Quasigroups and Related Systems **23** (2015), 165 – 173

Note on the power graph of finite simple groups

Narges Akbari and Ali Reza Ashrafi

Abstract. A graph Γ is said to be 2−connected if Γ does not have a cut vertex. The power graph $\mathcal{P}(G)$ of a group G is the graph which has the group elements as vertex set and two elements are adjacent if one is a power of the other. In an earlier paper, it is conjectured that there is no non-abelian finite simple group with a 2−connected power graph. Bubboloni et al. [3] and independently Doostabadi and Farrokhi D. G. [11], presented counterexamples for this conjecture. The aim of this paper is to first modify this conjecture and then prove this modified conjecture for the sporadic groups, Ree groups ${}^2F_4(q)$ and ${}^2G_2(q)$, the Chevalley groups $A_1(q), B_2(q), C_3(q)$ and $F_4(q)$, the unitary group $U_3(q)$, the symplectic group $S_4(q)$ and the projective special linear group $PSL(3, q)$, where q is a prime power.

1. Introduction

The investigation of graphs related to groups is an important topic in algebraic combinatorics. This paper is devoted to the study of power graphs, which were introduced by Kelarev and Quinn in [13]. These authors in [16, 14, 15] studied the same structures on a semigroup. The power graph $\mathcal{P}(G)$ of a finite group G is a simple graph in which $V(\mathcal{P}(G)) = G$ and two vertices are adjacent if and only if one of them is a power of the other. We encourage the interested reader to consult [1] for a survey of all recent results on this topic.

Let us review some facts on power graphs of a finite group. Chakrabarty et al. [6] classified the complete power graphs and obtained a formula for the number of edges in a power graph. Cameron and Ghosh [4] proved that non-isomorphic finite groups may have isomorphic power graphs, but that finite abelian groups with isomorphic power graphs must be isomorphic. It is also conjectured that [4] two finite groups with isomorphic power graphs have the same number of elements of each order. Later Cameron [5] responded affirmatively to this conjecture.

Mirzargar et al. [20] considered some graph invariants of the power graphs into account and conjectured that the power graph of a cyclic group of order n has the maximum number of edges between the power graphs of all groups of order n. This conjecture recently proved by Curtin and Pourgholi [9]. Moghaddamfar et al. [21] defined the proper power graph $\mathcal{P}^\star(G)$ as a graph constructed from $\mathcal{P}(G)$ by deleting the identity element of G. They provided necessary and sufficient

2010 Mathematics Subject Classification: 20D05, 20D08, 05C10
Keywords: Power graph, proper power graph, simple group.
Partially supported by the University of Kashan under grant number 364988/26.

conditions for a proper power graph $\mathcal{P}^\star(G)$ to be a strongly regular graph, a bipartite graph or a planar graph. In a recent paper [22], the authors determined, up to isomorphism, the structure of a finite group G whose power graph has exactly n spanning trees, $n < 5^3$, and obtained a new characterization of the alternating group A_5 by tree-number of its power graph. Finally in [19], the second author of the present paper computed the automorphism group of the power graphs of cyclic groups.

A graph Γ is said to be $2-$*connected* if Γ does not have a cut vertex. It is easy to see that $\mathcal{P}^\star(G)$ is connected if and only if $\mathcal{P}(G)$ is $2-$connected. Pourgholi et al. [23], proved some results about characterization of simple groups by power graphs. They proposed the following open question:

Question. *Does there exist a non-abelian simple group with a $2-$connected power graph?*

Following Bubboloni et al. [3], we assume that P is the set of prime numbers and $b, c \in \mathbb{N}$, where $\mathbb{N}$ denotes the set of all positive integers. Set

$$bP + c = \{x \in \mathbb{N} \mid x = bp + c, for\ some\ p \in P\}$$

and define

$$A = P \cup (P + 1) \cup (P + 2) \cup (2P) \cup (2P + 1).$$

They proved that $\mathcal{P}(A_n)$ is $2-$connected if and only if $n = 3$ or $n \notin A$. In Theorems 3.6 and 3.7 of [11], the authors proved that the proper power graphs of the projective special linear group $PSL(2, q)$, q is prime power, and the Suzuki group $Sz(2^{2n+1})$ are disconnected. This shows that their power graphs are not $2-$connected. They also reproved [3, Theorem A] with a difference in the case that $\frac{n-2}{2}$ is prime. We conjecture that:

Conjecture. *The power graph of a non-abelian simple group G is $2-$connected if and only if G is isomorphic to the alternating group A_n, where $n = 3$ or $n \notin A$.*

The aim of this paper is to prove this conjecture for some classes of finite simple groups. For a finite group G, we denote by $\pi_e(G)$ a set of all element orders of group G. This set is closed under divisibility and hence is uniquely determined by a set $\mu(G)$ of elements in $\pi_e(G)$ which are maximal under the divisibility relation. The set of all divisors of a natural number n is denoted by $\beta(n)$. Our other notations are standard and taken mainly from [8].

We will prove the following theorem:

Main Theorem. *Let q be a power of a prime number. The proper power graphs of the sporadic groups, Ree groups ${}^2F_4(q)$ and ${}^2G_2(q)$, the Chevalley groups $A_1(q)$, $A_2(q)$, $B_2(q)$, $C_3(q)$ and $F_4(q)$, the projective unitary group $U_3(q)$ and the projective symplectic group $S_4(q)$ are disconnected.*

2. Proof of the main theorem

The aim of this section is to prove our main theorem. We separated our proof into four subsections. In the first subsection, it is proved that the power graph of sporadic groups are not 2−connected. In the second subsection, the 2−connectivity of $\mathcal{P}(^2F_4(q))$ and $\mathcal{P}(^2G_2(q))$ are investigated. Our third subsection is devoted to connectedness of the proper power graph of the Chevalley groups $A_1(q)$, $A_2(q)$, $B_2(q)$, $C_2(q)$ and $F_4(2^m)$. In our final subsection, the power graphs of $U_3(q)$ and $S_4(q)$ are taken into account.

2.1. The sporadic groups

Two positive integers r and s are said to be incomparable if r is not divisible by s and s is not divisible by r. Suppose G is a finite group and $G \setminus \{e\}$ can be partitioned into two subsets A and B such that for each element $a \in A$ and $b \in B$, $|a|$ and $|b|$ are coprime. Then the proper power graph $\mathcal{P}^\star(G)$ will be disconnected. We apply this simple fact to prove that the power graphs of the sporadic groups are not 2−connected.

Define $S(M_{11}) = S(M_{12}) = S(M_{22}) = S(McL) = \{11\}$, $S(M_{23}) = S(M_{24}) = \{23\}$, $S(J_1) = S(J_3) = S(HN) = \{19\}$, $S(J_2) = \{7\}$, $S(He) = \{17\}$, $S(J_4) = \{23, 29, 31, 37, 43\}$, $S(Co_1) = S(Co_3) = \{23\}$, $S(Co_2) = \{11, 23\}$, $S(O'N) = \{31\}$, $S(Ly) = \{67\}$, $S(Ru) = S(Fi_{24}) = \{29\}$, $S(HS) = \{7, 11\}$, $S(Th) = \{13, 19, 31\}$, $S(Suz) = \{11, 13\}$, $S(B) = \{31, 47\}$, $S(M) = \{41, 71\}$, $S(Fi_{22}) = \{13, 17\}$, $S(Fi_{23}) = \{17, 23\}$. For an arbitrary sporadic group G, we assume that $A(G) = \{g \in G \mid |g| \in S(G)\}$ and $B(G) = G \setminus (A(G) \cup \{e\})$. We now apply computer algebra system GAP [12] to prove that for each $x \in A(G)$ and $y \in B(G)$, $|x|$ and $|y|$ are coprime, proving the following result:

Theorem 1. *The power graphs of the sporadic groups are not* 2−*connected.*

2.2. The power graph of the Ree groups $^2F_4(q)$ and $^2G_2(q)$

The aim of this section is to prove the power graph of $^2F_4(q)$ and $^2G_2(q)$ are not 2−connected. Suppose $\mu(G)$ denotes the set of all maximal elements of $\pi_e(G)$ with divisibility order. We first consider the group $^2F_4(q)$, where $q = 2^{2m+1}$ and $m \geqslant 1$. Deng and Shi [10, Lemma 3] proved that

$$\begin{aligned}\pi_e(^2F_4(q)) = &\{1, 2, 4, 8, 12, 16\} \cup \beta(2(q+1)) \cup \beta(4(q-1))\\ &\cup \beta(4(q+\sqrt{2q}+1)) \cup \beta(4(q-\sqrt{2q}+1)) \cup \beta(q^2-1) \cup \beta(q^2+1)\\ &\cup \beta(q^2-q+1) \cup \beta((q-1)(q+\sqrt{2q}+1)) \cup \beta((q-1)(q-\sqrt{2q}+1))\\ &\cup \beta(q^2+q\sqrt{2q}+q+\sqrt{2q}+1) \cup \beta(q^2-q\sqrt{2q}+q-\sqrt{2q}+1).\end{aligned}$$

Set $\alpha = q^2 + q\sqrt{2q} + q + \sqrt{2q} + 1, X = \beta(\alpha) \setminus \{1\}$, $Y = \pi_e(G) \setminus (X \cup \{1\})$ and $Z = \{q+1, q-1, q^2+1, q+\sqrt{2q}+1, q-\sqrt{2q}+1, q^2-q+1, q^2-q\sqrt{2q}+q-\sqrt{2q}+1\}$.

We claim that for integer $\gamma \in Z$, $(\alpha, \gamma) = 1$. To prove this, it is enough to notice that by simple divisions of appropriate components, we have:

$$\begin{aligned}
\alpha &= (q+\sqrt{2q})(q+1)+1\\
&= (q+\sqrt{2q}+2)(q-1)+(2\sqrt{2q}+3)\\
&= q(q+\sqrt{2q}+1)+(\sqrt{2q}+1)\\
&= (q^2-q+1)+\sqrt{2q}(q+\sqrt{2q}+1) \qquad (1)\\
&= (q^2-q\sqrt{2q}+q-\sqrt{2q}+1)+2\sqrt{2q}(q+1)\\
&= (q+2\sqrt{2q}+4)(q-\sqrt{2q}+1)+(3\sqrt{2q}-3)\\
&= (1+\sqrt{2q})(q^2+1)+(q\sqrt{2q}+q-q^2\sqrt{2q}).
\end{aligned}$$

To explain, we choose the case of $q-\sqrt{2q}+1$. If the prime p divides α and $q-\sqrt{2q}+1$ then by the fourth equation in (1),

$$\alpha = (3\sqrt{2q}-3)+(q+2\sqrt{2q}+4)(q-\sqrt{2q}+1).$$

This shows that $p|3\sqrt{2q}-3 = 3\times 2^{m+1}-3$ and so $p|3\times 2^{2m+1}$. Since p is odd, $p=3$ and $3|q-\sqrt{2q}+1 = 2^{2m+1}-2^{m+1}+1$. Thus, $2^{2m+1}-2^{m+1} \equiv -1(\mod 3)$. On the other hand, for each positive integer k, $2^{2k+1} \equiv 2\ (\mod 3)$ which implies that $3|2^{m+1}$, a contradiction. Using a similar argument, all cases lead to contradiction. Hence, we obtain a partition $\pi_e(G)X \cup Y \cup \{1\}$ such that elements of X and Y are mutually coprime. Therefore, we have proved the following result:

Theorem 2. *The power graph of the Ree group* $^2F_4(q)$ *is not* $2-$*connected.*

We now consider the groups $^2G_2(q)$, where $q = 3^{2m+1}$ and $m \geq 0$. It is well-known that $^2G_2(3) \cong Aut(SL(2,8))$ and for $m \geqslant 1$ the groups $^2G_2(q)$ are simple. Staroletove [26, Lemma 3.5], proved that

$$\mu(^2G_2(q)) = \left\{q+\sqrt{3q}+1, q-\sqrt{3q}+1, q-1, \frac{q+1}{2}, 6\right\}.$$

Set $\alpha = q+\sqrt{3q}+1$ and $T = \{q-\sqrt{3q}+1, q-1, \frac{q+1}{2}, 6\}$. We prove that α does not have a common prime factor with an element of T. This is an immediate consequence of the fact that $\alpha = (q-\sqrt{3q}+1)+2\sqrt{3q} = (q-1)+(2+\sqrt{3q}) = 2\frac{q+1}{2}+\sqrt{3q}$. This shows that by removing the identity element, the resulting graph will be disconnected. We have proved the following result:

Theorem 3. *The power graph of the Ree group* $^2G_2(q)$ *is not* $2-$*connected.*

2.3. The power graphs of $A_1(q), A_2(q), B_2(q), C_2(q)$ and $F_4(2^m)$

In this section, it is proved that the power graphs of the groups $A_1(q)$, $A_2(q)$, $B_2(q), C_2(q)$ and $F_4(2^m)$ are not $2-$connected. We start by the simple group

$G = A_1(q)$, where q is an odd prime power. Staroletove [26, Lemma 3.5], proved that $\mu(A_1(q)) = \left\{\dfrac{q+1}{2}, \dfrac{q-1}{2}, p\right\}$. Since $p \not| \frac{q+1}{2}$ and $p \not| \frac{q-1}{2}$, by removing the identity element, the elements of order p will be separate from other elements. Thus, we proved the following:

Theorem 4. *The graph $\mathcal{P}(A_1(q))$ is not $2-$connected.*

We now consider the simple group $A_2(q)$, where q is a prime power. Simpson [24] proved that

$$\mu(A_2(q)) = \begin{cases} \left\{q-1, \frac{p(q-1)}{3}, \frac{q^2-1}{3}, \frac{q^2+q+1}{3}\right\} & d = 3 \textit{ and } q \textit{ is odd,} \\ \left\{p(q-1), q^2-1, q^2+q+1\right\} & d = 1 \textit{ and } q \textit{ is odd,} \\ \left\{4, q-1, \frac{2(q-1)}{3}, \frac{q^2-1}{3}, \frac{q^2+q+1}{3}\right\} & d = 3 \textit{ and } q \textit{ is even,} \\ \left\{4, 2(q-1), q^2-1, q^2+q+1\right\} & d = 1 \textit{ and } q \textit{ is even,} \end{cases}$$

where $d = (3, q-1)$.

We first assume that q is odd and $d = 3$. Set

$$\alpha = \frac{q^2+q+1}{3} \quad \text{and} \quad X = \left\{q-1, \frac{p(q-1)}{3}, \frac{q^2-1}{3}\right\}.$$

Since $\alpha = (q+2)\frac{q-1}{3} + 1 = q\frac{q-1}{3} + \frac{2q+1}{3}$, by a similar argument as Proposition 2, α and elements of X are coprime. Hence $\mathcal{P}(A_2(q))$ is not $2-$connected. Next assume that q is odd, $d = 1$, $\alpha = q^2+q+1$ and $X = \{p(q-1), q^2-1\}$. Again since $\alpha = q(q-1) + (2q+1)$, α is coprime with $p(q-1)$ and q^2-1 which shows that $\mathcal{P}(A_2(q))$ is not $2-$connected.

We now assume that $q = 2^m$ and $d = 3$. Define:

$$\alpha = \frac{q^2+q+1}{3} \quad \text{and} \quad X = \left\{4, \frac{q-1}{3}, \frac{q^2-1}{3}\right\}.$$

Since $\alpha = (q+2)\frac{q-1}{3} + 1$, it can easily prove that α is coprime to all elements of X which implies that the proper power graph of $A_2(q)$ is disconnected. Finally, if $q = 2^m$, $d = 1$, $\alpha = q^2+q+1$ and $X = \{4, q-1, q^2-1\}$, then α an elements of X are coprime. Therefore, we have proved the following:

Theorem 5. *The proper power graph of $A_2(q)$ is not connected.*

We now proceed to consider the simple group $G = B_2(q)$, where q is a prime power. Srinivasan [25] proved that:

$$\mu(B_2(q)) = \begin{cases} \frac{q^2+1}{(2,q-1)}, \frac{q^2-1}{(2,q-1)}, p(q+1), p(q-1) & p > 3 \\ \\ \frac{q^2+1}{(2,q-1)}, \frac{q^2-1}{(2,q-1)}, p(q+1), p(q-1), p^2 & p \in \{2,3\} \end{cases}$$

We consider three cases as follows:

a. *$q = p^m$, where $p > 3$ is prime and m is a natural number.* In this case $(2, q-1) = 2$. Define $\alpha = \frac{q^2+1}{2}$ and $X = \{p(q+1), p(q-1), \frac{q^2-1}{2}\}$. Then α is coprime with all elements of X and by a similar argument as Proposition 2, $\mathcal{P}(B_2(q))$ is not $2-$connected.

b. *$q = 3^m$, where m is a natural number.* In this case we have again $(2, q-1) = 2$ and by choosing $\alpha = \frac{q^2+1}{2}$ and $X = \{3(q+1), 3(q-1), \frac{q^2-1}{2}, 9\}$, we can see that α does not have a common divisor with an element of X. So, $\mathcal{P}(B_2(q))$ is not $2-$connected.

c. *$q = 2^m$, where m is a natural number.* In this case, $(2, q-1) = 1$. Set $\alpha = q^2+1$ and $X = \{p(q+1), p(q-1), q^2-1, 4\}$. Then a similar argument as Cases a and b shows that $\mathcal{P}(B_2(q))$ is not $2-$connected.

Thus, we have proved the following result:

Theorem 6. *The proper power graph of $B_2(q)$ is not connected.*

We now consider the group $C_2(q)$, where q is an odd prime power. Staroletove [26, Lemma 3.5] proved that:

$$\mu(C_2(q)) = \begin{cases} \left\{\frac{q^2+1}{2}, \frac{q^2-1}{2}, p(q+1), p(q-1)\right\} & p \neq 3, \\ \left\{\frac{q^2+1}{2}, \frac{q^2-1}{2}, p(q+1), p(q-1), 9\right\} & p = 3. \end{cases}$$

We consider two separate cases as follows:

a. *$q = p^m$, where $p > 3$ is prime and m is a natural number.* In this case, we define $\alpha = \frac{q^2+1}{2}$ and $X = \{p(q+1), p(q-1), \frac{q^2-1}{2}\}$. Some similar calculations as above show that α is coprime with all elements of X and so $\mathcal{P}(B_2(q))$ is not $2-$connected.

b. *$q = 3^m$, where m is a natural number.* A similar argument as Case b in the proof of Proposition 6 completes this case.

Hence, we have proved the following result:

Theorem 7. *The proper power graph of $C_2(q)$ is not connected.*

We end this subsection by investigation of the power graph of the group $F_4(q)$, $q = 2^m$ and $m \geq 1$. Coa et al. [7, Lemma 1.6] proved that:

$\mu(F_4(q)) = \{16,\ 8(q-1), 8(q+1), 4(q^2-1), 4(q^2+1), 4(q^2-q+1), 4(q^2+q+1), 2(q-1)(q^2+1), 2(q+1)(q^2+1), 2(q^3-1), 2(q^3+1), (q^2-1)(q^2-q+1), q^4-q^2+1, (q^2-1)(q^2+q+1), q^4-1, q^4+1\}$.

Define $\alpha = q^4 - q^2 + 1$ and

$$X = \{q-1, q+1, q^2+1, q^2-q+1, q^2+q+1, q^4-1, q^4+1\}.$$

By using a similar argument as above, one can see that it is possible to partition the group $F_4(2^m)$ into the set of all elements that their orders are divisors of α and its complement. Again by deleting the identity element, the resulting graph will be disconnected. So, we have:

Theorem 8. *The proper power graph of $F_4(2^m)$ is not connected.*

2.4. The power graphs of $U_3(q)$ and $S_4(q)$

The aim of this section is to prove the proper power graph of $U_3(q)$ and $S_4(q)$ are disconnected. We start by the simple groups $U_3(q)$, where q is an odd prime power. This group is defined as $U_3(q) = \frac{SU_3(q)}{Z(SU_3(q))}$, where $SU_3(q)$ is the set of all invertible 3×3 matrices A on $GF(q^2)$ such that $detA = 1$ and $A\overline{A^T} = I$, and $Z(SU_3(q))$ denotes its center. It is well-known that $|U_3(q)| = \frac{q^3(q^3+1)(q^2-1)}{d}$, where $d = (3, q-1)$. Aleeva [2, Lemma 10] proved that if q is odd then the maximal element orders of this group is as follows:

$$\mu(U_3(q)) = \begin{cases} \left\{\frac{q^2-q+1}{3}, \frac{q^2-1}{3}, \frac{p(q+1)}{3}, q+1\right\} & d = 3, \\ \left\{q^2-q+1, q^2-1, p(q+1)\right\} & d = 1. \end{cases}$$

We now consider the following two cases:

1. $d = 3$. Suppose $\alpha = \frac{q^2-q+1}{3}$ and $X = \left\{q+1, \frac{p(q+1)}{3}, \frac{q^2-1}{3}\right\}$. If we partition $U_3(q)$ into the set of all elements such that their orders are divisors of α and its complement, then by removing the identity element the resulting graph will be disconnected.

2. $d = 1$. In this case by choosing $\alpha = q^2 + q + 1$ and $X = \left\{p(q+1), q^2-1\right\}$, one can easily prove that α and elements of X are coprime. Thus, $U_3(q)$ is not $2-$connected.

We have proved the following:

Theorem 9. *The proper power graph of $U_3(q)$ is not connected.*

We end this paper by considering the simple group $S_4(q)$, $q = p^m$ and p is an odd prime. Srinivasan [25] proved that:

$$\pi_e(S_4(q)) = \beta(\frac{q^2+1}{2}) \cup \beta(\frac{q^2-1}{2}) \cup \beta(p(q+1)) \cup \beta(p(q-1));\ p \neq 3,$$
$$\mu(S_4(q)) = \left\{\frac{q^2+1}{2}, \frac{q^2-1}{2}, 3(q+1), 3(q-1), 9\right\};\ p = 3.$$

We consider two separate cases as follows:

1. Set $\alpha = \frac{q^2+1}{2}$ and $X = \left\{\frac{q^2-1}{2}, p(q+1), p(q-1)\right\}$. Then
$$A = \{x \in S_4(q) \mid o(x)|\alpha\} \quad \text{and} \quad B = S_4(q) \setminus A$$
is a partition of $S_4(q)$ such that by removing the identity element, the resulting graph will disconnected. This proves that $\mathcal{P}(S_4(q))$ is $2-$connected.

2. Set $\alpha = \frac{q^2+1}{2}$ and $X = \left\{\frac{q^2-1}{2}, 3(q+1), 3(q-1), 9\right\}$. A similar argument as Case (1), completes our argument.

Therefore, the following result is proved.

Theorem 10. *The proper power graph of $S_4(q)$, $q = p^m$ and p is an odd prime, is not connected.*

The proof of the main theorem follows from Theorems $1 - 10$.

Acknowledgments. The authors are indebted to anonymous referee for his/her suggestions and helpful remarks. We also indebted to professor Daniela Bubboloni for her comments on the conjecture of this paper.

References

[1] **J. Abawajy, A.V. Kelarev and M. Chowdhury**, *Power graphs: a survey*, Electron. J. Graph Theory Appl. (EJGTA) **1** (2013), no. 2, 125 – 147.

[2] **M.R. Aleeva**, *Composition factors of finite groups whose element order set coincides with one for $U_3(q)$*, Sib. Mat. Zh. **43** (2002), 249 – 267.

[3] **D. Bubboloni, M.A. Iranmanesh and S.M. Shaker**, 2-*Connectivity of the power graph of finite alternating groups*, arXiv:1412.7324v1.

[4] **P.J. Cameron and S. Ghosh**, *The power graph of a finite group*, Discrete Math. **311** (2011), 1220 – 1222.

[5] **P.J. Cameron**, *The power graph of a finite group II*, J. Group Theory **13** (2010), 779 – 783.

[6] **I. Chakrabarty, S. Ghosh and M.K. Sen**, *Undirected power graphs of semigroups*, Semigroup Forum **78** (2009), 410 – 426.

[7] **H.P. Coa, G. Chen, M.A. Grechkoseeva, V.D. Mazurov, W.J. Shi and A.V. Vasilev**, *Recognition of the finite simple groups $F_4(2^m)$ by spectrum*, Sib. Math. J. **45** (2004), 1031 – 1035.

[8] **J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson**, *Atlas of Finite Groups*, Oxford University Press, Eynsham, 1985.

[9] **B. Curtin and G.R. Pourgholi**, *Edge-maximality of power graphs of finite cyclic groups*, J. Algebraic Combin. **40** (2014), 313 – 330.

[10] **H. Deng and W. Shi**, *The characterization of Ree groups ${}^2F_4(q)$ by their element orders*, J. Algebra **217** (1999), 180 – 187.

[11] **A. Doostabadi and M.D.G. Farrokhi**, *On the connectivity of proper power graphs of finite groups*, Commun. Algebra **43** (2015), 4305 – 4319.

[12] **GAP** – Groups, Algorithms, and Programming, Version 4-4-10, 2007.

[13] **A.V. Kelarev and S.J. Quinn**, *A combinatorial property and power graphs of groups*, Contributions to General Algebra **12** (1999), Vienna, pp. 229 – 235, Heyn, Klagenfurt, 2000.

[14] **A.V. Kelarev and S.J. Quinn**, *Directed graphs and combinatorial properties of semigroups*, J. Algebra **251** (2002), no. 1, 16 – 26.

[15] **A.V. Kelarev and S.J. Quinn**, *A combinatorial property and power graphs of semigroups*, Comment. Math. Univ. Carolinae **45** (2004), 1 – 7.

[16] **A.V. Kelarev, S.J. Quinn and R. Smolikova**, *Power graphs and semigroups of matrices*, Bull. Austral. Math. Soc. **63** (2001), 341 – 344.

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

[18] **V.D. Mazurov**, *Recognition of finite simple groups $S_4(q)$ by their element order*, Algebra and Logic **41** (2002), no. 2, 92 – 110.

[19] **Z. Mehranian, A. Gholami and A.R. Ashrafi**, *A note on the power graph of a finite group*, Int. J. Group Theory **5** (2015), 1 – 10.

[20] **M. Mirzargar, A.R. Ashrafi and M.J. Nadjafi-Arani**, *On the power graph of a finite group*, Filomat **26** (2012), 1201 – 1208.

[21] **A.R. Moghaddamfar, S. Rahbariyan and W.J. Shi**, *Certain properties of the power graph associated with a finite group*, J. Algebra Appl. **13** (2014), no. 7, 1450040 (18 pages).

[22] **A.R. Moghaddamfar, S. Rahbariyan, S. Navid Salehy and S. Nima Salehy**, *The number of spanning trees of power graphs associated with specific groups and some applications*, to appear in Ars Combinatoria.

[23] **G.R. Pourgholi, H. Yousefi-Azari and A.R. Ashrafi**, *The undirected power graph of a finite group*, Bull. Malaysian Math. Sci. Soc. **38** (2015), 1517 – 1525.

[24] **W.A. Simpson and S. Frame**, *The character tables for $SL(3,q)$, $SL(3,q^2)$, $PSL(3,q)$, $PSU(3,q^2)$*, Canad. J. Math. **25** (1973), no. 3, 486 – 494.

[25] **B. Srinivasan**, *The characters of the finite symplectic group $Sp(4,q)$*, Trans. Amer. Math. Soc. **131** (1968), no. 2, 488 – 525.

[26] **A.M. Staroletove**, *On recognition by spectrum of the simple groups $B_3(q)$, $C_3(q)$, $D_4(q)$*, Sib. Math. J **53** (2012), no. 3, 532 – 538.

Received December 21, 2014

Department of Pure Mathematics
Faculty of Mathematical Sciences
University of Kashan
Kashan 87317–51167
I. R. Iran
E-mail: ashrafi@kashanu.ac.ir

The Coxeter group $G^{5,5,12}$

Muhammad Ashiq and Tahir Imran

Abstract. The groups $G^{l,m,n}$ are studied extensively by Coxeter. Higman has posed the question that how small l, m, n can be made while maintaining the property that all but finitely many alternating and symmetric groups are quotients of $G^{l,m,n}$. In this paper, by using the coset diagrams, we have proved that for all but finitely many positive integers n either A_n or S_n are quotients of $G^{5,5,12}$.

1. Introduction

The groups $G^{l,m,n}$ are studied by Coxeter. He has defined it as

$$\langle R, S, T : R^l = S^m = T^n = (RS)^2 = (ST)^2 = (TR)^2 = (RST)^2 = 1\rangle$$

in his paper [4] published in 1939. This group can take another presentation

$$\langle x, y, t : x^2 = y^l = t^2 = (xt)^2 = (yt)^2 = (xy)^m = (xyt)^n = 1\rangle$$

by replacing $x = RS$, $y = R$ and $t = ST$. He has revealed that these groups are infinite and insoluble if $\frac{1}{l} + \frac{1}{m} + \frac{1}{m} \leqslant 1$ and are finite or Euclidean triangle group if $\frac{1}{l} + \frac{1}{m} + \frac{1}{m} > 1$, which are soluble. Conder [3] has used coset diagrams to prove the fact that A_n is a Hurwitz group for all $n \geqslant 168$, and for all but 64 integers n in the range $3 \leqslant n \leqslant 167$. He has shown that "all but finitely many positive integers n the alternating group A_n and the symmetric group S_n are homomorphic images of the group $G^{6,6,6}$ having the presentation

$$\langle R, S, T : R^6 = S^6 = T^6 = (RS)^2 = (ST)^2 = (TR)^2 = (RST)^2 = 1\rangle \quad \text{or}$$

$$\langle x, y, t : x^2 = y^6 = t^2 = (xt)^2 = (yt)^2 = (xy)^6 = (xyt)^6 = 1\rangle$$

by replacing $x = RS$, $y = R$ and $t = ST$. As a corollary of the proof it is shown that a similar theorem for the triangle group $\Delta(2, 6, 6)$ is given by the presentation $\langle x, y : x^2 = y^6 = (xy)^6 = 1\rangle$. In [7] it was shown by Q. Mushtaq, M. Ashiq that same result is true for the group $G^{5,5,24}$. It was also explained by Conder [3] that "we lose no generality in assuming that $l \leqslant m \leqslant n$ because $G^{l,m,n}$ is isomorphic to $G^{p,q,r}$ for any rearrangement (p, q, r) of (l, m, n). The

2010 Mathematics Subject Classification: Primary 20F05, Secondary 20G40

Key words and phrases: Coxeter groups, symmetric and alternating groups, coset diagrams, permutation action, imprimitivity.

group $H = \langle x, y : x^2 = y^l = (xy)^m = 1\rangle$ is of index 1 or 2 in $G^{l,m,n} = \langle x, y, t : x^2 = y^l = t^2 = (xt)^2 = (yt)^2 = (xy)^m = (xyt)^n = 1\rangle$ and is isomorphic to $\Delta(2, l, m; q) = \langle x, y, : x^2 = y^l = (xy)^m = (x^{-1}y^{-1}xy)^q = 1\rangle$ where $q = n$ if n is odd and $q = \frac{p}{2}$ if n is even. It was the question asked by Higman that how small the integers l, m, n can be made while maintaining the property that all but finitely many A_n and S_n are factor groups of $G^{l,m,n}$. In many cases $G^{l,m,n}$ is isomorphic to $PSL(2, q)$ or $PGL(2, q)$ for some prime power q, when l, m, n are small. For all values of n, Coxeter [4] has mentioned that: $G^{5,5,m}$ is trivial when $m = 1$ or 2. $G^{5,5,3}$ is homomorphic to $PSL(2, 5)$.

In this paper, we use pictorial argument to show that alternating groups A_n and symmetric groups S_n of degree n can be obtained as quotients of the group $G^{5,5,12} = \langle x, y, t : x^2 = y^5 = t^2 = (xt)^2 = (yt)^2 = (xy)^5 = (xyt)^{12} = 1\rangle$ for all but finitely many positive integers n.

2. Diagrams for $G^{5,5,12}$

To prove our result for the group $G^{5,5,12}$ we will use coset diagrams as used in [3], [6] and [7]. We also need a method for combination of smaller diagrams in order to make large diagrams of desired type. A coset diagram for $G^{5,5,12}$ with n vertices is the action of its generators on the cosets of some particular subgroup in the usual right representation. Generators x, y, t are used to draw the coset diagrams. The coset diagrams, accredited to Higman show an action of $G^{5,5,12} = \langle x, y, t : x^2 = y^5 = t^2 = (xt)^2 = (yt)^2 = (xy)^5 = (xyt)^{12} = 1\rangle$ on a finite set and defined as follows: Pentagons represents cycles of y and vertices of pentagons permuted anti-clockwise by y. An edge denotes those vertices of x which are interchanged by involution while reflection about vertical line of axis represents action of t. A method is also required to connect smaller diagrams to obtain a larger diagram of same condition.

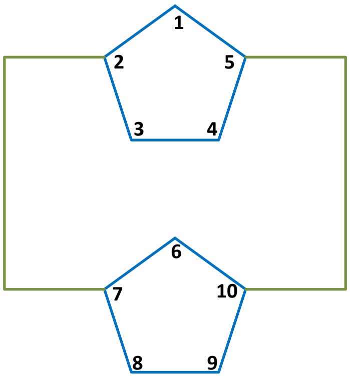


Figure 1: Basic Example

For example, Figure 1 is transitive depiction of $G = \langle x, y, t : x^2 = y^5 = t^2 = (xt)^2 = (yt)^2 = (xy)^5 = 1\rangle$ of degree 10. In this diagram, x act as: (5 6) (2 8) (1) (3) (4) (7) (9) (10); y act as: (1 2 3 4 5) (6 7 8 9 10); t act as: (2 5) (3 4) (6 8) (9 10) (1) (7).

For proof of we will need basic diagrams and portion of a coset diagram for connecting them in different ways and in different numbers. This fragment is known as handle and is denoted as $[A, B]$ as shown in Figure 2 which means a coset diagram containing vertices A and B fixed by x while vertex A is mapped onto B by both y and t and A is fixed by xyt.

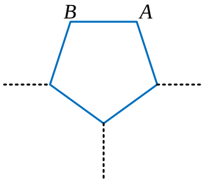


Figure 2: 1-handle

We can combine two coset diagrams namely R and S by placing them one above the other on common vertical axis of symmetry and then by joining them as shown in Figure 3:

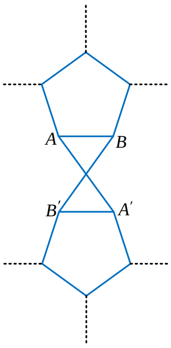


Figure 3: 2-Handle

The diagram thus we get is again a coset diagram for $G^{5,5,12}$ because it satisfies the relation $x^2 = y^5 = t^2 = (xt)^2 = (yt)^2 = 1$. Also, if (A, B, b_1, b_2, b_3) and (A, B, b_1', b_2', b_3') are the suitable 5-cycles of xy then since we have
$(B, B')(A, A')(A, B, b_1, b_2, b_3)(A, B, b_1', b_2', b_3') = (A, B', b_1, b_2, b_3)(A', B, b_1', b_2', b_3')$
the two afterward 5-cycles will be cycles of xy while other cycles remains unaffected in the new diagram. So in resulting diagram xy is of order 5. The cycles ending in A and A' will be juxtaposed to form a single cycle if B and B' will be joined in same way.

3. Jordan's Theorem

Let p be a prime number and G is a primitive group of degree $n = p + k$, $k = 3$. If G contains an element of degree and order p, then G is either alternating or symmetric (Theorem 3.9 [8]).

4. Basic Diagrams

To prove our result, we will need three basic diagrams and fragment of a coset diagram in order to connect them in different ways and in different numbers. Specification is given to each diagram consisting of the degree of the corresponding permutation representation of the group $G^{5,5,12}$, number of handles to be used, parity of action of t and the cycle organization of xyt and xy^2t. Let we have a coset diagram of n vertices denoted by $D(n)$ and here we need copies of three diagrams $D(20), D(21)$ and $D(10)$ for the construction of required diagram of n vertices.

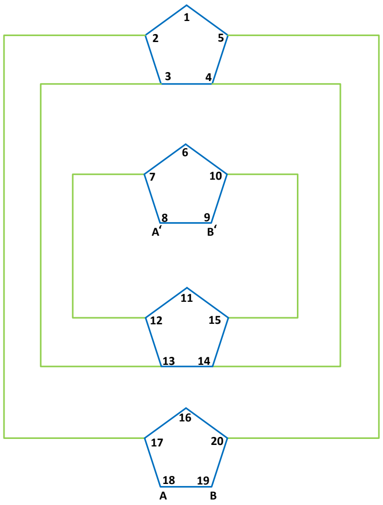


Figure 4: D(20)

Specification of $D(20)$ as in Figure 4: 2(1)-handles: x even, y even, t even. $xyt : AA'(B3B'3)2.4^2$, $xy^2t : (A3A'3)(B1B'1)2^2.4$, which means that on 20 points of the diagram, t is even and xyt has 5 cycles namely two of length 1 corresponding to A and A', one containing both the points B and B' is of length 8, one of length 2 and two of length 4. Similarly xy^2t has five cycles namely one containing points A and A' is of length 8, one of length 2 corresponding to point B, one of length 2 corresponding to point B', two of lengths 2 and one of length 4.

Specification of D(21) as in Figure 5: 1(1)-handle: x even, y even, t even. $xyt : A(B7)2.6.4$, $xy^2t : (A6)(B1)2.5$. which means that on 21 points of the diagram, t is even and xyt has 5 cycles namely one corresponding to A is of length 1, one corresponding to B is having length 8, one of length 2, one of length 4 and one of length 6.

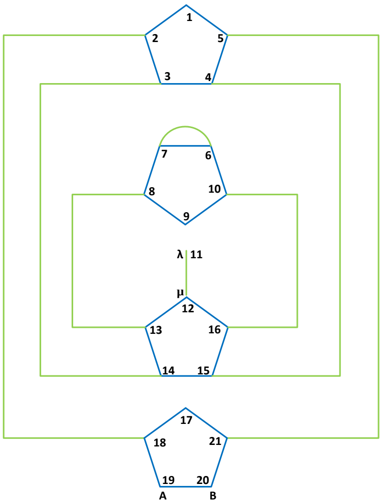


Figure 5: D(21)

Similarly xy^2t has 4 cycles namely one of length 7 containing point A, one of length 2 containing points B two of lengths 5 and one of length 2.

Specification of D(10) as in Figure 6: 2(1)-handles: x even, y even, t even. $xyt : AA'(B1B'1)4$, $xy^2t : (B1)(A1A'1)(B'1).2$.

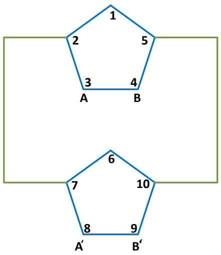


Figure 6: D(10)

Theorem. *For all but finitely many positive integers n, the alternating group A_n and the symmetric group S_n can be obtained as a quotient of the group $G^{5,5,12}$.*

Proof. Take P copies of $D(20)$, Q copies of $D(10)$ and R copies of $D(21)$ and then connect P copies of $D(20)$ with Q copies of $D(10)$ where P, Q are positive integers. Now join R copies of $D(21)$ with $D(10)$ where $R = 1$ or 2. However we cannot connect any copy of $D(21)$ with $D(20)$. The diagram thus obtained will have n vertices and is a coset diagram of group $G^{5,5,12}$. Depending upon the values of P, Q, R reflection t will act as even or odd permutation. The diagram $D(n)$ gives a permutation depiction of group $G^{5,5,12}$ because every cycle of xyt divide 12. Also, we noticed that xy^2t has cycle lengths $2, 4, 5, 7, 8$ with the exception 5, all lengths of xy^2t are divisors of 56, thus the element $(xy^2t)^{56}$ produces exponent of the cycle, fixing the remaining $n-5$ vertices.Now, we have to show that the representation $G^{5,5,12}$ is primitive on the vertices of $D(n)$. By contradiction, suppose that $G^{5,5,12}$ is not primitive then since $(xy^2t)^{12}$ fixes $n-5$ vertices, then 5 vertices of the cycle should lie down in the same area, say Z, of imprimitivety. Amongst the vertices in this cycle are the ones labeled λ and μ . But, x takes λ to μ and μ lies on the vertical line of axis. Thus, Z is conserved by all generators x, y and t. By transitivity it implies that Z has n number of vertices, which is a contradiction to assumption of imprimitivety. Hence, the depiction is primitive. Hence by Jordan's Theorem (Theorem 3.9, [8]), permutation representation is alternating or symmetric of degree n. Thus either A_n or S_n is homomorphic image of $G^{5,5,12}$. Since y and xy is odd order, they yield even permutations and as a result, x will also be even. Depending upon the values of P, Q and R, t is even or odd and in the case t produces an even permutation, we get A_n and if t produces odd permutation, we will get S_n. In either case, A_n is the group $\Delta(2,5,5;6)$ and is of index 2 in the group $G^{5,5,12}$. Hence for all but finitely many positive integers n the alternating group A_n and the symmetric group S_n can be obtained as a quotient of the group $G^{5,5,12}$. □

Corollary. *For all but finitely many positive integers n, the groups A_n and S_n have the presentation $\langle x, y : x^2 = y^5 = (x^{-1}y^{-1}xy)^6 = 1\rangle$.*

References

[1] **W. Burnside**, *Theory of groups of finite order*, Dover publications Inc. (1995).

[2] **A. Cayley**, *The theory of groups: graphical representation*, Amer. J. Math. **1** (1878), 174 – 176.

[3] **M.D.E. Conder**, *On the group $G^{6,6,6}$*, Qurat. J. Math. Oxford **39** (1988), 175 – 183.

[4] **H.S.M. Coxeter**, *The abstract groups $G^{m,n,p}$*, Trans. Amer. Math. Soc. **45** (1939), 73 – 150.

[5] **H.S.M. Coxeter and W.O.J Moser**, *Generators and relations for discrete groups*, Springer-Verlag, Berlin (1980).

[6] **Q. Mushtaq, M. Ashiq and T. Maqsood**, *Factor groups of $G^{5,5,12}$*, Commun. Algebra **12** (1992), 3759 – 3767.

[7] **Q. Mushtaq, M. Ashiq, T. Maqsood and M. Aslam**, *The Coxeter group $G^{5,5,24}$*, Commun. Algebra **30** (2002), 2175 – 2182.

[8] **W.W. Stothers**, *Subgroup of the* $(2,3,7)$ *triangle group*, Manuscripta Math. **20** (1997), 323 – 334.

[9] **H. Wielandt**, *Finite permutation groups*, Academic Press, London (1964).

Received March 15, 2014

M. Ashiq
Department of Mathematics, National University of Sciences and Technology (NUST), MCS Campus, Rawalpindi, Pakistan
E-mail: ashiqjaved@yahoo.co.uk

T. Imran
Riphah International University, Islamabad, Pakistan
E-mail: tahirimran_78@yahoo.com

On generalized bi-Γ-ideals in Γ-semigroups

Abul Basar and Mohammad Yahya Abbasi

Abstract. We study generalized bi-Γ-ideals, prime, semiprime and irreducible generalized bi-Γ-ideals in Γ-semigroups.

1. Introduction

Let S and Γ be two nonempty sets. Then a triple of the form $(S,\Gamma,\cdot)$ is called a Γ-*semigroup*, where $\cdot$ is a ternary operation $S\times\Gamma\times S\to S$ such that $(x\cdot\alpha\cdot y)\cdot\beta\cdot z = x\cdot\alpha\cdot(y\cdot\beta\cdot z)$ for all $x,y,z\in S$ and all $\alpha,\beta\in\Gamma$.

We will denote $(S,\Gamma,\cdot)$ by S and $a\cdot\gamma\cdot b$ by $a\gamma b$.

Definition 1.1. A nonempty subset B of S is called

- a *sub*-Γ-*semigroup* of S if $a\gamma b\in B$, for all $a,b\in B$ and $\gamma\in\Gamma$,
- a *generalized bi*-Γ-*ideal* of S if $B\Gamma S\Gamma B\subseteq B$,
- a *bi*-Γ-*ideal* of S if $B\Gamma S\Gamma B\subseteq B$ and $B\Gamma B\subset B$.

A Γ-semigroup S is called a *gb-simple* if it does not contain the proper generalized bi-Γ-ideal.

Definition 1.2. A generalized bi-Γ-ideal B of a Γ-semigroup S is

- *prime* if $B_1\Gamma B_2\subseteq B$ implies $B_1\subseteq B$ or $B_2\subseteq B$,
- *strongly prime* if $B_1\Gamma B_2\cap B_2\Gamma B_1\subseteq B$ implies $B_1\subseteq B$ or $B_2\subseteq B$,
- *irreducible* if $B_1\cap B_2=B$ implies $B_1=B$ or $B_2=B$,
- *strongly irreducible* if $B_1\cap B_2\subseteq B$ implies $B_1\subseteq B$ or $B_2\subseteq B$

for any generalized bi-Γ-ideals B_1 and B_2 of S.

A quasi Γ-ideal is prime if it is prime as a bi-Γ-ideal.

Definition 1.3. A generalized bi-Γ-ideal B of S is

- *semiprime* if $B_1\Gamma B_1\subseteq B$ implies that $B_1\subseteq B$

for any bi-Γ-ideal B_1 of S.

Other definition one can find in [1] and [2].

2010 Mathematics Subject Classification: 16D25, 20M12
Keywords: Γ-semigroup, prime and irreducible generalized bi-Γ-ideal.

2. Properties of generalized bi-Γ-ideals

Lemma 2.1. *The smallest generalized bi-Γ-ideal of a Γ-semigroup S containing a nonempty subset T of S has the form $T \cup T\Gamma S\Gamma T$*

Proof. Let $B = T \cup T\Gamma S\Gamma T$. Then $T \subseteq B$. So,

$$\begin{aligned} B\Gamma S\Gamma B &= (T \cup T\Gamma S\Gamma T)\Gamma S\Gamma(T \cup T\Gamma S\Gamma T) \\ &\subseteq [T(\Gamma S\Gamma)(T \cup T\Gamma S\Gamma T)] \cup [T\Gamma S\Gamma T(\Gamma S\Gamma)(T \cup T\Gamma S\Gamma T)] \\ &\subseteq [T(\Gamma S\Gamma)T \cup T(\Gamma S\Gamma)T\Gamma S\Gamma T] \cup [T\Gamma S\Gamma T(\Gamma S\Gamma)T \cup T\Gamma S\Gamma T(\Gamma S\Gamma)T\Gamma S\Gamma T] \\ &\subseteq [T\Gamma S\Gamma T \cup T\Gamma S\Gamma T] \cup [T\Gamma S\Gamma T \cup T\Gamma S\Gamma T] \\ &= T\Gamma S\Gamma T \subseteq T \cup T\Gamma S\Gamma T = B. \end{aligned}$$

Hence $B = T \cup T\Gamma S\Gamma T$ is a generalized bi-Γ-ideal of S.

To prove that B is the smallest generalized bi-Γ-ideal of S containing T suppose that G is a generalized bi-Γ-ideal of S containing T. Then $T\Gamma S\Gamma T \subseteq G\Gamma S\Gamma G \subseteq G$. Therefore, $B = T \cup T\Gamma S\Gamma T \subseteq G$. Hence B is the smallest generalized bi-Γ-ideal of S containing T. □

The smallest generalized bi-Γ-ideal of S containing T will be denoted by (T).

Lemma 2.2. *Suppose that A is a sub-Γ-semigroup of a Γ-semigroup S, $s \in S$ and $(s\Gamma A\Gamma s) \cap A \neq \emptyset$. Then $(s\Gamma A\Gamma s) \cap A$ is a generalized bi-Γ-ideal of A.*

Proof. Indeed,

$$\begin{aligned} (s\Gamma A\Gamma s \cap A)\Gamma A\Gamma(s\Gamma A\Gamma s \cap A) &\subseteq [(s\Gamma A\Gamma s)\Gamma A \cap A\Gamma A]\Gamma(s\Gamma A\Gamma s \cap A) \\ &\subseteq [(s\Gamma A\Gamma s)\Gamma A \cap A]\Gamma(s\Gamma A\Gamma s \cap A) \\ &\subseteq [[(s\Gamma A\Gamma s\Gamma A)\Gamma(s\Gamma A\Gamma s)] \cap [A\Gamma(s\Gamma A\Gamma s \cap A)]] \\ &\subseteq [(s\Gamma A\Gamma s) \cap (A\Gamma s\Gamma A\Gamma s)] \cap A \\ &\subseteq (s\Gamma A\Gamma s) \cap A. \end{aligned}$$

Hence $(s\Gamma A\Gamma s) \cap A$ is a generalized bi-Γ-ideal of A. □

Theorem 2.3. *For a Γ-semigroup S the following assertions are equivalent:*

(i) *S is a gb-simple Γ-semigroup,*

(ii) *$s\Gamma S\Gamma s = S$ for all $s \in S$,*

(iii) *$(s) = S$ for all $s \in S$.*

Proof. $(i) \Rightarrow (ii)$. Let S be a gb-simple Γ-semigroup and $s \in S$. Then $s\Gamma S\Gamma s$ is a generalized bi-Γ-ideal of S. As S is a gb-simple Γ-semigroup, $s\Gamma S\Gamma s = S$.

$(ii) \Rightarrow (iii)$. If $s\Gamma S\Gamma s = S$ for all s in S, then, $(s) = \{s\} \cup s\Gamma S\Gamma s = \{s\} \cup S = S$.

$(iii) \Rightarrow (i)$. Let $(s) = S$, for all $s \in S$, and assume B is a generalized bi-Γ-ideal of S and $s \in B$. Then $(s) \subseteq B$. By our hypothesis, we obtain $S = (s) \subseteq B \subseteq S$. So, $S = B$. Hence S is a gb-simple Γ-semigroup. □

Theorem 2.4. *A bi-Γ-ideal B of a Γ-semigroup S is a minimal generalized bi-Γ-ideal of S if and only if B is a gb-simple Γ-semigroup.*

Proof. Let B be a minimal generalized bi-Γ-ideal of S. By our hypothesis, B is a Γ-semigroup. Suppose D is a generalized bi-Γ-ideal of B. Then $D\Gamma B\Gamma D \subseteq D \subseteq B$. As B is a generalized bi-Γ-ideal of S, we obtain $D\Gamma B\Gamma D$ is a generalized bi-Γ-ideal of S. As B is a minimal generalized bi-Γ-ideal of S, we obtain $D\Gamma B\Gamma D = B$. So, we have $B = D$. Therefore, B is a *gb*-simple Γ-semigroup.

Conversely, let B be a *gb*-simple Γ-semigroup. Suppose D is a generalized bi-Γ-ideal of S so that $D \subseteq B$. Then $D\Gamma B\Gamma D \subseteq D\Gamma S\Gamma D \subseteq D$. So D is a generalized bi-Γ-ideal of B. As B is a *gb*-simple Γ-semigroup, we obtain $B = D$. Hence B is a minimal generalized bi-Γ-ideal of S. □

Theorem 2.5. *Every generalized bi-Γ-ideal of a Γ-semigroup S is a bi-Γ-ideal of S if and only if $x\alpha y \in \{x, y\}\Gamma S\Gamma\{x, y\}$, for every $x, y \in S$ and $\alpha \in \Gamma$.*

Proof. Suppose S is a Γ-semigroup in which every generalized bi-Γ-ideal is a bi-Γ-ideal. Then, for every $x, y \in S$, the generalized bi-Γ-ideal generated by subset $\{x, y\}$ is given by $\{x, y\} \cup \{x, y\}\Gamma S\Gamma\{x, y\}$ which is a bi-Γ-ideal of S, so we have $x\alpha y \in \{x, y\}\Gamma S\Gamma\{x, y\}$.

Conversely, if x, y are elements of a generalized bi-Γ-ideal B of S, then we have $x\alpha y \in B\Gamma S\Gamma B \subseteq B$. Hence B is a bi-Γ-ideal of S. □

3. Prime and irreducible generalized bi-Γ-ideals

Proposition 3.1. *A semiprime generalized bi-Γ-ideal of S is a quasi-Γ-ideal of S.*

Proof. Suppose that B is semiprime and let $x \in (S\Gamma B \cap B\Gamma S)$. Then $x\Gamma S\Gamma x \subseteq (B\Gamma S)\Gamma S\Gamma(S\Gamma B) = B\Gamma S\Gamma B \subseteq B$ and since B is semiprime, we obtain $x \in B$. Hence $B = S\Gamma B \cap B\Gamma S$. □

Proposition 3.2. *A Γ-semigroup S is regular if and only if every generalized bi-Γ-ideal of S is semiprime.*

Proof. Let S be regular and suppose that B is any generalized bi-Γ-ideal of S. If $b \notin B$, then $b \in s\Gamma S\Gamma s$, so we obtain $s\Gamma S\Gamma s \nsubseteq B$ and hence B is semiprime. Conversely, if every generalized bi-Γ-ideal of S is semiprime, then so is $B = s\Gamma S\Gamma s$ for any $s \in S$. As $s\Gamma S\Gamma s \subseteq B$, we obtain $b \in B$ and hence S is regular. □

Proposition 3.3. *The intersection of any nonempty family of prime generalized bi-Γ-ideals of a Γ-semigroup is a semiprime bi-Γ-ideal.*

Proof. Suppose that S is a Γ-semigroup and $\mathcal{P} = \{P \mid P$ is a prime generalized bi-Γ-ideal of $S\}$. As $0 \in P$, for all $P \in \mathcal{P}$, we obtain $0 \in \bigcap\mathcal{P}$. Thus $\bigcap\mathcal{P} \neq \emptyset$. Suppose $q \in (\bigcap\mathcal{P})\Gamma S\Gamma(\bigcap\mathcal{P})$. Then $q = q_1\alpha s\beta q_2$, for some $q_1, q_2 \in \bigcap\mathcal{P}$,$s \in S$

and $\alpha, \beta, \gamma \in \Gamma$. Thus $q = q_1 \alpha s \beta q_2 \in P\Gamma S\Gamma P \subseteq P$, for all $P \in \mathcal{P}$. Therefore, $q \in \bigcap \mathcal{P}$. So $(\bigcap \mathcal{P})\Gamma S\Gamma(\bigcap \mathcal{P}) \subseteq \bigcap \mathcal{P}$. Therefore, $\bigcap \mathcal{P}$ is a generalized bi-Γ-ideal of S. Suppose B be a generalized bi-Γ-ideal of S such that $B^2 \subseteq \bigcap \mathcal{P}$. We have $B^2 \subseteq$P, for all $P \in \mathcal{P}$. As P is a prime generalized bi-Γ-ideal of S, we obtain $B \subseteq P$, for all $P \in \mathcal{P}$. Thus $B \subseteq \bigcap \mathcal{P}$. Hence $\bigcap \mathcal{P}$ is a semiprime generalized bi-Γ-ideal of S. □

Proposition 3.4. *A prime generalized bi-Γ-ideal is a prime one-sided Γ-ideal.*

Proof. Let $S\Gamma B \nsubseteq B$ and $B\Gamma S \nsubseteq B$. Since B is prime, it follows that $B\Gamma S\Gamma B = (B\Gamma S)\Gamma S\Gamma(S\Gamma B) \nsubseteq B$, which is a contradiction. Hence B is a prime one-sided Γ-ideal. □

Corollary 3.5. *A quasi-Γ-ideal of S is a prime one-sided Γ-ideal of S.* □

Proposition 3.6. *A generalized bi-Γ-ideal B of a Γ-semigroup S is prime if and only if $R\Gamma L \subseteq B$ implies $R \subseteq B$ or $L \subseteq B$, where R and L are right and left Γ-ideal of S.*

Proof. If B is prime and $R\Gamma L \subseteq B$ with $R \nsubseteq B$, then for every $r \in R \setminus B$, $r\Gamma S\Gamma l \subseteq B$, for all $l \in L$, therefore $L \subseteq B$. Conversely, if B is not prime, there exists $a, b \notin B$ such that $a\Gamma S\Gamma b \subseteq B$. But then $(a\Gamma S)\Gamma(S\Gamma b) \subseteq B$ and $a\Gamma S, S\Gamma b \nsubseteq B$. □

Proposition 3.7. *If a bi-Γ-ideal B of S is prime, then*

$$I(B) = \{s \in B \mid S\Gamma s\Gamma S \subseteq B\}$$

is a prime Γ-ideal of S.

Proof. Suppose B is prime and let $J_1\Gamma J_2 \subseteq I(B)$, for two-sided ideals J_1 and J_2. Then, since $J_1\Gamma J_2 \subseteq B$, by Proposition 3.6, $J_1 \subseteq B$ or $J_2 \subseteq B$. Now $I(B)$ is the largest Γ-ideal in B, it follows that $J_1 \subseteq I(B)$ or $J_2 \subseteq I(B)$. □

Theorem 3.8. *Every strongly irreducible, semiprime generalized bi-Γ-ideal of a Γ-semigroup S is a strongly prime generalized bi-Γ-ideal.*

Proof. Let B be a strongly irreducible semiprime generalized bi-Γ-ideal of S. Suppose that B_1, B_2 are generalized bi-Γ-ideals of S such that $B_1\Gamma B_2 \cap B_2\Gamma B_1 \subseteq B$. As $(B_1 \cap B_2)^2 \subseteq B_1\Gamma B_2$ and $(B_1 \cap B_2)^2 \subseteq B_2\Gamma B_1$, it follows that $(B_1 \cap B_2)^2 \subseteq B_1\Gamma B_2 \cap B_2\Gamma B_1 \subseteq B$. As B is semiprime, we obtain $B_1 \cap B_2 \subseteq B$ and since B is strongly irreducible, we obtain $B_1 \subseteq B$ or $B_2 \subseteq B$. Hence B is a strongly prime generalized bi-Γ-ideal of S. □

Theorem 3.9. *For any generalized bi-Γ-ideal B of a Γ-semigroup S and any $s \in S \setminus B$ there exists an irreducible generalized bi-Γ-ideal J of S such that $B \subseteq J$ and $s \notin J$.*

Proof. Suppose $GB_B = \{B_1 \mid B_1$ is a generalized bi-Γ-ideal of S and $B \subseteq B_1$ and $s \notin B_1\}$. Obviously, $B \in GB_B$ and so $GB_B \neq \emptyset$. We have GB_B is a partially ordered set under inclusion. Suppose C is a chain of GB_B. Suppose $c \in (\bigcup C)\Gamma S\Gamma(\bigcup C)$. Then $c = c^{'}\alpha s\beta c^{''}$, for some $c^{'}, c^{''} \in \bigcup C$, $s \in S$ and $\alpha, \beta \in \Gamma$. Therefore, $c^{'} \in B_1$ and $c^{''} \in B_2$, for some $B_1, B_2 \in C$. As C is a chain of GB_B, we obtain B_1 and B_2 are comparable. Thus $B_1 \subseteq B_2$ or $B_2 \subseteq B_1$; so $c^{'}, c^{''} \in B_1$ or $c^{'}, c^{''} \in B_2$. As B_1 and B_2 are generalized bi-Γ-ideals of S, it follows that $c = c^{'}\alpha s\beta c^{''} \in B_1\Gamma S\Gamma B_1 \subseteq B_1 \subseteq \bigcup C$ or $c = c^{'}\alpha s\beta c^{''} \in B_2\Gamma S\Gamma B_2 \subseteq B_2 \subseteq \bigcup C$. Therefore, $c \in \bigcup C$, so $\bigcup C$ is a generalized bi-Γ-ideal of S. As $s \notin C$, for all $c \in C$, we obtain $s \notin \bigcup C$. Obviously, $B \subseteq \bigcup C$. Therefore, $\bigcup C \in GB_B$. We have $C \subseteq \bigcup C$, for any $c \in C$. Therefore $\bigcup C$ is an upper bound C in GB_B. By Zorn's Lemma, there exists a maximal element $J \in GB_B$. Therefore, J is a generalized bi-Γ-ideal of S such that $B \subseteq J$ and $b \notin J$. Suppose P and Q are generalized bi-Γ-ideals of S such that $P \cap Q = J$. Let $P \neq J$ and $Q \neq J$. Then $J = P \cap Q \subseteq P$ and $J = P \cap Q \subseteq Q$. So $B \subseteq J \subset P$ and $B \subseteq J \subset Q$. If $s \notin P$, then $C \in GB_B$. This is a contradiction since J is a maximal element of GB_B, therefore $s \in P$. In a similar fashion, we obtain $s \in Q$. Thus $s \in P \cap Q = J$ which is not possible. Therefore, $P = J$ or $Q = J$. Hence J is an irreducible generalized bi-Γ-ideal. □

Theorem 3.10. *For a Γ-semigroup S the following statements are equivalent:*

(*i*) *S is regular and intra-regular Γ-semigroup.*

(*ii*) *$B\Gamma B = B$ for every generalized bi-Γ-ideal B of S.*

(*iii*) *$B_1 \cap B_2 = B_1\Gamma B_2 \cap B_2\Gamma B_1$ for all generalized bi-Γ-ideals B_1 and B_2 of S.*

(*iv*) *Every generalized bi-Γ-ideal of S is semiprime.*

(*v*) *Every proper generalized bi-Γ-ideal B of S is the intersection of irreducible semiprime generalized bi-Γ-ideals of S containing B.*

Proof. It follows by Theorem 3.9 [3]. □

Theorem 3.11. *A generalized bi-Γ-ideal of a regular and intra-regular Γ-semigroup is strongly irreducible if and only if it is strongly prime.*

Proof. Follows by Proposition 3.10 [3]. □

Theorem 3.12. *In a Γ-semigroup S each generalized bi-Γ-ideal is strongly prime if and only if S is regular, intra-regular and the set of generalized bi-Γ-ideals of S is a totally ordered under inclusion.*

Proof. If each generalized bi-Γ-ideal of S be strongly prime, then each generalized bi-Γ-ideal of S is semiprime. Hence, by Theorem 3.10, S is a regular and intra-regular Γ-semigroup. Thus the set of all its generalized bi-Γ-ideals is partially ordered by inclusion. If B_1 and B_2 are generalized bi-Γ-ideals of S, then $B_1 \cap B_2 = B_1\Gamma B_2 \cap B_2\Gamma B_1$, by Theorem 3.10. As $B_1 \cap B_2$ is a strongly prime generalized bi-Γ-ideal, we obtain $B_1 \subseteq B_1 \cap B_2$ or $B_2 \subseteq B_1 \cap B_2$. If $B_1 \subseteq B_1 \cap B_2$, then $B_1 \subseteq B_2$.

If $B_2 \subseteq B_1 \cap B_2$, then $B_2 \subseteq B_1$. Thus the set of all generalized bi-Γ-ideals of S is totally ordered by inclusion.

The converse statement is a consequence of Theorem 3.12 in [3]. □

Theorem 3.13. *If the set of all generalized bi-Γ-ideals of a Γ-semigroup S is a totally ordered by inclusion, then S is both regular and intra-regular if and only if each generalized bi-Γ-ideal of S is prime.*

Proof. By Theorem 3.13 in [3], each generalized bi-Γ-ideal of S is prime.

Conversely, if each generalized bi-Γ-ideal of S is prime, then it is semiprime. Theorem 3.10 completes the proof. □

Theorem 3.14. *For a Γ-semigroup S the following statements are equivalent:*

(i) *The set of all generalized bi-Γ-ideals of S is totally ordered by inclusion.*

(ii) *Every generalized bi-Γ-ideal of S is strongly irreducible.*

(iii) *Every generalized bi-Γ-ideal of S is irreducible.*

Proof. $(i) \Rightarrow (ii)$. Let B, B_1, B_2 be generalized bi-Γ-ideals of S such that $B_1 \cap B_2 \subseteq B$. Then by (i) we obtain $B_1 \subseteq B_2$ or $B_2 \subseteq B_1$. Therefore $B_1 = B_1 \cap B_2 \subseteq B$ or $B_2 = B_1 \cap B_2 \subseteq B$. Hence S is strongly irreducible.

$(ii) \Rightarrow (iii)$. Let B_1, B_2 be generalized bi-Γ-ideals of S such that $B_1 \cap B_2 = B$ for some strongly irreducible generalized bi-Γ-ideal B. Then $B \subseteq B_1$ and $B \subseteq B_2$. By the hypothesis, we obtain $B_1 \subseteq B$ or $B_2 \subseteq B$. So $B_1 = B$ or $B_2 = B$. Hence B is irreducible.

$(iii) \Rightarrow (i)$. Suppose that B_1, B_2 are generalized bi-Γ-ideals of S. Then $B_1 \cap B_2$ also is a generalized bi-Γ-ideal of S and by the assumption, $B_1 = B_1 \cap B_2 \subseteq B_2$ or $B_2 = B_1 \cap B_2 \subseteq B_1$. Therefore $B_1 \subseteq B_2$ or $B_2 \subseteq B_1$. This proves (i). □

References

[1] **R. Chinram**, *On quasi-gamma-ideals in gamma-semigroups*, Science Asia **32** (2006), 351 – 353.

[2] **A. Iampan**, *Note on bi-ideals in Γ-semigroups*, Int. J. Algebra Comput. **3**(4) (2009), 181 – 188.

[3] **M. Shabir and S. Ali**, *Prime bi-ideals of Γ-semigroups*, J. Adv. Research Pure Math. **4** (2012), 757 – 764.

Received October 20, 2014
Revised March 8, 2015

Department of Mathematics, Jamia Millia Islamia, New Delhi-110 025, India
E-mail: basar.jmi@gmail.com, yahya_alig@yahoo.co.in

Finite 2-generated entropic quasigroups with a quasi-identity

Grzegorz Bińczak and *Joanna Kaleta*

Abstract. We describe all 2-generated entropic quasigroups with a quasi-identity.

1. Introduction

Entropic quasigroups with a quasi-identity are term equivalent to abelian groups with involution (i.e., every fundamental operation of abelian groups with involution is the composition of fundamental operations of corresponding entropic quasigroup with a quasi-identity and conversely).

Obviously every finite abelian group with involution is isomorphic to a finite product of directly indecomposable finite abelian groups with involution. This decomposition is unique up to reindexing and isomorphism of factors (cf. [6], Theorem 6.39).

Hence to obtain structural theorem describing finite abelian groups with involution it remains to find all finite directly indecomposable abelian groups with involution.

We have already described (in [2]) directly indecomposable finite one-generator abelian groups with involution.

There exists an infinite family of non-isomorphic two-generated abelian groups with involution which are directly indecomposable (see [3]). Exact describtion of finite abelian groups with involution by indecomposable finite abelian groups with involution is difficult.

In this paper we propose another method. First we give some fundamental definitions and facts. Next, we prove several technical results which will be used later. In the main theorems we characterize finite two-generated abelian groups with involution and finite two-generated quasigroups with a quasi-identity.

Finally using the equivalence between abelian groups with involution and entropic quasigroup with a quasi-identity we obtain characterization of 2-generated finite entropic quasigroups with a quasi-identity .

2010 Mathematics Subject Classification: 20N05.

Keywords: quasigroup, entropic quasigroup, abelian group, involution.

Research supported by the Warsaw University of Technology under grant number 504G/1120/0054/000.

Definition 1.1. An abelian group $(G, +, -, 0)$ is called an *abelian group with involution* if there is an unary operation $^*\colon G \to G$ such that

$$\forall a, b \in G \quad 0^* = 0,\ a^{**} = a,\ (a+b)^* = a^* + b^*.$$

We denote the variety of all abelian groups with involution by AGI.

Definition 1.2. An algebra $(Q, \cdot, /, \backslash, 1)$ is an *entropic quasigroup with a quasi-identity* if it satisfies the following axioms:

(1) $a \cdot (a \backslash b) = b, \quad (b/a) \cdot a = b,$

(2) $a \backslash (a \cdot b) = b, \quad (b \cdot a)/a = b,$

(3) $(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d),$

(4) $a \cdot 1 = a, \quad 1 \cdot (1 \cdot a) = a.$

One-generated entropic quasigroups with a quasi-identity are called *monogenic* or *cyclic*.

Let us observe that the identities (1), (2) and (3) define entropic quasigroups, whereas the identities (4) define the quasi-identity. We denote the variety of all entropic quasigroups with a quasi-identity by EQ1.

More information on entropic quasigroups may be found in [4], [5], [7] and [8]. In the paper [1], it is proved that abelian groups with involution are equivalent (in the sense of Theorems: 1.3 – 1.6) to entropic quasigroups with a quasi-identity.

Theorem 1.3. *If $\mathcal{G} = (G, +, -, 0, ^*)$ is an abelian group with involution, then $\Psi(\mathcal{G}) = (G, \cdot, /, \backslash, 1)$ is an entropic quasigroup with a quasi-identity, where $a \cdot b := a + (b^*)$, $a \backslash b := b^* + (-a^*)$, $a/b := a + (-b^*)$, $1 := 0$.*

Theorem 1.4. *If $\mathcal{Q} =(Q, \cdot, /, \backslash, 1)$ is an entropic quasigroup with a quasi-identity, then $\Phi(\mathcal{Q}) = (Q, +, -, 0, ^*)$ is an abelian group with involution, where $a + b := a \cdot (1 \cdot b)$, $(-a) := 1/(1 \cdot a)$, $0 := 1$, $a^* := 1 \cdot a$.*

Theorem 1.5. *If $\mathcal{Q} =(Q, \cdot, /, \backslash, 1)$ is an entropic quasigroup with a quasi-identity, then $\Psi(\Phi(\mathcal{Q})) = \mathcal{Q}$.*

Theorem 1.6. *If $\mathcal{G} = (G, +, -, 0, ^*)$ is an abelian group with involution, then $\Phi(\Psi(\mathcal{G})) = \mathcal{G}$.*

Let $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ be a monogenic entropic quasigroup with a quasi-identity. Let $Q = \langle x \rangle$ and let $\Phi(\mathcal{Q}) = (Q, +, -, 0, ^*)$ be the abelian group with involution equivalent to $(Q, \cdot, /, \backslash, 1)$.

We will consider three types of *rank* of the generator x:

$r_+(x) = \min\{n \in \mathbb{N} \mid nx = 0,\ n \geqslant 1\}$, (additive rank)

$r_*(x) = \min\{n \in \mathbb{N} \mid n \geqslant 1,\ \exists k \in \mathbb{Z}\ nx^* = kx\}$,

$$r_{*+}(x) = \min\{n \in \mathbb{N} \mid r_*(x)x^* = (r_*(x)+n)x\}.$$

Then we define

$$r_+(\mathcal{Q}) = r_+(x), \quad r_*(\mathcal{Q}) = r_*(x), \quad r_{*+}(\mathcal{Q}) = r_{*+}(x).$$

This definition does not depend on the choice of the generator x (see [1]).

Theorem 1.7. (cf. [1]) *If $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ is a finite monogenic entropic quasigroup with a quasi-identity, then:*

(*a*) *$r_*(\mathcal{Q})$ is a divisor of $r_+(\mathcal{Q})$,*

(*b*) *$r_*(\mathcal{Q})$ is a divisor of $r_{*+}(\mathcal{Q})$,*

(*c*) *$0 \leqslant r_{*+}(\mathcal{Q}) < r_+(\mathcal{Q})$,*

(*d*) *$r_+(\mathcal{Q})$ is a divisor of $2r_{*+}(\mathcal{Q}) + \frac{r_{*+}(\mathcal{Q})^2}{r_*(\mathcal{Q})}$.*

Proposition 1.8. (cf. [1]) *Let $\mathcal{Q}$ =$(Q, \cdot, /.\backslash, 1)$ be a finite cyclic entropic quasigroup with a quasi-identity and $Q = \langle a \rangle$ for some $a \in Q$. If $c \in Z$ then $ca = 0 \Leftrightarrow r_+(Q)|c$.*

Let $E(a)$ be the integer part of a, $(a)_b$ – the remainder obtained after dividing a by b, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.

Proposition 1.9. (cf. [1]) *Let $b, t, y \in \mathbb{Z}$ and $b \geq 1$. Then*

$$E\left(\frac{t}{b}\right) + E\left(\frac{y+(t)_b}{b}\right) = E\left(\frac{y+t}{b}\right), \tag{1}$$

$$\left(y + (t)_b\right)_b = (y+t)_b \ . \tag{2}$$

2. Auxiliary results

Abelian groups with involution generated by x can be described by three ranks: $r_+(x)$, $r_*(x)$ and $r_{*+}(x)$ (cf. [1]). Abelian groups with involution generated by two elements x_1, x_2 will be described by ten ranks defined below.

Definition 2.1. Let $\mathcal{Q} = (Q, \cdot, /, \backslash, 1) = \langle x_1, x_2 \rangle$ be a 2-generated finite entropic quasigroup with a quasi-identity. Let $A = \Phi(\mathcal{Q})$. Let
$a_1 = \min\{n \in \mathbb{N} \setminus \{0\} \,|\, nx_1 \in \langle x_2 \rangle\}$,
$b_1 = \min\{n \in \mathbb{N} \setminus \{0\} \,|\, \exists m \in \mathbb{Z} \quad nx_1^* - mx_1 \in \langle x_2 \rangle\}$,
$k_1 = \min\{n \in \mathbb{N} \cup \{0\} \,|\, b_1 x_1^* - (b_1+n)x_1 \in \langle x_2 \rangle\}$,
$a_2 = \min\{n \in \mathbb{N} \setminus \{0\} \,|\, nx_2 = 0\}$,
$b_2 = \min\{n \in \mathbb{N} \setminus \{0\} \,|\, \exists k \in \mathbb{Z} \quad nx_2^* - kx_2 = 0\}$,
$k_2 = \min\{n \in \mathbb{N} \cup \{0\} \,|\, b_2 x_2^* - (b_2+n)x_2 = 0\}$.

Then there exist $a_{12}, a'_{12} \in \mathbb{Z}_{a_2}$, $b_{12}, b'_{12} \in \mathbb{Z}_{b_2}$ such that

$$a_1 x_1 = a_{12} x_2 + b_{12} x_2^* \in \langle x_2 \rangle, \quad b_1 x_1^* - (b_1 + k_1) x_1 = a'_{12} x_2 + b'_{12} x_2^* \in \langle x_2 \rangle.$$

So, to every finite entropic quasigroup with a quasi-identity generated by x_1, x_2 we assign ten parameters:

$$\psi(A, x_1, x_2) = (a_1, b_1, k_1, a_{12}, b_{12}, a'_{12}, b'_{12}, a_2, b_2, k_2) \in \mathbb{Z}^{10}.$$

Example 2.2. Let $n, m \in \mathbb{Z}$, $m > 1$ and $n \geqslant 1$ be fixed. Consider $W_{n,m} = (\mathbb{Z}_{2^m} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^n}, +, -, (0,0,0), ^*)$, where

$$(y_1, y_2, y_3) + (y'_1, y'_2, y'_3) = ((y_1 + y'_1 + E(\tfrac{y_2 + y'_2}{2})2)_{2^m}, (y_2 + y'_2)_2, (y_3 + y'_3)_{2^n}),$$

$$-(y_1, y_2, y_3) = ((-y_1 + E(\tfrac{-y_2}{2})2)_{2^m}, (-y_2)_2, (-y_3)_{2^n}),$$

$$(y_1, y_2, y_3)^* = \begin{cases} ((y_2 + E(\frac{y_1}{2})2)_{2^m}, (y_1)_2, y_3) & for \quad 2 | y_3, \\ ((y_2 + 2^{m-1} + E(\frac{y_1}{2})2)_{2^m}, (y_1)_2, y_3) & for \quad 2 \nmid y_3. \end{cases}$$

Then, by Theorem 9 in [3], $W_{n,m} = \langle x_1, x_2 \rangle = W_{n,(2^{m-1},0)}(Q^0_{2^m,2}) \in AGI$, where $x_1 = (1,0,0)$, $x_2 = (0,0,1)$. So $x_1^* = (0,1,0)$, $x_2^* = (2^{m-1}, 0, 1)$ and

- $2^{m-1} x_1 = (2^n - 1) x_2 + x_2^*$,
- $2 x_1^* = 0$,
- $2^n x_2 = 0$,
- $2 x_2^* - 2 x_2 = 0$.

Thus $a_1 = 2^{m-1}$, $b_1 = 2$, $k_1 = 0$, $a_{12} = 2^n - 1$, $b_{12} = 1$, $a'_{12} = 0$, $b'_{12} = 0$, $a_2 = 2^n$, $b_2 = 2, k_2 = 0$. □

Definition 2.3. For $t = (a_1, b_1, k_1, a_{12}, b_{12}, , a'_{12}, b'_{12}, a_2, b_2, k_2) \in \mathbb{Z}^{10}$ let γ_t be the function $\mathbb{Z}^4 \to \mathbb{Z}_{a_1} \times \mathbb{Z}_{b_1} \times \mathbb{Z}_{a_2} \times \mathbb{Z}_{b_2}$ such that

$$\pi_1(\gamma_t(y)) = (\pi_1(y) + E(\tfrac{\pi_2(y)}{b_1})(b_1 + k_1))_{a_1} ,$$

$$\pi_2(\gamma_t(y)) = (\pi_2(y))_{b_1} ,$$

$$\pi_3(\gamma_t(y)) = (\pi_3(y) + E(\tfrac{\pi_2(y)}{b_1}) a'_{12} + \alpha a_{12} + E\left(\frac{\pi_4(y) + E(\frac{\pi_2(y)}{b_1}) b'_{12} + \alpha b_{12}}{b_2}\right)(b_2 + k_2))_{a_2} ,$$

$$\pi_4(\gamma_t(y)) = \left(\pi_4(y) + E(\tfrac{\pi_2(y)}{b_1}) b'_{12} + \alpha b_{12}\right)_{b_2}$$

for every $y \in \mathbb{Z}^4$, where $\alpha = E\left(\frac{\pi_1(y) + E(\frac{\pi_2(y)}{b_1})(b_1 + k_1)}{a_1}\right)$ and $\pi_i(y_1, y_2, y_3, y_4) = y_i$ for $i = 1, 2, 3, 4$ and $(y_1, y_2, y_3, y_4) \in \mathbb{Z}^4$.

Definition 2.4. For $t = (a_1, b_1, k_1, a_{12}, b_{12}, a'_{12}, b'_{12}, a_2, b_2, k_2) \in \mathbb{Z}^{10}$ we define $Q_t = (\mathbb{Z}_{a_1} \times \mathbb{Z}_{b_1} \times \mathbb{Z}_{a_2} \times \mathbb{Z}_{b_2}, +_t, -_t, \underline{0}, ^{*_t})$, and

- $(y_1, y_2, y_3, y_4) +_t (z_1, z_2, z_3, z_4) = \gamma_t(y_1 + z_1, y_2 + z_2, y_3 + z_3, y_4 + z_4)$,
- $-_t(y_1, y_2, y_3, y_4) = \gamma_t(-y_1, -y_2, -y_3, -y_4)$, $\quad \underline{0} = (0, 0, 0, 0)$,
- $(y_1, y_2, y_3, y_4)^* = (y_2, y_1, y_4, y_3)$,
- $(y_1, y_2, y_3, y_4)^{*_t} = \gamma_t(y_2, y_1, y_4, y_3)$, i.e., $y^{*_t} = \gamma_t(y^*)$.

Definition 2.5. Let D be the set of tuples $(a_1, b_1, k_1, a_{12}, b_{12}, a'_{12}, b'_{12}, a_2, b_2, k_2)$ such that:

$$b_1|a_1,\ b_1|k_1,\ a_1|\Big(2k_1 + \tfrac{k_1^2}{b_1}\Big),\ a_1 \geqslant 1,\ b_1 \geqslant 1,\ 0 \leqslant k_1 < a_1,$$
$$b_2|a_2,\ b_2|k_2,\ a_2|\Big(2k_2 + \tfrac{k_2^2}{b_2}\Big),\ a_2 \geqslant 1,\ b_2 \geqslant 1,\ 0 \leqslant k_2 < a_2,$$
$$b_2|\Big(a_{12} - (1 + \tfrac{k_1}{b_1})b_{12} - \tfrac{a_1}{b_1}b'_{12}\Big), \quad b_2|\Big(a'_{12} + (1 + \tfrac{k_1}{b_1})b'_{12} + \tfrac{2k_1 + \frac{k_1^2}{b_1}}{a_1}b_{12}\Big),$$
$$a_2|\Big(b_{12} - (1 + \tfrac{k_1}{b_1}))a_{12} - \tfrac{a_1}{b_1}a'_{12} + (1 + \tfrac{k_2}{b_2})(a_{12} - (1 + \tfrac{k_1}{b_1})b_{12} - \tfrac{a_1}{b_1}b'_{12}\Big),$$
$$a_2|\Big(b'_{12} + (1 + \tfrac{k_1}{b_1}))a'_{12} + \tfrac{2k_1 + \frac{k_1^2}{b_1}}{a_1}a_{12} + (1 + \tfrac{k_2}{b_2})(a'_{12} + (1 + \tfrac{k_1}{b_1})b'_{12} + \tfrac{2k_1 + \frac{k_1^2}{b_1}}{a_1}b_{12}\Big),$$
$$a_{12}, a'_{12} \in \mathbb{Z}_{a_2}, b_{12}, b'_{12} \in \mathbb{Z}_{b_2}.$$

Lemma 2.6. *If $G = \langle x \rangle$ is a finite abelian group with involution, $a = r_+(\langle x \rangle)$, $b = r_*(\langle x \rangle)$, $k = r_{*+}(\langle x \rangle)$, $m, n \in \mathbb{Z}$ and $mx + nx^* = 0$, then $b|n$ and $a|m + (1 + \frac{k}{b})n$.*

Proof. If $mx + nx^* = 0$, then $mx + (E(\frac{n}{b})b + (n)_b)x^* = 0$. Thus we have $(n)_b x^* = (-m - E(\frac{n}{b})b)x$ and $0 \leqslant (n)_b < b$. By definition of b we obtain $(n)_b = 0$ so $b|n$.

Moreover, $mx = -nx^* = -\frac{n}{b}bx^* = -n\frac{n}{b}(b + k)x$, so $(m + \frac{n}{b}(b + k))x = 0$ and by Proposition 1.8 we have $a|(m + \frac{n}{b}(b + k))$. Thus $a|m + (1 + \frac{k}{b})n$. □

Proposition 2.7. *If $G = \langle x_1, x_2 \rangle$ is a finite abelian group with involution, then $t = \psi(G, x_1, x_2) \in D$.*

Proof. Let $G = \langle x_1, x_2 \rangle$ be a finite abelian group with involution and $t = \psi(G, x_1, x_2) = (a_1, b_1, k_1, a_{12}, b_{12}, a'_{12}, b'_{12}, a_2, b_2, k_2)$. Then $a_2 = r_+(\langle x_2 \rangle)$, $b_2 = r_*(\langle x_2 \rangle)$ and $k_2 = r_{*+}(\langle x_2 \rangle)$, $a_1 = r_+(G/\langle x_2 \rangle)$, $b_1 = r_*(G/\langle x_2 \rangle)$, $k_1 = r_{*+}(G/\langle x_2 \rangle)$.

By Theorem 1.7 we have $b_1|a_1,\ b_1|k_1,\ a_1|(2k_1 + \frac{k_1^2}{b_1}),\ a_1 \geqslant 1,\ b_1 \geqslant 1,\ 0 \leqslant k_1 < a_1,$ $b_2|a_2,\ b_2|k_2,\ a_2|(2k_2 + \frac{k_2^2}{b_2}),\ a_2 \geqslant 1,\ b_2 \geqslant 1,\ 0 \leqslant k_2 < a_2.$

Now we prove that

$$b_2|(a'_{12} + (1 + \tfrac{k_1}{b_1})b'_{12} + \tfrac{2k_1 + \frac{k_1^2}{b_1}}{a_1}b_{12}) \text{ and}$$
$$a_2|(b'_{12} + (1 + \tfrac{k_1}{b_1}))a'_{12} + \tfrac{2k_1 + \frac{k_1^2}{b_1}}{a_1}a_{12} + (1 + \tfrac{k_2}{b_2})(a'_{12} + (1 + \tfrac{k_1}{b_1})b'_{12} + \tfrac{2k_1 + \frac{k_1^2}{b_1}}{a_1}b_{12}).$$

By definition of t we obtain

$$a_1 x_1 = a_{12}x_2 + b_{12}x_2^* \in \langle x_2 \rangle, \tag{3}$$

$$b_1x_1^* - (b_1+k_1)x_1 = a'_{12}x_2 + b'_{12}x_2^* \in \langle x_2\rangle. \tag{4}$$

So, $(b_1+k_1)x_1^* = (1+\frac{k_1}{b_1})b_1x_1^* \overset{(4)}{=} (1+\frac{k_1}{b_1})((b_1+k_1)x_1 + a'_{12}x_2 + b'_{12}x_2^*)$ and $(b_1+k_1)x_1^* = ((b_1+k_1)x_1)^* \overset{(4)}{=} (b_1x_1^* - a'_{12}x_2 - b'_{12}x_2^*)^* = b_1x_1 - a'_{12}x_2^* - b'_{12}x_2$. Hence $0 = ((1+\frac{k_1}{b_1})(b_1+k_1)-b_1)x_1 + (b'_{12}+(1+\frac{k_1}{b_1})a'_{12})x_2 + (a'_{12}+(1+\frac{k_1}{b_1})b'_{12})x_2^*$ and $((1+\frac{k_1}{b_1})(b_1+k_1)-b_1)x_1 = (2k_1+\frac{k_1^2}{b_1})x_1 = \frac{2k_1+\frac{k_1^2}{b_1}}{a_1}a_1x_1 \overset{(3)}{=} \frac{2k_1+\frac{k_1^2}{b_1}}{a_1}(a_{12}x_2+b_{12}x_2^*)$. So, $0 = (b'_{12}+(1+\frac{k_1}{b_1})a'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}a_{12})x_2 + (a'_{12}+(1+\frac{k_1}{b_1})b'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12})x_2^*$.

From this, applying Lemma 2.6, we obtain $b_2|(a'_{12}+(1+\frac{k_1}{b_1})b'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12})$ and $a_2|(b'_{12}+(1+\frac{k_1}{b_1}))a'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}a_{12}+(1+\frac{k_2}{b_2})(a'_{12}+(1+\frac{k_1}{b_1})b'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12})$.

Now we prove that $b_2|(a_{12}-(1+\frac{k_1}{b_1})b_{12}-\frac{a_1}{b_1}b'_{12})$ and $a_2|(b_{12}-(1+\frac{k_1}{b_1}))a_{12}-\frac{a_1}{b_1}a'_{12}+(1+\frac{k_2}{b_2})(a_{12}-(1+\frac{k_1}{b_1})b_{12}-\frac{a_1}{b_1}b'_{12})$.

Let us observe that $a_{12}x_2^*+b_{12}x_2 = (a_{12}x_2+b_{12}x_2^*)^* \overset{(3)}{=} a_1x_1^* = \frac{a_1}{b_1}b_1x_1^* \overset{(4)}{=} \frac{a_1}{b_1}((b_1+k_1)x_1+a'_{12}x_2+b'_{12}x_2^*) = (1+\frac{k_1}{b_1})a_1x_1+\frac{a_1}{b_1}a'_{12}x_2+\frac{a_1}{b_1}b'_{12}x_2^* \overset{(3)}{=} (1+\frac{k_1}{b_1})(a_{12}x_2+b_{12}x_2^*)+\frac{a_1}{b_1}a'_{12}x_2+\frac{a_1}{b_1}b'_{12}x_2^*$.

Thus $0 = (b_{12}-(1+\frac{k_1}{b_1})a_{12}-\frac{a_1}{b_1}a'_{12})x_2+(a_{12}-(1+\frac{k_1}{b_1})b_{12}-\frac{a_1}{b_1}b'_{12})x_2^*$.

After applying Lemma 2.6 we conclude that $b_2|(a_{12}-(1+\frac{k_1}{b_1})b_{12}-\frac{a_1}{b_1}b'_{12})$ and $a_2|(b_{12}-(1+\frac{k_1}{b_1}))a_{12}-\frac{a_1}{b_1}a'_{12}+(1+\frac{k_2}{b_2})(a_{12}-(1+\frac{k_1}{b_1})b_{12}-\frac{a_1}{b_1}b'_{12})$. □

The following two lemmas and proposition serve as technical help to prove the Theorem 3.1.

Lemma 2.8. *If $t = (a_1,b_1,k_1,a_{12},b_{12},a'_{12},b'_{12},a_2,b_2,k_2) \in D$, $x,y \in \mathbb{Z}^4$, then*

$$\gamma_t(x+y) = \gamma_t(x+\gamma_t(y)). \tag{5}$$

If $x \in \mathbb{Z}_{a_1}\times\mathbb{Z}_{b_1}\times\mathbb{Z}_{a_2}\times\mathbb{Z}_{b_2}$, then

$$\gamma_t(x) = x. \tag{6}$$

Proof. Let $t = (a_1,b_1,k_1,a_{12},b_{12},a'_{12},b'_{12},a_2,b_2,k_2) \in D$, $x,y \in \mathbb{Z}^4$. We show that $\pi_i(\gamma_t(x+\gamma_t(y))) = \pi_i(\gamma_t(x+y))$ for $i = 1,2,3,4$.

We have

- $\pi_1(\gamma_t(x+\gamma_t(y))) = (\pi_1(x+\gamma_t(y))+E(\frac{\pi_2(x+\gamma_t(y))}{b_1})(b_1+k_1))_{a_1}$
  $= (\pi_1(x)+\pi_1(\gamma_t(y))+E(\frac{\pi_2(x)+\pi_2(\gamma_t(y))}{b_1})(b_1+k_1))_{a_1}$
  $= (\pi_1(x)+(\pi_1(y)+E(\frac{\pi_2(y)}{b_1})(b_1+k_1))_{a_1}+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})(b_1+k_1))_{a_1}$
  $\overset{(1),(2)}{=} (\pi_1(x)+\pi_1(y)+E(\frac{\pi_2(y)}{b_1})(b_1+k_1)+(E(\frac{\pi_2(x)+\pi_2(y)}{b_1})-E(\frac{\pi_2(y)}{b_1}))(b_1+k_1))_{a_1}$
  $= (\pi_1(x)+\pi_1(y)+(E(\frac{\pi_2(x)+\pi_2(y)}{b_1}))_{a_1} = \pi_1(\gamma_t(x+y))$,

- $$\begin{aligned}\pi_2(\gamma_t(x+\gamma_t(y)) &= (\pi_2(x+\gamma_t(y)))_{b_1} = (\pi_2(x)+\pi_2(\gamma_t(y)))_{b_1} \\ &= (\pi_2(x)+(\pi_2(y)_{b_1}))_{b_1} \overset{(2)}{=} (\pi_2(x)+\pi_2(y))_{b_1} = \pi_2(\gamma_t(x+y)).\end{aligned}$$

- Let us introduce the following abbreviations:

$$\begin{aligned}
\alpha_1 &= \pi_1(y) + E(\tfrac{\pi_2(y)}{b_1})(b_1+k_1),\\
\alpha_2 &= E\left(\frac{\pi_1(x+\gamma_t(y))+E(\frac{\pi_2(x+\gamma_t(y))}{b_1})(b_1+k_1)}{a_1}\right)\\
&= E\left(\frac{\pi_1(x)+(\alpha_1)_{a_1}+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})(b_1+k_1)}{a_1}\right),\\
\alpha_3 &= \pi_4(y) + E(\tfrac{\pi_2(y)}{b_1})b'_{12} + E(\tfrac{\alpha_1}{a_1})b_{12},\\
\alpha_4 &= E\left(\frac{\pi_4(x)+(\alpha_3)_{b_2}+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})b'_{12}+\alpha_2 b_{12}}{b_2}\right),\\
\alpha'_2 &= E\left(\frac{\pi_1(x)+\pi_1(y)+E(\frac{\pi_2(x)+\pi_2(y)}{b_1})(b_1+k_1)}{a_1}\right),\\
\alpha'_4 &= E\left(\frac{\pi_4(x)+\pi_4(y)+\alpha'_2 b_{12}+E(\frac{\pi_2(x)+\pi_2(y)}{b_1})b'_{12}}{b_2}\right).
\end{aligned}$$

By Proposition 1.9 we have

$$\begin{aligned}
E(\tfrac{\alpha_1}{a_1})+\alpha_2 &= E(\tfrac{\alpha_1}{a_1}) + E\left(\frac{\pi_1(x)+(\alpha_1)_{a_1}+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})(b_1+k_1)}{a_1}\right)\\
&\overset{(1)}{=} E\left(\frac{\pi_1(x)+\pi_1(y)+E(\frac{\pi_2(y)}{b_1})(b_1+k_1)+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})(b_1+k_1)}{a_1}\right)\\
&= E\left(\frac{\pi_1(x)+\pi_1(y)+\left(E(\frac{\pi_2(y)}{b_1})+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})\right)(b_1+k_1)}{a_1}\right)\\
&\overset{(1)}{=} E\left(\frac{\pi_1(x)+\pi_1(y)+E(\frac{\pi_2(x)+\pi_2(y)}{b_1})(b_1+k_1)}{a_1}\right) = \alpha'_2,
\end{aligned}$$

so

$$E(\frac{\alpha_1}{a_1}) + \alpha_2 = \alpha'_2. \tag{7}$$

Moreover,

$$\begin{aligned}
E(\tfrac{\alpha_3}{b_2})+\alpha_4 &= E(\tfrac{\alpha_3}{b_2}) + E\left(\frac{\pi_4(x)+(\alpha_3)_{b_2}+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})b'_{12}+\alpha_2 b_{12}}{b_2}\right)\\
&\overset{(1)}{=} E\left(\frac{\pi_4(x)+\alpha_3+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})b'_{12}+\alpha_2 b_{12}}{b_2}\right)\\
&\quad +E\left(\frac{\pi_4(x)+\pi_4(y)+E(\frac{\pi_2(y)}{b_1})b'_{12}+E(\frac{\alpha_1}{a_1})b_{12}+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})b'_{12}+\alpha_2 b_{12}}{b_2}\right)\\
&\overset{(7)}{=} E\left(\frac{\pi_4(x)+\pi_4(y)+E(\frac{\pi_2(y)}{b_1})b'_{12}+\alpha'_2 b_{12}+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})b'_{12}}{b_2}\right)
\end{aligned}$$

$$\overset{(1)}{=} E\left(\frac{\pi_4(x)+\pi_4(y)+\alpha_2' b_{12}+E(\frac{\pi_2(x)+\pi_2(y)}{b_1})b_{12}'}{b_2}\right) = \alpha_4',$$

so

$$E(\frac{\alpha_3}{b_2}) + \alpha_4 = \alpha_4'. \tag{8}$$

Hence,

$$\pi_3(\gamma_t(x+\gamma_t(y))) =$$
$$\left(\pi_3(x+\gamma_t(y))+E(\frac{\pi_2(x+\gamma_t(y))}{b_1})a_{12}'+\alpha_2 a_{12}+E\left(\frac{\pi_4(x+\gamma_t(y))+E(\frac{\pi_2(x+\gamma_t(y))}{b_1})b_{12}'+\alpha_2 b_{12}}{b_2}\right)(b_2+k_2)\right)_{a_2}$$
$$= \left(\pi_3(x)+\left(\pi_3(y)+E(\frac{\pi_2(y)}{b_1})a_{12}'+E(\frac{\alpha_1}{a_1})a_{12}+E(\frac{\alpha_3}{b_2})(b_2+k_2)\right)_{a_2}+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})a_{12}'\right.$$
$$\left.+\alpha_2 a_{12}+E(\frac{\pi_4(x)+(\alpha_3)_{b_2}+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})b_{12}'+\alpha_2 b_{12}}{b_2})(b_2+k_2)\right)_{a_2}$$
$$\overset{(2)}{=} \left(\pi_3(x)+\pi_3(y)+a_{12}'\left(E(\frac{\pi_2(y)}{b_1})+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})\right)+a_{12}(E(\frac{\alpha_1}{a_1})+\alpha_2)+\right.$$
$$\left.(b_2+k_2)(\alpha_4+E(\frac{\alpha_3}{b_2}))\right)_{a_2}$$
$$\overset{(1),(7),(8)}{=} \left(\pi_3(x)+\pi_3(y)+a_{12}'E(\frac{\pi_2(x)+\pi_2(y)}{b_1})+a_{12}\alpha_2'+(b_2+k_2)\alpha_4'\right)_{a_2}$$
$$= \left(\pi_3(x+y)+a_{12}'E(\frac{\pi_2(x+y)}{b_1})+a_{12}\alpha_2'+(b_2+k_2)E\left(\frac{\pi_4(x+y)+\alpha_2' b_{12}+E(\frac{\pi_2(x+y)}{b_1})b_{12}'}{b_2}\right)\right)_{a_2}$$
$$= \pi_3(\gamma_t(x+y))$$

- Let $\beta_1 = \pi_1(y) + E(\frac{\pi_2(y)}{b_1})(b_1+k_1)$, $\beta_2 = E\left(\frac{\pi_1(x+\gamma_t(y))+E(\frac{\pi_2(x+\gamma_t(y))}{b_1})(b_1+k_1)}{a_1}\right)$ $= E\left(\frac{\pi_1(x)+(\beta_1)_{a_1}+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})(b_1+k_1)}{a_1}\right)$.

Then

$$E(\frac{\beta_1}{a_1})+\beta_2 \overset{(1)}{=} E\left(\frac{\pi_1(x)+\beta_1+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})(b_1+k_1)}{a_1}\right)$$
$$= E\left(\frac{\pi_1(x)+\pi_1(y)+E(\frac{\pi_2(y)}{b_1})(b_1+k_1)+E(\frac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})(b_1+k_1)}{a_1}\right)$$
$$\overset{(1)}{=} E\left(\frac{\pi_1(x)+\pi_1(y)+E(\frac{\pi_2(x)+\pi_2(y)}{b_1})(b_1+k_1)}{a_1}\right).$$

Therefore

$$E(\frac{\beta_1}{a_1})+\beta_2 = E\left(\frac{\pi_1(x)+\pi_1(y)+E(\frac{\pi_2(x)+\pi_2(y)}{b_1})(b_1+k_1)}{a_1}\right). \tag{9}$$

So we conclude that

$$\begin{aligned}
&\pi_4(\gamma_t(x+\gamma_t(y)))\\
&= \left(\pi_4(x+\gamma_t(y)) + E(\tfrac{\pi_2(x+\gamma_t(y))}{b_1})b'_{12} + E(\tfrac{\pi_1(x+\gamma_t(y))+E(\frac{\pi_2(x+\gamma_t(y)}{b_1})(b_1+k_1)}{a_1})b_{12}\right)_{b_2}\\
&= \left(\pi_4(x) + \left(\pi_4(y) + E(\tfrac{\pi_2(y)}{b_1})b'_{12} + E(\tfrac{\pi_1(y)+E(\frac{\pi_2(y)}{b_1})(b_1+k_1)}{a_1})b_{12}\right)_{b_2} + \right.\\
&\qquad\qquad\qquad\qquad\qquad\qquad \left. E(\tfrac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1})b'_{12} + \beta_2 b_{12}\right)_{b_2}\\
&\overset{(2)}{=} \left(\pi_4(x) + \pi_4(y) + (E(\tfrac{\pi_2(y)}{b_1}) + E(\tfrac{\pi_2(x)+(\pi_2(y))_{b_1}}{b_1}))b'_{12} + (E(\tfrac{\beta_1}{a_1}) + \beta_2)b_{12}\right)_{b_2}\\
&\overset{(1)}{=} \left(\pi_4(x) + \pi_4(y) + (E(\tfrac{\pi_2(x)+\pi_2(y)}{b_1}))b'_{12} + (E(\tfrac{\beta_1}{a_1}) + \beta_2)b_{12}\right)_{b_2}\\
&\overset{(9)}{=} \left(\pi_4(x+y) + (E(\tfrac{\pi_2(x+y)}{b_1}))b'_{12} + E\left(\tfrac{\pi_1(x)+\pi_1(y)+E(\frac{\pi_2(x)+\pi_2(y)}{b_1})(b_1+k_1)}{a_1}\right) b_{12}\right)_{b_2}\\
&= \pi_4(\gamma_t(x+y)).
\end{aligned}$$

Let $x=(x_1,x_2,x_3,x_4)\in\mathbb{Z}_{a_1}\times\mathbb{Z}_{b_1}\times\mathbb{Z}_{a_2}\times\mathbb{Z}_{b_2}$. It is clear that if $y\in\mathbb{Z}_n$, then $(y)_n=y$ and $E(\frac{y}{n})=0$. So,

- $\pi_1(\gamma_t(x)) = (x_1+E(\frac{x_2}{b_1})(b_1+k_1))_{a_1} = (x_1)_{a_1} = x_1$,
- $\pi_2(\gamma_t(x)) = (x_2)_{b_1} = x_2$,
- $$\begin{aligned}\pi_3(\gamma_t(x)) &= (x_3+E(\tfrac{x_2}{b_1})a'_{12}+\alpha a_{12}+E\left(\tfrac{x_4+E(\frac{x_2}{b_1})b'_{12}+\alpha b_{12}}{b_2}\right)(b_2+k_2))_{a_2}\\ &= (x_3)_{a_2} = x_3 \ \text{ since } \alpha = E\left(\tfrac{x_1+E(\frac{x_2}{b_1})(b_1+k_1)}{a_1}\right) = E(\tfrac{x_1}{a_1}) = 0,\end{aligned}$$
- $\pi_4(\gamma_t(x)) = (x_4+E(\frac{x_2}{b_1})b'_{12}+\alpha b_{12})_{b_2} = (x_4)_{b_2} = x_4$.

Hence $\gamma_t(x)=x$. □

Proposition 2.9. *If $x,y,b\in\mathbb{Z}$ and $b\geqslant 1$ is a divisor of $x-y$, then*

$$E\left(\frac{x}{b}\right) - E\left(\frac{y}{b}\right) = \frac{x-y}{b}\,.$$

Proof. It is obvious. □

Lemma 2.10. *For $t\in D$ and $y\in\mathbb{Z}^4$ we have*

$$\gamma_t(y^*) = \gamma_t((\gamma_t(y))^*), \tag{10}$$

where $y^*=(y_1,y_2,y_3,y_4)^*=(y_2,y_1,y_4,y_3)$.

Proof. Let $y\in\mathbb{Z}^4$, $t=(a_1,b_1,k_1,a_{12},b_{12},a'_{12},b'_{12},a_2,b_2,k_2)\in D$ and

- $\pi_1(\gamma_t(y^*)) = (L_1)_{a_1}, \quad \pi_2(\gamma_t(y^*)) = (L_2)_{b_1}$,

- $\pi_3(\gamma_t(y^*)) = (L_3)_{a_2}, \quad \pi_4(\gamma_t(y^*)) = (L_4)_{b_2}$,
- $\pi_1(\gamma_t((\gamma_t(y))^*)) = (R_1)_{a_1}, \quad \pi_2(\gamma_t((\gamma_t(y))^*)) = (R_2)_{b_1}$,
- $\pi_3(\gamma_t((\gamma_t(y))^*)) = (R_3)_{a_2}, \quad \pi_4(\gamma_t((\gamma_t(y))^*)) = (R_4)_{b_2}$.

We show that $a_1|R_1 - L_1$, $b_1|R_2 - L_2$, $a_2|R_3 - L_3$ and $b_2|R_4 - L_4$. Let

$\beta_1 = \pi_1(y) + E(\frac{\pi_2(y)}{b_1})(b_1 + k_1)$,

$\beta_2 = E(\frac{(\pi_2(y))_{b_1} + E(\frac{(\beta_1)_{a_1}}{b_1})(b_1 + k_1)}{a_1})$,

$\beta_3 = E(\frac{\pi_4(y) + E(\frac{\pi_2(y)}{b_1})b'_{12} + E(\frac{\beta_1}{a_1})b_{12}}{b_2})$,

$\beta_4 = \pi_3(y) + E(\frac{\pi_2(y)}{b_1})a'_{12} + E(\frac{\beta_1}{a_1})a_{12} + \beta_3(b_2 + k_2)$,

$\beta'_1 = \pi_2(y) + E(\frac{\pi_1(y)}{b_1})(b_1 + k_1)$.

First we show that

$$E\left(\frac{(\beta_1)_{a_1}}{b_1}\right) - E\left(\frac{\pi_1(y)}{b_1}\right) = (1 + \frac{k_1}{b_1})E\left(\frac{\pi_2(y)}{b_1}\right) - \frac{a_1}{b_1}E\left(\frac{\beta_1}{a_1}\right), \tag{11}$$

$$\beta_2 - E\left(\frac{\beta'_1}{a_1}\right) = \frac{2k_1 + \frac{k_1^2}{b_1}}{a_1}E\left(\frac{\pi_2(y)}{b_1}\right) - (1 + \frac{k_1}{b_1})E\left(\frac{\beta_1}{a_1}\right). \tag{12}$$

$$\left.\begin{array}{l} E\left(\frac{(\beta_4)_{a_2} + E(\frac{(\beta_1)_{a_1}}{b_1})b'_{12} + \beta_2 b_{12}}{b_2}\right) - E\left(\frac{\pi_3(y) + E(\frac{\pi_1(y)}{b_1})b'_{12} + E(\frac{\beta'_1}{a_1})b_{12}}{b_2}\right) \\ = \left(E(\frac{\pi_2(y)}{b_1})(a'_{12} + (1 + \frac{k_1}{b_1})b'_{12} + \frac{2k_1 + \frac{k_1^2}{b_1}}{a_1}b_{12}) + \right. \\ \left. E(\frac{\beta_1}{a_1})(a_{12} - (1 + \frac{k_1}{b_1})b_{12} - \frac{a_1}{b_1}b'_{12}) + (b_2 + k_2)\beta_3 - E(\frac{\beta_4}{a_2})a_2\right)\frac{1}{b_2}. \end{array}\right\} \tag{13}$$

- Let us observe that $(\beta_1)_{a_1} - \pi_1(y) = \beta_1 - E(\frac{\beta_1}{a_1})a_1 - \pi_1(y) = \pi_1(y) + E(\frac{\pi_2(y)}{b_1})(b_1 + k_1) - E(\frac{\beta_1}{a_1})a_1 - \pi_1(y)$ $= E(\frac{\pi_2(y)}{b_1})(b_1 + k_1) - E(\frac{\beta_1}{a_1})a_1$ so $b_1|(\beta_1)_{a_1} - \pi_1(y)$, and by Proposition 2.9 we conclude $E\left(\frac{(\beta_1)_{a_1}}{b_1}\right) - E\left(\frac{\pi_1(y)}{b_1}\right) = \frac{(\beta_1)_{a_1} - \pi_1(y)}{b_1} = \frac{E(\frac{\pi_2(y)}{b_1})(b_1 + k_1) - E(\frac{\beta_1}{a_1})a_1}{b_1} =$ $(1 + \frac{k_1}{b_1})E\left(\frac{\pi_2(y)}{b_1}\right) - \frac{a_1}{b_1}E\left(\frac{\beta_1}{a_1}\right)$. So, we obtain (11).

- $(\pi_2(y))_{b_1} + E(\frac{(\beta_1)_{a_1}}{b_1})(b_1 + k_1) - (\pi_2(y) + E(\frac{\pi_1(y)}{b_1})(b_1 + k_1))$
  $= -E(\frac{\pi_2(y)}{b_1}) + (b_1 + k_1)(E\left(\frac{(\beta_1)_{a_1}}{b_1}\right) - E\left(\frac{\pi_1(y)}{b_1}\right))$
  $\overset{(11)}{=} -E(\frac{\pi_2(y)}{b_1}) + (b_1 + k_1)((1 + \frac{k_1}{b_1})E\left(\frac{\pi_2(y)}{b_1}\right) - \frac{a_1}{b_1}E\left(\frac{\beta_1}{a_1}\right))$
  $= E(\frac{\pi_2(y)}{b_1})(2k_1 + \frac{k_1^2}{b_1}) - a_1(1 + \frac{k_1}{b_1})E\left(\frac{\beta_1}{a_1}\right)$
  is divided by a_1 since $a_1|(2k_1 + \frac{k_1^2}{b_1})$.

By Proposition 2.9 we have

$$\beta_2 - E\left(\frac{\beta_1'}{a_1}\right) = \frac{(\pi_2(y))_{b_1} + E(\frac{(\beta_1)_{a_1}}{b_1})(b_1+k_1) - (\pi_2(y) + E(\frac{\pi_1(y)}{b_1})(b_1+k_1))}{a_1} =$$
$$\frac{E(\frac{\pi_2(y)}{b_1})(2k_1+\frac{k_1^2}{b_1}) - a_1(1+\frac{k_1}{b_1})E\left(\frac{\beta_1}{a_1}\right)}{a_1} = \frac{2k_1+\frac{k_1^2}{b_1}}{a_1}E\left(\frac{\pi_2(y)}{b_1}\right) - (1+\frac{k_1}{b_1})E\left(\frac{\beta_1}{a_1}\right),$$

so we obtain (12).

- $(\beta_4)_{a_2} + E(\frac{(\beta_1)_{a_1}}{b_1})b_{12}' + \beta_2 b_{12} - \left(\pi_3(y) + E(\frac{\pi_1(y)}{b_1})b_{12}' + E(\frac{\beta_1'}{a_1})b_{12}\right)$

$$= (\beta_4)_{a_2} - \pi_3(y) + b_{12}'(E(\frac{(\beta_1)_{a_1}}{b_1}) - E(\frac{\pi_1(y)}{b_1})) + b_{12}(\beta_2 - E(\frac{\beta_1'}{a_1}))$$
$$\overset{(11),(12)}{=} \beta_4 - E(\frac{\beta_4}{a_2})a_2 - \pi_3(y) + b_{12}'\left((1+\frac{k_1}{b_1})E(\frac{\pi_2(y)}{b_1}) - \frac{a_1}{b_1}E(\frac{\beta_1}{a_1})\right) +$$
$$b_{12}\left(\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}E(\frac{\pi_2(y)}{b_1}) - (1+\frac{k_1}{b_1})E(\frac{\beta_1}{a_1})\right)$$
$$= \pi_3(y) + E(\frac{\pi_2(y)}{b_1})a_{12}' + E(\frac{\beta_1}{a_1})a_{12} + \beta_3(b_2+k_2) - \pi_3(y) - E(\frac{\beta_4}{a_2})a_2 +$$
$$b_{12}'\left((1+\frac{k_1}{b_1})E(\frac{\pi_2(y)}{b_1}) - \frac{a_1}{b_1}E(\frac{\beta_1}{a_1})\right) + b_{12}\left(\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}E(\frac{\pi_2(y)}{b_1}) - (1+\frac{k_1}{b_1})E(\frac{\beta_1}{a_1})\right)$$
$$= E(\frac{\pi_2(y)}{b_1})(a_{12}' + (1+\frac{k_1}{b_1})b_{12}' + \frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12}) +$$
$$E(\frac{\beta_1}{a_1})(a_{12} - (1+\frac{k_1}{b_1})b_{12} - \frac{a_1}{b_1}b_{12}') + (b_2+k_2)\beta_3 - E(\frac{\beta_4}{a_2})a_2)$$

is divided by b_2 because $b_2|a_2$, $b_2|(b_2+k_2)$, $b_2|(a_{12}' + (1+\frac{k_1}{b_1})b_{12}' + \frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12})$, $b_2|(a_{12} - (1+\frac{k_1}{b_1})b_{12} - \frac{a_1}{b_1}b_{12}')$, whereas last two divisions are consequence of the assumption that $t \in D$.

By Lemma 2.9 we have

$$E\left(\frac{(\beta_4)_{a_2} + E(\frac{(\beta_1)_{a_1}}{b_1})b_{12}' + \beta_2 b_{12}}{b_2}\right) - E\left(\frac{\pi_3(y) + E(\frac{\pi_1(y)}{b_1})b_{12}' + E(\frac{\beta_1'}{a_1})b_{12}}{b_2}\right)$$
$$= \frac{1}{b_2}\left((\beta_4)_{a_2} + E(\frac{(\beta_1)_{a_1}}{b_1})b_{12}' + \beta_2 b_{12} - (\pi_3(y) + E(\frac{\pi_1(y)}{b_1})b_{12}' + E(\frac{\beta_1'}{a_1})b_{12})\right)$$
$$= \left(E(\frac{\pi_2(y)}{b_1})(a_{12}' + (1+\frac{k_1}{b_1})b_{12}' + \frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12}) + E(\frac{\beta_1}{a_1})(a_{12} - (1+\frac{k_1}{b_1})b_{12}\right.$$
$$\left. - \frac{a_1}{b_1}b_{12}') + (b_2+k_2)\beta_3 - E(\frac{\beta_4}{a_2})a_2\right)\frac{1}{b_2}.$$

So we obtain (13).

In this part of the proof we show that $a_1|(R_1 - L_1)$. Indeed:

$$R_1 - L_1 = (\pi_1(\gamma_t(y)^*) + E(\frac{\pi_2(\gamma_t(y)^*)}{b_1})(b_1+k_1)) - \pi_2(y) + E(\frac{\pi_1(y)}{b_1})(b_1+k_1)$$
$$= ((\pi_2(y))_{b_1} + E(\frac{(\pi_1(y) + E(\frac{\pi_2(y)}{b_1})(b_1+k_1))_{a_1}}{b_1})(b_1+k_1)) - \pi_2(y) - E(\frac{\pi_1(y)}{b_1})(b_1+k_1)$$
$$= -E(\frac{\pi_2(y)}{b_1})b_1 + E(\frac{(\beta_1)_{a_1}}{b_1})(b_1+k_1) - E(\frac{\pi_1(y)}{b_1})(b_1+k_1)$$

$$\overset{(11)}{=} -E(\tfrac{\pi_2(y)}{b_1})b_1 + (b_1+k_1)\left((1+\tfrac{k_1}{b_1})E\left(\tfrac{\pi_2(y)}{b_1}\right) - \tfrac{a_1}{b_1}E\left(\tfrac{\beta_1}{a_1}\right)\right)$$

$= E(\tfrac{\pi_2(y)}{b_1})(2k_1+\tfrac{k_1^2}{b_1}) - (1+\tfrac{k_1}{b_1})a_1E\left(\tfrac{\beta_1}{a_1}\right)$ is divided by a_1 since $a_1|(2k_1+\tfrac{k_1^2}{b_1})$.

Now we show that $b_1|(R_2-L_2)$:
$R_2 - L_2 = \pi_2(\gamma_t(y)^*) - \pi_2(y^*) = (\pi_1(y) + E(\tfrac{\pi_2(y)}{b_1})(b_1+k_1))_{a_1} - \pi_1(y)$
$= \pi_1(y) + E(\tfrac{\pi_2(y)}{b_1})(b_1+k_1) - E(\tfrac{\pi_1(y)+E(\frac{\pi_2(y)}{b_1})(b_1+k_1)}{a_1})a_1 - \pi_1(y)$
$= E(\tfrac{\pi_2(y)}{b_1})(b_1+k_1) - E(\tfrac{\pi_1(y)+E(\frac{\pi_2(y)}{b_1})(b_1+k_1)}{a_1})a_1$ is divided by b_1 since $b_1|a_1$ and $b_1|k_1$.

The third our task is to show that $a_2|(R_3-L_3)$:

$$L_3 = \pi_3(y^*) + E(\tfrac{\pi_2(y^*)}{b_1})a'_{12} + \alpha a_{12} + E\left(\tfrac{\pi_4(y^*)+E(\frac{\pi_2(y^*)}{b_1})b'_{12}+\alpha b_{12}}{b_2}\right)(b_2+k_2),$$

where $\alpha = E\left(\tfrac{\pi_1(y^*)+E(\frac{\pi_2(y^*)}{b_1})(b_1+k_1)}{a_1}\right) = E\left(\tfrac{\pi_2(y)+E(\frac{\pi_1(y)}{b_1})(b_1+k_1)}{a_1}\right) = E(\tfrac{\beta'_1}{a_1})$. So,

$$L_3 = \pi_4(y) + E(\tfrac{\pi_1(y)}{b_1})a'_{12} + E(\tfrac{\beta'_1}{a_1})a_{12} + E\left(\tfrac{\pi_3(y)+E(\frac{\pi_1(y)}{b_1})b'_{12}+E(\frac{\beta'_1}{a_1})b_{12}}{b_2}\right)(b_2+k_2).$$

$$R_3 = \pi_3(\gamma_t(y)^*) + E(\tfrac{\pi_2(\gamma_t(y)^*)}{b_1})a'_{12} + \alpha' a_{12} + E\left(\tfrac{\pi_4(\gamma_t(y)^*)+E(\frac{\pi_2(\gamma_t(y)^*)}{b_1})b'_{12}+\alpha' b_{12}}{b_2}\right)(b_2+k_2),$$

where $\alpha' = E\left(\tfrac{\pi_1(\gamma_t(y)^*)+E(\frac{\pi_2(\gamma_t(y)^*)}{b_1})(b_1+k_1)}{a_1}\right) = E\left(\tfrac{\pi_2(\gamma_t(y))+E(\frac{\pi_1(\gamma_t(y))}{b_1})(b_1+k_1)}{a_1}\right) = E\left(\tfrac{(\pi_2(y))_{b_1}+E(\frac{(\beta_1)_{a_1}}{b_1})(b_1+k_1)}{a_1}\right) = \beta_2$.

Moreover,

$$\left.\begin{array}{l} \pi_3(\gamma_t(y)) = \\ \left(\pi_3(y) + E(\tfrac{\pi_2(y)}{b_1})a'_{12} + \alpha'' a_{12} + E\left(\tfrac{\pi_4(y)+E(\frac{\pi_2(y)}{b_1})b'_{12}+\alpha'' b_{12}}{b_2}\right)(b_2+k_2)\right)_{a_2} \\ = (\beta_4)_{a_2} \end{array}\right\} \quad (14)$$

where
$\alpha'' = E\left(\tfrac{\pi_1(y)+E(\frac{\pi_2(y)}{b_1})(b_1+k_1)}{a_1}\right) = E(\tfrac{\beta_1}{a_1})$.
Hence

$$R_3 = \pi_4(\gamma_t(y)) + E(\tfrac{\pi_1(\gamma_t(y))}{b_1})a'_{12} + \beta_2 a_{12} + E\left(\tfrac{\pi_3(\gamma_t(y))+E(\frac{\pi_1(\gamma_t(y))}{b_1})b'_{12}+\beta_2 b_{12}}{b_2}\right)(b_2+k_2)$$

$$= \left(\pi_4(y) + E(\tfrac{\pi_2(y)}{b_1})b'_{12} + E(\tfrac{\beta_1}{a_1})b_{12}\right)_{b_2} + E(\tfrac{(\beta_1)_{a_1}}{b_1})a'_{12} + \beta_2 a_{12} + \\ E\left(\tfrac{\pi_3(\gamma_t(y))+E(\frac{(\beta_1)_{a_1}}{b_1})b'_{12}+\beta_2 b_{12}}{b_2}\right)(b_2+k_2)$$

$$\overset{(14)}{=} \left(\pi_4(y) + E(\tfrac{\pi_2(y)}{b_1})b'_{12} + E(\tfrac{\beta_1}{a_1})b_{12}\right)_{b_2} + E(\tfrac{(\beta_1)_{a_1}}{b_1})a'_{12} + \beta_2 a_{12} +$$

$$E\left(\frac{(\beta_4)_{a_2}+E(\frac{(\beta_1)_{a_1}}{b_1})b'_{12}+\beta_2 b_{12}}{b_2}\right)(b_2+k_2).$$

Thus
$R_3 - L_3\left(\pi_4(y)+E(\frac{\pi_2(y)}{b_1})b'_{12}+E(\frac{\beta_1}{a_1})b_{12}\right)_{b_2} + E(\frac{(\beta_1)_{a_1}}{b_1})a'_{12}+\beta_2 a_{12}+$
$E\left(\frac{(\beta_4)_{a_2}+E(\frac{(\beta_1)_{a_1}}{b_1})b'_{12}+\beta_2 b_{12}}{b_2}\right)(b_2+k_2) - \Bigg(\pi_4(y)+E(\frac{\pi_1(y)}{b_1})a'_{12}+E(\frac{\beta'_1}{a_1})a_{12}+$
$E\left(\frac{\pi_3(y)+E(\frac{\pi_1(y)}{b_1})b'_{12}+E(\frac{\beta'_1}{a_1})b_{12}}{b_2}\right)(b_2+k_2)\Bigg) = \pi_4(y)+E(\frac{\pi_2(y)}{b_1})b'_{12}+E(\frac{\beta_1}{a_1})b_{12} -$
$E\left(\frac{\pi_4(y)+E(\frac{\pi_2(y)}{b_1})b'_{12}+E(\frac{\beta_1}{a_1})b_{12}}{b_2}\right)b_2 + a'_{12}(E(\frac{(\beta_1)_{a_1}}{b_1}) - E(\frac{\pi_1(y)}{b_1})) + a_{12}(\beta_2 - E(\frac{\beta'_1}{a_1}))+$
$(b_2+k_2)(E\left(\frac{(\beta_4)_{a_2}+E(\frac{(\beta_1)_{a_1}}{b_1})b'_{12}+\beta_2 b_{12}}{b_2}\right)-E\left(\frac{\pi_3(y)+E(\frac{\pi_1(y)}{b_1})b'_{12}+E(\frac{\beta'_1}{a_1})b_{12}}{b_2}\right))-\pi_4(y)\overset{(11),(12)}{=}$
$E(\frac{\pi_2(y)}{b_1})b'_{12}+E(\frac{\beta_1}{a_1})b_{12}-\beta_3 b_2 + a'_{12}((1+\frac{k_1}{b_1})E\left(\frac{\pi_2(y)}{b_1}\right) - \frac{a_1}{b_1}E\left(\frac{\beta_1}{a_1}\right))+$
$a_{12}(\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}E\left(\frac{\pi_2(y)}{b_1}\right)-(1+\frac{k_1}{b_1})E\left(\frac{\beta_1}{a_1}\right))+(b_2+k_2)(E\left(\frac{(\beta_4)_{a_2}+E(\frac{(\beta_1)_{a_1}}{b_1})b'_{12}+\beta_2 b_{12}}{b_2}\right)-$
$E\left(\frac{\pi_3(y)+E(\frac{\pi_1(y)}{b_1})b'_{12}+E(\frac{\beta'_1}{a_1})b_{12}}{b_2}\right))\overset{(13)}{=} a'_{12}((1+\frac{k_1}{b_1})E\left(\frac{\pi_2(y)}{b_1}\right) - \frac{a_1}{b_1}E\left(\frac{\beta_1}{a_1}\right))+$
$a_{12}(\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}E\left(\frac{\pi_2(y)}{b_1}\right)-(1+\frac{k_1}{b_1})E\left(\frac{\beta_1}{a_1}\right))+(b_2+k_2)\Bigg(E(\frac{\pi_2(y)}{b_1})(a'_{12}+(1+\frac{k_1}{b_1})b'_{12}+$
$\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12}) + E(\frac{\beta_1}{a_1})(a_{12}-(1+\frac{k_1}{b_1})b_{12}-\frac{a_1}{b_1}b'_{12}) + (b_2+k_2)\beta_3 - E(\frac{\beta_4}{a_2})a_2\Bigg)\frac{1}{b_2}+$
$E(\frac{\pi_2(y)}{b_1})b'_{12}+E(\frac{\beta_1}{a_1})b_{12}-\beta_3 b_2 = E(\frac{\pi_2(y)}{b_1})\Bigg(b'_{12}+(1+\frac{k_1}{b_1})a'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}a_{12}+$
$(1+\frac{k_2}{b_2})(a'_{12}+(1+\frac{k_1}{b_1})b'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12})\Bigg)+E(\frac{\beta_1}{a_1})\Bigg(b_{12}-(1+\frac{k_1}{b_1})+a_{12}-\frac{a_1}{b_1}a'_{12}+$
$(1+\frac{k_2}{b_2})(a_{12}-(1+\frac{k_1}{b_1})b_{12}-\frac{a_1}{b_1}b'_{12})\Bigg)+\beta_3((b_2+k_2)^2\frac{1}{b_2}-b_2)-\frac{b_2+k_2}{b_2}E(\frac{\beta_4}{a_2})a_2 =$
$E(\frac{\pi_2(y)}{b_1})\Bigg(b'_{12}+(1+\frac{k_1}{b_1})a'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}a_{12}+(1+\frac{k_2}{b_2})(a'_{12}(1+\frac{k_1}{b_1})b'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12})\Bigg)+$
$E(\frac{\beta_1}{a_1})\Bigg(b_{12}-(1+\frac{k_1}{b_1})a_{12}-\frac{a_1}{b_1}a'_{12}+(1+\frac{k_2}{b_2})(a_{12}-(1+\frac{k_1}{b_1})b_{12}-\frac{a_1}{b_1}b'_{12})\Bigg)+\beta_3(2k_2+$
$\frac{k_2^2}{b_2})-(1+\frac{k_2}{b_2})E(\frac{\beta_4}{a_2})a_2$ is divided by a_2 because we have $a_2|(2k_2+\frac{k_2^2}{b_2})$ and
$a_2|\Bigg(b'_{12}+(1+\frac{k_1}{b_1})a'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}a_{12}+(1+\frac{k_2}{b_2})(a'_{12}+(1+\frac{k_1}{b_1})b'_{12}+\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12})\Bigg),$
$a_2|\Bigg((b_{12}-(1+\frac{k_1}{b_1})a_{12}-\frac{a_1}{b_1}a'_{12}+(1+\frac{k_2}{b_2})(a_{12}-(1+\frac{k_1}{b_1})b_{12}-\frac{a_1}{b_1}b'_{12})\Bigg),$ where two last divisions are consequence of the assumption on $t \in D$.

It remains to show that $b_2|(R_4 - L_4)$:

$$\begin{aligned}
R_4 &= \pi_4(\gamma_t(y)^*) + E(\tfrac{\pi_2(\gamma_t(y)^*)}{b_1})b'_{12} + E\left(\frac{\pi_1(\gamma_t(y)^*)+E(\frac{\pi_2(\gamma_t(y)^*)}{b_1})(b_1+k_1)}{a_1}\right)b_{12}\\
&= \pi_3(\gamma_t(y)) + E(\tfrac{\pi_1(\gamma_t(y))}{b_1})b'_{12} + E\left(\frac{\pi_2(\gamma_t(y))+E(\frac{\pi_1(\gamma_t(y))}{b_1})(b_1+k_1)}{a_1}\right)b_{12}\\
&\overset{(14)}{=} (\beta_4)_{a_2} + E(\tfrac{(\beta_1)_{a_1}}{b_1})b'_{12} + E\left(\frac{(\pi_2(y))_{b_1}+E(\frac{(\beta_1)_{a_1}}{b_1})(b_1+k_1)}{a_1}\right)b_{12}\\
&= (\beta_4)_{a_2} + E(\tfrac{(\beta_1)_{a_1}}{b_1})b'_{12} + \beta_2 b_{12}.\\
L_4 &= \pi_4(y^*) + E(\tfrac{\pi_2(y^*)}{b_1})b'_{12} + E\left(\frac{\pi_1(y^*)+E(\frac{\pi_2(y^*)}{b_1})(b_1+k_1)}{a_1}\right)b_{12}\\
&= \pi_3(y) + E(\tfrac{\pi_1(y)}{b_1})b'_{12} + E\left(\frac{\pi_2(y)+E(\frac{\pi_1(y)}{b_1})(b_1+k_1)}{a_1}\right)b_{12}\\
&= \pi_3(y) + E(\tfrac{\pi_1(y)}{b_1})b'_{12} + E\left(\frac{\beta'_1}{a_1}\right)b_{12}.
\end{aligned}$$

Hence

$$\begin{aligned}
R_4 - L_4 &= (\beta_4)_{a_2} + E(\tfrac{(\beta_1)_{a_1}}{b_1})b'_{12} + \beta_2 b_{12} - (\pi_3(y) + E(\tfrac{\pi_1(y)}{b_1})b'_{12} + E\left(\frac{\beta'_1}{a_1}\right)b_{12})\\
&= \beta_4 - E(\tfrac{\beta_4}{a_2})a_2 - \pi_3(y) + b'_{12}(E(\tfrac{(\beta_1)_{a_1}}{b_1}) - E(\tfrac{\pi_1(y)}{b_1})) + b_{12}(\beta_2 - E(\tfrac{\beta'_1}{a_1}))\\
&\overset{(11),(12)}{=} -E(\tfrac{\beta_4}{a_2})a_2 + \pi_3(y) + E(\tfrac{\pi_2(y)}{b_1})a'_{12} + E(\tfrac{\beta_1}{a_1})a_{12} + \beta_3(b_2+k_2) - \pi_3(y)\\
&\qquad +b'_{12}\Big((1+\tfrac{k_1}{b_1})E(\tfrac{\pi_2(y)}{b_1}) - \tfrac{a_1}{b_1}E(\tfrac{\beta_1}{a_1})\Big) + b_{12}\Big(\frac{2k_1+\frac{k_1^2}{b_1}}{a_1}E(\tfrac{\pi_2(y)}{b_1}) - (1+\tfrac{k_1}{b_1})E(\tfrac{\beta_1}{a_1})\Big)\\
&= -E(\tfrac{\beta_4}{a_2})a_2 + \beta_3(b_2+k_2) + E(\tfrac{\pi_2(y)}{b_1})(a'_{12} + b'_{12}(1+\tfrac{k_1}{b_1}) + b_{12}\frac{2k_1+\frac{k_1^2}{b_1}}{a_1})\\
&\qquad +E(\tfrac{\beta_1}{a_1})(a_{12} - b'_{12}\tfrac{a_1}{b_1} - b_{12}(1+\tfrac{k_1}{b_1}))
\end{aligned}$$

is divided by b_2 because $b_2|a_2$, $b_2|k_2$ and $b_2|(a'_{12} + (1+\frac{k_1}{b_1})b'_{12} + \frac{2k_1+\frac{k_1^2}{b_1}}{a_1}b_{12})$, $b_2|(a_{12} - (1+\frac{k_1}{b_1})b_{12} - \frac{a_1}{b_1}b'_{12})$, where last two divisions are consequence of the assumption on $t \in D$.

Therefore $\gamma_t(y^*) = \gamma_t(\gamma_t(y)^*)$ and the proof of Lemma 2.10 is finished. □

3. Main results

Theorem 3.1. *If $t \in D$, then Q_t is a 2-generated abelian group with involution.*

Proof. Obviously the operation $+_t$ is commutative. We show that $+_t$ is associative:

$$\begin{aligned}
x +_t (y +_t z) &= x +_t \gamma_t(y+z) = \gamma_t(x + \gamma_t(y+z)) \overset{(5)}{=} \gamma_t(x + (y+z))\\
&= \gamma_t((x+y)+z) \overset{(5)}{=} \gamma_t(\gamma_t(x+y)+z)) = \gamma_t((x +_t y) + z) = (x +_t y) +_t z).
\end{aligned}$$

If $x \in \mathbb{Z}_{a_1} \times \mathbb{Z}_{b_1} \times \mathbb{Z}_{a_2} \times \mathbb{Z}_{b_2}$ then $\gamma_t(x) \overset{(6)}{=} x$, so $x +_t \underline{0} = \gamma_t(x + \underline{0}) = \gamma_t(x) = x$.

Moreover, $x +_t (-_t x) = \gamma_t(x + (-_t x)) = \gamma_t(x + \gamma_t(-x)) \overset{(5)}{=} \gamma_t(x + (-x)) = \gamma_t(\underline{0}) = \underline{0}$.

Hence the group reduct of Q_t is an abelian group.

If $x \in \mathbb{Z}_{a_1} \times \mathbb{Z}_{b_1} \times \mathbb{Z}_{a_2} \times \mathbb{Z}_{b_2}$ then $(x^{*_t})^{*_t} = \gamma_t((x^{*_t})^*) = \gamma_t(\gamma_t(x^*)^*) \overset{(10)}{=} \gamma_t((x^*)^*) = \gamma_t(x) \overset{(6)}{=} x$.

If $x, y \in \mathbb{Z}_{a_1} \times \mathbb{Z}_{b_1} \times \mathbb{Z}_{a_2} \times \mathbb{Z}_{b_2}$ then $(x +_t y)^{*_t} = \gamma_t((x +_t y)^*) = \gamma_t((\gamma_t(x+y))^*) \overset{(10)}{=} \gamma_t((x+y)^*) = \gamma_t(x^* + y^*) \overset{(5)}{=} \gamma_t(\gamma_t(x^*) + \gamma_t(y^*)) = \gamma_t(x^{*_t} + y^{*_t}) = (x^{*_t} +_t y^{*_t})$. Also $\underline{0}^{*_t} = \gamma_t(\underline{0}^*) = \gamma_t(\underline{0}) = \underline{0}$. Thus Q_t is an abelian group with involution.

Let $x_1 = (1,0,0,0)$ and $x_2 = (0,0,1,0)$, then $Q_t = \langle x_1, x_2 \rangle$ since $(y_1, y_2, y_3, y_4) = y_1 x_1 + y_2 x_1^* + y_3 x_2 + y_4 x_2^*$ for every $(y_1, y_2, y_3, y_4) \in \mathbb{Z}_{a_1} \times \mathbb{Z}_{b_1} \times \mathbb{Z}_{a_2} \times \mathbb{Z}_{b_2}$. Therefore Q_t is 2-generated. □

Proposition 3.2. *If $G = \langle x_1, x_2 \rangle$ is a finite abelian group with involution and $\phi \colon \mathbb{Z}^4 \to G$ is such that $\phi(y_1, y_2, y_3, y_4) = y_1 x_1 + y_2 x_1^* + y_3 x_2 + y_4 x_2^*$, then*

$$\gamma_t \phi = \phi$$

for $t = \psi(G, x_1, x_2) = (a_1, b_1, k_1, a_{12}, b_{12}, a'_{12}, b'_{12}, a_2, b_2, k_2)$.

In other words, *if $\underline{Z} = \mathbb{Z}_{a_1} \times \mathbb{Z}_{b_1} \times \mathbb{Z}_{a_2} \times \mathbb{Z}_{b_2}$, then the following diagram*

$$\begin{tikzcd}
\mathbb{Z}^4 \arrow[r, "\phi"] \arrow[d, "\gamma_t"] & G \\
\underline{\mathbb{Z}} \arrow[r, hook] & \mathbb{Z}^4 \arrow[u, "\phi"]
\end{tikzcd}$$

is commutative.

Proof. Let $G = \langle x_1, x_2 \rangle$ be a finite abelian group with involution and $t = \psi(G, x_1, x_2) = (a_1, b_1, k_1, a_{12}, b_{12}, a'_{12}, b'_{12}, a_2, b_2, k_2)$. Then

$$a_1 x_1 = a_{12} x_2 + b_{12} x_2^* \in \langle x_2 \rangle, \tag{15}$$

$$b_1 x_1^* - (b_1 + k_1) x_1 = a'_{12} x_2 + b'_{12} x_2^* \in \langle x_2 \rangle, \tag{16}$$

$$a_2 x_2 = 0, \tag{17}$$

$$b_2 x_2^* = (b_2 + k_2) x_2. \tag{18}$$

For $\alpha_1 = y_1 + E(\frac{y_2}{b_1})(b_1 + k_1)$ and $\beta = y_4 + E(\frac{y_2}{b_1}) b'_{12} + E(\frac{\alpha_1}{a_1}) b_{12}$, where $y = (y_1, y_2, y_3, y_4) \in \mathbb{Z}^4$, we obtain

$$\begin{aligned}
\phi(y) &= y_1 x_1 + y_2 x_1^* + y_3 x_2 + y_4 x_2^* = y_1 x_1 + (E(\tfrac{y_2}{b_1}) b_1 + (y_2)_{b_1}) x_1^* + y_3 x_2 + y_4 x_2^* \\
&\overset{(16)}{=} y_1 x_1 + E(\tfrac{y_2}{b_1})((b_1 + k_1) x_1 + a'_{12} x_2 + b'_{12} x_2^*) + (y_2)_{b_1} x_1^* + y_3 x_2 + y_4 x_2^* \\
&= (y_1 + E(\tfrac{y_2}{b_1})(b_1 + k_1)) x_1 + (y_2)_{b_1} x_1^* + (y_3 + E(\tfrac{y_2}{b_1}) a'_{12}) x_2 + (y_4 + E(\tfrac{y_2}{b_1}) b'_{12}) x_2^* \\
&= \alpha_1 x_1 + (y_2)_{b_1} x_1^* + (y_3 + E(\tfrac{y_2}{b_1}) a'_{12}) x_2 + (y_4 + E(\tfrac{y_2}{b_1}) b'_{12}) x_2^* \\
&= (E(\tfrac{\alpha_1}{a_1}) a_1 + (\alpha_1)_{a_1}) x_1 + (y_2)_{b_1} x_1^* + (y_3 + E(\tfrac{y_2}{b_1}) a'_{12}) x_2 + (y_4 + E(\tfrac{y_2}{b_1}) b'_{12}) x_2^*
\end{aligned}$$

$$\overset{(15)}{=} E(\tfrac{\alpha_1}{a_1})(a_{12}x_2+b_{12}x_2^*)+(\alpha_1)_{a_1}x_1+(y_2)_{b_1}x_1^*+(y_3+E(\tfrac{y_2}{b_1})a'_{12})x_2+(y_4+E(\tfrac{y_2}{b_1})b'_{12})x_2^*$$
$$= (\alpha_1)_{a_1}x_1+(y_2)_{b_1}x_1^*+(y_3+E(\tfrac{y_2}{b_1})a'_{12}+E(\tfrac{\alpha_1}{a_1})a_{12})x_2+(y_4+E(\tfrac{y_2}{b_1})b'_{12}+E(\tfrac{\alpha_1}{a_1})b_{12})x_2^*$$
$$= (\alpha_1)_{a_1}x_1 + (y_2)_{b_1}x_1^* + (y_3 + E(\tfrac{y_2}{b_1})a'_{12} + E(\tfrac{\alpha_1}{a_1})a_{12})x_2 + \beta x_2^*$$
$$= (\alpha_1)_{a_1}x_1 + (y_2)_{b_1}x_1^* + (y_3 + E(\tfrac{y_2}{b_1})a'_{12} + E(\tfrac{\alpha_1}{a_1})a_{12})x_2 + (E(\tfrac{\beta}{b_2})b_2 + (\beta)_{b_2})x_2^*$$
$$\overset{(18)}{=}(\alpha_1)_{a_1}x_1+(y_2)_{b_1}x_1^*+(y_3+E(\tfrac{y_2}{b_1})a'_{12}+E(\tfrac{\alpha_1}{a_1})a_{12})x_2+E(\tfrac{\beta}{b_2})(b_2+k_2)x_2+(\beta)_{b_2}x_2^*$$
$$= (\alpha_1)_{a_1}x_1 + (y_2)_{b_1}x_1^* + \Big(y_3 + E(\tfrac{y_2}{b_1})a'_{12} + E(\tfrac{\alpha_1}{a_1})a_{12} + E(\tfrac{\beta}{b_2})(b_2 + k_2)\Big)x_2 + (\beta)_{b_2}x_2^*$$
$$\overset{(17)}{=}(\alpha_1)_{a_1}x_1+(y_2)_{b_1}x_1^*+\Big(y_3+E(\tfrac{y_2}{b_1})a'_{12}+E(\tfrac{\alpha_1}{a_1})a_{12}+E(\tfrac{\beta}{b_2})(b_2+k_2)\Big)_{a_2}x_2+(\beta)_{b_2}x_2^*$$
$$= \phi(\gamma_t(y)). \qquad \square$$

The main theorem of this paper is formulated in the following way:

Theorem 3.3. *If $G = \langle x_1, x_2\rangle$ is a finite abelian group with involution, then $G \cong Q_t$ for $t = \psi(G, x_1, x_2)$.*

Proof. Indeed, let $t = \psi(G, x_1, x_2) = (a_1, b_1, k_1, a_{12}, b_{12}, a'_{12}, b'_{12}, a_2, b_2, k_2) \in \mathbb{Z}^{10}$ and $\underline{\mathbb{Z}} = \mathbb{Z}_{a_1} \times \mathbb{Z}_{b_1} \times \mathbb{Z}_{a_2} \times \mathbb{Z}_{b_2}$. Consider the map $\phi\colon \mathbb{Z}^4 \to G$ defined by

$$\phi(y_1, y_2, y_3, y_4) = y_1x_1 + y_2x_1^* + y_3x_2 + y_4x_2^*.$$

Then $\phi|_{\underline{\mathbb{Z}}}$ is an isomorphism of Q_t and G.

In fact,

- $\phi|_{\underline{\mathbb{Z}}}$ is onto: if $g \in G$ then there exist $y_1, y_2, y_3, y_4 \in \mathbb{Z}$ such that

  $g = y_1x_1 + y_2x_1^* + y_3x_2 + y_4x_2^* = \phi(y_1, y_2, y_3, y_4) = \phi(\gamma_t(y_1, y_2, y_3, y_4))$ and $\gamma_t(y_1, y_2, y_3, y_4) \in \underline{\mathbb{Z}}$.

- $\phi|_{\underline{\mathbb{Z}}}$ is injective: if $\phi(y_1, y_2, y_3, y_4) = \phi(y'_1, y'_2, y'_3, y'_4)$, then

  $$y_1x_1 + y_2x_1^* + y_3x_2 + y_4x_2^* = y'_1x_1 + y'_2x_1^* + y'_3x_2 + y'_4x_2^*.$$

  Thus $(y_2 - y'_2)x_1^* - (y'_1 - y_1)x_1 \in \langle x_2\rangle$ and $|y_2 - y'_2| \in \mathbb{Z}_{b_1}$, which by definition of b_1, implies $y_2 = y'_2$. Hence $(y'_1 - y_1)x_1 \in \langle x_2\rangle$ and $|y_1 - y'_1| \in \mathbb{Z}_{a_1}$, and by definition of a_1, we have $y_1 = y'_1$. So $y_3x_2 + y_4x_2^* = y'_3x_2 + y'_4x_2^*$ and $(y_4 - y'_4)x_2^* = (y'_3 - y_3)x_2$ and $|y_4 - y'_4| \in \mathbb{Z}_{b_2}$. This by definition of b_2 gives $y_4 = y'_4$. Therefore, $(y'_3 - y_3)x_2 = 0$ and $|y'_3 - y_3| \in \mathbb{Z}_{a_2}$, which by definition of a_2 implies $y_3 = y'_3$. This shows that $\phi|_{\underline{\mathbb{Z}}}$ is injective.

- $\phi|_{\underline{\mathbb{Z}}}$ is a homomorphism since for all $y, y' \in \underline{\mathbb{Z}}$ we have
  $$\phi(y +_t y') = \phi(\gamma_t(y + y')) = \phi(y + y') = \phi(y) + \phi(y').$$

Moreover, for all $(y_1, y_2, y_3, y_4) \in \underline{Z}$ we also have:

$$\begin{aligned}\phi((y_1, y_2, y_3, y_4)^{*_t}) &= \phi(\gamma_t(y_2, y_1, y_4, y_3)) = \phi(y_2, y_1, y_4, y_3)\\ &= y_2x_1 + y_1x_1^* + y_4x_2 + y_3x_2^* = (y_1x_1 + y_2x_1^* + y_3x_2 + y_4x_2^*)^*\\ &= (\phi(y_1, y_2, y_3, y_4))^*. \qquad \square\end{aligned}$$

Corollary 3.4. *G is a 2-generated finite abelian group with involution if and only if $G \cong Q_t$ for some $t \in D$.*

Proof. If G is a 2-generated finite abelian group with involution, then by Theorem 3.3 we have $G \cong Q_t$, where $t = \psi(G, x_1, x_2)$ and $t \in D$ by Proposition 2.7.

The converse statement is a consequence of Theorem 3.1. □

Corollary 3.5. *Q is a 2-generated finite entropic quasigroup with a quasi-identity if and only if $G \cong \Psi(Q_t)$ for some $t \in D$.*

References

[1] **G. Bińczak and J. Kaleta**, *Cyclic entropic quasigroups*, Demonstratio Math. **42** (2009), 269 – 281.

[2] **G. Bińczak and J. Kaleta**, *Finite directly indecomposable monogenic entropic quasigroups with a quasi-identity*, Demonstratio Math. **45** (2012), 519 – 532.

[3] **G. Bińczak and J. Kaleta**, *Some finite directly indecomposable non-monogenic entropic quasigroups with a quasi-identity*, Discuss. Math. General Algebra and Applications **34** (2014), 5 – 26.

[4] **O. Chein, H.O. Pflugfelder, and J.D.H. Smith**, *Quasigroups and Loops: Theory and Applications*, Heldermann Verlag, Berlin, 1990.

[5] **V.J. Havel and A. Vanžurová**, *Medial Quasigroups and Geometry*, Olomouc, 2006.

[6] **J.J. Rotman**, *An Introduction to the Theory of Groups*, Springer-Verlag, New York, 1994.

[7] **J.D.H. Smith**, *Representation Theory of Infinite Groups and Finite Quasigroups*, Université de Montréal, 1986.

[8] **J.D.H. Smith**, *An Introduction to Quasigroups and Their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.

Received July 4, 2014
Revised September 25, 2014

G. Bińczak
Faculty of Mathematics and Information Sciences, Warsaw University of Technology, 00-661 Warsaw, Poland
E-mail: binczak@mini.pw.edu.pl

J. Kaleta
Department of Applied Mathematics, Warsaw University of Agriculture, 02-787 Warsaw, Poland
E-mail: joanna_kaleta@sggw.pl

K-loops from classical subgroups of $GL(\mathcal{H})$, $\mathcal{H}$ being a separable Hilbert space

Alper Bulut

Abstract. We study some examples of infinite dimensional K-loops from subgroups of invertible bounded linear operators $GL(\mathcal{H})$, where $\mathcal{H}$ is infinite dimensional separable Hilbert space. We use Kreuzer and Wefelscheid method given in [10] to show that if G is one of the classical complex Banach Lie group in $\{GL(\mathcal{H}), O(\mathcal{H}, J_{\mathbb{R}}), Sp(\mathcal{H}, J_{\mathbb{Q}})\}$, then the intersection of G and the set of positive self-adjoint operators form a K-loop with respect to a new binary operation induced by the group operation in G.

1. Introduction

A Bol loop satisfying the automorphic inverse property is called a K-loop. Karzel introduced the notion of near-domain $(F, \oplus, \cdot)$ in [4], [5] which is a generalization of a near-field where the additive structure of a near-domain is not necessarily associative. Kerby and Wefelsheid investigated the additive structure of a near-domain $(F, \oplus)$ with extra axioms, and then they called the new structure a K-loop, but according to [6], they used the term *K-loop* only in talks in 1970's and the beginning of 1980's. On the other hand, the first appearance of the term *K-loop* in literature goes back to A.A. Ungar's paper in [15].

The early history of the "K-loop" notion, with K named after Karzel, is unfolded in [12]. For different purposes, the term "K-loop" was already in use earlier by L.R. Soikis, in 1970 [13], and later but independently by A.S. Basarab, in 1992 [1]. The origin of the "K" in the term K-loop coined by Soikis and by Basarab, which certainly does not refer to "Karzel", is unclear.

Ungar investigated the Einsten's velocity addition binary operation $\oplus$ over $\mathbb{R}^3_c$. The elements of $\mathbb{R}^3_c$ are called relativistically admissible velocities that are vectors in $\mathbb{R}^3$ whose norms are strictly less than c, where c is the vacuum speed of light. The Einstein velocity addition of x and y in $\mathbb{R}^3_c$ is given by

$$x \oplus y = \frac{1}{1 + \frac{x.y}{c^2}} \left\{ x + y + \frac{1}{c^2} \frac{\gamma_x}{1 + \gamma_x} (x \times (x \times y)) \right\} \tag{1}$$

In (1) "." and "$\times$" stand for inner product and cross product respectively, and $\gamma_x = \frac{1}{\sqrt{1 - (\frac{\|x\|}{c})^2}}$ is called *Lorentz factor* [15, 17].

2010 Mathematics Subject Classification: Primary 20N05, 22E65; Secondary 46C05
Keywords: K-loops, Banach Lie groups, Hilbert space, polar decomposition theorem.

Ungar showed in [15] that Einstein's velocity addition over the $\mathbb{R}^3_c$ has unusual algebraic properties. For instance $(\mathbb{R}^3_c, \oplus)$ is a non-associative and non-commutative loop. Ungar stated that this loop can be placed in the context of K-loop, see [15], that was studied by Kerby and Wefelscheid. In literature, K-loops are also known as gyrocommutative gorogroups, see [16]. The non-associativity and non-commutativity of Einstein velocity addition in $\mathbb{R}^3_c$ can be upgraded to a weak form of associativity and commutativity by a linear map in $End(\mathbb{R}^3)$ that is called *Thomas Rotation*, see [14].

The weak forms of associativity and commutativity for the $x, y, z \in \mathbb{R}^3_c$ are given by

$$x \oplus (y \oplus z) = (x \oplus y) \oplus tom[x; y](z) \tag{2}$$

$$x \oplus y = tom[x; y](y \oplus x) \tag{3}$$

Thomas precession (or Thomas rotation) is also called *Thomas gyration* and denoted by $gyr[x, y]$ for $x, y \in \mathbb{R}^3_c$, and 2 and 3 are called gyroassociative and gyrocommutative laws respectively in [16]. It is quiet interesting that some of the properties of Thomas gyration are identical with the properties of a bijective map in the definition of a near-domain $(F, \oplus, .)$, namely $d_{a,b} : F \to F$ where $a, b \in F$, and $d_{a,b}$ sends the element x to $d_{a,b}.x$ such that $a \oplus (b \oplus x) = (a \oplus b) \oplus +d_{a,b}.x$ [9]. Ungar's example in physics motivated many people to investigate K-loop structures, hence many K-loop examples were derived. Kreuzer and Wefelscheid pioneered an abstract way to construct a K-loop from group transversals [10], and Kiechle in [7] gave many examples of K-loops derived from classical groups over ordered fields. Kiechle showed that

Theorem 1.1. *Let R be n-real, and $G \leq GL(n, K)$ with $G = L_G\Omega_G$, then there are $A \oplus B \in L_G$ and $d_{A,B} \in \Omega_G$ with $AB = (A \oplus B)d_{A,B}$ such that $(L_G, \oplus)$ is a K-loop.*

Here R is an ordered field and $K = R(i)$, where $i^2 = -1$. L is the set of positive definite hermitian $n \times n$ matrices over K and Ω is the unitary group as given below.

$$L = \left\{A \in K^{n\times n} : A = A^*, \forall v \in K^n \setminus \{0\} : v^*Av > 0\right\}, \tag{4}$$

$$\Omega = \left\{U \in K^{n\times n} : UU^* = I_n\right\}. \tag{5}$$

Moreover, $L_G = L \cap G$ and $\Omega_G = \Omega \cap G$. Kiechle remarks in [7] that the construction of K-loops from classical groups over ordered fields can be generalized to K-loops from $GL(\mathcal{H})$ by using the polar decomposition theorem, where $GL(\mathcal{H})$ is the unit group of bounded linear operators over the Hilbert space $\mathcal{H}$.

In the second section we summarize Kerby and Wefelscheid's method in [10] to form K-loops from group transversals. This method enable us to extend the examples of K-loops not only from the purely algebraic groups, but also algebraic groups with additional structures such as groups with differentiable manifolds or topological groups.

In the third section we form infinite dimensional K-loops refer to Kiechle's remark not only from $GL(\mathcal{H})$, but also from some subgroups of $GL(\mathcal{H})$ such as symplectic and orthogonal classical Banach Lie groups.

2. Preliminaries

Let Q be a nonempty set and let $\oplus : Q \times Q \to Q$ be a binary operation. Consider the following axioms:

1. For all $a, b \in Q$ there exists a unique $x \in Q$ such that $a \oplus x = b$.
2. For all $a, b \in Q$ there exists a unique $y \in Q$ such that $y \oplus a = b$
3. There exists an $e \in Q$ satisfying $a \oplus e = e \oplus a = a$ for all $a \in Q$.

$(Q, \oplus)$ is called a ***right loop*** if (1) and (3) are satisfied, is called a ***left loop*** if (2) and (3) are satisfied. $(Q, \oplus)$ is a *loop* if (1), (2), and (3) are satisfied. A *K-loop*, $(Q, \oplus)$, is a loop which satisfies (6) (the left Bol identity) and (7) (the automorphic inverse property) for all a, b and c in Q.

$$a \oplus (b \oplus (a \oplus c)) = (a \oplus (b \oplus a)) \oplus c, \tag{6}$$

$$(a \oplus b)^{-1} = a^{-1} \oplus b^{-1}. \tag{7}$$

Kreuzer and Wefelscheid [10] undertook an axiomatic investigation and provided a new construction method for K-loops from the groups as follow:

Theorem 2.1. *Let G be a group. Let A be a subgroup of G and let K be a subset of G such that:*

1. *$G = KA$ is an exact decomposition, i.e., for every element $g \in G$ there are unique elements $k \in K$ and $a \in A$ such that $g = ka$.*
2. *If e is the neutral element of G, then $e \in K$.*
3. *For each $x \in K$, $xKx \subseteq K$.*
4. *For each $y \in A$, $yKy^{-1} \subseteq K$.*
5. *For each $k_1, k_2 \in K$ and $\alpha \in A$, if $k_1k_2\alpha \in K$, then there exists $\beta \in A$ such that $k_1k_2\alpha = \beta k_2k_1$.*

Then for all $a, b \in K$ there exists unique $a \oplus b \in K$ and $d_{a,b} \in A$ such that $ab = (a \oplus b)d_{a,b}$. Moreover, $(K, \oplus)$ is a K-loop.

2.1. Classical Banach-Lie Groups of bounded operators

In this section, we follow Pierre de la Harpe [3].

Let $\mathcal{H}$ be an infinite dimensional separable Hilbert space over $\mathbb{C}$. A semi-linear operator $J : \mathcal{H} \to \mathcal{H}$ is called *conjugation* if $\langle Jx, Jy\rangle = \overline{\langle x, y\rangle}$ and $J^2 = I$.

A semi-linear operator is called *anti-conjugation* if the last axiom is replaced by $J^2 = -I$. The conjugation and anti-conjugations will be denoted by $J_{\mathbb{R}}$ and $J_{\mathbb{Q}}$ respectively.

Examples of infinite dimensional classical complex Banach-Lie groups of bounded operators are given in [3]. Here we only focus $GL(\mathcal{H})$, $O(\mathcal{H}, J_{\mathbb{R}})$ and $Sp(\mathcal{H}, J_{\mathbb{Q}})$. Let $\mathcal{L}(\mathcal{H})$ be the set of bounded linear operators on $\mathcal{H}$, and let $GL(\mathcal{H})$ be the group of invertible operators in $\mathcal{L}(\mathcal{H})$. We use $Pos(\mathcal{H})$ and $U(\mathcal{H})$ to denote positive self-adjoint and unitary operators respectively. The Orthogonal and Symplectic Banach-Lie groups consist of those operators in $GL(\mathcal{H})$ that leave invariant the following bilinear forms respectively: $\mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C}$; $(x, y) \mapsto \langle x, J_{\mathbb{R}} y\rangle$ and $(x, y) \mapsto \langle x, J_{\mathbb{Q}} y\rangle$. Therefore the orthogonal and symplectic complex Banach-Lie groups can be defined by

1. $O(\mathcal{H}, J_{\mathbb{R}}) := \{T \in GL(\mathcal{H}) : \langle Tx, J_{\mathbb{R}} Ty\rangle = \langle x, J_{\mathbb{R}} y\rangle\}$,
2. $Sp(\mathcal{H}, J_{\mathbb{Q}}) := \{T \in GL(\mathcal{H}) : \langle Tx, J_{\mathbb{Q}} Ty\rangle = \langle x, J_{\mathbb{Q}} y\rangle\}$.

An operator $T \in \mathcal{L}(\mathcal{H})$ is called self-adjoint if $T = T^*$ i.e., $\langle Tx, y\rangle = \langle x, Ty\rangle$ for all $x, y \in \mathcal{H}$. If T is self-adjoint, then $\langle Tx, x\rangle$ is real for each $x \in \mathcal{H}$. If T is a self-adjoint operator we say that T is positive, $T \geqslant 0$, if and only if $\langle Tx, x\rangle \geqslant 0$ for all $x \in \mathcal{H}$.

Theorem 2.2 ([11]). *Let $T \in L(\mathcal{H})$. Then there is a $U \in L(\mathcal{H})$ such that:*

1. *$T = UA$, where $A = \sqrt{TT^*}$,*
2. *$\|Ux\| = \|x\|$ for $x \in \overline{R(A)}$,*
3. *$Ux = 0$ for $x \in \overline{R(A)}^{\perp}$.*

Remark 2.3. The closure of the range of A is closed, so $\mathcal{H} = \overline{R(A)} \oplus \overline{R(A)}^{\perp}$. If T is invertible, then TT^* and its positive square root are both invertible, hence U as well. Therefore, the only solution of $Ux = 0$ is $x = 0$, i.e., $\overline{R(A)}^{\perp} = \{0\}$, hence $\mathcal{H} = \overline{R(A)}$. That is U is an isometry on $\mathcal{H}$ (or U is unitary). The polar decomposition theorem is unique if T is invertible. There is also reverse polar decomposition theorem, i.e., for any $T \in GL(\mathcal{H})$ there exists unique $Q \in Pos(\mathcal{H})$ and $R \in U(\mathcal{H})$ such that $T = QR$. In this paper we always use the reverse (or left) polar decomposition theorem.

Corollary 2.4. *Let $T \in Sp(\mathcal{H}, J_{\mathbb{Q}})$, then there exists unique $U \in U(\mathcal{H}) \cap Sp(\mathcal{H}, J_{\mathbb{Q}})$ and $P \in Pos(\mathcal{H}) \cap Sp(\mathcal{H}, J_{\mathbb{Q}})$ such that $T = PU$.*

Proof. Let $T \in Sp(\mathcal{H}, J_{\mathbb{Q}}) \subseteq GL(\mathcal{H})$, then the reverse polar decomposition theorem for invertible operators indicates that T has already a unique decomposition $T = PU$, where $P = \sqrt{TT^*} \in Pos(\mathcal{H})$ and $U \in U(\mathcal{H})$. We only need to check that P and U are also elements of Symplectic Banach Lie group. If $T \in Sp(\mathcal{H}, J_{\mathbb{Q}})$, then $\langle Tx, J_{\mathbb{Q}} Ty\rangle = \langle x, J_{\mathbb{Q}} y\rangle$ for all $x, y \in \mathcal{H}$. Letting $x = y$ and using the linearity of the inner product yield that $T^* J_{\mathbb{Q}} T = J_{\mathbb{Q}}$, and this is equivalent to $T = J_{\mathbb{Q}}^{-1}(T^*)^{-1} J_{\mathbb{Q}}$. Replacing T with PU gives that

$$T = J_{\mathbb{Q}}^{-1}((PU)^*)^{-1} J_{\mathbb{Q}} = J_{\mathbb{Q}}^{-1} P^{-1} (U^*)^{-1} J_{\mathbb{Q}} = [J_{\mathbb{Q}}^{-1} P^{-1} J_{\mathbb{Q}}][J_{\mathbb{Q}}{}^{-1} (U^*)^{-1} J_{\mathbb{Q}}].$$

It can be easily verified that $J_{\mathbb{Q}}^{-1}P^{-1}J_{\mathbb{Q}} \in Pos(\mathcal{H})$ and $J_{\mathbb{Q}}{}^{-1}(U^*)^{-1}J_{\mathbb{Q}} \in U(\mathcal{H})$ by using the facts that $J_{\mathbb{Q}}J_{\mathbb{Q}}^* = I$ and $J_{\mathbb{Q}}^* = -J_{\mathbb{Q}}$. Uniqueness of the polar decomposition theorem forces that $J_{\mathbb{Q}}^{-1}P^{-1}J_{\mathbb{Q}} = P$ and $J_{\mathbb{Q}}{}^{-1}(U^*)^{-1}J_{\mathbb{Q}} = U$, so P and U are in $Sp(\mathcal{H}, J_{\mathbb{Q}})$. □

Corollary 2.5. *Let $T \in O(\mathcal{H}, J_{\mathbb{R}})$, then there exists unique $U \in U(\mathcal{H}) \cap O(\mathcal{H}, J_{\mathbb{R}})$ and $P \in Pos(\mathcal{H}) \cap O(\mathcal{H}, J_{\mathbb{R}})$ and such that $T = PU$.* □

3. Main results

Theorem 3.1. *Let G be one of the classical complex Banach-Lie groups in $\{GL(\mathcal{H}), O(\mathcal{H}, J_{\mathbb{R}}), Sp(\mathcal{H}, J_{\mathbb{Q}})\}$, and let $Pos(\mathcal{H})$ and $U(\mathcal{H})$ are collection of positive self-adjoint operators and unitary operators respectively over $\mathbb{C}$. Let $P_G := G \cap Pos(\mathcal{H})$, and $U_G := G \cap U(\mathcal{H})$. Then for all $A, B \in P_G$ there exist unique $A \oplus B \in P_G$ and $d_{A,B} \in U_G$ such that $AB = (A \oplus B)d_{A,B}$. Moreover, $(P_G, \oplus)$ is a K-loop.*

Proof. Let $A, B \in P_G$, then $A, B \in G$. G is a group, so $AB \in G$. By polar decomposition theorem there exists unique $M \in P_G$ and $N \in U_G$ such that $AB = MN$. If we let $M := A \oplus B$ and $N := d_{A,B}$, then $AB = (A \oplus B)d_{A,B}$. This decomposition is exact due to uniqueness of M and N.

It is clear that $A \oplus B = (AB)d_{A,B}^{-1}$ for all $A, B \in P_G$, hence $\oplus$ is a new binary operation for P_G induced by the group operation in G. We use the Theorem 2.1 to see $(P_G, \oplus)$ is a K-loop.

1. $G = P_G U_G$ is an exact decomposition by Theorem 2.2, Corollary 2.4, and Corollary 2.5.
2. The identity operator $I \in G$ since G is a group, and $\langle Ix, x\rangle = \langle x, x\rangle = \|x\|^2 \geqslant 0$ for all $x \in \mathcal{H}$, so I is positive. On the other hand $\langle x, x\rangle = \langle Ix, x\rangle = \langle x, Ix\rangle = \langle x, I^*x\rangle$ for all $x \in \mathcal{H}$. The last equality indicates that $I = I^*$, thus I is self-adjoint, thus $I \in P_G$.
3. $\langle (PQP)(x), x\rangle = \langle Q(P(x)), P^*(x)\rangle = \langle Q(P(x)), P(x)\rangle \geqslant 0$ for $P, Q \in P_G$ since Q is positive. Moreover, $(PQP)^* = (P^*)(Q^*)(P^*) = PQP$. Therefore, $PP_GP \subseteq P_G$ for all $P \in P_G$.
4. Let $T \in U_G$ and let $P \in P_G$. $T \in U_G$ implies that $T^* = T^{-1}$. To see $TPT^{-1} \in P_G$, observe that $\langle (TPT^{-1})(x), x\rangle = \langle P(T^{-1}(x)), T^*(x)\rangle = \langle P(T^{-1}(x)), T^{-1}(x)\rangle \geqslant 0$ since P is positive operator, and $(TPT^{-1})^* = (T^{-1})^*P^*T^* = (T^*)^*PT^{-1} = TPT^{-1}$, thus TPT^{-1} is positive and self-adjoint. Therefore, $TP_GT^{-1} \subseteq P_G$ for all $T \in U_G$.
5. Let $P, Q \in P_G$ and let $U \in U_G$. Notice that $U^* = U^{-1} \in U_G$ since U is unitary and U_G is a group. We want to show that if $PQU \in P_G$, then there exist $\beta \in U_G$ such that $PQU = \beta QP$. Assume that $PQU \in P_G$, so $(PQU)^* = PQU = U^*Q^*P^* = U^*QP$ where $U^* \in U_G$.

We conclude that $(P_G, \oplus)$ is a K-loop. □

References

[1] **A.S. Basarab**, *K-loops*, Izv. Akad. Nauk Respub. Moldova Mathematics **1** (1992), 28 – 33.

[2] **C. Chevalley**, *Theory of Lie Groups*, Princeton University Press (1976).

[3] **P. de la Harpe**, *Classical Banach-Lie algebras and Banach-Lie groups of operators in Hibert space*, Lecture Notes in Math. **285** (1972).

[4] **H. Karzel**, *Inzidenzgruppen I*, Lecture notes by I. Pieper and K. Sorensen, Universitat Hamburg (1965).

[5] **H. Karzel**, *Zusammenhange zwischen Fastberichen, scharf und zweifach transitiven Permutationsgruppen und* 2*-Strukturen mit Rechtecksaxiom*, Abh. Math. Sem. Univ. Hamburg (32) (1968), 191 – 206.

[6] **H. Kiechle**, *Theory of K-loops*, Springer-Verlag,Berlin Heidelberg New York (2002).

[7] **H. Kiechle**, *K-loops from classical groups over ordered fields*, J. Geom. **113** (1998), 105 – 127.

[8] **A.W. Knapp**, *Representation Theory of Semisimple Groups*, Princeton University Press, Princeton, New Jersey, (1986).

[9] **A. Kreuzer and H. Wefelscheid**, *The Maximal sub near-field of a near domain*, J. Algebra **28** (1974), 319 – 325.

[10] **A. Kreuzer and H. Wefelscheid**, *On K-loops of finite order*, Results in Math. **25** (1994), 79 – 102.

[11] **J.R. Retherford**, *Hilbert Space: Compact Operators and the Trace Theorem*, London Math. Soc. Student Texts, Cambridge University Press **27**, (1993).

[12] **R.U. Sexl and H.K. Urbantke**, *Relativity, groups, particles*, Springer Physics, Vienna, 2001. Special relativity and relativistic symmetry in field and particle physics, (1992).

[13] **L.R. Soikis**, *The special loops*, (Russian), Questions of the Theory of Quasigroups and Loops, Akad. Nauk Moldav. SSR, Kishinev (1970), 122 – 131.

[14] **A.A. Ungar**, *The Thomas rotation formalism underlying a nonassociative group structure for relativistic velocities*, Appl. Math Lett. **1** (1988), 403 – 405.

[15] **A.A. Ungar**, *The relativistic noncommutative nonassociative group of velocities and the Thomas rotation*, Results in Math. **16** (1989), 168 – 179.

[16] **A.A. Ungar**, *Thomas Precession: Its Underlying Gyrogroup Axioms and Their Use in hyperbolic Geometry and Relativistic Physics*, Foundations of Physics **27**, No. 6, (1997).

[17] **A.A. Ungar**, *Beyond the Einstein Addition Law and its Gyroscopic Thomas Precession: The Theory of Gyrogroups and Gyrovector Spaces*, **117** Fumdamental Theories of Physics, Kluwer Academic publisher Group, Dordrecht (2001).

Received June 25, 2015

Department of Mathematics, Western Michigan University, 1903 W Michigan Ave, Kalamazoo MI 49008-5248, USA

Department of Mathematics, American University of the Middle East, Block 3, Eqaila, Kuwait
E-mail: alper.bulut@aum.edu.kw

A note on (m,n)-ideals in regular duo ordered semigroups

Limpapat Bussaban and *Thawhat Changphas*

Abstract The purpose of this note is to prove that, for a regular duo ordered semigroup, every (m, n)-ideal is a two-sided ideal. The result obtained is more general than that of the result for regular duo semigroups (without order) proved by Lajos.

1. Introduction

Let S be a semigroup (without order). Then S is said to be *regular* if $a \in aSa$ for any $a \in S$, i.e., if for any $a \in S$ there exists $x \in S$ such that $a = axa$. The semigroup S is called a *duo semigroup* if every one-sided (left or right) ideal of S is a two-sided ideal of S. In [9], S. Lajos introduced the concept of (m, n)-ideal of S as follows: let m, n be non-negative integers. A subsemigroup A of S is called an *(m, n)-ideal* of S if

$$A^m S A^n \subseteq A.$$

Here, $A^0 S = SA^0 = S$. The author proved in [10] that every (m, n)-ideal of a regular duo semigroup is two-sided ideal.

In this paper, using the concept of (m, n)-ideals for ordered semigroups introduced and studied by J. Sanborisoot and the second author in [11], we extend the results obtained by S. Lajos in [10] to ordered semigroups.

A semigroup $(S, \cdot)$ together with a partial order $\leqslant$ that is *compatible* with the semigroup opration, that is, for any a, b, c in S,

$$a \leqslant b \Rightarrow ac \leqslant bc, \quad ca \leqslant cb,$$

is called an *ordered semigroup*.

The subset $(A]$ of S is defined to be the set of all elements $x \in S$ such that $x \leqslant a$ for some $a \in A$, that is,

$$(A] = \{x \in S \mid x \leqslant a \text{ for some } a \in A\}.$$

2010 Mathematics Subject Classification: 20M12, 20M17, 06F05

Keywords: semigroup, ordered semigroup, regular duo ordered semigroup, (m, n)-ideal, bi-ideal, π-ideal

The research was supported by the National Research Council of Thailand (NRCT), Project No. 580009

Note that the following conditions hold: (1) $A \subseteq (A]$; (2) $(A](B] \subseteq (AB]$; (3) If $A \subseteq B$, then $(A] \subseteq (B]$ (cf. [6]).

A non-empty subset A of an ordered semigroup $(S, \cdot, \leqslant)$ is called a *left* (resp. *right*) *ideal* of S if it satisfies the following conditions:

(i) $SA \subseteq A$ (resp. $AS \subseteq A$);

(ii) $(A] = A$.

And, A is called a *two-sided ideal*, or simply an *ideal* of S if it is both a left and a righ ideal of S [6, 8].

A subsemigroup B of an ordered semigroup $(S, \cdot, \leqslant)$ is called a *bi-ideal* [7] of S if it satisfies the following conditions:

(i) $BSB \subseteq B$;

(ii) $(B] = B$.

Let m, n be non-negative integers. A subsemigroup A of an ordered semigroup $(S, \cdot, \leqslant)$ is called an (m, n)*-ideal* of S if it satisfies the following conditions:

(i) $A^mSA^n \subseteq A$;

(ii) $(A] = A$.

Here, let $A^0S = SA^0 = S$ [11].

An ordered semigroup $(S, \cdot, \leqslant)$ is *regular* if, for every $a \in S$, $a \in (aSa]$, i.e., if for any $a \in S$, $a \leq axa$ for some $x \in S$ [7]. It was proved in [3] that the following holds for a regular ordered semigroup.

Theorem 1.1. *Let $(S, \cdot, \leqslant)$ be a regular ordered semigroup. Then a non-empty subset A of S is a bi-ideal of S if and only if there exists a left ideal L of S and a right ideal R of S such that $A = (RL]$.*

As in [9], the concept of π-ideal of an ordered semigroup $(S, \cdot, \leqslant)$ are defined by: a subsemigroup S_n of S will be called *attainable* if there are subsemigroups S_i $(i = 1, 2, \ldots, n-1)$ of S such that

$$S_n \subseteq S_{n-1} \subseteq \ldots \subseteq S_2 \subseteq S_1 \subseteq S_0 = S$$

holds, where S_i $(i = 1, 2, \ldots, n)$ is an one-sided (left or right) ideal of S_{i-1}. With every such chain above, we use the letters l (resp. r) in which the i-th for a subsemigroup S_i of S which is contained in S_{i-1} is a left (resp. a right) ideal of S_{i-1}. If S_i is a two-sided ideal of S_{i-1}, then either of l and of r can be choosen. And, a product of the letters l and r will be denoted by π. Now, a subsemigroup A of S will be called a π*-ideal* of S if A is attainable.

In what follows, for the product π, we let m and n be the numbers of the factors l and r, respectively. The following two theorems can be found in [2].

Theorem 1.2. *Let A be a subset of an ordered semigroup $(S, \cdot, \leqslant)$. Then the following three statements are equivalent:*

(1) *A is an lr-ideal of S;*

(2) *A is an rl-ideal of S;*

(3) *A is an* $(1,1)$*-ideal of* S.

Consequently,

Corollary 1.3. *Let* A *be a subset of an ordered semigroup* $(S,\cdot,\leqslant)$. *Then* A *is a* π*-ideal of* S *if and only if* A *is an* $r^m l^n$*-ideal of* S.

Theorem 1.4. *Let* $(S,\cdot,\leqslant)$ *be an ordered semigroup. Then a subset* A *of* S *is a* π*-ideal of* S *if and only if* A *is an* (m,n)*-ideal of* S.

2. Main results

An ordered semigroup $(S,\cdot,\leqslant)$ will be called a *duo ordered semigroup* if every one-sided (left or right) ideal of S is a two-sided ideal of S. An ordered semigroup S will be called a *regular duo ordered semigroup* if it is both regular and duo [3].

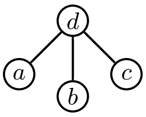
Example 2.1. Let $S=\{a,b,c,d\}$ be an ordered semigroup such that the multiplication and the partial order are defined by:

$\cdot$	a	b	c	d
a	c	d	d	d
b	c	c	d	d
c	d	d	d	d
d	d	d	d	d

$$\leq=\{(a,a),(b,b),(c,c),(d,d),(a,d),(b,d),(c,d)\}$$

We give a covering relation and the figure of S by:

$$\prec=\{(a,d),(b,d),(c,d)\}$$



Then we obtain $(S,\cdot,\leqslant)$ is a regular duo ordered semigroup.

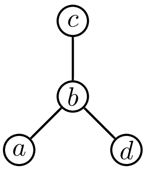
Example 2.2. Let $S=\{a,b,c,d\}$ be an ordered semigroup such that the multiplication and the partial order are defined by:

$\cdot$	a	b	c	d
a	d	b	b	d
b	b	b	b	b
c	b	b	c	b
d	d	b	b	d

$$\leq = \{(a,a),(b,b),(c,c),(d,d),(a,b),(a,c),(b,c),(d,b),(d,c)\}$$

We give a covering relation and the figure of S by:

$$\prec = \{(a,b),(d,b),(b,c)\}$$



Then we obtain $(S,\cdot,\leqslant)$ is a regular duo ordered semigroup.

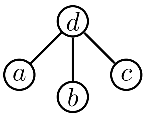
Example 2.3. Let $S=\{a,b,c,d\}$ be an ordered semigroup such that the multiplication and the partial order are defined by:

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	b	d
c	a	b	b	d
d	a	d	d	d

$$\leq = \{(a,a),(b,b),(c,c),(d,d),(a,d),(b,d),(c,d)\}$$

We give a covering relation and the figure of S as follows:

$$\prec = \{(a,d),(b,d),(c,d)\}$$



Then we obtain that $(S,\cdot,\leqslant)$ is a regular duo ordered semigroup.

The following theorem was shown in [3].

Theorem 2.4. *Let $(S,\cdot,\leqslant)$ be a regular duo ordered semigroup. Then every bi-ideal of S is a two-sided ideal of S.*

We now present the main result of this paper.

Theorem 2.5. *Let $(S,\cdot,\leqslant)$ be a regular duo ordered semigroup, and let m,n be non-negative integers such that $m+n>0$. Then every (m,n)-ideal of S is a two-sided ideal of S.*

Proof. Let A be an (m,n)-ideal of S; thus $A^m S A^n \subseteq A$ and $(A] = A$. There are four cases to consider:
CASE 1: $m = 0, n \neq 0$. If $n = 1$, then A is a left ideal of S; hence A is a two-sided ideal of S, since S is a regular duo ordered semigroup. Suppose that every $(0,k)$-ideal of S is a two-sided ideal of S for integers $k \geq 1$. Assume now that A is an $(0,k+1)$-ideal of S. By Theorem 1.4, there are subsemigroups $L_i (i = 1,2,\ldots,k)$ of S such that

$$A = L_{k+1} \subseteq L_k \subseteq L_{k-1} \subseteq \ldots \subseteq L_2 \subseteq L_1 \subseteq L_0 = S$$

where $L_{i-1}L_i \subseteq L_i (i = 1,2,3,\ldots,k+1)$.

We have

$$\begin{aligned} SA^k = SAA^{k-1} &\subseteq S(ASA]A^{k-1} \subseteq (SASA^k] \subseteq (L_1A^k] \subseteq (L_1L_2A^{k-1}] \\ &\subseteq (L_2A^{k-1}] \subseteq \ldots \subseteq (L_kA] \subseteq (A] = A. \end{aligned}$$

Hence A is an $(0,k)$-ideal of S, and so A is a two-sided ideal of S.

CASE 2: $m \neq 0, n = 0$. This can be proceed as the case before.

CASE 3: $m \neq 0, n \neq 0$. Let A be an $(1,n)$-ideal of S. If $n = 1$, then A is a bi-ideal of S. By Theorem 2.4, A is a two-sided ideal of S.

Let $n > 1$. By Theorem 1.4, there are subsemigroups $R, L_i (i = 1,2,\ldots,n-1)$ of S such that

$$A = L_n \subseteq L_{n-1} \subseteq L_{n-2} \subseteq \ldots \subseteq L_2 \subseteq L_1 \subseteq R \subseteq S$$

where $L_{i-1}L_i \subseteq L_i$ $(i = 2,3,\ldots,n)$, $RL_1 \subseteq L_1$, $RS \subseteq S$.

We consider

$$\begin{aligned} SA^n &\subseteq S(ASA]A^{n-1} \subseteq (SASA^n] \subseteq (RA^n] \subseteq (RL_1A^{n-1}] \\ &\subseteq (L_1A^{n-1}] \subseteq \ldots \subseteq (L_{n-1}A] \subseteq (A] = A. \end{aligned}$$

Then A is an $(0,n)$-ideal of S, and so A is a two-sided ideal of S.

Suppose that every (k,n)-ideal of S is a two-sided ideal of S for integer $k \geqslant 1$. Assume that A is an $(k+1,n)$-ideal of S. By Theorem 1.4, there are subsemigroups R_j $(j = 1,2,\ldots,k+1)$, L_i $(i = 1,2,\ldots,n-1)$ of S such that

$$\begin{aligned} A = L_n \subseteq L_{n-1} \subseteq L_{n-2} &\subseteq \ldots \subseteq L_2 \subseteq L_1 \\ &\subseteq R_{k+1} \subseteq R_k \subseteq \ldots \subseteq R_2 \subseteq R_1 \subseteq R_0 = S, \end{aligned}$$

where

$$L_{i-1}L_i \subseteq L_i \quad (i = 2,3,\ldots,n),$$

$$R_{k+1}L_1 \subseteq L_1,$$

$$R_jR_{j-1} \subseteq R_j \quad (j = 1,2,\ldots,k+1).$$

Consider:

$$\begin{aligned} A^kSA^n &\subseteq A^{k-1}(ASA]SA^n \subseteq (A^kSASA^n] \subseteq (A^kR_1A^n] \subseteq (A^{k-1}R_2R_1A^n] \\ &\subseteq (A^{k-1}R_2A^n] \subseteq \ldots \subseteq (R_{k+1}A^n] \subseteq (R_{k+1}L_1A^{n-1}] \subseteq (L_1A^{n-1}] \\ &\subseteq (L_1L_2A^{n-2}] \subseteq (L_2A^{n-2}] \subseteq \ldots \subseteq (L_{n-1}A] \subseteq (A] = A. \end{aligned}$$

Hence A is an (k,n)-ideal of S. Therefore, A is a two-sided ideal of S.

This completes the proof of the theorem. □

References

[1] **G. Birkhoff**, *Lattice Theory*, Amer. Math. Soc. Coll. Publ., Am. Math. Soc., R. I., Providence, 1984.

[2] **T. Changphas**, *Generalized ideals in ordered semigroups*, Far East J. Math. Sci. **65** (2013), 147–156.

[3] **T. Changphas**, *On regular duo ordered semigroups*, Far East J. Math. Sci. **65** (2013), 177–183.

[4] **T. Changphas**, *On (m,n)-ideals of an ordered semigroup*, Far East J. of Math. Sci. **88** (2014), 137–145.

[5] **L. Fuch**, *Partially Ordered Algebraic Systems*, Pregamon Press, 1963.

[6] **N. Kehayopulu**, *On weakly prime ideals of ordered semigroups*, Math. Japon. **35** (1990), 1051–1056.

[7] **N. Kehayopulu**, *On completely regular poe-semigroups*, Math. Japon. **37** (1992), 123–130.

[8] **N. Kehayopulu, G. Lepouras and M. Tsingelis**, *On right regular and right duo ordered semigroups*, Math. Japon. **46** (1997), 311–315.

[9] **S. Lajos**, *Generalized ideals in semigroups*, Acta Sci. Math. **22** (1961), 217–222.

[10] **S. Lajos**, *On (m,n)-ideals in regular duo semigroups*, Acta Sci. Math. **31** (1970), 179–180.

[11] **J. Sanborisoot, T. Changphas**, *On characterizations of (m,n)-regular ordered semigroups*, Far East J. Math. Sci. **65** (2012), 75–86.

Received June 16, 2015

Department of Mathematics, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
E-mail: lim.bussaban@gmail.com, thacha@kku.ac.th

Autotopisms of some quasigroups

Ivan I. Deriyenko

Abstract. We present one method of construction of some autotopisms for quasigroups satisfying the identity $\alpha(x) \cdot \beta(x \cdot y) = \gamma(y)$.

Denote by S_n the set of all permutations of the set $Q = \{1, 2, \ldots, n\}$. The triplet $A = (\omega, \varphi, \psi)$, where $\omega, \varphi, \psi \in S_n$, is called an *autotopism* of a quasigroup $(Q, \cdot)$ if

$$\omega(x \cdot y) = \varphi(x) \cdot \psi(y)$$

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

The set of all autotopisms of a quasigroup of order n form a group. The order of this group is a divisor of $(n!)^3$ but it cannot exceed $(n!)^2$. Moreover, two components of an autotopism determine the third one uniquely (see [1] or [5]). There are quasigroups that have only one (trivial) autotopism. Such quasigroups are called *super rigid*. The smallest super rigid quasigroups has 7 elements [3].

In this note we will consider quasigroups satisfying the identity

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

where $\alpha, \beta, \gamma \in S_n$. Such triplet of permutations will be denoted by $R = (\alpha, \beta, \gamma)$.

Note that parastrophes of a quasigroup satisfying (1) are pairwise isotopic [4].

Theorem 1. *A quasigroup $(Q, \cdot)$ satisfying the identity (1) has an autotopism of the form $(\gamma\beta, \alpha^2, \beta\gamma)$.*

Proof. Indeed, (1) implies

$$\beta(\alpha(x) \cdot \beta(x \cdot y)) = \beta\gamma(y).$$

Multiplying this identity by $\alpha^2(x)$ we obtain

$$\alpha^2(x) \cdot \beta(\alpha(x) \cdot \beta(x \cdot y)) = \alpha^2(x) \cdot \beta\gamma(y).$$

From this, applying (1) to the left side, we get

$$\gamma\beta(x \cdot y) = \alpha^2(x) \cdot \beta\gamma(y). \tag{2}$$

So, $A = (\gamma\beta, \alpha^2, \beta\gamma)$ is an autotopism of $(Q, \cdot)$. □

2010 Mathematics Subject Classification: 20N05, 05B15
Keywords: quasigroup, autotopism

Theorem 2. *A quasigroup* $(Q,\cdot)$ *satisfying* (1) *satisfies the identity*

$$\alpha_k(x)\cdot\beta_k(x\cdot y)=\gamma_k(y) \tag{3}$$

with $\alpha_k=\alpha^{3^k}$, $\beta_k=\beta(\gamma\beta)^{\frac{3^k-1}{2}}$, $\gamma_k=\gamma(\beta\gamma)^{\frac{3^k-1}{2}}$, *where* $k=0,1,\ldots,p-1$ *and* $\alpha_p=\alpha$, $\beta_p=\beta$, $\gamma_p=\gamma$.

Proof. Since a quasigroup $(Q,\cdot)$ satisfying (1) has an autotopism $A=(\gamma\beta,\alpha^2,\beta\gamma)$, from (1) we obtain

$$\gamma\beta\gamma(y)=\gamma\beta(\alpha(x)\cdot\beta(x\cdot y))=\alpha^2(\alpha(x))\cdot\beta\gamma(\beta(x\cdot y))=\alpha^3(x)\cdot\beta\gamma\beta(x\cdot y),$$

which means that in this quasigroup

$$\alpha_1(x)\cdot\beta_1(x\cdot y)=\gamma_1(y),$$

where $\alpha_1=\alpha^3,\ \ \beta_1=\beta\gamma\beta,\ \ \gamma_1=\gamma\beta\gamma.$

Thus, $(Q,\cdot)$ has an autotopism $A_1=(\gamma_1\beta_1,\alpha_1^2,\beta_1\gamma_1)$ and satisfies the identity

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

where $\alpha_2=\alpha_1^3=\alpha^{3^2}$, $\beta_2=\beta(\gamma\beta)^{\frac{3^2-1}{2}}$, $\gamma_2=\gamma(\beta\gamma)^{\frac{3^2-1}{2}}$, and so on. □

Corollary. *A quasigroup satisfying the identity* (1) *has an autotopism of the form* $A_k=(\omega_k,\varphi_k,\psi_k)$ *with* $\omega_k=\gamma_k\beta_k=(\gamma\beta)^{3^k}$, $\varphi_k=\alpha_k^2=\alpha^{2\cdot 3^k}$, $\psi_k=\beta_k\gamma_k=(\beta\gamma)^{3^k}$, *where* $k=0,1,\ldots,p-1$ *and* $\omega_p=\omega$, $\varphi_p=\varphi$, $\psi_p=\psi$. *Moreover, then* $\alpha_{k+1}=\varphi_k\alpha_k$, $\beta_{k+1}=\psi_k\beta_k$, $\gamma_{k+1}=\omega_k\gamma_k$.

Example. A quasigroup determined by the table

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

is an isotope of a quasigroup defined in [2]. This quasigroup satisfies (1) with $\alpha=(1287465.3.)$, $\beta=(18.46.2.357.)$, $\gamma=(175.28.34.6.)$, where (175.28.34.6.) means that this permutation is a composition of cycles (175), (28) and (34).

Let $R=(\alpha,\beta,\gamma)$, where α,β,γ are as in the above. According to Theorem 1 this quasigroup has an autotopism $A=(\omega,\varphi,\psi)$ such that

$$\omega=\gamma\beta=(1287463.5.),\quad \varphi=\alpha^2=(1845276.3.),\quad \psi=\beta\gamma=(1364582.7.).$$

By Theorem 2, this quasigroup satisfies (3) with $R_1 = (\alpha_1, \beta_1, \gamma_1)$, where, in view of Corrollary, $\alpha_1, \beta_1, \gamma_1$ have the form

$$\alpha_1 = \varphi\alpha = (1758624.3.), \quad \beta_1 = \psi\beta = (12.38.4.576.), \quad \gamma_1 = \omega\gamma = (14.275.36.8.).$$

Then we compute $A_1 = (\omega_1, \varphi_1, \psi_1)$ and $R_2 = (\alpha_2, \beta_2, \gamma_2)$:

$$\begin{cases} \omega_1 = \gamma_1\beta_1 = (1738624.5.), \\ \varphi_1 = \alpha_1^2 = (1564782.3.), \\ \psi_1 = \beta_1\gamma_1 = (1426835.7.), \end{cases} \quad \text{and} \quad \begin{cases} \alpha_2 = \varphi_1\alpha_1 = (1845276.3.), \\ \beta_2 = \psi_1\beta_1 = (16.24.3.578.), \\ \gamma_2 = \omega_1\gamma_1 = (1.23.475.68.). \end{cases}$$

$A_2 = (\omega_2, \varphi_2, \psi_2)$ and $R_3 = (\alpha_3, \beta_3, \gamma_3)$:

$$\begin{cases} \omega_2 = \gamma_2\beta_2 = (1843276.5.), \\ \varphi_2 = \alpha_2^2 = (1426857.3.), \\ \psi_2 = \beta_2\gamma_2 = (1652348.7.), \end{cases} \quad \text{and} \quad \begin{cases} \alpha_3 = \varphi_2\alpha_2 = (1564782.3.), \\ \beta_3 = \psi_2\beta_2 = (157.28.34.6.), \\ \gamma_3 = \omega_2\gamma_2 = (18.2.3.46.375.). \end{cases}$$

$A_3 = (\omega_3, \varphi_3, \psi_3)$ and $R_4 = (\alpha_4, \beta_4, \gamma_4)$:

$$\begin{cases} \omega_3 = \gamma_3\beta_3 = (1364782.5.), \\ \varphi_3 = \alpha_3^2 = (1672548.3.), \\ \psi_3 = \beta_3\gamma_3 = (1285463.7.), \end{cases} \quad \text{and} \quad \begin{cases} \alpha_4 = \varphi_3\alpha_3 = (1426857.3.), \\ \beta_4 = \psi_3\beta_3 = (14.257.36.8.), \\ \gamma_4 = \omega_3\gamma_3 = (12.38.4.567.). \end{cases}$$

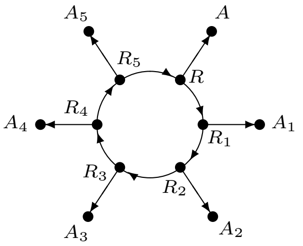
$A_4 = (\omega_4, \varphi_4, \psi_4)$ and $R_5 = (\alpha_5, \beta_5, \gamma_5)$:

$$\begin{cases} \omega_4 = \gamma_4\beta_4 = (1426837.5.), \\ \varphi_4 = \alpha_4^2 = (1287465.3.), \\ \psi_4 = \beta_4\gamma_4 = (1538624.7.), \end{cases} \quad \text{and} \quad \begin{cases} \alpha_5 = \varphi_4\alpha_4 = (1672548.3.), \\ \beta_5 = \psi_4\beta_4 = (1.23.457.68.), \\ \gamma_5 = \omega_4\gamma_4 = (16.24.3.587.). \end{cases}$$

$A_5 = (\omega_5, \varphi_5, \psi_5)$ and $R_6 = (\alpha_6, \beta_6, \gamma_6)$:

$$\begin{cases} \omega_5 = \gamma_5\beta_5 = (1672348.5.), \\ \varphi_5 = \alpha_5^2 = (1758624.3.), \\ \psi_5 = \beta_5\gamma_5 = (1843256.7.), \end{cases} \quad \text{and} \quad \begin{cases} \alpha_6 = \varphi_5\alpha_5 = (1287465.3.) = \alpha, \\ \beta_6 = \psi_5\beta_5 = (18.46.2.357.) = \beta, \\ \gamma_6 = \omega_5\gamma_5 = (175.28.34.6.) = \gamma. \end{cases}$$

Relationships between A_i and R_i we can present by the following graph.



The set autotopisms $A, A_1, A_2, A_3, A_4, A_5$ together with the identity autotopism $E = (\varepsilon, \varepsilon, \varepsilon)$ forma a cyclic group of order 7. The group of all autotopisms of this quasigroup has 42 elements.

Note also that in this quasigroup the identity (1) also is satisfied with $\alpha = \varepsilon$ (the identity permutation) and $\beta = \gamma = (13.48.26.57.)$. So, in this case $R = (\varepsilon, \beta, \beta)$, and consequently $A = (\varepsilon, \varepsilon, \varepsilon)$, $R_1 = R$, $A_1 = A$.

Remark. A similar results can be obtained for quasigroups satisfying one of the identities

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

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

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

$$\beta(xy) = \gamma(y) \cdot \alpha(x), \tag{7}$$

where α, β, γ are fixed permutations of the set Q, used in [4] to the description of isotopy classes of parastrophes.

References

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

[2] **D. Bryanta, M. Buchanana and I.M. Wanless**, *The spectrum for quasigroups with cyclic automorphisms and additional symmetries*, Discrete Math. **309** (2009), 821 – 833.

[3] **A.I. Deriyenko, I.I. Deriyenko, W.A. Dudek**, *Rigid and super rigid quasigroups*, Quasigroups and Related Systems **17** (2009), 17 – 28.

[4] **W.A. Dudek**, *Parastrophes of quasigroups*, Quasigroups and Related Systems **23** (2015), 221 – 230.

[5] **A. D. Keedwell and J. Dénes**, *Latin squares and their applications*, Second edition, Elsevier, 2015.

Received November 28, 2015

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 **23** (2015), 221 − 230

Parastrophes of quasigroups

Wieslaw A. Dudek

Abstract. Parastrophes (conjugates) of a quasigroup can be divided into separate classes containing isotopic parastrophes. We prove that the number of such classes is always 1, 2, 3 or 6. Next we characterize quasigroups having a fixed number of such classes.

1. Introduction

Denote by S_Q the set of all permutations of the set Q. We say that a quasigroup $(Q,\cdot)$ is *isotopic* to $(Q,\circ)$ if there are $\alpha,\beta,\gamma\in S_Q$ such that $\alpha(x)\circ\beta(y)=\gamma(x\cdot y)$ for all $x,y\in Q$. The triplet (α,β,γ) is called an *isotopism.* Quasigroups $(Q,\cdot)$ and $(Q,\circ)$ for which there are $\alpha,\beta,\gamma\in S_Q$ such that $\alpha(x)\circ\beta(y)=\gamma(y\cdot x)$ for all $x,y\in Q$ are called *anti-isotopic.* This fact is denoted by $(Q,\cdot)\sim(Q,\circ)$. In the case when $(Q,\cdot)$ and $(Q,\circ)$ are isotopic we write $(Q,\cdot)\approx(Q,\circ)$. It is clear that the relation $\approx$ is an equivalence and divides all quasigroups into disjoint classes containing isotopic quasigroups.

Each quasigroup $Q=(Q,\cdot)$ determines five new quasigroups $Q_i=(Q,\circ_i)$ with the operations $\circ_i$ defined as follows:

$$\begin{aligned}
x\circ_1 y=z &\longleftrightarrow x\cdot z=y\\
x\circ_2 y=z &\longleftrightarrow z\cdot y=x\\
x\circ_3 y=z &\longleftrightarrow z\cdot x=y\\
x\circ_4 y=z &\longleftrightarrow y\cdot z=x\\
x\circ_5 y=z &\longleftrightarrow y\cdot x=z
\end{aligned}$$

Such defined (not necessarily distinct) quasigroups are called *parastrophes* or *conjugates* of Q. Traditionally they are denoted as

$$Q_1=Q^{-1}=(Q,\backslash),\quad Q_2={}^{-1}Q=(Q,/),\quad Q_3={}^{-1}(Q^{-1})=(Q_1)_2,$$
$$Q_4=({}^{-1}Q)^{-1}=(Q_2)_1\ \text{ and }\ Q_5=({}^{-1}(Q^{-1}))^{-1}=((Q_1)_2)_1=((Q_2)_1)_2.$$

Each parastrophe Q_i can be obtained from Q by the permutation σ_i, where $\sigma_1=(23)$, $\sigma_2=(13)$, $\sigma_3=(132)$, $\sigma_4=(123)$, $\sigma_5=(12)$.

Generally, parastrophes Q_i do not save properties of Q. Parastrophes of a group are not a group, but parastrophes of an idempotent quasigroup also are idempotent

2010 Mathematics Subject Classification: 20N05, 05B15
Keywords: quasigroup, isotopism, anti-isotopism, conjugate quasigroup, parastrophe.

quasigroups. Moreover, in some cases (described in [7]) parastrophes of a given quasigroup Q are pairwise equal or all are pairwise distinct (see also [2] and [8]). In [7] it is proved that the number of distinct parastrophes of a quasigroup is always a divisor of 6 and does not depend on the number of elements of a quasigroup.

Parastrophes of each quasigroup can be divided into separate classes containing isotopic parastrophes. We prove that the number of such classes is always 1, 2, 3 or 6. The number of such classes depends on the existence of an anti-isotopism of a quasigroup and some parastrophe of it.

2. Classification of parastrophes

As it is known (see for example [1]) a quasigroup $(Q,\cdot)$ can be considered as an algebra $(Q,\cdot,\backslash,/)$ with three binary operations satisfying the following axioms

$$x(x\backslash z)=z,\quad (z/y)y=z,\quad x\backslash xy=y,\quad xy/y=x,$$

where

$$x\backslash z=y\longleftrightarrow xy=z\quad\text{and}\quad z/y=x\longleftrightarrow xy=z.$$

We will use these axioms to show the relationship between parastrophes. But let's start with the following simple observation.

Lemma 2.1. *Let Q be a quasigroup. Then*

(a) $xy=y\circ_5 x,\ \ x\circ_1 y=y\circ_3 x,\ \ x\circ_2 y=y\circ_4 x,$

(b) $Q\sim Q_5,\ \ Q_1\sim Q_3,\ \ Q_2\sim Q_4,$

(c) $xy=yx\longleftrightarrow Q=Q_5\longleftrightarrow Q_1=Q_3\longleftrightarrow Q_2=Q_4,$

(d) $Q_1=Q\longleftrightarrow Q_2=Q_3\longleftrightarrow Q_4=Q_5,$

(e) $Q_2=Q\longleftrightarrow Q_1=Q_4\longleftrightarrow Q_3=Q_5.$

To describe the relationship between the parastrophes, we will need these two simple lemmas.

Lemma 2.2. *Let A,B,C,D be quasigroups. Then*

(a) $A\sim B,\ B\sim C\longrightarrow A\approx C,$

(b) $A\sim B,\ B\approx C\longrightarrow A\sim C,$

(c) $A\approx B,\ B\sim C\longrightarrow A\sim C.$

Lemma 2.3. *Let Q_i° be the i-th parastrophe of the quasigroup $Q^\circ=(Q,\circ)$. Then*

(a) $Q\approx Q^\circ$ *implies* $Q_i\approx Q_i^\circ$ *for each* $i=1,2,3,4,5,$

(b) $Q_i\approx Q_i^\circ$ *for some* $i=1,2,3,4,5$ *implies* $Q\approx Q^\circ.$

(c) *Moreover, if* $Q\approx Q^\circ$, *then for each* $i=1,\dots,5$

$$Q\sim Q_i\longleftrightarrow Q^\circ\sim Q_i^\circ,\ \textit{and}\ \ Q\approx Q_i\longleftrightarrow Q^\circ\approx Q_i^\circ.$$

Now we will present a series of lemmas about anti-isotopies of quasigroups and their parastrophes.

Lemma 2.4. $Q \sim Q \longleftrightarrow Q \approx Q_5 \longleftrightarrow Q_1 \approx Q_3 \longleftrightarrow Q_2 \approx Q_4$.

Proof. Indeed,

$$Q \sim Q \longleftrightarrow \gamma(xy) = \alpha(y)\beta(x) \longleftrightarrow \gamma(xy) = \beta(x) \circ_5 \alpha(y) \longleftrightarrow Q \approx Q_5.$$

Also

$$Q \sim Q \longleftrightarrow \gamma(xy) = \alpha(y)\beta(x) \longleftrightarrow \gamma(z) = \alpha(y)\beta(z/y) \longleftrightarrow \alpha(y)\backslash\gamma(z) = \beta(z/y).$$

Thus $Q \sim Q \longleftrightarrow Q_1 \sim Q_2$. Moreover,

$$\begin{aligned} Q_1 \sim Q_2 &\longleftrightarrow \alpha(y)\backslash\gamma(z) = \beta(z/y) \longleftrightarrow \gamma(z) = \alpha(y)\beta(z/y) \\ &\longleftrightarrow \beta(z/y) = \gamma(z) \circ_4 \alpha(y) \longleftrightarrow Q_2 \approx Q_4. \end{aligned}$$

Similarly, for some $\alpha', \beta', \gamma' \in S_Q$ we have

$$\begin{aligned} Q_1 \sim Q_2 &\longleftrightarrow \gamma'(x/y) = \alpha'(y)/\beta'(x) \longleftrightarrow \gamma'(x\backslash y)\beta'(x) = \alpha'(y) \\ &\longleftrightarrow \gamma'(x\backslash y) = \beta'(x) \circ_3 \alpha'(y) \longleftrightarrow Q_1 \approx Q_3. \end{aligned}$$

This completes the proof. □

Lemma 2.5. $Q \sim Q_1 \longleftrightarrow Q \sim Q_2 \longleftrightarrow Q_1 \approx Q_2$.

Proof. Indeed, according to the definition of the operations $\backslash$ and $/$, we have

$$\gamma(x\backslash z) = \alpha(z)\beta(x) \longleftrightarrow \gamma(y) = \alpha(xy)\beta(x) \longleftrightarrow \alpha(xy) = \gamma(y)/\beta(x).$$

So, $Q_1 \sim Q \longleftrightarrow Q \sim Q_2$, which by Lemma 2.2 implies $Q_1 \approx Q_2$.

Conversely, if $Q_1 \approx Q_2$, then $\gamma(x\backslash y) = \alpha(x)/\beta(y)$, i.e., $\gamma(x\backslash y)\beta(y) = \alpha(x)$ for some $\alpha, \beta, \gamma \in S_Q$. From this, for $y = xz$, we obtain $\gamma(z)\beta(xz) = \alpha(x)$, i.e., $\beta(xz) = \gamma(z)\backslash\alpha(x)$. Thus, $Q \sim Q_1$, and consequently, also $Q \sim Q_2$. □

Lemma 2.6. *For any quasigroup* Q

(a) $Q_1 \sim Q \longleftrightarrow Q_1 \sim Q_3 \longleftrightarrow Q \approx Q_3 \longleftrightarrow Q_1 \approx Q_5$,

(b) $Q_2 \sim Q \longleftrightarrow Q_2 \sim Q_4 \longleftrightarrow Q \approx Q_4 \longleftrightarrow Q_2 \approx Q_5$.

Proof. Replacing in Lemma 2.5 a quasigroup Q by Q_1 we get the first two equivalences. The third equivalence is a consequence of Lemma 2.3.

Similarly, replacing Q by Q_2 we obtain (b). □

Lemma 2.7. $Q_3 \sim Q \longleftrightarrow Q \approx Q_2 \longleftrightarrow Q_1 \approx Q_4 \longleftrightarrow Q_3 \approx Q_5$.

Proof. Obviously $Q_3 \sim Q \longleftrightarrow Q_3 \approx Q_5$. Moreover,

$$Q_3 \sim Q \longleftrightarrow \gamma(xy)\alpha(y) = \beta(x) \longleftrightarrow \gamma(xy) = \beta(x)/\alpha(y) \longleftrightarrow Q \approx Q_2.$$

Analogously, $xy = z$ we obtain

$$Q_3 \sim Q \longleftrightarrow \gamma(z)\alpha(x\backslash z) = \beta(x) \longleftrightarrow Q_1 \approx Q_4.$$

This completes the proof. □

Lemma 2.8. $Q_4 \sim Q \longleftrightarrow Q \approx Q_1 \longleftrightarrow Q_2 \approx Q_3 \longleftrightarrow Q_4 \approx Q_5$.

Proof. Of course $Q_4 \sim Q \longleftrightarrow Q_4 \approx Q_5$. Since $Q_4 \sim Q \longleftrightarrow \beta(x)\gamma(xy) = \alpha(y)$, we obtain $Q_4 \sim Q \longleftrightarrow Q \approx Q_1$ and $Q_4 \sim Q \longleftrightarrow Q_2 \approx Q_3$ for $x = z/y$. □

Theorem 2.9. *All parastrophes of a quasigroup Q are isotopic to Q if and only if $Q \sim Q$ and $Q \sim Q_i$ for some $i = 1, 2, 3, 4$.*

Proof. If $Q \sim Q$, then, by Lemma 2.4, we have $Q \approx Q_5$, $Q_1 \approx Q_3$ and $Q_2 \approx Q_4$. This for $Q \sim Q_i$, $i = 1, 2, 3, 4$, by Lemmas 2.6, 2.7 and 2.8, gives $Q \approx Q_1 \approx Q_2 \approx Q_3 \approx Q_4 \approx Q_5$. So, in this case all parastrophes are isotopic to Q.

The converse statement is obvious. □

Corollary 2.10. *If $Q \sim Q$ and $Q \sim Q_i$ for some $i = 1, 2, 3, 4$, then also $Q \sim Q_i$ for other $i = 1, 2, 3, 4, 5$.*

Theorem 2.11. *A quasigroup Q has exactly two classes of isotopic parastrophes if and only if*

(1) *$Q \not\sim Q$, $Q \sim Q_1$ and $Q \not\sim Q_i$ for $i = 2, 3, 4$, or equivalently,*

(2) *$Q \not\sim Q$, $Q \sim Q_2$ and $Q \not\sim Q_i$ for $i = 1, 3, 4$.*

In this case $Q \approx Q_3 \approx Q_4$ and $Q_1 \approx Q_2 \approx Q_5$.

Proof. Let Q have exactly two classes of isotopic parastrophes. Then it must be true that $Q \approx Q_i$ for some $i = 1, 2, 3, 4, 5$ because $Q \not\approx Q_i$ for all $i = 1, 2, 3, 4, 5$ gives $Q_1 \approx Q_j$ for some j which by previous lemmas implies $Q \approx Q_k$ for some k.

Case $Q \approx Q_1$. In this case $Q_2 \approx Q_3$ and $Q_4 \approx Q_5$ (Lemma 2.8). So, the following classes of isotopic parastrophes are possible:

1) $\{Q, Q_1, Q_2, Q_3\}$, $\{Q_4, Q_5\}$,

2) $\{Q, Q_1, Q_4, Q_5\}$, $\{Q_2, Q_3\}$,

3) $\{Q, Q_1\}$, $\{Q_2, Q_3, Q_4, Q_5\}$.

In the first case from $Q_1 \approx Q_3$, by Lemma 2.4, we conclude $Q \approx Q_5$ which shows that in this case we have only one class. This contradics our assumption on the number of classes. So, this case is impossible.

In the second case, $Q \approx Q_5$, by the same lemma, implies $Q_2 \approx Q_4$ which (similarly as in previous case) is impossible. Also the third case is impossible because $Q_2 \approx Q_4$ leads to $Q_1 \approx Q_3$. Hence must be $Q \not\approx Q_1$.

Case $Q \approx Q_2$. Then, according to Lemma 2.7, $Q_1 \approx Q_4$ and $Q_3 \approx Q_5$. Thus

1) $\{Q, Q_1, Q_2, Q_4\}$, $\{Q_3, Q_5\}$, or

2) $\{Q, Q_2, Q_3, Q_5\}$, $\{Q_1, Q_4\}$, or

3) $\{Q, Q_2\}$, $\{Q_1, Q_3, Q_4, Q_5\}$.

Using the same argumentation as in the case $Q \approx Q_1$ we can see that the case $Q \approx Q_2$ is impossible.

Case $Q \approx Q_3$. By Lemmas 2.1, 2.2 and 2.5 only the following classes are possible: $\{Q, Q_3, Q_4\}$ and $\{Q_1, Q_2, Q_5\}$. In this case $Q \not\sim Q$ (Lemma 2.4) and $Q \sim Q_1$ (Lemma 2.6). Then also $Q \sim Q_2$ (Lemma 2.5).

Case $Q \approx Q_4$. Analogously as $Q \approx Q_3$.

Case $Q \approx Q_5$. Then $Q_1 \approx Q_3$ and $Q_2 \approx Q_4$. Is a similar way as for $Q \approx Q_1$ we can verify that this case is not possible.

So, if Q has exactly two classes of isotopic parastrophes, then $Q \not\sim Q$ and $Q \sim Q_1$, or $Q \not\sim Q$ and $Q \sim Q_2$.

Conversely, if $Q \not\sim Q$ and $Q \sim Q_1$, or equivalently, $Q \not\sim Q$ and $Q \sim Q_2$, then by Lemmas 2.5 and 2.6 we have two classes: $\{Q, Q_3, Q_4\}$ and $\{Q_1, Q_2, Q_5\}$. Since $Q_1 \not\approx Q_3$ (Lemma 2.4), these classes are disjoint. □

Theorem 2.12. *A quasigroup Q has exactly three classes of isotopic parastrophes if and only if*

(1) *$Q \not\sim Q$, $Q \sim Q_3$ and $Q \not\sim Q_i$ for $i = 1, 2, 4$, or*

(2) *$Q \not\sim Q$, $Q \sim Q_4$ and $Q \not\sim Q_i$ for $i = 1, 2, 3$, or*

(3) *$Q \sim Q$, $Q \sim Q_5$ and $Q \not\sim Q_i$ for $i = 1, 2, 3, 4$.*

In the first case we have $\{Q, Q_2\}$, $\{Q_1, Q_4\}$ and $\{Q_3, Q_5\}$; in the second $\{Q, Q_1\}$, $\{Q_2, Q_3\}$ and $\{Q_4, Q_5\}$; in the third $\{Q, Q_5\}$, $\{Q_1, Q_3\}$ and $\{Q_2, Q_4\}$.

Proof. Suppose that a quasigroup Q has exactly three classes of isotopic parastrophes. From the above lemmas it follows that in this case $Q \approx Q_i$ for some i.

Case $Q \approx Q_1$. Then, by Lemma 2.8, we have three classes $\{Q, Q_1\}$, $\{Q_2, Q_3\}$, $\{Q_4, Q_5\}$ and $Q \sim Q_4$. Since $Q_1 \not\approx Q_3$ we also have $Q \not\sim Q$ (Lemma 2.4).

Case $Q \approx Q_2$. In this case $\{Q, Q_2\}$, $\{Q_1, Q_4\}$, $\{Q_3, Q_5\}$ and $Q \sim Q_3$ (Lemma 2.7). Analogously as in the previous case $Q_1 \not\approx Q_3$ gives $Q \not\sim Q$.

Case $Q \approx Q_3$. This case is impossible because by Lemmas 2.5 and 2.6 it leads to two classes.

Case $Q \approx Q_4$. Analogously as $Q \approx Q_3$.

Case $Q \approx Q_5$. Then $Q_1 \approx Q_3$, $Q_2 \approx Q_4$ and $Q \sim Q$. Since classes $\{Q, Q_5\}$, $\{Q_1, Q_3\}$, $\{Q_2, Q_5\}$ are disjoint $Q \not\sim Q_i$ for each $i = 1, 2, 3, 4$.

The converse statement is obvious. □

As a consequence of the above results we obtain

Corollary 2.13. *Parastrophes of a quasigroup Q are non-isotopic if and only if $Q \not\sim Q$ and $Q \not\sim Q_i$ for all $i = 1, 2, 3, 4$.*

Corollary 2.14. *The number of non-isotopic parastrophes of a quasigroup Q is always* 1, 2, 3, *or* 6.

Depending on the relationship between parastrophes quasigroups can be divided into six types presented below.

type	classes of isotoipic parastrophes
A	$\{Q, Q_1, Q_2, Q_3, Q_4, Q_5\}$
B	$\{Q, Q_3, Q_4\}$, $\{Q_1, Q_2, Q_5\}$
C	$\{Q, Q_2\}$, $\{Q_1, Q_4\}$, $\{Q_3, Q_5\}$
D	$\{Q, Q_1\}$, $\{Q_2, Q_3\}$, $\{Q_4, Q_5\}$
E	$\{Q, Q_5\}$, $\{Q_1, Q_3\}$, $\{Q_2, Q_4\}$
F	$\{Q\}$, $\{Q_1\}$, $\{Q_2\}$, $\{Q_3\}$, $\{Q_4\}$, $\{Q_5\}$

Our results are presented in the following table where "+" means that the corresponding relation holds. The symbol "−" means that this relation has no place.

$Q \sim Q$	+	−	−	−	−	+	−	$Q \approx Q_5$
$Q \sim Q_1$	+	+	−	−	−	−	−	$Q \approx Q_3$
$Q \sim Q_2$	+	−	+	−	−	−	−	$Q \approx Q_4$
$Q \sim Q_3$	+	−	−	+	−	−	−	$Q \approx Q_2$
$Q \sim Q_4$	+	−	−	−	+	−	−	$Q \approx Q_1$
type	A	B	B	C	D	E	F	

The parastrophe Q_5 plays no role in our research since always is $Q \sim Q_5$.

3. Parastrophes of selected quasigroups

In this section we present characterizations of parastrophes of several classical types of quasigroups. We start with parastrophes of IP-quasigroups.

As a consequence of our results, we get the following well-known fact (see for example [1])

Proposition 3.1. *All parastrophes of an IP-quasigroup are isotopic.*

Proof. Indeed, in any IP-quasigroup Q there are permutations $\alpha, \beta \in S_Q$ such that $\alpha(x) \cdot xy = y = yx \cdot \beta(x)$ for all $x, y \in Q$. So, $Q \approx Q_1 \approx Q_2$, i.e., Q is a quasigroup of type A. □

Corollary 3.2. *Parastrophes of a group are isotopic.*

The same is true for the parastrophes of Moufang quasigroups since groups and Moufang quasigroups are IP-quasigroups.

Also parastrophes of T-quasigroups, linear and alinear quasigroups (studied in [3]) are isotopic. This fact follows from more general result proved below.

Theorem 3.3. *All parastrophes of a quasigroup isotopic to a group are isotopic.*

Proof. Let $G = (G, \circ)$ be a group. Then $\varphi(x \circ y) = \varphi(y) \circ \varphi(x)$ for $\varphi(x) = x^{-1}$. Since $(Q, \cdot) \approx (G, \circ)$, for some α, β, γ we have

$$\gamma(xy) = \alpha(x) \circ \beta(y) = \varphi^{-1}(\varphi\beta(y) \circ \varphi\alpha(x)) = \varphi^{-1}\gamma\left(\alpha^{-1}\varphi\beta(y) \cdot \beta^{-1}\varphi\alpha(x)\right).$$

Thus $\gamma^{-1}\varphi\gamma(xy) = \alpha^{-1}\varphi\beta(y) \cdot \beta^{-1}\varphi\alpha(x)$. So, $Q \sim Q$.

Moreover, from $\gamma(xy) = \alpha(x) \circ \beta(y)$ for $xy = z$ we obtain

$$\alpha(x) \backslash\!\!\backslash \gamma(z) = \beta(x \backslash z) \quad \text{and} \quad \gamma(z) /\!\!/ \beta(y) = \alpha(z/y),$$

where $\backslash\!\!\backslash$ and $/\!\!/$ are inverse operations in a group G. Thus $Q_1 \approx G_1$ and $Q_2 \approx G_2$. Since $G \approx G_1 \approx G_2$, also $Q \approx Q_1 \approx Q_2$. This shows that a quasigroup isotopic to a group is a quasigroup of type A. Hence (Lemma 2.3) all its parastrophes are isotopic. □

D-loops (called also *loops with anti-automorphic property*) are defined as loops with the property $(xy)^{-1} = y^{-1}x^{-1}$, where x^{-1} denotes the inverse element [5].

Theorem 3.4. *Let Q be a D-loop. Then*

(1) *all parastrophes of Q coincide with Q, or*

(2) *Q has three classes of isotopic parastrophes: $\{Q, Q_5\}$, $\{Q_1, Q_3\}$, $\{Q_2, Q_4\}$.*

The second case holds if and only if $Q \not\sim Q_1$ or $Q \not\approx Q_1$.

Proof. Let Q be a D-loop. Then $Q \sim Q$. Thus all its parastrophes are isotopic to Q or they are divided into three classes $\{Q, Q_5\}$, $\{Q_1, Q_3\}$, $\{Q_2, Q_4\}$ (see Table). By Lemmas 2.6 and 2.8 they are disjoint if and only if $Q \not\sim Q_1$ or $Q \not\approx Q_1$. □

Corollary 3.5. *A D-loop Q has three classes of isotopic parastrophes if and only if $Q \not\sim Q_2$ or $Q \not\approx Q_2$.*

In [5] is proved that parastrophes of a D-loop Q are isomorphic to one of the quasigroups Q, Q_1, Q_2. Comparing this fact with our results we obtain

Theorem 3.6. *For a D-loop Q the following conditions are equivalent:*

(1) *all parastrophes of Q are isomorphic,*

(2) *Q and Q_1 are isomorphic,*

(3) *Q and Q_2 are isomorphic,*

(4) *Q_1 and Q_2 are isomorphic.*

Example 3.7. Consider the following three loops.

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

$\circ_1$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	5	6	4	3
3	3	4	1	5	6	2
4	4	3	6	1	2	5
5	5	6	2	3	1	4
6	6	5	4	2	3	1

$\circ_2$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	5	1	6	2	4
4	4	6	5	1	3	2
5	5	4	6	2	1	3
6	6	3	2	5	4	1

The first loop is a D-loop, the second and the third are parastrophes of the first. They are not D-loops and are not isotopic to the first. So this D-loop has three classes of isotopic parastrophes. In this case $Q = Q_5$, $Q_1 = Q_3$ and $Q_2 = Q_4$. □

4. Some consequences

Note first of all that the proofs of our results remain true also for the case when $\alpha = \beta = \gamma$. In this case an anti-isotopism is an anti-isomorphism and an isotopism is an isomorphism. So, the above results will be true if we replace an anti-isotopism by an anti-isomorphism, and an isotopism by an isomorphism. Moreover, an isotopism of parastrophes can be characterized by the identities:

$$\alpha_1(x) \cdot \beta_1(yx) = \gamma_1(y), \tag{1}$$

$$\beta_2(xy) \cdot \alpha_2(x) = \gamma_2(y), \tag{2}$$

$$\beta_3(yx) \cdot \alpha_3(x) = \gamma_3(y), \tag{3}$$

$$\alpha_4(x) \cdot \beta_4(xy) = \gamma_4(y), \tag{4}$$

$$\beta_5(xy) = \gamma_5(y) \cdot \alpha_5(x), \tag{5}$$

where $\alpha_i, \beta_i, \gamma_i$ are fixed permutations of the set Q.

Namely, from our results it follows that

$$\begin{array}{l} Q \ \text{ satisfies } (1) \longleftrightarrow Q_1 \sim Q \longleftrightarrow Q_3 \approx Q, \\ Q \ \text{ satisfies } (2) \longleftrightarrow Q_2 \sim Q \longleftrightarrow Q_4 \approx Q, \\ Q \ \text{ satisfies } (3) \longleftrightarrow Q_3 \sim Q \longleftrightarrow Q_2 \approx Q, \\ Q \ \text{ satisfies } (4) \longleftrightarrow Q_4 \sim Q \longleftrightarrow Q_1 \approx Q, \\ Q \ \text{ satisfies } (5) \longleftrightarrow Q \sim Q \longleftrightarrow Q_5 \approx Q. \end{array}$$

Lemma 2.3 shows that these identities are universal in some sense, i.e., if one of these identities is satisfied in a quasigroup Q, then in a quasigroup isotopic to Q is satisfied the identity of the same type, i.e., it is satisfied with other permutations.

Since $Q \sim Q_1 \longleftrightarrow Q \sim Q_2$ we have

Proposition 4.1. *A quasigroup Q satisfies for some $\alpha_1, \beta_1, \gamma_1 \in S_Q$ the identity* (1) *if and only if for some $\alpha_2, \beta_2, \gamma_2 \in Q_S$ it satisfies the identity* (2).

As a consequence we obtain the following classification of quasigroups>

Theorem 4.2. *Let Q be a quasigroup. Then*

- *Q is type A if and only if it satisfies all of the identities* $(1) - (5)$,
- *Q is type B if and only if it satisfies only* (1) *and* (2),
- *Q is type C if and only if it satisfies only* (3),
- *Q is type D if and only if it satisfies only* (4),
- *Q is type E if and only if it satisfies only* (5),
- *Q is type F if and only if it satisfies none of the identities* $(1) - (5)$.

If all permutations used in $(1) - (5)$ are the identity permutations, then these equations have of the form:

$$x \cdot yx = y, \tag{6}$$

$$xy \cdot x = y, \tag{7}$$

$$yx \cdot x = y, \tag{8}$$

$$x \cdot xy = y, \tag{9}$$

$$xy = yx. \tag{10}$$

Basing on our results we conclude that

$$Q \text{ satisfies } (6) \longleftrightarrow Q = Q_4,$$
$$Q \text{ satisfies } (7) \longleftrightarrow Q = Q_3,$$
$$Q \text{ satisfies } (8) \longleftrightarrow Q = Q_2,$$
$$Q \text{ satisfies } (9) \longleftrightarrow Q = Q_1,$$
$$Q \text{ satisfies } (10) \longleftrightarrow Q = Q_5.$$

Since Q satisfies (7) $\longleftrightarrow Q_5 = Q_2 \longleftrightarrow ((Q_1)_2)_1 = Q_2 \longleftrightarrow Q_1 = ((Q_2)_1)_2 \longleftrightarrow Q_1 = Q_5 \longleftrightarrow Q$ satisfies (6), we see that identities (7) and (6) are equivalent, i.e., Q satisfies (7) if and only if it satisfies (6).

As a consequence we obtain the stronger version of Theorem 4 in [7].

Theorem 4.3. *Parastrophes of a quasigroup Q can be characterized by the identities* $(6) - (10)$ *in the following way:*

- $Q = Q_i$ *for* $1 \leqslant i \leqslant 5$ *if and only if it satisfies all of the identities* $(6) - (10)$,
- $Q = Q_3 = Q_4,\ Q_1 = Q_2 = Q_5$ *if and only if Q satisfies only* (7) *and* (6),
- $Q = Q_2,\ Q_1 = Q_4,\ Q_3 = Q_5$ *if and only if Q satisfies only* (8),
- $Q = Q_1,\ Q_2 = Q_3,\ Q_4 = Q_5$ *if and only if Q satisfies only* (9),
- $Q = Q_5,\ Q_1 = Q_3,\ Q_2 = Q_4$ *if and only if Q satisfies only* (10),
- $Q \neq Q_i \neq Q_j$ *for all* $1 \leqslant i < j \leqslant 5$ *if and only if Q satisfies none of the identities* $(6) - (10)$.

Corollary 4.4. *Parastrophes of a commutative quasigroup Q coincide with Q or are divided into three classes: $\{Q = Q_5\}$, $\{Q_1 = Q_3\}$, $\{Q_2 = Q_4\}$.*

Corollary 4.5. *For a commutative quasigroup Q the following conditions are equivalent:*

(1) *all parastrophes of Q coincide with Q,*

(2) $Q = Q_1$,

(3) $Q = Q_2$,

(4) $Q_1 = Q_2$,

(5) *Q satisfies at least one of the identities* $(6) - (9)$.

Proof. We prove only the equivalence $(1) \longleftrightarrow (2)$. Other equivalences can be proved in a similar way.

For a commutative Q we have $Q = Q_5$, $Q_1 = Q_3$, $Q_2 = Q_4$. If $Q = Q_1$, then $Q = Q_1 = Q_3 = Q_5$. Hence $Q_1 = Q_5 = ((Q_2)_1)_2$ which gives $(Q_1)_2 = (Q_2)_1$. So, $Q_3 = Q_4$, i.e., (2) implies (1). The converse implication is obvious. □

Corollary 4.6. *Parastrophes of a boolean group coincide with this group.*

Note finally that identities $(6)-(10)$ can be used to determine some autotopisms of quasigroups [4].

References

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

[2] **G.B. Belyavskaya and T.V. Popovich**, *Conjugate sets of loops and quasigroups. DC-quasigroups*, Bul. Acad. Ştiinţe Repub. Mold. Mat. **1(68)** (2012), 21 – 31.

[3] **G.B. Belyavskaya and A.Kh. Tabarov**, *Characterization of linear and alinear quasigroups*, (Russian), Diskr. Mat. **4** (1992) 142 – 147.

[4] **A.I. Deriyenko**, *Autotopisms of some quasigroups*, Quasigroups and Related Systems **23** (2015), 217 – 220.

[5] **I.I. Deriyenko and W.A. Dudek**, *D-loops*, Quasigroups and Related Systems **20** (2012), 183 – 196.

[6] **A.D. Keedwell and J. Dénes**, *Latin squares and their applications*, Second edition, Elsevier, 2015.

[7] **C.C. Lindner and D. Steedly**, *On the number of conjugates of a quasigroups*, Algebra Universalis **5** (1975), 191 – 196.

[8] **T.V. Popovich**, *On conjugate sets of quasigroups*, Bul. Acad. Ştiinţe Repub. Mold. Mat. **3(67)** (2011), 69 – 76.

Received November 12, 2015

Faculty of Pure and Applied Mathematics
Wroclaw University of Technology
Wyb. Wyspiańskiego 27
50-370 Wroclaw, Poland
E-mail: wieslaw.dudek@pwr.edu.pl

Quasigroups and Related Systems **23** (2015), 231 − 236

Eventually regular perfect semigroups

Roman S. Gigoń

Abstract. A congruence ρ on a semigroup S is called *perfect* if $(a\rho)(b\rho) = (ab)\rho$ for all $a, b \in S$, as sets, and S is said to be *perfect* if each of its congruences is perfect. We show that all eventually regular perfect semigroups are necessarily regular. Finally, we apply our result to perfect group-bound semigroups.

1. Introduction and preliminaries

The concept of a perfect semigroup was introduced by Vagner [12]. Groups are very well-known examples of perfect semigroups. Another examples of such semigroups are congruence-free semigroups S with the property $S = S^2$ (i.e., S is *globally idempotent*; note that perfect semigroups have this property). Perfect semigroups were studied first by Fortunatov (see e.g. [4, 5]) and then by Hamilton and Tamura [8], Hamilton [7], and by Goberstein [6]. In [1] the authors gave an example of a cancellative simple perfect semigroup without idempotents.

It is known that *any commutative perfect semigroup is inverse*, and that *all finite perfect semigroups are regular*; recall that a semigroup S is *regular* if S coincides with the set $\mathrm{Reg}(S)$ of its *regular* elements, where

$$\mathrm{Reg}(S) = \{s \in S : s \in sSs\}.$$

We extend the last result for eventually regular semigroups (a semigroup S is *eventually regular* if every element of S has a regular power, that is, for all $a \in S$ there is a positive integer $n = n(a)$ such that $a^n \in \mathrm{Reg}(S)$ [3]). Moreover, we apply this result to perfect group-bound semigroups (Corollary 2.2, below). Before we start our study, we recall some definitions and facts. For undefined terms, we refer the reader to the books [2, 9, 10].

Denote the set of all *idempotents* of a semigroup S by E_S, that is,

$$E_S = \{e \in S : e^2 = e\}.$$

If A is an *ideal* of a semigroup S, i.e., $AS \cup SA \subseteq A$, then the relation

$$\rho_A = (A \times A) \cup 1_S,$$

2010 Mathematics Subject Classification: Primary 20M99, Secondary 06B10
Key words and phrases: perfect semigroup, eventually regular semigroup, group-bound semigroup, intra-regular semigroup, completely semisimple semigroup.

where 1_S is the identity relation on S, is a congruence on S (the so-called *Rees congruence* on S). It is obvious that A is an idempotent ρ_A-class of S. Finally, we shall write S/A instead of S/ρ_A.

A generalization of the concept of regularity will also prove convenient. Define a semigroup S to be *idempotent-surjective* if and only if whenever ρ is a congruence on S and $a\rho$ is an idempotent of S/ρ, then $a\rho$ contains some idempotent of S. Edwards showed that eventually regular semigroups are idempotent-surjective [3].

Let S be a semigroup and let $a \in S$. Denote by S^1 the semigroup obtained from S by adjoining an identity if necessary. Then $S^1 a S^1$ is the least ideal of S containing a. Denote it by $J(a)$. We shall say that the elements a, b of S are *$\mathcal{J}$-related* if $J(a) = J(b)$. Also, an equivalence $\mathcal{J}$-class containing a will be denoted by J_a. We can define a partial order on $S/\mathcal{J}$ by the rule:

$$J_a \leq J_b \iff J(a) \subseteq J(b)$$

for all $a, b \in S$ (a similar notation may be used for the Green's relations $\mathcal{L}$ and $\mathcal{R}$, cf. Section 2.1 of [10]).

We say that a semigroup S without zero is *simple* if and only if it has no proper ideals, that is, if and only if $SaS = S$ for every a of S. Further, a semigroup S with zero is called 0-*simple* if S is *not null* (i.e., $S^2 \neq \{0\}$) and S contains exactly two ideals (namely: $\{0\}$ and S). Clearly, S is 0-simple if and only if $S^2 \neq \{0\}$ and $S/\mathcal{J} = \{\{0\}, S \setminus \{0\}\}$.

By a 0-*minimal* ideal of a semigroup S we shall mean an ideal of S that is a minimal element in the set of all non-zero ideals of S.

The following result of Clifford is well-known.

Lemma 1.1. [2] *Any* 0*-minimal ideal of a semigroup is either null, or it is a* 0*-simple semigroup.* □

Let a be an element of a semigroup S. Suppose first that J_a is minimal among the $\mathcal{J}$-classes of S. Then $J(a) = J_a$ is the least ideal of S. On the other hand, if J_a is not minimal in $S/\mathcal{J}$, then the set

$$I(a) = \{b \in J(a) : J_b \leq J_a \ \& \ J_b \neq J_a\}$$

is an ideal of S such that $J(a) = I(a) \cup J_a$ (and this union is disjoint), and if B is a proper ideal of $J(a)$ and $I(a) \subseteq B$, then $I(a) = B$. This implies that $J(a)/I(a)$ is a 0-minimal ideal of $S/I(a)$, i.e., $J(a)/I(a)$ is either null, or it is a 0-simple semigroup (Lemma 1.1). For convenience, we shall write $J(a)/\emptyset = J(a)$. The semigroups $J(a)/I(a)$ ($a \in S$) are the so-called *principal factors* of S. Remark that we can think of the principal factor $J(a)/I(a)$ as consisting of the $\mathcal{J}$-class $J_a = J(a) \setminus I(a)$ with zero adjoined (if $I(a) \neq \emptyset$). Clearly, $J(a)/I(a)$ is null if and only if the product of any two elements of J_a always falls into a lower $\mathcal{J}$-class. In particular, if J_a is a subsemigroup of S, then the principal factor $J(a)/I(a)$ is not null. Finally, $J(a)/I(a)$ is simple if and only if $I(a)$ is empty.

Recall that among idempotents in an arbitrary semigroup there is a *natural partial order relation* defined by the rule that

$$e \leqslant f \Leftrightarrow e = ef = fe.$$

We say that an idempotent $e \neq 0$ of a semigroup S is *primitive* if it is minimal (with respect to the natural partial order) within the set of non-zero idempotents of S. Also, a (0)-simple semigroup is called *completely* (0)*-simple* if it is (0)-simple and contains a primitive idempotent. Notice that in the both cases each non-zero idempotent of S is primitive. For some equivalent definitions of these notions, we refer the reader to the book [10] (cf. Section 3.2). Munn showed that a (0)-simple semigroup S is completely (0)-simple if and only if it is *group-bound* (a semigroup S is called *group-bound* if every element of S has a power which belongs to some subgroup of S). Obviously, group-bound semigroups are eventually regular.

A semigroup is called (*completely*) *semisimple* if each of its principal factors is either (completely) 0-simple or (completely) simple. Recall that a semigroup is semisimple if and only if all its ideals are globally idempotent (see e.g. [2]).

Observe that every idempotent congruence class of a perfect semigroup S is globally idempotent. In particular, all ideals of S are globally idempotent, that is, S is semisimple.

Recall that an idempotent commutative semigroup is *semilattice*. Clearly, the least semilattice congruence η on an arbitrary semigroup S exists (note that $\mathcal{J} \subseteq \eta$). This relation induces the greatest semilattice decomposition of S, say $[Y; S_\alpha]$ $(\alpha \in Y)$, where $Y \cong S/\eta$, each S_α is an η-class and $S = \bigcup\{S_\alpha : \alpha \in Y\}$. To indicate this fact we shall always write $S = [Y; S_\alpha]$ $(\alpha \in Y)$ or briefly $S = [Y; S_\alpha]$. Notice that $S_\alpha S_\beta \subseteq S_{\alpha\beta}$ for all $\alpha, \beta \in Y$, where $\alpha\beta$ is the product of α and β in the semilattice Y.

We say that a semigroup S is *intra-regular* if for every $a \in S$, $a \, \mathcal{J} \, a^2$ [2]. It is easy to see that if S is intra-regular, then $\mathcal{J}$ is a semilattice congruence on S, so we have the following well-known result [2].

Lemma 1.2. *A semigroup S is intra-regular if and only if $\eta = \mathcal{J}$, where every $\mathcal{J}$-class is a simple semigroup.* □

We say that a $\mathcal{J}$-class J of a semigroup is *regular* if consists entirely of regular elements.

The following result, which is contained in the paper of Jones et al. [11], is due to Ciri̇č.

Lemma 1.3. *Let a $\mathcal{J}$-class J of an eventually regular semigroup contains an idempotent. Then J is regular. Equivalently,* 0*-simple eventually regular semigroups are regular.* □

We recall now some known results concerning perfect semigroups in general. For beginning, from the First and Second Isomorphism Theorems we obtain the following result [5].

Lemma 1.4. *Every homomorphic image of a perfect semigroup is a perfect semigroup.* □

An ideal A of a semigroup S is called *completely prime* if $ab \in A$ implies that $a \in A$ or $b \in A$.

The following fact [5] follows from the definition of a Rees congruence.

Lemma 1.5. *Every non-zero ideal of a perfect semigroup is completely prime.* □

It is not difficult to see that every chain is perfect. Also, if the elements a, b of a semilattice A are incomparable, then the congruence induced by the ideal aA is not perfect.

Lemma 1.6. [5] *A semilattice is perfect if and only if it is a chain.* □

Let $S = [Y; S_\alpha]$. Assume that S is perfect. In the light of Lemmas 1.4 and 1.6, Y is a chain. Moreover, from [5] we can extract the following result. We give a simple proof for the sake of completeness.

Corollary 1.7. *Let $S = [Y; S_\alpha]$ be a perfect semigroup. Then Y is a chain and the following statements hold*:

(a) *if S does not have a zero, then each S_α is simple and $Y \cong S/\mathcal{J}$*;

(b) *if S contains a zero 0, then Y has a least element 0_Y, S_α is a simple semigroup for $\alpha \neq 0_Y$, and either $S_{0_Y} = \{0\}$* (*then $Y \cong S/\mathcal{J}$*) *or S_{0_Y} is a 0-simple semigroup whose zero is not adjoined* (*and $J_a = a\eta \setminus \{0\}$ if $a \neq 0$*).

Proof. (a). Suppose first that S has no a zero element. As $a^2 \in S^1a^2S^1$, $a \in S^1a^2S^1$ (Lemma 1.5) and so S is intra-regular. Thus every S_α is a simple semigroup and $Y \cong S/\mathcal{J}$ (Lemma 1.2).

(b). Let now S contains a zero 0, say $0 \in S_{0_Y}$. Because $S_{0_Y}S_\alpha \subseteq S_{0_Y}$ for all $\alpha \in Y$, then $S_{0_Y}S_\alpha = S_{0_Y}$ for all $\alpha \in Y$ (since S is perfect). This implies that Y has a least element 0_Y.

Since Y is a chain and every S_α is a semigroup, then the condition $a^2 = 0$ implies that $a \in S_{0_Y}$. Thus S_α is a simple semigroup for all $\alpha \neq 0_Y$.

If $S_{0_Y} \neq \{0\}$, then $S_{0_Y}^2 = S_{0_Y} \neq \{0\}$, since it is clear that S_{0_Y} is an ideal of S, i.e., S_{0_Y} is *not null*. Suppose that $A \subseteq S_{0_Y}$ is a non-zero ideal of S. Then A is completely prime (by Lemma 1.5). It follows that A is a non-zero completely prime ideal of S_{0_Y}. Hence the partition $\{A, S_{0_Y} \setminus A\}$ of S_{0_Y} induces a semilattice congruence on S_{0_Y}. On the other hand, it is well-known that every η-class of S has no semilattice congruences except the universal relation. In particular, S_{0_Y} possesses this property. It follows that $A = S_{0_Y}$, i.e., S_{0_Y} is a 0-minimal ideal of S. Finally, observe that if 0 is adjoined to S_{0_Y}, then the partition

$$\{S_\alpha\,(\alpha \neq 0_Y), S_{0_Y} \setminus \{0\}, \{0\}\}$$

of S induces a semilattice congruence on S which is properly contained in the least semilattice congruence η, a contradiction, so S_{0_Y} is a 0-minimal ideal of S whose zero is not adjoined. Consequently, S_{0_Y} is a 0-simple semigroup whose zero is not adjoined (Lemma 1.1). Clearly, $J_a = a\eta \setminus \{0\}$ if $a \neq 0$. □

2. The main results

Remark that if ρ is a semilattice congruence on an eventually regular semigroup S, then every ρ-class of S is eventually regular.

Theorem 2.1. *Every eventually regular perfect semigroup S is regular.*

Proof. Suppose first that S has no a zero. Then S is a semilattice Y of simple semigroups S_α $(\alpha \in Y)$, where each S_α is a $\mathcal{J}$-class of S (cf. Corollary 1.7). Since each S_α is an idempotent $\mathcal{J}$-class, then it contains an idempotent element of S (because S is idempotent-surjective). In the light of Lemma 1.3, S is regular.

Let S has a zero. In view of Corollary 1.7, Y has a least element 0_Y. Put $A = S \backslash S_{0_Y}$. It is evident that the semigroup A is a semilattice of simple semigroups. Take any $a \in A$. Then the elements a and a^2 belong to the same *simple* subsemigroup B of A. Hence $a \in Ba^2B \subseteq Aa^2A$. Thus A is intra-regular. By the above A is regular. Finally, consider a 0-simple semigroup S_{0_Y} (see Corollary 1.7). This semigroup is also eventually regular, so S_{0_Y} is regular (by Lemma 1.3). Consequently, S is a regular semigroup. □

A semigroup is called *completely regular* if it is a union of groups. Recall from [9] that a semigroup is completely regular if and only if it is a semilattice of completely simple semigroups.

Corollary 2.2. *Let $S = [Y; S_\alpha]$ be a perfect group-bound semigroup. Then S is regular, Y is a chain and the following statements hold*:

(*a*) *if S does not have a zero, then every S_α is a completely simple semigroup* (*and $Y \cong S/\mathcal{J}$*), *that is, S is completely regular*;

(*b*) *if S contains a zero, say 0, then Y has a least element 0_Y, S_α is completely simple for $\alpha \neq 0_Y$, and either $S_{0_Y} = \{0\}$* (*then clearly $Y \cong S/\mathcal{J}$*) *or S_{0_Y} is a completely 0-simple semigroup whose zero 0 is not adjoined* (*and then $J_a = a\eta \setminus \{0\}$ if $a \neq 0$*).

In the former case, S is a completely regular semigroup with 0 adjoined.

Proof. (*a*). Indeed, every S_α is a simple (regular) group-bound semigroup, so each S_α is a completely simple semigroup.

(*b*). It is sufficient to show that if $S_{0_Y} \neq \{0\}$, then S_{0_Y} is a completely 0-simple semigroup. In that case, S_{0_Y} is a 0-simple (regular) group-bound semigroup. Thus S_{0_Y} is completely 0-simple semigroup. □

Corollary 2.3. *Every perfect group-bound semigroup is completely semisimple.* □

Finally, we shall show that an eventually regular perfect semigroup satisfying one of the following minimal conditions is group-bound (note that any group-bound semigroup meets both of these conditions). We shall say that a semigroup S *satisf ies the condition* $\min_L^*$ (resp. $\min_R^*$) if and only if for every $\mathcal{J}$-class J of S, the set of all $\mathcal{L}$-classes (resp. $\mathcal{R}$-classes) contained in J has a minimal element (for more details cf. Section 6.6 [2]). Recall only that a regular semigroup satisfies $\min_L^*$ if and only if it meets $\min_R^*$.

Proposition 2.4. *Let S be an eventually regular perfect semigroup satisfying* $\min_L^*$ *or* $\min_R^*$. *Then S is completely semisimple. In particular, S is group-bound.*

Proof. Indeed, in that case, S is regular (Theorem 2.1), so every η-class of S is a regular subsemigroup of S. In view of the above remark, S satisfies $\min_L^*$ and $\min_R^*$ (cf. also Corollary 1.7). As S is semisimple, S is completely semisimple (see Theorem 6.45 in [2]). In particular, S is group-bound. □

References

[1] **S. Bulman-Fleming and K. McDowell**, *A non-regular perfect semigroup*, Semigroup Forum **35** (1987), 119–121.

[2] **A.H. Clifford and G.B. Preston**, *The algebraic theory of semigroups*, Vol. I & II, Math. Surveys, no. 7, Amer. Math. Soc., Providence, R.I. (1961 & 1967).

[3] **P.M. Edwards**, *Eventually regular semigroups*, Bull. Austral. Math. Soc. **28** (1983), 23–38.

[4] **V.A. Fortunatov**, *Perfect semigroups that decompose into a commutative band of rectangular groups*, (Russian), Studies in algebra (Izdat. Saratov, Univ.) **2** (1970), 67–78.

[5] **V.A. Fortunatov**, *Perfect semigroups*, (Russian), Izv. Vysš. Učebn. Zaved. Matematika **3** (1972), 80–89.

[6] **F.S. Goberstein**, *Perfect Completely Semisimple Inverse Semigroups*, Semigroup Forum **45** (1992), 395–397.

[7] **H. Hamilton**, *Perfect completely regular semigroups*, Math. Nachr. **123** (1984), 169–176.

[8] **H. Hamilton and T. Tamura**, *Finite inverse perfect semigroups and their congruences*, J. Austral. Math. Soc. **32A** (1982), 114–128.

[9] **J.M. Howie**, *An introduction to semigroup theory*, Academic Press, London (1976).

[10] **J.M. Howie**, *Fundamentals of semigroup theory*, Oxford University Press, New York (1995).

[11] **P.R. Jones et al.**, *On the lattice of full eventually regular subsemigroups*, Comm. Algebra **33** (2005), 2587–2600.

[12] **V.V. Vagner**, *Algebraic topics of the general theory of partial connections in fiber bundles*, Izv. Vysš. Učebn. Zaved. Matematika **11** (1968), 26–32.

Received October 4, 2014

Department of Mathematics, University of Bielsko-Biała, Ul. Willowa 2, 43–309 Bielsko-Biała
Poland
E-mails: rgigon@ath.bielsko.pl, romekgigon@tlen.pl

Quasigroups and Related Systems **23** (2015), 237 − 242

Semidirect extensions of the Klein group leading to automorphic loops of exponent 2

Přemysl Jedlička

Abstract. In this paper we study automorphic loops of exponent 2 which are semidirect products of the Klein group with an elementary abelian group. It turns out that they fall into two classes: extensions of index 2 and extension using a symmetric bilinear form.

1. Introduction

A loop is called *automorphic* if all inner mappings are automorphisms. An automorphic loop of exponent 2 is always commutative due to the anti-automorphic inverse property [7]. There are several papers dealing with the structure of commutative automorphic loops, e.g. [1], [4] or [6]. It turns out that the structure of commutative automorhic 2-loops differs much from the theory of commutative automorphic p-loops, for odd primes p, and it is less understood.

The structure of commutative automorhic 2-loops is based on the structure of automorphic loops of exponent 2. It is already known that they are solvable [2] and that they need not be nilpotent [5]. Some constructions of automorphic loops of exponent 2 appeared in [5] and [8].

In this paper we construct automorphic loops of exponent 2 via the nuclear semidirect product defined in [3]. More precisely, we describe all the automorphic loops of exponent 2 that are nuclear semidirect extensions of the Klein group by an elementary abelian 2-group.

Theorem 1.1. *Let Q be an automorphic loop of exponent 2, let $K \lhd Q$ be a 4-element subgroup of $N_\mu(Q)$ and let H be a subgroup of Q such that $KH = Q$ and $|K \cap H| = 1$. Then one of the following situations occurs:*

(*a*) *Q is a group;*

(*b*) *$[Q : N_\mu(Q)] = 2$ and we can use Proposition 2.2;*

(*c*) *Q is a semidirect product based on a symmetric bilinear form described in Proposition 2.3.*

2010 Mathematics Subject Classification: 20N05
Keywords: automorphic loop, semidirect product, middle nucleus, exponent 2

The paper is organized as follows: in Section 2 we present the notion of the nuclear semidirect product of automorphic loops and also two situations when the semidirect product gives a loop of exponent 2. In Section 3 we analyze the semidirect product in the case when the image of the auxiliary mapping is a three-element group. Finally, in Section 4 we focus on the case when the image is a subgroup of order 2.

2. Preliminaries

We start our paper by recalling the notion of the nuclear semidirect product defined in [3] and by presenting two constructions that yield loops of exponent 2. Unlike in most loop theory papers, we shall use the additive notation here rather than the multiplicative one; the reason is that subgroups of our loops will appear as additive groups of vector spaces.

A semidirect product is a configuration of subloops in a loop $(Q,+)$: we have $H < Q$ and $K \triangleleft Q$ such that $K + H = Q$ and $K \cap H = 0$. In [3] an external point of view was given, assuming additionally that $K \leqslant N_\mu(Q)$ and K being an abelian group. Such loops can be constructed given a special mapping φ.

Proposition 2.1 ([3]). *Let H and K be abelian groups and let us have a mapping $\varphi : H^2 \to \mathrm{Aut}(K)$. We define an operation $*$ on $Q = K \times H$ as follows:*

$$(a,i) * (b,j) = (\varphi_{i,j}(a+b), i+j)\,.$$

This loop is denoted by $K \rtimes_\varphi H$. Let us denote $\varphi_{i,j,k} = \varphi_{i,j+k} \circ \varphi_{j,k}$. Then Q is a commutative A-loop if and only if the following properties hold:

$$\varphi_{i,j} = \varphi_{j,i} \tag{1}$$

$$\varphi_{0,i} = \mathrm{id}_K \tag{2}$$

$$\varphi_{i,j} \circ \varphi_{k,n} = \varphi_{k,n} \circ \varphi_{i,j} \tag{3}$$

$$\varphi_{i,j,k} = \varphi_{j,k,i} = \varphi_{k,i,j} \tag{4}$$

$$\varphi_{i,j+k} + \varphi_{j,i+k} + \varphi_{k,i+j} = \mathrm{id}_K + 2 \cdot \varphi_{i,j,k} \tag{5}$$

Moreover, $K \times 0$ is a normal subgroup of Q, $0 \times H$ is a subgroup of Q and $(K \times 0) \cap (0 \times H) = 0 \times 0$ and $(K \times 0) + (0 \times H) = Q$.

Q is associative if and only if $\varphi_{i,j} = \mathrm{id}_K$, for all $i, j \in H$. The nuclei are $N_\mu(Q) = K \times \{i \in H;\ \forall j \in H :\ \varphi_{i,j} = \mathrm{id}_K\}$ and
$N_\lambda = \{a \in K;\ \forall j,k \in H :\ \varphi_{j,k}(a) = a\} \times \{i \in H;\ \forall j \in H :\ \varphi_{i,j} = \mathrm{id}_K\}$.

On the other hand, if Q is a commutative automorphic loop, $K \triangleleft Q$ is a subgroup of $N_\mu(Q)$ and H is a subgroup of Q such that $K + H = Q$ and $K \cap H = \{0\}$ then there exists $\varphi : H^2 \to \mathrm{Aut}\, K$ such that $Q \cong K \rtimes_\varphi H$.

The conditions (1) – (5) are not too transparent and therefore it is worthwhile to present some special cases which are easier to describe. The simplest such a situation is probably the middle nucleus of index 2 which was described already in [5], not using the notion of a semidirect product.

Proposition 2.2 ([5], [3], exponent 2 version)**.** *Let K be an elementary abelian 2-group and let H be a two-element group. Then a mapping $\varphi : H^2 \to \operatorname{Aut} K$ satisfies the conditions $(1) - (5)$ if and only if φ satisfies (2).*

On the other hand, if an automorphic loop Q has exponent 2 and $[Q : N_\mu(Q)] = 2$ then there exists such a φ with $Q \cong K \rtimes_\varphi H$.

In this paper, we are interested in loops of exponent 2. Among several configurations described in [3], there is one more that yields loops of exponent two: when the mapping φ is a symmetric bilinear form.

Proposition 2.3 ([3], exponent p version)**.** *Let K and H be elementary abelian p groups and let $f \in \operatorname{Aut} K$ be an automorphism of order p. Let $\varphi : H^2 \to \langle f \rangle$ be a symmetric bilinear form. Then φ satisfies conditions $(1) - (5)$.*

In the rest of the paper we analyze the mapping φ when K is the Klein group. It will eventually turn out that all the possible solutions of φ are already described in Propositions 2.2 and 2.3.

3. Order 3 case

The automorphism group of the Klein group has only two non-trivial commutative subgroups, up to conjugacy. Each case will be analyzed separately. In this section we shall suppose that some of $\varphi_{i,j}$ is an automorphism of order 3. All the results can be proved under more general conditions.

Lemma 3.1. *Let K, H be elementary abelian 2-groups and let $\varphi : H^2 \to \operatorname{Aut} K$ satisfy $(1) - (5)$. Then, for all $i, j \in H$,*

$$\varphi_{i,i} + \varphi_{j,j} + \varphi_{i+j,i+j} = \mathrm{id}_K \tag{6}$$

$$\varphi_{i,i+j} = \varphi_{i,i} \circ \varphi_{i,j}^{-1} \tag{7}$$

$$\varphi_{i,j}^2 = \varphi_{i,i} \circ \varphi_{j,j} \circ \varphi_{i+j,i+j}^{-1} \tag{8}$$

Proof. (6) is obtained from (5) via $k = i + j$. Then (4) gives

$$\varphi_{i,i} \circ \mathrm{id}_K = \varphi_{i,i} \circ \varphi_{0,j} = \varphi_{i,i,j} = \varphi_{i,j} \circ \varphi_{i,i+j}$$

which is (7). Finally (4) again gives

$$\varphi_{i+j,i+j} \circ \varphi_{i,j} = \varphi_{i,j,i+j} = \varphi_{i,i+j} \circ \varphi_{j,j}$$

and substituting (7) yields (8). □

If an automorphism of order 3 is contained within $\operatorname{Im} \varphi$, it turns out that the whole mapping φ is determined by its behavior on the planes of H.

Lemma 3.2. *Let K, H be elementary abelian 2-groups and let $\varphi : H^2 \to \operatorname{Aut} K$ satisfy* (1) – (5). *Let* $\operatorname{Im}\varphi \subseteq \{\mathrm{id}_K, f, f^2\}$, *for some* $f \in \operatorname{Aut} K$ *with* $f^3 = \mathrm{id}_K$, $f \neq \mathrm{id}_K$. *Then, for all* $i, j \in H$,

(*i*) $|\{\alpha \in \{\varphi_{i,i}, \varphi_{j,j}, \varphi_{i+j,i+j}\};\ \alpha = f\}| \in \{0, 2\}$;

(*ii*) *there exists* $k \in \langle i, j\rangle$ *and* $g \in \{\mathrm{id}_K, f, f^2\}$ *such that, for all* $v, w \in \langle i, j\rangle$,

$$\varphi_{v,w} = \begin{cases} \mathrm{id}_K & \textit{if } v \in \langle k\rangle \textit{ or } w \in \langle k\rangle, \\ g & \textit{if } v \notin \langle k\rangle \textit{ and } w \notin \langle k\rangle. \end{cases}$$

Proof. (*i*) We find all the possible solutions of (6) within $\{\mathrm{id}_K, f, f^2\}$. They are, up to reordering, $(\mathrm{id}_K, \mathrm{id}_K, \mathrm{id}_K)$, (id_K, f, f) and $(\mathrm{id}_K, f^2, f^2)$.

(*ii*) We know from (*i*) all the possible choices of $\varphi_{i,i}$, $\varphi_{j,j}$ and $\varphi_{i+j,i+j}$. We put g to be that automorphism that appears at least twice within $\varphi_{i,i}$, $\varphi_{j,j}$ and $\varphi_{i+j,i+j}$ and we choose $k \in \{i, j, i+j\}$ such that $\varphi_{k,k} = \mathrm{id}_K$.

Then (8) gives

$$\varphi^2_{k,u} = \varphi_{k,k} \circ \varphi_{u,u} \circ \varphi^{-1}_{k+u,k+u} = \mathrm{id}_K,$$

for each $u \in \langle i, j\rangle$, since $\varphi_{u,u} = \varphi_{k+u,k+u} = g$ and hence $\varphi_{k,u} = \mathrm{id}_K$. On the other hand, if $u, v \notin \langle k\rangle$ then

$$\varphi^2_{u,v} = \varphi_{u,u} \circ \varphi_{v,v} \circ \varphi^{-1}_{u+v,u+v} = g^2,$$

for each $u \in \langle i, j\rangle$, since $u + v \in \langle k\rangle$ and therefore $\varphi_{u,v} = g$. □

Proposition 3.3. *Let K, H be elementary abelian 2-groups and let $\varphi : H^2 \to \operatorname{Aut} K$ satisfy* (1) – (5). *Let* $\operatorname{Im}\varphi \subseteq \{\mathrm{id}_K, f, f^2\}$, *for some* $f \in \operatorname{Aut} K$ *with* $f^3 = \mathrm{id}_K$. *Then*

(*i*) $\varphi_{i,j} \neq \mathrm{id}_K$ *if and only if* $\varphi_{i,i} = \varphi_{j,j} \neq \mathrm{id}_K$ *and then* $\varphi_{i,j} = \varphi_{i,i}$;

(*ii*) $|\operatorname{Im}\varphi| < 3$;

(*iii*) *the set* $M = \{k;\ \varphi_{k,k} = \mathrm{id}_K\}$ *is a subspace of H of Co-dimension at most* 1;

(*iv*) *the middle nucleus of* $K \rtimes_\varphi H$ *is a subloop of index at most* 2.

Proof. For (*i*) we can restrict our focus to the subspace of dimension 2 and this was solved in Lemma 3.2.

(*ii*) Suppose $\varphi_{i,j} = f$ and $\varphi_{k,m} = f^2$. Due to (*i*) we can suppose $j = i$ and $m = k$. But this situation contradicts Lemma 3.2 (*ii*).

(*iii*) The set M is closed on addition due to Lemma 3.2 (*ii*). Moreover, every 2-dimensional subspace of H intersects M non-trivially and hence M is a hyperplane or $M = H$.

(*iv*) According to to Proposition 2.1, we have $N_\mu(K \rtimes_\varphi H) = K \times M$. □

4. Involutory case

In this section we analyze the second case, namely some $\varphi_{i,j}$ being an involution. Most lemmas can be pronounced in a more general setting again.

Lemma 4.1. *Let K, H be elementary abelian 2-groups and let $\varphi : H^2 \to \operatorname{Aut} K$ satisfy $(1) - (5)$. Moreover, let $\varphi_{i,j}^2 = \mathrm{id}_K$, for each $i, j \in H$. Then*

$$\varphi_{i,j} + \varphi_{i,k} + \varphi_{j,k} = \varphi_{i,j,k} \tag{9}$$

$$\varphi_{i,j+k} = (\varphi_{i,j} + \varphi_{i,k} + \varphi_{j,k}) \circ \varphi_{j,k} \tag{10}$$

for all $i, j, k \in H$.

Proof. When we multiply (5) by $\varphi_{i,j,k}$, we obtain

$$\varphi_{i,j,k} \circ \varphi_{i,j+k} + \varphi_{i,j,k} \circ \varphi_{j,i+k} + \varphi_{i,j,k} \circ \varphi_{k,i+j} = \varphi_{i,j,k}$$

which is (9) since $\varphi_{i,j,k} \circ \varphi_{i,j+k} = \varphi_{j,k}$ due to (4). And plugging (9) into (4), namely $\varphi_{i,j+k} = \varphi_{i,j,k} \circ \varphi_{j,k}$, gives (10). □

Corollary 4.2. *Let K and H be elementary abelian 2-groups and let B be a basis of H. Suppose that we have a mapping $\varphi' : B^2 \to \operatorname{Aut} K$ such that $(\varphi'_{i,j})^2 = \mathrm{id}_K$, for each $i, j \in B$. Then there exists at most one mapping $\varphi : H^2 \to \operatorname{Aut} K$, satisfying $(1) - (5)$ such that $\varphi_{i,j}^2 = \mathrm{id}_K$, for each $i, j \in H$, and $\varphi|_{B^2} = \varphi'$.*

Proof. By an induction using (10). □

Corollary 4.2 claims that φ is uniquely determined whenever we know its values on a basis. It need not exist though, e.g. conditions (1) or (3) may be violated already by φ'. But it exists if φ' is a symmetric matrix with two different entries.

Proposition 4.3. *Let K and H be two elementary abelian 2-groups and let $\varphi : H^2 \to \operatorname{Aut} K$ satisfy $(1) - (5)$. Suppose that $\operatorname{Im} \varphi = \{\mathrm{id}_K, f\}$, for some involutory $f \in \operatorname{Aut} K$. Then φ is a bilinear mapping.*

Proof. Let us take a basis B of the space H. The restriction $\varphi|_{B^2}$ is symmetric and hence induces a symmetric bilinear form, let us say φ', from H^2 to $\{\mathrm{id}_K, f\} \cong \mathbb{Z}_2$. According to Proposition 2.3, the mapping φ' satisfies the conditions $(1) - (5)$. Since $\varphi'|_{B^2} = \varphi|_{B^2}$, Corollary 4.2 gives $\varphi = \varphi'$. □

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. Conditions of Proposition 2.1 are met and hence there exists a mapping $\varphi : H^2 \to \operatorname{Aut} K$ satisfying (1)–(5).

If $\varphi_{i,j}$ is an involution, for some $i, j \in H$, then $|\operatorname{Im} \varphi| = 2$, due to (1), since involutions in $\operatorname{Aut} \mathbb{Z}_2^2$ commute only with themselves and with the identity. Then Proposition 4.3 gives that φ is bilinear.

On the other hand, if no involution appears in $\operatorname{Im} \varphi$ then $\operatorname{Im} \varphi \subseteq \{\mathrm{id}_K, f, f^2\}$, where f and f^2 are the automorphisms of order 3. And Proposition 3.3 states that the middle nucleus is a subgroup of index at most 2. □

What if K is a larger elementary abelian group? There are three more types of subgroups even in $\operatorname{Aut}\mathbb{Z}_2^3$ and therefore it is likely that some new construction type will be needed.

References

[1] **R.H. Bruck, L.J. Paige**, *Loops whose inner mappings are automorphisms*, Ann. Math. **63** (1956), 308 – 323.

[2] **A. Grishkov, M.K. Kinyon, G.P. Nagy**, *Solvability of commutative automorphic loops*, Proceedings AMS **142** (2014), 3029 – 3037.

[3] **J. Hora, P. Jedlička**, *Nuclear semidirect product of commutative automorphic loops*, J. Algebra Appl. **13** (2014), no.1, paper 1350077.

[4] **P. Jedlička, M. Kinyon, P. Vojtěchovský**, *Structure of commutative automorphic loops*, Trans. AMS **363** (2011), 365384.

[5] **P. Jedlička, M. Kinyon, P. Vojtěchovský**, *Constructions of commutative automorphic loops*, Commun. Algebra **38** (2010), 3243 – 3267.

[6] **P. Jedlička, M. Kinyon, P. Vojtěchovský**, *Nilpotency in automorphic loops of prime power order*, J. Algebra **350** (2012), 64 – 76.

[7] **K.W. Johnson, M.K. Kinyon, G.P. Nagy, P. Vojtěchovský**, *Searching for small simple automorphic loops*, LMS J. Comput. Math. **14** (2011), 200 – 213.

[8] **G.P. Nagy**, *On centerless commutative automorphic loops*, Comment. Math. Univ. Carol. **55** (2014), 485 – 491.

Received October 14, 2014

Department of Mathematics
Faculty of Engineering
Czech University of Life Sciences in Prague
Kamýcká 129, 165 21, Prague 6 – Suchdol
Czech Republic
E-mail: jedlickap@tf.czu.cz

Quasigroups and Related Systems **23** (2015), 243 − 256

Subquasigroups in the framework of fuzzy points

Young Bae Jun, Seok Zun Song and Ghulam Muhiuddin

Abstract. A relation between $(\in, \in\vee q)$-fuzzy subquasigroups and $(q, \in\vee q)$-fuzzy subquasigroups is provided, and conditions for an $(\in,\in\vee q)$-fuzzy subquasigroup to be a $(q,\in\vee q)$-fuzzy subquasigroup are considered. Conditions for the t-q-set (resp., the t-$\in\vee q$-set) to be a subquasigroup are provided. The notion of (ε,δ)-characteristic fuzzy sets is introduced. Given a subquasigroup S of a quasigroup $\mathcal{Q}$, conditions for the (ε,δ)-characteristic fuzzy set in $\mathcal{Q}$ to be an $(\in,\in\vee q)$-fuzzy subquasigroup, an $(\in,q)$-fuzzy subquasigroup, an $(\in,\in\wedge q)$-fuzzy subquasigroup, a (q,q)-fuzzy subquasigroup, a $(q,\in)$-fuzzy subquasigroup, a $(q,\in\vee q)$-fuzzy subquasigroup and a $(q,\in\wedge q)$-fuzzy subquasigroup are provided. Using the notions of (α,β)-fuzzy subquasigroup $\mu_S^{(\varepsilon,\delta)}$, conditions for the S to be a subquasigroup of $\mathcal{Q}$ are investigated where (α,β) is one of $(\in,\in\vee q)$, $(\in,\in\wedge q)$, $(\in,q)$, $(q,\in\vee q)$, $(q,\in\wedge q)$, $(q,\in)$ and (q,q).

1. Introduction

Quasigroups has useful applications in cryptography, physics and geometry etc. In mathematics, especially in abstract algebra, a quasigroup is an algebraic structure resembling a group in the sense that "division" is always possible. Quasigroups differ from groups mainly in that they need not be associative. The fuzzy subquasigroup of a quasigroup is studied by W. A. Dudek in the paper [3]. M. Akram and W. A. Dudek [1] introduced the notion of (α,β)-fuzzy subquasigroups where α, $\beta\in\{\in,\ q\,,\ \in\vee q\,,\ \in\wedge q\,\}$ and $\alpha\neq\ \in\wedge q$, and investigated some related properties. They characterized $(\in,\in\vee q\,)$-fuzzy subquasigroups by their level subquasigroups, and studied fuzzy subquasigroups with thresholds.

In this paper, we discuss a relation between $(\in,\ \in\vee q\,)$-fuzzy subquasigroups and $(q,\ \in\vee q\,)$-fuzzy subquasigroups, and provide conditions for an $(\in,\in\vee q\,)$-fuzzy subquasigroup to be a $(q,\in\vee q\,)$-fuzzy subquasigroup. We consider conditions for the t-q-set (resp., the t-$\in\vee q$-set) to be a subquasigroup. We introduce the notion of (ε,δ)-characteristic fuzzy sets in quasigroups. Given a subquasigroup S of a quasigroup $\mathcal{Q}$, we provide conditions for the (ε,δ)-characteristic fuzzy set in $\mathcal{Q}$ to be an $(\in,\in\vee q)$-fuzzy subquasigroup, an $(\in,q)$-fuzzy subquasigroup, an $(\in,\in\wedge q)$-fuzzy subquasigroup, a (q,q)-fuzzy subquasigroup, a $(q,\in)$-fuzzy subquasigroup, a $(q,\in\vee q)$-fuzzy subquasigroup and a $(q,\in\wedge q)$-fuzzy subquasigroup. Using the notions of (α,β)-fuzzy subquasigroup $\mu_S^{(\varepsilon,\delta)}$, we investigate conditions for the S

2010 Mathematics Subject Classification: 20N15, 94D05
Keywords: (fuzzy) subquasigroup, (α,β)-fuzzy subquasigroup, t-q-set, t-$\in\vee q$-set.

to be a subquasigroup of $\mathcal{Q}$ where (α, β) is one of $(\in, \in \vee q)$, $(\in, \in \wedge q)$, $(\in, q)$, $(q, \in\vee q)$, $(q, \in\wedge q)$, $(q, \in)$ and (q, q).

2. Preliminaries

A *quasigroup* $(Q, \cdot)$ is a set Q with a binary operation "$\cdot$" such that for each a and b in Q there exist unique elements x and y in Q such that $a \cdot x = b$ and $y \cdot a = b$. The unique solutions to these equations are denoted by $x = a\backslash b$ and $y = b/a$. The operations "$\backslash$" and "/" denote the defined binary opersations of left and right division (sometimes called *parastrophe*), respectively. This axiomatization of quasigroups requires existential quantification and hence first order logic. The second definition of a quasigroup is grounded in universal algebra, which prefers that algebraic structures be varieties, i.e., that structures be axiomatized solely by identities. An identity is an equation in which all variables are tacitly universally quantified, and the only operations are the primitive operations proper to the structure. Quasigroups can be axiomatized in this manner if left and right division are taken as primitive.

A quasigroup $\mathcal{Q} = (Q, \cdot, \backslash, /)$ is a type $(2, 2, 2)$ algebra satisfying the identities:

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

(cf. [2] or [4]). Hence if $(Q, \cdot)$ is a quasigroup according to the first definition, then $\mathcal{Q} = (Q, \cdot, \backslash, /)$ is an equivalent quasigroup in the universal algebra sense. We say also that $(Q, \cdot, \backslash, /)$ is an *equasigroup* (i.e. equationally definable quasigroup) [4] or a *primitive quasigroup* [2]. The equasigroup $\mathcal{Q} = (Q, \cdot, \backslash, /)$ corresponds to quasigroup $(Q, \cdot)$ where

$$x\backslash\, y = z \iff x \cdot z = y, \quad x/y = z \iff z \cdot y = x.$$

A nonempty subset S of a quaisgroup $\mathcal{Q} = (Q, \cdot, \backslash, /)$ is called a *subquasigroup* of $\mathcal{Q}$ if it is closed with respect to these three operations, i.e., $x * y \in S$ for all $x, y \in S$ and $* \in \{\cdot, \backslash, /\}$.

A fuzzy set μ in a set X of the form

$$\mu(y) := \begin{cases} t \in (0, 1] & \text{if } y = x, \\ 0 & \text{if } y \neq x, \end{cases}$$

is said to be a *fuzzy point* with support x and value t and is denoted by x_t.

For a fuzzy point x_t and a fuzzy set μ in a set X, Pu and Liu [5] introduced the symbol $x_t \alpha \mu$, where $\alpha \in \{\in,\, q\,, \in\vee\, q\,, \in\wedge\, q\,\}$. To say that $x_t \in \mu$ (resp. $x_t\ q\ \mu$), we mean $\mu(x) \geqslant t$ (resp. $\mu(x) + t > 1$), and in this case, x_t is said to *belong to* (resp. *be quasi-coincident with*) a fuzzy set μ. To say that $x_t \in\vee\, q\ \mu$ (resp. $x_t \in\wedge\, q\ \mu$), we mean $x_t \in \mu$ or $x_t\, q\, \mu$ (resp. $x_t \in \mu$ and $x_t\, q\, \mu$). To say that $x_t\, \overline{\alpha}\, \mu$, we mean $x_t \alpha \mu$ does not hold, where $\alpha \in \{\in, q, \in\vee\, q\,, \in\wedge\, q\,\}$.

Definition 2.1. ([3, Definition 3.2]) A fuzzy set μ in a quasigroup $\mathcal{Q}$ is called a *fuzzy subquasigroup* of $\mathcal{Q}$ if it satisfies:

$$\mu(x * y) \geqslant \min\{\mu(x), \mu(y)\} \tag{1}$$

for all $x, y \in Q$ and $* \in \{\cdot, \backslash, /\}$.

We have the following characterization of a fuzzy subquasigroup.

Proposition 2.2. *Let $\mathcal{Q}$ be a quasigroup. A fuzzy set μ in $\mathcal{Q}$ is a fuzzy subquasigroup of $\mathcal{Q}$ if and only if the following assertion is valid.*

$$x_t \in \mu,\ y_s \in \mu \implies (x * y)_{\min\{t,s\}} \in \mu \tag{2}$$

for all $x, y \in Q$, $t, s \in (0, 1]$ and $* \in \{\cdot, \backslash, /\}$.

Proof. Straightforward. □

3. Subquasigroups in the framework of (α, β)-type fuzzy sets

In what follows, let $\mathcal{Q} = (Q, \cdot, \backslash, /)$ be a quasigroup unless otherwise specified.

Definition 3.1. ([1, Definition 3.1]) A fuzzy set μ in Q is said to be an (α, β)-*fuzzy subquasigroup* of $\mathcal{Q}$, where $\alpha, \beta \in \{\in, q, \in\vee q, \in\wedge q\}$ and $\alpha \neq \in\wedge q$, if it satisfies the following condition:

$$x_{t_1} \alpha\, \mu,\ y_{t_2} \alpha\, \mu \Rightarrow (x * y)_{\min\{t_1,t_2\}}\, \beta\, \mu. \tag{3}$$

for all $x, y \in Q$, $t_1, t_2 \in (0, 1]$ and $* \in \{\cdot, \backslash, /\}$.

Lemma 3.2. ([1, Theorem 3.13]) *A fuzzy set μ in $\mathcal{Q}$ is an $(\in, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$ if and only if it satisfies:*

$$(\forall x, y \in Q)\,(\mu(x * y) \geqslant \min\{\mu(x), \mu(y), 0.5\}) \tag{4}$$

where $* \in \{\cdot, \backslash, /\}$.

We know that there are twelve different types of (α, β)-fuzzy subquasigroups in Q, that is, (α, β) is any one of $(\in, \in)$, $(\in, q)$, $(\in, \in\wedge q)$, $(\in, \in\vee q)$, $(q, \in)$, (q, q), $(q, \in\wedge q)$, $(q, \in\vee q)$, $(\in\vee q, \in)$, $(\in\vee q, q)$, $(\in\vee q, \in\wedge q)$, and $(\in\vee q, \in\vee q)$. Clearly, we have relations among these types which are described in the following diagrams.

$$\begin{tikzcd}
(\in, \in) \arrow[dr, Rightarrow] & (\in, \in\wedge q) \arrow[l, Rightarrow] \arrow[r, Rightarrow] \arrow[d, Rightarrow] & (\in, q) \arrow[dl, Rightarrow] \\
 & (\in, \in\vee q) & \\
 & (\in\vee q, \in\vee q) \arrow[u, Rightarrow] & \\
(\in\vee q, \in) \arrow[ur, Rightarrow] & (\in\vee q, \in\wedge q) \arrow[l, Rightarrow] \arrow[r, Rightarrow] \arrow[u, Rightarrow] & (\in\vee q, q) \arrow[ul, Rightarrow]
\end{tikzcd} \tag{5}$$

and

$$\begin{tikzcd}
(q, \in) \arrow[dr, Rightarrow] & (q, \in\wedge q) \arrow[l, Rightarrow] \arrow[r, Rightarrow] \arrow[d, Rightarrow] & (q, q) \arrow[dl, Rightarrow] \\
 & (q, \in\vee q) &
\end{tikzcd} \tag{6}$$

If there exists $x \in Q$ such that $\mu(x) > 0.5$, then we have the following relation:

$$\begin{tikzcd}
(\in\wedge q, \in) \arrow[dr, Rightarrow] & (\in\wedge q, \in\wedge q) \arrow[l, Rightarrow] \arrow[r, Rightarrow] \arrow[d, Rightarrow] & (\in\wedge q, q) \arrow[dl, Rightarrow] \\
 & (\in\wedge q, \in\vee q) & \\
 & (\in, \in\vee q) \arrow[u, Rightarrow] &
\end{tikzcd} \tag{7}$$

We provide a relation between $(\in, \in\vee q)$-fuzzy subquasigroups and $(q, \in\vee q)$-fuzzy subquasigroups.

Theorem 3.3. *Every $(q, \in\vee q)$-fuzzy subquasigroup is an $(\in, \in\vee q)$-fuzzy subquasigroup.*

Proof. Let μ be a $(q, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$. Let $* \in \{\cdot, \backslash, /\}$ and let $x, y \in Q$ and $t_1, t_2 \in (0, 1]$ be such that $x_{t_1} \in \mu$ and $y_{t_2} \in \mu$. Then $\mu(x) \geqslant t_1$ and $\mu(y) \geqslant t_2$. Suppose $(x * y)_{\min\{t_1,t_2\}} \overline{\in\vee q}\, \mu$. Then

$$\mu(x * y) < \min\{t_1, t_2\}, \tag{8}$$

$$\mu(x * y) + \min\{t_1, t_2\} \leqslant 1. \tag{9}$$

It follows that

$$\mu(x * y) < 0.5. \tag{10}$$

and from (8) and (10) that

$$\mu(x * y) < \min\{t_1, t_2, 0.5\}.$$

Thus

$$1 - \mu(x * y) > 1 - \min\{t_1, t_2, 0.5\} \geqslant \max\{1 - \mu(x), 1 - \mu(y), 0.5\},$$

and so there exists $\delta \in (0, 1]$ such that

$$1 - \mu(x * y) \geqslant \delta > \max\{1 - \mu(x), 1 - \mu(y), 0.5\}. \tag{11}$$

The right inequality in (11) induces $\mu(x) + \delta > 1$ and $\mu(y) + \delta > 1$, that is, $x_\delta \, q \, \mu$ and $y_\delta \, q \, \mu$. Since μ is a $(q, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$, it follows that $(x * y)_\delta = (x * y)_{\min\{\delta,\delta\}} \in \vee \, q \, \mu$. But, from the left inequality in (11), we get $\mu(x * y) + \delta \leqslant 1$, that is, $(x * y)_\delta \, \overline{q} \, \mu$, and $\mu(x * y) \leqslant 1 - \delta < 1 - 0.5 = 0.5 < \delta$, i.e., $(x*y)_\delta \, \overline{\in} \, \mu$. Hence $(x*y)_\delta \, \overline{\in\vee q} \, \mu$, a contradiction. Therefore $(x*y)_{\min\{t_1,t_2\}} \in\vee \, q \, \mu$, and thus μ is an $(\in, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$. □

Regarding (α, β)-fuzzy subquasigroups, Theorem 3.3 and figure (6) induces the the following relations.

$$\begin{tikzcd}
(q, \in) \arrow[dr, Rightarrow] & (q, \in\wedge q) \arrow[l, Rightarrow] \arrow[r, Rightarrow] \arrow[d, Rightarrow] & (q, q) \arrow[dl, Rightarrow] \\
 & (q, \in\vee q) \arrow[d, Rightarrow] & \\
 & (\in, \in\vee q) &
\end{tikzcd} \tag{12}$$

The converse of Theorem 3.3 is not true in general (see [1, Example 3.6]).

We provide conditions for an $(\in, \in\vee q)$-fuzzy subquasigroup to be a $(q, \in\vee q)$-fuzzy subquasigroup.

Theorem 3.4. *If μ is an $(\in, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$ in which $\mu(x) \leqslant 0.5$ for all $x \in Q$, then μ is a $(q, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$.*

Proof. Let μ be an $(\in, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$ such that $\mu(x) \leqslant 0.5$ for all $x \in Q$. Let $* \in \{\cdot, \backslash, /\}$, $x, y \in Q$ and $t_1, t_2 \in (0, 0.5]$ be such that $x_{t_1} \, q \, \mu$ and $y_{t_2} \, q \, \mu$. Then $\mu(x) > 1 - t_1 \geqslant t_1$ and $\mu(y) > 1 - t_2 \geqslant t_2$, that is, $x_{t_1} \in \mu$ and $y_{t_2} \in \mu$. Since μ is an $(\in, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$, it follows that $(x * y)_{\min\{t_1,t_2\}} \in\vee \, q \, \mu$. Consequently, μ is a $(q, \in\vee q)$-fuzzy subquasigroup. □

The figure (5) and Theorem 3.4 induces the following corollary.

Corollary 3.5. *Let μ be an (α, β)-fuzzy subquasigroup of $\mathcal{Q}$ where (α, β) is any one of* $(\in, \in)$, $(\in, q)$, $(\in, \in\wedge q)$, $(\in\vee q, \in)$, $(\in\vee q, q)$, $(\in\vee q, \in\wedge q)$, *and* $(\in\vee q, \in\vee q)$. *If every fuzzy point has the value t in* $(0, 0.5]$, *then μ is a $(q, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$.* □

For a fuzzy set μ in $\mathcal{Q}$ and $t \in (0,1]$, consider the q-set and $\in\vee q$-set with respect to t (briefly, t-q-set and t-$\in\vee q$-set, respectively) as follows:

$$\mathcal{Q}_q^t := \{x \in Q \mid x_t \, q \, \mu\} \text{ and } \mathcal{Q}_{\in\vee q}^t := \{x \in Q \mid x_t \in\vee q \, \mu\}.$$

Note that, $\mathcal{Q}_q^r \subseteq \mathcal{Q}_q^t$ and $\mathcal{Q}_{\in\vee q}^r \subseteq \mathcal{Q}_{\in\vee q}^t$ for all $t, r \in (0,1]$ with $t \geqslant r$. Obviously, $\mathcal{Q}_{\in\vee q}^t = U(\mu; t) \cup \mathcal{Q}_q^t$, where

$$U(\mu; t) := \{x \in Q \mid \mu(x) \geqslant t\}.$$

Theorem 3.6. *If μ is an $(\in, \in)$-fuzzy subquasigroup of $\mathcal{Q}$, then the t-q-set $\mathcal{Q}_q^t$ is a subquasigroup of $\mathcal{Q}$ for all $t \in (0,1]$ whenever it is nonempty.*

Proof. Let $* \in \{\cdot, \backslash, /\}$ and $x, y \in \mathcal{Q}_q^t$. Then $x_t \, q \, \mu$ and $y_t \, q \, \mu$, that is, $\mu(x) + t > 1$ and $\mu(y) + t > 1$. It follows that

$$\mu(x * y) + t \geqslant \min\{\mu(x), \mu(y)\} + t = \min\{\mu(x) + t, \mu(y) + t\} > 1$$

and so that $(x*y)_t \, q \, \mu$. Hence $x*y \in \mathcal{Q}_q^t$, and therefore $\mathcal{Q}_q^t$ is a subquasigroup. □

Corollary 3.7. *If μ is an $(\in, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$, then the t-q-set $\mathcal{Q}_q^t$ is a subquasigroup of $\mathcal{Q}$ for all $t \in (0,1]$ whenever it is nonempty.* □

Theorem 3.8. *If μ is a $(q, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$, then the t-q-set $\mathcal{Q}_q^t$ and the t-$\in\vee q$-set $\mathcal{Q}_{\in\vee q}^t$ are subquasigroups of $\mathcal{Q}$ for all $t \in (0.5, 1]$ whenever it is nonempty.*

Proof. Let $* \in \{\cdot, \backslash, /\}$ and μ a $(q, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$. Let $x, y \in Q$ be such that $x \in \mathcal{Q}_q^t$ and $y \in \mathcal{Q}_q^t$ for all $t \in (0.5, 1]$. Then $x_t \, q \, \mu$ and $y_t \, q \, \mu$, which imply that $(x*y)_t \in\vee q \, \mu$, i.e., $(x*y)_t \in \mu$ or $(x*y)_t \, q \, \mu$. If $(x*y)_t \, q \, \mu$, then $x*y \in \mathcal{Q}_q^t$. If $(x*y)_t \in \mu$, then $\mu(x*y) \geqslant t > 1-t$ since $t > 0.5$. Hence $(x*y)_t \, q \, \mu$, that is, $x*y \in \mathcal{Q}_q^t$. Therefore $\mathcal{Q}_q^t$ is a subquasigroup of $\mathcal{Q}$. Now, let $x, y \in \mathcal{Q}_{\in\vee q}^t$. Then $x_t \in\vee q \, \mu$ and $y_t \in\vee q \, \mu$. Hence we have the following four cases:

(i) $x_t \in \mu$ and $y_t \in \mu$,

(ii) $x_t \in \mu$ and $y_t \, q \, \mu$,

(iii) $x_t \, q \, \mu$ and $y_t \in \mu$,

(iv) $x_t \, q \, \mu$ and $y_t \, q \, \mu$.

For the first case, we have $\mu(x)+t \geqslant 2t > 1$ and $\mu(y)+t \geqslant 2t > 1$, that is, $x_t\, q\, \mu$ and $y_t\, q\, \mu$. It follows that $(x*y)_t \in\vee\, q\, \mu$ and so that $x*y \in \mathcal{Q}^t_{\in\vee\, q}$. In the case (ii), $x_t \in \mu$ implies $\mu(x)+t \geqslant 2t > 1$, that is, $x_t\, q\, \mu$. Hence $(x*y)_t \in\vee\, q\, \mu$ and so $x*y \in \mathcal{Q}^t_{\in\vee\, q}$. Similarly, the third case implies $x*y \in \mathcal{Q}^t_{\in\vee\, q}$. The last case implies $(x*y)_t \in\vee\, q\, \mu$ and so $x*y \in \mathcal{Q}^t_{\in\vee\, q}$. Consequently, t-$\in\vee\, q$-set $\mathcal{Q}^t_{\in\vee\, q}$ is a subquasigroup of $\mathcal{Q}$ for all $t \in (0.5, 1]$. □

Corollary 3.9. *If μ is any one of a $(q,\in)$-fuzzy subquasigroup, a $(q,\in\wedge\, q)$-fuzzy subquasigroup and a (q,q)-fuzzy subquasigroup of $\mathcal{Q}$, then the t-q-set $\mathcal{Q}^t_q$ and the t-$\in\vee\, q$-set $\mathcal{Q}^t_{\in\vee\, q}$ are subquasigroups of $\mathcal{Q}$ for all $t \in (0.5, 1]$ whenever it is nonempty.*

Proof. It follows from the figure (6) and Theorem 3.8. □

Lemma 3.10. ([1, Theorem 3.12]) *For a subquasigroup S of $\mathcal{Q}$, let μ be a fuzzy set in $\mathcal{Q}$ such that*

(1) $\mu(x) \geqslant 0.5$ *for all* $x \in S$,

(2) $\mu(x) = 0$ *for all* $x \in Q \setminus S$.

Then μ is a $(q,\in\vee\, q)$-fuzzy subquasigroup of $\mathcal{Q}$.

Using Theorem 3.8 and Lemma 3.10, we have the following result.

Theorem 3.11. *For a subquasigroup S of $\mathcal{Q}$, if μ is a fuzzy set in $\mathcal{Q}$ such that*

(1) $\mu(x) \geqslant 0.5$ *for all* $x \in S$,

(2) $\mu(x) = 0$ *for all* $x \in Q \setminus S$,

then the nonempty t-q-set $\mathcal{Q}^t_q$ and the t-$\in\vee\, q$-set $\mathcal{Q}^t_{\in\vee\, q}$ are subquasigroups of $\mathcal{Q}$ for all $t \in (0.5, 1]$. □

Theorem 3.12. *If μ is an $(\in,\in\vee\, q)$-fuzzy subquasigroup of $\mathcal{Q}$, then the nonempty t-q-set Q^t_q is a subquasigroup of $\mathcal{Q}$ for all $t \in (0.5, 1]$.*

Proof. Let $* \in \{\cdot, \backslash, /\}$. Assume that $Q^t_q \neq \emptyset$ for all $t \in (0.5, 1]$. Let $x, y \in Q^t_q$. Then $x_t\, q\, \mu$ and $y_t\, q\, \mu$, that is, $\mu(x)+t > 1$ and $\mu(y)+t > 1$. It follows from Lemma 3.2 that

$$\begin{aligned}\mu(x*y)+t &\geqslant \min\{\mu(x), \mu(y), 0.5\}+t\\ &= \min\{\mu(x)+t, \mu(y)+t, 0.5+t\}\\ &> 1.\end{aligned}$$

So $(x*y)_t\, q\, \mu$. Hence $x*y \in Q^t_q$, and therefore Q^t_q is a subquasigroup. □

In what follows, let $\varepsilon, \delta \in [0,1]$ be such that $\varepsilon > \delta$ unless otherwise specified. For a nonempty subset S of $\mathcal{Q}$, define a fuzzy set $\mu_S^{(\varepsilon,\delta)}$ in $\mathcal{Q}$ as follows:

$$\mu_S^{(\varepsilon,\delta)}(x) := \begin{cases} \varepsilon & \text{if } x \in S, \\ \delta & \text{otherwise.} \end{cases}$$

We say that $\mu_S^{(\varepsilon,\delta)}$ is an (ε,δ)-*characteristic fuzzy set* in $\mathcal{Q}$ over S. In particular, the $(1,0)$-characteristic fuzzy set $\mu_S^{(1,0)}$ in $\mathcal{Q}$ over S is the characteristic function χ_S of S.

Theorem 3.13. *For any nonempty subset S of $\mathcal{Q}$, the following are equivalent:*

(1) *S is a subquasigroup of $\mathcal{Q}$.*

(2) *The (ε,δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a fuzzy subquasigroup of $\mathcal{Q}$.*

Proof. Assume that S is a subquasigroup of $\mathcal{Q}$ and let $x, y \in Q$. If $x, y \in S$, then $x * y \in S$ and so

$$\mu_S^{(\varepsilon,\delta)}(x * y) = \varepsilon = \min\left\{\mu_S^{(\varepsilon,\delta)}(x), \mu_S^{(\varepsilon,\delta)}(y)\right\}.$$

If $x \notin S$ or $y \notin S$, then $\mu_S^{(\varepsilon,\delta)}(x) = \delta$ or $\mu_S^{(\varepsilon,\delta)}(y) = \delta$. Hence

$$\mu_S^{(\varepsilon,\delta)}(x * y) \geqslant \delta = \min\left\{\mu_S^{(\varepsilon,\delta)}(x), \mu_S^{(\varepsilon,\delta)}(y)\right\}.$$

Therefore $\mu_S^{(\varepsilon,\delta)}$ is a fuzzy subquasigroup of $\mathcal{Q}$.

Conversely, suppose that $\mu_S^{(\varepsilon,\delta)}$ is a fuzzy subquasigroup of $\mathcal{Q}$. Let $x, y \in S$. Then $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon$ and $\mu_S^{(\varepsilon,\delta)}(y) = \varepsilon$. It follows that

$$\mu_S^{(\varepsilon,\delta)}(x * y) \geq \min\left\{\mu_S^{(\varepsilon,\delta)}(x), \mu_S^{(\varepsilon,\delta)}(y)\right\} = \varepsilon.$$

Thus $x * y \in S$, and therefore S is a subquasigroup of $\mathcal{Q}$. □

Theorem 3.14. *If S is a subquasigroup of $\mathcal{Q}$, then the (ε,δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$.*

Proof. Assume that S is a subquasigroup of $\mathcal{Q}$ and let $x, y \in Q$. If $x, y \in S$, then $x * y \in S$ and so

$$\mu_S^{(\varepsilon,\delta)}(x * y) = \varepsilon \geqslant \min\left\{\mu_S^{(\varepsilon,\delta)}(x), \mu_S^{(\varepsilon,\delta)}(y), 0.5\right\}.$$

If $x \notin S$ or $y \notin S$, then $\mu_S^{(\varepsilon,\delta)}(x) = \delta$ or $\mu_S^{(\varepsilon,\delta)}(y) = \delta$. Hence

$$\mu_S^{(\varepsilon,\delta)}(x * y) \geqslant \delta \geqslant \min\left\{\mu_S^{(\varepsilon,\delta)}(x), \mu_S^{(\varepsilon,\delta)}(y), 0.5\right\}.$$

It follows from Lemma 3.2 that $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, \in\vee q)$-fuzzy subquasigroup. □

In order to consider the converse of Theorem 3.14, we need additional conditions.

Theorem 3.15. *For any nonempty subset S of $\mathcal{Q}$, if $\delta < 0.5$ and the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$, then S is a subquasigroup of $\mathcal{Q}$.*

Proof. Assume that $\delta < 0.5$ and the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$. Let $x, y \in S$. Then $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon = \mu_S^{(\varepsilon,\delta)}(y)$. Using Lemma 3.2, we have

$$\begin{aligned}\mu_S^{(\varepsilon,\delta)}(x * y) &\geqslant \min\left\{\mu_S^{(\varepsilon,\delta)}(x), \mu_S^{(\varepsilon,\delta)}(y), 0.5\right\}\\ &= \min\{\varepsilon, 0.5\}\\ &= \begin{cases} 0.5 & \text{if } \varepsilon \geqslant 0.5,\\ \varepsilon & \text{otherwise,}\end{cases}\end{aligned}$$

and so that $\mu_S^{(\varepsilon,\delta)}(x * y) = \varepsilon$. Thus $x * y \in S$, and S is a subquasigroup of $\mathcal{Q}$. □

Corollary 3.16. *A nonempty subset S of $\mathcal{Q}$ is a subquasigroup of $\mathcal{Q}$ if and only if the characteristic function χ_S of S is an $(\in, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$.* □

Theorem 3.17. *If S is a subquasigroup of $\mathcal{Q}$, then the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, q)$-fuzzy subquasigroup of $\mathcal{Q}$ whenever if any element t in $(0, 1]$ satisfies $x_t \in \mu_S^{(\varepsilon,\delta)}$ for $x \in Q$ then $\delta < t$ and $1 - t < \varepsilon$.*

Proof. Let $* \in \{\cdot, \backslash, /\}$ and let $x, y \in Q$ and $t_1, t_2 \in (0, 1]$ be such that $x_{t_1} \in \mu_S^{(\varepsilon,\delta)}$ and $y_{t_2} \in \mu_S^{(\varepsilon,\delta)}$. Then $\mu_S^{(\varepsilon,\delta)}(x) \geqslant t_1 > \delta$ and $\mu_S^{(\varepsilon,\delta)}(y) \geqslant t_2 > \delta$. It follows that $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon = \mu_S^{(\varepsilon,\delta)}(y)$, and so $x, y \in S$. Since S is a subquasigroup of $\mathcal{Q}$, we have $x * y \in S$. Hence $\mu_S^{(\varepsilon,\delta)}(x * y) = \varepsilon$, and thus $\mu_S^{(\varepsilon,\delta)}(x * y) + \min\{t_1, t_2\} = \varepsilon + \min\{t_1, t_2\} > 1$ which shows that $(x * y)_{\min\{t_1,t_2\}}\, q\, \mu_S^{(\varepsilon,\delta)}$. Therefore $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, q)$-fuzzy subquasigroup of $\mathcal{Q}$. □

Corollary 3.18. *If S is a subquasigroup of $\mathcal{Q}$, then the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$ whenever if any element t in $(0, 1]$ satisfies $x_t \in \mu_S^{(\varepsilon,\delta)}$ for $x \in Q$ then $\delta < t$ and $1 - t < \varepsilon$.* □

Theorem 3.19. *Let S be a nonempty subset of $\mathcal{Q}$. If $\varepsilon + \delta \leqslant 1$ and the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, q)$-fuzzy subquasigroup of $\mathcal{Q}$, then S is a subquasigroup of $\mathcal{Q}$.*

Proof. Let $* \in \{\cdot, \backslash, /\}$. Assume that $\varepsilon + \delta \leqslant 1$ and the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, q)$-fuzzy subquasigroup of $\mathcal{Q}$. Let $x, y \in S$. Then $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon = \mu_S^{(\varepsilon,\delta)}(y)$, and so $x_\varepsilon \in \mu_S^{(\varepsilon,\delta)}$ and $y_\varepsilon \in \mu_S^{(\varepsilon,\delta)}$. Hence $(x * y)_\varepsilon = (x * y)_{\min\{\varepsilon,\varepsilon\}}\, q\, \mu_S^{(\varepsilon,\delta)}$, which implies that $\mu_S^{(\varepsilon,\delta)}(x*y)+\varepsilon>1$. Therefore $\mu_S^{(\varepsilon,\delta)}(x*y)>1-\varepsilon\geqslant\delta$, and thus $\mu_S^{(\varepsilon,\delta)}(x*y)=\varepsilon$, that is, $x*y\in S$. Consequently, S is a subquasigroup. □

Corollary 3.20. *Let S be a nonempty subset of Q. If $\varepsilon+\delta\leqslant 1$ and the (ε,δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in,\in\wedge\, q)$-fuzzy subquasigroup of Q, then S is a subquasigroup of Q.* □

If we take $\varepsilon=1$ and $\delta=0$ in Theorems 3.17 and 3.19, then we have the following corollary.

Corollary 3.21. *A nonempty subset S of Q is a subquasigroup of Q if and only if the characteristic function χ_S of S is an $(\in,q)$-fuzzy subquasigroup of Q.* □

Theorem 3.22. *If S is a subquasigroup of Q, then the (ε,δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a (q,q)-fuzzy subquasigroup of Q whenever if any element t in $(0,1]$ satisfies $x_t\in\mu_S^{(\varepsilon,\delta)}$ for $x\in Q$ then $\delta\leqslant 1-t<\varepsilon$.*

Proof. Let $*\in\{\cdot,\backslash,/\}$. Let $x,y\in Q$ and $t_1,t_2\in(0,1]$ be such that $x_{t_1}\,q\,\mu_S^{(\varepsilon,\delta)}$ and $y_{t_2}\,q\,\mu_S^{(\varepsilon,\delta)}$. Then $\mu_S^{(\varepsilon,\delta)}(x)+t_1>1$ and $\mu_S^{(\varepsilon,\delta)}(y)+t_2>1$, which imply that $\mu_S^{(\varepsilon,\delta)}(x)>1-t_1\geqslant\delta$ and $\mu_S^{(\varepsilon,\delta)}(y)>1-t_2\geqslant\delta$. It follows that $\mu_S^{(\varepsilon,\delta)}(x)=\varepsilon=\mu_S^{(\varepsilon,\delta)}(y)$ and so that $x,y\in S$. Since S is a subquasigroup of Q, we have $x*y\in S$ and so $\mu_S^{(\varepsilon,\delta)}(x*y)=\varepsilon$. Thus

$$\mu_S^{(\varepsilon,\delta)}(x*y)+\min\{t_1,t_2\}=\varepsilon+\min\{t_1,t_2\}>1,$$

that is, $(x*y)_{\min\{t_1,t_2\}}\,q\,\mu_S^{(\varepsilon,\delta)}$. This shows that $\mu_S^{(\varepsilon,\delta)}$ is a (q,q)-fuzzy subquasigroup. □

Corollary 3.23. *If S is a subquasigroup of Q, then the (ε,δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a $(q,\in\vee\, q)$-fuzzy subquasigroup of Q whenever if any element t in $(0,1]$ satisfies $x_t\in\mu_S^{(\varepsilon,\delta)}$ for $x\in Q$ then $\delta\leqslant 1-t<\varepsilon$.* □

Theorem 3.24. *Let S be a nonempty subset of Q. Assume that $\varepsilon>\max\{\delta,0.5\}$ and $\varepsilon+\delta\leqslant 1$. If the (ε,δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a (q,q)-fuzzy subquasigroup of Q, then S is a subquasigroup of Q.*

Proof. Let $*\in\{\cdot,\backslash,/\}$ and let $x,y\in S$. Then $\mu_S^{(\varepsilon,\delta)}(x)=\varepsilon=\mu_S^{(\varepsilon,\delta)}(y)$, which implies that

$$\mu_S^{(\varepsilon,\delta)}(x)+\varepsilon=\varepsilon+\varepsilon>1 \text{ and } \mu_S^{(\varepsilon,\delta)}(y)+\varepsilon=\varepsilon+\varepsilon>1,$$

that is, $x_\varepsilon\,q\,\mu_S^{(\varepsilon,\delta)}$ and $y_\varepsilon\,q\,\mu_S^{(\varepsilon,\delta)}$. Since $\mu_S^{(\varepsilon,\delta)}$ is a (q,q)-fuzzy subquasigroup of Q, it follows that $(x*y)_\varepsilon=(x*y)_{\min\{\varepsilon,\varepsilon\}}\,q\,\mu_S^{(\varepsilon,\delta)}$. Hence $\mu_S^{(\varepsilon,\delta)}(x*y)>1-\varepsilon\geqslant\delta$, and therefore $\mu_S^{(\varepsilon,\delta)}(x*y)=\varepsilon$. This proves that $x*y\in S$, and S is a subquasigroup. □

Corollary 3.25. *Let S be a nonempty subset of $\mathcal{Q}$. Assume that $\varepsilon > \max\{\delta, 0.5\}$ and $\varepsilon + \delta \leqslant 1$. If the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in \wedge\, q\,)$-fuzzy subquasigroup of $\mathcal{Q}$, then S is a subquasigroup.* □

If we take $\varepsilon = 1$ and $\delta = 0$ in Theorems 3.22 and 3.24, then we have the following corollary.

Corollary 3.26. *A nonempty subset S of $\mathcal{Q}$ is a subquasigroup of $\mathcal{Q}$ if and only if the characteristic function χ_S of S is a (q, q)-fuzzy subquasigroup of $\mathcal{Q}$.* □

Theorem 3.27. *For any nonempty subset S of $\mathcal{Q}$ and the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$, assume that if any element t in $(0, 1]$ satisfies $x_t \in \mu_S^{(\varepsilon,\delta)}$ for $x \in Q$ then $\delta \leqslant 1 - t$ and $t < \varepsilon$. If S is a subquasigroup of $\mathcal{Q}$, then $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in)$-fuzzy subquasigroup of $\mathcal{Q}$.*

Proof. Let $* \in \{\cdot, \backslash, /\}$. Let $x, y \in Q$ and $t_1, t_2 \in (0, 1]$ be such that $x_{t_1}\, q\, \mu_S^{(\varepsilon,\delta)}$ and $y_{t_2}\, q\, \mu_S^{(\varepsilon,\delta)}$. Then $\mu_S^{(\varepsilon,\delta)}(x) + t_1 > 1$ and $\mu_S^{(\varepsilon,\delta)}(y) + t_2 > 1$, which imply that $\mu_S^{(\varepsilon,\delta)}(x) > 1 - t_1 \geqslant \delta$ and $\mu_S^{(\varepsilon,\delta)}(y) > 1 - t_2 \geqslant \delta$. Hence $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon = \mu_S^{(\varepsilon,\delta)}(y)$, and so $x, y \in S$. Since S is a subquasigroup of $\mathcal{Q}$, we have $x * y \in S$ and thus

$$\mu_S^{(\varepsilon,\delta)}(x * y) = \varepsilon \geqslant \min\{t_1, t_2\},$$

that is, $(x * y)_{\min\{t_1,t_2\}} \in \mu_S^{(\varepsilon,\delta)}$. This shows that $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in)$-fuzzy subquasigroup of $\mathcal{Q}$. □

Corollary 3.28. *For any nonempty subset S of $\mathcal{Q}$ and the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$, assume that if any element t in $(0, 1]$ satisfies $x_t \in \mu_S^{(\varepsilon,\delta)}$ for $x \in Q$ then $\delta \leqslant 1 - t$ and $t < \varepsilon$. If S is a subquasigroup of $\mathcal{Q}$, then $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\vee\, q\,)$-fuzzy subquasigroup of $\mathcal{Q}$.* □

Theorem 3.29. *Let S be a nonempty subset of $\mathcal{Q}$. Assume that $\varepsilon > \max\{\delta, 0.5\}$. If the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in)$-fuzzy subquasigroup of $\mathcal{Q}$, then S is a subquasigroup of $\mathcal{Q}$.*

Proof. Let $* \in \{\cdot, \backslash, /\}$ and let $x, y \in S$. Then $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon = \mu_S^{(\varepsilon,\delta)}(y)$, which implies that

$$\mu_S^{(\varepsilon,\delta)}(x) + \varepsilon = \varepsilon + \varepsilon > 1 \text{ and } \mu_S^{(\varepsilon,\delta)}(y) + \varepsilon = \varepsilon + \varepsilon > 1,$$

that is, $x_\varepsilon\, q\, \mu_S^{(\varepsilon,\delta)}$ and $y_\varepsilon\, q\, \mu_S^{(\varepsilon,\delta)}$. Since $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in)$-fuzzy subquasigroup of $\mathcal{Q}$, it follows that $(x * y)_\varepsilon = (x * y)_{\min\{\varepsilon,\varepsilon\}} \in \mu_S^{(\varepsilon,\delta)}$ and so that $\mu_S^{(\varepsilon,\delta)}(x * y) = \varepsilon$, that is, $x * y \in S$. Therefore S is a subquasigroup of $\mathcal{Q}$. □

Corollary 3.30. *Let S be a nonempty subset of $\mathcal{Q}$. Assume that $\varepsilon > \max\{\delta, 0.5\}$. If the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\wedge\, q\,)$-fuzzy subquasigroup of $\mathcal{Q}$, then S is a subquasigroup of $\mathcal{Q}$.* □

If we take $\varepsilon = 1$ and $\delta = 0$ in Theorems 3.27 and 3.29, then we have the following corollary.

Corollary 3.31. *A nonempty subset S of $\mathcal{Q}$ is a subquasigroup of $\mathcal{Q}$ if and only if the characteristic function χ_S of S is a $(q, \in)$-fuzzy subquasigroup of $\mathcal{Q}$.* □

Theorem 3.32. *If S is a subquasigroup of $\mathcal{Q}$, then the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$ whenever if any element t in $(0,1]$ satisfies $x_t \in \mu_S^{(\varepsilon,\delta)}$ for $x \in Q$ then $\delta < t$ and $1 - t < \varepsilon$.*

Proof. Let $x, y \in Q$ and $t_1, t_2 \in (0,1]$ be such that $x_{t_1} \in \mu_S^{(\varepsilon,\delta)}$ and $y_{t_2} \in \mu_S^{(\varepsilon,\delta)}$. Then $\mu_S^{(\varepsilon,\delta)}(x) \geqslant t_1 > \delta$ and $\mu_S^{(\varepsilon,\delta)}(y) \geqslant t_2 > \delta$, which imply that $x, y \in S$ and $\varepsilon \geqslant \min\{t_1, t_2\}$. Since S is a subquasigroup of $\mathcal{Q}$, we have $x*y \in S$. Hence $\mu_S^{(\varepsilon,\delta)}(x*y) = \varepsilon \geqslant \min\{t_1, t_2\}$, i.e., $(x*y)_{\min\{t_1,t_2\}} \in \mu_S^{(\varepsilon,\delta)}$. Now, $\mu_S^{(\varepsilon,\delta)}(x*y) + \min\{t_1, t_2\} = \varepsilon + \min\{t_1, t_2\} > 1$ and so $(x*y)_{\min\{t_1,t_2\}}\, q\, \mu_S^{(\varepsilon,\delta)}$. Therefore $(x*y)_{\min\{t_1,t_2\}} \in\wedge q\, \mu_S^{(\varepsilon,\delta)}$, and consequently $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$. □

Corollary 3.33. *If S is a subquasigroup of $\mathcal{Q}$, then the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is both an $(\in, \in\vee q)$-fuzzy subquasigroup and an $(\in, q)$-fuzzy subquasigroup of $\mathcal{Q}$ whenever if any element t in $(0,1]$ satisfies $x_t \in \mu_S^{(\varepsilon,\delta)}$ for $x \in Q$ then $\delta < t$ and $1 - t < \varepsilon$.* □

Theorem 3.34. *Let S be a nonempty subset of $\mathcal{Q}$. If $\varepsilon + \delta \leqslant 1$ and the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$, then S is a subquasigroup of $\mathcal{Q}$.*

Proof. Assume that $\varepsilon + \delta \leqslant 1$ and the (ε, δ)-characteristic fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an $(\in, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$. Let $x, y \in S$. Then $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon = \mu_S^{(\varepsilon,\delta)}(y)$, and so $x_\varepsilon \in \mu_S^{(\varepsilon,\delta)}$ and $y_\varepsilon \in \mu_S^{(\varepsilon,\delta)}$. Hence $(x*y)_\varepsilon = (x*y)_{\min\{\varepsilon,\varepsilon\}} \in\wedge q\, \mu_S^{(\varepsilon,\delta)}$, that is, $(x*y)_\varepsilon = (x*y)_{\min\{\varepsilon,\varepsilon\}} \in \mu_S^{(\varepsilon,\delta)}$ and $(x*y)_\varepsilon = (x*y)_{\min\{\varepsilon,\varepsilon\}}\, q\, \mu_S^{(\varepsilon,\delta)}$. Hence $\mu_S^{(\varepsilon,\delta)}(x*y) \geqslant \varepsilon$ and $\mu_S^{(\varepsilon,\delta)}(x*y) + \varepsilon > 1$. If $\mu_S^{(\varepsilon,\delta)}(x*y) \geqslant \varepsilon$, then $\mu_S^{(\varepsilon,\delta)}(x*y) = \varepsilon$ and thus $x*y \in S$. If $\mu_S^{(\varepsilon,\delta)}(x*y) + \varepsilon > 1$, then $\mu_S^{(\varepsilon,\delta)}(x*y) > 1 - \varepsilon \geqslant \delta$ and so $\mu_S^{(\varepsilon,\delta)}(x*y) = \varepsilon$, which shows that $x*y \in S$. Therefore S is a subquasigroup of $\mathcal{Q}$. □

If we take $\varepsilon = 1$ and $\delta = 0$ in Theorems 3.32 and 3.34, then we have the following corollary.

Corollary 3.35. *A nonempty subset S of $\mathcal{Q}$ is a subquasigroup of $\mathcal{Q}$ if and only if the characteristic function χ_S of S is an $(\in, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$.* □

Theorem 3.36. *If S is a subquasigroup of $\mathcal{Q}$, then the fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$ under the condition that if any element t in $(0,1]$ satisfies $x_t \in \mu_S^{(\varepsilon,\delta)}$ for $x \in Q$ then $\delta \leqslant 1 - t$ and $t < \varepsilon$.*

Proof. Let $x, y \in Q$ and $t_1, t_2 \in (0,1]$ be such that $x_{t_1}\, q\, \mu_S^{(\varepsilon,\delta)}$ and $y_{t_2}\, q\, \mu_S^{(\varepsilon,\delta)}$. Then $\mu_S^{(\varepsilon,\delta)}(x)+t_1 > 1$ and $\mu_S^{(\varepsilon,\delta)}(y)+t_2 > 1$, which imply that $\mu_S^{(\varepsilon,\delta)}(x) > 1-t_1 \geqslant \delta$ and $\mu_S^{(\varepsilon,\delta)}(y) > 1-t_2 \geqslant \delta$. Hence $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon = \mu_S^{(\varepsilon,\delta)}(y)$ and $\varepsilon > \max\{1-t_1, 1-t_2\}$, and so $x, y \in S$. Since S is a subquasigroup of $\mathcal{Q}$, we have $x * y \in S$ and thus

$$\mu_S^{(\varepsilon,\delta)}(x * y) = \varepsilon \geqslant \min\{t_1, t_2\},$$

that is, $(x*y)_{\min\{t_1,t_2\}} \in \mu_S^{(\varepsilon,\delta)}$. Now, $\mu_S^{(\varepsilon,\delta)}(x*y)+\min\{t_1,t_2\} = \varepsilon+\min\{t_1,t_2\} > 1$, and so $(x*y)_{\min\{t_1,t_2\}}\, q\, \mu_S^{(\varepsilon,\delta)}$. Hence $(x*y)_{\min\{t_1,t_2\}} \in\wedge q\, \mu_S^{(\varepsilon,\delta)}$, and $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$. □

Corollary 3.37. *If S is a subquasigroup of $\mathcal{Q}$, then the fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$ under the condition that if any element t in $(0,1]$ satisfies $x_t \in \mu_S^{(\varepsilon,\delta)}$ for $x \in Q$ then $\delta \leqslant 1-t$ and $t < \varepsilon$.* □

Theorem 3.38. *Let S be a nonempty subset of $\mathcal{Q}$. Assume that $\varepsilon > \max\{\delta, 0.5\}$. If the fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$, then S is a subquasigroup of $\mathcal{Q}$.*

Proof. Let $x, y \in S$. Then $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon = \mu_S^{(\varepsilon,\delta)}(y)$, which implies that

$$\mu_S^{(\varepsilon,\delta)}(x) + \varepsilon = \varepsilon + \varepsilon > 1 \text{ and } \mu_S^{(\varepsilon,\delta)}(y) + \varepsilon = \varepsilon + \varepsilon > 1,$$

that is, $x_\varepsilon\, q\, \mu_S^{(\varepsilon,\delta)}$ and $y_\varepsilon\, q\, \mu_S^{(\varepsilon,\delta)}$. Since $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$, it follows that $(x*y)_\varepsilon = (x*y)_{\min\{\varepsilon,\varepsilon\}} \in\wedge q\, \mu_S^{(\varepsilon,\delta)}$ and so that $\mu_S^{(\varepsilon,\delta)}(x*y) \geqslant \varepsilon$. Hence $x * y \in S$ and S is a subquasigroup of $\mathcal{Q}$. □

If we take $\varepsilon = 1$ and $\delta = 0$ in Theorems 3.36 and 3.38, then we have the following corollary.

Corollary 3.39. *A nonempty subset S of $\mathcal{Q}$ is a subquasigroup of $\mathcal{Q}$ if and only if the characteristic function χ_S of S is a $(q, \in\wedge q)$-fuzzy subquasigroup of $\mathcal{Q}$.* □

Theorem 3.40. *Let S be a nonempty subset of $\mathcal{Q}$. Assume that if any element t in $(0,1]$ satisfies $x_t \in \mu_S^{(\varepsilon,\delta)}$ for $x \in Q$ then $\delta \leqslant 1-t$. If S is a subquasigroup of $\mathcal{Q}$, then the fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$.*

Proof. Let $x, y \in Q$ and $t_1, t_2 \in (0,1]$ be such that $x_{t_1}\, q\, \mu_S^{(\varepsilon,\delta)}$ and $y_{t_2}\, q\, \mu_S^{(\varepsilon,\delta)}$. Then $\mu_S^{(\varepsilon,\delta)}(x)+t_1 > 1$ and $\mu_S^{(\varepsilon,\delta)}(y)+t_2 > 1$, which imply that $\mu_S^{(\varepsilon,\delta)}(x) > 1-t_1 \geqslant \delta$ and $\mu_S^{(\varepsilon,\delta)}(y) > 1-t_2 \geqslant \delta$. Hence $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon = \mu_S^{(\varepsilon,\delta)}(y)$, and so $\varepsilon > \max\{1-t_1, 1-t_2\}$ and $x, y \in S$. Since S is a subquasigroup of $\mathcal{Q}$, we have $x * y \in S$ and thus $\mu_S^{(\varepsilon,\delta)}(x*y) = \varepsilon$ which implies that $\mu_S^{(\varepsilon,\delta)}(x*y)+\min\{t_1,t_2\} = \varepsilon+\min\{t_1,t_2\} > 1$, i.e., $(x*y)_{\min\{t_1,t_2\}}\, q\, \mu_S^{(\varepsilon,\delta)}$. It follows that $(x*y)_{\min\{t_1,t_2\}} \in\vee q\, \mu_S^{(\varepsilon,\delta)}$. Therefore $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\vee q)$-fuzzy subquasigroup of $\mathcal{Q}$. □

Theorem 3.41. *Let S be a nonempty subset of Q. Assume that $\varepsilon > \max\{\delta, 0.5\}$ and $\varepsilon + \delta \leqslant 1$. If the fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\vee\, q)$-fuzzy subquasigroup of Q, then S is a subquasigroup of Q.*

Proof. Let $x, y \in S$. Then $\mu_S^{(\varepsilon,\delta)}(x) = \varepsilon = \mu_S^{(\varepsilon,\delta)}(y)$, which implies that

$$\mu_S^{(\varepsilon,\delta)}(x) + \varepsilon = \varepsilon + \varepsilon > 1 \text{ and } \mu_S^{(\varepsilon,\delta)}(y) + \varepsilon = \varepsilon + \varepsilon > 1,$$

that is, $x_\varepsilon\, q\, \mu_S^{(\varepsilon,\delta)}$ and $y_\varepsilon\, q\, \mu_S^{(\varepsilon,\delta)}$. Since $\mu_S^{(\varepsilon,\delta)}$ is a $(q, \in\vee\, q)$-fuzzy subquasigroup of Q, it follows that $(x * y)_\varepsilon = (x * y)_{\min\{\varepsilon,\varepsilon\}} \in\vee\, q\, \mu_S^{(\varepsilon,\delta)}$, that is, $\mu_S^{(\varepsilon,\delta)}(x * y) \geqslant \varepsilon$ or $\mu_S^{(\varepsilon,\delta)}(x*y)+\varepsilon > 1$. If $\mu_S^{(\varepsilon,\delta)}(x*y) \geqslant \varepsilon$, then $x*y \in S$. If $\mu_S^{(\varepsilon,\delta)}(x*y)+\varepsilon > 1$, then $\mu_S^{(\varepsilon,\delta)}(x * y) > 1 - \varepsilon \geqslant \delta$ and so $\mu_S^{(\varepsilon,\delta)}(x * y) = \varepsilon$. Thus $x * y \in S$, and therefore S is a subquasigroup of Q. □

Corollary 3.42. *Let S be a nonempty subset of Q. Assume that $\varepsilon > \max\{\delta, 0.5\}$ and $\varepsilon + \delta \leqslant 1$. If the fuzzy set $\mu_S^{(\varepsilon,\delta)}$ is an (α, β)-fuzzy subquasigroup of Q for $(\alpha, \beta) \in \{(q, \in), (q, \in\wedge\, q), (q, q)\}$, then S is a subquasigroup of Q.* □

If we take $\varepsilon = 1$ and $\delta = 0$ in Theorems 3.40 and 3.41, then we have the following corollary.

Corollary 3.43. *A nonempty subset S of Q is a subquasigroup of Q if and only if the characteristic function χ_S of S is a $(q, \in\vee\, q)$-fuzzy subquasigroup of Q.* □

References

[1] **M. Akram and W.A. Dudek**, *Generalized fuzzy subquasigroups,* Quasigroups and Related Systems **16** (2008), 133 – 146.

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

[3] **W.A. Dudek**, *Fuzzy subquasigroups,* Quasigroups and Related Systems **5** (1998), 81 – 98.

[4] **H.O. Pflugfelder**, *Quasigroups and loops: introduction,* Sigma Series in Pure Math., vol. 7, Heldermann Verlag, Berlin 1990.

[5] **P.M. Pu and Y.M. Liu**, *Fuzzy topology I, Neighborhood structure of a fuzzy point and Moore-Smith convergence,* J. Math. Anal. Appl. **76** (1980), 571 – 599.

Received December 8, 2014

Y.B.Jun
Department of Mathematics Education, Gyeongsang National University, Jinju 660-701, Korea
e-mail: skywine@gmail.com

S.Z.Song
Department of Mathematics, Jeju National University, Jeju 690-756, Korea
e-mail: szsong@jejunu.ac.kr

G.Muhiuddin
Department of Mathematics, University of Tabuk, Tabuk 71491, Saudi Arabia
e-mail: chishtygm@gmail.com

Actions over monoids and hypergroups

Abolghasem Karimi Feizabadi and Hamid Rasouli

Abstract. We construct the hypergroups by actions over monoids. Particularly, some non-unital hypergroups are constructed. Here, hypergroups are obtained by orbit neighborhood collections that make a complete lattice.

1. Introduction and preliminaries

A generating technique of examples in a theory can be very useful, in particular if it is not given various fundamental examples in that theory. One of these theories is the theory of hypergroups which was introduced in 1934 by Marty [3].

A *hyperoperation* on a set H is a map $\cdot : H \times H \to P^*(H)$, where $P^*(H)$ is the set of all non-empty subsets of H. The set H with a hyperoperation $\cdot$ is called a *hypergroup* if for every $x, y, z \in H$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (*association law*), and $x \cdot H = H \cdot x = H$. For more information, see [1] and [4].

In the sense of category theory, an action over monoids is a monoid in the category T-**Act** of all T-acts for a monoid T. Let M be a monoid with no zero element. For any monoid T, a homomorphism of monoids:

$$\Phi : T \to H(M);\ t \mapsto \varphi_t : M \to M,$$

where $H(M)$ denotes the monoid of all endomorphisms of M is said to be an *action over monoids*. Note that $H(M)$ has a (unique) zero element which is a constant mapping equals 1. If T has a zero element 0, we impose the assumption that $T \backslash \{0\}$ is a monoid. So letting φ_0 be the zero element of $H(M)$, $\Phi : T \to H(M)$ is a homomorphism of semigroups. In this case, $m\varphi_0 = 1$ for every $m \in M$ and then Φ is called a *zero faithful action*.

In this paper a generating technique for constructing hypergroups is presented. Using neighborhood collections, we construct a class of hypergroups, and describe how an action over monoids can be applied to obtain a hypergroup. We consider hypergroup actions over monoids, which are those actions $\Phi : T \to H(M)$ over monoids for which $(M, \bullet)$ is a hypergroup. It is obtained a necessary and sufficient condition for a hypergroup action over monoids to be unital, that is, $1 \in x \bullet y$ for all $x, y \in M$.

2010 Mathematics Subject Classification: 20N20, 20M30, 20M32, 20M50, 20M99
Keywords:Action over monoids, hypergroup, orbit neighborhood collection.
We thank the kind hospitality of Hakim Sabzevari University during the several times we stayed there.

For a monoid M, on the monoid $H(M)$ of all endomorphisms of M we consider the operation $\star : M \to M$ defined by $\sigma \star \mu := \mu \circ \sigma$, for each $\mu, \sigma \in H(M)$. To denote the image of $x \in M$ under σ we will use the postfix notation. Also $Sub(M)$ denotes the set of all submonoids of M. Throughout M stands for a monoid with no zero element unless otherwise stated.

2. Actions over monoids

In this section first we give some instances of actions over monoids

Example 2.1. Each of the following is an action over monoids:

(i) For any commutative monoid M and $T = (\mathbb{N}, \cdot), \Phi : T \to H(M); m\varphi_k = m^k$.

(ii) For any submonoid T of $H(M), \Phi : T \to H(M); \Phi := id_T$ (*natural action*).

(iii) For any monoid T with zero, $\Phi : T \to H(M); \varphi_t := id_M$ for each $0 \neq t \in T$. If $t = 0, m\varphi_0 := 1$, for each $m \in M$. □

Let M be a monoid. By a *neighborhood collection* on M we mean the sequence $\mathcal{V} = \{V_x : x \in M\}$ indexed by M, such that for each $x \in M$, $V_x \subseteq M$ and $x \in V_x$. If $\mathcal{V}$ is a neighborhood collection, we define a hyperoperation, called *the hyperoperation induced by* $\mathcal{V}$ in the following way: for each $x, y \in M$, $x \bullet y = V_x V_y$, where $V_x V_y$ is the usual product of subsets V_x and V_y of M. It is clear that for every $x, y \in M$, $xy \in x \bullet y$. For every $a \in M$ and a non-empty subset X of M, we put $a \bullet X := \bigcup_{x \in X} a \bullet x$ and $X \bullet a := \bigcup_{x \in X} x \bullet a$. Clearly, $a \bullet M = V_a M$ and $M \bullet a = M V_a$ for each $a \in M$. Also we have:

Lemma 2.2. *If M is a group, then $(M, \bullet)$ is a hypergroup.*

Proof. Let M be a monoid and $\emptyset \neq A \subseteq M$. If there is an invertible element $a \in A$, then $AM = M = MA$. Moreover, if M is a group, then the operation on subsets of M is also associative. Therefore, if M is a group and $\bullet$ is a hyperoperation induced by any neighborhood collection, then M is a hypergroup. □

Definition 2.3. Let $\Phi : T \to H(M)$ be an action over monoids. Then the set $\{m\varphi_t : t \in T\}$ of all images of an element $m \in M$ under the mappings $\Phi(t)$ is usually called *the orbit* of m and it is denoted by $Orb_T(m)$. It is obvious that for each $m \in M, m \in Orb_T(m)$. Hence, $\mathcal{V}_T = \{V_m = Orb_T(m) : m \in M\}$ is the set of all orbits of elements from M which is called *the orbit neighborhood collection*.

From now on, $\bullet$ stands for the hyperoperation induced by orbit neighborhood collection. Also, for a submonoid S of $H(M)$, by $\mathcal{V}_S$ we mean the orbit neighborhood collection induced by the natural action from S to $H(M)$. In this case, $\mathcal{V}_S = \{Orb_S(m) : m \in M\}$, where $Orb_S(m) = \{m\sigma : \sigma \in S\}$ for each $m \in M$.

Definition 2.4. An action $\Phi : T \to H(M)$ over monoids is called *right* (*left*) *multiplicative* if for each $m \in M$ and $0 \neq t \in T$, there exists $x \in M$ such that $m\varphi_t = mx$ ($m\varphi_t = xm$).

The action over monoids in Example 2.1(i) is (left and right) multiplicative. If $\Phi : T \to H(M)$ is a (left) right multiplicative zero faithful action, then M is a group.

Proposition 2.5. *Let $\Phi : T \to H(M)$ be a (left) right multiplicative action over monoids. Then $(M, \bullet)$ is a hypergroup if and only if M is a group.*

Proof. Suppose $(M, \bullet)$ is a hypergroup. Let $m \in M$. By assumption, for each $t \in T$, $m\varphi_t M = mxM \subseteq mM$ for some $x \in M$. Thus

$$M = m \bullet M = Orb_T(m)M = \bigcup_{t\in T} m\varphi_t M \subseteq mM.$$

Then $M = mM$. Hence, M is a group. The converse follows from Lemma 2.2. □

Remark 2.6. An action $\Phi : T \to H(M)$ over monoids and the natural action $\Psi = id_{\Phi(T)} : \Phi(T) \to H(M)$ defined as in Example 2.1(ii) have the same orbits of elements from M.

Let M be a monoid and $\mathcal{V}, \mathcal{W}$ be two neighborhood collections on M. We say $\mathcal{V} \leq \mathcal{W}$ if for every $x \in M$, $V_x \subseteq W_x$. Clearly, $\leq$ is a partial order relation on the set of all neighborhood collections.

A neighborhood collection $\mathcal{V} = \{V_x : x \in M\}$ is called a *basis neighborhood collection* if for every $y \in V_x$, $V_y \subseteq V_x$. For instance, if $\Phi : T \to H(M)$ is an action over monoids, then the orbit neighborhood collection $\mathcal{V}_T$ is a basis neighborhood collection. Indeed, for any $x, y \in M$, $y \in Orb_T(x)$ implies that $y = x\varphi_t$ for some $t \in T$ and then $Orb_T(y) = \{x\varphi_{ts} : s \in T\} \subseteq Orb_T(x)$.

Lemma 2.7. *Let $\mathcal{V} = \{V_x : x \in M\}$ be a basis neighborhood collection and $S = \{\sigma \in H(M) : x\sigma \in V_x$ for all $x \in M\}$. The following statements hold:*

(i) *S is a submonoid of $H(M)$ and $\mathcal{V}_S \leq \mathcal{V}$.*

(ii) *For every action $\Phi : T \to H(M)$ over monoids satisfying $\mathcal{V}_T \leq \mathcal{V}$, we have $\mathcal{V}_T \leq \mathcal{V}_S$.*

Proof. (i) For every $x \in M$, $x\ id_M = x \in V_x$, so $id_M \in S$. Let $\sigma, \mu \in S$. Then $x\sigma \in V_x$ and $x\sigma\mu \in V_{x\sigma}$ for all $x \in M$, and so $x\sigma\mu = (x\sigma)\mu \in V_{x\sigma} \subseteq V_x$ because $\mathcal{V}$ is a basis. Therefore, $\sigma\mu \in S$. (ii) It follows from Remark 2.6. □

For a monoid M, let $\mathbf{ONC}(M)$ denote the set of all orbit neighborhood collections $\mathcal{V}_T$, for all monoids T such that there is an action over monoids T and M.

Theorem 2.8. *For a monoid M, $(\mathbf{ONC}(M), \leq)$ is a complete lattice.*

Proof. Let $\{T_i : i \in I\}$ be a non-empty family of monoids such that $\Phi_i : T_i \to H(M)$ is an action over monoids for all $i \in I$. For every $x \in M$, let $V_x = \bigcap_{i\in I} Orb_{T_i}(x)$. Also take $\mathcal{V} = \{V_x : x \in M\}$. It is easy to check that $\mathcal{V}$ is a basis neighborhood collection. Put $S := \{\sigma \in H(M) : x\sigma \in V_x$ for all $x \in M\}$. We claim that $\mathcal{V}_S = \bigwedge_{i\in I} \mathcal{V}_{T_i}$. By Lemma 2.7(i), $\mathcal{V}_S \leq \mathcal{V}$. So $\mathcal{V}_S \leq \mathcal{V}_{T_i}$ for all

$i \in I$. Suppose $\mathcal{V}_T \in \mathbf{ONC}(M)$ and $\mathcal{V}_T \leq \mathcal{V}_{T_i}$ for all $i \in I$. Let $x \in M$. We have $Orb_T(x) \subseteq Orb_{T_i}(x)$ for all $i \in I$. Then $Orb_T(x) \subseteq \bigcap_{i\in I} Orb_{T_i}(x) = V_x$. Since $\mathcal{V}$ is a basis neighborhood collection, $\mathcal{V}_T \leq \mathcal{V}_S$ by Lemma 2.7(ii), as desired. Note that $\mathcal{V}_{\{id_M\}}$ is the bottom element, and $\mathcal{V}_{H(M)}$ is the top element of $\mathbf{ONC}(M)$. □

Remark 2.9. Let $\{T_i : i \in I\}$ be a non-empty family of submonoids of a monoid T and $\Phi : T \to H(M)$ be an action over monoids. Then, using Lemma 2.7 and Theorem 2.8, $\mathcal{V}_{\bigcap_{i\in I} T_i} \leq \bigwedge_{i\in I} \mathcal{V}_{T_i} \leq \mathcal{V}$, where $V_x = \bigcap_{i\in I} Orb_{T_i}(x)$ and $\mathcal{V} = \{V_x : x \in M\}$. But, $\mathcal{V}_{\bigcap_{i\in I} T_i}$ and $\mathcal{V}$ are not necessarily equal. For instance, let $M = (\mathbb{Z}_{100}, \cdot)$ and $T = (\mathbb{N}, \cdot)$. Consider the action $\Phi : T \to H(M)$ over monoids defined by $a\varphi_n := a^n$ for each $n \in \mathbb{N}$ and $a \in \mathbb{Z}_{100}$. Let $T_1 = \{2^k : k \in \mathbb{N} \cup \{0\}\}$ and $T_2 = \{3^k : k \in \mathbb{N} \cup \{0\}\}$. Then T_1 and T_2 are submonoids of T such that $T_1 \cap T_2 = \{1\}$. Let $a = 5 \in \mathbb{Z}_{100}$. We have $a^2 \neq a$, $a^3 \neq a$ and $a^2 = a^3$. So $a^2 \in Orb_{T_1}(a) \cap Orb_{T_2}(a)$, but $a^2 \notin Orb_{T_1 \cap T_2}(a)$. Therefore, $Orb_{T_1\cap T_2}(a) \neq Orb_{T_1}(a) \cap Orb_{T_2}(a)$.

Question: The map $\psi : Sub(H(M)) \to \mathbf{ONC}(M)$ given by $T \mapsto \mathcal{V}_T$ is a poset homomorphism. Is ψ a lattice homomorphism? Generally: Let $\Phi : S \to H(M)$ be an action over monoids. When is the map $\phi : Sub(S) \to \mathbf{ONC}(M)$, given by $\phi(T) = \mathcal{V}_T$, a lattice homomorphism?

3. Non-unital hypergroup actions over monoids

In this section, we introduce and study the notion of hypergroup action over monoids and construct two kinds of non-unital hypergroup actions over monoids.

Definition 3.1. An action over monoids $\Phi : T \to H(M)$ is called a *hypergroup action over monoids* if $(M, \bullet)$ is a hypergroup, where the hyperoperation $\bullet$ is induced by orbit neighborhood collection.

In view of Lemma 2.2, any action $\Phi : T \to H(M)$ is a hypergroup action over monoids provided M is a group.

Proposition 3.2. *For every monoids T and M, $\Phi : T \to H(M)$ is a hypergroup action over monoids if and only if for every $m \in M$ there exist $s, t \in T$ such that $m\varphi_s$ is right invertible and $m\varphi_t$ is left invertible in M.*

Proof. clearly $\Phi : T \to H(M)$ is a hypergroup action over monoids if and only if for each $m \in M$, $Orb_T(m)M = M = MOrb_T(m)$. Then the assertion holds. □

Example 3.3. Consider the monoid $T = \{0, 1\}$. For a zero faithful action $\Phi : T \to H(M)$ over monoids, $(M, \bullet)$ is a hypergroup by Proposition 3.2. To describe the hyperoperation $\bullet$ induced by $\mathcal{V}_T$, let $x, y \in M$. We have $x \bullet y = Orb_T(x)Orb_T(y) = \{1, x\}\{1, y\} = \{1, x, y, xy\}$. □

Definition 3.4. Let M be a monoid without zero and $\odot$ be a hyperoperation on M. Then $(M, \odot)$ is called *unital* if for every $x, y \in M$, $1 \in x \odot y$. A hypergroup action $\Phi : T \to H(M)$ over monoids is called *unital* if $(M, \bullet)$ is unital, where $\bullet$ is the hyperoperation induced by $\mathcal{V}_T$.

Lemma 3.5. *A hypergroup action $\Phi : T \to H(M)$ over monoids is unital if and only if $1 \in Orb_T(x)$ for any $x \in M$.*

Proof. Let $\Phi : T \to H(M)$ be a hypergroup action over monoids. If Φ is non-unital, then there are $x, y \in M$ such that $1 \notin x \bullet y \supseteq Orb_T(xy)$ which is a contradiction. The converse follows from the fact that $x \bullet 1 = Orb_T(x)$ for each $x \in M$. □

By virtue of Proposition 3.2 and Lemma 3.5, the following is immediate:

Corollary 3.6. *Every zero faithful action is a unital hypergroup action over monoids.* □

Corollary 3.6 provides an easy construction of a unital hypergroup action over monoids. But, finding a non-unital hypergroup action over monoids is not so easy.

Let G be a non-trivial group. For any $* \notin G$, put $G^* := G \cup \{*\}$. Define $*a = a* = *$ for all $a \in G^*$. Then G^* is a monoid in which $*$ is a zero element, and every non-zero element is invertible. For a non-empty set X, let G_X denote the set of all mappings $f : X \to G^*$ satisfying $xf \neq *$ for some $x \in X$. For every $f, g \in G_X$ and $x \in X$, define $(x)fg := (xf)(xg)$. Under this multiplication, G_X is a monoid with no zero element. Also the identity of G_X is the map $\mathbb{I}_{G_X}$ given by $x\mathbb{I}_{G_X} = 1$, for each $x \in X$. Note that $H(G_X)$ has a zero element given by the endomorphism $\mathcal{O} : G_X \to G_X$ such that for any $f \in G_X, f\mathcal{O} = \mathbb{I}_{G_X}$.

Now, take a map $\alpha : X \to X$. Define $\tilde{\alpha} : G_X \to G_X$ by $f\tilde{\alpha} := \alpha f$ and put $T_X := \{\tilde{\alpha} \mid \alpha : X \to X \text{ is a map}\}$. Then we get the following:

Lemma 3.7.

(i) *$\tilde{\alpha} \in H(G_X)$, and T_X is a submonoid of $H(G_X)$ such that $\mathcal{O} \notin T_X$.*

(ii) *An $f \in G_X$ is invertible if and only if for every $x \in X$, $xf \neq *$. In this case, $xf^{-1} = (xf)^{-1}$ for all $x \in X$.*

Proof. (i) For every $g, h \in G_X$, $(gh)\tilde{\alpha} = \alpha(gh) = (\alpha g)(\alpha h) = (g\tilde{\alpha})(h\tilde{\alpha})$. So $\tilde{\alpha}$ is an endomorphism of G_X. To prove T_X is a submonoid of $H(G_X)$, let $\alpha, \beta : X \to X$ be two maps. For every $f \in G_X$ we have $f\tilde{\alpha}\tilde{\beta} = (\alpha f)\tilde{\beta} = \beta(\alpha f) = (\beta\alpha)f = f\widetilde{\beta\alpha}$. Then $\tilde{\alpha}\tilde{\beta} = \widetilde{\beta\alpha} \in T_X$. Also $id_{G_X} = \widetilde{id_X} \in T_X$. Finally, if $\mathcal{O} \in T_X$, then there is a mapping $\alpha : X \to X$ such that $\tilde{\alpha} = \mathcal{O}$. Take an $f \in G_X$ satisfying $xf \neq 1$ for each $x \in X$. Then $\alpha f = f\tilde{\alpha} = f\mathcal{O} = \mathbb{I}_{G_X}$ which is a contradiction.

(ii) Note that $f \in G_X$ is invertible if and only if xf is invertible for all $x \in X$. Since every $a \neq *$ in G^* is invertible, the assertion holds. □

In light of Lemma 3.7(i), we have the natural action $\Phi_X : T_X \to H(G_X)$ over monoids. Now the following result is obtained.

Theorem 3.8. *The natural action $\Phi_X : T_X \to H(G_X)$ is a non-unital hypergroup action over monoids.*

Proof. First we show that for every $f \in G_X$ there exists an endomorphism $\sigma : G_X \to G_X$ such that $\sigma \in T_X$ and $f\sigma$ is invertible. To this end, let $f \in G_X$, $Y = \{x \in X : xf \neq *\} \neq \emptyset$ and $\alpha : X \to X$ be a mapping such that $X\alpha = Y$. Considering $\sigma = \tilde{\alpha} \in T_X$, we have $xf\sigma = xf\tilde{\alpha} = x\alpha f \neq *$ for each $x \in X$. Then it follows from Lemma 3.7(ii) that $f\sigma$ is invertible. Now, using Proposition 3.2, Φ_X is a hypergroup action over monoids. To complete the proof, using Lemma 3.5, it suffices to find an $f \in G_X$ such that $\mathbb{I}_{G_X} \notin Orb_{T_X}(f)$. Take any $a \in G$ such that $a \neq 1$, and the constant map f corresponding to a such that $xf = a$ for all $x \in X$. For every map $\alpha : X \to X$ and $x \in X$, $xf\tilde{\alpha} = x\alpha f = a$. Thus $f\tilde{\alpha} \neq \mathbb{I}_{G_X}$, and hence $\mathbb{I}_{G_X} \notin Orb_{T_X}(f)$. □

Let M be a monoid and G be a non-trivial group. Then $M \times G$ is a monoid without zero under the usual componentwise binary operation. Define $\xi : M \times G \to M \times G$ by $(m, g)\xi = (1, g)$ for every $m \in M, g \in G$. Clearly, ξ is an endomorphism of $M \times G$ such that for every $x \in M \times G$, $x\xi$ is invertible, and $\xi^2 = \xi$. Now we have the following:

Proposition 3.9. *If T is a submonoid of $H(M \times G)$ without zero that contains ξ, then the natural action $\Phi : T \to H(M \times G)$ is a hypergroup action over monoids. In particular, $\Phi_\xi : T_\xi \to H(M \times G)$ is a non-unital hypergroup action over monoids, where $T_\xi = \{id, \xi\}$.*

Proof. We have $\xi \in T$ and $x\xi$ is invertible for all $x \in M \times G$. It follows from Proposition 3.2 that $\Phi : T \to H(M \times G)$ is a hypergroup action over monoids. Consider T_ξ, and let $x = (1, g) \in M \times G$ such that $g \neq 1$. Then we get $(1, 1) \notin Orb_{T_\xi}(x) = \{x\}$. Using Lemma 3.5, Φ_ξ is a non-unital hypergroup action over monoids. □

References

[1] **P. Corsini**, *Prolegomena of hypergroup theory*, Aviani Editor, 1993.

[2] **M. Kilp, U. Knauer, and A.V. Mikhalev**, *Monoids, Acts and Categories*, de Gruyter, Berlin, 2000.

[3] **F. Marty**, *Sur une généralization de la notion de groupe*, 8th Congress Math. Scandenaves, Stockholm, (1934), 45-49.

[4] **T. Vougiouklis**, *Hyperstructures and their representations*, Hadronic Press, Inc., 1994.

Received May 26, 2014
Revised April 7, 2015

A. Karimi Feizabadi
Department of Math., Gorgan Branch, Islamic Azad University, Gorgan, Iran
E-mail: akarimi@gorganiau.ac.ir, karimimath@yahoo.com
H. Rasouli
Department of Math., Science and Research Branch, Islamic Azad University, Tehran, Iran
E-mail: hrasouli@srbiau.ac.ir

On intra-regular and some left regular Γ-semigroups

Niovi Kehayopulu and *Michael Tsingelis*

Abstract. We characterize the intra-regular Γ-semigroups and the left regular Γ-semigroups M in which $x\Gamma M \subseteq M\Gamma x$ for every $x \in M$ in terms of filters and we prove, among others, that every intra-regular Γ-semigroup is decomposable into simple components, and every Γ-semigroup M for which $x\Gamma M \subseteq M\Gamma x$ is left regular, is decomposable into left simple components.

1. Introduction and prerequisites

A structure theorem concerning the intra-regular semigroups, another one concerning some left regular semigroups have been given in [3]. These are the two theorems in [3]:

Theorem II.4.9. *The following conditions on a semigroup S are equivalent:*
(1) *Every $\mathcal{N}$-class of S is simple.*
(2) *Every ideal of S is completely semiprime.*
(3) *For every $x \in S$, $x \in Sx^2S$.*
(4) *For every $x \in S$, $N(x) = \{y \in S \mid x \in SyS\}$.*
(5) $\mathcal{N} = \mathcal{I}$.
(6) *Every ideal of S is a union of $\mathcal{N}$-classes.*

Theorem II.4.5. *The following conditions on a semigroup S are equivalent:*
(1) *Every $\mathcal{N}$-class of S is left simple.*
(2) *Every left ideal of S is completely semiprime and two-sided.*
(3) *For every $x \in S$, $x \in Sx^2$ and $xS \subseteq Sx$.*
(4) *For every $x \in S$, $N(x) = \{y \in S \mid x \in Sy\}$.*
(5) $\mathcal{N} = \mathcal{L}$.
(6) *Every left ideal of S is a union of $\mathcal{N}$-classes.*

Note that we always use the term “semiprime" instead of “completely semiprime" given by Petrich in [3]. So the condition (2) in the two theorems above should be read as “Every ideal (resp. left ideal) of S is semiprime", meaning that if A is an ideal (resp. left ideal) of S, then for every $x \in S$ such that $x^2 \in A$, we have $x \in A$. In the present paper we generalize these results in case of Γ-semigroups.

2010 Mathematics Subject Classification: 20M99, 06F99
Keywords: Γ-semigroup; left (right) congruence; semilattice congruence; left (right) ideal; left (right) simple; simple; intra-regular; left (right) regular.

Let M be a Γ-semigroup. An equivalence relation σ on M is called *left* (resp. *right*) *congruence* (on M) if $(a,b)\in\sigma$ implies $(c\gamma a, c\gamma b)\in\sigma$ (resp. $(a\gamma c, b\gamma c)\in\sigma$) for every $c\in M$ and every $\gamma\in\Gamma$. A relation σ which is both left and right congruence on M is called a *congruence* on M. A congruence σ on M is called *semilattice congruence* if $(a\gamma b, b\gamma a)\in\sigma$ and $(a\gamma a, a)\in\sigma$ for every $a,b\in M$ and every $\gamma\in\Gamma$. A nonempty subset A of M is called a *left* (resp. *right*) *ideal* of M if $M\Gamma A\subseteq A$ (resp. $A\Gamma M\subseteq A$). A subset A of M which is both a left and right ideal of M is called an *ideal* of M. For an element a of M, we denote by $L(a)$, $R(a)$, $I(a)$ the left ideal, right ideal and the ideal of M, respectively, generated by a, and we have $L(a)=a\cup M\Gamma a$, $R(a)=a\cup a\Gamma M$, $I(a)=a\cup M\Gamma a\cup a\Gamma M\cup M\Gamma a\Gamma M$. We denote by $\mathcal{L}$ the equivalence relation on M defined by $\mathcal{L}:=\{(a,b)\mid L(a)=L(b)\}$, by $\mathcal{R}$ the equivalence relation on M defined by $\mathcal{R}:=\{(a,b)\mid R(a)=R(b)\}$ and by $\mathcal{I}$ the equivalence relation on M defined by $\mathcal{I}:=\{(a,b)\mid I(a)=I(b)\}$. A nonempty subset A of M is called a *subsemigroup* of M if $a,b\in A$ and $\gamma\in\Gamma$ implies $a\gamma b\in A$, that is, $A\Gamma A\subseteq A$. A subsemigroup F of M is called a *filter* of M if $a,b\in F$ and $\gamma\in\Gamma$ such that $a\gamma b\in F$ implies $a\in F$ and $b\in F$. We denote by $\mathcal{N}$ the relation on M defined by $\mathcal{N}:=\{(a,b)\mid N(a)=N(b)\}$ where $N(x)$ is the filter of M generated by x $(x\in M)$. It is well known that the relation $\mathcal{N}$ is a semilattice congruence on M. So, if $z\in M$ and $\gamma\in\Gamma$, then we have $(z\gamma z, z)\in\mathcal{N}$, $(z\gamma z\gamma z, z\gamma z)\in\mathcal{N}$, $(z\gamma z\gamma z\gamma z, z\gamma z\gamma z)\in\mathcal{N}$ and so on. A subset A of M is called *semiprime* if $a\in M$ and $\gamma\in\Gamma$ such that $a\gamma a\in A$ implies $a\in A$. A Γ-semigroup $(M,\Gamma,.)$ is called *left simple* if for every left ideal L of M, we have $L=M$, that is, M is the only left ideal of M. A subsemigroup T of M is called *left simple* if the Γ-semigroup $(T,\Gamma,.)$ (that is, the set T with the same Γ and the multiplication "." on M) is left simple. Which means that for every left ideal A of T, we have $A=T$. A subsemigroup of M which is both left simple and right simple is called *simple*. If M is a Γ-semigroup and σ a semilattice congruence on M, then the class $(a)_\sigma$ of M containing a is a subsemigroup of M for every $a\in M$. Let now M be a Γ-semigroup and σ a congruence on M. For $a,b\in M$ and $\gamma\in\Gamma$, we define $(a)_\sigma\gamma(b)_\sigma:=(a\gamma b)_\sigma$. Then the set $M/\sigma:=\{(a)_\sigma\mid a\in M\}$ is a Γ-semigroup as well. A Γ-semigroup M is said to be a *semilattice of simple semigroups* if there exists a semilattice congruence σ on M such that the class $(x)_\sigma$ is a simple subsemigroup of M for every $x\in M$.

2. Intra-regular Γ-semigroups

We characterize here the intra-regular Γ-semigroups in terms of filtres and we prove that every intra-regular Γ-semigroup is decomposable into simple subsemigroups.

Definition 1. (cf. [2]) A Γ-semigroup M is called *intra-regular* if

$$x\in M\Gamma x\gamma x\Gamma M$$

for every $x\in M$ and every $\gamma\in\Gamma$.

Lemma 2. (cf. [1]) *If M is a Γ-semigroup, then $\mathcal{I} \subseteq \mathcal{N}$.*

Theorem 3. *Let M be a Γ-semigroup. The following are equivalent:*

(1) *M is intra-regular.*

(2) *$N(x) = \{y \in M \mid x \in M\Gamma y\Gamma M\}$ for every $x \in M$.*

(3) *$\mathcal{N} = \mathcal{I}$.*

(4) *For every ideal I of M, we have $I = \bigcup\limits_{x\in I} (x)_{\mathcal{N}}$.*

(5) *$(x)_{\mathcal{N}}$ is a simple subsemigroup of M for every $x \in M$.*

(6) *M is a semilattice of simple semigroups.*

(7) *Every ideal of M is semiprime.*

Proof. (1) $\Longrightarrow$ (2). Let $x \in M$ and $T := \{y \in M \mid x \in M\Gamma y\Gamma M\}$. T is a filter of M. In fact: Take an element $\gamma \in \Gamma$ ($\Gamma \neq \emptyset$). Since M is intra-regular, we have

$$x \in M\Gamma x\gamma x\Gamma M = (M\Gamma x)\gamma x\Gamma M \subseteq (M\Gamma M)\gamma x\Gamma M \subseteq M\Gamma x\Gamma M,$$

then $x \in T$, and T is a nonempty subset of M. Let $a, b \in T$ and $\gamma \in \Gamma$. Then $a\gamma b \in T$. Indeed: Since $b \in T$, we have $x \in M\Gamma b\Gamma M$. Since $a \in T$, $x \in M\Gamma a\Gamma M$. Since M is intra-regular, we have

$$\begin{aligned} x \in M\Gamma x\gamma x\Gamma M &\subseteq M\Gamma(M\Gamma b\Gamma M)\gamma(M\Gamma a\Gamma M)\Gamma M \\ &= (M\Gamma M)\Gamma(b\Gamma M\gamma M\Gamma a)\Gamma(M\Gamma M) \\ &\subseteq M\Gamma(b\Gamma M\gamma M\Gamma a)\Gamma M. \end{aligned}$$

We prove that $b\Gamma M\gamma M\Gamma a \subseteq M\Gamma(a\gamma b)\Gamma M$. Then we have

$$x \in M\Gamma\Big(M\Gamma(a\gamma b)\Gamma M\Big)\Gamma M \subseteq M\Gamma(a\gamma b)\Gamma M,$$

and $a\gamma b \in T$. For this purpose, let $b\delta u\gamma v\rho a \in b\Gamma M\gamma M\Gamma a$, where $u, v \in M$ and $\delta, \rho \in \Gamma$. Since M is intra-regular, $b\delta u\gamma v\rho a \in M$ and $\gamma \in \Gamma$, we have

$$\begin{aligned} b\delta u\gamma v\rho a &\in M\Gamma(b\delta u\gamma v\rho a)\gamma(b\delta u\gamma v\rho a)\Gamma M \\ &= (M\Gamma b\delta u\gamma v)\rho(a\gamma b)\delta(u\gamma v\rho a\Gamma M) \\ &\subseteq M\Gamma(a\gamma b)\Gamma M, \end{aligned}$$

so $b\delta u\gamma v\rho a \in M\Gamma(a\gamma b)\Gamma M$. Let $a, b \in M$ and $\gamma \in \Gamma$ such that $a\gamma b \in T$. Then $a, b \in T$. Indeed: Since $a\gamma b \in T$, we have

$$x \in M\Gamma(a\gamma b)\Gamma M = M\Gamma a\gamma(b\Gamma M) \subseteq M\Gamma a\Gamma M \text{ and}$$

$$x \in (M\Gamma a)\gamma b\Gamma M \subseteq M\Gamma b\Gamma M,$$

so $a, b \in T$. Let now F be a filter of M such that $x \in F$. Then $T \subseteq F$. Indeed: Let $a \in T$. Then $x \in M\Gamma a\Gamma M$, so $x = u\gamma a\rho v$ for some $u, v \in M$, $\gamma, \rho \in \Gamma$. Since $u, a\rho v \in M$, $u\gamma(a\rho v) \in F$ and F is a filter of M, we have $u \in F$ and $a\rho v \in F$. Since $a, v \in M$, $a\rho v \in F$ and F is a filter, we have $a \in F$ and $v \in F$, so $a \in F$.

(2) $\Longrightarrow$ (3). Let $(a,b)\in\mathcal{N}$. Then $a\in N(a)=N(b)$. Since $a\in N(b)$, by (2), we have $b\in M\Gamma a\Gamma M\subseteq a\cup M\Gamma a\cup a\Gamma M\cup M\Gamma a\Gamma M=I(a)$. Since $I(a)$ is an ideal of M containing b, we have $I(b)\subseteq I(a)$. Since $b\in N(a)$, by symmetry, we get $I(a)\subseteq I(b)$. Then $I(a)=I(b)$, and $(a,b)\in\mathcal{I}$. Thus we have $\mathcal{N}\subseteq\mathcal{I}$. On the other hand, by Lemma 2, $\mathcal{I}\subseteq\mathcal{N}$. Thus $\mathcal{N}=\mathcal{I}$.

(3) $\Longrightarrow$ (4). Let I be an ideal of M. If $y\in I$, then $y\in(y)_{\mathcal{N}}\subseteq\bigcup\limits_{x\in I}(x)_{\mathcal{N}}$. Let $y\in\bigcup\limits_{x\in I}(x)_{\mathcal{N}}$. Then $y\in(x)_{\mathcal{N}}$ for some $x\in I$. Then, by (3), $(y,x)\in\mathcal{N}=\mathcal{I}$, so $I(y)=I(x)$. Since $x\in I$ and $I(x)$ is the ideal of M generated by x, we have $I(x)\subseteq I$. Thus we have $y\in I(y)=I(x)\subseteq I$, and $y\in I$.

(4) $\Longrightarrow$ (5). Let $x\in M$. Since $\mathcal{N}$ is a semilattice congruence on M, $(x)_{\mathcal{N}}$ is a subsemigroup of M. Let I be an ideal of $(x)_{\mathcal{N}}$. Then $I=(x)_{\mathcal{N}}$. In fact: Let $y\in(x)_{\mathcal{N}}$. Take an element $z\in I$ and an element $\gamma\in\Gamma$ ($I,\Gamma\neq\emptyset$). The set $M\Gamma z\gamma z\gamma z\Gamma M$ is an ideal of M. Indeed, it is a nonempty subset of M, and we have

$$M\Gamma(M\Gamma z\gamma z\gamma z\Gamma M)=(M\Gamma M)\Gamma z\gamma z\gamma z\Gamma M\subseteq M\Gamma z\gamma z\gamma z\Gamma M \text{ and}$$

$$(M\Gamma z\gamma z\gamma z\Gamma M)\Gamma M=M\Gamma z\gamma z\gamma z\Gamma(M\Gamma M)\subseteq M\Gamma z\gamma z\gamma z\Gamma M.$$

By hypothesis, we have $M\Gamma z\gamma z\gamma z\Gamma M=\bigcup\limits_{t\in M\Gamma z\gamma z\gamma z\Gamma M}(t)_{\mathcal{N}}$.

Since $z\gamma z\gamma z\gamma z\gamma z\in M\Gamma z\gamma z\gamma z\Gamma M$, we have $(z\gamma z\gamma z\gamma z\gamma z)_{\mathcal{N}}\subseteq M\Gamma z\gamma z\gamma z\Gamma M$. Since $(z\gamma z,z)\in\mathcal{N}$ and $z\in I\subseteq(x)_{\mathcal{N}}$, we have $(z\gamma z\gamma z\gamma z\gamma z)_{\mathcal{N}}=(z)_{\mathcal{N}}=(x)_{\mathcal{N}}$. Then $y\in(x)_{\mathcal{N}}\subseteq M\Gamma z\gamma z\gamma z\Gamma M$ and $y=a\delta z\gamma z\gamma z\xi b=(a\delta z)\gamma z\gamma(z\xi b)$ for some $a,b\in M$, $\delta,\xi\in\Gamma$.

We prove that $a\delta z$, $z\xi b\in(x)_{\mathcal{N}}$. Then, since I is an ideal of $(x)_{\mathcal{N}}$, we have $(a\delta z)\gamma z\gamma(z\xi b)\in(x)_{\mathcal{N}}\Gamma I\Gamma(x)_{\mathcal{N}}\subseteq I$, and $y\in I$. We have

$$\begin{aligned}a\delta z\in(a\delta z)_{\mathcal{N}}:=(a)_{\mathcal{N}}\delta(z)_{\mathcal{N}}&=(a)_{\mathcal{N}}\delta(y)_{\mathcal{N}} \text{ (since } (z)_{\mathcal{N}}=(x)_{\mathcal{N}}=(y)_{\mathcal{N}})\\&=(a)_{\mathcal{N}}\delta(a\delta z\gamma z\gamma z\xi b)_{\mathcal{N}}\\&=(a)_{\mathcal{N}}\delta(a)_{\mathcal{N}}\delta(z\gamma z\gamma z\xi b)_{\mathcal{N}}\\&=(a)_{\mathcal{N}}\delta(z\gamma z\gamma z\xi b)_{\mathcal{N}} \text{ (since } (a\delta a,a)\in\mathcal{N})\\&=\Big(a\delta(z\gamma z\gamma z\xi b)\Big)_{\mathcal{N}}\\&=(y)_{\mathcal{N}}=(x)_{\mathcal{N}}\end{aligned}$$

and

$$\begin{aligned}z\xi b\in(z\xi b)_{\mathcal{N}}:=(z)_{\mathcal{N}}\xi(b)_{\mathcal{N}}&=(y)_{\mathcal{N}}\xi(b)_{\mathcal{N}}=(a\delta z\gamma z\gamma z\xi b)_{\mathcal{N}}\xi(b)_{\mathcal{N}}\\&=(a\delta z\gamma z\gamma z)_{\mathcal{N}}\xi(b)_{\mathcal{N}}\xi(b)_{\mathcal{N}}\\&=(a\delta z\gamma z\gamma z)_{\mathcal{N}}\xi(b\xi b)_{\mathcal{N}}\\&=(a\delta z\gamma z\gamma z)_{\mathcal{N}}\xi(b)_{\mathcal{N}}\\&=(a\delta z\gamma z\gamma z\xi b)_{\mathcal{N}}=(y)_{\mathcal{N}}=(x)_{\mathcal{N}}.\end{aligned}$$

(5) $\Longrightarrow$ (6). Since $\mathcal{N}$ is a semilattice congruence on M.

(6) $\Longrightarrow$ (7). Suppose σ be a semilattice congruence on M such that $(x)_\sigma$ is a simple subsemigroup of M for every $x \in M$. Let I be an ideal of M, $x \in M$ and $\gamma \in \Gamma$ such that $x\gamma x \in I$. The set $I \cap (x)_\sigma$ is an ideal of $(x)_\sigma$. In fact: Since $x\gamma x \in I$ and $x\gamma x \in (x)_\sigma$, the set $I \cap (x)_\sigma$ is a nonempty subset of $(x)_\sigma$ and, since $(x)_\sigma$ is a subsemigroup of M, we have

$$(x)_\sigma\Gamma(I \cap (x)_\sigma) \subseteq (x)_\sigma\Gamma I \cap (x)_\sigma\Gamma(x)_\sigma \subseteq M\Gamma I \cap (x)_\sigma \subseteq I \cap (x)_\sigma \text{ and}$$

$$(I \cap (x)_\sigma)\Gamma(x)_\sigma \subseteq I\Gamma(x)_\sigma \cap (x)_\sigma\Gamma(x)_\sigma \subseteq I\Gamma M \cap (x)_\sigma \subseteq I \cap (x)_\sigma.$$

Since $(x)_\sigma$ is a simple subsemigroup of M, we have $I \cap (x)_\sigma = (x)_\sigma$, and $x \in I$.

(7) $\Longrightarrow$ (1). Let $a \in M$ and $\gamma \in \Gamma$. Then $a \in M\Gamma a\gamma a\Gamma M$. Indeed: The set $M\Gamma a\gamma a\Gamma M$ is an ideal of M. This is because it is a nonempty subset of M and

$$M\Gamma(M\Gamma a\gamma a\Gamma M) = (M\Gamma M)\Gamma a\gamma a\Gamma M \subseteq M\Gamma a\gamma a\Gamma M,$$

$$(M\Gamma a\gamma a\Gamma M)\Gamma M = M\Gamma a\gamma a\Gamma(M\Gamma M) \subseteq M\Gamma a\gamma a\Gamma M.$$

By hypothesis, $M\Gamma a\gamma a\Gamma M$ is semiprime. Since $(a\gamma a)\gamma(a\gamma a) \in M\Gamma a\gamma a\Gamma M$, we have $a\gamma a \in M\Gamma a\gamma a\Gamma M$, and $a \in M\Gamma a\gamma a\Gamma M$. Thus M is intra-regular. □

3. On some left regular Γ-semigroups

Again using filters, we characterize here the left regular Γ-semigroups M in which $x\Gamma M \subseteq M\Gamma x$ for every $x \in M$ and we prove that this type of Γ-semigroups are decomposable into left simple components. If $x\Gamma M \subseteq M\Gamma x$ for every $x \in M$, then $A\Gamma M \subseteq M\Gamma A$ for every $A \subseteq M$. Indeed: If $a \in A$, $\gamma \in \Gamma$ and $b \in M$, then $a\gamma b \in a\Gamma M \subseteq M\Gamma a \subseteq M\Gamma A$. Thus if A is a left ideal of M, then A is a right ideal of M as well. As a consequence, the left regular Γ-semigroups in which $x\Gamma M \subseteq M\Gamma x$ for every $x \in M$, are left regular and left duo. We also remark that the left regular Γ-semigroups are intra-regular. Indeed: Let $a \in M$. Since M is left regular, we have $a \in M\Gamma a\gamma a \subseteq M\Gamma(M\Gamma a\gamma a)\gamma a \subseteq M\Gamma a\gamma a\Gamma M$. The right regular Γ-semigroups are also intra-regular, and the right regular Γ-semigroups for which $M\Gamma x \subseteq x\Gamma M$ for every $x \in M$ are right regular and right duo, and decomposable into right simple subsemigroups.

Definition 4. (cf. [2]) A Γ-semigroup M is called *left* (resp. *right*) *regular* if $x \in M\Gamma x\gamma x$ (resp. $x \in x\gamma x\Gamma M$) for every $x \in M$ and every $\gamma \in \Gamma$.

Lemma 5. (cf. [1]) *If M is a Γ-semigroup, then $\mathcal{L} \subseteq \mathcal{N}$ and $\mathcal{R} \subseteq \mathcal{N}$.*

Theorem 6. *Let M be a Γ-semigroup. The following are equivalent:*

(1) *M is left regular and $x\Gamma M \subseteq M\Gamma x$ for every $x \in M$.*

(2) *$N(x) = \{y \in M \mid x \in M\Gamma y\}$ for every $x \in M$.*

(3) *$\mathcal{N} = \mathcal{L}$.*

(4) *For every left ideal L of M, we have $L = \bigcup_{x \in L} (x)_{\mathcal{N}}$.*

(5) $(x)_{\mathcal{N}}$ *is a left simple subsemigroup of* M *for every* $x \in M$.
(6) M *is a semilattice of left simple semigroups.*
(7) *Every left ideal of* M *is semiprime and two-sided.*

Proof. (1) $\Longrightarrow$ (2). Let $x \in M$ and $T := \{y \in M \mid x \in M\Gamma y\}$. The set T is a filter of M containing x. In fact: Take an element $\gamma \in \Gamma$ ($\Gamma \neq \emptyset$). Since M is left regular, we have

$$x \in M\Gamma x\gamma x = (M\Gamma x)\gamma x \subseteq (M\Gamma M)\gamma x \subseteq M\Gamma x,$$

then $x \in T$, and T is a nonempty subset of M. Let $a, b \in T$ and $\gamma \in \Gamma$. Then $a\gamma b \in T$. Indeed: Since $b, a \in T$, we have $x \in M\Gamma b$ and $x \in M\Gamma a$. Since M is left regular, we have

$$\begin{aligned} x \in M\Gamma x\gamma x &\subseteq M\Gamma(M\Gamma b)\gamma(M\Gamma a) = (M\Gamma M)\Gamma(b\gamma M\Gamma a) \\ &\subseteq M\Gamma(b\gamma M\Gamma a). \end{aligned}$$

We prove that $b\gamma M\Gamma a \subseteq M\Gamma a\gamma b$. Then we have

$$x \in M\Gamma(M\Gamma a\gamma b) = (M\Gamma M)\Gamma(a\gamma b) \subseteq M\Gamma(a\gamma b),$$

and $a\gamma b \in T$. Let now $b\gamma u\mu a \in b\gamma M\Gamma a$ for some $u \in M$, $\mu \in \Gamma$. Since M is left regular, we have

$$\begin{aligned} b\gamma u\mu a &\in M\Gamma(b\gamma u\mu a)\gamma(b\gamma u\mu a) = (M\Gamma b\gamma u)\mu(a\gamma b)\gamma(u\mu a) \\ &\subseteq M\Gamma\Big((a\gamma b)\Gamma M\Big) \\ &\subseteq M\Gamma(M\Gamma a\gamma b) \text{ (since } x\Gamma M \subseteq M\Gamma x \ \forall x \in M) \\ &\subseteq M\Gamma a\gamma b. \end{aligned}$$

Let $a, b \in M$ and $\gamma \in \Gamma$ such that $a\gamma b \in T$. Then $a, b \in T$. Indeed: Since $a\gamma b \in T$, we have $x \in M\Gamma a\gamma b \subseteq (M\Gamma M)\Gamma b \subseteq M\Gamma b$, so $b \in T$. By hypothesis, $a\gamma b \in a\Gamma M \subseteq M\Gamma a$. Then $x \in M\Gamma a\gamma b \subseteq M\Gamma(M\Gamma a) \subseteq M\Gamma a$, so $a \in T$. Let now F be a filter of M such that $x \in F$. Then $T \subseteq F$. Indeed: Let $a \in T$. Then $x \in M\Gamma a$, that is $x = u\rho a$ for some $u \in M$, $\rho \in \Gamma$. Since $u \in M$, $\rho \in \Gamma$, $u\rho a \in F$ and F is a filter of M, we have $u \in F$ and $a \in F$, then $a \in F$.

(2) $\Longrightarrow$ (3). Let $(a, b) \in \mathcal{N}$. Then $a \in N(a) = N(b)$. Since $a \in N(b)$, by (2), we have $b \in M\Gamma a \subseteq a \cup M\Gamma a = L(a)$, so $L(b) \subseteq L(a)$. Since $b \in N(a)$, by symmetry, we get $L(a) \subseteq L(b)$. Then we have $L(a) = L(b)$, and $(a, b) \in \mathcal{L}$. By Lemma 5, $\mathcal{L} \subseteq \mathcal{N}$, so $\mathcal{L} = \mathcal{N}$.

(3) $\Longrightarrow$ (4). Let L be a left ideal of M. If $y \in L$, then $y \in (y)_{\mathcal{N}} \subseteq \bigcup\limits_{x \in L} (x)_{\mathcal{N}}$. Let $y \in \bigcup\limits_{x \in L} (x)_{\mathcal{N}}$. Then $y \in (x)_{\mathcal{N}}$ for some $x \in L$. Then, by (3), $(y, x) \in \mathcal{N} = \mathcal{L}$, so $L(y) = L(x)$. Since $x \in L$ and $L(x)$ is the left ideal of M generated by x, we have $L(x) \subseteq L$. Then $y \in L(y) = L(x) \subseteq L$, so $y \in L$.

(4) $\Longrightarrow$ (5). Let L be a left ideal of $(x)_{\mathcal{N}}$. Then $L=(x)_{\mathcal{N}}$. In fact: Let $y\in(x)_{\mathcal{N}}$. Take an element $z\in L$ and an element $\gamma\in\Gamma$ $(L,\Gamma\neq\emptyset)$. Since $M\Gamma z\gamma z$ is a left ideal of M, by hypothesis, we have $M\Gamma z\gamma z=\bigcup\limits_{t\in M\Gamma z\gamma z}(t)_{\mathcal{N}}$. Since $z\gamma z\gamma z\in M\Gamma z\gamma z$, we have $(z\gamma z\gamma z)_{\mathcal{N}}\subseteq M\Gamma z\gamma z$. Since $(z\gamma z,z)\in\mathcal{N}$ and $z\in L\subseteq(x)_{\mathcal{N}}$, we have $(z\gamma z\gamma z)_{\mathcal{N}}=(z)_{\mathcal{N}}=(x)_{\mathcal{N}}$. Then $y\in(x)_{\mathcal{N}}\subseteq M\Gamma z\gamma z$, thus $y=a\mu z\gamma z$ for some $a\in M$ and $\mu\in\Gamma$. We prove that $a\mu z\in(x)_{\mathcal{N}}$. Then, since L is a left ideal of $(x)_{\mathcal{N}}$, we have $(a\mu z)\gamma z\in(x)_{\mathcal{N}}\Gamma L\subseteq L$, and $y\in L$. We have

$$\begin{aligned}a\mu z\in(a\mu z)_{\mathcal{N}}&=(a)_{\mathcal{N}}\mu(z)_{\mathcal{N}}=(a)_{\mathcal{N}}\mu(y)_{\mathcal{N}}\text{ (since }(z)_{\mathcal{N}}=(x)_{\mathcal{N}}=(y)_{\mathcal{N}})\\&=(a)_{\mathcal{N}}\mu(a\mu z\gamma z)_{\mathcal{N}}=(a)_{\mathcal{N}}\mu(a)_{\mathcal{N}}\mu(z\gamma z)_{\mathcal{N}}\\&=(a)_{\mathcal{N}}\mu(z\gamma z)_{\mathcal{N}}=(a\mu z\gamma z)_{\mathcal{N}}\\&=(y)_{\mathcal{N}}=(x)_{\mathcal{N}}.\end{aligned}$$

(5) $\Longrightarrow$ (6). Since $\mathcal{N}$ is a semilattice congruence on M.

(6) $\Longrightarrow$ (7). Let σ be a semilattice congruence on M such that $(x)_\sigma$ is a left simple subsemigroup of M for every $x\in M$. Let L be a left ideal of M and $x\in M$, $\gamma\in\Gamma$ such that $x\gamma x\in L$. The set $L\cap(x)_\sigma$ is a left ideal of $(x)_\sigma$. Indeed: The set $L\cap(x)_\sigma$ is a nonempty subset of $(x)_\sigma$ (since $x\gamma x\in L$ and $x\gamma x\in(x)_\sigma$) and

$$(x)_\sigma\Gamma(L\cap(x)_\sigma)\subseteq(x)_\sigma\Gamma L\cap(x)_\sigma\Gamma(x)_\sigma\subseteq M\Gamma L\cap(x)_\sigma\subseteq L\cap(x)_\sigma.$$

Since $(x)_\sigma$ is a left simple subsemigroup of M, we have $L\cap(x)_\sigma=(x)_\sigma$, then $x\in L$. Thus L is semiprime. Let now L be a left ideal of M. Then $L\Gamma M\subseteq L$. Indeed: Let $y\in L$, $\gamma\in\Gamma$ and $x\in M$. Since L is a left ideal of M, we have $x\gamma y\in M\Gamma L\subseteq L$. The set $L\cap(x\gamma y)_\sigma$ is a left ideal of $(x\gamma y)_\sigma$. Indeed:

$\emptyset\neq L\cap(x\gamma y)_\sigma\subseteq(x\gamma y)_\sigma$ (since $x\gamma y\in L$ and $x\gamma y\in(x\gamma y)_\sigma$) and

$$(x\gamma y)_\sigma\Gamma(L\cap(x\gamma y)_\sigma)\subseteq(x\gamma y)_\sigma\Gamma L\cap(x\gamma y)_\sigma\Gamma(x\gamma y)_\sigma\subseteq M\Gamma L\cap(x\gamma y)_\sigma.$$

Since $(x\gamma y)_\sigma$ is left simple, we have $L\cap(x\gamma y)_\sigma=(x\gamma y)_\sigma=(y\gamma x)_\sigma$, so $y\gamma x\in L$.

(7) $\Longrightarrow$ (1). Let $x\in M$ and $\gamma\in\Gamma$. Since $M\Gamma x\gamma x$ is a left ideal of M, by hypothesis it is semiprime. Since $(x\gamma x)\gamma(x\gamma x)\in M\Gamma x\gamma x$, we have $x\gamma x\in M\Gamma x\gamma x$, and $x\in M\Gamma x\gamma x$, thus M is left regular. Let now $x\in M$. Then $x\Gamma M\subseteq M\Gamma x$. Indeed: Since M is left regular, we have $x\in M\Gamma x\gamma x\subseteq(M\Gamma M)\Gamma x\subseteq M\Gamma x$, so $M\Gamma x$ is a nonempty subset of M. In addition, $M\Gamma(M\Gamma x)=(M\Gamma M)\Gamma x\subseteq M\Gamma x$, so $M\Gamma x$ is a left ideal of M. By hypothesis, $M\Gamma x$ is a right ideal of M as well. Since $M\Gamma x$ is an ideal of M containing x, we have $I(x)\subseteq M\Gamma x$. On the other hand, $x\Gamma M\subseteq x\cup M\Gamma x\cup x\Gamma M\cup M\Gamma x\Gamma M=I(x)$. Thus we obtain $x\Gamma M\subseteq M\Gamma x$. □

The right analogue of Theorem 6 also holds, and we have the following:

Theorem 7. *Let M be a Γ-semigroup. The following are equivalent:*

(1) *M is right regular and $M\Gamma x\subseteq x\Gamma M$ for every $x\in M$.*

(2) *$N(x)=\{y\in M\mid x\in y\Gamma M\}$ for every $x\in M$.*

(3) $\mathcal{N} = \mathcal{R}$.

(4) *For every right ideal R of M, we have* $R = \bigcup\limits_{x \in R} (x)_{\mathcal{N}}$.

(5) $(x)_{\mathcal{N}}$ *is a right simple subsemigroup of M for every $x \in M$.*

(6) *M is a semilattice of right simple semigroups.*

(7) *Every right ideal of M is semiprime and two-sided.*

References

[1] **N. Kehayopulu,** *Green's relations and the relation $\mathcal{N}$ in Γ-semigroups*, Quasigroups and Related Systems **22** (2014), $89 - 96$.

[2] **N. Kehayopulu,** *On left regular Γ-semigroups*, Int. J. Algebra **8** (2014), $389 - 394$.

[3] **M. Petrich,** *Introduction to Semigroups*, Merrill Research and Lecture Series. Charles E. Merrill Publishing Co., Columbus, Ohio, 1973.

Received October 1, 2014

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

M. Tsingelis
School of Science and Technology
Studies in Natural Sciences
Hellenic Open University, Greece
E-mail: mtsingelis@hol.gr

A new block ciphers based on wavelet decomposition of splines

Alla B. Levina

Abstract. This paper presents the idea of using wavelet decomposition of splines in cryptography. The cryptoalgorithms based on wavelet decomposition of splines uses just the algebraic calculation. With the help of algebraic formulas we can code and decode information that algorithms do not have the XOR using the round key, also it does not use S-boxes.

1. Introduction

The proposed paper discusses a new class of algorithms obtained using a new theory of the spline-wavelet decompositions on nonuniform sets. The theory of wavelet decomposition of splines has been used before to process discreet signals but never in cryptography.

Our proposal is to create cryptoalgoritms which will use only mathematical calculation that can process data blocks up to 2048 bits and more quickly. This research were carried out for splines of the first, second and third degree. Algorithms based on splines of an upper degree works slower but they remain stronger against different cryptoattacks.

The theory of wavelet-decomposition of splines can apply to different areas of cryptography. In this work we will illustrate just one way of use - creation of block ciphers, which will be presented on splines of the third degree.

The presented algorithms do not have the XOR operation with the round key and they do not use S-boxes as block ciphers GOST 28147-89 [10], 3DES [9], AES [3,8] and others. At the present time, only algorithm Threefish [11] is not using S-boxes and can process data blocks up to 1024 bits. Diffusion over multiple rounds we get by mathematical functions.

As a minus of the algorithms we can mention that not all the bytes are receiving enciphering on each round; some of them are just getting moved to several positions, unlike in the Feistel Structure. Present research explores algorithms which will cipher each byte on each round.

As a plus for the presented algorithms, we can mention that it is based only on the mathematical calculation, however it does help in the analyzing of algorithms.

2010 Mathematics Subject Classification: 11T71, 94A60, 68P25
Keywords: Block ciphers, splines, grids, formulas of decomposition and reconstruction.

The structure of the presented algorithms is absolutely new - and has the possibility for modernization of the process. The process of enciphering is based only on mathematical formulas, the formulas of decomposition from wavelet theory, process of deciphering is based on the formulas of reconstruction.

In this paper the basic concepts of algorithm, mathematical basics of process of enciphering/deciphering, illustration of spline-wavelet decomposition, and a demonstration of the work of algorithm is presented.

2. Idea of wavelet decomposition of splines

In this section we will briefly provide a concept of wavelet decomposition of splines [4, 5, 6]. We will illustrate spline-wavelet decomposition on the splines of the third degree. For splines of the first and second degree, the same theory is used.

On the set X we build splines. Set X consists of the elements $\{x_i\}_{i=0,\dots,L-1}$, where $\{x_i\}_{i=0,\dots,L-1}$ natural numbers. L is the number of elements in the set X.

Splines of the third degree built on the set X are presented in the formulas below:

$$\sum_{j=k-3}^{k} \omega_j(t) = 1, \quad t \in [x_k, x_{k+1})$$

$$\sum_{j=k-3}^{k} \frac{1}{3}\left(x_{j+1} + x_{j+2} + x_{j+3}\right) \omega_j(t) = t, \quad t \in [x_{k+1}, x_{k+2})$$

$$\sum_{j=k-3}^{k} \frac{1}{3}\left(x_{j+1}x_{j+2} + x_{j+1}x_{j+3} + x_{j+2}x_{j+3}\right) \omega_j(t) = t^2, \quad t \in [x_{k+2}, x_{k+3})$$

$$\sum_{j=k-3}^{k} x_{j+1}x_{j+2}x_{j+3}\, \omega_j(t) = t^3, \quad t \in [x_{k+3}, x_{k+4}).$$

With splines defined as $\omega_j(t)$ and x_j elements of our set X.

For wavelet decomposition of splines, we take out one element x_k from our set X and we will obtain a new set $\overline{X}$. Elements of this set can be presented with the help of elements from the old set, as presented below:

$$\overline{x}_j = x_j \ \text{ if } \ j \leqslant k-1, \ \text{ and } \ \overline{x}_j = x_{j+1} \ \text{ if } \ j \geqslant k, \quad \xi = x_k.$$

On the new set $\overline{X}$, we can build new splines $\overline{\omega}_j$ *but these new splines can be present as a combination of splines which were built before on the set X. Also splines $\omega_j(t)$ can be obtained with the help of the new splines $\overline{\omega}_j(t)$ — it helps us to restore the information.*

This idea gives us two types of formulas: 1) formulas of decomposition 2) formulas of reconstruction. Step by step we take out elements from our primary set X and build splines which use the new set (in this realization each time we take out just one element we get a new set and new splines, in another realization it can be taken a few elements each time).

The mathematical process of getting these formulas will not be introduced in this paper, instead we will present only a final version to show, how these formulas will look.

We have an information stream c_i and we want to get new stream $\overline{c_i}$ based on the set $\overline{X}$. Formulas of decomposition will reform information stream c_i in to the information stream $\overline{c_i}$ and wavelet part — element b. Formulas of reconstruction will restore stream c_i, using stream $\overline{c_i}$ and element b.

Formulas of decomposition:

$$\overline{c}_i = c_i \quad \text{if} \quad 0 \leqslant i \leqslant k-5, \quad \overline{c}_i = c_{i+1} \quad \text{if} \quad k-1 \leqslant i \leqslant M-2,$$

$$\overline{c}_{k-3} = \frac{\xi - \overline{x}_k}{\xi - \overline{x}_{k-3}} \cdot c_{k-4} + \frac{\overline{x}_k - \overline{x}_{k-3}}{\xi - \overline{x}_{k-3}} \cdot c_{k-3},$$

$$\overline{c}_{k-2} = (\xi - \overline{x}_k)(\xi - \overline{x}_{k+1}) \cdot c_{k-4} + (\xi - \overline{x}_{k+1})(\overline{x}_k - \overline{x}_{k-3}) \cdot c_{k-3} +$$

$$+ (\overline{x}_{k+1} - \overline{x}_{k-2})(\xi - \overline{x}_{k-3}) \cdot c_{k-2}) \cdot [\xi - \overline{x}_{k-2}]^{-1} [\xi - \overline{x}_{k-3}]^{-1},$$

$$b = c_{k-1} - \frac{\overline{x}_{k+2} - \xi}{\overline{x}_{k+2} - \overline{x}_{k-1}} \cdot \overline{c}_{k-2} - \frac{\xi - \overline{x}_{k-1}}{\overline{x}_{k+2} - \overline{x}_{k-1}} \cdot \overline{c}_{k-1}.$$

Formulas of reconstruction:

$$c_i = \overline{c}_i \quad \text{if} \quad 0 \leqslant i \leqslant k-4, \quad c_i = \overline{c}_i \quad \text{if} \quad k \leqslant i \leqslant M-1,$$

$$c_{k-3} = \frac{\overline{x}_k - \xi}{\overline{x}_k - \overline{x}_{k-3}} \cdot \overline{c}_{k-4} + \frac{\xi - \overline{x}_{k-3}}{\overline{x}_k - \overline{x}_{k-3}} \cdot \overline{c}_{k-3},$$

$$c_{k-2} = \frac{\overline{x}_{k+1} - \xi}{\overline{x}_{k+1} - \overline{x}_{k-2}} \cdot \overline{c}_{k-3} + \frac{\xi - \overline{x}_{k-2}}{\overline{x}_{k+1} - \overline{x}_{k-2}} \cdot \overline{c}_{k-2},$$

$$c_{k-2} = \frac{\overline{x}_{k+2} - \xi}{\overline{x}_{k+2} - \overline{x}_{k-1}} \cdot \overline{c}_{k-2} + \frac{\xi - \overline{x}_{k-1}}{\overline{x}_{k+2} - \overline{x}_{k-1}} \cdot \overline{c}_{k-1} + b.$$

We will now present how we can use this idea in construction of block ciphers, for it we will illustrate these formulas in a more readable way.

3. Specification

The presented algorithm is an iterated block cipher with a variable block length and it is relative to the class of block cipher algorithms.

3.1. Basic concepts of the algorithm

A process of enciphering and deciphering consists of K identical rounds.

This algorithm can work with the block length up to 2048 bits and more. The number of rounds is denoted by K, $\mathbf{K}_{X\gamma}$ is a key length, M is a block length (In the table below M and $\mathbf{K}_{X\gamma}$ are bytes).

Let $\mathbb{K} = (X, \gamma)$ be *a key*; here X is an ordered set, $X = \{x_j\}_{j=0,\dots,L-1}$, where L is a number of elements in the set X and γ is the order of ejection of elements from the set. The key consist from two sets.

We have determined the number of rounds by looking at the maximum number of rounds for which attacks have been found and has added a considerable level of security and provides a higher margin of safety, in some cases there can be less rounds held and the key will be smaller. Key length is equal to (number of rounds + 3)+(number of rounds) bytes.

Number of rounds and key length as a function of the block length is given in Table 1.

	K	$\mathbf{K}_{X\gamma}$
$M = 8$ bytes	6	15
$M = 16$ bytes	14	31
$M = 24$ bytes	22	47
$M = 32$ bytes	30	63
$M = 64$ bytes	62	127
$M = 128$ bytes	126	255
$M = 256$ bytes	254	511

Table 1.

Number of elements in the set X as a function of the block length are presented in the Table 2.

	L
$M = 8$ bytes	9
$M = 16$ bytes	17
$M = 24$ bytes	25
$M = 32$ bytes	33
$M = 64$ bytes	65
$M = 128$ bytes	129
$M = 256$ bytes	257

Table 2.

The process of creating round key will be explained in section 3.2 more detailed.

A *sequence* $C = \{c_i\}_{i=0,\dots,M-1}$ is a *plaintext;* $|C| = M$ is a quantity of elements which are ciphered, C is the ordered set.

Elements $\{c_i\}_{i=0,\dots,M-1}$ and $\{x_j\}_{j=0,\dots,L-1}$ are bytes (we are working with one-byte words, but we can also work with 4-bytes words).

Let us suppose that the set X and C can be periodic with the period T so $x_j = x_{j+T}$ and $c_i = c_{i+T}, \quad \forall j \in \mathbf{Z}$.

The process ofenciphering bases on the formulas of decomposition from wavelet theory, after K rounds we obtain the ciphertext. For deciphering we will use formulas of reconstruction.

The process of enciphering and deciphering consists of two steps: 1) creation of round key and 2) round transformation.

3.2. The round key creation

Round key transformation consist of two steps. We will now check the first round – all rounds are the same.

1. We eject element x_{γ_1} from the primary set X. The received set is defined as X_{-1} and $X_{-1} = \{x_{-1,j}\}^1$, elements of new set are equal:

$$x_{-1,j} = x_j \quad \text{if} \quad j < \gamma_1, \tag{1}$$

$$x_{-1,j} = x_{j+1} \quad \text{if} \quad j > \gamma_1. \tag{2}$$

The element x_{γ_1} which has been taken out of the set X is defined as ξ, $\xi = x_{\gamma_1}$.

In the next round we will be working with the set X_{-1} and x_{γ_2}.

Example:

We will now calculate the set X_{-1} from the set X. For example: X consists of 6 bytes $(\{1, 3, 5, 9, 10, 6\}$ and the number of the element which will eject is $\gamma_i = 4$. All numerations starts from 0, it means that our ejected element $\xi = x_{\gamma_i} = 10$ and the new set $X_{-1} = (\{1, 3, 5, 9, 6\}$.

2. We enter the following designations - elements which we use in the process of enciphering we mark $...^{en}$, for deciphering $...^{de}$:

$$A^{en}_{-1} = \xi - x_{-1,\gamma_1}, \quad B^{en}_{-1} = \xi - x_{-1,\gamma_1-1}, \quad C^{en}_{-1} = \xi - x_{-1,\gamma_1-2},$$

$$D^{en}_{-1} = \xi - x_{-1,\gamma_1-3}, \quad E^{en}_{-1} = \xi - x_{-1,\gamma_1+1}, \quad F^{en}_{-1} = x_{-1,\gamma_1+2} - x_{-1,\gamma_1-1}.$$

$$A^{de}_{-1} = x_{-1,\gamma_1} - x_{-1,\gamma_1-3}, \quad B^{de}_{-1} = x_{-1,\gamma_1} - \xi \quad C^{de}_{-1} = x_{-1,\gamma_1+1} - x_{-1,\gamma_1-2},$$

$$D^{de}_{-1} = x_{-1,\gamma_1+1} - \xi, \quad E^{de}_{-1} = x_{-1,\gamma_1+2} - x_{-1,\gamma_1-1}, \quad F^{de}_{-1} = x_{-1,\gamma_1+2} - \xi.$$

These designations will help us in the future realization of the formulas. As we can see from calculating these elements we are using our new set; X_{-1} and element ξ from our set X.

[1] To avoid misunderstanding with numeration in this work if it's written $\{...\}_{-i,j}$ $-i$ is a number of the round and j is a number of the element, if it's just $\{...\}_{-i}$ $-i$ is a number of round.

With the help of these designations we can calculate elements of the round key:

$$I^{en} = \frac{A^{en}_{-1}}{D^{en}_{-1}}(\mathrm{mod}N), \quad II^{en} = \frac{E^{en}_{-1}}{C^{en}_{-1}}(\mathrm{mod}N), \quad III^{en} = \frac{B^{en}_{-1}}{F^{en}_{-1}}(\mathrm{mod}N).$$

$$I^{de} = \frac{B^{de}_{-1}}{A^{de}_{-1}}(\mathrm{mod}N), \quad II^{de} = \frac{D^{de}_{-1}}{C^{de}_{-1}}(\mathrm{mod}N), \quad III^{de} = \frac{F^{de}_{-1}}{E^{de}_{-1}}(\mathrm{mod}N).$$

We use mod N, where N is a prime number and it gives us possibility to get elements that will take one byte. All future calculations will be made by mod, we will use the same mod as in algorithm Rijndael $x^8+x^4+x^3+x+1$.

Example:

Now we will illustrate how we calculate elements I^{en}, II^{en}, III^{en}, I^{de}, II^{de}, III^{de}. For it we will use set $X_{-1} = (\{1,3,5,9,6\}$, $\xi = 10$, $\gamma_1 = 4$.

$$A^{en}_{-1} = \xi - x_{-1,\gamma_1} = 10 - 6 = 4, \quad B^{en}_{-1} = \xi - x_{-1,\gamma_1-1} = 10 - 9 = 1,$$

$$C^{en}_{-1} = \xi - x_{-1,\gamma_1-2} = 10 - 5 = 5, \quad D^{en}_{-1} = \xi - x_{-1,\gamma_1-3} = 10 - 3 = 7,$$

$$E^{en}_{-1} = \xi - x_{-1,\gamma_1+1} = 10 - 1 = 9, \quad F^{en}_{-1} = x_{-1,\gamma_1+2} - x_{-1,\gamma_1-1} = 3 - 9 = -6.$$

$$A^{de}_{-1} = x_{-1,\gamma_1} - x_{-1,\gamma_1-3} = 6 - 3 = 3, \quad B^{de}_{-1} = x_{-1,\gamma_1} - \xi = 6 - 10 = -4,$$

$$C^{de}_{-1} = x_{-1,\gamma_1+1} - x_{-1,\gamma_1-2} = 1 - 5 = -4, \quad D^{de}_{-1} = x_{-1,\gamma_1+1} - \xi = 1 - 10 = -9,$$

$$E^{de}_{-1} = x_{-1,\gamma_1+2} - x_{-1,\gamma_1-1} = 3 - 9 = -6, \quad F^{de}_{-1} = x_{-1,\gamma_1+2} - \xi = 3 - 10 = -7.$$

Instead of mod N, we will use mod 11, we need a prime number, for this example it will be easer to use 11.

$$I^{en} = \frac{A^{en}_{-1}}{D^{en}_{-1}}(\mathrm{mod}11) = \frac{4}{7}(\mathrm{mod}11) = 4 \cdot 8(\mathrm{mod}11) = 10,$$

$$II^{en} = \frac{E^{en}_{-1}}{C^{en}_{-1}}(\mathrm{mod}11) = \frac{9}{5}(\mathrm{mod}11) = 9 \cdot 9(\mathrm{mod}11) = 4,$$

$$III^{en} = \frac{B^{en}_{-1}}{F^{en}_{-1}}(\mathrm{mod}11) = \frac{1}{-6}(\mathrm{mod}11) = -2(\mathrm{mod}11) = 9.$$

$$I^{de} = \frac{B^{de}_{-1}}{A^{de}_{-1}}(\mathrm{mod}11) = \frac{-4}{3}(\mathrm{mod}11) = 6,$$

$$II^{de} = \frac{D^{de}_{-1}}{C^{de}_{-1}}(\mathrm{mod}11) = \frac{-9}{-4}(\mathrm{mod}11) = 5,$$

$$III^{de} = \frac{F^{de}_{-1}}{E^{de}_{-1}}(\mathrm{mod}11) = \frac{-7}{-6}(\mathrm{mod}11) = 3.$$

All the calculations by mod goes by the rules of calculation in finite fields.

On each round, key transformation goes as it was presented.

3.3. Process of enciphering

The process of enciphering also consists of two steps. For the encoding of information we will use formulas of decomposition for the splines of the third degree.

On the first round our plaintext is $\{c_i\}_{i=0,\ldots,M-1}$.

First round:

1. With the help of round key, we will present formulas of decomposition for splines of the third degree, and we will code our plain text.

$$c_{-1,j} = c_j \quad \text{if} \quad 0 \leqslant j \leqslant \gamma_1 - 5, \tag{3}$$

$$c_{-1,j} = c_{j+1} \quad \text{if} \quad \gamma_1 - 1 \leqslant j \leqslant M - 2, \tag{4}$$

$$c_{-1,\gamma_1-3} = \big(I^{en} \cdot (c_{\gamma_1-4} - c_{\gamma_1-3}) + c_{\gamma_1-3}\big)(\text{mod}N), \tag{5}$$

$$c_{-1,\gamma_1-2} = \big(I^{en} \cdot II^{en}(c_{\gamma_1-4} - c_{\gamma_1-3}) + II^{en} \cdot (c_{\gamma_1-3} - c_{\gamma_1-2}) + c_{\gamma_1-2}\big)(\text{mod}N), \tag{6}$$

$$b_{-1} = \big(c_{\gamma_1-1} - c_{-1,\gamma_1-2} + III^{en} \cdot (c_{-1,\gamma_1-2} - c_{-1,\gamma_1-1})\big)(\text{mod}N). \tag{7}$$

As we can see from the formulas (3) – (7) on the first round formulas of decomposition, we are taking out element c_{γ_1-1} from our plain text, elements c_{-1,γ_1-2} and c_{-1,γ_1-3} is getting transformed, with the help of formulas (5) – (6) while other elements of our plain text starts from the element $\gamma_1 - 1$ that we are moving. Element b_{-1} is the element of a wavelet stream, which will help us to restore the initial information.

From

c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7

we obtain

c_0	c_1	$I^{en}\cdot(c_1-c_2)+c_2$	$I^{en}\cdot II^{en}(c_1-c_2)+II^{en}\cdot(c_2-c_3)+c_3$	c_5	c_6	c_7	b_{-1}

Figure 1. Illustration of the process of enciphering for 8 bytes on the first round if $\gamma_1 = 5$.

We use mod N as it will insure that we will still stay in the byte in spite of multiplying.

2. At the end we make a shift of sequence $c_{-1,j}$ as follows:

$$c_{-1,0} \rightarrow c_{-1,1} \rightarrow c_{-1,2} \ldots \rightarrow c_{-1,M-1} \rightarrow c_{-1,0}.$$

It gives us more transformations.

From

c_0	c_1	$I^{en}\cdot(c_1-c_2)+c_2$	$I^{en}\cdot II^{en}(c_1-c_2)+II^{en}\cdot(c_2-c_3)+c_3$	c_5	c_6	c_7	b_{-1}

we obtain

c_7	c_0	c_1	$I^{en}\cdot(c_1-c_2)+c_2$	$I^{en}\cdot II^{en}(c_1-c_2)+II^{en}\cdot(c_2-c_3)+c_3$	c_5	c_6	b_{-1}

Figure 2. Illustration of the shift.

On the next round we will be working with the set $\{c_{-1,j}\}_{j=0,\ldots,M-2}$.

All rounds except the final round go the same, on the last round we do not do the shift.

As a result, after K rounds we get two sequences

$$\{b_{-n}\}_{n=1,2,\ldots,K}, \quad \{c_{-K,j}\}_{j=0,1,2,\ldots,M-K-1}.$$

Sequence $\{c_{-K,j}, b_{-n}\}_{n=1,2,\ldots,K;j=0,1,2,\ldots,M-K-1}$ *is the ciphertext.*

Example:

We continue our previous example $I^{en}=10$, $II^{en}=4$, $III^{en}=9$.

We will use mod 11 for our calculations again.

The plain text will consist also of 6 bytes $C=\{4,6,7,9,1,8\}$, $\gamma_1=4$. With the help of formulas (3) – (4) we get:

$c_{-1,0}=c_0=4$, $c_{-1,3}=c_4=1$, $c_{-1,4}=c_5=8$.

Elements $c_{-1,1}$ and $c_{-1,2}$ we calculate by formulas (5) – (6):

$c_{-1,1}=\big(10\cdot(4-6)+6)\big)(\mathrm{mod}11)=8$,

$c_{-1,2}=\big(4\cdot10(4-6)+4\cdot(6-7)+7\big)(\mathrm{mod}11)=0$.

Element $b_{-1}=\big(9-0+9\cdot(0-1)\big)(\mathrm{mod}11)=0$.

We obtain $c_{-1}=\{4,8,0,1,8\}$, $\quad b_{-1}=0$.

After the shift, our text for the next round will be $\{8,4,8,0,1,8,0\}$.

3.4. Process of deciphering

The process of decryption goes by analogy with the process of encryption.

For the restoring of information we will use formulas of reconstruction from wavelet theory. For deciphering we need the reverse order of round keys.

1. We write formulas of reconstruction for the splines of third degree:

$$c_{-K+1,j}=c_{-K,j} \quad \text{if} \quad 0\leqslant j\leqslant\gamma_K-4, \tag{8}$$

$$c_{-K+1,j}=c_{-K,j-1} \quad \text{if} \quad \gamma_K\leqslant j\leqslant M-K, \tag{9}$$

$$c_{-K+1,\gamma_K-3}=\big(I^{de}\cdot(c_{-k,\gamma_k-4}-c_{-k,\gamma_k-3})+c_{-k,\gamma_k-3}\big)(\mathrm{mod}N), \tag{10}$$

$$c_{-k+1,\gamma_k-2}=\big(II^{de}\cdot(c_{-k,\gamma_k-3}-c_{-k,\gamma_k-2})+c_{-k,\gamma_k-2}\big)(\mathrm{mod}N), \tag{11}$$

$$c_{-k+1,\gamma_k-1}=\big(III^{de}\cdot(c_{-k,\gamma_k-2}-c_{-k,\gamma_k-1})+c_{-k,\gamma_k-1}+b_{-k}\big)(\mathrm{mod}N). \tag{12}$$

2. At the end we make a shift of sequence $c_{-1,i}$ as follows:

$$c_{-1,0}\leftarrow c_{-1,1}\leftarrow c_{-1,2}\ldots\leftarrow c_{-1,M-K+1}\leftarrow c_{-1,0}$$

On the next round we will be working with the set X_{-K+1}. We will also use $\{c_{-K+1,i}\}_{i=0,....,M-K+1}$ and b_{-K+1}, on the second round of the process of deciphering we get the sequence $\{c_{-K+2,i}\}_{i=0,....,M-K+2}$ etc.

Example:
To illustrate the process of enciphering we will restore information $\{4,6,7,9,1,8\}$, if we know ciphertext $\{4,8,0,1,8\}$, $b_{-1}=0$ and we know round key I^{de}, II^{de},III^{de}.

With the help of formulas (8) – (12) we get:

$c_0 = c_{-1,0} = 4,$

$c_4 = c_{-1,3} = 1,\ c_5 = c_{-1,4} = 8,$

$c_1 = \Big(6\cdot(4-8)+8\Big)(\mathrm{mod}11) = 6,$

$c_2 = \Big(5\cdot(8-0)+0\Big)(\mathrm{mod}11) = 7,$

$c_3 = \Big(3\cdot(0-1)+1+0\Big)(\mathrm{mod}11) = 9.$

We obtain the plain text $c = \{4,6,7,9,1,8\}$.

This small example just illustrated how formulas of reconstruction and decomposition works.

4. Implementation

This algorithm has been implemented on the 32-bit processors. These results were obtained with Java, which does not provide the best of possible results.

The speed figures given in the Table 3 have been scaled on the Pentium 2,33 GHz. It was calculated only for blocks equal to 32, 64, 128 bytes, and it is far from the best results which can obtained.

Block length, key length	Encryption time for the block	Cycles per bytes for encryption
32 bytes, 63 bytes	0,00004 sec	2920
64 bytes, 127 bytes	0,00008 sec	2864
128 bytes, 255 bytes	0,000189 sec	3398

Table 3. Performance for the process of enciphering (Java).

Block length, key length	Decryption time for the block	Cycles per bytes for encryption
32 bytes, 63 bytes	0,000051 sec	3653
64 bytes, 127 bytes	0,0001 sec	3589
128 bytes, 255 bytes	0,000238 sec	4273

Table 4. Performance for the process of deciphering (Java).

Results which are presented in this work are very far from the results which can be obtained, C++ will give us a much better result and the program can be optimized.

5. Strength against known attacks

The presented algorithm has an absolutely new structure and it is difficult to analyze the strength of this algorithm and other algorithms based on wavelet decomposition of splines.

5.1. Differential cryptanaysis

Differential cryptanalysis [1] attacks are possible if there are predictable difference in propagations over all but a few rounds larger than 2^{1-M}, if M is the block length. Usually they are based on the analysis of results of S-boxes, which we do not have in these algorithms.

If we will check formulas of ciphering (5) – (7) we can see that the XOR operation will not give us any information. Lets examine these formulas. Elements of one plain text is c_i and the other is $c_i^{'}$.

$$\begin{gathered}
I^{en} \cdot (c_{\gamma_1-4} - c_{\gamma_1-3}) + c_{\gamma_1-3} \otimes I^{en} \cdot (c^{'}_{\gamma_1-4} - c^{'}_{\gamma_1-3}) + c^{'}_{\gamma_1-3} \\
I^{en} \cdot II^{en}(c_{\gamma_1-4} - c_{\gamma_1-3}) + II^{en} \cdot (c_{\gamma_1-3} - c_{\gamma_1-2}) + c_{\gamma_1-2} \otimes \\
I^{en} \cdot II^{en}(c^{'}_{\gamma_1-4} - c^{'}_{\gamma_1-3}) + II^{en} \cdot (c^{'}_{\gamma_1-3} - c^{'}_{\gamma_1-2}) + c^{'}_{\gamma_1-2} \\
c_{\gamma_1-1} - c_{-1,\gamma_1-2} + III^{en} \cdot (c_{-1,\gamma_1-2} - c_{-1,\gamma_1-1}) \otimes \\
c^{'}_{\gamma_1-1} - c^{'}_{-1,\gamma_1-2} + III^{en} \cdot (c^{'}_{-1,\gamma_1-2} - c^{'}_{-1,\gamma_1-1})
\end{gathered}$$

As we can see, the data from the parts is all that we can gather; where we have I^{en}, II^{en}, III^{en}:

$$\begin{gathered}
I^{en} \cdot (c_{\gamma_1-4} - c_{\gamma_1-3}), \quad I^{en} \cdot II^{en}(c_{\gamma_1-4} - c_{\gamma_1-3}) + II^{en} \cdot (c_{\gamma_1-3} - c_{\gamma_1-2}), \\
III^{en} \cdot (c_{-1,\gamma_1-2} - c_{-1,\gamma_1-1}).
\end{gathered}$$

These formulas do not give to us any predictable difference in propagations, because in each round I^{en}, II^{en}, III^{en} are different and they depend only on the round key. It depends on γ_i in i - th round, as they are different on each round.

5.2. The Square attack

The Square attack [2] based on the analysis of chosen plaintexts of which part is held constant and another part varies through all possibilities.

Here we can see the same situation as with the differential cryptanalysis. The process of enciphering is based on the multiplication of elements of plain text on the elements I^{en}, II^{en}, III^{en}. Changes of plaintexts would not give us any information about round key and the key.

5.3. Linear cryptanalysis

For the linear cryptanalysis [7] we need to obtained a linear approximation of the form:

$$P_{i1} \otimes P_{i2} \otimes ... \otimes P_{ia} \otimes c_{j1} \otimes c_{j2} \otimes ... \otimes c_{jb} = K_{k1} \otimes K_{k2} \otimes ... \otimes K_{kn}$$

where P_n, c_n, K_n bytes of plaintext, ciphertext and key.

This attack is also based on the analysis of S-boxes, which we are not considering. Yet it has not been discovered to be the way to obtain linear approximation.

5.4. Possible attack

There is an attack which is possible to apply to the algorithm in the way it appears to look at this juncture.

As we see from formulas $(5) - (7)$, two of equations are linear and one is square. We will use a plain text attack and we need a possibility to get cipher bytes after each round. If we will get such possibilities for restoring a key we will need to use $2^{8 \cdot 2 \cdot K}$, where K is a number of round. If we will find I^{en} we will find II^{en}, but III^{en} we can not find this way.

Results of this attack is presented in the Table 5.

	results of attack
M = 8 bytes	2^{96}
M = 16 bytes	2^{224}
M = 24 bytes	2^{352}
M = 32 bytes	2^{480}
M = 64 bytes	2^{992}
M = 128 bytes	2^{2016}
M = 256 bytes	2^{4064}

Table 5.

We can avoid this attack if we will encipher each byte on the round; it will require more time but it will be secure.

6. Conclusion

We have presented block cipher based on wavelet decomposition of splines of the third degree. Research for using spline-wavelet decomposition can be applied in different areas of cryptography and the presented algorithm can be improved on and can show better results in security and speed.

This is new way of creating block ciphers which are only based on the mathematics, which can help in the analysis and proofing of strength.

References

[1] **E. Biham and A. Shamir**, *Differential cryptanalysis of DES-like cryptosystems,* J. Cryptology **4** (1991), 3 – 72.

[2] **J. Daemen, L.R. Knudsen and V. Rijmen**, *The block cipher Square*, Fast Software Encryption, LNCS **1267** (1997), 149 – 165.

[3] **J. Daemen, V. Rijmen**, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer, (2002).

[4] **Y.K. Demjanovish**, *Minmal splines and splaches*, Vestnic of St. Petersburg Univ. **1** (2008), 8 – 22 (in Russian).

[5] **Y.K. Demjanovish**, *Splaches and minimal splines*, St. Petersburg, (2003), 200–207 (in Russian).

[6] **Y.K. Demjanovich**, *On wavelet decompositions of linear space for arbitrary field and some applications*, J. Math. Modelling B **20** (2008), 104 – 108 (in Russian).

[7] **M. Matsui**, *Linear cryptanalysis method for DES cipher*, Advances in Cryptology, Proc. Eurocrypt93. LNCS **765**, (1994), 386 – 397.

[8] **AES page** http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[9] **DES and 3 DES page** at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[10] **GOST 2814789 page** http://gostshifr.narod.ru/

[11] **Threefish page** http://www.skein-hash.info/

Received February 1, 2014
Revised 17 December 2014

ITMO University
49 Kronverksky Ave.
St.Petersburg, 197101
Russia
E-mail: levina@cit.ifmo.ru

The categories of actions of a dcpo-monoid on directed complete posets

Mojgan Mahmoudi and *Halimeh Moghbeli-Damaneh*

Abstract. In this paper, some categorical properties of the category **Cpo**-S of all S-cpo's; cpo's equipped with a compatible right action of a cpo-monoid S, with strict continuous action-preserving maps between them is considered. We also define and consider similarly, the category **Dcpo**-S of all S-dcpo's, and continuous action-preserving maps between them. In particular, we characterize products and coproducts in these categories. Also, epimorphisms and monomorphisms in **Dcpo**-S are studied. Further, we show that **Cpo**-S is not cartesian closed but **Dcpo**-S is cartesian closed.

1. Introduction and preliminaries

The category **Dcpo** of directed complete partial ordered sets plays an important role in Theoretical Computer Science, and specially in Domain Theory (see [1]). This category is complete and cocomplete. The completeness of **Dcpo** has been proved (in a constructive way) by Achim Jung ([1]) and it is stated there that to describe colimits is quite difficult. In [5], Fiech characterizes and describes colimits in **Dcpo**, but his construction is rather complicated. The cartesian closeness of **Dcpo** has also been proved by Achim Jung (see [7]). It is also shown that the category **Cpo** of directed complete partially ordered sets with bottom elements and strict continuous maps between them is monoidal closed, complete and cocomplete (see [1, 7]).

In this paper, we study some categorical properties of the categories **Dcpo**-S (and **Cpo**-S) of the actions of a dcpo(cpo)-monoid S on dcpo's (cpo's). In particular, we show that the category **Dcpo**-S is complete and cocomplete, and describe products and coproducts in these categories. Also, epimorphisms and monomorphisms in these categories are considered. Further, we show that **Cpo**-S is not cartesian closed but **Dcpo**-S is so.

Let us now give some preliminaries needed in the sequel.

Let **Pos** denote the category of all partially ordered sets (posets) with order preserving (monotone) maps between them. A nonempty subset D of a partially ordered set is called *directed*, denoted by $D \subseteq^d P$, if for every $a, b \in D$ there exists

2010 Mathematics Subject Classification: 06F05, 06F30, 20M30, 18A30
Keywords: Directed complete partially ordered set, product, coproduct, cartesian closed.

$c \in D$ such that $a, b \leqslant c$; and P is called *directed complete*, or briefly a *dcpo*, if for every $D \subseteq^d P$, the directed join $\bigvee^d D$ exists in P. A dcpo which has a bottom element $\perp$ is said to be a *cpo*.

A *dcpo map* or a *continuous map* $f\colon P \to Q$ between dcpo's is a map with the property that for every $D \subseteq^d P$, $f(D)$ is a directed subset of Q and $f(\bigvee^d D) = \bigvee^d f(D)$. A dcpo map $f\colon P \to Q$ between cpo's is called *strict* if $f(\perp) = \perp$. Thus we have the categories **Dcpo** (and **Cpo**) of all dcpo's (cpo's) with (strict) continuous maps between them.

The following lemmas are frequently used in this paper.

Lemma 1.1. [3, 7] *Let $\{A_i\colon i \in I\}$ be a family of dcpo's. Then the directed join of a directed subset $D \subseteq^d \prod_{i\in I} A_i$ is calculated as $\bigvee^d D = (\bigvee^d D_i)_{i\in I}$ where*

$$D_i = \{a \in A_i\colon \exists d = (d_k)_{k\in I} \in D,\ a = d_i\}$$

for all $i \in I$.

Lemma 1.2. [7] *Let P, Q, and R be dcpo's, and $f\colon P \times Q \to R$ be a function of two variables. Then f is continuous if and only if f is continuous in each variable; which means that for all $a \in P$, $b \in Q$, $f_a\colon Q \to R$ $(b \mapsto f(a, b))$ and $f_b\colon P \to R$ $(a \mapsto f(a, b))$ are continuous.*

Remark 1.3. The categories **Dcpo** and **Cpo** are both complete and cocomplete. In fact,

(i) The product of a family of dcpo's (cpo's) is their cartesian product, with componentwise order and ordinary projection maps. In particular, the terminal object of **Dcpo** (and **Cpo**) is the singleton poset $\{\theta\}$.

The equalizer of a pair $f, g\colon P \to Q$ of (strict) continuous maps is given by $E = \{x \in P : f(x) = g(x)\}$ with the order inherited from P.

Moreover, the pullback of (strict) continuous maps $f\colon P \to R$ and $g\colon Q \to R$ is the sub-dcpo $P = \{(a, b)\colon f(a) = g(b)\}$ of the product $P \times Q$ together with the restriction of projection maps.

(ii) The coproduct of a family of dcpo's is their disjoint union, with the order arising from each factor. In particular, the initial object of **Dcpo** is the empty poset.

The coproduct of a family of cpo's is their *coalesced sum*. Recall that *the coalesced sum* of the family $\{A_i\colon i \in I\}$ of cpo's is defined to be

$$\biguplus_{i\in I} A_i = \perp \oplus \dot{\bigcup}_{i\in I}(A_i \setminus \{\perp_{A_i}\}).$$

In particular, the initial object of **Cpo** is the singleton poset $\{\theta\}$.

Recall that a *po-monoid* is a monoid with a partial order $\leqslant$ which is compatible with the monoid operation: for $s, t, s', t' \in S$, $s \leqslant t$, $s' \leqslant t'$ imply $ss' \leqslant tt'$.

Similarly, a *dcpo* (*cpo*)*-monoid* is a monoid which is also a dcpo (cpo) whose binary operation is a (strict) continuous map.

Now, we recall the preliminary notions of the action of a (po)monoid on a set(poset). For more information, see [2, 4, 8].

Let S be a monoid. A (*right*) *S-act* or *S-set* is a set A equipped with an action $A \times S \to A$, $(a, s) \rightsquigarrow as$, such that $a1 = a$ and $a(st) = (as)t$, for all $a \in A$ and $s, t \in S$. Let **Act-**S denote the category of all S-acts with action-preserving maps (maps $f : A \to B$ with $f(as) = f(a)s$).

Also, recall that an element a of an S-act A is said to be a *zero element* if $as = a$ for all $s \in S$.

Let S be a po-monoid. A (*right*) *S-poset* is a poset A which is also an S-act whose action $\lambda\colon A \times S \to A$ is order-preserving, where $A \times S$ is considered as a poset with componentwise order. The category of all S-posets with action-preserving monotone maps between them is denoted by **Pos-**S.

Remark 1.4. Recall (see [2]) that:

(i) The product in the category of S-posets is the cartesian product with the componentwise action and order. In particular, the terminal S-poset is the singleton S-poset.

Also, recall that the equalizer of a pair $f, g\colon A \to B$ of S-poset maps is given by $E = \{a \in A\colon f(a) = g(a)\}$ with action and order inherited from A.

The pullback of S-poset maps $f\colon A \to C$ and $g\colon B \to C$ is the sub-S-poset $P = \{(a, b)\colon f(a) = g(b)\}$ of $A \times B$.

(ii) The coproduct is the disjoint union with the usual action and order. In particular, the initial S-poset is the empty set.

Finally, we introduce the notion which we work on in this paper.

Definition 1.5. Let S be a (cpo) dcpo-monoid. By a (*right*) *S-dcpo* (*S-cpo*) we mean a dcpo (cpo) A which is also an S-act whose action $\lambda\colon A \times S \to A$ is (strict) continuous, where $A \times S$ is considered as a dcpo with componentwise order.

By an *S-dcpo map* (*S-cpo map*) between S-dcpo's (S-cpo's), we mean a map $f\colon A \to B$ which is both (strict) continuous and action-preserving.

We denote the categories of all S-dcpo's (S-cpo's) and S-dcpo (S-cpo) maps between them by **Dcpo**-S (**Cpo**-S) .

Remark 1.6. (1) In the definition of an S-cpo, we can omit the property that the action is strict. Notice that $\perp_{A\times S} = (\perp_A, \perp_S)$, and the action being strict means that $\perp_A\perp_S = \perp_A$. But, assumig that there is a continuous (monotone) action on a cpo A, the fact that $\perp_S \leqslant 1$ implies $\perp_A\perp_S \leqslant \perp_A 1 = \perp_A$. Also, since $\perp_A$ is the bottom element in A, we have $\perp_A \leqslant \perp_A\perp_S$. Thus, $\perp_A\perp_S = \perp_A$ as required.

(2) Note that, by Lemma 1.2, the action $\lambda\colon A \times S \to A$ is continuous if and only if each $\lambda_a\colon S \to A$, $s \mapsto as$, and $\lambda_s\colon A \to A$, $a \mapsto as$, is continuous.

(3) Notice that the above note is not true for strictness. For example, consider the pomonoid $S = \{0 < 1\}$ with the binary operation max. It is clear that max is

strict continuous, so S is a cpo-monoid and hence an S-cpo. But the continuous map $\lambda_1 : S \to S$, $t \mapsto \max(t, 1)$ is not strict, because $\max(0, 1) = 1 \neq 0 = \bot_S$.

2. Limits and coproduts in Cpo-S and Dcpo-S

In this section, we give the description of products, equalizers, terminal object and pullback in the categories **Dcpo**-S and **Cpo**-S. We also, find coproducts in these two categories.

Remark 2.1. In both the categories **Dcpo**-S and **Cpo**-S, the terminal object is the one element object.

Proposition 2.2. *The product of a family of S-dcpo's (S-cpo's) is their cartesian product with componentwise action and order.*

Proof. Let $\{A_i \colon i \in I\}$ be a family of S-dcpo's (S-cpo's). Let $A = \prod_{i\in I} A_i$. First we see that A with componentwise action and order is a S-dcpo (S-cpo). By Remark 1.4, A is an S-poset. Also, the action on A is continuous. Applying Lemma 1.2, it is enough to check the continuity of the action in each component. Let $D \subseteq^d A$ and $s \in S$. We show that $(\bigvee^d D)s = \bigvee_{x\in D} xs$. By Lemma 1.1, $\bigvee^d D = (\bigvee^d D_i)_{i\in I}$, where $D_i = \{a \in A_i \colon \exists (d_k)_{k\in I} \in D,\ d_i = a\}$ is a directed subset of A_i, for all $i \in I$. Then we have $(\bigvee^d D)s = (\bigvee^d D_i)_{i\in I} s = ((\bigvee^d D_i)s)_{i\in I} = (\bigvee^d D_i s)_{i\in I}$, where the latter equality is because the action on each A_i is continuous. Now, we see that $(\bigvee^d D_i s)_{i\in I} = \bigvee^d_{x\in D} xs$. First, notice that $(\bigvee^d D_i s)_{i\in I}$ is an upper bound of the set $\{xs \colon\ x \in D\}$, since for $x = (d_i)_{i\in I} \in D$, we have $d_i \in D_i$, for all $i \in I$, and so $xs = (d_i s)_{i\in I} \leqslant ((\bigvee^d D_i)s)_{i\in I} = (\bigvee^d D_i s)_{i\in I}$. Secondly, if $c = (c_i)_{i\in I}$ is any upper bound of the set $\{xs \colon\ x \in D\}$, then for $i \in I$ and $a \in D_i$, taking $x = (d_i)_{i\in I}$ with $d_i = a$, we have $as = d_i s \leqslant c_i$. Thus $(\bigvee^d D_i s)_{i\in I} \leqslant c$, as required. Similarly, the action on A is continuous in the second component; that is for $T \subseteq^d S$ and $a = (a_i)_{i\in I} \in A$, $a(\bigvee^d T) = \bigvee^d_{t\in T} at$. Consequently, $A = \prod_{i\in I} A_i$ with the componentwise order and action is an S-dcpo (S-cpo). Also, the projection maps $p_i : A \to A_i$ are S-dcpo (S-cpo) maps, since by Remark 1.3 they are (strict) continuous, also they are action-preserving (see [8]). To see the universal property of products, notice that for every S-dcpo (S-cpo) B with S-dcpo (S-cpo) maps $f_i \colon B \to A_i$, $i \in I$, the unique S-poset map $f : B \to A$ given by $f(b) = (f_i(b))_{i\in I}$, $b \in B$ which exists by the universal property of products in **Pos**-S (see Remark 1.4), and satisfies $p_i \circ f = f_i$, for all $i \in I$, is a (strict) continuous map. This is because, $f(\bot_B) = (f_i(\bot_B))_{i\in I} = (\bot_{A_i})_{i\in I} = \bot_A$. Also, it is straightforward to see that for $D \subseteq^d B$, $f(\bigvee^d D) = \bigvee^d f(D)$. □

Remark 2.3. (i) It is clear that the initial object in the category **Dcpo**-S is the empty set.

(ii) The category **Cpo**-S has initial object if the identity of the cpo-monoid S is its bottom element. In fact S is the initial object. Since, for every S-cpo A the map $\lambda_\perp \colon S \to A$, defined by $\lambda_\perp(s) = \perp_A s$ is the unique S-cpo map from S to A. To show the uniqueness, let $\alpha \colon S \to A$ be an S-cpo map, then $\alpha(s) = \alpha(1s) = \alpha(1)s = \perp_A s = \lambda_\perp(s)$, for all $s \in S$. Thus, $\alpha = \lambda$.

Now, we consider coproducts.

Theorem 2.4. *The coproduct of a family of S-dcpo's is their disjoint union.*

Proof. Let $\{A_i \colon i \in I\}$ be a family of S-dcpo's. Let $A = \bigcup_{i\in I} A_i$ be the disjoint union of A_i, $i \in I$. By Remark 1.4, A with the order and the action inherited from A_i, $i \in I$; that is

$$x \leqslant y \text{ in } A \text{ if and only if } x \leqslant y \text{ in } A_i, \text{ for some } i \in I$$

and $a.s = as$ for $a \in A_i$, $s \in S$, is an S-poset. Applying Lemma 1.2, we see that this the action is also continuous. Therefore, A is an S-dcpo. Moreover, the injection maps $u_i \colon A_i \to A$, defined by $u_i = id_A|_{A_i}, i \in I$ are S-poset maps, by Remark 1.4, and they are continuous, by Remark 1.3. Finally, since A satisfies the universal property of coproducts in **Pos**-S, for every S-dcpo B and S-dcpo maps $f_i \colon A_i \to B$, $i \in I$, the mapping $f \colon A \to B$ given by $f(a) = f_i(a)$ for $a \in A_i$, is the unique S-poset map with $f \circ u_i = f_i$, for all $i \in I$. This map is also continuous, because if D is a directed subset of A then by the definition of the order on A, $D \subseteq^d A_i$ for some $i \in I$, and $\bigvee^d_A D = \bigvee^d_{A_i} D$. Thus $f(\bigvee^d D) = f_i(\bigvee^d D) = \bigvee^d f_i(D) = \bigvee^d f(D)$. □

To describe the coproduct in **Cpo**-S, using the coalesced sum of cpo's, we need the following lemma.

Lemma 2.5. *The coalesced sum of a family of S-cpo's in which the bottom element is a zero element is an S-cpo.*

Proof. Let $\{A_i \colon i \in I\}$ be a family of S-cpo's. By Remark 1.3, the coalesced sum $A = \biguplus_{i\in I} A_i$ is a cpo. Define the action on A as:

$$a \cdot s = \begin{cases} as & \text{if} \quad as \neq \perp_{A_i} \\ \perp_A & \text{if} \quad as = \perp_{A_i} \end{cases}$$

for $a \in A_i$, $i \in I$, $s \in S$, and $\perp_A \cdot s = \perp_A$. In particular, $\perp_A \cdot 1 = \perp_A$. We see that also for $a \neq \perp_A$, $a \cdot 1 = a$, because, for some $i \in I$, $a \in A_i$, and so $a \cdot 1 = a1 = a$. Also, $a \cdot (st) = (a \cdot s) \cdot t$, for $a \in A$, $s, t \in S$. This is because, $\perp_A \cdot (st) = (\perp_A \cdot s) \cdot t$, by the definition, and for $a \neq \perp_A$, $a \in A_i$ for some $i \in A$. If $a(st) \neq \perp_{A_i}$, then $as \neq \perp_{A_i}$, (otherwise since $\perp_{A_i}$ is a zero element, $a(st) = (as)t = \perp_{A_i} t = \perp_{A_i}$); also $(as)t = a(st) \neq\perp_{A_i}$. So $(a\dot{s}) \cdot t = (as) \cdot t = (as)t = a(st) = a \cdot (st)$. Secondly, if $a(st) = \perp_{A_i}$, then $a \cdot (st) = \perp_A$. Now, if $as = \perp_{A_i}$ then $a \cdot s = \perp_A$ and so $(a \cdot s) \cdot t = \perp_A \cdot t = \perp_A$. Also, if $as \neq \perp_{A_i}$ then $a \cdot s = as$, and since $(as)t = a(st) = \perp_{A_i}$, $(a \cdot s) \cdot t = \perp_A$. Thus $(a \cdot s) \cdot t = (a \cdot s) \cdot t = \perp_A$, as required.

Now, we show that the action is continuous. Notice that $D \subseteq^d A$ is directed if and only if $D \subseteq^d A_i$, for some $i \in I$, or $D = D' \cup \{\perp_A\}$, where $D' = \emptyset$ or D' is a directed subset of A_i, for some $i \in I$. This is because, if $D \subseteq^d A$ and $\bot_A \notin D$, and on the contrary, if there exist $d_1, d_2 \in D$ such that $d_1 \in A_i$ and $d_2 \in A_j$, $i \neq j$, then there exists $d_3 \in D$ such that $d_1 \leqslant d_3$ and $d_2 \leqslant d_3$. Also, by the definition of the order on A, $d_3 \in A_i \cap A_j = \emptyset$, which is a contradiction. So $D \subseteq^d A_i$, for some $i \in I$. Now, let $\bot_A \in D$. We show that $D' = D - \{\bot_A\}$ is a directed subset of A_i, for some $i \in I$. On the contrary, let there exist ${d_1}', {d_2}' \in D'$ such that ${d_1}' \in A_i$ and ${d_2}' \in A_j$, $i \neq j$. Since D is directed, there exists $d_3 \in D$ such that ${d_1}' \leqslant d_3$ and ${d_2}' \leqslant d_3$. By the definition of the order on A, $d_3 \in A_i \cap A_j = \emptyset$, which is a contradiction. So $D' \subseteq^d A_i$, for some $i \in I$. Now, applying Lemma 1.2, we show that the action is continuous. Let $D \subseteq^d \biguplus_{i \in I} A_i$ and $s \in S$. By the above discussion, two cases may occur:

CASE (i): $D \subseteq^d A_i$, for some $i \in I$.

SUBCASE (i1): If $(\bigvee^d D)s \neq \bot_{A_i}$, then we have $(\bigvee^d D) \cdot s = (\bigvee^d D)s = \bigvee^d_{x \in D} xs$, where the last equality is because A_i is an S-cpo. Now we claim that

$$\bigvee_{x \in D}^{d} xs = \bigvee_{x \in D}^{d} x \cdot s \qquad (*)$$

Let $K = \{x \in D \colon xs \neq \bot_{A_i}\}$. Then K satisfies:

(1) $K \neq \emptyset$, because otherwise $(\bigvee^d D)s = \bigvee^d_{x \in D} xs = \bot_{A_i}$, which is a contradiction.

(2) For all $x \in K$, $x \cdot s = xs$, by the definition of the action on A.

(3) For all $x \in K$ and $x' \in D \backslash K$, there exists $x'' \in K$ with $x \leqslant x''$ and $x' \leqslant x''$, since D is directed. But, then $xs \leqslant x''s$, and hence $x'' \in K$, since $x \in K$.

Now to prove $(*)$, first we see that $\bigvee^d_{x \in D} xs$ is an upper bound of the set $\{x \cdot s \colon x \in D\}$. Also for all $x \in K$, $x \cdot s = xs \leqslant \bigvee^d_{x \in D} xs$. For $x \in D \setminus K$, $x \cdot s = \bot_A \leqslant \bigvee^d_{x \in D} xs$, as required. Secondly, if c is an upper bound of the set $\{x \cdot s : x \in D\}$. For all $x \in K$, we have $x \cdot s = xs \leqslant c$. For $x \in D \setminus K$ and $x' \in K$ (which exists, since $K \neq \emptyset$), by (3) there exists $x'' \in K$ such that $x < x''$ and $x' \leqslant x''$. This gives $xs \leqslant x''s = x'' \cdot s \leqslant c$. Then for all $x \in D$, we have $xs \leqslant c$, and so $\bigvee^d_{x \in D} xs \leqslant c$, as required.

SUBCASE (i2): If $(\bigvee^d D)s = \bot_{A_i}$, then we again have $(\bigvee^d D)s = \bigvee^d_{x \in D} xs$. This is because, the action on A_i is continuous on the second component. Also, $(\bigvee^d D)s = \bot_{A_i}$ gives $xs = \bot_{A_i}$, for all $x \in D$. This is because, $\bot_{A_i} = (\bigvee^d D)s = \bigvee^d_{x \in D} xs$. Hence by the definition of the action on A, $(\bigvee^d D) \cdot s = \bigvee^d_{x \in D} x \cdot s = \bot_A$.

CASE (ii): $D = D' \cup \bot_A$, where $D' \subseteq^d A_i$, for some $i \in I$.

By case (i), we have $(\bigvee^d D') \cdot s = \bigvee^d_{x' \in D'} x' \cdot s$. Also, we have $(\bigvee^d D) \cdot s = (\bigvee^d D') \cdot s = \bigvee^d_{x' \in D'} x' \cdot s = \bigvee^d_{x \in D} x \cdot s$, as required.

Now to prove that the action is continuous in the second component, let $T \subseteq^d S$ and $a \in A$. We show that $a \cdot \bigvee^d T = \bigvee^d_{t \in T} a \cdot t$. Consider the following two cases:

(a): If $a = \bot_A$, then by the definition of the action on A, $a \cdot \bigvee^d T = \bigvee^d_{t \in T} a \cdot t = \bot_A$.

(b): If $a \neq \bot_A$, then for some $i \in I$, $a \in A_i$. We have the following two situations:

(b1): If $a(\bigvee^d T) \neq \bot_{A_i}$ then we have $a \cdot (\bigvee^d T) = a(\bigvee^d T) = \bigvee^d_{t \in T} at$, where the last equality is true because A_i is an S-cpo. Now, we claim that

$$\bigvee_{t\in T}^{d} a \cdot t = \bigvee_{t\in T}^{d} at \qquad (**).$$

Let $L = \{t \in T : at \neq \bot_{A_i}\}$. Then one can prove (in a similar way to the set K in the above discussion) that L satisfies:

(1) $L \neq \emptyset$.

(2) For all $t \in L$, $a \cdot t = at$.

(3) For all $t \in L$ and $t' \in T \setminus L$, there exists $t'' \in L$ with $t \leqslant t''$ and $t' \leqslant t''$.

Now to prove $(**)$, we see that first $\bigvee^d_{t \in T} at$ is an upper bound of the set $\{a \cdot t : t \in T\}$. Also for all $t \in L$, $a \cdot t = at \leqslant \bigvee^d_{t \in T} at$. For $t \in T \setminus L$, $a \cdot t = \bot_A \leqslant \bigvee^d_{t \in T} at$, as required. Secondly, if c is an upper bound of the set $\{a \cdot t : t \in T\}$, then for all $t \in L$, we have $at = a \cdot t \leqslant c$. Now, by (3) and in the same way of Subcase (i1), for $t \in T \setminus L$ there exists $t'' \in L$ such that $at \leqslant at'' \leqslant c$. Then for all $t \in T$, we have $at \leqslant c$, and so $\bigvee^d_{t \in T} at \leqslant c$. Therefore, $(**)$ has been proved.

(b2): If $a(\bigvee^d T) = \bot_{A_i}$, we show that $a \cdot (\bigvee^d T) = \bigvee^d_{t \in T} a \cdot t$. Since A_i is an S-cpo, we have $\bigvee^d_{t \in T} at = a(\bigvee^d T) = \bot_{A_i}$. So for all $t \in T$, $at = \bot_{A_i}$. Then by the definition of the action on A, $a \cdot (\bigvee^d T) = \bigvee^d_{t \in T} a \cdot t = \bot_A$.

Therefore, the action on A is continuous, and so $A = \biguplus_{i \in I} A_i$ is an S-cpo. □

Theorem 2.6. *Let $\{A_i : i \in I\}$ be a family of S-cpo's whose bottom elements are zero elements. Then their coproduct exists in* **Cpo-**S.

Proof. Let $A = \biguplus_{i \in I} A_i$. By Proposition 2.5, A is an S-cpo and by Remark 1.3, the injections $u_i \colon A_i \to A$, $i \in I$, defined by

$$u_i(x) = \begin{cases} x & \text{if} \quad x \neq \bot_{A_i} \\ \bot_A & \text{if} \quad x = \bot_{A_i} \end{cases}$$

are cpo maps. Also we show that $u_i \colon A_i \to A$, $i \in I$ are action-preserving. First notice that $u_i(\bot_{A_i s}) = u_i(\bot_{A_i}) = \bot_A = \bot_A \cdot s = u_i(\bot_{A_i}) \cdot s$. Now, let $\bot_{A_i} \neq x \in A_i$ and $s \in S$. If $xs = \bot_{A_i}$, then by the definition of the action on A, $x \cdot s = \bot_A$, and so $u_i(xs) = \bot_A = x \cdot s = u_i(x) \cdot s$. If $xs \neq \bot_{A_i}$, then $x \cdot s = xs$, and so $u_i(xs) = xs = x \cdot s = u_i(x) \cdot s$. Moreover for every S-cpo B with S-cpo maps $f_i \colon A_i \to B$, $i \in I$, the unique cpo map $f \colon A \to B$ given by

$$f(a) = \begin{cases} f_i(a) & \text{if} \quad a \in A_i \\ \bot_B & \text{if} \quad x = \bot_A \end{cases}$$

which exists by the universal property of coproducts in **Cpo**, and satisfies $f \circ u_i = f_i$ for all $i \in I$, is action-preserving. First notice that since each f_i is action-preserving and $\bot_{A_i}$ is a zero element, $f_i(\bot_{A_i}) = \bot_B$ is a zero element. Now, $f(\bot_A \cdot s) = f(\bot_A) = \bot_B = \bot_B s = f(\bot_A)s$, for all $s \in S$. Also, for $a \neq \bot_A$, we have $a \in A_i$, for some $i \in I$. Therefore, if $as = \bot_{A_i}$ we get $a \cdot s = \bot_A$, and so $f(a \cdot s) = f(\bot_A) = \bot_B = f_i(\bot_{A_i}) = f_i(as) = f_i(a)s = f(a)s$. If $as \neq \bot_A$, then we have $a \cdot s = as$, and so $f(a \cdot s) = f(as) = f_i(as) = f_i(a)s = f(a)s$. □

Corollary 2.7. *Let S be a cpo-monoid in which the identity element is the top element. Then* **Cpo**-*S has all coproducts.*

Proof. By Theorem 2.6, it is enough to show that the bottom element of every S-cpo A is a zero element. For all $s \in S$, we have $s \leqslant 1$, and so $\bot_A s \leqslant \bot_A 1 = \bot_A$. But, $\bot_A$ is the bottom element of A and so $\bot_A s = \bot_A$. □

Theorem 2.8. *Pullbacks and equalizers exist in the categories* **Cpo**-*S and* **Dcpo**-*S.*

Proof. Let $f, g \colon A \to B$ be S-cpo (S-dcpo) maps. Then

$$E = \{x \in A \colon f(x) = g(x)\}$$

is a sub S-cpo (S-dcpo) of A, and the inclusion map satisfies $f \circ i = g \circ i$. Also, if $e : K \to L$ is an S-cpo (S-dcpo) map with $f \circ e = g \circ e$ then the map $\gamma : K \to E$ given by $\gamma(x) = e(x)$ is the unique S-cpo (S-dcpo) map such that $i \circ \gamma = e$.

Also, it is easily seen that the pullback of S-cpo (S-dcpo) maps $f \colon A \to C$ and $g \colon B \to C$ is the sub-S-cpo (S-dcpo) $P = \{(a, b) \colon f(a) = g(b)\}$ of $A \times B$, together with the restricted projection maps. □

As a consequence of Theorems 2.2 and 2.8, we get the following result.

Proposition 2.9. *The categories* **Cpo**-*S and* **Dcpo**-*S are complete.*

3. Cocompleteness and cartesian closedness

In this section, we consider some other categorical properties of **Cpo**-S and **Dcpo**-S. We show that monomorphism in **Dcpo**-S are exactly one-one S-dcpo maps, while epimorphisms are not necessarily onto S-dcpo maps. Also, we prove that **Dcpo**-S is a cocomplete category. Further, it is proved that **Dcpo**-S is cartesian closed while **Cpo**-S is not so, and hence it is neither a topos nor a quasitopos (see [9]).

Lemma 3.1. *A morphism in* **Dcpo**-*S is a monomorphism if and only if it is one-one.*

Proof. Let $h\colon A \to B$ be a monomorphism in **Dcpo**-S, and $h(a) = h(a')$. Consider the S-dcpo maps $f, g\colon S \to A$ given by $f(s) = as$ and $g(s) = a's$, for $s \in S$. Then, $h \circ f = h \circ g$ and so $f = g$. Thus, $a = a'$. □

In the following we show that the category **Dcpo**-S is cocomplete.

Recall that an object C of a category $\mathcal{C}$ is called a *coseparator* if the functor $hom(-, C) : \mathcal{C}^{op} \to$ **Set** is faithful; in other words, for each distinct arrows $f, g\colon A \to B$ there exists an arrow $h\colon B \to C$ such that $h \circ f \neq h \circ g$.

Also, recall from [6], Theorem 23.14 that a complete well-powered category which has a coseparator, is cocomplete. Therefore, we show that **Dcpo**-S has a coseparator and is well-powered.

Proposition 3.2. *The forgetful functor* $U_1\colon$ **Dcpo**-$S \to$ **Dcpo** *has a right adjoint.*

Proof. We define the cofree functor $K_1\colon$ **Dcpo** $\to$ **Dcpo**-S as $K_1(P) = P^{(S)}$, where $P^{(S)}$ is the set of all dcpo maps from S to P. We give it the pointwise order and the action by $(fs)(t) = f(st)$, for $s, t \in S$ and $f \in P^{(S)}$. Then, $P^{(S)}$ is an S-dcpo. We know that $P^{(S)}$ is a dcpo (see [7]). Now, we show that the action defined above is a continuous map. Applying Lemma 1.2, let $F \subseteq^d P^{(S)}$. Then

$$((\overset{d}{\bigvee} F)s)(t) = (\overset{d}{\bigvee} F)(st) = \overset{d}{\bigvee_{f\in F}} f(st) = \overset{d}{\bigvee_{f\in F}} (fs)(t) = (\overset{d}{\bigvee_{f\in F}} fs)(t)$$

so we have $(\bigvee^d F)s = \bigvee^d (Fs)$. Now, assume that $T \subseteq^d S$ and $f \in P^{(S)}$, then

$$\begin{aligned}(f(\textstyle\bigvee^d T))(s) &= f((\textstyle\bigvee^d T)s) = f(\textstyle\bigvee^d_{t\in T} ts)\\ &= \textstyle\bigvee^d_{t\in T} f(ts) = \bigvee^d_{t\in T} (ft)(s) = (\bigvee^d_{t\in T} ft)(s)\end{aligned}$$

and so $f(\bigvee^d T) = \bigvee^d_{t\in T} ft$, as required. Consequently $P^{(S)}$ is an S-dcpo.

Now, consider the cofree map (the counit of the adjunction) $\sigma : P^{(S)} \to P$, given by $\sigma(f) = f(1)$. We show that it is continuous. Let $F \subseteq^d P^{(S)}$. Then

$$\sigma(\overset{d}{\bigvee_{f\in F}} f) = (\overset{d}{\bigvee_{f\in F}} f)(1) = \overset{d}{\bigvee_{f\in F}} f(1) = \overset{d}{\bigvee_{f\in F}} \sigma(f).$$

To see the universal property, let $\alpha\colon A \to P$ be a continuous map from an S-dcpo A. Then the unique S-poset map $\overline{\alpha}\colon A \to P^{(S)}$ given by $\overline{\alpha}(a)(s) = \alpha(as)$ and satisfying $\sigma \circ \overline{\alpha} = \alpha$ (see [2]) is continuous. To show this, let $D \subseteq^d A$ and $s \in S$. Then

$$\begin{aligned}\overline{\alpha}(\textstyle\bigvee^d D)(s) &= \alpha((\textstyle\bigvee^d D)s) = \alpha(\textstyle\bigvee^d_{x\in D} xs)\\ &= \textstyle\bigvee^d_{x\in D} \alpha(xs) = \bigvee^d_{x\in D} \overline{\alpha}(x)(s) = (\bigvee^d_{x\in D} \overline{\alpha}(x))(s)\end{aligned}$$

as required. □

Notice that the forgetful functor $U\colon \mathbf{Cpo}\text{-}S \to \mathbf{Cpo}$ does not necessarily have a right adjoint. This is because, U does not preserve initial object in general. For example, let S be the 2-element chain $\{1, a\}$ with $1 < a$, and $aa = a$, $1a = a = a1$. Then S is an S-cpo, and it is the initial object of $\mathbf{Cpo}\text{-}S$ (see Remark 2.3), whereas the initial object in the category $\mathbf{Cpo}$ is the singleton cpo.

Corollary 3.3. *The category* $\mathbf{Dcpo}$*-S has a coseparator.*

Proof. We show that for each dcpo P with $|P| \geq 2$ and non discrete order, the cofree object $P^{(S)}$ described in Proposition 3.2 is a coseparator.

Let $f, g\colon A \to B$ be S-dcpo maps with $f \neq g$. We should define an S-dcpo map $h : B \to P^{(S)}$ with $h \circ f \neq h \circ g$. To this end, we define a dcpo map $k\colon B \to P$ such that $k \circ f \neq k \circ g$.

Since $f \neq g$, there exists $a \in A$ with $f(a) \neq g(a)$. We consider three cases

$$(1)\ \ f(a) < g(a) \qquad (2)\ \ g(a) < f(a) \qquad (3)\ \ f(a) \parallel g(a)$$

Let $f(a) < g(a)$. Take $B' = \{b \in B \mid\ b \leqslant f(a)\}$. Define $k : B \to P$ by

$$k(b) = \begin{cases} x & \text{if } b \in B' \\ y & \text{otherwise} \end{cases}$$

where $x, y \in P$ and $x < y$ (such x, y exist since $|P| \geq 2$ and the order on P is not discrete). First we show that k is order-preserving, and hence it take directed subsets to directed ones. Let $b_1, b_2 \in B$ with $b_1 \leqslant b_2$. If $b_1 \in B'$, then for the case where $b_2 \in B'$, $x = k(b_1) = k(b_2)$; and for the case where $b_2 \notin B'$, $x = k(b_1) < y = k(b_2)$. Also, if $b_1 \notin B'$ then $b_2 \notin B'$, and so $k(b_1) = k(b_2) = y$. To prove the continuity of k, let $D \subseteq^d B$. Notice that $\bigvee^d D \in B'$ if and only if $D \subseteq B'$. Now, if $\bigvee^d D \in B'$, then $D \subseteq B'$ and so $k(\bigvee^d D) = x = \bigvee^d_{z \in D} k(z)$. Also, if $\bigvee^d D \notin B'$ then $k(\bigvee^d D) = y$, and $D \nsubseteq B'$. Thus $D \setminus B' \neq \emptyset$, and

$$\bigvee_{z \in D}^{d} k(z) = \bigvee_{z \in (D \setminus B') \cup (B' \cap D)}^{d} k(z) = y \vee x = y$$

as required. Finally, since $P^{(S)}$ is the cofree S-dcpo on P, there exists a unique S-dcpo map $h : B \to P^{(S)}$ such that $\sigma \circ h = k$, where σ is the cofree map defined in the above proposition. This gives that $h \circ f \neq h \circ g$, and so $P^{(S)}$ is a coseparator.

The cases (2) and (3) are proved similarly. □

Lemma 3.4. *The category* $\mathbf{Dcpo}$*-S is well-powered.*

Proof. We should prove that the class of isomorphic subobjects of any S-dcpo is a set. Let B be an S-dcpo and A be a suboject of B; that is there exists a monomorphism $f\colon A \to B$. By Lemma 3.1, f is one-one and so A is isomorphic to a subset of B. Hence the class of isomorphic subobjects of B is a subset of the powerset of B, and therefore is a set. □

Theorem 3.5. *The category* **Dcpo**-S *is cocomplete.*

Proof. By Theorem 23.14 of [6], Corollary 3.3, Lemma 3.4, and Proposition 2.9, **Dcpo**-S is cocomplete. □

The following example shows that epimorphisms in the categories **Dcpo**-S and **Cpo**-S are not necessarily surjective.

Example 3.6. Let S be an arbitrary dcpo(cpo)-monoid. Take A to be the dcpo(cpo) $\perp \oplus \mathbb{N}$ in which the order on $\mathbb{N}$ is discrete and $B = \perp \oplus \mathbb{N} \oplus \top$ in which the order on $\mathbb{N}$ is the usual order. Then both of A and B with the trivial action are S-dcpo's (cpo's). Let $h\colon A \to B$ be the inclusion map. Then h clearly preserves the action. Also, h is (strict) continuous. To see this, let $D \subseteq^d \perp \oplus \mathbb{N}$. Then $D = \{\perp\}$, or there exists $n \in \mathbb{N}$ such that $D = \{\perp, n\}$, or there exists $n \in \mathbb{N}$ such that $D = \{n\}$. If $D = \{\perp, n\}$ for some $n \in \mathbb{N}$, then

$$h(\bigvee^d D) = h(n) = n = \bigvee^d \{\perp, n\} = \bigvee^d \{h(\perp), h(n)\} = \bigvee^d h(D).$$

This is clearly true for other kinds of D. Now we claim that h is an S-dcpo(cpo) map which is an epimorphism but is not surjective. The latter is because $\top$ is not in the image of h. To show that h is an epimorphism, let $f_1, f_2\colon B \to P$ be S-dcpo(cpo) maps with $f_1 \circ h = f_2 \circ h$, and P be an S-dcpo(cpo). Then $f_1(\perp) = f_1(h(\perp)) = f_2(h(\perp)) = f_2(\perp)$ and $f_1(n) = f_1(h(n)) = f_2(h(n)) = f_2(n)$, for all $n \in \mathbb{N}$. Also

$$f_1(\top) = f_1(\bigvee^d \mathbb{N}) = \bigvee^d_{n\in\mathbb{N}} f_1(n) = \bigvee^d_{n\in\mathbb{N}} f_2(n) = f(\bigvee^d \mathbb{N}) = f_2(\top).$$

Therefore, $f_1 = f_2$, and so h is an epimorphism.

Finally, we consider cartesian closedness. Recall that a category $\mathcal{C}$ which has finite products, is called *cartesian closed* if, for every pair of objects A and B of $\mathcal{C}$, an object B^A and a morphism $ev\colon A \times B^A \to B$ exist with the universal property that for every morphism $f\colon A \times C \to B$ in $\mathcal{C}$, there exists a unique morphism $\hat{f}\colon C \to B^A$ such that $ev \circ (id_A \times \hat{f}) = f$. In this definition, the objects B^A are called *power objects or exponentials*, and ev is said to be *the evaluation map*, and $\hat{f}$ is called *the exponential map* associated to f.

Theorem 3.7. *The category* **Cpo**-S *is not necessarily cartesian closed.*

Proof. Let $S = \{1\}$, then the category **Cpo**-S is isomorphic to the category **Cpo** which is not cartesian closed (See [4]).

For an example in which S is not trivial, let S be the 2-element chain $\{1, a\}$ with identity 1, $1 < a$ and $aa = a$. Then S is an S-cpo, and by Remark 2.3, it is the initial object of **Cpo**-S. Then for a non trivial S-cpo A, the functor

$A \times -\colon$ **Cpo**-$S \to$ **Cpo**-S does not have preserve the initial object (since $|A| \times 2 \neq 2$), and so does not have a right adjoint. Therefore, the category **Cpo**-S is not cartesian closed. □

In the following, we show that **Dcpo**-S is cartesian closed.

Theorem 3.8. *The category* **Dcpo**-S *is cartesian closed.*

Proof. By Proposition 2.9, **Dcpo**-S has finite products. Given S-dcpo's A, B, we define the exponential object B^A to be $Hom(S \times A, B)$, the set of all S-dcpo maps from the product object $S \times A$ to B. This set is an S-dcpo with pointwise order, and action given by $(fs)(t,a) = f(st,a)$. The evaluation arrow $ev\colon A \times B^A \to B$ is defined by $ev(a,f) = f(1,a)$, is an S-dcpo map. It is an S-poset map (see [2]), to prove continuity, let $D \subseteq^d A$ and $f \in B^A$, then

$$ev(\bigvee^d D, f) = f(1, \bigvee^d D) = \bigvee^d_{x \in D} f(1,x) = \bigvee^d_{x \in D} ev(x,f)$$

since f is continuous. Also, for $F \subseteq^d B^A$ and $a \in A$, we have

$$ev(a, \bigvee^d F) = (\bigvee^d F)(1,a) = \bigvee^d_{f \in F} f(1,a) = \bigvee^d_{f \in F} ev(a,f)$$

To prove the universal property, take an S-dcpo C and an S-dcpo map $f\colon A \times C \to B$. Define the map $\hat{f}\colon C \to B^A$ by $\hat{f}(x)(s,a) = f(a,xs)$, for $x \in C$, $a \in A$, and $s \in S$. As in the case of S-sets (see [4]), it can be shown that $\hat{f}$ and $\hat{f}(x)$, for each $x \in C$, preserve the action. Also, we show that each $\hat{f}(x)$ is continuous. Let $T \subseteq^d S$ and $a \in A$. Then

$$\hat{f}(x)(\bigvee^d T, a) = f(a, x(\bigvee^d T)) = f(a, \bigvee^d_{t \in T} xt) = \bigvee^d_{t \in T} f(a,xt) = \bigvee^d_{t \in T} \hat{f}(x)(t,a)$$

Now, let $D \subseteq^d A$ and $s \in S$. Then

$$\hat{f}(x)(s, \bigvee^d D) = f(\bigvee^d D, xs) = \bigvee^d_{d \in D} f(d,xs) = \bigvee^d_{d \in D} \hat{f}(x)(s,d)$$

as required. Further, $\hat{f}$ is continuous, because for every $D \subseteq^d C$ and $(s,a) \in S \times A$, we have

$$\begin{aligned} \hat{f}(\textstyle\bigvee^d D)(s,a) &= f(a, (\textstyle\bigvee^d D)s) = f(a, \textstyle\bigvee^d_{x \in D} xs) \\ &= \textstyle\bigvee^d_{x \in D} f(a,xs) = \textstyle\bigvee^d_{x \in D} \hat{f}(x)(s,a) \end{aligned}$$

as required. □

Remark 3.9. The above proof for the case where S is a one-element dcpo-monoid shows that the exponential object B^A in **Dcpo** is the set of all continuous maps from A into B, with pointwise order (for another proof of this fact, see [7]).

Open Problems:

1. *Is the category* **Cpo**-S *cocomplete? If yes, what is the description of coequalizers and pushouts?*

2. *For which class of semigroups* S*, the category* **cpo**-S *is cartesian closed?*

Acknowledgment. The authors gratefully acknowledge Professor M. Mehdi Ebrahimi's comments and conversation during this work. Also, thanks to the kind hospitality of Hakim Sabzevari University, during our stay there, which helped us to finish this paper. Also, our sincere thanks goes to the referee for the very valuable comments which improved the paper.

References

[1] **S. Abramsky and A. Jung**, *Domain Theory*, Handbook of logic in Computer Science **3** (1994), 1 – 168.

[2] **S. Bulman-Fleming, and M. Mahmoudi**, *The category of S-posets*, Semigroup Forum **71** (2005), no. 3, 443 – 461.

[3] **B.A. Davey, and H.A. Priestly**, *Introduction to Lattices and Order*, Cambridge University Press, Cambridge, 1990.

[4] **M.M. Ebrahimi and M. Mahmoudi**, *The category of M-Sets*, Ital. J. Pure Appl. Math. **9** (2001), 123 – 132.

[5] **A. Fiech**, *Colimits in the category Dcpo*, Math. Structures Comput. Sci. **6** (1996), 455 – 468.

[6] **H. Herrlich and G.E. Strecker**, *Category Theory*, Allyn and Bacon, 1973.

[7] **A. Jung**, *Cartesian closed categories of Domain*, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, (1989).

[8] **M. Kilp, U. Knauer, and A. Mikhalev**, *Monoids, Acts and Categories*, Walter de Gruyter, Berlin, New York, 2000.

[9] **S. Mac Lane, I. Moerdijk**, *Sheaves in Geometry and Logic*: A First Introduction to Topos Theory, Springer-Verlag, 1992.

Received December 15, 2014
Revised June 14, 2015

Department of Mathematics, Shahid Beheshti University G.C., Tehran 19839, Iran
E-mails: m-mahmoudi@sbu.ac.ir, h_moghbeli@sbu.ac.ir

Quasigroups and Related Systems **23** (2015), 297 − 308

An investigation on fuzzy hyperideals of ordered semihypergroups

Bundit Pibaljommee, Kantapong Wannatong and Bijan Davvaz

Abstract. We introduce the notions of fuzzy hyperideals, fuzzy bi-hyperideals and fuzzy quasi-hyperideals of an ordered semihypergroup and show that every fuzzy quasi-hyperideal is a fuzzy bi-hyperideal and in a regular ordered semihypergroup, fuzzy quasi-hyperideals and fuzzy bi-hyperideals coincide. Moreover, we show that in an ordered semihypergroup every fuzzy quasi-hyperideal is an intersection of a fuzzy right hyperideal and a fuzzy left hyperideal.

1. Introduction

The concept of algebraic hyperstructures was introduced in 1934 by Marty [13]. The concept of a semihypergroup is a generalization of the concept of a semigroup. Semihypergroups are studied by many authors, for example, Bonansinga and Corsini [1], Davvaz [4, 5], De Salvo et al. [6], Freni [7], Hila et al. [9], Leoreanu [14], and many others. In [8], Heidari and Davvaz studied a semihypergroup $(H, \circ)$ with a binary relation $\leqslant$, where $\leqslant$ is a partial order so that the monotony condition is satisfied. This structure is called an ordered semihypergroup. The study of fuzzy algebras was started in [15] by Rosenfeld. In [10], the relationships between some types of fuzzy ideals in ordered semigroups were investigated. In [11], some equivalent definitions of fuzzy ideals of ordered semigroups were given. In [3], Davvaz introduced the concept of a fuzzy right (resp. left, two-sided) hyperideal of a semihypergroup and proved some results in this respect. Now, in this paper we study the notions of fuzzy hyperideals of ordered semihypergroups.

The paper is structured as follows. After an introduction, in Section 2 we present some basic notions and examples on ordered semihypergroups. In Section 3, we introduce the notions of fuzzy hyperideals, fuzzy bi-hyperideals and fuzzy quasi-hyperideals of an ordered semihypergroup and we give some results in this respect. In particular, we show that every fuzzy quasi-hyperideal is a fuzzy bi-hyperideal and in a regular ordered semihypergroup, fuzzy quasi-hyperideals and fuzzy bi-hyperideals coincide. Moreover, we show that in an ordered semihypergroup every fuzzy quasi-hyperideal is an intersection of a fuzzy right hyperideal and a fuzzy left hyperideal.

2010 Mathematics Subject Classification: 20N20, 20N25, 06F05
Keywords: Ordered semihypergroup, regular ordered semihypergroup, fuzzy hyperideal, fuzzy bi-hyperideal, fuzzy quasi-hyperideal.

2. Preliminaries

A *hypergroupoid* consists of a non-empty set H and a mapping $\circ : H \times H \to \mathcal{P}^*(H)$ called a *hyperoperation*, where $\mathcal{P}^*(H)$ denotes the set of all non-empty subsets of H. We denote by $a \circ b$ the image of the pair (a, b) in $H \times H$.

A hypergroupoid $(H, \circ)$ is called a *semihypergroup* if it satisfies the associative property, namely,

$$(a \circ b) \circ c = a \circ (b \circ c).$$

For any non-empty subsets A, B of H, we denote

$$A \circ B := \bigcup_{a \in A, b \in B} a \circ b.$$

Instead of $\{a\} \circ A$ and $B \circ \{a\}$, we write $a \circ A$ and $B \circ a$, respectively.

Definition 2.1. Let H be a non-empty set and $\leqslant$ be an ordered relation on H. The triplet $(H, \circ, \leqslant)$ is called an *ordered semihypergroup* if the following conditions are satisfied.

(1) $(H, \circ)$ is a semihypergroup,

(2) $(H, \leqslant)$ is a partially order set,

(3) for every $a, b, c \in H$, $a \leqslant b$ implies $a \circ c \leqslant b \circ c$ and $c \circ a \leqslant c \circ b$, where $a \circ c \leqslant b \circ c$ means that for every $x \in a \circ c$ there exists $y \in b \circ c$ such that $x \leqslant y$.

A non-empty subset A of an ordered semihypergroup $(H, \circ, \leqslant)$ is called a *subsemihypergroup* of H if $(A, \circ, \leqslant)$ is an ordered semihypergroup.

We note that for every $a, b, c, d, e, f \in H$ with $a \circ b \leqslant c \circ d$ and $e \leqslant f$, we obtain $a \circ b \circ e \leqslant c \circ d \circ f$.

For $K \subseteq H$, we denote

$$(K] := \{a \in H \mid a \leqslant k \text{ for some } k \in K\}.$$

Definition 2.2. A non-empty subset A of an ordered semihypergroup $(H, \circ, \leqslant)$ is called a *right* (resp. *left*) *hyperideal* of H if

(1) $A \circ H \subseteq A$ (resp. $H \circ A \subseteq A$),

(2) for every $a \in H$, $b \in A$ and $a \leqslant b$ implies $a \in A$.

If A is both right hyperideal and left hyperideal of H, then A is called a *hyperideal (or two-side hyperideal)* of H.

Definition 2.3. A subsemihypergroup A of an ordered semihypergroup $(H, \circ, \leqslant)$ is called a *bi-hyperideal* of H if

(1) $A \circ H \circ A \subseteq A$,

(2) for every $a \in H$, $b \in A$ and $a \leqslant b$ implies $a \in A$.

Definition 2.4. A non-empty subset Q of an ordered semihypergroup $(H, \circ, \leqslant)$ is called a *quasi-hyperideal* of H if

(1) $(Q \circ H] \cap (H \circ Q] \subseteq Q$,

(2) for every $a \in H$, $b \in Q$ and $a \leqslant b$ implies $a \in Q$.

Example 2.5. The set $H = \{a, b, c, d, e\}$ and the hyperoperation defined by the table

$\circ$	a	b	c	d	e
a	a	$\{a,b,d\}$	a	$\{a,b,d\}$	$\{a,b,d\}$
b	a	b	a	$\{a,b,d\}$	$\{a,b,d\}$
c	a	$\{a,b,d\}$	$\{a,c\}$	$\{a,b,d\}$	$\{a,b,c,d,e\}$
d	a	$\{a,b,d\}$	a	$\{a,b,d\}$	$\{a,b,d\}$
e	a	$\{a,b,d\}$	$\{a,c\}$	$\{a,b,d\}$	$\{a,b,c,d,e\}$

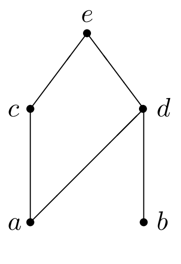
is a semihypergroup (cf. [2]).

We define order relation $\leqslant$ as follows:

$$\leqslant := \{(a,a),(b,b),(c,c),(d,d),(e,e),(a,c),(a,d),(a,e),(b,d),(b,e),(c,e),(d,e)\}.$$

We give the covering relation $\prec$ and the figure of H:

$$\prec = \{(a,c),(a,d),(b,d),(c,e),(d,e)\}.$$



Now, $(H, \circ, \leqslant)$ is an ordered semihypergroup, $\{a, b, d\}$ is a hyperideal and $\{a\}, \{a, c\}$ are left hyperideals and also bi-hyperideals of $(H, \circ, \leqslant)$. □

Now, we use the ordered semigroup defined in Example 3.3 in [16] to construct a semihypergroup in a similarly way of Example 3.10 in [2] and give an example of quasi-hyperideals of an ordered semihypergroup.

Example 2.6. Let $H = \{a, b, c, d, e\}$. Define the hyperoperation $\circ$ on H by the following table.

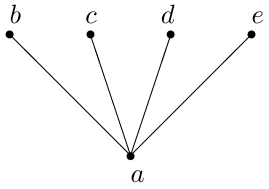
$\circ$	a	b	c	d	e
a	a	a	a	a	a
b	a	$\{a,b\}$	a	$\{a,d\}$	a
c	a	$\{a,e\}$	$\{a,c\}$	$\{a,c\}$	$\{a,e\}$
d	a	$\{a,b\}$	$\{a,d\}$	$\{a,d\}$	$\{a,b\}$
e	a	$\{a,e\}$	a	$\{a,c\}$	a

Suppose that the order relation $\leqslant$ as follows:

$$\leqslant := \{(a,a),(b,b),(c,c),(d,d),(e,e),(a,b),(a,c),(a,d),(a,e)\}.$$

We give the covering relation $\prec$ and the figure of H:

$$\prec = \{(a,b),(a,c),(a,d),(a,e)\}.$$



Now, $(H,\circ,\leqslant)$ is an ordered semihypergroup. It is easy to show that all proper quasi-hyperideals of H are $\{a\}, \{a,b\}, \{a,c\}, \{a,d\}, \{a,e\}, \{a,b,d\}, \{a,c,d\}, \{a,b,e\}$ and $\{a,c,e\}$. □

Let $(H,\circ,\leqslant)$ be an ordered semihypergroup and $a \in H$. We denote

$$A_a := \{(b,c) \in H \times H \mid a \leqslant b \circ c\}.$$

A *fuzzy subset* μ of a semihypergroup $(H,\circ)$ is a function $\mu : H \to [0,1]$. Let $t \in [0,1]$ and μ be a fuzzy subset of H. The set $\mu_t = \{a \in H \mid \mu(a) \geqslant t\}$ is called a *level subset* of μ. For fuzzy subsets μ and ν of H, we define the fuzzy subset $\mu \circ \nu$ of H by letting $a \in H$,

$$(\mu \circ \nu)(a) := \begin{cases} \sup\limits_{(b,c)\in A_a} \{\min\{\mu(b),\nu(c)\}\}, & \text{if } A_a \neq \emptyset, \\ 0, & \text{otherwise.} \end{cases}$$

At the end of this section, we recall the notions of a fuzzy subsemihypergroup of a semihypergroup introduced by Davvaz in [5] as the following. A fuzzy subset μ of a semihypergroup is called a *fuzzy subsemihypergroup* if $\inf\limits_{x\in a\circ b} \mu(x) \geqslant \min\{\mu(a),\mu(b)\}$ for all $a,b \in H$.

3. Fuzzy hyperideals of ordered semihypergroups

In this section, we define the concepts of a fuzzy right (left) hyperideal, a fuzzy bi-hyperideal and a fuzzy quasi-hyperideal and give relationships between them.

Definition 3.1. Let $(H, \circ, \leqslant)$ be an ordered semihypergroup. A fuzzy subset $\mu : H \to [0,1]$ is called a *fuzzy right* (resp. *left*) *hyperideal* of H if

(1) $\mu(a) \leqslant \inf\limits_{c \in a \circ b} \{\mu(c)\}$ (resp. $\mu(b) \leqslant \inf\limits_{c \in a \circ b} \{\mu(c)\}$ for every $a, b \in H$,

(2) for every $a, b \in H, a \leqslant b$ implies $\mu(b) \leqslant \mu(a)$.

If μ is both fuzzy right hyperideal and fuzzy left hyperideal of H, then μ is called a *fuzzy hyperideal* (or *fuzzy two-sided hyperideal*) of H.

Example 3.2. Consider the ordered semihypergroup $(H, \circ, \leqslant)$ defined in Example 2.5. We define two fuzzy subset μ and λ of H as follows:

$$\mu(x) = \begin{cases} 0.7 & \text{if} \quad x = a, b, d \\ 0.3 & \text{if} \quad x = c, e. \end{cases} \qquad \lambda(x) = \begin{cases} 0.9 & \text{if} \quad x = a \\ 0.8 & \text{if} \quad x = c \\ 0.5 & \text{if} \quad x = b, d, e \end{cases}$$

Then, μ is a fuzzy hyperideal and λ is a fuzzy left hyperideal of H. □

Definition 3.3. Let $(H, \circ, \leqslant)$ be an ordered semihypergroup. A fuzzy subsemihypergroup $\mu : H \to [0,1]$ is called a *fuzzy bi-hyperideal* of H if the following assertions are satisfied:

(1) $\min\{\mu(b), \mu(d)\} \leqslant \inf\limits_{a \in b \circ c \circ d} \{\mu(a)\}$ for every $b, c, d \in H$,

(2) for every $a, b \in H, a \leqslant b$ implies $\mu(b) \leqslant \mu(a)$.

Definition 3.4. Let $(H, \circ, \leqslant)$ be an ordered semihypergroup. A fuzzy subset $\mu : H \to [0,1]$ is called a *fuzzy quasi-hyperideals* of H if the following assertions are satisfied:

(1) $(\mu \circ 1) \cap (1 \circ \mu) \subseteq \mu$,

(2) for every $a, b \in H, a \leqslant b$ implies $\mu(b) \leqslant \mu(a)$,

where $1 : H \to [0,1]$ is a constant function defined by $1(a) = 1$ for all $a \in H$.

Lemma 3.5. *Let $(H, \circ, \leqslant)$ be an ordered semihypergroup and μ be a fuzzy subset of H. Then, μ is a fuzzy right (resp. left) hyperideal of H if and only if for every $t \in [0,1]$, the non-empty level subset μ_t is a right (resp. left) hyperideal of H.*

Proof. Assume that μ is a fuzzy right hyperideal of H. Let $t \in [0,1]$ with $\mu_t \neq \emptyset$. Let $a \in \mu_t \circ H$. We have $a \in b \circ h$ for some $b \in \mu_t, h \in H$. By assumption, $t \leqslant \mu(b) \leqslant \inf\limits_{a \in b \circ h}\{\mu(a)\}$, we have $\mu(a) \geqslant t$. This implies $\mu_t \circ H \subseteq \mu_t$. Let $x \in \mu_t, y \in H$ with $y \leqslant x$. Since $t \leqslant \mu(x) \leqslant \mu(y)$, we obtain $y \in \mu_t$. Therefore, μ_t is a right hyperideal of H.

Conversely, we assume that for every $t \in [0,1]$, μ_t is a right hyperideal of H. We show that $\mu(a) \leqslant \inf\limits_{c \in a \circ b}\{\mu(c)\}$ for all $a, b \in H$. We put $t_0 = \mu(a)$. By assumption μ_{t_0} is a right hyperideal of H. Since $a \in \mu_{t_0}$, $a \circ b \subseteq \mu_{t_0}$. Then, for every $c \in a \circ b$, we obtain $t_0 \leqslant \mu(c)$ and hence, $\mu(a) = t_0 \leqslant \inf\limits_{c \in a \circ b}\{\mu(c)\}$. Let $a, b \in H$ with $a \leqslant b$. Since $a \leqslant b, b \in \mu_{\mu(b)}$ and $\mu_{\mu(b)}$ is a right hyperideal of H, we get $a \in \mu_{\mu(b)}$. So, $\mu(b) \leqslant \mu(a)$. Therefore, μ is a fuzzy right hyperideal of H. □

Corollary 3.6. *Let $(H, \circ, \leqslant)$ be an ordered semihypergroup and χ_I be the characteristic function of I. Then, I is a left (resp. right) hyperideal of H if and only if χ_I is a fuzzy left (resp. right) hyperideal of H.* □

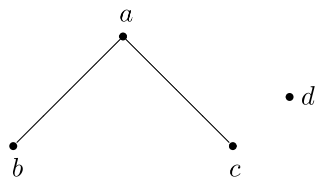
Example 3.7. Let $H = \{a, b, c, d\}$. We consider the ordered semihypergroup $(H, \circ, \leqslant)$, where the hyperoperation $\circ$ and the order relation $\leqslant$ on H are defined as follows:

$\circ$	a	b	c	d
a	a	$\{a,b\}$	$\{a,c\}$	a
b	a	$\{a,b\}$	$\{a,c\}$	a
c	a	$\{a,b\}$	$\{a,c\}$	a
d	a	$\{a,b\}$	$\{a,c\}$	a

$$\leqslant := \{(a,a), (b,b), (c,c), (d,d), (b,a), (c,a)\}.$$

We give the covering relation $\prec$ and the figure of H:

$$\prec = \{(b,a), (c,a)\}.$$



Now, we define the fuzzy subset μ of H as follows:

$$\mu(x) = \begin{cases} 0.8 & \text{if} \quad x = a, b, c, \\ 0.3 & \text{if} \quad x = d. \end{cases}$$

Then, μ is a fuzzy hyperideal of H. □

Lemma 3.8. *Let $(H, \circ, \leqslant)$ be an ordered semihypergroup and μ be a fuzzy subset of H. Then, μ is a fuzzy bi-hyperideal of H if and only if for every $t \in [0, 1]$, the non-empty level subset μ_t is a bi-hyperideal of H.*

Proof. Assume that μ is a fuzzy bi-hyperideal of H. Let $t \in [0, 1]$ with $\mu_t \neq \emptyset$. Let $a \in \mu_t \circ H \circ \mu_t$. We have $a \in b \circ h \circ c$ for some $b, c \in \mu_t, h \in H$. Since $t \leqslant \min\{\mu(b), \mu(c)\} \leqslant \inf\limits_{a \in b \circ h \circ c} \{\mu(a)\}$, we have $\mu(a) \geqslant t$. This implies $\mu_t \circ H \circ \mu_t \subseteq \mu_t$. Let $x \in \mu_t, y \in H$ with $y \leqslant x$. Since $t \leqslant \mu(x) \leqslant \mu(y)$, we obtain $y \in \mu_t$. Therefore, μ_t is a bi-hyperideal of H.

Conversely, we assume that for every $t \in [0, 1]$, μ_t is a bi-hyperideal of H. We show that $\min\{\mu(b), \mu(c)\} \leqslant \inf\limits_{a \in b \circ h \circ c} \{\mu(a)\}$ for all $b, c, h \in H$. We choose $t_0 = \min\{\mu(b), \mu(c)\}$. By assumption μ_{t_0} is a bi-hyperideal of H. Since $b, c \in \mu_{t_0}$, $b \circ h \circ c \subseteq \mu_{t_0}$. Then, for every $a \in b \circ h \circ c$, we have $t_0 \leqslant \mu(a)$ and so $\min\{\mu(b), \mu(c)\} = t_0 \leqslant \inf\limits_{a \in b \circ h \circ c} \{\mu(a)\}$. Let $a, b \in H$ with $a \leqslant b$. Since $a \leqslant b$, $b \in \mu_{\mu(b)}$ and $\mu_{\mu(b)}$ is a bi-hyperideal of H, we get $a \in \mu_{\mu(b)}$. So, $\mu(b) \leqslant \mu(a)$. Therefore, μ is a bi-hyperideal of H. □

Corollary 3.9. *Let $(H, \circ, \leqslant)$ be an ordered semihypergroup and χ_I be the characteristic function of I. Then, I is a bi-hyperideal of H if and only if χ_I is a fuzzy bi-hyperideal of H.* □

Lemma 3.10. *Let $(H, \circ, \leqslant)$ be an ordered semihypergroup and μ be a fuzzy subset of H. Then, μ is a fuzzy quasi-hyperideal of H if and only if for every $t \in [0, 1]$, the non-empty level subset μ_t is a quasi-hyperideal of H.*

Proof. Assume that μ is a fuzzy quasi-hyperideal of H. Let $t \in [0, 1]$ with $\mu_t \neq \emptyset$. We show that $(\mu_t \circ H] \cap (H \circ \mu_t] \subseteq \mu_t$. Let $a \in (\mu_t \circ H] \cap (H \circ \mu_t]$. Then, $a \in (\mu_t \circ H]$ and $a \in (H \circ \mu_t]$, i.e., $a \leqslant b \circ h$ and $a \leqslant k \circ c$ for some $b, c \in \mu_t, h, k \in H$, i.e., $(b, h), (k, c) \in A_a$. This implies $(\mu \circ 1)(a) = \sup\limits_{(x,y) \in A_a} \{\min\{\mu(x), 1(y)\}\} \geqslant t$ and $(1 \circ \mu)(a) = \sup\limits_{(x,y) \in A_a} \{\min\{1(x), \mu(y)\}\} \geqslant t$. By assumption, we obtain $\mu(a) \geqslant \min\{(\mu \circ 1)(a), (1 \circ \mu)(a)\} \geqslant t$. Therefore, $(\mu_t \circ H] \cap (H \circ \mu_t] \subseteq \mu_t$. Let $x \in \mu_t, y \in H$ with $y \leqslant x$. Since $t \leqslant \mu(x) \leqslant \mu(y)$, we obtain $y \in \mu_t$. Therefore, μ_t is a quasi-hyperideal of H.

Conversely, we assume that for every $t \in [0, 1], \mu_t$ is a quasi-hyperideal of H. We show that $(\mu \circ 1) \cap (1 \circ \mu) \subseteq \mu$. Let $a \in H$. If $A_a = \emptyset$, then it is clear that $\min\{(\mu \circ 1)(a), (1 \circ \mu)(a)\} \leqslant \mu(a)$. If $A_a \neq \emptyset$, then there exist $x, y \in H$ such that $a \leqslant x \circ y$. Let $t_0 = \min\{\mu(x), \mu(y)\}$. Since μ_{t_0} is a quasi-hyperideal, $a \leqslant x \circ y$ and $x, y \in \mu_{t_0}$, we have $a \in (\mu_{t_0} \circ H] \cap (H \circ \mu_{t_0}] \subseteq \mu_{t_0}$. Then, $\mu(a) \geqslant t_0$. This means $\mu(a) \geqslant \min\{\mu(x), \mu(y)\}$ for all $(x, y) \in A_a$. Now, we have:

$$\begin{aligned}((\mu \circ 1) \cap (1 \circ \mu))(a) &= \min\{(\mu \circ 1)(a), (1 \circ \mu)(a)\} \\ &= \min\{\sup_{(x,y) \in A_a} \{\min\{\mu(x), 1(y)\}\}, \sup_{(x,y) \in A_a} \{\min\{1(x), \mu(y)\}\}\}\end{aligned}$$

$$\begin{aligned} &= \min\{\sup_{(x,y)\in A_a}\{\mu(x)\}, \sup_{(x,y)\in A_a}\{\mu(y)\}\} \\ &= \sup_{(x,y)\in A_a}\{\min\{\mu(x),\mu(y)\}\} \\ &\leqslant \mu(a). \end{aligned}$$

Thus, $(\mu\circ 1)\cap(1\circ\mu)\subseteq\mu$. Let $a, b\in H$ with $a\leqslant b$. Since $a\leqslant b, b\in\mu_{\mu(b)}$ and $\mu_{\mu(b)}$ is a quasi-hyperideal of H, we get $a\in\mu_{\mu(b)}$. So, $\mu(b)\leqslant\mu(a)$. Therefore, μ is a qausi-hyperideal of H. □

Corollary 3.11. *Let $(H,\circ,\leqslant)$ be an ordered semihypergroup and χ_I be the characteristic function of I. Then, I is a qausi-hyperideal of H if and only if χ_I is a fuzzy quasi-hyperideal of H.* □

Example 3.12. Consider the ordered semihypergroup $(H,\circ,\leqslant)$ defined in Example 2.5. Define fuzzy subsets μ and ν of H by letting $x\in H$,

$$\mu(x)=\begin{cases} 0.7 & \text{if} \quad x=a, \\ 0.5 & \text{if} \quad x=b,d, \\ 0.3 & \text{if} \quad x=c,e, \end{cases} \qquad \nu(x)=\begin{cases} 0.8 & \text{if} \quad x=a, \\ 0.6 & \text{if} \quad x=c, \\ 0.2 & \text{if} \quad x=b,d,e. \end{cases}$$

By Lemma 3.5, μ is a fuzzy left hyperideal of H, since every non-empty level subset of μ is a left hyperideal of H. Similarly, by Lemma 3.8, ν is a fuzzy bi-hyperideal of H. □

Example 3.13. Consider the ordered semihypergroup $(H,\circ,\leqslant)$ defined in Example 2.6. Define a fuzzy subset $\rho: H\to[0,1]$ by letting $x\in H$,

$$\rho(x)=\begin{cases} 0.9 & \text{if} \quad x=a \\ 0.8 & \text{if} \quad x=c \\ 0.5 & \text{if} \quad x=d \\ 0 & \text{if} \quad x=b,e. \end{cases}$$

By Lemma 3.10, ρ is a fuzzy quasi-hyperideal of H, since every non-empty level subset of ρ is a quasi-hyperideal of H. □

Theorem 3.14. *Let $(H,\circ,\leqslant)$ be an ordered semihypergroup. Then, every fuzzy right (resp. left) hyperideal of H is a fuzzy quasi-hyperideal of H.*

Proof. Let μ be a fuzzy right hyperideal of H and $a\in H$. We have

$$((\mu\circ 1)\cap(1\circ\mu))(a)=\min\{(\mu\circ 1)(a),(1\circ\mu)(a)\}.$$

If $A_a=\emptyset$, then it is clear that $\min\{(\mu\circ 1)(a),(1\circ\mu)(a)\}\subseteq\mu$.

Let $A_a\neq\emptyset$. Let $(x,y)\in A_a$. We have $a\leqslant x\circ y$. This means $a\leqslant z$ for some $z\in x\circ y$. Since μ is a fuzzy right hyperideal of H, $\mu(a)\geqslant\mu(z)\geqslant\inf_{z\in x\circ y}\{\mu(z)\}\geqslant$

$\mu(x)$. It follows

$$\begin{aligned}\mu(a) &\geqslant \sup_{a\leqslant x\circ y}\{\mu(x)\}\\ &= \sup_{(x,y)\in A_a}\{\min\{\mu(x),1(y)\}\} = (\mu\circ 1)(a)\\ &\geqslant \min\{(\mu\circ 1)(a),(1\circ\mu)(a)\}\\ &= ((\mu\circ 1)\cap(1\circ\mu))(a).\end{aligned}$$

Therefore, μ is a fuzzy quasi-hyperideal of H. □

Theorem 3.15. *Let $(H,\circ,\leqslant)$ be an ordered semihypergroup. Then, every fuzzy quasi-hyperideal of H is a fuzzy bi-hyperideal of H.*

Proof. Let μ be a fuzzy quasi-hyperideal of H and $x,y,z\in H$. We show that $\min\{\mu(x),\mu(z)\}\leqslant \inf\limits_{a\in x\circ y\circ z}\{\mu(a)\}$. Since $a\in x\circ y\circ z\leqslant x\circ(y\circ z)$, we obtain

$$(\mu\circ 1)(a) = \sup_{(u,v)\in A_a}\{\min\{\mu(u),1(v)\}\}\geqslant \min\{\mu(x),1(w)\} = \mu(x),\quad \forall w\in y\circ z.$$

Since $a\in x\circ y\circ z\leqslant (x\circ y)\circ z$, we obtain

$$(1\circ\mu)(a) = \sup_{(u,v)\in A_a}\{\min\{1(u),\mu(v)\}\}\geqslant \min\{1(t),\mu(z)\} = \mu(z),\quad \forall t\in x\circ y.$$

By assumption, we have

$$\mu(a)\geqslant ((\mu\circ 1)\cap(1\circ\mu))(a) = \min\{(\mu\circ 1)(a),(1\circ\mu)(a)\}.$$

Hence,

$$\inf_{a\in x\circ y\circ z}\{\mu(a)\}\geqslant \min\{(\mu\circ 1)(a),(1\circ\mu)(a)\}\geqslant \min\{\mu(x),\mu(z)\}.$$

Therefore, μ is a bi-hyperideal of H. □

An ordered semihypergroup $(H,\circ\leqslant)$ is called *regular*, if for every $a\in H$, there exists $x\in H$ such that $a\leqslant a\circ x\circ a$.

Theorem 3.16. *Let $(H,\circ,\leqslant)$ be a regular ordered semihypergroup and μ is a fuzzy subset of H. Then, μ is a fuzzy quasi-hyperideal if and only if μ is a fuzzy bi-hyperideal.*

Proof. Let μ is a fuzzy bi-hyperideal. We show that μ is a fuzzy quasi-hyperideal of H, i.e., $(\mu\circ 1)\cap(1\circ\mu)\subseteq\mu$.

Let $a\in H$. If $A_a=\emptyset$, then it is clear that $((\mu\circ 1)\cap(1\circ\mu))(a)\leqslant\mu(a)$.

If $A_a\neq\emptyset$, then

$$(\mu\circ 1)(a) = \sup_{(x,y)\in A_a}\{\min\{\mu(x),1(y)\} \text{ and } (1\circ\mu)(a) = \sup_{(u,v)\in A_a}\{\min\{1(u),\mu(v)\}.$$

If $(\mu\circ 1)(a)\leqslant\mu(a)$, then $\mu(a)\geqslant((\mu\circ 1)\cap(1\circ\mu))(a)$.

If $(\mu\circ 1)(a)>\mu(a)$, then there exists $(x,y)\in A_a$ such that $\min\{\mu(x),1(y)\}=\mu(x)>\mu(a)$. We claim that $(1\circ\mu)(a)\leqslant\mu(a)$. Let $(u,v)\in A_a$. Since H is regular, there exists $w\in H$ such that $a\leqslant a\circ w\circ a$. It turns out $a\leqslant x\circ y\circ w\circ u\circ v$, i.e., there exists $b\in x\circ y\circ w\circ u\circ v$ such that $a\leqslant b$. Since μ is a fuzzy bi-hyperideal of H,

$$\mu(a)\geqslant\mu(b)\geqslant\inf_{c\in x\circ y\circ w\circ u\circ v}\{\mu(c)\}\geqslant\min\{\mu(x),\mu(v)\}.$$

If $\min\{\mu(x),\mu(v)\}=\mu(x)$, then $\mu(a)\geqslant\mu(x)$. This gives a contradiction. Then, $\min\{\mu(x),\mu(v)\}=\mu(v)$ and so $\mu(a)\geqslant\mu(v)=\min\{1(u),\mu(v)\}$ for all $(u,v)\in A_a$. Hence, $\mu(a)\geqslant\sup\limits_{(u,v)\in A_a}\min\{1(u),\mu(v)\}=(1\circ\mu)(a)$. Now, the claim was proved. Therefore, $\min\{(\mu\circ 1)(a),(1\circ\mu)(a)\}\leqslant\mu(a)$, i.e., $(\mu\circ 1)\cap(1\circ\mu)\subseteq\mu$. □

Lemma 3.17. *Let $(H,\circ,\leqslant)$ be an ordered semihypergroup and μ a fuzzy subset of H such that $\mu(a)\geqslant\mu(b)$ for every $a,b\in H$ with $a\leqslant b$. Then,*

(1) *$\mu\cup(1\circ\mu)$ is a fuzzy left hyperideal of H,*

(2) *$\mu\cup(\mu\circ 1)$ is a fuzzy right hyperideal of H.*

Proof. (1) Let $a,b\in H$ and $c\in a\circ b$. We have

$$\begin{aligned}(\mu\cup(1\circ\mu))(c)&=\max\{\mu(c),(1\circ\mu)(c)\}\\ &\geqslant(1\circ\mu)(c)=\sup_{(x,y)\in A_c}\{\min\{1(x),\mu(y)\}\}=\sup_{(x,y)\in A_c}\{\mu(y)\}\\ &\geqslant\mu(b),\quad(\text{ since } c\in a\circ b \text{ and then } (a,b)\in A_c).\end{aligned}$$

Next, we show that $(1\circ\mu)(c)\geqslant(1\circ\mu)(b)$. Let $A_b\neq\emptyset$ and $(r,s)\in A_b$. Since $(a,b)\in A_c$, we have

$$\begin{aligned}(r,s)\in A_b&\Rightarrow b\leqslant r\circ s\\ &\Rightarrow a\circ b\leqslant(a\circ r)\circ s\\ &\Rightarrow c\leqslant(a\circ r)\circ s\\ &\Rightarrow c\leqslant t\circ s,\qquad\text{for some } t\in a\circ r.\end{aligned}$$

We have $(1\circ\mu)(c)\geqslant\min\{1(t),\mu(s)\}=\mu(s)=\min\{1(r),\mu(s)\}$. Thus, $(1\circ\mu)(c)\geqslant\sup\limits_{(r,s)\in A_b}\{\min\{1(r),\mu(s)\}\}=(1\circ\mu)(b)$ and then $(\mu\cup(1\circ\mu)(c)\geqslant(1\circ\mu)(b)$. This implies $\inf\limits_{c\in a\circ b}\{(\mu\cup(1\circ\mu))(c)\}\geqslant(\mu\cup(1\circ\mu))(b)$. Next, we show that for any $a,b\in H$ and $a\leqslant b$ implies $(\mu\cup(1\circ\mu))(a)\geqslant(\mu\cup(1\circ\mu))(b)$. Since $A_a\supseteq A_b$, we have $(1\circ\mu)(a)\geqslant(1\circ\mu)(b)$. Then, $\max\{\mu(a),(1\circ\mu)(a)\}\geqslant\max\{\mu(b),(1\circ\mu)(b)\}$. This means $(\mu\cup(1\circ\mu)(a)\geqslant(\mu\cup(1\circ\mu)(b)$. Altogether, $\mu\cup(1\circ\mu)$ is a fuzzy left hyperideal of H.

(2) It can be proved similarly. □

Similarly to Corollary 1 in [10], we have the following lemma.

Lemma 3.18. *If H is an ordered semihypergroup, then the set of all fuzzy subsets of H is a distributive lattice.* □

Now, we show that every fuzzy quasi-hyperideal is exactly an intersection of a fuzzy right hyperideal and a fuzzy left hyperideal and vice versa.

Theorem 3.19. *Let $(H, \circ, \leqslant)$ be an ordered semihypergroup and μ a fuzzy subset of H. Then, μ is a fuzzy quasi-hyperideal of H if and only if there exist a fuzzy right hyperideal ν and a fuzzy left hyperideal ρ of H such that $\mu = \nu \cap \rho$.*

Proof. By Lemma 3.17 and Lemma 3.18, we have $\mu = (\mu \cup (1 \circ \mu)) \cap (\mu \cup (\mu \circ 1))$. Conversely, let ν be a fuzzy right hyperideal and ρ be a fuzzy left hyperideal of H such that $\mu = \nu \cap \rho$. We show that μ is a fuzzy quasi-hyperideal of H. Let $a \in H$. If $A_a = \emptyset$, then it is clear that $((\mu \circ 1) \cap (1 \circ \mu)) \subseteq \mu$. Let $A_a \neq \emptyset$ and $(x, y) \in A_a$. We have $a \leqslant x \circ y$. Then, there exists $b \in x \circ y$ such that $a \leqslant b$. Since ν is a fuzzy right hyperideal of H and $\mu = \nu \cap \rho$, we have $\nu(a) \geqslant \nu(b) \geqslant \inf\limits_{c \in x \circ y} \{\nu(c)\} \geqslant \nu(x) \geqslant \mu(x)$. Now, we have $\nu(a) \geqslant \mu(x)$ for all $(x, y) \in A_a$. Hence,

$$(\mu \circ 1)(a) = \sup_{(x,y) \in A_a} \{\min\{\mu(x), 1(y)\}\} = \sup_{(x,y) \in A_a} \{\min\{\mu(x)\}\} \leqslant \nu(a).$$

Similarly, we can show that $(1 \circ \mu)(a) \leqslant \rho(a)$. Thus,

$$\begin{aligned} ((\mu \circ 1) \cap (1 \circ \mu))(a) &= \min\{(\mu \circ 1)(a), (1 \circ \mu)(a)\} \\ &\leqslant \min\{\nu(a), \rho(a)\} \\ &= (\nu \cap \rho)(a) = \mu(a). \end{aligned}$$

Therefore, μ is a fuzzy quasi-hyperideal of H. □

Acknowledgments. This work has been supported by Khon Kaen University under Incubation Researcher Project.

References

[1] **P. Bonansinga and P. Corsini**, *On semihypergroup and hypergroup homomorphisms*, Boll. Un. Mat. Ital. B (6) **1(2)** (1982), 717 – 727.

[2] **P. Corsini, M. Shabir and T. Mahmood**, *Semisimple semihypergroups in terms of hyperideals and fuzzy hyperideals*, Iran. J. Fuzzy Syst. **8** (2011), 95 – 111.

[3] **B. Davvaz**, *Fuzzy hyperideals in semihypergroups*, Italian J. Pure and Appl. Math. **8** (2000), 67 – 74.

[4] **B. Davvaz**, *Some results on congruences in semihypergroups*, Bull. Malays. Math. Sci. So.(2) **23** (2000), 53 – 58.

[5] **B. Davvaz**, *Characterizations of sub-semihypergroups by various triangular norms*, Czech. Math. J. **55(4)** (2005), 923 – 932.

[6] **M. De Salvo, D. Freni and G. Lo Faro**, *Fully simple semihypergroups*, J. Algebra **399** (2014), 358 – 377.

[7] **D. Freni**, *Minimal order semihypergroups of type U on the right, II*, J. Algebra **340** (2011), 77 – 89.

[8] **D. Heidari and B. Davvaz**, On ordered hyperstructures, U.P.B. Sci. Bull. Series A **73** (2011), 85 – 96.

[9] **K. Hila, B. Davvaz and K. Naka**, *On quasi-hyperideals in semihypergroups*, Commun. Algebra **39** (2011), 4183 – 4194.

[10] **N. Kehayopulu and M. Tsingelis**, *Fuzzy ideals in ordered semigroups*, Quasigroups and Related Systems **15** (2007), 279 – 289.

[11] **N. Kehayopulu and M. Tsingelis**, *Fuzzy right, left, quasi-ideals, bi-ideals in ordered semigroups*, Lobachevskii J. Math. **30(1)** (2009), 17 – 22.

[12] **A. Khan, N. H. Sarmin, B. Davvaz and F.M. Khan**, *New types of fuzzy bi-ideals in ordered semigroups*, Neural Comput. Appl. **21** (2012), 295 – 305.

[13] **F. Marty**, *Sur une generalization de la notion de groupe*, 8th Congress Math. Scandinaves, Stockholm (1934), 45 – 49.

[14] **V. Leoreanu**, *About the simplifiable cyclic semihypergroups*, Italian J. Pure Appl. Math. **7** (2000), 69 – 76.

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

[16] **J. Tang and X. Xie**, *On fuzzy quasi-ideals of ordered semigroups*, J. Math. Research Appl. **32** (2012), 589 – 598.

Received December 16, 2014
Revised April 7, 2015

B. Pibaljommee, K. Wannatong
Department of Mathematics Faculty of Science
Khon Kaen University Thailand
E-mail: banpib@kku.ac.th, kantapong_w@kkumail.com

B. Davvaz
Department of Mathematics, Yazd University, Yazd, Iran
E-mail: davvaz@yazd.ac.ir

Quasigroups and Related Systems **23** (2015), 309 − 317

Free semiabelian n-ary groups

Nikolay A. Shchuchkin

Abstract. Free n-ary groups in the class of semiabelian n-ary groups are described.

1. Introduction

The non-empty set G together with an n-ary operation $f : G^n \to G$ is called an *n-ary groupoid* (or an *n-ary operative* – in the Gluskin terminology, cf. [10]) and is denoted by $\langle G, f\rangle$. We will assume that $n \geqslant 2$.

According to the general convention used in the theory of such groupoids we will use the following abbreviated notation:

$$f(x_1,\dots,x_i,\underbrace{x,\dots,x}_{t},x_{i+t+1},\dots,x_n)=f(x_1^i,\overset{(t)}{x},x_{i+t+1}^n),$$

$$f_{(k)}(x_1^{k(n-1)+1})=\underbrace{f(f(\dots,f(f}_{k}(x_1^n),x_{n+1}^{2n-1}),\dots),x_{(k-1)(n-1)+2}^{k(n-1)+1}),$$

where $\overset{(0)}{x}$ and x_i^j for $i>j$ are empty symbols. In certain situations, when the arity of the operation $f_{(k)}$ does not play a crucial role or when it will differ depending on additional assumptions, we will write $f_{(.)}$ instead of $f_{(k)}$.

The algebra $\langle G, f\rangle$ is called an *n-ary group* if it satisfies the *generalized associative law*:

$$f(x_1^{i-1},f(x_i^{n+i-1}),x_{n+i}^{2n-1})=f(x_1^{j-1},f(x_j^{n+j-1}),x_{n+j}^{2n-1}) \tag{1}$$

and for all $a_1,\dots,a_{j-1},a_{j+1},\dots,a_n,b\in G$ the equation

$$f(a_1,\dots,a_{j-1}x_j,a_{j+1},\dots,a_n)=b$$

is uniquely solvable for each $j=1,\dots,n$. Other equivalent definitions of n-ary groups one can find in [4] and [5].

For $n=2$ we obtain usual (binary) groups. Thus n-ary groups are a generalization of groups.

Initial investigations of n-ary groups were presented in [2], [15] and [20]. The necessity for such research is explained in the Kurosh's book [13].

2010 Mathematics Subject Classification: 20N15

Keywords: n-ary group, semiabelian n-ary group, free n-ary group.

The theory of n-ary groups differs from the theory of ordinary groups. This is stipulated, for example, by absence of neutral elements. Therefore the invertibility is also absent. Instead of this in n-ary groups is considered the *skew element* defined as a solution of the equation $f(a,\ldots,a,x)=a$. It is denoted by $\bar{a}$ and is called the *skew element* for a. Since for each $a\in G$ it is uniquely defined we have the map $^{-}\colon x\to\bar{x}$. Thus any n-ary group $\langle G,f\rangle$ may be considered as an algebra $\langle G,f,^{-}\rangle$ in which the generalized associative law (1) and the identities

$$f(y,x,\ldots,x,\bar{x},x)=f(x,\bar{x},x,\ldots,x,y)=y. \tag{2}$$

are fulfilled (for details see [3], [4] and [5]).

An n-ary group $\langle G,f\rangle$ is called *semiabelian* if

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

and *abelian* or *commutative* if $f(x_1,\ldots,x_n)=f(x_{\sigma(1)},\ldots,x_{\sigma(n)})$ is valid for all $x_1,\ldots,x_n\in G$ and all $\sigma\in S_n$. An n-ary group is semiabelian $\langle G,f\rangle$ if and only if $f(x,a,\ldots,a,y)=f(y,a,\ldots,a,x)$ for some $a\in G$ and all $x,y\in G$ (cf. [3]).

Note that in semiabelian n-ary groups the map$^{-}\colon x\to\bar{x}$ is an endomorphism (cf. [4]), but it is an endomorphism also in some n-ary groups which are not semiabelian (cf. [8]).

The class of all n-ary groups considered as algebras of the form $\langle G,f,^{-}\rangle$ forms a variety determined by (1) and (2). Free n-ary groups in this class are described in [1]. Free n-ary groups in the class of all abelian n-ary groups were investigated in [19], [17] and [18]. The description of structure of free n-ary groups in class of abelian semicyclic (precyclic) n-ary groups one can find in [14].

In this paper we describe the structure of free n-ary groups in class of semiabelian n-ary groups.

2. Some facts on semiabelian n-ary groups

There is a close relationship between binary (i.e., classical) and n-ary groups. For example, on any semiabelian n-ary group $\langle G,f\rangle$ the abelian group $\langle G,+\rangle$ may be defined by putting $a+b=f(a,c,\ldots,c,\bar{c},b)$ for fixed element c from G. Then (cf. [10], [11]) for the element $d=f(c,\ldots,c)$ and for the map $\varphi(x)=f(c,x,c,\ldots,c,\bar{c})$, which is an automorphism of the group $\langle G,+\rangle$, we obtain

$$\varphi(d)=d, \qquad \varphi^{n-1}(x)=x \ \text{ for any } x\in G, \ \text{ and} \tag{3}$$

$$f(a_1,\ldots,a_n)=a_1+\varphi(a_2)+\ldots+\varphi^{n-2}(a_{n-1})+a_n+d. \tag{4}$$

It is easily to see that c is a zero of the group $\langle G,+\rangle$, and $-a=f(c,a,\ldots,a,\bar{a},c)$. Moreover,

$$\varphi^s(x)=f(\overset{(s)}{c},x,\overset{(n-2-s)}{c},\bar{c}). \tag{5}$$

Since $f(x,\ldots,x,\bar{x}) = x$, from (4) we get $x + \varphi(x) + \ldots + \varphi^{n-2}(x) + \bar{x} + d = x$. Thus, $\bar{x} = -\varphi(x) - \ldots - \varphi^{n-2}(x) - d$, and consequently,

$$\begin{aligned}
\varphi^s(\bar{x}) &= \varphi^s(-\varphi(x) - \ldots - \varphi^{n-2}(x) - d) = -\varphi^s(\varphi(x)) - \ldots - \varphi^s(\varphi^{n-2}(x)) - \varphi^s(d) \\
&= -\varphi^{s+1}(x) - \ldots - \varphi^{n-2}(x) - x - \varphi(x) - \ldots - \varphi^{s-1}(x) - d \\
&= -\varphi^{s+1}(x) - \ldots - \varphi^{n-2}(x) - \varphi(x) - \ldots - \varphi^{s-1}(x) - \varphi^s(x) - d - x + \varphi^s(x) \\
&= \bar{x} - x + \varphi^s(x).
\end{aligned}$$

Hence

$$\varphi^s(\bar{x}) = \bar{x} - x + \varphi^s(x). \tag{6}$$

The group $\langle G,+\rangle$ is called the *retract* of an n-ary group $\langle G,f\rangle$ and is denoted by $ret_c\langle G,f\rangle$. Two retracts of the same n-ary group are isomorphic (cf. [6]). For an abelian n-ary group $\langle G,f\rangle$ the automorphism φ is the identity map.

The converse is also true: if $\langle G,+\rangle$ is an abelian group, φ its automorphism such that for some $d \in G$ the conditions (3) are satisfied, then $\langle G,f\rangle$ with the operation defined by (4) is a semiabelian n-ary group. Such obtained an n-ary group $\langle G,f\rangle$ is called (φ,d)-*derived* from the group $\langle G,+\rangle$ and is denoted by $der_{\varphi,d}\langle G,+\rangle$. In the case $\varphi = 1_G$, $d = 0$ we say that an n-ary group $der_{\varphi,d}\langle G,+\rangle$ is *derived* from the group $\langle G,+\rangle$.

One can prove (cf. [6]) that

$$\langle G,+\rangle = ret_c der_{\varphi,d}\langle G,+\rangle, \qquad \langle G,f\rangle = der_{\varphi,d} ret_c\langle G,f\rangle. \tag{7}$$

An n-ary group with a cyclic retract is called *semicyclic* [16] or *precyclic* [8]. A semicyclic n-ary group $\langle (a),f\rangle$ which is (φ,d)-derived from the cyclic group $\langle (a),+\rangle$ of order k has the form $der_{m,la}\langle (a),+\rangle$, i.e.,

$$f(s_1a,\ldots,s_na) = (s_1 + s_2m + s_3m^2 \ldots + s_{n-1}m^{n-2} + s_n + l)a,$$

where $0 \leqslant m,l < k$, m and k are relatively prime, $lm \equiv l \pmod{k}$ and $m|n-1$. Any finite semicyclic n-ary group of order k is isomorphic to an n-ary group $\langle (a),f\rangle = der_{m,la}\langle (a),+\rangle$, where $l|\gcd(1 + m + m^2 + \ldots + m^{n-2}, k)$ (see [16]).

Using the basic idea of [7], the structure of homomorphisms of n-ary groups was investigated in [12]. We need the special case of Theorem 1.2 from [12].

Theorem 2.1. *Let $\langle G,f\rangle = der_{\varphi,d}\langle G,+\rangle$ and $\langle H,h\rangle = der_{\mu,b}\langle H,\oplus\rangle$ be two semiabelian n-ary groups and $\psi : \langle G,f\rangle \to \langle H,h\rangle$ be a homomorphism. Then there exists $a \in H$ and a group homomorphism $\sigma : \langle G,+\rangle \to \langle H,\oplus\rangle$ such that $\psi(x) = \sigma(x) \oplus a$ for any $x \in G$. In this case*

$$h(a,\ldots,a) = \sigma(d) \oplus a \quad \text{and} \quad \sigma \circ \varphi = \mu \circ \sigma.$$

Moreover, if a and σ satisfy these two conditions, then $\psi(x) = \sigma(x) \oplus a$ is a homomorphism $\langle G,f\rangle \to \langle H,h\rangle$.

3. Generating sets of semiabelian n-ary groups

It is not difficult to see that

$$\overline{f(x_1^n)} = f_{(\cdot)}(\underbrace{\overset{(n-3)}{x_n}, \bar{x}_n, \ldots, \overset{(n-3)}{x_1}, \bar{x}_1}_{n-2}), \quad \bar{\bar{x}} = f_{(n-3)}(x, \ldots, x).$$

Theorem 3.1. *If a semiabelian n-ary group $\langle G, f\rangle$ is generated by the set $X = \{x_\alpha | \alpha \in I\}$, then its retract $ret_{x_\beta}\langle G, f\rangle$ is generated by the set*

$$Y = \left\{ f(\overset{(i-1)}{x_\beta}, x_\alpha, \overset{(n-i-1)}{x_\beta}, \bar{x}_\beta) \,|\, x_\alpha \in X\backslash\{x_\beta\},\ i = 1, \ldots, n-1 \right\} \cup \left\{ f(\overset{(n)}{x_\beta}) \right\}.$$

Proof. Let $\langle G, +\rangle = ret_{x_\beta}\langle G, f\rangle$ for some $x_\beta \in X$. Then x_β is a zero of $\langle G, +\rangle$ and (3) is valid for $d = f(\overset{(n)}{x_\beta})$ and $\varphi(x) = f(x_\beta, x, \overset{(n-3)}{x_\beta}, \bar{x}_\beta)$.

Denote by B the subset of $\langle G, +\rangle$ generated (in $\langle G, +\rangle$) by Y. Obviously $d \in Y$. So, also $-d, x_\beta \in B$. We will show that $B = G$.

First observe that $\varphi^s(x_\alpha) \in Y \subseteq B$ for every $s = 1, \ldots, n-1$ and $x_\alpha \in X\backslash\{x_\beta\}$. For x_β we obtain $\varphi^s(x_\beta) = x_\beta \in B$. Since $\bar{x}_\alpha = -\varphi(x_\alpha) - \ldots - \varphi^{n-2}(x_\alpha) - d$, by (2) and (4), we see that $\varphi^s(\bar{x}_\alpha) \in B$ for every $x_\alpha \in X$.

Now consider an arbitrary element $g \in G$. By our assumption each element $g \in G$ has the form $g = f_{(k)}(y_{\alpha_1}, \ldots, y_{\alpha_m})$, where $m = k(n-1)+1$, $y_{\alpha_i} = x_{\alpha_i}$ or $y_{\alpha_i} = \bar{x}_{\alpha_i}$, $x_{\alpha_i} \in X$, $i = 1, \ldots, m$. This, according to (4), means that each element g of G can be written in the form

$$g = y_{\alpha_1} + h_0 + \varphi(h_1) + \varphi^2(h_2) + \ldots + \varphi^{n-2}(h_{n-2}) + h_{n-1} + d,$$

where

$$h_j = y_{\alpha_{j(n-1)+2}} + \varphi(y_{\alpha_{j(n-1)+3}}) + \ldots + \varphi^{n-2}(y_{\alpha_{j(n-1)+n-1}}) + y_{\alpha_{j(n-1)+n}} + d$$

and $j = 0, 1, \ldots, k-1$. Since x_β is a zero of $\langle G, +\rangle$, each y_j, and consequently, g depends only on $x_\alpha, \bar{x}_\alpha$ and $\bar{x}_\beta$. But $\bar{x}_\beta = -d$ and $d \in Y$. Thus g depends only on d and $x_\alpha \in X\backslash\{x_\beta\}$. Therefore Y generates G, so $B = G$. □

Corollary 3.2. *If a semiabelian n-ary group $\langle G, f\rangle$ is generated by the set $X = \{x_\alpha | \alpha \in I\}$, then the retract $ret_c\langle G, f\rangle$ is generated by the set*

$$\left\{ f(f(\overset{(i-1)}{x_\beta}, x_\alpha, \overset{(n-i-1)}{x_\beta}, \bar{x}_\beta), \overset{(n-3)}{c}, \bar{c}, x_\beta) \,|\, x_\alpha \in X\backslash\{x_\beta\}, 1 \leqslant i \leqslant n-1 \right\} \cup$$
$$\left\{ f(f(\overset{(n)}{x_\beta}), \overset{(n-3)}{c}, \bar{c}, x_\beta) \right\},$$

where x_β is an arbitrary fixed element of X.

Proof. It is not difficult to see that the map $\sigma : ret_{x_\beta}\langle G, f\rangle \to ret_c\langle G, f\rangle$ defined by $\sigma(x) = f(x, \overset{(n-3)}{c}, \bar{c}, x_\beta)$ is an isomorphism of retracts which transfers generators of $red_{x_\beta}\langle G, f\rangle$ onto generators of $red_c\langle G, f\rangle$. □

Theorem 3.3. *If an abelian group $\langle G, +\rangle$ is generated by the set $Z = \{z_\alpha | \alpha \in I\}$, then a semiabelian n-ary group $\langle G, f\rangle = der_{\varphi,d}\langle G, +\rangle$ is generated by the set $X = \{-d + z_\alpha \mid \alpha \in I\} \cup \{0\}$.*

Proof. In this case $a + b = f(a, \overset{(n-3)}{0}, \bar{0}, b)$, $\varphi(x) = f(0, x, \overset{(n-3)}{0}, \bar{0})$, $d = f(\overset{(n)}{0})$ and $-d = \bar{0}$. Thus $z_{\alpha_i} = f(\overset{(n-1)}{0}, -d + z_{\alpha_i})$. Moreover, for $n_i > 0$ we obtain

$$\begin{aligned} n_i z_{\alpha_i} &= f_{(n_i-1)}(z_{\alpha_i}, \overset{(n-3)}{0}, \bar{0}, z_{\alpha_i}, \overset{(n-3)}{0}, \bar{0}, \ldots, z_{\alpha_i}, \overset{(n-3)}{0}, \bar{0}, z_{\alpha_i}) \\ &= f_{(n_i-1)}(f(\overset{(n-1)}{0}, -d + z_{\alpha_i}), \overset{(n-3)}{0}, \bar{0}, \ldots, \overset{(n-3)}{0}, \bar{0}, f(\overset{(n-1)}{0}, -d + z_{\alpha_i})). \end{aligned}$$

Since

$$\begin{aligned} -d+z_{\alpha_i} &= f(-d + z_{\alpha_i}, \overline{-d + z_{\alpha_i}}, \overset{(n-2)}{-d + z_{\alpha_i}}) \\ &= -d+z_{\alpha_i}+\varphi(\overline{-d+z_{\alpha_i}})+\varphi^2(-d+z_{\alpha_i})+ \ldots +\varphi^{n-2}(-d+z_{\alpha_i})-d + z_{\alpha_i}+d, \end{aligned}$$

we have

$$\begin{aligned} -z_{\alpha_i} &= \varphi(\overline{-d + z_{\alpha_i}}) + \varphi^2(-d + z_{\alpha_i}) + \ldots + \varphi^{n-2}(-d + z_{\alpha_i}) \\ &= -d + \varphi(\overline{-d + z_{\alpha_i}}) + \varphi^2(-d + z_{\alpha_i}) + \ldots + \varphi^{n-2}(-d + z_{\alpha_i}) + 0 + d \\ &= f(-d, \overline{-d + z_{\alpha_i}}, \overset{(n-3)}{-d + z_{\alpha_i}}, 0) = f(\bar{0}, \overline{-d + z_{\alpha_i}}, \overset{(n-3)}{-d + z_{\alpha_i}}, 0). \end{aligned}$$

Thus, for $n_i < 0$ we have

$$\begin{aligned} n_i z_{\alpha_i} &= (-n_i)(-z_{\alpha_i}) = f_{(-n_i-1)}(-z_{\alpha_i}, \overset{(n-3)}{0}, \bar{0}, -z_{\alpha_i}, \overset{(n-3)}{0}, \bar{0}, \ldots, -z_{\alpha_i}, \overset{(n-3)}{0}, \bar{0}, -z_{\alpha_i}) \\ &= f_{(-n_i-1)}(f(\bar{0}, \overline{-d+z_{\alpha_i}}, \overset{(n-3)}{-d+z_{\alpha_i}}, 0), \overset{(n-3)}{0}, \bar{0}, f(\bar{0}, \overline{-d+z_{\alpha_i}}, \overset{(n-3)}{-d+z_{\alpha_i}}, 0), \overset{(n-3)}{0}, \bar{0}, \\ &\qquad \ldots, f(\bar{0}, \overline{-d+z_{\alpha_i}}, \overset{(n-3)}{-d+z_{\alpha_i}}, 0), \overset{(n-3)}{0}, \bar{0}, f(\bar{0}, \overline{-d+z_{\alpha_i}}, \overset{(n-3)}{-d+z_{\alpha_i}}, 0)). \end{aligned}$$

Hence, in any case $n_i z_{\alpha_i}$ can be expressed in $\langle G, f\rangle = der_{\varphi,d}\langle G, +\rangle$ by elements of X. Since each element of G has the form $g = n_1 z_{\alpha_1} + \ldots + n_k z_{\alpha_k}$, the above means that an n-group $\langle G, f\rangle = der_{\varphi,d}\langle G, +\rangle$is generated by X. □

4. Structure of free semiabelian n-ary groups

Let $\mathfrak{K}$ be the class of n-ary groups. An n-ary group $\langle F, f\rangle$ from $\mathfrak{K}$ is *free* in $\mathfrak{K}$ with the set X of *free generators* if any map ψ_0 of X to any n-ary group $\langle B, f\rangle$ from the class $\mathfrak{K}$ can be uniquely extended to a homomorphism $\psi : \langle F, f\rangle \to \langle B, f\rangle$.

Denote by C_l, where $0 \leqslant l \leqslant [\frac{n-1}{2}]$, the class of all abelian semicyclic n-ary groups $(1, la)$-derived from cyclic groups. An abelian semicyclic n-ary group constructed on a cyclic group $\langle (a), +\rangle$ of order k has the form $der_{1,l_1a}\langle (a), +\rangle$, where $0 \leqslant l_1 \leqslant k-1$. By Lemma 1 in [9], n-ary groups $der_{1,l_1a}\langle (a), +\rangle$ and $der_{1,l_2a}\langle (a), +\rangle$ of order k are isomorphic if and only if $\gcd(l_1, n-1, k) = \gcd(l_2, n-1, k)$. So, an n-ary group $der_{1,l_1a}\langle (a), +\rangle$ is isomorphic to an n-ary group $der_{1,l_2a}\langle (a), +\rangle$, where $\gcd(l_1, n-1, k) = l_2$. If $l_2 = n-1$, then $der_{1,l_2a}\langle (a), +\rangle \cong der_{1,0}\langle (a), +\rangle$. Thus, $der_{1,l_1a}\langle (a), +\rangle \in C_0$. If $l_2 < n-1$, then $1 \leqslant l_2 \leqslant [\frac{n-1}{2}]$ which means that $der_{1,l_1a}\langle (a), +\rangle \in C_{l_2}$. If $der_{1,l_1a}\langle (a), +\rangle$ is an infinite abelian semicyclic n-ary group, then $der_{1,l_1a}\langle (a), +\rangle \cong der_{1,la}\langle (a), +\rangle$, where $0 \leqslant l \leqslant [\frac{n-1}{2}]$ (see Theorem 3 in [16]). Thus $der_{1,,l_1a}\langle (a), +\rangle \in C_l$. This shows that each abelian semicyclic n-ary group belongs only to one class C_l, where $0 \leqslant l \leqslant [\frac{n-1}{2}]$.

Each class C_l has only one (up to isomorphism) free n-ary group. It has the form $der_{1,l}Z$, where Z is the additive group of integers (see [14]).

Free n-ary groups in the class of all abelian n-ary groups are described in the following theorem proved in [18].

Theorem 4.1. *An n-ary group is free in the class of abelian n-ary groups if and only if it is an infinite cyclic n-ary group or a direct product of an infinite cyclic n-ary group and an n-ary group derived from a free abelian group.*

To describe all free n-ary groups in the class of all semiabelian n-ary groups consider the set $\{x_\alpha \,|\, \alpha \in I\}$. For each element x_α we determine the direct sum $\langle A_\alpha, +\rangle = \sum_{j=1}^{n-1}\langle (x_{\alpha j}), +\rangle$ of infinite cyclic groups $\langle (x_{\alpha j}), +\rangle$ and the direct sum $\langle F, +\rangle = \langle (a), +\rangle + \sum_{\alpha \in I}\langle A_\alpha, +\rangle$, where $\langle (a), +\rangle$ is an infinite cyclic group. On each group $\langle A_\alpha, +\rangle$ we select an automorphism φ_α such that

$$\varphi_\alpha(t_1x_{\alpha 1} + t_2x_{\alpha 2} + \ldots + t_{n-1}x_{\alpha n-1}) = t_{n-1}x_{\alpha 1} + t_1x_{\alpha 2} + \ldots + t_{n-2}x_{\alpha n-1}$$

for any $t_1x_{\alpha 1} + t_2x_{\alpha 2} + \ldots + t_{n-1}x_{\alpha n-1} \in A_\alpha$.

Then φ defined by $\varphi(sa + \sum_{i=1}^{k} z_{\alpha_i}) = sa + \sum_{i=1}^{k}\varphi_{\alpha_i}(z_{\alpha_i})$ is an automorphism of the group $\langle F, +\rangle$. Since $d = a$ and φ satisfy (3), on the group $\langle F, +\rangle$ we can construct the semiabelian n-ary group $\langle F, f\rangle = der_{\varphi,a}\langle F, +\rangle$ with the operation f defined by (4).

Proposition 4.2. *The n-ary group $\langle F, f\rangle$ is generated by the set*

$$X = \{-a + x_{\alpha 1} \,|\, \alpha \in I\} \cup \{0\}.$$

Proof. The abelian group $\langle F, +\rangle$ is generated by the set

$$Z = \{a\} \cup \{x_{\alpha 1} \,|\, \alpha \in I\} \cup \{x_{\alpha 2} \,|\, \alpha \in I\} \cup \ldots \cup \{x_{\alpha n-1} \,|\, \alpha \in I\}.$$

Thus, according to Theorem 3.3, the n-ary group $\langle F, f\rangle$ is generated by the set

$$T = \{0\} \cup \{-a + x_{\alpha 1} \,|\, \alpha \in I\} \cup \{-a + x_{\alpha 2} \,|\, \alpha \in I\} \cup \ldots \cup \{-a + x_{\alpha n-1} \,|\, \alpha \in I\}.$$

Note that for $\alpha \in I$ and $j = 2, \ldots, n-1$ we have

$$\begin{aligned} -a + x_{\alpha j} &= -a + \varphi_{\alpha}^{j-1}(x_{\alpha 1}) = \varphi^{j-1}(-a + x_{\alpha 1}) = f(\overset{(i-1)}{0}, -a + x_{\alpha 1}, \overset{(n-i-1)}{0}, \bar{0}), \\ \overline{-a + x_{\alpha j}} &= \overline{f(\overset{(i-1)}{0}, -a + x_{\alpha 1}, \overset{(n-i-1)}{0}, \bar{0})} = f(\overset{(i-1)}{\bar{0}}, \overline{-a + x_{\alpha 1}}, \overset{(n-i-1)}{\bar{0}}, \bar{\bar{0}}) \\ &= f(\overset{(i-1)}{\bar{0}}, \overline{-a + x_{\alpha 1}}, \overset{(n-i-1)}{\bar{0}}, f_{(n-3)}(\overset{((n-2)^2)}{0})). \end{aligned}$$

This completes the proof. □

Theorem 4.3. *The n-ary group $\langle F, f \rangle$ is free in the class of semiabelian n-ary groups.*

Proof. Let $\langle B, f' \rangle$ be an arbitrary semiabelian n-ary group and ψ_0 be a map of the set X into B. Let $\psi_0(0) = c$ and $\psi_0(-a + x_{\alpha 1}) = y_\alpha$ for all $\alpha \in I$. Choose in $\langle B, f' \rangle$ an n-ary subgroup $\langle G, f' \rangle$ generated by the set $Y = \{c\} \cup \{y_\alpha \,|\, \alpha \in I\}$ and consider the retract $\langle G, + \rangle = ret_c \langle G, f' \rangle$. By Theorem 3.1, this retract is generated by the set

$$U = \{f'(\overset{(i-1)}{c}, y_\alpha, \overset{(n-i-1)}{c}, \bar{c}) \,|\, \alpha \in I,\ i = 1, \ldots, n-1\} \cup \{f'(\overset{(n)}{c})\}.$$

Since $d' = f'(\overset{(n)}{c})$ and $\varphi'(x) = f'(c, x, \overset{(n-3)}{c}, \bar{c})$ satisfy (3), we see that $\langle G, f' \rangle = der_{\varphi', d'} \langle G, + \rangle$.

Moreover, the map $\sigma_0 : Z \to U$ such that $\sigma_0(a) = d'$ and

$$\sigma_0(x_{\alpha j}) = f'(\overset{(j-1)}{c}, y_\alpha, \overset{(n-j-1)}{c}, \bar{c}) + d' = {\varphi'}^{j-1}(y_\alpha) + d'$$

for all $\alpha \in I$, $j = 1, \ldots, n-1$, can be extended to the homomorphism

$$\sigma : \langle F, + \rangle \to \langle G, + \rangle$$

with the property $\sigma(0) = c$ and $\sigma(-a + x_{\alpha 1}) = -\sigma(a) + \sigma(x_{\alpha 1}) = y_\alpha$.

Let us show that σ is a homomorphism of an n-ary group $\langle F, f \rangle$ into an n-ary group $\langle B, f' \rangle$. For this consider $x = sa + \sum_{i=1}^{k} z_{\alpha_i} \in \langle F, + \rangle$, where $z_{\alpha_i} = t_{i1} x_{\alpha_i 1} + t_{i2} x_{\alpha_i 2} + \ldots + t_{in-1} x_{\alpha_i n-1}$. Then

$$\begin{aligned} \varphi' \circ \sigma(x) &= \varphi'(s\sigma(a) + \textstyle\sum_{i=1}^{k} (t_{i1}\sigma(x_{\alpha_i 1}) + t_{i2}\sigma(x_{\alpha_i 2}) + \ldots + t_{in-1}\sigma(x_{\alpha_i n-1}))) \\ &= \varphi'(sd' + \textstyle\sum_{i=1}^{k} (t_{i1}(y_{\alpha_i} + d') + t_{i2}(\varphi'(y_{\alpha_i}) + d') + \ldots + t_{in-1}({\varphi'}^{n-2}(y_{\alpha_i}) + d'))) \\ &= sd' + \textstyle\sum_{i=1}^{k} (t_{in-1}(y_{\alpha_i} + d') + t_{i1}(\varphi'(y_{\alpha_i}) + d') + \ldots + t_{in-2}({\varphi'}^{n-2}(y_{\alpha_i}) + d')). \end{aligned}$$

On the other hand

$$\begin{aligned} \sigma \circ \varphi(x) &= \sigma(sa + \textstyle\sum_{i=1}^{k} \varphi_{\alpha_i}(t_{i1} x_{\alpha_i 1} + t_{i2} x_{\alpha_i 2} + \ldots + t_{in-1} x_{\alpha_i n-1})) \\ &= \sigma(sa + \textstyle\sum_{i=1}^{k} (t_{in-1} x_{\alpha_i 1} + t_{i1} x_{\alpha_i 2} + \ldots + t_{in-2} x_{\alpha_i n-1})) \end{aligned}$$

$= s\sigma(a) + \sum_{i=1}^{k}(t_{in-1}\sigma(x_{\alpha_i 1}) + t_{i1}\sigma(x_{\alpha_i 2}) + \ldots + t_{in-2}\sigma(x_{\alpha_i n-1})))$

$= sd' + \sum_{i=1}^{k}(t_{in-1}(y_{\alpha_i} + d') + t_{i1}(\varphi'(y_{\alpha_i}) + d') + \ldots + t_{in-2}({\varphi'}^{n-2}(y_{\alpha_i}) + d'))).$

Thus $\sigma \circ \varphi(x) = \varphi' \circ \sigma(x)$ for any $x \in F$.

Since the neutral element of $\langle G, +\rangle$ (i.e., the element c) and σ satisfy the conditions of Theorem 2.1, σ is the homomorphism of an n-ary group $\langle F, f\rangle$ into an n-ary group $\langle B, f'\rangle$. Obviously, σ is the extension of the map $\psi_0 : X \to B$. □

Theorem 4.4. *In the class of semiabelian n-ary groups a free n-ary group freely generated by the set $W = \{x_\alpha \mid \alpha \in I\} \cup \{c\}$ is isomorphic to an n-ary group $\langle F, f\rangle$.*

Proof. Let $\langle H, h\rangle$ be a free n-ary group generated by W. Then there is a homomorphism ψ from $\langle H, h\rangle$ into an n-ary group $\langle F, f\rangle$, which is the extension of the map $c \to 0$, $x_\alpha \to -a + x_{\alpha 1}$, $\alpha \in I$. On the other hand, by Theorem 4.3, there exists a homomorphism $\tau : \langle F, f\rangle \to \langle H, h\rangle$, which is the extension of the map $0 \to c$, $-a + x_{\alpha 1} \to x_\alpha$, $\alpha \in I$. This means that $\tau \circ \psi(w) = w$ for all $w \in W$. Also, $\tau \circ \psi(\bar{w}) = \overline{\tau \circ \psi(w)} = \bar{w}$ for all $w \in W$.

Now if $\psi(u) = \psi(v)$ for some $u, v \in H$, then

$$u = h_{(k)}(y_{\alpha_1}, \ldots, y_{\alpha_{k(n-1)+1}}), \qquad v = h_{(l)}(z_{\alpha_1}, \ldots, z_{\alpha_{l(n-1)+1}}),$$

where y_{α_i} and z_{α_j} are elements of W or are skew to some elements of W. Thus

$$\begin{aligned}\tau \circ \psi(u) &= \tau \circ \psi(h_{(k)}(y_{\alpha_1}, \ldots, y_{\alpha_{k(n-1)+1}}))\\ &= \tau(f_{(k)}(\psi(y_{\alpha_1}), \ldots, \psi(y_{\alpha_{k(n-1)+1}})))\\ &= h_{(k)}(\tau(\psi(y_{\alpha_1})), \ldots, \tau(\psi(y_{\alpha_{k(n-1)+1}})))\\ &= h_{(k)}(y_{\alpha_1}, \ldots, y_{\alpha_{k(n-1)+1}}) = u.\end{aligned}$$

In a similar way we obtain $\tau \circ \psi(v) = v$, whence, by the uniqueness of τ, we conclude $u = v$. So, ψ is one-to-one. It is surjective too. Indeed, each $g \in F$ has the form

$$g = f_{(k)}(y_{\alpha_1}, \ldots, y_{\alpha_{k(n-1)+1}}),$$

where $y_{\alpha_i} \in X$ or is skew to some element from X. For each $y_{\alpha_i} \in X$ there exists $z_{\alpha_i} \in W$ such that $\psi(z_{\alpha_i}) = y_{\alpha_i}$. If y_{α_i} is skew to some element from X, then also there exists $z_{\alpha_i} \in W$ which is skew to some element from W and such that $\psi(z_{\alpha_i}) = y_{\alpha_i}$. This means that for each $u = h_{(k)}(z_{\alpha_1}, \ldots, z_{\alpha_{k(n-1)+1}})$ we have

$$\begin{aligned}\psi(u) &= \psi(h_{(k)}(z_{\alpha_1}, \ldots, z_{\alpha_{k(n-1)+1}}))\\ &= f_{(k)}(\psi(z_{\alpha_1}), \ldots, \psi(z_{\alpha_{k(n-1)+1}}))\\ &= f_{(k)}(y_{\alpha_1}, \ldots, y_{\alpha_{k(n-1)+1}}) = g.\end{aligned}$$

So ψ is surjective. Therefore ψ is a bijection. This completes the proof. □

References

[1] **V.A. Artamonov**, *Free n-groups*, (Russian), Mat. Zamietki **8** (1970), 499 – 507.

[2] **W. Dörnte**, *Untersuchungen über einen verallgemeinerten Gruppenbegrieff*, Math. Zeitshr. **29** (1928), 1 – 19.

[3] **W.A. Dudek**, *Remarks on n-groups*, Demonstratio Math. **13** (1980), 165 – 181.

[4] **W.A. Dudek**, *On some old and new problems in n-ary groups*, Quasigroups and Related Systems **8** (2001), 15 – 36.

[5] **W.A. Dudek, K. Glazek and B. Gleichgewicht**, *A note on the axioms of n-groups*, Colloquia Math. Soc. J. Bolyai, **29** (1977), 195 – 202.

[6] **W.A. Dudek and J. Michalski**, *On a generalization of Hosszú theorem*, Demonstratio Math. **15** (1982), 783 – 805.

[7] **W.A. Dudek and J. Michalski**, *On retracts of polyadic groups*, Demonstratio Math. **17** (1984), 281 – 301.

[8] **W.A. Dudek and N.A. Shchuchkin**, *Skew endomorphisms on some n-ary groups*, Quasigroups and Related Systems **17** (2009), 205 – 228.

[9] **K. Glazek, J. Michalski and I. Sierocki**, *On evaluation of numbers of some polyadic groups*, Contributions to General Algebra **3** (1985), 159 – 171.

[10] **L.M. Gluskin**, *Positional operatives*, (Russian), Mat. Sbornik **68(110)** (1965), 444 – 472.

[11] **M. Hosszú**, *On the explicit form of n-group operations*, Publ. Math. Debrecen **10** (1963), 88 – 92.

[12] **H. Khodabandeh and M. Shahryari**, *Simple polyadic groups*, Siberian Math. J. **55** (2014), 734 – 744.

[13] **A.G. Kurosh**, *General algebra, Lectures 1969-1970*, (Russian), Nauka, Moscow, 1974.

[14] **V.M. Kusov and N.A. Shchuchkin**, *Free abelian semicyclic n-ary groups*, (Russian), Chebyshevskii Sb. **12** (2011), no. 2(38), 68 – 76.

[15] **E.L. Post**, *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1940), 208 – 350.

[16] **N.A. Shchuchkin**, *Semicyclic n-ary groups*, (Russian), Izv. Gomel Univ. **3(54)** (2009), 186 – 194.

[17] **N.A. Shchuchkin**, *Free abelian n-ary groups* (Russian), Chebyshevskii Sb. **12** (2011), no. 2(38), 163 – 170.

[18] **N.A. Shchuchkin**, *Subgroups of free abelian n-ary group*, (Russian), Izv. Gomel State Univ. **6(81)** (2013), 94 – 103.

[19] **F.M. Sioson**, *On free abelian n-groups II*, Proc. Japan. Acad. **43** (1967), 880 – 883.

[20] **A.K. Sushkevitch**, *Thory of generalized groups*, (Russian), Chostechizdat, Kharkov – Kiev, 1937.

Received 6 May, 2015

Volgograd State Pedagogical University, Lenina prosp., 27, 400131 Volgograd, Russia
E-mail: shchukin@fizmat.vspu.ru, nikolaj_shchuchkin@mail.ru

Quasigroups and Related Systems **23** (2015), 319 − 324

On two-sided bases of ternary semigroups

Boonyen Thongkam and Thawhat Changphas

Abstract. We introduce the concept of two-sided bases of a ternary semigroup, and study the structure of ternary semigroups containing two-sided bases.

1. Introduction

The notion of a ternary semigroup which is a natural generalization of a ternary group was defined as follows: a *ternary semigroup* is a non-empty set T together with a ternary operation, written as $(a,b,c) \mapsto [abc]$, satisfying the *associative law*

$$[[abc]uv] = [a[bcu]v] = [ab[cuv]]$$

for all $a,b,c,u,v \in T$.

A non-empty subset A of a ternary semigroup T is called

- a *left ideal* of T if $[TTA] \subseteq A$;
- a *right ideal* of T if $[ATT] \subseteq A$;
- a *middle ideal* of T if $[TAT] \subseteq A$.

If A is both a left and a right ideal of T then A is called a *two-sided ideal* of T. Finally, A is called an *ideal* of T if it is a left, a right and a middle ideal of T (see [6], [9]). Note that the union of two two-sided ideals of T is a two-sided ideal of T, and the intersection of two two-sided ideals of T, if it is non-empty, is a two-sided ideal of T.

It is known that, for a non-empty subset A of a ternary semigroup T,

$$A_t = A \cup [TTA] \cup [ATT] \cup [T[TAT]T]$$

is the two-sided ideal of T containing A (see [7], [9]). If $A = \{a\}$ we write A_t as $(a)_t$, called the *principal two-sided ideal* of T generated by a.

We introduce the *quasi-ordering* on a ternary semigroup T as follows:

$$a \leqslant_t b \text{ if and only if } (a)_t \subseteq (b)_t.$$

2010 Mathematics Subject Classification: 20N15, 20N10

Keywords: ternary semigroup, selfpotent, ternary subsemigroup, left ideal, two-sided ideal, two-sided base, maximal two-sided ideal

The second author is supported by the Centre of Excellence in Mathematics, the Commission on Higher Education, Thailand.

Tamura [10] introduced one-sided bases including left bases and right bases of a semigroup. Fabrici [4] introduced two-sided bases of a semigroup and studied the structure of a semigroup containing two-sided bases. In the line of Fabrici, the results were extended to ordered semigroups by the second author and Summaprab [1]. The purpose of this paper is to introduce two-sided bases of a ternary semigroup and study the structure of a ternary semigroup containing two-sided bases.

2. Two-sided bases of a ternary semigroup

As in [4], we define two-sided bases of a ternary semigroup as follows.

Definition 2.1. A subset A of a ternary semigroup T is called a *two-sided* base of T if it satisfies the following two conditions:

(i) $A_t = T$;

(ii) there exists no a proper subset B of A such that $B_t = T$.

Example 2.2. Consider the multiplication over the complex numbers, the set $T = \{-i, 0, i\}$ is a ternary semigroup [3]. We have $\{i\}$ and $\{-i\}$ are the two-sided bases of T.

Example 2.3. Under the usual multiplication of integers, the set $\mathbb{Z}^-$ of all negative integers is a ternary semigroup. We have $\{-1\}$ is a two-sided base of $\mathbb{Z}^-$.

Example 2.4. Let $T = \mathbb{Z}^- \times \mathbb{Z}^- = \{(a, b) \mid a, b \in \mathbb{Z}^-\}$. Then (cf. [5]) T is a ternary semigroup under the ternary operation which is defined by

$$[(a, b)(c, d)(e, f)] = (a, f).$$

Then, for all $(a, b) \in T$, $\{(a, b)\}$ is a two-sided base of T.

Example 2.5. Let T be a non-empty set such that $0 \in T$ and the cardinality $|T| > 3$. Then T with the ternary operation defined by

$$[xyz] = \begin{cases} x & \text{if } x = y = z; \\ 0 & \text{otherwise,} \end{cases}$$

is a ternary semigroup [8]. We have $T \setminus \{0\}$ is a two-sided base of T.

Example 2.6. Consider a ternary semigroup

$$T = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

under the matrix multiplication [2], we have

$$A = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

is a two-sided base of T.

Example 2.7. Let $T = \{0, 1, 2, 3, 4, 5\}$. Define the ternary operation on T by

$$[abc] = (a * b) * c \text{ for all } a, b, c \in T$$

where the binary operation $*$ is defined by

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

Then T is a ternary semigroup [8] and $\{2, 3\}$, $\{2, 4\}$, $\{2, 5\}$, $\{3, 4\}$, $\{3, 5\}$, $\{4, 5\}$ are two-sided bases of T.

We now give some elementary results:

Lemma 2.8. *Let A be a two-sided base of a ternary semigroup T. If $a, b \in A$ and $a \in [TTb] \cup [bTT] \cup [T[TbT]T]$, then $a = b$.*

Proof. Let $a, b \in A$ be such that $a \in [TTb] \cup [bTT] \cup [T[TbT]T]$. Suppose that $a \neq b$. We set $B = A \setminus \{a\}$; then $b \in B$. By

$$(a)_t \subseteq [TTb] \cup [bTT] \cup [T[TbT]T] \subseteq (b)_t \subseteq B_t,$$

it follows that $A_t \subseteq B_t$, and so $T = B_t$. This is a contradiction. Hence $a = b$. □

Theorem 2.9. *A non-empty subset A of a ternary semigroup T is a two-sided base of T if and only if A satisfies the following conditions:*

(1) *for any $x \in T$ there exists $a \in A$ such that $x \leqslant_t a$;*

(2) *for any $a, b \in A$, if $a \neq b$, then a and b are incomparable.*

Proof. Assume that A is a two-sided base of ternary semigroup T, and let $x \in T$. Thus $x \in A_t$. Then there exists $a \in A$ such that $x \in (a)_t$, and hence $x \leqslant_t a$. This shows that (1) hold. Let $a, b \in A$ be such that $a \neq b$ and $a \leqslant_t b$. Then $(a)_t \subseteq (b)_t$. Since $a \neq b$, we have $a \in (b)_t \setminus \{b\}$. By Lemma 2.8, $a = b$. This is a contradiction. Thus (2) follows.

Conversely, assume that the conditions (1) and (2) hold. By (1), for any $x \in T$, there is $a \in A$ such that $(x)_t \subseteq (a)_t \subseteq A_t$. Thus $T = A_t$. Suppose that there exists a proper subset B of A such that $T = B_t$. Let $a \in A \setminus B$. Then

$$a \in A_t = T = B_t.$$

By (1), there exists $b \in B \subseteq A$ such that $a \leqslant_t b$. This contradicts to (2). Hence A is a two-sided base of T. □

3. Main results

Throughout this section, the symbol $\subset$ stands for proper inclusion for sets.

Theorem 3.1. *Let A be a two-sided base of a ternary semigroup T such that $(a)_t = (b)_t$ for some $a \in A$ and $b \in T$. If $a \neq b$, then T contains at least two two-sided bases.*

Proof. Let $a \neq b$ be such that $(b)_t = (a)_t$, it follows that

$$b \in [TTa] \cup [aTT] \cup [T[TaT]T].$$

By Lemma 2.8, $b \notin A$. Hence $b \in T \setminus A$. We set $B = (A \setminus \{a\}) \cup \{b\}$. Thus $A \neq B$. We will show that B is a two-sided base of T. Let $x \in T$. Since A is a two-sided base of T, there exists $c \in A$ such that $x \leqslant_t c$. If $c \neq a$, then $c \in B$. If $c = a$, then $(c)_t = (a)_t = (b)_t$; hence $x \leqslant_t c \leqslant_t b \in B$. Therefore B satisfies the condition (1) of Theorem 2.9. Let $x, y \in B$ be such that $x \neq y$. If $x \neq b$ and $y \neq b$, then $x, y \in A$, that is, neither $x \leqslant_t y$ nor $y \leqslant_t x$. There are two cases to consider: $x = b$ or $y = b$. If $x = b$, then $y \in A$. Suppose that $x \leqslant_t y$. Then $a \leqslant_t b = x \leqslant_t y$ and $a, y \in A$. This is a contradiction. Suppose that $y \leqslant_t x$. Then $y \leqslant_t x = b \leqslant_t a$ and $a, y \in A$. This is a contradiction. Thus neither $x \leqslant_t y$ nor $y \leqslant_t x$. The case $y = b$ can be probed in the same manner. Therefore, B satisfies the condition (2) of Theorem 2.9. □

By Theorem 3.1, we have the following.

Corollary 3.2. *Let A be a two-sided base of a ternary semigroup T, and let $a \in A$. If $(a)_t = (x)_t$ for some $x \in T$ and $x \neq a$, then x is an element of a two-sided base of T which is different from A.*

Theorem 3.3. *Any two two-sided bases of a ternary semigroup T have the same cardinality.*

Proof. Let A and B be two-sided bases of a ternary semigroup T. Let $a \in A$. Since B is a two-sided base of T, we have $a \leqslant_t b$ for some $b \in B$. For $a \in A$, we choose and fix $b \in B$ such that $a \leqslant_t b$ and define a mapping $f : A \to B$ by $f(a) = b$ for all $a \in A$.

If $a_1, a_2 \in A$ such that $f(a_1) = f(a_2) = b$. We have $a_1 \leqslant_t b$ and $a_2 \leqslant_t b$. Since A is a two-sided base of T, we have $b \leqslant_t a'$ for some a' in A. Thus $a_1 \leqslant_t a', a_2 \leqslant_t a'$ and $a_1, a_2, a' \in A$. By Theorem 2.9, we have $a_1 = a' = a_2$. Hence f is one to one. Now, let $b \in B$. Then there exists $a \in A$ such that $b \leqslant_t a$. Similarly, there exists $b' \in B$ such that $a \leqslant_t b'$. Then $b \leqslant_t b'$. By Theorem 2.9, we have $b = b'$. Thus $a \leqslant_t b' = b$. Let $f(a) = c$ for some $c \in B$. Then $a \leqslant_t c$. Since $c, b \in T$ and A is a two-sided base of T, there exist $a', a'' \in A$ such that $c \leqslant_t a'$ and $b \leqslant_t a''$. Then $a \leqslant_t a'$ and $a \leqslant_t a''$. By Theorem 2.9, we have $a = a' = a''$. Then $b \leqslant_t a'' = a \leqslant_t c$. Thus $b = c$ by Theorem 2.9. Hence f is onto. □

A two-sided base of a ternary semigroup need not to be a ternary subsemigroup, in general. Consider Example 2.2 we have $\{i\}$ is a two-sided base of T, but it is not a ternary subsemigroup of T.

Theorem 3.4. *Let A be a two-sided base of a ternary semigroup T. Then A is a ternary subsemigroup of T if and only if it has only one element.*

Proof. Let $a, b \in A$, where A is a ternary subsemigroup of T. Then $[aab] \in A$. Since

$$[aab] \in [TTb] \cup [bTT] \cup [T[TbT]T]$$

and

$$[aab] \in [TTa] \cup [aTT] \cup [T[TaT]T],$$

it follows by Lemma 2.8 that $[aab] = a = b$. Then $A = \{a\}$.

The converse statement is obvious. □

Theorem 3.5. *Let $\mathcal{A}$ be the union of all two-sided bases of a ternary semigroup T. If $M = T \setminus \mathcal{A}$ is non-empty, then it is a two-sided ideal of T.*

Proof. Let $x, y \in T$ and $a \in M$. Suppose that $[xya] \notin M$ or $[axy] \notin M$. Then $[xya] \in \mathcal{A}$ or $[axy] \in \mathcal{A}$. Thus, there exists a two-sided base B of T such that $[xya] \in B$ or $[axy] \in B$. Hence, there is $b \in B$ such that $[xya] = b$ or $[axy] = b$. It implies $b \in (a)_t$. Then $(b)_t \subseteq (a)_t$. Thus $b \leqslant_t a$. If $(b)_t = (a)_t$, then $a \in \mathcal{A}$. This contradicts to $a \in M$. Hence $(b)_t \neq (a)_t$. Since B is a two-sided base of T, there exists $c \in B$ such that $a \leqslant_t c$. If $b = c$, then $(a)_t \subseteq (c)_t = (b)_t \subseteq (a)_t$; hence $(a)_t = (b)_t$. This is a contradiction. Thus $b \neq c$. We have $b \leqslant_t a \leqslant_t c$, $b \neq c$ and $b, c \in B$. This contradicts to Theorem 2.9. Therefore, $[xya], [axy] \in M$. □

Theorem 3.6. *Let $\mathcal{A}$ be the union of all two-sided bases of a ternary semigroup T such that $\emptyset \neq \mathcal{A} \subset T$. Let M^* be a maximal two-sided ideal of T containing all proper two-sided ideals of T. The following statements are equivalent:*

(1) *$T \setminus \mathcal{A}$ is a maximal two-sided ideal of T;*

(2) *$\mathcal{A} \subseteq (a)_t$ for every $a \in \mathcal{A}$;*

(3) *$T \setminus \mathcal{A} = M^*$;*

(4) *every two-sided base of T has only one element.*

Proof. (1) ⇔ (2). Assume that $T \setminus \mathcal{A}$ is a maximal two-sided ideal of T. Suppose that $\mathcal{A} \nsubseteq (a)_t$. Since $\mathcal{A} \nsubseteq (a)_t$, there exists $x \in \mathcal{A}$ such that $x \notin (a)_t$. Thus $x \notin T \setminus \mathcal{A}$. Then $(T \setminus \mathcal{A}) \cup (a)_t \neq T$, and thus $(T \setminus \mathcal{A}) \cup (a)_t$ is a proper two-sided ideal of T such that $(T \setminus \mathcal{A}) \subset (T \setminus \mathcal{A}) \cup (a)_t$. This contradicts to the maximality of $T \setminus \mathcal{A}$.

Conversely, assume that $\mathcal{A} \subseteq (a)_t$ for every element $a \in \mathcal{A}$. By Theorem 3.5, $T \setminus \mathcal{A}$ is a proper two-sided ideal of T. Suppose that M is a two-sided ideal of T such that $T \setminus \mathcal{A} \subset M \subset T$. Then $M \cap \mathcal{A}$ is non-empty. Let $c \in M \cap \mathcal{A}$. We have $(c)_t \subseteq M$, and so

$$T = (T \setminus \mathcal{A}) \cup \mathcal{A} \subseteq (T \setminus \mathcal{A}) \cup (c)_t \subseteq M.$$

This is a contradiction. Hence $T \setminus \mathcal{A}$ is a maximal two-sided ideal of T.

(3) $\Leftrightarrow$ (4). Assume that $T \setminus \mathcal{A} = M^*$. Then $T \setminus \mathcal{A}$ is a maximal two-sided ideal of T. Let $a \in \mathcal{A}$. Using (1) $\Leftrightarrow$ (2), $\mathcal{A} \subseteq (a)_t$. Then $T = \mathcal{A}_t \subseteq (a)_t$. This implies $T = (a)_t$. Hence, for any $a \in \mathcal{A}$, $\{a\}$ is a two-sided base of T. Let B be a two-sided base of T, and let $a, b \in B$. Then $B \subseteq \mathcal{A}$, that is, $a, b \in \mathcal{A}$. Hence $b \in T = (a)_t$. By Lemma 2.8, $a = b$ (i.e., B has only one element).

Conversely, assume that every two-sided base of T has only one element. Then $T = (a)_t$ for all $a \in \mathcal{A}$. Suppose that there is a proper two-sided ideal M of T such that M is not contained in $T \setminus \mathcal{A}$. Then there exists $x \in \mathcal{A} \cap M$. Since $x \in M$, $T = (x)_t \subseteq M$, and so $T = M$. This is a contradiction.

(1) $\Leftrightarrow$ (3). Assume that $T \setminus \mathcal{A}$ is a maximal two-sided ideal of T. Let M be a two-sided ideal of T such that M is not contained in $T \setminus \mathcal{A}$. Hence, there exists $x \in M \cap \mathcal{A}$. Using (1) $\Leftrightarrow$ (2), $\mathcal{A} \subseteq (x)_t \subseteq M$. Thus $M = \mathcal{A} \cup X$ for some $X \subseteq T \setminus \mathcal{A}$. For any $y \in T$, there exists $c \in \mathcal{A}$ such that $y \leqslant_t c$. Then $y \in (y)_t \subseteq (c)_t \subseteq M$. This implies that $M = T$. Thus $T \setminus \mathcal{A} = M^*$.

The converse is obvious. □

References

[1] **T. Changphas and P. Summaprab**, *On two-sided bases of an ordered semigroup*, Quasigroups and Related Systems **22** (2014), 59 – 66.

[2] **S. Dewan**, *Quasi-relations on ternary semigroups*, Indian J. Pure Appl. Math. **28** (1997), 753 – 766.

[3] **V.N. Dixit and S. Dewan**, *A note on quasi and bi-ideals in ternary semigroups*, Int. J. Math. Math. Sci. **18** (1995), 501 – 508.

[4] **I. Fabrici**, *Two-sided bases of semigroups*, Matem. časopis **25** (1975), 173 – 178.

[5] **S. Kar and B.K. Maity**, *Some ideals of ternary semigroups*, Annals of the Alexandru Ioan Cuza University - Mathematics, **57** (2011), 247 – 258.

[6] **J. Los**, *On the extending of models I*, Fund. Math. **42** (1955), 38 – 54.

[7] **M.L. Santiago and S. Sri Bala**, *Ternary semigroups*, Semigroup Forum **81** (2010), 380 – 388.

[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. Japon. **10** (1965), 63 – 84.

[10] **T. Tamura**, *One-sided bases and translations of a semigroup*, Math. Japan. **3** (1955), 137 – 141.

Received March 24, 2015

B. Thongkam
Department of Mathematics, Faculty of Science Khon Kaen Univ., Khon Kaen, 40002, Thailand
E-mail: basis_119@hotmail.com

T. Changphas
Department of Mathematics, Faculty of Science Khon Kaen Univ., Khon Kaen, 40002, Thailand
Centre of Excellence in Mathematics, CHE, Si Ayuttaya Rd., Bangkok 10400, Thailand
E-mail: thacha@kku.ac.th

Quasigroups and Related Systems **23** (2015), 325 − 332

Relations between n-ary and binary comodules

Biljana Zekovich

Abstract. We construct a binary algebra $R = C^{\otimes(n-1)}/I$ for an n-ary algebra C and prove that M is an n-ary left C-module if and only if M is a binary left R-module. In the dual case, for an n-ary coalgebra C, we construct a binary coalgebra:

$$C^{\square(n-1)} = \bigcap_{j=1}^{n-2} \operatorname{Ker}\left[\Delta \otimes 1_C^{\otimes(n-2)} - 1_C^{\otimes j} \otimes \Delta \otimes 1_C^{\otimes(n-2-j)}\right] \subset C^{\otimes(n-1)}$$

and prove that M is an n-ary right C-comodule if and only if M is a binary right $C^{\square(n-1)}$-comodule. In the end, we prove that for n-ary finite generated coalgebra C over a field k, $C^{\square(n-1)}$ is the binary coalgebra, on the other hand, C^* is an n-ary algebra, for which, we construct the binary algebra $R = (C^*)^{\otimes(n-1)}/I$. If C is a finite-dimensional n-ary coalgebra over a field k, then C^* is a n-ary algebra and $(\mathrm{C}^{\square(n-1)})^* \cong (C^*)^{\otimes(n-1)}/I$. Dually, if C is an n-ary finite generated algebra over a field k, then $R = C^{\otimes(n-1)}/I$ is a binary algebra and C^* is an n-ary coalgebra. Moreover, $(C^*)^{\square(n-1)} \cong \left(C^{\otimes(n-1)}/I\right)^*$.

1. Introduction

Let k be a ground commutative associative ring with a unit, C and M modules over k. In what follows, $\otimes$ is a tensor product over k. All homomorphisms are k-linear maps. In [3], the concept of *n-ary algebra* (C, m) is defined, where

$$m : C \otimes \cdots \otimes C \to C$$

is n-ary multiplication, which is associative. It means that the following diagram is commutative:

$$\begin{tikzcd}
C^{\otimes(2n-1)} \arrow[r, "m\otimes 1_C^{\otimes(n-1)}"] \arrow[d, "1_C^{\otimes i}\otimes m\otimes 1_C^{\otimes(n-i-1)}"'] & C^{\otimes n} \arrow[d, "m"] \\
C^{\otimes n} \arrow[r, "m"] & C
\end{tikzcd}$$

i.e.,

$$m \circ (m \otimes 1_C^{\otimes(n-1)}) = m \circ (1_C^{\otimes i} \otimes m \otimes 1_C^{\otimes(n-i-1)}).$$

2010 Mathematics Subject Classification: 20N15
Keywords: n-ary (co)algebra, n-ary (co)module, isomorphism of binary (co)algebras

The concept of *n-ary coalgebra* (C, Δ) is defined in [4], where

$$\Delta{:}C \to C \otimes \cdots \otimes C$$

is n-ary comultiplication, which is coassociative, that is the following diagram is commutative:

$$\begin{tikzcd}
C \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & C^{\otimes n} \arrow[d, "1_C^{\otimes i} \otimes \Delta \otimes 1_C^{\otimes (n-i-1)}"] \\
C^{\otimes n} \arrow[r, "\Delta \otimes 1_C^{\otimes (n-1)}"] & C^{\otimes (n-1)}
\end{tikzcd}$$

i.e.,

$$(\Delta \otimes 1_C^{\otimes (n-1)}) \circ \Delta = (1_C^{\otimes i} \otimes \Delta \otimes 1_C^{\otimes (n-i-1)}) \circ \Delta.$$

Similary, the concept of *n-ary bialgebra* (C, m, Δ) is introduced, where m is an associative n-ary multiplication and Δ is a coassociative n-ary comultiplication and Δ is a homomorphism of n-ary algebras. An example of n-ary algebra is given in [6]. We do not suppose the existence of an unit and a counit.

In the paper [3], the notion of homomorphism of n-ary algebras

$$(C, m_C) \to (C', m_{C'})$$

is defined as a morphism $f{:}C \to C'$, such that the following diagram is commutative

$$\begin{tikzcd}
C^{\otimes n} \arrow[r, "f^{\otimes n}"] \arrow[d, "m_C"'] & (C')^{\otimes n} \arrow[d, "m_{C'}"] \\
C \arrow[r, "f"] & C'
\end{tikzcd}$$

i.e.,

$$f \circ m_C = m_{C'} \circ f^{\otimes n}.$$

Let C be an n-ary coalgebra and a finitely generated projective k-module. Denote by C^* the k-module $\mathrm{Hom}(C, k)$. Then C^* is an n-ary algebra with multiplication $l_1 * \cdots * l_n$, where for $c \in C$

$$(l_1 * \cdots * l_n)(c) = \sum_{(c)} l_1(c_{(1)}) \cdots l_n(c_{(n)}) \tag{1}$$

if

$$\Delta(c) = \sum_{(c)} c_{(1)} \otimes \cdots \otimes c_{(n)} \in C^{\otimes n}.$$

Conversely, let C be an n-ary algebra and a finitely generated projective k-module. Define an n-ary comultiplication in $C^* = \mathrm{Hom}(C, k)$ by the rule:

$$(\Delta l)(x_1 \otimes \cdots \otimes x_n) = l(x_1 \cdots x_n) \tag{2}$$

where $x_1, \dots, x_n \in C$. Hence we use the isomorphism of k-modules:

$$(C \otimes \cdots \otimes C)^* = C^* \otimes \cdots \otimes C^*$$

(cf. [2]), because C is a finitely generated projective k-module. Then, C^* is an n-ary coalgebra. If C is an n-ary (co)algebra, then $(C^*)^* \cong C$ (cf. [3] and [4]).

In [5] are defined the concepts of a right (left) n-ary (co)modules in the following way: k-module M is called a *right n-ary C-comodule*, where C is an n-ary coalgebra, if there is a map $\rho : M \to M \otimes C^{\otimes(n-1)}$, such that the following diagram is commutative:

$$\begin{tikzcd}
M \arrow[r, "\rho"] \arrow[d, "\rho"'] & M \otimes C^{\otimes(n-1)} \arrow[d, "1_M \otimes 1_C^{\otimes i} \otimes \Delta \otimes 1_C^{\otimes(n-i-2)}"] \\
M \otimes C^{\otimes(n-1)} \arrow[r, "\rho \otimes 1_C^{\otimes(n-1)}"'] & M \otimes C^{\otimes 2(n-1)}
\end{tikzcd}$$

i.e.,

$$(1_M \otimes 1_C^{\otimes i} \otimes \Delta \otimes 1_C^{\otimes(n-i-2)}) \circ \rho = (\rho \otimes 1_C^{\otimes(n-1)}) \circ \rho.$$

k-module M is called a *left n-ary C-module*, where C is an n-ary algebra, if there is a map $\gamma : C^{\otimes(n-1)} \otimes M \to M$, such that the following diagram is commutative:

$$\begin{tikzcd}
C^{\otimes(n-1)} \otimes M \arrow[r, "\gamma"] & M \\
C^{\otimes 2(n-1)} \otimes M \arrow[u, "1_C^{\otimes(n-1)} \otimes \gamma"'] \arrow[r, "1_C^{\otimes i} \otimes m \otimes 1_C^{\otimes(n-i-2)} \otimes 1_M"'] & C^{\otimes(n-1)} \otimes M \arrow[u, "\gamma"']
\end{tikzcd}$$

i.e.,

$$\gamma \circ (1_C^{\otimes(n-1)} \otimes \gamma) = \gamma \circ (1_C^{\otimes i} \otimes m \otimes 1_C^{\otimes(n-i-2)} \otimes 1_M).$$

Now, we define the concept of an n-ary ideal: a submodule I of the module C is called an *n-ary ideal*, if

$$C^{\otimes i} \otimes I \otimes C^{\otimes(n-i-1)} \subseteq I,$$

where $0 \leqslant i \leqslant n-1$, C is an n-ary algebra.

2. Relations between n-ary and binary modules

Let C be an n-ary algebra over commutative ring k. There is not necessarily a unit in C, but the multiplication is associative, i.e.,

$$(c_1 \cdots c_n)c_{n+1} \cdots c_{2n-1} = c_1 \cdots c_j(c_{j+1} \cdots c_{j+n})c_{j+n+1} \cdots c_{2n-1} \qquad (3)$$

for all $j = 0, \dots, n-1$ and $c_1, \dots, c_{2n-1} \in C$. Consider the submodule I in the tensor-degree $C^{\otimes(n-1)}$ (see [4]), which is generated by all differences:

$$(c_1 \cdots c_n) \otimes c_{n+1} \otimes \cdots \otimes c_{2n-2} - c_1 \otimes \cdots \otimes c_j \otimes (c_{j+1} \cdots c_{j+n}) \otimes c_{j+n+1} \otimes \cdots \otimes c_{2n-2}$$

for $c_1, \dots, c_{2n-2} \in C$ and $j = 0, \dots, n-2$. Then, I is an n-ary ideal in the n-ary algebra $C^{\otimes(n-1)}$. Denote by R the factor-module $C^{\otimes(n-1)}/I$.

Theorem 2.1. *R is an associative binary k-algebra with respect to multiplication*

$$(c_1 \otimes \cdots \otimes c_{n-1} + I)(c_n \otimes \cdots \otimes c_{2n-2} + I) = (c_1 \cdots c_n) \otimes c_{n+1} \otimes \cdots \otimes c_{2n-2} + I \quad (4)$$

Proof. Let us check that the multiplication (4) is correctly defined. It is sufficient to show that:

$$\begin{aligned} [(c_1 \cdots c_n) &\otimes c_{n+1} \otimes \cdots \otimes c_{2n-2} + I\,[c_{2n-1} \otimes \cdots \otimes c_{3n-3} + I] \\ &= [c_1 \otimes \cdots \otimes c_j \otimes (c_{j+1} \cdots c_{j+n}) \otimes c_{j+n+1} \otimes \cdots \otimes c_{2n-2} + I] \\ &\quad \cdot [c_{2n-1} \otimes \cdots \otimes c_{3n-3} + I] \end{aligned}$$

for all $c_1, \dots, c_{3n-3} \in C$.

Similar equality holds after multiplication by $c_{2n-1} \otimes \cdots \otimes c_{3n-3} + I$, on the left. By (4), we have:

$$\begin{aligned} &[(c_1 \cdots c_n) \otimes c_{n+1} \otimes \cdots \otimes c_{2n-2} + I]\,[c_{2n-1} \otimes \cdots \otimes c_{3n-3} + I] \\ &\qquad = [(c_1 \cdots c_n) c_{n+1} \cdots c_{2n-1}] \otimes c_{2n} \otimes \cdots \otimes c_{3n-3} + I \end{aligned}$$

On the other hand:

$$\begin{aligned} &[c_1 \otimes \cdots \otimes c_j \otimes (c_{j+1} \cdots c_{j+n}) \otimes c_{j+n+1}! \otimes \cdots \otimes c_{2n-2} + I]\,[c_{2n-1} \otimes \cdots \otimes c_{3n-3} + I] \\ &\qquad = [c_1 \cdots c_j (c_{j+1} \cdots c_{j+n}) c_{j+n+1} \cdots c_{2n-2} c_{2n-1}] \otimes c_{2n} \otimes \cdots \otimes c_{3n-3} + I. \end{aligned}$$

By the associativity(3), the previous products are equal. The condition:

$$\begin{aligned} &[c_{2n-1} \otimes \cdots \otimes c_{3n-3} + I]\,[(c_1 \cdots c_n) \otimes c_{n+1} \otimes \cdots \otimes c_{2n-2} + I] \\ &= [c_{2n-1} \otimes \cdots \otimes c_{3n-3} + I]\,[c_1 \otimes \cdots \otimes c_j \otimes (c_{j+1} \cdots c_{j+n}) \otimes c_{j+n+1} \otimes \cdots \otimes c_{2n-2} + I] \end{aligned}$$

is checked in a similar way. Consequently, the multiplication in R is well defined.

Let us show that it is associative. We have:

$$\begin{aligned} &[(c_1 \otimes \cdots \otimes c_{n-1} + I)(c_n \otimes \cdots \otimes c_{2n-2} + I)]\,(c_{2n-1} \otimes \cdots \otimes c_{3n-3} + I) \\ &= [(c_1 \cdots c_n) \otimes c_{n+1} \otimes \cdots \otimes c_{2n-2} + I]\,(c_{2n-1} \otimes \cdots \otimes c_{3n-3} + I) \\ &= [(c_1 \cdots c_n) c_{n+1} \cdots c_{2n-1}] \otimes c_{2n} \otimes \cdots \otimes c_{3n-3} + I. \end{aligned}$$

On the other hand,

$$\begin{aligned} &(c_1 \otimes \cdots \otimes c_{n-1} + I)\,[(c_n \otimes \cdots \otimes c_{2n-2} + I)\,(c_{2n-1} \otimes \cdots \otimes c_{3n-3} + I)] \\ &= (c_1 \otimes \cdots \otimes c_{n-1} + I)\,[(c_n \ldots c_{2n-1}) \otimes c_{2n} \cdots \otimes c_{3n-3} + I] \\ &= [c_1 \cdots c_{n-1}\,(c_n \ldots c_{2n-1})] \otimes c_{2n} \otimes \cdots \otimes c_{3n-3} + I \end{aligned}$$

By (3), we obtain that the multiplication in R is associative. □

Theorem 2.2. *M is an n-ary left C-module if and only if M is a binary left R-module.*

Proof. Suppose that M is an n-ary left C-module. If $c_1, \dots, c_{n-1} \in C$ and $m \in M$, then we put:

$$(c_1 \otimes \cdots \otimes c_{n-1} + I)m = (c_1 \otimes \cdots \otimes c_{n-1})m.$$

The definition of the ideal I and the n-ary C-module implies that $I \cdot m = 0$. So, M is a left R-module.

Conversely, if M is a left R-module, then for $c_1, \dots, c_{n-1} \in C$ and $m \in M$, we put

$$(c_1 \otimes \cdots \otimes c_{n-1})m = (c_1 \otimes \cdots \otimes c_{n-1} + I)m.$$

We see that M is an n-ary left C-module. □

What is proved here is an equivalence of categories between the category of n-ary left modules over C and the category of left modules over R.

3. Dual situation

Let C be an n-ary coalgebra over a field k. Denote by $C^{\square(n-1)}$ the set:

$$\bigcap_{j=1}^{n-2} \mathrm{Ker}[\Delta \otimes 1_C^{\otimes(n-2)} - 1_C^{\otimes j} \otimes \Delta \otimes 1_C^{\otimes(n-2-j)}] \subset C^{\otimes(n-1)}.$$

In the other words, $C^{\square(n-1)}$ contains all elements

$$f = \sum c_1 \otimes \cdots \otimes c_{n-1} \in C^{\otimes(n-1)},$$

such that

$$\sum \Delta c_1 \otimes c_2 \otimes \cdots \otimes c_{n-1} = \sum c_1 \otimes \cdots \otimes c_j \otimes \Delta c_{j+1} \otimes c_{j+2} \otimes \cdots \otimes c_{n-1}$$

for all $j = 0, \dots, n-2$.

Theorem 3.1. *The n-ary comultiplication in C induces a comultiplication:*

$$\Delta' : C^{\square(n-1)} \to C^{\square(n-1)} \otimes C^{\square(n-1)}$$

i.e., $C^{\square(n-1)}$ is a binary coalgebra.

Proof. Define the map

$$\Delta' : C^{\otimes(n-1)} \to C^{\otimes(n-1)} \otimes C^{\otimes(n-1)}$$

by the following rule:

$$\Delta'(c_1 \otimes \cdots \otimes c_{n-1}) = \Delta c_1 \otimes c_2 \otimes \cdots \otimes c_{n-1} \in\in C^{\otimes n} \otimes C^{\otimes(n-2)} = C^{\otimes(n-1)} \otimes C^{\otimes(n-1)}.$$

It is necessary show that

$$\Delta'(C^{\Box(n-1)}) \subseteq C^{\Box(n-1)} \otimes C^{\Box(n-1)}.$$

Let $f \in C^{\Box(n-1)}$. Then, for $j = 1, \ldots, n-2$:

$$\begin{aligned}
&\left\{\left[\Delta \otimes 1_C^{\otimes(n-2)} - 1_C^{\otimes j} \otimes \Delta \otimes 1_C^{\otimes(n-2-j)}\right] \otimes 1_C^{\otimes(n-1)}\right\} \Delta'(f)\\
&= \left\{\left[\Delta \otimes 1_C^{\otimes(n-2)} - 1_C^{\otimes j} \otimes \Delta \otimes 1_C^{\otimes(n-2-j)}\right] \otimes 1_C^{\otimes(n-1)}\right\} (\Delta \otimes 1_C^{\otimes(n-2)}) f\\
&= \left\{\left[(\Delta \otimes 1_C^{\otimes(n-1)} - 1_C^{\otimes j} \otimes \Delta \otimes 1_C^{\otimes(n-1-j)}) \otimes 1_C^{\otimes(n-2)}\right] (\Delta \otimes 1_C^{\otimes(n-2)})\right\} f = 0
\end{aligned}$$

by the coassociativity. Analogously, for $j = 1, \ldots, n-2$:

$$\left\{1_C^{\otimes(n-1)} \otimes \left[\Delta \otimes 1_C^{\otimes(n-2)} - 1_C^{\otimes j} \otimes \Delta \otimes 1_C^{\otimes(n-2-j)}\right]\right\} \Delta'(f) = 0,$$

see [2]. □

Theorem 3.2. *k-module M is an n-ary right C-comodule if and only if M is a binary right $C^{\Box(n-1)}$-comodule.*

Proof. If M is a binary right $C^{\Box(n-1)}$-comodule, then M is an n-ary right C-comodule, because $C^{\Box(n-1)} \subset C^{\otimes(n-1)}$.

Conversely, let M be an n-ary right C-comodule and $\rho{:}M \to M \otimes C^{\otimes(n-1)}$. It is necessary show that

$$\rho(M) \subseteq M \otimes C^{\Box(n-1)},$$

i.e.,

$$(\Delta \otimes 1_C^{\otimes(n-2)} - 1_C^{\otimes j} \otimes \Delta \otimes 1_C^{\otimes(n-2-j)})\rho = 0.$$

This follows from the definition of an n-ary C-comodule. □

What is proved here is an equivalence of categories between the category of n-ary right comodules over C and the category of right comodules over $C^{\Box(n-1)}$.

4. Isomorphisms of binary (co)algebras

In this part, as in previous, we shall suppose that k is a field.

Theorem 4.1. *Let C be an n-ary finite dimensional coalgebra over the field k. Then $C^{\Box(n-1)}$ is a binary coalgebra. Moreover, C^* is an n-ary algebra, for which we construct the binary algebra $R = (C^*)^{\otimes(n-1)}/I$. Then there exists an isomorphism of binary algebras:*

$$(C^{\Box(n-1)})^* \cong (C^*)^{\otimes(n-1)}/I.$$

Proof. By definition:

$$C^{\square(n-1)} = \bigcap_{j=1}^{n-2} \mathrm{Ker}[\Delta \otimes 1_C^{\otimes(n-2)} - 1_C^{\otimes j} \otimes \Delta \otimes 1_C^{\otimes(n-2-j)}].$$

In other words, we obtain the exact sequence of the vector spaces:

$$0 \to C^{\square(n-1)} \to C^{\otimes(n-1)} \xrightarrow{\varphi} \bigoplus_{j=1}^{n-2} C^{\otimes(2n-2)},$$

where

$$\varphi(x) = \left(\Delta \otimes 1_C^{\otimes(n-2)} - 1_C \otimes \Delta \otimes 1_C^{\otimes(n-3)}\right)(x) + \cdots \\ + \left(\Delta \otimes 1_C^{\otimes(n-2)} - 1_C^{\otimes(n-2)} \otimes \Delta\right)(x).$$

Moving to the dual finite dimensional spaces, we obtain the exact sequence:

$$0 \leftarrow (C^{\square(n-1)})^* \leftarrow (C^{\otimes(n-1)})^* \xleftarrow{\varphi^*} \bigoplus_{j=1}^{n-2} (C^{\otimes(2n-2)})^* \tag{5}$$

Since C has finite dimension:

$$(C^{\otimes(n-1)})^* = (C^*)^{\otimes(n-1)}$$
$$(C^{\otimes(2n-2)})^* = (C^*)^{\otimes(2n-2)}.$$

Moreover, for $l_1, \dots, l_{2n-2}$ from j-th summand $(C^*)^{\otimes(2n-2)}$, we have:

$$\varphi^*(l_1 \otimes \cdots \otimes l_{2n-2}) = (l_1 * \cdots * l_n) \otimes l_{n+1} \otimes \cdots \otimes l_{2n-2} \\ - l_1 \otimes \cdots \otimes l_j \otimes (l_{j+1} * \cdots * l_{j+n}) \otimes l_{j+n+1} \otimes \cdots \otimes l_{2n-2} \tag{6}$$

In that way, by the exactness of the sequence (5), we obtain that:

$$(\mathrm{C}^{\square(n-1)})^* \cong (C^*)^{\otimes(n-1)}/I,$$

where I is the subspace generated by all elements of the form (6). We need to show that the constructed isomorphism

$$(C^*)^{\otimes(n-1)}/I \to (\mathrm{C}^{\square(n-1)})^*$$

is an isomorphism of binary algebras. Let

$$l_1, \dots, l_{2n-2} \in C^* \quad \text{and} \quad f = \sum c_1 \otimes \cdots \otimes c_{n-1} \in C^{\square(n-1)}.$$

Then,

$$[(l_1 \otimes \cdots \otimes l_{n-1} + I)(l_n \otimes \cdots \otimes l_{2n-2} + I)]\,(f) \\ = [(l_1 * \cdots * l_n) \otimes l_{n+1} \otimes \cdots \otimes l_{2n-2} + I]\,(f) \\ = \mu(l_1 \otimes \cdots \otimes l_{2n-2})(\Delta \otimes 1_C^{\otimes(n-2)})(f)$$

But, for $u, v \in (\mathrm{C}^{\square(n-1)})^*$ and $\mathrm{f} \in \mathrm{C}^{\square(n-1)}$:

$$(u * v)(f) = \mu(u \otimes v)\Delta'(f) == \mu(u \otimes v)(\Delta \otimes 1^{\otimes(n-2)})f$$

Let

$$u = l_1 \otimes \cdots \otimes l_{n-1} + I, \quad v = l_n \otimes \cdots \otimes l_{2n-2} + I.$$

Then,

$$\mu(u \otimes v)(\Delta \otimes 1^{\otimes(n-2)}) = \mu(l_1 \otimes \cdots \otimes l_{2n-2})(\Delta \otimes 1^{\otimes(n-2)})$$

i.e., the map

$$R \to (\mathrm{C}^{\square(n-1)})^*$$

is a homomorphism of binary algebras. □

Analogically, we prove:

Theorem 4.2. *Let C be an n-ary finite dimensional algebra over a field. Then, $R = C^{\otimes(n-1)}/I$ is a binary algebra, and C^* is an n-ary coalgebra. Moreover,*

$$(C^*)^{\square(n-1)} \cong R^*.$$

References

[1] **N. Burbaki**, *Algebra*, Moscow, 1962.

[2] **N. Burbaki**, *Commutative algebra*, Mir, Moscow, 1971.

[3] **B. Zekovich**, *On n-ary bialgebras. I*, (Russian), Chebyshevskii Sb. **4** (2003), N3, 65 – 73.

[4] **B. Zekovich**, *On n-ary bialgebras. II,* (Russian), Chebyshevskii Sb. **4** (2003), N3, 73 – 80.

[5] **B. Zekovich**, *n-ary comodules over n-ary (co)algebras*, Algebra and Discrete Math. (2008), N4, 80 – 89.

[6] **B. Zekovich**, *Example of n-ary bialgebra*, Days of Difraction 2012, 250 – 253.

Received June 28, 2014

Faculty of Natural Science
Department of Mathematics
University of Montenegro
Podgorica, Montenegro
E-mail: biljanaz@t-com.me