Quasigroups and Related Systems **26** (2018), 1 – 12

A representation theorem for bounded distributive hyperlattices

Abdelaziz Amroune and Ali Oumhani

Abstract. A representation theorem for bounded distributive hyperlattices is given. The equivalence between the category of Priestley spaces and the dual of the category of bounded distributive hyperlattices is established.

1. Introduction

The notion of hyperstructures was introduced 80 years ago [6], it has been studied by several authors see for example [1, 4, 5, 10, 11, 12], this bibliography and the references therein is not exhaustive.

Later, Koguep *et al.* [4], Konstantinidou [5] introduced respectively the notion of hyperlattices and studied ideals and filters in these structures. Prime ideals and prime filters in hyperlattices have been examined by R. Ameri *et al.* [1]. Rasouli and Davvaz defined a fundamental relation on a hyperlattice to get a lattice from a hyperlattice. Moreover, they defined a topology on the set of prime ideals of a distributive hyperlattice [11, 12].

The Stone's representation theorems [13, 14] proved that every Boolean algebra is isomorphic to a set of $\{I_a : a \in A\}$ (where I_a denotes the set of prime ideals of A not containing a). Since then, representation theorems for distributive lattices has known a vast development.

H. A. Priestley developed another kind of duality for bounded distributive lattices [8, 9]. Such representation theorems enable a deep and a concrete comprehension of the lattices as well as their structures. Our motivation finds its place in the following opinion:

"Stone's duality and its variants are central in making the link between syntactical and semantic approaches to logic. Also in theoretical computer science, this link is central as the two sides correspond to specification languages and the space of computational states. This ability to translate faithfully between algebraic specification and spatial dynamics has often proved itself to be a powerful theoretical tool as well as a handle for making practical problems decidable" see [3].

2010 Mathematics Subject Classification: 03E72, 06B20, 06D72
Keywords: Hyperlattices, distributive hyperlattices, filter and ideal of hyperlattice, Priestley space, homomorphism of hyperlattices, homomorphism of Priestley spaces.

In this paper, we extend some results of [8, 9], where a representation theorem of bounded distributive hyperlattices is presented. In other words, the category of Priestley spaces is equivalent to the dual of the category of bounded distributive hyperlattices.

2. Preliminaries

Let X be a nonempty set and $P^*(X)$ denotes the set of all nonempty subsets of X. Maps $f : X \times X \to P^*(X)$, are called *hyperoperations* [6].

Definition 2.1. Let L be a nonempty set, $\wedge$ be a binary operation and $\sqcup$ be a hyperoperation on L. L is called a *hyperlattice* if for all $a, b, c \in L$ the following conditions hold:

(i) $a \in a \sqcup a$, and $a \wedge a = a$;

(ii) $a \sqcup b = b \sqcup a$, and $a \wedge b = b \wedge a$;

(iii) $a \in [a \wedge (a \sqcup b)] \cap [a \sqcup (a \wedge b)]$;

(iv) $a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c$, and $a \wedge (b \wedge c) = (a \wedge b) \wedge c$;

(v) $a \in a \sqcup b \Rightarrow a \wedge b = b$.

A hyperlattice L with the property

$$a \wedge (b \sqcup c) = (a \wedge b) \sqcup (a \wedge c)$$

is called *distributive*, where for all nonempty subsets A and B of L we define

$$A \sqcup B = \cup \{a \sqcup b \,|\, a \in A, b \in B\} \quad \text{and} \quad A \wedge B = \{a \wedge b \,|\, a \in A, b \in B\}.$$

The converse of condition (v) in Definition 2.1 is true. Indeed using (iii) in Definition 2.1, we obtain $a \in a \sqcup b$ by taking $b = a \wedge b$.

Hence, we can define a partial order on L by:

$$a \leq b \Leftrightarrow b \in a \sqcup b \Leftrightarrow a \wedge b = a.$$

A hyperlattice L is called *bounded* if there exist $0, 1 \in L$ such that for all $a \in L$, $0 \leq a \leq 1$.

Consider a lattice $(L, \wedge, \vee)$. We define the Nakano hyperoperation $\sqcup$ on L by $x \sqcup y = \{z \in L / z \vee x = z \vee y = x \vee y\}$, for all $x, y \in L$. To the best of our knowledge, the $\sqcup$ hyperoperation was first introduced by Nakano in [7], which is an investigation of hyperrings.

Lemma 2.2. *If $(L, \wedge, \vee)$ is a distributive lattice, then $(L, \wedge, \sqcup)$ is a distributive hyperlattice where $a \sqcup b = \{x \in L \,|\, a \vee b = a \vee x = b \vee x\}$ for all $a, b \in L$.*

Proof. Straightforward. □

Lemma 2.3. *Let $L = \{0, 1\}$. Then, $(\{0, 1\}, \wedge, \sqcup)$ is a bounded distributive hyperlattice, where*

$\wedge$	0	1
0	0	0
1	0	1

and

$\sqcup$	0	1
0	$\{0\}$	$\{1\}$
1	$\{1\}$	$\{0, 1\}$

.

Definition 2.4. [10] A nonempty subset I of a hyperlattice L is called an *ideal* if the following conditions hold

(i) If $a, b \in I$, then $a \sqcup b \subseteq I$;

(ii) If $a \in I$, $b \leq a$, and $b \in L$, then $b \in I$.

A proper ideal I is called *prime* if $a \wedge b \in I$ implies $a \in I$ or $b \in I$ for all $a, b \in L$.

Definition 2.5. [10] A nonempty subset F of a hyperlattice L is called a *filter* if the following conditions hold

(i) If $a, b \in F$, then $a \wedge b \in F$;

(ii) If $a \in F$, $a \leq b$, and $b \in L$, then $b \in F$.

A proper filter F is called *prime* if for all $a, b \in L$ $(a \sqcup b) \cap F \neq \emptyset$ implies $a \in F$ or $b \in F$.

Theorem 2.6. [1] *If P is a prime ideal of a hyperlattice L, then $L - P$ is a prime filter of L. Similarly, if F is a prime filter of L, then $L - F$ is a prime ideal of L.*

Proposition 2.7. *If δ is a nonempty subset of a hyperlattice L, then the smallest filter containing δ has the form*

$$\langle \delta \rangle = \{x \in L \,|\, a_1 \wedge ... \wedge a_n \leq x, \text{ for some } a_1, .., a_n \in \delta\}.$$

Proof. First, we prove that $\langle \delta \rangle$ is nonempty. Let $a \in \delta$, since $a \leq a$, then $a \in \langle \delta \rangle$, hence $\langle \delta \rangle \neq \emptyset$. To proof that $\langle \delta \rangle$ is a filter let $x \in \langle \delta \rangle$, $y \in X$ such that $x \leq y$, then $\wedge_{i=1}^{n} a_i \leq x \leq y$, so $y \in F$.

On the other hand, for $x, y \in \langle \delta \rangle$, there exist $a_1, a_2, \ldots, a_n$, $b_1, b_2, \ldots, b_m$ such that $\wedge_{i=1}^{n} a_i \leq x$ and $\wedge_{j=1}^{m} b_j \leq y$. Then, $(\wedge_{i=1}^{n} a_i) \wedge (\wedge_{j=1}^{m} b_j) \leq x \wedge y$. Therefore, $x \wedge y \in \langle \delta \rangle$.

Next, let $a \in \delta$, since $a \leq a$, we have $a \in \langle \delta \rangle$. Then $\delta \subseteq \langle \delta \rangle$.

Finally, suppose that F is a filter with $\delta \subseteq F$. Then for any $x \in \langle \delta \rangle$, then there exist $a_1, a_2, .., a_n \in \delta$ such that $\wedge_{i=1}^{n} a_i \leq x$, then $x \in F$. Therefore $\langle \delta \rangle \subseteq F$. □

If $\delta = \{a\}$, we write $\langle \delta \rangle = \uparrow a = \{x \in L \,|\, a \leq x\}$.

Proposition 2.8. [10] *Let $(L, \wedge, \sqcup)$ be a distributive hyperlattice. If $a \in L$ then $\downarrow a = \{x \in L \,|\, x \leq a\}$ is an ideal.*

Theorem 2.9. *Let X be a distributive hyperlattice, F be a filter and I an ideal of X. If $F \cap I = \emptyset$, then there is a prime filter P such that $F \subseteq P$ and $P \cap I = \emptyset$.*

Proof. Let $\mathcal{G}$ be the family of those filters F' which satisfy $F \subseteq F'$ and $F' \cap I = \emptyset$. It follows from the Zorn's lemma that $\mathcal{G}$ has a maximal element P. Since $P \in \mathcal{G}$ it remains to prove that the filter P is prime. Since $P \cap I = \emptyset$, P is proper. Suppose P is not prime. Then there exist $a, b \in X$ such that $(a \sqcup b) \cap P \neq \emptyset$, and $a \notin P$ and $b \notin P$. Let $a_0 \in (a \sqcup b) \cap P$ and let $\delta = P \cup \{a\}$. Then $\langle \delta \rangle \cap I \neq \emptyset$, otherwise $P \subseteq \langle \delta \rangle \in G$ contradicting the maximality of P. Take $x \in \langle \delta \rangle \cap I$. This implies easily there exists $p \in P$ that $p \wedge a \leq x$, it follows that $a_0 \wedge p \wedge a \leq x$ and since $x \in I$, it follows that $a_0 \wedge p \wedge a \in I$. Similarly $a_0 \wedge q \wedge b \in I$. Then, $a_0 \wedge m \wedge a \in I$ and $a_0 \wedge m \wedge b \in I$ such that $m = p \wedge q$, it follows that $(a_0 \wedge m \wedge a) \sqcup (a_0 \wedge m \wedge b) \subseteq I$, which implies $a_0 \wedge m \in (a_0 \wedge m) \wedge (a \sqcup b) \subseteq I$, and $a_0 \wedge m \in P$, therefore $I \cap P \neq \emptyset$, which is a contradiction. □

Corollary 2.10. *Let L be a distributive hyperlattice. If I is an ideal and $a \in L - I$, then there exists a prime filter P such that $a \in P$ and $P \cap I = \emptyset$.*

Proof. Let I be an ideal, $a \in L - I$ and take $F = \langle a \rangle$, it follows $F \cap I = \emptyset$. By Theorem 2.9, there is a prime filter P such that $F \subseteq P$ and $P \cap I = \emptyset$. □

Definition 2.11. Let L and L' be two hyperlattices and $f : L \to L'$ be a mapping.

1. f is said to be a *hyperlattices homomorphism* if $f(x \wedge y) = f(x) \wedge f(y)$ and $f(x \sqcup y) \subseteq f(x) \sqcup f(y)$, for all $x, y \in L$.
2. f is said to be a *strong homomorphism* of a hyperlattices, if $f(x \wedge y) = f(x) \wedge f(y)$ and $f(x \sqcup y) = f(x) \sqcup f(y)$, for all $x, y \in L$. If f is a bijection, then f is said to be a *hyperlattices isomorphism* (*strong isomorphism*).

Proposition 2.12. *Let $(L, \wedge, \sqcup)$ be a hyperlattice, $(\{0,1\}, \wedge, \sqcup)$ be the hyperlattice in Lemma 2.3 and F be a subset of L. If F is a prime filter, then there is a surjective hyperlattices homomorphism $f : L \to \{0,1\}$, such that $F = f^{-1}(\{1\})$.*

Proof. Set $f(X) = 1$ if $X \subseteq F$, and $f(X) = 0$ otherwise. Since $(x \sqcup y) \cap F \neq \emptyset \Leftrightarrow (x \in F$ or $y \in F)$, then $f(x \sqcup y) = 1 \Rightarrow x \sqcup y \subseteq F \Rightarrow (x \sqcup y) \cap F \neq \emptyset \Rightarrow x \in F$ or $y \in F \Rightarrow f(x) = 1$ or $f(y) = 1$. Hence, $f(x \sqcup y) \subseteq f(x) \sqcup f(y)$.

If $f(x \sqcup y) = 0$, we have $x \sqcup y \nsubseteq F$, it follows that $(x \sqcup y) \cap F = \emptyset$, which implies $x \notin F$ and $y \notin F$, it follows that $f(x) = 0$ and $f(y) = 0$, which implies $f(x) \sqcup f(y) = 0$. Therefore, $f(x \sqcup y) \subseteq f(x) \sqcup f(y)$.

For the second homomorphism axiom, we have $f(x \wedge y) = 0 \Leftrightarrow x \wedge y \subseteq L - F \Leftrightarrow (x \in L - F$ or $y \in L - F) \Leftrightarrow (f(x) = 0$ or $f(y) = 0) \Leftrightarrow f(x) \wedge f(y) = 0$. Hence, $f(x \wedge y) = f(x) \wedge f(y)$. □

Corollary 2.13. *Let L be a distributive hyperlattice. If $a, b \in X$ are such that $a \nleq b$ there is a prime filter F such that $a \in F$ and $b \notin F$.*

Proof. Take $I = {\downarrow} b$ in Corollary 2.10. □

3. Priestley duality

Definition 3.1. Let $(L, \leq)$ be a poset. A subset $E \subseteq L$ is said to be *increasing* (*decreasing*) if $\forall x, y \in L$, $x \in E$ and $x \leq y$ $(y \leq x)$ implies $y \in E$.

Definition 3.2. An *ordered topological space* is a triple $(X, \tau, \leq)$ such that (X, τ) is a topological space and $(X, \leq)$ is a poset. A *clopen set* in a topological space is a set which is both open and closed. The ordered topological space is said to be *totally disconnected* if for every $x, y \in X$ such that $x \not\leq y$ there exists an increasing τ-clopen U and a decreasing τ-clopen V such that $U \cap V = \emptyset$ with $x \in U$ and $y \in V$.

Definition 3.3. *A Priestley space is a compact totally disconnected ordered topological space.*

If A is a bounded distributive hyperlattice, then its *dual space* is defined to be $T(A) = (X, \tau, \leq)$, where X is the set of homomorphisms from A onto $(\{0,1\}, \wedge, \sqcup)$, preserving 0 and 1, τ is the product topology induced from $\{0,1\}^A$, and $\leq$ is the partial order defined by $f \leq g$ in X if and only if $f(a) \leq g(a)$ for all $a \in A$. $T(A)$ is compact, and it is also totally order disconnected, i.e., a Priestley space.

Definition 3.4. [2] Let $(X, \tau, \leq)$, and $(X', \tau', \preceq)$ be two Priestley spaces. Then $f : X \to X'$ is called

1. *increasing* if for all $x, y \in X$, $x \leq y \Rightarrow f(x) \preceq f(y)$.

2. a *Priestley spaces homomorphism* if is increasing and continuous. If it is a bijection, then it is a *Priestley spaces isomorphism.*

Lemma 3.5. *If $\delta = (X, \tau, \leq)$ is a Priestley space, then there exists a hyperoperation $\sqcup$ such that $(L(\delta), \cap, \sqcup, \emptyset, X)$ is a bounded distributive hyperlattice, where $L(\delta) = \{Y \subseteq X \mid Y$ is increasing and τ-clopen$\}$ and $\sqcup$ is defined by*

$$A \sqcup B = \{X \in L(\delta) \mid A \cup B = A \cup X = B \cup X\}$$

for all $A, B \in L(\delta)$.

Proof. By Lemma 2.2. □

Lemma 3.6. *Let A be a bounded distributive hyperlattice. Then $F_A \colon A \to L(T(A))$ defined by $F_A(a) = \{f \in X \mid f(a) = 1\}$ is a hyperlattices isomorphism.*

Proof. For all $a, b \in A$ we have

$$\begin{aligned} F_A(a \wedge b) &= \{f \in X \mid f(a \wedge b) = 1\} = \{f \in X \mid f(a) = 1\} \cap \{f \in X \mid f(b) = 1\} \\ &= F_A(a) \sqcap F_A(b), \end{aligned}$$

and

$$\begin{aligned} F_A(a \sqcup b) &= \{F_A(t) \mid t \in a \sqcup b\} = \{\{f \in X \mid f(a \sqcup b) = 1\}\} \\ &\subseteq \{\{f \in X \mid f(a) = 1\} \cup \{f \in X \mid f(b) = 1\}\} = \{F_A(a) \cup F_A(b)\} \\ &\subseteq F_A(a) \sqcup F_A(b). \end{aligned}$$

Suppose that $a \neq b$. If $a \not\leq b$, there exist a prime filter F such that $a \in F$ and $b \notin F$ (Corollary 2.13). Thus, by Proposition 2.12, there is a hyperlattices homomorphism $f: A \to \{0,1\}$ such that $a \in f^{-1}(\{1\})$ and $b \notin f^{-1}(\{1\})$, hence $f(a) = 1$ and $f(b) = 0$, i.e., $F_A(a) \not\leq F_A(b)$.

Similarly, $b \not\leq a$ gives $F_A(b) \not\leq F_A(a)$. Hence, $a \neq b$ implies $F_A(a) \neq F_A(b)$ i.e., F_A is injective.

To prove that F_A is surjective, let $U \in L(T(A))$. Then, for all $f \in U$ and $g \in L(T(A)) - U$, since U is increasing, we have $g < f$. Thus, $f(a_{fg}) = 1$ and $g(a_{fg}) = 0$ for some $a_{fg} \in A$. Hence, $f \in F_A(a_{fg})$ and $g \in L(T(A)) - F_A(a_{fg})$.

For fixed $f \in U$ we have $g \in L(T(A)) - U \subseteq \bigcup_{i=1}^{n} (L(T(A)) - F_A(a_{fgi})) = L(T(A)) - F_A(\bigwedge_{i=1}^{n} a_{fgi})$ (because $L(T(A)) - U$ is compact). For $a_f = \bigwedge_{i=1}^{n} a_{fgi} =$, we have $F_A(a_f) = F_A(\bigwedge_{i=1}^{n} a_{fgi}) \subset U$. On the other hand, $f(a_f) = 1$, thus $f \in F_A(a_f)$. Therefore, $U = \cup_{f \in U} F_A(a_f)$. We find again a finite covering $U = \bigcup_{j=1}^{n} F_A(a_{fj})$. Hence, $\{U\} \supseteq \bigsqcup_{j=1}^{n} F_A(a_{fj}) \supseteq F_A(\bigsqcup_{j=1}^{n} a_{fj})$, (since $B \subset B' \Rightarrow F_A^{-1}(B) \subset F_A^{-1}(B')$ and F_A injective). Consequently, $F_A^{-1}(F_A(\bigsqcup_{j=1}^{n} a_{fj})) = \bigsqcup_{j=1}^{n} a_{fj}))$.

We have $\bigsqcup_{j=i}^{n} a_{fj} \subseteq F_A^{-1}(U)$, since $\bigsqcup_{j=1}^{n} a_{fj} \in \mathcal{P}^*(A)$, i.e., $\emptyset \neq \bigsqcup_{j=1}^{n} a_{fj} \subseteq A$, i.e., F_A is surjective. Since F_A is injective, there exists $a \in A$ such that $U = F_A(a)$. Therefore, F_A is a hyperlattices isomorphism. □

Lemma 3.7. *If $f: A_1 \to A_2$ is a hyperlattices homomorphism, then the map $T(f): T(A_1) \to T(A_2)$ defined by $T(f)(g) = g \circ f$ is a homomorphism of Priestley spaces.*

Proof. For all $g_1, g_2 \in T(A_1)$, from $g_1 \leq g_2$ it follows $g_1 \circ f \leq g_2 \circ f$. Hence $T(f)$ is increasing. The continuity of $T(f)$ follows from the fact that for every $a \in A_1$,

$$\begin{aligned} T(f)^{-1}(F_{A_1}(a)) &= \{g \in T(A_2) / T(f)(g) \in F_{A_1}(a)\} \\ &= \{g \in T(A_2) / g \circ f(a) = 1\} = \{g \in T(A_2) / g(f(a)) = 1\} \\ &= F_{A_2}(f(a)). \end{aligned}$$

This completes the proof. □

Lemma 3.8. *If $\delta = (X, \tau, r)$ is a Priestley space, then the map $G_\delta: \delta \to T(L(\delta))$ defined by*

$$G_\delta(x)(Y) = \begin{cases} 1 & \text{if } x \in Y, \\ 0 & \text{if } x \notin Y, \end{cases}$$

for all $Y \in L(\delta)$, is an isomorphism of Priestley spaces.

Proof. To prove the surjectivity, for each $f \in T(L(\delta))$ we consider the sets $U = \{Y \in L(\delta) \mid f(Y) = 1\}$, $V = \{Z \in L(\delta) \mid f(Z) = 0\}$, $A = \cap_{Y \in U} Y$ and $B = \cup_{Z \in V} Z$. Suppose that $A - B = \emptyset$. Then $(\cap_{Y \in U} Y) \cap (\cup_{Z \in V} Z)^c = \emptyset$, consequently $(\cap_{Y \in U} Y) \cap (\cap_{Z \in V} Z^C) = \emptyset$. Since X is compact, we have $(\overset{n}{\underset{i=1}{\cap}} Y_i) \cap (\overset{m}{\underset{j=1}{\cap}} Z_j^C) = \emptyset$. Thus, $\overset{n}{\underset{i=1}{\cap}} Y_i \subseteq \overset{m}{\underset{j=1}{\cup}} Z_j$ and $f(\overset{m}{\underset{j=1}{\cup}} Z_j) = 1$, a contradiction because $f(\overset{m}{\underset{j=1}{\cup}} Z_j) = \overset{m}{\underset{j=i}{\vee}} f(Z_j) = 0$. Hence $A - B \neq \emptyset$. Then, there exists $x \in A - B$ such that $G_\delta(x) = f$. Therefore $G_\delta(x)(Y) = 1 \Leftrightarrow x \in Y \Leftrightarrow Y \in U \Leftrightarrow f(Y) = 1$. So, G_δ is surjective.

Let $x_1, x_2 \in \delta$, $x_1 \neq x_2$. If $x_1 \not\leq x_2$, then there exists $Y_0 \in L(\delta)$ such that $x_1 \in Y_0$ and $x_2 \notin Y_0$, hence $G_\delta(x_1)(Y_0) \neq G_\delta(x_2)(Y_0)$. If $x_2 \not\leq x_1$, then there exists $Y_1 \in L(\delta)$ such that $x_2 \in Y_1$ and $x_1 \notin Y_1$, hence $G_\delta(x_2)(Y_1) \neq G_\delta(x_1)(Y_1)$. Thus $x_1 \neq x_2$ implies $G_\delta(x_1)(Y) \neq G_\delta(x_2)(Y)$, so G_δ is injective.

To prove that G_δ is continuous, let Z be a τ-clopen subset of $T(L(\delta))$. Then, there exists $y \in L(\delta)$ such that $Y = F_{L(\delta)}(y)$. Thus

$$\begin{aligned} G_\delta^{-1}(Y) &= G_\delta^{-1}(F_{L(\delta)}(y)) = \left\{x \in X / G_\delta(x) \in F_{L(\delta)}(y)\right\} \\ &= \{x \in X / G_\delta(x)(y) = 1\} = \{x \in X / x \in y\} = X \cap y = y. \end{aligned}$$

Hence, G_δ is continuous.

Note that, since $Y \in L(\delta)$ are increasing, $x \leq y$ implies $G_\delta(x)(Y) \leq G_\delta(y)(Y)$. □

Lemma 3.9. *If $h\colon \delta_1 \to \delta_2$ is a homomorphism of Priestley spaces, then the map $L(h)\colon L(\delta_2) \to L(\delta_1)$ defined by $L(h)(y) = h^{-1}(y)$ for every $y \in L(\delta_2)$ is a hyperlattices homomorphism.*

Proof. For all $y \in L(\delta_2)$ we have $L(h)(y) \in L(\delta_1)$. For all $y, z \in L(\delta_2)$ since h^{-1} commutes with set-theoretical operations we have,

$$\begin{aligned} L(h)(y \sqcup z) &\subseteq \left\{h^{-1}(x) \mid h^{-1}(y \cup z) = h^{-1}(y \cup x) = h^{-1}(z \cup x)\right\} \\ &= \left\{h^{-1}(x) \mid h^{-1}(y) \cup h^{-1}(z) = h^{-1}(y) \cup h^{-1}(x) = h^{-1}(z) \cup h^{-1}(x)\right\} \\ &\subseteq L(h)(y) \sqcup L(h)(z). \end{aligned}$$

and $L(h)(y \cap z) = h^{-1}(y \cap z) = h^{-1}(y) \cap h^{-1}(z) = L(h)(y) \cap L(h)(z)$.

Hence, $L(h)$ is a hyperlattices homomorphism. □

Theorem 3.10. *$L(T(f)) \circ F_{A_1} = F_{A_2} \circ f$ for any hyperlattices homomorphism $f\colon A_1 \to A_2$.*

$$\begin{array}{ccc} A_1 & \xrightarrow{\quad f \quad} & A_2 \\ {\scriptstyle F_{A_1}}\downarrow & & \downarrow{\scriptstyle F_{A_2}} \\ L(T(A_1)) & \xrightarrow[L(T(f))]{} & L(T(A_2)) \end{array}$$

Proof. For all $a \in A_1$,

$$\begin{aligned}(L(T(f)) \circ F_{A_1})(a) &= L(T(f))(F_{A_1}(a)) = T^{-1}(f)(F_{A_1}(a)) \\ &= \{g \in T(A_2) \mid T(f)(g) \in F_{A_1}(a)\} \\ &= \{g \in T(A_2) \mid g \circ f \in F_{A_1}(a)\} \\ &= \{g \in T(A_2) \mid g(f(a)) = 1\} \\ &= F_{A_2}(f(a)) = (F_{A_2} \circ f)(a),\end{aligned}$$

which completes the proof. □

Theorem 3.11. *For any homomprphism $h\colon \delta_1 \to \delta_2$ of Priestley spaces, we have $T(L(h)) \circ G_{\delta_1} = G_{\delta_2} \circ h$.*

$$\begin{array}{ccc} \delta_1 & \xrightarrow{\quad h \quad} & \delta_2 \\ {\scriptstyle G_{\delta_1}}\downarrow & & \downarrow{\scriptstyle G_{\delta_2}} \\ L(T(\delta_1)) & \xrightarrow[L(T(h))]{} & L(T(\delta_2)) \end{array}$$

Proof. $(T(L(h)) \circ G_{\delta_1})(f) = T(L(h))(G_{\delta_1}(f)) = G_{\delta_1}(f) \circ L(h)$ for all $f \in \delta_1$. Hence for all $y \in L(\delta_2)$ we have

$$\begin{aligned}(T(L(h)) \circ G_{\delta_1})(f)(y) &= (G_{\delta_1}(f) \circ L(h))(y) = G_{\delta_1}(f)\left(h^{-1}(y)\right) \\ &= \begin{cases} 1 \text{ if } f \in h^{-1}(y) \\ 0 \text{ if } f \notin h^{-1}(y) \end{cases} = \begin{cases} 1 \text{ if } h(f) \in y \\ 0 \text{ if } h(f) \notin y \end{cases} \\ &= G_{\delta_2}(h(f))(y) = (G_{\delta_2} \circ h)(f)(y).\end{aligned}$$

This completes the proof. □

Theorem 3.12. *The dual of the category of Priestley spaces is equivalent to the category of distributive hyperlattices.*

Proof. By Lemma 3.6, Lemma 3.8, Theorem 3.10 and Theorem 3.11. □

4. Examples

Example 4.1. Let $A = \{0, a, b, 1\}$. Consider the following Cayley tables

$\wedge$	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

$\sqcup$	0	a	b	1
0	$\{0\}$	$\{a\}$	$\{b\}$	$\{1\}$
a	$\{a\}$	$\{0, a\}$	$\{1\}$	$\{b, 1\}$
b	$\{b\}$	$\{1\}$	$\{0, b\}$	$\{a, 1\}$
1	$\{1\}$	$\{b, 1\}$	$\{a, 1\}$	A

Then $(A, \wedge, \sqcup, 0, 1)$ is a bounded distributive hyperlattice. $T(A)$ is the set of homomorphisms from A onto $\{0, 1\} = \{f_1, f_2\}$ and its bidual is: $L(T(A)) = \{\emptyset, \{f_1\}, \{f_2\}, \{f_1, f_2\}\}$, where

	0	a	b	1
f_1	0	1	0	1
f_2	0	0	1	1

$\sqcup$	$\emptyset$	$\{f_1\}$	$\{f_2\}$	$\{f_1, f_2\}$
$\emptyset$	$\emptyset$	$\{f_1\}$	$\{f_2\}$	$\{f_1, f_2\}$
$\{f_1\}$	$\{f_1\}$	$\{\emptyset, \{f_1\}\}$	$\{f_1, f_2\}$	$\{\{f_2\}, \{f_1, f_2\}\}$
$\{f_2\}$	$\{f_2\}$	$\{f_1, f_2\}$	$\{\emptyset, \{f_2\}\}$	$\{\{f_1\}, \{f_1, f_2\}\}$
$\{f_1, f_2\}$	$\{f_1, f_2\}$	$\{\{f_2\}, \{f_1, f_2\}\}$	$\{\{f_1\}, \{f_1, f_2\}\}$	$\{\emptyset, \{f_1\}, \{f_2\}, \{f_1, f_2\}\}$

Then $(L(T(A)), \cap, \sqcup, \emptyset, X)$ is a bounded distributive hyperlattice with $X = \{f_1, f_2\}$. $F_A \colon A \to L(T(A))$ is given by $F_A(0) = \emptyset$, $F_A(a) = \{f_1\}$, $F_A(b) = \{f_2\}$, $F_A(1) = \{f_1, f_2\}$.

Example 4.2. Let $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$ be the set of positive divisors of 30 and $(D(30), \wedge, \vee)$ the lattice where $a \wedge b$ and $a \vee b$ are respectively the greatest common divisor and the least common multiplier of a and b. Define on $D(30)$ the hyperoperation by: $a \sqcup b = \{x \in D(30) | a \vee b = a \vee x = b \vee x\}$, for all $a, b \in L$. Then $(D(30), \wedge, \sqcup, 1, 30)$ is a bounded distributive hyperlattice. $T(D(30))$ is the set of homomorphisms from $D(30)$ onto $\{0, 1\} = \{f_1, f_2, f_3\}$.

$D(30)$	1	2	3	5	6	10	15	30
f_1	0	1	0	0	1	1	0	1
f_2	0	0	1	0	1	0	1	1
f_3	0	0	0	1	0	1	1	1

Its bidual is: $L(T(D(30))) = \{\emptyset, \{f_1\}, \{f_2\}, \{f_3\}, \{f_1, f_2\}, \{f_1, f_3\}, \{f_2, f_3\}, X\}$, where $X = \{f_1, f_2, f_3\}$.

$\sqcup$	$\emptyset$	$\{f_1\}$	$\{f_2\}$	$\{f_3\}$
$\emptyset$	$\emptyset$	$\{f_1\}$	$\{f_2\}$	$\{f_3\}$
$\{f_1\}$	$\{f_1\}$	$\{\emptyset, \{f_1\}\}$	$\{f_1, f_2\}$	$\{f_1, f_3\}$
$\{f_2\}$	$\{f_2\}$	$\{f_1, f_2\}$	$\{\emptyset, \{f_2\}\}$	$\{f_2, f_3\}$
$\{f_3\}$	$\{f_3\}$	$\{f_1, f_3\}$	$\{f_2, f_3\}$	$\{\emptyset, \{f_3\}\}$
$\{f_1, f_2\}$	$\{f_1, f_2\}$	$\{\{f_2\}, \{f_1, f_2\}\}$	$\{\{f_1\}, \{f_1, f_2\}\}$	$\{X$
$\{f_1, f_3\}$	$\{f_1, f_3\}$	$\{\{f_3\}, \{f_1, f_3\}\}$	X	$\{\{f_1\}, \{f_1, f_3\}\}$
$\{f_2, f_3\}$	$\{f_2, f_3\}$	$\{X\}$	$\{\{f_3\}, \{f_2, f_3\}\}$	$\{\{f_2\}, \{f_2, f_3\}\}$
X	X	$\{\{f_2, f_3\}, X\}$	$\{\{f_1, f_3\}, X\}$	$\{\{f_1, f_2\}, X\}$

$\sqcup$	$\{f_1, f_2\}$	$\{f_1, f_3\}$
$\emptyset$	$\{f_1, f_2\}$	$\{f_1, f_3\}$
$\{f_1\}$	$\{\{f_2\}, \{f_1, f_2\}\}$	$\{\{f_3\}, \{f_1, f_3\}\}$
$\{f_2\}$	$\{\{f_1\}, \{f_1, f_2\}\}$	X
$\{f_3\}$	X	$\{\{f_1\}, \{f_1, f_3\}\}$
$\{f_1, f_2\}$	$\{\emptyset, \{f_1\}, \{f_2\}, \{f_1, f_2\}\}$	$\{\{f_2, f_3\}, X\}$
$\{f_1, f_3\}$	$\{\{f_2, f_3\}, X\}$	$\{\emptyset, \{f_1\}, \{f_3\}, \{f_1, f_3\}\}$
$\{f_2, f_3\}$	$\{\{f_1, f_3\}, X\}$	$\{\{f_1, f_2\}, X\}$
X	$\{\{f_3\}, \{f_1, f_3\}, \{f_2, f_3\}, X\}$	$\{\{f_2\}, \{f_1, f_2\}, \{f_2, f_3\}, X\}$

$\sqcup$	$\{f_2, f_3\}$	X
$\emptyset$	$\{f_2, f_3\}$	X
$\{f_1\}$	X	$\{\{f_2, f_3\}, X\}$
$\{f_2\}$	$\{\{f_3\}, \{f_2, f_3\}\}$	$\{\{f_1, f_3\}, X\}$
$\{f_3\}$	$\{\{f_2\}, \{f_2, f_3\}\}$	$\{\{f_1, f_2\}, X\}$
$\{f_1, f_2\}$	$\{\{f_1, f_3\}, X\}$	$\{\{f_3\}, \{f_1, f_3\}, \{f_2, f_3\}, X\}$
$\{f_1, f_3\}$	$\{\{f_1, f_2\}, X\}$	$\{\{f_2\}, \{f_1, f_2\}, \{f_2, f_3\}, X\}$
$\{f_2, f_3\}$	$\{\emptyset, \{f_2\}, \{f_3\}, \{f_2, f_3\}\}$	$\{\{f_1\}, \{f_1, f_2\}, \{f_1, f_3\}, X\}$
X	$\{\{f_1\}, \{f_1, f_2\}, \{f_1, f_3\}, X\}$	$L(T(A))$

Then $(L(T(A)), \cap, \sqcup, \emptyset, X)$ is a bounded distributive hyperlattice. $F_A(1) = \emptyset$, $F_A(2) = \{f_1\}$, $F_A(3) = \{f_2\}$, $F_A(5) = \{f_3\}$, $F_A(6) = \{f_1, f_2\}$, $F_A(10) = \{f_1, f_3\}$, $F_A(15) = \{f_2, f_3\}$, $F_A(30) = X$.

Example 4.3. Let $(X, \tau, \leq)$ be a Priestley space, where $X = \{a, b, c\}$ and $\leq$ is given by

$\leq$	a	b	c
a	1	0	1
b	0	1	1
c	0	0	1

and $L(X) = \{\emptyset, \{c\}, \{a, c\}, \{b, c\}, X\}$, where

$\sqcup$	$\emptyset$	$\{c\}$	$\{a, c\}$	$\{b, c\}$	X
$\emptyset$	$\emptyset$	$\{c\}$	$\{a, c\}$	$\{b, c\}$	X
$\{c\}$	$\{c\}$	$\{\emptyset, \{c\}\}$	$\{a, c\}$	$\{b, c\}$	X
$\{a, c\}$	$\{a, c\}$	$\{a, c\}$	$\{\emptyset, \{c\}, \{a, c\}\}$	X	$\{\{b, c\}, X\}$
$\{b, c\}$	$\{b, c\}$	$\{b, c\}$	X	$\{\emptyset, \{c\}, \{b, c\}\}$	$\{\{a, c\}, X\}$
X	X	X	$\{\{b, c\}, X\}$	$\{\{a, c\}, X\}$	$L(X)$

$\leq$	$\emptyset$	$\{c\}$	$\{a, c\}$	$\{b, c\}$	X
$\emptyset$	1	1	1	1	1
$\{c\}$	0	1	1	1	1
$\{a, c\}$	0	0	1	0	1
$\{b, c\}$	0	0	0	1	1
X	0	0	0	0	1

and $T(L(X)) = \{f_1, f_2, f_3\}$ such that

$L(X)$	f_1	f_2	f_3
$\emptyset$	0	0	0
$\{c\}$	0	0	1
$\{a, c\}$	1	0	1
$\{b, c\}$	0	1	1
X	1	1	1

The isomorphism $G_X : X \to T(L(X))$ is defined by $G_X(a) = f_1$, $G_X(b) = f_2$, $G_X(c) = f_3$.

Conclusion

In this paper, we propose a new way to represent distributive hyperlattices. It is shown that the dual of the category of Priestley spaces is equivalent to the category of bounded distributive hyperlattices.

For further investigations, we give the following open question.

Question. *Is there a relation between the category of bounded distributive hyperlattices and the category of bounded distributive lattices?*

References

[1] **R. Ameri, M. Amiri-Bideshki, A.B. Saeid, S. Hoskova-Mayerova**, *Prime filters of hyperlattices*, An. Stiint. Univ. "Ovidius" Constanta, Ser. Mat. **24(2)** (2016), $15 - 26$.

[2] **V. Boicescu, A. Filipoiu, G. Georgescu, S. Rudeanu**, *Lukasiewicz-Moisil Algebras*, North Holland, Amsterdam, 1991.

[3] **M. Gehrke**, *Stone duality, topological algebra, and recognition*, J. Pure Appl. Algebra **220(7)**, (2016) $2711 - -2747$.

[4] **B.B.N. Koguep, C. Nkuimi, C. Lele**, *On fuzzy ideals of hyperlattice*, Internat. J. Algebra **2** (2008), $739 - 750$.

[5] **M. Konstantinidou, J. Mittas**, *An introduction to the theory of hyperlattice*, Math Balcanica **7** (1977), $187 - 193$.

[6] **F. Marty**, *Sur une generalization de la notion de groupe*, 8^{th} Congress Math. Scandenaves, Stockholm, (1934), $45 - 49$.

[7] **T. Nakano**, *Rings and partly ordered systems*, Math. Zeitschr. **99** (1967), $355-376$.

[8] **H.A. Priestley**, *Representation of distributive lattices by means of ordered Stone spaces*, Bull. London Math. Soc. **2** (1970), $186 - 190$.

[9] **H.A. Priestley**, *Ordered topological spaces and the presentation of distributive lattices*, Proc. London. Math. Soc. **24(3)** (1972), $507 - 530$.

[10] **A. Rahnemai-Barghi**, *The prime ideal theorem for distributive hyperlattices*, Ital. J. Pure Appl. Math. **10** (2010), 75 – 78.

[11] **S. Rasouli, B. Davvaz**, *Lattice derived from hyperlattices*, Commun. Algebra **38** (2010), 2720 – 2737.

[12] **S. Rasouli, B. Davvaz**, *Construction and spectral topology on hyperlattice*, Mediterr. J. Math. **7** (2010), 249 – 262.

[13] **M.H. Stone**, *The theory of representation for Boolean algebras*, Trans. Amer. Math. Soc. **74** (1936), no.1, 37 – 111.

[14] **M.H. Stone**, *Topological representations of distributive lattices and Brouwerian logics*, Časopis Pěst. Math., **67** (1937), 1 – 25.

Received September 14, 2017

A. Amroune
Laboratory of pure and applied Mathematics, Department of Mathematics, University Mohamed Boudiaf, P. O. BOX 166, Icheblia, M'sila, Algeria
E-mail: aamrounedz@yahoo.fr

A. Oumhani
Ecole Normale Supèrieure de Bou Saada, 28001 Bou saada, M'sila, Algeria.
E-mail: alioumhani@yahoo.fr

Quasigroups and Related Systems **26** (2018), 13 – 34

Implication zroupoids and identities of associative type

Juan M. Cornejo and Hanamantagouda P. Sankappanavar

Abstract. An algebra $\mathbf{A} = \langle A, \to, 0\rangle$, where $\to$ is binary and 0 is a constant, is called an $\mathcal{I}$-*zroupoid* if $\mathbf{A}$ satisfies the identities: $(x \to y) \to z \approx [(z' \to x) \to (y \to z)']'$ and $0'' \approx 0$, where $x' := x \to 0$, and $\mathcal{I}$ denotes the variety of all $\mathcal{I}$-zroupoids. An $\mathcal{I}$-zroupoid is *symmetric* if it satisfies $x'' \approx x$ and $(x \to y')' \approx (y \to x')'$. The variety of symmetric $\mathcal{I}$-zroupoids is denoted by $\mathcal{S}$. An identity $p \approx q$, in the groupoid language $\langle\to\rangle$, is called *an identity of associative type of length* 3 if p and q have exactly 3 (distinct) variables, say x, y, z, and are grouped according to one of the two ways of grouping: (1) $\star \to (\star \to \star)$ and (2) $(\star \to \star) \to \star$, where $\star$ is a place holder for a variable. A subvariety of $\mathcal{I}$ is said to be of *associative type of length* 3, if it is defined, relative to $\mathcal{I}$, by a single identity of associative type of length 3. In this paper we give a complete analysis of the mutual relationships of all subvarieties of $\mathcal{I}$ of associative type of length 3. We prove, in our main theorem, that there are exactly 8 such subvarieties of $\mathcal{I}$ that are distinct from each other and describe explicitly the poset formed by them under inclusion. As an application of the main theorem, we derive that there are three distinct subvarieties of the variety $\mathcal{S}$ of associative type, each defined relative to $\mathcal{S}$, by a single identity of associative type of length 3.

1. Introduction

In 1934, Bernstein gave a system of axioms for Boolean algebras in [3] using implication alone. Even though his system was not equational, it is not hard to see that one could easily convert it into an equational one by using an additional constant. In 2012, the second author extended this "modified Bernstein's theorem" to De Morgan algebras in [24] by showing that the variety of De Morgan algebras, is term-equivalent to the variety $\mathcal{DM}$ (defined below) whose defining axioms use only an implication $\to$ and a constant 0.

The primary role played by the identity (I): $(x \to y) \to z \approx [(z' \to x) \to (y \to z)']'$, where $x' := x \to 0$, in the axiomatization of each of those new varieties motivated the second author to study the identity (I) in its own right and led him

2010 Mathematics Subject Classification: 06D30, 08B15, 20N02, 03G10
Keywords: implication zroupoid, variety, identity of associative type
The first author wishes to dedicate this work to the memory of Oscar Foresi, his second dad.
The second author wishes to dedicate this work to the memory of his sister, Paddawwa R. Hooli.
The work of Juan M. Cornejo was supported by CONICET (Consejo Nacional de Investigaciones Cientificas y Tecnicas) and Universidad Nacional del Sur.

to introduce a new equational class of algebras called *implication zroupoids* in [24] (also called *implicator groupoids* in [7]).

An algebra $\mathbf{A} = \langle A, \to, 0\rangle$, where $\to$ is binary and 0 is a constant, is called a *zroupoid*. A zroupoid $\mathbf{A} = \langle A, \to, 0\rangle$ is an *implication zroupoid* ($\mathcal{I}$*-zroupoid*, for short) if $\mathbf{A}$ satisfies:

(I) $(x \to y) \to z \approx [(z' \to x) \to (y \to z)']'$, where $x' := x \to 0$,

(I_0) $0'' \approx 0$.

$\mathcal{I}$ denotes the variety of implication zroupoids. The varieties $\mathcal{DM}$ and $\mathcal{SL}$ are defined relative to $\mathcal{I}$, respectively, by the following identities:

(DM) $(x \to y) \to x \approx x$ (De Morgan Algebras);
(SL) $x' \approx x$ and $x \to y \approx y \to x$ (semilattices with the least element 0).

The variety $\mathcal{BA}$ of Boolean algebras is defined relative to $\mathcal{DM}$ by the following identity:

(BA) $x \to x \approx 0'$.

The variety $\mathcal{I}$ exhibits (see [24]) several interesting properties; for example, the identity $x''' \to y \approx x' \to y$ holds in $\mathcal{I}$; in particular, $\mathcal{I}$ satisfies $x'''' \approx x''$. Two of the subvarieties of $\mathcal{I}$ that are of interest in this paper are: $\mathcal{I}_{2,0}$ and $\mathcal{MC}$ which are defined relative to $\mathcal{I}$, respectively, by the following identities, where $x \wedge y := (x \to y')'$:

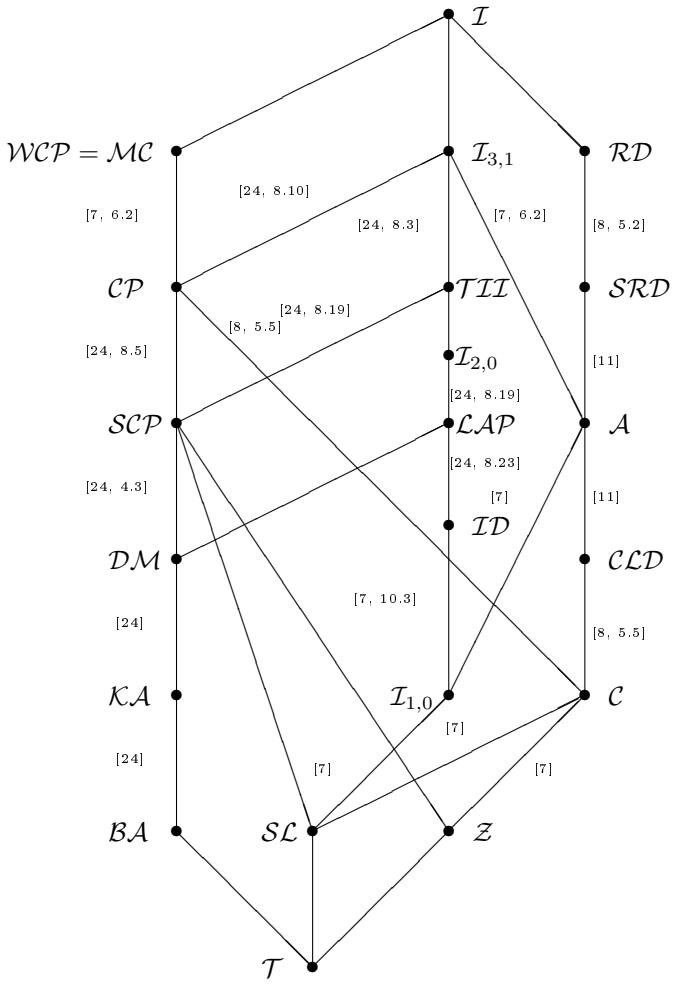
($\mathrm{I}_{2,0}$) $x'' \approx x$;
(MC) $x \wedge y \approx y \wedge x$.

The (still largely unexplored) lattice of subvarieties of $\mathcal{I}$ seems to be fairly complex. In fact, Problem 6 of [24] calls for an investigation of the structure of the lattice of subvarieties of $\mathcal{I}$.

The papers [5], [6], [7], [8], [9], [10] and [11] have addressed further the above-mentioned problem, but still partially, by introducing several new subvarieties of $\mathcal{I}$ and investigating relationships among them. The (currently known) size of the poset of subvarieties of $\mathcal{I}$ is at least 30; but it is still unknown whether the lattice of subvarieties is finite or infinite. We conjecture that its cardinality is 2^ω.

Motivated by the fact that not all algebras in $\mathcal{I}$ are associative with respect to the operation $\to$, the quest for finding more new subvarieties of $\mathcal{I}$ led us naturally to consider the question as to whether generalizations of the associative law would yield some new subvarieties of $\mathcal{I}$ and thereby reveal further insight into the structure of the lattice of subvarieties of $\mathcal{I}$. This quest led to the results in [9], [10] and this paper, which will show that this is indeed the case.

The poset of the (then) known varieties that appears in [8] is given below for the reader's convenience (for the definitions of the varieties in the picture, see [8]).



A look at the associative law would reveal the following characteristics:

(1) Length of the left side term = length of the right side term = 3,

(2) The number of distinct variables on the left = the number of distinct variables on right = the number of occurrences of variables on either side,

(3) The order of the variables on the left side is the same as the order of the variables on the right side,

(4) The bracketings used in the left side term and in the right side term are different from each other.

One way to generalize the associative law is to relax somewhat the restrictions (1) and (2) by choosing m distinct variables and setting the length of the left term = that of right term = n, with $n \geqslant m$, and keeping (3) and (4). But then, for $n \geqslant 4$, there will be more than two possible bracketings. So, we order all possible bracketings and assign a number to each, called bracketing number. Such identities are called "weak associative identities of length n". For a precise definition and notation of weak associative identities, we refer the reader to [10] and the references therein.

A second way to generalize the associative law is to relax (3) and to keep (2), (4) and the first half of (1). So, we consider the laws of the form $p \approx q$ of length n such that (a) each of p and q contains the n (an integer $\geqslant 3$) distinct variables, say, $x_1, x_2, \ldots, x_n$, (b) p and q are terms obtained by distinct bracketings of permutations of the n variables. Let us call such laws as "identities of associative type of length n".

A third way to generalize the associative law is to relax all of four features mentioned above by allowing number of occurrences of variables on one side be different from the number on the other side. Let us refer to these as "identities of mixed type".

Specific instances of all such generalizations of the associative law have already occurred in the literature at least since late 19th century. We mention below a few such instances.

Weak associative identities of length 4 with 3 distinct variables, called "identities of Bol-Moufang type", have been investigated in the literature quite extensively for the varieties of quasigroups and loops. In fact, the first systematic analysis of the relationships among the identities of Bol-Moufang type appears to be in [12] in the context of loops. For more information about these identities in the context of quasigroups and loops, see [12], [15], [19], [20]) and the references therein.

More recently, in [9] and [10], we have made a complete analysis of relationships among weak associative identities of length $\leqslant 4$, relative to the variety $\mathcal{S}$ of symmetric I-zroupoids (i.e., satisfying $x'' \approx x$ and $(x \to y')' \approx (y \to x')'$). We have shown that 6 of the 155 subvarieties of $\mathcal{S}$, each being defined by a single weak associative law of length $m \leqslant 4$ (including the Bol-Moufang type), are distinct. Furthermore, we describe explicitly by a Hasse diagram the poset formed by them, together with the varieties $\mathcal{BA}$ and $\mathcal{SL}$.

We should mention here that such an analysis of weak associative laws of length $\leqslant 4$ relative to the variety $\mathcal{I}$ is still open.

The identities of associative type have also appeared in the literature. We mention several examples below, using $\cdot$ for the binary operation instead of $\to$.

- The identity $x \cdot (y \cdot z) \approx (z \cdot x) \cdot y$ was considered in [28] by Suschkewitsch (see also [27, Theorem 11.5]).

- Abbott [1] uses the identity $x \cdot (y \cdot z) \approx y \cdot (x \cdot z)$ as one of the defining identities in his definition of implication algebras.

- The identities $x\cdot(y\cdot z)\approx z\cdot(y\cdot x)$, $x\cdot(y\cdot z)\approx y\cdot(x\cdot z)$, and $x\cdot(y\cdot z)\approx(z\cdot x)\cdot y$ were investigated for quasigroups by Hosszú in [13].
- The identity $x\cdot(z\cdot y)\approx(x\cdot y)\cdot z$ is investigated by Pushkashu in [22].
- The identities $x\cdot(z\cdot y)\approx(x\cdot y)\cdot z$ and $x\cdot(y\cdot z)\approx z\cdot(y\cdot x)$ have appeared in [14] of Kazim and Naseeruddin.

The identities of mixed type have also been considered in the literature. A few are listed below:

- left distributivity: $x\cdot(y\cdot z)\approx(x\cdot y)\cdot(x\cdot z)$, appears, according to [18], already in the late 19th century publications of logicians Peirce and Schroeder (see [17] and [25], respectively),
- right distributive: $(z\cdot y)\cdot x\approx(z\cdot x)\cdot(y\cdot x)$ (see [26]),
- distributive if it is both left and right distributive (see [26]),
- medial: $(x\cdot y)\cdot(u\cdot v)\approx(x\cdot u)\cdot(y\cdot v)$ (see [26]),
- idempotent: $x\cdot x\approx x$ (see [26]),
- left involutory (or left symmetric): $x\cdot(x\cdot y)\approx y$ (see [26]).

Several identities of associative type have appeared in the literatiure on groupoids as well. For instance,

- $(x\cdot y)\cdot z\approx(z\cdot y)\cdot x$: Abel-Grassmann's groupoid (AG-groupoid) (see [21]),
- $(x\cdot y)\cdot z\approx(z\cdot y)\cdot x$ and $x\cdot(y\cdot z)\approx y\cdot(x\cdot z)$ (AG**-groupoid),
- $x\cdot(z\cdot y)\approx(x\cdot y)\cdot z$: Hosszú-Tarski identity (see [22]),
- $(x\cdot y)\cdot z\approx(z\cdot y)\cdot x$: Left almost semigroup (LA-semigroup) (see [22]),
- $x\cdot(y\cdot z)\approx z\cdot(y\cdot x)$: Right almost semigroup (RA-semigroup) (see [22]).

Similar to the problem mentioned in [10] for weak associative identities, the following general problem presents itself naturally if we restrict our attention to identities of associative type.

Problem. *Let $\mathcal{V}$ be a given variety of algebras (whose language includes a binary operation symbol, say, '$\to$'). Investigate the mutual relationships among the subvarieties of $\mathcal{V}$, each of which is defined by a single identity of associative type of length n, for small values of the positive integer n.*

We will now consider the above problem for the variety $\mathcal{I}$. We begin a systematic analysis of the relationships among the identities of associative type of length 3 relative to the variety $\mathcal{I}$.

Definition 1.1. An identity $p \approx q$, in the groupoid language $\langle\to\rangle$, is called an *identity of associative type of length* 3 if p and q have exactly 3 (distinct) variables, say x, y, z, and these variables are grouped according to one of the following two ways of grouping:

(a) $o \to (o \to o)$, (b) $(o \to o) \to o$.

In the rest of the paper, we refer to an "identity of associative type of length 3" as simply an "identity of associative type".

We wish to determine the mutual relationships of all the subvarieties of $\mathcal{I}$ defined by the identities of associative type, which will be referred to as "subvarieties of associative type".

Our main theorem says that there are 8 of such subvarieties of $\mathcal{I}$ that are distinct from each other and describes explicitly, by a Hasse diagram, the poset formed by them, together with the varieties $\mathcal{SL}$ and $\mathcal{BA}$. As an application, we show that there are 3 distinct subvarieties of $\mathcal{S}$ of associative type.

We would like to acknowledge that the software "Prover 9/Mace 4" developed by McCune [16] has been useful to us in some of our findings presented in this paper. We have used it to find examples and to check some conjectures.

2. Preliminaries

We refer the reader to the standard references [2], [4] and [23] for concepts and results used, but not explained, in this paper.

Recall from [24] that $\mathcal{SL}$ is the variety of semilattices with a least element 0. It was shown in [7] that $\mathcal{SL} = \mathcal{C} \cap \mathcal{I}_{1,0}$, where $\mathcal{I}_{1,0}$ is defined by $x' \approx x$, and $\mathcal{C}$ is defined by $x \to y \approx y \to x$, to relative to $\mathcal{I}$.

The two-element algebras $\mathbf{2_z}$, $\mathbf{2_s}$, $\mathbf{2_b}$ were introduced in [24]. Their operations $\to$ are respectively as follows:

$\to$	0	1
0	0	0
1	0	0

$\to$	0	1
0	0	1
1	1	1

$\to$	0	1
0	1	1
1	0	1

Recall that $\mathcal{V}(\mathbf{2_b}) = \mathcal{BA}$. Recall also from [7, Corollary 10.4] that $\mathcal{V}(\mathbf{2_s}) = \mathcal{SL}$.

The following lemmas will be useful in the sequel.

Lemma 2.1. [24, 7.16] *Let* $\mathbf{A}$ *be an* $\mathcal{I}$*-zroupoid. Then* $\mathbf{A} \models x''' \to y \approx x' \to y$.

Lemma 2.2. [7, 3.4] *Let* $\mathbf{A}$ *be an I-zroupoid. Then* $\mathbf{A}$ *satisfies:*

(a) $(x \to y) \to z \approx [(x \to y) \to z]''$,

(b) $(x \to y)' \approx (x'' \to y)'$.

Lemma 2.3. [24, 8.15] *Let* $\mathbf{A}$ *be an* $\mathcal{I}$*-zroupoid. Then the following are equivalent:*

1. $0' \to x \approx x$,
2. $x'' \approx x$,
3. $(x \to x')' \approx x$,
4. $x' \to x \approx x$.

Recall that $\mathcal{I}_{2,0}$ and $\mathcal{MC}$ are the subvarieties of $\mathcal{I}$, defined, respectively, by the equations

$$x'' \approx x. \tag{$I_{2,0}$}$$

$$x \wedge y \approx y \wedge x. \tag{MC}$$

Lemma 2.4. [24] *Let* $\mathbf{A} \in \mathcal{I}_{2,0}$. *Then*

1. $x' \to 0' \approx 0 \to x$,
2. $0 \to x' \approx x \to 0'$.

Lemma 2.5. *Let* $\mathbf{A} \in \mathcal{I}_{2,0}$. *Then* $\mathbf{A}$ *satisfies:*

(a) $(x \to 0') \to y \approx (x \to y') \to y$,

(b) $(y \to x) \to y \approx (0 \to x) \to y$,

(c) $0 \to x \approx 0 \to (0 \to x)$,

(d) $(0 \to x) \to (0 \to y) \approx x \to (0 \to y)$,

(e) $x \to y \approx x \to (x \to y)$,

(f) $0 \to (x \to y) \approx x \to (0 \to y)$,

(g) $0 \to (x \to y')' \approx 0 \to (x' \to y)$,

(h) $x \to (y \to x') \approx y \to x'$.

Proof. For the proofs of items (a), (b), (c), (f), (g), and (h) we refer the reader to [7]. The proofs of items (d) and (e) are in [5]. □

Theorem 2.6. [8] *Let* $t_i(\overline{x}), i = 1, \ldots, 6$ *be terms and* $\mathcal{V}$ *a subvariety of* $\mathcal{I}$. *If*

$$\mathcal{V} \cap \mathcal{I}_{2,0} \models [t_1(\overline{x}) \to t_2(\overline{x})] \to t_3(\overline{x}) \approx [t_4(\overline{x}) \to t_5(\overline{x})] \to t_6(\overline{x}),$$

then

$$\mathcal{V} \models [t_1(\overline{x}) \to t_2(\overline{x})] \to t_3(\overline{x}) \approx [t_4(\overline{x}) \to t_5(\overline{x})] \to t_6(\overline{x}).$$

2.1. Identities of associative type

We now turn our attention to identities of associative type of length 3. Recall that such an identity will contain three distinct variables that occur in any order and that are grouped in one of the two (obvious) ways. The following identities play a crucial role in the sequel.

Let Σ denote the set consisting of the following 14 identities of associative type (of length 3 in the binary language $\langle\rightarrow\rangle$):

$(A1)$ $x \rightarrow (y \rightarrow z) \approx (x \rightarrow y) \rightarrow z$ (Associative law)

$(A2)$ $x \rightarrow (y \rightarrow z) \approx x \rightarrow (z \rightarrow y)$

$(A3)$ $x \rightarrow (y \rightarrow z) \approx (x \rightarrow z) \rightarrow y$

$(A4)$ $x \rightarrow (y \rightarrow z) \approx y \rightarrow (x \rightarrow z)$

$(A5)$ $x \rightarrow (y \rightarrow z) \approx (y \rightarrow x) \rightarrow z$

$(A6)$ $x \rightarrow (y \rightarrow z) \approx y \rightarrow (z \rightarrow x)$

$(A7)$ $x \rightarrow (y \rightarrow z) \approx (y \rightarrow z) \rightarrow x$

$(A8)$ $x \rightarrow (y \rightarrow z) \approx (z \rightarrow x) \rightarrow y$

$(A9)$ $x \rightarrow (y \rightarrow z) \approx z \rightarrow (y \rightarrow x)$

$(A10)$ $x \rightarrow (y \rightarrow z) \approx (z \rightarrow y) \rightarrow x$

$(A11)$ $(x \rightarrow y) \rightarrow z \approx (x \rightarrow z) \rightarrow y$

$(A12)$ $(x \rightarrow y) \rightarrow z \approx (y \rightarrow x) \rightarrow z$

$(A13)$ $(x \rightarrow y) \rightarrow z \approx (y \rightarrow z) \rightarrow x$

$(A14)$ $(x \rightarrow y) \rightarrow z \approx (z \rightarrow y) \rightarrow x$.

We will denote by $\mathcal{A}_i$ the subvariety of $\mathcal{I}$ defined by the identity (Ai), for $1 \leqslant i \leqslant 14$. Such varieties will be referred to as subvarieties of $\mathcal{I}$ of associative type.

The following proposition is crucial for the rest of the paper.

Proposition 2.7. *Let $\mathcal{G}$ be the variety of all groupoids of type $\{\rightarrow\}$ and Let $\mathcal{V}$ denote the subvariety of $\mathcal{G}$ defined by a single identity of associative type. Then $\mathcal{V} = \mathcal{A}_i$, for some $i \in \{1, 2, \ldots, 14\}$.*

Proof. In an identity $p \approx q$ of associative type of length 3, p and q have exactly 3 (distinct) variables, say x,y,z, and these variables are grouped according to one of the two ways of bracketing mentioned above. Thus, there are six permuatations of 3 variables which give rise to the following 12 terms:

1a: $x \rightarrow (y \rightarrow z)$ 1b: $(x \rightarrow y) \rightarrow z$

2a: $x \rightarrow (z \rightarrow y)$ 2b: $(x \rightarrow z) \rightarrow y$

3a: $y \rightarrow (x \rightarrow z)$ 3b: $(y \rightarrow x) \rightarrow z$

4a: $y \rightarrow (z \rightarrow x)$ 4b: $(y \rightarrow z) \rightarrow x$

5a: $z \rightarrow (x \rightarrow y)$ 5b: $(z \rightarrow x) \rightarrow y$

6a: $z \rightarrow (y \rightarrow x)$ 6b: $(z \rightarrow y) \rightarrow x$.

It is clear that these 12 terms, in turn, will lead to 66 identities in view of the symmetric property of equality. It is routine to verify that each of the 66 identities is equivalent to one of the 14 identities of Σ in the variety of groupoids. Then the proposition follows. □

Our goal, in this paper, is to determine the distinct subvarieties of $\mathcal{I}$ and to describe the poset of subvarieties of $\mathcal{I}$ of associative type. It suffices to concentrate on the varieties defined by identities (A1)-(A14), in view of the above proposition.

3. Properties of subvarieties of $\mathcal{I}$ of associative type

In this section we present properties of several subvarieties of $\mathcal{I}$ which will play a crucial role in our analysis of the identities of associative type relative to $\mathcal{I}$.

Lemma 3.1. *Let* $\mathbf{A} \in \mathcal{I}$ *such that* $\mathbf{A} \models x' \to y \approx x \to y'$, *then* $\mathbf{A} \models (x \to y) \to y' \approx x \to y'$.

Proof. Let $a, b \in A$. Then $(a \to b) \to b' \overset{2.5(a)\,\&\,2.6}{=} (a \to 0') \to b' \overset{hyp}{=} (a' \to 0) \to b' = a'' \to b' \overset{hyp}{=} a''' \to b \overset{2.1}{=} a' \to b \overset{hyp}{=} a \to b'$. □

Lemma 3.2. *Let* $\mathbf{A} \in \mathcal{I}_{2,0}$ *such that* $\mathbf{A} \models (x \to y)' \approx x \to (0 \to y)$, *then* $\mathbf{A} \models x \to y' \approx x \to (0 \to y)$.

Proof. Let $a, b \in A$. Then $a \to b' \overset{2.3(1)}{=} a \to (0' \to b)' \overset{hyp}{=} a \to [0' \to (0 \to b)] \overset{2.3(1)}{=} a \to (0 \to b)$. □

Lemma 3.3. *Let* $\mathbf{A} \in \mathcal{I}_{2,0}$ *such that* $\mathbf{A} \models (x \to y)' \approx x \to (0 \to y)$. *Then* $\mathbf{A} \models [x \to (y \to z)']' \approx x \to (y \to (0 \to z))'$.

Proof. Let $a, b, c \in A$. We have that $[a \to (b \to c)']' \overset{hyp}{=} a \to (0 \to (b \to c)') \overset{hyp}{=} a \to (0 \to (b \to (0 \to c))) \overset{2.5(f)}{=} a \to (b \to (0 \to (0 \to c))) \overset{hyp}{=} a \to [b \to (0 \to c)']$. □

Lemma 3.4. *Let* $\mathbf{A} \in \mathcal{I}$ *such that* $\mathbf{A}$ *satisfies:*

(1) $(x \to y)' \approx x \to (0 \to y)$,

(2) $x' \to y \approx x \to y'$.

Then, $\mathbf{A} \models 0 \to [x \to (y \to z)] \approx 0 \to [(x \to y) \to z]$.

Proof. Let $a, b, c \in A$. Then, $0 \to [(a \to b) \to c] \overset{(I)}{=} 0 \to [(c' \to a) \to (b \to c)']' \overset{(I)}{=} 0 \to \{[(b \to c)'' \to c'] \to [a \to (b \to c)']\}'' \overset{2.6}{=} 0 \to \{[(b \to c) \to c'] \to [a \to (b \to c)']\}'' \overset{3.1}{=} 0 \to \{[b \to c'] \to [a \to (b \to c)']\}'' \overset{3.2\,\&\,2.6\,\&\,hyp}{=} 0 \to \{[b \to (0 \to c)] \to$

$[a \to (b \to c)']\}'' \overset{3.3\,\&\,hyp}{=} 0 \to \{[b \to (0 \to c)] \to [a \to [b \to (0 \to c)]']\}'' \overset{2.5(h)\,\&\,2.6}{=} 0 \to \{a \to [b \to (0 \to c)]'\}'' \overset{(3.4)}{=} 0 \to \{a \to [b \to c]''\}'' \overset{2.6}{=} 0 \to \{a \to [b \to c]\}'' \overset{(3.4)}{=} 0' \to \{a \to [b \to c]\}' \overset{(3.4)}{=} 0'' \to \{a \to [b \to c]\} = 0 \to \{a \to [b \to c]\}$. □

Lemma 3.5. *Let* $\mathbf{A} \in \mathcal{I}$ *such that* $\mathbf{A} \models (x \to y)' \approx (y \to x)'$. *Then* $\mathbf{A} \models (x \to y) \to z \approx (y \to x) \to z$.

Proof. Let $a, b, c \in A$. Then, $(a \to b) \to c \overset{2.6}{=} (a \to b)'' \to c \overset{hyp}{=} (b \to a)'' \to c \overset{2.6}{=} (b \to a) \to c$. □

Definition 3.6. Let $\mathbf{A} \in \mathcal{I}$. We say that $\mathcal{A}$ is of *type* 1 if the following identities hold in $\mathbf{A}$:

$(E1)$ $(x \to y)' \approx x \to (0 \to y)$,

$(E2)$ $x' \to y \approx x \to y'$,

$(E3)$ $0 \to (x \to y) \approx 0 \to (y \to x)$,

$(E4)$ $x \to (y \to z) \approx (p(x) \to p(y)) \to p(z)$, where p is some permutation of $\{x, y, z\}$.

Theorem 3.7. *If* $\mathbf{A} \in \mathcal{I}$ *is of type 1 then* $\mathbf{A} \models (Aj)$ *for all* $1 \leqslant j \leqslant 14$.

Proof. Let $\mathbf{A} \in \mathcal{I}$ be of type 1, and $a, b, c \in A$. In view of equations $(E1)$, $(E2)$ and Lemma 3.4 we have that

$$\mathbf{A} \models 0 \to [x \to (y \to z)] \approx 0 \to [(x \to y) \to z]. \tag{3.1}$$

Then we can consider the following cases.

- Assume that $j = 1$. Then $a \to (b \to c) \overset{(E4)}{=} (p(a) \to p(b)) \to p(c) \overset{2.2}{=} [(p(a) \to p(b)) \to p(c)]'' \overset{(E1)}{=} [(p(a) \to p(b)) \to (0 \to p(c))]' \overset{2.5(f)\,\&\,2.6}{=} [0 \to [(p(a) \to p(b)) \to p(c)]]' \overset{(E3)\,\&\,(3.1)}{=} [0 \to [(a \to b) \to c]]' \overset{2.5(f)\,\&\,2.6}{=} [(a \to b) \to [0 \to c]]' \overset{(E1)}{=} [(a \to b) \to c]'' \overset{2.2}{=} (a \to b) \to c$.

  The cases $j = 3, 5, 7, 8, 10$ are similar.

- Assume that $j = 2$. Then, in the same way as in the case of $j = 1$ we have that

  $$\mathbf{A} \models x \to (y \to z) \approx [0 \to [(p(x) \to p(y)) \to p(z)]]'. \tag{3.2}$$

  Then, $a \to (b \to c) \overset{(3.2)}{=} [0 \to [(p(a) \to p(b)) \to p(c)]]' \overset{(E3)\,\&\,(3.1)}{=} [0 \to [(p(a) \to p(c)) \to p(b)]]' \overset{2.5(f)\,\&\,2.6}{=} [(p(a) \to p(c)) \to [0 \to p(b)]]' \overset{(E1)}{=} [(p(a) \to p(c)) \to p(b)]'' \overset{2.2(a)}{=} (p(a) \to p(c)) \to p(b) \overset{(E4)}{=} (a \to c) \to b$.

  The cases $j = 4, 6, 9$ are similar.

- Assume that $j = 11$. $(a \to b) \to c \overset{2.2(a)}{=} [(a \to b) \to c]'' \overset{(E1)}{=} [(a \to b) \to (0 \to c)]' \overset{2.5(f)\,\&\,2.6}{=} [0 \to [(a \to b) \to c]]' \overset{(E3)\,\&\,(3.1)}{=} [0 \to [(a \to c) \to b]]' \overset{2.5(f)\,\&\,2.6}{=} [(a \to c) \to [0 \to b]]' \overset{(E1)}{=} [(a \to c) \to b]'' \overset{2.2}{=} (a \to c) \to b$.

  The cases $j = 12, 13, 14$ are similar. □

To prove that the variety $\mathcal{A}_j$ is of type 1, with $j \in \{3, 5, 7, 8, 10\}$, we need the following lemmas.

Lemma 3.8. *If* $\mathbf{A} \in \mathcal{A}_5$ *then* $\mathbf{A}$ *satisfies*

(a) $x' \to y \approx x \to y'$,

(b) $(x \to y)' \approx 0 \to (x \to y)$,

(c) $x \to (0 \to y) \approx 0 \to (x \to y)$.

Proof. Let $a, b \in A$. Then

(a) $a \to b' = a \to (b \to 0) \overset{(A5)}{=} (b \to a) \to 0 \overset{2.6}{=} (b \to a'') \to 0 = (b \to (a' \to 0)) \to 0 \overset{(A5)}{=} [(a' \to b) \to 0] \to 0 = (a' \to b)'' \overset{2.6}{=} a' \to b$.

(b) Observe that $(a \to b)' = (a \to b) \to 0 \overset{(A5)}{=} b \to (a \to 0) = b \to a' \overset{3.8(a)}{=} b' \to a = (b \to 0) \to a \overset{(A5)}{=} 0 \to (b \to a)$.

(c) Notice that $0 \to (a \to b) \overset{(A5)}{=} (a \to 0) \to b \overset{2.6}{=} (a'' \to 0) \to b \overset{3.8(a)}{=} (a' \to 0') \to b \overset{2.4(2)\,\&\,2.6}{=} (0 \to a) \to b \overset{(A5)}{=} a \to (0 \to b)$.

□

Lemma 3.9. *If* $\mathbf{A} \in \mathcal{A}_8$ *then* $\mathbf{A}$ *satisfies:*

(a) $x \to y' \approx x' \to y'$,

(b) $x \to y' \approx 0 \to (y' \to x)$.

Proof. Let $a, b \in A$. Then $a \to b' = a \to (b \to 0) \overset{(A8)}{=} (0 \to a) \to b \overset{(I)}{=} [(b' \to 0) \to (a \to b)']' = [(b' \to 0) \to (a \to b)'] \to 0 \overset{(A8)}{=} (a \to b)' \to (0 \to (b' \to 0)) \overset{(A8)}{=} (a \to b)' \to ((0 \to 0) \to b') = (a \to b)' \to (0' \to b') \overset{2.3(1)\,\&\,2.6}{=} (a \to b)' \to b' = ((a \to b) \to 0) \to b' \overset{(A8)}{=} 0 \to (b' \to (a \to b)) \overset{(A8)}{=} 0 \to ((b \to b') \to a) \overset{2.6}{=} 0 \to ((b'' \to b') \to a) \overset{2.3(4)\,\&\,2.6}{=} 0 \to (b' \to a)$, implying that $\mathbf{A}$ satisfies the identity (b). Next, $0 \to (b' \to a) \overset{(A8)}{=} (a \to 0) \to b' = a' \to b'$, thus $\mathbf{A}$ satisfies the identity (a). □

Lemma 3.10. *If* $\mathbf{A} \in \mathcal{A}_{10}$ *then* $\mathbf{A}$ *satisfies:*

(a) $[0 \to (x \to y)]' \approx x \to y'$,

(b) $(y \to x)'' \approx x \to y'$,

(c) $(x \to y)' \approx x \to y'$.

Proof. Let $a, b \in A$.

(a) We have that $\mathbf{A} \models [0 \to (x \to y)]' \approx x \to y'$, since

$$\begin{array}{rcll}
a \to b' & = & a \to (b \to 0) & \\
& = & (0 \to b) \to a & \text{by (A10)} \\
& = & [(a' \to 0) \to (b \to a)']' & \text{by (I)} \\
& = & [((a \to 0) \to 0) \to (b \to a)']' & \\
& = & [(0 \to (0 \to a)) \to (b \to a)']' & \text{by (A10)} \\
& = & [(0 \to a) \to (b \to a)']' & \text{by 2.5 (c) and 2.6} \\
& = & [(0 \to a) \to [(b \to a) \to 0]]' & \\
& = & [(0 \to a) \to [0 \to (a \to b)]]' & \text{by (A10)} \\
& = & [(0 \to a) \to [(0 \to a) \to (0 \to b)]]' & \text{by 2.5 (f) and (d) and by 2.6} \\
& = & [(0 \to a) \to (0 \to b)]' & \text{by 2.5 (e) and 2.6} \\
& = & [0 \to (a \to b)]' & \text{by 2.5 (d), (f) and by 2.6.}
\end{array}$$

(b) Observe that $a \to b' \overset{3.10(a)}{=} [0 \to (a \to b)]' \overset{(A10)}{=} [(b \to a) \to 0]' = (b \to a)''$. Hence, $\mathbf{A} \models$ (b).

(c) Since $a \to b' \overset{3.10(a)}{=} [0 \to (a \to b)]' \overset{2.5(c)\,\&\,2.6}{=} [0 \to (0 \to (a \to b))]' \overset{(A10)}{=} [((a \to b) \to 0) \to 0]' = (a \to b)''' = (a \to b)'$, we conclude that $\mathbf{A} \models$ (c).

□

Lemma 3.11. *If* $\mathbf{A} \in \mathcal{A}_3 \cup \mathcal{A}_5 \cup \mathcal{A}_7 \cup \mathcal{A}_8 \cup \mathcal{A}_{10}$ *then* $\mathbf{A}$ *satisfies*

(1) $(x \to y)' \approx x \to (0 \to y)$,

(2) $x' \to y \approx x \to y'$ *and*

(3) $0 \to (x \to y) \approx 0 \to (y \to x)$.

Proof. Let $a, b \in A$.

- Suppose $\mathbf{A} \in \mathcal{A}_3$. Then $(a \to b)' = (a \to b) \to 0 \overset{(A3)}{=} a \to (0 \to b)$, implying $\mathbf{A} \models$ (1). Observe that $a' \to b = (a \to 0) \to b \overset{(A3)}{=} a \to (b \to 0) = a \to b'$. So, (2) holds in $\mathbf{A}$. Also, $0 \to (a \to b) \overset{(A3)}{=} (0 \to b) \to a \overset{(I)}{=} [(a' \to 0) \to (b \to a)']' = [a'' \to (b \to a)']' \overset{2.6}{=} [a \to (b \to a)']' \overset{(3.11)}{=} [a' \to (b \to a)]' \overset{2.5(h)\,\&\,2.6}{=} (b \to a)' \overset{2.3(1)\,\&\,2.6}{=} 0' \to (b \to a)' \overset{3.11(2)}{=} 0'' \to (b \to a) = 0 \to (b \to a)$, proving that (3) holds in $\mathbf{A}$.

- Assume that $\mathbf{A} \in \mathcal{A}_5$. Then $(a \to b)' \overset{3.8(b)}{=} 0 \to (b \to a) = 0'' \to (b \to a) \overset{3.8(a)}{=} 0' \to (b \to a)' \overset{2.3(1)\,\&\,2.6}{=} (b \to a)' = (b \to a) \to 0 \overset{(A5)}{=} a \to (b \to 0) = a \to b' \overset{3.8(a)}{=} a' \to b \overset{2.3(1)\,\&\,2.6}{=} (0' \to a') \to b \overset{3.8(a)}{=} (0 \to a'') \to b \overset{2.6}{=} (0 \to a) \to b \overset{(A5)}{=} a \to (0 \to b)$, proving that (1) is true in $\mathbf{A}$. (2) is immediate from Lemma 3.8 (a). Next, $0 \to (a \to b) \overset{3.8(b)}{=} (a \to b)' = (a \to b) \to 0 \overset{(A5)}{=} b \to (a \to 0) = b \to a' \overset{3.8(a)}{=} b' \to a \overset{2.6}{=} (b' \to a)'' \overset{3.8(a)}{=} (b \to a')'' \overset{3.8(b)}{=} [0 \to (b \to a')]' \overset{3.8(c)}{=} [b \to (0 \to a')]' \overset{3.8(a)}{=} [b \to (0' \to a)]' \overset{2.3(1)\,\&\,2.6}{=} (b \to a)' \overset{3.8(b)}{=} 0 \to (b \to a)$, proving (3) holds in $\mathbf{A}$.

- Assume that $\mathbf{A} \in \mathcal{A}_7$. Then $(a \to b)' \overset{2.6}{=} (a \to b)''' = [(a \to b) \to 0]'' \overset{(A7)}{=} [0 \to (a \to b)]'' \overset{2.5(f)\,\&\,2.6}{=} [a \to (0 \to b)]'' \overset{(A7)}{=} [(0 \to b) \to a]'' \overset{2.6}{=} (0 \to b) \to a \overset{(A7)}{=} a \to (0 \to b)$, proving that $\mathbf{A}$ satisfies (1).

  Next, $a' \to b \overset{2.6}{=} [a' \to b]'' = [(a' \to b) \to 0]' \overset{(A7)}{=} [0 \to (a' \to b)]' \overset{2.6}{=} [0 \to (a' \to b'')]' \overset{2.5(g)\,\&\,2.6}{=} [0 \to (a \to b')']' = [0 \to ((a \to b') \to 0)]' \overset{(A7)}{=} [0 \to (0 \to (a \to b'))]' \overset{2.5(c)\,\&\,2.6}{=} [0 \to (a \to b')]' = [0 \to (a \to b')] \to 0 \overset{(A7)}{=} [(a \to b') \to 0] \to 0 = (a \to b')'' = (a \to (b \to 0))'' \overset{(A7)}{=} ((b \to 0) \to a)'' \overset{2.6}{=} (b \to 0) \to a \overset{(A7)}{=} a \to (b \to 0) = a \to b'$, proving that (2) is true in $\mathbf{A}$. Finally, observe that $0 \to (a \to b) \overset{(A7)}{=} (a \to b) \to 0 \overset{2.6}{=} (a'' \to b) \to 0 = [(a' \to 0) \to b] \to 0 \overset{(A7)}{=} [b \to (a' \to 0)] \to 0 = [b \to a''] \to 0 \overset{2.6}{=} [b \to a] \to 0 \overset{(A7)}{=} 0 \to (b \to a)$, proving that (3) holds in $\mathbf{A}$.

- Let $\mathbf{A} \in \mathcal{A}_8$. First, we will prove (2) hold in $\mathbf{A}$. Now, $a \to b' \overset{3.9(b)}{=} 0 \to (b' \to a) \overset{2.6}{=} 0 \to (b' \to a'') \overset{3.9(a)}{=} 0 \to (b'' \to a'') \overset{(A8)}{=} (a'' \to 0) \to b'' \overset{2.6}{=} (a'' \to 0) \to b = a''' \to b \overset{2.1}{=} a' \to b$, proving (2).

  Notice that $a \to (0 \to b) \overset{(A8)}{=} (b \to a) \to 0 = (b \to a)' \overset{2.6}{=} (b \to a)''' = (b \to a)'' \to 0 \overset{(2)}{=} (b \to a)' \to 0' \overset{2.3(1)\,\&\,2.6}{=} [0' \to (b \to a)'] \to 0' \overset{(2)}{=} [0'' \to (b \to a)] \to 0' = [0 \to (b \to a)] \to 0' \overset{2.5(f)\,\&\,2.6}{=} [b \to (0 \to a)] \to 0' \overset{(A8)}{=} [(a \to b) \to 0] \to 0' = (a \to b)' \to 0' \overset{(2)}{=} (a \to b) \to 0'' = (a \to b) \to 0 = (a \to b)'$, proving (1) holds in $\mathbf{A}$.

  The identity

$$0 \to (x \to y) \approx (x \to y)' \tag{3.3}$$

  holds in $\mathbf{A}$, since $0 \to (a \to b) = 0'' \to (a \to b) \overset{(2)}{=} 0' \to (a \to b)' \overset{2.3(1)\,\&\,2.6}{=} (a \to b)'$.

Then $0 \to (a \to b) \overset{(3.3)}{=} (a \to b)' = (a \to b) \to 0 \overset{(A8)}{=} b \to (0 \to a) \overset{(1)}{=} (b \to a)' \overset{(3.3)}{=} 0 \to (b \to a)$, proving (3) is true in $\mathbf{A}$.

- Assume that $\mathbf{A} \in \mathcal{A}_{10}$. Hence

$$\begin{array}{rcll} a' \to b & = & a' \to b'' & \text{by 2.6} \\ & = & (a' \to b')' & \text{by 3.10 (c)} \\ & = & (a' \to b') \to 0 & \\ & = & 0 \to (b' \to a') & \text{by (A10)} \\ & = & 0 \to (b' \to (a \to 0)) & \\ & = & 0 \to ((0 \to a) \to b') & \text{by (A10)} \\ & = & (b' \to (0 \to a)) \to 0 & \text{by (A10)} \\ & = & (b' \to (0 \to a))' & \\ & = & ((b \to 0) \to (0 \to a))' & \\ & = & [(0 \to a) \to (0 \to b)]' & \text{by (A10)} \\ & = & [0 \to (a \to b)]' & \text{by 2.5 (f) \& (d) and by 2.6} \\ & = & [(b \to a) \to 0]' & \text{by (A10)} \\ & = & (b \to a)'' & \\ & = & a \to b' & \text{by 3.10 (b),} \end{array}$$

proving (2) holds in $\mathbf{A}$.

Consider $a \to (0 \to b) \overset{(A10)}{=} (b \to 0) \to a \overset{(I)}{=} [(a' \to b) \to (0 \to a)']' \overset{3.10(c)}{=} [(a' \to b) \to (0 \to a')]' \overset{(2)}{=} [(a' \to b) \to (0' \to a)]' \overset{2.3(1)\,\&\,2.6}{=} [(a' \to b) \to a]' \overset{(2)}{=} [(a \to b') \to a]' \overset{2.5(b)\,\&\,2.6}{=} [(0 \to b') \to a]' \overset{(A10)}{=} [a \to (b' \to 0)]' = [a \to b'']' \overset{2.6}{=} (a \to b)'$, proving (1).

To finish off the proof, $0 \to (a \to b) \overset{(A10)}{=} (b \to a) \to 0 \overset{3.10(c)}{=} b \to a' \overset{(2)}{=} b' \to a = (b \to 0) \to a \overset{(A10)}{=} a \to (0 \to b) \overset{(1)}{=} (a \to b)' = (a \to b) \to 0 \overset{(A10)}{=} 0 \to (b \to a)$.

□

Theorem 3.12. $\mathcal{A}_3 = \mathcal{A}_5 = \mathcal{A}_7 = \mathcal{A}_8 = \mathcal{A}_{10}$.

Proof. Let $\mathbf{A} \in \mathcal{A}_3 \cup \mathcal{A}_5 \cup \mathcal{A}_7 \cup \mathcal{A}_8 \cup \mathcal{A}_{10}$. By Lemma 3.11 we have that $\mathbf{A}$ is of type 1. Then, using Theorem 3.7, $\mathbf{A} \in \mathcal{A}_j$ for all $j \in \{3, 5, 7, 8, 10\}$. □

Lemma 3.13. *If* $\mathbf{A} \in \mathcal{A}_{13}$ *then* $\mathbf{A}$ *satisfies*

(a) $(x \to y)' \approx (0 \to x) \to y$,

(b) $(x \to y)' \approx x' \to y'$,

(c) $(x \to y)' \approx (0 \to y) \to x'$,

(d) $(x \to y)' \approx (x \to y)''$,

(e) $(x \to y)' \approx (y \to x)'$.

Proof. Let us consider $a, b \in A$.

(a) $(a \to b)' = (a \to b) \to 0 \overset{(A13)}{=} (b \to 0) \to a \overset{(A13)}{=} (0 \to a) \to b$. Hence $\mathbf{A} \models$ (a).

(b) Observe that $(a \to b)' \overset{2.6}{=} 0' \to (a \to b)' = (0 \to 0) \to (a \to b)' \overset{(A13)}{=} [0 \to (a \to b)'] \to 0 \overset{(I20)\,\&\,2.6}{=} [0 \to (a \to b'')'] \to 0 \overset{2.5(g)\,\&\,2.6}{=} [0 \to (a' \to b')] \to 0 \overset{(A13)}{=} [(a' \to b') \to 0] \to 0 = (a' \to b')'' \overset{2.6}{=} a' \to b'$

(c) Observe $(a \to b)' \overset{(a)}{=} (0 \to a) \to b \overset{2.6}{=} (0 \to a)'' \to b \overset{(b)}{=} (0' \to a')' \to b \overset{2.6}{=} a'' \to b \overset{(A13)}{=} (0 \to b) \to a'$.

(d) Note that $(a \to b)' \overset{(c)}{=} (0 \to b) \to a' \overset{(I)}{=} [(a'' \to 0) \to (b \to a')']' = [a''' \to (b \to a')']' \overset{2.1}{=} [a' \to (b \to a')']' \overset{(b)}{=} [a' \to (b' \to a'')]' \overset{2.6}{=} [a' \to (b' \to a)]' \overset{2.5(h)\,\&\,2.6}{=} (b' \to a)' \overset{(A13)}{=} ((0 \to a) \to b)' \overset{(A13)}{=} ((a \to b) \to 0)' = (a \to b)''$.

(e) We have $(b \to a)' \overset{(c)}{=} (0 \to a) \to b' \overset{2.6}{=} [(0 \to a) \to b']'' \overset{(b)}{=} [(0 \to a)' \to b'']' \overset{(d)}{=} [(0 \to a)'' \to b'']' \overset{2.6}{=} [(0 \to a) \to b]' \overset{(d)}{=} [(0 \to a) \to b]'' \overset{2.6}{=} (0 \to a) \to b \overset{(a)}{=} (a \to b)'$.

□

Theorem 3.14. $\mathcal{A}_{11} = \mathcal{A}_{12} = \mathcal{A}_{13}$.

Proof. Let us consider $\mathbf{A} \in \mathcal{A}_{11}$ and $a, b, c \in A$. Hence $(a \to b) \to c \overset{2.3(1)\,\&\,2.6}{=} ((0' \to a) \to b) \to c \overset{(A11)}{=} ((0' \to b) \to a) \to c \overset{2.3(1)\,\&\,2.6.}{=} (b \to a) \to c$. Hence, $\mathbf{A} \in \mathcal{A}_{12}$, implying $A_{11} \subseteq A_{12}$.

Now assume that $\mathbf{A} \in \mathcal{A}_{12}$ and $a, b, c \in A$. Then $(a \to b) \to c \overset{(I)}{=} [(c' \to a) \to (b \to c)']' \overset{(I)}{=} \{[(b \to c)'' \to c'] \to [a \to (b \to c)']'\}'' \overset{2.6}{=} \{[(b \to c) \to c'] \to [a \to (b \to c)']'\}'' \overset{(A12)}{=} \{[c' \to (b \to c)] \to [a \to (b \to c)']'\}'' \overset{2.5(h)\,\&\,2.6}{=} \{(b \to c) \to [a \to (b \to c)']'\}'' \overset{(A12)}{=} \{[a \to (b \to c)']' \to (b \to c)\}'' = \{[[a \to (b \to c)'] \to 0] \to (b \to c)\}'' \overset{(A12)}{=} \{[0 \to [a \to (b \to c)']] \to (b \to c)\}'' \overset{2.5(b)\,\&\,2.6}{=} \{[(b \to c) \to [a \to (b \to c)']] \to (b \to c)\}'' \overset{2.5(h)\,\&\,2.6}{=} \{[a \to (b \to c)'] \to (b \to c)\}'' \overset{2.5(a)\,\&\,2.6}{=} \{[a \to 0'] \to (b \to c)\}'' \overset{(A12)}{=} \{[0' \to a] \to (b \to c)\}'' \overset{2.3(1)\,\&\,2.6}{=} \{a \to (b \to c)\}'' \overset{(A12)}{=} \{(b \to c) \to a\}'' \overset{2.6}{=} (b \to c) \to a$, which implies that $A_{12} \subseteq A_{13}$.

If $\mathbf{A} \in \mathcal{A}_{13}$ and $a, b, c \in A$, then $(a \to b) \to c \overset{(A13)}{=} (b \to c) \to a \overset{(A13)}{=} (c \to a) \to b \overset{2.6}{=} (c \to a)'' \to b \overset{3.13(e)}{=} (a \to c)'' \to b \overset{2.6}{=} (a \to c) \to b$, concluding that $A_{13} \subseteq A_{11}$. □

4. Main theorem

In this section we will prove our main theorem. But first we need one more lemma.

Lemma 4.1. *If* $\mathbf{A} \in \mathcal{A}_2 \cup \mathcal{A}_6 \cup \mathcal{A}_9$ *then* $\mathbf{A} \in \mathcal{A}_{11}$.

Proof. We will see that $\mathbf{A} \models (x \to y)' \approx (y \to x)'$.
Let $a, b \in A$.

- If $\mathbf{A} \in \mathcal{A}_2$, $(a \to b) \to 0 \overset{2.3(1)\,\&\,2.6}{=} (0' \to (a \to b)) \to 0 \overset{(A2)}{=} (0' \to (b \to a)) \to 0 \overset{2.3(1)\,\&\,2.6}{=} (b \to a) \to 0$.
- If $\mathbf{A} \in \mathcal{A}_6$, $(a \to b) \to 0 \overset{2.3(1)\,\&\,2.6}{=} (0' \to (a \to b)) \to 0 \overset{(A6)}{=} (a \to (b \to 0')) \to 0 \overset{(A6)}{=} (b \to (0' \to a)) \to 0 \overset{2.3(1)\,\&\,2.6}{=} (b \to a) \to 0$.
- If $\mathbf{A} \in \mathcal{A}_9$, then

$$\begin{array}{rcll} (a \to b)' & = & (a \to b) \to 0 & \\ & = & (a \to (0' \to b)) \to 0 & \text{by 2.3 (1) and 2.6} \\ & = & (b \to (0' \to a)) \to 0 & \text{by (A9)} \\ & = & (b \to a) \to 0 & \text{by 2.3 (1) and 2.6} \\ & = & (b \to a)' & \end{array}$$

Now, apply Lemma 3.5, to get $\mathbf{A} \in A_{12}$. Therefore, using Theorem 3.14, we conclude $\mathbf{A} \in \mathcal{A}_{11}$. □

We are now ready to present the main theorem of this paper.

Theorem 4.2. *We have*

(a) *The following are the* 8 *subvarieties of* $\mathcal{I}$ *of associative type that are distinct from each other.*

$$\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4, \mathcal{A}_6, \mathcal{A}_9, \mathcal{A}_{11} \text{ and } \mathcal{A}_{14}.$$

(b) *They satisfy the following relationships:*

1. $\mathcal{SL} \subset \mathcal{A}_3 \subset \mathcal{A}_4$,
2. $\mathcal{BA} \subset \mathcal{A}_4 \subset \mathcal{I}$,
3. $\mathcal{A}_3 \subset \mathcal{A}_1 \subset \mathcal{I}$,
4. $\mathcal{A}_3 \subset \mathcal{A}_2 \subset \mathcal{A}_{11}$, $\mathcal{A}_3 \subset \mathcal{A}_6 \subset \mathcal{A}_{11}$ *and* $\mathcal{A}_3 \subset \mathcal{A}_9 \subset \mathcal{A}_{11}$,
5. $\mathcal{A}_{11} \subset \mathcal{A}_{14} \subset \mathcal{I}$.

Proof. Observe that, in view of Theorem 3.12 and Theorem 3.14 we can conclude that each of the 14 subvarieties of associative type of $\mathcal{I}$ is equal to one of the following varieties:

$$\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4, \mathcal{A}_6, \mathcal{A}_9, \mathcal{A}_{11}, \mathcal{A}_{14}.$$

We first wish to prove (b). Notice that by Lemma 3.11 we have that $\mathbf{A} \in \mathcal{A}_3$ is of type 1. Then, using Theorem 3.7, $\mathbf{A} \in \mathcal{A}_j$ for all $1 \leqslant j \leqslant 14$. Hence

$$\mathcal{A}_3 \subseteq \mathcal{A}_j \text{ for all } 1 \leqslant j \leqslant 14. \tag{4.4}$$

1. Recall that $\mathcal{SL} = \mathcal{C} \cap I_{1,0}$. Then, we get $\mathcal{C} \subseteq \mathcal{A}_1$ and $\mathcal{I}_{1,0} \subseteq \mathcal{A}_1$ by [7, Theorem 8.2] and [7, Theorem 9.3], respectively, implying $\mathcal{SL} \subseteq \mathcal{A}_3$, and $\mathcal{A}_3 \subseteq \mathcal{A}_4$ by (4.4).

   The algebras $\mathbf{2_z}$ and $\mathbf{2_b}$ show that $\mathcal{SL} \neq \mathcal{A}_3$ and $\mathcal{A}_3 \neq \mathcal{A}_4$, respectively.

2. In view of [10] we have that $\mathcal{BA} \subset \mathcal{S}$. By [9, Lemma 3.1], $\mathcal{S} \models x \to (y \to z) \approx y \to (x \to z)$. Thus, $\mathcal{BA} \subseteq \mathcal{A}_4$.

   The algebra $\mathbf{2_s}$ shows that $\mathcal{BA} \neq \mathcal{A}_4$ and the following algebra shows that $\mathcal{A}_4 \neq \mathcal{I}$, respectively.

$\to$	0	1	2
0	0	0	0
1	2	0	0
2	0	0	0

3. The algebra $\mathbf{2_b}$ shows that $\mathcal{A}_1 \neq \mathcal{I}$ and the following algebra witnesses that $\mathcal{A}_3 \neq \mathcal{A}_1$.

$\to$	0	1	2
0	0	1	2
1	1	1	2
2	2	1	2

4. Using (4.4) and Lemma 4.1 we can conclude that $\mathcal{A}_3 \subseteq \mathcal{A}_2 \subseteq \mathcal{A}_{11}$, $\mathcal{A}_3 \subseteq \mathcal{A}_6 \subseteq \mathcal{A}_{11}$ and $\mathcal{A}_3 \subseteq \mathcal{A}_9 \subseteq \mathcal{A}_{11}$.

   The following algebras show that $\mathcal{A}_3 \neq \mathcal{A}_2$ and $\mathcal{A}_2 \neq \mathcal{A}_{11}$, respectively.

$\to$	0	1	2
0	0	0	0
1	2	0	2
2	0	0	0

$\to$	0	1	2
0	0	0	0
1	2	0	0
2	0	0	0

   The following algebras show that $\mathcal{A}_3 \neq \mathcal{A}_6$ and $\mathcal{A}_6 \neq \mathcal{A}_{11}$, respectively.

$\to$	0	1	2	3
0	0	0	0	0
1	0	2	3	0
2	0	0	0	0
3	0	0	0	0

$\to$	0	1	2
0	0	0	0
1	2	0	0
2	0	0	0

   The following algebras show that $\mathcal{A}_3 \neq \mathcal{A}_9$ and $\mathcal{A}_9 \neq \mathcal{A}_{11}$, respectively.

$\to$	0	1	2	3
0	0	0	0	0
1	0	2	3	0
2	0	0	0	0
3	0	0	0	0

$\to$	0	1	2
0	0	0	0
1	2	0	0
2	0	0	0

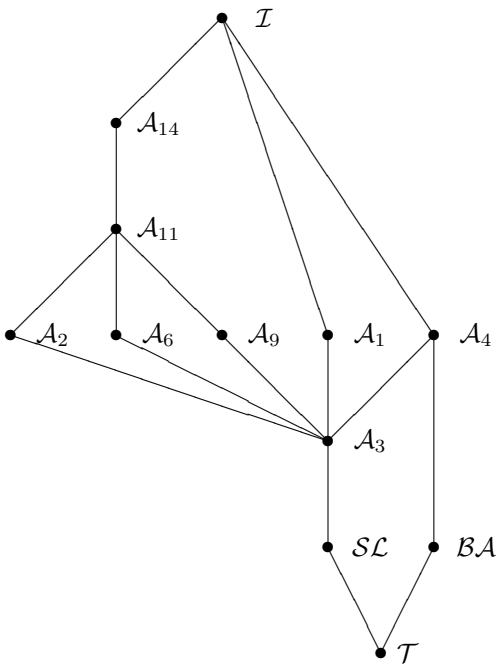
5. Let $\mathbf{A} \in \mathcal{A}_{11}$ and $a, b, c \in A$. By Theorem 3.14, $\mathcal{A}_{11} = \mathcal{A}_{12} = \mathcal{A}_{13}$. Hence $(a \to b) \to c \overset{(A13)}{=} (b \to c) \to a \overset{(A12)}{=} (c \to b) \to a$. Therefore $\mathcal{A}_{11} \subseteq \mathcal{A}_{14}$.

   The algebra $\mathbf{2_b}$ shows that $\mathcal{A}_{14} \neq \mathcal{I}$ and the following algebra shows that $\mathcal{A}_{11} \neq \mathcal{A}_{14}$.

$\to$	0	1	2	3
0	0	1	2	3
1	2	3	2	3
2	1	1	3	3
3	3	3	3	3

The proof of the theorem is now complete since (a) is an immediate consequence of (b). □

The Hasse diagram of the poset of subvarieties of $\mathcal{I}$ of associative type, together with $\mathcal{SL}$ and $\mathcal{BA}$, is:



5. Identities in symmetric implication zroupoids

Let $\mathbf{A} \in \mathcal{I}$. $\mathbf{A}$ is involutive if $\mathbf{A} \in \mathcal{I}_{2,0}$. $\mathbf{A}$ is meet-commutative if $\mathbf{A} \in \mathcal{MC}$. $\mathbf{A}$ is symmetric if $\mathbf{A}$ is both involutive and meet-commutative. Let $\mathcal{S}$ denote the variety of symmetric $\mathcal{I}$-zroupoids. In other words, $\mathcal{S} = \mathcal{I}_{2,0} \cap \mathcal{MC}$. The variety $\mathcal{S}$ was investigated in [7], [9] and [10] and has some interesting properties.

In this section we give an application of the main theorem, Theorem 4.2, to describe the poset of the subvarieties of the variety $\mathcal{S}$.

Lemma 5.1. [9, Lemma 3.1 (a)] *Let* $\mathbf{A} \in \mathcal{S}$. *Then* $\mathbf{A}$ *satisfies* $x \to (y \to z) \approx y \to (x \to z)$.

Lemma 5.2. [9, Lemma 2.1] $\mathcal{MC} \cap \mathcal{I}_{1,0} \subseteq \mathcal{C} \cap \mathcal{I}_{1,0} = \mathcal{SL}$.

Lemma 5.3. [9, Lemma 3.2] *Let* $\mathbf{A} \in \mathcal{S}$ *such that* $\mathbf{A} \models x \to x \approx x$. *Then* $\mathbf{A} \models x' \approx x$.

Lemma 5.4. $\mathcal{A}_{11} \cap \mathcal{S} = \mathcal{SL}$.

Proof. Let $\mathbf{A} \in \mathcal{A}_{11} \cap \mathcal{S}$ and $a \in A$. Since $\mathcal{S} \subseteq \mathcal{I}_{2,0}$, we have

$$\begin{array}{rcll} a & = & a' \to a & \text{by Lemma 2.3 (4)} \\ & = & (0' \to a') \to a & \text{by Lemma 2.3 (1)} \\ & = & (0' \to a) \to a' & \text{by (A11)} \\ & = & a \to a' & \text{by Lemma 2.3 (1)} \\ & = & a'' \to a' & \\ & = & a' & \text{by Lemma 2.3 (4).} \end{array}$$

Therefore, $\mathbf{A} \models x \approx x'$. Then, by Lemma 5.2, $\mathbf{A} \in \mathcal{SL}$. □

Lemma 5.5. $\mathcal{A}_1 \cap \mathcal{S} \subseteq \mathcal{SL}$.

Proof. Let $\mathbf{A} \in \mathcal{A}_1 \cap \mathcal{S}$ and $a \in A$. Then

$$\begin{array}{rcll} a & = & 0' \to a & \text{by Lemma 2.3 (1)} \\ & = & (0 \to 0) \to a & \\ & = & 0 \to (0 \to a) & \text{by (A1)} \\ & = & 0 \to a & \text{by Lemma 2.5 (c).} \end{array}$$

Consequently,

$$\mathbf{A} \models x \approx 0 \to x. \tag{5.5}$$

Therefore,

$$\begin{array}{rcll} a & = & a' \to a & \text{by Lemma 2.3 (4)} \\ & = & (a \to 0) \to a & \\ & = & a \to (0 \to a) & \text{by (A1)} \\ & = & a \to a & \text{by equation (5.5)} \end{array}$$

Thus, by Lemma 5.3, $\mathbf{A} \models x' \approx x$. Using Lemma 5.2 we can conclude the proof. □

We will denote by $\mathcal{S}_i$ the variety $\mathcal{A}_i \cap \mathcal{S}$ with $1 \leqslant i \leqslant 14$.

Proposition 5.6. *Each of the* 14 *subvarieties of associative type of* $\mathcal{S}$ *is equal to one of the following varieties:*

$$\mathcal{SL},\ \mathcal{S}_{14},\ \mathcal{S}.$$

Proof. From Theorem 3.12 and Theorem 3.14 we know that each of the 14 subvarieties of associative type of $\mathcal{I}$ is equal to one of the following varieties:

$$\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4, \mathcal{A}_6, \mathcal{A}_9, \mathcal{A}_{11}, \mathcal{A}_{14}.$$

Using Theorem 4.2, Lemma 5.4 and Lemma 5.5 we have that

$$\mathcal{SL} \subseteq \mathcal{S}_3 \subseteq \mathcal{S}_2 \subseteq \mathcal{S}_{11} \subseteq \mathcal{SL},$$

$$\mathcal{SL} \subseteq \mathcal{S}_6 \subseteq \mathcal{S}_{11} \subseteq \mathcal{SL},$$

$$\mathcal{SL} \subseteq \mathcal{S}_9 \subseteq \mathcal{S}_{11} \subseteq \mathcal{SL}$$

and

$$\mathcal{SL} \subseteq \mathcal{S}_1 \subseteq \mathcal{SL}$$

By Lemma 5.1, $\mathcal{A}_4 = \mathcal{S}$, So, $\mathcal{S}_4 = \mathcal{S}$. □

We are now ready to present the main theorem of this section.

Theorem 5.7. *We have*

(a) *The following are the* 3 *subvarieties of* $\mathcal{S}$ *of associative type that are distinct from each other.*

$$\mathcal{SL},\ \mathcal{S}_{14},\ \mathcal{S}.$$

(b) *They satisfy the following relationships*

1. $\mathcal{SL} \subset \mathcal{S}_{14} \subset \mathcal{S}$,
2. $\mathcal{BA} \not\subset \mathcal{S}_{14}$.

Proof. We first prove (b).

1. By Theorem 4.2, $\mathcal{SL} \subseteq \mathcal{S}_{14}$.

   The following algebras show that $\mathcal{SL} \neq \mathcal{S}_{14}$ and $\mathcal{S}_{14} \neq \mathcal{S}$, respectively.

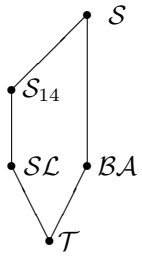
$\rightarrow$	0	1	2	3
0	0	1	2	3
1	2	3	2	3
2	1	1	3	3
3	3	3	3	3

$\rightarrow$	0	1
0	1	1
1	0	1

2. Since $\mathbf{2_b} \not\models (S_{14})$, it follows that $\mathcal{BA} \not\subseteq \mathcal{S}_{14}$.

The proof of the theorem is now complete since (a) is an immediate consequence of Proposition 5.6 and (b). □

The Hasse diagram of the poset of subvarieties of $\mathcal{S}$ of associative type, together with $\mathcal{BA}$, is:



References

[1] **J.C. Abbott**, *Semi-boolean algebra*, Matematicki Vesnik **19** (1967), 177 – 198.

[2] **R. Balbes, PH. Dwinger**, *Distributive lattices*, Univ. of Missouri Press, Columbia, 1974.

[3] **B.A. Bernstein**, *A set of four postulates for Boolean algebras in terms of the implicative operation*, Trans. Amer. Math. Soc. **36** (1934), 876 – 884.

[4] **S. Burris, H.P. Sankappanavar**, *A Course in universal algebra*, Gradute texts in Mathematics 78, Springer-Verlag, New York, 1981.

[5] **J.M. Cornejo, H.P. Sankappanavar**, *Order in implication zroupoids*. Stud Logica **104** (2016), no. 3, 417 – 453.

[6] **J.M. Cornejo, H.P. Sankappanavar**, *Semisimple varieties of implication zroupoids*, Soft Comput. **20** (2016), 3139 – 3151.

[7] **J.M. Cornejo, H.P. Sankappanavar**, *On implicator groupoids*, Algebra Univers. **77** (2017), no. 2, 125 – 146.

[8] **J.M. Cornejo, H.P. Sankappanavar**, *On derived algebras and subvarieties of implication zroupoids*, Soft Comput. **21** (2017), 6963 – 6982.

[9] **J.M. Cornejo, H.P. Sankappanavar**, *Symmetric implication zroupoids and the identities of Bol-Moufang type*, Soft Comput. **2017** (published online: 25 October 2017), 1-15. DOI 10.1007/s00500-017-2869-z.

[10] **J.M. Cornejo, H.P. Sankappanavar**, *Symmetric implication zroupoids and the weak associative identities*, (submitted), 2016.

[11] **J.M. Cornejo, H.P. Sankappanavar**, *Varieties of implication zroupoids*, Preprint, 2018.

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

[13] **M. Hosszú**, *Some functional equations related with the associative law*, Publ. Math. Debrecen **3** (1954), 205 – 214.

[14] **M.A. Kazim, M. Naseeruddin**, *On almost-semigroups*, The Alig. Bull Math **2** (1972), 1 – 7.

[15] **K. Kunen**, *Quasigroups, loops, and associative laws*, J. Algebra **185** (1996), 194 – 204.

[16] **W. McCune**, *Prover9 and Mace4* `http://www.cs.unm.edu/mccune/prover9/` (2005 – 2010).

[17] **C.S. Peirce**, *On the algebra of logic*, Amer. J. Math. **3** (1880), 15 – 57.

[18] **H.O. Pflugfelder**, *Historical notes on loop theory*, Comment. Math. Univ. Carolin. **41** (2000), no. 2, 359 – 370.

[19] **J.D. Phillips, P. Vojtechovsky**, *The varieties of loops of Bol-Moufang type*, Algebra Univers. **54** (2005), 259 – 271.

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

[21] **P.V. Protic, N. Stevanovic**, *Abel-Grassmann bands*, Quasigroups and Related Systems **11** (2004), 95 – 101.

[22] **D.I. Pushkashu**, *Para-associative groupoids*, Quasigroups and Related Systems **18** (2010), 187 – 194.

[23] **H. Rasiowa**, *An algebraic approach to non-classical logics*, North-Holland Publishing Co., Amsterdam, Studies in Logic and the Foundations of Mathematics, **78**, 1974.

[24] **H.P. Sankappanavar**, *De Morgan algebras: new perspectives and applications*, Sci. Math. Jpn. **75** (2012), no. 1, 21 – 50.

[25] **E. Schroeder**, *Uber algorithmen und calculi*, Arch. der Math. und Phys. **5** (1887), 225 – 278.

[26] **D. Stanovsky**, *A guide to self-distributive quasigroups, or latin quandles*, Quasigroups and Related Systems **23** (2015), 91 – 128.

[27] **S.K. Stein**, *On the foundations of quasigroups*, Trans Amer. Math Soc. **85** (1957), 228 – 256.

[28] **A. Suschkewitsch**, *On a generalization of the associative law*, Trans. Amer. Math. Soc. **31** (1929), no. 1, 204 – 214.

Received October 10, 2017

J.M. Cornejo
Departamento de Matemática
Universidad Nacional del Sur
Alem 1253, Bahía Blanca, Argentina
INMABB - CONICET
e-mail: jmcornejo@uns.edu.ar

H. P. Sankappanavar
Department of Mathematics
State University of New York
New Paltz, New York 12561
U.S.A.
e-mail: sankapph@newpaltz.edu

Quasigroups and Related Systems **26** (2018), 35 – 40

A characterization of almost simple groups related to $L_3(37)$

Ashraf Daneshkhah and Younes Jalilian

Abstract. Let G be a finite group, and let $\Gamma(G)$ be its prime graph. The degree pattern of G is denoted by $\mathsf{D}(G) = (\deg(p_1), \ldots, \deg(p_k))$, where $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $\deg(p_i)$ is the degree of vertex p_i in $\Gamma(G)$. The group G is called k-fold OD-characterizable if there exist exactly k non-isomorphic groups H satisfying $|G| = |H|$ and $\mathsf{D}(G) = \mathsf{D}(H)$. In this paper, we characterize all finite groups with the same order and degree pattern as almost simple groups related to the projective special linear group $L_3(37)$.

1. Introduction

Let G be a finite group. We denote by $\omega(G)$ the set of orders of elements of G and by $\pi(G)$ the set of prime divisors of the order of G. The *spectrum* $\mu(G)$ of G is the set of elements of $\omega(G)$ that are maximal with respect to divisibility relation. Let $\pi(G) = \{p_1, \ldots, p_k\}$. The prime graph $\Gamma(G)$ of a group G is the graph whose vertex set is $\pi(G)$ and two distinct primes p and q are adjacent (we write $p \sim q$) if and only if G contains an element of order pq, that is to say, $pq \in \omega(G)$. For $p \in \pi(G)$, the degree $\deg(p)$ of p is the degree of the vertex p in $\Gamma(G)$, that is to say, the number of vertices $q \in \pi(G)$ which are adjacent to p. If $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then we denote $\mathsf{D}(G) := (\deg(p_1), \deg(p_2), \ldots, \deg(p_k))$, where $p_1 < p_2 < ... < p_k$. This k-tuple is called the degree pattern of G. A group G is called *k-fold OD-characterizable* if there exist exactly k non-isomorphic finite groups having the same order and degree pattern as G. In particular, a 1-fold OD-characterizable group is simply called *OD-characterizable*. A group G is said to be an almost simple group related to L if and only if $L \trianglelefteq G \lesssim \mathsf{Aut}(L)$ for some non-abelian simple group L.

The notion of degree patterns of prime graphs and related topics has been introduced in [9]. There are natural questions mentioned in [9] about the structure of finite groups with the same degree patterns and the same orders:

Let G and M be finite groups satisfying the conditions (1) $|G| = |M|$ *and* (2) $D(G) = D(M)$.

(i) *How far do these conditions affect the structure of G?*

2010 Mathematics Subject Classification: 20D05, 20D06
Keywords: Projective special linear groups, almost simple groups, k-fold OD-characterization, prime graph

(ii) *Is the number of non-isomorphic groups satisfying (1) and (2) finite?*

It is therefore important to investigate the number of non-isomorphic groups satisfying conditions (1) and (2) for important families of groups M. In a series of articles, it has been proved that some finite almost simple groups are OD-characterizable or k-fold OD-characterizable for $k \geqslant 2$, for example see [5, 11, 15]. Note in passing that a few classes of finite simple groups have been in general characterized by their degree patterns and orders, see for example [9, 13, 16]. To our knowledge, the lack of information on the spectra of almost simple groups is the main reason which makes this characterization somehow difficult in general argument but the situation for some simple groups is rather different as the spectra of these groups are known, see for example [2, 3, 8].

Motivated by [4], in this paper, we focus on groups related to $L_3(37)$ and show that $L_3(37)$ and $L_3(37) : \mathbb{Z}_2$ are OD-characterizable while $L_3(37) : \mathbb{Z}_3$ and $L_3(37) : S_3$ are 3-fold and 5-fold OD-characterizable, respectively. Indeed, we prove that

Theorem 1.1. *Let H be an almost simple group related to $L := L_3(37)$. If G is a finite group such that $\mathsf{D}(G) = \mathsf{D}(H)$ and $|G| = |H|$, then the following hold:*

(a) *If $H = L$, then $G \cong H$.*

(b) *If $H = L : \mathbb{Z}_2$, then $G \cong H$.*

(c) *If $H = L : \mathbb{Z}_3$, then G is isomorphic to H, $\mathbb{Z}_3 \times L$ or $\mathbb{Z}_3 \cdot L$ (non-split).*

(d) *If $H = L : S_3$, then G is isomorphic to H, $\mathbb{Z}_3 \times (L : \mathbb{Z}_2)$, $\mathbb{Z}_3 \cdot (L : \mathbb{Z}_2)$ (non-split), $(\mathbb{Z}_3 \times L) \cdot \mathbb{Z}_2$ or $(\mathbb{Z}_3 : L) \cdot \mathbb{Z}_2$.*

Throughout this article, all groups under consideration are finite. For $p \in \pi(G)$, we denote by G_p and $Syl_p(G)$ a Sylow p-subgroup of G and the set of all Sylow p-subgroups of G, respectively. All further definitions and notation are standard and can be found in [1, 7].

2. Preliminaries

In this section, we mention some useful results to be used in proof of Theorem 1.1. Here the independence number $\alpha(\Gamma)$ of a graph Γ is the maximum cardinality of an independent set among all independent sets of Γ. Let now G be a finite group, and let $\Gamma(G)$ be its prime graph. Then we set $\alpha(G) := \alpha(\Gamma(G))$. Moreover, for a vertex $r \in \pi(G)$, let $\alpha(r, G)$ denote the maximal number of vertices in independent sets of $\Gamma(G)$ containing r.

Lemma 2.1. [12, Theorem 1] *Let G be a finite group with $\alpha(G) \geqslant 3$ and $\alpha(2, G) \geqslant 2$, and let K be the maximal normal solvable subgroup of G. Then the quotient group G/K is an almost simple group, that is, there exists a finite non-abelian simple group S such that $S \leqslant G/K \leqslant \mathsf{Aut}(S)$.*

Lemma 2.2. [10, Theorem 1] *Let S be a finite non-abelian simple group, and let p be the largest prime divisor of $|S|$ with $|S|_p = p$. Then $p \nmid |\mathsf{Out}(S)|$.*

Lemma 2.3. *The orders, spectra and degree patterns of the almost simple groups related to $L_3(37)$ are as in Table 1.*

Proof. Note that $\mathsf{Aut}(L_3(37)) \cong L_3(37) : S_3$. So if G is an almost simple group related to $L_3(37)$, then G is isomorphic to one of the groups $L_3(37)$, $L_3(37) : \mathbb{Z}_2$, $L_3(37) : \mathbb{Z}_3$, $L_3(37) : S_3$. The result for $H = L_3(37)$ can be obtained by [8, Theorem 9] and for the remaining groups we use GAP [6]. □

Table 1: The orders, spectra and degree patterns of H, where H is an almost simple group related to $L_3(37)$.

H	$\lvert H\rvert$	$\mu(H)$	$\mathsf{D}(H)$
$L_3(37)$	$2^5 \cdot 3^4 \cdot 7 \cdot 19 \cdot 37^3 \cdot 67$	$\{7 \cdot 67, 2^3 \cdot 3 \cdot 19, 2^2 \cdot 3^2, 2^2 \cdot 3 \cdot 37\}$	$(3,3,1,2,2,1)$
$L_3(37) : \mathbb{Z}_2$	$2^6 \cdot 3^4 \cdot 7 \cdot 19 \cdot 37^3 \cdot 67$	$\{7 \cdot 67, 2^3 \cdot 3 \cdot 19, 2^3 \cdot 3^2, 2^2 \cdot 3 \cdot 37\}$	$(3,3,1,2,2,1)$
$L_3(37) : \mathbb{Z}_3$	$2^5 \cdot 3^5 \cdot 7 \cdot 19 \cdot 37^3 \cdot 67$	$\{3 \cdot 7 \cdot 67, 2^3 \cdot 3^2 \cdot 19, 2^2 \cdot 3^2 \cdot 37\}$	$(3,5,2,2,2,2)$
$L_3(37) : S_3$	$2^6 \cdot 3^5 \cdot 7 \cdot 19 \cdot 37^3 \cdot 67$	$\{3 \cdot 7 \cdot 67, 2^3 \cdot 3^2 \cdot 19, 2^2 \cdot 3^2 \cdot 37\}$	$(3,5,2,2,2,2)$

3. Proof of the main result

In this section, we prove Theorem 1.1 through a series of Lemmas and propositions. Observe that Theorem 1.1(a) follows from [4, Proposition 3.4]. Therefore in what follows we deal with the remaining cases.

Proposition 3.1. *Let $H := L : \mathbb{Z}_2$ where $L := L_3(37)$. If $|G| = |H|$ and $\mathsf{D}(G) = \mathsf{D}(H)$, then $G \cong H$.*

Proof. Note by Table 1 that $|G| = 2^6 \cdot 3^4 \cdot 7 \cdot 19 \cdot 37^3 \cdot 67$ and $\mathsf{D}(G) = (3,3,1,2,2,1)$. Since $\deg(7) = 1$, there exists the unique prime $p_2 \in \pi(G)$ such that 7 is adjacent to p_2. Since also $|\pi(G)| = 6$, there are four more primes which are not adjacent to 7. If these four vertices, say p_3, p_4, p_5 and p_6, are pairwise adjacent, then the degrees of the vertices p_3, p_4, p_5 and p_6 are at least 3, which is impossible. Hence there exist at least two non-adjacent vertices p_3 and p_4. Let $\Delta = \{7, p_3, p_4\}$ be an independent set in $\Gamma(G)$. Then $\alpha(G) \geqslant 3$. Furthermore, $\alpha(2, G) \geqslant 2$ since $\deg(2) = 3$ and $|\pi(G)| = 6$. By Lemma 2.1, there is a non-abelian finite simple group S such that $S \leqslant G/K \leqslant \mathsf{Aut}(S)$, where K is a maximal normal solvable subgroup of G. We show that $67 \notin \pi(K)$. Assume to the contrary, that is, $67 \in \pi(K)$. We prove that p would be adjacent to 67, where $p \in \{7, 19\}$. If $p \in \pi(K)$, then K contains a cyclic Hall subgroup of order $p \cdot 67$, and so p is adjacent to 67. If $p \notin \pi(K)$, then it follows from Frattini argument that $G = K\mathbf{N}_G(P)$, where P is a Sylow 67-subgroup of K, and so $\mathbf{N}_G(P)$ has an element x of order p. Thus $P\langle x\rangle$ is a cyclic subgroup of G of order $p \cdot 67$. Therefore both 7 and 19 are adjacent to 67

which contradicts the fact that the degree of 67 is 1. Therefore, $67 \notin \pi(K)$, and hence $\pi(K) \subseteq \{2, 3, 7, 19, 37\}$.

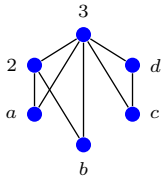
Now we prove that S is isomorphic to L. By Lemma 2.2, $67 \notin \pi(\mathsf{Out}(S))$, then $67 \notin \pi(K) \cup \pi(\mathsf{Out}(S))$, and so $67 \in \pi(S)$. Therefore by [14, Table 1], S is isomorphic to L as claimed. Moreover, since $|G| = |L : \mathbb{Z}_2| = 2|L|$, we deduce that K is isomorphic to 1 or $\mathbb{Z}_2$.

If K is isomorphic to $\mathbb{Z}_2$, then $G = \mathbf{C}_G(K)$ as $G/\mathbf{C}_G(K)$ isomorphic to a subgroup of $\mathsf{Aut}(K) = 1$. Therefore $K \leqslant Z(G)$ which implies that $\deg(2) = 5$, which is a contradiction. Thus $K = 1$, and so $G \cong L : \mathbb{Z}_2$. □

Proposition 3.2. *Let $H := L : \mathbb{Z}_3$ where $L := L_3(37)$. If $|G| = |H|$ and $\mathsf{D}(G) = \mathsf{D}(H)$, then G is isomorphic to one of the groups H, $\mathbb{Z}_3 \times L$ and $\mathbb{Z}_3 \cdot L$ (non-split).*

Proof. Note by Table 1 that $|G| = 2^5 \cdot 3^5 \cdot 7 \cdot 19 \cdot 37^3 \cdot 67$ and $\mathsf{D}(G) = (3, 5, 2, 2, 2, 2)$. Therefore, $\Gamma(G)$ must be the graph as in Figure 1 in which $\{a, b, c, d\} = \{7, 19, 37, 67\}$.

Figure 1: The prime graph $\Gamma(G)$ of G in Propositions 3.2 and 3.3.



We observe by Figure 1 that $\{a, b, c\}$ is an independent set in $\Gamma(G)$, and so $\alpha(G) \geqslant 3$. Furthermore, $\alpha(2, G) \geqslant 2$ since $\deg(2) = 3$ and $|\pi(G)| = 6$. By Lemma 2.1, there is a finite non-abelian simple group S such that $S \leqslant G/K \leqslant \mathsf{Aut}(S)$, where K is a maximal normal solvable subgroup of G. By the same argument as in Proposition 3.1, we can show that $67 \notin \pi(K)$, and so $\pi(K) \subseteq \{2, 3, 7, 19, 37\}$. It follows from Lemma 2.2, $67 \notin \pi(\mathsf{Out}(S))$, then $67 \in \pi(S)$. Therefore by [14, Table 1], S is isomorphic to L. Thus $L \leqslant G/K \leqslant \mathsf{Aut}(L)$, and so $|K| = 1$ or 3, which implies that K is isomorphic to 1 or $\mathbb{Z}_3$.

If $K = 1$, then since $L \leqslant G/K \leqslant \mathsf{Aut}(L)$ and $|G| = |L : \mathbb{Z}_3|$, we conclude that G is isomorphic to $L : \mathbb{Z}_3$.

If K is isomorphic to $\mathbb{Z}_3$, then $G/K \cong L$. In this case, we have that $G/\mathbf{C}_G(K) \leqslant \mathsf{Aut}(K) = \mathbb{Z}_2$. Thus $|G/\mathbf{C}_G(K)|$ is 1 or 2. If $|G/\mathbf{C}_G(K)| = 2$, then K is a proper subgroup of $\mathbf{C}_G(K)$, and so $1 \neq \mathbf{C}_G(K)/K \trianglelefteq G/K \cong L$. This implies that $G = \mathbf{C}_G(K)$, which is a contradiction. Therefore, $|G/\mathbf{C}_G(K)| = 1$. Then $K \leqslant Z(G)$, that is to say, G is a central extension of $\mathbb{Z}_3$ by L. If G splits over K, then G is isomorphic to $\mathbb{Z}_3 \times L$, otherwise, G is isomorphic to $\mathbb{Z}_3 \cdot L$ (non-split). □

Proposition 3.3. *Let $H := L : S_3$ where $L := L_3(37)$. If $|G| = |H|$ and $\mathsf{D}(G) = \mathsf{D}(H)$, then G is isomorphic to one of the groups H, $\mathbb{Z}_3 \times (L : \mathbb{Z}_2)$, $\mathbb{Z}_3 \cdot (L : \mathbb{Z}_2)$ (non-split), $(\mathbb{Z}_3 \times L) \cdot \mathbb{Z}_2$ and $(\mathbb{Z}_3 : L) \cdot \mathbb{Z}_2$.*

Proof. According to Table 1, we have that $|G| = 2^6 \cdot 3^5 \cdot 7 \cdot 19 \cdot 37^3 \cdot 67$ and $\mathsf{D}(G) = (3, 5, 2, 2, 2, 2)$. Therefore, the prime graph $\Gamma(G)$ is the graph as in Figure 1, where $\{a, b, c\}$ forms an independent set in $\Gamma(G)$, and so $\alpha(G) \geqslant 3$. Moreover, $\alpha(2, G) \geqslant 2$ as $\deg(2) = 3$ and $|\pi(G)| = 6$. Now we apply Lemma 2.1 and conclude that there is a finite non-abelian simple group S such that $S \leqslant G/K \leqslant \mathsf{Aut}(S)$, where K is a maximal normal solvable subgroup of G. Again, by the same manner as in Proposition 3.1, we have that $67 \notin \pi(K)$, and hence $\pi(K) \subseteq \{2, 3, 7, 19, 37\}$. By Lemma 2.2, $67 \notin \pi(\mathsf{Out}(S))$, and since $67 \notin \pi(K) \cup \pi(\mathsf{Out}(S))$, it follows that $67 \in \pi(S)$, and so by [14, Table 1], S is isomorphic to L. Thus $L \leqslant G/K \leqslant \mathsf{Aut}(L)$ implying that $|K| \in \{1, 2, 3, 6\}$. Hence K is isomorphic to one of the groups 1, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_6$ and S_3.

If $K = 1$, then since $L \leqslant G/K \leqslant \mathsf{Aut}(L)$ and $|G| = 6|L|$, we conclude that G is isomorphic to $L : S_3$.

If K is isomorphic to $\mathbb{Z}_2$, then K is central in G, and so $\deg(2) = 5$ in $\Gamma(G)$, which is a contradiction.

If K is isomorphic to $\mathbb{Z}_3$, then $K \leqslant \mathbf{C}_G(K)$ and $G/K \cong L : \mathbb{Z}_2$, and so $G/\mathbf{C}_G(K)$ is isomorphic to a subgroup of $\mathsf{Aut}(K) \cong \mathbb{Z}_2$. Thus, $|G/\mathbf{C}_G(K)| = 1$ or 2. If $|G/\mathbf{C}_G(K)| = 1$, then $K \leqslant Z(G)$, that is to say, G is a central extension of $\mathbb{Z}_3$ by $L : \mathbb{Z}_2$. This implies that G is isomorphic to $\mathbb{Z}_3 \times (L : \mathbb{Z}_2)$ or $\mathbb{Z}_3 \cdot (L : \mathbb{Z}_2)$ (non-split). If $|G/\mathbf{C}_G(K)| = 2$, then K is a proper subgroup of $\mathbf{C}_G(K)$, and so $\mathbf{C}_G(K)/K$ is a nontrivial normal subgroup of $G/K \cong L : \mathbb{Z}_2$. Thus $\mathbf{C}_G(K)/K \cong L$. Since $K \leqslant Z(\mathbf{C}_G(K))$, it follows that $\mathbf{C}_G(K)$ is a central extension of K by L, and hence $\mathbf{C}_G(K)$ is isomorphic to $\mathbb{Z}_3 \times L$ or $\mathbb{Z}_3 \cdot L$ (non-split). Therefore G is isomorphic to $(\mathbb{Z}_3 \times L) \cdot \mathbb{Z}_2$ or $(\mathbb{Z}_3 \cdot L) \cdot \mathbb{Z}_2$.

If K is isomorphic to $\mathbb{Z}_6$, then $K \leqslant \mathbf{C}_G(K)$ and $G/K \cong L$. Since $G/\mathbf{C}_G(K)$ is isomorphic to a subgroup of $\mathbb{Z}_2$, it follows that $|G/\mathbf{C}_G(K)| = 1$ or 2. If $|G/\mathbf{C}_G(K)| = 1$, then $K \leqslant Z(G)$, and so $\deg(2) = 5$, which is a contradiction. Thus $|G/\mathbf{C}_G(K)| = 2$. Since K is a proper subgroup of $\mathbf{C}_G(K)$, the group $\mathbf{C}_G(K)/K$ is a nontrivial normal subgroup of $G/K \cong L$, which is a contradiction.

If K is isomorphic to S_3, then $K \cap \mathbf{C}_G(K) = 1$ and $G/K \cong L$. Note that $G/\mathbf{C}_G(K)$ is isomorphic to a subgroup of $\mathsf{Aut}(K) \cong S_3$. Then $\mathbf{C}_G(K) \neq 1$. Since $\mathbf{C}_G(K) \cong \mathbf{C}_G(K)K/K$ is a non-identity normal subgroup of $G/K \cong L$, we conclude that $G = \mathbf{C}_G(K)K$, where $\mathbf{C}_G(K) \cong L$ and $K \cap \mathbf{C}_G(K) = 1$. This implies that G is isomorphic to $K \times \mathbf{C}_G(K) \cong S_3 \times L$, however this case can be ruled out as $\deg(2) = 3$. □

Proof of Theorem 1.1. The proof of Theorem 1.1 follows immediately from Proposition 3.4 in [4] and Propositions 3.1–3.3.

Acknowledgement

The authors would like to thank editors and anonymous referees for their constructive comments and suggestions to improve the results of this paper.

References

[1] **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.

[2] **A.A. Buturlakin**, *Spectra of finite linear and unitary groups*, Algebra Logic **47** (2008), no. 2, 91 – 99.

[3] **A.A. Buturlakin**, *Spectra of finite simple groups $E_6(q)$ and ${}^2E_6(q)$*, Algebra Logic **52** (2013), no. 3, 188 – 202.

[4] **A. Daneshkkhah and Y. Jalilian**, *A characterization of some projective special linear groups*, Italian J. Pure Appl. Math. **38** (2017), 38, 32 – 44.

[5] **M.R. Darafsheh, G. Rezaeezadeh, M. Sajjadi, and M. Bibak**, *OD-characterization of almost simple groups related to $U_3(17)$*, Quasigroups Related Systems **21** (2013), 49 – 58.

[6] **The GAP Group**, *GAP – Groups, Algorithms, and Programming*, Version 4.6.4, 2013.

[7] **D. Gorenstein**, *Finite groups*, Chelsea Publishing Co., New York, second edition, 1980.

[8] **M.A. Grechkoseeva, W. Shi, and A.V. Vasilev**, *Recognition by spectrum for finite simple groups of Lie type*, Front. Math. China **3** (2008), no. 2, 275 – 285.

[9] **A.R. Moghaddamfar, A.R. Zokayi and M.R. Darafsheh**, *A characterization of finite simple groups by the degrees of vertices of their prime graphs*, Algebra Colloq. **12** (2005), 431 – 442.

[10] **S. Liu**, *OD-characterization of some alternating groups*, Turkish J. Math. **39** (2015), 395 – 407.

[11] **G.R. Rezaeezadeh, M.R. Darafsheh, M. Sajjadi, and M. Bibak**, *OD-characterization of almost simple groups related to $L_3(25)$*, Bull. Iranian Math. Soc. **40** (2014), 765 – 790.

[12] **A.V. Vasilev and I.B. Gorshkov**, *On the recognition of finite simple groups with a connected prime graph*, Sibirsk. Mat. Zh. **50** (2009), no. 2, 292 – 299.

[13] **Y. Yang, S. Liu, and Z. Zhang**, *OD-characterization of alternating groups A_{p+d}*, Open Mathematics **15** (2017), no. 1, 1090 – 1098.

[14] **A.V. Zavarnitsine**, *Finite simple groups with narrow prime spectrum*, ArXiv e-prints, 2008.

[15] **L. Zhang and W. Shi**, *OD-characterization of almost simple groups related to $L_2(49)$*. Arch. Math. (Brno) **44** (2008), no. 3, 191 – 199.

[16] **L. Zhang and W. Shi**, *OD-characterization of the projective special linear groups $L_2(q)$*, Algebra Colloq. **19** (2012), no. 3, 509 – 524.

Received April 19, 2017

Department of Mathematics, Faculty of Science, Hamedan, Iran
E-mails: adanesh@basu.ac.ir, daneshkhah.ashraf@gmail.com, jalilianyounes@yahoo.com

Quasigroups and Related Systems **26** (2018), 41 – 44

Pseudoisomorphisms of quasigroups

Ivan I. Deriyenko

Abstract. A simple method of construction of autotopies of quasigroups is presented.

1. In this short note all considered quasigroups are defined on a finite set Q, α, β, γ are permutations of the set Q. The composition of permutations is defined as $\alpha\beta(x) = \alpha(\beta(x))$. Let $(Q, \cdot)$ and $(Q, \circ)$ be two quasigroups. Their permutations $L_a(x) = a \cdot x$, $R_a(x) = x \cdot a$, $M_a(x) : x \cdot M_a(x) = a$ and $L^\circ_a(x) = a \circ x$, $R^\circ_a(x) = x \circ a$, $M^\circ_a(x) : x \circ M^\circ_a(x) = a$ are called *left*, *right* and *middle translations* of the corresponding quasigroup. Quasigroups $A = (Q, \cdot)$ and $B = (Q, \circ)$ are *isotopic* if there exists triplet $T = (\alpha, \beta, \gamma)$, called an *isotopism*, such that

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

or equivalently

$$\gamma^{-1}(x \circ y) = \alpha^{-1}(x) \cdot \beta^{-1}(y), \tag{2}$$

for all $x, y \in Q$. In this case, we will write $A \sim B$. Obviously $A \sim A$. In this case we say that $T = (\alpha, \beta, \gamma)$ is an *autotopism*.

Left, right and middle translations play an important role in the investigation of isotopies of quasigroups (see for example [2], [3] and [4]). They also are used in the construction of prolongations and contractions of Latin squares (see [5] and [6]). Below we present a simple method of construction of autotopies of quasigroups based on such translations.

2. An isotopy of the form $T_l = (\alpha, \beta, \alpha)$ is called a *left pseudoisomorphism*. An isotopy $T_r = (\alpha, \beta, \beta)$ is called a *right pseudoisomorphism*, and an isotopy $T_m = (\alpha, \alpha, \gamma)$ is called a *middle pseudoisomorphism*.

As a simple consequence of (1) we obtain

Lemma 1. *Two quasigroups $(Q, \cdot)$ and $(Q, \circ)$ are isotopic if and only if at least one of the following identities*

$$L_i = \gamma^{-1} L^\circ_{\alpha(i)} \beta, \quad R_i = \gamma^{-1} R^\circ_{\beta(i)} \alpha, \quad M_i = \beta^{-1} M^\circ_{\gamma(i)} \alpha$$

is satisfied for some permutations α, β, γ of Q.

2010 Mathematics Subject Classification: 20N05
Keywords: Quasigroup, autotopism, pseudoisomorphism.

Corollary 1. *The triplet $T = (\alpha, \beta, \gamma)$ is an autotopism of a quasigroup $(Q, \cdot)$ if and only if at least one of the following identities*

$$L_i = \gamma^{-1} L_{\alpha(i)} \beta, \quad R_i = \gamma^{-1} R_{\beta(i)} \alpha, \quad M_i = \beta^{-1} M_{\gamma(i)} \alpha$$

is satisfied for some permutations α, β, γ of Q.

By a *left b-adjoint quasigroup* of a quasigroup $(Q, \cdot)$ we mean a quasigroup $(Q, *)$ with the operation $x * y = L_b^{-1}(x \cdot y)$, where $b \in Q$ is fixed. A *right b-adjoint quasigroup* is defined analogously. A a *middle b-adjoint quasigroup* of a quasigroup $(Q, \cdot)$ is defined as a quasigroup $(Q, *)$ with the operation
$x * M_b^{-1}(y) = x \cdot y$.

Theorem 1. *Two quasigroups are isotopic if and only if its left b-adjoint quasigroups are right pseudoisomorphic.*

Proof. Let quasigroups $(Q, \cdot)$ and $(Q, \circ)$ be isotopic and let this isotopism has the form (1). If $(Q, *)$ and $(Q, \diamond)$ are left b-adjoint quasigroups of quasigroups $(Q, \cdot)$ and $(Q, \circ)$, respectively, then $x * y = L_b^{-1}(x \cdot y)$ and $x \diamond y = (L_b^{\circ})^{-1}(x \circ y)$. Thus, $L_x^{\diamond} = (L_b^{\circ})^{-1} L_x^{\circ}$. This, by Lemma 1, gives

$$L_x^{*} = L_b^{-1} L_x = (\gamma^{-1} L_{\alpha(b)}^{\circ} \beta)^{-1} \gamma^{-1} L_{\alpha(x)}^{\circ} \beta = \beta^{-1} (L_{\alpha(b)}^{\circ})^{-1} L_{\alpha(x)}^{\circ} \beta = \beta^{-1} L_{\alpha(x)}^{\diamond} \beta.$$

Hence $\beta(x * y) = \alpha(x) \diamond \beta(y)$.

The converse statement is obvious. □

Corollary 2. *If quasigroups $(Q, \cdot)$ and $(Q, \circ)$ are isotopic, then, for every $b \in Q$, its left b-adjoint quasigroups are right pseudoisomorphic. Conversely, if for some $b \in Q$ left b-adjoint quasigroups of quasigroups $(Q, \cdot)$ and $(Q, \circ)$ are pseudoisomorphic, then $(Q, \cdot)$ and $(Q, \circ)$ are isotopic.*

In a similar way we can prove the following two theorems.

Theorem 2. *Two quasigroups are isotopic if and only if its right b-adjoint quasigroups are left pseudoisomorphic.*

Theorem 3. *Two quasigroups are isotopic if and only if its middle b-adjoint quasigroups are middle pseudoisomorphic.*

3. As it is well known, any permutation φ of the set $\{1, 2, \ldots, n\}$ can be decomposed into $r \leqslant n$ cycles of the length $k_1, k_2, \ldots, k_r$ with $k_1 + k_2 + \ldots + k_r = n$. We denote this fact by $C(\varphi) = \{k_1, k_2, \ldots, k_r\}$. $C(\varphi)$ is called a *cyclic type* of φ.

Two permutations $\varphi, \psi \in S_n$ are *conjugate* if there exists a permutation $\rho \in S_n$ such that $\rho\varphi\rho^{-1} = \psi$. Two permutations are conjugate if and only if they have the same cyclic type (cf. [7]).

Let $(Q, \circ)$, where $Q = \{1, 2, \ldots, n\}$ be a quasigroup and let

$$C(L^{\circ}) = \{C(L_1^{\circ}), C(L_2^{\circ}), \ldots, C(L_n^{\circ})\},$$

$$C(R^\circ) = \{C(R_1^\circ), C(R_2^\circ), \ldots, C(R_n^\circ)\},$$
$$C(M^\circ) = \{C(M_1^\circ), C(M_2^\circ), \ldots, C(M_n^\circ)\}.$$

Then as a consequence of the above results we obtain

Theorem 4. *If quasigroups $(Q,\cdot)$ and $(Q,\circ)$ are isotopic, then $C(L^*) = C(L^\diamond)$, $C(R^*) = C(R^\diamond)$, $C(M^*) = C(M^\circ)$ for all its left (right, middle) b-adjoint quasigroups $(Q,*)$ and $(Q,\diamond)$.*

The converse statement is not true.

Example 1. Consider two loops defined by the following tables.

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

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

The first loop is a group isomorphic to the cyclic group $\mathbb{Z}_6$; the second is not a group because $(5 \circ 4) \circ 3 \neq 5 \circ (4 \circ 3)$. So, by the Albert's theorem, they are not isotopic, but, as it is not difficult to see, $C(L^*) = C(L^\diamond)$, $C(R^*) = C(R^\diamond)$, $C(M^*) = C(M^\circ)$ for all its b-adjoint quasigroups $(Q,*)$ and $(Q,\diamond)$.

4. Basing on the above results we can find autotopies of quasigroups for which left, right or middle translations have different cyclic types.

For simplicity permutations will be written in the form of cycles and cycles will be separated by points, e.g.

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

Example 2. Let $(Q,\cdot)$ be a quasigroup defined by the following table:

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

This quasigroup has the following left and right translations:

	left translations	*cyclic type*
L_1	(1.2.3.4.5.6.7.8.)	{1,1,1,1,1,1,1,1}
L_2	(128367.45.)	$\{2,6\}$
L_3	(13864.275.)	$\{3,5\}$
L_4	(14876.253.)	$\{3,5\}$
L_5	(158.26374.)	$\{3,5\}$
L_6	(165.23478.)	$\{3,5\}$
L_7	(17243.568.)	$\{3,5\}$
L_8	(18462.357.)	$\{3,5\}$

	right translations	*cyclic type*
R_1	(1.2.3.4.5.6.7.8.)	{1,1,1,1,1,1,1,1}
R_2	(128.37456.)	$\{3,5\}$
R_3	(13857.264.)	$\{3,5\}$
R_4	(148673.25.)	$\{2,6\}$
R_5	(15876.243.)	$\{3,5\}$
R_6	(16534.278.)	$\{3,5\}$
R_7	(172.35468.)	$\{3,5\}$
R_8	(18475.236.)	$\{3,5\}$

If this quasigroup has an autotopy of the form $\beta(x \cdot y) = \alpha(x) \cdot \beta(y)$, then by Corollary 2 we have $L_i = \beta^{-1} L_{\alpha(i)} \beta$ for every $i \in Q$. Since L_i and $L_{\alpha(i)}$, as a conjugate permutations, have the same cyclic type, in the case $i = 2$ must be $L_2 = L_{\alpha(2)}$, so $\alpha(2) = 2$. Thus $L_2 = \beta^{-1} L_2 \beta$, i.e., $\beta L_2 = L_2 \beta$. The last equation is satisfied by $\beta = (128367.5.4.)$. Now, using $\beta L_i = L_{\alpha(i)} \beta$, we see that $\alpha = (1.2.354786.)$. This shows that our quasigroups has an autotopy (α, β, β). Since autotopies form a group (cf. [1]), $(\alpha^k, \beta^k, \beta^k)$ also are autotopies for each natural k.

An autotopy of the form (σ, ρ, σ) is induced by right translations. Indeed, from the fact that $R_i = \sigma^{-1} R_{\rho(i)} \sigma$ have the same cyclic type we obtain $R_4 = R_{\rho(4)}$. So, $\rho(4) = 4$. Hence, analogously, as in the previous part, we calculate $\sigma = (137684.2.5.)$ and $\rho = (1.4.257863.)$. Obviously $(\sigma^t, \rho^t, \sigma^t)$ also is an autotopy for each natural t. Moreover, composition of $(\alpha^k, \beta^k, \beta^k)$ and $(\sigma^t, \rho^t, \sigma^t)$ is an autotopy too. For example, composition of (α, β, β) and (σ, ρ, σ) gives an autotopy $(\alpha_1, \beta_1, \gamma_1)$ with $\alpha_1 = \alpha\sigma = (154.387.2.6.)$, $\beta_1 = \beta\rho = (125.387.4.6.)$, $\gamma_1 = \beta\sigma = (163.284.5.7.)$.

References

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

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

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

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

[5] **I.I. Deriyenko and A.I. Deriyenko**, *Prolongations of quasigroups by middle translations*, Quasigroups Related Systems **17** (2009), 177 – 190.

[6] **I.I. Deriyenko and W.A. Dudek**, *Contractions of quasigroups and Latin squares*, Quasigroups Related Systems **21** (2013), 165 – 174.

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

Received February 10, 2018

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

Quasigroups and Related Systems **26** (2018), 45 – 52

Menger algebras of associative and self-distributive n-ary operations

Wieslaw A. Dudek and Valentin S. Trokhimenko

Abstract. The necessary and sufficient conditions under which a Menger algebra of rank n can be isomorphically represented by associative or (i,j)-associative n-ary operations are given. Also the conditions under which a Menger algebra of rank n can be homomorphically represented by self-distributive n-ary operations are found.

1. Multiplace functions are known to have various applications not only in mathematical analysis, but are also widely used in the theory of many-valued logics, cybernetics and general systems theory. Algebras of such functions (called *Menger algebras*) are studied in various directions [4]. In particular, many authors studied algebras of functions with some additional properties, see for example [4, 6, 7, 8, 9, 10, 11, 12]. Menger algebras of n-place functions closed with respect to certain additional operations and allow fixed exchange of some variables are described in [4].

As it is known semigroups and groups can be isomorphically represented by functions of one variable. Similar results are obtained for $(n+1)$-ary Menger algebras of some types. Namely, it is proved (see for example [4]) that some types of $(n+1)$-ary Menger algebras can be represented by n-place functions.

In this short paper we give necessary and sufficient conditions under which a Menger algebra of rank n can be isomorphically represented by associative or (i,j)-associative n-ary operations defined on some set. We also find conditions under which a Menger algebra of rank n can be homomorphically represented by self-distributive n-ary operations and prove that in the case when this algebra is also reductive then it can be isomorphically represented by these functions.

2. In the whole article, we assume that $n \geqslant 2$ and A is a nonempty set. Any function $f\colon A^n \to A$ defined for each element of the set A^n is called an *n-ary operation on A*. The set of all such operations, for fixed A and $n \geqslant 2$, is denoted by $\Omega_n(A)$. On the set $\Omega_n(A)$ we can consider the *Menger superposition* $\mathcal{O}$ defined by:

$$\mathcal{O}(f,g_1,\dots,g_n)(a_1,\dots,a_n) = f(g_1(a_1,\dots,a_n),\dots,g_n(a_1,\dots,a_n)),$$

where $f,g_1,\dots,g_n \in \Omega_n(A)$, $a_1,\dots,a_n \in A$.

2010 Mathematics Subject Classification: 20N05, 08A05
Keywords: Algebra of multiplace functions; Menger algebra.

Any subset $\Phi \subset \Omega_n(A)$ closed with respect to this superposition is called a *Menger algebra of n-ary operations* and is denoted by $(\Phi, \mathcal{O})$.

This superposition satisfies (cf. [4]) the following *superassociative law*:

$$\mathcal{O}(\mathcal{O}(f, g_1, \ldots, g_n), h_1, \ldots, h_n) =$$

$$\mathcal{O}(f, \mathcal{O}(g_1, h_1, \ldots, h_n), \ldots, \mathcal{O}(g_n, h_1, \ldots, h_n)),$$

where $f, g_1, \ldots, g_n, h_1, \ldots, h_n \in \Omega_n(A)$.

According to general convention used in theory of n-ary operations, the above superassociative law can be written in the shorted form as:

$$\mathcal{O}(\mathcal{O}(f, g_1^n), h_1^n) = \mathcal{O}(f, \mathcal{O}(g_1, h_1^n), \ldots, \mathcal{O}(g_n, h_1^n)). \tag{1}$$

In the case when $g_1 = g_2 = \ldots = g_k = g$ instead of g_1^k we will write $\overset{k}{g}$.

Any nonempty set G with an $(n+1)$-ary superassociative operation o is called an *$(n+1)$-ary Menger algebra* or a *Menger algebra of rank n* and is denoted by (G, o). If in a Menger algebra (G, o) of rank n from the fact that the equation $o(g_1, x_1^n) = o(g_2, x_1^n)$ is valid for all $x_1, \ldots, x_n \in G$ it follows $g_1 = g_2$, then this Menger algebra is called *reductive* [4]. An element $e \in G$ is called a *left* (*right*) *diagonal unit* of a Menger algebra (G, o) of rank n if $o(e, \overset{n}{x}) = x$ (respectively $o(x, \overset{n}{e}) = x$) holds for all $x \in G$. If e is both left and right diagonal unit, then it is called a *diagonal unit*. If a Menger algebra has an element that is a left diagonal unit and an element that is a right diagonal unit, then these elements are equal and no other elements which are left or right diagonal units. A left (right) diagonal unit of (G, o) is a left (right) neutral element of a *diagonal semigroup* of (G, o), i.e., a semigroup $(G, \cdot)$ with the operation $x \cdot y = o(x, \overset{n}{y})$. It is clear that a Menger algebra with right diagonal unit is reductive. Also a Menger algebra (G, o) of rank n in which there are $x_1, \ldots, x_n$ such that $o(g, x_1^n) = g$ for all $g \in G$ is reductive.

3. We say that an n-ary operation $f \in \Omega_n(A)$ is

- (i, j)-*associative*, where $1 \leqslant i < j \leqslant n$, if it satisfies the identity

$$f(a_1^{i-1}, f(a_i^{i+n-1}), a_{i+n}^{2n-1}) = f(a_1^{j-1}, f(a_j^{j+n-1}), a_{j+n}^{2n-1}), \tag{2}$$

- *associative*, if it is (i, j)-associative for all $1 \leqslant i < j \leqslant n$,

- *superassociative*, if it satisfies the identity

$$f(f(a, b_1^{n-1}), c_1^{n-1}) = f(a, f(b_1, c_1^{n-1}), \ldots, f(b_{n-1}, c_1^{n-1})). \tag{3}$$

- *self-distributive* or *autodistributive*, if for all $1 \leqslant i \leqslant n$, it satisfies the identity

$$f(a_1^{i-1}, f(b_1^n), a_{i+1}^n) = f(f(a_1^{i-1}, b_1, a_{i+1}^n), \ldots, f(a_1^{i-1}, b_n, a_{i+1}^n)). \tag{4}$$

It is clear that the operation $f \in \Omega_n(A)$ is associative if and only if it is $(1,j)$-associative for all $j = 2, 3, \ldots, n$.

Unfortunately, the set of all associative ((i,j)-associative, superassociative) n-ary operations defined on the set A may not be closed with respect to the Menger superposition. Indeed, ternary operations $f(x,y,z) = x \wedge y \wedge z$ and $g(x,y,z) = x \vee y \vee z$ defined on a lattice L are associative and superassociative, but their Menger superposition $h = \mathcal{O}(f,g,g,g)$ is neither associative nor superassociative.

We will say that an $(n+1)$-ary operation $o \in \Omega_{n+1}(A)$ is

- *quasi-(i,j)-associative*, where $1 \leqslant i < j \leqslant n$, if it satisfies the identity

$$o(a, b_1^{i-1}, o(a, b_i^{i+n-1}), b_{i+n}^{2n-1}) = o(a, b_1^{j-1}, o(a, b_j^{j+n-1}), b_{j+n}^{2n-1}), \tag{5}$$

- *quasi-associative*, if it is quasi-(i,j)-associative for all $1 \leqslant i < j \leqslant n$,

- *quasi-superassociative*, if it satisfies the identity

$$o(a, o(a, b, c_1^{n-1}), d_1^{n-1}) = o(a, b, o(a, c_1, d_1^{n-1}), \ldots, o(a, c_{n-1}, d_1^{n-1})), \tag{6}$$

- *quasi-self-distributive* or *quasi-autodistributive*, if for all $1 \leqslant i \leqslant n$ it satisfies the identity

$$o(a, b_1^{i-1}, o(a, c_1^n), b_{i+1}^n) = o(a, o(a, b_1^{i-1}, c_1, b_{i+1}^n), \ldots, o(a, b_1^{i-1}, c_n, b_{i+1}^n)). \tag{7}$$

Note that an $(n+1)$-ary operation $o \in \Omega_{n+1}(A)$ is quasi-associative if and only if all n-ary operations $f_a \in \Omega_n(A)$ defined by

$$f_a(x_1^n) = o(a, x_1^n) \tag{8}$$

are associative in the above sense. Thus any algebra (A, o) with one $(n+1)$-ary quasi-associative operation o can be characterized by the algebra $(A, \mathbb{F})$ with the family $\mathbb{F} = \{f_a \,|\, a \in A\}$ of n-ary associative operations defined by (8), i.e., by the class of n-ary semigroups (A, f_a), where $a \in A$. Analogously a quasi-superassociative (quasi-self-distributive) algebra (A, o) can be characterized by the class of n-ary superassociative (self-distributive) algebras (A, f_a). A group-like Menger algebra (A, o) of rank n (cf. [2] or [4]) which is simultaneously quasi-associative and quasi-self-distributive can be characterized by self-distributive n-ary groups (A, f_a), i.e., by self-distributive associative n-ary quasigroups (cf. [1]). This means that these Menger algebras can be described by commutative groups and one of their automorphisms (cf. [3, Theorem 3]).

Example 1. On a commutative semigroup $(G, +)$ with the property $nx = x$ for each $x \in G$ and fixed $n \geqslant 2$ we define the $(n+1)$-ary operation

$$o(x_0, x_1^n) = \varphi(x_0) + x_1 + x_2 + \cdots + x_n + b,$$

where $b \in G$ is fixed and φ is an idempotent endomorphism of $(G, \cdot)$ such that $\varphi(b) = b$. Direct computations show that (G, o) is a quasi-associative Menger algebra of rank n. If φ is not the identity map, then this Menger algebra is not associative. So, the class of quasi-associative Menger algebras contains non-trivial non-associative algebras.

Example 2. Let $(G, +)$ be a commutative semigroup in which $nx = x$ for all $x \in G$ and fixed $n \geqslant 2$. Then for every $a \in G$ the set G with the operation

$$f_a(x_0, x_1^n) = x_0 + x_1 + x_2 + \cdots + x_n + a$$

is a Menger algebra of rank n that is both associative, quasi-associative and self-distributive. Moreover, the set $\Phi_G = \{f_a \,|\, a \in G\}$ is closed with respect to the Menger superposition $\mathcal{O}$. Thus, $(\Phi_G, \mathcal{O})$ is a Menger algebra of associative, quasi-associative, quasi-superassociative and self-distributive $(n+1)$-ary operations.

4. Now we present a characterization of quasi-associative Menger algebras by algebras of associative n-place functions.

First, we characterize quasi-(i, j)-associative Menger algebras.

Theorem 1. *A Menger algebra (G, o) of rank n is isomorphically represented by (i, j)-associative n-ary operations if and only if it is quasi-(i, j)-associative.*

Proof. NECESSITY. Let $(\Phi, \mathcal{O})$ be a Menger algebra of (i, j)-associative n-ary operations defined on the set A. Then, for all $f, g_1, \ldots, g_{2n-1} \in \Phi$ and all elements $a_1, \ldots, a_n \in A$, we have

$$\begin{aligned}
&\mathcal{O}(f, g_1^{i-1}, \mathcal{O}(f, g_i^{i+n-1}), g_{i+n}^{2n-1})(a_1^n) = \\
&f(g_1(a_1^n), \ldots, g_{i-1}(a_1^n), \mathcal{O}(f, g_i^{i+n-1})(a_1^n), g_{i+n}(a_1^n), \ldots, g_{2n-1}(a_1^n)) = \\
&f(g_1(a_1^n), \ldots, g_{i-1}(a_1^n), f(g_i(a_1^n), \ldots, g_{i+n-1}(a_1^n))(a_1^n), g_{i+n}(a_1^n), \ldots, g_{2n-1}(a_1^n)) = \\
&f(g_1(a_1^n), \ldots, g_{j-1}(a_1^n), f(g_j(a_1^n), \ldots, g_{j+n-1}(a_1^n))(a_1^n), g_{j+n}(a_1^n), \ldots, g_{2n-1}(a_1^n)) = \\
&f(g_1(a_1^n), \ldots, g_{j-1}(a_1^n), \mathcal{O}(f, g_j^{j+n-1})(a_1^n), g_{j+n}(a_1^n), \ldots, g_{2n-1}(a_1^n)) = \\
&\mathcal{O}(f, g_1^{j-1}, \mathcal{O}(f, g_j^{j+n-1}), g_{j+n}^{2n-1})(a_1^n).
\end{aligned}$$

Thus, $\mathcal{O}(f, g_1^{i-1}, \mathcal{O}(f, g_i^{i+n-1}), g_{i+n}^{2n-1})(a_1^n) = \mathcal{O}(f, g_1^{j-1}, \mathcal{O}(f, g_j^{j+n-1}), g_{j+n}^{2n-1})(a_1^n)$, i.e., a Menger algebra $(\Phi, \mathcal{O})$ is quasi-(i, j)-associative.

SUFFICIENCY. Let (G, o) be a quasi-(i, j)-associative Menger algebra of rank n. For every $g \in G$ we define on the set $G_0 = G \cup \{e, c\}$, where $e \neq c$ and $e \notin G$, $c \notin G$, the n-ary operation ω_g by putting:

$$\omega_g(x_1^n) = \begin{cases} o(g, x_1^n), & \text{if } x_1, \ldots, x_n \in G, \\ g, & \text{if } x_1 = \ldots = x_n = e, \\ c, & \text{otherwise.} \end{cases}$$

To prove that this operation is associative, we must consider a few cases.

First, we consider the case when $x_1, \ldots, x_{2n-1} \in G$. In this case

$$\omega_g(x_1^{i-1}, \omega_g(x_i^{i+n-1}), x_{i+n}^{2n-1}) = o(g, x_1^{i-1}, o(g, x_i^{i+n-1}), x_{i+n}^{2n-1}) =$$
$$o(g, x_1^{j-1}, o(g, x_j^{j+n-1}), x_{j+n}^{2n-1}) = \omega_g(x_1^{j-1}, \omega_g(x_j^{j+n-1}), x_{j+n}^{2n-1}).$$

If $x_1 = \ldots = x_{2n-1} = e$, then, according to the definition, we have

$$\omega_g(\overset{i-1}{e}, \omega_g(\overset{n}{e}), \overset{n-i}{e}) = \omega_g(\overset{i-1}{e}, g, \overset{n-i}{e}) = c$$

and

$$\omega_g(\overset{j-1}{e}, \omega_g(\overset{n}{e}), \overset{n-j}{e}) = \omega_g(\overset{j-1}{e}, g, \overset{n-j}{e}) = c.$$

Thus,

$$\omega_g(\overset{i-1}{e}, \omega_g(\overset{n}{e}), \overset{n-i}{e}) = \omega_g(\overset{j-1}{e}, \omega_g(\overset{n}{e}), \overset{n-j}{e}).$$

In all other cases

$$\omega_g(x_1^{i-1}, \omega_g(x_i^{i+n-1}), x_{i+n}^{2n-1}) = c = \omega_g(x_1^{j-1}, \omega_g(x_j^{j+n-1}), x_{j+n}^{2n-1}).$$

So, in any case the operation ω_g is (i,j)-associative.

Now we show that $P\colon g \mapsto \omega_g$ is an isomorphism between (G, o) and $(\Phi_G, \mathcal{O})$, where $\Phi_G = \{\omega_g \mid g \in G\}$. To prove this fact we also must consider a few cases.

Let $g, g_1, \ldots, g_n \in G$.

1) If $x_1, \ldots, x_n \in G$, then

$$\omega_{o(g,g_1^n)}(x_1^n) = o(o(g, g_1^n), x_1^n) = o(g, o(g_1, x_1^n), \ldots, o(g_n, x_1^n))$$
$$= \omega_g(\omega_{g_1}(x_1^n), \ldots, \omega_{g_n}(x_1^n)) = \mathcal{O}(\omega_g, \omega_{g_1}, \ldots, \omega_{g_n})(x_1^n).$$

2) If $x_1 = x_2 = \ldots x_n = e$, then, according to the definition of ω_g, we obtain

$$\mathcal{O}(\omega_g, \omega_{g_1}, \ldots, \omega_{g_n})(\overset{n}{e}) = \omega_g(\omega_{g_1}(\overset{n}{e}), \ldots, \omega_{g_n}(\overset{n}{e})) = \omega_g(g_1^n) = o(g, g_1^n)$$

and $\omega_{o(g,g_1^n)}(\overset{n}{e}) = o(g, g_1^n)$. Thus, $\omega_{o(g,g_1^n)}(\overset{n}{e}) = \mathcal{O}(\omega_g, \omega_{g_1}, \ldots.\omega_{g_n})(\overset{n}{e})$.

3) In other cases we have $\omega_{o(g,g_1^n)}(x_1^n) = c$ and

$$\mathcal{O}(\omega_g, \omega_{g_1}, \ldots, \omega_{g_n})(x_1^n) = \omega_g(\omega_{g_1}(x_1^n), \ldots, \omega_{g_n}(x_1^n)) = \omega_g(\overset{n}{c}) = c.$$

Thus, in any case $\omega_{o(g,g_1^n)} = \mathcal{O}(\omega_g, \omega_{g_1}, \ldots, \omega_{g_n})$ This means that $P(o(g, g_1^n)) = \mathcal{O}(P(g), P(g_1), \ldots, P(g_n))$. Hence, P is a homomorphism.

Obviously P is onto $(\Phi_G, \mathcal{O})$. Moreover, if $P(g_1) = P(g_2)$, for some $g_1, g_2 \in G$, then also $\omega_{g_1}(x_1^n) = \omega_{g_2}(x_1^n)$ for $x_1, \ldots x_n \in G_0$. In particular, $\omega_{g_1}(\overset{n}{e}) = \omega_{g_2}(\overset{n}{e})$, which gives $g_1 = g_2$. So, P is an isomorphism. □

In the same way, using the same construction of the operations ω_g, we can prove the following two theorems.

Theorem 2. *A Menger algebra (G, o) of rank n is isomorphically represented by associative n-ary operations if and only if it is quasi-associative.*

Theorem 3. *Any quasi-superassociative Menger algebra (G, o) of rank n can be isomorphically represented by suprassociative n-ary opertations defined on some set.*

From the above results we can deduce the following corollary.

Corollary 1. *If a Menger algebra of rank n is at the same time quasi-(i, j)-associative and quasi-superassociative, then it can be isomorphically represented by n-ary operations which are at the same time (i, j)-associative and superassociative.*

Analogous result is valid for Menger algebras which are at the same time quasi-associative and quasi-superassociative.

Problem A. *Find necessary and sufficient conditions under which a Menger algebra of rank n can be isomorphically represented by superassociative n-ary operations defined on some set.*

5. We will now consider a Menger algebra of self-distributive n-ary operations.

Theorem 4. *A Menger algebra (G, o) of rank n is homomorphically represented by self-distributive n-ary operations if and only if it is quasi-self-distributive.*

Proof. NECESSITY. Let $(\Phi, \mathcal{O})$ be a Menger algebra of self-distributive n-ary operations defined on the set A. Then for all $f, g_i, h_i \in \Phi$, $i = 1, 2, \ldots, n$, and all $a_1, \ldots, a_n \in A$ we have

$$\begin{aligned}
&\mathcal{O}(f, g_1^{i-1}, \mathcal{O}(f, h_1^n), g_{i+1}^n)(a_1^n) = \\
&f(g_1(a_1^n), \ldots, g_{i-1}(a_1^n), f(h_1(a_1^n), \ldots, h_n(a_1^n)), g_{i+1}(a_1^n), \ldots g_n(a_1^n)) \overset{(4)}{=} \\
&f(f(g_1(a_1^n), \ldots, g_{i-1}(a_1^n), h_1(a_1^n), g_{i+1}(a_1^n), \ldots g_n(a_1^n)), \ldots, \\
&\qquad\qquad f(g_1(a_1^n), \ldots, g_{i-1}(a_1^n), h_n(a_1^n), g_{i+1}(a_1^n), \ldots g_n(a_1^n))) = \\
&\mathcal{O}(f, \mathcal{O}(f, g_1^{i-1}, h_1, g_{i+1}^n), \ldots, \mathcal{O}(f, g_1^{i-1}, h_n, g_{i+1}^n))(a_1^n).
\end{aligned}$$

Thus, $(\Phi, \mathcal{O})$ is a quasi-self-distributive Menger algebra.

SUFFICIENCY. Let (G, o) be a quasi-self-distributive Menger algebra of rank n. For every $g \in G$ we define on G the n-ary operation ω_g by putting

$$\omega_g(x_1^n) = o(g, x_1^n).$$

Then for all $x_i, y_i \in G$ and $i = 1, \ldots, n$, we obtain:

$$\begin{aligned}&\omega_g(x_1^{i-1}, \omega_g(y_1^n), x_{i+1}^n) = o(g, x_1^{i-1}, o(g, y_1^n), x_{i+1}^n) \overset{(7)}{=} \\ &o(g, o(g, x_1^{i-1}, y_1, x_{i+1}^n), \ldots, o(g, x_1^{i-1}, y_n, x_{i+1}^n)) = \\ &\omega_g(\omega_g(x_1^{i-1}, y_1, x_{i+1}^n), \ldots, \omega_g(x_1^{i-1}, y_n, x_{i+1}^n)).\end{aligned}$$

So, the operation ω_g is self-distributive.

Now we show that $P\colon g \mapsto \omega_g$ is a homomorphism between (G, o) and $(\Phi_G, \mathcal{O})$, where $\Phi_G = \{\omega_g \mid g \in G\}$. Indeed, for all $g, g_1, \ldots, g_n, x_1, \ldots, x_n \in G$ we have:

$$\begin{aligned}\omega_{o(g,g_1^n)}(x_1^n) &= o(o(g, g_1^n), x_1^n) = o(g, o(g_1, x_1^n), \ldots, o(g_n, x_1^n)) \\ &= o(g, \omega_{g_1}(x_1^n), \ldots, \omega_{g_n}(x_1^n)) = \omega_g(\omega_{g_1}(x_1^n), \ldots, \omega_{g_n}(x_1^n)) \\ &= \mathcal{O}(\omega_g, \omega_{g_1}, \ldots, \omega_{g_n})(x_1^n),\end{aligned}$$

which means that

$$P(o(g, g_1^n)) = \mathcal{O}(P(g), P(g_1), \ldots, P(g_n)).$$

This completes the proof. □

Note that the homomorphism $P\colon g \mapsto \omega_g$ may not be one-to-one, but if a Menger algebra (G, o) is reductive, then it is one-to-one, and consequently, it is an isomorphism. Thus the following result is valid.

Corollary 2. *If a quasi-self-distributive Menger algebra of rank n is reductive, then it can be isomorphically represented by self-distributive n-ary operations defined on some set.*

In a similar way we can prove

Theorem 5. *Any quasi-associative (quasi-(i, j)-associative, quasi-superassociative) Menger algebra (G, o) of rank n satisfying* (7) *can be homomorphically represented by self-distributive associative (respectively, (i, j)-associative, superassociative) n-ary operations defined on some set.*

Problem B. *Find necessary and sufficient conditions under which a Menger algebra of rank n can be isomorphically represented by self-distributive n-ary operations defined on some set.*

Problem C. *Find necessary and sufficient conditions under which a quasi-(i, j)-associative (quasi-associative, quasi-superassociative) Menger algebra of rank n satisfying* (7) *can be isomorphically represented by self-distributive (i, j)-associative (associative, superassociative) n-ary operations defined on some set.*

References

[1] **W.A. Dudek**, *Autodistributive n-groups*, Commentationes Math. Annales Soc. Math. Polonae, Prace Matematyczne **23** (1983), 1 – 11.

[2] **W.A. Dudek**, *On some n-ary Menger groupoids*, Mathematica **43(66)** (2001), 195 – 201.

[3] **W.A. Dudek**, *On distributive n-ary groups*, Quasigroups and Related Systems **2** (1995), 132 – 151.

[4] **W.A. Dudek and V.S. Trokhimenko**, *Algebras of multiplace functions*, Walter de Gruyter GmbH & Co. KG, Berlin/Boston, 2012.

[5] **W.A. Dudek and V.S. Trokhimenko**, *On (i,j)-commutativity in Menger algebras of n-place functions*, Quasigroups Related Syst. **24** (2016), 219 – 230

[6] **J. Henno**, *On the completeness of associative idempotent functions*, Z. Math. Logik Grundlag. Math. **25** (1973), 37 – 43.

[7] **H. Länger**, *A characterization of full function algebras*, J. Algebra **119** (1988), 261 – 264.

[8] **J. Pashazadeh and Yu. Movsisyan**, *A characterization of $(2,n)$-semigroup of n-place functions and De Morgan $(2,n)$-semigroup of n-place functions*, Commun. Algebra **40** (2012), 3430 – 3441.

[9] **H. Skala**, *Grouplike Menger algebras*, Fund. Math. **79** (1973), 199 – 207.

[10] **B. Schweizer and R. Sklar**, *The algebra of vector-valued functions*, Bull. Amer. Math. Soc. **73** (1967), 510 – 515.

[11] **F.M. Sokhatsky**, *On the associativity of multiplace operations*, Quasigroups and Related Systems, **4** (1997), 51 – 66.

[12] **V.S. Trokhimenko**, *Algebras of vector-valued functions*, Quasigroups and Related Systems **8** (2001), 73 – 85.

Received February 20, 2018

W.A. Dudek
Faculty of Pure and Applied Mathematics, Wroclaw University of Science and Technology,
50-370 Wroclaw, Poland
E-mail: wieslaw.dudek@pwr.edu.pl

V.S. Trokhimenko
Department of Mathematics, Pedagogical University, 21100 Vinnitsa, Ukraine
E-mail: vtrokhim@gmail.com

Quasigroups and Related Systems **26** (2018), 53 – 66

Retractions of cyclic finitely supported Cb-sets

Mohammad M. Ebrahimi, Khadijeh Keshvardoost and Mojgan Mahmoudi

Abstract. The monoid Cb of name substitutions originated by Pitts in name abstraction, and the notion of a finitely supported Cb-set appeared in the study of models of homotopy type theory in the works of Gabbay and Pitts. On the other hand, retracts and retractions play a crucial role in most branches of mathematics as well as in computer science where partial morphisms need to be completed. Retracts are the subobjects whose related inclusion morphism have a left inverse, called retraction.

In this paper, we study the retracts and retractions of cyclic finitely supported Cb-sets. We find the general definition of retractions from a cyclic Cb-set, and give necessary conditions under which retractions exist. Also, fix-simple retracts of a cyclic Cb-set are characterized. Further, the cyclic finitely supported Cb-sets all whose subobjects are retract, are studied. In particular, we give a necessary condition for a cyclic finitely supported Cb-set to be retractable.

1. Introduction and preliminaries

The notion of a nominal set was originated by Fraenkel in 1922 and developed by Mostowski in the 1930s under the name of legal sets. The legal sets were applied to prove the independence of the axiom of choice with the other axioms (in the classical Zermelo-Fraenkel (ZF) set theory).

In 2001, Gabbay and Pitts rediscovered those sets in the context of name abstraction. They called them nominal sets, and applied this notion to properly model the syntax of formal systems involving variable binding operations (see [5]).

In [10], Pitts generalized the notion of nominal sets, by first adding two elements 0, 1 to $\mathbb{D}$, then generalizing the notion of a finitary permutation to *finite substitution*, and considering the monoid Cb instead of the group G. Then he defined the notion of a support for Cb-sets, sets with an action of Cb on them, and invented the notion of *finitely supported* Cb-sets, a generalization of nominal sets. He has shown that the category of finitely supported Cb-sets is in fact isomorphic to the category of nominal sets equipped with two families of unary operations which substitute names (elements of $\mathbb{D}$) by the constants 0 or 1; and the category of finitely supported Cb-sets is a coreflective subcategory of the category of Cb-sets.

The notion of retractions appears when one can find a left inverse (reflection) for a morphism. This notion plays a crucial role in many areas of mathematics, such as homological algebra, topology, ordered algebraic structures, etc. The retracts

2010 Mathematics Subject Classification: 08A30, 18A20, 20B30, 20M30, 20M50, 68Q70.
Keywords: Cb-set, finitely supported, retract, retractable.

are also known as complete or partial objects in recursion theory by computer scientists (see [7]).

On the other hand, we recall from [6] that every Cb-set is a disjoint union of all its indecomposable sub Cb-sets, where an indecomposable Cb-set is a Cb-set which can not be written as a disjoint union of non-empty sub Cb-sets. Therefore, to find retractions of a Cb-set, it is sufficient to obtain retractions of its indecomposable sub Cb-sets. Also, it is known that cyclic finitely supported Cb-sets are indecomposable (see Proposition I.5.8 of [6]). These facts provided our motivation to study the retracts of cyclic finitely supported Cb-sets in this paper. First, applying the characterization of cyclic finitely supported Cb-sets from [3], and assuming the existence of retractions from a cyclic Cb-set to its proper sub Cb-sets, we find the possible definition of them.

Moreover, using the characterization of cyclic fix-simple finitely supported Cb-sets given in [3], we find a characterization of retracts of cyclic finitely supported Cb-sets. Also, we prove that simple finitely supported Cb-sets which are fix-simple with one zero element are retracts of cyclic finitely supported Cb-sets.

Finally, retractable (the ones all whose subobjects are retract) finitely supported Cb-sets are studied; and a necessary condition for cyclic finitely supported Cb-sets to be retractable is obtained.

1.1. M-sets

In the following, we recall some notions and facts about M-sets, for a general monoid M. For more information, see ([2, 6]).

A (left) *M-set* for a monoid M with identity e is a set X equipped with a map $M \times X \to X, (m, x) \rightsquigarrow mx$, called an *action* of M on X, such that $ex = x$ and $m(m'x) = (mm')x$, for all $x \in X$ and $m, m' \in M$. An *equivariant map* from an M-set X to an M-set Y is a map $f : X \to Y$ with $f(mx) = mf(x)$, for all $x \in X, m \in M$.

An element x of an M-set X is called a *zero* (or a *fixed*) element if $mx = x$, for all $m \in M$. We denote the set of all zero elements of an M-set X by $\operatorname{Fix} X$. The M-set X all of whose elements are zero is called a *discrete* M-set, or an M-set with *identity action*.

An equivalence relation ρ on an M-set X is called a *congruence* on X if $x \rho x'$ implies $mx \,\rho\, mx'$, for $x, x' \in X$, $m \in M$. We denote the set of all congruences on X by $\operatorname{Con}(X)$. Also, for $x, x' \in X$, the smallest congruence on X containing (x, x') is denoted by $\rho(x, x')$. It is in fact, the equivalence relation generated by $\{(mx, mx') \mid m \in M\}$.

A subset Y of an M-set X is a *sub M-set* (or *M-subset*) of Y if for all $m \in M$ and $y \in Y$ we have $my \in Y$. The subset $\operatorname{Fix} X$ of X is in fact a sub M-set.

1.2. Cb-sets

Now, we give some basic notions about the monoid Cb, and Cb-sets. For more information one can see [9, 10].

Let $\mathbb{D}$ be an infinite countable set, whose elements are sometimes called *directions* (*atomic names* or *data values*) and Perm$\mathbb{D}$ be the group of all permutations (bijection maps) on $\mathbb{D}$. A permutation $\pi \in \text{Perm}\mathbb{D}$ is said to be *finite* if $\{d \in \mathbb{D} \mid \pi(d) \neq d\}$ is finite. Clearly the set $\text{Perm}_{\text{f}}\mathbb{D}$ of all finitary permutations is a subgroup of Perm$\mathbb{D}$.

Also, we take $2 = \{0, 1\}$ with $0, 1 \notin \mathbb{D}$.

Definition 1.1. (a) A finite *substitution* is a function $\sigma : \mathbb{D} \to \mathbb{D} \cup 2$ for which $\text{Dom}_{\text{f}}\sigma = \{d \in \mathbb{D} \mid \sigma(d) \neq d\}$ is finite.

(b) If $d \in \mathbb{D}$ and $b \in 2$, we write (b/d) for the finite substitution which maps d to b, and maps identically on other elements of $\mathbb{D}$. Each (b/d) is called a *basic substitution*.

(c) If $d, d' \in \mathbb{D}$ then we write $(d\,d')$ for the finite substitution that transposes d and d', and keeps fixed all other elements. Each $(d\,d')$ is called a *transposition substitution*.

Definition 1.2. (a) Let Sb be the monoid whose elements are finite substitutions, with the monoid operation given by $\sigma \cdot \sigma' = \hat{\sigma}\sigma'$, where $\hat{\sigma} : \mathbb{D} \cup 2 \to \mathbb{D} \cup 2$ maps 0 to 0, 1 to 1, and on $\mathbb{D}$ is defined the same as σ. The identity element of Sb is the inclusion $\iota : \mathbb{D} \hookrightarrow \mathbb{D} \cup 2$.

(b) Let Cb be the submonoid of Sb satisfying the following *injectivity condition*:

$$(\forall d, d' \in \mathbb{D}),\ \sigma(d) = \sigma(d') \notin 2 \Rightarrow d = d'.$$

(c) Take S to be the subsemigroup of Cb generated by basic substitutions. The members of S are of the form $\delta = (b_1/d_1) \cdots (b_k/d_k) \in S$ for some $d_i \in \mathbb{D}$ and $b_i \in 2$, and we denote the set $\{d_1, \ldots, d_k\}$ by $\mathbb{D}_\delta$.

Remark 1.3. (1) Notice that each finite permutation π on $\mathbb{D}$, can be considered as a finite substitution $\iota \circ \pi : \mathbb{D} \to \mathbb{D} \cup 2$. Doing so, throughout this paper, we consider the group $\text{Perm}_{\text{f}}\mathbb{D}$ as a submonoid of Cb, and denote $\iota \circ \pi$ with the same notation π.

(2) Let $d \in \mathbb{D}$ and $b \in 2$. Then, for a finite permutation π and a basic substitution (b/d), one can compute that in Cb, $\pi(b/d) = (b/\pi(d))\pi$ and $(b/d)\pi = \pi(b/\pi^{-1}(d))$. Then, by induction, we also have:

$$\pi(b_1/d_1) \cdots (b_k/d_k) = (b_1/\pi d_1) \cdots (b_k/\pi d_k)\pi,$$

and

$$(b_1/d_1) \cdots (b_k/d_k)\pi = \pi(b_1/\pi^{-1}d_1) \cdots (b_k/\pi^{-1}d_k),$$

for $\pi \in \text{Perm}_{\text{f}}(\mathbb{D})$, $d_1, \cdots, d_k \in \mathbb{D}$, and $b_i \in 2$, for $i = 1, \ldots, k$.

(3) Let $d \neq d' \in \mathbb{D}$ and $b, b' \in 2$. Then $(b/d)(b'/d') = (b'/d')(b/d)$. But, we see that $(1/d)(0/d) = (0/d)$ and $(0/d)(1/d) = (1/d)$, and hence $(1/d)(0/d) \neq (0/d)(1/d)$.

Theorem 1.4. [3] *For the monoid Cb, we have:*

$$Cb = \mathrm{Perm_f}(\mathbb{D}) \cup \mathrm{Perm_f}(\mathbb{D})S, \quad \mathrm{Perm_f}(\mathbb{D}) \cap \mathrm{Perm_f}(\mathbb{D})S = \emptyset.$$

1.3. Finitely supported Cb-sets

In this subsection, we give some basic notions of finitely supported Cb-sets needed in the sequel, some of which are given in [10].

The following definition introduces the notion of a, so called, *support*, which is the central notion to define finitely supported Cb-sets.

Definition 1.5. (a) Suppose X is a Cb-set. A subset $C_x \subseteq \mathbb{D}$ supports an element x of X if, for every $\sigma, \sigma' \in Cb$,

$$(\sigma(c) = \sigma'(c), (\forall c \in C_x)) \Rightarrow \sigma x = \sigma' x$$

If there is a finite (possibly empty) support C_x then we say that x is *finitely supported*.

(b) A Cb-set X all of whose elements has a finite support, is called a *finitely supported Cb-set*.

We denote the category of all Cb-sets with equivariant maps between them by $\mathbf{Set}^{Cb}$, and its full subcategory of all finitely supported Cb-sets by $\mathbf{Set}^{Cb}_{\mathrm{fs}}$.

Remark 1.6. [3] Suppose that X is a non-empty finitely supported Cb-set and $x \in X \setminus \mathrm{Fix}\, X$.

(1) By Remark 1.3(3), it is clear that

$$\{d \in \mathbb{D} \mid (0/d)\, x \neq x\} = \{d \in \mathbb{D} \mid (1/d)\, x \neq x\}.$$

This set is in fact the least finite support of x. First notice that, by Lemma 2.4 of [10], this set is a finite support for x. Now, let C be a finite support for x. Then for any $d \in \mathbb{D}$ with $(0/d)\, x \neq x$, by taking $\sigma = (0/d)$ and $\sigma' = \iota$ in the Definition 1.5(a), we get $(0/d)d' \neq d'$, for some $d' \in C$. So, by the definition of $(0/d)$, we have $d = d'$, and therefore $d \in C$.

From now on, we call the least finite support for x *the support* for x, and denote it by $\mathrm{supp}\, x$.

(2) Let $\delta \in S$. Then, by (1),

$$\delta\, x = x \text{ if and only if } \mathbb{D}_\delta \cap \mathrm{supp}\, x = \emptyset.$$

(3) Let $\{d_1, \ldots, d_k\} \subseteq \mathrm{supp}\, x$. Then,

$$\mathrm{supp}\, (b_1/d_1) \cdots (b_k/d_k)\, x \subseteq \mathrm{supp}\, x \setminus \{d_1, \ldots, d_k\},$$

for any $b_i \in 2$ and $i = 1, \cdots, k$.

(4) Let $\delta \in S$. Then,

$$\delta\, x = x \quad \text{if and only if} \quad |\mathrm{supp}\, \delta\, x| = |\mathrm{supp}\, x|.$$

(5) By (3) and (4), we have

$$\delta\, x \neq x \quad \text{if and only if} \quad |\mathrm{supp}\,\delta\, x| < |\mathrm{supp}\, x|.$$

(6) Let $\pi \in \mathrm{Perm_f}(\mathbb{D})$. Then, $\mathrm{supp}\,\pi x = \pi\,\mathrm{supp}\, x$, and so $|\mathrm{supp}\,\pi x| = |\pi \mathrm{supp}\, x| = |\mathrm{supp}\, x|$.

(7) X has a zero element.

Remark 1.7. [3] Let X be a finitely supported Cb-set and $x \in X$. Then,

(1) $S_x \doteq \{\delta \in S \mid \delta\, x = x\}$ is a subsemigroup of S;

(2) $S'_x \doteq S \setminus S_x = \{\delta \in S \mid \delta\, x \neq x\}$ is also a subsemigroup of S;

(3) If $\delta \in S'_x$ then $\delta\, x = \delta_1\, x$, for some $\delta_1 \in S'_x$ with $\mathbb{D}_{\delta_1} \subseteq \mathrm{supp}\, x$;

(4) If $\delta \in S'_x$ then $\pi x \neq \pi'\delta x$, for some $\pi, \pi' \in \mathrm{Perm_f}(\mathbb{D})$. Since otherwise, if $\pi x = \pi'\delta x$ then by Remark 1.6(5,6),

$$|\mathrm{supp}\, x| = |\mathrm{supp}\,\pi x| = |\mathrm{supp}\,\pi'\delta x| = |\mathrm{supp}\,\delta x| < |\mathrm{supp}\, x|$$

which is impossible.

Definition 1.8. A cyclic finitely supported Cb-set X is said to be *cyclic*, if it is generated by only one element, that is $X = Cb\, x$, for some $x \in X$.

Lemma 1.9. [3] *Let $Cb\, x$ be a cyclic finitely supported Cb-set. Then,*

$$Cb\, x = \mathrm{Perm_f}(\mathbb{D})S'_x\, x \cup \mathrm{Perm_f}(\mathbb{D})\, x, \quad \mathrm{Perm_f}(\mathbb{D})S'_x\, x \cap \mathrm{Perm_f}(\mathbb{D})\, x = \emptyset.$$

2. Retractions of cyclic finitely supported Cb-sets

In this section, we study retracts and retractions of cyclic finitely supported Cb-sets. We find the general definition of a retraction, and give some necessary and sufficient conditions for a sub Cb-set of a cyclic finitely supported Cb-set to be a retract.

First, we give the definition of a *retraction*.

Let X be an object of a category $\mathfrak{C}$. A subobject J of X is called a *retract* of X if there exists a morphism $g : X \to J$, called *a retraction*, such that $g|_J = id_J$.

Notice that, for a proper sub Cb-set Cbx' of Cbx, Cbx' is a retract of Cbx if and only if $Cb\delta_0 x$ is a retract of Cbx, where $x' = \pi\delta_0 x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta_0 \in S'_x$.

Lemma 2.1. *Suppose $\pi\delta_0 x$ is a non-zero element in Cbx, where $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta_0 \in S'_x$. If there exists a retraction φ from Cbx to $Cb\delta_0 x$ then*

(i) $\varphi(x) \in \mathrm{Perm_f}(\mathbb{D})\delta_0 x$;

(ii) $\varphi(x) = \delta_0 x$.

Proof. (i) We have $\varphi(x) \in Cb\delta_0 x$. So by Lemma 1.9, $\varphi(x) \in \mathrm{Perm_f}(\mathbb{D})S'_{\delta_0 x}\delta_0 x$ or $\varphi(x) \in \mathrm{Perm_f}(\mathbb{D})\delta_0 x$. We show $\varphi(x) \in \mathrm{Perm_f}(\mathbb{D})\delta_0 x$. On the contrary, let $\varphi(x) \in \mathrm{Perm_f}(\mathbb{D})S'_{\delta_0 x}\delta_0 x$. Then, $\varphi(x) = \pi'\delta'\delta_0 x$ where $\delta' \in S'_{\delta_0 x}$ and $\pi' \in \mathrm{Perm_f}(\mathbb{D})$. Since φ is a retraction and $\delta_0 x \in Cb\delta_0 x$, we get

$$\delta_0 x = \varphi(\delta_0 x) = \delta_0\varphi(x) = \delta_0\pi'\delta'\delta_0 x.$$

Now, by Remark 1.6(5,6),

$$|\mathrm{supp}\,\delta_0 x| = |\mathrm{supp}\,\delta_0\pi'\delta'\delta_0 x| < |\mathrm{supp}\,\delta_0 x|,$$

which is impossible.

(ii) By (i), we get $\varphi(x) \in \mathrm{Perm_f}(\mathbb{D})\delta_0 x$. So there exists $\pi' \in \mathrm{Perm_f}(\mathbb{D})$ such that $\varphi(x) = \pi'\delta_0 x$. Since φ is a retraction and $\delta_0 x \in Cb\delta_0 x$, we get

$$\delta_0 x = \varphi(\delta_0 x) = \delta_0\varphi(x) = \delta_0\pi'\delta_0 x = \pi'\delta'_0\delta_0 x,$$

where the last equality is true by Remark 1.3(2). Now, $\delta'_0 \in S_{\delta_0 x}$, since otherwise, if $\delta'_0 \in S'_{\delta_0 x}$ then by Remark 1.6(5,6),

$$|\mathrm{supp}\,\delta_0 x| = |\mathrm{supp}\,\pi'\delta'_0\delta_0 x| = |\mathrm{supp}\,\delta'_0\delta_0 x| < |\mathrm{supp}\,\delta_0 x|,$$

which is impossible. Thus, $\delta'_0 \in S_{\delta_0 x}$ and so $\delta_0 x = \pi'\delta'_0\delta_0 x = \pi'\delta_0 x$. Therefore, $\varphi(x) = \delta_0 x$. □

Corollary 2.2. *Suppose $\pi\delta_{_0}x$ is a non-zero element of Cbx, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta_0 \in S'_x$. Let $\varphi : Cbx \to Cb\delta_0 x$ be a retraction. Then,*

(i) *If $\delta x \in Cb\delta_0 x$ then $\delta\delta_{_0}\, x = \delta x$;*

(ii) *If $\pi\delta_0 x = \pi'\delta'_{_0}x$ then $\delta_{_0}x = \delta'_{_0}x$.*

Proof. (i) Since φ is a retraction, by Lemma 2.1, we get

$$\delta x = \varphi(\delta x) = \delta\varphi(x) = \delta\delta_{_0}x.$$

(ii) Let $\pi\delta_0 x = \pi'\delta'_{_0}x$. Then $\delta'_{_0}x \in Cb\delta_0 x$ and $|\mathrm{supp}\,\delta'_{_0}x| = |\mathrm{supp}\,\delta_{_0}x|$. Since $\delta'_{_0}x \in Cb\delta_0 x$, by (i) $\delta'_{_0}x = \delta'_{_0}\delta_{_0}x$. So $\mathrm{supp}\,\delta'_{_0}x \subseteq \mathrm{supp}\,\delta_{_0}x$. Now, since $|\mathrm{supp}\,\delta'_{_0}x| = |\mathrm{supp}\,\delta_{_0}x|$ and $\mathrm{supp}\,\delta_0 x$ is finite, we get $\mathrm{supp}\,\delta'_{_0}x = \mathrm{supp}\,\delta_{_0}x$. Thus for all $d \in \mathbb{D}_{\delta'_0}$, we have $d \notin \mathrm{supp}\,\delta_{_0}x$ and so $\delta'_{_0}x = \delta'_{_0}\delta_0 x = \delta_0 x$. □

Remark 2.3. Let $Cb\delta_0 x$ be a proper sub Cb-set of Cbx. Then,

(1) $B = \{\pi\delta x \in \mathrm{Perm_f}(\mathbb{D})S'_x x \mid \mathbb{D}_\delta \cap \mathrm{supp}\,\delta_0 x \neq \emptyset\}$ is a proper sub Cb-set of Cbx.

(2) If $a \in B$ then $a = \pi\delta x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta \in S'_{\delta_0 x}$. This is because, since $\delta\, x \in B$, we get $\mathbb{D}_\delta \cap \mathrm{supp}\,\delta_0 x \neq \emptyset$. So by Remark 1.6(2), $\delta\delta_0 x \neq \delta_0 x$. Therefore, $\delta \in S'_{\delta_0 x}$.

(3) If $a \in Cbx \setminus B$ then $a = \pi x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ or $a = \pi\delta x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta \in S_{\delta_0 x}$. Notice that, if $\delta x \notin B$ then $\mathbb{D}_\delta \cap \mathrm{supp}\, x = \emptyset$, and so by Remark 1.6(2), $\delta\delta_0 x = \delta_0 x$. Thus $\delta \in S_{\delta_0 x}$.

Theorem 2.4. *Let $Cb\delta_0 x$ be a proper sub Cb-set of Cbx. Then, $Cb\delta_0 x$ is a retract of Cbx if and only if the assignment $\varphi : Cbx \to Cb\delta_0 x$ defined by*

$$\varphi(a) = \begin{cases} \pi\delta\delta_0 x, & \text{if } a = \pi\delta x \in B \\ \pi\delta_0 x, & \text{if } a = \pi x \text{ or } \pi\delta x \notin B \end{cases}$$

is a map retraction, where B is considered as in Remark 2.3.

Proof. To prove the non-trivial part, let $Cb\delta_0 x$ be a retract of Cbx and $\psi : Cbx \to Cb\delta_0 x$ be a retraction. Then, by Lemma 2.1, $\psi(x) = \delta_0 x$. Let $a = a'$. Then, we show $\varphi(a) = \varphi(a')$.

Case (1): Suppose $a = a' \in B$. By Remark 2.3(2), $\pi\delta x = a = a' = \pi'\delta' x$, for some $\pi, \pi' \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta, \delta' \in S'_{\delta_0 x}$. Now, $\psi(a) = \psi(a')$ and so

$$\begin{aligned} \varphi(a) &= \pi\delta\delta_0 x = \pi\delta\psi(x) = \psi(\pi\delta x) = \psi(a) = \psi(a') = \psi(\pi'\delta' x) \\ &= \pi'\delta'\psi(x) = \pi'\delta'\delta_0 x = \varphi(a'). \end{aligned}$$

Case (2): Suppose $a = a' \notin B$. By Remark 2.3(3), $a = \pi x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ or $a = \pi\delta x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta \in S_{\delta_0 x}$. Then, by Remark 1.7(4), we have the following subcases;

Subcase (2a): If $\pi x = a = a' = \pi' x$ then

$$\begin{aligned} \varphi(a) &= \pi\delta_0 x = \pi\psi(x) = \psi(\pi x) = \psi(a) = \psi(a') = \psi(\pi' x) = \pi'\psi(x) \\ &= \pi'\delta_0 x = \varphi(a'). \end{aligned}$$

Subcase (2b): If $\pi\delta x = a = a' = \pi'\delta' x$ then $\delta\delta_0 x = \delta_0 x$ and so

$$\begin{aligned} \varphi(a) &= \pi\delta_0 x = \pi\delta\delta_0 x = \pi\delta\psi(x) = \psi(\pi\delta x) = \psi(a) = \psi(a') = \psi(\pi'\delta' x) \\ &= \pi'\delta'\psi(x) = \pi'\delta'\delta_0 x = \pi'\delta_0 x = \varphi(a'). \end{aligned}$$

Now, we show φ is equivariant and $\varphi\mid_{Cb\delta_0 x} = id\mid_{Cb\delta_0 x}$. Suppose $a \in Cbx$ and $\sigma_1 \in Cb$. We have the following cases:

Case (a): Let $a \in B$. Then, $\sigma_1 a \in B$ and by Remark 2.3(2), $a = \pi\delta x$, where $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta \in S'_{\delta_0 x}$. Now,

$$\sigma_1\varphi(a) = \sigma_1\pi\delta\delta_0 x = \varphi(\sigma_1\pi\delta x) = \varphi(\sigma_1 a).$$

Case (b): Let $a \notin B$. Then, by Remark 2.3(3), $a = \pi x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ or $a = \pi\delta x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta \in S_{\delta_0 x}$ and by Remark 1.7(4), we have the following subcases;

Subcase (b1): Let $a = \pi x$ and $\sigma_1 = \pi_1$. Then,

$$\sigma_1\varphi(a) = \pi_1\varphi(\pi x) = \pi_1\pi\delta_0 x = \varphi(\pi_1\pi x) = \varphi(\pi_1 a) = \varphi(\sigma_1 a).$$

Subcase (b2): Let $a = \pi\delta x$ and $\sigma_1 = \pi_1$. Then,

$$\sigma_1\varphi(a) = \pi_1\varphi(\pi\delta x) = \pi_1\pi\delta_0 x = \varphi(\pi_1\pi\delta x) = \varphi(\pi_1 a) = \varphi(\sigma_1 a).$$

SUBCASE (B3): If $a = \pi x$ and $\sigma_1 = \pi_1\delta_1$ or $a = \pi\delta x$ and $\sigma_1 = \pi_1\delta_1$ then

$$\sigma_1\varphi(a) = \pi_1\delta_1\varphi(a) = \pi_1\delta_1\pi\delta_0 x = \pi_1\pi\delta_1'\delta_0 x.$$

Now, if $\sigma_1 a \in B$ then

$$\sigma_1 a = \pi_1\delta_1\pi x = \pi_1\pi\delta_1' x \text{ or } \sigma_1 a = \pi_1\delta_1\pi\delta x = \pi_1\pi\delta_1'\delta x,$$

and so $\mathbb{D}_{\delta_1'} \cap \operatorname{supp}\delta_0 x \neq \emptyset$. Thus $\varphi(\sigma_1 a) = \pi_1\pi\delta_1'\delta_0 x = \sigma_1\varphi(a)$.

Also, if $\sigma_1 a \notin B$ then

$$\pi_1\delta_1 a = \pi_1\delta_1\pi x = \pi_1\pi\delta_1' x \text{ or } \pi_1\delta_1 a = \pi_1\delta_1\pi\delta x = \pi_1\pi\delta_1'\delta x,$$

and so $\mathbb{D}_{\delta_1'} \cap \operatorname{supp}\delta_0 x = \emptyset$. Thus $\delta_1'\delta_0 x = \delta_0 x$, and so

$$\varphi(\sigma_1 a) = \pi_1\pi\delta_0 x = \pi_1\pi\delta_1'\delta_0 x = \sigma_1\varphi(a).$$

It remains to show $\varphi\mid_{Cb\delta_0 x} = id_{Cb\delta_0 x}$. Let $a \in Cb\delta_0 x$. Then, $a = \pi'\delta'\delta_0 x$, for some $\pi' \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta' \in S'_{\delta_0 x}$ or $a = \pi'\delta_0 x$, for some $\pi' \in \mathrm{Perm_f}(\mathbb{D})$. Now, if $a = \pi'\delta'\delta_0 x$ then $a \in B$ and so $\varphi(a) = \pi'\delta'\delta_0 x = a$. Also, if $a = \pi'\delta_0 x$ then $a \notin B$, and so $\varphi(a) = \pi'\delta_0 x = a$. □

Now, we recall the following definition and theorem from [3].

Definition 2.5. We call a finitely supported Cb-set X, *fix-simple* if its only non-trivial sub Cb-sets are of the form $\bigcup_{i\in I}\{\theta_i\}$, for a set I, and $\theta_i \in \operatorname{Fix} X$.

If X is a fix-simple Cb-set and $\operatorname{Fix} X = \{\theta_1, \ldots, \theta_k\}$, then we simply call X, $\{\theta_1, \ldots, \theta_k\}$-simple. A $\{\theta\}$-simple Cb-set is said to be θ-simple or 0-simple.

Theorem 2.6. *If X is a non-discrete fix-simple finitely supported Cb-set, then X is cyclic and of one of the forms*

$$\mathrm{Perm_f}(\mathbb{D})\, x \cup \{\theta\} \quad \textit{or} \quad \mathrm{Perm_f}(\mathbb{D})\, x \cup \{\theta_1, \theta_2\}$$

where $\theta, \theta_1, \theta_2 \in \operatorname{Fix} X$, and $|\operatorname{Fix} X| \leq 2$.

Recall that simple algebras are the one whose only congruences are Δ and ∇. Now, using the above theorem, we have:

Lemma 2.7. *Let Cbx be a cyclic finitely supported Cb-set. Then, each simple sub Cb-set of Cbx is a retract of Cbx.*

Proof. Let A be a simple sub Cb-set and $\theta \in \operatorname{Fix} Cb\, x$. Then, by Theorem 6.3 of [3], A is θ-simple and so by Theorem 2.6, $A = \mathrm{Perm_f}(\mathbb{D})x' \cup \{\theta\}$, where $x' \in Cbx$. Take $x' = \pi\delta_0 x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta_0 \in S'_x$. Now, applying Theorem 2.4, it is sufficient to show that the assignment φ mentioned there, is a map. Notice

that, if $\pi\delta x \in B$ then $\mathbb{D}_\delta \cap \operatorname{supp}\delta_0 x \neq \emptyset$ and since A is $\operatorname{Perm_f}(\mathbb{D})\, x' \cup \{\theta\}$, we get $\delta\delta_0 x = \theta$. Thus, we have

$$\varphi(a) = \begin{cases} \theta, & \text{if } a \in B \\ \pi\delta_0 x, & \text{if } a = \pi x \text{ or } \pi\delta x \notin B \end{cases}$$

To see that it is well-defined, assume $a = a'$. If $a = a' \in B$, then $\varphi(a) = \theta = \varphi(a')$. Let $a \notin B$. Then, by Remark 2.3(3), $a, a' \in \{\pi x, \pi' x, \pi\delta x, \pi'\delta' x\}$, for some $\pi, \pi' \in \operatorname{Perm_f}(\mathbb{D})$ and $\delta, \delta' \in S_{\delta_0 x}$. So by Remark 1.7(4), we have the following cases:

Case (1): $\pi x = a = a' = \pi' x$.

Case (2): $\pi\delta x = \pi'\delta' x$.

In each case, we must show $\pi\delta_0 x = \pi'\delta_0 x$. To show this, by Theorem 6.4 of [3], it is sufficient to show $\operatorname{supp}\pi\delta_0 x = \operatorname{supp}\pi'\delta_0 x$. Notice that, $\operatorname{supp}\delta_0 x \subseteq \operatorname{supp}\delta x$, for all $\delta \in S_{\delta_0 x}$. This is because, if there exists some $d \in \operatorname{supp}\delta_0 x \setminus \operatorname{supp}\delta x$ then $(0/d)\delta x = \delta x$, and so $\delta x \in B$, which is impossible. We prove case (2). The other case is proved similarly. Suppose $\pi\delta x = \pi'\delta' x$. Let $d' \in \operatorname{supp}\pi\delta x_0$. Then, $\pi^{-1}d' \in \operatorname{supp}\delta_0 x$, and so

$$\pi(0/\pi^{-1}d')\delta x = (0/d')\pi\delta x = (0/d')\pi'\delta' x = \pi'(0/\pi'^{-1}d')\delta' x.$$

Now, since $\pi^{-1}d' \in \operatorname{supp}\delta_0 x$, we get $(0/\pi^{-1}d')\delta x \in B$, and so $(0/\pi'^{-1}d')\delta' x \in B$. Therefore, $\pi'^{-1}d' \in \operatorname{supp}\delta_0 x$. Similarly $\operatorname{supp}\pi'\delta_0 x \subseteq \operatorname{supp}\pi\delta_0 x$, and so the result holds. □

Remark 2.8. Let $Cb\, x_0$ be a non-discrete fix-simple sub Cb-set of $Cb\, x$ with two zero elements $\theta_1, \theta_2 \in \operatorname{Fix} Cbx_0$. Then, by Theorem 2.6,

$$Cb\, x_0 = \operatorname{Perm_f}(\mathbb{D})\delta_0 x \cup \{\theta_1, \theta_2\}.$$

Take $\operatorname{supp}\delta_0 x = \{d\}$, $(0/d)\delta_0 x = \theta_1$, and $(1/d)\delta_0 x = \theta_2$. Then,

(1) the sets

$$B_0 = \{\pi\delta x \mid \delta(d) = 0, \delta \in S'_x, \pi \in \operatorname{Perm_f}(\mathbb{D})\}$$

and

$$B_1 = \{\pi\delta x \mid \delta(d) = 1, \delta \in S'_x, \pi \in \operatorname{Perm_f}(\mathbb{D})\}$$

are non-empty sub Cb-sets of $Cb\, x$.

(2) $\delta x \in B_0 \cup B_1$ if and only if $d \in \mathbb{D}_\delta$ if and only if $\mathbb{D}_\delta \cap \operatorname{supp}\delta_0 x \neq \emptyset$.

(3) If $\delta x \in \operatorname{Fix} Cb\, x$ then $\delta x \in B_0 \cup B_1$. This is because, $\operatorname{supp}\delta x = \emptyset$ and so $d \notin \operatorname{supp}\delta x$. Thus $(b/d)\delta x = \delta x$. Now, since $(b/d)\delta x \in B_0 \cup B_1$, we get $\delta x \in B_0 \cup B_1$.

(4) Let $a \notin B_0 \cup B_1$. Then, $a = \pi\delta x$, for some $\delta \in S_{\delta_0 x}$ and $\pi \in \operatorname{Perm_f}(\mathbb{D})$ or $a = \pi x$, for some $\pi \in \operatorname{Perm_f}(\mathbb{D})$.

Theorem 2.9. *Let $Cb\,x_0 = \mathrm{Perm_f}(\mathbb{D})\delta_0 x \cup \{\theta_1, \theta_2\}$ be a non-discrete fix-simple sub Cb-set of $Cb\,x$ with two zero elements $\theta_1, \theta_2 \in \mathrm{Fix}\,Cbx_0$, and $\mathrm{supp}\,\delta_0 x = \{d\}$, $(0/d)\delta_0 x = \theta_1$, $(1/d)\delta_0 x = \theta_2$. Then,*

$Cb\delta_0 x$ is a retract of Cbx if and only if for all $\delta \in Cb$, $\delta x \in \mathrm{Fix}\,Cbx$ implies $d \in \mathbb{D}_\delta$.

Proof. Let $\varphi : Cbx \to Cb\delta_0 x$ be a retraction. Then, by Lemma 2.1, $\varphi(\sigma x) = \sigma\delta_0 x$, for $\sigma \in Cb$. Suppose $\delta x \in \mathrm{Fix}\,Cbx$. We show $d \in \mathbb{D}_\delta$. On the contrary, if $d \notin \mathbb{D}_\delta$ then $\mathbb{D}_\delta \cap \mathrm{supp}\,\delta_0 x = \emptyset$, and so by Remark 1.6(2), $\delta\delta_0 x = \delta_0 x$. Also, notice that since $\delta x \in \mathrm{Fix}\,Cbx$, we get $\mathrm{supp}\,\delta x = \emptyset$, and so $d \notin \mathrm{supp}\,\delta x$. Thus $\delta x = (0/d)\delta x = (1/d)\delta x \in B$. Now,

$$\begin{aligned}\theta_1 &= (0/d)\delta_0 x = (0/d)\delta\delta_0 x = \varphi((0/d)\delta x) = \varphi(\delta x) = \varphi((1/d)\delta x)\\ &= (1/d)\delta\delta_0 x = (1/d)\delta_0 x = \theta_2,\end{aligned}$$

which is impossible.

To prove the converse, we show that the assignment φ mentiones in Theorem 2.4, is a map. Notice that, if $a \notin B_0 \cup B_1$, then by Remark 2.8(4), $a = \pi x$ or $a = \pi\delta x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta \in S_{\delta_0 x}$. Thus, we have

$$\varphi(a) = \begin{cases} \theta_1, & \text{if } a \in B_0 \\ \theta_2, & \text{if } a \in B_1 \\ \pi\delta_0 x, & \text{if } a \notin B_0 \cup B_1 \end{cases}$$

To show that φ is well-defined, let $a = a'$. Then, $\mathrm{supp}\,a = \emptyset$ or $\mathrm{supp}\,a \neq \emptyset$. If $\mathrm{supp}\,a = \emptyset$ then by Remark 2.8, $a \in B_0 \cup B_1$, and so $a = \pi'\delta' x$, for some $\pi' \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta' \in S_{\delta_0 x}$. Now, by the assumption, $d \in \mathbb{D}_{\delta'}$. Thus, if $\delta'(d) = 0$ then $a' = a \in B_0$, and so $\varphi(a) = \varphi(a') = \theta_1$. Also, if $\delta'(d) = 1$ then $a' = a \in B_1$, and so $\varphi(a) = \varphi(a') = \theta_2$.

In the case that $\mathrm{supp}\,a \neq \emptyset$ and $a = a' \in B_0 \cup B_1$, it is clear that the result holds.

Let $a \notin B_0 \cup B_1$. Then, by Remark 2.8, $a, a' \in \{\pi x, \pi' x, \pi\delta x, \pi'\delta' x\}$, for some $\pi, \pi' \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta, \delta' \in S_{\delta_0 x}$. So by Remark 1.7(4), we have two following cases:

Case (1): $\pi x = a = a' = \pi' x$;

Case (2): $\pi\delta x = \pi'\delta' x$.

In each case, we must show $\pi\delta_0 x = \pi'\delta_0 x$. To show this, it is sufficient to prove that $\mathrm{supp}\,\pi\delta_0 x = \mathrm{supp}\,\pi'\delta_0 x$. Notice that, $\mathrm{supp}\,\delta_0 x \subseteq \mathrm{supp}\,\delta x$, for all $\delta \in S_{\delta_0 x}$. This is because, if $d \notin \mathrm{supp}\,\delta x$ then $(0/d)\delta x = \delta x$ and so $\delta x \in B_0 \cup B_1$, which is impossible. We prove case (2). The other case is proved similarly. Suppose $\pi\delta x = \pi'\delta' x$. Let $d' \in \mathrm{supp}\,\pi\delta x_0$. Then, $\pi^{-1}d' \in \mathrm{supp}\,\delta_0 x$, and so

$$\pi(0/\pi^{-1}d')\delta x = \pi'(0/\pi'^{-1}d')\delta' x.$$

Now, since $\pi^{-1}d' \in \mathrm{supp}\,\delta_0 x$, we have $(0/\pi^{-1}d')\delta x \in B_0 \cup B_1$, and so $(0/\pi'^{-1}d')\delta' x \in B_0 \cup B_1$. Therefore, $\pi'^{-1}d' \in \mathrm{supp}\,\delta_0 x$. Similarly $\mathrm{supp}\,\pi'\delta_0 x \subseteq \mathrm{supp}\,\pi\delta_0 x$, and the proof is complete. □

Theorem 2.10. *Let $Cb\delta_0x$ be a non-zero and proper sub Cb-set of Cbx. Also, let the following conditions hold:*

(i) *if $d \in \operatorname{supp}\delta_0x$ then $(b/d)x \in Cb\delta_0x$,*

(ii) *if $\operatorname{Perm_f}(\mathbb{D})(b_1/d_1)\delta_0x \cap \operatorname{Perm_f}(\mathbb{D})(b_2/d_2)\delta_0x \neq \emptyset$, then $d_1 = d_2$.*

Then, $Cb\delta_0x$ is a retract of Cbx if and only if for all $\delta x \in Cb\delta_0x$ we have $\delta x = \delta\delta_0x$.

Proof. If $Cb\delta_0x$ is a retract of Cbx then applying Corollary 2.2, for all $\delta x \in Cb\delta_0x$ we have $\delta x = \delta\delta_0x$. To prove the converse, let $\delta x = \delta\delta_0x$, for all $\delta x \in Cb\delta_0x$. Then to get the result, using Theorem 2.4, we show that φ is a map. First, we prove

$$a \in B \Rightarrow a \in Cb\delta_0x \quad (*).$$

Since $a \in B$, $a = \pi\delta x$, for some $\pi \in \operatorname{Perm_f}(\mathbb{D})$ and $\delta \in S'_{\delta_0x}$. So $\mathbb{D}_\delta \cap \operatorname{supp}\delta_0x \neq \emptyset$. Thus there exists some $d \in \mathbb{D}$ with $d \in \mathbb{D}_\delta \cap \operatorname{supp}\delta_0x$, and so by (i), $\delta x \in Cb\delta_0x$.

Let $a = a' \in B$. Then, $\pi\delta x = a = a' = \pi'\delta' x$, for some $\pi, \pi' \in \operatorname{Perm_f}(\mathbb{D})$ and $\delta, \delta' \in S'_{\delta_0x}$. So by $(*)$, $a, a' \in Cb\delta_0x$. Thus $a = \pi_1\delta_1\delta_0x$ and $a' = \pi_2\delta_2\delta_0x$, for some $\pi_1, \pi_2 \in \operatorname{Perm_f}(\mathbb{D})$ and $\delta_1, \delta_2 \in S'_{\delta_0x}$. Now,

$$\begin{aligned}\varphi(a) &= \varphi(\pi\delta x) = \varphi(\pi_1\delta_1\delta_0x) = \pi_1\delta_1\delta_0\delta_0x = \pi_1\delta_1\delta_0x = a = a' = \pi_2\delta_2\delta_0x\\ &= \pi_2\delta_2\delta_0\delta_0x = \varphi(\pi_2\delta_2\delta_0x) = \varphi(a').\end{aligned}$$

Let $a = a' \notin B$. Then, we have the following cases:

Case (1): $\pi x = a = a' = \pi' x$.

Case (2): $\pi\delta x = a = a' = \pi'\delta' x$, for some $\pi, \pi' \in \operatorname{Perm_f}(\mathbb{D})$ and $\delta, \delta' \in S'_x$.

In each case, we show $\pi\delta_0x = \pi'\delta_0x$. We prove case (1). The other case is proved similarly. Let $d \in \operatorname{supp}\delta_0x$. Then $(b/\pi d)\pi x = (b/\pi d)\pi' x$. So $\pi(b/d)x = \pi'(b/\pi'^{-1}\pi d)x$. Since $d \in \operatorname{supp}\delta_0x$, by (i), we get $(b/d)x \in Cb\delta_0x$. So $(b/\pi'^{-1}\pi d)x \in Cb\delta_0x$, and we have

$$\begin{aligned}\pi(b/d)\delta_0x &= \pi(b/d)x \quad \text{(by the assumption)}\\ &= \pi'(b/\pi'^{-1}\pi d)x\\ &= \pi'(b/\pi'^{-1}\pi d)\delta_0x \quad \text{(by the assumption)}.\end{aligned}$$

Now, if $\pi'^{-1}\pi d \notin \operatorname{supp}\delta_0x$ then $\pi(b/d)\delta_0x = \pi'\delta_0x$, which is impossible, since in this case, by Lemma 3.4 of [3], $|\operatorname{supp}(b/d)\delta_0x| < |\operatorname{supp}\delta_0x|$. Therefore $\pi'^{-1}\pi d \in \operatorname{supp}\delta_0x$, and so by (ii), $\pi'^{-1}\pi d = d$. Thus for all $d \in \operatorname{supp}\delta_0x$, we have $\pi'^{-1}\pi d = d$ which implies that $\pi'^{-1}\pi\delta_0x = \delta_0x$. □

Theorem 2.11. *Let Cbx be a cyclic finitely supported Cb-set and $Cb\delta_0x$ be a proper sub Cb-set such that for all $z, z' \in \operatorname{Cb}\delta_0x$, $\operatorname{supp} z = \operatorname{supp} z'$ implies $z = z'$. Also, suppose for all $\delta, \delta' \in S'_x$ with $\operatorname{Perm_f}(\mathbb{D})\delta x \cap \operatorname{Perm_f}(\mathbb{D})\delta' x \neq \emptyset$ we have $|\mathbb{D}_\delta \cap \operatorname{supp}\delta_0x| = |\mathbb{D}_{\delta'} \cap \operatorname{supp}\delta_0x|$. Then, there exists a retraction from Cbx to $Cb\delta_0x$.*

Proof. Applying Theorem 2.4, we show that φ is a map. If $a = a' \notin B$ then by Remark 2.8, we have the following cases:

Case (1) $\pi x = a = a' = \pi' x$.

Case (2) $\pi\delta x = a = a' = \pi'\delta' x$, for some $\pi, \pi' \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta, \delta' \in S'_x$.

In each case, we must show $\pi\delta_0 x = \pi'\delta_0 x$. By the assumption, it is sufficient to show that $\operatorname{supp}\pi\delta_0 x = \operatorname{supp}\pi'\delta_0 x$. We prove case (1). The other case is proved similarly. Let $d \in \operatorname{supp}\pi\delta_0 x$. Then $(b/d)\pi x = (b/d)\pi' x$. So $\pi(b/\pi^{-1}d)x = \pi'(b/\pi'^{-1}d)x$. Since $\pi^{-1}d \in \operatorname{supp}\delta_0 x$, by the assumption, $\pi'^{-1}d \in \operatorname{supp}\delta_0 x$, and so $d \in \operatorname{spp}\pi'\delta_0 x$. Similarly, $\operatorname{supp}\pi'\delta_0 x \subseteq \operatorname{supp}\pi\delta_0 x$. Thus $\operatorname{supp}\pi\delta_0 x = \operatorname{supp}\pi'\delta_0 x$, and so by the assumption, $\pi\delta_0 x = \pi'\delta_0 x$.

Now, suppose $a = a' \in B$. Then, $a = \pi\delta x$ and $a' = \pi'\delta' x$, for some $\pi, \pi' \in \mathrm{Perm_f}(\mathbb{D})$ and $\delta, \delta' \in S'_{\delta_0 x}$. We show that $\operatorname{supp}\pi\delta\delta_0 x = \operatorname{supp}\pi'\delta'\delta_0 x$, and so by the assumption, $\pi\delta\delta_0 x = \pi'\delta'\delta_0 x$. First, notice that $\operatorname{supp}\delta\delta_0 x \subseteq \operatorname{supp}\delta x$. To show this, suppose $d \in \operatorname{supp}\delta\delta_{\circ} x$. So $d \in \operatorname{supp}\delta_{\circ} x$. If $d \notin \operatorname{supp}\delta x$, then $(b/d)\delta x = \delta x$, which is impossible. Let $d \in \operatorname{supp}\pi\delta\delta_0 x$. Then, $d \in \operatorname{supp}\pi\delta x$. Now, $\pi(0/\pi^{-1}d)\delta x = (0/d)\pi\delta x = (0/d)\pi'\delta' x = \pi'(0/\pi'^{-1}d)\delta' x$. Thus by the assumption, $\pi'^{-1}d \in \operatorname{supp}\delta_0 x$. Now, if $d \notin \operatorname{supp}\pi'\delta'\delta_0 x$ then $\pi'(0/\pi'^{-1}d)\delta'\delta_0 x = (0/d)\pi'\delta'\delta_0 x = \pi'\delta'\delta_0 x$, which is a contradiction. □

Theorem 2.12. *Let Z be a finitely supported Cb-set, and $Y = Cb\,x \cup Z$, where $Cb\,x \cap Z = \emptyset$ or $Cb\,x \cap Z = \{\theta\}$ for $\theta \in \operatorname{Fix} Cb\,x \cap \operatorname{Fix} Z$. Then, there exists a retraction from Y to $Cb\,x$.*

Proof. Let $i : Cb\,x \hookrightarrow Y$ be the inclusion map and $\theta \in Cb\,x$, which exists by Remark 1.6(7). Then, $g : Y \to Cb\,x$ which is defined by

$$g(z) = \begin{cases} z & \text{if} \quad z \in Cb\,x \\ \theta & \text{if} \quad z \in Z \end{cases}$$

is a retraction. □

Here, to have a better scenery, we summarize the results of this section. In Lemma 2.1, assuming the existence of a retraction from Cbx to a sub Cb-set, we found some necessary conditions to have a retraction. We gave a characterization of retracts of cyclic finitely supported Cb-sets in Theorem 2.4. In Lemma 2.7, we showed that all simple sub Cb-sets of a cyclic finitely supported Cb-sets are retracts. Further, in Theorem 2.9, a sufficient and necessary condition for a fix-simple finitely supported Cb-set with two zero elements is stated to make it into a retract of a cyclic Cb-set.

3. Retractable finitely supported Cb-sets

In this section, we consider retractable cyclic finitely supported Cb-set.

Definition 3.1. A finitely supported Cb-set X is called *retractable* if for every non-empty sub Cb-set Y of X, there exists a retraction from X to Y.

Example 3.2. (1) Discrete Cb-sets are retractable. The converse is not correct.
(2) Each fix-simple Cb-set with a unique zero is retractable.

Remark 3.3. Every sub Cb-set of a retractable Cb-set is retractable.

Lemma 3.4. *A retractable cyclic finitely supported Cb-set has a unique zero.*

Proof. Take $X = Cb\,x$, for some $x \in X$. If $\operatorname{supp} x = \emptyset$ then X is a singleton, and so the result holds. Suppose $\operatorname{supp} x \neq \emptyset$. By Remark 1.6(7), X has a zero element. We show X has a uniuqe zero element. On the contrary, suppose $\theta_1 \neq \theta_2 \in \operatorname{Fix} X$. Since X is retractable, there exists an equivariant map $f : X \to \{\theta_1, \theta_2\}$ with $fi = id$, where $i : \{\theta_1, \theta_2\} \hookrightarrow X$ is an inclusion arrow. Now, $f(x) \in \{\theta_1, \theta_2\}$. If $f(x) = \theta_1$ then $f(Cb\,x) \subseteq \{\theta_1\}$. In particular, $\theta_2 = f(\theta_2) = \theta_1$, which is impossible. Similarly, $f(x) = \theta_2$ is impossible. Thus X has a unique zero element. □

Lemma 3.5. *Every non-trivial cyclic sub Cb-set of a non-discrete retractable Cb-set X has a unique infinite θ-simple sub Cb-set.*

Proof. Let $Cb\,x$ be a non-trivial sub Cb-set of X. Then, by Remark 3.3, $Cb\,x$ is retractable, and so by Lemma 3.4, $Cb\,x$ has a unique zero θ. Also, by Lemma 7.6 of [3], $Cb\,x$ has a θ-simple sub Cb-set, say B. Now, if B, B' are two θ-simple sub Cb-sets of $Cb\,x$ then $B \cap B' = \{\theta\}$ or $B = B'$. Suppose $B \cap B' = \{\theta\}$. Since Cbx is retractable, there exists a retraction $f : Cb\,x \to B \cup B'$, which is impossible, because $f(x) \in B$ or $f(x) \in B'$, and so $f(Cb\,x) \subseteq B$ or $f(Cb\,x) \subseteq B'$. Now, since f is a retraction, we get $f(B \cup B') = B \cup B'$, and so $B \cup B' \subseteq B$. Thus $B' \subseteq B$, which is impossible. □

Theorem 3.6. *Let $Cb\,x = \operatorname{Perm_f}(\mathbb{D})x \cup A$, where $A = \operatorname{Perm_f}(\mathbb{D})\delta_0 x \cup \{\theta\}$ is a simple sub Cb-set of X, $\operatorname{Fix} Cb\,x = \{\theta\}$ and $\delta_0 \in S'_x$. Then,*

(i) *the non-empty sub Cb-sets of Cbx are $\{\theta\}$, A, and $Cb\,x$;*

(ii) *Cbx is retractable;*

(iii) *$(b/d)x = \theta$, for all $d \in \operatorname{supp} \delta_0 x$.*

Proof. (i) Let C be a non-empty non-trivial proper sub Cb-set of $Cb\,x$. Then $x \notin C$, and so $C \subseteq A$. Now, since $\delta_0 x \in C$, $A \subseteq C$, and so $C = A$.

(ii) It is sufficient to show that A is a retract of $Cb\,x$. Applying Theorem 2.4, we show that $\varphi : Cb\,x \to A$ is a map. First, we show $\varphi = \psi$, where

$$\psi(a) = \begin{cases} a, & \text{if } a \in Cb\delta_0 x \\ \pi\delta_0 x, & \text{if } a \notin Cb\delta_0 x \end{cases}$$

Let $a \in A$. Then, $a = \theta = (0/d)\delta_0 x$, where $d \in \operatorname{supp} \delta_0 x$ or $a = \pi\delta_0 x$, for some $\pi \in \operatorname{Perm_f}(\mathbb{D})$. If $a = \theta = (0/d)\delta_0 x$ then $\theta \in B$, and so $\varphi(\theta) = \theta = \psi(\theta)$. Also, if $a = \pi\delta_0 x$ then $a \notin B$, and so

$$\varphi(\pi\delta_0 x) = \pi\delta_0 x = \psi(\pi\delta_0 x).$$

Let $a \notin A$. Then, $a = \pi x$, for some $\pi \in \mathrm{Perm_f}(\mathbb{D})$, and so $a \notin B$. Thus $\varphi(a) = \pi\delta_0 x = \psi(a)$.

Now, we show that ψ is well-defined. Let $a = a' \notin A = Cb\delta_0 x$. Then $\pi x = a = a' = \pi' x$, for some $\pi, \pi' \in \mathrm{Perm_f}(\mathbb{D})$. Take $\pi'^{-1}\pi = \pi_1$. We must show that $\pi_1\delta_0 x = \delta_0 x$. First, notice that, since A is simple, it is sufficient to show that $\operatorname{supp}\pi_1\delta_0 x = \operatorname{supp}\delta_0 x$. To prove this, let $d \in \operatorname{supp}\pi_1\delta_0 x$, then $d \in \operatorname{supp}\pi_1 x$, and so $(0/d)x = (0/d)\pi_1 x = \pi_1(0/\pi_1^{-1}d)x$. Now, since $\pi_1^{-1}d \in \operatorname{supp}\delta_0 x$, $(0/\pi^{-1}d)x \in B$, and so $(0/d)x \in B$. Thus $d \in \operatorname{supp}\delta_0 x$. Similarly, $\operatorname{supp}\delta_0 x \subseteq \operatorname{supp}\pi_1\delta_0 x$, and so $\operatorname{supp}\pi_1\delta_0 x = \operatorname{supp}\delta_0 x$.

Now, since ψ is a map, we get that φ is a retraction.

(iii) Let $d \in \operatorname{supp}\delta_0 x$. Then, $Cb(b/d)\,x$ is a proper sub Cb-set of $Cb\,x$, for $b \in 2$. Since otherwise, if $Cb\,x = Cb(b/d)x$ then $x = \sigma(b/d)x$, and so by Remark 2.4(4) of [3], $|\operatorname{supp} x| = |\operatorname{supp}\sigma(b/d)x| \leq |\operatorname{supp}(b/d)x| < |\operatorname{supp}(b/d)x|$, which is impossible. Therefore, $Cb(b/d)x = A$ or $Cb(b/d)x = \{\theta\}$, and so $(b/d)x \in A$. Since Cbx is retractable, there exists a retraction $\varphi : Cbx \to A$. Applying Lemma 2.1(ii), $\varphi(x) = \delta_0 x$, $(b/d)x = \varphi((b/d)x) = (b/d)\delta_0 x = \theta$. □

References

[1] **M. Bojanczyk, B. Klin and S. Lasota**, *Automata theory in nominal sets*, Log. Methods Comput. Sci. **10(3)** (2014), 1 – 44.

[2] **M.M. Ebrahimi and M. Mahmoudi**, *The category of M-sets*, Ital. J. Pure Appl. Math. **9** (2001), 123 – 132.

[3] **M.M. Ebrahimi, Kh. Keshvardoost and M. Mahmoudi**, *Simple and subdirectly irreducible finitely supported Cb-sets*, Theoret. Comput. Sci. **706** (2018), 1 – 21.

[4] **M. Gabbay and A. Mathijssen**, *One-and-a-halfth-order logic*, J. Logic Comput. **18** (2008), 521 – 562.

[5] **M. Gabbay and A. Pitts**, *A new approach to abstract syntax with variable binding*, Form. Asp. Comput. **13(3-5)** (2002), 341 – 363.

[6] **M. Kilp, U. Knauer and A. Mikhalev**, *Monoids, Acts and Categories*, Walter de Gruyter, Berlin, New York, 2000.

[7] **M. Main, A. Melton, M. Mislove and D. Schmidt**, *Mathematical foundations of programming language semantics*, Lect. Notes Comp. Sci. **298** (1988).

[8] **A. Pitts**, *Nominal logic, a first order theory of names and binding*, Inform. and Comput. **186** (2003), 165 – 193.

[9] **A. Pitts**, *Nominal Sets, Names and Symmetry in Computer Science*, Cambridge University Press, 2013.

[10] **A. Pitts**, *Nominal presentations of the cubical sets model of type theory*, LIPIcs. Leibniz Int. Proc. Inform. (2015), 202 – 220.

Received August 14, 2017

Department of Mathematics, Shahid Beheshti University, G.C., Tehran 19839, Iran
E-mails: m-ebrahimi@sbu.ac.ir, kh_keshvardoost@sbu.ac.ir, m-mahmoudi@sbu.ac.ir

Quasigroups and Related Systems **26** (2018), 67 – 76

The Cayley graph of commutative ring on triangular subsets

Kazem Hamidizadeh and Gholamreza Aghababaei

Abstract. Let R be a commutative ring with nonzero identity, and T be a triangular subset of R^n. We investigate the structure of the Cayley graph $TCay(R^n, T^*)$, where $T^* = T \setminus \{0\}$ is the triangular subset of R^n.

1. Introduction

The investigation of algebraic structures of graphs is a very large and growing area of research. In particular, Cayley graphs and their generalizations have been a main topic in algebraic graph theory (see [1], [2], [3], [4]). Several other classes of graphs associated with algebraic structures, such as power graph, total graph and zero divisor graph, have been investigated in [5] and [6].

Let R be a commutative ring with nonzero identity, $L_n(R)$ be the set of all lower triangular $n \times n$ matrices, and U be a subset of R^n, where n is a positive integer. We say that U is a *triangular subset* of R^n if the following condition holds:

$$\text{for all } (u_1, \ldots, u_n) \in U, \ \ A \in L_n(R) \text{ and } (w_1, \ldots, w_n) \in R^n,$$

$$\text{if } A[(u_1, \ldots, u_n)]^T = [w_1, \ldots, w_n]^T, \text{ then } (w_1, \ldots, w_n) \in U.$$

If T be a triangular subset of R^n, then for every $(x_1, \ldots, x_n) \in T$, we have $Rx_1 \times \ldots \times Rx_n \subseteq T$. Hence $T = \bigcup_{i \in \Omega} \sqcap_{j=1}^{n} I_{ij}$, where $I_{i1} \subseteq \ldots \subseteq I_{in}$, for every $i \in \Omega$.

Let R be an arbitary commutative ring and T be a triangular subset of R^n. In this paper, we study the Cayley graph $TCay(R^n, T^*)$, which is an undirected graph with vertex set R^n, and two distinct vertices $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ are adjacent if and only if $(x_1 - y_1, \ldots, x_n - y_n) \in T^*$. For simplicity our notations, we denote the graph $TCay(R^n, T^*)$ by $TCay(R^n)$. We study the structure of $TCay(R^n)$, in the cases that T is closed under addition and T is not closed under addition. In sections 2 and 3, we investigate the diameter and the girth of the $TCay(R^n)$, where the proofs of the results in these two sections are similar to that in [7]. In section 4, we investigate the planarity of graph $TCay(R^n)$.

Now, we recall some definitions and notations on graphs. We use the standard terminology of graphs in [9]. Let G be a simple graph. We say that G is *connected* if

2010 Mathematics Subject Classification: 05C10, 13A15.
Keywords: Cayley graph, commutative ring, triangular subset.

there is a path between any two distinct vertices of G, otherwise G is *disconnected*. Also, we say that G is *totally disconnected* if no two vertices of G are adjacent. For vertices x and y of G, we use the notation $x \sim y$ to denote that x and y are adjacent. Also, the length of a shortest path from x to y is denoted by $d(x, y)$ if a path from x to y exists. Also we define $d(x, y) = 0$, and $d(x, y) = \infty$ if there is no path between x and y. The *diameter* of G is $diam(G) = sup\{d(x, y) : x, y \in V(G)\}$. The *girth* of G, denoted by $gr(G)$, is length of a smallest cycle in G (if G contains no cycles, then $gr(G) = \infty$). A graph G is said to be *complete bipartite* if the vertices of G can be partitioned into two disjoint sets V_1, V_2 such that no two vertices in any V_1 or V_2 are adjacent, but for every $u \in V_1, v \in V_2$, the vertices u and v are adjacent. Then we use the symbol $K_{m,n}$ for the complete bipartite graph where the cardinal numbers of V_1 and V_2 are m, n, respectively. A graph with n vertices in which each pair of distinct vertices is joined by an edge is called a *complete graph*, and it is denoted by K_n. A graph G is said to be *planar* if it can be drawn in the plane so that its edges intersect only at their ends. A *subdivision* of a graph is any graph that can be obtained from the original graph by replacing edges by paths.

We investigate this graph in case that $n \geqslant 2$. First, assume that T is closed under addition.

2. The case that T is closed under addition

The proofs of the following theorems are similar to that in [7], and hence we omit the proofs.

Theorem 2.1. *Let R be a commutative ring and T be a triangular subst of R^n. Then $TCay(T)$ is disjoint from $TCay(R^n \setminus T)$.*

Proof. This is clear according to the definitions. □

Theorem 2.2. *Let R be a commutative ring, T be a triangular subset of R^n, which is closed under addition, $|T| = \alpha$ and $|R^n/T| = \beta$. Then $TCay(T)$ is a complete graph K_α and $TCay(R^n \setminus T)$ is the union of $\beta - 1$ disjoint K_α.*

Theorem 2.3. *Let R be a commutative ring, T be a triangular subset of R^n that closed under addition, then the following statements hold.*

(1) *$TCay(R^n \setminus T)$ is complete if and only if $R^n/T \cong \mathbb{Z}_2$.*

(2) *$TCay(R^n \setminus T)$ is connected if and only if $R_n/T \cong \mathbb{Z}_2$.*

The following corollary follows from Theorems 2.1 and 2.2.

Corollary 2.4. *Let R be a commutative ring, T be a triangular subset of R^n that closed under addition, then the following statements hold.*

(1) *$diam(TCay(R^n \setminus T)) = 1$ if and only if $R^n/T \cong \mathbb{Z}_2$ and $| T | \geqslant 2$. Otherwise $diam(TCay(R^n \setminus T)) = \infty$.*

(2) $gr(TCay(R^n \setminus T)) = 3$ *if and only if* $|T| \geqslant 3$. *Otherwise* $gr(TCay(R^n \setminus T)) = \infty$.

(3) $gr(TCay(T)) = 3$ *if and only if* $|T| \geqslant 3$. *Otherwise* $gr(TCay(T)) = \infty$.

(4) $diam(TCay(R)) = \infty$, *and* $gr(TCay(R)) = 3$ *if and only if* $|T| \geqslant 3$, *otherwise* $gr(TCay(R)) = \infty$.

3. The case that T is closed under addition

The following results and their proofs are analogous to some of the results in [7].

Theorem 3.1. *Let R be a commutative ring and T be a triangular subset of R^n which is not closed under addition. Then the following statements hold.*

(1) $TCay(T)$ *is connected and* $diam TCay(T) = 2$.

(2) *The graphs* $TCay(T)$ *and* $TCay(R^n \setminus T)$ *are not disjoint.*

(3) *If* $TCay(R^n \setminus T)$ *is connected, then so is* $TCay(R^n)$.

Proof. (1). Let $(x_1, \ldots, x_n) \in T$. Then $(x_1, \ldots, x_n)$ is adjacent to $(0, \ldots, 0)$. Thus $(x_1, \ldots, x_n) \sim (0, \ldots, 0) \sim (y_1, \ldots, y_n)$ is a path in $TCay(T)$ of length two between any two distinct vertices $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in T^*$. Moreover there are nonzero distinct vertices $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in T$ that are not adjacent, because U is not closed under addition. Therefore $diam TCay(T) = 2$.

(2). Since U is not closed under addition, there are nonzero distinct vertices $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in T$ such that $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) \in R^n \setminus T$. We have $(x_1, \ldots, x_n) \in T$ is adjacent to $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) \in R^n \setminus T$ because

$$((x_1, \ldots, x_n) + (y_1, \ldots, y_n)) - (y_1, \ldots, y_n) = (x_1, \ldots, x_n) \in T.$$

(3). This follows from (1) and (2). □

Theorem 3.2. *Let R be a commutative ring and T be a triangular subset of R^n that is not closed under addition. Then $TCay(R)$ is connected if and only if $\langle T \rangle = R^n$.*

Proof. Suppose that $TCay(R^n)$ is connected. Hence there is a path

$$(0, \ldots, 0) \sim (x_{1,1}, \ldots, x_{1,n}) \sim \cdots \sim (x_{k,1}, \ldots, x_{k,n}) \sim (1, \ldots, 1)$$

from $(0, \ldots, 0)$ to $(1, \ldots, 1)$ in $TCay(R^n)$. Now clearly we have

$$(x_{1,1}, \ldots, x_{1,n}), (x_{2,1} - x_{1,1}, \ldots, x_{2,n} - x_{1,n}), \ldots, (1 - x_{k,1}, \ldots, 1 - x_{k,n}) \in T.$$

Hence $(1, \ldots, 1)$ belongs to the set

$$\langle (x_{1,1}, \ldots, x_{1,n}), (x_{2,1} - x_{1,1}, \ldots, x_{2,n} + x_{1,n}), \ldots, (1 - x_{k,1}, \ldots, 1 - x_{k,n}) \rangle \subseteq \langle T \rangle.$$

Conversly, suppose that $\langle T\rangle = R^n$. We show that for each $(x_1, \ldots, x_n) \in T$, there exists a path in $TCay(R^n)$ from $(0, \ldots, 0)$ to $(x_1, \ldots, x_n)$. By assumption, there are elements $(x_{1,1}, \ldots, x_{1,n}), (x_{2,1}, \ldots, x_{2,n}), \ldots, (x_{k,1}, \ldots, x_{k,n}) \in T$ such that

$$(x_1, \ldots, x_n) = (x_{1,1}, \ldots, x_{1,n}) + \cdots + (x_{k,1}, \ldots, x_{k,n}).$$

Let $c_0 = (0, \ldots, 0)$ and $c_l = (x_{1,1}, \ldots, x_{1,n}) + \cdots + (x_{l,1}, \ldots, x_{l,n}))$ for every integer l with $1 \leqslant l \leqslant k$. Thus $c_l - c_{l-1} = (x_{l,1}, \ldots, x_{l,n})$ for each integer l with $1 \leqslant l \leqslant k$ and thus

$$(0, \ldots, 0) = c_0 \sim c_1 \sim \cdots \sim c_k = (x_1, \ldots, x_n)$$

is a path from $(0, \ldots, 0)$ to $(x_1, \ldots, x_n)$ in $TCay(R^n)$ of length at most k. Now, let $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ be in R^n. Then, by the preceding argument, there are paths from $(x_1, \ldots, x_n)$ to $(0, \ldots, 0)$ and $(0, \ldots, 0)$ to $(y_1, \ldots, y_n)$ in $TCay(R^n)$. Hence there is a path from $(x_1, \ldots, x_n)$ to $(y_1, \ldots, y_n)$ in $TCay(R^n)$. Therefore $TCay(R^n)$ is connected. □

Theorem 3.3. *Let R be a commutative ring, T be a triangular subset of R^n which is not closed under addition such that $\langle T\rangle = R^n$. Let $k \geqslant 2$ be the least integer that $R = \langle (x_{1,1}, \ldots, x_{1,n}), \ldots, (x_{k,1}, \ldots, x_{k,n})\rangle$, for some distinct elements $(x_{1,1}, \ldots, x_{1,n}), \ldots, (x_{k,1}, \ldots, x_{k,n}) \in U$. Then $diam(TCay(R^n)) = k$.*

Proof. First, we show that any path from $(0, \ldots, 0)$ to $(1, \ldots, 1)$ has length at least l. Suppose that

$$(0, \ldots, 0) \sim (y_{1,1}, \ldots, y_{1,n}) \sim \cdots \sim (y_{l-1,1}, \ldots, y_{l-1,n}) \sim (1, \ldots, 1)$$

is a path from $(0, \ldots, 0)$ to $(1, \ldots, 1)$ in $TCay(R^n)$ of length l. Thus

$$(y_{1,1}, \ldots, y_{1,n}), (y_{2,1} - y_{1,1}, \ldots, y_{2,n} - y_{1,n}), (1 - y_{l-1,1}, \ldots, 1 - y_{l-1,n}) \in T.$$

Therefore $(1, \ldots, 1)$ belongs to

$$\langle (y_{1,1}, \ldots, y_{1,n}), (y_{2,1} - y_{1,1}, \ldots, y_{2,n} - y_{1,n}), (1 - y_{l-1,1}, \ldots, 1 - y_{l-1,n})\rangle \subseteq T.$$

Hence $l \geqslant k$. Now let $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ be distinct elements in R^n. We show that there is a path from $(a_1, \ldots, a_n)$ to $(b_1, \ldots, b_n)$ in $TCay(R^n)$ with length at most k. Let $(1, \ldots, 1) = (x_{1,1}, \ldots, x_{1,n}) + \cdots + (x_{k,1}, \ldots, x_{k,n})$, for some $(x_{1,1}, \ldots, x_{1,n}), \ldots, (x_{k,1}, \ldots, x_{k,n}) \in T$. Define $z_0 = (a_1, \ldots, a_n)$ and

$$z_l = (b_1 - a_1, \ldots, b_n - a_n)((x_{1,1}, \ldots, x_{1,n}) + \cdots + (x_{l,1}, \ldots, x_{l,n}))(a_1, \ldots, a_n)$$

for every integer l with $1 \leqslant l \leqslant k$. Then

$$z_{k+1} - z_k = (b_1 - a_1, \ldots, b_n - a_n)(b_{l+1,1}, \ldots, b_{l+1,n}) \in T$$

for every integer l with $0 \leqslant l \leqslant n - 1$. Thus

$$(a_1, \ldots, a_n) \sim z_1 \sim z_2 \sim \cdots \sim z_{k-1} \sim (b_1, \ldots, b_n)$$

is a path from $(a_1, \ldots, a_n)$ to $(b_1, \ldots, b_n)$ in $TCay(R^n)$ with length at most n. Specially, a shortest path between $(0, \ldots, 0)$ and $(1, \ldots, 1)$ in $TCay(R^n)$ has length at most k, and thus $\mathrm{diam}(TCay(R)) = k$. □

Corollary 3.4. *Let R be a commutative ring and T be a triangular subset of R^n which is not closed under addition and $TCay(R^n)$ is connected. Then the following statements hold.*

(1) *$diam(TCay(R^n)) = d((0, \ldots, 0), (1, \ldots, 1))$.*

(2) *If $diam(TCay(R^n)) = k$, then $diam(TCay(R^n \setminus T)) \geqslant m - 2$.*

Proof. (1). This follows from Theorem 2.6.

(2). $\mathrm{diam}(TCay(R^n)) = d((0, \ldots, 0), (1, \ldots, 1))$, by (1). So, let

$$(0, \ldots, 0) \sim (c_{1,1}, \ldots, c_{1,n}) \sim \cdots \sim (c_{k-1,1}, \ldots, c_{k-1,n}) \sim (1, \ldots, 1)$$

be the shortest path from $(0, \ldots, 0)$ to $(1, \ldots, 1)$ in $TCay(R^n)$.

Clearly $(c_{1,1}, \ldots, c_{1,n}) \in T^*$. If $(c_{i,1}, \ldots, c_{i,n}) \in T^*$, for $2 \leqslant i \leqslant k-1$, then we can construct the path

$$(0, \ldots, 0) \sim (c_{i,1}, \ldots, c_{i,n}) \sim \cdots \sim (c_{k-1,1}, \ldots, c_{k-1,n}) \sim (1, .., 1)$$

from $(0, \ldots, 0)$ to $(1, \ldots, 1)$ in $TCay(R^n)$ which has length less than k, which is a contradication. Thus $(c_{i,1}, \ldots, c_{i,n}) \in R^n \setminus T$, for $2 \leqslant i \leqslant k-1$. Hence

$$(c_{2,1}, \ldots, c_{2,n}) \sim \cdots \sim (c_{k-1,1}, \ldots_{k-1,n}) \sim (1, \ldots, 1)$$

is the shortest path from $(c_{2,1}, \ldots, c_{2,n})$ to $(1, \ldots, 1)$ in $R^n \setminus T$ and it has length $k-2$. Thus $\mathrm{diam}(TCay(R^n \setminus T)) \geqslant m - 2$. □

Now, for each $X \in T$, let i_X be a positive integer that the first nonzero component of X is in the i_X-th place. Also let

$$m := \min\{i_X \mid X \in U\}.$$

Lemma 3.5. *Let R be a commutative ring and T be a triangular subset of R^n which is not closed under addition. If $m \geqslant 2$, then*

$$gr(TCay(R^n \setminus T)) = gr(TCay(T)) = 3.$$

Proof. If $n \geqslant 3$, since $m \geqslant 2$, then exist $(0, \ldots, 0, a, 0) \in T$ such that $a \neq 0$. Hence

$$(0, \ldots, 0, a, 0), (0, \ldots, 0, a), (0, \ldots, 0)$$

are adjacent in T. Also

$$(1, \ldots, 1, a, 0), (1, \ldots, 1, 0, 0), (1, \ldots, 1, 0, a)$$

are adjacent in $R^n \setminus T$.

If $n = 2$, since $m = 2$ and $R^n \neq T$, then exist $(a, 0)$ in T and (x, y) in $R^n \setminus T$ such that $a, x \neq 0$. Hence $(a, 0), (a, a), (0, 0) \in T$ that are adjacent. Also $(x, 0), (x, a), (x + a, 0) \in R^n \setminus T$ that are adjacent. Therefore $gr(TCay(R^n \setminus T)) = gr(TCay(T)) = 3$. □

Theorem 3.6. *Let R be a commutative ring and T be a triangular subset of R^n which is not closed under addition. If $m = 1$, then $gr(TCay(R^n \setminus T)) \leqslant 4$ and $gr(TCay(T)) \in \{3, 4, \infty\}$.*

Proof. Since T is traingular subset of R^n, then $T = \bigcup_{i\in\gamma} I_{i1} \times \ldots \times I_{in}$, where $I_{i1} \subseteq \ldots \subseteq I_{in}$ and I_{ij} are ideals of R, for $1 \leqslant j \leqslant n$ and $i \in \gamma$. Also T is not closed under addition and $m = 1$, therefore $i \geqslant 2$ and $T = \bigcup_{i\in\gamma}\{0\} \times \ldots \{0\} \times I_{in}$, which $I_{in} \neq \{0\}$.

Case 1: If $|I_{kn}| \geqslant 3$ for some $k \in \gamma$, then $gr(TCay(R^n \setminus T)) = gr(TCay(T)) = 3$.

Case 2: If $|I_{in}| \leqslant 2$ for every $i \in \gamma$, then $i \geqslant 2$, since T is not closed under addition. So, we have two subcases.

Case 2a: If exist nonzero element $(0, \ldots, 0, a), (0, \ldots, 0, b), (0, \ldots, 0, c) \in T$ such that $a, b, c \neq 0$ and $a + b = c$, then

$$(0, \ldots, 0), (0, \ldots, 0, a), (0, \ldots, 0, a + b), (0, \ldots, 0, b), (0, \ldots, 0)$$

is a cycle of length 4 in $TCay(T)$. Also

$$(1, \ldots, 1), (1, \ldots, 1, a), (1, \ldots, 1, a + b), (1, \ldots, 1, b), (1, \ldots, 1)$$

is a cycle of length 4 in $TCay(R \setminus T)$. Thus $gr(TCay(T)) = gr(TCay(R \setminus T)) = 3$.

Case 2b: If for every nonzero element $(0, \ldots, 0, x), (0, \ldots, 0, y) \in T$, then $(0, \ldots, 0, x + y) \notin T$. Since $i \geqslant 2$, then exist $(0, \ldots, 0, a), (0, \ldots, 0, b) \in T$, such that $a, b \neq 0$ and $a \neq b$. Now

$$(1, \ldots, 1, 0) \sim (1, \ldots, 1, a) \sim (1, \ldots, 1, a + b) \sim (1, \ldots, 1, b) \sim (1, \ldots, 1, 0)$$

is a cycle of length 4 in $TCay(R \setminus T)$, then $gr(TCay(R \setminus T)) \leqslant 4$. The graph $TCay(T)$ is isomorphic to $K_{1,i}$. Hence $gr(TCay(T)) = \infty$. □

4. Planarity

The graph G is said to be planar if it can be drawn in the plane so that its edges intersect only at their ends. A subdivision of a graph is any graph that can be obtained from the original graph by replacing edges by paths. A remarkable simple characterization of the planar graphs was given by Kuratowski in 1930. Kuratowski's Theorem says that a graph is planar if and only if it contains no subdivision of K_5 or $K_{3,3}$.

Theorem 4.1. *Let R be a commutative ring and T be a triangular subset of R^n which is closed under addition, then $TCay(R^n)$ is planar if and only if $|T| \leqslant 4$.*

Proof. Let $|T| = \alpha$ and $|R^n/T| = \beta$. Since T is closed under addition, then T is an ideal and by Theorem 2.2, $TCay(T)$ is a complete graph K_α and $TCay(R^n \setminus T)$ is the union of $\beta - 1$ disjoint K_α. Therefore $TCay(R^n)$ is planar if and only if $|T| \leqslant 4$. □

Theorem 4.2. *Let R be a commutative ring and T be a triangular subset of R^n which is not closed under addition and $m \leqslant n-1$, then $TCay(R^n)$ is not planar.*

Proof. Since T is not an ideal and $m \leqslant n-1$, then exist $(0,\ldots,0,a,0),(0,\ldots,0,b)$ in T where $a \neq b$ and $a, b \neq 0$. Then the vertices

$$(0,\ldots,0),(0,\ldots,0,a,0),(0,\ldots,0,a),(0,\ldots,0,a,a),$$

$$(0,\ldots,0,a+b,0),(0,\ldots,0,b),(0,\ldots,0,a+b),(0,\ldots,0,a+b,a)$$

forms a subdivision of K_5, hence $TCay(R^n)$ is not planar. □

Now, the only remaining case for investigating the planarity of $TCay(R^n)$, is the case that $m = n$. If T is not closed under addition, since T is a triangular subset of R^n, then $T = \bigcup_{i\in\gamma} I_{i1} \times \ldots \times I_{in}$, where $I_{i1} \subseteq \ldots \subseteq I_{in}$ and $i \geqslant 2$.

Theorem 4.3. *Let R be a commutative ring and T be a triangular subset of R^n which is not closed under addition and $m = n$ and $i \geqslant 4$, then $TCay(R^n)$ is not planar.*

Proof. Since $i \geqslant 4$, there exist ideals of R^n such that $\{0\} \times \ldots \times \{0\} \times \{x_1\}$, $\{0\} \times \ldots \times \{0\} \times \{x_2\}$, $\{0\} \times \ldots \times \{0\} \times \{x_3\}$ and $\{0\} \times \ldots \times \{0\} \times \{x_4\}$ where $x_1, x_2, x_3, x_4 \neq 0$.

Case 1: If $x_r + x_p = x_q$, for $1 \leqslant r, p, q \leqslant 4$, then we may assume that $x_1 + x_2 = x_3$. Hence

$$(0,\ldots,0),(0,\ldots,0,x_1),(0,\ldots,0,x_2),(0,\ldots,0,x_3),(0,\ldots,0,x_4),$$

$$(0,\ldots,0,x_1+x_4),(0,\ldots,0,x_2+x_4),(0,\ldots,0,x_3+x_4)$$

forms a subdivision of K_5, and so $TCay(R^n)$ is not planar.

Case 2: If $x_r + x_p \neq x_q$ for every $1 \leqslant r, p, q \leqslant 4$, then

$$(0,\ldots,0),(0,\ldots,0,x_1),(0,\ldots,0,x_2),(0,\ldots,0,x_3),(0,\ldots,0,x_2+x_3),$$

$$(0,\ldots,0,x_1+x_3),(0,\ldots,0,x_1+x_2),(0,\ldots,0,x_1+x_4),(0,\ldots,0,x_3+x_4)$$

$$(0,\ldots,0,x_2+x_3+x_4),(0,\ldots,0,x_1+x_2+x_4),(0,\ldots,0,x_1+x_2+x_3)$$

forms a subdivision of $K_{3,3}$, and so $TCay(R^n)$ is not planar. □

Theorem 4.4. *Let R be a commutative ring and T be a triangular subset of R^n which is not closed under addition and $m = n$ and $i = 3$, then $TCay(R^n)$ is planar if and only if $|T| = 4$.*

Proof. Since $i = 3$, then

$$T = (\{0\} \times \ldots \times \{0\} \times I_1) \cup (\{0\} \times \ldots \times \{0\} \times I_2) \cup (\{0\} \times \ldots \times \{0\} \times I_3)$$

where $|I_1|$,$|I_2|$ and $|I_3|$ are at least 2.

Case 1: If $|T| > 4$, then there exists $|I_i| \geqslant 3$, for $1 \leqslant i \leqslant 3$. Hence, the elements $(0, \ldots, 0, a), (0, \ldots, 0, 2a), (0, \ldots, 0, b), (0, \ldots, 0, c)$ are belong T, where $a, 2a, b, c \neq 0$. Therefore

$$(0, \ldots, 0), (0, \ldots, 0, a), (0, \ldots, 0, 2a), (0, \ldots, 0, b), (0, \ldots, 0, b), (0, \ldots, 0, a+b),$$

$$(0, ..., 0, 2a+b), (0, ..., 0, 2a+c), (0, ..., 0, b+c), (0, ..., 0, a+b+c), (0, ..., 0, 2a+b+c)$$

forms a subdivision of $K_{3,3}$, and so $TCay(R^n)$ is not planar.

Case 2: If $|T| = 4$, then $|I_1| = |I_2| = |I_3| = 2$. Since

$$T = (\{0\} \times \ldots \times \{0\} \times \{a\}) \cup (\{0\} \times \ldots \times \{0\} \times \{b\}) \cup (\{0\} \times \ldots \times \{0\} \times \{c\}).$$

Hence the graph $TCay(R^n)$ is the union of some copies of graph as Figure 1.

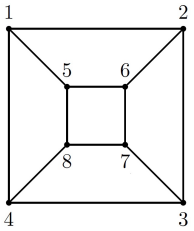


Figure 1.

The converse statement is clear. □

The proof of following lemma is similar to the proof of Lemma 4.1 in [3] and hence we omit it.

Lemma 4.5. *Let R be a commutative ring and T be a triangular subset of R^n which is not closed under addition, $m = n$ and $i = 2$. Then*

(1) *if T contains ideals P_1 and P_2 with $|P_1| \geqslant 4$, $|P_2| \geqslant 2$ and $|P_1 \cup P_2| \geqslant 5$, then $TCay(R^n)$ is not planar;*

(2) *If T contains ideals P_1 and P_2 with $|P_1|, |P_2| \geqslant 3$ and $|P_1 \cup P_2| \geqslant 5$, then $TCay(R^n)$ is not planar.*

Theorem 4.6. *Let R be a commutative ring and T be a triangular subset of R^n which is not closed under addition, $m = n$ and $i = 2$, then $TCay(R^n)$ is planar if and only if $|T| \leqslant 4$.*

Proof. Let $|T| \leqslant 4$.

Case 1: $|T| = 4$, then T contains ideals P_1 and P_2 with $|P_1| = 3$, $|P_2| = 2$. We may assume that $P_1 = \{(0,\ldots,0),(0,\ldots,0,a),(0,\ldots,0,2a)\}$ and $P_2 = \{(0,\ldots,0),(0,\ldots,0,b)\}$, where $a,b \neq 0$ and $a \neq b$. then $TCay(R^n)$ is the union of some copies of grpah as Figure 2. For everv $(x_1,\ldots,x_n) \in R^n$, we have

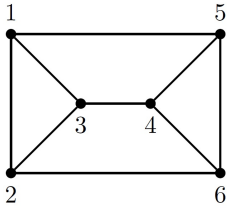


Figure 2.

$$x_1 = (x_1,\ldots,x_n+a), \qquad x_2 = (x_1,\ldots,x_n+2a),$$
$$x_3 = (x_1,\ldots,x_n), \qquad x_4 = (x_1,\ldots,x_n+b),$$
$$x_5 = (x_1,\ldots,x_n+a+b), \qquad x_6 = (x_1,\ldots,x_n+2a+b).$$

Therefore $TCay(R^n)$ is planar.

Case 2: If $|T| = 4$, then T contains ideals P_1 and P_2 with $|P_1| = |P_2| = 2$ and hence the graph $TCay(R^n)$ is the union of some copies of C_4. Therefore $|T| = 4$ is planar.

The converse statement is a consequence of Theorem 4.5. □

Now we have the following corollary.

Corollary 4.7. *Let R be a commutative ring and T be a triangular subset of R^n, then $TCay(R^n)$ is planar if and only if following statment is hod:*

(1) *T is closed under addition and $|T| \leqslant 4$.*

(2) *T not closed under addition, $i = 3$ and $|T| = 4$.*

(3) *T not closed under addition, $i = 2$ and $|T| \leqslant 4$.*

References

[1] **M. Afkhami, M.R. Ahmadi, R. Jahani-Nezhad and K. Khashyarmanesh,** *Cayley graphs of ideals in a commutative ring*, Bull. Malays. Math. Sci. Soc. **37** (2014), 833 – 843.

[2] **M. Afkhami, Z. Barati, K. Khashyarmanesh and N. Paknejad,** *Cayley sum graphs of ideals of a commutative ring*, J. Aust. Math. Soc. **96** (2014), 289 – 302.

[3] **M. Afkhami, K.Hamidizadeh and K. Khashyarmanesh,** *On the generalization of Cayley graphs of commutative ring*, Beitrage Algebra Geom. **58** (2016), 395 – 404.

[4] **G. Alipour, S. Akbari,** *Some properties of a Cayley graph of a commutative ring,* Commun. Algebra **42** (2014) 1582 – 1593.

[5] **D.F. Anderson, A. Badawi,** *On the zero-divisor graph of a ring,* Commun. Algebra **36** (2008), 3073 – 3092.

[6] **D.F. Anderson, A. Badawi,** *The generelized total graph of a commutative ring,* J. Algebra Appl. **12** (2013), 1250212.

[7] **D.F. Anderson, A. Badawi,** *The total graph of a commutative ring,* J. Algebra. **320** (2008), 2706 – 2719.

[8] **D.F. Anderson, A. Badawi,** *The total graph of a commutative ring with out the zero element,* J. Algebra Appl. **11** (2012), 12500740.

[9] **J.A. Bondy, U.S.R. Murty,** *Graph Theory with applications,* American Elsevier, New York, 1976.

[10] **I. Kaplansky,** *Commutative Rings,* 1976.rev. ed., University of Chicago Press, Chicago, 1974

[11] **A.V. Kelarev,** *Directed graphs and nilpotent rings,* J. Austral. Math. Soc. **65** (1998), 326 – 332.

[12] **A.V. Kelarev,** *On undirected Cayley graphs,* Australasian J. Combinatorics **25** (2002), 73 – 78.

[13] **A.V. Kelarev,** *Ring Constructions and Applications,* World Scientific, River Edge, NJ, 2002.

[14] **A.V. Kelarev,** *Graph Algebras and Automata,* Marcel Dekker, New York, 2003.

[15] **A.V. Kelarev,** *Labelled Cayley graphs and minimal automata,* Australasian J. Combinatorics **30** (2004), 95 – 101.

[16] **A.V. Kelarev,** *On Cayley graphs of inverse semigroups,* Semigroup Forum **72** (2006), 411 – 418.

[17] **A.V. Kelarev, C.E. Praeger,** *On transitive Cayley graphs of groups and semigroups,* European J. Combinatorics **24** (2003), 59 – 72.

[18] **A.V. Kelarev, S.J. Quinn,** *A combinatorial property and power graphs of groups,* Contrib. General Algebra **12** (2000), 229 – 235.

[19] **A.V. Kelarev, S.J. Quinn,** *Directed graphs and combinatorial properties of semigroups,* J. Algebra **251** (2002), 16 – 26.

Received May 14, 2017

K. Hamidizadeh
Department of Mathematics, Payame Noor University, P.O.Box 19395-3697, Tehran, Iran
E-mail: k.hamidizadeh@pnu.ac.ir

G. Aghababaei
Department of Mathematics, University of Applied Sciences and Technology, Tehran, Iran
E-mail: g-aghababaei@yahoo.com

Quasigroups and Related Systems **26** (2018), 77 – 78

There exist semigroups which have bi-bases with different cardinalities

Dariush Heidari

Abstract. Kummoon and Changphas in Quasigroups and Related Systems 25(2017), 87 – 94 state the following question: *"Is it true that for any two bi-bases of a semigroup have the same cardinality?"*

In this paper, we provide a semigroup of order n for every $n \geq 5$ which has two bi-bases with different cardinalities that is shown the answer of question is negative.

1. Introduction

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

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

Kummoon and Changphas in [1] introduced the concept which is called bi-base of semigroups and proved some properties.

Definition. Let S be a semigroup. A subset B of S is called a *bi-base* of S if it satisfies the following two conditions:

(i) $S = B \cup BB \cup BSB$;

(ii) if A is a subset of B such that $S = A \cup AA \cup ASA$, then $A = B$.

2. Main results

In [1] the authors asked the following question:

Is it true that for any two bi-bases of a semigroup have the same cardinality?

We would like to answer the question by providing a semigroup of order $n \geqslant 5$ which has two bi-bases with different cardinalities.

Answer. Let $S_n = \{1, 2, \ldots, n\}$ for every $n \geqslant 5$ and consider the following binary operation on S_n:

$$x \cdot y = \begin{cases} 1, & \text{if } x \notin \{n-2, n\} \text{ and } y \notin \{n-1, n\}, \\ n-1, & \text{if } x \notin \{n-2, n\} \text{ and } y \in \{n-1, n\}, \\ n-2, & \text{if } x \in \{n-2, n\} \text{ and } y \notin \{n-1, n\}, \\ n, & \text{if } x \in \{n-2, n\} \text{ and } y \in \{n-1, n\}. \end{cases}$$

2010 Mathematics Subject Classification: 20M20

Keywords: Semigroup, bi-base.

To verify the associativity condition let $x, y, z \in S_n$. Then there are four cases:

Case 1. If $x \notin \{n-2, n\}$ and $z \notin \{n-1, n\}$ then $x \cdot (y \cdot z) = 1 = (x \cdot y) \cdot z$.

Case 2. If $x \notin \{n-2, n\}$ and $z \in \{n-1, n\}$ then $x \cdot (y \cdot z) = n-1 = (x \cdot y) \cdot z$.

Case 3. If $x \in \{n-2, n\}$ and $z \notin \{n-1, n\}$ then $x \cdot (y \cdot z) = n-2 = (x \cdot y) \cdot z$.

Case 4. If $x \in \{n-2, n\}$ and $z \in \{n-1, n\}$ then $x \cdot (y \cdot z) = n = (x \cdot y) \cdot z$.

In each case $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ so $(S_n, \cdot)$ is a semigroup.

Now, let $A \subseteq \{2, 3, \ldots, n-3, n-1\}$ then $AA = ASA = A$ so every bi-base of $(S_n, \cdot)$ contains $\{2, 3, \ldots, n-3, n-1\}$. Also, if $A = \{2, n\}$ or $A = \{n-2, n-1\}$ then $AA = ASA = \{1, n-2, n-1, n\}$. Therefore, the subsets $B = \{2, 3, \ldots, n-3, n\}$ and $B' = \{2, 3, \ldots, n-1\}$ are two bi-bases of $(S_n, \cdot)$ with cardinality $n-3$ and $n-2$, respectively.

Example. Consider $n = 5$. Then the Cayley table of $(S_5, \cdot)$ is as follows

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

Also, the subsets $B = \{2, 5\}$ and $B' = \{2, 3, 4\}$ are two bi-bases of $(S_5, \cdot)$.

References

[1] **P. Kummoon and T. Changphas**, *On bi-bases of a semigroup*, Quasigroups and Related Systems **25** (2017), 87 – 94.

Received December 13, 2017

Faculty of science
Mahallat Institute of Higher Education
Mahallat
Iran
E-mail: dheidari82@gmail.com

Quasigroups and Related Systems **26** (2018), 79 – 85

A note on hyperideals in ordered hypersemigroups

Niovi Kehayopulu

Abstract. For an ordered hypersemigroup H, we denote by $\mathcal{N}$the semilattice congruence on H defined by $x\mathcal{N}y$ if and only if the hyperfilters of H generated by the elements x and y coincide. We first prove that this is a complete semilattice congruence on H. Moreover, if H is an ordered hypersemigroup, T a hyperfilter of H and, for a class $(z)_{\mathcal{N}}$ of H there is an element in the intersection $T \cap (z)_{\mathcal{N}}$, then the class $(z)_{\mathcal{N}}$ is a subset of T. From these two statements, the following two important results can be obtained: (1) If H is an ordered hypersemigroup, then each hyperideal of some $(z)_{\mathcal{N}}$-class of H does not contain proper hyperfilters. As a consequence, (2) every prime hyperideal of an ordered hypersemigroup is decomposable into its $\mathcal{N}$-classes.

1. Introduction

The concept of the hypergroup introduced by the French Mathematician F. Marty at the 8th Congress of Scandinavian Mathematicians in 1933 is as follows: A *hypergroup* is a nonempty set H endowed with a multiplication xy such that the following assertions are satisfied: (i) $xy \subseteq H$; (ii) $x(yz) = (xy)z$; (iii) $xH = Hx = H$ for every $x, y, z \in H$ (see [10]). The first researchers who investigate hypergroups using the definition given by Marty were Mittas and Corsini. The concept of the hypersemigroup follows at the usual way and in the recent years many groups in the world investigate these two subjects, related subjects as well, in research programs and hundreds of papers on hypergroups and hypersemigroups appeared using the definition introduced by Marty. As it is no possible to refer to all of them, we will mention only some, related to the present paper, in the references such as the [1–5, 7–10, 12]. If H is a hypergroupoid, a relation σ on H is called *congruence* if $(a, b) \in \sigma$ and $c \in H$ implies $(c \circ a, c \circ b) \in \sigma$ and $(a \circ c, b \circ c) \in \sigma$; in the sense that for every $u \in c \circ a$ and every $v \in c \circ b$ we have $(u, v) \in \sigma$ and for every $u \in a \circ c$ and every $v \in b \circ c$ we have $(u, v) \in \sigma$. A congruence σ on H is called *semilattice congruence* if, for any $a, b \in H$, we have $(a, a \circ a) \in \sigma$ and $(a \circ b, b \circ a) \in \sigma$; in the sense that for every $a \in H$ and every $u \in a \circ a$ we have $(a, u) \in \sigma$ and for every $a, b \in H$, every $u \in a \circ b$ and every $v \in b \circ a$, we have $(u, v) \in \sigma$. An *ordered hypergroupoid* is an ordered set

2010 Mathematics Subject Classification: 06F99.

Keywords: Ordered hypersemigroup, complete semilattice congruence, hyperfilter, hyperideal, prime hyperideal.

$(H, \leq)$ at the same time a hypergroupoid such that $a \leq b$ implies $x \circ a \leq x \circ b$ and $a \circ x \leq b \circ x$ for all $x \in H$, in the sense that for every $x \in H$ and every $u \in x \circ a$ there exists $v \in x \circ b$ such that $u \leq v$ and for every $u \in a \circ x$ there exists $v \in b \circ x$ such that $u \leq v$ [5]. A nonempty subset I of an ordered hypergroupoid is called a *hyperideal* of H if the following hold: (1) $H \circ I \subseteq I$ and $I \circ H \subseteq I$ and (2) if $a \in I$ and $b \in H$ such that $b \leq a$, then $b \in I$. A hyperideal I of H is called *prime* if (1) $a, b \in H$ such that $a \circ b \subseteq I$ implies $a \in I$ or $b \in I$ and (2) for every $a, b \in H$, either $a \circ b \subseteq I$ or $(a \circ b) \cap I = \emptyset$. A hyperideal (hyperfilter) T of H is called *proper* if H is the only hyperideal (hyperfilter) of H. If I is an ideal of an $\mathcal{N}$-class of a semigroup, then I has no completely prime ideals. As a consequence every complete prime ideal of a semigroup is a union of $\mathcal{N}$-classes [11]. In ordered semigroups, we always use the terms prime, weakly prime instead of completely prime, prime given by Petrich and we will keep the same for hypersemigroups as well. For an ordered hypersemigroup H, we denote by $\mathcal{N}$ the semilattice congruence on H defined by $x\mathcal{N}y$ if and only if $N(x) = N(y)$, where $N(a)$ is the hyperfilter of H generated by the element a of H. The present paper deals with the decomposition of prime hyperideals of an ordered hypersemigroup into its $\mathcal{N}$-classes. First of all, the class $\mathcal{N}$ is a complete semilattice congruence on H. If now H is an ordered hypersemigroup, T a hyperfilter of H and z an element of H that belongs to $T \cap (z)_{\mathcal{N}}$, then the class $(z)_{\mathcal{N}}$ is a subset of T, that yields to the following two important results: Firstly, if H is an ordered hypersemigroup, $z \in H$ and I a hyperideal of $(z)_{\mathcal{N}}$, then I does not contain proper hyperfilters, as so does not contain proper prime hyperideals as well. Secondly, if H is an ordered hypersemigroup and I a prime hyperideal of H, then I is decomposable into its $\mathcal{N}$-classes. The corresponding results on hypersemigroup (or semigroups) (without order) can be also obtained as application of the results of the present paper as each hypersemigroup (semigroup) endowed with the equality relation "=" is an ordered hypersemigroup (ordered semigroup).

2. Main results

Definition 2.1. Let $(H, \circ, \leq)$ be an ordered hypergroupoid. A nonempty subset F of H is called a *hyperfilter* of H if the following assertions are satisfied:

1) if $x, y \in F$, then $x \circ y \subseteq F$,

2) if $x, y \in H$ such that $x \circ y \subseteq F$, then $x \in F$ and $y \in F$,

3) for any $x, y \in H$, we have $x \circ y \subseteq F$ or $(x \circ y) \cap F = \emptyset$,

4) if $x \in F$ and $y \in H$ such that $y \geq x$, then $y \in F$.

That is, it is a hypersubgroupoid of H satisfying the relations 2–4.

Definition 2.2. Let H be a hypergroupoid. A nonempty subset T of H is called a *prime subset* of H if the following assertions are satisfied:

1) if $a, b \in H$ such that $a \circ b \subseteq T$, then $a \in T$ or $b \in T$ and

2) for every $a, b \in H$, we have $a \circ b \subseteq T$ or $(a \circ b) \cap T = \emptyset$.

Definition 2.3. Let $(H, \circ, \leq)$ be an ordered hypergroupoid. A semilattice congruence σ on H is called *complete* if $a \leq b$ implies $(a, a \circ b) \in \sigma$, in the sense that if $u \in a \circ b$, then $(a, u) \in \sigma$.

Proposition 2.4. *Let $(H, \circ, \leq)$ be an ordered hypergroupoid. Then the semilattice congruence $\mathcal{N}$ is a complete semilattice congruence on H.*

Proof. Let $a \leq b$. Then $(a, a \circ b) \in \mathcal{N}$. In fact: Let $u \in a \circ b$. Then $(a, u) \in \mathcal{N}$, that is $N(a) = N(u)$. Indeed: Since $N(a) \ni a \leq b$, we have $b \in N(a)$. Since $a, b \in N(a)$, we have $a \circ b \subseteq N(a)$. Since $u \in a \circ b$, we have $u \in N(a)$, then $N(u) \subseteq N(a)$. On the other hand, since $u \in a \circ b$ and $u \in N(u)$, we have $u \in (a \circ b) \cap N(u)$. Since $(a \circ b) \cap N(u) \neq \emptyset$, we have $a \circ b \subseteq N(u)$. Then $a \in N(u)$, and $N(a) \subseteq N(u)$. Hence we obtain $N(u) = N(a)$ and the proof is complete. □

In a similar way as in the Lemma in [6] we can prove the following:

Proposition 2.5. *Let H be an ordered hypergroupoid and F a nonempty subset of H. The following are equivalent:*

(1) *F is a hyperfilter of H.*

(2) *$H \backslash F = \emptyset$ or $H \backslash F$ is a prime hyperideal of H.*

Proposition 2.6. *An ordered hypergroupoid H does not contain proper hyperfilters if and only if H does not contain proper prime hyperideals.*

Proof. ($\Rightarrow$). Let I be a prime hyperideal of H and $I \subset H$. Then $\emptyset \neq H \backslash I \subseteq H$ and $H \backslash (H \backslash I) (= I)$ is a prime hyperideal of H ($H \backslash I$ is the complement of I to H). By Proposition 2.5, $H \backslash I$ is a hyperfilter of H. Then $H \backslash I = H$ and $I = \emptyset$ which is impossible.

($\Leftarrow$). Let F be a hyperfilter of H and $F \subset H$. Since $H \backslash F \neq \emptyset$, by Proposition 2.5, $H \backslash F$ is a prime hyperideal of H. Then $H \backslash F = H$ and $F = \emptyset$ which is impossible. □

Remark 2.7. *Let H be an ordered hypergroupoid, T a hyperfilter of H, $z \in H$ and $a \in T \cap (z)_{\mathcal{N}}$. Then we have $(z)_{\mathcal{N}} \subseteq T$.*

Proof. Let $y \in (z)_{\mathcal{N}}$. Then $(y)_{\mathcal{N}} = (z)_{\mathcal{N}} = (a)_{\mathcal{N}}$, so $(y, a) \in \mathcal{N}$ and $N(y) = N(a)$. Since T is a hyperfilter of H containing the element a, we have $N(a) \subseteq T$. Thus we have $y \in N(y) = N(a) \subseteq T$ and so $y \in T$. □

Theorem 2.8. *Let H be an ordered hypersemigroup and $z \in H$. If I is a hyperideal of $(z)_{\mathcal{N}}$, then I does not contain proper hyperfilters.*

Proof. Let F be a hyperfilter of I. Then $F = I$. In fact: Take an element $a \in F$ (such an element exists as F is a nonempty set) and consider the set

$$T := \{x \in H \mid a^2 \circ x \subseteq F\}.$$

Then the following assertions are satisfied:

(1). $F = T \cap I$. Indeed: Let $y \in F$. Since $a^2 \subseteq F$, we have $a^2 \circ y \subseteq F$ and so $y \in T$. Besides, $F \subseteq I$, so $F \subseteq T \cap I$. Let now $y \in T \cap I$. Since $y \in T$, we have $a^2 \circ y \subseteq F$. Then, since $a^2 \subseteq F \subseteq I$, we have $y \in I$ and, since F hyperfilter of I, we have $y \in F$.

(2). T is a hyperfilter of H. In fact: This is a nonempty subset of H because $a^3 \subseteq F$ and $a \in T$. Let $x, y \in T$. Then $x \circ y \subseteq T$. In fact: The following properties are satisfied:

(A). $y \circ a^2 \subseteq F$. Indeed: Since $a^2 \circ y \subseteq F$ and $a^2 \subseteq F$, we have

$$F \supseteq (a^2 \circ y) \circ a^2 = a^2 \circ (y \circ a^2), \text{ where } a^2 \subseteq I \qquad (*)$$

Moreover, we have $y \circ a^2 \subseteq I$. Indeed: Since $a^2 \circ y \subseteq F \subseteq I \subseteq (z)_{\mathcal{N}}$, we have

$$\begin{aligned}(z)_{\mathcal{N}} = (a^2 \circ y)_{\mathcal{N}} &:= (a^2)_{\mathcal{N}} \circ (y)_{\mathcal{N}} = (a)_{\mathcal{N}} \circ (y)_{\mathcal{N}} \\ &= (y)_{\mathcal{N}} \circ (a)_{\mathcal{N}} = (y \circ a)_{\mathcal{N}},\end{aligned}$$

so $y \circ a \subseteq (z)_{\mathcal{N}}$. Then, since $a \in F \subseteq I$ and I is a hyperideal of $(z)_{\mathcal{N}}$, we have

$$y \circ a^2 = (y \circ a) \circ a \subseteq (z)_{\mathcal{N}} \circ I \subseteq I,$$

thus $y \circ a^2 \subseteq I$. Since $a^2 \subseteq I$ and $y \circ a^2 \subseteq I$, by $(*)$, we have $y \circ a^2 \subseteq F$.

(B). $a^2 \circ x \circ y \subseteq I$. In fact: Clearly, $a^2 \circ x \circ y = a \circ (a \circ x \circ y)$. On the other hand, $a \circ x \circ y \subseteq (z)_{\mathcal{N}}$. Indeed: Since $a^2 \circ x \subseteq F \subseteq I \subseteq (z)_{\mathcal{N}}$, we have

$$(z)_{\mathcal{N}} = (a^2 \circ x)_{\mathcal{N}} = (a^2)_{\mathcal{N}} \circ (x)_{\mathcal{N}} = (a)_{\mathcal{N}} \circ (x)_{\mathcal{N}} = (a \circ x)_{\mathcal{N}}.$$

We have seen in (A) that $(z)_{\mathcal{N}} = (y \circ a)_{\mathcal{N}}$ $(= (a \circ y)_{\mathcal{N}})$. Thus we have

$$\begin{aligned}(z)_{\mathcal{N}} = (z^2)_{\mathcal{N}} &:= (z)_{\mathcal{N}} \circ (z)_{\mathcal{N}} = (a \circ x)_{\mathcal{N}} \circ (a \circ y)_{\mathcal{N}} \\ &= (a)_{\mathcal{N}} \circ \Big((x)_{\mathcal{N}} \circ (a)_{\mathcal{N}}\Big) \circ (y)_{\mathcal{N}} = (a)_{\mathcal{N}} \circ \Big((a)_{\mathcal{N}} \circ (x)_{\mathcal{N}}\Big) \circ (y)_{\mathcal{N}} \\ &= (a^2)_{\mathcal{N}} \circ (x)_{\mathcal{N}} \circ (y)_{\mathcal{N}} = (a)_{\mathcal{N}} \circ (x \circ y)_{\mathcal{N}} = (a \circ x \circ y)_{\mathcal{N}}\end{aligned}$$

and so $a \circ x \circ y \subseteq (z)_{\mathcal{N}}$. Then, since I is a hyperideal of $(z)_{\mathcal{N}}$, we have

$$a \circ (a \circ x \circ y) \subseteq I \circ (z)_{\mathcal{N}} \subseteq I,$$

and so $a^2 \circ x \circ y \subseteq I$.

Since $x \in T$, we have $a^2 \circ x \subseteq F$. Then, by (A), $(a^2 \circ x) \circ (y \circ a^2) \subseteq F$, and then we have

$$F \supseteq (a^2 \circ x) \circ (y \circ a^2) = (a^2 \circ x \circ y) \circ a^2,$$

where $a^2 \subseteq I$ and $a^2 \circ x \circ y \subseteq I$ (by (B)). Since F is a hyperfilter of I, we have $a^2 \circ x \circ y \subseteq F$ and so $x \circ y \subseteq T$.

If $x, y \in H$ such that $x \circ y \subseteq H$, then $x \in T$ and $y \in T$. In fact, since $x \circ y \subseteq T$, we have $a^2 \circ x \circ y \subseteq F$. We remark first that

$$F \supseteq (a^2 \circ x \circ y) \circ a^2 = (a^2 \circ x) \circ (y \circ a^2) \qquad (*)$$

In addition, the following properties are satisfied:

(A). $a^2 \circ x \subseteq I$. In fact: We have $a^2 \circ x = a \circ (a \circ x)$, where $a \in I$. Moreover, $a \circ x \subseteq (z)_{\mathcal{N}}$. Indeed, since $a^2 \circ x \circ y \subseteq F \subseteq (z)_{\mathcal{N}}$, we have $(a^2 \circ x \circ y) = (z)_{\mathcal{N}}$. Since $a \in F \subseteq I \subseteq (z)_{\mathcal{N}}$, we have $(z)_{\mathcal{N}} = (a)_{\mathcal{N}}$. Thus we get $(a^2 \circ x \circ y)_{\mathcal{N}} = (a)_{\mathcal{N}}$. On the other hand,

$$\begin{aligned}(a \circ x)_{\mathcal{N}} &= (a)_{\mathcal{N}} \circ (x)_{\mathcal{N}} = (a^2 \circ x \circ y)_{\mathcal{N}} \circ (x)_{\mathcal{N}} \\ &= (a^2)_{\mathcal{N}} \circ (x)_{\mathcal{N}} \circ (y)_{\mathcal{N}} \circ (x)_{\mathcal{N}} = (a^2)_{\mathcal{N}} \circ (x)_{\mathcal{N}} \circ (x)_{\mathcal{N}} \circ (y)_{\mathcal{N}} \\ &= (a^2)_{\mathcal{N}} \circ (x^2)_{\mathcal{N}} \circ (y)_{\mathcal{N}} = (a^2)_{\mathcal{N}} \circ (x)_{\mathcal{N}} \circ (y)_{\mathcal{N}} \\ &= (a^2 \circ x \circ y)_{\mathcal{N}} = (z)_{\mathcal{N}},\end{aligned}$$

thus $a \circ x \subseteq (z)_{\mathcal{N}}$. Since I is a hyperideal of $(z)_{\mathcal{N}}$, we have $a \circ (a \circ x) \subseteq I \circ (z)_{\mathcal{N}}$ and so $a^2 \circ x \subseteq I$.

(B). $y \circ a^2 \subseteq I$. In fact: First of all, $y \circ a^2 = (y \circ a) \circ a$ and $a \in I$. Besides, $y \circ a \subseteq (a)_{\mathcal{N}}$, Indeed, since

$$\begin{aligned}(y \circ a)_{\mathcal{N}} &= (y)_{\mathcal{N}} \circ (a)_{\mathcal{N}} = (y)_{\mathcal{N}} \circ (a^2 \circ x \circ y)_{\mathcal{N}} = (a^2 \circ x \circ y)_{\mathcal{N}} \circ (y)_{\mathcal{N}} \\ &= (a^2 \circ x)_{\mathcal{N}} \circ (y)_{\mathcal{N}} \circ (y)_{\mathcal{N}} = (a^2 \circ x)_{\mathcal{N}} \circ (y^2)_{\mathcal{N}} \\ &= (a^2 \circ x)_{\mathcal{N}} \circ (y)_{\mathcal{N}} = (a^2 \circ x \circ y)_{\mathcal{N}} = (z)_{\mathcal{N}},\end{aligned}$$

$y \circ a$ is a subset of $(z)_{\mathcal{N}}$. Since $a \in I$ and I a hyperideal of $(z)_{\mathcal{N}}$, we get $(y \circ a) \circ a \subseteq (z)_{\mathcal{N}} \circ I \subseteq I$ and so $y \circ a^2 \subseteq I$.

Since $a^2 \circ x \subseteq I$, $y \circ a^2 \subseteq I$ and F is a hyperfilter of I, by $(*)$, we have $a^2 \circ x \subseteq F$ and $y \circ a^2 \subseteq F$. Finally, $y \circ a^2 \subseteq F$ implies $a^2 \circ y \subseteq F$. In fact: Since $a^2, y \circ a^2 \subseteq F$, we have $a^2 \circ (y \circ a^2) \subseteq F$, then $(a^2 \circ y) \circ a^2 \subseteq F$. On the other hand, $a^2 \circ y \subseteq I$. Indeed: Since $a \circ y \subseteq (a \circ y)_{\mathcal{N}} = (z)_{\mathcal{N}}$ and $a \in I$ $(F \subseteq I)$, we have

$$a^2 \circ y = a \circ (a \circ y) \subseteq I \circ (z)_{\mathcal{N}} \subseteq I,$$

so $a^2 \circ y \subseteq I$. Since $(a^2 \circ y) \circ a^2 \subseteq F$, $a^2 \circ y \subseteq I$, $a^2 \subseteq I$ and F is a hyperfilter of I, we have $a^2 \circ y \subseteq F$.

For any $x, y \in T$ it is clear that either $a \circ b \subseteq T$ or $(a \circ b) \cap T = \emptyset$. Finally, let $x \in T$ and $y \in H$ such that $y \geq x$. Then $y \in T$. In fact: We have $a^2 \circ y \geq a^2 \circ x$ and $a^2 \circ x \subseteq F$. It is enough to prove that $a^2 \circ y \subseteq I$. Then, since F is a hyperfilter of I, we have $a^2 \circ y \subseteq F$ and so $y \in T$. On the other site, $a^2 \circ y = a \circ (a \circ y)$, where $a \in F \subseteq I \subseteq (z)_{\mathcal{N}}$. We prove that $a \circ y \subseteq (z)_{\mathcal{N}}$. Then, since I is a hyperideal

of $(z)_{\mathcal{N}}$, we have $a \circ (a \circ y) \subseteq I \circ (z)_{\mathcal{N}}$ and so $a^2 \circ y \subseteq I$. First of all, since $a^2 \circ x \subseteq F \subseteq I \subseteq (z)_{\mathcal{N}}$, we have

$$(z)_{\mathcal{N}} = (a^2x)_{\mathcal{N}} := (a^2)_{\mathcal{N}}(x)_{\mathcal{N}} = (a)_{\mathcal{N}}(x)_{\mathcal{N}} = (a \circ x)_{\mathcal{N}}.$$

On the other hand, since $x \leq y$, we have $a \circ x \leq a \circ y$ then, by Proposition 2.4, we have $(a \circ x, a \circ x \circ a \circ y) \in \mathcal{N}$, hence we obtain

$$\begin{aligned}(a \circ x)_{\mathcal{N}} &= (a \circ x \circ a \circ y)_{\mathcal{N}} := (a)_{\mathcal{N}} \circ (x)_{\mathcal{N}} \circ (a)_{\mathcal{N}} \circ (y)_{\mathcal{N}} \\ &= (a^2)_{\mathcal{N}} \circ (x)_{\mathcal{N}} \circ (y)_{\mathcal{N}} = (a^2 \circ x)_{\mathcal{N}} \circ (y)_{\mathcal{N}} = (z)_{\mathcal{N}} \circ (y)_{\mathcal{N}} \\ &= (a)_{\mathcal{N}} \circ (y)_{\mathcal{N}} \text{ (since } a \in (z)_{\mathcal{N}}) \\ &= (a \circ y)_{\mathcal{N}}.\end{aligned}$$

Hence $a \circ y \subseteq (a \circ y)_{\mathcal{N}} = (a \circ x)_{\mathcal{N}} = (z)_{\mathcal{N}}$. Since T is a hyperfilter of H, $a \in T$ and $a \in (z)_{\mathcal{N}}$, by Remark 2.7, we have $(z)_{\mathcal{N}} \subseteq T$. Thus we have

$$I \subseteq F = T \cap I \supseteq (z)_{\mathcal{N}} \cap I = I,$$

and then $F = I$. □

By Proposition 2.5 and Theorem 2.8 we have the following

Corollary 2.9. *If H is an ordered hypersemigroup, $z \in H$ and I a hyperideal of $(z)_{\mathcal{N}}$, then I does not contain proper prime hyperideals (of I).*

Theorem 2.10. *Let H be an ordered hypersemigroup and I a prime hyperideal of H. Then we have $I = \bigcup_{x \in I} \{(x)_{\mathcal{N}} \mid x \in I\}$.*

Proof. Let $t \in (x)_{\mathcal{N}}$ for some $x \in I$. Since $(x)_{\mathcal{N}}$ is a hyperideal of (the hypersemigroup) $(x)_{\mathcal{N}}$, by Corollary 2.9, $(x)_{\mathcal{N}}$ does not contain proper prime hyperideals. We prove that $(x)_{\mathcal{N}} \cap I$ is a prime hyperideal of $(x)_{\mathcal{N}}$. Then we get $(x)_{\mathcal{N}} \cap I = (x)_{\mathcal{N}}$, and then $t \in I$. First of all, $(x)_{\mathcal{N}} \cap I$ is a nonempty subset of $(x)_{\mathcal{N}}$ and this is because $x \in (x)_{\mathcal{N}}$ and $x \in I$. Moreover we have

$$\begin{aligned}(x)_{\mathcal{N}} \circ ((x)_{\mathcal{N}} \cap I) &\subseteq (x)^2_{\mathcal{N}} \cap (x)_{\mathcal{N}} \circ I = (x^2)_{\mathcal{N}} \cap (x)_{\mathcal{N}} \circ I \\ &= (x)_{\mathcal{N}} \cap (x)_{\mathcal{N}} \circ I \subseteq (x)_{\mathcal{N}} \cap H \circ I \\ &\subseteq (x)_{\mathcal{N}} \cap I\end{aligned}$$

and $((x)_{\mathcal{N}} \cap I) \circ (x)_{\mathcal{N}} \subseteq (x)^2_{\mathcal{N}} \cap I \circ (x)_{\mathcal{N}} \subseteq (x)_{\mathcal{N}} \cap I \circ H \subseteq (x)_{\mathcal{N}} \cap I$. In addition, if $a \in (x)_{\mathcal{N}} \cap I$ and $b \in (x)_{\mathcal{N}}$ such that $b \leq a$ then, since $b \leq a \in I$ and I is a hyperideal of H, we have $b \in I$. Thus we have $b \in (x)_{\mathcal{N}} \cap I$.

Let now $y, z \in (x)_{\mathcal{N}}$ such that $y \circ z \subseteq (x)_{\mathcal{N}} \cap I$. Since $y \circ z \subseteq I$ and I is a prime hyperideal of H, we have $y \in I$ or $z \in I$. Hence $y \in (x)_{\mathcal{N}} \cap I$ or $z \in (x)_{\mathcal{N}} \cap I$ and the proof is complete. □

References

[1] **T. Changphas, B. Davvaz**, *Properties of hyperideals in ordered semihypergroups*, Ital. J. Pure Appl. Math. **33** (2014), 425 – 432.

[2] **P. Corsini**, *Hypergroupes et groupes ordonnés*, (French) Univ. Genova Pubbl. Ist. Mat. (2) No. 21 (1972), 1 – 23.

[3] **B. Davvaz**, *Semihypergroup Theory*, Elsevier, 2016.

[4] **B. Davvaz, A. Dehghan-Nezhad**, *Chemical examples in hypergroups*, Ratio Matematica **14** (2003), 71 – 74.

[5] **D. Heidari, B. Davvaz**, *On ordered hyperstructures*, Politehn. Univ. Bucharest Sci. Bull. Ser. A Appl. Math. Phys. **73** (2011), 85 – 96.

[6] **N. Kehayopulu**, *Remark on ordered semigroups*, Math. Japon. **35** (1990), 1061 – 1063.

[7] **S. Lekkoksung**, *On weakly semi-prime hyperideals in semihypergroups*, Int. J. Algebra **6** (2012), 613 – 616.

[8] **J. Mittas**, *Sur une classe d'hypergroupes commutatifs*, C. R. Acad. Sci. Paris Sér. A-B **269** (1969), $A485 - A488$.

[9] **J. Mittas**, *Hypergroupes et hyperanneaux polysymétriques*, C. R. Acad. Sci. Paris Sér. A-B **271** (1970), $A920 - A923$.

[10] **J. Mittas**, *Hypergroupes canoniques valués et hypervalués*, Math. Balkanica **1** (1971), 181 – 185.

[11] **M. Petrich**, *Introduction to Semigroups*, Merrill Research and Lecture Series. Charles E. Merrill Publishing Co., 1973.

[12] **B. Pibaljommee, K. Wannatong, B. Davvaz**, *An investigation on fuzzy hyperideals of ordered semihypergroups*, Quasigroups Related Systems **23** (2015), 297 – 308.

Received February 25, 2018

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

Quasigroups and Related Systems **26** (2018), 87 – 102

Symmetry groups and Graovac–Pisanski index of some linear polymers

Fatemeh Koorepazan-Moftakhar, Ali Reza Ashrafi and Ottorino Ori

Abstract. Suppose G is a graph with vertex set $V(G)$. The Graovac–Pisanski index of G is defined as $GP(G) = \frac{1}{2}|V(G)|^2\delta(G)$, where

$$\delta(G) = \frac{1}{|\Gamma||V(G)|}\sum_{u\in V(G)}\sum_{g\in\Gamma} d(u, g(u)).$$

This is a type of graph invariant that is combined distance and symmetry of molecules under consideration. The aim of this paper is to compute the symmetry groups and Graovac–Pisanski index of some linear polymers.

1. Introduction

Throughout this paper all graphs will be assumed to be simple and undirected. This means that they don't have loops, multiple and directed edges. Suppose G is such a graph with vertex set $V(G)$ and edge set $E(G)$. An edge $e \in E(G)$ will be written as $e = xy$, where $x, y \in V(G)$. A graph G is called *r-regular* if degrees of all vertices are equal to r.

The *molecular graph* of a molecule M is a simple graph in which atoms and chemical bonds are in one-to-one correspondences with vertices and edges, respectively. A *path* P_n is a sequence $x_1, x_2, \ldots, x_n$ of different vertices in which x_i and x_{i+1}, $1 \leqslant i \leqslant n-1$, are adjacent. The number of edges in a path is called its length. A *cycle graph* C_n is a graph constructed from the path P_n by adding a new edge x_1x_n. The *complete graph* K_n is an $n-$vertex graph in which all pairs of different vertices are adjacent. A graph G is *connected* if for each vertex x, y in G, there exists a path connecting them.

A *permutation* on a set X is a one-to-one function from X onto X. The set of all permutations on a set X is denoted by S_X. It is well-known that S_X is a group under composition of functions. The order of an element x in a group G is denoted by $O(x)$. An element $\theta \in S_{V(G)}$ is said to be an *automorphism* if the following condition is satisfied:

$$\forall x, y \in V(G) \quad xy \in E(G) \Longleftrightarrow \theta(x)\theta(y) \in E(G).$$

2010 Mathematics Subject Classification: 05C12, 20B25.
Keywords: Automorphism group, Graovac–Pisanski index, linear polymer, Wiener index.
The research of the first and second authors are partially supported by the University of Kashan under grant no 785149/1.

The set of all automorphisms of G is denoted by $Aut(G)$ which is a group under composition of functions. It is easy to see that $Aut(G)$ is a subgroup of $S_{V(G)}$. The graph G is called *vertex-transitive* if and only if for each $x, y \in V(G)$ there exists an automorphism $g \in Aut(G)$ such that $g(x) = y$. It is easy to see that vertex-transitive graphs are regular. We refer the interested readers to the famous book of Biggs [3], for more information on this topic.

Suppose G is a group containing two subgroups H and K in such a way that $H \trianglelefteq G$, $|H \cap K| = 1$ and $G = HK = \{xy \mid x \in H,\ y \in K\}$. Then we say that G is a *semi-direct product* of H by K and write $G = H : K$. For an example, we consider the set of all permutations on $X = \{1, 2, 3\}$, i.e., $S_X = \{(), (1,2,3), (1,3,2), (1,2), (1,3), (2,3)\}$, where () is the identity permutation. Then by choosing $H = \{(), (1,2,3),\ (1,3,2)\}$ and $K = \{(), (1,2)\}$, we can see that $H \trianglelefteq S_X$, $K \leqslant S_X$, $|H \cap K| = 1$ and $S_X = HK$. Hence, S_X can be written as the semi-direct product $H : K$ of its subgroups.

Suppose G is a graph and $x, y \in V(G)$. The length of a minimum path connecting x and y is denoted by $d(x, y)$. It is easy to see that $(V(G), d)$ is a metric space with distance function $d(-,-)$. If G is connected then the *Wiener index* $W(G)$ is defined as the sum of distances between all pairs of vertices in G [18].

Graovac and Pisanski [8] in an innovating work applied the symmetry group of the graph under consideration to generalize the Wiener index and obtain a good correlation with some physico-chemical properties of molecules. To explain, we assume that G is a graph, $\Gamma \leqslant Aut(G)$ and $g \in \Gamma$. Define the *distance number* of g, $\delta(g)$, to be the average of $d(u, g(u))$ overall vertices $u \in V(G)$ and $\delta(G) = \frac{1}{|\Gamma|}\sum_{g\in G}\delta(g) = \frac{1}{|\Gamma||V(G)|}\sum_{u\in V(G)}\sum_{g\in\Gamma} d(u, g(u))$. The *Graovac–Pisanski index* (GP index for short) of G with respect to Γ, $GP_\Gamma(G)$, is defined as $GP_\Gamma(G) = \frac{|V(G)|^2}{2|\Gamma|}\sum_{g\in\Gamma}\delta(g)$. If $\Gamma = Aut(G)$ then we write $GP(G)$ as $GP_\Gamma(G)$. It is easy to see that the GP index of G can be computed by $GP(G) = \frac{1}{2}|V(G)|^2\delta(G)$. Ashrafi and Shabani [2] computed the GP index of graphs that can be represented as some graph operations and in [12], some upper and lower bounds for this graph invariant are presented. In 2016, Ghorbani and Klavžar [7] computed this topological index by cut method and Tratnik [17] generalized their method and calculated the closed formulas for the GP index of zig-zag tubulenes. In [13], the GP index of the cycle C_n with respect to all subgroups of $Aut(C_n)$ and the GP index of $(3,6)-$ and $(5,6)-$fullerene graphs with respect to a subgroup of their symmetry groups are computed. Finally in [15], the Graovac-Pisanski polynomial of a graph was presented by which the authors extended some well-known results from Hosoya polynomial to its symmetry-based version. In the mentioned paper, this polynomial for some classes of chemical graphs containing linear phenylene and its hexagonal squeeze, and the ortho-, meta- and para-polyphenylene chains were calculated.

Phenylenes are polycyclic conjugated molecules possessing both six- and four-membered rings [9]. Following Došlić and Litz [5], a polymer with phenylene as the basic building block is called a polyphenylene. In the mentioned paper, some

exact formulas for the numbers of matchings and independent sets in three types of uniform chains are given. The authors also presented some results on polyphenylene dendrimers. In this paper, the GP index of the molecular graphs presented in [6, 9] are computed. Our calculations are done with the aid of TopoCluj [4], HyperChem [11] and GAP [16]. Our group theory notations are standard and can be taken mainly from [1, 10, 14, 16].

2. Main result

The aim of this section is to compute the symmetry groups, their orbits and GP index of the para chain of length n, 3−uniform cactus chain, caterpilar $CAT(n_1, \ldots, n_r)$, corona product $P_n \circ P_2$, an ortho-chain of length n, ladder graph L_n and the 2−connected linear polymer with triangular faces R_n. These graphs will be defined later. We start by computing the GP index of a para chain of length n, Figure 1.

Suppose G is a group and X is a set. An action of G on X is a function $\star : G \times X \longrightarrow X$ such that for all $g, h \in G$ and $x \in X$, $e \star x = x$ and $(gh) \star x = g \star (h \star x)$. The orbit of an element $x \in X$ is defined as $G \star x = \{g \star x \mid g \in G\}$. We usually write gx as $g \star x$ when there is no confusion. The size of an orbit is called its length.

Let G be a connected graph, $A \cup B \subseteq V(G)$ and $V_1, V_2, \ldots, V_r$ be the orbits of $Aut(G)$ under its natural action on $V(G)$. Define $d(A, B) = \sum_{u \in A} \sum_{v \in B} d(u, v)$. Then it can easily seen that $W(G) = \frac{1}{2} d(V, V)$. Graovac and Pisanski [8], proved that $GP(G) = |V| \sum_{i=1}^{r} \frac{W(V_i)}{|V_i|}$, where $W(V_i) = \frac{1}{2} d(V_i, V_i)$. We apply this result to compute the GP index of all polymers presented in this paper.

Theorem 2.1. *The Graovac-Pisanski index of a para chain Q_n of length n can be computed as follows:*

$$GP(Q_n) = \begin{cases} \frac{9}{4}n^3 + \frac{15}{4}n^2 + \frac{7}{4}n + \frac{1}{4} & n \text{ is odd and } n \neq 1, \\ \frac{9}{4}n^3 + \frac{15}{4}n^2 + n & n \text{ is even.} \end{cases}$$

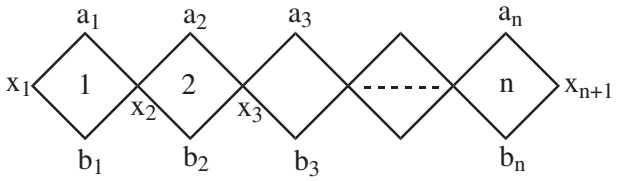


Figure 1: A para chain of length n.

Proof. The case of $n = 1$ is clear. Suppose $n > 1$ is even and consider the subset $X = \{x_1, x_2, \ldots, x_{n+1}\} \subseteq V(Q_n)$, see Figure 1. It is easy to see that for each automorphism α, $\alpha(\{x_1, x_{n+1}\}) = \{x_1, x_{n+1}\}$. Hence ($\alpha(x_1) = x_1$ and $\alpha(x_{n+1}) = x_{n+1}$) or ($\alpha(x_1) = x_{n+1}$ and $\alpha(x_{n+1}) = x_1$). If $\alpha(x_1) = x_1$ and $\alpha(x_{n+1}) = x_{n+1}$ then by definition of graph automorphism, $\alpha|_X = ()$, where $\alpha|_X$ denotes the restriction of α on the set X and $()$ is the identity permutation. If $\alpha(x_1) = x_{n+1}$ and $\alpha(x_{n+1}) = x_1$ then $\alpha|_X = (x_1\ x_{n+1})(x_2\ x_n)\ldots(x_{\frac{n}{2}}\ x_{\frac{n+4}{2}})$. Define $H = \langle (a_1\ b_2), \ldots, (a_n\ b_n)\rangle$. There are two permutations β_1 and β_2 induced by the unique automorphism of order two in the path graph P_{n+1} with vertex set $V(P_{n+1}) = \{1, 2, \ldots, n+1\}$ and edge set $E(P_{n+1}) = \{12, 23, 34, 45, \ldots, (n)(n+1)\}$. These permutations can be defined as follows:

$$\beta_1 = \begin{cases} (a_1\ a_n)(a_2\ a_{n-1})\ldots(a_{\frac{n}{2}}\ a_{\frac{n+2}{2}}) & 2 \mid n. \\ (a_1\ a_n)(a_2\ a_{n-1})\ldots(a_{\frac{n-1}{2}}\ a_{\frac{n+3}{2}})\ 2 \nmid n, \end{cases},$$

$$\beta_2 = \begin{cases} (b_1\ b_n)(b_2\ b_{n-1})\ldots(b_{\frac{n}{2}}\ b_{\frac{n+2}{2}}) & 2 \mid n, \\ (b_1\ b_n)(b_2\ b_{n-1})\ldots(b_{\frac{n-1}{2}}\ b_{\frac{n+3}{2}})\ 2 \nmid n. \end{cases}$$

It is now easy to prove $\gamma = \alpha\beta_1\beta_2$ is an automorphism of order 2 in Q_n. Define $K = \langle\gamma\rangle$. Since all generators of H has order two and they are disjoint permutations,

$$H \cong \underbrace{Z_2 \times \cdots \times Z_2}_{n\ times}.$$

It is clear $|H \cap K| = 1$ and for each element $t \in X$ and each automorphism $\gamma \in H$, $\gamma(t) = t$. Thus, $H \trianglelefteq Aut(Q_n)$. If an automorphism $\gamma \in Aut(Q_n)$ fixes elementwise each element of X then $\gamma \in H$ and in other case γ can be written as the product of an element of H by $\alpha\beta_1\beta_2$. This proves that $G = H : K \cong (Z_2 \times \cdots \times Z_2) : Z_2$. Therefore, the automorphism group of Q_n can be generated by automorphisms γ and $(a_i\ b_i)$, for $1 \leqslant i \leqslant n$. A similar argument shows that, when n is odd, the group $Aut(Q_n)$ can be generated by $\alpha\beta_1\beta_2$ and n permutations $(a_i\ b_i)$ for $1 \leqslant i \leqslant n$. Therefore,

$$Aut(Q_n) \cong \begin{cases} \underbrace{(Z_2 \times \cdots \times Z_2)}_{\text{n times}} : Z_2 & \text{n is even,} \\ Z_2 \times \left(\underbrace{(Z_2 \times \cdots \times Z_2)}_{\text{n-1 times}} : Z_2 \right) & \text{n is odd and } n \neq 1. \end{cases}$$

This proves that $|Aut(Q_n)| = 2^{n+1}$, $n \neq 1$, and $Aut(Q_1) \cong D_8$. If n is even, then the orbits of $Aut(Q_n)$ on $V(Q_n)$ are $V_1 = \{x_1, x_{n+1}\}$, $V_2 = \{a_1, b_1, a_n, b_n\}$, $V_3 = \{x_2, x_n\}$, $V_4 = \{a_2, b_2, a_{n-1}, b_{n-1}\}$, $V_5 = \{x_3, x_{n-1}\}$, ..., $V_{n-1} = \{x_{n/2}, x_{n/2+2}\}$, $V_n = \{a_{n/2}, a_{n/2+1}, b_{n/2}, b_{n/2+1}\}$ and $V_{n+1} = \{x_{n/2+1}\}$. If n is odd and $n \neq 1$, then the orbits of $Aut(Q_n)$ on $V(Q_n)$ will be $U_1 = \{x_1, x_{n+1}\}$,

$U_2 = \{a_1, b_1, a_n, b_n\}$, $U_3 = \{x_2, x_n\}$, $U_4 = \{a_2, b_2, a_{n-1}, b_{n-1}\}$, ..., $U_{n-1} = \{a_{(n-1)/2}, b_{(n-1)/2}, a_{(n+3)/2}, b_{(n+3)/2}\}$, $U_n = \{x_{(n+1)/2}, x_{(n+3)/2}\}$ and $U_{n+1} = \{a_{(n+1)/2}, b_{(n+1)/2}\}$. To compute the Graovac-Pisanski index of this graph, we consider the following cases:

1. n is even. In this case, $Aut(Q_n)$ has exactly $n+1$ orbits under its natural action on $V(Q_n)$. Since $|V_{n+1}| = 1$, $W(V_{n+1}) = 0$. On the other hand, we have exactly $\frac{n}{2}$ orbits of size 2 and $\frac{n}{2}$ orbits of size 4. Now a simple calculation shows that $W(V_1) = 2n$, $W(V_2) = 8n-4$, ..., $W(V_{n-3}) = 8$, $W(V_{n-2}) = 28$, $W(V_{n-1}) = 4$ and $W(V_n) = 4$. Therefore,

$$\begin{aligned} GP(Q_n) &= |V| \sum_{i=1}^{n+1} \frac{W(V_i)}{|V_i|} \\ &= (3n+1)\left(\frac{4+8+\cdots+2n}{2} + \frac{12+28+\cdots+8n-4}{4}\right) \\ &= \frac{9}{4}n^3 + \frac{15}{4}n^2 + n. \end{aligned}$$

2. n is odd and $n \neq 1$. In this case, again $Aut(Q_n)$ has exactly $n+1$ orbits under its natural action on $V(Q_n)$. On the other hand, by above calculations $\frac{n+3}{2}$ orbits have length 2 and other orbits have length 4. For orbits of length 2, we have $W(U_{n+1}) = 2$, $W(U_n) = 2$, $W(U_{n-2}) = 6$, ..., $W(U_1) = 2n$, and for orbits of length 4, $W(U_{n-1}) = 20$, $W(U_{n-3}) = 36$, ..., $W(U_2) = 8n-4$. Therefore,

$$\begin{aligned} GP(Q_n) &= |V| \sum_{i=1}^{n+1} \frac{W(V_i)}{|V_i|} \\ &= (3n+1)\left(\frac{2}{2} + \frac{2+6+\ldots+2n}{2} + \frac{20+36+\ldots+8n-4}{4}\right) \\ &= \frac{9}{4}n^3 + \frac{15}{4}n^2 + \frac{7}{4}n + \frac{1}{4}. \end{aligned}$$

This completes the proof. □

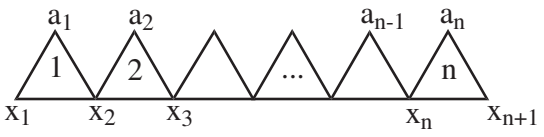


Figure 2: A 3-uniform cactus chain T_n.

Theorem 2.2. *The Graovac-Pisanski index of a 3-uniform cactus chain T_n, Figure 2, can be computed as follows:*

$$GP(T_n) = \begin{cases} \frac{1}{2}n^3 + \frac{5}{4}n^2 + n + \frac{1}{4} & n \text{ is odd and } n \neq 1, \\ \frac{1}{2}n^3 + \frac{5}{4}n^2 + \frac{3}{2}n + \frac{1}{2} & n \text{ is even.} \end{cases}$$

Proof. If n is odd and $n \neq 1$, then the automorphism group of T_n can be generated by $(x_1\ a_n)(a_1\ x_{n+1})\ (x_2\ x_n)(x_3\ x_{n-1})\cdots(x_{\frac{n+1}{2}}\ x_{\frac{n+3}{2}})(a_2\ a_{n-1})\cdots(a_{\frac{n-1}{2}}\ a_{\frac{n+3}{2}})$, $(x_1\ a_1)$ and $(a_n\ x_{n+1})$. Moreover, if n is even, then $Aut(T_n)$ is generated by $\alpha = (x_1\ a_n)(a_1\ x_{n+1})(x_2\ x_n)\cdots(x_{\frac{n}{2}}\ x_{\frac{n}{2}+2})(a_2\ a_{n-1})\cdots(a_{\frac{n}{2}}\ a_{\frac{n}{2}+1})$ and $\beta = (x_1\ a_1)$. Since $\alpha\beta \neq \beta\alpha$ and $\alpha\beta$ has order 4, $Aut(T_n) \cong D_8$. Note that two non-commuting elements δ and τ of order two generate a dihedral group of order $2O(\delta\tau)$. Therefore,

$$Aut(T_n) \cong \begin{cases} S_3 & n = 1 \\ D_8 & n \neq 1 \end{cases}.$$

To compute the GP index of T_n, we first calculate the orbits of $Aut(T_n)$ under its natural action on $V(T_n)$. If n is even, then $Aut(T_n)$ has exactly n orbits containing one orbit of length 1, one orbit of length 4 and $n-2$ orbits of length 2. These are $V_1 = \{x_{\frac{n}{2}+1}\}$, $V_2 = \{a_1, x_1, a_n, x_{n+1}\}$, $V_i = \{x_i, x_{n-i+2}\}$ and $V_i' = \{a_i, a_{n-i+1}\}$, $2 \leqslant i \leqslant \frac{n}{2}$. Our calculations show that $W(V_1) = 0$, $W(V_2) = 4n+2$ and $W(V_i) = W(V_i') = n - 2i + 2$, $2 \leqslant i \leqslant \frac{n}{2}$. Therefore,

$$\begin{aligned} GP(T_n) &= |V| \sum_{i=1}^{n} \frac{W(V_i)}{|V_i|} \\ &= (2n+1)\left(\frac{4n+2}{4} + \frac{1}{2} \times 2 \times (2 + 4 + \cdots + (n-2))\right) \\ &= \frac{1}{2}n^3 + \frac{5}{4}n^2 + \frac{3}{2}n + \frac{1}{2}. \end{aligned}$$

We now assume that n is odd. Then we have one orbit of length 1, one orbit of length 4 and $n-2$ orbits of length 2. These are $U_1 = \{a_{\frac{n+1}{2}}\}$, $U_2 = \{a_1, x_1, a_n, x_{n+1}\}$, $U_3 = \{x_{\frac{n+1}{2}}, x_{\frac{n+3}{2}}\}$, $U_4 = \{x_2, x_n\}$, $U_5 = \{a_2, a_{n-1}\}$, $U_6 = \{x_3, x_{n-1}\}$, $U_7 = \{a_3, a_{n-2}\}$, $\ldots$, $U_{n-1} = \{a_{\frac{n-1}{2}}, a_{\frac{n+3}{2}}\}$ and $U_n = \{x_{\frac{n-1}{2}}, x_{\frac{n+5}{2}}\}$. By our calculations, $W(U_1) = 0$, $W(U_2) = 4n+2$, $W(U_3) = 1$, $W(U_4) = W(U_5) = n-2$, $W(U_6) = W(U_7) = n-4$, $\ldots$, $W(U_{n-1}) = W(U_n) = 3$. Therefore,

$$\begin{aligned} GP(T_n) &= |V| \sum_{i=1}^{n} \frac{W(V_i)}{|V_i|} \\ &= (2n+1)\left(\frac{4n+2}{4} + \frac{1}{2} + \frac{1}{2} \times 2 \times (3 + 5 + \cdots + (n-2))\right) \\ &= \frac{1}{2}n^3 + \frac{5}{4}n^2 + n + \frac{1}{4}, \end{aligned}$$

which completes our proof. □

The *caterpilar* $CAT(n_1, \ldots, n_r)$ is a tree with vertex set

$$\underbrace{\{v_1, \ldots, v_r\}}_{A} \cup \underbrace{\{v_{11}, \ldots, v_{1n_1}\}}_{A_1} \cup \ldots \cup \underbrace{\{v_{r1}, \ldots, v_{rn_r}\}}_{A_r}$$

in which A is the vertex set for a path v_1, v_2, ..., v_r and A_i, $1 \leqslant i \leqslant r$, is a set of pendant vertices that all of them are adjacent with v_i, see Figure 3.

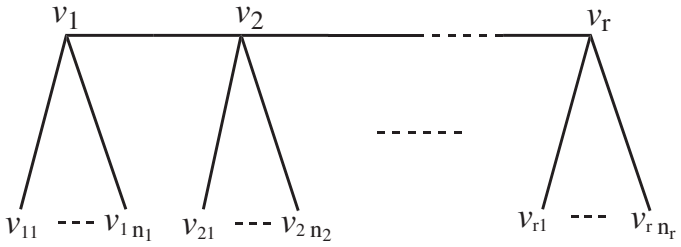


Figure 3: The caterpilar $CAT(n_1, \ldots, n_r)$.

Theorem 2.3. *The Graovac-Pisanski index of* $CAT(n_1, \ldots, n_r)$ *can be computed as follows:*

(1) *If for some* i *and* j *with* $i + j = r + 1$, *we have* $n_i \neq n_j$ *then*

$$GP(CAT(n_1, \ldots, n_r)) = \left(\sum_{i=1}^{r} n_i\right)^2 - r^2.$$

(2) *If* $n_1 = n_2 = \cdots = n_r = n$, *then*

$$GP(CAT(n, \ldots, n)) = \begin{cases} f(n,r) & r \text{ is even}, \\ \\ g(n,r) & r \text{ is odd}, \end{cases}$$

where $f(n,r) = \left(\frac{1}{8}r^3 + r^2\right)n^2 + \left(\frac{1}{2}r^2 + \frac{1}{4}r^3\right)n - \frac{1}{2}r^2 + \frac{1}{8}r^3$ *and*

$$g(n,r) = \left(\frac{1}{8}r^3 + r^2 - \frac{1}{8}r\right)n^2 + \left(-\frac{3}{4}r + \frac{1}{2}r^2 + \frac{1}{4}r^3\right)n - \frac{5}{8}r - \frac{1}{2}r^2 + \frac{1}{8}r^3.$$

Proof. Set $\mathcal{L} = CAT(n_1, \ldots, n_r)$ and P is the induced subgraph of A. It is easy to see that $S_{A_i} \leqslant Aut(\mathcal{L})$, $1 \leqslant i \leqslant r$. Since $A_i \cap A_j = \emptyset$, $1 \leqslant i \neq j \leqslant r$, one can easily seen that $S_{A_1} S_{A_2} \ldots S_{A_r} \cong S_{A_1} \times S_{A_2} \times \cdots \times S_{A_r}$ and so $Aut(\mathcal{L})$ has a subgroup H isomorphic to $S_{A_1} \times S_{A_2} \times \cdots \times S_{A_r}$. Our main proof will consider two separate cases as follows:

1. Suppose for some i and j with $i+j=r+1$, we have $n_i \neq n_j$. From Figure 3, one can easily seen that $H = Aut(\mathcal{L})$ and H has exactly $2r$ orbits under its natural action on $V(\mathcal{L})$. These orbits are $\{v_1\}$, $\{v_2\}$, ..., $\{v_r\}$ and A_1, ..., A_r. Since $W(A_i) = {n_i}^2 - n_i$, $|A_i| = n_i$ and $|V| = r + \sum_{i=1}^{r} n_i$,

$$\begin{aligned} GP(\mathcal{L}) &= |V| \sum_{i=1}^{2r} \frac{W(V_i)}{|V_i|} \\ &= \left(r + \sum_{i=1}^{r} n_i\right)\left(\sum_{i=1}^{r} \frac{{n_i}^2 - n_i}{n_i}\right) \\ &= \left(\sum_{i=1}^{r} n_i\right)^2 - r^2. \end{aligned}$$

2. $n_1 = n_2 = \cdots = n_r = n$. Choose f to be the automorphism of order 2 in $Aut(P)$ and extend f to an automorphism $\overline{f}$ of $\mathcal{L}$ by defining $f(x) = x$, for each $x \in \bigcup_{i=1}^{r} A_i$. If r is even then $Aut(\mathcal{L}) = H \cup \overline{f}H$ and so $Aut(\mathcal{L}) \cong (S_{A_1} \times S_{A_2} \times \cdots \times S_{A_r}) : Z_2$. Furthermore, $Aut(\mathcal{L})$ can be generated by $(v_{i1}\ v_{i2})$, $(v_{i1}\ v_{i3})$, ..., $(v_{i1}\ v_{in_i})$ and $\prod(v_i\ v_j)(v_{i1}\ v_{j1})(v_{i2}\ v_{j2})(v_{i3}\ v_{j3})\cdots(v_{in_i}\ v_{jn_i})$, where $1 \leqslant i \leqslant \frac{n}{2}$, $\frac{n}{2}+1 \leqslant j \leqslant n$ and $i+j=r+1$. Therefore, $Aut(\mathcal{L})$ has exactly r orbits such that $\frac{r}{2}$ of them have length 2 and others have length $2n$. These are $V_i = \{v_i, v_j\}$ and $V_i' = \{v_{i1}, v_{i2}, v_{i3}, \ldots, v_{in}, v_{j1}, v_{j2}, v_{j3}, \ldots, v_{jn}\}$, where $1 \leqslant i \leqslant \frac{r}{2}$, $\frac{r}{2}+1 \leqslant j \leqslant r$ and $i+j=r+1$. Our calculations show that, $W(V_i) \in \{1, 3, 5, 7, \ldots, r-1\}$ and $W(V_i') \in \{5n^2 - 2n, 5n^2 - 2n + 2n^2, \ldots, (r+3)n^2 - 2n\}$, where $1 \leqslant i \leqslant \frac{r}{2}$. Therefore,

$$\begin{aligned} GP(\mathcal{L}) &= |V| \sum_{i=1}^{r} \frac{W(V_i)}{|V_i|} \\ &= (n+1)r\left[\frac{1+3+\cdots+r-1}{2} + \frac{5n^2 - 2n + \cdots + (r+3)n^2 - 2n}{2n}\right] \\ &= \left(\frac{1}{8}r^3 + r^2\right)n^2 + \left(\frac{1}{2}r^2 + \frac{1}{4}r^3\right)n - \frac{1}{2}r^2 + \frac{1}{8}r^3. \end{aligned}$$

If r is odd then $S_{A_{\frac{r+1}{2}}}$ will be a characteristic subgroup and

$$\begin{aligned} Aut(\mathcal{L}) &\cong \left[\left(S_{A_1} \times S_{A_2} \times \cdots \times S_{A_{\frac{r-1}{2}}} \times S_{A_{\frac{r+3}{2}}} \times \cdots \times S_{A_r}\right) : Z_2\right] \times S_{A_{\frac{r+1}{2}}} \\ &\cong \left[\underbrace{(S_n \times S_n \times \cdots \times S_n \times S_n \times \cdots \times S_n)}_{\text{r-1 times}} : Z_2\right] \times S_n. \end{aligned}$$

Moreover, $Aut(\mathcal{L})$ can be generated by $(v_{i1}\ v_{i2})$, ..., $(v_{i1}\ v_{in_i})$ and $\prod(v_i\ v_j)$ $(v_{i1}\ v_{j1})\cdots(v_{in_i}\ v_{jn_i})$, where $1 \leqslant i \leqslant \frac{n-1}{2}$, $\frac{n+3}{2} \leqslant j \leqslant n$ and $i+j=r+1$. On the other hand, $Aut(\mathcal{L})$ has exactly $r+1$ orbits, one orbit of length 1,

one orbit of length n, $\frac{r-1}{2}$ orbits of length 2, and $\frac{r-1}{2}$ orbits of length $2n$. These are $U_1 = \{v_{\frac{r+1}{2}}\}$, $U_2 = \{v_{\frac{r+1}{2}1}, v_{\frac{r+1}{2}2}, \cdots, v_{\frac{r+1}{2}n}\}$, $U_i = \{v_i, v_j\}$ and $U_i' = \{v_{i1}, v_{i2}, \ldots, v_{in}, v_{j1}, v_{j2}, \ldots, v_{jn}\}$, where $1 \leqslant i \leqslant \frac{r-1}{2}$, $\frac{r+3}{2} \leqslant j \leqslant r$ and $i + j = r + 1$. By our calculations, $W(U_1) = 0$, $W(U_2) = n(n-1)$, $W(U_i) \in \{2, 4, \ldots, r-1\}$ and $W(U_i') \in \{6n^2-2n, 8n^2-2n, \ldots, (r+3)n^2-2n\}$. Therefore,

$$\begin{aligned} GP(\mathcal{L}) &= |V| \sum_{i=1}^{r+1} \frac{W(V_i)}{|V_i|} \\ &= (n+1)r \left[\frac{n(n-1)}{n} + \frac{2+4+\cdots+r-1}{2} \right. \\ &\qquad \left. + \frac{6n^2-2n+\cdots+(r+3)n^2-2n}{2n} \right] \\ &= \left(\frac{1}{8}r^3 + r^2 - \frac{1}{8}r\right) n^2 + \left(-\frac{3}{4}r + \frac{1}{2}r^2 + \frac{1}{4}r^3\right) n - \frac{5}{8}r - \frac{1}{2}r^2 + \frac{1}{8}r^3. \end{aligned}$$

This completes our argument. □

Note that our previous theorem covers the case when for some i, j with $i + j = r + 1$, n_i is not equal to n_j and another case when all n_i are the same. It is easy to see that $Aut(\mathcal{L}) = H$ or $H : Z_2$. For example, we do not cover the case that $CAT(2, 3, 4, 3, 2)$. Our method shows that $Aut(CAT(2, 3, 4, 3, 2)) \cong (Z_2 \times S_3 \times S_4 \times S_3 \times Z_2) : Z_2$ and a simple GAP program shows that in this case $GP(\mathcal{L}) = 399$.

Suppose G and H are two graphs. The *corona product* $G \circ H$ is a graph constructed from G and $|V(G)|$ copies of H by connecting the i^{th} vertex of G to each vertex of the i^{th} copy of H, $1 \leqslant i \leqslant |V(G)|$.

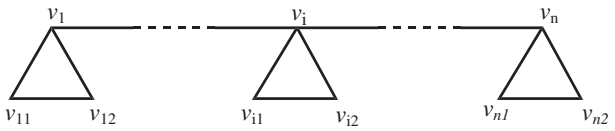


Figure 4: The corona product $P_n \circ P_2$.

Theorem 2.4. *The Graovac-Pisanski index of $P_n \circ P_2$, Figure 4, can be computed by the following formula:*

$$GP(P_n \circ P_2) = \begin{cases} \frac{9}{8}n^3 + \frac{15}{4}n^2 & n \text{ is even}, \\ \frac{9}{8}n^3 + \frac{15}{4}n^2 - \frac{27}{8}n & n \text{ is odd}, \\ 3 & n = 1. \end{cases}$$

Proof. Depending on whether n is an even or odd number, our proof will consider two cases.

1. n is even. In this case, the generators of $Aut(P_n \circ P_2)$ are $(v_{k1}\ v_{k2})$, $1 \leqslant k \leqslant n$, and $\prod(v_i\ v_j)(v_{i1}\ v_{j1})(v_{i2}\ v_{j2})$, $1 \leqslant i \leqslant \frac{n}{2}$, $\frac{n}{2}+1 \leqslant j \leqslant n$ and $i+j=n+1$. Our calculations show that the orbits of this action are $V_i = \{v_i, v_j\}$ and $V_i' = \{v_{i1}, v_{i2}, v_{j1}, v_{j2}\}$. Furthermore, $W(V_1) = n-1$, $W(V_2) = n-3$, ..., $W(V_{\frac{n}{2}}) = 1$, $W(V_1') = 4n+6$, $W(V_2') = 4n-2$, ..., $W(V_{\frac{n}{2}}') = 14$. Therefore,

$$\begin{aligned} GP(P_n \circ P_2) &= |V| \sum_{i=1}^{n} \frac{W(V_i)}{|V_i|} \\ &= 3n\left[\frac{1+3+\cdots+n-1}{2} + \frac{14+22+30+\cdots+4n+6}{4}\right] \\ &= \frac{9}{8}n^3 + \frac{15}{4}n^2. \end{aligned}$$

2. n is odd. The generators of $Aut(P_n \circ P_2)$ are $(v_{k1}\ v_{k2})$, $1 \leqslant k \leqslant n$ and $\prod(v_i\ v_j)(v_{i1}\ v_{j1})(v_{i2}\ v_{j2})$, $1 \leqslant i \leqslant \frac{n-1}{2}$, $\frac{n+3}{2} \leqslant j \leqslant n$ and $i+j=n+1$. This group has exactly $n+1$ orbits under its natural action. These orbits are $U = \{v_{\frac{n+1}{2}}\}$, $U' = \{v_{\frac{n+1}{2}1}, v_{\frac{n+1}{2}2}\}$, $\frac{n+1}{2}$ orbits $U_i = \{v_i, v_j\}$ of size 2 and $\frac{n-1}{2}$ orbits $U_i' = \{v_{i1}, v_{i2}, v_{j1}, v_{j2}\}$ of size 4. Moreover, $W(U) = 0$, $W(U') = 1$, $W(U_1) = n-1$, $W(U_2) = n-3$, ..., $W(U_{\frac{n-1}{2}}) = 2$, $W(U_1') = 4n+6$, $W(U_2') = 4n-2$, ..., $W(U_{\frac{n-1}{2}}') = 18$. Therefore,

$$\begin{aligned} GP(P_n \circ P_2) &= |V| \sum_{i=1}^{n+1} \frac{W(V_i)}{|V_i|} \\ &= 3n\left[0 + \frac{1}{2} + \frac{2+4+\cdots+n-1}{2} + \frac{18+26+\cdots+4n+6}{4}\right] \\ &= \frac{9}{8}n^3 + \frac{15}{4}n^2 - \frac{27}{8}n. \end{aligned}$$

This completes the proof. □

Theorem 2.5. *The Graovac-Pisanski index of an ortho-chain O_n, Figures 5 – 7, of length n is computed as follows:*

$$GP(O_n) = \begin{cases} \frac{9}{8}n^3 + \frac{33}{8}n^2 + \frac{17}{4}n + 1 & n \text{ is even,} \\ \frac{9}{8}n^3 + \frac{33}{8}n^2 + \frac{19}{8}n + \frac{3}{8} & n \text{ is odd.} \end{cases}$$

Proof. There are two possible cases, depending on whether n is even or odd.

1. n is even. It can be proved that the automorphism group $Aut(O_n)$ is generated by the permutations $(1\ a_2)$, $(n+1\ b_{n-1})$ and $(a_1\ b_n)(1\ b_{n-1})(a_2\ n+1)(2\ n)(b_1\ a_n)(a_3\ b_{n-2})(3\ n-1)\ (b_2\ a_{n-1})(a_4\ b_{n-3})\cdots(\frac{n}{2}\ \frac{n}{2}+2)(b_{\frac{n}{2}-1}\ a_{\frac{n}{2}+2})$

$(a_{\frac{n}{2}+1}\ b_{\frac{n}{2}})$. Moreover, the group has exactly $\frac{3n}{2}$ orbits. These orbits are $U_1 = \{\frac{n}{2}+1\}$, $U_2 = \{a_{\frac{n}{2}+1}, b_{\frac{n}{2}}\}$, $U_3 = \{\frac{n}{2}, \frac{n}{2}+2\}$, $U_4 = \{a_{\frac{n}{2}}, b_{\frac{n}{2}+1}\}$, $U_5 = \{\frac{n}{2}-1, \frac{n}{2}+3\}$, $U_6 = \{b_{\frac{n}{2}-1}, a_{\frac{n}{2}+2}\}$, $U_7 = \{a_{\frac{n}{2}-1}, b_{\frac{n}{2}+2}\}$, $U_8 = \{\frac{n}{2}-2, \frac{n}{2}+4\}$, $U_9 = \{b_{\frac{n}{2}-2}, a_{\frac{n}{2}+3}\}$, ..., $U_{\frac{3n-10}{2}} = \{a_3, b_{n-2}\}$, $U_{\frac{3n-8}{2}} = \{2, n\}$, $U_{\frac{3n-6}{2}} = \{b_2, a_{n-1}\}$, $U_{\frac{3n-4}{2}} = \{b_1, a_n\}$, $U_{\frac{3n-2}{2}} = \{a_1, b_n\}$ and $U_{\frac{3n}{2}} = \{1, a_2, b_{n-1}, n+1\}$. On the other hand, $W(U_1) = 0$, $W(U_2) = W(U_3) = 2$, $W(U_4) = W(U_5) = W(U_6) = 4$, $W(U_7) = W(U_8) = W(U_9) = 6$, $W(U_{\frac{3n-10}{2}}) = W(U_{\frac{3n-8}{2}}) = W(U_{\frac{3n-6}{2}}) = n-2$, $W(U_{\frac{3n-4}{2}}) = n$, $W(U_{\frac{3n-2}{2}}) = n+2$ and $W(U_{\frac{3n}{2}}) = 4n+4$.

Therefore,

$$\begin{aligned} GP(O_n) &= |V| \sum_{i=1}^{\frac{3n}{2}} \frac{W(V_i)}{|V_i|} \\ &= (3n+1)\left[\frac{0}{1} + \frac{2+2}{2} + \frac{4+4+4}{2} + \frac{6+6+6}{2}\right. \\ &+ \left. \cdots + \frac{n-2+n-2+n-2}{2} + \frac{n}{2} + \frac{n+2}{2} + \frac{4n+4}{4}\right] \\ &= (3n+1)\left[0+2+\frac{3}{2}\left(\underbrace{4+6+\cdots+n-2}_{\frac{n-4}{2}}\right) + \frac{n}{2} + \frac{n+2}{2} + n + 1\right] \\ &= \frac{9}{8}n^3 + \frac{33}{8}n^2 + \frac{17}{4}n + 1. \end{aligned}$$

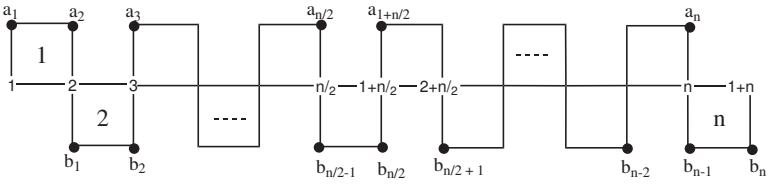


Figure 5: An ortho-chain of length n, n is even.

2. n is odd. The generators of $Aut(O_n)$ are $(1\ 1{+}n)(2\ n)\cdots(\frac{1+n}{2}\ \frac{3+n}{2})\,(a_1\ a_{1+n})\,(a_2\ a_n)\ \cdots\ (a_{\frac{1+n}{2}}\ a_{\frac{3+n}{2}})\,(b_1\ b_{n-1})\,(b_2\ b_{n-2})\cdots(b_{\frac{n-1}{2}}\ b_{\frac{n+1}{2}})$, $(1\ a_2)$ and $(1{+}n\ a_n)$. Furthermore, the number of orbits of this group under its natural action is $\frac{3n-1}{2}$ and the orbits are $V_1 = \{a_{\frac{n+1}{2}}, a_{\frac{n+3}{2}}\}$, $V_2 = \{\frac{n+1}{2}, \frac{n+3}{2}\}$, $V_3 = \{b_{\frac{n-1}{2}}, b_{\frac{n+1}{2}}\}$, $V_4 = \{\frac{n-1}{2}, \frac{n+5}{2}\}$, $V_5 = \{a_{\frac{n-1}{2}}, a_{\frac{n+5}{2}}\}$, $V_6 = \{\frac{n-3}{2}, \frac{n+7}{2}\}$, $V_7 = \{b_{\frac{n-3}{2}}, b_{\frac{n+3}{2}}\}$, $V_8 = \{a_{\frac{n-3}{2}}, a_{\frac{n+7}{2}}\}$, $V_9 = \{\frac{n-5}{2}, \frac{n+9}{2}\}$, $V_{10} = \{b_{\frac{n-5}{2}}, b_{\frac{n+5}{2}}\}$, ..., $V_{\frac{3n-11}{2}} = \{a_3, a_{n-1}\}$, $V_{\frac{3n-9}{2}} = \{2, n\}$, $V_{\frac{3n-7}{2}} = \{b_2, b_{n-2}\}$, $V_{\frac{3n-5}{2}} = \{b_1, b_{n-1}\}$, $V_{\frac{3n-3}{2}} = \{a_1, a_{n+1}\}$ and $V_{\frac{3n-1}{2}} = \{1, a_2, 1+n, a_n\}$.

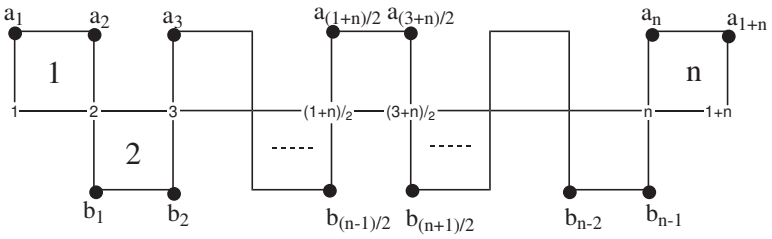


Figure 6: An ortho-chain of length n, $n \overset{4}{\equiv} 1$.

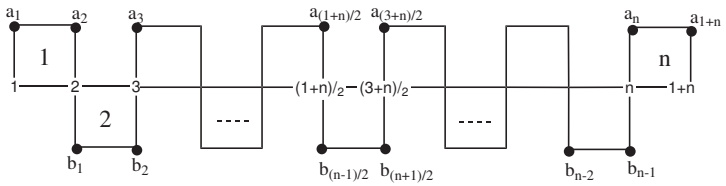


Figure 7: An ortho-chain of length n, $n \overset{4}{\equiv} 3$.

To compute the Graovac-Pisanski index of this graph, $n \neq 3$, we note that $W(V_5) = W(V_6) = W(V_7) = 5$, $W(V_8) = W(V_9) = W(V_{10}) = 7$, $W(V_{\frac{3n-11}{2}}) = W(V_{\frac{3n-9}{2}}) = W(V_{\frac{3n-7}{2}}) = n-2$, $W(V_{\frac{3n-5}{2}}) = n$, $W(V_{\frac{3n-3}{2}}) = n+2$, $W(V_{\frac{3n-1}{2}}) = 4n+4$. Finally, if $n \overset{4}{\equiv} 1$ then $W(V_1) = W(V_2) = 1$, $W(V_3) = W(V_4) = 3$, and if $n \overset{4}{\equiv} 3$ then $W(V_2) = W(V_3) = 1$ and $W(V_1) = W(V_4) = 3$.
Therefore,

$$\begin{aligned} GP(O_n) &= |V| \sum_{i=1}^{\frac{3n-1}{2}} \frac{W(V_i)}{|V_i|} \\ &= (3n+1)\left[\frac{1+1}{2} + \frac{3+3}{2} + \frac{5+5+5}{2} + \frac{7+7+7}{2}\right. \\ &\left. + \cdots + \frac{n-2+n-2+n-2}{2} + \frac{n}{2} + \frac{n+2}{2} + \frac{4n+4}{4}\right] \\ &= (3n+1)\left[1+3+\frac{3}{2}(5+7+\cdots+n-2) + \frac{n}{2} + \frac{n+2}{2} + n + 1\right] \\ &= \frac{9}{8}n^3 + \frac{33}{8}n^2 + \frac{19}{8}n + \frac{3}{8}. \end{aligned}$$

This completes the proof of our theorem. □

In the next theorem the Graovac-Pisanski index of ladder graph L_n, Figures $8-9$, which is also known as the linear polyomino is computed [6].

Theorem 2.6. *The Graovac-Pisanski index of the ladder graph L_n can be computed as follows:*

$$GP(L_n) = \begin{cases} \frac{n^3}{2} + \frac{5n^2}{2} + 3n + 1 & n \text{ is even,} \\ \frac{n^3}{2} + \frac{5n^2}{2} + \frac{7n}{2} + \frac{3}{2} & n \text{ is odd.} \end{cases}$$

Proof. We first note that $Aut(L_1) \cong D_8$ and $Aut(L_n) \cong Z_2 \times Z_2$, for $n \neq 1$. If n is even, then $Aut(L_n)$ can be generated by $\prod_{k=1}^{n+1}(a_k\ b_k)$ and $\prod_{i=1}^{n-1}(a_i\ a_{i+1})(b_i\ b_{i+1})$, i is odd. If n is odd, then the permutations $\prod_{t=1}^{n+1}(a_t\ b_t)$ and $\prod_{j=1}^{n}(a_j\ a_{j+1})$ $(b_j\ b_{j+1})$ will generate the group $Aut(L_n)$, where j is odd positive integer.

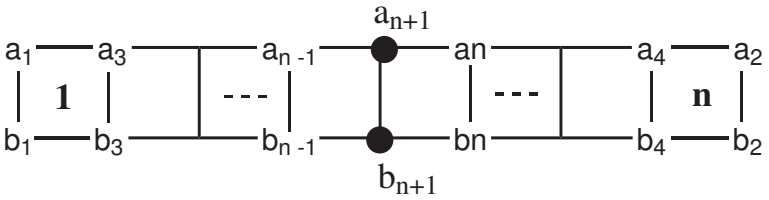


Figure 8: The graph L_n, when n is even.

If n is even, then this group has $\frac{n}{2} + 1$ orbits, and the orbits are $V_1 = \{a_{n+1}, b_{n+1}\}$ of length 2 and other orbits which have length 4 are $V_2 = \{a_1, b_1, a_2, b_2\}$, $V_3 = \{a_3, b_3, a_4, b_4\}, \ldots, V_{\frac{n}{2}+1} = \{a_{n-1}, b_{n-1}, a_n, b_n\}$. On the other hand, $W(V_1) = 1$, $W(V_{\frac{n}{2}+1}) = 12$, $W(V_{\frac{n}{2}}) = 20$, $W(V_{\frac{n}{2}-1}) = 28, \ldots, W(V_2) = 4n + 4$. Therefore,

$$\begin{aligned} GP(L_n) &= |V| \sum_{i=1}^{\frac{n}{2}+1} \frac{W(V_i)}{|V_i|} \\ &= (2n+2)\left(\frac{1}{2} + \frac{12 + 20 + 28 + \cdots + 4n + 4}{4}\right) \\ &= \frac{n^3}{2} + \frac{5n^2}{2} + 3n + 1. \end{aligned}$$

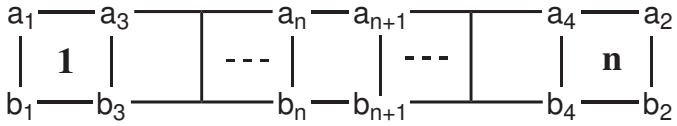


Figure 9: The graph L_n, when n is odd.

If n is odd, then this group has $\frac{n+1}{2}$ orbits of length 4, and the orbits are $V_1 = \{a_1, b_1, a_2, b_2\}$, $V_2 = \{a_3, b_3, a_4, b_4\}, \ldots, V_{\frac{n+1}{2}} = \{a_n, b_n, a_{n+1}, b_{n+1}\}$. Furthermore,

$W(V_{\frac{n+1}{2}}) = 8$, $W(V_{\frac{n-1}{2}}) = 16$, $W(V_{\frac{n-3}{2}}) = 24$, ..., $W(V_1) = 4n + 4$. Therefore,

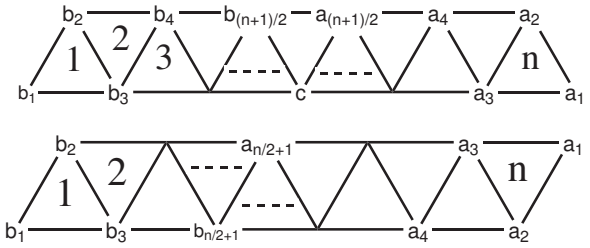
$$\begin{aligned} GP(L_n) &= |V| \sum_{i=1}^{\frac{n+1}{2}} \frac{W(V_i)}{|V_i|} \\ &= (2n+2)\left(\frac{8+16+24+\cdots+4n+4}{4}\right) \\ &= \frac{n^3}{2} + \frac{5n^2}{2} + \frac{7n}{2} + \frac{3}{2}, \end{aligned}$$

which completes our argument. □

We end this paper by computing the Graovac-Pisanski index of a 2-connected linear polymer with triangular faces R_n.

Theorem 2.7. *The Graovac-Pisanski index of a 2−connected linear polymer with triangular faces R_n, Figure 10, is computed as*

$$GP(R_n) = \begin{cases} \frac{n^3}{16} + \frac{n^2}{2} + \frac{5n}{4} + 1 & n \text{ is even,} \\ \frac{n^3}{16} + \frac{3n^2}{8} + \frac{11n}{16} + \frac{3}{8} & n \text{ is odd.} \end{cases}$$



(a)

(b)

Figure 10: (a) R_n, n is odd; (b) R_n, n is even.

Proof. It is clear that $Aut(R_1) \cong S_3$, $Aut(R_2) \cong Z_2 \times Z_2$ and $Aut(R_n) \cong Z_2$, when $n \geq 3$. To compute the Graovac-Pisanski index, we first assume that n is even. Then $V_i = \{a_i, b_i\}$, $1 \leqslant i \leqslant \frac{n}{2} + 1$, $W(V_1) = \frac{n}{2} + 1$, $W(V_2) = \frac{n}{2}$, ..., $W(V_{\frac{n}{2}}) = 2$ and $W(V_{\frac{n}{2}+1}) = 1$. Therefore,

$$\begin{aligned} GP(R_n) &= |V| \sum_{i=1}^{\frac{n}{2}+1} \frac{W(V_i)}{|V_i|} \\ &= (n+2)\left(\frac{1+2+3+\cdots+\frac{n}{2}+1}{2}\right) \\ &= \frac{n^3}{16} + \frac{n^2}{2} + \frac{5n}{4} + 1. \end{aligned}$$

If n is odd then $V_j = \{a_j, b_j\}$, $1 \leqslant j \leqslant \frac{n+1}{2}$, $V_{\frac{n+3}{2}} = \{c\}$, $W(V_1) = \frac{n+1}{2}$, $W(V_2) = \frac{n-1}{2}$, ..., $W(V_{\frac{n-1}{2}}) = 2$, $W(V_{\frac{n+1}{2}}) = 1$ and $W(V_{\frac{n+3}{2}}) = 0$. Therefore,

$$\begin{aligned} GP(R_n) &= |V| \sum_{j=1}^{\frac{n+3}{2}} \frac{W(V_j)}{|V_j|} \\ &= (n+2)\left(\frac{0}{1} + \frac{1+2+3+\cdots+\frac{n+1}{2}}{2}\right) \\ &= \frac{n^3}{16} + \frac{3n^2}{8} + \frac{11n}{16} + \frac{3}{8}. \end{aligned}$$

□

Acknowledgment. We are indebted to the referee for several corrections and useful comments.

References

[1] **A. R. Ashrafi, F. Koorepazan-Moftakhar, M.V. Diudea**, *Distance under symmetry:* $(3,6)$*-fullerenes*, In: Distance, Symmetry, and Topology in Carbon Nanomaterials, A.R. Ashrafi and M.V. Diudea(Eds.), Springer International Publishing, AG Switzerland, (2016) pp. 51 – 60.

[2] **A.R. Ashrafi, H. Shabani**, *The modified Wiener index of some graph operations*, Ars Math. Contemp. **11** (2016), 277 – 284.

[3] **N. Biggs**, *Algebraic Graph Theory*, Second edition, Cambridge Math. Library, Cambridge Univ. Press, Cambridge, (1993).

[4] **M.V. Diudea, O. Ursu, L.Cs. Nagy**, TOPOCLUJ, Babes Bolyai University, Cluj, Romania, (2002).

[5] **T. Došlić, M.S. Litz**, *Matchings and independent sets in polyphenylene chains*, MATCH Commun. Math. Comput. Chem. **67** (2012), 313 – 330.

[6] **T. Došlić, I. Zubac**, *Counting maximal matchings in linear polymers*, Ars Math. Contemp. **11** (2016), no. 2, 255 – 276.

[7] **M. Ghorbani, S. Klavžar**, *Modified Wiener index via canonical metric representation, and some fullerene patches*, Ars Math. Contemp. **11** (2016), 247 – 254.

[8] **A. Graovac, T. Pisanski**, *On the Wiener index of a graph*, J. Math. Chem. **8** (1991), 53 – 62.

[9] **I. Gutman, A.R. Ashrafi**, *On the PI index of phenylenes and their hexagonal squeezes*, MATCH Commun. Math. Comput. Chem. **60** (2008), 135 – 142.

[10] **I. Gutman, S.J. Cyvin, J. Brunvoil**, *Enumeration of the isomers of phenylenes*, Monatshefte für Chemie **125** (1994), 887 – 894.

[11] HyperChem package Release 7.5 for Windows, Hypercube Inc., Florida, USA, 2002.

[12] **F. Koorepazan-Moftakhar, A.R. Ashrafi**, *Distance under symmetry*, MATCH Commun. Math. Comput. Chem. **74** (2015), 259 – 272.

[13] **F. Koorepazan-Moftakhar, A.R. Ashrafi**, *Combination of distance and symmetry in some molecular graphs*, Appl. Math. Comput. **281** (2016), 223 – 232.

[14] **F. Koorepazan-Moftakhar, A.R. Ashrafi, O. Ori, M.V. Putz**, *An algebraic modification of Wiener and hyper-Wiener indices and their calculations for fullerenes*, In: Distance, Symmetry, and Topology in Carbon Nanomaterials, A.R. Ashrafi and M.V. Diudea (Eds.), Springer International Publishing, AG Switzerland, (2016) pp. 33 – 50.

[15] **H. Shabani, A.R. Ashrafi**, *Symmetry-moderated Wiener index*, MATCH Commun. Math. Comput. Chem. **76** (2016), 3 – 18.

[16] The GAP Team, GAP-Groups, Algorithms, and Programming, Lehrstuhl De für Mathematik, Rheinisch Westfalische Technische Hochschule, Aachen, Germany, 1997.

[17] **N. Tratnik**, *The Graovac-Pisanski index of zig-zag tubulenes and the generalized cut method*, J. Math. Chem. **55** (2017), no. 8, 1622 – 1637.

[18] **H. Wiener**, *Structural determination of the paraffin boiling points*, J. Am. Chem. Soc. **69** (1947), 17 – 20.

Received November 08, 2017

F. Koorepazan-Moftakhar
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan 87317-53153, I. R. Iran
e-mail: f.k.moftakhar@gmail.com

A. R. Ashrafi
Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan 87317-53153, I. R. Iran
e-mail: ashrafi@kashanu.ac.ir

O. Ori
Actinium Chemical Research, Via Casilina 1626/A, 00133 Rome, Italy
e-mail: ottorino.ori@gmail.com

Quasigroups and Related Systems **26** (2018), 103 – 108

Retractive nil-extensions of completely simple semirings

Sunil Kumar Maity, Rumpa Chatterjee and Rituparna Ghosh

Abstract. A semiring S is said to be a quasi completely regular semiring if for any $a \in S$ there exists a positive integer n such that na is completely regular. The study of completely Archimedean semirings have shown that completely Archimedean semirings are nil-extensions of completely simple semirings. In this paper we introduce retractive nil-extensions of completely simple semirings and establish a relation with completely Archimedean semirings.

1. Introduction

In the year 1984, S. Bogdanovic and S. Milic [5] first studied nil-extensions of completely simple semigroups. Decomposition of completely π-regular semigroups into a semilattice of Archimedean semigroups was discussed by S. Bogdanovic in [1]. The study of nil-extensions of completely regular semigroups has been proven of great importance in semigroup theory. A completely Archimedean semigroup has been proven to be a nil-extension of a completely simple semigroup and furthermore it is Archimedean and completely π- regular. Furthermore, characterization of retractive nil-extensions of class of regular semigroups, union of groups and band of groups have been studied in the papers [2], [3] and [4]. Retractive nil-extension of a completely simple semigroup has been proved to be a rectangular band of π-groups. Therefore, retractive extension of a semigroup has been an area of great attraction in recent years of study.

In recent years, semirings have been studied by many authors, for example, by F. Pastijn, Y. Q. Guo, M. K. Sen, K. P. Shum and others (See [10], [13]). In the paper [13], completely regular semirings were introduced and it was derived that a completely regular semiring is a union of skew-rings and also a b-lattice of completely simple semirings. After this work, many interesting results on completely regular semigroups and inverse semigroups have been extended to semirings by M. K. Sen, S. K. Maity and K. P. Shum in ([12], [14]). Furthermore, extension of completely π-regular semigroups to quasi completely regular semirings in [9] have further enriched the study of analogous results. It has also been derived that quasi completely regular semiring can be described as the b-lattice of completely Archimedean semirings. In the paper [8], we had shown that a semiring

2010 Mathematics Subject Classification: 16A78, 20M10, 20M07.
Keywords: ideal extension, nil-extension, completely Archimedean semiring, completely simple semiring, retractive nil-extension, b-lattice of skew-rings, quasi skew-ring

is completely Archimedean if and only if it is nil-extension of a completely simple semiring if and only if it is Archimedean and quasi completely regular.

In this paper we further study retractive extension of a semiring. We characterize completely Archimedean semirings as retractive nil-extension of completely simple semirings. Thus we establish a relation between retractive nil-extensions of completely simple semirings and nil-extensions of completely simple semirings. The preliminaries and prerequisites for this article are discussed in section 2. In section 3 we prove some characterization theorems of completely Archimedean semirings as retractive nil-extensions of completely simple semirings. Further, we study properties on retractive nil-extension of b-lattice of skew-rings.

2. Preliminaries

A semiring $(S, +, \cdot)$ has both the additive reduct $(S, +)$ and the multiplicative reduct $(S, \cdot)$ as semigroups and multiplication distributes over addition, that is, $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in S$. We do not assume that the additive reduct $(S, +)$ is commutative. An element a of a semiring S is said to be *infinite* [7] if and only if $a + x = a = x + a$ for all $x \in S$. Infinite element in a semiring is unique and is denoted by ∞. An infinite element ∞ in a semiring S having the property that $x \cdot \infty = \infty = \infty \cdot x$ for all $x(\neq 0) \in S$ is called *strongly infinite* [7]. A semiring S is *additively regular* if for every element $a \in S$ there exists an element $x \in S$ such that $a + x + a = a$. A semiring S is said to be *additively quasi regular* if for every element $a \in S$ there exists a positive integer n such that the element $na = \underbrace{a + a + \cdots + a}_{n \text{ times}}$ is additively regular. A semiring S is *completely regular* [13] if for every element $a \in S$, there exists an element $x \in S$ such that $a = a + x + a$, $a + x = x + a$ and $a(a + x) = a + x$. A semiring $(S, +, \cdot)$ is a *quasi completely regular semiring* [9] if for every element $a \in S$, there exists a positive integer n such that na is completely regular, that is, $na = na + x + na$, $na + x = x + na$ and $na(na + x) = na + x$ for a suitable element $x \in S$. A semiring $(S, +, \cdot)$ is called a *skew-ring* if its additive reduct $(S, +)$ is a group, not necessarily an abelian group. In [13] we proved that an element a in a semiring S is completely regular if and only if it is contained in a subskew-ring of S. Let S be a semiring and R be a subskew-ring of S. If for every $a \in S$ there exists a positive integer n such that $na \in R$, then S is said to be a *quasi skew-ring*. A semiring S is said to be a *b-lattice* [13] if $(S, \cdot)$ is a band and $(S, +)$ is a semilattice. A semiring S is said to be an *idempotent semiring* if all the elements of S are additive idempotent as well as multiplicative idempotent, i.e., $a + a = a = a^2$ for all $a \in S$. An idempotent semiring satisfying the identity $a = a + x + a$ is called a *rectangular band semiring*. Throughout this paper, we let $E^+(S)$ be the set of all additive idempotents of the semiring S. We observe that the set $E^+(S)$ is non-empty and it forms an ideal of the multiplicative reduct $(S, \cdot)$ of the semiring S. If $(S, +, \cdot)$ is a semiring, we denote the Green's relations on the semigroup $(S, +)$ by $\mathscr{L}^+$, $\mathscr{R}^+$, $\mathscr{J}^+$, and

$\mathscr{H}^+$. In fact, the relations $\mathscr{L}^+$, $\mathscr{R}^+$, $\mathscr{J}^+$ and $\mathscr{H}^+$ are all congruences of the multiplicative reduct $(S,\cdot)$. Thus, if any one of these happens to be a congruence on the additive reduct $(S,+)$, it will be a congruence on the semiring $(S,+,\cdot)$. Let $(S,+,\cdot)$ be an additively quasi regular semiring. We consider the relations $\mathscr{L}^{*+}$, $\mathscr{R}^{*+}$, and $\mathscr{J}^{*+}$ on S defined by: for $a,b\in S$,

$$a\,\mathscr{L}^{*+}\,b \text{ if and only if } pa\,\mathscr{L}^{+}\,qb,$$
$$a\,\mathscr{R}^{*+}\,b \text{ if and only if } pa\,\mathscr{R}^{+}\,qb,$$
$$a\,\mathscr{J}^{*+}\,b \text{ if and only if } pa\,\mathscr{J}^{+}\,qb;$$

where p and q are the smallest positive integers such that pa and qb are respectively additively regular. We also let $\mathscr{H}^{*+}=\mathscr{L}^{*+}\cap\mathscr{R}^{*+}$. A quasi completely regular semiring $(S,+,\cdot)$ is said to be *completely Archimedean* if $\mathscr{J}^{*+}=S\times S$.

A nonempty subset I of a semiring $(S,+,\cdot)$ is said to be a *bi-ideal* of S if $a\in I$ and $x\in S$ imply that $a+x,x+a,ax,xa\in I$. Let I be a bi-ideal of a semiring S. We define a relation ρ_I on S by $a\rho_I b$ if and only if either $a,b\in I$ or $a=b$ where $a,b\in S$. It is easy to verify that ρ_I is a congruence on S. This congruence is said to be *Rees congruence* on S and the quotient semiring S/ρ_I contains a strongly infinite element, namely I. This quotient semiring S/ρ_I is said to be the *Rees quotient semiring* and is denoted by S/I. In this case the semiring S is said to be an *ideal extension* of I by the semiring S/I. An ideal extension S of a semiring I is a *nil-extension* of I if for any $a\in S$ there exists a positive integer n such that $na\in I$.

A subsemiring T of a semiring S is a *retract* of S if there exists a homomorphism $\phi: S\longrightarrow T$ such that $\phi(t)=t$ for all $t\in T$. Such a homomorphism is called a *retraction*. A nil-extension S of T is said to be a *retractive nil-extension* of T if T is a retract of S.

3. Retractive nil-extension

In this section we characterize completely Archimedean semirings as a retractive nil-extensions of completely simple semirings. For this first we state the following two results.

Theorem 3.1 ([6], [9]). *The following conditions on a semiring $(S,+,\cdot)$ are equivalent.*

(*i*) *S is a quasi completely regular semiring.*

(*ii*) *Every $\mathscr{H}^{*+}$- class is a quasi skew-ring.*

(*iii*) *S is (disjoint) union of quasi skew-rings.*

(*iv*) *S is a b-lattice of completely Archimedean semirings.*

(*v*) *S is an idempotent semiring of quasi skew-rings.*

Theorem 3.2 ([8]). *The following conditions on a semiring are equivalent:*

(*i*) *S is a completely Archimedean semiring;*

(*ii*) *S is a nil-extension of a completely simple semiring;*

(*iii*) *S is Archimedean and quasi completely regular.*

Remark. Let a be a quasi completely regular element in a semiring $(S, +, \cdot)$. Then there exists a positive integer n such that na is completely regular and hence na lies in a subskew-ring of S. The zero of the subskew-ring containing na is denoted by a^0. Here it is interesting to mention that if S is a quasi completely regular semiring then S is (disjoint) union of quasi skew-rings. We know that every quasi skew-ring contains a unique additive idempotent. According to our notation a^0 is the unique additive idempotent in the quasi skew-ring containing a.

Theorem 3.3. *Let S be a completely Archimedean semiring. Then S is a retractive nil-extension of a completely simple semiring.*

Proof. Since S is a completely Archimedean semiring, hence S is a quasi completely regular semiring. Therefore, S is an idempotent semiring I of quasi skew-rings S_i, $i \in I$. Let $a, b \in S$. Then $a \in S_i$ and $b \in S_j$ for some $i, j \in I$. This implies $a+b, 2a+b, a+2b \in S_{i+j}$. Since S_{i+j} is a quasi skew-ring, we must have a positive integer n such that $n(a+b) \in (2a+b)+S+(a+2b)$. Hence for any two elements $a, b \in S$, there exists a positive integer n such that $n(a+b) \in (2a+b)+S+(a+2b) \subseteq 2a+S+2b$. Let $a \in S$. Then $a \in S_i$ for some $i \in I$. Let e be the unique additive idempotent in the quasi skew-ring S_i. Let $f \in E^+(S)$. We first prove that $a+f = e+a+f$ and $f+a = f+a+e$. First we prove that for every $m \in \mathbb{N}$, there exists $n \in \mathbb{N}$ and $u \in S$ such that $n(a+f) = ma+u+f$. Clearly, the result holds if $m = 1$. Let us assume that $n(a+f) = ma+u+f$ for some $n \in \mathbb{N}$ and $u \in S$. Now for the elements ma and $u+f$ there exists a positive integer k and $v \in S$ such that $k(ma+u+f) = 2ma+v+2(u+f) = (m+1)a+w+f$, where $w = (m-1)a+v+u+f+u \in S$. Hence for every $m \in \mathbb{N}$, there exists $n \in \mathbb{N}$ and $u \in S$ such that $n(a+f) = ma+u+f$. Let $r \in \mathbb{N}$ be such that ra is completely regular and hence ra lies in a subskew-ring R_i. Clearly, e is the zero of R_i. Then there exists $p \in \mathbb{N}$ and $x \in S$ such that $p(a+f) = ra+x+f$. Now since S is a completely Archimedean semiring, so S is a nil-extension of a completely simple semiring K. Clearly, $f \in K$ and since K is a bi-ideal of S, it follows $a+f \in K$. Hence $(a+f)\,\mathscr{H}^+\,p(a+f)$ and $(a+f) = p(a+f)+y$ for some $y \in S$. Therefore, $a+f = p(a+f)+y = ra+x+f+y = e+ra+x+f+y = e+a+f$. Similarly, we can prove that $f+a = f+a+e$. We define a mapping $\phi : S \longrightarrow K$ by $\phi(a) = a^0+a$, for all $a \in S$. Let $a, b \in S$. Then $\phi(a+b) = (a+b)^0+a+b = (a+b)^0+a+a^0+b = (a+b)^0+a+a^0+b+b^0 = (a+b)^0+a+b+b^0 = a+b+b^0 = a+b^0+b = a^0+a+b^0+b = \phi(a)+\phi(b)$. Again, $\phi(a)\phi(b) = (a^0+a)(b^0+b) = a^0b^0+a^0b+ab^0+ab = (ab)^0+ab = \phi(ab)$. Therefore, ϕ is a homomorphism and since $\phi(a) = a$ for all $a \in K$, then ϕ is a retraction. Hence S is a retractive nil-extension of a completely simple semiring K. □

Corollary 3.4. *The following conditions on a semiring S are equivalent:*

(*i*) *S is a completely Archimedean semiring.*

(*ii*) *S is a retractive nil extension of a completely simple semiring.*

(*iii*) *S is a nil-extension of a completely simple semiring.*

Theorem 3.5. *A semiring S is a completely Archimedean semiring if and only if S is a rectangular band semiring of quasi skew-rings.*

Proof. Let S be a completely Archimedean semiring. Hence S is a quasi completely regular semiring and hence S is an idempotent semiring $I(= S/\mathscr{H}^{*+})$ of quasi skew-rings S_i $(i \in I)$. To show I is a rectangular band semiring, let $x = a\mathscr{H}^{*+}$, $y = b\mathscr{H}^{*+} \in I$, where $a, b \in S$. Since S is completely Archimedean, we must have $a^0 = (a+b+a)^0$. Then $x = a\mathscr{H}^{*+} = a^0\mathscr{H}^{*+} = (a+b+a)^0\mathscr{H}^{*+} = (a+b+a)\mathscr{H}^{*+} = a\mathscr{H}^{*+} + b\mathscr{H}^{*+} + a\mathscr{H}^{*+} = x + y + x$. Thus I is a rectangular band semiring and consequently, S is a rectangular band semiring of quasi skew-rings.

Conversely, let S be a rectangular band semiring Y of quasi skew-rings, T_i $(i \in Y)$. Then clearly S is a quasi completely regular semiring and $Y = S/\mathscr{H}^{*+}$. To show S is completely Archimedean, we only show that $\mathscr{J}^{*+} = S \times S$. Let $a, b \in S$. Then $a\mathscr{H}^{*+} = a\mathscr{H}^{*+} + b\mathscr{H}^{*+} + a\mathscr{H}^{*+} = (a+b+a)\mathscr{H}^{*+}$ implies $a^0 = (a+b+a)^0$. Since $\mathscr{J}^{*+}$ is b-lattice congruence, we have $a\,\mathscr{J}^{*+} = a^0\,\mathscr{J}^{*+} = (a+b+a)^0\,\mathscr{J}^{*+} = (a+b+a)\,\mathscr{J}^{*+} = (a+b)\,\mathscr{J}^{*+} = (b+a+b)\,\mathscr{J}^{*+} = (b+a+b)^0\,\mathscr{J}^{*+} = b^0\,\mathscr{J}^{*+} = b\,\mathscr{J}^{*+}$. Therefore, $\mathscr{J}^{*+} = S \times S$ and hence S is a completely Archimedean semiring. □

Corollary 3.6. *A semiring S is a completely simple semiring if and only if S is a rectangular band semiring of skew-rings.*

Theorem 3.7. *The following conditions on a semiring S are equivalent:*

(*i*) *S is a nil-extension of a b-lattice of skew-rings.*

(*ii*) *S is a retractive nil-extension of b-lattice of skew-rings.*

Proof. (*i*) $\Rightarrow$ (*ii*): Let S be a nil-extension of K, where K is a b-lattice Y of skew-rings $R_\alpha(\alpha \in Y)$. Then $(K, +)$ is a semilattice $(Y, +)$ of groups $(R_\alpha, +)$ and hence $(K, +)$ is a Clifford semigroup. Thus for any $k \in K$ and $e \in E^+(K)$ we must have $e + k = k + e$. Now we define a mapping $\phi : S \longrightarrow K$ by: for $a \in S$,

$$\phi(a) = a^0 + a.$$

Let $a, b \in S$. Then $\phi(a+b) = (a+b)^0 + (a+b) = (a^0 + b^0) + (a+b) = (b^0 + a^0) + (a+b) = b^0 + (a^0 + a) + b = (a^0 + a) + (b^0 + b) = \phi(a) + \phi(b)$ and $\phi(a)\phi(b) = (a^0 + a)(b^0 + b) = a^0b^0 + a^0b + ab^0 + ab = (ab)^0 + ab = \phi(ab)$. Hence ϕ is a homomorphism. Moreover for any $x \in K$, $\phi(x) = x^0 + x = x$. Consequently, S is a retractive nil-extension of b-lattice of skew-rings K.

(*ii*) $\Rightarrow$ (*i*): This part is obvious. □

References

[1] **S. Bogdanović**, *Semigroups with a system of subsemigroups*, Novi Sad (1985).

[2] **S. Bogdanović and M. Ćirić**, *Retractive nil-extensions of regular semigroups I*, Proc. Japan Acad. **68** (5), Ser. A (1992), 115 – 117.

[3] **S. Bogdanović and M. Ćirić**, *Retractive nil-extensions of regular semigroups II*, Proc. Japan Acad. **68** (6), Ser. A (1992), 126 – 130.

[4] **S. Bogdanović and M. Cirić**, *Retractive nil-extensions of bands of groups*, Facta Univ. Niš, Ser. Math. Inform. **8** (1993), 11 – 20.

[5] **S. Bogdanović and S. Milić**, *A nil-extension of a completely simple semigroup*, Publ. Inst. Math. **36(50)** (1984), 45 – 50.

[6] **R. Debnath, S.K. Maity and A.K. Bhuniya**, *Subdirect products of an idempotent semiring and a b-lattice of skew-rings*, submitted for publication.

[7] **J.S. Golan**, *The theory of semirings with applications in mathematics and theoretical computer science*, Pitman Monographs and Surveys in Pure and Appl. Math. 54, Longman Scientific (1992).

[8] **S.K. Maity and R. Ghosh**, *Nil-extensions of completely simple semirings*, Discussiones Math. General Algebra Appl. **33** (2013), 201 – 209.

[9] **S.K. Maity and R. Ghosh**, *On quasi completely regular semirings*, Semigroup Forum **89** (2014), 422 – 430.

[10] **F. Pastijn and Y.Q. Guo**, *The lattice of idempotent distributive semiring varieties*, Science in China (Series A) **42** (8) (1999), 785 – 804.

[11] **M. Petrich and N.R. Reilly**, *Completely regular semigroups*, Wiley, New York (1999).

[12] **M.K. Sen, S.K. Maity and K.P. Shum**, *Clifford semirings and generalized Clifford semirings*, Taiwanese J. Math. **9** (2005), 433 – 444.

[13] **M.K. Sen, S.K. Maity and K.P. Shum**, *On completely regular semirings*, Bull. Cal. Math. Soc. **98** (2006), 319 – 328.

[14] **M.K. Sen, S.K. Maity and H.J. Weinert**, *Completely simple semirings*, Bull. Cal. Math. Soc. **97** (2005), 163 – 172.

Received August 13, 2017

S.K. Maity
Department of Pure Mathematics, University of Calcutta, 35, Ballygunge Circular Road, Kolkata-700019, India.
E-mail: skmpm@caluniv.ac.in

R. Chatterjee
Department of Mathematics, The University of Burdwan, Golapbag, Burdwan-713104, India.
E-mail: rumpachatterjee13@gmail.com

R. Ghosh
Department of Mathematics, Heritage Institute of Technology, Anandapur, P.O East Kolkata Township, Kolkata - 700 107, India.
E-mail: rituparna.ghosh@heritageit.edu

Quasigroups and Related Systems **26** (2018), 109 – 120

Non-commutative finite associative algebras of 3-dimensional vectors

Dmitriy Moldovyan, Nicolai Moldovyan and Victor Shcherbacov

Abstract. Properties of the non-commutative finite associative algebras of 3-dimensional vectors are presented. An interesting feature of these algebras is mutual associativity of all modifications of the defined parameterized multiplication operation and existence of a large set of single-side unit elements. In the ordinary case one unique two-side unit element is connected with every element of the algebra, except the elements that are square roots of zero element. It is shown that the used method suites for defining finite non-commutative associative algebras of arbitrary dimension $m \geqslant 2$. The considered finite associative algebras are interesting for cryptographic applications.

1. Introduction

Finite non-commutative associative algebras (FNAAs) are interesting for applications in design of public-key cryptoschemes characterized in using hidden conjugacy search problem (called also discrete logarithm problem in hidden cyclic group) [2, 3, 6]. In literature there are considered different FNAAs defined over finite vector spaces with dimensions $m = 4, 6$, and 8. The main attention was paid to the case $m = 4$ that provides lower computational difficulty of multiplication operation in the FNAA while defining vector spaces over the same finite field $GF(p)$. Recently it has been introduced the 2-dimension FNAA [4].

In the present paper it is shown that the method for defining 2-dimension FNAA can be generalized and used to define m-dimensional FNAAs for an arbitrary value $m \geqslant 2$. Some properties of the FNAA relating to the case $m = 3$ are investigated. Other types of 3-dimension non-commutative algebras with associative multiplication operation are defined as well. All investigated FNAAs contain only local unit elements, therefore defining the discrete logarithm problem in a hidden group [2] on the base of such FNAAs has some peculiarities that are discussed in relation of cryptographic application of the considered finite algebras.

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: finite associative algebra, difficult problem, homomorphism, non-commutative group, non-commutative ring, public-key cryptoscheme.
The reported study was funded by Russian Foundation for Basic Research (project #18-07-00932).

2. Unit elements in 3-dimensional FNAA

Suppose $\mathbf{e}$, $\mathbf{i}$, and $\mathbf{j}$ are some formal basis vectors and $a, b, c \in GF(p)$, where prime $p \geqslant 3$, to be coordinates. Three-dimensional vectors are denoted as $a\mathbf{e}+b\mathbf{i}+c\mathbf{j}$ or as (a, b, c). Terms $\tau\mathbf{v}$, where $\tau \in GF(p)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \mathbf{j}\}$ are called components of the vector.

Addition of two vectors (a, b, c) and (x, y, z) is defined as addition of the corresponding coordinates, i.e., with the following formula $(a, b, c) + (x, y, z) = (a + x, b + y, c + z)$.

The multiplication operation in finite 3-dimensional vector space is defined with the formula

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) =$$
$$= ax(\mathbf{e}\circ\mathbf{e})+bx(\mathbf{i}\circ\mathbf{e})+cx(\mathbf{j}\circ\mathbf{e})+ay(\mathbf{e}\circ\mathbf{i})+by(\mathbf{i}\circ\mathbf{i})+cy(\mathbf{j}\circ\mathbf{i})+az(\mathbf{e}\circ\mathbf{j})+bz(\mathbf{i}\circ\mathbf{j})+cz(\mathbf{j}\circ\mathbf{j}),$$

where products of different pairs of formal basis vectors $\mathbf{e}$, $\mathbf{i}$, and $\mathbf{j}$ are to be replaced by some one-component vector in accordance with the basis-vector multiplication table (BVMT) shown in Table 1. The left basis vector defines the row and the right one defines the column. At the intersection of the row and column we have the value of the product of two formal basis vectors.

Table 1 defines non-commutative associative multiplication of the vectors $V = (a, b, c) = a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$ and $X = (x, y, z) = x\mathbf{e} + y\mathbf{i} + z\mathbf{j}$. The BVMT contains structural coefficients $\mu, \tau, \lambda \in GF(p)$ defining different modifications of the multiplication operation, i.e., the last is parameterized. The defined non-commutative multiplication operation is characterized in the mutual associativity of all its modifications, i.e., for the considered FNAA of 3-dimensional vectors the following statement is valid:

Proposition 1. *Suppose $\circ$ and $\star$ are two arbitrary modifications of the vector multiplication operation, which correspond to different triples of structural coefficients $(\mu_1, \tau_1, \lambda_1)$ and $(\mu_2, \tau_2, \lambda_2) \neq (\mu_1, \tau_1, \lambda_1)$. Then for arbitrary three vectors A, B, and C the following formula $(A \circ B) \star C = A \circ (B \star C)$ holds.*

Proof of this statement consists in straightforward using of the definition of the multiplication operation and Table 1.

Table 1: The BVMT defining associative multiplication in the finite vector space of the dimension $m = 3$ ($\mu \neq 0$; $\tau \neq 0$; $\lambda \neq 0$)

$\circ$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$
$\mathbf{e}$	$\mu\mathbf{e}$	$\tau\mathbf{e}$	$\lambda\mathbf{e}$
$\mathbf{i}$	$\mu\mathbf{i}$	$\tau\mathbf{i}$	$\lambda\mathbf{i}$
$\mathbf{j}$	$\mu\mathbf{j}$	$\tau\mathbf{j}$	$\lambda\mathbf{j}$

Structure of Table 1 is similar to structure of the BVMT used for defining the 2-dimension FNAA [4] (see Table 2), i.e., every cell in every fixed row contains the

same formal basis vector and every cell in every fixed column contains the same structural coefficient.

Table 2: The basis-vector multiplication table for the case $m = 2$ [4]

$\circ$	$\mathbf{e}$	$\mathbf{i}$
$\mathbf{e}$	$\mu\mathbf{e}$	$\tau\mathbf{e}$
$\mathbf{i}$	$\mu\mathbf{i}$	$\tau\mathbf{i}$

Finding the right-side unit elements in the considered 3-dimension FNAA is connected with solving the vector equation

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) = a\mathbf{e} + b\mathbf{i} + c\mathbf{j}, \tag{1}$$

where $V = a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$ is an arbitrary vector and $X = x\mathbf{e} + y\mathbf{i} + z\mathbf{j}$ is the unknown one.

Equation (1) can be reduced to the following system of three linear equations:

$$\begin{cases} \mu ax + \tau ay + \lambda az = a, \\ \mu bx + \tau by + \lambda bz = b, \\ \mu cx + \tau cy + \lambda cz = c. \end{cases} \tag{2}$$

Solution of the system (2) defines the following set of the local right-side unit elements

$$E_r = (x,\ y,\ z) = \left(x,\ y,\ \lambda^{-1}(1 - \mu x - \tau y)\right), \tag{3}$$

where x and y take on all possible values in $GF(p)$. Every value E_r from set (3) represents a global right-side unit element acting on all 3-dimensional vectors of the considered FNAA.

The vector equation

$$(x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) \circ (a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) = a\mathbf{e} + b\mathbf{i} + c\mathbf{j} \tag{4}$$

that defines the left-side unit elements can be reduced to the following system of three linear equations:

$$\begin{cases} (\mu a + \tau b + \lambda c)x = a, \\ (\mu a + \tau b + \lambda c)y = b, \\ (\mu a + \tau b + \lambda c)z = c. \end{cases} \tag{5}$$

Solving the system (5) one gets the following statement.

Proposition 2. *To every vector $V = (a, b, c)$, such that $\mu a + \tau b + \lambda c \neq 0$, there corresponds a unique local left-side unit vector*

$$E_l = (x, y, z) = \left(\frac{a}{\mu a + \tau b + \lambda c}, \frac{b}{\mu a + \tau b + \lambda c}, \frac{c}{\mu a + \tau b + \lambda c}\right). \tag{6}$$

It is easy to show that the local left-side unit element is contained in the set (3), i.e., it is equal to the local bi-side unit of the vector V.

Let us consider the sequence $V, V^2, \ldots, V^i$ (for $i = 1, 2, 3, \ldots$). If the vector V is not a zero-divisor relatively some of its power (zero-divisors are considered below, where it is shown that vectors satisfying the condition $a\mu + b\tau + c\lambda \neq 0$ are not zero-divisors), then for some two integers h and $k > h$ we have $V^k = V^h$ and $V^k = V^{k-h} \circ V^h = V^h \circ V^{k-h} = V^{k-h} \circ V^h$. Thus, the mentioned sequence is periodic and for some integer ω (that can be called order of the vector V) the equality $V^\omega = V^{k-h} = E'$ holds, where E' is a bi-side local unit such that $V^i \circ E' = E' \circ V^i = V^i$ holds for all integers i.

Thus, taking into account that the local right-side unit element corresponding to the vector V is a unique one, we can conclude the following:

Proposition 3. *Suppose $V = (a, b, c)$ is a vector such that $a\mu + b\tau + c\lambda \neq 0$. Then the vector E_r described with the formula (6) acts as a unique bi-side local unit element E' in the subset $\{V, V^2, \ldots, V^i, \ldots\}$, and the value E' can be computed as some power of V.*

Thus, the element E_l defined by the vector $V = (a, b, c)$ acts on vectors $V, V^2, \ldots, V^i$ as a local bi-side unit for an arbitrary integer $i \geqslant 1$.

Example. The last fact can be illustrated by the following computations using the values

$p = 99161514659781804607 1879$, $\mu = 3176589117$, $\tau = 1$, $\lambda = 8766554$, and

$$N = (a, b, c) = (8654389874321123, 35172879913271, 185758463523115).$$

Computation of the value E' as $E' = N^{p^2-1}$ and using formula (6) from Statement 2 gives the same result

$$E' = (73697875749428423568471, 45051144211088924326 1952, 50136619611775872069 0571).$$

Finding the right-side zero-divisors for the vector $V = (a, b, c)$ is connected with consideration of the vector equation

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) = (0, 0, 0)$$

that can be reduced to the following system of equations:

$$\begin{cases} (\mu x + \tau y + \lambda z)a = 0, \\ (\mu x + \tau y + \lambda z)b = 0, \\ (\mu x + \tau y + \lambda z)c = 0. \end{cases} \tag{7}$$

Solution of system (7) defines the following set of the right-side zero-divisors

$$D_r = (x,\ y,\ z) = \left(x,\ y,\ \lambda^{-1}(-\mu x - \tau y)\right), \tag{8}$$

where x and y take on all values in $GF(p)$. Every value D_r from set (8) represents a global right-side zero-divisor acting on all 3-dimensional vectors of the considered FNAA. Formula (8) describes the vectors to which no left-side unit corresponds. Below it is shown that formula (8) describes square roots of zero vector $(0,0,0)$.

The vector equation

$$(x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) \circ (a\mathbf{e} + b\mathbf{i} + c\mathbf{j}) = (0,0,0)$$

that defines the left-side zero-divisor can be reduced to the following system of three linear equations:

$$\begin{cases} (\mu a + \tau b + \lambda c)x = 0, \\ (\mu a + \tau b + \lambda c)y = 0, \\ (\mu a + \tau b + \lambda c)z = 0. \end{cases} \tag{9}$$

Solving system (9) one gets the following statement.

Proposition 4. *To every vector $V = (a,b,c)$ such that $\mu a + \tau b + \lambda c \neq 0$, there corresponds no left-side zero-divisor, except $(0,0,0)$. Every vector of the considered FNAA acts on vectors $V' = (a',b',c')$, such that $\mu a' + \tau b' + \lambda c' = 0$, as a left-side zero-divisor.*

Consideration of the vector equation

$$D \circ D = (0,0,0),$$

where $D = (x,y,z)$ is unknown, leads to solving the system

$$\begin{cases} (\mu x + \tau y + \lambda z)x = 0, \\ (\mu x + \tau y + \lambda z)y = 0, \\ (\mu x + \tau y + \lambda z)z = 0, \end{cases}$$

that defines the following set of square roots of the zero vector $(0,0,0)$:

$$D = \left(x,\ y,\ -\lambda^{-1}(\mu x + \tau y)\right),$$

where x and y take on all values in $GF(p)$. Thus, vectors $V = (a',b',c')$, coordinates of which satisfy condition $\mu a' + \tau b' + \lambda c' = 0$, are square roots of zero.

Taking into account Proposition 4 and finiteness of the considered vector space it is easy to see that the vector V, such that $\mu a + \tau b + \lambda c \neq 0$, generates periodic sequence $V, V^2, \ldots, V^i$, where $i = 1,2,3,\ldots$, and for some value $i = \omega$ we have $V^\omega = E'$, where $E' = E_l$ is the local bi-side unit determined by coordinates of the vector V in accordance with the formula (6) from Proposition 2.

Like in the case of FNAA of two-dimensional vectors, non-commutative associative multiplication of the 3-dimensional vectors can be defined alternatively with Table 3 that represents transposition of the Table 1. It is easy to see that Table 3 defines the FNAA having the properties very close to the properties of the

considered FNAA of 3-dimensional vectors. Indeed, suppose V and W to be arbitrary 3-dimensional vectors and $\circ$ and $\star$ to be the vector multiplication operations defined with Table 1 and Table 3 respectively. Then

$$V \circ W = W \star V.$$

The proof of this fact consists in straightforward using of the definition of the multiplication operation and the indicated two BVMTs.

Table 3: Alternative BVMT defining associative multiplication in the finite vector space of the dimension $m = 3$

$\circ$	**e**	**i**	**j**
e	μ**e**	μ**i**	μ**j**
i	τ**e**	τ**i**	τ**j**
j	λ**e**	λ**i**	λ**j**

4. Particular variants of 3-dimensional FNAAs

Except Tables 1 and 3, other particular BVMTs defining 3-dimension FNAAs are possible, which can be attributed to the type of unbalanced BVMTs. If the BVMT is such that while multiplying two input vectors the **e**-coordinate does not influence the **i**- and **j**-coordinates of the output vector, then the BVMT is called **e**-unbalanced. Similar definitions can be formulated for **i**- and **j**-unbalanced BVMTs. In such sense the BVMTs presented by Table 1 and 3 can be called balanced. Four different unbalanced BVMTs and formulas for describing local unit elements (left-side E_l, right-side E_r, and bi-side E' ones) for the vector $V = (a, b, c)$ relating to the FNAAs defined with these BVMTs, are presented bellow.

Table 4: The **j**-unbalanced BVMT

$\circ$	**e**	**i**	**j**
e	μ**e**	μ**i**	**0**
i	τ**e**	τ**i**	**0**
j	μ**j**	τ**j**	**0**

Case of Table 4. The set of the left-side local unit elements of the vector $V = (a, b, c)$ such that $\tau \neq 0$ and $\mu a + \tau b \neq 0$, is described as follows:

$$E_l = \left(h, \frac{1 - \mu h}{\tau}, \frac{c}{\mu a + \tau b}\right),$$

where $h = 0, 1, \ldots, p-1$.

The set of the right-side local units of the vector V is described as follows (where $h = 0, 1, \ldots, p-1$):

$$E_r = \left(\frac{a}{\mu a + \tau b}, \frac{b}{\mu a + \tau b}, h \right).$$

For the vector V there exists only one local bi-side unit:

$$E' = \left(\frac{a}{\mu a + \tau b}, \frac{b}{\mu a + \tau b}, \frac{c}{\mu a + \tau b} \right).$$

Table 5: The **e**-unbalanced BVMT

$\circ$	**e**	**i**	**j**
e	**0**	**0**	**0**
i	μ**e**	μ**i**	τ**i**
j	τ**e**	μ**j**	τ**j**

Case of Table 5. The set of the left-side local units corresponding to the vector $V = (a, b, c)$ such that $\mu b + \tau c \neq 0$, is described by the following formula (where $h = 0, 1, \ldots, p-1$):

$$E_l = \left(h, \frac{b}{\mu b + \tau c}, \frac{c}{\mu b + \tau c} \right).$$

The set of the right-side local units of the vector V is described by the following formula ($h = 0, 1, \ldots, p-1$):

$$E_r = \left(\frac{a}{\mu b + \tau c}, h, \frac{1}{\tau} - \frac{\mu}{\tau} h \right).$$

The single local bi-side unit of the vector V is

$$E' = \left(\frac{a}{\mu b + \tau c}, \frac{b}{\mu b + \tau c}, \frac{c}{\mu b + \tau c} \right).$$

Table 6: The **i**-unbalanced BVMT

$\circ$	**e**	**i**	**j**
e	**e**	**i**	**j**
i	**0**	**0**	**0**
j	**j**	**i**	**e**

Case of Table 6. The set of the left-side local units corresponding to the vector $V = (a, b, c)$ such that $a + b \neq 0$, is described by the following formula (where $h = 0, 1, \ldots, p-1$):

$$E_l = (1, h, 0)\,.$$

There exists only one local right-side unit E_r corresponding to the vector $V = (a, b, c)$, which is equal to the local bi-side unit E':

$$E_r = E' = \left(1, \frac{b}{a+b}, 0\right).$$

Table 7: Alternative **i**-unbalanced BVMT

$\circ$	**e**	**i**	**j**
e	μ**e**	μ**i**	τ**e**
i	μ**i**	**0**	τ**i**
j	μ**j**	τ**i**	τ**j**

Case of Table 7. The set of the right-side local units of the vector $V = (a, b, c)$, where $\tau \neq 0$ and $\mu a + \tau c \neq 0$, is described as follows (where $h = 0, 1, \ldots, p-1$):

$$E_l = \left(h, 0, \frac{1}{\tau} - \frac{\mu}{\tau}h\right).$$

There exists only one local left-side unit E_l for the vector V, which is equal to the local bi-side unit E':

$$E_r = E' = \left(\frac{a}{\mu a + \tau c}, 0, \frac{c}{\mu a + \tau c}\right).$$

We note that Tables 1 and 3 define some new unbalanced BMVTs, when one of structural coefficients is equal to zero. For FNAAs defined with every one of the considered unbalanced BVMTs (see Tables 4 to 7) Proposition 1 is not valid. However Proposition 1 is valid for FNAAs defined by unbalanced BVMTs obtained by taking one structural coefficient equal to zero in Tables 1 and 3.

5. Discussion and potential application

One of the interesting properties of the investigated FNAAs is mutual associativity of all modifications of the parameterized non-commutative multiplication operation.

In the literature, parameterized commutative multiplication operation for the cases $m = 2$ and $m = 3$ [5] does not possess such property. Like in BVMTs used

in [4] for defining 2-dimensional FNAAs, each of Tables 1 and 3 represents m repetitions of the sequence of m basis vectors which are written as strings or as columns of the table. Every cell of the given column in Table 1 and every cell of the given row in Table 3 contains the same structural coefficient. In general case coefficients relating to different columns in Table 1 and different rows in Table 3 are different.

It is easy to check that BVMT with such structure defines associative non-commutative multiplication in finite vector space having arbitrary dimension m. We have preliminary considered the properties of the FNAA of the vectors having dimensions $m = 4, 5, 6$. Properties of such FNAAs resemble the results described in Sections 2 and 3, including mutual associativity of the modifications of the multiplication operation parameterized with different sets of structural coefficients. Detailed consideration of the cases $m > 3$ represents interest for independent research. One can expect that for $m > 3$ there are significantly more variants of different BVMT defining associative non-commutative multiplication operation. An example relating to the case $m = 4$ is presented in [2], though the modifications of the parameterized multiplication operation of that example are not mutually associative.

The FNAA considered in [2] represents a finite non-commutative ring with (global) bi-side unit. One can expect that in the cases $m \geq 4$, when designing different types of BVMTs, it is possible to construct FNAAs having qualitatively different properties.

During execution of the described research we have performed many different computational experiments to check practically the results of analytic consideration. Only results of computing local bi-side unit elements as an integer power of the corresponding vectors have been presented in the paper, since such computational experiment is more interesting due to its indirect connection with the results of analytic consideration of the systems of linear equations defining properties of the multiplication operation.

In the case of FNAA defined with balanced BVMT described by Table 1 one can remark the following. If some vector $V = (a, b, c)$ satisfies the condition $\mu a + \tau b + \lambda c \neq 0$, then for arbitrary integer i the vector V^i can not act as the right zero-divisor relatively all 3-dimensional vectors, except $(0, 0, 0)$.

Indeed, assumption $D \circ V^i = (0, 0, 0)$ leads to contradiction with Proposition 4. Therefore the sequence $V, V^2, \ldots V^i, \ldots$, does not contain the vector $(0, 0, 0)$ and is periodic. The last leads to conclusion that such sequence contains local bi-side unit element E' corresponding to V, i.e., for some integer ω we have $V^\omega = E'$. Thus, the subset $\left\{V, V^2, \ldots V^\omega\right\}$ of 3-dimensional vectors represents a cyclic finite group contained in the FNAA.

Mutual associativity of the multiplication modifications represent interest as cryptographic primitive for designing secret key cryptoschemes in which operations are used as key elements.

Regarding the public-key cryptoschemes it is interesting to consider designs based on computational complexity of the hidden conjugacy search problem (that

can be called alternatively the discrete logarithm problem in a hidden cyclic subgroup) in FNAAs of 3-dimensional vectors.

Suppose W to be some vector generating commutative finite multiplicative group having sufficiently large order ω, in which the bi-side local unit element E'' connected with W is the unit of such group.

One can define the following homomorphism $\varphi_{W,t}$ over the subset of elements $\{V_{E''}\}$ of the FNAA which are described as follows $V_{E''} = V \circ E''$, where V takes on all values in the FNAA.

Like standard automorphisms ψ_U of some finite non-commutative ring, which are described by formula $\psi_U(V) = U^{-1} \circ V \circ U$, where U is an invertible element of the ring and V takes on all values in the ring, one can define the homomorphism $\varphi_{W,t}$ as follows:

$$\varphi_{W,t}\left(V_{E''}\right) = W^{\omega-t} \circ V_{E''} \circ W^{t}.$$

To construct public-key cryptoschemes, like that described in [2, 3], one can select some vector G generating a cyclic group (that is a subset of elements of the FNAA) having sufficiently large order g, which satisfies the condition $G \circ W \neq W \circ G$ and use the formula

$$Y = W^{\omega-t} \circ (G \circ E'')^{x} \circ W^{t},$$

where Y is public key and the pair of numbers (t, x) is private key (the integers $t < \omega$ and $x < \omega$ are to be selected at random).

Suppose Y_A and Y_B are public keys of the users A and B respectively. Then they are able to generate a common secret key

$$Z_{AB} = W^{\omega-t_A} \circ (Y_B)^{x_A} \circ W^{t_B} = W^{\omega-t_B} \circ (Y_A)^{x_B} \circ W^{t_B},$$

where (t_A, x_A) and (t_B, x_B) are private keys of the users A and B respectively.

It should be noted that the used balanced BVMTs for defining 3-dimensional FNAAs are particular cases of the BVMTs for defining m-dimensional FNAAs, which are presented as Tables 8 and 9, where $\mu_i \in GF(p)$, $(i = 1, 2, \ldots, m)$ are structural coefficients.

Proposition 5. *The multiplication of the m-dimensional vectors*

$$V = (v_1, v_2, \ldots, v_i, \ldots, v_m) = v_1\mathbf{e}_1 + v_2\mathbf{e}_2 + \ldots + v_i\mathbf{e}_i + \ldots + v_m\mathbf{e}_m$$

for an arbitrary integer $m \geqslant 2$, defined by Tables 8 and 9, is an associative operation.

Table 8: The BVMT for defining m-dimensional FNAA

$\circ$	$\mathbf{e_1}$	$\mathbf{e_2}$	$\ldots$	$\mathbf{e_m}$
$\mathbf{e_1}$	$\mu_1\mathbf{e}_1$	$\mu_2\mathbf{e}_1$	$\ldots$	$\mu_m\mathbf{e_1}$
$\mathbf{e_2}$	$\mu_1\mathbf{e}_2$	$\mu_2\mathbf{e}_2$	$\ldots$	$\mu_m\mathbf{e_2}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$\mathbf{e_m}$	$\mu_1\mathbf{e}_m$	$\mu_2\mathbf{e}_m$	$\ldots$	$\mu_m\mathbf{e}_m$

Table 9: Alternative BVMT for defining m-dimensional FNAA

$\circ$	$\mathbf{e_1}$	$\mathbf{e_2}$	...	$\mathbf{e}_m$
$\mathbf{e_1}$	$\mu_1\mathbf{e}_1$	$\mu_1\mathbf{e}_2$	...	$\mu_1\mathbf{e}_m$
$\mathbf{e_2}$	$\mu_2\mathbf{e}_1$	$\mu_2\mathbf{e}_2$	...	$\mu_2\mathbf{e}_m$
...	...	...	...	...
$\mathbf{e}_m$	$\mu_m\mathbf{e}_1$	$\mu_m\mathbf{e}_2$	...	$\mu_m\mathbf{e}_m$

To prove the last statement it is sufficient to show that for arbitrary ordered set of three basis vectors $\mathbf{e}_i$, $\mathbf{e}_j$ and $\mathbf{e}_k$ the following formula holds:

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = \mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k)\,.$$

In the case of Table 8 we have

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = (\mu_j\mathbf{e}_i) \circ \mathbf{e}_k = \mu_j\mu_k\mathbf{e}_i$$

and

$$\mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ (\mu_k\mathbf{e}_j) = \mu_j\mu_k\mathbf{e}_i.$$

In the case of Table 9 we have

$$(\mathbf{e}_i \circ \mathbf{e}_j) \circ \mathbf{e}_k = (\mu_i\mathbf{e}_j) \circ \mathbf{e}_k = \mu_i\mu_j\mathbf{e}_k$$

and

$$\mathbf{e}_i \circ (\mathbf{e}_j \circ \mathbf{e}_k) = \mathbf{e}_i \circ (\mu_j\mathbf{e}_k) = \mu_i\mu_j\mathbf{e}_k.$$

5. Conclusion

In the present paper, the 3-dimensional FNAAs are introduced. The used BVMTs define the parameterized non-commutative multiplication operation in finite space of 3-dimensional vectors. They have sufficiently simple structure and represent particular cases of two general-type BVMTs (see Tables 8 and 9) that can be used for defining FNAAs of arbitrary dimension $m \geqslant 2$.

An interesting feature of the considered FNAAs is existence of different sets of elements that act (on some other sets of elements) as the single-side unit elements. Except the elements that are square roots of zero, to every element W of the FNAAs corresponds one two-side unit E''_W. Usually, to different elements correspond different two-side units and therefore the lasts are called local.

For the given local unit E''_W over the subset $\{V \circ E''_W\}$ a homomorphism can be defined and used for constructing public-key cryptoschemes based on computational difficulty of the discrete logarithm problem in a hidden cyclic group of the FNAAs.

Future research in the context of the concerned topic is connected with study of the m-dimensional FNAAs for the cases $m \geqslant 4$, which are defined by Tables 8 and 9. It is also interesting to consider other variants of BVMTs for defining 3-dimensional FNAAs and to investigate the properties of the lasts.

References

[1] **A.S. Kuzmin, V.T. Markov, A.A. Mikhalev, A.V. Mikhalev, A.A. Nechaev**, *Crypto-graphic algorithms on groups and algebras*, J. Math. Sci. **223** (2017), 629 – 641.

[2] **D.N. Moldovyan**, *Non-commutative finite groups as primitive of public-key cryptoschemes*, Quasigroups and Related Systems **18** (2010), 165 – 176.

[3] **D.N. Moldovyan, N.A. Moldovyan**, *Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms*, Quasigroups Related Systems **18** (2010), 177 – 186.

[4] **A.A. Moldovyan, N.A. Moldovyan, and V.A. Shcherbacov**, *Non-commutative finite associative algebras of 2-dimension vectors*, Computer Sci. J. Moldova **25** (2017), 344 – 356.

[5] **N.A. Moldovyan and P.A. Moldovyanu**, *Vector form of the finite fields* $GF(p^m)$, Bul. Acad. Ştiinţe Repub. Mold. Mat. **3** (2009), 57 – 63.

[6] **E. Sakalauskas, P. Tvarijonas, and A. Raulynaitis**, *Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level*, Informatica **18** (2007), 115 – 124.

Received March 29, 2018

D. Moldovyan
St. Petersburg Electrotechnical University "LETI"
Email: maa1305@yandex.ru

N.Moldovyan
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
Email: nmold@mail.ru

V. Shcherbacov
Institute of Mathematics and Computer Science of the Academy of Sciences of Moldova
victor.scerbacov@math.md

Quasigroups and Related Systems **26** (2018), 121 – 138

Torsion-unitary Cayley graph of an R-module as a functor

Ali Ramin and Ahmad Abbasi

Abstract. Let R be a commutative ring with $1 \neq 0$ and $U(R)$ be the set of unit elements. Let M be an R-module and $T(M)$ the set of torsion elements. In this paper, we introduce and investigate the torsion-unitary *Cayley graph* of M, denoted by $\Upsilon_R(M)$. It is a simple graph with vertex set $M \times R$, and two elements $(m,r),(n,s) \in M \times R$ are adjacent if and only if $(m,r)-(n,s) \in T(M) \times U(R)$. We observe that $\Upsilon_R(-)$ acts as a functor on the category of modules. We also introduce the exact sequence of Cayley graphs and determine the properties of functor $\Upsilon_R(-)$.

1. Introduction

The Cayley graph introduced by Arthur Cayley in 1878 is a useful tool for connection between group theory and the theory of algebraic graphs. Let G be an abelian additive group, C be a subset of G. Whenever $0 \notin C$ and $-C = \{-c \,|\, c \in C\} \subseteq C$, then the Cayley graph $Cay(G,C)$ is the graph with vertex set G and edge set $\{\{a,b\} \,|\, a-b \in C\}$. The Cayley graphs as a subcategory of category of graphs is denoted by $\mathfrak{C}$. We refer the reader to [8] for general properties of Cayley graphs.

In recent years, for a ring R and M as an R-module, Cayley graphs of the abelian group $(R,+)$ and $(M,+)$ with respect to subsets of R and M have received much attention in the literature. Suppose that $Z(R)$, $U(R)$, $J(R)$ and $Nil(R)$ are the set of zero-divisors, the set of unit elements, the Jacobson radical of R and the ideal of nilpotent elements, respectively. In [4] and [12], the authors obtained some basic properties of $Cay(R,U(R))$, denoted by G_R, which is usually called the unitary Cayley graph. Also in [11], D. Kiani and M. Molla Haji Aghaei show that if $G_R \cong G_S$, then $R/J(R) \cong S/J(S)$ where R and S are finite commutative rings. Moreover, in [13], J. Sato and K. Baba studied the chromatic number of $Cay(R, Z(R) \setminus \{0\})$. In [14], Shekarriz et al. tried to answer the naturally arising question: Under what conditions on a finite commutative ring R, do we have $\tau(R) \cong Cay(R, Z(R) \setminus \{0\})$? where $\tau(R)$ is the total graph defined in [5]. Also G. G. Aalipour and S. Akbari continued to investigate the properties of $Cay(R, Z(R) \setminus \{0\})$ in [1] and [2]. Let M be an R-module where the collection of prime submodules is non-empty. Let N_Λ be an arbitrary union of prime

2010 Mathematics Subject Classification: 05C25, 05C60, 13C60
Keywords: Cayley graph, torsion element, unit element, categorical product of graph.

submodules and $T(M) = \{m \in M \,|\, rm = 0 \text{ for some } 0 \neq r \in R\}$ be the set of torsion elements of M. Also, suppose that $c \in U(R)$ such that $c^{-1} = c$. In [3], we define the extended total graph of M as a simple graph $T\Gamma_c(M, N_\Lambda)$ with vertex set M, and two distinct elements $x, y \in M$ are adjacent if and only if $x + cy \in N_\Lambda$ and study some graph theoretic results of it. Also In [6], the authors show that if $M \neq T(M)$, then $T(M)$ is a union of prime submodules of M. Hence in [3], we investigate some properties of $T\Gamma_{-1}(M, T(M)) = Cay(M, T(M) \setminus \{0\})$ too. These provide a motivation to introduce a graph over an R-module as a functor from category of modules to subcategory of graphs.

In this paper, we introduce the torsion-unitary Cayley graph of M, denoted by $\Upsilon_R(M)$. It is a simple graph with vertex set $M \times R$, and two elements $(m, r), (n, s) \in M \times R$ are adjacent if and only if $(m, r) - (n, s) \in T(M) \times U(R)$. We show that it acts as a functor over an R-module. Also we introduce two functors, unitary Cayley graph and torsion graph and study some category theoretic properties of them. The motivation is based the fact that any ring homomorphism and R-module homomorphism preserves the unit elements and the torsion elements, respectively. Of course, any ring homomorphism preserves idempotent and nilpotent elements too. But to make a simple graph (without loop), the set of unit elements is used in definition.

In Section 2, we determine some basic properties of $\Upsilon_R(M)$. In section 3, the graph $\Upsilon_R(M)$ will be studied in finite mode. Also in the end of this section, an example will be provided to demonstrate defects of proof given in [14, Theorem 5.2]. It is not counterexample for [14, Theorem 5.2], which is only indicated counting the number of vertices of a maximal clique of $\tau(R)$ is very complicated in this case (a clique in a graph G is a subset of pairwise adjacent vertices). We also show errors underlying their proof. In the last section, we define the functor $\Upsilon_R : \mathfrak{M}_R \to \mathfrak{C}$ with $\Upsilon_R(M) = Cay(M \times R, T(M) \times U(R))$ where $\mathfrak{M}_R$ is the R-module category. Let $\phi : M \to N$ be an R-module homomorphism, then $\Upsilon_R(\phi) : \Upsilon_R(M) \to \Upsilon_R(N)$ given by $\Upsilon_R(\phi)((m, r)) = (\phi(m), r)$ is a homomorphism of graphs. Also let $\mathfrak{R}$ be the category of ring and let $T\Gamma_R(M)$ be $Cay(M, T(M) \setminus \{0\})$ with loop on all vertices. Then $\Upsilon^u : \mathfrak{R} \to \mathfrak{C}$ and $\Upsilon^t : \mathfrak{M}_R \to \mathfrak{C}$ are functors, with $\Upsilon^u(R) = G_R$ and $\Upsilon^t(M) = T\Gamma_R(M)$ respectively. In this section, we investigate the properties of these functors and introduce an exact sequence of cayley graphs.

Throughout this article, all rings are assumed to be commutative with nonzero identity. Let R be an Artinian ring, the structure theorem [7, Theorem 8.7] implies that $R \cong R_1 \times \ldots \times R_t$, where each R_i is a local ring with maximal ideal $\mathfrak{m}_i$; this decomposition is unique up to permutation of factors. We denote by k_i the residue field $R_i/\mathfrak{m}_i$ and $f_i = |k_i|$. We also assume (after appropriate permutation of factors) that $f_1 \leqslant f_2 \leqslant \ldots \leqslant f_t$. As usual, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_n$, and $\mathbb{F}_q$ will denote the integers, rational numbers, integers modulo n, and the finite field with q elements, respectively. R is reduced if $Nil(R) = \{0\}$. For more notations, we refer the reader to [7].

Let G be a graph with the vertex set $V(G)$. A graph G is totally disconnected if no two vertices of G are adjacent. The complement of G is denoted by $\overline{G}$.

For vertices x and y of G, the length of a shortest path from x to y is denoted by $d_G(x,y)$ ($d_G(x,x)=0$ and $d_G(x,y)=\infty$ if there is no such path). The diameter of G is $diam(G)=sup\{d_G(x,y)|x$ and y are vertices of $G\}$. The girth of G, denoted by $gr(G)$, is the length of a shortest cycle in G ($gr(G)=\infty$ if G contains no cycles). The complete graph on n vertices is denoted by K_n. A graph G is called bipartite if its vertex set can be represented as the union of two disjoint sets V_1 and V_2, such that every edge of G connects an element of V_1 with one of V_2. We call V_1, V_2 a bipartition of $V(G)$. The union of two simple graphs (with loop) G and H is the graph $G\cup H$ with the vertex set $V(G)\cup V(H)$ and the edge set $E(G)\cup E(H)$. Also $\bigcup_{i=1}^{t} G$ is denoted by tG. Let $\mathcal{P}=\{V_1,...,V_k\}$ be a partition of the vertex set of G into non-empty classes. The quotient $G/\mathcal{P}$ of G by $\mathcal{P}$ is the graph whose vertices are the sets $V_1,...,V_k$ and whose edges are the pairs $[V_i,V_j]$ such that there are $u_i\in V_i, u_j\in V_j$ with $[u_i,u_j]\in E(G)$. The mapping $\pi_{\mathcal{P}}: V(G)\to V(G/\mathcal{P})$ defined by $\pi_{\mathcal{P}}(u)=V_i$ such that $u\in V_i$, is the natural map for $\mathcal{P}$. Quotients often provide a way of deriving the structure of an object from the structure of a larger one. Observe that $\pi_{\mathcal{P}}$ is a homomorphism and it is automatically faithful. If φ is a homomorphism of graph from X to Y, then the preimages $\varphi^{-1}(y)$ of each vertex y in Y are called the fibres of φ. The fibres of φ determine a partition $\mathcal{K}_\varphi$ of $V(X)$ called the kernel of φ. If Y has no loops, then the kernel is a partition into independent sets. Given a graph X together with a partition $\mathcal{K}_\varphi$ of $V(X)$, define a graph $X/\mathcal{K}_\varphi$ with vertex set the cells of $\mathcal{K}_\varphi$ and with an edge between two cells if there is an edge of X with an endpoint in each cell (and a loop if there is an edge within a cell). The set of finite simple graphs, denoted by Θ. A graph with loop on all vertices, denoted by G°. The set of finite simple graphs in which loops are admitted is denoted by Θ°. The *categorical product* of G and H is the graph, denoted by $G\times H$, and vertex set $V(G)\times V(H)$, such that vertices (g,h) and (g',h') are adjacent precisely if $gg'\in E(G)$ and $hh'\in E(H)$. Other names for the categorical product that have appeared in the literature are *tensor product*, *Kronecker product* or *direct product*. We know that the categorical product is commutative and associative. Let G_1 and G_2 be graphs. Also let G be a subgraph of G_1 and $V\subseteq V(G_2)$ be the set of disjoint vertices, then $G\times V$ is denoted by G^V.

2. Torsion-unitary Cayley graph

In this section, we define the torsion-unitary Cayley graph of M and we obtain some its basic properties and categorical product. Also, the relationship between the torsion-unitary Cayley graph and the unitary Cayley graph will be expressed.

Definition 2.1. Let R be a commutative ring with nonzero identity and M be an R-module. The *torsion-unitary Cayley graph* of M is a simple graph with vertex set $M\times R$, and two elements $(m,r),(n,s)\in M\times R$ are adjacent if and only if $(m,r)-(n,s)\in T(M)\times U(R)$. This graph is denoted by $\Upsilon_R(M)$.

Definition 2.2. Let R be a commutative ring with nonzero identity and M be an R-module. The *torsion graph* of M, denoted by $T\Gamma_R(M)$, is the graph, whose vertex set is M, and in which $\{m,n\}$ is an edge if and only if $m-n \in T(M)$ (i.e., $T\Gamma_R(M) \cong Cay(M, T(M)\setminus\{0\})^\circ$).

In what follows, the some properties of categorical product is recalled.

Remark 2.3. Let $K_1^\circ \in \Theta^\circ$ denote the graph with exactly one vertex, on which there is a loop. Observe that $K_1^\circ \times G \cong G$ for any $G \in \Theta^\circ$. Therefore, under the operations $\times$ and $+$, the set Θ° is a commutative semiring with unit K_1°. Also if G has no loop at g, then $H^{\{g\}}$ is totally disconnected; whereas if G has a loop at g, then $H^{\{g\}}$ is isomorphic to H. Let $G = G_1 \times G_2 \times \cdots \times G_k = \prod_{i=1}^k G_i$. By simple rewording of the definitions, each projection $p_i : G \to G_i$ is a homomorphism. Furthermore, given a graph H and a collection of homomorphisms $\varphi_i : H \to G_i$, for $1 \leqslant i \leqslant k$, observe that the map $\varphi : x \mapsto (\varphi_1(x), \varphi_2(x), \ldots, \varphi_k(x))$ is a homomorphism $H \to G$. From the two facts just mentioned, we see that every homomorphism $\varphi : H \to G$ has the form $\varphi : x \mapsto (\varphi_1(x), \varphi_2(x), \ldots, \varphi_k(x))$, for homomorphisms $\varphi_i : H \to G_i$, where $\varphi_i = p_i\varphi$. Clearly φ is uniquely determined by the p_i and φ_i.

Proposition 2.4. [9, Proposition 5.7] *Suppose (g,h) and (g',h') are vertices of a categorical product $G\times H$, and n is an integer for which G has a g,g'-walk of length n and H has an h,h'-walk of length n. Then $G \times H$ has a walk of length n from (g,h) to (g',h'). The smallest such n (if it exists) equals $d_{G\times H}((g,h),(g',h'))$. If no such n exists, then $d_{G\times H}((g,h),(g',h')) = \infty$.*

Proposition 2.5. [9, Proposition 5.8] *Suppose x and y are vertices of $G = G_1 \times G_2 \times \cdots \times G_k$. Then $d_G(x,y) = \min\{n \in \mathbb{N} \mid$ each factor G_i has a walk of length n from $p_i(x)$ to $p_i(y)\}$, where it is understood that $d_G(x,y) = \infty$ if no such n exists.*

Theorem 2.6. (**Weichsel's Theorem**, [9, Theorem 5.9]) *Suppose G and H are connected nontrivial graphs in Θ°. If at least one of G or H has an odd cycle, then $G \times H$ is connected.*

In view of the above theorem, we have the following corollary.

Corollary 2.7. *A categorical product of connected nontrivial graphs is connected if and only if at most one of the factors is bipartite.*

Remark 2.8. (1). $\Upsilon_R(M) \cong T\Gamma_R(M) \times G_R$. Since every vertex $m \in T\Gamma_R(M)$ has a loop, every $G_R^{\{m\}}$ is isomorphic to G_R, also since every vertex $r \in G_R$ has no loop, every $T\Gamma_R(M)^{\{r\}}$ is totally disconnected.

(2). Let R be an Artinian ring and suppose that $f_1 = 2$, then G_R is a bipartite graph. Note that $G_R = \prod G_{R_i}$.

Theorem 2.9. *G_R is a bipartite graph if and only if $\Upsilon_R(M)$ is a bipartite graph.*

Proof. Suppose that G_R is bipartite. Let V_1 and V_2 be bipartition of $V(G_R)$, then $T\Gamma_R(M)^{V_1}$ and $T\Gamma_R(M)^{V_2}$ are bipartition of $V(\Upsilon_R(M))$. Therefore $\Upsilon_R(M)$ is bipartite. Conversely, if G_R is not bipartite, then it has an odd cycle namely O. Hence $O^{\{m\}}$ is an odd cycle in $\Upsilon_R(M)$, since m has a loop in $T\Gamma_R(M)$, a contradiction. Therefore G_R is a bipartite graph. □

Proposition 2.10. *Let R be a commutative ring with identity and let $T(M) \neq \{0\}$, then $gr(\Upsilon_R(M)) \leq 4$. In particular, if $T(M) = \{0\}$, then $\Upsilon_R(M)$ is the union of $|M|$ disjoint G_R's, and $gr(\Upsilon_R(M)) = gr(G_R)$.*

Proof. G_R is not totally disconnected, also since $T(M) \neq \{0\}$, $\Upsilon_R(M)$ is not totally disconnected too. Since $K_2^\circ \times K_2$ is a cycle of length four, $gr(\Upsilon_R(M)) \leqslant 4$. In particular, if $T(M) = \{0\}$, then $\Upsilon_R(M) \cong \bigcup_M K_1^\circ \times G_R \cong \bigcup_M G_R$ and it is clear that $gr(\Upsilon_R(M)) = gr(G_R)$. □

By Remark 2.3, $G_R^{\{m\}}$ is isomorphic to G_R for all $m \in M$. Therefore we have the following corollary in the light of Proposition 2.4.

Corollary 2.11. *$gr(\Upsilon_R(M)) \leqslant gr(G_R)$. In particular, $gr(\Upsilon_R(M)) = 3$ if and only if $gr(G_R) = 3$. Moreover $gr(\Upsilon_R(M)) = 4$, if $gr(G_R) = 4$.*

Lemma 2.12. [8, Lemma 3.7.4] *$Cay(G, C)$ is connected if and only if C is a generating set for G.*

Remark 2.13. Let $\mathcal{G}_\mathcal{R} = \{V_1(G_R), \ldots, V_k(G_R)\}$ be a partition of the vertex set of $\Upsilon_R(M)$ where $V_i(G_R) = m_i \times R$ for $m_i \in M$ and $|M| = k$ (k can be infinite). Since m_i has a loop in $T\Gamma_R(M)$, ${G_R}^{\{m_i\}} \cong G_R$ by Remark 2.3. Hence the vertices $V_i(G_R), V_j(G_R) \in \Upsilon_R(M)/\mathcal{G}_\mathcal{R}$ are adjacent if and only if the vertices $m_i, m_j \in T\Gamma_R(M)$ are adjacent since $(m_i, 0) \in V_i(G_R)$ and $(m_j, 1) \in V_j(G_R)$ are adjacent in $\Upsilon_R(M)$ if and only if $m_i - m_j \in T(M)$. Therefore, $\Upsilon_R(M)/\mathcal{G}_\mathcal{R} \cong T\Gamma_R(M)$.

As usual, if $A \subseteq M$, then $< A >$ denotes the $\mathbb{Z}$-submodule of M generated by A.

Theorem 2.14. *Let R be a commutative ring and M an R-module. Then $\Upsilon_R(M)$ is connected if and only if $M =< T(M) >$ and $R =< U(R) >$.*

Proof. Let $\Upsilon_R(M)$ be connected. By Lemma 2.12, $M \times R =< T(M) \times U(R) >$ and so $M =< T(M) >$ and $R =< U(R) >$. Conversely, suppose that $M =< T(M) >$ and $R =< U(R) >$. By Lemma 2.12, G_R is connected and also $T\Gamma_R(M)$ is connected with loops. Consider ${G_R}^{\{m_i\}}$ for some $m_i \in M$, then ${G_R}^{\{m_i\}} \cong G_R$ by Remark 2.3. Hence there is a path in $\Upsilon_R(M)$ from (m_i, r) to (m_i, r') for $r, r' \in R$ since G_R is connected. Also since $T\Gamma_R(M)$ is connected, there is a path in $\Upsilon_R(M)/\mathcal{G}_\mathcal{R}$ from $V_i(G_R)$ to $V_j(G_R)$ for every $m_j \in M$ by the above remark. Therefore there is a path from (m_i, r) to (m_j, r') and $\Upsilon_R(M)$ is a connected graph. □

As an applications of the algebraic graph theory in modules theory, the following corollary hold by Lemma 2.12 and the above theorem.

Corollary 2.15. *Let M be an R-module, then $M \times R =< T(M) \times U(R) >$ if and only if $M =< T(M) >$ and $R =< U(R) >$.*

Theorem 2.16. *Let R be a commutative ring and M an R-module. Suppose that $\Upsilon_R(M)$ is a connected graph (i.e., $M \times R =< T(M) \times U(R) >$). If there is k which is a greatest integer i such that $m = n_1 + n_2 + \cdots + n_i$ where, $m \in M \times R$ and $n_1, ..., n_i \in T(M) \times U(R)$ with $n_1 + n_2 + \cdots + n_i$ is a shortest representation of m, then $diam(\Upsilon_R(M)) = k$. Otherwise, $diam(\Upsilon_R(M)) = \infty$. Moreover, if $\Upsilon_R(M)$ is a connected graph, then $diam(\Upsilon_R(M)) = d_{M \times R}(0, m)$.*

Proof. The proof is similar to the proof of [3, Theorem 14]. □

Remark 2.17. Let $u \in U(R)$ and $j \in J(R)$, then $u + j \in U(R)$. Hence, whenever x and y are adjacent vertices in G_R, then every element of $x + J(R)$ is adjacent to every element of $y + J(R)$. Moreover, $x + \mathfrak{m}$ is a totally disconnected subgraph of G_R where $\mathfrak{m}$ is a maximal ideal. Therefore $\bigcup_{m \in M} (x + \mathfrak{m})^{\{m\}}$ is a totally disconnected subgraph of $\Upsilon_R(M)$. Also, suppose that $M \neq T(M)$ and $\{N_\lambda\}_{\lambda \in \Omega}$ is the set of all prime submodules of M. We know that $T(M) = \bigcup_{\lambda \in \Lambda} N_\lambda$ for $\Lambda \subseteq \Omega$ as shown in [6]. Let $N^\Lambda = \bigcap_{\lambda \in \Lambda} N_\lambda$, then every element of $m + N^\Lambda$ is adjacent to every element of $n + N^\Lambda$ if m and n are adjacent vertices in $T\Gamma_R(M)$. Furthermore, $m + N_\lambda$ is a clique with loop in $T\Gamma_R(M)$, where $\lambda \in \Lambda$.

Lemma 2.18. *Let R be a commutative ring and M be an R-module. Then :*

(*i*) *$\Upsilon_R(M)$ is complete graph if and only if $M = 0$ and R is a field,*

(*ii*) *$\Upsilon_R(M)$ is vertex transitive,*

(*iii*) *$\Upsilon_R(M)$ is a regular graph of degree $|T(M)| \times |U(R)|$ with isomorphic components.*

Proof. Let $\Upsilon_R(M)$ is complete graph. Then $M = 0$ since (m, r) and (n, r) are not adjacent for every $m, n \in M$ and $r \in R$. Also R is a field since if there exists a nonunit $x \neq 0$ in R, then $(m, 0)$ and (n, x) are not adjacent. Part (*ii*) holds for every Cayley graph of a group. To prove the last part, note that under an automorphism of graph G, any component of G is isomorphically mapped to another component. Since $\Upsilon_R(M)$ is vertex-transitive, we conclude that the components of $\Upsilon_R(M)$ are isomorphic and so part (*iii*) is proved. □

3. The case when M and R are finite

In this section, all graphs considered to be finite. It is natural to seek the conditions under which $A \times C \cong B \times C$ implies $A \cong B$. We call this the cancellation problem

for the categorical product. In general, cancellation for the categorical product fails dramatically. If C is any bipartite graph, then there are always non-isomorphic graphs A and B for which $A \times C \cong B \times C$. Indeed, just take $A = K_2$ and $B = 2K_1^\circ$ (two loops), then $A \times C \cong 2C \cong B \times C$. But we say that cancellation holds for the torsion-unitary Cayley graphs in this section. Finally, we examine the validity of the proof of Theorem 5.2 in [14].

Remark 3.1. Let R be a finite commutative ring, then $\Upsilon_R(R) = \overline{G_R}^\circ \times G_R$ since R is an union of zero divisor and unit elements. Therefore if $G_R \cong G_S$, then $\Upsilon_R(R) \cong \Upsilon_S(S)$.

Corollary 3.2. *Let R be a finite commutative reduced ring and let S be a commutative ring. Then $T\Gamma_R(R) \cong T\Gamma_S(S)$ if and only if $R \cong S$.*

Proof. Let R be a finite commutative ring, then $\overline{G_R}^\circ \cong T\Gamma_R(R)$. By [11, Corollary 5.4], $R \cong S$ if and only if $T\Gamma_R(R) \cong T\Gamma_S(S)$. □

Theorem 3.3. *Suppose that R and S are commutative ring and let M be an R-S-bimodule. Then $\Upsilon_S(M) \cong \Upsilon_R(M)$ if and only if $G_S \cong G_R$ where $\Upsilon_S(M) \in \Theta$.*

Proof. It is clear by [9, Proposition 9.6]. □

Corollary 3.4. *Suppose that R and S are commutative reduced ring. let M be an R-S-bimodule such that $\Upsilon_R(M) \in \Theta$. Then $\Upsilon_S(M) \cong \Upsilon_R(M)$ if and only if $R \cong S$.*

Proof. This follow directly from [11, Corollary 5.4] and the above theorem. □

Theorem 3.5. *Suppose that there is a ring homomorphism $\psi : S \to R$ and $\Upsilon_R(M), \Upsilon_S(M) \in \Theta$. Also let M and N be R-modules. If $\Upsilon_R(M) \cong \Upsilon_R(N)$, then $\Upsilon_S(M) \cong \Upsilon_S(N)$.*

Proof. It is clear by [9, Proposition 9.9]. □

By Theorem 2.9 and [9, Proposition 9.10], if $\Upsilon_R(M) \in \Theta$ and it has an odd cycle, then $\Upsilon_R(M) \cong \Upsilon_R(N)$ if and only if $T\Gamma_R(M) \cong T\Gamma_R(N)$. Also by Lemma 2.18(*iii*), if M is a torsion or torsion-free module, then $\Upsilon_R(M) \cong \Upsilon_R(N)$ if and only if $T\Gamma_R(M) \cong T\Gamma_R(N)$ since $T\Gamma_R(M)$ and $T\Gamma_R(N)$ have loop on all vertices and minimum and maximum degree of $T\Gamma_R(M)$ and $T\Gamma_R(N)$ equal two and $|T(M)|+1$ respectively (a loop is incident to only one vertex, when measuring the degree of such a vertex, the loop is counted twice). By the following theorem, the condition that $\Upsilon_R(M)$ has an odd cycle can be omitted.

Theorem 3.6. *Let M and N be R-modules and let $\Upsilon_R(M) \in \Theta$, then*

$$\Upsilon_R(M) \cong \Upsilon_R(N) \text{ if and only if } T\Gamma_R(M) \cong T\Gamma_R(N).$$

Proof. Suppose that $\Upsilon_R(M) \cong \Upsilon_R(N)$. Since $\Upsilon_R(M) = T\Gamma_R(M) \times G_R$ and $\Upsilon_R(N) = T\Gamma_R(N) \times G_R$, $|T(M)| = |T(N)|$ by Lemma 2.18(*iii*). Hence

$$T\Gamma_R(M) \times G_R/\mathcal{G}_\mathcal{R} \cong T\Gamma_R(N) \times G_R/\mathcal{G}_\mathcal{R},$$

where $\mathcal{G}_\mathcal{R}$ is as mentioned in Remark 2.13. Therefore $T\Gamma_R(M) \cong T\Gamma_R(N)$ by Remark 2.13. □

Also, by the similar proof, the following corollary is obtained in the cancellation for the categorical product.

Corollary 3.7. *Let $A, B, C \in \Theta^\circ$. Suppose that A and B have loop on all vertices and C has at least one edge. Then $A \times C \cong B \times C$ if and only if $A \cong B$.*

Shekarriz et al. answered the isomorphic question in [14, Theorem 5.2]: Let R be a finite commutative ring, then $\tau(R) \cong Cay(R, Z(R) \setminus \{0\})$ if and only if at least one of the following conditions is true: (a) $R \cong R_1 \oplus \cdots \oplus R_k$, where $k \geq 1$ and each R_i is a local ring of an even order; (b) $R \cong R_1 \oplus \cdots \oplus R_k$, where $k \geq 2$ and each R_i is a local ring and $f_1 = 2$. But, they have errors in its proof when they conclude $\tau(R) \ncong Cay(R, Z(R) \setminus \{0\})$, supposed (a) and (b) do not hold for a finite commutative ring R. In the following, an example will be provided to demonstrate defects of proof given in [14, Theorem 5.2], and we investigate the method of proof too. The equivalence class $Z(R_i) + a_i$, is denoted by $[a_i]$.

Example 3.8. Let $R = \mathbb{F}_4 \oplus \mathbb{F}_4 \oplus \mathbb{Z}_3$ and $(1,1,1), (0,0,-1) \in R$, denoted by 1 and x, respectively. Then $\tau(\mathbb{F}_4 \oplus \mathbb{F}_4 \oplus \mathbb{Z}_3)$ has five maximal cliques, all containing the edge $\{1, x\}$, which are given separately as follows:

(*a*). Let $c_1 = ([1],[0],\mathbb{Z}_3)$, $c_2 = (\mathbb{F}_4,[0],[-1])$ and $c_3 = ([1],\mathbb{F}_4,[1])$, then $c_1 \cup c_2 \cup c_3$ forms a maximal clique, where $|c_1 \cup c_2 \cup c_3| = |c_1| + |c_2| + |c_3| - |c_1 \cap c_2| - |c_1 \cap c_3| - |c_2 \cap c_3| + |c_1 \cap c_2 \cap c_3| = 3 + 4 + 4 - 1 - 1 - 0 + 0 = 9$.

By permuting the first two components, a new maximal clique will be generated: $([0],[1],\mathbb{Z}_3) \cup ([0],\mathbb{F}_4,[-1]) \cup (\mathbb{F}_4,[1],[1])$. Since, $|R|/f_1 = |R|/f_2$, these two cliques will be equal in size. Moreover, in these maximal cliques, vertices 1 and x are already counted.

(*b*). Let $c_1 = ([1],\mathbb{F}_4,[1])$ and $c_2 = ([0],\mathbb{F}_4,[-1])$, then $c_1 \cup c_2$ forms a maximal clique, where $|c_1 \cup c_2| = |c_1| + |c_2| - |c_1 \cap c_2| = 4 + 4 - 0 = 8$. By permuting the first two components, a new maximal clique will be generated:

$$(\mathbb{F}_4,[1],[1]) \cup (\mathbb{F}_4,[0],[-1]).$$

Since, in this example, $|R|/f_1 = |R|/f_2$, these two cliques will be equal in size. Moreover, in these maximal cliques, vertices 1 and x are already counted.

(*c*). Let $c_1 = ([1],[0],[0])$, $c_2 = ([0],[1],[0])$, $c_3 = ([1],[1],[1])$ and $c_4 = ([0],[0],[-1])$, then $c_1 \cup c_2 \cup c_3 \cup c_4$ forms a clique of maximal size 4. It should be noted that, the mutual intersection of every pair of c_i's is empty, for $i = 1, \ldots, 4$, and vertices 1 and x are already counted.

Remark 3.9. Note that this example is not contra example for [14, Theorem 5.2], this is an example which determines the method of counting the number of vertices of a maximal clique of $\tau(R)$ is not true. Let $R = R_1 \oplus R_2 \oplus R_3$ where R_1 and R_2 are even such that $R_i/Z(R_i) \cong \mathbb{F}_{2^t}$, for $i = 1, 2$ and $t \geqslant 2$, and R_3 is odd. Then the layouts of equivalence classes of maximal cliques containing the edge $\{1, x\}$ are as the above example.

Now, let us return to the main subject concerning the flaws in the proof of [14, Theorem 5.2].

The findings discussed in the proof are well-reasoned until they were going to show that for $i = 1, \ldots, k$, the edge $\{1, x\}$ does not belong to a maximal $(|R|/f_i)$-clique in $\tau(R)$. In that proof, it is supposed that $\{y_s | s \in S\}$ is a set of elements of R of maximal size which are adjacent to both 1 and x and also to themselves. It is also cited that if $\{y_s \,|\, s \in S\} \cup \{1, x\}$ forms a clique of maximal size $|R|/f_i$, then there must be $1 \leqslant m_1 < m_2 < \cdots < m_q \leqslant k$; $0 \leqslant q \leqslant k$ such that all y_s's belong to

$$R_1 \oplus \cdots \oplus R_{m_1-1} \oplus [a_{m_1}] \oplus R_{m_1+1} \oplus \cdots \oplus R_{m_q-1} \oplus [a_{m_q}] \oplus R_{m_q+1} \oplus \cdots \oplus R_k. \quad (1)$$

Now, according to this direct sum and ambiguity in the assumption, y_s's could be chosen in three following ways:

(1) y_s's belong to (1) in which a_{m_i} and m_i are fixed for all $i = 1, \ldots, q$. Based on maximal cliques in the example 3.8(a), 3.8(b) and 3.8(c), $\{y_s | s \in S\} \cup \{1, x\}$ is not a maximal clique. It shows that the argument can not be true.

(2) y_s's belong to (1) in which only m_i are fixed for all $i = 1, \ldots, q$. Now, example 3.8(a) shows that $\{y_s | s \in S\} \cup \{1, x\}$ is not a maximal clique.

(3) y_s's belong to (1) in such away a_{m_i}, m_i and q can vary. Thus q will be replaced with q_λ in (1), for some $\lambda \in \Lambda$ such that $1 \leqslant q_\lambda \leqslant k$, and $y_{S_\lambda} = \{y_s | s \in S_\lambda\}$'s are contained in the representation (1), where $S_\lambda \subseteq S$ such that for all $s \in S_\lambda$, the elements of y_{S_λ} in (1) have a fixed representation (i.e., m_{i_λ} and q_λ are fixed). In Example 3.8, y_{S_λ} is the set of vertices of a clique c_i. Based on deduction in [14, Theorem 5.2], $q_\lambda \neq 1$. If $q_\lambda \geqslant 2$, then $|y_{S_\lambda}| = \dfrac{|R|}{\prod_{i=1}^{q_\lambda} f_{m_i}}$, and the required number is calculated by $|\bigcup y_{S_\lambda}|$ as in Example 3.8.

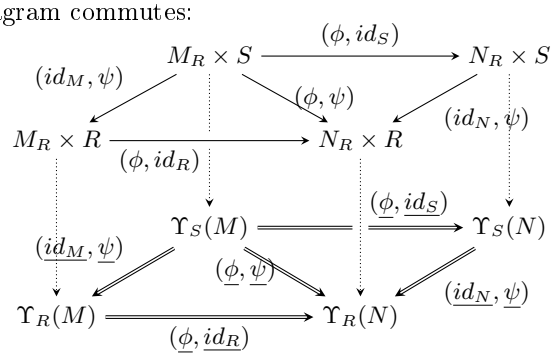
The counting method given in [14, Theorem 5.2] implies that the authors have considered either conditions (1) or (2). Moreover, in the proof, where it is supposed that $2 \leqslant q \leqslant k$, if $[a_{m_p}] = [-1_{m_p}]$ and $[a_{m_v}] = [-x_{m_v}]$ for some $v \neq p$, $1 \leqslant p \leqslant j$ and $j+1 \leqslant v \leqslant k$, then 1 may belong to $\{y_s | s \in S\}$. Correspondingly, if $1 \leqslant v \leqslant j$ and $j + 1 \leqslant p \leqslant k$, then x may belong to $\{y_s | s \in S\}$. Therefore, it is generally incorrect to add 2 in counting the total number of vertices of maximal cliques.

4. Torsion-unitary Cayley functor

In this section, we define torsion-unitary Cayley functor and determine some of its categorical properties.

Definition 4.1. Let R be a commutative ring with nonzero identity and M be an R-module. The functor $\Upsilon_R : \mathfrak{M}_R \to \mathfrak{C}$ with $\Upsilon_R(M) = Cay(M \times R, T(M) \times U(R))$ is a covariant functor. It is easily verified that if $\phi : M \to N$ is an R-module homomorphism, then $\Upsilon_R(\phi) : \Upsilon_R(M) \to \Upsilon_R(N)$ given by $\Upsilon_R(\phi)((m,r)) = (\phi(m), r)$ is a homomorphism of graph.

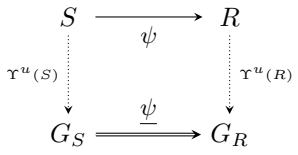
Remark 4.2. In general, let R and S be commutative rings, $\psi : S \to R$ a ring homomorphism. Suppose that M_R and N_R are R-modules and $\phi : M \to N$ is an R-module homomorphism. Then $M_R \times S$ and $N_R \times S$ are S-modules, $\Upsilon_R(\underline{\phi}, \underline{\psi}) : \Upsilon_S(M_R) \to \Upsilon_R(N_R)$ given by $\Upsilon_S(\underline{\phi}, \underline{\psi})((m,r)) = (\underline{\phi}(m), \underline{\psi}(r))$ is a homomorphism of graph ($(\underline{\phi}, \underline{id_R})$ replace by $(\underline{\phi}, \underline{\psi})$ in the above definition) and the following diagram commutes:



where, $(\longrightarrow)$ denotes S-module homomorphisms, $(\Longrightarrow)$ denotes homomorphisms of graph and $(\dashrightarrow)$ denotes functors.

By Remark 2.3, if $R = M = 0$, then $G_R = T\Gamma_R(M) = K_1^\circ$. So the followings hold:

(a) Let $M = 0$, then $M \times R \cong R$, $\Upsilon_R(M) \cong G_R$, $\Upsilon_-(0)$ is a functor from category of rings to unitary Cayley graphs as a subcategory of graphs category, denoted by $\Upsilon^u(-)$, and the following diagram commutes:



(b) Let M be an R-module, then $\Upsilon_0(-)$ is a functor from $\mathfrak{M}_R$ to torsion graphs as a subcategory of category of graphs, denoted by $\Upsilon^t(-)$. Note that, in this case, graphs are not simple such that every vertex has a loop.

We say that a functor $F : C \to D$ preserves a property $\mathfrak{P}$ of a morphism f in C if $F(f)$ in D also has the property $\mathfrak{P}$. We say that F reflects a property $\mathfrak{P}$ if f has $\mathfrak{P}$ in C whenever $F(f)$ has $\mathfrak{P}$ in D. Analogous definitions can be made with respect to properties of objects. It is clear that every functor preserves commutative diagrams. A homomorphism f from G to $f(G) \subseteq H$ is called a retraction if there exists an injective homomorphism g from $f(G)$ to G such that $fg = id_{f(G)}$. In this case $f(G)$ is called a retract of G, and then G is called a coretract of $f(G)$ while g is called a coretraction. According to the definition of the functor Υ, we have the following corollary.

Corollary 4.3. *The functor Υ preserves and reflects injective mappings and surjective mappings. It preserves retractions and coretractions.*

A homomorphism $\varphi : G \to H$ is called $faithful$ if $\varphi(G)$ is an induced subgraph of H. It will be called $full$ if $\{g, g'\} \in E(G)$ if and only if $\{\varphi(g), \varphi(g')\} \in E(H)$. Let G be a simple graph and φ a full homomorphism, then $\varphi^{-1}(h) \cup \varphi^{-1}(h')$ induces a complete bipartite graph whenever $\{h, h'\} \in E(H)$.

Corollary 4.4. *Let S be a commutative ring and M be an R-module. Suppose that $\psi' : S \to S/J(S)$ and $\phi' : M \to M/N^{\Lambda}$ are the canonical homomorphism, where N^{Λ} is as mentioned in Remark* 2.17. *Then $\Upsilon^u(\psi')$ and $\Upsilon^t(\phi')$ are full homomorphism of graph.*

Let $m' \in T(M)$, then $\underline{\sigma_{m'}} : G_R \to T\Gamma_R(M)$ given by $\underline{\sigma_{m'}}(r) = rm'$ is a homomorphism since $Im(\underline{\sigma_{m'}})$ is a complete graph with loop.

Proposition 4.5. *Let $m \in M \setminus T(M)$ such that $U(R) = R \setminus (T(M) : m)$, then $\underline{\phi_m} : G_R \to \overline{T\Gamma_R(M)}$ given by $\underline{\phi_m}(r) = rm$ is a full homomorphism. In particular, if R is a finite commutative ring, then $\underline{\phi_m}$ is a full homomorphism for all $m \in M \setminus T(M)$.*

Proof. It is clear that $\underline{\phi_m}$ is a homomorphism of graphs. Suppose that $\{r_1m, r_2m\}$ is an edge in $\overline{T\Gamma_R(M)}$ for some $r_1, r_2 \in R$, then $u = r_2 - r_1 \in U(R)$ since $um \in T(M)$ if and only if $u \in R \setminus U(R) = (T(M) : m)$ for $m \in M \setminus T(M)$. Therefore $\underline{\phi_m}$ is full. For the "in particular" statement, suppose that R is finite. Hence $U(R) = R \setminus (T(M) : m)$ for all $m \in M \setminus T(M)$ since every regular element of a finite commutative ring is a unit. □

Remark 4.6. In Remark 4.2, $\underline{\psi}$ is a faithful homomorphism if and only if $\psi^{-1}(\psi(s)) \cap U(S) \neq \varnothing$ for all $\psi(s) \in U(R)$ because if $\{\underline{\psi}(s_1), \underline{\psi}(s_2)\}$ is an edge in G_R for some $s_1, s_2 \in S$, then $(s_2 + k_2) - (s_1 + k_1) \in U(S)$ for some $k_1, k_2 \in Ker(\psi)$. According to the same reason, $\underline{\phi}$ is a faithful homomorphism if and only if $\phi^{-1}(\phi(s)) \cap T(M) \neq \varnothing$ for all $\phi(s) \in T(N)$. Also, $\underline{\psi}$ is a full homomorphism if and only if $\psi^{-1}(\psi(s)) \subseteq U(S)$ for all $\psi(s) \in U(R)$ because if $\psi(s) \in U(R)$, then $\{\psi(s), \psi(0)\}$ is a edge in G_R and so $s - 0 \in U(S)$ since $\underline{\psi}$ is a full homomorphism. According to the same reason, $\underline{\phi}$ is a full homomorphism if and only if $\phi^{-1}(\phi(m)) \subseteq T(M)$

for every $\phi(m) \in T(N)$. Moreover, the homomorphism $(\underline{\phi}, \underline{\psi})$ is faithful (full) if and only if each of $\underline{\phi}$ and $\underline{\psi}$ is faithful (full).

Proposition 4.7. *Let $\psi : S \to R$ be a ring homomorphism such that the induced map $Spec(R) \to Spec(S)$ is surjective. Then $\underline{\psi} : G_S \to G_R$ is a full homomorphism.*

Proof. Let $\psi(x)$ is an unit, then $\psi(x) \notin \mathfrak{q}$ for all $\mathfrak{q} \in Spec(R)$. Hence $x \notin \psi^{-1}(\mathfrak{q})$ for all $\mathfrak{q} \in Spec(R)$. Since induced map is surjective, x is an unit and $\underline{\psi}$ is full homomorphism by the above remark. □

Theorem 4.8. *In Remark 4.2, $\underline{\psi}$ is a surjective full homomorphism of graph if and only if ψ is surjective and $\overline{Ker}(\psi) \subseteq J(S)$. In particular, if ψ is a surjective ring homomorphism and S is a local commutative ring, then $\underline{\psi}$ is a full surjective homomorphism.*

Proof. Suppose that $\underline{\psi}$ is full. Hence, $\psi^{-1}(\psi(s)) \subseteq U(S)$ for all $\psi(s) \in U(R)$ by Remark 4.6. Let $s \in \overline{Ker}(\psi)$. Then $\psi(1+ss') = 1$ for all $s' \in S$, hence $1+ss'$ has inverse and it follows that $s \in J(S)$. Therefore $Ker(\psi) \subseteq J(S)$ and ψ is a surjective ring homomorphism by Corollary 4.3. Conversely, let $\psi(s) \in U(R)$, then there is $s' \in S$ such that $(s'+Ker(\psi))(s+Ker(\psi)) = 1+Ker(\psi)$ since $S/Ker(\psi) \cong R$. Hence $ss'-1 \in Ker(\psi)$ and so $(ss'-1) \in J(S)$ since $Ker(\psi) \subseteq J(S)$. Therefore $ss' \in U(S)$ and so $s \in U(S)$ since $1 + J(R) \subseteq U(R)$ and $U(S)$ is a saturated multiplicatively closed subset of S. Moreover, if ψ is surjective, then $\underline{\psi}$ is surjective too by Corollary 4.3. The "in particular" statement is clear since $Ker(\psi) \subseteq J(S) = \mathfrak{m}_S$, where $\mathfrak{m}_S$ is a maximal ideal. □

Corollary 4.9. *Let $\psi : S \to R$ be a surjective ring homomorphism. Then $\underline{\psi} : G_S \to G_R$ is a full homomorphism if and only if the map $\psi^* : Max(R) \to Max(S)$ is surjective.*

Proof. Let $\underline{\psi}$ be a surjective full homomorphism. Then $Ker(\psi) \subseteq J(S)$ by the above theorem. Now, ψ^* is a surjective map because if $Ker(\psi)$ contained in the every maximal ideal and ψ is surjective, then $\psi(\mathfrak{m}_S)$ and $\psi^{-1}(\mathfrak{m}_R)$ are maximal ideals for $\mathfrak{m}_S \in Max(S)$ and $\mathfrak{m}_R \in Max(R)$. Conversely, by the proof of Proposition 4.7, $\underline{\psi}$ is a full homomorphism. □

Recall that a ring homomorphism $S \to R$ is called flat (faithfully flat) if R is flat(faithfully flat) as an S-module.

Theorem 4.10. *Let $\psi : S \to R$ be a surjective flat homomorphism. Then $\underline{\psi} : G_S \to G_R$ is full if and only if ψ is faithfully flat.*

Proof. Let $\underline{\psi}$ be a surjective full homomorphism, then $Ker(\psi) \subseteq J(S)$, by Theorem 4.8. Also, $\psi^* : Max(R) \to Max(S)$ is surjective and so for all $\mathfrak{m} \in Max(S)$, $R/\psi(\mathfrak{m})$ is nonzero by Corollary 4.9. Therefore, by [10, Lemma 10.38.15], $\psi : S \to R$ is faithfully flat. Conversely, the induced map on $Spec$ is surjective by [10, Lemma 10.38.16]. Therefore, by Proposition 4.7, $\underline{\psi}$ is a full homomorphism. □

Lemma 4.11. *If ϕ in Remark 4.2 is an injective homomorphism of modules, then $\underline{\phi}$ is a full injective homomorphism of graphs. Moreover, $\Upsilon_R(\phi)$ is a full injective homomorphism of graphs too.*

Proof. It is clear by Corollary 4.3 and Remark 4.6. □

Theorem 4.12. *Let M and N be R-modules where R is an integral domain and let $\phi : M \to N$ be an R-module homomorphism. Then $Ker(\phi) \subseteq T(M)$ if and only if $\Upsilon^t(\phi) = \underline{\phi} : T\Gamma_R(M) \to T\Gamma_R(N)$ is a full homomorphism of graph.*

Proof. Suppose $\phi(m) \in T(N)$ for some $m \in M$. Then $r\phi(m) = \phi(rm) = 0$ for some $r \in R$. Hence $rm \in T(M)$ since $Ker(\phi) \subseteq T(M)$. Therefore $m \in T(M)$ since R is an integral domain. Conversely, if $\underline{\phi}$ is full, then inverse map of any torsion elements of N is a torsion element in M by Remark 4.6. Hence, $\phi^{-1}(0) = Ker(\phi) \subseteq T(M)$. □

Remark 4.13. A homomorphism φ of a graph G into H gives rise to an equivalence relation $\equiv_\varphi$. In other words, the kernel of φ, defined on V by $u \equiv_\varphi v$ if and only if $\varphi(u) = \varphi(v)$. Therefore, a homomorphism of graphs $\varphi : G \to H$ is surjective and faithful if and only if $\omega : G/\mathcal{K}_\varphi \to H$ is an isomorphism.

Theorem 4.14. *According to the assumptions of Remark 4.2, let $\underline{\psi}$ and $\underline{\phi}$ be faithful homomorphisms of graphs. Then*

(1) $\Upsilon^u(S/Ker(\psi)) \cong G_S/\mathcal{K}_{\underline{\psi}}$,

(2) $\Upsilon^t(M/Ker(\phi)) \cong T\Gamma_R(M)/\mathcal{K}_{\underline{\phi}}$,

(3) $\Upsilon_R(M/Ker(\phi)) \cong \Upsilon_R(M)/\mathcal{K}_{\underline{\phi}\times\underline{id}}$.

Proof. (1). By the above remark, if $\underline{\psi} : G_S \to G_R$ is a faithful homomorphism, then $G_S/\mathcal{K}_{\underline{\psi}} \cong \underline{\psi}(G_S)$. Since the diagram commutes in Remark 4.2(a), $\underline{\psi}(\Upsilon^u(S)) = \Upsilon^u(\psi(S))$. Therefore $G_S/\mathcal{K}_{\underline{\psi}} \cong \underline{\psi}(G_S) \cong \Upsilon^u(S/Ker(\psi))$.

(2) The proof is similar to the proof of part (1).

(3) Let $\underline{\phi}$ be faithful and $\underline{\phi}\times\underline{id} : \Upsilon_R(M) \to \Upsilon_R(N)$ be the graph homomorphism induced by ϕ. Then $\underline{\phi} \times \underline{id}$ is faithful by Remark 4.6. Hence

$$(\underline{\phi} \times \underline{id})(\Upsilon_R(M)) \cong \Upsilon_R(M)/\mathcal{K}_{\underline{\phi}\times\underline{id}},$$

by the above remark. Since the diagram is commutative in Remark 4.2,

$$(\underline{\phi} \times \underline{id})(\Upsilon_R(M)) = \Upsilon_R(\phi(M)) \cong \Upsilon_R(M/Ker(\phi)).$$

Therefore $\Upsilon_R(M/Ker(\phi)) \cong \Upsilon_R(M)/\mathcal{K}_{\underline{\phi}\times\underline{id}}$. □

Corollary 4.15. *Let $\mathcal{I}$ and $\mathcal{N}$ be the partitions of ring S and R-module M which generated by the equivalence relation modulo I as an ideal of S and N as a submodule of M, respectively. Let $\underline{\psi} : G_S \to G_{S/I}$ and $\underline{\phi} : T\Gamma_R(M) \to T\Gamma_R(M/N)$ be faithful. Then*

(1) $\Upsilon^u(S/I) \cong G_S/\mathcal{I}$,

(2) $\Upsilon^t(M/N) \cong T\Gamma_R(M)/\mathcal{N}$,

(3) $\Upsilon_R(M/N) \cong T\Gamma_R(M)/\mathcal{N} \times G_R$.

Proof. Let $\psi : S \to S/I$ and $\phi : M \to M/N$ are ring and module homomorphism, respectively. Then $\mathcal{I} = \mathcal{K}_{\underline{\psi}}$ and $\mathcal{N} = \mathcal{K}_{\underline{\phi}}$. Hence the three parts are clear by the above theorem. □

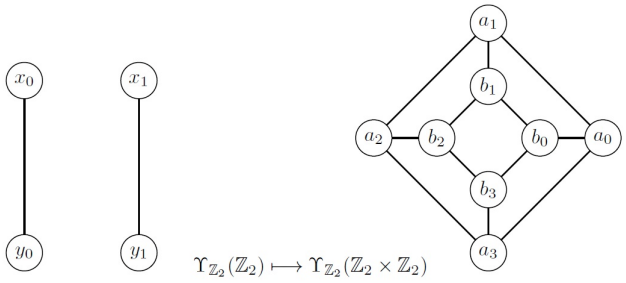
Example 4.16. (a). Let $n \geq 4$ be an integer and $\psi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a ring homomorphism. Then $\psi^{-1}(\bar{m}) \cap U(\mathbb{Z}) = \varnothing$, where $-1, 1 \neq \bar{m} \in U(\mathbb{Z}_n)$. Hence $\underline{\psi} : G_{\mathbb{Z}} \to G_{\mathbb{Z}_n}$ is not faithful by Remark 4.6.

(b). Let $\theta : \mathbb{Z}_6 \to \mathbb{Z}_6/3\mathbb{Z}_6$ be the canonical homomorphism of rings. Then $\theta^{-1}(\bar{m}) \cap U(\mathbb{Z}_6) \neq \varnothing$ and $\theta^{-1}(\bar{m}) \nsubseteq U(\mathbb{Z}_6)$ for $m = 1, 2$. Hence the graph homomorphism $\underline{\theta} : G_{\mathbb{Z}_6} \to G_{\mathbb{Z}_3}$ is faithful, but is not full by Remark 4.6. Also, consider θ as a homomorphism of $\mathbb{Z}_6$-modules, then $\theta^{-1}(\bar{m}) \cap T(\mathbb{Z}_6) \neq \varnothing$ and $\theta^{-1}(\bar{m}) \nsubseteq T(\mathbb{Z}_6)$ for $m = 0, 1, 2$. Therefore, $\underline{\theta} : T\Gamma_{\mathbb{Z}_6}(\mathbb{Z}_6) \to T\Gamma_{\mathbb{Z}_6}(\mathbb{Z}_3)$ is faithful, but is not full by Remark 4.6. Moreover, let $\underline{\theta} \times \underline{id_{\mathbb{Z}_6}} : \Upsilon_{\mathbb{Z}_6}(\mathbb{Z}_6) \to \Upsilon_{\mathbb{Z}_6}(\mathbb{Z}_3)$. Since $\underline{id_{\mathbb{Z}_6}}$ is a full homomorphism of graph and $\underline{\theta}$ is faithful, $\underline{\theta} \times \underline{id_{\mathbb{Z}_6}}$ is a faithful homomorphism of graph by Remark 4.6.

(c). Let R be a Noetherian ring and let $f = \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$, where a_n is nilpotent and Let $\mathcal{R}$ be the partition of ring $R[[x]]$ which generated by the equivalence relation modulo $Nil(R)$ as an ideal of nilpotent elements. Then $\{f | a_n \in Nil(R)\} = Nil(R[[x]]) \subseteq J(R[[x]]) = \sum_{n=0}^{\infty} b_n x^n$ where $b_0 \in J(R)$ by Exercise 2 in [7, p. 84] and Exercise 5 in [7, p. 11]. Therefore $\underline{\psi} : G_{R[[x]]} \to G_{R[[x]]}/\mathcal{R}$ is a full homomorphism of graphs by Theorem 4.8 and Corollary 4.15.

Let C and D be categories. A covariant functor $F : C \to D$ is said to be $faithful$ if the mapping $Hom_C(A, A') \to Hom_D(F(A), F(A'))$ is injective for all $A, A' \in C$, and it will be called $full$ if this mapping is surjective.

Example 4.17. Let $\phi : \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ be an $\mathbb{Z}_2$-module homomorphism and let $\varphi : \Upsilon_{\mathbb{Z}_2}(\mathbb{Z}_2) \to \Upsilon_{\mathbb{Z}_2}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ be a graph homomorphism with $\varphi(x_0) = a_0$, $\varphi(x_1) = a_2$ and $\varphi(y_i) = a_1$ for $i = 1, 2$ by the following figure:



then there is not a module homomorphism such that $\underline{\phi} \times \underline{id_{\mathbb{Z}_2}} = \varphi$ since $Im(\phi)$ is a submodule of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Corollary 4.18. *The functor $\Upsilon_R : \mathfrak{M}_R \to Cay(G, C)$ is faithful. But is not full.*

Proof. The first part follows directly from the definition. By the above example, a homomorphism of graph is not a module homomorphism in general. Therefore the functor Υ is not full. □

Let R_i be a commutative ring for $1 \leqslant i \leqslant t$. The element $(u_1, u_2, \ldots, u_t)$ is a unit of $\bigoplus R_i$ if and only if each u_i is a unit element in R_i. Hence $G_{\bigoplus R_i} \cong \prod G_{R_i}$.

Remark 4.19. (1). Note that unlike in group theory, the inverse of a bijective homomorphism of graph need not be a homomorphism. For example, any bijective homomorphism from $\overline{K}_n$ to K_n. A faithful bijective homomorphism is an isomorphism of graphs.

(2). Since $T(N \oplus M) \subseteq T(N) \times T(M)$, the map

$$i : T\Gamma_R(N \oplus M) \to T\Gamma_R(N) \times T\Gamma_R(M)$$

is a graph homomorphism.

Proposition 4.20. *Let R be an integral domain and let M and N be R-modules. Then $\Upsilon_R(N \oplus M) \cong T\Gamma_R(N) \times \Upsilon_R(M)$.*

Proof. Consider the map $\iota : \Upsilon_R(N \oplus M) \to T\Gamma_R(N) \times \Upsilon_R(M)$ given by $\iota(n, m, r) = (n, (m, r))$. Hence by Remark 4.19(2), it is a bijective homomorphism of graph. Since R is an integral domain, $(n, m) \in T(N \oplus M)$ if and only if $n \in T(N)$ and $m \in T(M)$. Therefore ι is faithful and $\Upsilon_R(N \oplus M) \cong T\Gamma_R(N) \times \Upsilon_R(M)$. □

Definition 4.21. Suppose that $\{G_i\}_{i \in \mathbb{Z}}$ is a family of groups where e_i is the identity element of G_i. A sequence of Cayley graphs

$$\cdots \to Cay(G_{i-1}, C_{i-1}) \xrightarrow{\varphi_{i-1}} Cay(G_i, C_i) \xrightarrow{\varphi_i} Cay(G_{i+1}, C_{i+1}) \to \cdots, \qquad (2)$$

is called exact if $\varphi_i^{-1}(e_{i+1}) = Im(\varphi_{i-1})$ and $\varphi_j(C_j) \subseteq C_{j+1}$ for all $i, j \in \mathbb{Z}$. In particular, the short exact sequence of Cayley graph is an exact sequence in the form

$$Cay(G_1, C_1) \xrightarrow{\varphi_1} Cay(G_2, C_2) \xrightarrow{\varphi_2} Cay(G_3, C_3),$$

such that φ_1 and φ_2 are injective and surjective, respectively.

The above definition may be extended to the Cayley graph with loop on all vertices (i.e., $e_i \in C_i$).

Remark 4.22. By the above definition and Corollary 4.3, the functors Υ^u and Υ^t are exact. Let

$$\cdots \to M_{i-1} \xrightarrow{\phi_{i-1}} M_i \xrightarrow{\phi_i} M_{i+1} \to \cdots$$

is an exact sequence of R-modules and R-homomorphisms, then

$$\cdots \to \Upsilon_R(M_{i-1}) \xrightarrow{\phi_{i-1}} \Upsilon_R(M_i) \xrightarrow{\phi_i} \Upsilon_R(M_{i+1}) \to \cdots$$

is not the exact sequence since $Ker(\underline{\phi_i}) \subsetneqq Im(\underline{\phi_{i-1}})$, where $\underline{\phi} = (\phi, id)$. Also if (2) is the sequence of Cayley graphs such that $Im(\varphi_{i-1}) = \varphi_i^{-1}(g_{i+1})$ for some $g_{i+1} \in G_{i+1}$ and every $i \in \mathbb{Z}$, then it can be turned into an exact sequence whenever φ_i's replace with $\sigma_{i+1}\varphi_i\sigma_i^{-1}$, where σ_i is an automorphism of vertex transitive graph $Cay(G_i, C_i)$ with $\sigma_i(g_i) = e_{i+1}$, for all $i \in \mathbb{Z}$.

Theorem 4.23. *Let R be a commutative ring and*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{\phi_1} & M_2 & \xrightarrow{\phi_2} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \eta_1} & & \downarrow{\scriptstyle \eta_2} & & \downarrow{\scriptstyle \eta_3} & & \\ 0 & \longrightarrow & M_1' & \xrightarrow{\phi_1'} & M_2' & \xrightarrow{\phi_2'} & M_3' & \longrightarrow & 0 \end{array}$$

a commutative diagram of R-modules and R-module homomorphisms such that each row is a short exact sequence. Consider the commutative diagram:

$$\begin{array}{ccccc} TUC_R(M_1) & \xrightarrow{(\underline{\phi_1}, \underline{id_R})} & TUC_R(M_2) & \xrightarrow{(\underline{\phi_2}, \underline{id_R})} & TUC_R(M_3) \\ \downarrow{\scriptstyle (\underline{\eta_1}, \underline{id_R})} & & \downarrow{\scriptstyle (\underline{\eta_2}, \underline{id_R})} & & \downarrow{\scriptstyle (\underline{\eta_3}, \underline{id_R})} \\ TUC_R(M_1') & \xrightarrow{(\underline{\phi_1'}, \underline{id_R})} & TUC_R(M_2') & \xrightarrow{(\underline{\phi_2'}, \underline{id_R})} & TUC_R(M_3') \end{array}.$$

(1) *If η_1 and η_3 are injective then so is $(\underline{\eta_2}, \underline{id_R})$.*

(2) *If η_1 and η_3 are surjective then so is $(\underline{\eta_2}, \underline{id_R})$.*

(3) *If η_1 and η_3 are isomorphism of module then $(\underline{\eta_2}, \underline{id_R})$ is an isomorphism of graph.*

Proof. Parts (1) and (2) follow directly from Corollary 4.3 and Short Five Lemma (Note that by the above remark, rows of the second diagram in this theorem is not the short exact sequences of Cayley graphs).

(3). This follows directly from parts above, Lemma 4.11 and Remark 4.6. □

Let R be a ring and let $0 \to M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} M_3 \to 0$ be a short exact sequence of R-modules. The sequence is said to be split if $\phi_1(M_1)$ is a direct summand of M_2. Up to isomorphism, one has $M_2 = M_1 \oplus M_3$.

Theorem 4.24. *Let*

$$0 \to M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} M_3 \to 0 \tag{3}$$

be a split short exact sequence of R-modules and let $T(M_2)$ be a submodule of M_2. Then

$$\Upsilon_R(M_2) \cong T\Gamma_R(M_1) \times \Upsilon_R(M_3) \cong T\Gamma_R(M_3) \times \Upsilon_R(M_1).$$

Proof. Since (3) is a split short exact sequence of R-module, there are R-module homomorphisms $\psi_1 : M_2 \to M_1$ and $\psi_2 : M_3 \to M_2$ such that $\psi_1 \circ \phi_1 = id_{M_1}$ and $\phi_2 \circ \psi_2 = id_{M_3}$. Consider map $\varphi : \Upsilon_R(M_2) \to T\Gamma_R(M_1) \times \Upsilon_R(M_3)$ given by $\varphi(m_2, r) = (\underline{\psi_1}(m_2), \underline{\phi_2} \times \underline{id_R}(m_2, r))$. Since $\underline{\psi_1}$ and $\underline{\phi_2} \times \underline{id_R}$ are homomorphisms of graph, so is φ. Let $\varphi(m_2, r) = \varphi(m_2', r')$, then $\underline{\psi_1}(m_2) = \underline{\psi_1}(m_2')$ and $\underline{\phi_2} \times \underline{id_R}(m_2, r) = \underline{\phi_2} \times \underline{id_R}(m_2', r')$. So $\psi_1(m_2 - m_2') = 0$, $m_2 - m_2' \in Ker(\phi_2)$ and $r = r'$ since $(\underline{\phi_2}(m_2), r) = (\phi_2(m_2'), r')$. Hence $m_2 - m_2' \in Im(\phi_1)$ since (3) is a short exact sequence of R-modules. So $m_2 = m_2'$ since $\psi_1 \circ \phi_1 = id_{M_1}$ and $\psi_1(m_2 - m_2') = 0$. Therefore $(m_2, r) = (m_2', r')$ and φ is injective. Moreover, φ is a surjective homomorphism of graph because if $(m_1, (m_3, r)) \in T\Gamma_R(M_1) \times \Upsilon_R(M_3)$, then $\varphi(\phi_1(m_1) + \psi_2(m_3) - \phi_1 \circ \psi_1 \circ \psi_2(m_3), r) = (m_1, (m_3, r))$ since $\phi_2 \circ \phi_1 = 0$, $\psi_1 \circ \phi_1 = id_{M_1}$ and $\phi_2 \circ \psi_2 = id_{M_3}$. Also we need to prove that φ is faithful for being an isomorphism of graphs. Suppose that vertices $a = (\underline{\psi_1}(m_2), \underline{\phi_2} \times \underline{id_R}(m_2, r))$ and $b = (\underline{\psi_1}(m_2'), \underline{\phi_2} \times \underline{id_R}(m_2', r'))$ are adjacent in $T\Gamma_R(M_1) \times \Upsilon_R(M_3)$, then $m_1' = \psi_1(m_2 - m_2') \in T(M_1)$ and $m_3' = \phi_2(m_2 - m_2') \in T(M_3)$. Since $T(M_2)$ is a submodule of M_2, $(\phi_1(m_1') + \psi_2(m_3') - \phi_1 \circ \psi_1 \circ \psi_2(m_3') \in T(M_2)$. Therefore the vertices $\varphi^{-1}(a) = (\phi_1 \circ \psi_1(m_2) + \psi_2 \circ \phi_2(m_2) - \phi_1 \circ \psi_1 \circ \psi_2 \circ \phi_2(m_2), r)$ and $\varphi^{-1}(b) = (\phi_1 \circ \psi_1(m_2') + \psi_2 \circ \phi_2(m_2') - \phi_1 \circ \psi_1 \circ \psi_2 \circ \phi_2(m_2'), r')$ are adjacent in $\Upsilon_R(M_2)$. □

Corollary 4.25. *Let* (3) *be a split short exact sequence of R-module and $T(M_2)$ is a submodule of M_2. Then*

$$\Upsilon_R(M_2) \cong \Upsilon_R(M_1 \oplus M_3) \cong T\Gamma_R(M_1) \times \Upsilon_R(M_3) \cong T\Gamma_R(M_3) \times \Upsilon_R(M_1).$$

Proof. By Theorem 4.23 and the above theorem, it is clear. □

Example 4.26. Let $T(M)$ be a proper submodule of R-module M such that $|T(M)| = \alpha$ and $|M/T(M)| = \beta$. If R is a principal ideal domain, then the short exact sequence of R-modules

$$0 \to T(M) \to M \to M/T(M) \to 0 \tag{4}$$

splits, so $M \cong T(M) \oplus M/T(M)$ as a direct sum of a torsion module and a free module. Then

$$\Upsilon_R(M) \cong T\Gamma_R(T(M)) \times T\Gamma_R(M/T(M)) \times G_R = \beta K_\alpha^\circ \times G_R$$

by the above corollary and [3, Theorem 7(1)]. But if ring R is not a domain, then $M/T(M)$ is torsion by [6, Theorem 2.8]. By [3, Theorem 7(1)], $T\Gamma_R(M) =$

$K_\alpha^\circ \times \beta K_1^\circ = \beta K_\alpha^\circ$. Hence $\Upsilon^t(M) \ncong T\Gamma_R(T(M)) \times T\Gamma_R(M/T(M))$ because if ring R is not a domain, then $T\Gamma_R(T(M)) \times T\Gamma_R(M/T(M)) = K_\alpha^\circ \times K_\beta^\circ$ (let $K_\alpha^\circ \times K_\beta^\circ = K_\alpha^\circ \times \beta K_1^\circ$. By [9, Proposition 9.6], $K_\beta^\circ = \beta K_1^\circ$, so $\beta = 1$ and $M = T(M)$).

As an applications of the algebraic graph theory in modules theory, the following corollary hold by the above example.

Corollary 4.27. *Suppose that the short exact sequence of R-modules* (4) *splits, then R is a domain.*

References

[1] **G.G. Aalipour and S. Akbari**, *On the Cayley graph of a commutative ring with respect to its zero-divisors*, Comm. Algebra **44** (2016), 1443 – 1459.

[2] **G.G. Aalipour and S. Akbari**, *Some properties of a Cayley graph of a commutative ring*, Comm. Algebra **42** (2014), 1582 – 1593.

[3] **A. Abbasi, A. Ramin**, *An extension of total graph over a module*, Miskolc Math. Notes **18** (2017), 17 – 29.

[4] **R. Akhtar, M. Boggess, T. Jackson-Henderson, I. Jiménez, R. Karpman, A. Kinzel and D. Pritikin**, *On the unitary Cayley graph of a finite ring*, Electron. J. Combin. **16** (2009), Research Paper R117, 13 pp.

[5] **D.F. Anderson and A. Badawi**, *The total graph of a commutative ring*, J. Algebra **320** (2008), 2706 – 2719.

[6] **D.D. Anderson and S. Chun**, *The set of torsion elements of a module*, Comm. Algebra **42** (2014), 1835 – 1843.

[7] **M.F. Atiyah and I.G. Macdonald**, *Introduction to commutative algebra*, Addison-Wesley Publishing Co, (1969).

[8] **C. Godsil and G. Royle**, *Algebraic graph theory*, Springer, (2001).

[9] **R. Hammack, W. Imrich and S. Klavžar**, *Handbook of product graphs*, Second Edition. CRC Press: Taylor and Francis Group, (2011).

[10] http://stacks.math.columbia.edu/download/book.pdf

[11] **D. Kiani and M. Molla Haji Aghaei**, *On the unitary Cayley graph of a ring*, Electron. J. Combin. **19 (2)** (2012), P10.

[12] **C. Lanski and A. Maróti**, *Rings elements as sums of units*, Cent. Eur. J. Math. **7** (2009), 395 – 399.

[13] **J. Sato and K. Baba**, *The chromatic number of the simple graph associated with a commutative ring*, Sci. Math. Jpn. **71** (2010), 187 – 194.

[14] **M.H. Shekarriz, M.H. Shirdareh Haghighi and H. Sharif**, *On the total graph of a finite commutative ring*, Comm. Algebra **40** (2012), 2798 – 2807.

Received November 27, 2017

Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Guilan, Rasht, Iran
E-mails: ramin2068@webmail.guilan.ac.ir, aabbasi@guilan.ac.ir

Quasigroups and Related Systems **26** (2018), 139 – 148

Action of the group $\langle x, y : x^2 = y^6 = 1 \rangle$ on imaginary quadratic fields

Abdul Razaq

Abstract. Let $H =< x, y : x^2 = y^6 = 1 >$ be acting on $\mathbb{Q}\left(\sqrt{-n}\right)$ and denote the subset $\left\{\frac{a+\sqrt{-n}}{3c} : a, \frac{a^2+n}{3c}, c \in \mathbb{Z} \setminus \{0\}\right\}$ of $\mathbb{Q}\left(\sqrt{-n}\right)$ by $\mathbb{Q}^*\left(\sqrt{-n}\right)$. Also $d(n)$ denotes the arithmetic function which is defined as the number of positive divisors of n which are multiple of 3. In this paper, we show that the total number of orbits of $\mathbb{Q}^*\left(\sqrt{-n}\right)$ under the action of H are

$$\begin{cases} 4 & \text{if } n = 3, \\ d(n) & \text{if } n \equiv 0 \pmod 3, \text{ but } n \neq 3, \\ 2d(n+1) & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

1. Introduction

Let F be an extension field of degree two over the field $\mathbb{Q}$ of rational numbers. Then any element $x \in F \setminus \mathbb{Q}$ is of degree two over $\mathbb{Q}$ and is a primitive element of F (that is $F = \mathbb{Q}[x]$ and $\{1, x\}$ is a base of F over $\mathbb{Q}$). Let $p(x) = x^2 + bx + c$, where $b, c \in \mathbb{Q}$, be the minimal polynomial of such an element $x \in F$. Then $2x = -b \pm \sqrt{b^2 - 4c}$ and so, $F = \mathbb{Q}(\sqrt{b^2 - 4c})$. Since $b^2 - 4c$ is a rational number $\frac{u}{v} = \frac{uv}{v^2}$ with $u, v \in \mathbb{Z}$, we obtain $F = \mathbb{Q}(\sqrt{uv})$. In fact it is possible to write $F = \mathbb{Q}(\sqrt{n})$, where n is a square-free integer. If n is a negative square-free integer, then $\mathbb{Q}(\sqrt{n})$ is called an *imaginary quadratic field* and the elements of $\mathbb{Q}(\sqrt{n})$ are of the form $a + b\sqrt{n}$ with $a, b \in \mathbb{Q}$. The imaginary quadratic fields are usually denoted by $\mathbb{Q}(\sqrt{-n}) = \left\{a + b\sqrt{-n} : a,\ b \in \mathbb{Q}\right\}$, where n is a square-free positive integer. Imaginary quadratic fields are the only type (apart from $\mathbb{Q}$) with a finite unit group. This group has order 4 for $\mathbb{Q}(\sqrt{-1})$ $\left(\text{and generator } \sqrt{-1}\right)$, order 6 for $\mathbb{Q}(\sqrt{-3})$ $\left(\text{and generator } \frac{1+\sqrt{-3}}{2}\right)$, and order 2 (and generator -1) for all other imaginary quadratic fields. We denote the subset $\left\{\frac{a+\sqrt{-n}}{3c} : a, \frac{a^2+n}{3c} \in \mathbb{Z} \text{ and } c \in \mathbb{Z} \setminus \{0\}\right\}$ of $\mathbb{Q}\left(\sqrt{-n}\right)$ by $\mathbb{Q}^*\left(\sqrt{-n}\right)$. Some fundamental properties of imaginary quadratic fields have been discussed in [2] and [3].

Let G be a group generated by the linear fractional transformations x and y satisfying the relations $x^2 = y^m = 1$. If $y : z \longrightarrow \frac{az+b}{cz+d}$ is to act on all imaginary

2010 Mathematics Subject Classification: 20G40, 05C25
Keywords: Imaginary quadratic field, orbits, coset diagrams.

quadratic fields, then a, b, c, d must be rational numbers and can taken to be integers, so that $\frac{(a+d)^2}{ad-bc}$ is rational. But if $y : z \longrightarrow \frac{az+b}{cz+d}$ is of order m, one must have $\frac{(a+d)^2}{ad-bc} = w + w^{-1} + 2$, where w is a primitive mth root of unity. Now $w + w^{-1}$ is rational, for a primitive mth root w, only if $m = 1, 2, 3, 4$ or 6. So these are the only possible orders of y. The group $< x, y >$ is cyclic of order 2, when $m = 1$. When $m = 2$, it is an infinite dihedral group and does not give inspiring information while studying its action on imaginary quadratic numbers. For $m = 3$, the group $< x, y >$ is the modular group $PSL(2, \mathbb{Z})$ and its action on real quadratic numbers has been discussed in detail in [4] and [5].

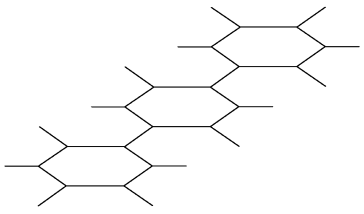
In this paper, we are interested in the action of the group $H =< x, y : x^2 = y^6 = 1 >$, where $(z)\, x = \frac{-1}{3z}$ and $(z)\, y = \frac{-1}{3(z+1)}$ are linear fractional transformations, on $\mathbb{Q}^*\left(\sqrt{-n}\right) = \left\{\frac{a+\sqrt{-n}}{3c} : a, \frac{a^2+n}{3c} \in \mathbb{Z} \text{ and } c \in \mathbb{Z} \diagdown \{0\}\right\}$. Note that, $\mathbb{Q}^*\left(\sqrt{-n}\right)$ remains invariant under the action of H. We show that the total number of orbits of $\mathbb{Q}^*\left(\sqrt{-n}\right)$ under the action of H are

$$\begin{cases} 4 & \text{if } n = 3 \\ d(n) & \text{if } n \equiv 0 \pmod 3, \text{ but } n \neq 3 \\ 2d(n+1) & \text{if } n \equiv 2 \pmod 3 \end{cases}.$$

2. Coset Diagrams

We use coset diagrams for the group H and study its action on the projective line over imaginary quadratic fields. The coset diagrams for the group H are defined as follows. The six cycles of transformation y are represented by six unbroken edges of a hexagon (may be irregular) permuted counter-clockwise by y. Any two vertices which are interchanged by involution x, is joined by an edge. The fixed points of x and y, if they exist, are denoted by heavy dots. This graph can be interpreted as a coset diagram,with the vertices identified with the cosets of $Stab_v(H)$, the stabilizer of some vertex v of the graph, or as 1-skeleton of the cover of the fundamental complex of the presentation which corresponds to the subgroup $Stab_v(H)$. For more details about coset diagrams, one can refer to [1],[6],[7] and [8].

A general fragment of the coset diagram of the action of H on $\mathbb{Q}^*\left(\sqrt{-n}\right)$ will look as follows.



Definition 2.1. If $\alpha = \frac{a+\sqrt{-n}}{3c} \in \mathbb{Q}^*\left(\sqrt{-n}\right)$ is such that $ac < 0$ then α is called a *totally negative imaginary quadratic number* and it is called a *totally positive imaginary quadratic number* if $ac > 0$.

As $d = \frac{a^2+n}{3c}$, so dc is always positive. Thus d and c will have the same sign. Hence an imaginary quadratic number $\alpha = \frac{a+\sqrt{-n}}{3c} \in \mathbb{Q}^*\left(\sqrt{-n}\right)$ is totally negative if either $a < 0$ and $d, c > 0$ or $a > 0$ and $d, c < 0$. Similarly $\alpha = \frac{a+\sqrt{-n}}{3c} \in \mathbb{Q}^*\left(\sqrt{-n}\right)$ is totally positive if either $a, d, c > 0$ or $a, d, c < 0$.

For $\alpha = \frac{a+\sqrt{-n}}{3c} \in \mathbb{Q}^*\left(\sqrt{-n}\right)$, norm of α is denoted by $\| \alpha \|$ and $\| \alpha \| = | a |$.

3. Main results

Theorem 3.1. *If $\alpha = \frac{a+\sqrt{-n}}{3c} \in Q^*\left(\sqrt{-n}\right)$, then n does not change its value in the orbit αH.*

Proof. Let $\alpha = \frac{a+\sqrt{-n}}{3c}$ and $d = \frac{a^2+n}{3c}$. Since $(\alpha)x = \frac{-1}{3\alpha} = \frac{-1}{3\left(\frac{a+\sqrt{-n}}{3c}\right)} = \frac{-c}{a+\sqrt{-n}} = \frac{-c\left(a-\sqrt{-n}\right)}{a^2+n} = \frac{-a+\sqrt{-n}}{3d}$, therefore the new values of a and c for $(\alpha)x$ are $-a$ and d respectively. The new value of d for $(\alpha)x$ is $\frac{a^2+n}{3d} = \frac{a^2+n}{3\left(\frac{a^2+n}{3c}\right)} = c$. Since $(\alpha)y = \frac{-1}{3(\alpha+1)} = \frac{-1}{3\left(\frac{a+\sqrt{-n}}{3c}+1\right)} = \frac{-1}{3\left(\frac{a+\sqrt{-n}+3c}{3c}\right)} = \frac{-3c\left(a+3c-\sqrt{-n}\right)}{3[(a+3c)^2+n]} = \frac{-a-3c+\sqrt{-n}}{3(2a+d+3c)}$, therefore the new values of a and c for $(\alpha)y$ are $-a-3c$ and $(2a+d+3c)$ respectively. Moreover, the new value of d for $(\alpha)y$ is $\frac{(-a-3c)^2+n}{3(2a+d+3c)} = \frac{a^2+n+9c^2+6ac}{3(2a+d+3c)} = c$. Similarly we can calculate the new values of a, d and c for $(\alpha)\, y^j$, where $j = 2, 3, 4, 5$.

α	a	d	$3c$
$(\alpha)x$	$-a$	c	$3d$
$(\alpha)y$	$-a-3c$	c	$3\,(2a+d+3c)$
$(\alpha)y^2$	$-5a-3d-6c$	$2a+d+3c$	$3\,(4a+3d+4c)$
$(\alpha)y^3$	$-7a-6d-6c$	$4a+3d+4c$	$3\,(4a+4d+3c)$
$(\alpha)y^4$	$-5a-6d-3c$	$4a+4d+3c$	$3\,(2a+3d+c)$
$(\alpha)y^5$	$-a-3d$	$2a+3d+c$	$3d$
$(\alpha)yx$	$a+3c$	$(2a+d+3c)$	$3c$
$(\alpha)y^2x$	$5a+3d+6c$	$4a+3d+4c$	$3\,(2a+d+3c)$
$(\alpha)y^3x$	$7a+6d+6c$	$4a+4d+3c$	$3\,(4a+3d+4c)$
$(\alpha)y^4x$	$5a+6d+3c$	$2a+3d+c$	$3\,(4a+4d+3c)$
$(\alpha)y^5x$	$a+3d$	d	$3\,(2a+3d+c)$
$(\alpha)xy$	$a-3d$	d	$3\,(-2a+3d+c)$
$(\alpha)xy^2$	$5a-6d-3c$	$-2a+3d+c$	$3\,(-4a+4d+3c)$
$(\alpha)xy^3$	$7a-6d-6c$	$-4a+4d+3c$	$3\,(-4a+3d+4c)$
$(\alpha)xy^4$	$5a-3d-6c$	$-4a+3d+4c$	$3\,(-2a+d+3c)$
$(\alpha)xy^5$	$a-3c$	$-2a+d+3c$	$3c$

(Table 1)

From above information we see that all the elements in αH are of the form $\frac{a+\sqrt{-n}}{3c}$. Hence non square positive integer n does not change its value in αH. □

Theorem 3.2. *The fixed points under the action of H on $Q^*\left(\sqrt{-n}\right)$ exist only if $n = 3$.*

Proof. Let g be a linear fractional transformation in H. Therefore $(z)g$ can be taken as $\frac{az+b}{cz+d}$, where $ad-bc = 1$ or 3. Let $\frac{az+b}{cz+d} = z$ which yields quadratic equation $cz^2 + (d-a)z - b = 0$. It has imaginary roots only if $(a+d)^2 - 4(ad-bc) < 0$. If $ad - bc = 1$, then $(a+d)^2 < 4$ implies $a + d = 0, \pm 1$, and if $ad - bc = 3$, then $(a+d)^2 < 12$ implies $a + d = 0, \pm 1, \pm 2, \pm 3$. Hence we have the following cases.

(i) If $a + d =$trace$(g) = 0$, then g is involution and hence it is conjugate to the linear fractional transformation x or y^3.

(ii) If trace$(g) = \pm 1$ and $det\,(g) = 1$, then $(\text{trace}\,(g))^2 = \det(g)$ implying that order of g is 3 and hence g is conjugate to y^2 or y^4.

(iii) If trace$(g) = \pm 3$ and $det\,(g) = 3$, then $(\text{trace}\,(g))^2 = 3\det(g)$ implying that order of g will be six and hence it is conjugate to the linear fractional transformation y or y^5.

(iv) If trace$(g) = \pm 1$, $det\,(g) \neq 1$ or trace$(g) = \pm 3$, $det\,(g) \neq 3$ or trace$(g) = \pm 2$, then the order of g is infinite and it is conjugate to the linear fractional transformation $(xy)^n$.

Hence fixed points of g are imaginary if it is conjugate to the linear fractional transformation x, y, y^2, y^3, y^4 or y^5. Since fixed points of x and y are $\pm\frac{\sqrt{-3}}{3}$ and $\frac{-3\pm\sqrt{-3}}{6}$ respectively, and the conjugates of x and y having the same discriminant. Hence fixed points exist only if $n = 3$. □

Example 3.3. Let $g = xyx \in H$. Then $(z)g = z$ yields the quadratic equation $3z^2 - 3z + 1 = 0$, which has roots $\frac{3\pm\sqrt{-3}}{6}$ which are fixed points of $g = xyx$.

Example 3.4. Let $g = yxy^{-1} \in H$. Then $(z)g = z$ yields the quadratic equation $3z^2 + 6z + 4 = 0$. This equation has roots $\frac{-3\pm\sqrt{-3}}{3}$, which are fixed points of $g = yxy^{-1}$.

Theorem 3.5.

(i) *x maps a totally negative imaginary quadratic number onto a totally positive imaginary quadratic number and vice versa.*

(ii) *If $\alpha = \frac{a+\sqrt{-n}}{3c} \in Q^*\left(\sqrt{-n}\right)$ is totally positive imaginary quadratic number, then $(\alpha)y^j$ is totally negative imaginary quadratic number for $j = 1, 2, 3, 4, 5$.*

Proof. (i) Let α be a totally negative imaginary quadratic number, then $ac < 0$ implies that either $a > 0$ and $c, d < 0$ or $a < 0$ and $c, d > 0$. Now we have the following table.

α	a	d	$3c$
$(\alpha)x$	$-a$	c	$3d$

If $a < 0$ and $c, d > 0$, then from above information we can see that new values of a, d, c for $(\alpha)x$ are all positive. This implies that $(\alpha)x$ is totally positive imaginary quadratic number.

On the other hand, if $a > 0$ and $c, d < 0$ then new values of a, d, c are all negative. So $(\alpha)x$ is a totally positive imaginary quadratic number.

Similarly x maps a totally positive imaginary quadratic number to a totally negative imaginary quadratic number.

(ii) Following table gives the new values of a, d, c for $(\alpha)y^j$, where $j = 1, 2, 3, 4, 5$.

α	a	d	$3c$
$(\alpha)y$	$-a-3c$	c	$3(2a+d+3c)$
$(\alpha)y^2$	$-5a-3d-6c$	$2a+d+3c$	$3(4a+3d+4c)$
$(\alpha)y^3$	$-7a-6d-6c$	$4a+3d+4c$	$3(4a+4d+3c)$
$(\alpha)y^4$	$-5a-6d-3c$	$4a+4d+3c$	$3(2a+3d+c)$
$(\alpha)y^5$	$-a-3d$	$2a+3d+c$	$3d$

Since α is a totally positive, so either $a, d, c > 0$ or $a, d, c < 0$. If $a, d, c > 0$, then $(\alpha)y^j$ are all totally negative imaginary quadratic numbers. Now if $a, d, c < 0$, then again from above table, we can see $(\alpha)y^j$ are all totally negative imaginary quadratic numbers. Thus $(\alpha)y^j$ are all totally negative imaginary quadratic numbers. □

Theorem 3.6.

(i) *If* $\alpha = \frac{a+\sqrt{-n}}{3c} \in Q^*\left(\sqrt{-n}\right)$, *then* $\|\alpha\| = \|(\alpha)x\|$.

(ii) *If* $\alpha = \frac{a+\sqrt{-n}}{3c} \in Q^*\left(\sqrt{-n}\right)$ *is totally positive imaginary quadratic number, then* $\|\alpha\| < \|(\alpha)y^j\|$ *for* $j = 1, 2, 3, 4, 5$.

Proof. (i) Consider the following table.

α	a	d	$3c$
$(\alpha)x$	$-a$	c	$3d$

which implies $\|\alpha\| = \mid a \mid = \|(\alpha)x\|$.

(ii) The values of $(\alpha)y^j$ for $j = 1, 2, 3, 4, 5$ are given in the following table.

α	a	d	$3c$
$(\alpha)y$	$-a-3c$	c	$3(2a+d+3c)$
$(\alpha)y^2$	$-5a-3d-6c$	$2a+d+3c$	$3(4a+3d+4c)$
$(\alpha)y^3$	$-7a-6d-6c$	$4a+3d+4c$	$3(4a+4d+3c)$
$(\alpha)y^4$	$-5a-6d-3c$	$4a+4d+3c$	$3(2a+3d+c)$
$(\alpha)y^5$	$-a-3d$	$2a+3d+c$	$3d$

Since α is a totally positive imaginary quadratic number, so $ac > 0$. Therefore either $a, d, c > 0$ or $a, d, c < 0$. This implies $\|(\alpha)y\| = \mid a + c \mid > \mid a \mid$. Also, $\|(\alpha)y^2\| = \mid 5a + 3d + 2c \mid > \mid a \mid$, $\|(\alpha)y^3\| = \mid 7a + 6d + 2c \mid > \mid a \mid$, $\|(\alpha)y^4\| = \mid 5a + 6d + c \mid > \mid a \mid$, $\|(\alpha)y^5\| = \mid a + 3d \mid > \mid a \mid$.

Thus $\|\alpha\| < \|(\alpha)y^j\|$ for $j = 1, 2, 3, 4, 5$. □

Theorem 3.7. *If* $\alpha = \frac{a+\sqrt{-n}}{3c} \in Q^*\left(\sqrt{-n}\right)$, *then denominator of every element in* αH *has the same sign.*

Proof. Consider the following table.

α	a	d	$3c$
$(\alpha)x$	$-a$	c	$3d$
$(\alpha)y$	$-a-3c$	c	$3(2a+d+3c)$
$(\alpha)y^2$	$-5a-3d-6c$	$2a+d+3c$	$3(4a+3d+4c)$
$(\alpha)y^3$	$-7a-6d-6c$	$4a+3d+4c$	$3(4a+4d+3c)$
$(\alpha)y^4$	$-5a-6d-3c$	$4a+4d+3c$	$3(2a+3d+c)$
$(\alpha)y^5$	$-a-3d$	$2a+3d+c$	$3d$

If $\alpha = \frac{a+\sqrt{-n}}{3c} \in Q^*\left(\sqrt{-n}\right)$ with $c > 0$, then d is also positive. So it can be easily observed from the above information that every element in αH has positive denominator. If $\alpha = \frac{a+\sqrt{-n}}{3c} \in Q^*\left(\sqrt{-n}\right)$ with $c < 0$, then d is also negative. So it can be easily observed from the above information that every element in αH has negative denominator. □

Theorem 3.8. *If* $\alpha = \frac{a+\sqrt{-n}}{3c} \in Q^*\left(\sqrt{-n}\right)$, *then there exists a sequence of positive integers* $\|\alpha_0\|, \|\alpha_1\|, \|\alpha_2\|, \ldots, \|\alpha_m\|$ *such that* $\|\alpha_0\| > \|\alpha_1\| > \|\alpha_2\| > \ldots > \|\alpha_m\|$, *where* $\|\alpha_m\| = \begin{cases} 0,3 & \text{if } n = 3 \\ 0 & \text{if } n \equiv 0 \pmod 3, \text{ but } n \neq 3 \\ 1 & \text{if } n \equiv 2 \pmod 3 \end{cases}$.

Proof. Let $\alpha = \alpha_1$ be a totally positive imaginary quadratic number so $(\alpha_1)x$ is a totally negative imaginary quadratic number and $\| (\alpha_1)x \| = \| \alpha_1 \|$. Since $(\alpha_1)x$ is a totally negative imaginary quadratic number, then by Theorem 3.5 (ii), one of $(\alpha_1)xy^j$ for $j = 1, 2, 3, 4, 5$ is a totally positive imaginary quadratic number. If $(\alpha)xy^j = \alpha_2$ is a totally positive imaginary quadratic number, then by Theorem 3.6 $\| \alpha_2 \| < \| (\alpha_1)x \| = \| \alpha_1 \|$. Similarly, we obtain another totally positive imaginary quadratic number α_3 in the adjacent hexagon to that containing α_2 such that $\|\alpha_0\| > \|\alpha_1\| > \|\alpha_2\|$. Ultimately, we get a decreasing sequence of positive integers $\|\alpha_0\|, \|\alpha_1\|, \|\alpha_2\|, \ldots, \|\alpha_m\|$ such that $\|\alpha\| = \|\alpha_0\| > \|\alpha_1\| > \|\alpha_2\| \ldots > \|\alpha_m\|$. After a finite number of steps it must terminate.

(*i*) If $n = 3$, then after a finite number of steps we reach to α_m such that $\|\alpha_m\| = 0$ or 3. If $\alpha_m = \frac{-3\pm\sqrt{-3}}{6}$, then because $\frac{-3\pm\sqrt{-3}}{6}$ are fixed points of y, therefore, we can not reach at an imaginary quadratic number whose norm is equal to zero. Otherwise we reach at $\alpha_m = \frac{\sqrt{-3}}{\pm 3}$.

(*ii*) If $n \equiv 0 \pmod 3$, but $n \neq 3$, then we reach at an imaginary quadratic number α_m such that $\|\alpha_m\| = 0$.

(*iii*) If $n \equiv 2 \pmod 3$, then we reach at an imaginary quadratic number α_m such that $\|\alpha_m\| = 1$. □

Example 3.9. Let $\alpha_1 = \frac{7+\sqrt{-2}}{3}$, which is totally positive imaginary quadratic number. Then $(\alpha_1)x = \frac{-7+\sqrt{-2}}{51}$, which is totally negative imaginary quadratic

number. Also in the hexagon containing $(\alpha_1)\,x$, $(\alpha_1)\,xy^5 = \frac{4+\sqrt{-2}}{3}$ is totally positive imaginary quadratic number. Take $\alpha_1 = \frac{4+\sqrt{-2}}{3}$, so $\|\alpha_1\| > \|\alpha_2\|$. Now $(\alpha_2)x = \frac{-4+\sqrt{-2}}{18}$ is totally negative imaginary quadratic number, then in the hexagon containing $(\alpha_2)x$, $(\alpha_2)xy^5 = \frac{1+\sqrt{-2}}{3}$ is totally positive imaginary quadratic number. Take $\alpha_3 = \frac{1+\sqrt{-2}}{3}$, implying that $\|\alpha_0\| > \|\alpha_1\| > \|\alpha_3\|$.

Theorem 3.10. *There are exactly four orbits of $Q^*\left(\sqrt{-3}\right)$ under the action of H.*

Proof. Since we know that there exists a sequence of positive integers $\|\alpha_0\|, \|\alpha_1\|, \|\alpha_2\|, \ldots, \|\alpha_m\|$ such that $\|\alpha_0\| > \|\alpha_1\| > \|\alpha_2\| > \|\alpha_3\| > \|\alpha_4\| > \ldots > \|\alpha_m\|$, where $\|\alpha_m\| = 0$ or 3. If $\alpha_m = \pm\frac{\sqrt{-3}}{3}$ or $\frac{-3\pm\sqrt{-3}}{6}$, then $\pm\frac{\sqrt{-3}}{3}$ and $\frac{-3\pm\sqrt{-3}}{6}$ are fixed points of x and y respectively. Therefore in this case there are four orbits of $Q^*\left(\sqrt{-3}\right)$. That is, $\frac{\sqrt{-3}}{3}H$, $\frac{-\sqrt{-3}}{3}H$, $\frac{-3+\sqrt{-3}}{6}H$ and $\frac{3+\sqrt{-3}}{-6}H$. Hence there are exactly four orbits of $Q^*\left(\sqrt{-3}\right)$ under the action of H. □

Theorem 3.11. *Let $\alpha \in Q^*\left(\sqrt{-n}\right)$, where $n \neq 3$.*

(*i*) *If $\alpha = \frac{\sqrt{-n}}{3}$, where $n \equiv 0 \pmod 3$ then $\frac{\sqrt{-n}}{3}$ and $\frac{\sqrt{-n}}{n}$ lie in αH.*

(*ii*) *If $\alpha = \frac{1+\sqrt{-n}}{3}$, where $n \equiv 2 \pmod 3$ then $\frac{1+\sqrt{-n}}{3}$ and $\frac{-1+\sqrt{-n}}{n+1}$ lie in αH.*

(*iii*) *If $\alpha = \frac{-1+\sqrt{-n}}{3}$, where $n \equiv 2 \pmod 3$ then $\frac{-1+\sqrt{-n}}{3}$ and $\frac{1+\sqrt{-n}}{n+1}$ lie in αH.*

(*iv*) *If $\alpha = \frac{\sqrt{-n}}{3c}$, where $n \equiv 0 \pmod 3$ and $c \neq \pm 1, \pm\frac{n}{3}$, $n = 3cc_1$ then $\frac{\sqrt{-n}}{3c}$ and $\frac{\sqrt{-n}}{3c_1}$ lie in αH.*

(*v*) *If $\alpha = \frac{1+\sqrt{-n}}{3c}$ where $n \equiv 2 \pmod 3$ and $n+1 = 3cc_1$, then $\frac{1+\sqrt{-n}}{3c}$ and $\frac{-1+\sqrt{-n}}{3c_1}$ lie in αH.*

(*vi*) *If $\alpha = \frac{-1+\sqrt{-n}}{3c}$ where $n \equiv 2 \pmod 3$ and $n+1 = 3cc_1$, then $\frac{-1+\sqrt{-n}}{3c}$ and $\frac{1+\sqrt{-n}}{3c_1}$ lie in αH.*

Proof. (*i*) If $\alpha = \frac{\sqrt{-n}}{3}$, then we have the following information.

α	0	$\frac{n}{3}$	3
$(\alpha)x$	0	1	n
$(\alpha)y$	-3	1	$n+9$
$(\alpha)y^2$	$-6-n$	$\frac{n+9}{3}$	$3\,(4+n)$
$(\alpha)y^3$	$-2n-6$	$4+n$	$9+4n$
$(\alpha)y^4$	$-2n-3$	$\frac{9+4n}{3}$	$3\,(n+1)$
$(\alpha)y^5$	$-n$	$n+1$	n

Hence from the above table, we see that $\frac{\sqrt{-n}}{3}$ and $\frac{\sqrt{-n}}{n}$ lie in the same orbit.

(ii) If $\alpha = \frac{1+\sqrt{-n}}{3}$, then we have the following information.

α	1	$\frac{n+1}{3}$	3
$(\alpha)x$	-1	1	$1+n$
$(\alpha)y$	-4	1	$16+n$
$(\alpha)y^2$	$-12-n$	$\frac{16+n}{3}$	$27+3n$
$(\alpha)y^3$	$-15-2n$	$9+n$	$25+4n$
$(\alpha)y^4$	$-10-2n$	$\frac{25+4n}{3}$	$12+3n$
$(\alpha)y^5$	$-2-n$	$4+n$	$1+n$

Hence from the above table, we see that $\frac{1+\sqrt{-n}}{3}$ and $\frac{-1+\sqrt{-n}}{n+1}$ lie in αH.

(iii) If $\alpha = \frac{-1+\sqrt{-n}}{3}$, then we have the following information.

α	-1	$\frac{n+1}{3}$	3
$(\alpha)x$	1	1	$1+n$
$(\alpha)y$	-2	1	$4+n$
$(\alpha)y^2$	$-2-n$	$\frac{4+n}{3}$	$3\,(1+n)$
$(\alpha)y^3$	$-1-2n$	$1+n$	$1+4n$
$(\alpha)y^4$	$-2n$	$\frac{1+4n}{3}$	$3n$
$(\alpha)y^5$	$-n$	n	$n+1$

Hence from the above table, we see that $\frac{-1+\sqrt{-n}}{3}$ and $\frac{1+\sqrt{-n}}{n+1}$ lie in the same orbit.

(iv) If $\alpha = \frac{\sqrt{-n}}{3c}$, then we have the following information.

α	0	c_1	$3c$
$(\alpha)x$	0	c	$3\ c_1$
$(\alpha)y$	$-3c$	c	$3\,(3c+c_1\,)$
$(\alpha)y^2$	$-6c-3c_1$	$3c+c_1$	$3\,(4c+3c_1\,)$
$(\alpha)y^3$	$-6c-6c_1$	$4c+3c_1$	$3\,(3c+4c_1\,)$
$(\alpha)y^4$	$-3c-6c_1$	$3c+4c_1$	$3\,(c+3c_1\,)$
$(\alpha)y^5$	$-3c_1$	$c+3c_1$	$3c_1$

Hence from the above table, we see that $\frac{\sqrt{-n}}{3c}$ and $\frac{\sqrt{-n}}{3c_1}$ lie in the same orbit.

(v) If $\alpha = \frac{1+\sqrt{-n}}{3c}$, then we have the following information.

α	1	c_1	$3c$
$(\alpha)x$	-1	c	$3\ c_1$
$(\alpha)y$	$-1-3c$	c	$3\,(2+3c+c_1\,)$
$(\alpha)y^2$	$-5-6c-3c_1$	$2+3c+c_1$	$3\,(4+4c+3c_1\,)$
$(\alpha)y^3$	$-7-6c-6c_1$	$4+4c+3c_1$	$3\,(4+3c+4c_1\,)$
$(\alpha)y^4$	$-5-3c-6c_1$	$4+3c+4c_1$	$3\,(2+c+3c_1\,)$
$(\alpha)y^5$	$-1-3c_1$	$2+c+3c_1$	$3c_1$

Hence from the above table, we see that $\frac{1+\sqrt{-n}}{3c}$ and $\frac{-1+\sqrt{-n}}{3c_1}$ lie in αH.

(vi) If $\alpha = \frac{-1+\sqrt{-n}}{3c}$, then we have the following information.

α	-1	c_1	$3c$
$(\alpha)x$	1	c	$3\ c_1$
$(\alpha)y$	$1-3c$	c	$3\,(2+3c+c_1\,)$
$(\alpha)y^2$	$5-6c-3c_1$	$2+3c+c_1$	$3\,(4+4c+3c_1\,)$
$(\alpha)y^3$	$7-6c-6c_1$	$4+4c+3c_1$	$3\,(4+3c+4c_1\,)$
$(\alpha)y^4$	$5-3c-6c_1$	$4+3c+4c_1$	$3\,(2+c+3c_1\,)$
$(\alpha)y^5$	$1-3c_1$	$2+c+3c_1$	$3c_1$

Hence from the above table, we see that $\frac{-1+\sqrt{-n}}{3c}$ and $\frac{1+\sqrt{-n}}{3c_1}$ lie in αH. □

Example 3.12. By using Theorem 9, the orbits of $Q^*\left(\sqrt{-30}\right)$ are

(i) $\frac{\sqrt{-30}}{3}$ and $\frac{\sqrt{-30}}{30}$ lie in $\frac{\sqrt{-30}}{3}H$. (ii) $\frac{\sqrt{-30}}{-3}$ and $\frac{\sqrt{-30}}{-30}$ lie in $\frac{\sqrt{-30}}{-3}H$.

(iii) $\frac{\sqrt{-30}}{6}$ and $\frac{\sqrt{-30}}{15}$ lie in $\frac{\sqrt{-30}}{6}H$. (iv) $\frac{\sqrt{-30}}{-6}$ and $\frac{\sqrt{-30}}{-15}$ lie in $\frac{\sqrt{-30}}{-6}H$.

So, there are four orbits of $Q^*\left(\sqrt{-30}\right)$.

Example 3.13. By using Theorem 9, the orbits of $Q^*\left(\sqrt{-11}\right)$ are

(i) $\frac{1+\sqrt{-11}}{3}$ and $\frac{-1+\sqrt{-11}}{12}$ lie in $\frac{1+\sqrt{-11}}{3}H$.

(ii) $\frac{1+\sqrt{-11}}{-3}$ and $\frac{-1+\sqrt{-11}}{-12}$ lie in $\frac{1+\sqrt{-11}}{-3}H$.

(iii) $\frac{-1+\sqrt{-11}}{3}$ and $\frac{1+\sqrt{-11}}{12}$ lie in $\frac{-1+\sqrt{-11}}{3}H$.

(iv) $\frac{-1+\sqrt{-11}}{-3}$ and $\frac{1+\sqrt{-11}}{-12}$ lie in $\frac{-1+\sqrt{-11}}{-3}H$.

(v) $\frac{1+\sqrt{-11}}{6}$ and $\frac{-1+\sqrt{-11}}{6}$ lie in $\frac{1+\sqrt{-11}}{6}H$.

(vi) $\frac{1+\sqrt{-11}}{-6}$ and $\frac{-1+\sqrt{-11}}{-6}$ lie in $\frac{1+\sqrt{-11}}{-3}H$.

So, there are six orbits of $Q^*\left(\sqrt{-11}\right)$.

Definition 3.14. If n is a positive integer, then $d\,(n)$ denotes the arithmetic function defined by the number of positive divisors of n which are multiple of 3.

Theorem 3.15. *If $n \neq 3$ then the total number of orbits of $Q^*\left(\sqrt{-n}\right)$ under the action of H are*

$$\begin{cases} d\,(n) & \text{if } n \equiv 0\,(\mathrm{mod}\,3),\ \text{but } n \neq 3. \\ 2d\,(n+1) & \text{if } n \equiv 2\,(\mathrm{mod}\,3). \end{cases}$$

Proof. If $n \equiv 0\,(\mathrm{mod}\,3)$, then the divisors of n which are multiples of 3 are $\pm 3, \pm m_1, \pm m_2, \pm m_3, \ldots, \pm n$. Then by Theorem 3.11 (i) there exist two orbits of $Q^*\left(\sqrt{-n}\right)$ corresponding to the divisors $\pm 3, \pm n$ of n. We therefore left with

$2d(n)-4$ divisors of n. Then by Theorem 3.11 (iv), there exist $\frac{2d(n)-4}{2}$ orbits corresponding to the remaining $2d(n)-4$ divisors of n. Hence there are $2+\frac{2d(n)-4}{2}=d(n)$ orbits of $Q^*\left(\sqrt{-n}\right)$.

If $n\equiv 2\,(\mathrm{mod}\,3)$, then the divisors of $n+1$ which are multiples of 3 are $\pm 3, \pm n_1$, $\pm n_2, \pm n_3, \ldots, \pm(n+1)$. By Theorem 3.11 (ii) and (iii), there exist four orbits corresponding to the divisors $\pm 3, \pm(n+1)$ of $n+1$. Thus we are left with $2d(n+1)-4$ divisors of $n+1$. By Theorem 3.11 (v) and (vi) corresponding to the remaining $2d(n+1)-4$ divisors of $n+1$, there exist $2d(n+1)-4$ orbits. Hence there are $4+2d(n+1)-4=2d(n+1)$ orbits of $Q^*\left(\sqrt{-n}\right)$. □

Example 3.16. Consider $Q^*\left(\sqrt{-30}\right)$. Then the positive divisors of 30 which are multiple of 3 are $3, 6, 15, 30$. Therefore $d(30)=4$, which implies that the total number of orbits are four.

Example 3.17. In $Q^*\left(\sqrt{-11}\right)$. The number of positive divisors of 12 which are multiple of three are $3, 6, 12$. Therefore $d(12)=3$. Hence the total number of orbits are $2d(12)=2\times 3=6$.

Corollary 3.18. *The action of H on $Q^*\left(\sqrt{-n}\right)$ is intransitive.*

References

[1] **B. Everitt**, *Alternating quotients of the $(3,q,r)$ triangle groups*, Comm. Algebra **26** (1997), 1817 – 1832.

[2] **I. Kátai and B. Kovács**, *Canonical number systems in imaginary quadratic fields*, Acta Math. Hungar. **37** (1981) 159 – 164.

[3] **M.P. Lingham** *Modular forms and elliptic curves over imaginary quadratic fields*, Diss. University of Nottingham, 2005.

[4] **Q. Mushtaq**, *Modular group acting on real quadratic fields*, Bull. Austr. Math. Soc. **37** (1988), 303 – 309.

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

[6] **Q. Mushtaq and G.C. Rota**, *Alternating groups as quotients of two generator group*, Advances in Math. **96** (1992), 113 – 1211.

[7] **Q. Mushtaq and H. Servatius**, *Permutation representation of the symmetry groups of regular hyperbolic tessellations*, J. Lond. Math. Soc. **48** (1993), 77 – 86.

[8] **A. Torstensson**, *Coset diagrams in the study of finitely presented groups with an application to quotients of the modular group*, J. Commut. Algebra **2** (2010), 501–514.

Received September 17, 2017

Department of Mathematics, University of Education, Lahore, Jauharabad, Pakistan
E-mail: abdul.razaq@ue.edu.pk

Quasigroups and Related Systems **26** (2018), 149 – 154

On bi-ideals of ordered semigroups

Ze Gu

Abstract. The concepts of strongly quasi-prime, quasi-prime, quasi-semiprime, strongly irreducible and irreducible bi-ideals of an ordered semigroup are introduced. Moreover, we characterize regular and intra-regular ordered semigroups using bi-ideals, and investigate the ordered semigroups in which every bi-ideal is strongly quasi-prime.

1. Introduction and preliminaries

Ideal theory play an important role in characterizations of semigroups and ordered semigroups. Lajos first introduced the concept of bi-ideals in semigroups (see [7]). Li and He characterized the semigroups whose all bi-ideals are prime in [8]; the semigroups whose all bi-ideals are strongly prime were determined by Shabir in [9]. Kehayopulu did much work on characterizations of regular and intra-regular ordered semigroups by ideals, quasi-ideals and bi-ideals (see [1, 2, 3, 4, 5, 6]). The characterizations of regular and intra-regular ordered semigroups in terms of fuzzy subsets were given by Xie and Tang in [10]. In this paper, we first introduce the notions of strongly quasi-prime, quasi-prime, quasi-semiprime, strongly irreducible and irreducible bi-ideals in ordered semigroups, and then characterize regular and intra-regular ordered semigroups by bi-ideals. Finally, we characterize those ordered semigroups in which all bi-ideals are strongly quasi-prime.

We recall some basic notions in ordered semigroups. An *ordered semigroup* is a semigroup $(S, \cdot)$ endowed with an order relation $\leqslant$ such that

$$(\forall a, b, x \in S)\ a \leqslant b \Rightarrow xa \leqslant xb \text{ and } ax \leqslant bx.$$

Let $(S, \cdot, \leqslant)$ be an ordered semigroup. A non-empty subset B of S is called a *bi-ideal* of S if it satisfies the following conditions: (1) $BSB \subseteq B$; (2) $a \in B$ and $b \in S,\ b \leqslant a$ implies $b \in B$. For a nonempty subset H of S, we denote

$$(H] = \{t \in S \mid t \leqslant h \text{ for some } h \in H\}.$$

2010 Mathematics Subject Classification: 06F05, 20M12
Keywords: ordered semigroup, (strongly) quasi-prime bi-ideals, quasi-semiprime bi-ideals, (strongly) irreducible bi-ideals.
This research was supported by the National Natural Science Foundation of China (No. 11701504), the Young Innovative Talent Project of Department of Education of Guangdong Province (No. 2016KQNCX180) and the University Natural Science Project of Anhui Province (No. KJ2018A0329).

It is well known that the intersection of any number of bi-ideals of S is either empty or a bi-ideal of S. For any bi-ideals B_1, B_2 of S, $(B_1B_2]$ is a bi-ideal of S.

An ordered semigroup S is called *regular* ([2, 5]) if for every $a \in S$ there exists $x \in S$ such that $a \leqslant axa$. Equivalent definitions: (1) $A \subseteq (ASA]$ $(\forall A \subseteq S)$; (2) $a \in (aSa]$ $(\forall a \in S)$. An ordered semigroup S is called *intra-regular* ([2, 3]) if for every $a \in S$ there exist $x, y \in S$ such that $a \leqslant xa^2y$. Equivalent definitions: (1) $A \subseteq (SA^2S]$ $(\forall A \subseteq S)$; (2) $a \in (Sa^2S]$ $(\forall a \in S)$.

2. Several classes of bi-ideals

In this section, we mainly introduce and study quasi-prime, strongly quasi-prime, quasi-semiprime, irreducible and strongly irreducible bi-ideals in ordered semigroups.

Definition 2.1. Let S be an ordered semigroup and B a bi-ideal of S. B is called *quasi-prime* (*strongly quasi-prime*) if $B_1B_2 \subseteq B$ $((B_1B_2] \cap (B_2B_1] \subseteq B)$ implies $B_1 \subseteq B$ or $B_2 \subseteq B$ for any bi-ideals B_1 and B_2 of S. B is called *quasi-semiprime* if $B_1^2 \subseteq B$ implies $B_1 \subseteq B$ for any bi-ideal B_1 of S.

Remark 2.2. From Definition 2.1, we know that every strongly quasi-prime bi-ideal of an ordered semigroup S is quasi-prime, and every quasi-prime bi-ideal is quasi-semiprime. However, a quasi-prime bi-ideal is not necessarily strongly quasi-prime and a quasi-semiprime bi-ideal is not necessarily quasi-prime.

Example 2.3. (See [2]) Consider the ordered semigroup $S = \{a, b, c, d, e\}$ with the multiplication " $\cdot$ " and the order " $\leqslant$ " below:

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

$$\leqslant := \{(a,a),(a,b),(a,c),(a,d),(a,e),(b,b),(c,c),(d,d),(e,e)\}.$$

We can deduce that the bi-ideals of S are

$$\{a\},\{a,b\},\{a,c\},\{a,d\},\{a,e\},\{a,b,d\},\{a,c,d\},\{a,b,e\},\{a,c,e\},S.$$

It is easy to see that the bi-ideal $\{a,b,e\}$ is quasi-prime. But it is not strongly quasi-prime. Indeed: we have

$$(\{a,c\}\{a,d\}] = (\{a,c\}] = \{a,c\};$$
$$(\{a,d\}\{a,c\}] = (\{a,d\}] = \{a,d\};$$
$$\{a,c\} \cap \{a,d\} = \{a\} \subseteq \{a,b,e\}.$$

But neither $\{a,c\}$ nor $\{a,d\}$ is contained in $\{a,b,e\}$.

Example 2.4. (See [2]) Consider the ordered semigroup $S = \{a, b, c, d, e\}$ with the multiplication " $\cdot$ " and the order " $\leqslant$ " below:

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

$$\leqslant := \{(a,a),(a,b),(b,b),(c,a),(c,b),(c,c)(d,a),(d,b),(d,d),(e,e)\}.$$

We can obtain that the bi-ideals of S are

$$\{a,c,d\}, \{a,b,c,d\}, \{a,c,d,e\}, S.$$

It is easy to deduce that the bi-ideal $\{a,c,d\}$ is quasi-semiprime. But it is not quasi-prime. Indeed: we have

$$\{a,b,c,d\}\{a,c,d,e\} = \{a,c,d\}.$$

However, neither $\{a,b,c,d\}$ nor $\{a,c,d,e\}$ is contained in $\{a,c,d\}$.

Definition 2.5. A bi-ideal B of an ordered semigroup S is called *irreducible* (*strongly irreducible*) if $B_1 \cap B_2 = B$ ($B_1 \cap B_2 \subseteq B$) implies $B_1 = B$ or $B_2 = B$ ($B_1 \subseteq B$ or $B_2 \subseteq B$) for any bi-ideals B_1 and B_2 of S.

Remark 2.6. Clearly, every strongly irreducible bi-ideal of an ordered semigroup is irreducible. The following example shows that the converse is not true.

Example 2.7. Consider the ordered semigroup S in Example 2.3. The bi-ideal $\{a,b,d\}$ is irreducible but not strongly irreducible because

$$\{a,c\} \cap \{a,e\} = \{a\} \subseteq \{a,b,d\}.$$

But neither $\{a,c\}$ nor $\{a,e\}$ is contained in $\{a,b,d\}$.

Proposition 2.8. *The intersection of any family of quasi-prime bi-ideals of an ordered semigroup is either empty or a quasi-semiprime bi-ideal.*

Proof. Let Γ be a family of quasi-prime bi-ideals and B a bi-ideal. It is well-known that $\bigcap_{\alpha\in\Gamma} B_\alpha$ is either empty or a bi-ideal. Suppose that $\bigcap_{\alpha\in\Gamma} B_\alpha \neq \emptyset$ and $B^2 \subseteq \bigcap_{\alpha\in\Gamma} B_\alpha$. Then $B^2 \subseteq B_\alpha$ for every $\alpha \in \Gamma$. Since B_α is quasi-prime, we have $B \subseteq B_\alpha$. Thus $B \subseteq \bigcap_{\alpha\in\Gamma} B_\alpha$ and so $\bigcap_{\alpha\in\Gamma} B_\alpha$ is quasi-semiprime. □

Proposition 2.9. *Let B be a strongly irreducible quasi-semiprime bi-ideal of an ordered semigroup S. Then B is strongly quasi-prime.*

Proof. Let B_1, B_2 be two bi-ideals of S such that $(B_1B_2] \cap (B_2B_1] \subseteq B$. Since $(B_1 \cap B_2)^2 \subseteq B_1B_2$ and $(B_1 \cap B_2)^2 \subseteq B_2B_1$, we have $(B_1 \cap B_2)^2 \subseteq B_1B_2 \cap B_2B_1 \subseteq (B_1B_2] \cap (B_2B_1] \subseteq B$. Moreover, since B is a quasi-semiprime bi-ideal, $B_1 \cap B_2 \subseteq B$. In addition, from the strong irreducibility of B, we have $B_1 \subseteq B$ or $B_2 \subseteq B$. Thus B is a strongly prime bi-ideal of S. □

3. Regular and intra-regular ordered semigroups

In this section, we mainly characterize regular and intra-regular ordered semigroups by bi-ideals, and investigate the ordered semigroups in which all bi-ideals are strongly quasi-prime.

Theorem 3.1. *Let S be an ordered semigroup. Then the following statements are equivalent:*

(i) *S is both regular and intra-regular;*

(ii) *$(B^2] = B$ for every bi-ideal B of S;*

(iii) *$B_1 \cap B_2 = (B_1B_2] \cap (B_2B_1]$ for all bi-ideals B_1 and B_2 of S;*

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

Proof. $(i) \Rightarrow (ii)$. Let B be a bi-ideal of S. Then $BSB \subseteq B$. Since S is regular and intra-regular, $B \subseteq (BSB]$ and $B \subseteq (SB^2S]$. Thus $B \subseteq (BSB] \subseteq ((BSB](SB]] = (BSBSB] \subseteq ((BS](SB^2S](SB]] \subseteq (BSSB^2SSB] \subseteq (BSBBSB] \subseteq (B^2]$. Also, $(B^2] \subseteq ((BSB](BSB]] = (BSBBSB] \subseteq (BSB] \subseteq (B] = B$.

$(ii) \Rightarrow (i)$. Let $a \in S$. Then $B(a) = (a \cup aSa]$. Since $B = (B^2]$ for every bi-ideal B of S, we have $a \in B(a) = (B^2(a)] = ((B^2(a)](B(a)]] = (B^3(a)] = ((a \cup aSa](a \cup aSa](a \cup aSa]] \subseteq ((a \cup aSa)(a \cup aSa)(a \cup aSa)] \subseteq (aSa]$. Hence S is regular.

Similarly, we have $a \in B(a) = (B^2(a)] = ((B^2(a)](B^2(a)]] = (B^4(a)] = ((a \cup aSa](a \cup aSa](a \cup aSa](a \cup aSa]] \subseteq ((a \cup aSa)(a \cup aSa)(a \cup aSa)(a \cup aSa)] \subseteq (Sa^2S]$. Thus S is intra-regular.

$(ii) \Rightarrow (iii)$. Let B_1 and B_2 be two bi-ideals of S. Then $B_1 \cap B_2$ is either empty or a bi-ideal of S.

Case 1). Suppose that $B_1 \cap B_2 = \emptyset$. Next we prove that $(B_1B_2] \cap (B_2B_1] = \emptyset$. Otherwise, $(B_1B_2] \cap (B_2B_1]$ is a bi-ideal (Since $(B_1B_2]$ and $(B_2B_1]$ are bi-ideals). Thus $(B_1B_2] \cap (B_2B_1] = (((B_1B_2] \cap (B_2B_1])((B_1B_2] \cap (B_2B_1])] \subseteq ((B_1B_2](B_2B_1]] \subseteq ((B_1B_2B_2B_1]] = (B_1B_2B_2B_1] \subseteq (B_1SB_1] \subseteq (B_1] = B_1$. Similarly, $(B_1B_2] \cap (B_2B_1] \subseteq B_2$. Hence $(B_1B_2] \cap (B_2B_1] \subseteq B_1 \cap B_2 = \emptyset$, which is impossible.

Case 2). Suppose that $B_1 \cap B_2 \neq \emptyset$. By hypothesis, $B_1 \cap B_2 = ((B_1 \cap B_2)^2] = ((B_1 \cap B_2)(B_1 \cap B_2)] \subseteq (B_1B_2]$. In the same way, we have $B_1 \cap B_2 \subseteq (B_2B_1]$. Thus,

$$B_1 \cap B_2 \quad \subseteq \quad (B_1B_2] \cap (B_2B_1]. \tag{1}$$

Hence $(B_1B_2] \cap (B_2B_1] \neq \emptyset$ and so $(B_1B_2] \cap (B_2B_1]$ is a bi-ideal. Similar to the proof of Case 1), we have

$$(B_1B_2] \cap (B_2B_1] \subseteq B_1 \cap B_2. \tag{2}$$

By (1) and (2), we obtain that

$$B_1 \cap B_2 = (B_1B_2] \cap (B_2B_1].$$

$(iii) \Rightarrow (iv)$. Let B_1 and B be two bi-ideals of S such that $B_1^2 \subseteq B$. By hypothesis, $B_1 = B_1 \cap B_1 = (B_1^2] \cap (B_1^2] = (B_1^2]$. Thus, we have $B_1 = (B_1^2] \subseteq (B] = B$. Hence every bi-ideal of S is quasi-semiprime.

$(iv) \Rightarrow (ii)$. Let B be a bi-ideal of S. Then $(B^2]$ is a bi-ideal. By hypothesis, $(B^2]$ is quasi-semiprime. Since $B^2 \subseteq (B^2]$, we have $B \subseteq (B^2]$. Furthermore, $(B^2] \subseteq ((B^2](B]] = (B^3] \subseteq (BSB] \subseteq (B] = B$. Hence $B = (B^2]$. □

The following result can be directly obtained from Theorem 3.1.

Proposition 3.2. *Let S be a regular and intra-regular ordered semigroup and B a bi-ideal of S. Then the following statements are equivalent:*

(*i*) *B is strongly irreducible;*

(*ii*) *B is strongly quasi-prime.*

Next we characterize those ordered semigroups in which every bi-ideal is strongly quasi-prime and also those ordered semigroups in which every bi-ideal is strongly irreducible.

Lemma 3.3. *Let S be an ordered semigroup. Then the following statements are equivalent:*

(*i*) *The set of bi-ideals of S is totally ordered under inclusion;*

(*ii*) *Every bi-ideal of S is strongly irreducible and $B_1 \cap B_2 \neq \emptyset$ for any bi-ideals B_1 and B_2 of S;*

(*iii*) *Every bi-ideal of S is irreducible and $B_1 \cap B_2 \neq \emptyset$ for any bi-ideals B_1 and B_2 of S.*

Proof. $(i) \Rightarrow (ii)$. By condition (i), it is obvious that $B_1 \cap B_2 \neq \emptyset$ for any bi-ideals B_1 and B_2 of S. Let B be a bi-ideal of S and B_1, B_2 two bi-ideals such that $B_1 \cap B_2 \subseteq B$. Since the set of bi-ideals of S is totally ordered, either $B_1 \subseteq B_2$ or $B_2 \subseteq B_1$. Thus either $B_1 \cap B_2 = B_1$ or $B_1 \cap B_2 = B_2$. Hence $B_1 \cap B_2 \subseteq B$ implies that $B_1 \subseteq B$ or $B_2 \subseteq B$. This shows that B is strongly irreducible.

$(ii) \Rightarrow (iii)$. The conclusion is obvious.

$(iii) \Rightarrow (i)$. Let B_1 and B_2 be two bi-ideals of S. Since $B_1 \cap B_2 \neq \emptyset$, $B_1 \cap B_2$ is a bi-ideal. By hypothesis, either $B_1 = B_1 \cap B_2$ or $B_2 = B_1 \cap B_2$, that is, $B_1 \subseteq B_2$ or $B_2 \subseteq B_1$. Hence the set of bi-ideals of S is totally ordered. □

Theorem 3.4. *Let S be an ordered semigroup. Then every bi-ideal of S is strongly quasi-prime and $B_1 \cap B_2 \neq \emptyset$ for any bi-ideals B_1 and B_2 of S if and only if S is regular, intra-regular and the set of bi-ideals of S is totally ordered.*

Proof. ($\Rightarrow$). Let every bi-ideal of S be strongly quasi-prime. Then every bi-ideal of S is quasi-semiprime. From Theorem 3.1, we have S is regular and intra-regular. Furthermore, we know that every bi-ideal of S is strongly irreducible from Proposition 3.2. Thus by Lemma 3.3, the set of bi-ideals of S is totally ordered under inclusion.

($\Leftarrow$). Since the set of bi-ideals of S is totally ordered under inclusion, we have $B_1 \cap B_2 \neq \emptyset$ for any bi-ideals B_1 and B_2 of S and every bi-ideal of S is strongly irreducible from Lemma 3.3. Since S is regular and strongly regular, from Proposition 3.2, we obtain that every bi-ideal of S is strongly quasi-prime. □

Acknowledgments

The author are extremely grateful to the referees for their valuable comments and helpful suggestions which help to improve the presentation of this paper.

References

[1] **N. Kehayopulu**, *On prime, weakly prime ideals in ordered semigroups*, Semigroup Forum **44** (1992), 341 – 346.

[2] **N. Kehayopulu**, *On regular, intra-regular ordered semigroups*, Pure Math. Appl. **4** (1993), no. 4, 447 – 461.

[3] **N. Kehayopulu**, *On intra-regular ordered semigroups*, Semigroup Forum **46** (1993), 271 – 278.

[4] **N. Kehayopulu**, *Note on bi-ideals in ordered semigroups*, Pure Math. Appl. **6** (1995), no. 4, 333 – 344.

[5] **N. Kehayopulu**, *On regular ordered semigroups*, Math. Japon. **45** (1997), no. 3, 549 – 543.

[6] **N. Kehayopulu**, *Remark on quasi-ideals of ordered semigroups*, Pure Math. Appl. **25** (2015), no. 2, 144 – 150.

[7] **S. Lajos**, *On the bi-ideals in semigroups*, Proc. Japan Acad. **45** (1969), no. 8, 710 – 712.

[8] **S.Q. Li and Y. He**, *On semigroups whose bi-ideals are prime*, Acta Math. Sinica (in Chinese) **49** (2006), no. 5, 1189 – 1194.

[9] **M. Shabir**, *Prime bi-ideals of semigroups*, Southeast Asian Bull. Math. **31** (2007), 757 – 764.

[10] **X.Y. Xie and J. Tang**, *Regular ordered semigroups intra-regular ordered semigroups in terms of fuzzy subsets*, Iran. J. Fuzzy Syst. **7** (2010), no. 2, 121 – 140.

Received August 8, 2017

School of Mathematics and Statistics
Zhaoqing University
Zhaoqing, Guangdong, P.R. China
e-mail: guze528@sina.com