.6. The set $S = \{a, b, c, d\}$ with the multiplication table

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	a	a	a
c	a	a	b	a
d	a	a	b	b

and the order $\leqslant := \{(a,a),(b,b),(c,c),(d,d),(a,b)\}$ is an ordered semigroup.

$\{a, d\}$ is its bi-ideal but not a quasi-ideal.

For a fuzzy set $f(a) = f(d) = 0.7$, $f(b) = f(c) = 0.3$ we have

$$L(f;t) := \begin{cases} S & \text{if} \quad t \in [0.7, 1), \\ \{a, d\} & \text{if} \quad t \in [0.3, 0.7), \\ \emptyset & \text{if} \quad t \in [0, 0.3). \end{cases}$$

$L(f;t)$ is a bi-ideal for every t, but for $t \in [0.3, 0.7)$ it is not a quasi-ideal of S. By Theorem 3.3, f is an anti-fuzzy bi-ideal of S but not an anti-fuzzy quasi-ideal of S. □

4. Completely regular ordered semigroups

Theorem 4.1. *The the following are equivalent:*

(*i*) *S is regular, left and right simple,*

(*ii*) *every anti-fuzzy quasi-ideal of S is a constant function.*

Proof. $(i) \Longrightarrow (ii)$. Let S be a fixed regular, left and right simple ordered semigroup. Let f be an anti-fuzzy quasi-ideal of S. We consider the set $E_\Omega = \{e \in S \mid e^2 \geqslant e\}$. E_Ω is non-empty, because for $a \in S$ there exists $x \in S$ such that $a \leqslant axa$, hence $(ax)^2 = (axa)x \geqslant ax$, which means that $ax \in E_\Omega$.

(A) We first prove that f is a constant function on E_Ω. That is, $f(e) = f(t)$ for every $t \in E_\Omega$. In fact: since S is left and right simple, we have $(St] = S$ and $(tS] = S$. But $e \in S$. Then $e \in (St]$ and $e \in (tS]$. Thus $e \leqslant xt$ and $e \leqslant ty$ for some $x, y \in S$. If $e \leqslant xt$ then $e^2 = ee \leqslant (xt)(xt) = (xtx)t$ and $(xtx, t) \in A_{e^2}$. If $e \leqslant ty$ then $e^2 = ee \leqslant (ty)(ty) = t(yty)$ and $(t, yty) \in A_{e^2}$.

Since $A_{e^2} \neq \emptyset$ we have

$$\begin{aligned} f(e^2) &\leqslant ((f * \mathcal{O}) \vee (\mathcal{O} * f))(e^2) = \max[(f * \mathcal{O})(e^2), (\mathcal{O} * f)(e^2)] \\ &= \max\left[\bigwedge_{(y_1,z_1)\in A_{e^2}} \max\{f(y_1), \mathcal{O}(z_1)\}, \bigwedge_{(y_2,z_2)\in A_{e^2}} \max\{\mathcal{O}(y_2), f(z_2)\}\right] \\ &\leqslant \max[\max\{f(t), \mathcal{O}(yty)\}, \max\{\mathcal{O}(xtx), f(t)\}] \\ &= \max[\max\{f(t), 0\}, \max\{0, f(t)\}] = \max[f(t), f(t)] = f(t). \end{aligned}$$

Since $e \in E_\Omega$, we have $e^2 \geqslant e$ and $f(e^2) \geqslant f(e)$. Thus $f(e) \leqslant f(t)$. On the other hand since S is left and right simple and $e \in S$, we have $S = (Se]$ and $S = (eS]$. Since $t \in S$ we have $t \in (Se]$ and $t \in (eS]$. Then $t \leqslant ze$ and $t \leqslant es$ for some $z, s \in S$. If $t \leqslant ze$ then $t^2 = tt \leqslant (ze)(ze) = (zez)e$ and $(zez, e) \in A_{t^2}$. If $t \leqslant es$ then $t^2 = tt \leqslant (es)(es) = e(ses)$ and $(e, ses) \in A_{t^2}$. Since $A_{t^2} \neq \emptyset$ we have

$$\begin{aligned} f(t^2) &\leqslant ((f * \mathcal{O}) \vee (\mathcal{O} * f))(t^2) = \max[(f * \mathcal{O})(t^2), (\mathcal{O} * f)(t^2)] \\ &= \max\left[\bigwedge_{(y_1,z_1)\in A_{t^2}} \max\{f(y_1), \mathcal{O}(z_1)\}, \bigwedge_{(y_2,z_2)\in A_{t^2}} \max\{\mathcal{O}(y_2), f(z_2)\}\right] \\ &\leqslant \max[\max\{f(e), \mathcal{O}(ses)\}, \max\{\mathcal{O}(zez), f(e)\}] \\ &= \max[\max\{f(e), 0\}, \max\{0, f(e)\}] = \max[\max\{f(e), f(e)\}] = f(e). \end{aligned}$$

Since $t \in E_\Omega$ then $t^2 \geqslant t$ and $f(t^2) \geqslant f(t)$. Thus $f(t) \leqslant f(e)$. Consequently, $f(t) = f(e)$.

(B) Now we prove that f is a constant function on S. That is, $f(t) = f(a)$ for every $a \in S$. In fact: since S is regular and $a \in S$, there exists $x \in S$ such that $a \leqslant axa$. We consider the elements ax and xa of S. Then by $(OS3)$, we have $(ax)^2 = (axa)x \geqslant ax$ and $(xa)^2 = x(axa) \geqslant xa$, then $ax, xa \in E_\Omega$ and by (A) we have $f(ax) = f(t)$ and $f(xa) = f(t)$. Since $(ax)(axa) \geqslant axa \geqslant a$, then $(ax, axa) \in A_a$ and $(axa)(xa) \geqslant axa \geqslant a$, then $(axa, xa) \in A_a$ and hence $A_a \neq \emptyset$. Since f is an anti-fuzzy quasi-ideal of S, we have

$$\begin{aligned} f(a) &\leqslant ((f * \mathcal{O}) \vee (\mathcal{O} * f))(a) = \max[(f * \mathcal{O})(a), (\mathcal{O} * f)(a)] \\ &= \max\left[\bigwedge_{(y_1,z_1)\in A_a} \max\{f(y_1), \mathcal{O}(z_1)\}, \bigwedge_{(y_2,z_2)\in A_a} \max\{\mathcal{O}(y_2), f(z_2)\}\right] \\ &\leqslant \max[\max\{f(ax), \mathcal{O}(axa)\}, \max\{\mathcal{O}(axa), f(xa)\}] \\ &= \max\left[\max\{f(ax), 0\}, \max\{0, f(xa)\}\right] = \max\left[f(ax), f(xa)\right] = f(t). \end{aligned}$$

Since S is left and right simple we have $(Sa] = S$, and $(aS] = S$. Since $t \in S$, we have $t \in (Sa]$ and $t \in (aS]$. Then $t \leqslant pa$ and $t \leqslant aq$ for some $p, q \in S$. Then $(p, a) \in A_t$ and $(a, q) \in A_t$. Since $A_t \neq \emptyset$, and f is an anti-fuzzy quasi-ideal of S, we have

$$\begin{aligned} f(t) &\leqslant ((f * \mathcal{O}) \vee (\mathcal{O} * f))(t) = \max[(f * \mathcal{O})(t), (\mathcal{O} * f)(t)] \\ &= \max\left[\bigwedge_{(y_1,z_1)\in A_t} \max\{f(y_1), \mathcal{O}(z_1)\}, \bigwedge_{(y_2,z_2)\in A_t} \max\{\mathcal{O}(y_2), f(z_2)\}\right] \\ &\leqslant \max\left[\max\{f(a), \mathcal{O}(q)\}, \max\{\mathcal{O}(p), f(a)\}\right] \\ &= \max\left[\max\{f(a), 0\}, \max\{0, f(a)\}\right] = f(a). \end{aligned}$$

Thus $f(t) \leqslant f(a)$ and $f(t) = f(a)$.

$(ii) \Longrightarrow (i)$. Let $a \in S$. Then the set $(aS]$ is a quasi-ideal of S. Indeed: $(aS] \cap (Sa] \subseteq (aS]$, and $x \in (aS]$ and $S \ni y \leqslant x \in (aS]$ imply $y \in ((aS]] = (aS]$. Since $(aS]$ is quasi-ideal of S, by Theorem 3.2, the characteristic function $f_{(aS]^c}$ of $(aS]$ is an anti-fuzzy quasi-ideal of S. By hypothesis, $f_{(aS]^c}$ is a constant function, that is, there exists $t \in \{0, 1\}$ such that $f_{(aS]^c}(x) = t$ for every $x \in S$. Let $(aS] \subset S$ and a be an element of S such that $a \notin (aS]$, then $f_{(aS]^c}(a) = 1$. On the other hand, since $a^2 \in (aS]$, then $f_{(aS]^c}(a^2) = 0$, a contradiction to the fact that $f_{(aS]^c}$ is a constant function. Hence $(aS] = S$. By symmetry we can prove that $(Sa] = S$.

Since $a \in S$ and $S = (aS] = (Sa]$, we have $a \in (aS] = (a(Sa]] = (aSa]$, consequently S is regular. □

Theorem 4.2. *S is completely regular if and only if for every anti-fuzzy quasi-ideal f of S we have $f(a) = f(a^2)$ for every $a \in S$.*

Proof. Let S be completely regular and f be an anti-fuzzy quasi-ideal of S. Since S is left and right regular we have $a \in (Sa^2]$ and $a \in (a^2S]$ for every $a \in S$. Then there exists $x, y \in S$ such that $a \leqslant xa^2$ and $a \leqslant a^2y$. Hence $(x, a^2), (a^2, y) \in A_a$. Since $A_a \neq \emptyset$, we have

$$\begin{aligned} f(a) &\leqslant ((f * \mathcal{O}) \vee (\mathcal{O} * f))(a) = \max[(f * \mathcal{O})(a), (\mathcal{O} * f)(a)] \\ &= \max\left[\bigwedge_{(y_1,z_1)\in A_a} \max\{f(y_1), \mathcal{O}(z_1)\}, \bigwedge_{(y_2,z_2)\in A_a} \max\{\mathcal{O}(y_2), f(z_2)\}\right] \\ &\leqslant \max\left[\max\{f(a^2), \mathcal{O}(y)\}, \max\{\mathcal{O}(x), f(a^2)\}\right] \\ &= \max\left[\max\{f(a^2), 0\}, \max\{0, f(a^2)\}\right] \\ &= \max\left[f(a^2), f(a^2)\right] = f(a^2) = f(aa) \leqslant \max\{f(a), f(a)\} = f(a). \end{aligned}$$

Hence $f(a) = f(a^2)$.

Conversely, let $a \in S$ and let $Q(a^2)$ be the quasi-ideal generated by a^2. Then $Q(a^2) = (a^2 \cup (a^2S \cap Sa^2)]$. By Theorem 3.2, the characteristic function $f_{Q(a^2)^c}$ is an anti-fuzzy quai-ideal of S. By hypothesis $f_{Q(a^2)^c}(a) = f_{Q(a^2)^c}(a^2)$. Since $a^2 \in Q(a^2)$, we have $f_{Q(a^2)^c}(a^2) = 0$, then $f_{Q(a^2)^c}(a) = 0$ and $a \in Q(a^2) = (a^2 \cup (a^2S \cap Sa^2)]$. Then $a \leqslant a^2$ or $a \leqslant a^2x$ and $a \leqslant ya^2$ for some $x, y \in S$. If $a \leqslant a^2$ then $a \leqslant a^2 = aa \leqslant a^2a^2 = aaa^2 \leqslant a^2aa^2 \in a^2Sa^2$ and so $a \in (a^2Sa^2]$. If $a \leqslant a^2x$ and $a \leqslant ya^2$ then $a \leqslant (a^2x)(ya^2) = a^2(xy)a^2 \in a^2Sa^2$ and so $a \in (a^2Sa^2]$. □

A subset T of S is called *semiprime* if for every $a \in S$ such that $a^2 \in T$ we have $a \in T$. An anti-fuzzy quasi-ideal f of S is called *semiprime* if $f(a) \leqslant f(a^2)$ all $a \in S$.

Theorem 4.3. *S is completely regular if and only if every its anti-fuzzy quasi-ideal is semiprime.*

Proof. Let S be completely regular and f be its anti-fuzzy quasi-ideal. Then $f(a) \leqslant f(a^2)$ for $a \in S$. Indeed: since S is left and right regular, there exist $x, y \in S$ such that $a \leqslant xa^2$ and $a \leqslant a^2y$ then $(x, a^2) \in A_a$ and $(a^2, y) \in A_a$. Since $A_a \neq \emptyset$, and f is an anti-fuzzy quasi-ideal of S, we have

$$\begin{aligned} f(a) &\leqslant ((f * \mathcal{O}) \vee (\mathcal{O} * f))(a) = \max[(f * \mathcal{O})(a), (\mathcal{O} * f)(a)] \\ &= \max\left[\bigwedge_{(y_1,z_1)\in A_a} \max\{f(y_1), \mathcal{O}(z_1)\}, \bigwedge_{(y_2,z_2)\in A_a} \max\{\mathcal{O}(y_2), f(z_2)\}\right] \\ &= \max\left[\max\{f(a^2), \mathcal{O}(y)\}, \max\{\mathcal{O}(x), f(a^2)\}\right] \\ &\leqslant \max\left[\max\{f(a^2), 0\}, \max\{0, f(a^2)\}\right] = \max\left[f(a^2), f(a^2)\right] = f(a^2). \end{aligned}$$

Conversely. Let f be an anti-fuzzy quasi-ideal of S such that $f(a) \leqslant f(a^2)$ for all $a \in S$. By Theorem 3.2, the characteristic function $f_{Q(a^2)^c}$ of the quasi-ideal $Q(a^2)$ is an anti-fuzzy quai-ideal of S. By hypothesis $f_{Q(a^2)^c}(a) \leqslant f_{Q(a^2)^c}(a^2)$. Since $a^2 \in Q(a^2)$, we have $f_{Q(a^2)^c}(a^2) = 0$, then $f_{Q(a^2)^c}(a) = 0$ and $a \in Q(a^2) = (a^2 \cup (a^2S \cap Sa^2)]$. Thus $a \leqslant a^2$ or $a \leqslant a^2p$ and $a \leqslant qa^2$ for some $p, q \in S$. If $a \leqslant a^2$ then $a \leqslant a^2 = aa \leqslant a^2a^2 = aaa^2 \leqslant a^2aa^2 \in a^2Sa^2$ and so $a \in (a^2Sa^2]$. If $a \leqslant a^2p$ and $a \leqslant qa^2$ then $a \leqslant (a^2p)(qa^2) = a^2(pq)a^2 \in a^2Sa^2$ and so $a \in (a^2Sa^2]$. Consequently, S is completely regular. □

References

[1] **J. Ahsan, R. M. Latif, and M. Shabir**, *Fuzzy quasi-ideals of semigroups*, J. Fuzzy Math. **2** (2001), 259 – 270.

[2] **M. Akram and K. H. Dar**, *On anti fuzzy left h-ideals in hemirings*, International Math. Forum **46** (2007), 2295 – 2304.

[3] **R. Biswas**, *Fuzzy subgroups and anti-fuzzy subgroups*, Fuzzy Sets and Systems **35** (1990), 121 – 124.

[4] **W. A. Dudek and Y. B. Jun**, *$\mathcal{N}$-quasi-groups*, Quasigroups and Related Systems **17** (2009), 29 – 38.

[5] **S. M. Hong and Y. B. Jun**, *On anti-fuzzy ideals in BCK-algebras*, Kyungpook Math. J. **38** (1998), 145 – 150.

[6] **N. Kehayopulu**, *On completely regular ordered semigroups*, Sci. Math. **1** (1998), 27 – 32.

[7] **N. Kehayopulu, and M. Tsingelis**, *On the decomposition of prime ideals in ordered semigroups into their $\mathcal{N}$-classes*, Semigroup Forum **47** (1993), 393 – 395.

[8] **N. Kehayopulu and M. Tsingelis**, *Fuzzy sets in ordered groupoids*, Semigroup Forum **65** (2002), 128 – 132.

[9] **M. Kondo and W. A. Dudek**, *On the Transfer Principle in fuzzy theory*, Mathware Soft Comput. **12** (2005), 41 – 55.

[10] **J. N. Mordeson, D. S. Malik and N. Kuroki,** *Fuzzy semigroups*, Studies in Fuzziness and Soft Computing **131**, Springer-Verlag, Berlin, 2003.

[11] **M. Shabir and Y. Nawaz**, *Semigroups characterized by the properties of their anti-fuzzy ideals*, J. Advanced Research Pure Appl. Math. (2008), 1 – 18.

Received September 02, 2010
Revised February 8, 2011

Department of Mathematics, COMSATS Institute of Information Technology, Abbottabad, Pakistan
E-mails: anwar55.ciit@yahoo.com (A. Zeb) azhar4set@yahoo.com (A. Khan)