Quasigroups and Related Systems **32** (2024), 1 − 20
https://doi.org/10.56415/qrs.v32.01

On Baer filters of bounded distributive lattices

Shahabaddin Ebrahimi Atani

Abstract. Following the concept of Baer ideals, we define Baer filters and we will make an intensive investigate the basic properties and possible structures of these filters.

1. Introduction

All lattices considered in this paper are assumed to have a least element denoted by 0 and a greatest element denoted by 1, in other words they are *bounded*.

The notion of an order plays an important role not only throughout mathematics but also in adjacent such as logic, computer science and engineering and, hence, ought to be in the literature. Filters of lattices play a central role in the structure theory and are useful for many purposes. The main aim of this article is that of extending some results obtained for ring theory to the theory of lattices. The main difficulty is figuring out what additional hypotheses the lattice or filter must satisfy to get similar results. Nevertheless, growing interest in developing the algebraic theory of lattices can be found in several papers and books (see for example [2, 3, 4, 7, 8, 9, 10]).

An ideal I of a commutative ring R is called a d-ideal provided that for each $a \in I$ and $x \in R$, $\mathrm{Ann}(a) \subseteq \mathrm{Ann}(x)$ implies that $x \in I$. The concept of d-ideals has been studied by several authors in different forms and by different names. The notion of d-ideals in a commutative ring was introduced by Speed [17] who called them Baer ideals. These ideals were also put to good use in 1972 by Evans [5] when characterizing commutative rings that are finite direct sums of integral domains. In [11], Jayaram introduced fd-ideals (as strongly Baer ideals) and 0-ideals in reduced rings and characterize quasi regular and von Neumann regular rings. In [13], Khabazian, Safaeeyan and

2010 MSC: Primary: 05C69, 06B99; Secondary: 05C15, 05C25.
Keywords: lattice; filter; Baer filter; z-filter.

Vedadi extended the concept of d-ideals to the category of modules and investigated the modules for which their submodules are d-submodules. In [16], Safaeeyan and Taherifar studied d-ideals and fd-ideals in general rings, and not just the reduced ones. In [1], Anebri, Kim and Mahdou investigated the concepts of d-submodules, fd-submodules and 0-submodules of a module over a commutative ring. In [15], Mason investigated the concepts of z-ideals of a commutative ring.

Let $\pounds$ be a *bounded distributive lattice*. We say that a subset $S \subseteq \pounds$ is *join closed* if $0 \in S$ and $s_1 \vee s_2 \in S$ for all $s_1, s_2 \in S$ (clearly, if $\mathbf{p}$ is a prime filter of $\pounds$, then $\pounds \setminus \mathbf{p}$ is a join closed subset of $\pounds$). If F, G are filters of $\pounds$ and $y \in \pounds$, then we define the *filter quotients* $(G :_\pounds F) = \{x \in \pounds : x \vee F \subseteq G\}$ and $(\{1\} :_\pounds y) = (1 :_\pounds y) = \{z \in \pounds : z \vee y = 1\}$; clearly these are another filters of $\pounds$ and $G \subseteq (G :_\pounds F)$. A filter F is said to be a *Baer filter* (resp. *strongly Baer* filter) if $(1 :_\pounds f) \subseteq (1 :_\pounds x)$ for some $f \in F$ and $x \in \pounds$ implies that $x \in F$ (resp. $(1 :_\pounds G) \subseteq (1 :_\pounds x)$ for some finite subset G of F and $x \in \pounds$ implies that $x \in F$). F is said to be a 1-*filter* if $F = \{1\}_S(\pounds) = \{x \in \pounds : x \vee s = 1$ for some $s \in S\}$ for some join closed subset S of $\pounds$. For each element x in a lattice $\pounds$, the intersection of all minimal prime filters in $\pounds$ containing x is denoted by P_x, and a filter F in $\pounds$ is called a z^0-*filter* if $P_x \subseteq F$, for all $x \in F$. A filter F of $\pounds$ is a *strongly* z^0-*filter* if $P_A \subseteq F$ for each finite subset A of F. For each element x in a lattice $\pounds$, the intersection of all maximal filters in $\pounds$ containing x is denoted by M_x, and a filter F in $\pounds$ is called a z-*filter* if $M_x \subseteq F$, for all $x \in F$. In the present paper, we are interested in investigating Baer filters to use other notions of Baer, and associate which exist in the literature as laid forth in [1, 11, 15, 16].

Our objective in this paper is to extend the notion of Baer property in commutative rings to Baer property in the lattices, and to investigate the relations between Baer filters, Strongly Baer filters, z^0-filters, strongly z^0-filters and z-filters. Among many results in this paper, the first, introductional section contains elementatary observations needed later on.

In Section 2, we give basic properties of Baer filters. In particular, we show that the class of lattices for which their Baer filters, strongly Baer filters, z^0-filters and strongly z^0-filters are the same (see Proposition 2.4, Prposition 2.19 and Theorem 2.20). Also, we investigate Baer filters and specify some distinguished classes of Baer filters in a lattice. For example, 1-filters, the filter $(F :_\pounds G)$ where F is a Baer filter and G is a filter of $\pounds$ (so $(1 :_\pounds H)$ for every filter H of $\pounds$), direct meets and all minimal prime filters are Baer filters (see Lemma 2.5, Lemma 2.6, Proposition 2.7, Proposition 2.9 and Proposition 2.12). In this section we observe that in a lattice $\pounds$, If $\mathbf{p}$ is a prime filter of a lattice $\pounds$, then either $\mathbf{p}$ is a Baer filter or the maximal Baer filters contained in $\mathbf{p}$ are prime Baer filters (see Theorem 2.13).

Section 3 is dedicated to the study of z-filters. We show that every minimal prime filter in a semisimple lattice $\pounds$ is a z-filter (see Theorem 3.4). We also prove in Theorem 3.5 that if F is a z-filter of $\pounds$, then every $\mathbf{p} \in \min(F)$ is a z-filter. Here, we observe that in a lattice $\pounds$, Baer filters and z-filters are not coincide generally (see Example 3.7). The remaining part of this section is mainly devoted to investigation of lattices $\pounds$ such that when the class of Baer filters is contained in the class of z-filters (see Theorem 3.8).

Section 4 concentrates to the relation between Baer filters and prime filters. We prove in Theorem 4.4 that every prime filter of $\pounds$ is a Baer filter if and only if every filter of $\pounds$ is a Baer filter. We also show that $\pounds$ is a classical lattice such that for every finitely generated filter $F \subseteq \mathrm{I}(\pounds)$, $(1 :_{\pounds} F) \neq \{1\}$ if and only if every maximal filter of $\pounds$ is a Baer filter (see Theorem 4.5). Moreover, we prove that in a lattice $\pounds$, every prime Baer filter of $\pounds$ is either a minimal prime or a maximal filter if and only if for each maximal filter $\mathbf{m}$ of $\pounds$ and each $m, n \in \mathbf{m}$, there exists a finite subset $A \subseteq (1 :_{\pounds} m)$ and $d \notin \mathbf{m}$ such that $(1 :_{\pounds} T(A \cup \{m\})) \subseteq (1 :_{\pounds} d \vee n)$ (see Theorem 4.6). Finally, we will show that every prime Baer filter of $\pounds$ is a minimal prime filter if and only if for each $a \in \pounds$, there exists a finitely generated filter F such that $F \subseteq (1 :_{\pounds} a)$ and $(1 :_{\pounds} T(F \cup \{a\})) = \{1\}$ (see Theorem 4.7).

Let us recall some notions and notations. By a lattice we mean a poset $(\pounds, \leqslant)$ in which every couple elements x, y has a g.l.b. (called the meet of x and y, and written $x \wedge y$) and a l.u.b. (called the join of x and y, and written $x \vee y$). A lattice $\pounds$ is complete when each of its subsets X has a l.u.b. and a g.l.b. in $\pounds$. Setting $X = \pounds$, we see that any nonvoid complete lattice contains a least element 0 and greatest element 1 (in this case, we say that $\pounds$ is a lattice with 0 and 1). A lattice $\pounds$ is called a distributive lattice if $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$ for all a, b, c in $\pounds$ (equivalently, $\pounds$ is distributive if $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$ for all a, b, c in $\pounds$). A non-empty subset F of a lattice $\pounds$ is called a filter, if for $a \in F$, $b \in \pounds$, $a \leqslant b$ implies $b \in F$, and $x \wedge y \in F$ for all $x, y \in F$ (so if $\pounds$ is a lattice with 1, then $1 \in F$ and $\{1\}$ is a filter of $\pounds$). A proper filter F of $\pounds$ is called prime if $x \vee y \in F$, then $x \in F$ or $y \in F$. A proper filter F of $\pounds$ is said to be maximal if G is a filter in $\pounds$ with $F \subsetneqq G$, then $G = \pounds$. The radical of $\pounds$, denoted by $\mathrm{Rad}(\pounds)$, is the intersection of all maximal filters of $\pounds$.

Let A be subset of a lattice $\pounds$. Then the filter generated by A, denoted by $T(A)$, is the intersection of all filters that is containing A. A filter F is called finitely generated if there is a finite subset A of F such that $F = T(A)$. A lattice $\pounds$ with 1 is called $\pounds$-domain if $a \vee b = 1$ $(a, b \in \pounds)$, then $a = 1$ or $b = 1$. First we need the following lemma proved in [2, 4, 6, 8, 9].

Lemma 1.1. *Let $\pounds$ be a lattice.*

(1) *A non-empty subset F of $\pounds$ is a filter of $\pounds$ if and only if $x \vee z \in F$ and $x \wedge y \in F$ for all $x, y \in F$, $z \in \pounds$. Moreover, since $x = x \vee (x \wedge y)$, $y = y \vee (x \wedge y)$ and F is a filter, $x \wedge y \in F$ gives $x, y \in F$ for all $x, y \in \pounds$.*

(2) *If $F_1, \ldots, F_n$ are filters of $\pounds$ and $a \in \pounds$, then $\bigvee_{i=1}^n F_i = \{\bigvee_{i=1}^n a_i : a_i \in F_i\}$ and $a \vee F_i = \{a \vee a_i : a_i \in F_i\}$ are filters of $\pounds$ and $\bigvee_{i=1}^n F_i = \bigcap_{i=1}^n F_i$.*

(3) *Let A be an arbitrary non-empty subset of $\pounds$. Then*
$T(A) = \{x \in \pounds : \ a_1 \wedge a_2 \wedge \cdots \wedge a_n \leqslant x \text{ for some } a_i \in A \ (1 \leqslant i \leqslant n)\}$.
Moreover, if F is a filter and A is a subset of $\pounds$ with $A \subseteq F$, then $T(A) \subseteq F$, $T(F) = F$ and $T(T(A)) = T(A)$.

(4) *If $\pounds$ is distributive, F, G are filters of $\pounds$, and $y \in \pounds$, then*
$(G :_\pounds F) = \{x \in \pounds : x \vee F \subseteq G\}$,
$(F :_\pounds T(\{y\})) = (F :_\pounds y) = \{a \in \pounds : a \vee y \in F\}$ *and*
$(\{1\} :_\pounds y) = (1 :_\pounds y) = \{z \in \pounds : z \vee y = 1\}$ *are filters of $\pounds$.*

(5) *If $\{F_i\}_{i \in \Delta}$ is a chain of filters of $\pounds$, then $\bigcup_{i \in \Delta} F_i$ is a filter of $\pounds$.*

(6) *If $\pounds$ is distributive, $G, F_1, \cdots, F_n$ are filters of $\pounds$, then*
$G \vee (\bigwedge_{i=1}^n F_i) = \bigwedge_{i=1}^n (G \vee F_i)$.

(7) *If $\pounds$ is distributive and $F_1, \ldots, F_n$ are filters of $\pounds$, then for each i*
$\bigwedge_{i=1}^n F_i = \{\wedge_{i=1}^n a_i : a_i \in F_i\}$ *is a filter of $\pounds$ and $F_i \subseteq \bigwedge_{i=1}^n F_i$.*

2. Basic properties of Baer filters

In this section, we collect some basic properties concerning Baer filters and strongly Baer filters and then investigate the relationship among these filters. Throughout this paper we shall assume, unless otherwise stated, that $\pounds$ is a *bounded distributive lattice*. The proof of the following lemma can be found in [6] (with some different proof and notions), but we give the details for convenience.

Lemma 2.1. *For the lattice $\pounds$ the following statements hold:*

(1) *If F is a proper filter of $\pounds$ with $F \neq \{1\}$, then F contained in a maximal filter of $\pounds$;*
(2) *Every Maximal filter of $\pounds$ is a prime filter.*

Proof. (1). Since the filter F is proper, $\Omega = \{G : G$ is a filter of £ with $F \subseteq G, G \neq \pounds\} \neq \emptyset$. Moreover, $(\Omega, \subseteq)$ is a partial order. Clearly, Ω is closed under taking unions of chains and so the result follows by Zorn's Lemma.

(2). Assume that $\mathbf{m}$ is a maximal filter of $\pounds$ and let $a \vee b \in \mathbf{m}$ with $a, b \notin \mathbf{m}$. Then $\pounds = \mathbf{m} \wedge T(\{a\})$ which implies that $0 = m \wedge (a \vee s)$ for some $m \in \mathbf{m}$ and $s \in \pounds$. Then $\mathbf{m}$ is a filter gives $b = b \vee (m \wedge (a \vee s)) = (b \vee m) \wedge (b \vee a \vee s) \in \mathbf{m}$ which is impossible. Thus $\mathbf{m}$ is prime. □

Lemma 2.2. *Assume that F is a filter of $\pounds$ and let S be a join closed subset of $\pounds$. Then $F_S(\pounds) = \{x \in \pounds : x \vee s \in F$ for some $s \in S\}$ is a filter of $\pounds$ with $F \subseteq F_S(\pounds)$.*

Proof. If $f \in F$, then $f \vee s \in F$ $(s \in S)$ gives $F \subseteq F_S(\pounds)$. Let $x_1, x_2 \in F_S(L)$ and $t \in \pounds$. Then $x_1 \vee s_1, x_2 \vee s_2 \in F$ for some $s_1, s_2 \in S$ (so $s_1 \vee s_2 \in S$) gives $(x_1 \wedge x_2) \vee (s_1 \vee s_2), (x_1 \vee t) \vee s_1 \in F$; hence $x_1 \wedge x_2, x_1 \vee t \in F_S(\pounds)$, as needed. □

We remind the reader with the following definition.

Definition 2.3. Let F be a filter of $\pounds$.

(1) F is said to be a *Baer filter* if $(1 :_\pounds f) \subseteq (1 :_\pounds x)$ for some $f \in F$ and $x \in \pounds$ implies that $x \in F$.
(2) F is said to be a *strongly Baer filter* if $(1 :_\pounds G) \subseteq (1 :_\pounds x)$ for some finite subset G of F and $x \in \pounds$ implies that $x \in F$.
(3) F is said to be a 1-*filter* if $F = \{1\}_S(\pounds)$ for some join closed subset S of $\pounds$.

It can be easily seen that every strongly Baer filter is a Baer filter. It can also be verified that arbitrary intersection of Baer fiters is again a Baer filter. The next result determines the class of lattices for which their Baer filters and strongly Baer filters are the same.

Proposition 2.4. *A filter F of a lattice $\pounds$ is a Baer filter if and only if F is a strongly Baer filter.*

Proof. It is enough to show that if F is Baer filter, then F is a strongly Baer filter. Let $(1 :_\pounds A) \subseteq (1 :_\pounds x)$ for some finite subset $A = \{a_1, a_2, \cdots, a_k\}$ of F (so $\bigwedge_{i=1}^k a_i \in F$, as F is a filter) and $x \in \pounds$. Then $(1 :_\pounds \bigwedge_{i=1}^k a_i) = \bigcap_{i=1}^k (1 :_\pounds a_i) = (1 :_\pounds A) \subseteq (1 :_\pounds x)$ gives $x \in F$, as F is a Baer filter. This completes the proof. □

Lemma 2.5. *For a lattice $\pounds$ the following statements hold:*

(1) *If S is a join closed subset of $\pounds$, then $\{1\}_S(\pounds)$ is a Baer filter.*

(2) *A filter F of $\pounds$ is a Baer filter if and only if for each $f_1, f_2 \in F$ with $(1 :_\pounds f_1) \cap (1 :_\pounds f_2) \subseteq (1 :_\pounds x)$ implies $x \in F$.*

Proof. (1). Let $(1 :_\pounds a) \subseteq (1 :_\pounds x)$ for some $a \in \{1\}_S(\pounds)$ and $x \in \pounds$. Then there exists $s \in S$ such that $a \vee s = 1$ which implies that $s \in (1 :_\pounds a) \subseteq (1 :_\pounds x)$; hence $x \in \{1\}_S(\pounds)$.

(2). If F is a Baer filter, then $(1 :_\pounds f_1 \wedge f_2) = (1 :_\pounds f_1) \cap (1 :_\pounds f_2) \subseteq (1 :_\pounds x)$ gives $x \in F$. Conversely, let $(1 :_\pounds A) \subseteq (1 :_\pounds x)$ for some finite subset $A = \{a_, a_2, \ldots, a_k\}$ of F and $x \in \pounds$. Then $(1 :_\pounds A) = \bigcap_{i=1}^k (1 :_\pounds a_i)$ $= (1 :_\pounds a_1) \cap \bigcap_{i=2}^k (1 :_\pounds a_i) = (1 :_\pounds a_1) \cap (1 :_\pounds \bigwedge_{i=2}^k a_i) \subseteq (1 :_\pounds x)$ gives $x \in F$. □

Lemma 2.6. *Let F and G be filters of $\pounds$. If F is a Baer filter, then $(F :_\pounds G)$ is a Baer filter. In particular, $(1 :_\pounds H)$ is a Baer filter for every filter H of $\pounds$.*

Proof. Let $(1 :_\pounds f) \subseteq (1 :_\pounds x)$ for some $f \in (F :_\pounds G)$ (so $f \vee G \subseteq F$) and $x \in \pounds$. Then for each $g \in G$, $(1 :_\pounds f \vee g) \subseteq (1 :_\pounds x \vee g)$ and $f \vee g \in F$ gives $x \vee G \subseteq F$, as F is a Baer filter; hence $x \in (F :_\pounds G)$. The in particular statement is clear. □

A proper filter F of $\pounds$ is said to be a direct meet of $\pounds$ if $\pounds = F \wedge G$ and $F \cap G = \{1\}$ for some filter G of $\pounds$. Compare the next Proposition with Propostion 2.10 (4) in [16].

Proposition 2.7. *Every direct meet of a lattice $\pounds$ is a Baer filter.*

Proof. Let F be a direct meet of $\pounds$. Then $\pounds = F \wedge G$ and $G \cap F = F \vee G = \{1\}$ for some filter G of $\pounds$. Clearly, $G \cap (1 :_{\pounds} G) = \{1\}$ and $F \subseteq (1 :_{\pounds} G)$. If $x \in (1 :_{\pounds} G)$, then $x = x \wedge 1 \in \pounds = F \wedge G$ gives $x = a \wedge b$ for some $a \in F$ and $b \in G$. This implies that $a, b \in (1 :_{\pounds} G)$ by Lemma 1.1; so $b = 1$ which gives $x = a \in F$. Thus $F = (1 :_{\pounds} G)$. Now the assertion follows from Lemma 2.6. □

Compare the next Proposition with Lemma 3.9 in [12].

Proposition 2.8. *Assume that $\pounds$ be a lattice and let F be a filter of $\pounds$. The following statements are equivalent:*

(1) *F is a Baer filter of $\pounds$;*

(2) *$(1 :_{\pounds} (1 :_{\pounds} f)) \subseteq F$ for each $f \in F$;*

(3) *$F = \bigcup_{f \in F}(1 :_{\pounds} (1 :_{\pounds} f))$.*

Proof. (1) $\Rightarrow$ (2). Let $x \in (1 :_{\pounds} (1 :_{\pounds} f))$ for some $f \in F$. Then $x \vee (1 :_{\pounds} f) = \{1\}$ gives $(1 :_{\pounds} f) \subseteq (1 :_{\pounds} x)$; so $x \in F$, as F is a Baer filter.

(2) $\Rightarrow$ (3). By (2), $H = \bigcup_{f \in F}(1 :_{\pounds} (1 :_{\pounds} f)) \subseteq F$. If $e \in F$, then $e \in (1 :_{\pounds} (1 :_{\pounds} e)) \subseteq H$ and so we have equality.

(3) $\Rightarrow$ (1). Let $(1 :_{\pounds} f) \subseteq (1 :_{\pounds} x)$ for some $f \in F$ and $x \in \pounds$. This implies that $x \in (1 :_{\pounds} (1 :_{\pounds} x)) \subseteq (1 :_{\pounds} (1 :_{\pounds} f)) \subseteq F$ by (3), as required. □

Proposition 2.9. *Let $\pounds$ be a lattice. The following hold:*

(1) *If $\mathbf{p}$ is a prime filter of $\pounds$, then $1_{\mathbf{p}} = \{x \in \pounds : (1 :_{\pounds} x) \cap (\pounds \setminus \mathbf{p}) \neq \{1\}\}$ is a Baer filter;*

(2) *If $x \in \pounds$, then $F = (1 :_{\pounds} (1 :_{\pounds} x))$ is a Baer filter;*

(3) *If $x \in \pounds$, then $(1 :_{\pounds} x)$ is a Baer filter.*

Proof. (1). Let $x_1, x_2 \in 1_{\mathbf{p}}$ and $t \in \pounds$. Then there exist $1 \neq a \notin \mathbf{p}$ and $1 \neq b \notin \mathbf{p}$ (so $1 \neq a \vee b \notin \mathbf{p}$) such that $a \vee x_1 = 1 = b \vee x_2$ which implies that $a \vee b \in (1 :_{\pounds} (x_1 \wedge x_2)) \cap (\pounds \setminus \mathbf{p})$; hence $x_1 \wedge x_2 \in 1_{\mathbf{p}}$. Similarly, $x_1 \vee t \in 1_{\mathbf{p}}$. Thus $1_{\mathbf{p}}$ is a filter of $\pounds$. To see that $1_{\mathbf{p}}$ is a Baer filter, at first we show that $1_{\mathbf{p}} = \bigcup_{x \in \pounds \setminus \mathbf{p}}(1 :_{\pounds} x) = H$. If $x \in 1_{\mathbf{p}}$, then $x \vee z = 1$ for some $1 \neq z \in \pounds \setminus \mathbf{p}$. This implies that $1 \neq x \in (1 :_{\pounds} z) \subseteq H$; so $1_{\mathbf{p}} \subseteq H$. Similarly, $H \subseteq 1_{\mathbf{p}}$, and so we have equality. Let $(1 :_{\pounds} a) \subseteq (1 :_{\pounds} x)$ for some $a \in 1_{\mathbf{p}}$ and $x \in \pounds$. Then there exists $1 \neq t \in \pounds \setminus \mathbf{p}$ such that $a \vee t = 1$. Then $t \in (1 :_{\pounds} a) \subseteq (1 :_{\pounds} x)$ which gives $1 \neq t \in (1 :_{\pounds} x) \cap (\pounds \setminus \mathbf{p})$; thus $x \in 1_{\mathbf{p}}$.

(2). It suffices to show that for each $y \in F$, $(1 :_{\pounds} (1 :_{\pounds} y)) \subseteq F$ by Proposition 2.8. Let $z \in (1 :_{\pounds} (1 :_{\pounds} y))$. Then $z \vee (1 :_{\pounds} y) = \{1\} = y \vee (1 :_{\pounds} x)$ gives $(1 :_{\pounds} x) \subseteq (1 :_{\pounds} y) \subseteq (1 :_{\pounds} z)$ which implies that $z \vee (1 :_{\pounds} x) = \{1\}$; so $z \in F$.

(3). Since $(1 :_{\pounds} x) = (1 :_{\pounds} (1 :_{\pounds} (1 :_{\pounds} x)))$, $(1 :_{\pounds} x)$ is a Baer filter by (2) and Lemma 2.6. □

Proposition 2.10. *A lattice $\pounds$ is a $\pounds$-domain if and only if it has no nontrivial Baer filter.*

Proof. Assume that $F \neq \{1\}$ is a Baer filter of $\pounds$ and let $1 \neq x \in F$. Then $(1 :_{\pounds} x) = \{1\}$, as $\pounds$ is a $\pounds$-domain. Thus for each $y \in \pounds$, $(1 :_{\pounds} x) \subseteq (1 :_{\pounds} y)$ which implies that $y \in F$ since F is a Baer filter. Hence $F = \pounds$. Conversely, for each $x \in \pounds$, $(1 :_{\pounds} x)$ is a Baer filter by Proposition 2.9 (3); so either $(1 :_{\pounds} x) = \{1\}$ or $(1 :_{\pounds} x) = \pounds$. Thus for each $1 \neq x \in \pounds$, $(1 :_{\pounds} x) = \{1\}$. Hence $\pounds$ is a $\pounds$-domain. □

Let $\pounds$ be a lattice. We denote by Spec($\pounds$) the set of all prime filters of $\pounds$. If F is a filter in $\pounds$, the set of all minimal prime filters over F (or belonging to F) will be denoted by $\min(F)$. We need the following proposition proved in [6, Proposition 2.7].

Proposition 2.11. *For a lattice $\pounds$ the following statements hold:*

(1) *If F is a filter and $\mathbf{p}$ is a prime filter of $\pounds$, then $\mathbf{p} \in \min(F)$ if and only if for each $x \in \mathbf{p}$, there is a $y \notin \mathbf{p}$ such $y \vee x \in F$;*

(2) *If $\mathbf{p}$ is a prime filter of $\pounds$, then $\mathbf{p} \in \min(\pounds)$ if and only if for each $x \in \mathbf{p}$, there is a $y \notin \mathbf{p}$ such that $y \vee x = 1$.*

The next result shows that every minimal prime filter of a lattice $\pounds$ is a Baer filter. Compare the next Proposition with Propostion 2.13 (1) in [16].

Proposition 2.12. *If F is a Baer filter of a lattice $\pounds$, then every minimal prime filter over F is a Baer filter.*

Proof. Suppose that $\mathbf{p} \in \min(F)$ and let $(1 :_{\pounds} p) \subseteq (1 :_{\pounds} x)$ for some $p \in \mathbf{p}$ and $x \in \pounds$. Then $p \vee p' \in F$ for some $p' \notin \mathbf{p}$ by Proposition 2.11 (1). Clearly, $(1 :_{\pounds} p \vee p') \subseteq (1 :_{\pounds} p' \vee x)$. This implies that $x \vee p' \in F \subseteq \mathbf{p}$, as F is a Baer filter, and therefore $x \in \mathbf{p}$. □

Theorem 2.13. *If $\mathbf{p}$ is a prime filter of a lattice $\pounds$, then either $\mathbf{p}$ is a Baer filter or the maximal Baer filters contained in $\mathbf{p}$ are prime Baer filters.*

Proof. Set $\Omega = \{F : F$ is a Baer filter of $\pounds$ and $F \subseteq \mathbf{p}\}$. Then $\{1\} \in \Omega$ and $(\Omega, \subseteq)$ is a partial order. Clearly, Ω is closed under taking unions of chains and so by Zorn's Lemma, Ω has a maximal element, say $\mathbf{m}$. It is clear that $\mathbf{p} = \mathbf{m}$ if and only if $\mathbf{p}$ is a prime Baer filter. If $\mathbf{m} \subsetneqq \mathbf{p}$, then there exists a prime filter $\mathbf{m}'$ minimal with respect to $\mathbf{m} \subseteq \mathbf{m}'$ and $\mathbf{m}' \subsetneqq \mathbf{p}$ since $\mathbf{m}'$ will be a Baer filter by Proposition 2.12. So, either $\mathbf{m}' = \mathbf{m}$ which gives $\mathbf{m}$ is prime, or $\mathbf{m} \subsetneqq \mathbf{m}'$ which contradicts the maximality of $\mathbf{m}$. □

Theorem 2.14. If F is a 1-filter of $\pounds$, then every $\mathbf{p} \in \min(F)$ is a minimal prime filter of $\pounds$.

Proof. By assumption, $F = \{1\}_S(\pounds) = \{x \in \pounds : x \vee s = 1$ for some $s \in S\}$ for some join closed subset S of $\pounds$. By Proposition 2.11 (2), it suffices to show that for each $x \in \mathbf{p}$ there exists $y \notin \mathbf{p}$ such that $y \vee x = 1$. Let $x \in \mathbf{p}$. Then by Proposition 2.11 (1), there is $y \notin \mathbf{p}$ such that $x \vee y \in F$ and $\mathbf{p} \cap S = \emptyset$. So $x \vee y \vee s = 1$ for some $s \in S \setminus \mathbf{p}$. Thus $x \vee y \vee s = 1$ and $y \vee s \notin \mathbf{p}$ and hence $\mathbf{p}$ is a minimal prime filter of $\pounds$. □

Compare the next Theorem with Lemma 2.5 in [16].

Theorem 2.15. *Let F be a filter of a lattice $\pounds$. Then F contained in a proper Baer filter if and only if for each finite subset K of F, $(1 :_\pounds K) \neq \{1\}$.*

Proof. Assume to the contrary, that F is contained in a proper Bear filter G and K a finite subset of F such that $(1 :_\pounds K) = \{1\}$. Let $y \in \pounds$. Then $(1 :_\pounds K) \subseteq (1 :_\pounds y)$ gives $y \in G$; so $G = \pounds$ which is a contradiction. Conversely, suppose that F has the stated property and put

$$H = \{x \in \pounds : (1 :_\pounds K) \subseteq (1 :_\pounds x) \text{ for some finite subset } K \text{ of } F\}.$$

Let $x_1, x_2 \in H$ and $t \in \pounds$. Then there exist finite subsets H_1, H_2 of F such that $(1 :_\pounds H_1) \subseteq (1 :_\pounds x_1)$ and $(1 :_\pounds H_2) \subseteq (1 :_\pounds x_2)$. It follows that $(1 :_\pounds H_1 \wedge H_2) \subseteq (1 :_\pounds H_1) \cap (1 :_\pounds H_2) \subseteq (1 :_\pounds x_1) \cap (1 :_\pounds x_2) \subseteq (1 :_\pounds x_1 \wedge x_2)$ and $(1 :_\pounds H_1) \subseteq (1 :_\pounds x_1) \subseteq (1 :_\pounds x_1 \vee t)$; hence $x_1 \wedge x_2, x_1 \vee t \in H$. Therefore H is a filter of $\pounds$. Let $(1 :_\pounds K) \subseteq (1 :_\pounds y)$ for some finite subset $K = \{k_1, \cdots, k_m\}$ of H and $y \in \pounds$. There are finite subsets $K_1, \cdots, K_m$ of F such that $(1 :_\pounds K_i) \subseteq (1 :_\pounds k_i)$ for each $1 \leqslant i \leqslant m$. Set $K' = \bigvee_{i=1}^m K_i \subseteq F$. If $z \in (1 :_\pounds K')$, then $z \vee K' = \{1\}$ gives $z \vee K_i = \{1\}$ (so $z \vee k_i = 1$) for each $1 \leqslant i \leqslant m$ which implies that $z \in (1 :_\pounds K) \subseteq (1 :_\pounds x)$; hence $(1 :_\pounds K') \subseteq (1 :_\pounds x)$ and so $x \in H$. Thus H is a Baer filter. Moreover, if $f \in F$, then $(1 :_\pounds \{f\}) \subseteq (1 :_\pounds f)$ gives $F \subseteq H$. □

Compare the next Theorem with Proposition 2.14 in [16].

Theorem 2.16. *If $F_1, F_2, \cdots, F_m$ are filters of $£$ such that for each $i \neq j$, $F_i \wedge F_j = £$, then $\bigcap_{i=1}^m F_i$ is a Baer filter if and only if each F_i $(1 \leqslant i \leqslant m)$ is a Baer filter.*

Proof. (1). One side is clear. To see the other side, suppose that $\bigcap_{i=1}^m F_i$ is a Baer filter, $f \in F_j$ for some $1 \leqslant j \leqslant m$ and $b \in £$ such that $(1 :_£ f) \subseteq (1 :_£ b)$. Set $F = \bigcap_{i=1, i\neq j}^m F_i$. We claim that $F \wedge F_j = £$. On the contrary, assume that $F \wedge F_j \neq £$. Then there is a maximal filer $\mathbf{m}$ of $£$ such that $F \wedge F_j \subseteq \mathbf{m}$ by Lemma 2.1 (1) (so $F_j \subseteq \mathbf{m}$ and $F \subseteq \mathbf{m}$). Then there is a $1 \leqslant s \leqslant m$ with $s \neq j$ such that $F_s \subseteq \mathbf{m}$. Otherwise, for each $1 \leqslant i \leqslant m$ with $i \neq j$, there exists $f_i \in F_i \setminus \mathbf{m}$, but then $\bigvee_{i=1, i\neq j}^m f_i \in F \setminus \mathbf{m}$ By Lemma 2.1 (2), and this contradicts the statement of $F \subseteq \mathbf{m}$. So $£ = F_j \wedge F_s \subseteq \mathbf{m}$, a contradiction. Therefore $F_j \wedge F = £$ and hence $0 = f_j \wedge y$ for some $f_j \in F_j$ and $y \in F$. So $b = (b \vee f_j) \wedge (b \vee y)$ and $(1 :_£ f \vee y) \subseteq (1 :_£ b \vee y)$. Since $f \vee y \in \bigcap_{i=1}^m F_i$ and it is a Baer filter, $b \vee y \in \bigcap_{i=1}^m F_i$. Thus $b \vee y \in F_j$. Since $b \vee f_j \in F_j$ and $b \vee y \in F_j$, $b \in F_j$. Therefore F_j is a Baer filter. $\square$

For each element x in a lattice $£$, the intersection of all minimal prime filters in $£$ containing x is denoted by P_x, and a filter F in $£$ is called a z^0-filter if $P_x \subseteq F$, for all $x \in F$. Clearly, $P_1 = \bigcap_{1\in\mathbf{p}\in\min(£)} \mathbf{p} = \bigcap_{\mathbf{p}\in\min(£)} \mathbf{p} = \{1\}$ by [6, Lemma 2.6], $x \in P_x$ and if $a \in P_x$, then $P_a \subseteq P_x$. A filter F of $£$ is a strongly z^0-filter if $P_A \subseteq F$ for each finite subset A of F. It can be easily seen that every strongly z^0-filter is a z^0-filter. For each $a \in £$, set $V(a) = \{\mathbf{p} \in \min(£) : a \in \mathbf{p}\}$.

Proposition 2.17. *For a lattice $£$ the following statements hold:*

(1) *For every $x \in £$ and a finite subset A of $£$, $(1 :_£ A) \subseteq (1 :_£ x)$ if and only if $V(A) \subseteq V(x)$, i.e. $P_x \subseteq P_A$;*

(2) *For $a, b \in £$, $(1 :_£ a) \subseteq (1 :_£ b)$ if and only if $P_b \subseteq P_a$, i.e. $V(a) \subseteq V(b)$.*

Proof. (1). Let $\mathbf{p} \in P_A$ and $x \in £$ such that $(1 :_£ A) =$

$$(1 :_£ A) = \bigcap_{i=1}^k (1 :_£ a_i) = (1 :_£ \bigwedge_{i=1}^k a_i) \subseteq (1 :_£ x),$$

where $A = \{a_1, a_2, \cdots, a_k\} \subseteq \mathbf{p}$. By Proposition 2.11, there exist the sequence $\{b_1, b_2, \cdots, b_k\} \subseteq £ \setminus \mathbf{p}$ such that for each $1 \leqslant i \leqslant k$, $a_i \vee b_i = 1$.

Set $b = \bigvee_{i=1}^{k} b_i$. Then $1 \neq b \notin \mathbf{p}$. By assumption, $b \vee (\bigwedge_{i=1}^{k} a_i) = 1$ gives $b \in (1 :_{\pounds} x)$ and hence $b \vee x = 1 \in \mathbf{p}$. This implies that $x \in \mathbf{p}$, as $\mathbf{p}$ is prime. Thus $V(A) \subseteq V(x)$. Conversely, let $x \in \pounds$ and $A = \{a_1, a_2, \cdots, a_k\}$ be a finite subset of $\pounds$ and $y \in (1 :_{\pounds} A) = \bigcap_{i=1}^{k}(1 :_{\pounds} a_i)$. This implies that $y \vee a_i = 1$ for each $1 \leqslant i \leqslant k$. Then $P_x \subseteq P_A \subseteq \bigcap_{i=1}^{k} P_{a_i}$ gives $x \vee y \in P_{x \vee y} \subseteq \bigcap_{i=1}^{k} P_{a_i \vee y} = P_1 = \{1\}$ and hence $x \vee y = 1$, as needed.

(2). This is clear by (1). □

Lemma 2.18. *Let F be a filter of a lattice $\pounds$. The following hold:*

(1) *F is a z^0-filter if and only if for each $a \in F$ and $b \in \pounds$, $P_b \subseteq P_a$ implies $b \in F$.*

(2) *F is a strongly z^0-filter if and only if for each $a \in \pounds$ and a finite subset A of $\pounds$, $P_a \subseteq P_A$ implies $a \in F$.*

Proof. (1). Assume that F is a z^0-filter and let $P_b \subseteq P_a$, where $a \in F$ and $b \in \pounds$ which gives $b \in P_b \subseteq P_a \subseteq F$. Conversely, let $x \in F$ and $y \in Px$. Then by assumption, $P_y \subseteq P_x$ and $x \in F$ gives $y \in F$; so $P_x \subseteq F$.

(2). Suppose that F is a strongly z^0-filter and let $P_a \subseteq P_A$ for some $a \in \pounds$ and a finite subset A of $\pounds$. By assumption, $a \in P_a \subseteq P_A \subseteq F$. Conversely, let B be a finite subset of $\pounds$ and $z \in P_B$. Then by assumption, $P_z \subseteq P_B$ gives $z \in F$. Thus $P_B \subseteq F$. This completes the proof. □

Proposition 2.19. *A filter F of a lattice $\pounds$ is a z^0-filter if and only if F is a strongly z^0-filter.*

Proof. It is enough to show that if F is z^0-filter, then F is a strongly z^0-filter. Let $P_a \subseteq P_A$ for some $a \in \pounds$ and a finite set $A = \{a_1, a_2, \cdots, a_k\}$ of $\pounds$. Then $(1 :_{\pounds} \bigwedge_{i=1}^{k} a_i) = \bigcap_{i=1}^{k}(1 :_{\pounds} a_i) = (1 :_{\pounds} A) \subseteq (1 :_{\pounds} a)$ by Proposition 2.17; so again by Proposition 2.17, $P_a \subseteq P_{\bigwedge_{i=1}^{k} a_i}$ gives $a \in F$, as F is a z^0-filter. Thus F is a strongly z^0-filter by Lemma 2.18. □

The following result determines the class of lattices for which their Baer filters and z^0-filters are the same.

Theorem 2.20. *A filter F of a lattice $\pounds$ is a Baer filter if and only if F is a z^0-filter.*

Proof. Assume that F is a Baer filter and let $a \in F$ and $b \in \pounds$ such that $P_b \subseteq P_a$. By Proposition 2.17, $(1 :_{\pounds} a) \subseteq (1 :_{\pounds} b)$. Now F is a Baer filter gives $b \in F$. Thus F is a z^0-filter. Conversely, suppose that F is a z^0-filter and let $(1 :_{\pounds} a) \subseteq (1 :_{\pounds} b)$ for some $a \in F$ and $b \in \pounds$. Then by Proposition 2.17, we have $b \in P_b \subseteq P_a \subseteq F$, i.e. the result holds. □

3. Some properties of z-filters

For each element x in a lattice $\pounds$, the intersection of all maximal filters in $\pounds$ containing x is denoted by M_x, and a filter F in $\pounds$ is called a z-filter if $M_x \subseteq F$, for all $x \in F$. Clearly, $M_1 = \mathrm{Rad}(\pounds)$, $x \in M_x$ and if $a \in M_x$, then $M_a \subseteq M_x$. A lattice $\pounds$ is called semisimple provided that $\mathrm{Rad}(\pounds) = \{1\}$.

Lemma 3.1. *Let F be a filter of $\pounds$. Then F is a z-filter if and only if for each $a \in F$ and $b \in \pounds$, $M_b \subseteq M_a$ implies $b \in F$.*

Proof. Assume that F is a z-filter and let $M_b \subseteq M_a$, where $a \in F$ and $b \in \pounds$. It follows that $b \in M_b \subseteq M_a \subseteq F$. Conversely, let $x \in F$ and $y \in M_x$. Then by assumption, $M_y \subseteq M_x$ and $x \in F$ gives $y \in F$; so $M_x \subseteq F$. □

Remark 3.2. 1. If $\mathbf{m}$ is a maximal filter of $\pounds$, then $M_a \subseteq \mathbf{m}$ for all $a \in \mathbf{m}$. Thus the family of z-filters contains the set of maximal filters of $\pounds$.

2. It can be easily seen that any intersection of z-filters is a z-filter.

3. By (1) and (2), $\mathrm{Rad}(\pounds)$ is a z-filter. Moreover, if $x \in \mathrm{Rad}(\pounds)$, F is any z-filter and $y \in F$, then $M_x \subseteq M_y$ gives $x \in F$. Therefore $\mathrm{Rad}(\pounds)$ is contained in every z-filter.

4. The intersections of maximal filters are the most obvious z-filters and they will be called strong z-filters.

5. Suppose that $T(\{x\})$ is a z-filter; we show that

$$T(\{x\}) = \bigcap\{\mathbf{m} \in \mathrm{Max}(\pounds) : T(\{x\}) \subseteq \mathbf{m}\}.$$

If $y \in \bigcap\{\mathbf{m} \in \mathrm{Max}(\pounds) : T(\{x\}) \subseteq \mathbf{m}\}$, then $M_y \subseteq M_x$ gives $y \in T(\{x\})$, and so we have equality. Thus any cyclic z-filter is a strong z-filter.

Proposition 3.3. *If F is a z-filter, then $(F :_{\pounds} G)$ is a z-filter for any G.*

Proof. Let $M_b \subseteq M_a$ for some $a \in (F :_{\pounds} G)$ and $b \in \pounds$. Then $M_{b\vee g} \subseteq M_{a\vee g}$ for all $g \in G$. Since $a \vee g \in F$, $b \vee g \in F$ for all $g \in G$, i.e. $b \in (F :_{\pounds} G)$. □

Theorem 3.4. *Every minimal prime filter in a semisimple lattice $\pounds$ is a z-filter.*

Proof. Assume that $\mathbf{p}$ is a minimal prime filter of $\pounds$ and let $M_q \subseteq M_p$ for some $p \in \mathbf{p}$ and $q \in \pounds$. Since $\mathbf{p}$ is minimal prime, there exists a $y \notin \mathbf{p}$ such that $p \vee y = 1$ by Proposition 2.11. We claim that $q \vee y = 1$. Assume to the contrary, that $y \vee q \neq 1$. By Lemma 2.1, there exists a maximal filter $\mathbf{m}$ such that $y \vee q \notin \mathbf{m}$, since an element which belongs to every maximal filter is 1, as $\pounds$ is semisimple. Then $\mathbf{m} \wedge T(\{y \vee q\}) = \pounds$, as $\mathbf{m}$ is a maximal filter and so there would be elements $s \in \pounds$ and $m \in \mathbf{m}$ such that $0 = m \wedge (y \vee q \vee s)$, which then implies $p = (p \vee m) \wedge (p \vee y \vee q \vee s) = p \vee m$, and hence $p \in \mathbf{m}$. But $q \in M_q \subseteq M_p \subseteq \mathbf{m}$, so we would have $q \in \mathbf{m}$, and hence $q \vee y \in \mathbf{m}$, leading to a contradiction. Therefore $y \vee q = 1 \in \mathbf{p}$, and since $\mathbf{p}$ is prime with $y \notin \mathbf{p}$, we deduce that $q \in \mathbf{p}$. Thus, $\mathbf{p}$ is a z-filter. □

Compare the next theorem with Theorem 1.1 in [15].

Theorem 3.5. *If F is a z-filter of $\pounds$, then every $\mathbf{p} \in \min(F)$ is a z-filter.*

Proof. It suffices to show that if $\mathbf{p}$ is a prime filter containing F which is not a z-filter, it is not minimal. If $\mathbf{p}$ is not a z-filter, then there are elements $q \notin \mathbf{p}$ and $p \in \mathbf{p}$ such that $M_q \subseteq M_p$ by Lemma 3.1. Set $D = (\pounds \setminus \mathbf{p}) \cup H$, where $H = \{p \vee s : s \notin \mathbf{p}\}$. Clearly, $0 \in D$. Let $x, y \in D$. If $x, y \notin \mathbf{p}$, then $x \vee y \notin \mathbf{p}$ gives $x \vee y \in D$. If $x \notin \mathbf{p}$ and $y \in H$, then there exists $u \notin \mathbf{p}$ such that $y = u \vee p$ which implies that $x \vee y = (x \vee u) \vee p \in H \subseteq D$. Similarly, if $x \in H$ and $y \notin \mathbf{p}$, we have $x \vee y \in D$. If $x, y \in H$, then $x = p \vee u$ and $y = p \vee u'$ for some $u, u' \notin \mathbf{p}$. Then $x \vee y = p \vee (u \vee u') \in H \subseteq D$. Thus D is a join closed subset of $\pounds$. If $x \in F \cap D$, then $x \in H$; so $x = p \vee s$ for some $s \notin \mathbf{p}$. By assumption, $M_{q \vee s} \subseteq M_{p \vee s}$ and $p \vee s \in F$ gives $q \vee s \in F \subseteq \mathbf{p}$. But $q, s \notin \mathbf{p}$ and $\mathbf{p}$ is prime. Thus $D \cap F = \emptyset$. By [6, Lemma 2.6 (i)], There is a prime filter $F \subseteq \mathbf{p}'$ which is maximal with respect to the property $\mathbf{p}' \cap F = \emptyset$ and it is clear that $\mathbf{p}' \subsetneqq \mathbf{p}$. Thus $\mathbf{p}$ is not minimal. □

Compare the next corollary with Theorem 1.5 in [15].

Corollary 3.6. *If $\mathbf{p}$ is a prime filter of a semisimple lattice $\pounds$, then either $\mathbf{p}$ is a z-filter or the maximal z-filters contained in $\mathbf{p}$ are prime z-filters.*

Proof. Set $\Delta = \{G : G \text{ is a z-filter of } \pounds \text{ and } G \subseteq \mathbf{p}\}$. Then $\{1\} \in \Delta$ and Δ is inductive so by Zorn's lemma, Δ has a maximal element, say $\mathbf{q}$. It is clear that $\mathbf{p} = \mathbf{q}$ if and only if $\mathbf{p}$ is a prime z-filter. If $\mathbf{q} \subsetneqq \mathbf{p}$, then there exists a prime filter $\mathbf{q}'$ minimal with respect to $\mathbf{q} \subseteq \mathbf{q}'$ and $\mathbf{q}' \subsetneqq \mathbf{p}$ since $\mathbf{q}'$ will be a z-filter by Theorem 3.5. So, either $\mathbf{q}' = \mathbf{q}$ which gives $\mathbf{q}$ is prime, or $\mathbf{q} \subsetneqq \mathbf{q}'$ which contradicts the maximality of $\mathbf{q}$. □

The following example shows that z-filters are not necessarily Baer filters.

Example 3.7. Let $D = \{a, b, c\}$. Then $\pounds = \{X : X \subseteq D\}$ forms a distributive lattice under set inclusion greatest element D and least element $\emptyset$ (note that if $x, y \in \pounds$, then $x \vee y = x \cup y$ and $x \wedge y = x \cap y$). It can be easily seen that proper filters of $\pounds$ are $\{D\}$, $F_1 = \{D, \{a, b\}\}$, $F_2 = \{D, \{a, c\}\}$, $F_3 = \{D, \{b, c\}\}$, $F_4 = \{D, \{a, c\}, \{a, b\}\{a\}\}$, $F_5 = \{D, \{b, c\}, \{a, b\}\{b\}\}$ and $F_6 = \{D, \{a, c\}, \{c, b\}\{c\}\}$. Then

$$F_3 = (1 :_\pounds \{a\}) \subseteq (1 :_\pounds \{a, b\}) = F_6, \{a, b\} \in F_5$$

and $\{a\} \notin F_5$. This shows that F_5 is not a Baer filter, but F_5 is a z-filter since it is maximal. So Baer filters and z-filters are not coincide generally.

The following theorem shows when the class of Baer filters is contained in the class of z-filters. Compare the next Theorem with Propostion 2.9 in [16].

Theorem 3.8. *For a lattice $\pounds$ the following statements are equivalent:*

(1) *$\pounds$ is semisimple;*

(2) *Every Baer filter of $\pounds$ is a z-filter.*

Proof. (1) $\Rightarrow$ (2). Assume that F is a Baer filter of $\pounds$ and let $M_b \subseteq M_a$, where $a \in F$ and $b \in \pounds$. Let $x \in (1 :_\pounds a)$. Then $M_b \subseteq M_a$ gives $M_{b\vee x} \subseteq M_{x\vee a} \subseteq M_1 = \mathrm{Rad}(\pounds) = \{1\}$. Hence $b \vee x \in M_{b\vee x} = \{1\}$ which implies that $(1 :_\pounds a) \subseteq (1 :_\pounds b)$; thus $b \in F$, as F is Baer Filter. Therefore F is a z-filter.

(2) $\Rightarrow$ (1). Suppose that every Baer filter is a z-filter; so $\{1\}$ is a z-filter which gives $\mathrm{Rad}(\pounds) = M_1 \subseteq \{1\}$ and hence $\mathrm{Rad}(\pounds) = \{1\}$. Thus $\pounds$ is semisimple. □

4. Further results

This section is devoted to the relation between Baer filters and prime filters. Let us begin the following proposition.

Proposition 4.1. *For a lattice $\pounds$ the following statements hold:*

(1) *If F is a filter, $\mathbf{p}$ is a prime filter of $\pounds$ and $F \cap \mathbf{p}$ is a Baer filter, then either F or $\mathbf{p}$ is a Baer filter;*

(2) *If $\mathbf{p}$ and $\mathbf{q}$ are prime filters of $\pounds$ which do not belong to a chain,*

then $\mathbf{p}$ *and* $\mathbf{q}$ *are both Baer filters if and only if* $\mathbf{p}\cap\mathbf{q}$ *is a Baer filter;*

(3) *If* F *is a filter,* $\mathbf{m}$ *is a maximal filter of* $\pounds$ *such that* $F \nsubseteq \mathbf{m}$*, then* F *and* $\mathbf{m}$ *are both Baer filters if and only if* $F \cap \mathbf{m}$ *is a Baer filter.*

Proof. (1). If $F \subseteq \mathbf{p}$, then $\mathbf{p} \cap F = F$ is a Baer filter. So we may assume that there exists $x \in F$ with $x \notin \mathbf{p}$. Let $(1 :_\pounds p) \subseteq (1 :_\pounds y)$ for some $p \in \mathbf{p}$ and $y \in \pounds$. Then $(1 :_\pounds x \vee p) \subseteq (1 :_\pounds x \vee y)$ and $p \vee x \in \mathbf{p} \cap F$ gives $x \vee y \in \mathbf{p} \cap F$, as $\mathbf{p} \cap F$ is a Baer filter which implies that $y \in \mathbf{p}$. Thus $\mathbf{p}$ is a Baer filter.

(2). We need only prove the converse. Assume that $\mathbf{q} \nsubseteq \mathbf{p}$ (so there exists $x \in \mathbf{q}$ with $x \notin \mathbf{p}$) and let $(1 :_\pounds p) \subseteq (1 :_\pounds y)$ for some $p \in \mathbf{p}$ and $y \in \pounds$. Then $(1 :_\pounds x \vee p) \subseteq (1 :_\pounds x \vee y)$ and $p \vee x \in \mathbf{p} \cap \mathbf{q}$ gives $x \vee y \in \mathbf{q} \cap \mathbf{p} \subseteq \mathbf{p}$, as $\mathbf{q} \cap \mathbf{p}$ is a Baer filter; hence $y \in \mathbf{p}$. Consequently, $\mathbf{p}$ is a Baer filter and so is $\mathbf{q}$ via similar argument.

(3). Since $\mathbf{m} \subsetneqq \mathbf{m} \wedge F \subseteq \pounds$, we have $F \wedge \mathbf{m} = \pounds$. Now the assertion follows from Theorem 2.16. □

An element x of $\pounds$ is called *identity join* of a lattice $\pounds$, if there exists $1 \neq y \in \pounds$ such that $x \vee y = 1$. An element x of $\pounds$ is called *zero-divisor* of a lattice $\pounds$, if there exists $0 \neq y \in \pounds$ such that $x \wedge y = 0$. The set of all identity joins of a lattice $\pounds$ is denoted $\mathrm{I}(\pounds)$ and the set of all zero-divisors of $\pounds$ is denoted $Z(\pounds)$.

Lemma 4.2. *If* $\{1\} \neq \mathbf{p}$ *is a prime filter of* $\pounds$ *with* $(1 :_\pounds \mathbf{p}) \neq \{1\}$*, then* $\mathbf{p} \subseteq \mathrm{Id}(\pounds)$*.*

Proof. By [7, Proposition 2.2 (iv)], $\mathbf{p} = (1 :_\pounds (1 :_\pounds \mathbf{p}))$. This implies that $\mathbf{p} \subseteq \mathrm{Id}(\pounds)$. □

Following the concept of classical rings (see [13, 3]), we define classical lattices as follows:

Definition 4.3. A lattice $\pounds$ is called [*classical* if $\pounds = \mathrm{I}(\pounds) \cup Z(\pounds)$.

The following theorem shows that: when is every prime filter of $\pounds$ a Baer filter? (Compare the next theorem with Proposition 3.2 in [16]).

Theorem 4.4. *For a lattice* $\pounds$ *the following statements are equivalent:*

(1) *Every prime filter of* $\pounds$ *is a Baer filter;*

(2) *Every filter of* $\pounds$ *is a Baer filter;*

(3) *For each* $x \in \pounds$*,* $T(\{x\})$ *is a Bear filter;*

(4) *$\pounds$ is a classical lattice and for each $x, y \in \pounds$, $(1 :_{\pounds} x) \subseteq (1 :_{\pounds} y)$ implies $y \in T(\{x\})$.*

Proof. (1) $\Rightarrow$ (2). Let F be a filter of $\pounds$. Then $F = \bigcap_{F \subseteq \mathbf{p}} \mathbf{p}$ by [6, Lemma 2.6 (ii)]; hence F is a Baer filter of $\pounds$ by (1).

The implication (2) $\Rightarrow$ (3) is clear.

(3) $\Rightarrow$ (4). Let x be an arbitrary element of $\pounds$ such that $x \neq 0, 1$. If $x \notin Z(\pounds)$, then there exists a non-zero element y of $\pounds$ such that $x \wedge y \neq 0$; so $x \wedge y \neq 1$. If $T(\{x \wedge y\}) = \pounds$, then $0 = (x \wedge y) \vee s$ for some $s \in \pounds$ gives $x \wedge y = 0$, a contradiction. Thus $T(\{x \wedge y\}) \neq \pounds$. If $(1 :_{\pounds} x \wedge y) = \{1\}$, then for each $z \in \pounds$, we have $(1 :_{\pounds} x \wedge y) \subseteq (1 :_{\pounds} z)$ and hence $z \in T(\{x \wedge y\})$. Therefore, $T(\{x \wedge y\}) = \pounds$, a contradiction. Thus $(1 :_{\pounds} x \wedge y) \neq \{1\}$. Let $1 \neq a \in (1 :_{\pounds} x \wedge y)$. Then $a \vee (x \wedge y) = (a \vee x) \wedge (a \vee y) = 1$ gives $a \vee x = 1$ which implies that $x \in \mathrm{I}(\pounds)$. Thus $\pounds$ is a classical lattice. Let $x, y \in \pounds$ such that $(1 :_{\pounds} x) \subseteq (1 :_{\pounds} y)$. By assumption, $T(\{x\})$ is a Baer filter; hence $y \in T(\{x\})$.

(4) $\Rightarrow$ (1). Suppose that $\mathbf{p}$ is a prime filter of $\pounds$ and let $p \in \mathbf{p}$. We claim that $(1 :_{\pounds} p) \neq \{1\}$. Otherwise, for each $z \in \pounds$, we have $(1 :_{\pounds} p) \subseteq (1 :_{\pounds} z)$ and hence $z \in T(\{p\})$. Therefore, $T(\{p\}) = \pounds \subseteq \mathbf{p}$, a contradiction. Thus $p \in \mathrm{I}(\pounds)$ and so $\mathbf{p} \subseteq \mathrm{I}(\pounds)$. Let $(1 :_{\pounds} p) \subseteq (1 :_{\pounds} x)$ for some $p \in \mathbf{p}$ and $x \in \pounds$. By assumption, $x \in T(\{p\}) \subseteq \mathbf{p}$, as needed. $\square$

The following theorem is a lattice counterpart of Theorem 3.1 in [16] describing the structure of maximal ideals of a classical ring.

Theorem 4.5. *For a lattice $\pounds$ the following statements are equivalent:*

(1) *$\pounds$ is a classical lattice such that for every finitely generated filter $F \subseteq \mathrm{I}(\pounds)$, $(1 :_{\pounds} F) \neq \{1\}$;*

(2) *Every maximal filter of $\pounds$ is a Baer filter.*

Proof. (1) $\Rightarrow$ (2). Suppose that $\mathbf{m}$ is a maximal filter of $\pounds$. We claim that $\mathbf{m} \subseteq \mathrm{I}(\pounds)$. Assume to the contrary, that there is a $x \in \mathbf{m}$ such that $x \notin \mathrm{I}(\pounds)$. By assumption, there exists a non-zero element $y \notin \mathbf{m}$ such that $x \wedge y = 0$. Then $T(\{y\}) \wedge \mathbf{m} = \pounds$ gives $x = m \wedge (y \vee s)$ for some $m \in \mathbf{m}$ and $s \in \pounds$ which implies that $y \vee s \in \mathbf{m}$ by Lemma 1.1. Then $0 = x \wedge y = m \wedge y \wedge (y \vee s) = m \wedge (y \vee s) = x$, a contradiction. Thus $\mathbf{m} \subseteq \mathrm{I}(\pounds)$. Set

$$G = \{x \in \pounds : (1 :_{\pounds} A) \subseteq (1 :_{\pounds} x) \text{ for some finite subset } A \text{ of } \mathbf{m}\}.$$

If $x \in \mathbf{m}$, then $(1 :_{\pounds} x) \subseteq (1 :_{\pounds} x)$ gives $\mathbf{m} \subseteq G$. We claim that G is a proper Baer filter. Let $x, y \in G$ and $a \in \pounds$. Then there are two finite subsets A and B of $\mathbf{m}$ such that $(1 :_{\pounds} A) \subseteq (1 :_{\pounds} x)$ and $(1 :_{\pounds} B) \subseteq (1 :_{\pounds} y)$. Hence,

$$(1 :_{\pounds} A \wedge B) \subseteq (1 :_{\pounds} A) \cap (1 :_{\pounds} B) \subseteq (1 :_{\pounds} x) \cap (1 :_{\pounds} y) \subseteq (1 :_{\pounds} x \wedge y)$$

and $(1 :_{\pounds} A) \subseteq (1 :_{\pounds} x) \subseteq (1 :_{\pounds} x \vee a)$ gives $x \wedge y, x \vee a \in G$. Thus G is a filter of $\pounds$. Let $(1 :_{\pounds} g) \subseteq (1 :_{\pounds} z)$ for some $g \in G$ and $z \in \pounds$. By assumption, there exists a finite subset H of $\mathbf{m}$ such that $(1 :_{\pounds} H) \subseteq (1 :_{\pounds} g)$. Therefore $(1 :_{\pounds} H) \subseteq (1 :_{\pounds} g) \subseteq (1 :_{\pounds} z)$ and hence $z \in G$. So G is a Baer filter. If $y \in G$, then $\{1\} \neq (1 :_{\pounds} T(A)) \subseteq (1 :_{\pounds} A) \subseteq (1 :_{\pounds} y)$ for some finite subset A of $\mathbf{m}$ which implies that $y \in \mathrm{I}(\pounds)$ and so $G \subseteq \mathrm{I}(\pounds)$. Thus G is a proper filter and so by maximality of $\mathbf{m}$ we have $G = \mathbf{m}$ is a Baer filter.

(2) $\Rightarrow$ (1). Let $c \notin Z(\pounds)$. Then there exists a maximal filter $\mathbf{m}'$ of $\pounds$ such that $c \in T(\{c\}) \subseteq \mathbf{m}'$ by Lemma 2.1. If $m \in \mathbf{m}'$, then $(1 :_{\pounds} m) \neq \{1\}$ (otherwise, $T(\{m\}) = \pounds \subseteq \mathbf{m}'$, a contradiction since $\mathbf{m}'$ is a Baer filter) gives $\mathbf{m}' \subseteq \mathrm{I}(\pounds)$ by Lemma 4.2 and so $c \in \mathrm{I}(\pounds)$. Thus $\pounds$ is a classical lattice. Let H be a finitely generated filter of $\pounds$ such that $H \subseteq \mathrm{I}(\pounds)$. Then there is a maximal filter $\mathbf{Q}$ of $\pounds$ such that $H \subseteq \mathbf{Q}$. It follows that $(1 :_{\pounds} H) \neq \{1\}$, as $\mathbf{Q}$ is a Baer filter. This completes the proof. $\square$

Compare the next theorem with Theorem 3.2 in [16]).

Theorem 4.6. *For a lattice $\pounds$ the following statements are equivalent:*

(1) *Every prime Baer filter of $\pounds$ is either a minimal prime or a maximal filter;*

(2) *For each maximal filter $\mathbf{m}$ of $\pounds$ and each $m, n \in \mathbf{m}$, there exists a finite subset $A \subseteq (1 :_{\pounds} m)$ and $d \notin \mathbf{m}$ such that $(1 :_{\pounds} T(A \cup \{m\})) \subseteq (1 :_{\pounds} d \vee n)$.*

Proof. (1) $\Rightarrow$ (2) Assume to the contrary, that there exists a maximal filter $\mathbf{m}$ of $\pounds$ and $m, n \in \mathbf{m}$ such that $(1 :_{\pounds} T(A \cup \{m\})) \nsubseteq (1 :_{\pounds} n \vee d)$ for each $d \notin \mathbf{m}$ and each finite subset $A \subseteq (1 :_{\pounds} m)$. Set $S = \{n \vee c : c \notin \mathbf{m}\} \cup \{0\}$,

$$G = \{x \in \pounds : (1 :_{\pounds} T(A \cup \{m\})) \subseteq (1 :_{\pounds} x), \text{ where } A \subseteq (1 :_{\pounds} m) \text{ is finite}\}.$$

Let $x, y \in G$ and $a \in \pounds$. Then there are two finite subsets A and B of $(1 :_{\pounds} \mathbf{m})$ such that $(1 :_{\pounds} T(A \cup \{m\}) \subseteq (1 :_{\pounds} x)$ and $(1 :_{\pounds} T(B \cup \{m\}) \subseteq (1 :_{\pounds} y)$. Hence,

$$(1 :_{\pounds} T(A \cup B \cup \{m\}) \subseteq (1 :_{\pounds} T(A \cup \{m\}) \cap (1 :_{\pounds} T(B \cup \{m\})$$

$$\subseteq (1 :_{\pounds} x) \cap (1 :_{\pounds} y) \subseteq (1 :_{\pounds} x \wedge y)$$

and $(1 :_{\pounds} T(A \cup \{m\}) \subseteq (1 :_{\pounds} x) \subseteq (1 :_{\pounds} x \vee a)$ gives $x \wedge y, x \vee a \in G$. Thus G is a filter of $\pounds$. Let $(1 :_{\pounds} g) \subseteq (1 :_{\pounds} z)$ for some $g \in G$ and $z \in \pounds$. By assumption, there exists a finite subset C of $(1 :_{\pounds} m)$ such that $(1 :_{\pounds} T(C \cup \{m\}) \subseteq (1 :_{\pounds} g) \subseteq (1 :_{\pounds} z)$; so $z \in G$ which implies that G is a Baer filter. Clearly, S is a join closed subset of $\pounds$. If $s \in S \cap G$, then $s = n \vee t$ for some $t \notin \mathbf{m}$ and there exists a finite subset D of $(1 :_{\pounds} m)$ such that $(1 :_{\pounds} T(C \cup \{m\}) \subseteq (1 :_{\pounds} n \vee t)$ which is a contradiction. Thus $G \cap S = \emptyset$. Then there exists a $\mathbf{p} \in \min(G)$ such that $\mathbf{p} \cap S = \emptyset$ by [6, Lemma 2.6 (i)]. Moreover, by Proposition 2.12, $\mathbf{p}$ is a Baer filter. Since $(1 :_{\pounds} T(A \cup \{m\})) \subseteq (1 :_{\pounds} m)$, $m \in G \subseteq \mathbf{p}$. Then by Proposition 2.11, there exists $d \notin \mathbf{p}$ such that $m \vee d = 1$ which implies that $\{d\} \subseteq (1 :_{\pounds} m)$. On the other hand $(1 :_{\pounds} T(\{d, m\})) \subseteq (1 :_{\pounds} d)$. Thus $d \in G \subseteq \mathbf{p}$ which is a contradiction, i.e. (2) holds.

(2) $\Rightarrow$ (1). Let $\mathbf{p}$ be a prime Baer filter of $\pounds$. By Lemma 2.1, there exists a maximal filter $\mathbf{q}$ of $\pounds$ such that $\mathbf{p} \subseteq \mathbf{q}$. If $\mathbf{p} = \mathbf{q}$, then we are done. So we may assume that $\mathbf{p} \neq \mathbf{q}$. Suppose that $\mathbf{p}$ is neither maximal nor minimal prime. By Proposition 2.11, there exists $p \in \mathbf{p}$ such that $p \vee c \neq 1$ for each $c \in \pounds \setminus \mathbf{p}$. Suppose that $q \in \mathbf{q}$ such that $q \notin \mathbf{p}$. Thus $(1 :_{\pounds} p) \cap (\pounds \setminus \mathbf{p}) = \emptyset$ which implies that $(1 :_{\pounds} p) \subseteq \mathbf{p}$. Now by assumption, there exists a finite subset A of $(1 :_{\pounds} p)$ and $d \in \pounds \setminus \mathbf{q}$ such that $(1 :_{\pounds} T(A \cup \{p\})) \subseteq (1 :_{\pounds} q \vee d)$. Then $T(A \cup \{p\}) \subseteq \mathbf{p}$ and $\mathbf{p}$ is a Baer filter gives $q \vee d \in \mathbf{p}$; hence either $d \in \mathbf{p}$ or $q \in \mathbf{p}$, a contradiction, i.e. (1) holds. □

Compare the next theorem with Theorem 3.3 in [16].

Theorem 4.7. *For a lattice $\pounds$ the following statements are equivalent:*

(1) *Every prime Baer filter of $\pounds$ is a minimal prime filter;*

(2) *For each $a \in \pounds$, there exists a finitely generated filter F such that $F \subseteq (1 :_{\pounds} a)$ and $(1 :_{\pounds} T(F \cup \{a\})) = \{1\}$.*

Proof. (1) $\Rightarrow$ (2). Let $a \in \pounds$. If $(1 :_{\pounds} a) = \{1\}$, then $(1 :_{\pounds} T(\{1\} \cup \{a\})) = \{1\}$. So we may assume that $(1 :_{\pounds} a) \neq \{1\}$. Set $G = T(\{a\} \cup (1 :_{\pounds} a))$. We claim that there exists a finite subset A of G such that $(1 :_{\pounds} A) = \{1\}$. To the contrary assume that for each finite subset A of G, $(1 :_{\pounds} A) \neq \{1\}$. Set $H = \{x \in \pounds : (1 :_{\pounds} A) \subseteq (1 :_{\pounds} x)$ for some finite subset $A \subseteq G\}$.

Let $x, y \in H$ and $u \in \pounds$. So there exist two finite subsets A, B of G such that $(1 :_{\pounds} A) \subseteq (1 :_{\pounds} x)$ and $(1 :_{\pounds} B) \subseteq (1 :_{\pounds} y)$. Then

$$(1 :_{\pounds} A \wedge B) \subseteq (1 :_{\pounds} A) \cap (1 :_{\pounds} B) \subseteq (1 :_{\pounds} x) \cap (1 :_{\pounds} y) \subseteq (1 :_{\pounds} x \wedge y)$$

and $(1 :_{\pounds} A) \subseteq (1 :_{\pounds} x) \subseteq (1 :_{\pounds} x \vee u)$; hence $x \wedge y, x \vee u \in H$. Let $(1 :_{\pounds} h) \subseteq (1 :_{\pounds} z)$ for some $h \in H$ and $z \in \pounds$. Then there exists a finite subset C of G such that $(1 :_{\pounds} C) \subseteq (1 :_{\pounds} c) \subseteq (1 :_{\pounds} z)$; hence $z \in H$. Thus H is a Baer filter. Let $\mathbf{p}$ be a minimal prime filter over H. By Proposition 2.12, $\mathbf{p}$ is a Baer filter; so $\mathbf{p}$ is a minimal prime filter of $\pounds$ by (1). Since $\{a\} \subseteq G$ and $(1 :_{\pounds} a) \subseteq (1 :_{\pounds} a)$, $a \in H \subseteq \mathbf{p}$. Moreover, if $b \in (1 :_{\pounds} a)$, then $\{b\} \subseteq (1 :_{\pounds} a) \subseteq G$ and $(1 :_{\pounds} b) \subseteq (1 :_{\pounds} b)$ gives $(1 :_{\pounds} a) \subseteq \mathbf{p}$. Now by Proposition 2.11, there exists $c \in \pounds \setminus \mathbf{p}$ such that $c \vee a = 1$ which implies that $c \in (1 :_{\pounds} a) \subseteq \mathbf{p}$, a contradiction. Hence there is a finite subset $A = \{a_1, a_2, \cdots, a_k\}$ of G such that $(1 :_{\pounds} A) = \{1\}$. Assume that for each $1 \leqslant i \leqslant k$, $a \wedge b_i \leqslant a_i$ (so $a_i = (a_i \vee a) \wedge (a_i \vee b_i)$, where $b_i \in (1 :_{\pounds} a)$. Set $F = T(\{b_1, b_2, \cdots, b_k\}) \subseteq (1 :_{\pounds} a)$. It remains to show that $(1 :_{\pounds} T(F \cup \{a\})) = \{1\}$. Then for each $1 \leqslant i \leqslant k$,

$$\begin{aligned}(1 :_{\pounds} b_i) \cap (1 :_{\pounds} a) &\subseteq (1 :_{\pounds} a \vee a_i) \cap (1 :_{\pounds} a_i \vee b_i) = (1 :_{\pounds} (a_i \vee a) \wedge (a_i \vee b_i)) \\ &= (1 :_{\pounds} a_i).\end{aligned}$$

This implies that

$$\begin{aligned}(1 :_{\pounds} T(F \cup \{a\})) &\subseteq (1 :_{\pounds} F \cup \{a\}) = \cap_{i=1}^{k} (1 :_{\pounds} b_i) \cap (1 :_{\pounds} a) \subseteq \cap_{i=1}^{k} a_i \\ &= (1 :_{\pounds} A) = \{1\}.\end{aligned}$$

(2) $\Rightarrow$ (1). Let $\mathbf{p}$ be a prime Baer filter and $a \in \mathbf{p}$. By (2), there exits a finitely generated filter $F = T(A)$ of $\pounds$ such that $F \subseteq (1 :_{\pounds} a)$ and $(1 :_{\pounds} T(F \cup \{a\})) = \{1\}$, where A is a finite set. We claim that $A \cup \{a\} \nsubseteq \mathbf{p}$. Otherewise, for each $y \in \pounds$, $\{1\} = (1 :_{\pounds} A \cup \{a\}) \subseteq (1 :_{\pounds} y)$ gives $y \in \mathbf{p}$, as $\mathbf{p}$ is a Baer filter of $\pounds$, a contradiction. Hence there exists $z \in A \subseteq (1 :_{\pounds} a)$ such that $z \notin \mathbf{p}$ and $z \vee a = 1$. Therefor by Proposition 2.11, $\mathbf{p}$ is a minimal prime filter. $\square$

Acknowledgment. The author thanks referee for useful suggestion on the first draft of the manuscript.

References

[1] **A. Anebri, H. Kim and N. Mahdou**, *Baer submodules of modules over commutative rings*, Inter. Elec. J. Algebra, **34** (2023), 31 − 47.

[2] **G. Birkhoff**, *Lattice theory*, Amer. Math. Soc., 1973.

[3] **A.S. Bondarev**, *The presence of projections in quotient lineals of vector lattices*, (Russian), Dokl. Akad. Nauk SSSR **8** (1974), 5-7.

[4] **G. Călugăreanu**, *Lattice Concepts of Module Theory*, Kluwer Academic Publishers, 2000.

[5] **M.W. Evans**, On commutative P. P. rings, Pacific J. Math., **41** (1972), 687-697.

[6] **S. Ebrahimi Atani and M. Chenari**, Supplemented property in the lattices, Serdica Math. J. **46 (1)** (2020), 73-88.

[7] **S. Ebrahimi Atani and M. Sedghi Shanbeh Bazari**, *On* 2*-absorbing filters of lattices*, Discuss. Math. Gen. Algebra Appl. **36** (2016), 157-168.

[8] **S. Ebrahimi Atani and M. Sedghi Shanbeh Bazari**, Decomposable filters of lattices, Kragujevac J. Math. **43 (1)** (2019), 59-73.

[9] **G. Grätzer**, *Lattice Theory: First Concepts and Distributive Lattices*, W. H. Freeman and company, San Francisco, 1971.

[10] **G. Grätzer and F. Wehrung**, *Lattice Theory: Special Topics and Applications*, vol. 2 Springer International, 2016.

[11] **C. Jayaram**, *Baer ideals in commutative rings*, Indian. J. Pure Appl. Math., **15(8)** (1984), 855-864.

[12] **C. Jayaram, U. Tekir and S. Koc**, *On Baer modules*, Rev. Union Mat. Argentina **63(1)** (2022), 100-128.

[13] **H. Khabazian, S. Safaeeyan and M. R. Vedadi**, *Strongly duo modules and rings*, Comm. Algebra, **38** (2010), 2832-2842.

[14] **T.Y. Lam**, *Lectures on modules and rings*, Graduate Texts in Mathematics, Vol. 189, Springer-Verlag, New York, 1999.

[15] **G. Mason**, *z-Ideals and prime ideals*, J. Algebra, **26** (1973), 280-297.

[16] **S. Safaeeyan and A. Taherifar**, *d-ideals, fd-ideals and prime ideals*, Quaest. Math., **42(6)** (2019), 717-732.

[17] **T.P. Speed**, *A note on commutative Baer rings*, J. Austral. Math. Soc., **14** (1972), 257-263.

Received April 23, 2023

Department of Pure Mathematics
University of Guilan
P.O.Box 1914, Rasht, Iran
E-mail: ebrahimi@guilan.ac.ir

Quasigroups and Related Systems **32** (2024), 21 − 30
https://doi.org/10.56415/qrs.v32.02

A quasi-pseudometric on group-like Menger n-groupoids

Hamza Boujouf

Abstract. We introduce and investigate topologies on Menger n-groupoids. These topologies are defined by families of quasi-pseudometrics. We explore the relationship between the right X-closure property, continuity, and extension to an abelian binary group. Finally, we provide the necessary conditions for the topological embedding of group-like Menger n-groupoids in a locally compact binary group as an open subset.

1. Introduction and preliminaries

In the field of topological algebras, considerable attention has been devoted to the study of the properties of topological n-ary groups and n-ary semigroups. The properties of topological Menger n-groupoids have been recently explored in [2, 3, 4]. The generalization of some results is always interesting, and in this paper, we aim to extend some of the results from [1] to the case of Menger n-groupoids.

One of the generalized metric spaces is the pseudometric space introduced by Kuratowski. As the study of non-symmetric topology has gained renewed attention due to its application in various problems in applied physics, we have started utilizing quasi-pseudometric, which are another generalization of metric spaces introduced by Kelly J.C. in [11].

The question of describing families of quasi-pseudometrics that generate a topology on a Menger n-groupoid X, consistent with the n-ary operation and the operation resulting from the definition of Menger n-groupoid, is of interest. Notice that the topological Menger n-groupoid (X, g, τ) such that $g\colon X^n \to X\colon (x_1, \ldots, x_n) \mapsto g(x_1^n) = x_1$ is not uniformizable.

In this article we investigate the application of certain quasi-pseudometrics to define topologies on Menger n-groupoids, enabling the continuity of

2010 Mathematics Subject Classification: 20N15, 22A15, 22A30
Keywords: Menger n-groupoid, topological Menger n-groupoid, quasi-pseudometric

each translation within these structures and resulting in transformation into topological Menger n-groupoids. Specifically, we explore the use of invariant quasi-pseudometric families to generate topologies, examining their implications for the right X-closure property, continuity, and extension to an abelian binary group. By establishing compatibility conditions between these topologies and the n-ary operation, we emphasize the crucial contribution of invariant quasi-pseudometrics in defining and characterizing the topological properties of Menger n-groupoids. And at the end we gave the necessary conditions for the topological embeddable of group-like Menger n-groupoids in a locally compact binary group as an open set.

By a *Menger n-groupoid* (X, g) we mean the nonempty set X together with an n-ary operation $g\colon X^n \to X$ satisfying the superassociative law $g(g(x_1^n), y_1^{n-1}) = g(x_1, g(x_2, y_1^{n-1}), \ldots, g(x_n, y_1^{n-1}))$. A Menger n-groupoid (X, g) is *i-solvable* if for all $a_1^{n-1}, b \in X$, the equation $g(a_1^{k-1}, x, a_k^{n-1}) = b$, is uniquely solvable for the case $k = 1$ and $k = i + 1$. A Menger n-groupoid is called *$(1, j)$-commutative* if $g(x_1^{j-1}, x_j, x_{j+1}^n) = g(x_j, x_2^{j-1}, x_1, x_{j+1}^n)$, and *$(j, n)$-commutative* if $g(x_1^{j-1}, x_j, x_{j+1}^n) = g(x_1^{j-1}, x_n, x_{j+1}^{n-1}, x_j)$ for $x_1^n \in X$. And (X, g) is *abelian* if $g(x_1^n) = g(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$ for $x_1^n \in X$ and all permutations $\sigma \in \mathbb{S}_n$.

It should be noted (cf. [6]) that any Menger n-groupoid is isomorphic to some Menger algebra of full (n-1)-place functions. The necessary and sufficient conditions for partially commutative Menger n-groupoids to be isomorphic to Menger algebras of specific $(n-1)$-place functions are given in [7], [8] and [9]. Menger n-groupoids which are i-solvable are characterized in [5] (see also [6]).

A binary semigroup $(X, \cdot)$, where $x \cdot y = g(x, \overset{n-1}{y})$, is called a *diagonal semigroup* of a Menger n-groupoid (X, g). If a Menger n-groupoid (X, g) is i-solvable then its diagonal semigroup is a group (see [6]).

The triple (X, g, τ) is a *topological Menger n-groupoid* if g is continuous, in all variables together, in the topology τ defined on a Menger n-groupoid (X, g). Note that if the n-ay operation g is continuous on the topology τ defined on a Menger n-groupoid X, then the operation $g_{(2)}$ defined by $g_{(2)}(x_1^n, y_2^n) = g(g(x_1^n), y_2^n)$ will also be continuous in (X, τ). But the continuity of the operation $g_{(2)}$ does not always imply the continuity of g or the binary operation $\cdot$. As an example, we take the Menger 3-groupoid (X, g) such that $X =]1, +\infty)$ with the sum of the usual topology on $]1, 2] \cup [5, +\infty)$ and the discrete topology on the interval $[2, 5]$, i.e. the topology τ is defined as the set of all sets representable as unions of elements of the usual topology on $]1,2]\cup[5,+\infty)$ and of the discrete topology on $[2,5]$ (see [3]).

Algebraic properties of the Menger n-groupoid are considered in detail in the monograph [6].

2. Results

A mapping $f : X\times X\to[0,+\infty)$ is called a *quasi-pseudometric* on X if for every x,y and z from X, the following conditions hold: $f(x,x)=0$ and $f(x,y)\leqslant f(x,z)+f(z,y)$. If, in addition, $f(x,y)=f(y,x)$, then f is called a *pseudometric* (or *deviation*).

The maps $t_k : X\to X$, where $k\in N_n=\{1,2,\dots,n\}$, defined by $t_k(x)=g(a_1^{k-1},x,a_{k+1}^n)$, $a_1^n\in X$, are called the *translations*. A quasi-pseudometric on (X,g) is said to be *k-invariant*, if $f(t_k(x),t_k(y))=f(x,y)$ for all $x,y,a_1^n\in X$. If f is k-invariant for each $k\in N_n$, then f is *invariant.* Furthermore, f is *right* (resp. *left*) *invariant* if $f(t_n(x),t_n(y))=f(x,y)$ (resp. $f(t_1(x),t_1(y))=f(x,y)$), for all $x,y\in X$.

Every family Φ of quasi-pseudometrics generates a topology on X in a standard way: the sets $B_f(x,\epsilon)=\{x\in X : f(x,y)<\epsilon\}$, where $y\in X$, $f\in\Phi$, $\epsilon>0$, form a pre-base of such a topology.

Proposition 2.1. *If in a Menger n-groupoid (X,g) there are $c_1^j\in X$, $j<n$ and $i\in\{0,1,\dots,j-1\}$ such that $g(c_1^i,\overset{n-j}{x},c_{i+1}^j)=x$ for all $x\in X$, then every quasi-pseudometric f on X induces a new quasi-pseudometric $d_{a_1^k}$ defined by $d_{a_1^k}(x,y)=f(g(a_1^k,x,a_{k+1}^{n-1}),g(a_1^k,y,a_{k+1}^{n-1}))$. If f is additionally k-invariant, then $d_{a_1^k}$ is also k-invariant.*

Proof. Let f be a quasi-pseudometric on a Menger n-groupoid (X,g), and $x,y,z\in X$. Then $d_{a_1^k}(x,x)=f(g(a_1^k,x,a_{k+1}^{n-1}),g(a_1^k,x,a_{k+1}^{n-1}))=0$ and $d_{a_1^k}(x,y)=f(g(a_1^k,x,a_{k+1}^{n-1}),g(a_1^k,y,a_{k+1}^{n-1}))\leqslant f(g(a_1^k,x,a_{k+1}^{n-1}),g(a_1^k,z,a_{k+1}^{n-1}))$ $+\,f(g(a_1^k,z,a_{k+1}^{n-1}),g(a_1^k,y,a_{k+1}^{n-1}))=d_{a_1^k}(x,z)+d_{a_1^k}(z,y)$.

Thus, $d_{a_1^k}$ is a quasi-pseudometric on X. Moreover, if (X,g) satisfies the given condition and f is k-invariant. Then
$d_{a_1^k}(g(a_1^{k-1},x,a_{k+1}^n),g(a_1^{k-1},y,a_{k+1}^n))=$
$f(g(a_1^k,g(c_1^{i-1},x,c_{i+1}^n),a_{k+1}^{n-1}),g(a_1^k,g(c_1^{i-1},y,c_{i+1}^n),a_{k+1}^{n-1}))=f(g(a_1^k,x,a_{k+1}^{n-1}),$
$g(a_1^k,y,a_{k+1}^{n-1}))=d_{a_1^k}(x,y)$. Therefore, $d_{a_1^k}$ is also k-invariant. □

Proposition 2.2. *If a topological Menger n-groupoid (X,g,τ) satisfies the assumption of Proposition 2.1, then the continuity of the operation $g_{(2)}$ implies the continuity of the operation g.*

Proof. Since $g(x_1^n) = g(g(c_1^i, \overset{n-j}{x}, c_{i+1}^j), x_2^n) = g_{(2)}(c_1^i, \overset{n-j}{x}, c_{i+1}^j, x_2^n)$, the continuity of the operation $g_{(2)}$ implies the continuity of the operation g. □

Theorem 2.3. *Let Φ be a family of k-invariant quasi-pseudometrics on a Menger n-groupoid (X, g). If the topology τ_f on X, is generated by the family Φ, then (X, g, τ_f) is a topological Menger n-groupoid.*

Proof. Let $f_1, \ldots, f_m \in \Phi$, and let ϵ and $x_1^n \in X$. The collection of sets $W = \{s \in X : f_i(s, g(x_1^n)) < \epsilon, i \in N_m\}$ forms a fundamental system of neighborhoods of the point $g(x_1^n)$ in the topology τ_f induced by Φ. The set $U_k = \{h \in X : f_i(h, x_k) < \epsilon, i \in N_m\}$ is a neighborhood of a point x_k, where $k \in N_n$, in the topology τ_f on X. If $h_k \in U_k$, then for each $i \in N_m$, we obtain

$f_i(g(h_1^n), g(x_1^n)) \leqslant f_i(g(h_1^n), g(h_1^{n-1}, x_n)) + f_i(g(h_1^{n-1}, x_n), g(h_1^{n-2}, x_{n-1}, x_n))$
$+ \ldots + f_i(g(h_1^2, x_3^n), g(h_1, x_2^n)) + f_i(g(h_1, x_2^n), g(x_1^n)$
$= f_i(h_n, x_n) + f_i(h_{n-1}, x_{n-1}) + \ldots + f_i(h_2, x_2) + f_i(h_1, x_1) < n(\frac{\epsilon}{n}) = \epsilon.$

Consequently, $g(h_1^n) \in W$ and therefore the operation g is continuous in τ_f. Thus, (X, g, τ_f) is a topological Menger n-groupoid. □

Corollary 2.4. *Let Φ be a family of k-invariant quasi-pseudometrics on a Menger n-groupoid (X, g). Then all translations t_k of X are continuous in the topology τ_f on X, generated by the family Φ.*

Proof. Theorem 2.3 establishes that g on (X, τ_f) is continuous Thus each translation $x \mapsto g(a_1^{k-1}, x, a_{k+1}^n)$ of X is continuous in the topology τ_f. □

Corollary 2.5. *Let Φ be a family of k-invariant quasi-pseudometrics on a Menger n-groupoid (X, g). If the topology τ_f on X, is generated by the family Φ, then the operation $g_{(2)}$ is continuous in τ_f.*

Theorem 2.6. *If a Menger n-groupoid (X, g) with a topology τ_f generated by the family Φ of quasi-pseudometrics invariant from the right is $(1, j)$-commutative for some $j \in N_n$, then (X, g, τ_f) is a topological Menger n-groupoid.*

Proof. Let a Menger n-groupoid (X, g) be $(1, j)$-commutative. Then for any $f_1, \ldots, f_m \in \Phi$, $\epsilon > 0$, $x_1^n \in X$ the collection of sets

$$W = \{s \in X : f_i(s, g(x_1^n)) < \epsilon, i \in N_m\}$$

forms a basis for the topology τ_f induced by Φ on X. Consider the set $U_k = \{h \in X : f_i(h, x_k) < \epsilon, i \in N_m\}$, which is a neighborhood of a point

x_k, where $k \in N_n$, in the topology τ_f. If $h_k \in U_k$ for $k \in N_n$, then for each $i \in N_m$, we have:

$$\begin{aligned} f_i(g(h_1^n), g(x_1^n)) \leqslant\ & f_i(g(h_1, h_2^{n-1}, h_n), g(h_1, h_2^{n-1}, x_n)) + \\ & f_i(g(h_1, h_2^{n-1}, x_n), g(h_1, h_2^{n-2}, x_{n-1}, x_n)) + \ldots + \\ & f_i(g(h_1, h_2, x_3^n), g(h_1, x_2^n)) + f_i(g(h_1, x_2^n), g(x_1^n)) \\ =\ & f_i(g(h_n, h_2^{n-1}, h_1), g(x_n, h_2^{n-1}, h_1)) + \\ & f_i(g(h_{n-1}, h_2^{n-2}, h_1, x_n), g(x_{n-1}, h_2^{n-2}, h_1, x_n)) \\ & + \ldots + f_i(g(h_2, h_1, x_3^n), g(x_2, h_1, x_3^n)) + f_i(g(h_1, h_2^n), g(x_1^n)) \\ =\ & f_i(h_n, x_n) + f_i(h_{n-1}, x_{n-1}) + \ldots + f_i(h_2, x_2) + f_i(h_1, x_1) \\ <\ & n(\tfrac{\epsilon}{n}) = \epsilon. \end{aligned}$$

Consequently, we can conclude that $g(h_1^n) \in W$, and therefore the operation g is continuous in τ_f. Hence, (X, g, τ_f) is a topological Menger n-groupoid. □

In a similar manner, we can prove

Theorem 2.7. *If a Menger n-groupoid (X, g) with a topology τ_f generated by the family Φ of quasi-pseudometrics invariant from the left is (j, n)-commutative for some $j \in N_n$, then (X, g, τ_f) is a topological Menger n-groupoid.*

Corollary 2.8. *If an abelian Menger n-groupoid (X, g) with a topology τ_f generated by the family Φ of quasi-pseudometrics invariant either from the right or from the left, then (X, g, τ_f) is a topological Menger n-groupoid.*

Remark 2.9. Proposition 2.2 and the above theorems also are valid in the case of topologies generated by a family of pseudometrics.

Any i-solvable Menger n-groupoid is a commutative n-group derived from its diagonal group (see [5]). Then there exists a binary group $(G, \cdot)$ such that $G \supset X$ for which $A = \{a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} : a_i \in X, i \in N_{n-1}\}$ is a normal subgroup, and the quotient group of G/A is cyclic of order $n-1$ (see for example [12]). For all $y \in X$, $X = yA = Ay$, and $g(a_1^n) = a_1 \cdot a_2 \cdot \ldots \cdot a_n$, where $a_1 \cdot a_2 \cdot \ldots \cdot a_k = a_1^k$ is the product calculated in thee group $(G, \cdot)$. Such defined group $(G, \cdot)$ is called the *covering group* for (X, g).

Based on these findings, we can prove the following result.

Proposition 2.10. *Let (X, g) be i-solvable Menger n-groupoid and let f be a left invariant quasi-pseudometric on X such that for each $x, y \in X$, $f(x, y) \leqslant 1$. If f_G is an extension of f such that*

$$f_G(y^k a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}, y^k b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1}) = f(g(y, a_1^{n-1}), g(y, b_1^{n-1}))$$

if $k \in N_{n-1}$, $a_1^{n-1}, b_1^{n-1} \in X$, *and* $f_G(z,s) = 1$ *if* z *and* s *belong to different cosets, then* f_G *is a left-invariant quasi-pseudometric on* G.

Proof. Let a Megner n-groupoid (X, g) be i-solvalbe and let $(G, \cdot)$ be its covering group. It's clear that f_G is well-defined on $G \times G$, does not depend on the choice of $y \in X$, is non-negative, and it is a quasi-pseudometric on G. Moreover, if x, z belong to different cosets, then for any $t \in G$, the elements tx, tz also belong to different cosets. Then $f_G(tx, tz) = 1 = f_G(x, z)$. Now, if $x = y^k a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}$, $z = y^k b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1}$, $t = y^m c_1 \cdot c_2 \cdot \ldots \cdot c_{n-1}$, where $1 \leqslant k \leqslant n-1$, $1 \leqslant m \leqslant n-1$, $a_1^{n-1}, b_1^{n-1}, c_1^{n-1} \in X$, then $tx = y^m c_1 \cdot c_2 \cdot \ldots \cdot c_{n-1} y^k a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}$. Since $c_1 \cdot c_2 \cdot \ldots \cdot c_{n-1} y^k = y^k d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1}$, for some $d_1^{n-1} \in X$, then then $tx = y^{m+k} d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} y^k a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}$.

Similarly, we obtain $tz = y^{m+k} d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} y^k b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1}$.

Therefore,

$$\begin{aligned}
&f_G(tx, tz) = \\
&f_G(y^{m+k} d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}, y^{m+k} d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1}) = \\
&f(g(y d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}), g(y d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1})) = \\
&f(g(p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} y a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}), g(p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} y b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1})) = \\
&f(g(y a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}), g(y b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1})) = \\
&f_G(g(y^k a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}), g(y^k b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1})) = f_G(x, z),
\end{aligned}$$

where $d_1^{n-1} \in X^{n-1}$ such that $y d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} = p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} y$, with $m + k \leqslant n - 1$.

If $m + k > n - 1$, then

$$\begin{aligned}
&f_G(tx, tz) = \\
&f_G(y^{m+k-(n-1)} y^{n-1} d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}, y^{m+k-(n-1)} y^{n-1} d_1 \cdot d_2 \cdot \\
&\qquad \ldots \cdot d_{n-1} b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1}) = \\
&f(g(y^n d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}), g(y^n d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1})) = \\
&f(g(y^{n-1} \cdot g(p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} y a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1})), g(y^{n-1} \cdot g(p_1 \cdot p_2 \cdot \ldots \cdot \\
&\qquad p_{n-1} y b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1}))) = \\
&f(g(p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} y a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}), g(p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} y b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1})) \\
&\qquad = f(g(y a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}), g(y b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1})) \\
&= f_G(y^k a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}, y^k b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1}) = f_G(x, z),
\end{aligned}$$

where $d_1^{n-1} \in X$ such that $y d_1 \cdot d_2 \cdot \ldots \cdot d_{n-1} = p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} y$.
Thus, f_G is a left invariant quasi-pseudometric on G. $\square$

We will say that the family of quasi-pseudometrics Φ on a Menger n-groupoid (X, g) is *right* X*-closed*, if for all $f \in \Phi$, $a_1^{n-1} \in X$ the map

$d_{a_1^{n-1}}$ defined by $d_{a_1^{n-1}}(x,y) = f(g(x, a_1^{n-1}), g(y, a_1^{n-1}))$ for all $x, y \in X$, is a pseudo-metric on (X, g).

Theorem 2.11. *Let Φ be a right X-closed family of left-invariant quasi-pseudometrics on a Menger n-groupoid (X, g) such that for some $a \in X$, $f \in \Phi$, $k = 2, 3, \dots, n-1$, the map $d_{a,k}$ defined by*

$$d_{a,k}(x,y) = f(g(\overset{k}{a}, x, \overset{n-1-k}{a}), g(\overset{k}{a}, y, \overset{n-1-k}{a}))$$

is a quasi-pseudometric on (X, g). Then g is continuous in the topology τ generated by Φ. Moreover, if (X, g) is associative and i-solvable, then on the group $(G, \cdot)$ there exists τ_G consistent with the semigroup structure, X is an open subset of G and τ is a restriction topology on X from G.

Proof. According to Theorem 2.3 the operation g is continuous in (X, τ). If (X, g) is an associative and i-solvable Menger n-groupoid, then there exists an abelian binary group $(G, \cdot)$, such that $G \supset X$. If $\Phi_G = \{f_G\}$ is a family of quasi-pseudometrics on $(G, \cdot)$, generated by Φ, then Φ_G is right G-closed. Let's show it.

First, note that for any $f_G \in \Phi_G$, the function $\frac{f_G}{1+f_G} \in \Phi_G$ and satisfies $|\frac{f_G}{1+f_G}| \leqslant 1$. Therefore, without loss of generality, we can assume that every quasi-pseudometric $f_G \in \Phi_G$ satisfies the inequality $|f_G| \leqslant 1$. Let $x, z, t \in G$. Then $x = y^k a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}$, $z = y^l b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1}$, $t = y^m c_1 \cdot c_2 \cdot \ldots \cdot c_{n-1}$, where $1 \leqslant k \leqslant n-1$, $1 \leqslant l \leqslant n-1$, $1 \leqslant m \leqslant n-1$, $a_1^{n-1}, b_1^{n-1}, c_1^{n-1} \in X$. Thus $y \in X$.

If x, z belong to different cosets $y^k A$, then xt and zt belong to different cosets as well, and therefore $f_G(xt, zt) = 1$.

If $l = k$, then x and z belong to some coset. In this case,

$$\begin{aligned}
&f_G(xt, zt) = \\
&f_G(y^k a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} y^m c_1 \cdot c_2 \cdot \ldots \cdot c_{n-1}, y^k b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1} y^m c_1 \cdot c_2 \cdot \ldots \cdot c_{n-1}) = \\
&f_G(y^{n-m} a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} y^m c_1 \cdot c_2 \cdot \ldots \cdot c_{n-1}, y^{n-m} b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1} y^m c_1 \cdot c_2 \cdot \\
&\qquad \ldots \cdot c_{n-1}) = \\
&f(g(y^{n-m} a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} y^m c_1 \cdot c_2 \cdot \ldots \cdot c_{n-1}), g(y^{n-m} b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1} y^m c_1 \cdot \\
&\qquad c_2 \cdot \ldots \cdot c_{n-1})) = \\
&d_{c_1^{n-1}}(g(y^{n-m} a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} y^m c_1 \cdot c_2 \cdot \ldots \cdot c_{n-1}), g(y^{n-m} b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1} y^m c_1 \cdot \\
&\qquad c_2 \cdot \ldots \cdot c_{n-1})) = \\
&(d_{c_1^{n-1}})_{y^{n-m-1}}(g(y a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}), g(y b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1})) = \\
&((d_{c_1^{n-1}})_{y^{n-m-1}})_G(y^k a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1}, y^k b_1 \cdot b_2 \cdot \ldots \cdot b_{n-1}) = ((d_{c_1^{n-1}})_{y^{n-m-1}})_G(x, z),
\end{aligned}$$

which belongs to Φ_G since $(d_{c_1^{n-1}})_{y^{n-m-1}} \in \Phi$. Hence, Φ_G is right G-closed.

Since f_G is an extension of the quasi-pseudometric f, the topology τ_G on $(G, \cdot)$, generated by the family Φ_G induces a topology on X that coincides with the topology generated by the family Φ.

Since $f_G(x, z) = 1$ when x and z belong to different cosets $y^k A$ for $1 \leqslant k \leqslant n-1$, each $y^k A$ is an open subset of G, and in particular, X is an open subset of G.

The continuity of the multiplication follows from the Theorem 2.3 by considering $n = 2$ and $k \in \{1, 2\}$. Therefore, $(G, \cdot, \tau_G)$ is a topological semigroup. □

We say that a Menger n-groupoid (X, g) is *weakly left* (respectively, *right*)*-invertible* if for all elements $a, b \in X$ there exist $c_1^{n-2} \in X$ such that $g(c_1^{n-2}, a, X) \cap g(c_1^{n-2}, b, X) \neq \emptyset$ (respectively, $g(X, a, c_1^{n-2}) \cap g(X, b, c_1^{n-2}) \neq \emptyset$).

Theorem 2.12. *An associative i-solvable Menger n-groupoid* (X, g) *with a locally compact topology* τ *is a topological semigroup if all translations are injective, open, and continuous. Additionally, if* (X, g) *is weakly left* (*or weakly right*)*-invertible, then* (X, g, τ) *is topologically embeddable in a locally compact binary group as an open set.*

Proof. Let (X, g) be an associative i-solvable Menger n-groupoid. Then it is a commutative Menger n-group derived from its diagonal group $(X, \cdot\,)$ (cf. [5]). Let τ be a locally compact topology on X such that the translations are injective, open, and continuous. Then, by Ellis's theorem [10], the binary operation is continuous, and sequentially, g is continuous. Therefore, we can conclude that $(X, \cdot\,, \tau)$ is a topological semigroup, and in particular (X, g, τ) is a topological group.

Now, consider a weakly right-invertible Menger n-groupoid (X, g). Therefore, for any elements $a, b \in X$, and for certain sequence $c_1^{n-2} \in X$ the relation $g(X, a, c_1^{n-2}) \cap g(X, b, c_1^{n-2}) \neq \emptyset$ holds. Thus, for some $x, y \in X$, we have $g(x, a, c_1^{n-2}) = g(y, a, c_1^{n-2})$. Consequently, $xac_1^{n-2} = xac_1^{n-2}$ in $(G, \cdot)$. Invoking the injectivity of the translations of X we obtain $xa = yb$ or $Xa \cap Xb \neq \emptyset$. Hence, by [14], (X, g, τ) is topologically embeddable in a locally compact binary group as an open set. □

This theorem can be considered an extension of Ellis's theorem in [10] to the case of Menger n-groupoids with locally compact topologies.

Corollary 2.13. *Let (X, g) be an associative, weakly left (or weakly right)-invertible Menger n-quasigroup with a locally compact topology τ is topologically embeddable in a locally compact binary group as an open set if all translations are injective, open, and continuous in τ.*

Theorem 2.14. *An associative i-solvable Menger n-groupoid (X, g) with a locally compact topology τ is a topological semigroup if all translations are injective, open, and the operation $g_{(2)}$ is continuous. Additionally, if for every $x, y \in X$ and for every neighborhood V of point x there exists a neighborhood V' of point y such that $g(x, \overset{n-1}{y}) \in \bigcap_{y' \in V'} g(V, \overset{n-1}{y'})$. Then (X, g, τ) is topologically embeddable in a locally compact binary group as an open set.*

Proof. Let (X, g) be an associative i-solvable Menger n-groupoid. Again, from [5], it follows that (X, g) is a commutative Menger n-group derived from its diagonal group $(X, \cdot)$. Let τ be a locally compact topology on X such that the translations are injective, open, and $g_{(2)}$ is continuous. Then g is continuous, and according again to Ellis's theorem the binary operation is also continuous. Therefore, we can conclude that $(X, \cdot, \tau)$ is a topological semigroup, and in particular, (X, g, τ) is topological group.

If for every $x, y \in X$ and for every neighborhood V of point x there exists a neighborhood V' of point y such that $g(x, \overset{n-1}{y}) \in \bigcap_{y' \in V'} g(V, \overset{n-1}{y'})$. Then $xy = g(x, \overset{n-1}{y}) \in \bigcap_{y' \in V'} g(V, \overset{n-1}{y'}) = \bigcap_{y' \in V'} V \cdot y'$. As the diagonal-topological semigroup $(X, \cdot, \tau)$ is commutative, then $yx = g(x, \overset{n-1}{y}) \in \bigcap_{y' \in V'} y' \cdot V$. Consequently, $(X, \cdot, \tau)$ verifies the condition F of [13]. Thus, (X, g, τ) is topologically embeddable in a locally compact binary group as an open set. □

Corollary 2.15. *An associative Menger n-group (X, g) with a locally compact topology τ is topologically embeddable in a locally compact binary group as an open set if all translations are injective, open, the operation $g_{(2)}$ is continuous, and the following condition is satisfied: For every $x, y \in X$ and for every neighborhood V of point x there exists a neighborhood V' of point y such that $g(x, \overset{n-1}{y}) \in \bigcap_{y' \in V'} g(V, \overset{n-1}{y'})$.*

References

[1] **H.Boujouf**, *The topology of n-ary semigroups defined by the deflection systems*, (Russian), **10** (1997), Voprosy Algebry, $187-189$.

[2] **H. Boujouf**, *The pseudometric in the Menger n-groupoids*, J. Sebha Univ., Pure and Appl. Sci., **9** (2010), no. 1, $5-10$.

[3] **H. Boujouf**, *On the embedding Menger n-groupoids in n-ary topological groups*, J. Sebha Univ., Pure ans Appl. Sci., **12** (2013), no. 2, $108-113$.

[4] **H. Boujouf**, *On topological Menger n-groupoids*, Quasigroups and Related Systems, **31** (2023), $201-206$.

[5] **W.A. Dudek**, *On group-like Menger n-groupoids*, Radovi Matematićki, **2** (1986), $81-98$.

[6] **W.A. Dudek and V.S. Trokhimenko**, *Algebra of multiplace functions*, Walter de Gruyter GmbH Co.KG, Berlin/Boston, (2012).

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

[8] **W.A. Dudek and V.S. Trokhimenko**, *On σ-commutativity in Menger algebras of n-place functions*, Comm. Algebra. **45** (2017), $4557-4568$.

[9] **W.A. Dudek and V.S. Trokhimenko**, *Menger algebras of k-commutative n-place functions*, Georgian Math. J.. **28** (2021), $355-361$.

[10] **R. Ellis**, *Locally compact transformation groups*, Duke Math. J., **24** (1957), $119-125$.

[11] **J.C. Kelly**, *Bitopological spaces*, Proc. London Math. Soc., **13** (1963), no. 3, $71-89$.

[12] **S.A. Rusakov**, *Algebraic n-ary systems*, (Russian), Izd. Nauka, Minsk, (1992).

[13] **L.B. Šneperman**, *The imbedding of topological semigroups in topological groups*, (Russian), Mat. Zametki, **6** (1969), $401-409$.

[14] **N.A. Tserpes, A. Mukherjea**, *A note on the embedding of topological semigroups*, Semigroup Forum, **2**, (1971), 71-75.

Received December 15, 2023

Sebha University, Departement of Mathematics at Faculty of Science
P.O.Box:18758
Sebha, Libya
E-mail: hamzaan14@gmail.com

Quasigroups and Related Systems **32** (2024), 31 − 39

https://doi.org/10.56415/qrs.v32.03

On groups with the same type as large Ree groups

Ashraf Daneshkhah, Fatemeh Moameri and Hosein Parvizi Mosaed

Abstract. Let G be a finite group and $\mathsf{nse}(G)$ be the set of the number of elements with the same order in G. In this article, we prove that the large Ree groups ${}^2\mathrm{F}_4(q)$ with an odd order component prime are uniquely determined by $\mathsf{nse}({}^2\mathrm{F}_4(q))$ and their order. As an immediate consequence, we verify Thompson's problem (1987) for the large Ree groups ${}^2\mathrm{F}_4(q)$ with an odd order component prime.

1. Introduction

In 1987, J. G. Thompson possed a problem which is related to algebraic number fields [15, Problem 12.37]:

For a finite group G and natural number n, set $G(n) = \{x \in G \mid x^n = 1\}$ and define the type of G to be the function whose value at n is the order of $G(n)$. Is it true that a group is solvable if its type is the same as that of a solvable one?

This problem links to the set $\mathsf{nse}(G)$ of *the number of elements of the same order* in G. Indeed, it turns out that if two groups G and H are of the same type, then $\mathsf{nse}(G) = \mathsf{nse}(H)$ and $|G| = |H|$. Therefore, if a group G has been uniquely determined by its order and $\mathsf{nse}(G)$, then Thompson's problem is true for G. One may ask this problem for non-solvable groups, in particular, finite simple groups. In this direction, Shao et al [17] studied finite simple groups whose order is divisible by at most four primes. Following this investigation, such problem has been studied for some other families of simple groups including Suzuki groups $\mathrm{Sz}(q)$, small Ree groups ${}^2\mathrm{G}_2(q)$ and Chevalley groups $\mathrm{F}_4(q)$ with $q = 2^{4n} + 1$ prime [2, 3, 6], see also [4, 7, 8, 10, 12, 16]. In this paper, we study this problem for the large Ree groups ${}^2\mathrm{F}_4(q)$, and prove that

2010 Mathematics Subject Classification: Primary 20D60; Secondary 20D06

Keywords: Ree groups, order element, order of group, prime graph

Theorem 1.1. *Let G be a group with $\mathsf{nse}(G) = \mathsf{nse}({}^2\mathrm{F}_4(q))$ and $|G| = |{}^2\mathrm{F}_4(q)|$, where $q = 2^{2m+1}$ and $q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$ or $q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1$ is prime. Then $G \cong {}^2\mathrm{F}_4(q)$.*

As noted above, as an immediate consequence of Theorem 1.1, we have

Corollary 1.2. *If G is a group with the same type as ${}^2\mathrm{F}_4(q)$, where $q = 2^{2m+1}$ and $q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$ or $q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1$ is prime, then G is isomorphic to ${}^2\mathrm{F}_2(q)$.*

Finally, we give some brief comments on the notation used in this paper. Throughout this article all groups are finite. We denote a Sylow p-subgroup of G by G_p. We also use $\mathsf{n}_p(G)$ to denote the number of Sylow p-subgroups of G. For a positive integer n, the set of prime divisors of n is denoted by $\pi(n)$, and we set $\pi(G) := \pi(|G|)$, where $|G|$ is the order of G. We denote the set of element orders of G by $\omega(G)$ known as *spectrum* of G. For $i \in \omega(G)$, we denote the number of elements of order i in G by $\mathsf{m}_i(G)$ and the set of the number of elements with the same order in G by $\mathsf{nse}(G)$. In other words, $\mathsf{nse}(G) = \{\mathsf{m}_i(G) \mid i \in \omega(G)\}$. The *prime graph* $\Gamma(G)$ of a finite group G is a graph whose vertex set is $\pi(G)$, and two distinct vertices u and v are adjacent if and only if $uv \in \omega(G)$. Assume further that $\Gamma(G)$ has $t(G)$ connected components $\pi_i(G)$, for $i = 1, 2, \ldots, t(G)$. The positive integers n_i with $\pi(\mathsf{n}_i) = \pi_i(G)$ are called order components of G. In the case where G is of even order, we always assume that $2 \in \pi_1$, and π_1 is said to be the even component of G. In this way, π_i and n_i are called odd components and odd order components of G, respectively. Recall that $\mathsf{nse}(G)$ is the set of the number of elements in G with the same order. In other word, $\mathsf{nse}(G)$ consists of the numbers $\mathsf{m}_i(G)$ of elements of order i in G, for $i \in \omega(G)$. Here, φ is the *Euler totient* function.

2. Preliminaries

In this section, we state some useful lemmas which will be used in the proof of the main theorem.

Lemma 2.1. [14, Main Theorem] *The maximal subgroups of ${}^2\mathrm{F}_4(q)$ with $q = 2^{2m+1} \geqslant 8$ are conjugate to one of the subgroups listed in* Table 1.

Lemma 2.2. [5, Theorem 1] and [9, Theorem 2.7.6] *Let G be a Frobenius group of even order with kernel K and complement H. Then $t(G) = 2$,* *and $\pi(H)$ and $\pi(K)$ are vertex sets of the connected components of $\Gamma(G)$. Moreover, K is nilpotent and $|H|$ divides $|K|-1$.*

Table 1: The maximal subgroups of ${}^2\mathrm{F}_4(q)$ with $q = 2^{2m+1} \geqslant 8$.

Maximal subgroup	Conditions
$[q^{11}] : \mathrm{GL}_2(q)$	
$[q^{10}] : (\mathrm{Sz}(q) \times \mathbb{Z}_{q-1})$	
$\mathrm{SU}_3(q(), no.2,$	
$(\mathbb{Z}_{q+1} \times \mathbb{Z}_{q+1}) : \mathrm{GL}_2(3)$	
$(\mathbb{Z}_{q-\sqrt{2q}+1} \times \mathbb{Z}_{q-\sqrt{2q}+1}) : 4\mathrm{S}_4$	$q > 8$
$(\mathbb{Z}_{q+\sqrt{2q}+1} \times \mathbb{Z}_{q+\sqrt{2q}+1}) : 4\mathrm{S}_4$	
$\mathbb{Z}_{q^2-\sqrt{2q^3}+q-\sqrt{2q}+1} : 12$	
$\mathbb{Z}_{q^2+\sqrt{2q^3}+q+\sqrt{2q}+1} : 12$	
$\mathrm{PGU}_3(q) : 2$	
$\mathrm{Sz}(q) \wr 2$	
$\mathrm{Sp}_4(q) : 2$	
${}^2\mathrm{F}_4(q_0)$	$q = q_0^r$ with r prime

A group G is a 2-Frobenius group if there exists a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that G/H and K are Frobenius groups with kernels K/H and H, respectively.

Lemma 2.3. [5, Theorem 2] *Let G be a 2-Frobenius group of even order. Then $t(G) = 2$, $\pi_1(G) = \pi(G/K) \cup \pi(H)$ and $\pi_2(G) = \pi(K/H)$. Moreover, G/K and K/H are cyclic groups, and $|G/K|$ divides $|Aut(K/H)|$.*

Lemma 2.4. [11, Theorem 9.1.2] *Let G be a finite group, and let n be a positive integer dividing $|G|$. If $G(n) = \{g \in G \mid g^n = 1\}$, then $n \mid |G(n)|$.*

Lemma 2.5. *Let G be a finite group, and let $i \in \omega(G)$. Then $\mathsf{m}_i(G) = k\varphi(i)$, where k is the number of cyclic subgroups of order i in G. Moreover, $\varphi(i)$ divides $\mathsf{m}_i(G)$, and i divides $\sum_{j|i} \mathsf{m}_j(G)$. In particular, if $i > 2$, then $\mathsf{m}_i(G)$ is even.*

Proof. The proof is straightforward by Lemma 2.4. $\square$

Lemma 2.6. [1, Lemma 3.1] *The order of ${}^2\mathrm{F}_4(q)$ with $q = 2^{2m+1} \geqslant 8$ is coprime to 17.*

3. Proof of the main result

Let $q = 2^{2m+1} \geqslant 8$, and let p be a prime number. Suppose that p is $q^2+\sqrt{2q^3}+q+\sqrt{2q}+1$ or $q^2-\sqrt{2q^3}+q-\sqrt{2q}+1$, and set $F := {}^2\mathrm{F}_4(q)$. Let G be a finite group with $\mathsf{nse}(G) = \mathsf{nse}(F)$ and $|G| = |F|$. We note that ${}^2\mathrm{F}_4(q)$ with $q = 2^{2m+1} \geqslant 8$ is of order $q^{12}(q-1)(q^2+1)(q^3+1)(q^4-1)\cdot f_+(q)\cdot f_-(q)$, where

$$f_\epsilon(q) = q^2 + \epsilon\sqrt{2q^3} + q + \epsilon\sqrt{2q} + 1, \tag{3.1}$$

with $\epsilon = \pm$. We observe by [18] that the simple group ${}^2\mathrm{F}_4(q)$ with $q = 2^{2m+1} \geqslant 8$ has two odd order components, namely, $f_+(q)$ and $f_-(q)$.

Lemma 3.1. *Let $F := {}^2\mathrm{F}_4(q)$ with $q = 2^{2m+1} \geqslant 8$, and let $f_\epsilon(q)$ be as in (3.1). If $p = f_\epsilon(q)$ is prime, then*

(a) $\mathsf{m}_p(F) = (p-1)|F|/(12p)$;

(b) $p \mid \mathsf{m}_i(F)$ *for every* $i \in \omega(F) \setminus \{1, p\}$.

Proof. By Lemma 2.1, F_p is a cyclic group of order p, and so $\mathsf{m}_p(F) = \varphi(p)\mathsf{n}_p(F) = (p-1)\mathsf{n}_p(F)$. According to Lemma 2.1, $|\mathbf{N}_F(\mathrm{F}_p)| = 12p$, and so $\mathsf{n}_p(F) = |F|/12p$. If $i \in \omega(F) \setminus \{1, p\}$, then [13] implies that p is an isolated vertex of $\Gamma(F)$, and so $p \nmid i$ and $pi \notin \omega(F)$. Thus F_p acts fixed point freely on the set of elements of order i in G by conjugation, and hence $|\mathrm{F}_p| \mid \mathsf{m}_i(F)$. Therefore, $p \mid \mathsf{m}_i(F)$. □

Lemma 3.2. *Let $F := {}^2\mathrm{F}_4(q)$, and let G be a group such that $|G| = |F|$ and $\mathsf{nse}(G) = \mathsf{nse}(F)$. Let also p be $f_\epsilon(q)$ defined as in (3.1). If p is prime, then*

(a) $\mathsf{m}_2(G) = \mathsf{m}_2(F)$;

(b) $\mathsf{m}_p(G) = \mathsf{m}_p(F)$;

(c) $\mathsf{n}_p(G) = \mathsf{n}_p(F)$;

(d) *p is an isolated vertex of* $\Gamma(G)$;

(e) $p \mid \mathsf{m}_i(G)$ *for every* $i \in \omega(G) \setminus \{1, p\}$.

Proof. According to Lemma 2.5, for any $i \in \omega(G)$, $i > 2$ if and only if $\mathsf{m}_i(G)$ is even. So $\mathsf{m}_2(G) = \mathsf{m}_2(F)$. By Lemma 2.5, $(\mathsf{m}_p(G), p) = 1$, and so $p \nmid \mathsf{m}_p(G)$. Then by Lemma 3.1, $\mathsf{m}_p(G) \in \{\mathsf{m}_1(F), \mathsf{m}_p(F)\}$, and since

$\mathsf{m}_p(G)$ is even, we deduce that $\mathsf{m}_p(G) = \mathsf{m}_p(F)$. Since G_p and F_p are cyclic groups of order p, it follows that $\mathsf{m}_p(G) = \varphi(p)\mathsf{n}_p(G) = \varphi(p)\mathsf{n}_p(F) = \mathsf{m}_p(F)$. So $\mathsf{n}_p(G) = \mathsf{n}_p(F)$. If p is not an isolated vertex of $\Gamma(G)$, then there exists $r \in \pi(G) - \{p\}$ such that $pr \in \omega(G)$. Thus $\mathsf{m}_{pr}(G) = \varphi(pr)\mathsf{n}_p(G)k$, where k is the number of the cyclic subgroups of order r in $\mathbf{C}_G(G_p)$. Since $\mathsf{n}_p(G) = \mathsf{n}_p(F) = |F|/(12p)$ and $|F| = |G|$, we conclude that $\mathsf{n}_p(G) = |G|/(12p)$. Thus $(p-1)(r-1)|G|/(12p)$ divides $\mathsf{m}_{pr}(G)$. On the other hands, by Lemma 3.1, p is a divisor of $\mathsf{m}_{pr}(G)$. Then $p(p-1)(r-1)|G|/12p$ divides $\mathsf{m}_{pr}(G) < |G|$, and this implies that $r = 2$ and $p < 13$, which is a contradiction. Hence p is an isolated vertex of $\Gamma(G)$. $\square$

Proof of Theorem 1.1. We first prove that the group G is neither a Frobenius group, nor a 2-Frobenius group. Assume to the contrary that G is a Frobenius group or a 2-Frobenius group. If G is a Frobenius group with kernel K and complement H. Then Lemma 2.2 implies that $t(G) = 2, \pi(H)$ and $\pi(K)$ are vertex sets of the connected components of $\Gamma(G)$. Since p is an isolated vertex of $\Gamma(G)$, we deduce that $|K| = p$ and $|H| = |F|/p$, or $|H| = p$ and $|K| = |F|/p$. By Lemma 2.2, $|F|/f_\epsilon(q)$ divides $f_\epsilon(q)-1$ or $f_\epsilon(q)$ divides $[|F|/f_\epsilon(q)]-1$. This implies that $p \mid 11$, which is a contradiction. If G is a 2-Frobenius group, then Lemma 2.3 implies that $t(G) = 2$ and G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that G/H and K are Frobenius groups with kernels K/H and H, respectively, $\pi_1(G) = \pi(G/K) \cup \pi(H)$, $\pi_2(G) = \pi(K/H)$ and $|G/K|$ divides $|\mathrm{Aut}(K/H)|$. Since p is an isolated vertex of $\Gamma(G)$, we deduce that $|K/H| = f_\epsilon(q)$ and $|H| = q^{12}(q-1)(q^2+1)(q^4-1)(q^3+1)\mathrm{F}_{-\epsilon}(q)/|G/K|$. Since $|G/K|$ divides $|\mathrm{Aut}(K/H)|$, we deduce that $|G/K|$ divides $p-1$. On the other hand, since K is a Frobenius group with kernel H, Lemma 2.2 implies that p divides $[q^{12}(q-1)(q^2+1)(q^4-1)(q^3+1)\mathrm{F}_{-\epsilon}(q)/|G/K|]-1$, and hence p divides $12 - |G/K|$, which is a contradiction.

Therefore, G is neither a Frobenius group, nor a 2-Frobenius group, and hence by [18, Theorem A], G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that H and G/K are π_1-groups, K/H is a non-abelian simple group, H is a nilpotent group and $|G/K|$ divides $|\mathrm{Out}(K/H)|$. Moreover, any odd component of G is also an odd component of K/H. Since p is an isolated vertex of $\Gamma(G)$, we deduce that $p \mid |K/H|$ and $t(K/H) \geq 2$. The connected components of the simple group K/H can be read off from [13, 18], and in what follows we discuss all these possibilities. For convenience, we use Lie notation for the finite simple groups of Lie type.

Let K/H be a sporadic simple group or one of the simple groups $\mathrm{A}_2(2)$,

$\mathrm{A}_2(4)$, ${}^2\mathrm{A}_3(2)$, ${}^2\mathrm{A}_5(2)$, $\mathrm{E}_7(2)$, $\mathrm{E}_7(3)$, ${}^2\mathrm{E}_6(2)$ and ${}^2\mathrm{F}_4(2)'$. Then $f_\epsilon(q)$ is equal to one of the prime numbers 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 59, 67, 71, 73, 127, 757 and 1093. This is possible only for $q = 8$ when $\mathrm{F}_-(q) = 37$ and K/H is isomorphic to J_4 or Ly in which case $|K/H|$ does not divide $|G|$.

Let now K/H be an alternating group of degree n. Then since by Lemma 2.6, $17 \notin \pi(G)$, it follows that $n < 17$, and this violates the choice of p which is at least 37.

Let K/H be a finite simple classical group over a finite field of size q'. Then we easily observe by Lemma 2.6 that $17 \nmid q'$. Moreover, if $q'^{16} - 1$ is a divisor of $|K/H|$, then by the Fermat's little theorem, $q'^{16} - 1 \equiv 0 \pmod{17}$, and so $17 \mid |K/H|$ which violates Lemma 2.6. Therefore, we have one of the following possibilities:

K/H	Condition
$\mathrm{A}_n(q')$	$1 \leqslant n \leqslant 16$
${}^2\mathrm{A}_n(q')$	$1 \leqslant n \leqslant 16$
$\mathrm{C}_n(q')$	$2 \leqslant n \leqslant 7$
$\mathrm{B}_n(q')$	$2 \leqslant n \leqslant 7$, q' odd
$\mathrm{D}_n(q')$	$3 \leqslant n \leqslant 8$
${}^2\mathrm{D}_n(q')$	$2 \leqslant n \leqslant 8$

Suppose that K/H is isomorphic to $\mathrm{A}_n(q')$. If $n = 1$, then p is q', $(q' \pm 1)$ or $(q' \pm 1)/2$, and so $p \mp 1$ or $2p \mp 1$ divides $|K/H|$, so does $|G|$, which is a contradiction. If $2 \leqslant n \leqslant 16$ and $(n, q') \neq (2, 2), (2, 4)$, then $n = p'$ or $p' - 1$, and so p is $(q'^{p'} - 1)/[(q' - 1)(p', q' - 1)]$ or $(q'^{p'} - 1)/(q' - 1)$. Therefore, $(p', q' - 1)p - 1$ or $p - 1$ divides $|K/H|$, respectively. But none of these is a divisor of $|G|$, which is a contradiction.

Suppose that K/H is isomorphic to ${}^2\mathrm{A}_n(q')$ for $n = p', p' - 1$ with $(n, q') \neq (3, 2), (5, 2)$. Then p is $(q'^{p'} + 1)/[(q' + 1)(p', q' + 1)]$ or $(q'^{p'} + 1)/(q' + 1)$, which is impossible as neither $(p', q' - 1)p - 1$, nor $p - 1$ divides $|G|$.

Suppose that K/H is isomorphic to $\mathrm{B}_n(q')$ or $\mathrm{C}_n(q')$. Then p is $(q'^n \pm 1)/(2, q' - 1)$, and so $(2, q' - 1)p \mp 1$ has to divide $|G|$, which is a contradiction.

Suppose that K/H is isomorphic to $\mathrm{D}_n(q')$ with $n = p', p' + 1$ and $q' = 2, 3, 4$. Then p is $(q'^{p'} - 1)/(4, q' - 1)$, and so $(4, q' - 1)p + 1$ has to divide $|G|$, which is a contradiction.

Suppose that K/H is isomorphic to ${}^2\mathrm{D}_n(q')$. Then p is $(q'^{p'}+1)/(2,q'-1)$, $2^{n'-1}+1$, $2^{n'}+1$, $(3^n+1)/4$ or $(3^{n-1}+1)/2$. $(2,q'-1)p-1$, $p-1$, $p+1$, $2p-1$, $4p-1$ has to divide $|G|$, which is a contradiction.

If K/H is isomorphic to $G_2(q')$, $\mathrm{F}_4(q')$, $\mathrm{E}_6(q')$, ${}^2\mathrm{E}_6(q')$ or ${}^3\mathrm{D}_4(q')$, then p is $q'^2 \pm q' + 1$, $q'^4 - q'^2 + 1$ or $q'^4 + 1$, $q'^6 + q'^3 + 1$ or $(q'^6 + q'^3 + 1)/3$, $(q'^6 \pm q'^3 + 1)/(3, q \mp 1)$ or $q'^4 - q'^2 + 1$. So $p-1$ or $3p-1$ is a divisor of $|G|$, which is a contradiction.

Suppose that K/H is isomorphic to $\mathrm{E}_8(q')$. Then p is ${q'}^8 \pm {q'}^7 \mp {q'}^5 - {q'}^4 \mp {q'}^3 \pm q' + 1$, ${q'}^8 - {q'}^4 + 1$ or ${q'}^8 - {q'}^6 + {q'}^4 - {q'}^2 + 1$. If p is ${q'}^8 - {q'}^4 + 1$ or ${q'}^8 - {q'}^6 + {q'}^4 - {q'}^2 + 1$, then $p-1$ divides $|G|$, which is impossible. If $p = {q'}^8 \pm {q'}^7 \mp {q'}^5 - {q'}^4 \mp {q'}^3 \pm q' + 1$, then $2^{m+1}(2^m \pm 1)(2^{2m+1}+1) = q'({q'}^7 \pm {q'}^6 \mp {q'}^4 - {q'}^3 \mp {q'}^2 \pm 1)$, so we have three possibilities:

(1) $(q', 2^{m+1}) \neq 1$. Since $(2^{m+1}, 2^m \pm 1) = (2^{m+1}, 2^{2m+1}+1) = 1$, we have $q' = 2^{m+1}$. This implies that ${q'}^{120} \mid |K/H|$ so does $|G|$, which is a contradiction.

(2) $(q', 2^{2m+1}+1) \neq 1$. If $3 \nmid q'$, then $q' \mid 2^{2m+1}+1 = q+1$ and ${q'}^2 \nmid q+1$ because $(2^{2m+1}+1, 2^m \pm 1) = 1$ or 3. This also requires ${q'}^{120} \mid |G|$, which is a contradiction. If $3 \mid q'$, then $q' = 3^{m'}$ for some positive integer m'. If $(q', 2^{2m+1}+1) > 3$, then $3^{m'-1} \mid 2^{2m+1}+1 = q+1$ but $3^{m'+1} \nmid q+1$. Hence ${q'}^{120} \mid |G|$, which is impossible. We note that the case where $q' = 3$ and $(q', 2^{2m+1}+1) = 3$ cannot occur as $p = q^2 \pm \sqrt{2q^3} + q \pm \sqrt{2q} + 1$ is a prime number and $q = 2^{2m+1} > 2$. If $q' = 3^{m'} > 3$ and $(q', 2^{2m+1}+1) = 3$, then $3^{m'-1} \mid 2^m \pm 1$ but $3^{m'+1} \nmid 2^m \pm 1$. Since $|K/H| \mid |G|$ we have $q'^{120} \mid |G|$, which is a contradiction.

(3) $(q', 2^m \pm 1) \neq 1$. This case can be ruled out by the same manner as in case (2).

Suppose that K/H is isomorphic to ${}^2\mathrm{B}_2(q')$ with $q' = 2^{2m'+1}$. Then $p = q' - 1$ or $q' \pm \sqrt{2q'} + 1$. If $p = q' - 1$, then $2^{2m'+1} - 2 = 2^{m+1}(2^m \pm 1)(2^{2m+1}+1)$, and so $m = 0$, which is a contradiction. If $p = q' \pm \sqrt{2q'} + 1$, then $2^{m'+1}(2^{m'} \pm 1) = 2^{m+1}(2^m \pm 1)(2^{2m+1}+1)$ implying that $m = m'$, which is a contradiction.

Suppose that K/H is isomorphic to ${}^2G_2(q')$ with $q' = 3^{2m'+1}$. Then $p = q' \pm \sqrt{3q'} + 1$, and so $3^{m'+1}(3^{m'} \pm 1) = 2^{m+1}(2^m \mp 1)(2^{2m+1}+1)$. Therefore $2^{m+1} \mid 3^{m'} \pm 1$. Note that $(2^m \mp 1, 2^{2m+1}+1) = 1$ or 3. If $3^{m'} \mid 2^m \mp 1$, then $m = m' = 1$, which is impossible. If $3^{m'} \mid 2^{2m+1}+1$, then $q' \mid (q+1)^2$ but $q'^2 \nmid (q+1)^2$. Since $q'^3 \mid |K/H|$, we have $q'^3 \mid |G|$, which is a contradiction.

Therefore, K/H is isomorphic to ${}^2\mathrm{F}_4(q')$, and hence $q' = q$. This forces $H = 1$, and hence $G = K \cong {}^2\mathrm{F}_4(q)$, as claimed. □

References

[1] **Z. Akhlaghi, M. Khatami, and B. Khosravi**, *Quasirecognition by prime graph of the simple group* ${}^2F_4(q)$, Acta Math. Hungar., **122** (2009), 387 – 397.

[2] **S.H. Alavi, A. Daneshkhah, and H. Parvizi Mosaed**, *On quantitative structure of small Ree groups*, Comm. Algebra, **45** (2017), 4099 – 4108.

[3] **S.H. Alavi, A. Daneshkhah, and H. Parvizi Mosaed**, *Finite groups of the same type as Suzuki groups*, Int. J. Group Theory, **8** (2019), 35 – 42.

[4] **A.K. Asboei, S.S.S. Amiri, A. Iranmanesh, and A. Tehranian**, *A characterization of sporadic simple groups by nse and order*, J. Algebra Appl., **12** (2013), no. 23, Id/No 1250158.

[5] **G. Chen**, *On structure of Frobenius and* 2*-Frobenius group*, J. Southwest China Normal Univ., **20** (1995), 485 – 487.

[6] **A. Daneshkhah, F. Moameri, and H. Parvizi Mosaed**, *On finite groups with the same order type as chevalley groups* $F_4(q)$ *with* q *even*, Bull. Korean Math. Soc., **58** (2021), 1031 – 1038.

[7] **B. Ebrahimzadeh and A. Iranmanesh**, *A new characterization of projective special unitary groups* $U_3(3^n)$ *by the order of group and the number of elements with the same order*, Algebr. Struct. Appl., **9** (2022), 113 – 120.

[8] **B. Ebrahimzadeh, A. Iranmanesh, and M. H. Parvizi**, *A new characterization of Ree group* ${}^2G_2(q)$ *by the order of group and the number of elements with the same order*, Int. J. Group Theory, **6** (2017), no. 4, 1 – 6.

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

[10] **F. Hajati, A. Iranmanesh, and A. Tehranian**, *A characterization of* $U_4(2)$ *by* nse, Facta Univ., Ser. Math. Inf., **34** (2019), 641 – 649.

[11] **M. Hall, Jr** , *The theory of groups*, The Macmillan Co., New York, N.Y., 1959.

[12] **H. Hasanzadeh-Bashir, B. Ebrahimzadeh, and B. Azizi**, *A new characterization of orthogonal simple groups* $B_2(2^{4n})$, Quasigroups Relat. Syst., **31** (2023), 233 – 240.

[13] **A.S. Kondrat'ev**, *On prime graph components of finite simple groups*, Mat. Sb., **180** (1989), 787 – 797.

[14] **G. Malle**, *The maximal subgroups of* ${}^2F_4(q^2)$, J. Algebra, **139** (1991), 52 – 69.

[15] **V. Mazurov and E. Khukhro**, *Unsolved Problems in Group Theory: The Kourovka Notebook No. 16*, Kourovka notebook. Inst. Math., Russian Acad. Sci., Siberian Division, 2006.

[16] **S. Rahbariyan and A. Azad**, *On the NSE characterization of certain finite simple groups*, Algebr. Struct. Appl., **8** (2021), no. 2, 51 − 65.

[17] **C. Shao, W. Shi, and Q. Jiang**, *Characterization of simple K_4-groups*, Front. Math. China, **3** (2008), 355 − 370.

[18] **J.S. Williams**, *Prime graph components of finite groups*, J. Algebra, **69** (1981), 487 − 513.

Received November 16, 2023

A. Daneshkhah and F. Moameri
Department of Mathematics
Faculty of Science
Bu-Ali Sina University
Hamedan, Iran
E-mail: adanesh@basu.ac.ir, f.moameri@basu.ac.ir

H. Parvizi Mosaed
Alvand Institute of Higher Education
Hamedan, Iran
E-mail: h.parvizi.mosaed@gmail.com

Quasigroups and Related Systems **32** (2024), 41 − 48

https://doi.org/10.56415/qrs.v32.04

On pseudo-ideals in partially ordered ternary semigroups

Machchhindra Gophane and Dattatray Shinde

Abstract. We study the properties of different types of pseudo-ideals of a partially ordered ternary semigroup and prove that the space of all strongly irreducible pseudo-ideals of a partially ordered ternary semigroup is a compact space.

1. Introduction

In [2], Hewitt and Zuckerman specified the method of construction of ternary semigroups from binary and specified various connections between such semigroups. Ternary semigroups are a special case of n-ary semigroups. So many results on ternary semigroups has an analogous version for n-ary semigroups. F.M. Sioson [5] proved some results on ideals in ternary semigroups. In [1], W.A. Dudek and I.M. Groździńska characterized some classes of regular ternary semigroups by ideals can be deduced from general results proved for n-ary semigroups. The notion of prime, semiprime and strongly prime bi-ideals in ternary semigroups was introduced by M. Shabir and M. Bano in [4]. The concept of ordered ternary semigroups was developed by A. Iampan in [3].

Our aim of this article is to introduce the concepts of prime pseudo-ideals and irreducible pseudo-ideals in a partially ordered ternary semigroup and to study their properties. We also prove that the space of all strongly irreducible pseudo-ideals of a partially ordered ternary semigroup is a compact space.

2020 Mathematics Subject Classification: 20M12, 20N99, 06F99.
Keywords: partially ordered ternary semigroup, pseudo-ideal, prime pseudo-ideal, irreducible pseudo-ideal.

2. Preliminaries

A non-empty set T with a ternary operation $[\ ] : T \times T \times T \longrightarrow T$ is called a *ternary semigroup* if $[\ ]$ satisfies the associative law, $[abcde] = [[abc]de] = [a[bcd]e] = [ab[cde]]$, for all $a, b, c, d, e \in T$.

For non-empty subsets X, Y and Z of a ternary semigroup T, $[XYZ] = \{[xyz] : x \in X, y \in Y$ and $z \in Z\}$. We write, $[XYZ]$ as XYZ, $[xyz] = xyz$ and $[XXX] = X^3$.

A ternary semigroup T is said to be a *partially ordered ternary semigroup* if there exist a partially ordered relation $\leqslant$ on T such that, $a \leqslant b \Rightarrow xya \leqslant xyb$, $xay \leqslant xby$, $axy \leqslant bxy$ for all $a, b, x, y \in T$. In this article, we write T for a partially ordered ternary semigroup, unless otherwise specified.

An element $e \in T$ is said to be an *identity element* of T if $exx = xxe = xex = x$ for all $x \in T$.

The set $\{t \in T : t \leqslant x, \text{for some} x \in X\}$ is denoted by $(X]$. A non-empty subset X of T is said to be a *partially ordered ternary subsemigroup* of T, if $[XXX] \subseteq X$ and $(X] = X$. A non-empty subset I of T is said to be a *partially ordered left* (respectively, *right, lateral*) *ideal* of T if $TTI \subseteq I$ (respectively, $ITT \subseteq I$, $TIT \subseteq I$) and $(I] = I$.

A non-empty subset I of T is said to be *ideal* of T if it is a left ideal, a right ideal and a lateral ideal of T.

A partially ordered ternary subsemigroup I of T is called a *left* (respectively a *right*, a *lateral*) pseudo-ideal of T if $[xxxxI] \subseteq I$ (respectively, $[Ixxxx] \subseteq I$, $[xxIxx] \subseteq I$) for all $x \in T$. A pseudo-ideal I of T is said to be *proper pseudo-ideal* of T if it differs from T.

A non-empty subset I of T is said to be *two sided pseudo-ideal* of T, if it is both left and right pseudo-ideal of T. A non-empty subset I of T is said to be *pseudo-ideal* of T, if I is a left, a right and a lateral pseudo-ideal of T. Note that, the non-empty intersection of an arbitrary collection of pseudo-ideals of T is a pseudo-ideal of T.

Example 2.1. Let $\mathbb{N}$ be the set of all natural numbers. Define ternary operation $[\ ]$ on $\mathbb{N}$ by $[xyz] = xyz$ for all $x, y, z \in \mathbb{N}$, where $\cdot$ is a usual multiplication and a usual partial ordering relation $\leqslant$ on $\mathbb{N}$. Then $\mathbb{N}$ is a partially ordered ternary semigroup and $I = 3\mathbb{N}$ is a pseudo-ideal of $\mathbb{N}$.

Definition 2.2. A proper pseudo-ideal I of a partially ordered ternary semigroup T is called

(*i*) *prime pseudo-ideal* of T if $XYZ \subseteq I$ implies $X \subseteq I$ or $Y \subseteq I$ or $Z \subseteq I$ for any pseudo-ideals X, Y, Z of T, (*ii*) *strongly prime pseudo-ideal* of T if $XYZ \cap YZX \cap ZXY \subseteq I$ implies $X \subseteq I$ or $Y \subseteq I$ or $Z \subseteq I$ for any pseudo-ideals X, Y, Z of T,

(*iii*) *semiprime pseudo-ideal* of T if X is a pseudo-ideal of T and $X^n \subseteq I$ implies $X \subseteq I$ for some odd natural number n.

3. Main Results

Definition 3.1. A proper pseudo-ideal I of T is said to be *irreducible* (respectively, *strongly irreducible*) pseudo-ideal of T if $X \cap Y \cap Z = I$ (respectively $X \cap Y \cap Z \subseteq I$) implies $X = I$ or $Y = I$ or $Z = I$ (respectively $X \subseteq I$ or $Y \subseteq I$ or $Z \subseteq I$) for all pseudo-ideals X, Y, Z of T.

Remark 3.2. Every strongly irreducible pseudo-ideal of T is an irreducible pseudo-ideal of T but converse is not true in general.

Theorem 3.3. *Let X be a proper pseudo-ideal of T. For any $t(\neq 0) \in T \backslash X$ there exists an irreducible pseudo-ideal I of T such that $X \subseteq I$ and $t \notin I$.*

Proof. Let $\mathcal{I} = \{X_\alpha : X_\alpha$ is a pseudo-ideal of $T, X \subseteq X_\alpha, t \notin X_\alpha\}$, where $\alpha \in \Delta$ is any indexing set. As X is a pseudo-ideal of T and $t \notin X$, we have $X \in \mathcal{I}$, so $\mathcal{I} \neq \emptyset$. Evidently $\mathcal{I}$ is partially ordered set under the inclusion of sets. If $\{X_i : i \in \Delta\}$ is a totally ordered subset (chain) of $\mathcal{I}$ then $\bigcup_{i \in \Delta} X_i$ is a pseudo-ideal of T containing X and $t \notin \bigcup_{i \in \Delta} X_i$. Therefore $\bigcup_{i \in \Delta} X_i$ is an upper bound of $\{X_i : i \in \Delta\}$. Thus every chain in $\mathcal{I}$ has an upper bound in $\mathcal{I}$. Hence by Zorn's Lemma, there exists a maximal element say I in the collection $\mathcal{I}$. This shows that I is a pseudo-ideal of T such that $X \subseteq I$ and $t \notin I$.

Now we show that I is an irreducible pseudo-ideal of T. Let I_1, I_2 and I_3 be any three pseudo-ideals of T such that $I = I_1 \cap I_2 \cap I_3$ then $I \subseteq I_1, I \subseteq I_2$ and $I \subseteq I_3$. If I_1, I_2 and I_3 properly contain I, then according to hypothesis $t \in I_1, t \in I_2$ and $t \in I_3$. Thus $t \in I_1 \cap I_2 \cap I_3 = I$. Which contradicts to the fact that $t \notin I$. Therefore either $I = I_1$ or $I = I_2$ or $I = I_3$. Hence I is an irreducible. $\square$

Theorem 3.4. *Any proper pseudo-ideal of T is the intersection of all irreducible pseudo-ideals containing it.*

Proof. Let X be the any proper pseudo-ideal of T and $\{X_i : i \in \Delta\}$ be the family of all irreducible pseudo-ideals of T containing X. Then $X \subseteq \bigcap_{i\in\Delta} X_i$. If $X \subsetneq \bigcap_{i\in\Delta} X_i$ then there exists $t(\neq 0) \in \bigcap_{i\in\Delta} X_i$ such that $t \notin X$. This implies $t \in X_i \ \forall i \in \Delta$. Since $t \notin X$, then by Theorem 3.3, there exists an irreducible pseudo-ideal say Y of T containing X but not containing t. This is a contradiction to $t \in X_i \ \forall i \in \Delta$. Thus $\bigcap_{i\in\Delta} X_i \subseteq X$. Hence $X = \bigcap_{i\in\Delta} X_i$. □

Theorem 3.5. *Every strongly irreducible semiprime pseudo-ideal of T is a strongly prime pseudo-ideal of T.*

Proof. Let I be a strongly irreducible semiprime pseudo-ideal of T. If X, Y and Z are three pseudo-ideals of T such that $[XYZ] \cap [YZX] \cap [ZXY] \subseteq I$. Then $(X\cap Y\cap Z)^3 = [(X\cap Y\cap Z)(X\cap Y\cap Z)(X\cap Y\cap Z)] \subseteq [XYZ]$. Similarly $(X \cap Y \cap Z)^3 \subseteq [YZX]$ and $(X \cap Y \cap Z)^3 \subseteq [ZXY]$. This proves that $(X\cap Y\cap Z)^3 \subseteq [XYZ]\cap[YZX]\cap[ZXY] \subseteq I$. Therefore $(X\cap Y\cap Z)^3 \subseteq I$. Since I is a semiprime pseudo-ideal, $(X \cap Y \cap Z) \subseteq I$. Also since I is a strongly irreducible pseudo-ideal of T. Therefore, by definition of strongly irreducible pseudo-ideal, either $X \subseteq I$ or $Y \subseteq I$ or $Z \subseteq I$. Hence I is a strongly prime pseudo-ideal of T. □

Corollary 3.6. *Every strongly irreducible semiprime pseudo-ideal of T is prime pseudo-ideal of T.*

Definition 3.7. A pseudo-ideal X of partially ordered ternary semigroup T is called idempotent if $X^3 = X$.

Theorem 3.8. *The following assertions for a partially ordered ternary semigroup T with identity are equivalent.*

(*i*) *Every pseudo-ideal of T is idempotent.*

(*ii*) *For every three pseudo-ideals X, Y, Z of T,*
$X \cap Y \cap Z \subseteq [XYZ] \cap [YZX] \cap [ZXY]$.

(*iii*) *Every proper pseudo-ideal of T is semiprime.*

(*iv*) *Each proper pseudo-ideal of T is the intersection of all irreducible semiprime pseudo-ideals of T which contain it.*

Proof. $(i) \Rightarrow (ii)$: Suppose that, every pseudo-ideal of T is idempotent. Let X, Y and Z be three pseudo-ideals of T. Then $X \cap Y \cap Z$ is a pseudo-ideal of T, so $X \cap Y \cap Z = (X \cap Y \cap Z)^3 = [(X \cap Y \cap Z)(X \cap Y \cap Z)(X \cap Y \cap Z)] \subseteq [XYZ]$. Similarly $X \cap Y \cap Z \subseteq [YZX]$ and $X \cap Y \cap Z \subseteq [ZXY]$. Therefore $X \cap Y \cap Z \subseteq [XYZ] \cap [YZX] \cap [ZXY]$.

$(ii) \Rightarrow (i)$: Let X be a pseudo-ideal of T. Then from $(ii), X = X \cap X \cap X \subseteq [XXX] \cap [XXX] \cap [XXX] = [XXX] = X^3 \Rightarrow X \subseteq X^3$. As X be a pseudo-ideal of T, so $X^3 \subseteq X$. Thus $X^3 = X$. This shows that every pseudo-ideal of T is idempotent.

$(i) \Rightarrow (iii)$: Suppose that, every pseudo-ideal of T is idempotent. Let X be a proper pseudo-ideal of T. Let Y be a pseudo-ideal of T such that $Y^3 \subseteq X$, then by hypothesis $Y^3 = Y$. Thus $Y \subseteq X$. This shows that X is semiprime pseudo-ideal of T. Hence every pseudo-ideal of T is semiprime.

$(iii) \Rightarrow (iv)$: Suppose that each proper pseudo-ideal of T is semiprime. By Theorem 3.4, any proper pseudo-ideal X of T is the intersection of all irreducible pseudo-ideals of T containing it. By (iii), every proper pseudo-ideal of T is the intersection of all irreducible semiprime pseudo-ideals of T which containing it.

$(iv) \Rightarrow (i)$: Suppose that each proper pseudo-ideal of T is the intersection of all irreducible semiprime pseudo-ideals of T which contain it. Let X be a pseudo-ideal of T. Therefore it is the intersection of all irreducible semiprime pseudo-ideals of T which contain it. Therefore X is a semiprime pseudo-ideal of T. As $X^3 \subseteq X^3 \Rightarrow X \subseteq X^3$ but $X^3 \subseteq X$ always. This shows that $X = X^3$. Hence every pseudo-ideal of T is idempotent. □

Theorem 3.9. *If every pseudo-ideal of T is strongly prime pseudo-ideal of T then each pseudo-ideal of T is idempotent.*

Proof. Suppose that, each pseudo-ideal of T is strongly prime, then each pseudo-ideal of T is semiprime. Thus by Theorem 3.8, every pseudo-ideal of T is idempotent. □

Theorem 3.10. *If every pseudo-ideal of T is idempotent and the set of pseudo-ideals of T is totally ordered under set inclusion then each pseudo-ideal of T is strongly prime pseudo-ideal of T.*

Proof. Suppose that every pseudo-ideal of T is idempotent and the set of pseudo-ideals of T is totally ordered under set inclusion. Let I, X, Y and Z be pseudo-ideals of T such that $[XYZ] \cap [YZX] \cap [ZXY] \subseteq I$. As every pseudo-ideal of T is idempotent so, $X \cap Y \cap Z$ is idempotent. Then

$X \cap Y \cap Z = (X \cap Y \cap Z)^3 = [(X \cap Y \cap Z)(X \cap Y \cap Z)(X \cap Y \cap Z)] \subseteq [XYZ]$. Similarly $X \cap Y \cap Z \subseteq [YZX]$ and $X \cap Y \cap Z \subseteq [ZXY]$. Therefore $X \cap Y \cap Z \subseteq [XYZ] \cap [YZX] \cap [ZXY] \subseteq I$. As the set of all pseudo-ideal of T is totally ordered under set inclusion, therefore for pseudo-ideals X, Y, Z of T, we have the following six possibilities,

1) $X \subseteq Y \subseteq Z$, 2) $X \subseteq Z \subseteq Y$, 3) $Y \subseteq X \subseteq Z$
4) $Y \subseteq Z \subseteq X$, 5) $Z \subseteq X \subseteq Y$, 6) $Z \subseteq Y \subseteq X$.

In such cases, we have respectively,

1) $X \cap Y \cap Z = X$, 2) $X \cap Y \cap Z = X$, 3) $X \cap Y \cap Z = Y$,
4) $X \cap Y \cap Z = Y$, 5) $X \cap Y \cap Z = Z$, 6) $X \cap Y \cap Z = Z$.

Therefore $X \cap Y \cap Z = X$ or $X \cap Y \cap Z = Y$ or $X \cap Y \cap Z = Z$. Thus from $X \cap Y \cap Z \subseteq I$, either $X \subseteq I$ or $Y \subseteq I$ or $Z \subseteq I$. This shows that I is a strongly prime pseudo-ideal of T. □

Theorem 3.11. *If the set of pseudo-ideals of T is totally ordered under set inclusion then every pseudo-ideal of T is idempotent if and only if each pseudo-ideal of T is prime.*

Proof. Suppose that every pseudo-ideal of T is idempotent. Let I, X, Y and Z be pseudo-ideals of T such that $XYZ \subseteq I$. As every pseudo-ideal of T is idempotent so, $X \cap Y \cap Z$ is idempotent. Then $X \cap Y \cap Z = (X \cap Y \cap Z)^3 = [(X \cap Y \cap Z)(X \cap Y \cap Z)(X \cap Y \cap Z)] \subseteq XYZ \subseteq I$. Therefore $X \cap Y \cap Z \subseteq I$. As in the proof of the Theorem 3.10 we get $X \cap Y \cap Z = X$ or $X \cap Y \cap Z = Y$ or $X \cap Y \cap Z = Z$. Thus from $X \cap Y \cap Z \subseteq I$, either $X \subseteq I$ or $Y \subseteq I$ or $Z \subseteq I$. This shows that I is a prime pseudo-ideal of T.

Conversely, suppose that every pseudo-ideal of T is a prime pseudo-ideal of T. Since the set of pseudo-ideals of T is totally ordered under set inclusion, therefore the concepts of primeness and strongly primeness coincide. Hence by Theorem 3.9, every pseudo-ideal of T is idempotent. □

Definition 3.12. An proper pseudo-ideal X of T is said to be *maximal pseudo-ideal* of T if X is not properly contained in any proper pseudo-ideal of T.

Theorem 3.13. *Every maximal pseudo-ideal X of T is irreducible pseudo-ideal of T.*

Proof. Let X be a maximal pseudo-ideal of T. Suppose X is not irreducible pseudo-ideal of T. i.e. for any three pseudo-ideals A, B and C of T such that $A \cap B \cap C = X \Rightarrow A \neq X, B \neq X$ and $C \neq X \Rightarrow X \subset A \subset T, X \subset$

$B \subset T, X \subset C \subset T$. Which is contradiction to X be a maximal pseudo-ideal of T. Hence X is an irreducible pseudo-ideal of T. $\square$

Definition 3.14. Let X be the non-empty subset of T. Then the intersection of all pseudo-ideals of T containing X is the smallest pseudo-ideal of T containing X. This pseudo-ideal of T is called the pseudo-ideal of T generated by X and it is denoted by $(X)_{pi}$. A pseudo-ideal I of T is said to be the principal pseudo-ideal generated by an element x if I is a pseudo-ideal generated by $\{x\}$ for some $x \in T$ and is denoted by $(x)_{pi}$.

Let $\mathfrak{A}$ be the set of all pseudo-ideals of T and $\mathfrak{B}$ be the set of all strongly irreducible pseudo-ideals of T. For each $X \in \mathfrak{A}$, we define $\Psi_X = \{Y \in \mathfrak{B} : X \nsubseteq Y\}$

Theorem 3.15. *The family,* $\mathfrak{J}(\mathfrak{B}) = \{\Psi_X : X \in \mathfrak{A}\}$ *forms a topology on the set* $\mathfrak{B}$.

Proof. (i) As $\{0\} \in \mathfrak{A}$, so $\Psi_{\{0\}} = \{Y \in \mathfrak{B} : \{0\} \nsubseteq Y\} = \emptyset$. Thus $\emptyset \in \mathfrak{J}(\mathfrak{B})$.

(ii) Since $T \in \mathfrak{A}$, we have $\Psi_T = \{Y \in \mathfrak{B} : T \nsubseteq Y\} = \mathfrak{B}$ because $\mathfrak{B}$ is the collection of all proper strongly irreducible pseudo-ideals of T. Thus $\mathfrak{B} \in \mathfrak{J}(\mathfrak{B})$.

(iii) Let $\Psi_{X_1}, \Psi_{X_2} \in \mathfrak{J}(\mathfrak{B})$. We show that $\Psi_{X_1} \cap \Psi_{X_2} \in \mathfrak{J}(\mathfrak{B})$. Let $Y \in \Psi_{X_1} \cap \Psi_{X_2}$ then $Y \in \mathfrak{B}$ such that $X_1 \nsubseteq Y$ and $X_2 \nsubseteq Y$. Suppose that $X_1 \cap X_2 \subseteq Y$. Now, we have $X_1 \cap X_2 \cap T = X_1 \cap X_2 \subseteq Y$. Since Y is a strongly irreducible pseudo-ideal of T, therefore either $X_1 \subseteq Y$ or $X_2 \subseteq Y$ or $T \subseteq Y$. But $T \nsubseteq Y$ (since Y is proper). Therefore $X_1 \subseteq Y$ or $X_2 \subseteq Y$, which is a contradiction. Hence $X_1 \cap X_2 \nsubseteq Y$. Therefore $Y \in \Psi_{X_1 \cap X_2}$. Thus $\Psi_{X_1} \cap \Psi_{X_2} \subseteq \Psi_{X_1 \cap X_2}$. On the other hand if $Y \in \Psi_{X_1 \cap X_2}$ then $Y \in \mathfrak{B}$ and $X_1 \cap X_2 \nsubseteq Y$. This implies that $X_1 \nsubseteq Y$ and $X_2 \nsubseteq Y$. Therefore $Y \in \Psi_{X_1}$ and $Y \in \Psi_{X_2} \Rightarrow Y \in \Psi_{X_1} \cap \Psi_{X_2}$. Hence $\Psi_{X_1 \cap X_2} \subseteq \Psi_{X_1} \cap \Psi_{X_2}$.This shows that $\Psi_{X_1} \cap \Psi_{X_2} = \Psi_{X_1 \cap X_2}$. Thus $\Psi_{X_1} \cap \Psi_{X_2} \in \mathfrak{J}(\mathfrak{B})$.

(iv) Let $\{X_\alpha\}_{\alpha \in \Delta}$ (where Δ is any indexing set.) be family of pseudo-ideals of T and $\{\Psi_{X_\alpha} : \alpha \in \Delta\} \subseteq \mathfrak{J}(\mathfrak{B})$. Then $\bigcup_{\alpha \in \Delta} \Psi_{X_\alpha} = \{Y \in \mathfrak{B} : X_\alpha \nsubseteq Y$ for some $\alpha \in \Delta\} = \{Y \in \mathfrak{B} : \left(\bigcup_{\alpha \in \Delta} X_\alpha\right)_{pi} \nsubseteq Y\} = \Phi_{\left(\bigcup_{\alpha \in \Delta} X_\alpha\right)_{pi}} \in \mathfrak{J}(\mathfrak{B})$, where $\left(\bigcup_{\alpha \in \Delta} X_\alpha\right)_{pi}$ is the pseudo-ideal of T generated by $\left(\bigcup_{\alpha \in \Delta} X_\alpha\right)$. Therefore from $(i), (ii), (iii)$ and (iv), we get the set $\mathfrak{J}(\mathfrak{B})$ forms a topology on $\mathfrak{B}$. $\square$

Theorem 3.16. *If T is partially ordered ternary semigroup with identity then $\mathfrak{B}$ is a compact space.*

Proof. Suppose that $\{\Psi_{X_k} : k \in \Delta\}$ is an open covering of $\mathfrak{B}$, where Δ is an indexing set. That is $\mathfrak{B} = \bigcup_{k\in\Delta} \Psi_{X_k}$. By Theorem 3.15, $\Psi_T = \mathfrak{B}$, therefore $\Psi_T = \bigcup_{k\in\Delta} \Psi_{X_k} \Rightarrow \Psi_T = \Psi_{\left(\bigcup_{k\in\Delta} X_k\right)_{pi}} \Rightarrow T = \left(\bigcup_{k\in\Delta} X_k\right)_{pi}$. As $e \in T, e \in \left(\bigcup_{k\in\Delta} X_k\right)_{pi}$. Hence $e \in (\bigcup_{i=1}^{n} X_i)_{pi} \Rightarrow T = (\bigcup_{i=1}^{n} X_i)_{pi} \Rightarrow \mathfrak{B} = \bigcup_{k=1}^{n} \Psi_{X_k}$. This shows that every open cover of $\mathfrak{B}$ has finite subcover. Hence $\mathfrak{B}$ is compact space. □

References

[1] **W.A. Dudek and I.M. Groździńska**, *On ideals in regular n-semigroups*, Matematićki Bilten, (Skopje) **29/30** (1979-1980), 35 – 44.

[2] **E. Hewitt and H.S. Zuckerman**, *Ternary operations and semigroups*, Proc. Sympos. Wayne State Univ., Detroit (1968), 55 – 83.

[3] **A. Iampan**, *On characterizations of* (0−) *minimal and maximal ordered left* (*right*) *ideals in ordered ternary semigroups*, Global J. Pure Appl. Math., **4(1)** (2008), 91 – 100.

[4] **M. Shabir and M. Bano**, *Prime bi-ideals in partially ordered ternary semigroups*, Quasigroups Related Systems, **16** (2008), 239 – 256.

[5] **F.M. Sioson**, *Ideal theory in partially ordered ternary semigroups*, Math. Japan., **10** (1965), 63 – 84.

Received July 26, 2023

Department of Mathematics,
Shivaji University, Kolhapur- 416004,
Maharashtra (India)
E-mail: shindednmaths@gmail.com, mtg_maths@unishivaji.ac.in

Quasigroups and Related Systems **32** (2024), 49 − 57

https://doi.org/10.56415/qrs.v32.05

Prime one-sided ideals in ordered semigroups

Panuwat Luangchaisri and Thawhat Changphas

Abstract. We prove that the following are equivalent: (1) an ordered semigroup S with zero and identity is right weakly regular; (2) $(AA] = A$ for any right ideal A of S; (3) $A \cap I = (AI]$ for any right ideal A and two-sided ideal I of S; (4) $B \cap I \subseteq (BI]$ for any bi-ideal B and two-sided ideal I of S; (5) $B \cap I \cap A \subseteq (BIA]$ for any bi-ideal B, right ideal A and two-sided ideal I of S; and prove that S is a fully prime right ordered semigroup if and only if S is right weakly regular and the set of all two-sided ideals of S is totally ordered.

1. Introduction

One-sided ideals of a prime type of a ring have been studied by K. Koh in [6]. One-sided prime ideals have been considered by J. Dauns in [3], the author considered prime right ideals of a ring. F. Hansen [4] studied one-sided prime ideals, the paper contained some results on prime right ideals in a weakly regular ring. W.D. Blair and H. Tsutsui studied fully prime rings, it was shown a necessary and sufficient condition for a ring to be fully prime is that every ideal is idempotent and the set of ideals is totally ordered [2]. F. Alarcan and D. Polkawska described fully prime semirings, the authors characterized semirings where every ideal is prime (fully prime semirings) as those having a totally ordered lattice with every ideal idempotents [1]. Recently, prime one-sided ideals in a semiring and a Γ-semiring have been introduced and studied by R. Jagatap and Y. Pawar in [5] and by M. Shabir and M.S. Iqbal in [7]. An ordered semigroup $(S, ., \leqslant)$ is a semigroup $(S, .)$ together with an ordered relation $\leqslant$ on S which is compatible with the

2010 Mathematics Subject Classification: 06F05, 20M20
Keywords: ordered semigroup, prime right ideal, semiprime right ideal, right weakly regular, irreducible, strongly irreducible, fully prime right
This research received financial support from the National Science, Research and Innovation Fund (NSRF).

semigroup operation. In this paper, we consider prime one-sided ideals in an ordered semigroup. Indeed, we mainly consider right weakly regular ordered semigroups and fully prime right ordered semigroups. Let S be an ordered semigroup with zero and identity. It is proved that the following are equivalent: (1) S is right weakly regular; (2) $(AA] = A$ for any right ideal A of S; (3) $A \cap I = (AI]$ for any right ideal A and a two-sided ideal I of S; (4) $B \cap I \subseteq (BI]$ for any bi-ideal B and two-sided ideal I of S; (5) $B \cap I \cap A \subseteq (BIA]$ for any bi-ideal B, right ideal A and two-sided ideal I of S. Moreover, a characterization of fully prime right ordered semigroups will be given in terms of right weakly regularity and the set of all two-sided ideals. Indeed, it is proved that S is a fully prime right ordered semigroup if and only if S is right weakly regular and the set of all two-sided ideals of S is totally ordered (i.e., for any ideals A and B of S, $A \subseteq B$ or $B \subseteq A$).

An *ordered semigroup* $(S, ., \leqslant)$ consists of a semigroup $(S, .)$ together with an ordered relation $\leq$ on S which is compatible with the semigroup operation (i.e., for any $a, b, c \in S$, $a \leqslant b$ implies $ca \leqslant cb$ and $ac \leqslant bc$). For $A, B \subseteq S$, we write AB for $\{ab \in S \mid a \in A, b \in B\}$ and write $(A]$ for $\{x \in S \mid \exists a \in A, x \leqslant a\}$, i.e.

$$AB = \{ab \in S \mid a \in A, b \in B\};$$

$$(A] = \{x \in S \mid \exists a \in A, x \leqslant a\}.$$

It is observed that

(1) $A \subseteq (A]$;

(2) if $A \subseteq B$, then $(A] \subseteq (B]$;

(3) $((A]] = (A]$;

(4) $(A](B] \subseteq (AB]$;

(5) $((A](B]] = (AB]$;

(6) $(A \cup B] = (A] \cup (B]$;

(7) $(A \cap B] \subseteq (A] \cap (B]$.

A nonempty subset A of S is called a *right ideal* (of S) if

(1) $ax \in A$ for any $a \in A$ and $x \in S$ (i.e., $AS \subseteq A$);

(2) $(A] = A$ (i.e., if $a \in A$ and $x \in S$ such that $x \leqslant a$, then $x \in A$).

A left ideal of S can be defined similarly: a nonempty subset A of S is called a *left ideal* (of S) if

(1) $xa \in A$ for any $a \in A$ and $x \in S$ (i.e., $SA \subseteq A$);

(2) $(A] = A$ (i.e., if $a \in A$ and $x \in S$ such that $x \leqslant a$, then $x \in A$).

A nonempty subset A of S is called a *two-sided ideal* (it is abbreviated by *ideal*) of S if it is both a left and a right ideal of S. An element 0 of S is called a *zero* if $0a = a0 = 0$ for all $a \in S$. An element 1 of S is called an *identity* if $a1 = 1a = a$ for all $a \in S$. If S has the identity, then the principal right ideal of S generated by a is of the form $(aS]$; the principal left ideal of S generated by a is of the form $(Sa]$; and the principal ideal of S generated by a is of the form $(SaS]$.

2. Main results

Hereafter, S is an ordered semigroup with zero 0 and identity 1. We begin this section with the definition of prime right ideals of S.

Definition 2.1. Let P be a right ideal of S. Then P is called a *prime right ideal* of S if for any right ideals A and B of S, $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$.

Theorem 2.2. *Let P be a right ideal of S. Then P is a prime right ideal of S if and only if for any $a, b \in S$, $aSb \subseteq P$ implies $a \in P$ or $b \in P$.*

Proof. Assume that P is a prime right ideal of S. Let $a, b \in S$ be such that $aSb \subseteq P$; then

$$(aS](bS] \subseteq ((aS](bS]] = ((aS)(bS)] \subseteq (PS] \subseteq (P] = P.$$

Since $(aS]$ and $(bS]$ are right ideals of S, $(aS] \subseteq P$ or $(bS] \subseteq P$. Hence $a \in P$ or $b \in P$. Conversely, assume that for any $a, b \in S$, $aSb \subseteq P$ implies $a \in P$ or $b \in P$. Let A and B be right ideals of S such that $AB \subseteq P$. Suppose that $A \nsubseteq P$, i.e. there exists $a \in A \setminus P$. Let $b \in B$. Then

$$aSb \subseteq (aSb] \subseteq (ASB] \subseteq (AB] \subseteq (P] = P.$$

By assumption, $a \in P$ or $b \in P$. Thus $b \in P$. Therefore $B \subseteq P$ and hence P is a prime right ideal of S. $\square$

Definition 2.3. Let M be a proper right ideal of S. Then M is said to be *maximal* if there is no any proper right ideal of S containing M properly.

Theorem 2.4. *If M is a maximal right ideal of S, then M is a prime right ideal of S.*

Proof. Let M be a maximal right ideal of S. To show that M is a prime right ideal of S, let $a, b \in S$ be such that $aSb \subseteq M$. Suppose that $a \notin M$. We have $M \cup (aS]$ is a right ideal of S. Since M is a maximal right ideal of S and $M \subset M \cup (aS]$, $M \cup (aS] = S$. Then $1 \in M$ or $1 \in (aS]$. If $1 \in M$, then $b = 1b \in M$. If $1 \in (aS]$, let $1 \leqslant as$ for some $s \in S$. Consider:

$$b = 1b \leqslant asb \in aSb \subseteq M.$$

Therefore $b \in M$ and by Theorem 2.2, M is a prime right ideal of S. $\square$

Theorem 2.5. *Let P be a prime right ideal of S. For $a \in S \setminus P$,*

$$(P : a) = \{x \in S \mid ax \in P\}$$

is a prime right ideal of S.

Proof. Clearly, $0 \in (P : a)$. If $x \in (P : a)$ and $s \in S$, then $ax \in P$; hence $a(xs) = (ax)s \in P$. If $x \in (P : a)$ and $s \in S$ such that $s \leqslant x$, then $as \leqslant ax \in P$; hence $as \in P$ (i.e., $s \in (P : a)$). Therefore $(P : a)$ is a right ideal of S. Let B and C be right ideals of S such that $BC \subseteq (P : a)$; then $a(BC) \subseteq P$. Consider:

$$(aB](aC] \subseteq ((aB](aC]] = ((aB)(aC)] \subseteq (aBC] \subseteq (P] = P.$$

Then $(aB] \subseteq P$ or $(aC] \subseteq P$. Hence $B \subseteq (P : a)$ or $C \subseteq (P : a)$. Hence $(P : a)$ is a prime right ideal of S. $\square$

Similarly, we have the following result:

Theorem 2.6. *Let P be a prime right ideal of S. Then*

$$\{x \in S \mid Sx \subseteq P\}$$

is the largest ideal of S contained in P.

Definition 2.7. Let P be a right ideal of S. Then P is said to be a *semiprime right ideal* of S if for any right ideal A of S, $AA \subseteq P$ implies $A \subseteq P$.

It is observed that every prime right ideal is a semiprime right ideal.

Theorem 2.8. *Let P be a right ideal of S. Then P is a semiprime right ideal of S if and only if for any $a \in S$, $aSa \subseteq P$ implies $a \in P$.*

Proof. Assume that P is semiprime right ideal of S. Let $a \in S$ be such that $aSa \subseteq P$; then

$$(aS](aS] \subseteq ((aS](aS]] = ((aS)(aS)] \subseteq (PS] \subseteq (P] = P.$$

Since $(aS]$ is a right ideal of S, $(aS] \subseteq P$. Hence $a \in P$. Conversely, assume that for any $a \in S$, $aSa \subseteq P$ implies $a \in P$. Let A be a right ideal of S such that $AA \subseteq P$. Let $a \in A$. Then

$$aSa \subseteq (aSa] \subseteq (ASA] \subseteq (AA] \subseteq (P] = P.$$

By assumption, $a \in P$. Therefore $A \subseteq P$. Hence P is a semiprime right ideal of S. □

Definition 2.9. Let A be a right ideal of S. Then A is said to be *irreducible* if for any right ideals B and C of S, $B \cap C = A$ implies $B = A$ or $C = A$.

Definition 2.10. Let A be a right ideal of S. Then A is said to be *strongly irreducible* if for any right ideals B and C of S, $B \cap C \subseteq A$ implies $B \subseteq A$ or $C \subseteq A$.

Theorem 2.11. *Let A be a right ideal of S. If $x \notin A$, then there exists an irreducible right ideal of S containing A and not containing x.*

Proof. Assume that $x \notin A$. Clearly, the set of right ideals of S containing A and not containing x is nonempty. Consider a set $\{A_\alpha \mid \alpha \in \Lambda\}$ of a chain of right ideals of S containing A and not containing x. Then $\cup_{\alpha\in\Lambda} A_\alpha$ is a right ideal of S containing A and not containing x. By Zorn's lemma, the set of right ideals of S containing A and not containing x contains a maximal element, denoted by M. Let B and C be right ideals of S such that $B \cap C = M$. Suppose that $M \subset B$ and $M \subset C$. Then $x \in B$ and $x \in C$. Since $x \notin M$, $x \notin B$ or $x \notin C$. This is a contradiction. Hence $M = B$ or $M = C$. Therefore M is irreducible □

Theorem 2.12. *Any proper right ideal A of S is the intersection of irreducible right ideals of S containing A.*

Proof. Let A be a proper right ideal of S, $\{A_\alpha \mid \alpha \in \Lambda\}$ the set of irreducible right ideals of S containing A. Then $A \subseteq \cap_{\alpha\in\Lambda} A_\alpha$. If $x \notin A$, then there exists an irreducible right ideal A_{α_0} of S such that $A \subseteq A_{\alpha_0}$ and $x \notin A_{\alpha_0}$. Then $x \notin \cap_{\alpha\in\Lambda} A_\alpha$. Hence $\cap_{\alpha\in\Lambda} A_\alpha \subseteq A$. Thus $A = \cap_{\alpha\in\Lambda} A_\alpha$. Therefore A is the intersection of irreducible right ideals of S containing A. □

Theorem 2.13. *Let P be a right ideal of S. If P is strongly irreducible semiprime, then P is prime.*

Proof. Assume that P is strongly irreducible semiprime. To show that P is prime, let A and B be right ideals of S such that $AB \subseteq P$. We have

$$(A \cap B)(A \cap B) \subseteq AB \subseteq P.$$

Since $A \cap B$ is a right ideal of S and P is semiprime, $A \cap B \subseteq P$. From P is strongly irreducible, it follows that $A \subseteq P$ or $B \subseteq P$. Hence P is prime. □

Definition 2.14. An ordered semigroup S is called *right weakly regular* if $a \in (aSaS]$ for all $a \in S$.

Theorem 2.15. *The following conditions are equivalent:*

(1) *S is right weakly regular;*

(2) *$(AA] = A$ for any right ideal A of S;*

(3) *$A \cap I = (AI]$ for any right ideal A and ideal I of S.*

Proof. Assume that S is right weakly regular. Let A be a right ideal of S. Then $(AA] \subseteq A$. If $a \in A$, then

$$a \in (aSaS] \subseteq (ASAS] \subseteq (AA].$$

Then $A \subseteq (AA]$. Hence $A = (AA]$. Therefore $(AA] = A$ for any right ideal A of S. Conversely, assume that $(AA] = A$ for any right ideal A of S. To show that S is right weakly regular, let $a \in S$. Since $(aS]$ is a right ideal of S, $((aS](aS]] = (aS]$. Thus

$$a \in (aS] = ((aS](aS]] = (aSaS].$$

Therefore S is right weakly regular. This proves that (1) is equivalent to (2).

To show that (2) is equivalent to (3) assume that $(AA] = A$ for any right ideal A of S. Let A be a right ideal and I an ideal of S. We have $(AI] \subseteq A \cap I$. From $A \cap I$ is a right ideal of S, it follows that

$$A \cap I = ((A \cap I)(A \cap I)] \subseteq (AI].$$

Then $A \cap I = (AI]$. Hence $A \cap I = (AI]$ for any right ideal A and ideal I of S. Conversely, assume that $A \cap I = (AI]$ for any right ideal A and ideal I of S. Let B be a right ideal of S. We have $(SBS]$ is an ideal of S. Consider:

$$B = B \cap (SBS] = (B(SBS]] \subseteq ((B](SBS]] = (BSBS] \subseteq (BB].$$

Hence $(BB] = B$. Therefore, $(BB] = B$ for any right ideal B of S. □

Theorem 2.16. *S is right weakly regular if and only if every right ideal of S is semiprime.*

Proof. Assume that S is right weakly regular. Let P be a right ideal of S. Let A be a right ideal of S such that $AA \subseteq P$. By assumption and Theorem 2.15, $A = (AA]$. Thus $A \subseteq P$. Hence P is semiprime. Conversely, assume that every right ideal of S is semiprime. To show that S is right weakly regular, let B be a right ideal of S. Since $(BB]$ is a right ideal of S, $(BB]$ is semiprime. From $BB \subseteq (BB]$, it follows that $B \subseteq (BB]$. Since $(BB] \subseteq B \subseteq (BB]$, $(BB] = B$. By Theorem 2.15, S is right weakly regular. □

Theorem 2.17. *Let S be right weakly regular and P an ideal of S. Then P is prime if and only if P is irreducible.*

Proof. It is clear that if P is prime, then P is irreducible. Assume that P is irreducible. Let A and B be ideals of S such that $AB \subseteq P$. By Theorem 2.15, $A \cap B \subseteq P$. Then $(A \cap B) \cup P = P$. This means $(A \cup P) \cap (B \cup P) = P$. By assumption, $A \cup P = P$ or $B \cup P = P$. Hence $A \subseteq P$ or $B \subseteq P$. Therefore P is prime. □

Definition 2.18. We call S a *fully prime right ordered semigroup* if all right ideals of S are prime right ideals. For a *fully semiprime right ordered semigroup* can be defined similarly.

Theorem 2.19. *If S is a fully prime right ordered semigroup, then S is right weakly regular and the set of ideals of S is totally ordered.*

Proof. If S is a fully prime right ordered semigroup, then all right ideals of S are prime right ideals of S. Since every prime right ideal is semiprime and Theorem 2.16, S is right weakly regular. Let A and B be ideals of S. Then $A \cap B$ is a right ideal of S. By assumption, $A \cap B$ is prime. Since $AB \subseteq A \cap B$, $A \subseteq A \cap B$ or $B \subseteq A \cap B$. This means $A = A \cap B$ or $B = A \cap B$. Therefore $A \subseteq B$ or $B \subseteq A$. Hence S is right weakly regular and the set of ideals of S is totally ordered. □

Theorem 2.20. *If S is right weakly regular and the set of ideals of S is totally ordered, then S is a fully prime right ordered semigroup.*

Proof. Assume that S is right weakly regular and the set of ideals of S is totally ordered. It is to show that S is a fully prime right ordered semigroup. Let P be a right ideal of S. To show that P is prime, let A and B be right ideals of S such that $AB \subseteq P$. We have $A \subseteq B$ or $B \subseteq A$; $(AA] = A$, $(BB] = B$. If $A \subseteq B$, then

$$A = (AA] \subseteq (AB] \subseteq (P] = P.$$

Similarly, for $B \subseteq A$, we have $B \subseteq P$. Hence P is prime. Therefore S is a fully prime right ordered semigroup. □

Now we give a characterization of a fully prime right ternary semiring followed by Theorems 2.19 and Theorem 2.20.

Theorem 2.21. *S is a fully prime right ordered semigroup if and only if S is right weakly regular and the set of ideals of S is totally ordered.*

We recalled that a subsemigroup B of S is called a *bi-ideal* of S if $BSB \subseteq B$ and $(B] = B$ (i.e., if $b \in B$ and $x \in S$ such that $x \leqslant b$, then $x \in B$).

Theorem 2.22. *S is right weakly regular if and only if $B \cap I \subseteq (BI]$ for any bi-ideal B and ideal I of S.*

Proof. Assume that S is right weakly regular. Let B be a bi-ideal and I an ideal of S. Let $x \in B \cap I$. By assumption, $x \in (xSxS]$. Then

$$x \in (xSxS] \subseteq (xS(xSxS]S] \subseteq (xSxSxSS] \subseteq (BSBSISS] \subseteq (BI].$$

Hence $B \cap I \subseteq (BI]$. Conversely, assume that $B \cap I \subseteq (BI]$ for any bi-ideal B and an ideal I of S. Let A be a right ideal of S. It is observed that A is a bi-ideal of S. Using assumption, we have

$$A = A \cap (SAS] \subseteq (A(SAS]] = (ASAS] \subseteq (AA] \subseteq A.$$

Thus $A = (AA]$. By Theorem 2.15, S is right weakly regular. □

Theorem 2.23. *S is right weakly regular if and only if $B \cap I \cap A \subseteq (BIA]$ for any bi-ideal B, right ideal A and ideal I of S.*

Proof. Assume that S is right weakly regular. Let B be a bi-ideal, A a right ideal and I an ideal of S. Let $x \in B \cap I \cap A$. By assumption, $x \in (xSxS]$. Then

$$x \in (xSxS] = (xS(xSxS]S] \subseteq (xSxSxSS] \subseteq (B(SIS)(ASS)] \subseteq (BIA].$$

Hence $B \cap I \cap A \subseteq (BIA]$. Conversely, assume that $B \cap I \cap A \subseteq (BIA]$ for any bi-ideal B, right ideal A and ideal I of S. Let A be a right ideal of S. From A is a bi-ideal of S and assumption, we have

$$A = A \cap S \cap A \subseteq (ASA] \subseteq (AA] \subseteq (A] = A.$$

Thus $A = (AA]$. By Theorem 2.15, S is right weakly regular. □

References

[1] **F. Alarcan, D. Palkawska**, *Fully prime semirings*, Kyungpook Math. J., **40** (2000), 239 − 245.

[2] **W.D. Blair, H. Tsutsui**, *Fully prime rings*, Commun. Algebra, **22** (1994), 5389 − 5400.

[3] **J. Dauns**, *One sided prime ideals*, Pacific J. of Math., **47** (1973), 401 − 412.

[4] **F. Hansen**, *On one-sided prime ideals*, Pacific J. of Math., **58** (1975), 79−85.

[5] **R. Jagatap, Y. Pawar**, *Right ideals of* Γ*-semirings*, Novi Sad J. Math., **43** (2013), 11 − 19.

[6] **K. Koh**, *On one sided ideals of a prime type*, Proc. Amer. Math. Soc., **28** (1971), 321 − 329.

[7] **M. Shabir, M.S. Iqbal**, *One-sided prime ideals in semirings*, Kyungpook Math. J., **47** (2007), 473 − 480.

Received September 28, 2023

Department of Mathematics
Faculty of Science
Khon Kaen University
Khon Kaen
40002
Thailand
Email: panulu@kku.ac.th, thacha@kku.ac.th

Quasigroups and Related Systems **32** (2024), 59 – 67

https://doi.org/10.56415/qrs.v32.06

On idempotent ordered semigroups

Susmita Mallick and Kalyan Hansda

Abstract. An element e of an ordered semigroup $(S, \cdot, \leqslant)$ is called an ordered idempotent if $e \leqslant e^2$. We call an ordered semigroup S idempotent ordered semigroup if every element of S is an ordered idempotent. Every idempotent semigroup is a complete semilattice of rectangular idempotent semigroups and in this way we arrive to many other important classes of idempotent ordered semigroups.

1. Introduction

Idempotents play an important role in different major subclasses of the regular semigroups S. A regular semigroup S is called orthodox if the set of all idempotents $E(S)$ forms a subsemigroup, and S is a band if $S = E(S)$.

T. Saito studied systematically the influence of order on idempotent semigroup [4]. In [1], Bhuniya and Hansda introduced the notion of ordered idempotents and studied different classes of regular ordered semigroups, such as, completely regular, Clifford and left Clifford ordered semigroups by their ordered idempotents. If T is a subsemigroup of S, then the set of ordered regular elements of T is denoted by $Reg_{\leqslant}(T)$ [2]. If $T =< E_{\leqslant}(S) >$ then $Reg_{\leqslant}(T) = T = Reg_{\leqslant}(S) \cap T$, in general. In [2], Hansda proved several equivalent conditions so that $Reg_{\leqslant}(T) = T = Reg_{\leqslant}(S) \cap T$ for $T = (Se], (eS]$ and $(eSf]$, where e, f are ordered idempotents. The purpose of this paper to study ordered semigroups in which every element is an ordered idempotent. Complete semilattice decomposition of these semigroups automatically suggests the looks of rectangular idempotent semigroups and in this way we arrive to many other important classes of idempotent ordered semigroups.

2010 Mathematics Subject Classification: 20M10, 06F05.

Keywords: ordered idempotent; idempotent ordered semigroup; rectangular idempotent ordered semigroup normal idempotent ordered semigroup.

2. Preliminaries

An ordered semigroup is a partially ordered set $(S, \leqslant)$, and at the same time a semigroup $(S, \cdot)$ such that for all $a, b, c \in S$; $a \leqslant b$ implies that $ca \leqslant cb$ and $ac \leqslant bc$. It is denoted by $(S, \cdot, \leqslant)$. Throughout this article, unless stated otherwise, S stands for an ordered semigroup. For every subset $H \subseteq S$, denote $(H] = \{t \in S : t \leqslant h, \text{ for some } h \in H\}$. Kehayopulu [3] defined Green's relations on a regular ordered semigroup S as follows:

$$a\mathcal{L}b \; if \; (S^1a] = (S^1b], \; a\mathcal{R}b \; if \; (aS^1] = (bS^1],$$

$$a\mathcal{J}b \; if \; (S^1aS^1] = (S^1bS^1], \text{ and } \mathcal{H} = \mathcal{L} \cap \mathcal{R}.$$

These four relations $\mathcal{L}$, $\mathcal{R}$, $\mathcal{J}$ and $\mathcal{H}$ are equivalence relations.

An equivalence relation ρ on S is called left (right) congruence if for every $a, b, c \in S$; $a\rho b$ implies $ca\rho cb$ $(ac\rho bc)$. By a congruence we mean both left and right congruence. A congruence ρ is called a semilattice congruence on S if for all $a, b \in S$, $a\rho a^2$ and $ab\rho ba$. By a complete semilattice congruence we mean a semilattice congruence σ on S such that for $a, b \in S$, $a \leqslant b$ implies that $a\sigma ab$. An element e of an ordered semigroup $(S, \cdot, \leqslant)$ is called an ordered idempotent [1] if $e \leqslant e^2$. An ordered semigroup S is called $\mathcal{H}-$commutative if for every $a, b \in S$, $ab \in (bSa]$.

If F is a semigroup, then the set $P_f(F)$ of all finite subsets of F is a semilattice ordered semigroup with respect to the product $\cdot$ and partial order relation $\leqslant$ given by: for $A, B \in P_f(F)$,

$$A \cdot B = \{ab \mid a \in A, b \in B\} \text{ and } A \leqslant B \text{ if and only if } A \subseteq B.$$

3. Idempotent ordered semigroups

In this section we characterize ordered semigroups of which every element is an ordered idempotent. We show that these ordered semigroups are analogous to bands.

We first make a natural analogy between band and idempotent ordered semigroup.

Theorem 3.1. *Let B be a semigroup. Then $P_f(B)$ is idempotent ordered semigroup if and only if B is a band.*

Proof. Let B be a band and $U \in P_f(B)$. Choose $x \in U$. Then $x^2 \in U^2$ implies $x \in U^2$. Then $U \subseteq U^2$. So $P_f(B)$ is idempotent ordered semigroup.

Conversely, assume that B be a semigroup such that $P_f(B)$ is an idempotent ordered semigroup. Take $y \in B$. Then $Y = \{y\} \in P_f(B)$. Thus $Y \subseteq Y^2$, which implies $y = y^2$. Hence B is a band. $\square$

Proposition 3.2. *Let B be a band, S be an idempotent ordered semigroup and $f : B \longrightarrow S$ be a semigroup homomorphism. Then there is an ordered semigroup homomorphism $\phi : P_f(B) \longrightarrow S$ such that the following diagram is commutative:*

$$\begin{tikzcd}
B \arrow[r, "f"] \arrow[d, "l"] & S \\
P_f(B) \arrow[ur, "\phi"'] &
\end{tikzcd}$$

where $l : B \longrightarrow P_f(B)$ is given by $l(x) = \{x\}$.

Proof. Define $\phi : P_f(F) \longrightarrow S$ by: for $A \in P_f(F)$, $\phi(A) = \vee_{a\in A} f(a)$. Then for every $A, B \in P_f(F)$, $\phi(AB) = \vee_{a\in A, b\in B} f(ab) = \vee_{a\in A, b\in B} f(a)f(b) = (\vee_{a\in A} f(a))(\vee_{b\in B} f(b)) = \phi(A)\phi(B)$, and if $A \leqslant B$, then $\phi(A) = \vee_{a\in A} f(a) \leqslant \vee_{b\in B} f(b) = \phi(B)$ shows that ϕ is an ordered semigroup homomorphism. Also $\phi \circ l = f$. $\square$

Lemma 3.3. *In an idempotent ordered semigroup S, $a^m \leqslant a^n$ for every $a \in S$ and $m, n \in \mathbb{N}$ with $m \leqslant n$.*

Every idempotent ordered semigroup S is completely regular and hence $\mathcal{J}$ is the least complete semilattice congruence on S, by [Lemma 4.13, [1]]. In an idempotent ordered semigroup S, the Green's relation $\mathcal{J}$ can equivalently be expressed as: for $a, b \in S$,

$$a\mathcal{J}b \text{ if there are } x, y, u, v \in S \text{ such that } a \leqslant axbya \text{ and } b \leqslant buavb.$$

Now we characterize the $\mathcal{J}-$class in an idempotent ordered semigroup.

Definition 3.4. An idempotent ordered semigroup S is called *rectangular* if for all $a, b \in S$, there are $x, y \in S$ such that $a \leqslant axbya$.

Example 3.5. $(\mathbb{N}, \cdot, \leqslant)$ is a rectangular idempotent ordered semigroup, whereas if we define $a\ o\ b = \min\{a, b\}$ *for all* $a, b \in \mathbb{N}$ then $(\mathbb{N}, \circ, \leqslant)$ is an idempotent ordered semigroup but not rectangular.

Also we have the following equivalent conditions.

Lemma 3.6. *Let S be an idempotent ordered semigroup. Then the following conditions are equivalent:*

1. *S is rectangular;*
2. *for all $a, b \in S$, there is $x \in S$ such that $a \leqslant axbxa$;*
3. *for all $a, b, c \in S$ there is $x \in S$ such that $ac \leqslant axbxc$.*

Proof. (1) $\Rightarrow$ (3): Let $a, b, c \in S$. Then there are $x, y \in S$ such that $a \leqslant axbya$. This implies $ac \leqslant axbyac \leqslant ax(bya)(bya)c \leqslant (axbyab)(axbyab)yac \leqslant a(axbyabya)b(axbyabya)c \leqslant atbtc$, where $t = axbyabya \in S$.

(3) $\Rightarrow$ (2): Let $a, b \in S$. Then there is $x \in S$ such that $a^2 \leqslant axbxa$. Then $a \leqslant a^2$ implies that $a \leqslant axbxa$.

(2) $\Rightarrow$ (1): This follows directly. □

As we can expect, we show that the equivalence classes in an idempotent ordered semigroup S determined by $\mathcal{J}$ are rectangular.

Theorem 3.7. *Every idempotent ordered semigroup is a complete semilattice of rectangular idempotent ordered semigroups.*

Proof. Let S be an idempotent ordered semigroup. Then $\mathcal{J}$ is the least complete semilattice congruence on S. Now consider a $\mathcal{J}$-class $(c)_{\mathcal{J}}$ for some $c \in S$. Since $\mathcal{J}$ is a complete semilattice congruence, $(c)_{\mathcal{J}}$ is a subsemigroup of S. Let $a, b \in (c)_{\mathcal{J}}$. Then there is $x \in S$ such that $a \leqslant axbxa$, which implies that $a \leqslant a(axb)b(bxa)a$, that is, $a \leqslant aubva$ where $u = axb$ and $v = bxa$. Also the completeness of $\mathcal{J}$ implies that $(a)_{\mathcal{J}} = (a^2xbxa)_{\mathcal{J}} = (axb)_{\mathcal{J}} = (bxa)_{\mathcal{J}}$, and $u, v \in (c)_{\mathcal{J}}$. Thus $(c)_{\mathcal{J}}$ is a rectangular idempotent ordered semigroup. □

Definition 3.8. An idempotent ordered semigroup S is called *left* (*right*) *zero* if for every $a, b \in S$, there exists $x \in S$ such that $a \leqslant axb$ ($a \leqslant bxa$).

Proposition 3.9. *An idempotent ordered semigroup is left zero if and only if it is left simple.*

Proof. First suppose that S is a left zero idempotent ordered semigroup and $a \in S$. Then for any $b \in S$, there is $x \in S$ such that $b \leqslant bxa$, which shows that $b \in (Sa]$. Thus $S = (Sa]$ and hence S is left simple.

Conversely, assume that S is left simple. So for every $a, b \in S$, there is $s \in S$ such that $a \leqslant sb$. Then $a \leqslant a^2$ gives that $a^2 \leqslant asb$. Thus S is a left zero idempotent ordered semigroup. □

Lemma 3.10. *In an idempotent ordered semigroup S, the following conditions are equivalent:*

1. *For all $a, b \in S$, there is $x \in S$ such that $ab \leqslant abxba$.*
2. *For all $a, b \in S$, there is $x \in S$ such that $ab \leqslant axbxa$.*

3 *For all $a, b \in S$, there is $x, y \in S$ such that $ab \leqslant axbya$.*

Proof. (1) $\Rightarrow$ (3): This follows directly.

(3) $\Rightarrow$ (2): This is similar to the Lemma 3.6.

(2) $\Rightarrow$ (1): Let $a, b \in S$. Then there is $x \in S$ such that $bab \leqslant baxbxba$. Now since $ab \leqslant ababab$, we have $ab \leqslant ab(abaxbx)ba$. □

Definition 3.11. An idempotent ordered semigroup S is called *left regular* if for every $a, b \in S$ there is $x \in S$ such that $ab \leqslant axbxa$.

Theorem 3.12. *An idempotent ordered semigroup S is left regular if and only if $\mathcal{L} = \mathcal{J}$ is the least complete semilattice congruence on S.*

Proof. First we assume that S is left regular. Let $a, b \in S$ be such that $a\mathcal{J}b$. Then there are $u, v, x, y \in S$ such that $a \leqslant ubv$ and $b \leqslant xay$. Since S is left regular, there are $s, t \in S$ such that $bv \leqslant bsvsb$ and $ay \leqslant atyta$. Then $a \leqslant ubsvsb$ and $b \leqslant xatyta$; which shows that $a\mathcal{L}b$. Thus $\mathcal{J} \subseteq \mathcal{L}$. Again $\mathcal{L} \subseteq \mathcal{J}$ on every ordered semigroup and hence $\mathcal{L} = \mathcal{J}$. Since every idempotent ordered semigroup is completely regular, it follows that $\mathcal{L}$ is the least complete semilattice congruence on S, by [Theorem 5.10, [1]]

Conversely, let $\mathcal{L}$ is the least complete semilattice congruence on S. Consider $a, b \in S$. Then $ab\mathcal{L}ba$ implies that $ab \leqslant xba$ for some $x \in S$. This implies that

$$ab \leqslant abab \leqslant abxba.$$

Thus S is a left regular idempotent ordered semigroup, by Lemma 3.10. □

Theorem 3.13. *Let S be an idempotent ordered semigroup. Then the following conditions are equivalent:*

1. *S is left regular;*
2. *S is a complete semilattice of left zero idempotent ordered semigroups;*
3. *S is a semilattice of left zero idempotent ordered semigroups.*

Proof. (1) $\Rightarrow$ (2): In view of Theorem 3.12, it is sufficient to show that each $\mathcal{L}$-class is a left zero idempotent ordered semigroup. Let L be an $\mathcal{L}$-class and $a, b \in L$. Then L is a subsemigroup, since $\mathcal{L}$ is a semilattice congruence. Since $a\mathcal{L}b$ there is $x \in S$ such that $a \leqslant xb$. This implies that $a \leqslant a^3 \leqslant a^2xb \leqslant a^2xb^2 \leqslant aub$, where $u = axb$.

By the completeness of $\mathcal{L}$, $a \leqslant xb$ implies that $(a)_{\mathcal{L}} = (axb)_{\mathcal{L}}$, and hence $u \in L$. Thus S is left zero idempotent ordered semigroup.

(2) $\Rightarrow$ (3): This implication is trivial.

(3) $\Rightarrow$ (1): Let ρ be a semilattice congruence on S such that each ρ-class is a left zero idempotent ordered semigroup. Consider $a, b \in S$. Then ab, $ba \in (ab)_\rho$ shows that there is $s \in (ab)_\rho$ such that $ab \leqslant absba \leqslant absbsba \leqslant a(bsb)b(bsb)a$. Hence S is left regular. □

Lemma 3.14. *Let S be an idempotent ordered semigroup. Then the following conditions are equivalent:*

1. *S is $\mathcal{H}$-commutative;*
2. *for all $a, b \in S$, $ab \in (baS] \cap (Sba]$;*
3. *S is a complete semilattice of t-simple idempotent ordered semigroups;*
4. *S is a semilattice of t-simple idempotent ordered semigroups.*

Proof. (1) $\Rightarrow$ (2): Consider $a, b \in S$. Since S is $\mathcal{H}-$ commutative, there is $u \in S$ such that $ab \leqslant bua$. Also for $u, a \in S$, $ua \leqslant asu$ for some $s \in S$. Thus $ab \leqslant basu$, which shows that $ab \in (baS]$. Similarly $ab \in (Sba]$. Hence $ab \in (baS] \cap (Sba]$.

(2) $\Rightarrow$ (3): Suppose that J be an $\mathcal{J}$-class in S and $a, b \in J$. Since J is rectangular there is $x \in J$ such that $a \leqslant axbxa$. Also by the given condition (2) there is $u \in J$ such that $bxa \leqslant xaub$. So $a \leqslant ax^2aub \leqslant vb$, where $v = ax^2au$. Since $\mathcal{J}$ is a complete semilattice congruence on S, $(a)_{\mathcal{J}} = (a^2x^2aub)_{\mathcal{J}} = (ax^2au)_{\mathcal{J}} = (v)_{\mathcal{J}}$. So $v \in J$. This shows that J is left simple. Similarly it can be shown that J is also right simple. Thus S is a complete semilattice of t-simple idempotent ordered semigroups.

(3) $\Rightarrow$ (4): This follows trivially.

(4) $\Rightarrow$ (1): Let S be the semilattice Y of t-simple idempotent ordered semigroups $\{S_\alpha\}_{\alpha \in Y}$ and ρ be the corresponding semilattice congruence on S. Then there are $\alpha, \beta \in Y$ such that $a \in S_\alpha$ and $b \in S_\beta$. Then $ba, ab \in S_{\alpha\beta}$. Since $S_{\alpha\beta}$ is t-simple, $ab \leqslant xba$ for some $x \in S_{\alpha\beta}$. Now for $x, ba \in S_{\alpha\beta}$ there is $y \in S_{\alpha\beta}$ such that $x \leqslant bay$. This finally gives $ab \leqslant bta$, where $t = ayb$. □

Definition 3.15. An idempotent ordered semigroup $(S, ., \leqslant)$ is called *weakly commutative* if for any $a, b \in S$ there exists $u \in S$ such that $ab \leqslant bua$.

Theorem 3.16. *For an idempotent ordered semigroup S, the followings are equivalent:*

1. *S is weakly commutative;*
2. *for any $a, b \in S,\ ab \in (baS] \cap (sba]$;*
3. *S is complete semilattice of left and right simple idempotent ordered semigroups.*

Proof. (1) $\Rightarrow$ (2): Let $a, b \in S$. Then there exists $u \in S$ such that $ab \leqslant bua$, also for $u, a \in S$, there exists $z \in S$ such that $ua \leqslant azu$. Thus $ab \leqslant bua \leqslant baza\ for\ za \in S$. So $ab \leqslant (baS]$. Similarly $ab \in (Sba]$. Hence $ab \in (baS] \cap (sba]$.

(2) $\Rightarrow$ (3): Since S is an idempotent ordered semigroup, by Theorem 3.7 we have ρ is a complete semilattice congruence. We now have to show that, for each $z \in S, J = (z)_\rho$ is left and right simple. For this let us choose $a, b \in J$. Then there exists $x, y \in S$ such that $a \leqslant axbya$. So from the given condition $bya \in (syab]$ and therefore there is $s_1 \in S$ such that $bya \leqslant s_1yab$. Therefore $a \leqslant axs_1yab$. Now since ρ is complete semilattice congruence on S, we have $(a)_\rho = (a^2xs_1yab)_\rho = (axs_1yab)_\rho = (axs_1ya)_\rho$. Thus $a \leqslant ub$, where $u = axs_1ya \in J$. Hence J is left simple and similarly it is right simple.

(3) $\Rightarrow$ (1): Let S is complete semilattice Y of left and right simple idempotent ordered semigroups $\{S_\alpha\}_{\alpha \in Y}$. Thus $S = \{S_\alpha\}_{\alpha \in Y}$. Take $a, b \in S$. Then there are $\alpha, \beta \in Y$ such that $a \in S_\alpha$ and $b \in S_\beta$. Thus $ab \in S_{\alpha\beta}$. So $ab, ba \leqslant S_{\alpha\beta}$. Then there are $u, v \in S_{\alpha\beta}$ such that $ab \leqslant uba$ and $ab \leqslant bav$ implies $ab \leqslant ab^2 \leqslant bta$, where $t = avub$. Hence S is weakly commutative. This completes the proof. □

Definition 3.17. An idempotent ordered semigroup $(S, \cdot, \leqslant)$ is called *normal* if for any $a, b, c \in S$, there exists $x \in S$ such that $abca \leqslant acxba$.

Theorem 3.18. *For an idempotent ordered semigroup S, the followings are equivalent:*

1. *S is normal;*
2. *aSb is weakly commutative, for any $a, b \in S$;*
3. *aSa is weakly commutative, for any $a \in S$.*

Proof. (1) $\Rightarrow$ (2): Consider $axb, ayb \in aSb\ for\ x, y \in S$. As S is normal, $\exists u, v \in S$ such that $(axb)(ayb) \leqslant (axb)(ayb)(axb)(ayb) \leqslant aybuxba^2xbayb$, for $xba, yb \in S \leqslant (ayb)uxb(bay)v(a^2x)b$, for $a^2x, bay \in S \leqslant (ayb)(uxb^2ayva)(axb)$. This implies $(axb)(ayb) \leqslant (ayb)t(axb) \leqslant (ayb)(ayb)t(axb)(axb)$, $t = uxb^2ayva$ and thus $(axb)(ayb) \leqslant aybsaxb$, where $s = aybtaxb \in aSb$. Thus aSb is weakly commutative.

(2) $\Rightarrow$ (3): This is obvious by taking $b = a$.

(3) $\Rightarrow$ (1): Let $a, b, c \in S$. Then $abca, aca \in aSa$. Since aSa is weakly commutative. Then there is $s \in aSa$ such that $(abca)aca \leqslant acasaabca$. Now for $aba, abca \in aSa$, there is $t \in aSa$ such that $abaabca \leqslant abcataba$. Thus $abca \leqslant (abca)(abca) \leqslant abca^2ca^2bca \leqslant abca^2ca^2ba^2bca = (abcaaca)(abaabca) \leqslant (acasa^2ca)(abcataba) \leqslant acuba$; where $u = asa^2bca^2bcata \in S$. Hence S is normal. □

Definition 3.19. An idempotent ordered semigroup $(S, \cdot, \leqslant)$ is called *left normal* (*right normal*) if for any $a, b, c \in S$, there exists $x \in S$ such that $abc \leqslant acxb$ ($abc \leqslant bxac$).

Theorem 3.20. *Let S be a left normal idempotent ordered semigroup, then*

1. *$\mathcal{L}$ is the least complete semilattice congruence on S;*
2. *S is a complete semilattice of LZ-idempotent ordered semigroups.*

Proof. (1): Let $a, b \in S$ such that $a\rho b$. Then there are $x, y, u, v \in S$ such that

$$a \leqslant a(xbya), b \leqslant b(uavb). \tag{1}$$

Since S is left normal, we have for $x, b, ya \in S, xbya \leqslant xyatb$ for some $t \in S$. Similarly there is $s \in S$ such that $uavb \leqslant uvbsa$. So from (1), $a \leqslant (axyat)b$ and $b \leqslant (buvbs)a$. Hence $a\mathcal{L}b$. Thus $\rho \subseteq \mathcal{L}$.

Again, let $a, b \in S$ such that $a\mathcal{L}b$. Thus there are $u, v \in S$ such that $a \leqslant ub$ and $b \leqslant va$. Also we have $a \leqslant a^3 = aaa \leqslant auba \leqslant aubba$ for some $u, b \in S$. Therefore $a\rho b$. Thus $\mathcal{L} \subseteq \rho$. Thus $\mathcal{L} = \rho$.

(2): Here we are only to proof that each $\mathcal{L}$-class is a left zero. For this let $\mathcal{L}$-class $(x)_{\mathcal{L}} = L$, (say) for some $x \in S$. Clearly $(x)_{\mathcal{L}}$ is a subsemigroup of S. Take $a, b \in L$. Then $y, z \in S$ such that $a \leqslant yb, b \leqslant za$. Since S is left normal, there is $t \in S$ such that $a \leqslant yb \leqslant (yb)b \leqslant yzab$.

This implies $a \leqslant a^2 \leqslant a(ayzb)b$. Thus $(a)_{\mathcal{L}} = (a^2yzb)_{\mathcal{L}} = (ayzb)_{\mathcal{L}}$. Therefore L is left zero. Hence S is a complete semilattice of left zero idempotent ordered semigroups. □

Theorem 3.21. *Let S be a idempotent ordered semigroup, then S is normal if and only if $\mathcal{L}$ is right normal band congruence and $\mathcal{R}$ is left normal band congruence.*

Proof. First we shall see that $\mathcal{L}$ is left congruence on S. For this let us take $a, b \in S$ such that $a\mathcal{L}b$ and $c \in S$. Then there is $x, y \in S$ such that $a \leqslant xb, b \leqslant ya$. Now as S is normal idempotent ordered semigroup, $ca \leqslant cxb \leqslant cxbcxb \leqslant cxbx(s_1)cb$ for some $s_1 \in S$. Thus $a \leqslant s_2cb$, where $s_2 = cxbxs_1 \in S$. Again $cb \leqslant s_4ca$ where $s_4 = cyays_3 \in S$. So $ca\mathcal{L}cb$. It finally shows that $\mathcal{L}$ is congruence on S. Similarly it can be shown that $\mathcal{R}$ is congruence on S.

Next consider that $a, b, c \in S$ are arbitrary. Then since S is a normal idempotent ordered semigroup, $abc \leqslant abcabc \leqslant abcbt_1ac \leqslant acb(t_1t_2bac)$ for some $acbt_1t_2 \in S$. Also $bac \leqslant bacbac \leqslant bacat_3bc \leqslant (bct_3t_4abc)$ for some $bct_3t_4 \in S$. So $abc\mathcal{L}bac$. Similarly $abc\mathcal{R}acb$. This two relations respectively shows that $\mathcal{L}$ is right normal band congruence and $\mathcal{R}$ is left normal band congruence.

Conversely, suppose that $\mathcal{L}$ is a right normal band congruence and $\mathcal{R}$ is a left normal band congruence. Consider a, b, and $c \in S$. Then $abc\mathcal{R}acb$ *and* $bca\mathcal{L}cba$. Then $\exists x_1, x_2 \in S$ such that

$$abc \leqslant (acb)x_1 \text{ and } bca \leqslant x_2cba.$$

Now then $abc \leqslant (abc)bca \leqslant (acb)x_1bca \leqslant ac(bx_1x_2c)ba$ for some $bx_1x_2c \in S$. Hence S is an idempotent ordered semigroup. □

References

[1] **A.K. Bhuniya and K. Hansda**, *On completely regular and Clifford ordered semigroups*, Afrika Math., **31** (2020), 1029 – 1045.

[2] **K. Hansda**, *Regularity of subsemigroups generated by ordered idempotents*, Quasigroups and Related Systems, **22** (2014), 217 – 222.

[3] **N. Kehayopulu**, *Note on Green's relation in ordered semigroups*, Math. Japonica, **36** (1991), 211 – 214.

[4] **T. Saito**, *Ordered idempotent semigroups*, J. Math. Soc. Japan., **14** (1962), 150 – 169.

Received July 01, 2023

Department of Mathematics, Visva Bharati University, Santiniketan, Bolpur - 731235, West Bengal, India
E-mails: susmita.mallick3@gmail.com, kalyan.hansda@visva-bharati.ac.in

Quasigroups and Related Systems **32** (2024), 69 − 94

https://doi.org/10.56415/qrs.v32.07

Probabilistic groupoids

Smile Markovski and Lidija Goračinova-Ilieva

Abstract. Algebraic structures are commonly used as a tool in treatments of various processes. But their exactness reduces the opportunity of their application in nondeterministic environment. On the other hand, probability theory and fuzzy logic do not provide convenient means for expressing the result of combining elements in order to produce new ones. Moreover, these theories are not developed to "measure" algebraic properties. Therefore, we propose a new concept which relies both on universal algebra and probability theory.

We introduce probabilistic mappings, and by them we define the notion of a probabilistic algebra. Let A and B be non-empty sets, and let $\mathcal{D}_B$ be the set of all probability distributions on B. A probabilistic mapping from A to B is a mapping $h : A \to \mathcal{D}_B$. Let A be a set, $n \in \mathbb{N}$, and let $A^n = \{(a_1, a_2, \dots, a_n) |\ a_i \in A,\ i = 1, 2, \dots, n\}$ be the n-th power of A. Every probabilistic mapping from A^n to A is a probabilistic (n-ary) operation on A. A pair (A, F) of a set A and a family F of probabilistic operations on A is called a probabilistic algebra. When $F = \{f\}$ has one binary operation, then the probabilistic algebra (A, f) is a probabilistic groupoid. "Ordinary" groupoids are just a special type of probabilistic ones. Basic properties of probabilistic groupoids and some classes of probabilistic groupoids (with units, commutative, associative, idempotent, with cancellation, with inverses, quasigroups, groups) are treated in this paper. Here we consider only the finite case.

1. Probabilistic mappings

Let A and B be non-empty finite sets, and denote by $\mathcal{D}_B$ the set of all probability distributions on B, that is

$$\mathcal{D}_B = \{f |\ f : B \to \mathbb{R}, f(b) \geqslant 0 \text{ for } b \in B, \sum_{b \in B} f(b) = 1\}.$$

2010 Mathematics Subject Classification: 00A05, 08A99, 60B99

Keywords: probabilistic mapping; probabilistic groupoid; probabilistic group; probabilistic semigroup; probabilistic quasigroup; idempotent, cancellative, inversible probabilistic groupoid.

When $B = \{b_1, b_2, \dots, b_n\}$ is a finite set, a probability distribution $f : B \to \mathbb{R}$ can be also denoted, as usual, by the set of images $\{f(b_1), f(b_2), \dots, f(b_n)\}$.

For every mapping h from A to $\mathcal{D}_B$ we say that it is a *probabilistic mapping* from A to B. We denote such a mapping by $h : A \looparrowright B$. If $h(a) = f$ for some $a \in A$, then we write $f = h_a$, and when $h_a(b) = p,\ p \in [0,1]$, we say that the probability of mapping the element $a \in A$ into $b \in B$ is p, or that b is an image of a with probability p. The element a is called a *pre-image* of b with probability $p = h_a(b)$. Given a fixed element $b \in B$, each element of A is a pre-image of b with some probability, but the set $h^{-1}\{b\} = \{h_a(b) |\ a \in A\}$ is not necessarily a probability distribution on A.

Example 1.1. $A = \{1,2,3\},\quad B = \{a,b,c,d\},\quad h : A \looparrowright B$:

$$h_1 = \begin{pmatrix} a & b & c & d \\ 0.3 & 0 & 0.7 & 0 \end{pmatrix},\ h_2 = \begin{pmatrix} a & b & c & d \\ 0 & 0 & 0 & 1 \end{pmatrix},\ h_3 = \begin{pmatrix} a & b & c & d \\ 0.2 & 0 & 0.2 & 0.6 \end{pmatrix}.$$

In order to get the sets $\{h_a(b) |\ a \in A\}$, for every $b \in B$, to be probability distributions on A a necessary, but not sufficient, condition is to have the equality $|A| = |B|$. An example is given below.

Example 1.2. $A = \{1,2,3\},\quad B = \{a,b,c\},\quad s,h : A \looparrowright B$:

$$s_1 = \begin{pmatrix} a & b & c \\ 0.2 & 0.5 & 0.3 \end{pmatrix},\quad s_2 = \begin{pmatrix} a & b & c \\ 0.6 & 0.4 & 0 \end{pmatrix},\quad s_3 = \begin{pmatrix} a & b & c \\ 0.2 & 0.1 & 0.7 \end{pmatrix};$$

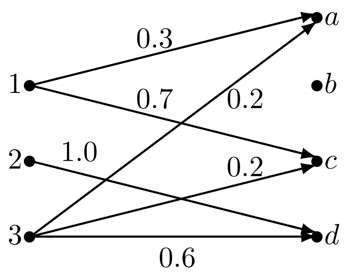
$$h_1 = \begin{pmatrix} a & b & c \\ 0.2 & 0.5 & 0.3 \end{pmatrix},\quad h_2 = \begin{pmatrix} a & b & c \\ 0.2 & 0.5 & 0.3 \end{pmatrix},\quad h_3 = \begin{pmatrix} a & b & c \\ 0.2 & 0.1 & 0.7 \end{pmatrix}.$$

The sets $s^{-1}\{a\} = \{0.2, 0.6, 0.2\}$, $s^{-1}\{b\} = \{0.5, 0.4, 0.1\}$, $s^{-1}\{c\} = \{0.3, 0, 0.7\}$ are probability distributions on A, while the set $h^{-1}\{a\} = \{0.2, 0.2, 0.2\}$ is not.

Note that every probabilistic mapping from A to B is actually a family of distributions on B indexed by the elements of A. In spite of the fact that this is a familiar notion (discrete stochastic process), the main idea is to consider some algebraic properties which are satisfied with certain "probability". Therefore, we start with this concept and appropriate new terminology.

2. Representations of probabilistic mappings

Besides using the usual representations of mappings, in the case when the sets are finite (and not having many elements), weighted digraphs, stochastic matrices and tables are particularly convenient for expressing probabilistic mappings. In what follows, we give the graph, matrix and table representation of the probability mapping from Example 1.



$$\Pi = \begin{bmatrix} 0.3 & 0 & 0.7 & 0 \\ 0 & 0 & 0 & 1 \\ 0.2 & 0 & 0.2 & 0.6 \end{bmatrix}$$

h	h_1	h_2	h_3
a	0.3	0	0.2
b	0	0	0
c	0.7	0	0.2
d	0	1	0.6

3. Compositions of probabilistic mappings

Let $f : A \looparrowright B$ and $g : B \looparrowright C$ be probabilistic mappings. Define *composition* of f and g to be the mapping $h = g \bullet f$ which maps every element a of A into a real-valued function h_a on C, determined by the rule

$$h_a(c) = \sum_{b \in B} f_a(b) g_b(c),$$

for every $c \in C$.

Theorem 3.1. *A composition of probabilistic mappings is a probabilistic mapping.*

Proof. Let $f : A \looparrowright B$ and $g : B \looparrowright C$ be probabilistic mappings, and h be the composition of f and g. Then for the image h_a of an arbitrary element

a of A, we obtain

$$\sum_{c\in C} h_a(c) = \sum_{c\in C}\sum_{b\in B} f_a(b)g_b(c) = \sum_{b\in B}\Big(f_a(b)\sum_{c\in C} g_b(c)\Big) = \sum_{b\in B} f_a(b)\cdot 1 = 1.$$

Clearly $h_a(c) \geqslant 0$ for each $c \in C$, hence for every $a \in A$, h_a is a probability distribution on C, so h is a probabilistic mapping, $h : A \looparrowright C$. □

By the definition of the notion composition of probabilistic mappings and the matrix representation, we get the following result.

Theorem 3.2. *Let A, B and C be finite sets, $f : A \looparrowright B$ and $g : B \looparrowright C$. If Π_1 and Π_2 are the corresponding matrices of f and g, respectively, then their product $\Pi_1 \cdot \Pi_2$ is the matrix representation of the composition $g \bullet f$.*

Example 3.3. $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$, $C = \{u, v\}$:

$$\Pi_1(A \looparrowright B) = \begin{bmatrix} 0.3 & 0 & 0 & 0.7 \\ 0 & 0 & 0 & 1 \\ 0.2 & 0.1 & 0.4 & 0.3 \end{bmatrix}, \qquad \Pi_2(B \looparrowright C) = \begin{bmatrix} 0.8 & 0.2 \\ 1 & 0 \\ 0 & 1 \\ 0.6 & 0.4 \end{bmatrix},$$

$$\Pi_1 \cdot \Pi_2(A \looparrowright C) = \begin{bmatrix} 0.66 & 0.34 \\ 0.6 & 0.4 \\ 0.44 & 0.56 \end{bmatrix}.$$

Theorem 3.4. *Let $f : A \looparrowright B, g : B \looparrowright C$ and $h : C \looparrowright D$. Then $h \bullet (g \bullet f) = (h \bullet g) \bullet f$.*

Proof. Let $a \in A$. For each $x \in D$ we have

$$\begin{aligned}(h \bullet (g \bullet f))_a(x) &= \sum_{c\in C}(g \bullet f)_a(c)h_c(x) = \sum_{c\in C}\Big(\sum_{b\in B} f_a(b)g_b(c)\Big)h_c(x) \\ &= \sum_{b\in B}\sum_{c\in C} f_a(b)g_b(c)h_c(x) = \sum_{b\in B} f_a(b)\Big(\sum_{c\in C} g_b(c)h_c(x)\Big) \\ &= \sum_{b\in B} f_a(b)(h \bullet g)_b(x) = ((h \bullet g) \bullet f)_a(x).\end{aligned}$$

□

4. Definition of probabilistic groupoids

Let $A \neq \emptyset$ and $\mathbb{N} = \{1, 2, \dots\}$ be the set of natural numbers. Then, for $n \in \mathbb{N}$, the n^{th} direct power of A is the set of ordered n-tuples $A^n = \{(a_1, a_2, \dots, a_n) | a_i \in A, i = 1, 2, \dots, n\}$. We take by definition $A^0 = \{\emptyset\}$.

Every probabilistic mapping $f : A^n \looparrowright A$, $n \in \mathbb{N} \cup \{0\}$, is said to be an *$n$-ary probabilistic operation on A*. The pair $(A, \mathcal{F})$ of a nonempty set A and a family $\mathcal{F}$ of probabilistic operations on A is called a *probabilistic algebra*. In the case when $\mathcal{F}$ consists of only one binary probabilistic operation $g : A \times A \looparrowright A$, we say that the probabilistic algebra is a *probabilistic groupoid*, denoted by (A, g), or just by A when g is known. We also use the notation $g_{a,b}$ for the probability distribution $g(a, b)$. If $g_{a,b}(c) = p$, then we say that the *probability the product of a and b to be c is p*.

The class of all "ordinary" groupoids can be considered as a subclass of the class of probabilistic groupoids. Namely, for $a \in A$, let $\epsilon_a \in \mathcal{D}_A$ be the probability distribution which is determined by

$$\epsilon_a(x) = \begin{cases} 1 : & x = a, \\ 0 : & x \neq a. \end{cases}$$

Denote by $\mathcal{D}_0$ the subset of $\mathcal{D}_A$ which consists of such functions, that is $\mathcal{D}_0 = \{\epsilon_a \in \mathcal{D}_A |\ a \in A\}$. Then an "ordinary" groupoid is the pair (A, g), where $g : A \times A \looparrowright \mathcal{D}_0$, under the identification $\epsilon_c \equiv c$.

For $A = \{a\}$ we have that $g : A \times A \to D_{\{a\}}$ is just $g_{a,a} = \epsilon_a$, so the probabilistic groupoid $(\{a\}, g)$ is in fact the (ordinary) trivial groupoid.

If $B \subseteq A$, we denote by $ext\mathcal{D}_B$ the subset of $\mathcal{D}_A$ determined by:

$$f \in ext\mathcal{D}_B \Leftrightarrow f(x) = 0 \text{ for every } x \in A \setminus B.$$

In the sequel we identify the distribution $ext\mathcal{D}_B$ on the set A and the distribution $\mathcal{D}_B$ on the set B. Clearly,

$$B_1 \subseteq B_2 \subseteq A \Rightarrow \mathcal{D}_{B_1} \subseteq \mathcal{D}_{B_2} \subseteq \mathcal{D}_A.$$

Unlike in the case of ordinary groupoids, for finite $|A| > 1$, there are infinitely many probabilistic groupoids. For instance, when $A = \{a, b\}$, one is given by

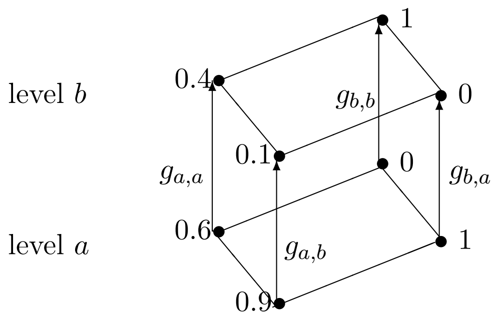
$$\begin{array}{c|cc} g & a & b \\ \hline a & g_{a,a} & g_{a,b} \\ b & g_{b,a} & g_{b,b} \end{array}, \quad \text{where}$$

$$g_{a,a} = \begin{pmatrix} a & b \\ 0.6 & 0.4 \end{pmatrix}, \qquad g_{b,a} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} = \epsilon_a,$$
$$g_{a,b} = \begin{pmatrix} a & b \\ 0.9 & 0.1 \end{pmatrix}, \qquad g_{b,b} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \epsilon_b.$$

This probabilistic groupoid can be presented in more convenient way by using only one table, as follows:

g	$g_{a,a}$	$g_{a,b}$	$g_{b,a}$	$g_{b,b}$
a	0.6	0.9	1	0
b	0.4	0.1	0	1

Finite probabilistic groupoids can be represented by "cubes" whose elements belong to $[0,1]$ and the sum of the elements along the vertical axes are equal to 1. The previous groupoid can be presented as follows.



5. Probabilistic subgroupoids

Let (A, g^A) and (B, g^B) be probabilistic groupoids, and $B \subseteq A$. If for every $a, b \in B$ we have that $g^B_{a,b} = g^A_{a,b}|_B$ ($g^A_{a,b}|_B$ is the restriction of $g^A_{a,b}$ on B, i.e., $g^B_{a,b} \in ext\mathcal{D}_B$), then we say that (B, g^B) is a *probabilistic subgroupoid* of (A, g^A).

Let (A, g) be a probabilistic groupoid and $B \subseteq A$. Then B is said to be a *closed subset* of A if $g_{a,b}(c) \neq 0$ implies $c \in B$, for every $a, b \in B$.

Theorem 5.1. *Let (A, g) be a probabilistic groupoid and $B \subseteq A$. Then B is a probabilistic subgroupoid of A if and only if B is a closed subset of A.*

Proof. Let B be a probabilistic subgroupoid of A, and $a, b \in B$ be arbitrary. Assume that there is $c \in A \backslash B$, such that $g_{a,b}(c) = p > 0$. Then

$$1 = \sum_{x \in A} g_{a,b}(x) = \sum_{x \in A \backslash B} g_{a,b}(x) + \sum_{x \in B} g_{a,b}(x) \geqslant p + \sum_{x \in B} g_{a,b}(x) = p + 1 > 1,$$

a contradiction.

If B is a closed subset of A then, for every $a, b \in B$, we have that

$$\sum_{x \in B} g_{a,b}(x) = 1,$$

since

$$\sum_{x \in A} g_{a,b}(x) = 1 \text{ and } x \notin B \text{ implies } g_{a,b}(x) = 0.$$

Hence, B is a probabilistic subgroupoid of A. □

6. Some classes of probabilistic groupoids

sectionSome classes of probabilistic groupoids Here we define several classes of probabilistic groupoids, corresponding to some classes of ordinary groupoids.

6.1 Probabilistic groupoids with units

Let (A, g) be a probabilistic grou-poid. An element $l \in A$ ($r \in A$) is said to be a *left* (*right*) unit if

$$(\forall x \in A)\ g_{l,x} = \epsilon_x \quad \Big((\forall x \in A)\ g_{x,r} = \epsilon_x\Big),$$

that is, the probability of the product of l and x to be x is 1 (the probability of the product of x and r to be x is 1), for every element $x \in A$. (Note that this implies $g_{l,x}(y) = 0$ ($g_{x,r}(y) = 0$), for each $y \neq x$.)

Let $a \in A$ be an arbitrary element, and consider the set

$$L_a = \{g_{a,x}(x) |\ x \in A\} \quad \Big(R_a = \{g_{x,a}(x) |\ x \in A\}\Big).$$

Let ${p_a}^L = inf\ L_a$ $({p_a}^R = inf\ R_a)$. Then ${p_a}^L$ $({p_a}^R)$ is called the *probability of the left* (*right*) *neutrality of a*. The following property is obvious.

Proposition 6.1. *An element l is a left unit* (*a right unit*) *if and only if the probability of its left neutrality* (*right neutrality*) *is one.*

Proposition 6.2. *Let (A, g) be a probabilistic groupoid and let $a \in A$. Then the probability ${p_b}^R$ $({p_b}^L)$ of the right neutrality (left neutrality) of an arbitrary element $b \in A,\ b \neq a$, does not exceed $1 - {p_a}^L$ $(1 - {p_a}^R)$.* Proof. *Let $a \in A$ be fixed element and let $b \neq a \in A$ be arbitrary element. Then we have:*

$$\begin{aligned} {p_b}^R &= inf\{g_{x,b}(x) | x \in A\} \leqslant g_{a,b}(a) = 1 - \sum_{\substack{x \in A \\ x \neq a}} g_{a,b}(x) \\ &\leqslant 1 - g_{a,b}(b) \leqslant 1 - inf\{g_{a,x}(x) | x \in A\} = 1 - {p_a}^L. \qquad \Box \end{aligned}$$

As a consequence of Proposition 6.2, we obtain the following statement.

Corollary 6.3. *Let l (r) be a left unit (a right unit) of a probabilistic groupoid (A, g). Then the probability of the right neutrality (left neutrality) of any other element of A is 0.*

It is clear that a probabilistic groupoid does not have to possess a left unit, but if it has one, then it does not need to be a unique one; the same holds for the right units. However, like in the case of ordinary groupoids, a probabilistic groupoid can not have distinct left and right units.

Theorem 6.4. *Let (A, g) be a probabilistic groupoid and let l be its left unit and let r be its right unit. Then $l = r$.*

Proof. Assume that $l \neq r$. Since l is a left unit, we have that $g_{l,r}(r) = \epsilon_r(r) = 1$, and since r is a right unit, $g_{l,r}(l) = \epsilon_l(l) = 1$ also holds. But then

$$1 = \sum_{x \in A} g_{l,r}(x) \geqslant g_{l,r}(r) + g_{l,r}(l) = 2,$$

a contradiction. □

An element $e \in A$ which is both left and right unit is said to be a *unit* of a probabilistic groupoid (A, g).

Having in mind the Corollary 6.3, we have the following property.

Corollary 6.5. *Let e be the unit of a probabilistic groupoid (A, g). Then the probability of both left and right neutrality of any other element of A which is distinct of e is 0.*

6.2 Idempotent probabilistic groupoids

Let (A, g) be a probabilistic groupoid and $a \in A$. Then the number $p = g_{a,a}(a)$ is called the *probability of the idempotence of* a. The element a is said to be *idempotent* if $p = 1$.

Proposition 6.6. *Let e be the unit of a probabilistic groupoid (A, g). Then e is an idempotent element.*

Let $I = \{g_{x,x}(x) | x \in A\}$ be the set of the probabilities of idempotence of the elements of (A, g). Then $p^I = infI$ is called the *probability of the idempotence of the probabilistic groupoid* (A, g). Hence, the probability of the idempotence of any particular element is at least p^I. Probabilistic groupoid (A, g) is said to be *idempotent* if $p^I = 1$ (i.e., if all of its elements are idempotent ones).

6.3 Commutative probabilistic groupoids

Let $a, b \in A$, and for every $z \in A$ let $p^z_{a,b} = min\{g_{a,b}(z), g_{b,a}(z)\}$. Let

$$p_{a,b} = \sum_{z \in A} p^z_{a,b}.$$

Then we say that the elements a and b *commute with probability* $p_{a,b}$. The value of $p^{com} = inf\{p_{a,b} | a, b \in A\}$ is said to be the *probability of the commutativity of the probabilistic groupoid* (A, g). (A, g) is called a *commutative probabilistic groupoid* if all of its elements commute with probability one, that is if $p^{com} = 1$.

Theorem 6.7. *A probabilistic groupoid (A, g) is commutative if and only if*

$$(\forall a, b \in A)\ g_{a,b} = g_{b,a}.$$

Proof. Let (A, g) be commutative and $a, b \in A$. Then $p^{com} = 1$ implies

$$\sum_{z \in A} min\{g_{a,b}(z), g_{b,a}(z)\} = 1.$$

Let us assume that $g_{a,b} \neq g_{b,a}$. It means that $g_{a,b}(u) \neq g_{b,a}(u)$, for some $u \in A$. Without loss of generality we can take that $g_{a,b}(u) < g_{b,a}(u)$. Then we obtain

$$1=\sum_{z\in A} min\{g_{a,b}(z),g_{b,a}(z)\}=\sum_{\substack{z\in A\\ z\neq u}} min\{g_{a,b}(z),g_{b,a}(z)\}+min\{g_{a,b}(u),g_{b,a}(u)\}$$

$$\leqslant \sum_{\substack{z\in A\\ z\neq u}} g_{b,a}(z)+g_{a,b}(u)<\sum_{\substack{z\in A\\ z\neq u}} g_{b,a}(z)+g_{b,a}(u)=\sum_{z\in A} g_{b,a}(z)=1,$$

a contradiction.

Let $g_{a,b}=g_{b,a}$, for all $a,b\in A$. Hence, $g_{a,b}(z)=g_{b,a}(z)$, for every $z\in A$. Then

$$p_{a,b}=\sum_{z\in A} p^z_{a,b}=\sum_{z\in A} min\{g_{a,b}(z),g_{b,a}(z)\}=\sum_{z\in A} g_{a,b}(z)=1.$$

By $p_{a,b}=1$ for all $a,b\in A$, we get $p^{com}=inf\{p_{a,b}|a,b\in A\}=1$, that is, (A,g) is a commutative probabilistic groupoid. □

6.4 Composite products of probabilistic groupoids

Given a set $A=\{a_1,a_2,\ldots,a_n\}$, we define inductively *terms* over the set A as follows. Each element $x\in A$ is a term of length 1, the terms of length 2 are (xy), where $x,y\in A$, and if T_1 and T_2 are already defined terms of lengths l_1 and l_2, then (T_1T_2) is a term of length l_1+l_2. For instance, given $x,y,z,t\in A$, $x(yz),(xy)z$ are terms of length 3 (and also $z(tz),(tz)y,\ldots$), terms of length 4 are $t(x(yz)),t((xy)z),(x(yz))t,((xy)z)t,(xy)(zt)$ (and also $t(x(xx)),y((xt)t),(t(yz))x,\ldots$). (Here, we avoided the non-necessary outside brackets.)

For a probabilistic groupoid (A,g), to each term T over the set A of length at least 2, we associate a probability distribution g_T in an inductive way as follows. To each term ab, $a,b\in A$, of length 2 we associate the probability distribution $g_{a,b}$ (the product of a and b in the probabilistic groupoid (A,g)). To the terms $T=T_1T_2$ of length $l\geqslant 3$ we associate inductively a probability distribution $g_T=g_{T_1,T_2}$ over A as follows.

(1) If $T_1\in A$ then $g_{T_1,T_2}(z)=\sum_{u\in A} g_{T_1,u}(z)g_{T_2}(u)$.

(2) If $T_2\in A$ then $g_{T_1,T_2}(z)=\sum_{u\in A} g_{T_1}(u)g_{u,T_2}(z)$.

(3) If $T_1,T_2\notin A$ then $g_{T_1,T_2}(z)=\sum_{u\in A} g_{T_1,u}(z)g_{T_2}(u)$

$$= \sum_{u\in A}\big(\sum_{v\in A} g_{T_1}(v)g_{v,u}(z)\big)g_{T_2}(u).$$

Note that $g_{T_1,u}$ and g_{u,T_2} are probability distributions and that, by the inductive hypothesis, when T_1 (or T_2) is of length $\geqslant 2$, the probability distribution g_{T_1} (or g_{T_2}) is defined.

Theorem 6.8. *Let (A, g) be a probabilistic groupoid and let T be a term of length at least 2. Then g_T is a probability distribution on A.*

Proof. The claim is trivial when the length of T is 2. Let T be of length at least 3, i.e., $T = T_1T_2$. We use an induction of the length of the terms.

By the definition of g_T we have to consider three cases.

(1) Let $T_1 \in A$. Then we have

$$\sum_{z\in A} g_{T_1,T_2}(z) = \sum_{z\in A}\sum_{u\in A} g_{T_1,u}(z)g_{T_2}(u) =$$
$$= \sum_{u\in A} g_{T_2}(u)\sum_{z\in A} g_{T_1,u}(z) = \sum_{u\in A} g_{T_2}(u)\cdot 1 = 1.$$

(2) The case $T_2 \in A$ follows the steps of the case (1).

(3) Let $T_1, T_2 \notin A$. Then we have

$$\sum_{z\in A} g_{T_1,T_2}(z) = \sum_{z\in A}\big(\sum_{u\in A} g_{T_1,u}(z)g_{T_2}(u)\big)$$
$$= \sum_{u\in A} g_{T_2}(u)\big(\sum_{z\in A} g_{T_1,u}(z)\big) = \text{(by case (2), since } u \in A)$$
$$= \sum_{u\in A} g_{T_2}(u)\cdot 1 = 1.$$

□

Example 6.9. Let (A, g), where $A = \{a, b\}$, be a probabilistic groupoid given by the table

g	$g_{a,a}$	$g_{a,b}$	$g_{b,a}$	$g_{b,b}$
a	0.3	0.8	1	0.4
b	0.7	0.2	0	0.6

.

We have $g_{a,(a,a)} = \begin{pmatrix} a & b \\ 0.65 & 0.35 \end{pmatrix}$, since $g_{a,(a,a)}(z) = \sum_{u\in A} g_{a,u}(z)g_{a,a}(u)$ and then $g_{a,(a,a)}(a) = \sum_{u\in A} g_{a,u}(a)g_{a,a}(u) = 0.3\cdot 0.3 + 0.8\cdot 0.7 = 0.65$, $g_{a,(a,a)}(b) = \sum_{u\in A} g_{a,u}(b)g_{a,a}(u) = 0.7\cdot 0.3 + 0.2\cdot 0.7 = 0.35$.

One can also compute that $g_{(a,a),a} = \begin{pmatrix} a & b \\ 0.79 & 0.21 \end{pmatrix}$, $g_{(b,a),(a,b)} = \begin{pmatrix} a & b \\ 0.4 & 0.6 \end{pmatrix}$, and so on.

6.5 Associative probabilistic groupoids

Consider a probabilistic grou-poid (A, g). Let $a, b, c \in A$ and let $p^z_{a,b,c} = min\{g_{(a,b),c}(z), g_{a,(b,c)}(z)\}$, where

$$g_{(a,b),c}(z) = \sum_{u\in A} g_{(a,b)}(u) g_{u,c}(z), \quad g_{a,(b,c)}(z) = \sum_{u\in A} g_{a,u}(z) g_{(b,c)}(u).$$

Define

$$p_{a,b,c} = \sum_{z\in A} p^z_{a,b,c}$$

to be the *probability of the associativity of the elements a,b and c*, while the probability $p^{ass} = inf\{p_{a,b,c} | a, b, c \in A\}$ is referred to be the *probability of the associativity of the probabilistic groupoid* (A, g). A probabilistic groupoid is said to be *associative* (or a *probabilistic semigroup*) if $p^{ass} = 1$.

We prove the following statement in the same manner as Theorem 6.7.

Theorem 6.10. *A probabilistic groupoid (A, g) is associative if and only if*

$$(\forall a, b, c \in A) g_{a,(b,c)} = g_{(a,b),c}.$$

Proof. Let (A, g) be associative probabilistic groupoid, and assume that $g_{a,(b,c)} \neq g_{(a,b),c}$ for some $a, b, c \in A$. Consequently, there is a $u \in A$ such that $g_{a,(b,c)}(u) < g_{(a,b),c}(u)$ (the assumption $g_{a,(b,c)}(u) > g_{(a,b),c}(u)$ would cause negligible changes of the proof). Since $1 = p^{ass} = inf\{p_{x,y,z} | x, y, z \in A\}$, we obtain that $p_{a,b,c} = 1$. Then we have:

$$\begin{aligned} 1 = p_{a,b,c} &= \sum_{z\in A} p^z_{a,b,c} = \sum_{z\in A} min\{g_{(a,b),c}(z), g_{a,(b,c)}(z)\} \\ &= \sum_{z\neq u} min\{g_{(a,b),c}(z), g_{a,(b,c)}(z)\} + min\{g_{(a,b),c}(u), g_{a,(b,c)}(u)\} \\ &\leqslant \sum_{z\neq u} g_{(a,b),c}(z) + min\{g_{(a,b),c}(u), g_{a,(b,c)}(u)\} \\ &< \sum_{z\neq u} g_{(a,b),c}(z) + g_{(a,b),c}(u) = \sum_{z\in A} g_{(a,b),c}(z) = 1, \end{aligned}$$

a contradiction. Hence, $g_{a,(b,c)} = g_{(a,b),c}$ for all $a, b, c \in A$.

On the other hand, if $(\forall a, b, c \in A) g_{a,(b,c)} = g_{(a,b),c}$ holds in a probabilistic groupoid (A, g), then $p^z_{a,b,c} = g_{(a,b),c}(z) = g_{a,(b,c)}(z)$, for all $a, b, c \in A$, and every $z \in A$. Therefore, $\sum\limits_{z \in A} p^z_{a,b,c} = \sum\limits_{z \in A} p_{a,(b,c)}(z) = 1$, that is $p_{a,b,c} = 1$, for every $a, b, c \in A$. This implies $p^{ass} = inf\{p_{a,b,c} | a, b, c \in A\} = 1$, which means that (A, g) is an associative probabilistic groupoid. $\square$

Example 6.11. We will find all probabilistic semigroups of order 2. Let $A = \{a, b\}$ and

g	$g_{a,a}$	$g_{a,b}$	$g_{b,a}$	$g_{b,b}$
a	α_1	α_2	α_3	α_4
b	β_1	β_2	β_3	β_4

,

where $\alpha_i \geqslant 0,\ \beta_i \geqslant 0,\ \alpha_i + \beta_i = 1$. Since we want the associativity to be satisfied, i.e., $g_{(a,a),a}(z) = g_{a,(a,a)}(z),\ g_{(a,a),b}(z) = g_{a,(a,b)}(z),\ g_{(a,b),a}(z) = g_{a,(b,a)}(z), \dots\ \dots, g_{(b,b),b}(z) = g_{b,(b,b)}(z)$, for $z \in \{a, b\}$, we obtain the following equations with unknowns α_i and β_i:

$$\begin{aligned}
&\alpha_1\alpha_1 + \beta_1\alpha_3 = \alpha_1\alpha_1 + \alpha_2\beta_1, && \alpha_1\beta_1 + \beta_1\beta_3 = \beta_1\alpha_1 + \beta_2\beta_1,\\
&\alpha_1\alpha_2 + \beta_1\alpha_4 = \alpha_1\alpha_2 + \alpha_2\beta_2, && \alpha_1\beta_2 + \beta_1\beta_4 = \beta_1\alpha_2 + \beta_2\beta_2,\\
&\alpha_2\alpha_1 + \beta_2\alpha_3 = \alpha_1\alpha_3 + \alpha_2\beta_3, && \alpha_2\beta_1 + \beta_2\beta_3 = \beta_1\alpha_3 + \beta_2\beta_3,\\
&\alpha_2\alpha_2 + \beta_2\alpha_4 = \alpha_1\alpha_4 + \alpha_2\beta_4, && \alpha_2\beta_2 + \beta_2\beta_4 = \beta_1\alpha_4 + \beta_2\beta_4,\\
&\alpha_3\alpha_1 + \beta_3\alpha_3 = \alpha_3\alpha_1 + \alpha_4\beta_1, && \alpha_3\beta_1 + \beta_3\beta_3 = \beta_3\alpha_1 + \beta_4\beta_1,\\
&\alpha_3\alpha_2 + \beta_3\alpha_4 = \alpha_3\alpha_2 + \alpha_4\beta_2, && \alpha_3\beta_2 + \beta_3\beta_4 = \beta_3\alpha_2 + \beta_4\beta_2,\\
&\alpha_4\alpha_1 + \beta_4\alpha_3 = \alpha_3\alpha_3 + \alpha_4\beta_3, && \alpha_4\beta_1 + \beta_4\beta_3 = \beta_3\alpha_3 + \beta_4\beta_3,\\
&\alpha_4\alpha_2 + \beta_4\alpha_4 = \alpha_3\alpha_4 + \alpha_4\beta_4, && \alpha_4\beta_2 + \beta_4\beta_4 = \beta_3\alpha_4 + \beta_4\beta_4.
\end{aligned}$$

After simplification of the above equalities, two cases remain to be considered.

Case 1: $\alpha_4 \neq 0$ or $\beta_1 \neq 0$. Then we have $\alpha_2 = \alpha_3$ and $\beta_2 = \beta_3$, and the above system reduces to

$$\begin{aligned}
&\beta_1\alpha_4 = \alpha_2\beta_2,\\
&\alpha_1\beta_2 + \beta_1\beta_4 = \beta_1\alpha_2 + \beta_2\beta_2,\\
&\alpha_2\alpha_2 + \beta_2\alpha_4 = \alpha_1\alpha_4 + \alpha_2\beta_4.
\end{aligned}$$

After replacing β_i by $1 - \alpha_i$ we get that the last system reduces to one equation

$$\alpha_4(1 - \alpha_1) = \alpha_2(1 - \alpha_2).$$

It follows that in the case $\alpha_1 \neq 1$ we can choose arbitrary value for $\alpha_1 \in [0,1)$ and then we have the solution

g	$g_{a,a}$	$g_{a,b}$	$g_{b,a}$	$g_{b,b}$
a	α_1	α_2	α_2	$\alpha_2\frac{1-\alpha_2}{1-\alpha_1}$
b	$1-\alpha_1$	$1-\alpha_2$	$1-\alpha_2$	$1-\alpha_2\frac{1-\alpha_2}{1-\alpha_1}$

,

for any α_2 such that $0 \leqslant \alpha_2\frac{1-\alpha_2}{1-\alpha_1} \leqslant 1$. In the case $\alpha_4 \neq 0$ we can choose arbitrary value for $\alpha_4 \in (0,1]$ and then we have the solution

g	$g_{a,a}$	$g_{a,b}$	$g_{b,a}$	$g_{b,b}$
a	$1-\alpha_2\frac{1-\alpha_2}{\alpha_4}$	α_2	α_2	α_4
b	$\alpha_2\frac{1-\alpha_2}{\alpha_4}$	$1-\alpha_2$	$1-\alpha_2$	$1-\alpha_4$

,

for any α_2 such that $0 \leqslant \alpha_2\frac{1-\alpha_2}{\alpha_4} \leqslant 1$.

We notice that in this case all probabilistic semigroups are commutative, since $g_{a,b} = g_{b,a}$.

Case 2: $\alpha_4 = 0$ and $\beta_1 = 0$. Then $\alpha_1 = 1$ and $\beta_4 = 1$ and the starting system of equations reduces to

$$\begin{array}{llll} \alpha_2 + \beta_2\alpha_3 = \alpha_3 + \alpha_2\beta_3, & \alpha_2\beta_2 = 0, & \beta_2\beta_2 = \beta_2, & \alpha_2\alpha_2 = \alpha_2, \\ \alpha_3\beta_2 + \beta_3 = \beta_2\alpha_2 + \beta_2, & \alpha_3\beta_3 = 0, & \alpha_3\alpha_3 = \alpha_3, & \beta_3\beta_3 = \beta_3. \end{array}$$

There are only three solutions in this case:

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \{(1,0,0,0), (1,0,1,0), \ (1,1,1,0)\},$$

and only for $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (1,0,1,0)$ we have non-commutative (ordinary) semigroup.

6.6 Probabilistic quasigroups

An ordinary groupoid $(Q,\cdot)$ is said to be a quasigroup if

$$(\forall a, b \in Q)(\exists! x, y \in Q)(ax = b \ \& \ ya = b).$$

We say that a probabilistic groupoid (Q, g) is a *probabilistic quasigroup with probability* p (or a p-*quasigroup*) if

$$(\forall a, b \in Q)(\exists x, y \in Q)(g_{a,x}(b) \geqslant p \ \& \ g_{y,a}(b) \geqslant p).$$

Note that for $0 \leqslant q < p \leqslant 1$, every $p - quasigroup$ is a $q - quasigroup$ as well. It is also clear that every probabilistic groupoid is a 0-quasigroup.

In the case of p-quasigroups, depending of the value of p, for some $a, b \in Q$ may exist several $x, y \in Q$ such that $g_{a,x}(b) \geqslant p$ and/or $g_{y,a}(b) \geqslant p$. Since in any distribution $g_{\alpha,\beta}$, when $p > 1/2$, may exist (if any) a unique element b such that $g_{\alpha,\beta}(b) = p$, we have the following.

Proposition 6.12. *If $p > 1/2$, then for any finite p-quasigroup it is true that*

$$(\forall a, b \in Q)(\exists! x, y \in Q)(g_{a,x}(b) \geqslant p \ \&\ g_{y,a}(b) \geqslant p).$$

Proof. The proof follows by the Pigeonhole Principal. Let $Q = \{q_1, \ldots, q_n\}$ be a p-quasigroup and $p > 1/2$. If $g_{a,x_1}(b) \geqslant p$ and $g_{a,x_2}(b) \geqslant p$ for some $a, b, x_1 \neq x_2 \in Q$, then we have for each of the rest $n-1$ elements $c \in Q \setminus \{b\}$ to find some $x \in Q \setminus \{x_1, x_2\}$ such that $g_{a,x}(c) \geqslant p$. □

Corollary 6.13. *1-quasigroups are ordinary quasigroups.*

A probabilistic groupoid (A, g) is said to be with *left* (*right*) *cancellation* if for every $a, b, c \in A$ we have

$$g_{a,b} = g_{a,c} \Rightarrow b = c \quad (g_{a,b} = g_{c,b} \Rightarrow a = c).$$

A probabilistic groupoid is said to be *cancellative* if it is with left and right cancellation.

Proposition 6.14. *If $p > 1/2$, then a p-quasigroup is a cancellative probabilistic groupoid.*

Proof. Let $p > 1/2$ and let (Q, g) be a p-quasigroup. If $g_{a,x} = g_{a,y}$, then for the distribution $g_{a,x}$ there is a unique $b \in Q$ such that $g_{a,x}(b) = g_{a,y}(b) \geqslant p$. Now, by Proposition 6.12, we have $x = y$. □

Example 6.15. A 0.5-quasigroup (Q, g), where $Q = \{1, 2, 3, 4\}$, is presented by the distributions given in Table 1. We can see there that $g_{2,1}(2) \geqslant 0.5$, $g_{1,4}(2) \geqslant 0.5$, $g_{4,4}(2) \geqslant 0.5$, etc.

6.7 Inverse elements

Let (A, g) be a probabilistic groupoid which possess a unit e, and let $a, b \in A$. If $g_{a,b}(e) = p$, then we say that a is a *left inverse of b with probability p* and that b is a *right inverse of a with probability p*. It is obvious that left/right p-inverses of an element do not have to exist, but if so, then there might be more than one. If an element a is both left p-inverse and right

	$g_{1,1}$	$g_{1,2}$	$g_{1,3}$	$g_{1,4}$	$g_{2,1}$	$g_{2,2}$	$g_{2,3}$	$g_{2,4}$
1	0	0.7	0.5	0.1	0	0.3	0.5	0.04
2	0.5	0.1	0	0.6	0.5	0.1	0.5	0.36
3	0.5	0.2	0	0	0.4	0.1	0	0.5
4	0	0	0.5	0.3	0.1	0.5	0	0.1

	$g_{3,1}$	$g_{3,2}$	$g_{3,3}$	$g_{3,4}$	$g_{4,1}$	$g_{4,2}$	$g_{4,3}$	$g_{4,4}$
1	0.5	0.2	0	0.1	0.1	0	0.2	0.5
2	0.4	0.55	0	0.1	0.4	0	0.5	0.5
3	0.1	0.25	0.5	0.3	0	0.5	0.13	0
4	0	0	0.5	0.5	0.5	0.5	0.17	0

Table 1: A probabilistic 0.5-quasigroup of order 4.

p-inverse of an element b, then the elements a and b are referred as *mutually p-inverse* or *p-inverse to each other.*

If e is a unit of (A, g), then $g_{a,e}(e) = \epsilon_a(e) = \begin{cases} 1 : e = a, \\ 0 : e \neq a. \end{cases}$ Hence, the only left p-inverse of e is e itself, and it can be only a 1-inverse as well. So, the next property holds.

Proposition 6.16. *Let e be the unit of a probabilistic groupoid (A, g). Then e is left and right 1-inverse element to itself.*

Further on, instead of a 1-inverse element, we will say simply an inverse element.

We will prove that an inverse element in a probabilistic semigroup is unique.

Theorem 6.17. *Let the element a of a probabilistic semigroup $A = (A, g)$ have left inverse b and right inverse c. Then $b = c$.*

Proof. Given that b is a left inverse and c is a right inverse of a, we will prove that $\epsilon_b = \epsilon_c$, that implies $b = c$. Denote by e the unit of A. We have

$$g_{b,(a,c)}(z) = \sum_{u \in A} g_{b,u}(z) g_{a,c}(u) = g_{b,e}(z) \cdot 1 = g_{b,e}(z) = \epsilon_b(z),$$

since $g_{a,c}(e) = 1$ and $g_{a,c}(u) = 0$ when $u \neq e$. In the same way

$$g_{(b,a),c}(z) = \textstyle\sum_{u \in A} g_{b,a}(u) g_{u,c}(z) = 1 \cdot g_{e,c}(z) = g_{e,c}(z) = \epsilon_c(z).$$

Now, $g_{b,(a,c)}(z) = g_{(b,a),c}(z)$ implies $\epsilon_b(z) = \epsilon_c(z)$ for every $z \in A$, i.e., $\epsilon_b = \epsilon_c$. □

The unique left and right inverse of an element $a \in A$ is called an inverse of a and is denoted by a^{-1}.

Proposition 6.18. *Let (A, g) be a probabilistic semigroup with unit e and let an element $b \in A$ has a left (right) inverse. Then for every $c, d \in A$ we have*

$$g_{b,c} = g_{b,d} \implies c = d \qquad (g_{c,b} = g_{d,b} \implies c = d).$$

Proof. Assume that a is a left inverse of b and $g_{b,c} = g_{b,d}$. Then $g_{a,(b,c)}(z) = \sum_{u \in A} g_{a,u}(z) g_{b,c}(u) = \sum_{u \in A} g_{a,u}(z) g_{b,d}(u) = g_{a,(b,d)}(z)$, and by associativity we have $g_{(a,b),c}(z) = g_{(a,b),d}(z)$. So, $\sum_{u \in A} g_{a,b}(u) g_{u,c}(z) = \sum_{u \in A} g_{a,b}(u) g_{u,d}(z)$ and, since $g_{a,b}(u) = 0$ when $u \neq e$, we obtain $g_{e,c}(z) = g_{e,d}(z)$. This means that $\epsilon_c = \epsilon_d$, i.e., $c = d$. □

As a corollary of Proposition 6.18 we have the following.

Theorem 6.19. *If each element of a probabilistic semigroup has inverse, then the semigroup is cancellative.*

The next simple lemma will be used in the next section.

Lemma 6.20. *If a and b are mutually inverse elements in a probabilistic groupoid (A, g) with unit e, then for each $c \in A$ we have $g_{c,(a,b)} = g_{c,e} = \epsilon_c$ and $g_{(a,b),c} = g_{e,c} = \epsilon_c$.*

Proof. We have $g_{c,(a,b)}(z) = \sum_{u \in A} g_{c,u}(z) g_{a,b}(u) = g_{c,e}(z) g_{a,b}(e) = g_{c,e}(z) = \epsilon_c(z)$, since $g_{a,b}(u) = 0$ when $u \neq e$. □

7. Probabilistic groups

A probabilistic semigroup is said to be a *p-probabilistic group* if it has a unit and each element has a p-inverse. In what follows we will consider several examples in order to support our opinion that there are not finite essential p-groups. In fact, we found (without proofs) that there are no finite p-groups when $p < 1$, and that for $p = 1$ the probabilistic 1-groups are ordinary groups. Further on, we will say a probabilistic group instead of a probabilistic 1-group.

Example 7.1. We are asking for all p-groups on the set $\{e, a, b\}$, where $0 < p < 1$, e is the unit and b is a p-inverse of a. We have the distributions

	$g_{e,e}$	$g_{a,e} = g_{e,a}$	$g_{b,e} = g_{e,b}$	$g_{a,b}$	$g_{b,a}$	$g_{a,a}$	$g_{b,b}$
e	1	0	0	p	p	γ_1	γ_2
a	0	1	0	α_1	α_2	α_3	α_4
b	0	0	1	β_1	β_2	β_3	β_4

for some $\alpha_i, \beta_i, \gamma_i \in [0, 1]$, $p + \alpha_1 + \beta_1 = 1$, $p + \alpha_2 + \beta_2 = 1, \gamma_1 + \alpha_3 + \beta_3 = 1, \gamma_2 + \alpha_4 + \beta_4 = 1$.

By the associativity, the following 8 equations have to be satisfied for $z \in \{e, a, b\}$: $g_{a,(a,a)}(z) = g_{(a,a),a}(z)$, $g_{a,(a,b)}(z) = g_{(a,a),b}(z), \dots,$ $g_{b,(b,b)}(z) = g_{(b,b),b}(z)$. We can infer several equations in unknowns $\alpha_i, \beta_i, \gamma_i$.

From $g_{a,(a,a)}(z) = g_{(a,a),a}(z)$, for $z = a$ we have

$$(\alpha_1 - \alpha_2)\beta_3 = 0, \tag{1}$$

and for $z = b$ we have

$$(\beta_1 - \beta_2)\beta_3 = 0. \tag{2}$$

From $g_{a,(a,b)}(z) = g_{(a,a),b}(z)$, for $z = e$ we have

$$\gamma_1\alpha_1 + p\beta_1 = p\alpha_3 + \beta_3\gamma_2, \tag{3}$$

for $z = a$ we have

$$p + \alpha_1\beta_1 = \beta_3\alpha_4, \tag{4}$$

and for $z = b$ we have

$$\beta_1\alpha_1 + \beta_1\beta_1 = \gamma_1 + \alpha_3\beta_1 + \beta_3\beta_4. \tag{5}$$

From $g_{a,(b,b)}(z) = g_{(a,b),b}(z)$, for $z = e$ we have

$$\gamma_1\alpha_4 + p\beta_4 = p\alpha_1 + \beta_1\gamma_2, \tag{6}$$

and for $z = a$ we have

$$\alpha_4 + \alpha_3\alpha_4 + \alpha_1\beta_4 = \alpha_1\alpha_1 + \beta_1\alpha_4. \tag{7}$$

From $g_{b,(a,a)}(z) = g_{(b,a),a}(z)$, for $z = e$ we have

$$\gamma_2\beta_3 + p\alpha_3 = p\beta_2 + \alpha_2\gamma_1, \tag{8}$$

and for $z = b$ we have

$$\beta_3 + \beta_2\alpha_3 + \beta_3\beta_4 = \alpha_2\beta_3 + \beta_2\beta_2. \tag{9}$$

Finally, from $g_{b,(b,a)}(z) = g_{(b,b),a}(z)$, for $z = e$ we have

$$p\alpha_2 + \gamma_2\beta_2 = \alpha_4\gamma_1 + p\beta_4, \tag{10}$$

and for $z = a$ we have

$$\alpha_2\alpha_2 + \alpha_4\beta_2 = \gamma_2 + \alpha_4\alpha_3 + \beta_4\alpha_2. \tag{11}$$

The equation (4), since $0 < p < 1$, implies $\alpha_4 > 0, \beta_3 > 0$, and then by (1) and (2) we conclude that $\alpha_1 = \alpha_2 = \alpha$ and $\beta_1 = \beta_2 = \beta$. Now, from (5) and (11) we have

$$\gamma_1 = \beta\alpha + \beta\beta - \alpha_3\beta - \beta_3\beta_4 \tag{12}$$

and

$$\gamma_2 = \alpha\alpha + \alpha_4\beta - \alpha_4\alpha_3 - \beta_4\alpha. \tag{13}$$

We replace γ_1 and γ_2 in (3) and we obtain the equation

$$\beta\alpha\alpha + \beta\beta\alpha - \alpha_3\beta\alpha - \beta_3\beta_4\alpha + p\beta = p\alpha_3 + \alpha\alpha\beta_3 + \alpha_4\beta\beta_3 - \alpha_4\alpha_3\beta_3 - \beta_4\alpha\beta_3. \tag{14}$$

After replacing $\alpha_4\beta_3$ by $p + \alpha\beta$ (according (4)) and after simplifying, we obtain the equation $\beta\alpha\alpha = \alpha\alpha\beta_3$. The last equation implies $\alpha = 0$ or $\beta = \beta_3$. We have to consider three cases.

Case $\alpha = 0$ *and* $\beta = \beta_3$.

We replace $\alpha = 0$ and $\beta = \beta_3$ in the equation (9) and we get $\beta + \beta\alpha_3 + \beta\beta_4 = \beta\beta$. Since $\beta = \beta_3 > 0$, it follows that $1 + \alpha_3 + \beta_4 = \beta$, i.e. $\beta = 1$. This is a contradiction with $p + \alpha + \beta = 1,\ p > 0$.

Case $\alpha = 0$ *and* $\beta \neq \beta_3$.

We replace $\alpha = 0$ in the equation (7) and we get $\alpha_4 + \alpha_3\alpha_4 = \beta\alpha_4$. Since $\alpha_4 > 0$, it follows that $1 + \alpha_3 = \beta$, that leads to a contradiction again.

Case $\alpha > 0$ *and* $\beta = \beta_3$.

We replace $\beta = \beta_3$ in the equation (9) and we get $\beta + \beta\alpha_3 + \beta\beta_4 = \alpha\beta + \beta\beta$. Since $\beta = \beta_3 > 0$, it follows that $1 + \alpha_3 + \beta_4 = \alpha + \beta$, implying $\alpha + \beta = 1$. This is a contradiction with $p + \alpha + \beta = 1,\ 0 < p < 1$.

The obtained contradictions shows that there are no probabilistic p-groups on the set $\{e,a,b\}$, where $0<p<1$, e is the unit and b is a p-inverse of a. In a similar way one can show that there are no probabilistic p-groups on the set $\{e,a,b\}$, where $0<p<1$, e is the unit and a (b) is a p-inverse of a (b).

Example 7.2. Let (A,g), where $A=\{e,a,b\}$, be a probabilistic group with unit e. Let us first assume that $a^{-1}=a$, and then $b^{-1}=b$. Then we have the distributions

	$g_{e,e}, g_{a,a}, g_{b,b}$	$g_{a,e}, g_{e,a}$	$g_{b,e}, g_{e,b}$	$g_{a,b}$	$g_{b,a}$
e	1	0	0	α	α_1
a	0	1	0	β	β_1
b	0	0	1	γ	γ_1

for some $\alpha,\beta,\gamma,\alpha_1,\beta_1,\gamma_1\in[0,1]$, $\alpha+\beta+\gamma=\alpha_1+\beta_1+\gamma_1=1$.

By associativity we have $g_{(a,a),b}=g_{a,(a,b)}$, where (according to Lemma 6.20) $g_{(a,a),b}(b)=\epsilon_b(b)=1$, and $g_{a,(a,b)}(b)=g_{a,e}(b)g_{a,b}(e)+g_{a,a}(b)g_{a,b}(a)+g_{a,b}(b)g_{a,b}(b)=\gamma\gamma$.

So we get the equation $\gamma\gamma=1$, i.e., $\gamma=1$. This means that $g_{e,b}=g_{a,b}$, i.e., $e=a$. The obtained contradiction implies that $a\neq a^{-1}$.

Now, let $a^{-1}=b$. Then, by Example 7.1, for $p=1$ we have $\alpha_1=\beta_1=\alpha_2=\beta_2=\alpha_3=\beta_4=\gamma_1=\gamma_2=0$ and $\alpha_4=\beta_3=1$. Hence, this probability group is in fact the cyclic group

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

.

Example 7.3. Let (A,g), where $A=\{e,a,b,c\}$, be a probabilistic group with unit e. We have to consider two cases, case *I* and case *II*.

I. Let first assume that $a^{-1}=a$, $b^{-1}=b$, $c^{-1}=c$. Then we have the following distributions, presented in more compact way,

	$g_{e,e}, g_{a,a}$ $g_{b,b}, g_{c,c}$	$g_{a,e}$ $g_{e,a}$	$g_{b,e}$ $g_{e,b}$	$g_{c,e}$ $g_{e,c}$	$g_{a,b}$	$g_{a,c}$	$g_{b,a}$	$g_{b,c}$	$g_{c,a}$	$g_{c,b}$
e	1	0	0	0	α_1	α_2	α_3	α_4	α_5	α_6
a	0	1	0	0	β_1	β_2	β_3	β_4	β_5	β_6
b	0	0	1	0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6
c	0	0	0	1	δ_1	δ_2	δ_3	δ_4	δ_5	δ_6

where $\alpha_i,\ \beta_i,\ \gamma_i,\ \delta_i \geqslant 0,\quad \alpha_i+\beta_i+\gamma_i+\delta_i=1$, for $i=1,2,\dots,6$.

By associativity we have the following equalities.

Case $g_{a,(a,b)} = g_{(a,a),b}$. By Lemma 6.20 we have $g_{(a,a),b}(z) = g_{e,b}(z) = \epsilon_b(z) = \begin{pmatrix} e & a & b & c \\ 0 & 0 & 1 & 0 \end{pmatrix}$, and we compute the distribution $g_{a,(a,b)}$.

$g_{a,(a,b)}(z) = g_{a,e}(z)g_{a,b}(e)+g_{a,a}(z)g_{a,b}(a)+g_{a,b}(z)g_{a,b}(b)+g_{a,c}(z)g_{a,b}(c) =$

$$= \begin{pmatrix} 0\\1\\0\\0 \end{pmatrix}\alpha_1 + \begin{pmatrix} 1\\0\\0\\0 \end{pmatrix}\beta_1 + \begin{pmatrix} \alpha_1\\ \beta_1\\ \gamma_1\\ \delta_1 \end{pmatrix}\gamma_1 + \begin{pmatrix} \alpha_2\\ \beta_2\\ \gamma_2\\ \delta_2 \end{pmatrix}\delta_1 = \begin{pmatrix} \beta_1+\alpha_1\gamma_1+\alpha_2\delta_1\\ \alpha_1+\beta_1\gamma_1+\beta_2\delta_1\\ \gamma_1\gamma_1+\gamma_2\delta_1\\ \delta_1\gamma_1+\delta_2\delta_1 \end{pmatrix}.$$

Hence, we have the following system of equations

$$\left\{\begin{array}{rcl} \beta_1+\alpha_1\gamma_1+\alpha_2\delta_1 &=& 0,\\ \alpha_1+\beta_1\gamma_1+\beta_2\delta_1 &=& 0,\\ \gamma_1\gamma_1+\gamma_2\delta_1 &=& 1,\\ \delta_1\gamma_1+\delta_2\delta_1 &=& 0, \end{array}\right. \quad \text{i.e.,} \quad \left\{\begin{array}{rcl} \alpha_1=\beta_1 &=& 0,\\ \alpha_1\gamma_1=\beta_1\gamma_1=\delta_1\gamma_1 &=& 0,\\ \alpha_2\delta_1=\beta_2\delta_1=\delta_2\delta_1 &=& 0,\\ \gamma_1\gamma_1+\gamma_2\delta_1 &=& 1. \end{array}\right.$$

We consider two possibilities.

$\gamma_1 \neq 0$. Then we have $\alpha_1=\beta_1=\delta_1=0,\ \gamma_1=1$, and this implies $g_{a,b}=g_{e,b}$. After cancellation we get the contradiction $a=e$.

$\gamma_1 = 0$. Then, from $\gamma_2\delta_1=1$ we have $\gamma_2=1,\ \delta_1=1$. Hence, we have $\alpha_1=\beta_1=\gamma_1=0,\ \delta_1=1$, and this implies $\mathbf{g_{a,b}}=\mathbf{g_{e,c}}$, and also $\alpha_2=\beta_2=\delta_2=0,\ \gamma_2=1$, implying $\mathbf{g_{a,c}}=\mathbf{g_{e,b}}$.

Case $g_{b,(b,c)} = g_{(b,b),c}$. By Lemma 6.20 we have $g_{(b,b),c}(z) = g_{e,c}(z) = \epsilon_c(z) = \begin{pmatrix} e & a & b & c \\ 0 & 0 & 0 & 1 \end{pmatrix}$, and we compute the distribution $g_{b,(b,c)}$.

$g_{b,(b,c)}(z) = g_{b,e}(z)g_{b,c}(e)+g_{b,a}(z)g_{b,c}(a)+g_{b,b}(z)g_{b,c}(b)+g_{b,c}(z)g_{b,c}(c) =$

$$= \begin{pmatrix} 0\\0\\1\\0 \end{pmatrix}\alpha_4 + \begin{pmatrix} \alpha_3\\ \beta_3\\ \gamma_3\\ \delta_3 \end{pmatrix}\beta_4 + \begin{pmatrix} 1\\0\\0\\0 \end{pmatrix}\gamma_4 + \begin{pmatrix} \alpha_4\\ \beta_4\\ \gamma_4\\ \delta_4 \end{pmatrix}\delta_4 = \begin{pmatrix} \alpha_3\beta_4+\gamma_4+\alpha_4\delta_4\\ \beta_3\beta_4+\beta_4\delta_4\\ \alpha_4+\gamma_3\beta_4+\gamma_4\delta_4\\ \delta_3\beta_4+\delta_4\delta_4 \end{pmatrix}.$$

Hence, we have the following system of equations

$$\left\{\begin{array}{rcl} \alpha_3\beta_4+\gamma_4+\alpha_4\delta_4 &=& 0,\\ \beta_3\beta_4+\beta_4\delta_4 &=& 0,\\ \alpha_4+\gamma_3\beta_4+\gamma_4\delta_4 &=& 0,\\ \delta_3\beta_4+\delta_4\delta_4 &=& 1, \end{array}\right. \quad \text{i.e.,} \quad \left\{\begin{array}{rcl} \alpha_4=\gamma_4 &=& 0,\\ \alpha_3\beta_4=\beta_3\beta_4=\gamma_3\beta_4 &=& 0,\\ \alpha_4\delta_4=\beta_4\delta_4=\gamma_4\delta_4 &=& 0,\\ \delta_3\beta_4+\delta_4\delta_4 &=& 1. \end{array}\right.$$

We consider two possibilities.

$\beta_4 \neq 0$. Then from $\beta_4\delta_4 = 0$ we get $\delta_4 = 0$, and so $\alpha_4 = \gamma_4 = \delta_4 = 0$, $\beta_4 = 1$, which implies $\mathbf{g_{b,c}} = \mathbf{g_{e,a}}$. On the other side, we have also $\alpha_3 = \beta_3 = \gamma_3 = 0$, $\delta_3 = 1$, implying $\mathbf{g_{b,a}} = \mathbf{g_{e,c}}$.

$\beta_4 = 0$. Then $\alpha_4 = \beta_4 = \gamma_4 = 0$, $\delta_4 = 1$, implying $g_{b,c} = g_{e,c}$, leading to the contradiction $b = e$.

Case $g_{c,(c,a)} = g_{(c,c),a}$. By Lemma 6.20 we have $g_{(c,c),a}(z) = g_{e,a}(z) = \epsilon_a(z) = \begin{pmatrix} e & a & b & c \\ 0 & 1 & 0 & 0 \end{pmatrix}$, and we compute the distribution $g_{c,(c,a)}$.

$$g_{c,(c,a)}(z) = g_{c,e}(z)g_{c,a}(e) + g_{c,a}(z)g_{c,a}(a) + g_{c,b}(z)g_{c,a}(b) + g_{c,c}(z)g_{c,a}(c) =$$
$$= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \alpha_5 + \begin{pmatrix} \alpha_5 \\ \beta_5 \\ \gamma_5 \\ \delta_5 \end{pmatrix} \beta_5 + \begin{pmatrix} \alpha_6 \\ \beta_6 \\ \gamma_6 \\ \delta_6 \end{pmatrix} \gamma_5 + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \delta_5 = \begin{pmatrix} \alpha_5\beta_5 + \alpha_6\gamma_5 + \delta_5 \\ \beta_5\beta_5 + \beta_6\gamma_5 \\ \gamma_5\beta_5 + \gamma_6\gamma_5 \\ \delta_5\beta_5 + \delta_6\gamma_5 + \alpha_5 \end{pmatrix}.$$

Hence, we have the following system of equations

$$\left\{ \begin{array}{rcl} \alpha_5\beta_5 + \alpha_6\gamma_5 + \delta_5 & = & 0, \\ \beta_5\beta_5 + \beta_6\gamma_5 & = & 1, \\ \gamma_5\beta_5 + \gamma_6\gamma_5 & = & 0, \\ \delta_5\beta_5 + \delta_6\gamma_5 + \alpha_5 & = & 0, \end{array} \right. \quad \text{i.e.,} \quad \left\{ \begin{array}{rcl} \alpha_5 = \delta_5 & = & 0, \\ \alpha_5\beta_5 = \gamma_5\beta_5 = \delta_5\beta_5 & = & 0, \\ \alpha_6\gamma_5 = \gamma_6\gamma_5 = \delta_6\gamma_5 & = & 0, \\ \beta_5\beta_5 + \beta_6\gamma_5 & = & 1. \end{array} \right.$$

We consider two possibilities.

$\beta_5 = 0$. Then from $\beta_6\gamma_5 = 1$ we get $\beta_6 = 1$, $\gamma_5 = 1$, that implies $\alpha_6 = \gamma_6 = \delta_6 = 0, \beta_6 = 1$, and we infer that $\mathbf{g_{c,b}} = \mathbf{g_{e,a}}$. On other side, we also have $\alpha_5 = \beta_5 = \delta_5 = 0, \gamma_5 = 1$, implying $\mathbf{g_{c,a}} = \mathbf{g_{e,b}}$.

$\beta_5 \neq 0$. Then $\alpha_5 = \gamma_5 = \delta_5 = 0, \beta_5 = 1$, and this implies $g_{c,a} = g_{e,a}$, leading to the contradiction $c = e$.

Altogether, we get $\mathbf{g_{a,b}} = \mathbf{g_{e,c}}$, $\mathbf{g_{a,c}} = \mathbf{g_{e,b}}$, $\mathbf{g_{b,c}} = \mathbf{g_{e,a}}$, $\mathbf{g_{b,a}} = \mathbf{g_{e,c}}$, $\mathbf{g_{c,b}} = \mathbf{g_{e,a}}$, $\mathbf{g_{c,a}} = \mathbf{g_{e,b}}$. This means that the probability group is in fact the ordinary Klein group

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

.

II. The other case is $c^{-1} = a$, $b^{-1} = b$ (or $c^{-1} = b, a^{-1} = a$, or $b^{-1} = a, c^{-1} = c$, these lead to isomorphic results). Then we have the following distributions,

	$g_{e,e}, g_{b,b}$ $g_{a,c}, g_{c,a}$	$g_{a,e}$ $g_{e,a}$	$g_{b,e}$ $g_{e,b}$	$g_{c,e}$ $g_{e,c}$	$g_{a,a}$	$g_{a,b}$	$g_{b,a}$	$g_{b,c}$	$g_{c,b}$	$g_{c,c}$
e	1	0	0	0	α_1	α_2	α_3	α_4	α_5	α_6
a	0	1	0	0	β_1	β_2	β_3	β_4	β_5	β_6
b	0	0	1	0	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6
c	0	0	0	1	δ_1	δ_2	δ_3	δ_4	δ_5	δ_6

where $\alpha_i,\ \beta_i,\ \gamma_i,\ \delta_i \geqslant 0,\quad \alpha_i+\beta_i+\gamma_i+\delta_i = 1$, for $i = 1, 2, \dots, 6$.

By associativity we have the following equalities.

Case $g_{(b,b),c} = g_{b,(b,c)}$. By Lemma 6.20 we have $g_{g_{(b,b),c}}(z) = g_{e,c}(z) = \epsilon_c(z) = \begin{pmatrix} e & a & b & c \\ 0 & 0 & 0 & \end{pmatrix}$, and we compute the distribution $g_{b,(b,c)}$.

$$g_{b,(b,c)}(z) = g_{b,e}(z)g_{b,c}(e) + g_{b,a}(z)g_{b,c}(a) + g_{b,b}(z)g_{b,c}(b) + g_{b,c}(z)g_{b,c}(c) =$$

$$= \begin{pmatrix} 0\\0\\1\\0 \end{pmatrix} \alpha_4 + \begin{pmatrix} \alpha_3\\ \beta_3\\ \gamma_3\\ \delta_3 \end{pmatrix} \beta_4 + \begin{pmatrix} 1\\0\\0\\0 \end{pmatrix} \gamma_4 + \begin{pmatrix} \alpha_4\\ \beta_4\\ \gamma_4\\ \delta_4 \end{pmatrix} \delta_4 = \begin{pmatrix} \alpha_3\beta_4+\gamma_4+\alpha_4\delta_4 \\ \beta_3\beta_4+\beta_4\delta_4 \\ \alpha_4+\gamma_3\beta_4+\gamma_4\delta_4 \\ \gamma_3\beta_4+\delta_4\delta_4 \end{pmatrix}.$$

Hence, we have the following system of equations

$$\begin{cases} \alpha_3\beta_4+\gamma_4+\alpha_4\delta_4 &= 0, \\ \beta_3\beta_4+\beta_4\delta_4 &= 0, \\ \alpha_4+\gamma_3\beta_4+\gamma_4\delta_4 &= 0, \\ \gamma_3\beta_4+\delta_4\delta_4 &= 1, \end{cases} \quad \text{i.e.,} \quad \begin{cases} \alpha_4=\gamma_4 &= 0, \\ \alpha_3\beta_4=\beta_3\beta_4=\gamma_3\beta_4 &= 0, \\ \alpha_4\delta_4=\beta_4\delta_4=\gamma_4\delta_4 &= 0, \\ \gamma_3\beta_4+\delta_4\delta_4 &= 1. \end{cases}$$

We consider two possibilities.

$\beta_4 \neq 0$. Then we have $\alpha_3 = \beta_3 = \gamma_3 = 0, \delta_3 = 1$, implying $\mathbf{g_{b,a}} = \mathbf{g_{e,c}}$. It follows from $\beta_4\delta_4 = 0$ that $\delta_4 = 0$, i.e., we have $\alpha_4 = \delta_4 = \gamma_4 = 0, \beta_4 = 1$, and so we have $\mathbf{g_{b,c}} = \mathbf{g_{e,a}}$.

$\beta_4 = 0$. Then from $\delta_4\delta_4 = 1$ we have $\alpha_4 = \beta_4 = \gamma_4 = 0, \delta_4 = 1$, leading to the contradiction $g_{b,c} = g_{e,c}$.

Case $g_{(a,a),c} = g_{a,(a,c)}$. By Lemma 6.20 we have $g_{a,(a,c)}(z) = g_{a,e}(z) = \epsilon_a(z) = \begin{pmatrix} e & a & b & c \\ 0 & 1 & 0 & 0 \end{pmatrix}$, and we compute the distribution $g_{(a,a),c}$.

$$g_{(a,a),c}(z) = g_{a,a}(e)g_{e,c}(z)+g_{a,a}(a)g_{a,c}(z)+g_{a,a}(b)g_{b,c}(z)+g_{a,a}(c)g_{c,c}(z) =$$

$$= \alpha_1 \begin{pmatrix} 0\\0\\0\\1 \end{pmatrix} + \beta_1 \begin{pmatrix} 1\\0\\0\\0 \end{pmatrix} + \gamma_1 \begin{pmatrix} \alpha_4\\ \beta_4\\ \gamma_4\\ \delta_4 \end{pmatrix} + \delta_1 \begin{pmatrix} \alpha_6\\ \beta_6\\ \gamma_6\\ \delta_6 \end{pmatrix} = \begin{pmatrix} \beta_1+\gamma_1\alpha_4+\delta_1\alpha_6 \\ \gamma_1\beta_4+\delta_1\beta_6 \\ \gamma_1\gamma_4+\delta_1\gamma_6 \\ \alpha_1+\gamma_1\delta_4+\delta_1\delta_6 \end{pmatrix}.$$

Hence, we have the following system of equations

$$\begin{cases} \beta_1+\gamma_1\alpha_4+\delta_1\alpha_6 &= 0,\\ \gamma_1\beta_4+\delta_1\beta_6 &= 1,\\ \gamma_1\gamma_4+\delta_1\gamma_6 &= 0,\\ \alpha_1+\gamma_1\delta_4+\delta_1\delta_6 &= 0,\end{cases} \quad \text{i.e.,} \quad \begin{cases} \alpha_1=\beta_1 &= 0,\\ \gamma_1\alpha_4=\gamma_1\gamma_4=\gamma_1\delta_4 &= 0,\\ \delta_1\alpha_6=\delta_1\gamma_6=\delta_1\delta_6 &= 0,\\ \gamma_1\beta_4+\delta_1\beta_6 &= 1.\end{cases}$$

We consider two possibilities.

$\delta_1 \neq 0$. Then we have $\alpha_6=\gamma_6=\delta_6=0, \beta_6=1$, leading to a contradiction $g_{c,c}=g_{a,e}$, since we have shown in the previous case that $g_{b,c}=g_{a,e}$.

$\delta_1 = 0$. Then we have $\alpha_1=\beta_1=\delta_1=0, \gamma_1=1$, and this gives $\mathbf{g_{a,a}}=\mathbf{g_{b,e}}$.

Case $g_{(a,b),b}=g_{a,(b,b)}$. By Lemma 6.20 we have $g_{a,(b,b)}(z)=g_{a,e}(z)=\epsilon_a(z)=\begin{pmatrix} e & a & b & c\\ 0 & 1 & 0 & 0\end{pmatrix}$, and we compute the distribution $g_{(a,b),b}$.

$$g_{(a,b),b}(z)=g_{a,b}(e)g_{e,b}(z)+g_{a,b}(a)g_{a,b}(z)+g_{a,b}(b)g_{b,b}(z)+g_{a,b}(c)g_{c,b}(z)=$$

$$=\alpha_2\begin{pmatrix}0\\0\\1\\0\end{pmatrix}+\beta_2\begin{pmatrix}\alpha_2\\\beta_2\\\gamma_2\\\delta_2\end{pmatrix}+\gamma_2\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+\delta_2\begin{pmatrix}\alpha_5\\\beta_5\\\gamma_5\\\delta_5\end{pmatrix}=\begin{pmatrix}\beta_2\alpha_2+\gamma_2+\delta_2\alpha_5\\\beta_2\beta_2+\delta_2\beta_5\\\alpha_2+\beta_2\gamma_2+\delta_2\gamma_5\\\beta_2\delta_2+\delta_2\delta_5\end{pmatrix}.$$

Hence, we have the following system of equations

$$\begin{cases} \beta_2\alpha_2+\gamma_2+\delta_2\alpha_5 &= 0,\\ \beta_2\beta_2+\delta_2\beta_5 &= 1,\\ \alpha_2+\beta_2\gamma_2+\delta_2\gamma_5 &= 0,\\ \beta_2\delta_2+\delta_2\delta_5 &= 0,\end{cases} \quad \text{i.e.,} \quad \begin{cases} \alpha_2=\gamma_2 &= 0,\\ \beta_2\alpha_2=\beta_2\gamma_2=\beta_2\delta_2 &= 0,\\ \delta_2\alpha_5=\delta_2\gamma_5=\delta_2\delta_5 &= 0,\\ \beta_2\beta_2+\delta_2\beta_5 &= 1.\end{cases}$$

We consider two possibilities.

$\delta_2 \neq 0$. Then we have $\alpha_5=\gamma_5=\delta_5=0, \beta_5=1$, implying $\mathbf{g_{c,b}}=\mathbf{g_{e,a}}$. It follows from $\beta_2\delta_2=0$ that $\beta_2=0$, i.e., we have $\alpha_2=\beta_2=\gamma_2=0, \delta_2=1$, and so we have $\mathbf{g_{a,b}}=\mathbf{g_{e,c}}$.

$\delta_2=0$. Then from $\beta_2\beta_2=1$ we have $\alpha_2=\gamma_2=\delta_2=0, \beta_2=1,$, leading to the contradiction $g_{a,b}=g_{a,e}$.

Until now he have proved that $\mathbf{g_{c,b}}=\mathbf{g_{e,a}}$, $\mathbf{g_{a,b}}=\mathbf{g_{e,c}}$, $\mathbf{g_{b,a}}=\mathbf{g_{e,c}}$, $\mathbf{g_{b,c}}=\mathbf{g_{e,a}}$, $\mathbf{g_{a,a}}=\mathbf{g_{b,e}}$. We will show that the equality $\mathbf{g_{c,c}}=\mathbf{g_{e,b}}$ is also true. Namely, from $g_{c,b}=g_{a,e}$, we have $g_{c,(c,b)}=g_{c,(a,e)}=g_{(c,a),e}=g_{e,e}=\epsilon_e$, and hence $g_{(c,c),b}=g_{c,(c,b)}=\epsilon_e$. Now, $g_{((c,c),b),b}=g_{e,b}$, i.e., $g_{(c,c),(b,b)}=g_{(c,c),e}=g_{c,c}=g_{e,b}$. The obtained equalities show that this probabilistic group is in fact the cyclic group

$$\begin{array}{c|cccc} & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & c & e \\ b & b & c & e & a \\ c & c & e & a & b \end{array}.$$

The careful analyses of the Examples 7.2 and 7.3 can give us a hint for proving the following Hypothesis.

Hypothesis. *Each finite probabilistic group is a group.*

We are not going to give a complete proof here, mainly because of technical reasons. We only show how a proof can be inferred for finite groups.

Let (A, g) be a probabilistic group with unit e, where $A = \{e, a_1, a_2, a_n\}$. Let suppose that $a_2^{-1} = a_1$, i.e., $g_{a_1,a_2} = g_{a_2,a_1} = \epsilon_e$. Take an element a_k, $k > 2$, and consider the associativity $g_{(a_1,a_2),a_k} = g_{a_1,(a_2,a_k)}$. By Lemma 6.20 we have $g_{(a_1,a_2),a_k} = \epsilon_{a_k} = \begin{pmatrix} e & a_1 & a_2 & \dots & a_k & \dots & a_n \\ 0 & 0 & 0 & \dots & 1 & \dots & 0 \end{pmatrix}$, and we compute the distribution $g_{a_1,(a_2,a_k)}(z) = \sum_{u \in A} g_{a_1,u}(z) g_{a_2,a_k}(u)$. (Note that $g_{a_2,a_k}(u) \in A$ and $g_{a_1,u}(z)$ are distributions.) The same way as in Examples 7.2 and 7.3 we will get a system of equations of type $\alpha = 0$, $\alpha\beta = 0$ for many unknowns α, β, γ, … and only one equation of type $\alpha\beta + \gamma\delta = 1$. From these equations one can infer equalities of type $g_{a_i,a_j} = g_{a_r,e}$. Note that, for the inverses a_1, a_2, we have $4(n-2)$ equalities of types $g_{(a_1,a_2),a_k} = g_{a_1,(a_2,a_k)}$, $g_{a_k,(a_1,a_2)} = g_{(a_k,a_1),a_2)}$, $g_{(a_2,a_1),a_k} = g_{a_2,(a_1,a_k)}$ and $g_{a_k,(a_2,a_1)} = g_{(a_k,a_2),a_1)}$ $(k = 3, 4, \dots, n)$. Totally, since there are altogether $n-1$ pairs of inverses of types (a_i, a_j), (a_j, a_i) or (a_i, a_i), we can produce $4(n-1)(n-2)$ system of equations of previous type. Since the probabilistic group (A, g) have $(n-1)(n-2)$ distributions of type g_{a_i,a_j}, where $a_i \neq e$ or $a_j \neq e$ or a_i, a_j are not mutually inverse, it is reasonable to assume that for each i, j one can find an r such that $g_{a_i,a_j} = g_{a_r,e}$.

8. Conclusion

We have introduced the concept of probabilistic algebras, and our attention was given mainly to some types of probabilistic groupoids, and we had considered only the finite case.

The ideas of this paper are, in best of our knowledge, quite new. By retrieving the literature we could not find any notion or concept for probabilistic algebras.

The future work on probabilistic algebras can include (and are not restricted to) the following problems:

1. Define and investigate probabilistic groupoids on arbitrary universe (finite or infinite).

2. Define and investigate other types of probabilistic algebras (rings, lattices, modules, ...).

3. Prove the Hypothesis from Section 7 for finite groups.

4. Prove the Hypothesis from Section 7 for infinite groups (if it is true in the infinite cases).

5. Is it true that there are no finite p-groups when $0 < p < 1$? What about the infinite case?

6. Define probabilistic varieties of algebras.

7. Is it true that the distribution of g_T, when the length of the term T goes to infinity, is uniform? Can be characterized the class of probabilistic groupoids with this property?

8. How it can be defined quotient operations for probabilistic quasigroups? Can we apply them in cryptography and coding theory?

Remark for **References**: We could not find any reliable reference, except standard college algebra textbooks.

Received March 23, 2023

S. Markovski
Ss Cyril and Methodius University, Faculty of Computer Science and Engineering, Skopje, MACEDONIA
E-mail: smile.markovski@gmail.com

L. Goračinova-Ilieva
University for Tourism and Management, Faculty for Informatics, Skopje, MACEDONIA
E-mail: lgorac@yahoo.com

Quasigroups and Related Systems **32** (2024), 95 – 108

https://doi.org/10.56415/qrs.v32.08

Complete signature randomization in an algebraic cryptoscheme with a hidden group

Alexandr A. Moldovyan

Abstract. The issue of the signature randomization in algebraic cryptoschemes with a hidden group, which are based on the computational difficulty of solving large systems of power equations, is considered. To ensure complete randomization of the signature, the technique of doubling the verification equation was used to specify the hidden group. A specific signature algorithm is proposed that uses 4-dimensional non-commutative associative algebra as an algebraic support. Known results on the study of the structure of this algebra were used in constructing the proposed algorithm and estimating its security. The question of implementing similar algorithms on finite non-commutative associative algebras of dimensions $m \geqslant 6$ is related to the open problem of studying their structure from the point of view of decomposition into a set of commutative subalgebras.

1. Introduction

Design of algebraic signature algorithms with a hidden group [11, 17] had been proposed as a way to solve the current problem of developing practical post-quantum signature algorithms [1]. One can distinguish two main types of the said signature schemes, which use finite non-commutative associative algebras as their algebraic carrier: 1) based on the computational difficulty of solving the hidden discrete logarithm problem [13, 16] and 2) based on the computational difficulty of solving lage systems of power equations with many unknowns [4, 9, 17].

The latter computationally difficult problem has been well tested as a post-quantum primitive of multivariate-cryptography algorithms developed

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: non-commutative algebra, finite associative algebra, hidden group, post-quantum cryptography, public-key cryptoscheme, signature randomization
This work was financially supported by Russian Science Foundation (project No. 24-21-00225).

from 1988 [8] to the present [7, 10]. However, the known multivariate-cryptography algorithms have a significant drawback for practical application, which is the very large size of the public key.

The second type of the said algebraic signature algorithms is of special interest as an approach to developing signature schemes possessing small-size public key, which are based on the computational complexity of systems of many power equations with many unknowns. In fact, only the first step has been taken in this direction and it is necessary to study various aspects of the design of the second type algebraic algorithms with a hidden group. A common feature of the known algorithms of this type is specifying a digital signature that includes a certain vector S as its element. In this case, a vector-type verification equation is used with the repeated entry of the vector S as a multiplier. In the next section it is shown that the said feature is connected with a restricted randomization of the signature (in sens that only a small part of the elements of the algebra used as algebraic support can be potentially spesified as the vector S).

The latter creates the preconditions for potential attacks on algorithms of the type under consideration, therefore this article proposes the design of algebraic signature schemes with a hidden group, which ensures complete randomization of the signature (in sens that all reversible vectors can be potentially spesified as the vector S).

2. Preliminaries

Some m-dimensional vector A usually is denoted as $A = (a_0, a_1, \ldots, a_{m-1})$ or as $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, where $a_0, a_1, \ldots, a_{m-1}$ are coodinates taking on the values in some finite field (for example, in $GF(p)$); $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are basis vectors. In a finite m-dimensional vector space we have two standard operations: 1) addition of vectors and 2) scalar multiplication. Suppose the vector multiplication operation is additionally specified so that it is closed and distributive at the right and at the left relatively the addition operation. Then we get a finite m-dimensional algebra.

The most interesting cases of the development of the algebraic signature algorithms with a hidden group relates to the use of finite non-commutative associative algebras (FNAA) with global two-sided unit. The property of associativity is required due to using the exponentiation operations in the signature-algorithms design (when multiplication is associative one can very efficiently perform the exponentiation to a degree of large size).

The operation of multiplying two vectors A and B (coordinates of which, for example, are elements of the field $GF(p)$) can be defined by the formula

$$AB = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j (\mathbf{e}_i \mathbf{e}_j),$$

where every of the products $\mathbf{e}_i\mathbf{e}_j$ is to be substituted by a vector (usually single-component vector $\lambda\mathbf{e}_k$, where $\lambda \in GF(p)$) indicated in the cell at the intersection of the ith row and jth column of basis vector multiplication table (BVMT). Table 1 shows a specific example of BVMTs. To define associative multiplication the BVMT should be composed so that multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$ satisfies the following equality:

$$(\mathbf{e}_i\mathbf{e}_j)\,\mathbf{e}_k = \mathbf{e}_i\,(\mathbf{e}_j\mathbf{e}_k)\,.$$

The multiplication operation specified by Table 1 is associative, namely, we have a four-dimensional FNAA with the global two-sided unit $E = (0, 0, 1, 1)$, structure of which is well studied from the point view of decomposition into the set of commutative subalgebras [14]. Every of the latter has order p^2. The full number of the latter is $\eta = p^2 + p + 1$. Arbitrary two subalgebras intersect exactly in the set of scalar vectors $L = \lambda E$, where $\lambda \in GF(p)$. Exactly three types of commutative subalgebras of order p^2 exist [14]:

1) containing multiplicative group possessing two-dimensional cyclicity and having order $\Omega = (p-1)^2$;
2) containing cyclic multiplicative group of order $\Omega = p(p-1)$;
3) containing cyclic multiplicative group of order $\Omega = (p^2 - 1)$.

The number of commutative subalgebras of the first (η_1), second (η_2), and third (η_3) type is equal to [14]:

$$\eta_1 = \frac{p(p+1)}{2}; \quad \eta_2 = p+1; \quad \eta_3 = \frac{p(p-1)}{2}. \tag{1}$$

In the paper [14] the formulas describing all elements of every type of the subalgebras are also derived, which provide possibility to express all elements of a subalgebra via coordinates of one given representtative (that is not a scalar vector) of the subalgebra.

The algebraic support of one of the algebraic signature schemes proposed in [17] represents a 4-dimensional FNAA (set over $GF(p)$ with $p = 2q + 1$, where q is a 128-bit prime) containing sufficiently large number of different

Table 1

The BVMT setting a sparse 4-dimensional FNAA over $GF(p)$; $\lambda \neq 0$ [14].

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	0	$\lambda\mathbf{e}_3$	$\mathbf{e}_0$	0
$\mathbf{e}_1$	$\lambda\mathbf{e}_2$	0	0	$\mathbf{e}_1$
$\mathbf{e}_2$	0	$\mathbf{e}_1$	$\mathbf{e}_2$	0
$\mathbf{e}_3$	$\mathbf{e}_0$	0	0	$\mathbf{e}_3$

commutative groups having order q^2 and possessing two-dimensional cyclicity (a minimum generator system of such groups includes two vectors of the same order equal to q). In that signature scheme the public key represents the set of the vectors Y, Z, U, and W calculated as follows:

$$\begin{aligned} Y &= AGB, \quad & Z &= AG^{x_1}B; \\ U &= AHB, \quad & W &= AH^{x_2}A^{-1}, \end{aligned} \tag{2}$$

where $x_1 < q$ and $x_2 < q$ are random natural numbers; the vectors G and H compose a minimum generator system of the commutative hidden group; the vectors A and B satisfy the conditions $AB \neq BA$, $AG \neq GA$, and $BG \neq GB$. The values x_1, x_2, A, and B are elements of the private key connected with the public key. The signature (e_1, e_2, e_3, S) to an electronic document M is generated as follows [17]:

1. Using random natural numbers $k < q$ and $t < q$, calculate the vector

$$R = AG^kH^tA^{-1}. \tag{3}$$

2. Using a specified 384-bit hash function f_h, calculate the first signature element $e = e_1||e_2||e_3 = f_h(M, R)$ represented as concatenation of three 128-bit integers e_1, e_2, and e_3.

3. Calculate the integers n and u:

$$n = \frac{k - x_1e_2e_3 - e_3}{e_3 + e_1e_3 + e_2e_3} \bmod q; \quad u = \frac{t - x_2e_2e_3 - e_1e_3}{e_3 + e_1e_3 + e_2e_3} \bmod q.$$

4. Calculate the second signature element

$$S = B^{-1}G^nH^uA^{-1}. \tag{4}$$

The signature verification procedure includes the next steps:

1. Calculate the vector $R' = \left(YS\,(US)^{e_1}\,(ZSW)^{e_2}\right)^{e_3}$.

2. Concatenate the vector R' to the document M and compute the hash value $e' = f_h(M, R')$.

3. If $e' = e$ ($e' \neq e$,), then the signature is genuine (false).

In the formulas (3) and (4) the integers k, t, n, and u are random, but the vectors G, H, A and B are fixed. Therefore, each of the vectors R and S takes only $q^2 = O(p^2)$, where $O(\cdot)$ is the order notation, different values in the FNAA containing p^4 different vectors. This shows that the signature randomization in the algorithm [17] is quite limitted. The latter creates potential preconditions for reducing security, which is assessed in [17] by the value of the computational difficulty of solving a system of quadratic equations connecting the elements of the public key with the elements of the secret key (see formulas (2)).

Indeed, one can show that a genuine signature $S_1 = B^{-1}G^{n_1}H^{u_1}A^{-1}$ defines four quadratic scalar equations with twelve fixed scalar uknowns (coordinates of the vectors B^{-1}, A^{-1}, and $G^{n_1}H^{u_1}$) and each additional genuine signature S_i ($i = 2, 3, \dots$) adds four cubic scalar equations containing only two new scalar unknowns (due to limitted signature randomization). The latter describes an unknown vector $G^{n_i}H^{u_i}$ from the hidden group that is fixed by coordinates of the vector $G^{n_1}H^{u_1}$ (see formula (8) in [17], which describes all elements of commutative subalgebra containing multiplicative group with two-dimensional cyclicity). For example, five (six) different genuine signatures set a system of 20 (24) scalar equations (quadratic and cubic) with 20 (22) unknowns.

A similar consideration of the system of scalar power equations defined by the vector $R' = R$ (for genuine signatures) and by formula (3) leads to a smaller system of quadratic and cubic equations (note that formula (3) defines the equation $RA = AG^kH^t$). Namely, three (four) different genuine signatures set a system of 12 (16) scalar equations (quadratic and cubic) with 12 (14) unknowns, whereas formulas (2) with the additional equations $GG^{x_1} = G^{x_1}G$, $GH = HG$, and $GH^{x_2} = H^{x_2}G$ define a system of 28 power equations with 24 unknowns [17].

In the algebraic signature algorithm [4] based on difficulty of solving large systems of power equations, consideration of the systems of scalar equation composed for both the randomization vectors R and the genuine signatures S is similar to the above case.

Thus, the limitted randomization of the signature in the known algebraic algorithms based on computational difficulty of solving large systems of power equations leads to potential reduction of the security. Therefore, the task of insuring the complete signature randomization is relevant.

3. Technique for complete randomization

Completeness of the signature randomization assumes the the signature element S can potentially take on arbitrary reversible value in the FNAA used as algebraic support. This can be provided with introducing a random reversible vector V as a multiplier in the formula for computation of the signature element S. However, this eliminates the possibility of using a verification equation with multiple entry of the signature element S. In order to get around this contradiction, you can use the technique of doubling the verification equation, which was previously used in the papers [12, 18] introducing specific signature algorithms with a hidden group, which are based on computational difficulty of the hidden discrete logarithm problem.

Namely, when using the FNAA specified by Table 1 over $GF(p)$, where $p = 2q+1$ with 192-bit prime q, we suppose the signature element S should satisfy the following two different verification equations in which the public key elements Y_1, T_1, Z_1, and U_1 in the first equation and Y_2, T_2, Z_2, and U_2 in the second equation are computed as masked elements of the hidden group $\Gamma_{<G,H>}$ set by the minumum generator system $<G, H>$:

$$\begin{cases} R_1' = Y_1^{e_1\sigma_1} T_1 Z_1^{e_2\sigma_2} U_1 S Q_1^{h_1 h_2}; \\ R_2' = Y_2^{e_1} T_2 Z_2^{e_2} U_2 S Q_2^{h}, \end{cases} \tag{5}$$

where Q_1 and Q_2 ($Q_1Q_2 \neq Q_2Q_1$) are two vectors of the order p^2-1, which represent common public parameters; $\sigma_1 < q$ and $\sigma_2 < q$ are auxiliary elements of the signature; $h = h_1||h_2 = f_h(M)$ is a 384-bit hash-function value represented as concatenation of two 192-bit integers h_1 and h_2.

The public key elements are computed as follows:

1. Generate a random pair of vectors $< G, H >$ of order q, which specify the minumum generator system of the hidden group of order q^2.

2. Generate at random natural numbers ($< q$) x_y, x_z, t_{11}, t_{12}, u_{11}, u_{12}, t_{21}, t_{22}, u_{21}, u_{22}.

3. Generate random vectors A, B, C, D, and F satisfying the inequalities $AB \neq BA$, $AG \neq GA$, $AC \neq CA$, $AD \neq DA$, $AF \neq FA$, $BG \neq GB$, $BC \neq CB$, $BD \neq DB$, $BF \neq FB$, $CG \neq GC$, $CD \neq DC$, $CF \neq FC$, $DG \neq GD$, $DF \neq FD$, and $FG \neq GF$.

4. Calculate the vectors $\{J_{t1}, J_{u1}, J_{t2}, J_{u2}\} \in \Gamma_{<G,H>}$: $J_{t1} = G^{t_{11}} H^{t_{12}}$, $J_{u1} = G^{u_{11}} H^{u_{12}}$, $J_{t2} = G^{t_{21}} H^{t_{22}}$, $J_{u2} = G^{u_{21}} H^{u_{22}}$.

5. Calculate the public key as the set of vectors $\{Y_1,Z_1,T_1,U_1,Y_2,Z_2,T_2,U_2\}$ (with total size equal to $\approx$768 bytes):

$$\begin{aligned} &Y_1 = AG^{x_y}A^{-1}; Z_1 = BH^{x_z}B^{-1}; T_1 = AJ_{t1}B^{-1}; U_1 = BJ_{u1}F^{-1};\\ &Y_2 = CGC^{-1}; Z_2 = DHD^{-1}; T_2 = CJ_{t2}D^{-1}; U_2 = DJ_{u2}F^{-1}. \end{aligned} \tag{6}$$

The private key corresponding to the public key is the next set of elements $\{x_y, x_u, G, H, J_{t1}, J_{u1}, J_{t2}, J_{u2}, A, B, C, D, F$ with total size equal to $\approx$1104 bytes.

If we specify computation of the pair of randomization vectors $R_1 = AG^{k_1}H^{r_1}J_{t1}J_{u1}VQ_1^{h_1h_2}$ and $R_2 = CG^{k_2}H^{r_2}J_{t2}J_{u2}VQ_2^h$ (where k_1, r_1, k_2, and r_2 are random natural numbers; h is the 384-bit hash value $h = h_1||h_2 = f_h(M)$ computed from the document M to be signed), then with the pair of verification equations (5) and with public key elements (6) the required signature element S is to be calculated as

$$S = FG^nH^uV, \tag{7}$$

where V is a random reversible vector and the integers n and u are precomputed, depending on the signature randomization elements e_1 and e_2, such that $e_1||e_2 = f_h(M, R_1, R_2)$, and on random integers k_1, r_1, k_2, and r_2.

Thus, the signature element S is computed depending on a random multiplier V, thefore complete signature randomization is provided.

4. The proposed signature scheme

The used algebraic support, the common public parameters Q_1, Q_2, the private key, and the public key have been presented in Section 3. The signature generation algorithm is described as follows:

1. Generate at random natural numbers k_1, r_1, k_2, and r_2 ($< q$) and calculate the 384-bit hash-function value $h = h_1||h_2 = f_h(M)$ (where M is a signed document; h_1 and h_2 are 192-bit integers) and the vectors R_1 and R_2:

$$\begin{aligned} &R_1 = AG^{k_1}H^{r_1}J_{t1}J_{u1}VQ_1^{h_1h_2};\\ &R_2 = CG^{k_2}H^{r_2}J_{t2}J_{u2}VQ_2^h. \end{aligned} \tag{8}$$

2. Compute the hash-function value $e = e_1||e_2$ (the first signature element), where $||$ denotes the concatenation operation, from the document M to which the vectors R_1 and R_2 are concatenated: $e = e_1||e_2 = f_h(M, R_1, R_2)$, where e_1 and e_2 are 192-bit integers.

3. Calculate the integers n, u, σ_1, and σ_2:

$$n = k_2 - e_1 \bmod q; \qquad u = r_2 - e_2 \bmod q;$$
$$\sigma_1 = \frac{k_1 - k_2 + e_1}{x_y e_1} \bmod q; \qquad \sigma_2 = \frac{r_1 - r_2 + e_2}{x_z e_2} \bmod q.$$

4. Calculate the second signature element S:

$$S = FG^n H^u V.$$

The signature is $e_1, e_2, \sigma_1, \sigma_2, S$ and has total size equal to $\approx$192 bytes. Computational complexity w of the signature generation alorithm is roughly equal to six exponentiations in the FNAA set by Table 1, i. e., to $w \approx 13,824$ multiplications modulo a 193-bit prime p.

The verification of the signature $e_1, e_2, \sigma_1, \sigma_2, S$ to the document M is performed with the following algorithm:

1. Calculate the hash-function value $h = h_1||h_2 = f_h(M)$ from the document M. Then calculate the vectors R'_1 and R'_2 by formulas (5).

2. Compute the hash-function value e' from the document M to which the vectors R'_1 and R'_2 are concatenated: $e' = f(M, R'_1, R'_2)$.

3. If $e' = e_1||e_2$, then the signature is genuine, else the signature is false.

The computational complexity w' of the signature verification algorithm is roughly equal to four exponentiations in the 4-dimensional FNAA used as algebraic support, i. e., $w' \approx 9,216$ multiplications modulo a 193-bit prime p.

Correctness proof of the signature scheme.
Taking into account that the vectors $G, H, J_{t1}, J_{u1}, J_{t2}, J_{u2}$ are elements of the commutative group $\Gamma_{<G,H>}$ and have order q, one can show that the correctly computed signature $e_1, e_2, \sigma_1, \sigma_2, S$ passes the verification procedure as genuine one:

$$\begin{aligned}
&R'_1 = Y_1^{e_1\sigma_1} T_1 Z_1^{e_2\sigma_2} U_1 S Q_1^{h_1 h_2} \\
&= \left(AG^{x_y}A^{-1}\right)^{e_1\sigma_1} AJ_{t1}B^{-1} \left(BH^{x_z}B^{-1}\right)^{e_2\sigma_2} BJ_{u1}F^{-1} \left(FG^n H^u V\right) Q_1^{h_1 h_2} \\
&= AG^{x_y e_1 \sigma_1} J_{t1} H^{x_z e_2 \sigma_2} J_{u1} G^n H^u V Q_1^{h_1 h_2} \\
&= AG^{x_y e_1 \frac{k_1 - k_2 + e_1}{x_y e_1}} J_{t1} H^{x_z e_2 \frac{r_1 - r_2 + e_2}{x_z e_2}} J_{u1} G^{k_2 - e_1} H^{r_2 - e_2} V Q_1^{h_1 h_2} \\
&= AG^{k_1 - k_2 + e_1} H^{r_1 - r_2 + e_2} G^{k_2 - e_1} H^{r_2 - e_2} J_{t1} J_{u1} V Q_1^{h_1 h_2} \\
&= AG^{k_1} H^{r_1} J_{t1} J_{u1} V Q_1^{h_1 h_2} = R_1;
\end{aligned}$$

$$R'_2 = Y_2^{e_1} T_2 Z_2^{e_2} U_2 S Q_2^{h}$$

$= \left(CGC^{-1}\right)^{e_1} CJ_{t2}D^{-1}\left(DHD^{-1}\right)^{e_2} DJ_{u2}F^{-1}\left(FG^nH^uV\right)Q_1^{h_1h_2}$
$= CG^{e_1}J_{t2}H^{e_2}J_{u2}G^{k_2-e_1}H^{r_2-e_2}VQ_2^h = R_2;$

$\{R_1' = R_1;\ R_2' = R_2\} \ \Rightarrow\ f_h(M, R_1', R_2') = f_h(M, R_1, R_2) \ \Rightarrow\ e' = e_1||e_2.$

5. Disscussion

The completeness of signature randomization in the algorithm described in Section 4 is connected with the fact that calculating a value of genuine signature involves multiplying by a random vector V, therefore, for arbitrary fixed set of values of the vectors F, G^n, and H^u (see formula (7)) the value of the signature can take any reversible value in the FNAA used as an algebraic support. However, for a certain number of genuine signatures it is possible to calculate the unknown value F (the unknown vectors G^n and H^u are not element of the private key).

The latter can be done by constructing a systems of vector equations set by formulas (7) and (8) for different signatures S connected with different pairs of the vectors R_1 and R_2. For example, one signature S defines the following three quadratic vector equations

$$\begin{aligned} &SV^{-1} = F\left(G^nH^u\right) \\ &R_1V^{-1}Q_1^{-h_1h_2} = A\left(G^{k_1}H^{r_1}J_{t1}J_{u1}\right); \\ &R_2V^{-1}Q_2^{-h} = C\left(G^{k_2}H^{r_2}J_{t2}J_{u2}\right), \end{aligned} \tag{9}$$

where the vectors R_1, R_2, $Q_1^{h_1h_2}$, and Q_2^h are calculated in framework of the signature verification procedure.

In the system of equations (9) each of the products G^nH^u, $G^{k_1}H^{r_1}J_{t1}J_{u1}$, and $G^{k_2}H^{r_2}J_{t2}J_{u2}$ sets a random selection of an element from a hidden group $\Gamma_{<G,H>}$. The latter is fixed, if we fix the unknown $G = (g_0,\ g_1,\ g_2,\ g_3)$. All elements $X = (x_0,\ x_1,\ x_2,\ x_3)$ of the commutative subalgebra that contains the group $\Gamma_{<G,H>}$ are described by the following formula including fixed coordinates (g_0, g_1, g_2, g_3) and two scalar variables $i, j \in \{0, 1, ..., p-1\}$ (see formula (8) in [14]):

$$X = (x_0, x_1, x_2, x_3) = \left(i,\ \frac{g_1}{g_0}i,\ j, j + \frac{g_3 - g_2}{g_0}i\right). \tag{10}$$

Therefore, a random selection from the hidden group can be described with the scalar unknowns i and j. Using formula (10) we can reduce the number of scalar unknowns, but the respective scalar equations become cubic (however, the computational complexity of solving a system of quadratic and of cubic equation is of the same order for the same number of equations [3]). Taking into account these remarks, we have four fixed vector unknowns A, C, F, and G (setting 16 scalar unknowns that are coodinates of the said vectors), a unique vector unknown V^{-1} for a triple of equations related to the same signature, and unique pair of scalar unknowns i and j in each vector equation of the considered system. If we have b different genuine signatures, then we can compose a system of $3b$ different vector equations and represent it as a system of $12b$ cubic scalar equations with d unknowns, where

$$d = 16 + 4b + 2{\cdot}3b = 16 + 10b.$$

From the condition $d = 12b$ we can fined the number of signatures $b = 8$, when the nuber of scalar unknowns is equal to the number of scalar equations and the system includes 96 power (quadratic and cubic) scalar equations.

A system of quadratic vector equations composed using formulas (6) describing connection of the public-key elements with the private-key elements is as follows:

$$\begin{cases} Y_1A = AG^{x_y}; \quad Z_1B = BH^{x_z}; \quad T_1B = AJ_{t1}; \quad U_1F = BJ_{u1}; \\ Y_2C = CG; \quad Z_2D = DH; \quad T_2D = CJ_{t2}; \quad U_2F = DJ_{u2}; \\ GH = HG; \quad GJ_{t2} = J_{t2}G; \quad GJ_{u2} = J_{u2}G; \\ GG^{x_y} = G^{x_y}G; \quad GH^{x_z} = H^{x_z}G; \quad GJ_{t1} = J_{t1}G; \quad GJ_{u1} = J_{u1}G, \end{cases} \tag{11}$$

where the last seven equations reflect the fact that the unknown vectors G, G^{x_y}, H, H^{x_z}, J_{t1}, J_{u1}, J_{t2}, and J_{u2} are selected from the hidden group $\Gamma_{<G,H>}$. When representing this system of vector equation as a system of scalar equations, the last seven equations in (11) can be reduced with using formula (10) and considering the unknown vector $G = (g_0,\ g_1,\ g_2,\ g_3)$ as element fixing the group $\Gamma_{<G,H>}$ (coordinates of arbitrary vector included in the hidden group can be described via coordinates of G and a unique pair of scalar unknowns i and j). For example, using Table 1, the first vector equation in (11), namely, $Y_1A = AG^{x_y}$ (where $Y_1 = (y_0, y_1, y_2, y_3)$ and

$A = (a_0, a_1, a_2, a_3))$ is represented by the following four scalar equations:

$$\begin{cases} y_0 a_2 + y_3 a_0 = a_0 j + a_3 i; \\ y_2 a_1 g_0 + y_1 a_3 g_0 = a_2 g_1 i + a_1 g_0 j + a_1 g_3 - a_1 g_2; \\ \lambda y_1 a_0 + y_2 a_2 = \lambda a_1 i + a_2 j; \\ \lambda y_0 a_1 g_0 + y_3 a_3 g_0 = \lambda a_0 g_1 i + a_3 g_0 j + a_3 g_3 - a_3 g_2, \end{cases}$$

Each of the other vector equations in (11) is transformed into a similar four scalar equations.

In this way we get a system of 32 quadratic and cubic scalar equations with 40 scalar unknowns. The latter suggests that there are numerous solutions defining many equivalent keys. However, their calculation involves solving a system of 32 cubic equations. The complexity of solving a system of power equations depends exponentially on the number of equation (and weakly depends on the degree of equations [3]) and determines the security of the algorithm under consideration to a direct attack.

A system of power equations composed for a set of known genuine signatures includes significantly larger number of equations than the system composed from formulas describing connection of public-key elements with the private-key elements, therefore one can conclude that using the known signatures can not be used to reduce the security level of the introduced signature algorithm, i. e. the proposed signature randomization technique is efficient.

The best-known methods for solving a large system of power equations use the algorithms F4 [5] and F5 [6]. Taken into account the latter algorithms, the paper [2] presents the minimum number of power equations in different fields $GF(q')$ that is requiered to get the security level (ψ) 2^{80}, 2^{100}, $2^{128,}$ 2^{192}, and 2^{256} for the case when the number of equations is approximately equal to the number of unknowns (see Table 2). Using that results, security of the introduced signature algorithm to direct attack can be estimeted as $\approx 2^{100}$. To improve the security level one can try to implement the algorithm from Section 4 on FNAAs having dimensions $m \geq 6$. Suitable non-commutative algebras are described, for example, in [15]. However, the decomposition of that FNAAs into the set of commutative subalgebras (results of which are useful for both the design and the security evaluation) has not been studied yet, therefore, for such versions of the algorithm it is not entirely clear how one can minimize the number of equations in the system of scalar equations, to which the system of vector equations (11) is reduced.

Table 2

The minimum number of equations in $GF(q')$ by [2].

$\psi = \dots$	2^{80}	2^{100}	2^{128}	2^{192}	2^{256}
$q' = 16$	30	39	51	80	110
$q' = 31$	28	36	49	75	103
$q' = 256$	26	33	43	68	93

Leaving the said implementations for future research, we note that at the moment, the assessment of the security level of the proposed algorithm is quite rough and applies only to direct attacks related to solving a system of quadratic vector equations (11) connecting elements of public and private keys. Obviously, further analysis of resistance to attacks of various types is required. At the moment we only claim that the randomization technique used ensures sufficient completeness of the signature randomization.

In the first and second verification equations (5) the most right multipliers $Q_1^{h_1 h_2}$ and Q_2^h are used to insure security to the following algorithm for forging a signature. Suppose a genuine signature $e_1, e_2, \sigma_1, \sigma_2, S$ is available and an attacker is intended to forge a signature $e_1'', e_2'', \sigma_1'', \sigma_2'', S''$ to the document M''. From equations (5) he can calculate the vectors $R_1'' = R_1'$ and $R_2'' = R_2'$, the values $e'' = e_1''||e_2'' = f_h\left(M'', R_1'', R_2''\right)$ and $h'' = h_1''||h_2'' = f_h\left(M''\right)$, where e_1'', e_2'', h_1'', and h_2'' are 192-bit integers.

Since $R_1'' = R_1'$, from the first of equations (5) one gets the value $S'' = S_1''$:

$$Y_1^{e_1\sigma_1} T_1 Z_1^{e_2\sigma_2} U_1 S Q_1^{h_1 h_2} = Y_1^{e_1''\sigma_1''} T_1 Z_1^{e_2''\sigma_2''} U_1 S_1'' Q_1^{h_1'' h_2''} \Rightarrow$$
$$\Rightarrow S_1'' = F G^{x_y(e_1\sigma_1 - e_1''\sigma_1'')} H^{x_z(e_2\sigma_2 - e_2''\sigma_2'')} F^{-1} S Q_1^{h_1 h_2 - h''_1 h_2''},$$

Since $R_2'' = R_2'$, from the second of equations (5) one gets the value $S'' = S_2''$:

$$Y_2^{e_1\sigma_1} T_2 Z_2^{e_2\sigma_2} U_2 S Q_2^{h} = Y_2^{e_1''\sigma_1''} T_2 Z_2^{e_2''\sigma_2''} U_2 S_2'' Q_2^{h''} \Rightarrow$$
$$\Rightarrow S_2'' = F G^{e_1\sigma_1 - e_1''\sigma_1''} H^{e_2\sigma_2 - e_2''\sigma_2''} F^{-1} S Q_2^{h - h''}.$$

Then the attacker calculates the signature elements $\sigma_1'' = \sigma_1 e_1 e_1''^{-1}$ and $\sigma_2'' = \sigma_2 e_2 e_2''^{-1}$ for which he has $S_1'' Q_1^{h_1'' h_2'' - h_1 h_2} = S_2'' Q_2^{h'' - h}$.

Thus, due to using the multiplications by $Q_1^{h_1 h_2}$ and Q_2^h (such that $Q_1 Q_2 \neq Q_2 Q_1$) in the first and second verification equations, correspondingly, the probability of the equality $S_1'' = S_2'' = S''$ that take place, if $h'' = h$ (i. e., probability of successful signature forgery) is negligible ($\approx 2^{-384}$ for the used 384-bit hash function).

6. Conclusion

The proposed technique for complete signature randomization can be implemented in algebraic signature algorithms with a hidden group and doubled verification equation. The structure of the algebra used as an algebraic carrier, from the point of view of decomposition into a set of commutative subalgebras, is essential for the development of signature schemes and assessment of their security. To develop new versions of the proposed algorithm on FNAAs of dimension $m \geq 6$, it is of interest to study the structure of the latter.

Acknowledgement. The author sincerely thanks the anonymous Referee for his comments on improving the content of the article.

References

[1] **G. Alagic, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, D. Apon**, *Status report on the third round of the NIST post-quantum cryptography standardization process* (2022) NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8413, (Accessed December 23, 2023)

[2] **J. Ding, A. Petzoldt**, *Current state of multivariate cryptography*, IEEE Security and Privacy Magazine, **15** (2017), no. 4, 28 – 36.

[3] **J. Ding, A. Petzoldt, D.S. Schmidt**, *Solving polynomial systems*, In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. **80** (2020), 185 – 248.

[4] **M.T. Duong, D.N. Moldovyan, B.V. Do, M.H. Nguyen**, *post-quantum signature algorithms on noncommutative algebras, using difficulty of solving systems of quadratic equations*, Computer Standards and Interfaces, **86** (2023), 103740.

[5] **J.-C. Faugére**, *A new efficient algorithm for computing Gröbner basis* ($F4$), J. Pure Appl. Algebra, **139** (1999), no. 1-3, 61 – 88.

[6] **J.-C. Faugére**, *A new efficient algorithm for computing Gröbner basis without reduction to zero* ($F5$). In: Proceedings of the International Symposium on Symbolic and Algebraic Computation (2002), 75 – 83.

[7] **Y. Ikematsu, S. Nakamura, T. Takagi**, *Recent progress in the security evaluation of multivariate publickey cryptography*, IET Information Security, (2022), 1 – 17.

[8] **T. Matsumoto, H. Imai**, *Public quadratic polynomial-tuples for efficient signature verification and message-encryption*, Advances in Cryptology (Eurocrypt'88), Springer Berlin Heidelberg, (1988), 419 – 453.

[9] **A.A. Moldovyan, D.N. Moldovyan**, *A new method for developing signature algorithms*, Bul. Acad. Sci. Moldova, Mathematics, (2022), no. 1(98), 56 – 65.

[10] **A.A. Moldovyan, N.A. Moldovyan**, *Vector finite fields of characteristic two as algebraic support of multivariate cryptography*, Computer Sci. J. Moldova, **32** (2024), no. 1(94), 46 – 60.

[11] **D.N. Moldovyan**, *A practical digital signature scheme based on the hidden logarithm problem*, Computer Sci. J. Moldova, **29** (2021), no. 2(86), 206 – 226.

[12] **D.N. Moldovyan, A.A. Moldovyan, N.A. Moldovyan**, *An enhanced version of the hidden discrete logarithm problem and its algebraic support*, Quasigroups and Related Systems. **28** (2020), no. 2, 269 – 284.

[13] **D.N. Moldovyan, A.A. Moldovyan, N.A. Moldovyan**, *A new design of the signature schemes based on the hidden discrete logarithm problem*, Quasigroups and Related Systems, **29** (2021), no. 1, 97 – 106.

[14] **D.N. Moldovyan, A.A. Moldovyan, N.A. Moldovyan**, *Structure of a finite non-commutative algebra set by a sparse multiplication table*, Quasigroups and Related Systems, **30** (2022), no. 1, 133 – 140.

[15] **N.A. Moldovyan**, *Unifed method for defining fnite associative algebras of arbitrary even dimensions*, Quasigroups and Related Systems, **26** (2018), no. 2, 263 – 270.

[16] **N.A. Moldovyan**, *Signature schemes on algebras, satisfying enhanced criterion of post-quantum security*, Bull. Acad. Sci. Moldova, Mathematics, (2020), no. 2(93), 62 – 67.

[17] **N.A. Moldovyan**, *Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations*, Quasigroups and Related Systems, **30** (2022), no. 2, 287 – 298.

[18] **N.A. Moldovyan, A.A. Moldovyan**, *Candidate for practical post-quantum signature scheme*, Vestnik Saint Petersburg Univ., Applied Math., Computer Sci., Control Processes, **16** (2020), no. 4, 455 – 464.

Received January 8, 2024

St. Petersburg Federal Research Center of the Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg, Russia
e-mail: maa1305@yandex.ru

Quasigroups and Related Systems **32** (2024), 109 – 118

https://doi.org/10.56415/qrs.v32.09

On weakly f-clean rings

Fatemeh Rashedi

Abstract. Let R be an associative ring with identity and $Id(R)$ and $K(R)$ denote the set of idempotents and full elements of R respectively. The notion of weakly f-clean rings where element r can be written as $r = f + e$ or $r = f - e$, $e \in Id(R)$ and $f \in K(R)$ was introduced. Different properties of weakly f-clean rings were studied. It was shown that a left quasi-duo ring R is weakly clean if and only if R is a weakly f-clean ring. Finally, it was shown that the ring of skew Hurwitz series $T = (HR, \alpha)$ where α is an automorphism of R is weakly f-clean if and only if R is weakly f-clean.

1. Introduction

Let R be an associative ring with identity and $U(R)$ and $Id(R)$ denote the set of units and idempotents of R respectively. The ring R is clean if for each $r \in R$ there exist $u \in U(R)$ and $e \in Id(R)$ such that $r = u + e$ [2, 15]. A ring R is weakly clean if each $r \in R$ can be written in the form $r = u+e$ or $r = u-e$ where $u \in U(R)$ and $e \in Id(R)$ [1, 5, 8, 13]. Other generalizations of clean rings have been introduced [3, 6, 9, 10, 16] An element $f \in R$ is full element if there exist $x, y \in R$ such that $xfy = 1$. $K(R)$ will denote the set of full elements of R. An element $r \in R$ is said to be f-clean if it can be written as the sum of an idempotent and a full element. A ring R is said to be f-clean if each element in R is a f-clean element [12, 14].

In this paper, we introduce the notion of a weakly f-clean ring as a new generalization of a weakly clean ring and a f-clean ring. Let R be a ring. An element $r \in R$ is called weakly f-clean if there exist $f \in K(R)$ and $e \in Id(R)$ of R such that $r = f + e$ or $r = f - e$. A ring R is called weakly f-clean if every element of R is weakly f-clean. Various properties of weakly f-clean rings and weakly f-clean elements were studied. We showed that, every homomorphic image of a weakly f-clean ring is weakly f-clean and

2010 Mathematics Subject Classification: 16U99, 16Z05.

Keywords: Weakly clean ring, f-clean ring, Weakly f- clean ring.

$\prod_{i\in I} R_i$ is weakly f-clean if and only if every R_i is weakly f-clean (Lemma 2.8). We also showed that, if R is a weakly f-clean ring and $e \in R$ is a central idempotent, then the corner ring eRe is weakly f-clean (Lemma 2.13). A left quasi-duo ring R is weakly clean if and only if R isa weakly f-clean ring (Theorem 2.17). Finally, we showed that the ring of skew Hurwitz series $T = (HR, \alpha)$ where α is an automorphism of R is weakly f-clean if and only if R is weakly f-clean (Theorem 2.23).

2. Main results

We start our work with the following definition.

Definition 2.1. An element $f \in R$ is said to be a *full element* if there exist $x, y \in R$ such that $xfy = 1$. The set of all full elements of a ring R will be denoted by $K(R)$. Obviously, invertible elements and one-sided invertible elements are all in $K(R)$ [14].

Definition 2.2. An element in R is said to be *f-clean* if it can be written as the sum of an idempotent and a full element. A ring R is called a *f-clean ring* if each element in R is a f-clean element [14].

In the following, we define the weakly f-clean rings. Then we study some of the basic properties of weakly f-clean rings. Moreover, we give some necessarily examples.

Definition 2.3. Let R be a ring. Then an element $r \in R$ is called *weakly f-clean* if there exist $f \in K(R)$ and $e \in Id(R)$ of R such that $r = f + e$ or $r = f - e$. A ring R is called *weakly f-clean* if every element of R is weakly f-clean.

Example 2.4. Every clean, weakly clean or f-clean ring is weakly f-clean. Since every purely infinite simple ring is a f-clean ring, and so is weakly f-clean [14]. $(\mathbb{Z}_8, +, .)$ is a weakly f-clean ring, but $(\mathbb{Z}, +, .)$ is not a weakly f-clean ring.

A weakly f-clean ring is not f-clean, in general.

Example 2.5. Let p and q be two distinct odd primes. Then the ring

$$\mathbb{Z}_{(p)} \cap \mathbb{Z}_{(q)} = \left\{ \frac{r}{s} \mid r, s \in \mathbb{Z}, s \neq 0, p \nmid s, q \nmid s \right\}$$

is a weakly f-clean ring that is not f-clean.

Proposition 2.6. *Let R be a ring and $r \in R$. Then r is weakly f-clean if and only if $-r$ weakly f-clean.*

Proof. Suppose that r is weakly f-clean. Hence $r = f + e$ or $r = f - e$ for some $f \in K(R)$ and $e \in Id(R)$. Then $-r = -f - e$ or $-r = -f + e$. Since $-f \in K(R)$, $-r$ weakly f-clean. □

Proposition 2.7. *Let R be a ring and every idempotent of R is central. Then $r \in R$ is weakly f-clean if and only if $1-r$ or $1+r$ is f-clean.*

Proof. Suppose r is weakly f-clean. Hence $r = f + e$ or $r = f - e$ for some $f \in K(R)$ and $e \in Id(R)$. Then $1 - r = -f + (1 - e)$ or $1 + r = f + (1 - e)$, and so $1 - r$ or $1 + r$ is f-clean. Conversely, assume that $1 - r$ or $1 + r$ is f-clean. Hence $1 - r = f + e$ or $1 + r = f + e$ for some $f \in K(R)$ and $e \in Id(R)$. Then $r = -f + (1 - e)$ or $r = f - (1 - e)$, thus r is weakly f-clean. □

Lemma 2.8.

(*i*) *Every homomorphic image of a weakly f-clean ring is weakly f-clean.*

(*ii*) *Let $\{R_i\}_{i\in I}$ be a family of rings. Then $\prod_{i\in I} R_i$ is weakly f-clean if and only if every R_i is weakly f-clean.*

Proof. (*i*). Is clear.
(*ii*). Suppose that every R_i is weakly f-clean and $r = (r_i) \in R$. Hence $r_i = f_i + e_i$ or $r_i = f_i - e_i$ for some $f_i \in K(R_i)$ and $e_i \in Id(R_i)$. Then $r = f + e$ such that $f = (f_i) \in K(R)$ and $e = (e_i) \in Id(R)$, and so R is weakly f-clean. The converse follows from (*i*). □

Let I be an ideal of a ring R. We say that *idempotents of R are lifted modulo I* if, for given $r \in R$ with $r - r^2 \in I$, there exists $e \in Id(R)$ such that $e - r \in Id(R)$ [15].

Lemma 2.9. *Let R be a ring such that idempotents are lifted modulo $J(R)$. Then R is weakly f-clean if and only if $R/J(R)$ is weakly f-clean.*

Proof. Suppose that R is weakly f-clean. Hence $R/J(R)$ is weakly f-clean, by Lemma 2.8. Conversely, assume that $R/J(R)$ is weakly f-clean and $r \in R$. Hence $r+J(R) = (f+J(R))+(e+J(R))$ or $r+J(R) = (f+J(R))-(e+J(R))$ with $e^2-e \in J(R)$ and $(x+J(R))(f+J(R))(y+J(R)) = 1+J(R)$ for some $x, y \in R$. Since idempotents can be lifted modulo $J(R)$, e is an idempotent and $r = f + b + e$ or $r = f + b - e$ for some $b \in J(R)$. Since $(x+J(R))(f+J(R))(y+J(R)) = 1+J(R)$, $xfy = 1+z \in 1+J(R) \subseteq U(R)$ for some $z \in J(R)$. Therefore, there exist $x_1, y_1 \in R$ such that $x_1 f y_1 = 1$. Hence $x_1(f+b)y_1 = 1+x_1 b y_1 \in 1+J(R) \subseteq U(R)$. Thus $x_1(f+b)y_1 u^{-1} = 1$ for some $u \in U(R)$, and so $f + b \in K(R)$. Then R is weakly f-clean. □

Lemma 2.10. *Let R be a ring. Then R is weakly f-clean if and only if for every $r \in R$ there exist $g \in Id(R)$ and $f \in K(R)$ such that $gr = gf$ and $(g-1)(r-1) = (g-1)f$ or $gr = gf$ and $(g-1)(r-1) = (g-1)f + 2(1-g)$.*

Proof. Suppose that R is weakly f-clean and $r \in R$. Hence $r = f + e$ or $r = f - e$ for some $e \in Id(R)$ and $f \in K(R)$. Assume $g = 1-e$. If $r = f+e$, then $gr = g(f + e) = gf$ and $(g - 1)(r - 1) = (g - 1)f$. If $r = f - e$, then $gr = g(f + e) = gf$ and $(g - 1)(r - 1) = (g - 1)f + 2(1 - g)$. Conversely, assume that for every $r \in R$ there exist $g \in Id(R)$ and $f \in K(R)$ such that $gr = gf$ and $(g - 1)(r - 1) = (g - 1)f$. Then $gf - f = gr - g - r + 1$, and so $r = f + (1 - g)$. If for every $r \in R$ there exist $g \in Id(R)$ and $f \in K(R)$ such that $gr = gf$ and $(g-1)(r-1) = (g-1)f + 2(1-g)$, then $gf - f + 2(1 - g) = gr - g - r + 1$, and so $r = f - (1 - g)$. Therefore R is weakly f-clean. □

Each polynomial ring over a nonzero commutative ring is not weakly clean [1, Theorem 1.9]. If R is commutative ring, then $U(R) = K(R)$, R is weakly clean if and only if R is weakly f-clean. Hence each polynomial ring over a nonzero commutative ring is not weakly f-clean.

Lemma 2.11. *Let R be a ring such that idempotents are lifted modulo $J(R)$ and $R[\alpha] = R + R\alpha + \cdots + R\alpha^n$ with $\alpha^{n+1} = 0$. Then R is weakly f-clean if and only if $R[\alpha]$ is weakly f-clean.*

Proof. Suppose that R is weakly f-clean. Since $J(R[\alpha]) = J(R) + \langle\alpha\rangle$,

$$R[\alpha]/J(R[\alpha]) \cong R/J(R).$$

Then $R[\alpha]/J(R[\alpha])$ is weakly f-clean, by Lemma 2.9. Since idempotents can be lifted modulo $J(R[\alpha])$, $R[\alpha]$ is weakly f-clean, by Lemma 2.9. Conversely, suppose that $R[\alpha]$ is weakly f-clean. Since $R[\alpha]/J(R[\alpha]) \cong R/J(R)$, $R/J(R)$ is weakly f-clean. Since idempotents can be lifted modulo $J(R)$, R is weakly f-clean, by Lemma 2.9. □

Proposition 2.12. *Let R be a ring and $e \in Id(R)$ such that $r \in eRe$ is weakly f-clean in eRe. Then r is weakly f-clean in R.*

Proof. Suppose $r \in eRe$ is weakly f-clean in eRe. Hence $r = f + g$ or $f - g$ for some $g \in Id(eRe)$ and $f \in K(eRe)$, and so there exist $x, y \in eRe$ such that $xfy = e$. If $r = f + g$, then $(x - (1 - e))(f - (1 - e))(y + (1 - e)) = (xfy + (1 - e)) = 1$, and so $f - (1 - e) \in K(R)$. It is clear that $g + (1 - e) \in Id(R)$. Hence $r = (f - (1 - e)) + (g + (1 - e))$. If $r = f - g$, then $(x + (1 - e))(f + (1 - e))(y + (1 - e)) = (xfy + (1 - e)) = 1$, and so $f + (1 - e) \in K(R)$. It is clear that $g + (1 - e) \in Id(R)$. Hence $r = (f + (1 - e)) - (g + (1 - e))$. Therefore r is weakly f-clean in R. $\square$

Lemma 2.13. *Let R be a weakly f-clean ring and $e \in R$ be a central idempotent. Then the corner ring eRe is weakly f-clean.*

Proof. Assume that R is a weakly f-clean ring and $e \in R$ is a central idempotent. Hence eRe is homomorphic image of R. Then eRe is weakly f-clean, by Lemma 2.8. $\square$

Let R be a ring and ${}_RM_R$ be an R-R-bimodule which is a ring possibly without a unity in which $(mn)r = m(nr)$, $(mr)n = m(rn)$ and $(rm)n = r(mn)$ held for all $m, n \in M$ and $r \in R$. The ideal extension of R by M is defined to be the additive abelian group $I(R, M) = R \oplus M$ with multiplication $(r, m)(s, n) = (rs, rn + ms + mn)$.

Lemma 2.14. *Let R be a weakly f-clean and ${}_RM_R$ be an R-R-bimodule such that for any $m \in M$, there exists $n \in M$ such that $m + n + nm = 0$. Then the ideal-extension $I(R, M)$ of R by M is weakly f-clean.*

Proof. Suppose that $(r, m) \in I(R, M)$. Hence $r = f + e$ or $r = f - e$ for some $e \in Id(R)$ and $f \in K(R)$. Then $(r, m) = (f, m) + (e, 0)$ or $(r, m) = (f, m) - (e, 0)$. It is clear that $(e, 0) \in Id(I(R, M))$. Assume that $xfy = 1$. Hence $xmy \in M$, and so there exists $n \in M$ such that $xmy + n + nxmy = 0$. Then $(x, nx)(f, m)(y, 0) = 1$, and so $(f, m) \in K(Id(I(R, M))$. Therefore $Id(I(R, M)$ is weakly f-clean. $\square$

Let R be a ring and σ be a ring endomorphism of R. Then the skew power series ring $R[[x; \sigma]]$ of R is the ring obtained by giving the formal power series ring over R with the new multiplication $xr = \sigma(r)x$ for all $a \in R$. In particular, $R[[x]] = R[[x; 1_R]]$.

Lemma 2.15. *Let R be a ring and σ be a ring endomorphism of R. Then the following statements are equivalent.*

(*i*) *R is a weakly f-clean ring.*

(*ii*) *The formal power series ring* $R[[x]]$ *of* R *is a weakly* f*-clean ring.*

(*iii*) *The skew power series ring* $R[[x;\sigma]]$ *of* R *is a weakly* f*-clean ring.*

Proof. $(ii) \Rightarrow (i)$. Suppose $R[[x]]$ is a weakly f-clean ring. Since R is a homomorphic image of $R[[x]]$, R is weakly f-clean, by Lemma 2.8.
$(iii) \Rightarrow (i)$. Suppose $R[[x;\sigma]]$ is a weakly f-clean ring. Since R is a homomorphic image of $R[[x;\sigma]]$, R is weakly f-clean, by Lemma 2.8.
$(i) \Rightarrow (iii)$. Suppose R is a weakly f-clean ring and $g = r_0 + r_1x + \cdots \in R[[x;\sigma]]$. Then $r_0 = f_0 + e_0$ or $r_0 = f_0 - e_0$ for some $f_0 \in K(R)$ and $e_0 \in Id(R)$. If $r_0 = f_0 + e_0$ and $g' = g - e_0 = f_0 + r_1x + \cdots$ such that $x_0f_0y_0 = 1$ for some $x_0, y_0 \in R$, then $u = (x_0 + \cdots)g'(y_0 + \cdots) = 1 + x_0r_1\sigma(y_0)x + \cdots \in U(R[[x;\sigma]])$. Hence $g' \in K(R[[x;\sigma]])$, and $g = g' + e_0$ with $e_0 \in Id(R[[x;\sigma]])$. If $r_0 = f_0 - e_0$ and $g' = g + e_0 = f_0 + r_1x + \cdots$ such that $x_0f_0y_0 = 1$ for some $x_0, y_0 \in R$, then $u = (x_0 + \cdots)g'(y_0 + \cdots) = 1 + x_0r_1\sigma(y_0)x + \cdots \in U(R[[x;\sigma]])$. Hence $g' \in K(R[[x;\sigma]])$, and $g = g' - e_0$ with $e_0 \in Id(R[[x;\sigma]])$. Therefore $R[[x;\sigma]]$ is weakly f-clean.
$(i) \Rightarrow (ii)$. Suppose R is a weakly f-clean ring. Since $R[[x]] = R[[x;1_R]]$, the proof is similar to $(i) \Longrightarrow (iii)$. $\square$

Theorem 2.16. *Let* R *be a ring and* $r \in R$ *is a weakly* f*-clean element. Then* $B = \begin{pmatrix} r & s \\ 0 & 0 \end{pmatrix}$ *is a weakly* f*-clean element in* $M_2(R)$ *for every* $s \in R$.

Proof. Suppose $r \in R$ is a weakly f-clean element. Then $r = f + e$ or $r = f - e$ for some $f \in K(R)$ and $e \in Id(R)$. Hence $xfy = 1$ for some $x, y \in R$. If $r = f + e$, then

$$B = \begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} f & y \\ 0 & -1 \end{pmatrix},$$

such that $\begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix} \in Id(M_2(R))$ and $\begin{pmatrix} f & y \\ 0 & -1 \end{pmatrix} \in K(M_2(R))$, by [14, Proposition 2.6]. If $r = f - e$, then

$$B = \begin{pmatrix} f & s \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} e & 0 \\ 0 & 0 \end{pmatrix}.$$

such that $\begin{pmatrix} e & 0 \\ 0 & 0 \end{pmatrix} \in Id(M_2(R))$ and

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} f & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and so $\begin{pmatrix} f & s \\ 0 & 1 \end{pmatrix} \in K(M_2(R))$. Therefore $B = \begin{pmatrix} r & s \\ 0 & 0 \end{pmatrix}$ is a weakly f-clean element in $M_2(R)$ for every $s \in R$. □

A ring R is said to be *left quasi-duo*, if every maximal left ideal of R is a two-sided ideal. Commutative rings, local rings, rings in which every nonunit has a power that is central are all belong to this class of rings [17] . A ring R is said to be *Dedekind finite* if $rs = 1$ always implies $sr = 1$ for any $r, s \in R$.

Theorem 2.17. *Let R be a left quasi-duo ring. Then the following statements are equivalent.*

(*i*) *R is a weakly clean ring.*

(*ii*) *R is a weakly f-clean ring.*

Proof. $(i) \Rightarrow (ii)$. Is clear.
$(ii) \Rightarrow (i)$. Suppose R is a weakly f-clean ring. Since R is a left quasi-duo ring, $K(R) \subseteq U(R)$, by [14, Theorem 2.9]. Hence R is a weakly clean ring. □

Corollary 2.18. *Let R be a commutative (local or Dedekind finite) ring. Then R is weakly clean if and only if R is weakly f-clean.*

Proof. Since every commutative (local or Dedekind finite) ring is a left quasi-duo ring, the assertion holds, by Theorem 2.17. □

Corollary 2.19. *Let R be a ring in which every nonunit has a power that is central. Then R is weakly clean if and only if R is weakly f-clean.*

Proof. Suppose every nonunit has a power that is central. Hence R is a left quasi-duo ring. Then the assertion holds, by Theorem 2.17. □

Corollary 2.20. *Let R be a ring in which all idempotents are central. Then R is weakly clean if and only if R is weakly f-clean.*

Proof. Since all idempotents are central, R is Dedekind finite. Hence the assertion holds, by Corollary 2.18. □

If G is a group and R is a ring, we denote the group ring over R by RG.

Lemma 2.21. *Let R be a ring such that $2 \in U(R)$. Then R is weakly f-clean if and only if RG is weakly f-clean.*

Proof. Suppose RG is weakly f-clean. Since R is a homomorphic image of RG, R is weakly f-clean, by Lemma 2.8. Conversely, since $2 \in U(R)$, $RG \cong R \times R$, by [11, Proposition 3]. Hence RG is weakly f-clean by Lemma 2.8. $\square$

Suppose that R is an associative ring with unity and $\alpha : R \longrightarrow R$ is an endomorphism such that $\alpha(1)$. The ring (HR, α) of skew Hurwitz series over a ring R is defined as follows: the elements of (HR, α) are functions $f : \mathbb{N} \longrightarrow R$, where $\mathbb{N}$ is the set of integers greater or equal than zero. The operation of addition in (HR, α) is componentwise and the operation of multiplication is defined, for every $f, g \in (HR, \alpha)$, by:

$$fg(n) = \textstyle\sum_{k=0}^{n} \binom{n}{k} f(k)\alpha^k(g(n-k)) \text{ for each } \ n \in \mathbb{N},$$

where $\binom{n}{k}$ is the binomial coefficient defined for all $n, k \in \mathbb{N}$ with $n \geqslant k$ by $n!/k!(n-k)!$. In the case where the endomorphism α is the identity, we denote HR instead of (HR, α). If one identifies a skew formal power series $\sum_{n=0}^{\infty} \in R[[x; \alpha]]$ with the function f such that $f(n) = a_n$, then multiplication in (HR, α) is similar to the usual product of skew formal power series, except that binomial coefficients appear in each term in the product introduced above. It can be easily shown that T is a ring with identity h_1, defined by $h_1(0) = 1$ and $h_1(n) = 0$ for all $n \geqslant 1$. It is clear that R is canonically embedded as a subring of (HR, α) via $r \in R \longmapsto h_r \in (HR, \alpha)$, where $h_r(0) = r$, $h_r(n) = 0$ for every $n \geqslant 1$ [4, 11].

Proposition 2.22. *Let R be a ring. Then $f \in K(T = (HR, \alpha))$ if and only if $f(0) \in K(R)$.*

Proof. [12, Proposition 2.11]. $\square$

Theorem 2.23. *Let R be a ring and α be an automorphism of R. Then $T = (HR, \alpha)$ is weakly f-clean if and only if R is weakly f-clean.*

Proof. Suppose that $W = \{h \in T \mid h(0) = 0\}$, where $T = (HR, \alpha)$ is weakly f-clean. Hence $R \cong T/W$, and so R is a homomorphic image of T. Then R is weakly f-clean, by Lemm 2.8. Conversely, asuume that R is weakly f-clean and $h \in T$. Hence $h(0) \in R$, and so $h(0) = f + e$ or $h(0) = f - e$ for some $e \in Id(R)$ and $f \in K(R)$. Define an element $g \in T$ by,

$$g(n) = \begin{cases} f & n = 0 \\ h(n) & n > 0. \end{cases}$$

Then $h = g + h_e$ or $h = g - h_e$, where $g \in K(T)$ and $h_e \in Id(T)$. Then $T = (HR, \alpha)$ is weakly f-clean. $\square$

Here we shall formulate two questions of interest.

Problem 2.24. *When is a matrix ring weakly f-clean?*

Problem 2.25. *Let R be a ring and $e \in Id(R)$ such that the subring eRe is weakly f-clean. Is R also weakly f-clean?*

Acknowledgements. I would like to thank the reviewers for their thoughtful comments and efforts towards improving our manuscript.

References

[1] **M.Y. Ahn, D.D. Anderson**, *Weakly clean rings and almost clean rings*, Rocky Mountain J. Math., **36** (2006), 783 – 799.

[2] **D.D. Anderson, V.P. Camillo**, *Commutative rings whose elements are a sum of a unit and an idempotent*, Comm. Algebra, **30** (2002), 3327 – 3336.

[3] **N. Ashrafi, E. Nasibi**, *r-clean rings*, Math. Reports, **15(65)** (2013), 125 – 132.

[4] **A. Benhissi, F. Koja**, *Basic properties of Hurwitz series rings*, Ricerche Math., **61** (2012), 255 – 273.

[5] **A.Y.M. Chin, K.T. Qua** *A note on weakly clean rings*, Acta Math. Hungar., **132** (2001), 113 – 116.

[6] **V.P. Camillo, H.P. Yu**, *Exchange rings, unit and idempotents* Commun. Algebra, **22** (1994), 4737 – 4749.

[7] **P.V. Danchev**, *On weakly clean and weakly exchange rings having the strong property*, Publ. Inst. Math. (Beograd), **101** (2017), 135 – 142.

[8] **P.D. Danchev**, *On weakly clean and weakly exchange rings having the strong property*, Publ. Inst. Math. (Beograd), **101** (2017), 135 – 142.

[9] **P.V. Danchev**, *Weakly clean and exchange UNI rings*, Ukrain. Math. J., **71** (2019), 1617 – 1623.

[10] **P.V. Danchev**, *Weakly exchange rings whose units are sums of two idempotents*, Vestnik St. Petersburg Univ., Math., Mekh., **6(64)** (2019), 265 – 269.

[11] **A.M. Hassanein**, *Clean rings of skew Hurwitz series*, Matematiche (Catania), **62** (2007), 47 – 54.

[12] **A.L. Handam**, *On f-clean rings and full elements*, Prayecciones J. Math., **30** (2011), 277 – 284.

[13] **T. Kosan, S. Sahinkaya, Y. Zhou**, *On weakly clean rings*, Comm. Algebra, **45** (2017), 3494 – 3502.

[14] **B. Li, L. Feng**, *f-clean rings and rings having full elements* J. Korean Math. Soc., **47** (2010), 247 – 261.

[15] **W.K. Nicholson**, *Lifting idempotents and exchange rings*, Trans. Amer. Math. Soc., **229** (1977), 269 – 278.

[16] **F. Rashedi**, *Invo-k-clean rings*, Bull. Transilvania Univ. Brašov, Math. Computer Sci., **2(64)** (2022), 167 – 172.

[17] **H. Yu**, *On quasi-duo rings*, Glasgow Math. J., **37** (1995), 21 – 31.

Received July 09, 2023

Department of Mathematics, Technical and Vocational University, Tehran, Iran
E-mail: frashedi@tvu.ac.ir

Quasigroups and Related Systems **32** (2024), 119 − 128

https://doi.org/10.56415/qrs.v32.10

Generalized essential ideals in R-groups

Tapatee Sahoo, Syam Prasad Kuncham, Babushri Srinivas Kedukodi, Harikrishnan Panackal

Abstract. In this paper, we consider an R-group where R is a zero-symmetric right nearring. We define generalized essential ideal of an R-group and prove several properties. Further, we extend this notion to obtain a one-one correspondence between s-essential ideals of R-group and those of $M_n(R)$-group R^n.

1. Preliminaries

The concept of uniform dimension in modules over rings is a generalization of the dimension of a vector space over a field. A module in which every non-zero submodule is essential is called uniform. Uniform submodules play a significant role to establish various finite dimension conditions in modules over associative rings. Goldie [11] characterized equivalent conditions for a module to have finite uniform dimension. In Bhavanari [20], uniform dimension was generalized to modules over nearrings (also known as, R-groups) and proved a characterization for a R-group to have finite Goldie dimension (in short, $f.G.d.$). Goldie dimension aspects in modules over nearrings were extensively studied by [5, 7, 20]. In case of a module over a matrix nearring, the notions essential ideal, uniform ideal were defined in [6], and proved a characterization for a module over a matrix nearring to have a $f.G.d.$. In [10], the authors studied prime and semiprime aspects in connection with $f.G.d.$ in R-groups and matrix nearrings.

In section 2, we introduce generalized essential ideal in R-groups and prove some properties. In section 3, we extend the notion of generalized essential ideal to modules over matrix nearrings and obtain a one-one correspondence between s-essential ideals of an R-group (over itself) and those

2000 Mathematics Subject Classification: 16Y30

Keywords: Nearring, essential ideal, uniform ideal, finite dimension.

of $M_n(N)$-group R^n.

A (right) nearring $(R, +, \cdot)$ is an algebraic system (Pilz [18]), where R is an additive group (need not be abelian), and a multiplicative semigroup, satisfying only one distributive axioms (say, right): $(n_1 + n_2)n_3 = n_1n_3 + n_2n_3$ for all $n_1, n_2, n_3 \in R$. If R is a right nearring, then $0a = 0$ and $(-a)b = -ab$, for all $a,\ b \in R$, but in general, $a0 \neq 0$ for some $a \in R$. R is zero-symmetric (denoted as, $R = R_0$) if $a0 = 0$ for all $a \in R$. An additive group $(G, +)$ is called an R-group (or module over a nearring R), denoted by $_RG$ (or simply by G) if there exists a mapping $R \times G \to G$ (image $(n, g) \to ng$), satisfying: $(n + m)g = ng + mg$; $(nm)g = n(mg)$ for all $g \in G$ and $n,\ m \in R$. It is evident that every nearring is an R-group (over itself). Also, if R is a ring, then each (left) module over R is an R-group. Throughout, G denotes an R-group where R is a right nearring.

A subgroup $(H, +)$ of G with $RH \subseteq H$ is called an R-subgroup of G. A normal subgroup H of G is called an ideal if $n(g + h) - ng \in H$ for all $n \in R,\ h \in H,\ g \in G$. For any two R-groups G_1 and G_2, a map $f\colon G_1 \to G_2$ is called an R-homomorphism, $f(x + y) = f(x) + f(y)$ and $f(nx) = nf(x)$ hold for all $x, y \in G_1$ and $n \in R$. If f is one-one and onto, then f is an R-isomorphism.

In case of a zero symmetric nearring, for any ideals A and B of G, $A+B$ is an ideal of G ([18], Corollary 2.3). For each $g \in G$, Rg is an R-subgroup of G. The ideal (or R-subgroup) generated by an element $g \in G$ is denoted by $\langle g\rangle$.

An ideal H of an R-group G is essential (see, [20]), if for any ideal K of G, $H \cap K = (0)$ implies $K = (0)$. If every ideal $(0) \neq H$ of G is essential then we say G is uniform. An ideal (R-subgroup) S of G is said to be superfluous ideal (see, [2, 3]), if $S + K = G$ and K is an ideal of G, imply $K = G$ and G is called hollow if every proper ideal of G is superfluous in G. Generalizations of essential ideals, prime ideals, superfluous ideals in R-groups, matrix nearrings, and hyperstructures were extensively studied in [13, 14, 17, 19, 21, 22, 23, 24, 25].

For standard definitions and notations in nearrings, we refer to [8, 18].

2. Generalized essential ideals

Definition 2.1. Let K be an R-ideal (or R-subgroup) of G. K is said to be *s-essential* in G (denoted by $K \trianglelefteq_s G$) if for any superfluous R-ideal (or R-subgroup) L of G, $K \cap L = (0)$ implies $L = (0)$.

Note 2.2. Every essential R-ideal of G is s-essential in G.

Remark 2.3. Converse of Note 2.2 need not be true. Let $R = \mathbb{Z}$ and $G = \mathbb{Z}_6$. Then $K_1 = \{\bar{0}, \bar{3}\}$ and $K_2 = \{\bar{0}, \bar{2}, \bar{4}\}$ are the R-ideals of G. Then K_2 is s-essential but not essential, since $K_2 \cap K_1 = (\bar{0})$. but $K_1 \neq (\bar{0})$.

Example 2.4. Consider the nearring with addition and multiplication tables listed in K(135) and K(139) of p.418 of Pilz [18]. Let $G = D_8 = \langle \{a, b \mid 4a = 2b = 0,\ a{+}b = b{-}a\} \rangle = \{a, 2a, 3a, 4a = 0, b, a{+}b, 2a{+}b, 3a{+}b\}$, where a is the rotation in an anti-clockwise direction about the origin through $\frac{\pi}{2}$ radians and b is the reflection about the line of symmetry, and $G = R$. Then G is an R-group. Consider the operations:

$+$	0	a	$2a$	$3a$	b	$a+b$	$2a+b$	$3a+b$
0	0	a	$2a$	$3a$	b	$a+b$	$2a+b$	$3a+b$
a	a	$2a$	$3a$	0	$a+b$	$2a+b$	$3a+b$	b
$2a$	$2a$	$3a$	0	a	$2a+b$	$3a+b$	b	$a+b$
$3a$	$3a$	0	a	$2a$	$3a+b$	b	$a+b$	$2a+b$
b	b	$3a+b$	$2a+b$	$a+b$	0	$3a$	$2a$	a
$a+b$	$a+b$	b	$3a+b$	$2a+b$	a	0	$3a$	$2a$
$2a+b$	$2a+b$	$a+b$	b	$3a+b$	$2a$	a	0	$3a$
$3a+b$	$3a+b$	$2a+b$	$a+b$	b	$3a$	$2a$	a	0

$*_1$	0	a	$2a$	$3a$	b	$a+b$	$2a+b$	$3a+b$
0	0	0	0	0	0	0	0	0
a	0	a	$2a$	$3a$	b	$a+b$	$2a+b$	$3a+b$
$2a$	0	$2a$	0	$2a$	0	0	0	0
$3a$	0	$3a$	$2a$	a	b	$a+b$	$2a+b$	$3a+b$
b	0	b	$2a$	$2a+b$	b	$a+b$	$2a+b$	$3a+b$
$a+b$	0	$a+b$	0	$a+b$	0	0	0	0
$2a+b$	0	$2a+b$	$2a$	b	b	0	$2a+b$	$3a+b$
$3a+b$	0	$3a+b$	0	$3a+b$	0	0	0	0

The proper ideals are $I_1 = \{0, 2a\}$, $I_2 = \{0, a+b, 2a, 3a+b\}$, and R-subgroups are $J_1 = \{0, 2a\}$, $J_2 = \{0, b\}$, $J_3 = \{0, a+b\}$, $J_4 = \{0, 2a+b\}$, $J_5 = \{0, 3a+b\}$, $J_6 = \{0, b, 2a, 2a+b\}$, $J_7 = \{0, 2a, a+b, 3a+b\}$. Then J_1 is s-essential but not essential, as $J_1 \cap J_3 = (0)$, whereas $J_3 \neq (0)$.

Proposition 2.5. *Let G be a unitary R-group and $(0) \neq K$ be an R-subgroup of G. Then $K \trianglelefteq_s G$ if and only if for each $0 \neq x \in G$, if $Rx \ll G$, then there exists an element $n \in R$ such that $0 \neq nx \in K$.*

Proof. Let $(0) \neq K$ be an R-subgroup of G such that $K \trianglelefteq_s G$. For each $0 \neq x \in G$, if $Rx \ll G$, then since $1 \in R$ and $x \neq 0$, we have $Rx \neq (0)$. Clearly, Rx is a R-subgroup of G. Since $K \trianglelefteq_s G$, we get $K \cap Rx \neq (0)$. Then there exists $0 \neq a \in K \cap Rx$. Since $a \in Rx$, there exists $n \in R$ such that $a = nx$. Therefore, $0 \neq nx \in K$. Conversely, suppose that L be an R-subgroup of G such that $(0) \neq L \ll G$. Then $0 \neq x \in L \subseteq G$. To show $Rx \ll G$, let T be an R-subgroup of G such that $Rx + T = G$. Now $Rx \subseteq RL \subseteq L$. Thus, $G = Rx + T \subseteq L + T$. So $L + T = G$. Now $L \ll G$ implies $T = G$. Therefore, $Rx \ll G$. Then by hypothesis, there exists an element $n \in R$ such that $0 \neq nx \in K$. Hence $0 \neq nx \in K \cap L$, and so $K \cap L \neq (0)$. Therefore, $K \trianglelefteq_s G$. □

Proposition 2.6. *Let K, L, T be R-ideals of G with $K \subseteq T$. If $K \trianglelefteq_s G$, then $K \trianglelefteq_s T$ and $T \trianglelefteq_s G$.*

Proof. Suppose that K be an R-ideal of G with $K \cap P = (0)$, where $P \ll T$. To show $P \ll G$, let M be an R-ideal of G such that $P + M = G$. Then $(P+M) \cap T = G \cap T$. Now by modular law, $P + (M \cap T) = T$. Since $P \ll T$, we get $M \cap T = T$. This implies $M \subseteq T$. Thus, $G = P + M \subseteq T = T$. Therefore, $T = G$. Hence $P \ll G$. Since $K \trianglelefteq_s G$, we have $P = (0)$. Thus $K \trianglelefteq_s T$. Now to show $T \trianglelefteq_s G$, let $Q \ll G$ such that $T \cap Q = (0)$. Since $K \subseteq T$, we have $K \cap Q \subseteq T \cap Q = (0)$. Then by hypothesis, $Q = (0)$. Therefore $T \trianglelefteq_s G$. □

Remark 2.7. *The converse of Proposition 2.6 need not be true. Let $R = \mathbb{Z}$ and $G = \mathbb{Z}_{36}$. $K = 6\mathbb{Z}_{36}$ and $L = 18\mathbb{Z}_{36}$ are R-ideals of G. Now $L \trianglelefteq_s K$ and $K \trianglelefteq_s G$. But $L \not\trianglelefteq_s G$, since $L \cap 12\mathbb{Z}_{36} = (0)$, but $12\mathbb{Z}_{36} \neq (0)$.*

Proposition 2.8. *Let K and L be R-ideals of G. Then $K \cap L \trianglelefteq_s G$ if and only if $K \trianglelefteq_s G$ and $L \trianglelefteq_s G$.*

Proof. Let $K \cap L \trianglelefteq_s G$. To show $K \trianglelefteq_s G$, let $P \ll G$ such that $K \cap P = (0)$. Now, $(K \cap L) \cap P \subseteq K \cap P = (0)$. Since $K \cap L \trianglelefteq_s G$, we have $P = (0)$. Thus $K \trianglelefteq_s G$. Similarly, $L \trianglelefteq_s G$. Conversely, suppose that $K \trianglelefteq_s G$ and $L \trianglelefteq_s G$. Let $P \ll G$ such that $(K \cap L) \cap P = (0)$. Then $K \cap (L \cap P) = (0)$. Now we show that $K \cap P \ll G$. Let T be a R-ideal of G such that $(K \cap P) + T = G$. Since $K \cap P \subseteq P$, we have $G = (K \cap P) + T \subseteq P + T$. Now $P \ll G$, implies $T = G$. Thus $K \cap P \ll G$. Now, $L \trianglelefteq_s G$ and $K \cap P \ll G$, implies $K \cap P = (0)$. Also $K \trianglelefteq_s G$ and $P \ll G$ implies $P = (0)$. Therefore, $K \cap L \trianglelefteq_s G$. □

Proposition 2.9. *Let $f : G \to G'$ be an N-epimorphism. If $K \trianglelefteq_s G'$, then $f^{-1}(K) \trianglelefteq_s G$.*

Proof. Let $L \ll G$ such that $f^{-1}(K) \cap L = (0)$. To show that $K \cap f(L) = (0)$, let $x \in K \cap f(L)$. Then $x \in K$ and $x \in f(L)$. This implies $x = f(y)$, for some $y \in L$. Then $y = f^{-1}(x) \in f^{-1}(K)$ and $y \in L$. Thus $y \in f^{-1}(K) \cap L = (0)$, and so $y = 0$. Hence $x = f(0) = 0$. Therefore, $K \cap f(L) = (0)$. Now we show that $f(L) \ll G'$. Let T be an N-ideal of G' such that $f(L) + T = G'$. Then $L + f^{-1}(T) = f^{-1}(G') = G$. This implies $f^{-1}(T) = G$, and so $T = f(G) = G'$. Therefore, $f(L) \ll G'$. Now since $K \trianglelefteq_s G_2$ and $K \cap f(L) = (0)$, we get $f(L) = (0)$. Hence $L \subseteq f^{-1}(0) \subseteq f^{-1}(K) \cap L = (0)$. Therefore, $L = (0)$. □

Theorem 2.10. *Suppose that $K_1 \leq_R G_1 \leq_R G$, $K_2 \leq_R G_2 \leq_R G$, and $G = G_1 \oplus G_2$; then $K_1 \oplus K_2 \trianglelefteq_s G_1 \oplus G_2$ if and only if $K_1 \trianglelefteq_s G_1$ and $K_2 \trianglelefteq_s G_2$.*

Proof. Suppose that $K_1 \trianglelefteq_s G_1$. That is, $K_1 \cap L_1 = (0)$, for some $(0) \neq L_1 \ll G_1$. We show that $(K_1 + K_2) \cap L_1 = (0)$. Let $x \in (K_1 + K_2) \cap L_1$. Then $x = k_1 + k_2$ and $x = l_1$, where $k_1 \in K_1$, $k_2 \in K_2$. This implies $l_1 = k_1 + k_2$, and so $k_2 = -k_1 + l_1 \in G_1 \cap G_2 = (0)$. Therefore, $k_2 = (0)$. Hence $l_1 = k_1 \in K_1 \cap L_1 = (0)$. Therefore, $x = 0$. This shows that $(K_1 + K_2) \cap L_1 = (0)$. Now to show $L_1 \ll G_1 + G_2$, let $T \trianglelefteq_R G_1 + G_2$ such that $L_1 + T = G_1 + G_2$. Then $(L_1 + T) \cap G_1 = (G_1 + G_2) \cap G_1$. Now by modular law, since $L_1 \subseteq G_1$, we get $L_1 + (T_1 \cap G_1) = G_1$. Since $L_1 \ll G_1$ and $T \cap G_1 \trianglelefteq_R G_1$, we have $T \cap G_1 = G_1$, and so $G_1 \subseteq T$. Thus, $G_1 + G_2 = L_1 + T \subseteq G_1 + T = T$. Therefore, $T = G_1 + G_2$ shows that

$$L_1 \ll G_1 + G_2 \cdots \qquad (*).$$

Now $K_1 \oplus K_2 \trianglelefteq_s G_1 \oplus G_2$ implies $L = (0)$, a contradiction. Therefore $K_1 \trianglelefteq_s G_1$. In a similar way, it can be proved that $K_2 \trianglelefteq_s G_2$. Conversely, suppose that $K_i \trianglelefteq_s G_i$ and $0 \neq g_i \in G_i$ $(i = 1, 2)$. Then by Proposition 2.5 and by $(*)$ we have $Rg_i \ll G_1 + G_2$. Then by Proposition 2.5, there exists $r_1 \in R$ such that $0 \neq r_1 g_1 \in K_1$. If $r_1 g_2 \in K_2$, then $0 \neq r_1 g_1 + r_1 g_2 \in K_1 \oplus K_2$. If $r_1 g_2 \notin K_2$, then again by Proposition 2.5, there exists an $r_2 \in R$ with $0 \neq r_2 r_1 g_2 \in K_2$, and we have $0 \neq r_2 r_1 g_1 + r_2 r_1 g_2 \in K_1 \oplus K_2$. Then $K_1 \oplus K_2 \trianglelefteq_s G_1 \oplus G_2$. □

3. Generalized essential ideals in $M_n(R)$-group R^n

For a zero-symmetric right nearring R with 1, let R^n will be the direct sum of n copies of $(R, +)$. The elements of R^n are column vectors and written as $(r_1, \cdots, r_n)$. The symbols i_j and π_j respectively, denote the i^{th} coordinate injective and j^{th} coordinate projective maps.
For an element $a \in R$, $i_i(a) = (0, \cdots, \underbrace{a}_{i^{th}}, \cdots, 0)$, and $\pi_j(a_1, \cdots, a_n) = a_j$, for any $(a_1, \cdots, a_n) \in R^n$. The nearring of $n \times n$ matrices over R, denoted by $M_n(R)$, is defined to be the subnearring of $M(R^n)$, generated by the set of functions $\{f_{ij}^a : R^n \to R^n \mid a \in R, 1 \leq i, j \leq n\}$ where $f_{ij}^a(k_1, \cdots, k_n) := (l_1, l_2, \cdots, l_n)$ with $l_i = ak_j$ and $l_p = 0$ if $p \neq i$. Clearly, $f_{ij}^a = i_i f^a \pi_j$, where $f^a(x) = ax$, for all $a, x \in R$. If R happens to be a ring, then f_{ij}^a corresponds to the $n \times n$-matrix with a in position (i, j) and zeros elsewhere.

Notation 3.1. ([6], Notation 1.1)
For any ideal $\mathcal{A}$ of $M_n(R)$-group R^n, we write

$$\mathcal{A}_{**} = \{a \in R : a = \pi_j A, \text{ for some } A \in \mathcal{A}, 1 \leq j \leq n\}, \text{ an ideal of } {}_RR.$$

We denote $M_n(R)$ for a matrix nearring, R^n for an $M_n(R)$-group R^n. We refer to Meldrum & Van der Walt [16] for preliminary results on matrix nearrings.

Theorem 3.2. (Theorem 1.4 of [6]) *Suppose $A \subseteq R$.*

1. *If A^n is an ideal of ${}_{M_n(R)}R^n$, then $A = (A^n)_{\star\star}$.*
2. *If A is an ideal of ${}_RR$ if and only if A^n is an ideal of ${}_{M_n(R)}R^n$.*
3. *If A is an ideal of ${}_RR$, then $A = (A^n)_{\star\star}$.*

Lemma 3.3. (Lemma 1.5 of [6])

1. *If $\mathcal{I}$ is an ideal of ${}_{M_n(R)}R^n$, then $(\mathcal{I}_{\star\star})^n = I$.*
2. *Every ideal $\mathcal{I}$ of ${}_{M_n(R)}R^n$ is of the form K^n for some ideal K of ${}_RR$.*

Remark 3.4. (Remark 1.6 of [6]) Suppose I, J are ideals of ${}_RR$. Then

(i) $(I \cap J)^n = I^n \cap J^n$;

(ii) $I \cap J = (0)$ if and only if $(I \cap J)^n = (\bar{\mathbf{0}})$ if and only if $I^n \cap J^n = (\bar{\mathbf{0}})$.

Lemma 3.5. *If I and J are ideals of R, then $(I+J)^n = I^n + J^n$.*

Proof. Clearly, $I \subseteq I+J$ and $I \subseteq I+J$ which implies $I^n \subseteq (I+J)^n$ and $J^n \subseteq (I+J)^n$ and so $I^n + J^n \subseteq (I+J)^n$. To prove the other part, let $(x_1, x_2, \cdots, x_n) \in (I+J)^n$. Then $x_i \in I+J$ for every $1 \leq i \leq n$ which implies $x_i = a_i + b_i$, where $a_i \in I$ and $b_i \in J$.
Now,

$$\begin{aligned}(x_1, x_2, \cdots, x_n) &= (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n) \\ &= (a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) \\ &\in I^n + J^n\end{aligned}$$

Therefore, $(I+J)^n \subseteq I^n + J^n$. Hence, $(I+J)^n = I^n + J^n$. □

Lemma 3.6. *$I + J = G$ if and only if $(I+J)^n = G^n$ if and only if $I^n + J^n = G^n$.*

Lemma 3.7. (Note 1.7(iii) of [6]) *Let A be an ideal of ${}_RR$. Then $A \leq_e {}_RR$ if and only if $A^n \leq_e {}_{M_n(R)}R^n$.*

Definition 3.8. An ideal $\mathcal{A}$ of $M_n(R)$-group R^n is said to be *superfluous* if for any ideal $\mathcal{K}$ of R^n, $\mathcal{A} + \mathcal{K} = R^n$ implies $\mathcal{K} = R^n$.

Definition 3.9. An ideal $\mathcal{K}$ of $M_n(R)$-group R^n is said to be *s-essential* if for any ideal $\mathcal{A}$ of R^n, $\mathcal{K} \cap \mathcal{A} = (\bar{\mathbf{0}})$ and $\mathcal{A} \ll R^n$ implies $\mathcal{K} = (\bar{\mathbf{0}})$.

Lemma 3.10. *Let K be an ideal of ${}_RR$. If $K \trianglelefteq_s {}_RR$, then $K^n \trianglelefteq_s {}_{M_n(R)}R^n$.*

Proof. Let $K \trianglelefteq_s {}_RR$. To show $K^n \trianglelefteq_s {}_{M_n(R)}R^n$, let $\mathcal{L}$ be an ideal of ${}_{M_n(R)}R^n$ such that $K^n \cap \mathcal{L} = (\bar{\mathbf{0}})$ and $\mathcal{L} \ll {}_{M_n(R)}R^n$. Now to show $\mathcal{L}_{\star\star} \ll {}_RR$, let $B \trianglelefteq {}_RR$ such that $\mathcal{L}_{\star\star} + B = R$. By Lemma 3.6, we have $(\mathcal{L}_{\star\star} + B)^n = R^n$. By Lemma 3.5, we have $(\mathcal{L}_{\star\star})^n + B^n = R^n$. Now by Lemma 3.3, we get $\mathcal{L} = (\mathcal{L}_{\star\star})^n$, which implies $\mathcal{L} + B^n = R^n$. Since $B^n \trianglelefteq {}_{M_n(R)}R^n$ and $\mathcal{L} \ll {}_{M_n(R)}R^n$, we have $B^n = R^n$. Let $n \in R$. Then $(n, 0, \cdots, 0) \in R^n = B^n$. Therefore, $n \in (B^n)_{\star\star} = B$ (by Theorem 3.2(3)). Therefore, $B = R$, and so $\mathcal{L}_{\star\star} \ll {}_RR$. So $K^n \cap \mathcal{L} = (\bar{\mathbf{0}})$ implies $K^n \cap (\mathcal{L}_{\star\star})^n = (\bar{\mathbf{0}})$, and by Remark 3.4 (ii), $K \cap (\mathcal{L}_{\star\star}) = (0)$. Now since $K \trianglelefteq_s R$, we get $\mathcal{L}_{\star\star} = (0)$. Thus $\mathcal{L} = (\mathcal{L}_{\star\star})^n = (\bar{\mathbf{0}})$. This shows that $K^n \trianglelefteq_s {}_{M_n(R)}R^n$. □

Lemma 3.11. *Let $\mathcal{A}$ be an ideal of ${}_{M_n(R)}R$. If $\mathcal{A} \trianglelefteq_s {}_{M_n(R)}R^n$, then $\mathcal{A}_{\star\star} \trianglelefteq_s {}_RR$.*

Proof. Let $\mathcal{A} \trianglelefteq_s {}_{M_n(R)}R^n$. To show $\mathcal{A}_{\star\star} \trianglelefteq_s {}_RR$, let $B \ll {}_RR$ such that $\mathcal{A}_{\star\star} \cap B = (0)$. Then by Remark 3.4, we have $(\mathcal{A}_{\star\star})^n \cap B^n = (\bar{\mathbf{0}})$ and by Lemma 3.3, we have $\mathcal{A} = (\mathcal{A}_{\star\star})^n$, and so $\mathcal{A} \cap B^n = (0)$. Now to show $B^n \ll {}_{M_n(R)}R^n$, let $\mathcal{L} \trianglelefteq {}_{M_n(R)}R^n$ such that $B^n + \mathcal{L} = R^n$. To show $\mathcal{L} = R^n$. Since $\mathcal{L} \trianglelefteq {}_{M_n(R)}R^n$, by Lemma 3.3, we have $\mathcal{L} = (\mathcal{L}_{\star\star})^n$, which implies $B^n + (\mathcal{L}_{\star\star})^n = R^n$. Now using Lemma 3.5, we get $(B + \mathcal{L}_{\star\star})^n = R^n$. Therefore, by Lemma 3.6, $B + \mathcal{L}_{\star\star} = R$, and since $B \ll {}_RR$, we get $\mathcal{L}_{\star\star} = R$. Hence, $\mathcal{L} = (\mathcal{L}_{\star\star})^n = R^n$. This shows that $B^n \ll {}_{M_n(R)}R^n$. Now $\mathcal{A} \trianglelefteq_s {}_{M_n(R)}R^n$ implies $B^n = (\bar{\mathbf{0}})$. Thus $B = (0)$. This shows that $\mathcal{A}_{\star\star} \trianglelefteq_s {}_RR$. $\square$

Theorem 3.12. *There is a one-one correspondence between the set of s-essential ideals of ${}_RR$ and those of $M_n(R)$-group R^n.*

Proof. Let $P = \{A \trianglelefteq {}_RR : A \trianglelefteq_s {}_RR\}$. $Q = \{\mathcal{A} \trianglelefteq {}_{M_n(R)}R^n : \mathcal{A} \trianglelefteq_s {}_{M_n(R)}R^n\}$. Define $\Phi : P \to Q$ by $\Phi(A) = A^n$. Then by Lemma 3.10, $A^n \trianglelefteq_s {}_{M_n(R)}R^n$. Define $\Psi : Q \to P$ by $\Psi(\mathcal{A}) = \mathcal{A}_{\star\star}$. By Lemma 3.11, $\mathcal{A}_{\star\star} \trianglelefteq_s {}_RR$. Now $(\Psi \circ \Phi)(A) = \Psi(\Phi(A)) = \Psi(A^n) = (A^n)_{\star\star} = A$. $(\Phi \circ \Psi)(\mathcal{A}) = \Phi(\Psi(\mathcal{A})) = \Phi(\mathcal{A}_{\star\star}) = (\mathcal{A}_{\star\star})^n = \mathcal{A}$. Therefore, $(\Psi \circ \Phi) = Id_P$ and $(\Phi \circ \Psi) = Id_Q$. $\square$

Acknowledgment. Authors thank the referees for the careful reading of the manuscript. The first author acknowledges Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, and the other authors acknowledge Manipal Institute of Technology (MIT), Manipal Academy of Higher Education, Manipal, India for their kind encouragement. The first author acknowledges Indian National Science Academy (INSA), Govt. of India, for selecting to the award of visiting scientist under the award number: INSA/SP/VSP-56/2023-24/. The last author (corresponding author) acknowledges SERB, Govt. of India for the TARE project fellowship TAR/2022/000219.

References

[1] **F.W. Anderson, K.R. Fuller**, *Rings and categories of modules*, Graduate Texts in Mathematics, Springer-Verlag New York, **13** (1992).

[2] **S. Bhavanari**, *On modules with finite spanning dimension*, Proc. Japan Acad., **61-A** (1985), 23-25.

[3] **S. Bhavanari**, *Modules with finite spanning dimension*, J. Austral. Math Soc., **57** (1994), 170-178.

[4] **S. Bhavanari**, *On modules with finite Goldie dimension*, J. Ramanujan Math. Soc., **5**(1) (1990), 61-75.

[5] **S. Bhavanari, S.P. Kuncham**, *On direct and inverse systems in N-groups*, Indian J. Math., **42**(2) (2000), 183-192.

[6] **S. Bhavanari, S.P. Kuncham**, *On finite Goldie dimension of $M_n(N)$-group N^n*, Proc. Confer. Nearrings and Nearfields, Springer, Dordrecht, 2005, 301–310. ISBN: 978-1-4020-3390-2; 1-4020-3390-7.

[7] **S. Bhavanari, S.P. Kuncham**, *Linearly independent elements in N-groups with finite Goldie dimension*, Bull. Korean Math. Soc., **42**(3) (2005), 433-441.

[8] **S. Bhavanari, S.P. Kuncham**, *Nearrings, fuzzy ideals, and graph theory*, CRC press, (2013).

[9] **S. Bhavanari, S.P. Kuncham, V.R. Paruchuri, B. Mallikarjuna**, *A note on dimensions in R-groups*, Italian J. Pure Appl. Math., **44** (2020), 649-657.

[10] **G.L. Booth and N.J. Groenewald**, *On primeness in matrix near-rings*, Arch. Math., **56**(6) (1991), 539-546.

[11] **A.W. Goldie**, *The structure of Noetherian rings*, Lectures on Rings and Modules, **246** (1972).

[12] **N. Hamsa, S.P. Kuncham, B.S. Kedukodi**, *$\Theta\Gamma$-N-group*, Matematicki Vesnik, **70**(1) (2018), 64-78.

[13] **P.K. Harikrishnan, P. Pallavi, Madeleine Al-Tahan, B. Vadiraja, S.P. Kuncham**, 2-*absorbing hyperideals and homomorphisms in join hyperlattices*, Results in Nonlinear Analysis, **6**(4) (2023), 128–139.

[14] **S.P. Kuncham, S. Tapatee, S. Rajani, B.S. Kedukodi, P.K. Harikrishnan**, *Matrix maps over seminearrings*, Global and Stochastic Analysis, **10**(2) (2023), 123–134.

[15] **J.D.P. Meldrum**, *Near-rings and their links with groups*, Bull. Amer. Math. Soc., **17** (1985), 156-160.

[16] **J.D.P. Meldrum, A.P.J. Van der Walt**, *Matrix near-rings*, Arch. Math., **47**(4) (1986), 312–319.

[17] **P. Pallavi, S.P. Kuncham, S. Tapatee, P.K. Harikrishnan**, *Twin zeros and triple zeros of a hyperlattice with respect to hyperideals*, Global and Stochastic Analysis, **11**(1) (2024), 39–50.

[18] **G. Pilz**, *Near-Rings: the theory and its applications*, **23** (1983), North Holland.

[19] **S. Rajani, S. Tapatee, P.K. Harikrishnan, B.S. Kedukodi, S.P. Kuncham**, *Superfluous ideals of N-groups*, Rendiconti Circolo Mat. Palermo, **2** (2013), 1-19.

[20] **Y.V. Reddy, S. Bhavanari**, *A note on N-groups*, Indian J. Pure Appl. Math., **19**(9) (1988), 842-845.

[21] **S. Tapatee, B. Davvaz, P.K. Harikrishnan, B.S. Kedukodi, S.P. Kuncham**, *Relative essential ideals in R-groups*, Tamkang J. Math., **54** (2023), 69–82.

[22] **S. Tapatee, P.K. Harikrishnan, B.S. Kedukodi, S.P. Kuncham**, *Graph with respect to superfluous elements in a lattice*, Miskolc Math. Notes, **23**(2) (2022), 929–945.

[23] **S. Tapatee, B.S. Kedukodi, P.K. Harikrishnan, S.P. Kuncham**, *On the finite Goldie dimension of sum of two ideals of an R-group*, Discussiones Math., General Algebra Appl., **43**(2) (2023), 177–187.

[24] **S. Tapatee, B.S. Kedukodi, S. Juglal, P.K. Harikrishnan, S.P. Kuncham**, *Generalization of prime ideals in $M_n(N)$-group N^n*, Rendiconti Circolo Mat. Palermo, **72**(1) (2023), 449–465.

[25] **S. Tapatee, J.H. Meyer, P.K. Harikrishnan, B.S. Kedukodi, S.P. Kuncham**, *Partial order in matrix nearrings*, Bull. Iranian Math. Soc., **48**(6) (2022), 3195–3209.

Received December 12, 2023

T. Sahoo
Department of Mathematics
Manipal Institute of Technology Bengaluru,
Manipal Academy of Higher Education, Manipal, India
e-mail: sahoo.tapatee@manipal.edu

S.P. Kuncham, B.S. Kedukodi, H. Panackal
Department of Mathematics
Manipal Institute of Technology
Manipal Academy of Higher Education, Manipal, India
e-mails: syamprasad.k@manipal.edu, babushrisrinivas.k@manipal.edu,
pk.harikrishnan@manipal.edu

Quasigroups and Related Systems **32** (2024), 129 – 140

https://doi.org/10.56415/qrs.v32.11

On primary ordered semigroups

Pisan Summaprab

Abstract. In this paper, left primary, right primary, primary and semiprimary ideals of ordered semigroups are introduced. Moreover, we introduce an ordered semigroups in which every ideal is primary and every ideal is semiprimary which is a generalization of primary and semiprimary semigroups.

1. Introduction and preliminaries

A primary semigroup was introduced and studied by M. Satyanarayana in [10] and some results from [10] were extended to semiprimary semigroups by H. Lal [8]. Their study was restricted to commutative semigroups. The concepts of primary and semiprimary semigroups pass to noncommutative semigroups by A. Anjaneyulu [1, 2]. In [2], a class of semigroups knows as pseudo symmetric semigroups, which includes the classes of commutative, narmal, idempotent, duo semigroups was introduced. In this paper, the notions of primary and semiprimary semigroups extended to ordered semigroups. We introduce left primary, right primary, primary and semiprimary ideals of ordered semigroups and also a class of ordered semigroups, namely pseudo symmetric ordered semigroups, which includes the classes of commutative, narmal, idempotent, duo ordered semigroups. Moreover, we study the connection between prime and semiprime ideals of an ordered semigroups.

We recall some certain definitions and results used throughout this paper. A semigroup $(S, \cdot)$ together with a partial oder $\leqslant$ that is *compatible* with the semigroup operation, meaning that for any x, y, z in S, $x \leqslant y$ implies $zx \leqslant zy$ and $xz \leqslant yz$, is called a *partially ordered semigroup*, or simply an *ordered semigroup* [4]. Under the trivial relation, $x \leqslant y$ if and only if $x = y$, it is observed that every semigroup is an ordered semigroup.

Let $(S, \cdot, \leqslant)$ be an ordered semigroup. For two nonempty subsets A, B of S, we write AB for the set of all elements xy in S where $x \in A$ and $y \in B$, and write $(A]$ for the set of all elements x in S such that $x \leqslant a$ for some a in A, i.e.,

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

2010 Mathematics Subject Classification: 06F05

Keywords: ordered semigroup, primary, semiprimary, semisimple, semiprime ideal, prime ideal

In particular, we write Ax for $A\{x\}$, and xA for $\{x\}A$. It was shown in [5] that the following hold: (1) $A \subseteq (A]$; (2) $A \subseteq B \Rightarrow (A] \subseteq (B]$; (3) $(A](B] \subseteq (AB]$; (4) $(A \cup B] = (A] \cup (B]$; (5) $((A]] = (A]$.

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

(i) $SA \subseteq A$ (respectively, $AS \subseteq A$);

(ii) $A = (A]$, that is, for any x in A and y in S, $y \leqslant x$ implies $y \in A$.

If A is both a left and a right ideal of S, then A is called a *two-sided ideal*, or simply an *ideal* of S. It is known that the union or intersection of two ideals of S is an ideal of S.

An element a of an ordered semigroup $(S, \cdot, \leqslant)$, the *principal left* (respectively, *right, two-sided*) *ideal* generated by a is of the form $L(a) = (a \cup Sa]$ (respectively, $R(a) = (a \cup aS]$, $I(a) = (a \cup Sa \cup aS \cup SaS]$).

Let $(S, \cdot, \leqslant)$ be an ordered semigroup. A left ideal A of S is said to be *proper* if $A \subset S$. A proper right and two-sided ideals are defined similarly. If S does not contain proper ideals then we call S *simple*. A proper ideal A of S is said to be *maximal* if for any ideal B of S, if $A \subset B \subseteq S$, then $B = S$.

Let $(S, \cdot, \leqslant)$ be an ordered semigroup. An ideal I of S is said to be *prime* if for any ideals A, B of S, $AB \subseteq I$ implies $A \subseteq I$ or $B \subseteq I$. An ideal I of S is said to be *completely prime* if for any $a, b \in S$, $ab \in I$ implies $a \in I$ or $b \in I$. An ideal I of S is said to be *semiprime* if for any ideal A of S, $A^2 \subseteq I$ implies $A \subseteq I$. An ideal I of S is said to be *completely semiprime* if for any $a \in S$, $a^n \in I$ for any positive integer n implies $a \in I$ [11].

An ideal A of an ordered semigroup $(S, \cdot, \leqslant)$, the intersection of all prime ideals of S containing A, will be denoted by $Q^*(A)$ and the intersection of all completely prime ideals of S containing A, will be denoted by $P^*(A)$.

A subset A of an ordered semigroup $(S, \cdot, \leqslant)$, the radical of A, will be denoted by $\sqrt{A}$ defined by

$$\sqrt{A} = \{x \in S \mid x^n \in A \text{ for some positive integer } n\ \} \text{ [3].}$$

An element a of an ordered semigroup $(S, \cdot, \leqslant)$ is called a *semisimple element* in S if $a \in (SaSaS]$. And S is said to be *semisimple* if every element of S is semisimple [11].

An element a of an ordered semigroup $(S, \cdot, \leqslant)$ is said to be *left regular* (respectively, *right regular*, *regular*, *intra-regular*) if there exist x, y in S such that $a \leqslant xa^2$ (respectively, $a \leqslant a^2x$, $a \leqslant axa$, $a \leqslant xa^2y$) [11]. It is observed that left regular elements, right regular elements, regular elements, and intra-regular elements are all semisimple.

A subset M of an ordered semigroup $(S, \cdot, \leqslant)$ is called an *m-system* of S, if for any $a, b \in M$, there exists $x \in S$ such that $(axb] \cap M \neq \emptyset$. A subset N of an ordered semigroup $(S, \cdot, \leqslant)$ is called an *n-system* of S, if for any $a \in N$, there exists $x \in S$ such that $(axa] \cap N \neq \emptyset$ [7].

An ordered semigroup $(S, \cdot, \leqslant)$ is said to be a *left(right) duo* if every left(right) ideal of S is a two-sided ideal of S. An ordered semigroup S is said to be a *duo* if it is both a left duo and a right duo. An ordered semigroup S is said to be *normal* if $(xS] = (Sx]$ for all $x \in S$.

An element a of an ordered semigroup $(S, \cdot, \leqslant)$ is called an *ordered idempotent* if $a \leqslant a^2$. We call an ordered semigroup S *idempotent ordered semigroup* if every element of S is an ordered idempotent [6]. The set of all ordered idempotents of an ordered semigroup S denoted by $E(S)$.

An element e of an ordered semigroup $(S, \cdot, \leqslant)$ is called an *identity element* of S if $ex = x = xe$ for any $x \in S$. The *zero element* of S, defined by Birkhoff, is an element 0 of S such that $0 \leqslant x$ and $0x = 0 = x0$ for all $x \in S$.

2. Pseudo symmetric ordered semigroups

In this section, we introduce a class of ordered semigroups, namely pseudo symmetric ordered semigroups, which includes the classes of commutative, narmal, idempotent, duo ordered semigroups.

Definition 2.1. Let $(S, \cdot, \leqslant)$ be an ordered semigroup. An ideal A of S is said to be *pseudo symmetric* if $xy \in A$ for some $x, y \in S$ implies $(xsy] \subseteq A$ for all $s \in S$.

Definition 2.2. An ordered semigroup $(S, \cdot, \leqslant)$ is said to be *pseudo symmetric* if every ideal of S is pseudo symmetric.

Example 2.3. Let $(S, \cdot, \leqslant)$ be an ordered semigroup such that the multiplication and the order relation are defined by:

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

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

The ideals of S are: $\{a\}$, $\{a, b\}$ and S. As is easily seen, $\{a\}$, $\{a, b\}$ and S, are pseudo symmetric. So, it is pseudo symmetric ordered semigroup.

Remark 1. Every commutative and normal ordered semigroup is a pseudo symmetric ordered semigroup.

Proposition 2.4. *Every duo ordered semigroup is a pseudo symmetric ordered semigroup.*

Proof. Let $(S, \cdot, \leqslant)$ be a duo ordered semigroup and A an ideal of S such that $xy \in A$ for some $x, y \in S$. Since S is duo, $L(a) = R(a)$ for all $a \in S$. Let $s \in S$. We have $xs \in (xS \cup x] = (Sx \cup x]$. Thus $xs \in (Sx]$ or $xs \in (x]$. And each of the cases implies $(xsy] \subseteq A$. Thus S is a pseudo symmetric. $\square$

Proposition 2.5. *Every idempotent ordered semigroup is a pseudo symmetric ordered semigroup.*

Proof. Let $(S, \cdot, \leqslant)$ be an idempotent ordered semigroup and A an ideal of S such that $xy \in A$ for some $x, y \in S$. Since S is an idempotent ordered semigroup, we have $yx \leqslant yxyx = y(xy)x \in A$ and also $xsy \leqslant xsyxsy \in A$ for all $s \in S$. Thus S is a pseudo symmetric. $\square$

Proposition 2.6. *Let $(S, \cdot, \leqslant)$ be a pseudo symmetric ordered semigroup and A an ideal of S. Then A is prime if and only if A is completely prime.*

Proof. Assume that A is prime. Let $ab \in A$ for any $a, b \in S$. Since S is pseudo symmetric, $(asb] \subseteq A$ for all $s \in S$. It follows that $(aSb] \subseteq A$. Thus $I(a)I(b) \subseteq A$. Since A is prime, we have $I(a) \subseteq A$ or $I(b) \subseteq A$. Thus $a \in A$ or $b \in A$, which shows that A is completely prime. The converse statement is clear. $\square$

Lemma 2.7. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and A an ideal of S. Then $Q^*(A) \subseteq \sqrt{A}$.*

Proof. Let $x \in Q^*(A)$. If $x^n \notin A$ for all positive integer n. By Lemma 2.4 in [11], then there exists a prime ideal P of S containing A such that $x^n \notin P$ for all positive integer n. Thus $x \notin Q^*(A)$. This is a contradiction. Thus $Q^*(A) \subseteq \sqrt{A}$. $\square$

Theorem 2.8. *Let $(S, \cdot, \leqslant)$ be a pseudo symmetric ordered semigroup and A an ideal of S. Then $Q^*(A) = \sqrt{A}$.*

Proof. We have $Q^*(A) \subseteq \sqrt{A}$ by Lemma 2.7. If $x \notin Q^*(A)$. Then there exists a prime ideal P of S containing A such that $x \notin P$. We have P is a completely prime ideal by Proposition 2.6. Thus $x^n \notin P$ for all positive integer n. It follows that $x^n \notin A$ for all positive integer n. Thus $x \notin \sqrt{A}$ and so $\sqrt{A} \subseteq Q^*(A)$. Hence $Q^*(A) = \sqrt{A}$. $\square$

3. Prime and semiprime ideals of ordered semigroups

In this section, we study the relation between prime and semiprime ideals of an ordered semigroups.

Lemma 3.1. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and A an ideal of S. Then A is prime if and only if for any $a, b \in S$, $(aSb] \subseteq A$ implies $a \in A$ or $b \in A$.*

Proof. Assume that A is prime. Let $(aSb] \subseteq A$ for any $a, b \in S$. Thus $I(a)I(b) \subseteq A$. Since A is prime, we have $a \in I(a) \subseteq A$ or $b \in I(b) \subseteq A$. Conversely, assume that for any $a, b \in S$, $(aSb] \subseteq A$ implies $a \in A$ or $b \in A$. Let B, C be ideals of S such that $BC \subseteq A$. If $B \nsubseteq A$ and $C \nsubseteq A$, then there exists $b \in B \setminus A$ and $c \in C \setminus A$. Thus $(bSc] \subseteq A$. It follows that $b \in A$ or $c \in A$. This is a contradiction. Thus $B \subseteq A$ or $C \subseteq A$. $\square$

Similarly, we prove the following:

Lemma 3.2. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and A an ideal of S. Then A is semiprime if and only if for any $a \in S$, $(aSa] \subseteq A$ implies $a \in A$.*

Proposition 3.3. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and A an ideal of S. Then A is prime if and only if either $S \setminus A = \emptyset$ or the set $S \setminus A$ is an m-system.*

Proof. Assume that A is prime. If $S \setminus A \neq \emptyset$. Let $a, b \in S \setminus A$. Since A is a prime, we have $(aSb] \nsubseteq A$ by Lemma 3.1. Then there exists $y \in S$ such that $ayb \notin A$. Thus $ayb \in S \setminus A$ and so $S \setminus A$ is an m-system. Conversely, assume that either $S \setminus A = \emptyset$ or the set $S \setminus A$ is an m-system. Let $a, b \in A$ such that $(aSb] \subseteq A$. If $a, b \notin A$. Since $S \setminus A$ is an m-system, then there exists $x \in S$ and $c \in S \setminus A$ such that $c \leqslant axb \in (aSb] \subseteq A$. This is a contradiction. Thus $a \in A$ or $b \in A$. $\square$

Similarly, we prove the following:

Proposition 3.4. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and A an ideal of S. Then A is semiprime if and only if either $S \setminus A = \emptyset$ or the set $S \setminus A$ is an n-system.*

Proposition 3.5. *Any semiprime ideal of an ordered semigroup $(S, \cdot, \leqslant)$ is an intersection of prime ideals of S.*

Proof. Let A be a semiprime ideal of S. If $x \notin A$, choose elements $x_1, x_2, x_3, ...$ inductively as follows: $x_1 = x$. Since $(x_1Sx_1] = (xSx] \nsubseteq A$, take $x_2 \in S$ such that $x_2 \in (x_1Sx_1]$ and $x_2 \notin A$. Since $(x_2Sx_2] \nsubseteq A$, we have $x_3 \in S$ such that $x_3 \in (x_2Sx_2]$, $x_3 \notin A, \cdots, x_{i+1} \in (x_iSx_i]$, $x_{i+1} \notin A, \cdots$. We set $B = \{x_1, x_2, x_3, \cdots\}$. Let $x_i, x_j \in B$ and $i \leqslant j$. Then $x_{j+1} \in (x_iSx_j]$, $x_{j+1} \in (x_jSx_i]$ and $x_{j+1} \in B$. Thus B is an m-system. Let $T = \{Q \mid Q$ is an m-system of S, $x \in Q$ and $Q \cap A = \emptyset$ $\}$. Then $T \neq \emptyset$. By Zorn's Lemma, there exists a maximal element in T, namely M. Let $H = \{J \mid J$ is an ideal of S, $A \subseteq J$ and $J \cap M = \emptyset$ $\}$. Then $H \neq \emptyset$. By Zorn's Lemma, there exists a maximal element in H, namely I. Let $a, b \in S \setminus I$, then $(I(a) \cup I) \cap M \neq \emptyset$ and $(I(b) \cup I) \cap M \neq \emptyset$. Thus there exists $m_1, m_2 \in M$ such that $m_1 \leqslant s_1as_2$, $m_2 \leqslant s_3bs_4$, where $s_1, s_2, s_3, s_4 \in S$. Since M is an m-system, then there exists $m \in M$ such that $m \leqslant m_1zm_2$ for some $z \in S$. We have $m \leqslant s_1as_2zs_3bs_4$ and so $s_1as_2zs_3bs_4 \notin I$. It follows that $as_2zs_3b \notin I$. Thus $as_2zs_3b \in S \setminus I$ and so $S \setminus I$ is an m-system. We have I is prime ideal of S containing A by Proposition 3.3. Since $x \notin I$, $x \notin Q^*(A)$. Thus $Q^*(A) \subseteq A$ and so $Q^*(A) = A$. □

Proposition 3.6. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and A an ideal of S. Then A is semiprime if and only if $Q^*(A) = A$.*

Proof. If A is semiprime, then $Q^*(A) = A$ by Proposition 3.5. The converse statement is obvious. □

It is easy to see the following:

Lemma 3.7. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and A an ideal of S. Then A is completely prime if and only if $S \setminus A$ is a subsemigroups of S.*

Proposition 3.8. *Any completely semiprime ideal of an ordered semigroup $(S, \cdot, \leqslant)$ is an intersection of completely prime ideals of S.*

Proof. Let A be completely semiprime ideal of S. If $x \notin A$, then $x^n \notin A$ for all positive integer n. Let $B = \{x, x^2, x^3, \cdots\}$. Then B is an m-system and $A \cap B = \emptyset$. Let $T = \{Q \mid Q$ is an m-system of S, $x \in Q$ and $Q \cap A = \emptyset$ $\}$. Then $T \neq \emptyset$. By Zorn's Lemma, there exists a maximal element in T, namely M. Let $H = \{J \mid J$ is an ideal of S, $A \subseteq J$ and $J \cap M = \emptyset$ $\}$. Then $H \neq \emptyset$. By Zorn's Lemma, there exists a maximal element in H, namely I. By the same method given in Proposition 3.6, we have $S \setminus I = M$. Let $< M >$ be a subsemigroup of S generated by M. Then $< M >$ is an m-system. If $< M > \cap A \neq \emptyset$, then there exists $m_1, m_2, m_3, \cdots, m_n \in M$ such that $m_1m_2m_3 \cdots m_n \in A$. Since M is an m-system, there exists $m \in M$ and $x_1, x_2, x_3, \cdots, x_{n-1} \in S$ such that $m \leqslant m_1x_1m_2x_2m_3 \cdots m_{n-1}x_{n-1}m_n$. Since A is a completely semiprime, $ab \in A$ implies $ba \in A$. It follows that $m_1x_1m_2x_2m_3 \cdots m_{n-1}x_{n-1}m_n \in A$. Thus $m \in A$. This is a contradiction. By the maximality of M, we have $< M >= M$. Thus I is a completely prime ideal of S containing A by Lemma 3.7. Since $x \notin I$, $x \notin P^*(A)$. Thus $P^*(A) \subseteq A$ and so $P^*(A) = A$. □

Corollary 3.9. *Any completely semiprime ideal of an ordered semigroup $(S, \cdot, \leqslant)$ is an intersection of prime ideals of S.*

Proposition 3.10. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and A an ideal of S. Then A is completely semiprime if and only if $P^*(A) = A$.*

Proof. If A is completely semiprime, then $P^*(A) = A$ by Proposition 3.8. The converse statement is obvious. □

Lemma 3.11. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. The following statements are equivalent:*

(1) *S is semisimple.*

(2) *$(A^2] = A$ for any ideal A of S.*

(3) *$A \cap B = (AB]$ for any ideal A, B of S.*

(4) *$I(a) \cap I(b) = (I(a)I(b)]$ for any $a, b \in S$.*

(5) *$(I(a)^2] = I(a)$ for any $a \in S$.*

Proof. The implications (3) $\Rightarrow$ (4) and (4) $\Rightarrow$ (5) are obvious and we will prove (1) $\Rightarrow$ (2) $\Rightarrow$ (3) and (5) $\Rightarrow$ (1). (1) $\Rightarrow$ (2). Let A be an ideal of S and $x \in A$. Then $x \leqslant s_1xs_2xs_3$ for some $s_1, s_2, s_3 \in S$. We have $s_1xs_2 \in A$ and $xs_3 \in A$. Then $x \leqslant s_1xs_2xs_3 \in A^2$ and so $x \in (A^2]$. Thus $(A^2] = A$. (2) $\Rightarrow$ (3). Let A and B be an ideals of S. Clearly $(AB] \subseteq A \cap B$. Since $A \cap B$ is an ideal, $A \cap B = ((A \cap B)(A \cap B)] \subseteq (AB]$. Thus $A \cap B = (AB]$. (5) $\Rightarrow$ (1). Let $a \in S$. Then $I(a)^3 = I(a)I(a)I(a) \subseteq SI(a)S \subseteq (SaS]$. We have

$$a \in I(a) = (I(a)^2] \subseteq (I(a)^5] = (I(a)^3I(a)I(a)] \subseteq ((SaS]I(a)S] \subseteq (SaSaS].$$

Thus S is semisimple. □

Proposition 3.12. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. Then S is semisimple if and only if every ideal of S is semiprime.*

Proof. Assume that S is semisimple. Let I and A be an ideals of S such that $A^2 \subseteq I$. We have $A = (A^2] \subseteq I$ by Lemma 3.11. Thus I is semiprime. Converesly, assume that every ideal of S is semiprime. Let A be an ideal of S. Since $A^2 \subseteq (A^2]$, $A \subseteq (A^2]$. Clearly $(A^2] \subseteq A$. Thus $A = (A^2]$, which shows that S is semisimple by Lemma 3.11. □

4. Primary ordered semigroups

In this section, we introduce left primary, right primary, primary and semiprimary ideals of ordered semigroups and an ordered semigroups in which every ideal is primary and every ideal is semiprimary.

Definition 4.1. Let $(S, \cdot, \leqslant)$ be an ordered semigroup. An ideal I of S is said to be *left(right) primary* if

(i) If A, B are ideals of S such that $AB \subseteq I$ and $B \not\subseteq I (A \not\subseteq I)$ implies $A \subseteq Q^*(I) (B \subseteq Q^*(I))$.

(ii) $Q^*(I)$ is a prime ideal.

An ideal I of S is said to be *primary* if it is both the left and right primary ideal.

Remark 2. An ideal I of S satisfies condition (i) of Definition 4.1 if and only if for every $x, y \in S$ such that $I(x)I(y) \subseteq I$ and $y \notin I(x \notin I)$, then $x \in Q^*(I)(y \in Q^*(I))$.

We have the example to show that left primary, right primary and primary ideals are different.

Example 4.2. Let $(S, \cdot, \leqslant)$ be an ordered semigroup such that the multiplication and the order relation are defined by:

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

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

The ideals of S are: $\{a\}$, $\{a,b\}$ and S. It is evident that the ideal $\{a\}$ is right primary but not left primary.

Definition 4.3. Let $(S, \cdot, \leqslant)$ be an ordered semigroup. An ideal I of S is said to be *semiprimary* if $Q^*(I)$ is a prime ideal.

It is clear that every left(right) primary ideal is a semiprimary ideal.

Definition 4.4. An ordered semigroup $(S, \cdot, \leqslant)$ is said to be *(left, right, semi)primary* if every ideal of S is (left, right, semi)primary.

Theorem 4.5. *Let $(S, \cdot, \leqslant)$ be a pseudo symmetric ordered semigroup and A an ideal of S. Then A is left(right) primary if and only if for $x, y \in S$ such that $xy \in A$ and $y \notin A(x \notin A)$, then $x \in Q^*(A)(y \in Q^*(A))$.*

Proof. Assume that A a left primary. Let $x, y \in S$ such that $xy \in A$ and $y \notin A$. Since S is pseudo symmetric, we have $(xsy] \subseteq A$ for all $s \in S$. Thus $(xSy] \subseteq A$. It follows that $I(x)I(y) \subseteq A$. Since A is left primary and $I(y) \nsubseteq A$, we have $x \in I(x) \subseteq Q^*(A)$. Conversely, let $x, y \in S$ such that $I(x)I(y) \subseteq A$ and $y \notin A$. Then $xy \in A$ and so $x \in Q^*(A)$. Let $ab \in Q^*(A)$ for any $a, b \in S$ and $b \notin Q^*(A)$. Then $(ab)^n \in A$ for some positive integer n by Theorem 2.8. Let k be the least positive integer such that $(ab)^k \in A$. If $k = 1$, then $ab \in A$. Thus $a \in Q^*(A)$, which shows that $Q^*(A)$ is completely prime. It follows that $Q^*(A)$ is prime. If $k > 1$, then $ab(ab)^{k-1} = (ab)^k \in A$. If $b(ab)^{k-1} \in A$. Since $(ab)^{k-1} \notin A$, we have $b \in Q^*(A)$. This is a contradiction. Thus $b(ab)^{k-1} \notin A$ and so $a \in Q^*(A)$. It follows that $Q^*(A)$ is prime. Thus A is a left primary. □

It is easy to see the following lemma:

Lemma 4.6. *Let A and B be an ideals of an ordered semigroup $(S, \cdot, \leqslant)$. Then*

(1) *If $A \subseteq B$ then $Q^*(A) \subseteq Q^*(B)$;*

(2) *$Q^*(Q^*(A)) = Q^*(A)$;*

(3) $Q^*(A \cap B) = Q^*(A) \cap Q^*(B)$.

Theorem 4.7. *An ordered semigroup $(S, \cdot, \leqslant)$ is a left(right) primary if and only if every ideal in S satisfies condition (i) in Definition* 4.1.

Proof. Assume that every every ideal in S satisfies condition (i) in Definition 4.1. Let I be an ideal of S such that $AB \subseteq Q^*(I)$ for any ideals A, B of S. If $B \nsubseteq Q^*(I)$, then $A \subseteq Q^*(Q^*(I)) = Q^*(I)$. Thus $Q^*(I)$ is prime and so I is a left primary. The converse statement is clear. $\square$

Proposition 4.8. *Let A be an ideal of a pseudo symmetric semiprimary ordered semigroup $(S, \cdot, \leqslant)$. Then A is completely semiprime if and only if A is completely prime.*

Proof. Assume that A is completely semiprime. Let $ab \in A$ for any $a, b \in S$. Since S is a pseudo symmetric, we have $Q^*(A)$ is completely prime by Proposition 2.6. Thus $a \in Q^*(A)$ or $b \in Q^*(A)$. If $a, b \notin A$. Since A is completely semiprime, $a^n, b^n \notin A$ for all positive integer n. Thus $a, b \notin Q^*(A)$ by Theorem 2.8. This is contradiction. Thus A is completely prime. The converse statement is obvious. $\square$

Proposition 4.9. *Let $(S, \cdot, \leqslant)$ be a pseudo symmetric ordered semigroup. Then S is semiprimary if and only if every ideal A of S satisfies the condition: If $xy \in A$ for any $x, y \in S$, then $x \in Q^*(A)$ or $y \in Q^*(A)$.*

Proof. Assume that S is semiprimary. Let A be an ideal of S such that $xy \in A$ for any $x, y \in S$. Since S is a pseudo symmetric, we have $Q^*(A)$ is completely prime. Thus $x \in Q^*(A)$ or $y \in Q^*(A)$. Conversely, let A be an ideal of S and $xy \in Q^*(A)$ for any $x, y \in S$. Then $x \in Q^*(Q^*(A)) = Q^*(A)$ or $y \in Q^*(Q^*(A)) = Q^*(A)$, which shows that $Q^*(A)$ is completely prime. Thus $Q^*(A)$ is prime. Hence S is semiprimary. $\square$

Lemma 4.10. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. Then a maximal ideal M of S is prime if and only if $M = Q^*(M)$.*

Proof. If a maximal ideal M is prime, then $M = Q^*(M)$ is clear. Conversely, assume that $M = Q^*(M)$. Since M is a maximal ideal, we have M is prime. $\square$

Proposition 4.11. *Let A be an ideal of an ordered semigroup $(S, \cdot, \leqslant)$. If $Q^*(A)$ is a maximal ideal of S, then A is a semiprimary ideal.*

Proof. If $Q^*(A)$ is a maximal ideal of S, then $Q^*(A)$ is prime by Lemma 4.10. Thus A is a semiprimary ideal. $\square$

Lemma 4.12. *Let A be an ideal of an ordered semigroup $(S, \cdot, \leqslant)$ with identity. If $Q^*(A) = M$, where M is the unique maximal ideal of S, then A is a primary ideal.*

Proof. Let $x, y \in S$ such that $I(x)I(y) \subseteq A$ and $y \notin A$. If $x \notin Q^*(A) = M$. Then $I(x) \nsubseteq M$. Since each proper ideal of S is contained in M, we have $I(x) = S$. Thus $y = ey \in I(x)I(y) \subseteq A$. This is contradiction. Thus $x \in Q^*(A)$. We have $Q^*(A)$ is prime by Lemma 4.10. Thus A is a left primary ideal. Similarly, we have A is a right primary ideal. Hence A is a primary ideal. $\square$

Theorem 4.13. *Let $(S,\cdot,\leqslant)$ be an ordered semigroup with identity. If every(nonzero, assume this if S has 0) proper prime ideals are maximal, then S is a primary.*

Proof. If S is not a simple, then S has a unique maximal ideal M, which is the union of all proper ideals of S. By hypothesis M is the only proper (nonzero) prime ideal of S. If A is a proper (nonzero) ideal, then $Q^*(A) = M$. Thus A is primary by Lemma 4.12. If S has 0. If $I(0)$ is a prime ideal, then $I(0)$ is primary. If $I(0)$ is not prime, then $Q^*(I(0)) = M$. Thus $I(0)$ is primary by Lemma 4.12. Hence S is primary. □

Proposition 4.14. *Let $(S,\cdot,\leqslant)$ be an ordered semigroup. If A is a semiprime ideal in S, then the following conditions are equivalent:*

(1) *A is a prime.*

(2) *A is a primary.*

(3) *A is a left primary.*

(4) *A is a right primary.*

(5) *A is a semiprimary.*

Proof. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (5) and (2) $\Rightarrow$ (4) $\Rightarrow$ (5) are obvious. Since A is a semiprime, we have $Q^*(A) = A$ by Proposition 3.6. Thus (1) and (5) are equivalent. □

Theorem 4.15. *Let $(S,\cdot,\leqslant)$ be an ordered semigroup. Then S is semiprimary if and only if the set of all prime ideals of S forms a chain under the set inclusion.*

Proof. Let A and B be any prime ideals of S. Thus $A\cap B = Q^*(A\cap B)$. Since S is a semiprimary, $A\cap B$ is prime. If $A \not\subseteq B$ and $B \not\subseteq A$, then there exists elements $a,b\in S$ such that $a\in A\setminus B$ and $b\in B\setminus A$. Thus $I(a)I(b)\subseteq A\cap B$ and $a,b\notin A\cap B$. This is contradiction. Hence either $A\subseteq B$ or $B\subseteq A$. Conversely, let A be any ideal of S. If the set of all prime ideals of S forms a chain under the set inclusion, then $Q^*(A)$ is a prime, which shows that A is a semiprimary ideal. Thus S is a semiprimary. □

Theorem 4.16. *Let $(S,\cdot,\leqslant)$ be a duo semiprimary ordered semigroup. Then S has the following properties:*

(1) *Set of all prime ideals of S forms a chain under the set inclusion.*

(2) *For any $e,f\in E(S)$, either $e\leqslant xf$ and $e\leqslant fy$ or $f\leqslant xe$ and $f\leqslant ey$ for some $x,y\in S$.*

Proof. (1) This follow by Theorem 4.15. (2) Let $e,f\in E(S)$. Since S is semiprimary, we have $Q^*(I(e))$ and $Q^*(I(f))$ are prime. Thus $Q^*(I(e))\subseteq Q^*(I(f))$ or $Q^*(I(f))\subseteq Q^*(I(e))$ by (1). If $Q^*(I(e))\subseteq Q^*(I(f))$. Then $e^n\in I(f)$ for some positive integer n by Lemma 2.7. It follows that $e\in I(f)$. Since S is a duo ordered semigroup, we have $I(f) = (Sf] = (fS]$. Thus $e\leqslant xf$ and $e\leqslant fy$ for some $x,y\in S$. Similarly, if $Q^*(I(f))\subseteq Q^*(I(e))$ then $f\leqslant xe$ and $f\leqslant ey$ for some $x,y\in S$. □

Theorem 4.17. *Let $(S,\cdot,\leqslant)$ be a regular pseudo symmetric ordered semigroup. The following statements are equivalent:*

(1) *Every ideal of S is prime.*

(2) *S is a primary ordered semigroup.*

(3) *S is a left primary ordered semigroup.*

(4) *S is a right primary ordered semigroup.*

(5) *S is a semiprimary ordered semigroup.*

(6) *The set of all prime ideals of S forms a chain under the set inclusion.*

Proof. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (5) and (2) $\Rightarrow$ (4) $\Rightarrow$ (5) are obvious. (5) $\Rightarrow$ (1) Let A be an ideal of S and $x^2 \in A$ for any $x \in S$. Since S is regular pseudo symmetric, we have $x \in (xSx] \subseteq A$, which shows that A is completely semiprime. It follows that A is prime by Proposition 4.8 and Proposition 2.6. We have (5) and (6) are equivalent by Theorem 4.15. □

Following result is obvious its proof is omitted.

Lemma 4.18. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. The following statements are equivalent:*

(1) *Set of all the principal ideals of S forms a chain under the set inclusion.*

(2) *Set of all the ideals of S forms a chain under the set inclusion.*

Theorem 4.19. *Let $(S, \cdot, \leqslant)$ be a semisimple ordered semigroup. The following statements are equivalent:*

(1) *Every ideal of S is prime.*

(2) *S is a primary ordered semigroup.*

(3) *S is a left primary ordered semigroup.*

(4) *S is a right primary ordered semigroup.*

(5) *S is a semiprimary ordered semigroup.*

(6) *The set of all prime ideals of S forms a chain under the set inclusion.*

(7) *The set of all principal ideals of S forms a chain under the set inclusion.*

(8) *The set of all the ideals of S forms a chain under the set inclusion.*

Proof. Let A be an ideal of S. Since S is semisimple, we have A is a semiprime by Proposition 3.12. Thus (1) to (5) are equivalent by Proposition 4.14. We have (5) and (6) are equivalent by Theorem 4.15. The implication (8) $\Rightarrow$ (6) is obvious. (6) $\Rightarrow$ (7). Let $I(a)$ and $I(b)$ be a principal ideals of S. We have $Q^*(I(a)) \subseteq Q^*(I(b))$ or $Q^*(I(b)) \subseteq Q^*(I(a))$. Since S is a semisimple, $I(a) \subseteq I(b)$ or $I(b) \subseteq I(a)$. We have (7) and (8) are equivalent by Lemma 4.18. This complete the proof of the theorem. □

Theorem 4.20. *Let $(S, \cdot, \leqslant)$ be a duo semisimple ordered semigroup. The following statements are equivalent:*

(1) *Every ideal of S is prime.*

(2) *S is a primary ordered semigroup.*

(3) *S is a left primary ordered semigroup.*

(4) *S is a right primary ordered semigroup.*

(5) *S is a semiprimary ordered semigroup.*

(6) *The set of all prime ideals of S forms a chain under the set inclusion.*

(7) *The set of all principal ideals of S forms a chain under the set inclusion.*

(8) *The set of all the ideals of S forms a chain under the set inclusion.*

(9) *For any $e, f \in E(S)$, either $e \leqslant xf$ and $e \leqslant fy$ or $f \leqslant xe$ and $f \leqslant ey$ for some $x, y \in S$.*

Proof. We have (1) to (8) are equivalent by Theorem 4.19. (5) $\Rightarrow$ (9). By Theorem 4.16. (9) $\Rightarrow$ (7). Let $I(a)$ and $I(b)$ be a principal ideals of S. Since S is duo semisimple , we have S is regular. Thus $a \leqslant axa$ and $b \leqslant byb$ for some $x, y \in S$. It follows that $ax, by \in E(S)$. Then either $ax \leqslant sby$ and $ax \leqslant byt$ or $by \leqslant sax$ and $by \leqslant axt$ for some $s, t \in S$ by (9). If $ax \leqslant sby$ and $ax \leqslant byt$. We have $a \leqslant axa \leqslant axaxa \leqslant sbybyta \in (SbS] \subseteq I(b)$. Thus $I(a) \subseteq I(b)$. Similarly, if $by \leqslant sax$ and $by \leqslant axt$ then $I(b) \subseteq I(a)$. This complete the proof. □

Corollary 4.21. *Let $(S, \cdot, \leqslant)$ be a duo regular ordered semigroup. The following statements are equivalent:*

(1) *Every ideal of S is prime.*

(2) *S is a primary ordered semigroup.*

(3) *S is a left primary ordered semigroup.*

(4) *S is a right primary ordered semigroup.*

(5) *S is a semiprimary ordered semigroup.*

(6) *The set of all prime ideals of S forms a chain under the set inclusion.*

(7) *The set of all principal ideals of S forms a chain under the set inclusion.*

(8) *The set of all the ideals of S forms a chain under the set inclusion.*

(9) *For any $e, f \in E(S)$, either $e \leqslant xf$ and $e \leqslant fy$ or $f \leqslant xe$ and $f \leqslant ey$ for some $x, y \in S$.*

Corollary 4.22. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. Then every ideal of S is prime if and only if S is a semisimple (semi)primary.*

Proof. Assume that every ideal of S is prime. Let $x \in S$. We have $I(x)I(x) \subseteq (I(x)^2]$. Since $(I(x)^2]$ is an ideal of S, $I(x) \subseteq (I(x)^2]$ and so $I(x) = (I(x)^2]$. Thus S is a semisimple (semi)primary by Lemma 3.11 and Theorem 4.19. Conversely, if S is a semisimple (semi)primary, then every ideal of S is prime by Theorem 4.19. □

Corollary 4.23. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup. Then every ideal of S is prime if and only if S is a semisimple and the set of all the ideals of S forms a chain under the set inclusion.*

Corollary 4.24. *Let $(S, \cdot, \leqslant)$ be a duo ordered semigroup. The following statements are equivalent:*

(1) *Every ideal of S is prime.*

(2) *S is regular semiprimary.*

(3) *S is regular and for any $e, f \in E(S)$, either $e \leqslant xf$ and $e \leqslant fy$ or $f \leqslant xe$ and $f \leqslant ey$ for some $x, y \in S$.*

Acknowledgements. The authors are deeply grateful to the referee for careful reading of the manuscript and helpful suggestions.

References

[1] **A. Anjaneyulu**, *Primary ideals in semigroups*, Semigroup Forum, **20** (1980), 129 – 144.

[2] **A. Anjaneyulu**, *On primary semigroups*, Czech. Math. J., **30** (1980), 382 – 386.

[3] **A.K. Bhuniya and K. Hansda**, *On radicals of Greens relations in ordered semigroups*, Canad. Math. Bull., **60** (2017), 246 – 252.

[4] **G. Birkhoff**, *Lattice Theory*, AMS, Providence, 1984.

[5] **T. Changphas, P. Luangchaisri and R. Mazurek**, *On right chain ordered semigroups*, Semigroup Forum, **96** (2018), 523 – 535.

[6] **K. Hansda**, *Idempotent ordered semigroups*, (2017), 1706.08213v1. ??????????????????

[7] **N. Kehayopulu**, *m-Systems and n-systems in ordered semigroups*, Quasigroups and Related Systems, **11** (2004), 55 – 58.

[8] **H. Lal**, *Commutative semi-primary semigroups*, Czech. Math. J., **25** (1975), 1 – 3.

[9] **Y.S. Park and J.P. Kim**, *Prime and semiprime ideals in semigroups*, Kyungpook Math. J., **32** (1992), 629 – 633.

[10] **M. Satyanarayana,** *Commutative primary semigroups*, Czech. Math. J., **22** (1972), 509 – 516.

[11] **P. Summaprab and T. Changphas**, *Generalized kernels of ordered semigroups*, Quasigroups and Related Systems, **26** (2018), 309 – 316.

Received September 19, 2023

Department of Mathematics
Rajamangala University of Technology Isan
Khon Kaen Campus
Khon Kaen 40000 Thailand
e-mail: pisansu9999@gmail.com

Quasigroups and Related Systems **32** (2024), 141 – 154
https://doi.org/10.56415/qrs.v32.12

On ϕ-2-absorbing primary subsemimodules over commutative semirings

Issaraporn Thongsomnuk, Ronnason Chinram
Pattarawan Singavananda and Patipat Chumket

Abstract. In this paper, we introduce the concepts of ϕ-2-absorbing primary subsemimodules over commutative semirings. Let R be a commutative semiring with identity and M be an R-semimodule. Let $\boldsymbol{\phi} : S(M) \longrightarrow S(M) \cup \{\emptyset\}$ be a function, where $S(M)$ is the set of subsemimodules of M. A proper subsemimodule N of M is said to be a ϕ-2-absorbing primary subsemimodule of M if $rsx \in N \setminus \phi(N)$ implies $rx \in N$ or $sx \in N$ or $rs \in \sqrt{(N : M)}$, where $r, s \in R$ and $x \in M$. We prove some basic properties of these subsemimodules, give a characterization of ϕ-2-absorbing primary subsemimodules, and investigate ϕ-2-absorbing primary subsemimodules of quotient semimodules.

1. Introduction

In 2007, the concept of 2-absorbing ideals of rings was introducted by Badawi [3]. He defined *a 2-absorbing ideal* I of a commutative ring R to be a proper ideal and if whenever $a, b, c \in R$ with $abc \in I$, then $ab \in I$ or $ac \in I$ or $bc \in I$. Later in 2011 [7], Darani and Soheilnia introduced the concept of 2-absorbing submodules and studied their properties. A proper submodule N of an R-module M is said to be a *2-absorbing submodule of* M if $a, b \in R$ and $m \in M$ with $abm \in N$, then $am \in N$ or $bm \in N$ or $ab \in (N : M)$.

In 2012, Chaudhari introduced the concept of 2-absorbing ideals of a commutative semiring in [6]. He defined a *2-absorbing ideal* I of a commutative semiring R to be a proper ideal and if whenever $a, b, c \in R$ with $abc \in I$, then $ab \in I$ or $ac \in I$ or $bc \in I$. In the same year, Thongsomnuk

2010 Mathematics Subject Classification: 13C05, 13C13, 16Y60
Keywords: Semimodule, ϕ-2-absorbing primary subsemimodule, subtractive subsemimodule, Q-subsemimodule

introduced the concept of 2-*absorbing subsemimodules over commutative semirings* as a proper subsemimodule N of an R-semimodule M such that if whenever $a, b \in R$ and $m \in M$ with $abm \in N$, then $am \in N$ or $bm \in N$ or $ab \in (N : M)$. The concept of 2-absorbing ideals of commutative semirings and 2-absorbing subsemimodules has been widely recognized by several mathematicians, see [8] and [11].

Atani and Kohan (2010) introduced and examined the concept of primary ideals in a commutative semiring, as well as primary subsemimodules in semimodules over a commutative semiring (see [5]). They defined *a primary ideal I of a commutative semiring R* as a proper ideal, such that whenever $a, b \in R$ with $ab \in I$, then $a \in I$ or $b^k \in I$ for some $k \in \mathbb{N}$. Similarly, *a primary subsemimodule N of an R-semimodule M* is defined as a proper subsemimodule, such that whenever $a \in R$ and $m \in M$ with $am \in N$, then $m \in N$ or $a^k \in (N : M)$ for some $k \in \mathbb{N}$. In 2015, Dubey and Sarohe [9] defined the concept of 2-absorbing primary subsemimodules of a semimodule M over a commutative semiring R with $1 \neq 0$ which is a generalization of primary subsemimodules of semimodules. A proper subsemimodule N of a semimodule M is said to be a *2-absorbing primary subsemimodule of M* if $abm \in N$ implies $ab \in \sqrt{(N : M)}$ or $am \in N$ or $bm \in N$ for some $a, b \in R$ and $m \in M$.

Anderson and Batanieh (2008) generalized the concept of prime ideals, weakly prime ideals, almost prime ideals, n-almost prime ideals and ω-prime ideals of rings to ϕ-prime ideals of rings with ϕ, see in [1]. They defined a *ϕ-prime ideal I* of a ring R with ϕ be a proper ideal and if for $a, b \in R$, $ab \in I \setminus \phi(I)$ implies $a \in I$ or $b \in I$. Later in 2016, Petchkaew, Wasanawichit and Pianskool [13] introduced the concept of ϕ-n-absorbing ideals which are a generalization of n-absorbing ideals. A proper ideal I of R is called a *ϕ-n-absorbing ideal* if whenever $x_1, x_2, \ldots, x_{n+1} \in I \setminus \phi(I)$ for $x_1, x_2, \ldots x_{n+1} \in R$, then $x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_{n+1} \in I$ for some $i \in \{1, 2, \ldots, n+1\}$. In 2017, Moradi and Ebrahimpour [12] introduced the concept of ϕ-2-absorbing primary and ϕ-2-absorbing primary submodules. Let $\phi : S(M) \to S(M) \cup \{\emptyset\}$ be a function, where $S(M)$ is the set of $R-$module M. They said that a proper submodule N of M is a *ϕ-2-absorbing primary submodule* if $rsx \in N \setminus \phi(N)$ implies $rx \in N$, or $sx \in N$, or $rs \in \sqrt{(N : M)}$, where $r, s \in R$ and $x \in M$.

In this paper, we extend the concepts of ϕ-2-absorbing primary submodules over commutative rings to the concepts of ϕ-2-absorbing primary subsemimodules over commutative semirings. We explore fundamental properties of these subsemimodules, provide a characterization of ϕ-2-absorbing primary subsemimodules, and investigate ϕ-2-absorbing primary subsemimodules of quotient semimodules.

2. Preliminaries

Definition 2.1. [10] Let R be a semiring. A *left R-semimodule* (or a left semimodule over R) is a commutative monoid $(M, +)$ with additive identity 0_M for which a function $R \times M \to M$, denoted by $(r, m) \mapsto rm$ and called the scalar multiplication, satisfies the following conditions for all elements r and r' of R and all elements m and m' of M:

(1) $(rr')m = r(r'm)$,

(2) $r(m + m') = rm + rm'$,

(3) $(r + r')m = rm + r'm$,

(4) $1_R m = m$, and

(5) $r0_M = 0_M = 0_R m$.

Throughout this paper, we assume that R is a commutative semirings identity $1 \neq 0$ and a left R-semimodule will be considered as a unitary semimodule.

Definition 2.2. [10] Let M be an R-semimodule and N a subset of M. We say N is a *subsemimodule of M* precisely when N is itself an R-semimodule with respect to the operations for M.

Definition 2.3. [5] Let M be an R-semimodule, N a subsemimodule of M, and $m \in M$. Then an *associated ideal* of N is denoted as
$(N : M) = \{r \in R \mid rM \subseteq N\}$ and $(N : m) = \{r \in R \mid rm \in N\}$.

Definition 2.4. [5] An ideal I of a semiring R is called a *subtractive ideal* if $a, a + b \in I$ and $b \in R$, then $b \in I$.

A subsemimodule N of an R-semimodule M is called a *subtractive subsemimodule* if $x, x + y \in N$ and $y \in M$, then $y \in N$.

Proposition 2.5. [5] *Let M be an R-semimodule. If N is a subtractive subsemimodule of M and $m \in M$, then $(N : M)$ and $(N : m)$ are subtractive ideals of R.*

Lemma 2.6. *Let* $(N : M)$ *be a subtractive ideal of* R. *If* $a \in (N : M)$ *and* $a + b \in \sqrt{(N : M)}$, *then* $b \in \sqrt{(N : M)}$.

Proof. Assume that $a \in (N : M)$ and $a + b \in \sqrt{(N : M)}$. There exists $k \in \mathbb{N}$ such that $(a + b)^k \in (N : M)$. Then $\sum_{i=0}^{k} \binom{k}{i} a^{k-i} b^i \in (N : M)$. Since $\sum_{i=0}^{k-1} \binom{k}{i} a^{k-i} b^i \in (N : M)$ and $(N : M)$ is a subtractive ideal, we obtain $b^k \in (N : M)$. Thus, $b \in \sqrt{(N : M)}$. □

Definition 2.7. [12] Let M be an R-semimodule. We define the functions $\phi_\alpha : S(M) \to S(M) \cup \{\emptyset\}$ as follows: $\phi_0(N) = 0$, $\phi_\emptyset(N) = \emptyset$, $\phi_{m+1}(N) = (N : M)^m N$ for every $m \geqslant 0$ and $\phi_\omega(N) = \bigcap_{m=0}^{\infty} (N : M)^m N$, where N is a subsemimodule of M and $S(M)$ is the set of subsemimodules of M.

Definition 2.8. [12] Let M be an R-semimodule, $S(M)$ the set of subsemimodules of M and let $f_1, f_2 \colon S(M) \to S(M) \cup \{\emptyset\}$ be two functions. Then $f_1 \leqslant f_2$ if $f_1(N) \subseteq f_2(N)$ for all $N \in S(M)$.

Definition 2.9. [2] A subsemimodule N of an R-semimodule M is called a *partitioning subsemimodule*(or Q-*subsemimodule*) if there exists a nonempty subset Q of M such that

1. $RQ \subseteq Q$ where $RQ = \{rq | r \in R \text{ and } q \in Q\}$,
2. $M = \cup\{q + N | q \in Q\}$ where $q + N = \{q + n | n \in N\}$, and
3. if $q_1, q_2 \in Q$, then $(q_1 + N) \cap (q_2 + N) \neq \emptyset$ if and only if $q_1 = q_2$.

Let M be an R-semimodule and N a Q-subsemimodule of M. Let $M/N_{(Q)} = \{q + N | q \in Q\}$. Then $M/N_{(Q)}$ is a semimodule over R under the addition $\oplus$ and the scalar multiplication $\odot$ defined as follow: for any $q_1, q_2, q \in Q$ and $r \in R$, $(q_1+N) \oplus (q_2+N) = q_3+N$ and $r \bigodot (q+N) = q_4+N$ where $q_3, q_4 \in Q$ are the unique elements such that $q_1 + q_2 + N \subseteq q_3 + N$ and $rq + N \subseteq q_4 + N$. The R-semimodule $M/N_{(Q)}$ is called the *quotient semimodule of* M *by* N.

Lemma 2.10. [4] *Let* M *be an* R-*semimodule,* N *a* Q-*subsemimodule of* M *and* P *a subtractive subsemimodule of* M *with* $N \subseteq P$. *Then the followings hold:*

1. N *is a* $Q \cap P$-*subsemimodule of* P.
2. $P/N_{(Q\cap P)} = \{q + N | q \in Q \cap P\}$ *is a subsemimodule of* $M/N_{(Q)}$.

Remark 2.11. *The zero element of* $P/N_{Q\cap P}$ *is the same as the zero element of* $M/N_{(Q)}$ *which is* $0_M + N$.

3. ϕ-2-absorbing primary subsemimodules

In this section, we investigate the ϕ-2-absorbing primary subsemimodules over commutative semirings. Initially, we introduce a novel definition for ϕ-2-absorbing primary subsemimodules. Subsequently, we explore various properties of ϕ-2-absorbing primary subsemimodules.

Definition 3.1. Let M be an R-semimodule, $\boldsymbol{\phi} : S(M) \longrightarrow S(M) \cup \{\emptyset\}$ a function, where $S(M)$ is the set of subsemimodules of M. We say a proper subsemimodule N of M is a *ϕ-2-absorbing primary subsemimodule* if whenever $rsx \in N \backslash \phi(N)$ implies $rx \in N$, or $sx \in N$, or $rs \in \sqrt{(N : M)} = \{a \in R \mid a^n M \subseteq N \text{ for some } n \in \mathbb{N}\}$, where $r, s \in R$ and $x \in M$.

Theorem 3.2. *Let M be an R-semimodule, N a ϕ-2-absorbing primary subsemimodule of M and K be a subsemimodule of M such that $\phi(N \cap K) = \phi(N)$. Then $N \cap K$ is a ϕ-2-absorbing primary subsemimodule of K.*

Proof. Clearly, $N \cap K$ is a proper subsemimodule of K. Let $rsx \in (N \cap K) \setminus \phi(N \cap K)$ where $r, s \in R$ and $x \in K$. We have $rsx \in N \setminus \phi(N \cap K)$. Thus, $rsx \in N \setminus \phi(N)$ because $\phi(N \cap K) = \phi(N)$. Since N is a ϕ-2-absorbing primary subsemimodule of M, we obtain $rx \in N$, or $sx \in N$, or $rs \in \sqrt{(N : M)}$. If $rx \in N$ or $sx \in N$, then $rx \in N \cap K$ or $sx \in N \cap K$ because $x \in K$ and K is an R-semimodule. If $rs \in \sqrt{(N : M)}$, then $(rs)^n M \subseteq N$ for some positive integer n. In particular, $(rs)^n K \subseteq (rs)^n M \subseteq N$ and we know that $(rs)^n K \subseteq K$. Then $(rs)^n K \subseteq N \cap K$ for some positive integer n. Thus, $rs \in \sqrt{(N \cap K : K)}$. Hence $N \cap K$ is a ϕ-2-absorbing primary subsemimodule of K. □

Consider the following example. Let $R = \mathbb{Z}_0^+$ and $M = \mathbb{Z}_0^+$, where throughout this paper, $\mathbb{Z}_0^+$ denotes the set of non-negative integers (including zero). We define the function $\phi : S(\mathbb{Z}_0^+) \to S(\mathbb{Z}_0^+) \cup \{\emptyset\}$ by $\phi(A) = \{0\}$ where $A \in S(\mathbb{Z}_0^+)$. Clearly, $8\mathbb{Z}_0^+$ is a ϕ-2-absorbing primary subsemimodule of $\mathbb{Z}_0^+$ and $m\mathbb{Z}_0^+$ is a subsemimodule of $\mathbb{Z}_0^+$ where $m \in \mathbb{Z}_0^+$. We see that $\phi(8\mathbb{Z}_0^+ \cap m\mathbb{Z}_0^+) = \{0\} = \phi(8\mathbb{Z}_0^+)$. Then $8\mathbb{Z}_0^+ \cap m\mathbb{Z}_0^+ = [8, m]\mathbb{Z}_0^+$ is a ϕ-2-absorbing primary subsemimodule of $m\mathbb{Z}_0^+$. This example demonstrates the concept outlined in Theorem 3.13.

Theorem 3.3. *Let M be an R-semimodule, $\boldsymbol{\phi} : S(M) \longrightarrow S(M) \cup \{\phi\}$ a function, and let N be a proper subsemimodule of M. Then the following conditions are equivalent:*

1. *N is a ϕ-2-absorbing primary subsemimodule of M.*

2. *For every $r \in R$ and $x \in M$ with $rx \notin N$,*

$$(N : rx) \subseteq (\sqrt{(N : M)} : r) \cup (N : x) \cup (\phi(N) : rx).$$

Proof. First, let $a \in (N : rx)$. Then $arx \in N$. If $arx \in \phi(N)$, then $a \in (\phi(N) : rx)$. If $arx \notin \phi(N)$, then $arx \in N \setminus \phi(N)$. Since N is a ϕ-2-absorbing primary subsemimodule of M and $rx \notin N$, we have $ax \in N$ or $a \in (\sqrt{(N : M)} : r)$. Hence $(N : rx) \subseteq (\sqrt{(N : M)} : r) \cup (N : x) \cup (\phi(N) : rx)$.

Conversely, let $r, s \in R$ and $x \in M$ with $rsx \in N \setminus \phi(N)$ and $rx \notin N$. Since $rsx \in N$ and $rsx \notin \phi(N)$, we obtain $s \in (N : rx)$ and $s \notin (\phi(N) : rx)$. From $(N : rx) \subseteq (\sqrt{(N : M)} : r) \cup (N : x) \cup (\phi(N) : rx)$. Thus, $s \in (\sqrt{(N : M)} : r)$ or $s \in (N : x)$. Hence, $sr \in \sqrt{(N : M)}$ or $sx \in N$. Therefore, N is a ϕ-2-absorbing primary subsemimodule of M. □

Moradi and Ebrahimpour [12] introduced the definition of ϕ-triple-zero within the context of submodules. In this work, we will extend and adapt this definition to apply specifically to subsemimodules.

Definition 3.4. Let M be an R-semimodule, and $\boldsymbol{\phi} : S(M) \longrightarrow S(M) \cup \{\emptyset\}$ a function. Assume that N is a ϕ-2-absorbing primary subsemimodule of M, $r, s \in R$ and $x \in M$. We say (r, s, x) is a *ϕ-triple-zero* of N if $rsx \in \phi(N), rx, sx \notin N$ and $rs \notin \sqrt{(N : M)}$.

Theorem 3.5. *Let M be an R-semimodule, $\boldsymbol{\phi} : S(M) \longrightarrow S(M) \cup \{\emptyset\}$ a function, and let N be a subtractive subsemimodule of M such that $\phi(N) \subseteq N$. Assume that N is a ϕ-2-absorbing primary subsemimodule of M and (r, s, x) is a ϕ-triple-zero of N. Then the following statements hold:*

1. *$r(N : M)x \subseteq \phi(N)$ and $s(N : M)x \subseteq \phi(N)$.*

2. *$(N : M)^2 x \subseteq \phi(N)$.*

3. *$rsN \subseteq \phi(N)$.*

4. *$r(N : M)N \subseteq \phi(N)$ and $s(N : M)N \subseteq \phi(N)$.*

Proof. (1). Suppose that there exists $t \in (N : M)$ such that $rtx \notin \phi(N)$. Since (r, s, x) is a ϕ-triple-zero of N, we have $rsx \in \phi(N)$. So, $r(s + t)x = rsx + rtx \notin \phi(N)$. Since $\phi(N) \subseteq N$, we obtain $r(s + t)x \in N \setminus \phi(N)$.

Since N is a ϕ-2-absorbing primary subsemimodule of M and $rx, sx \notin N$, we have $r(t+s) \in \sqrt{(N:M)}$. By Lemma 2.6 and $rt \in (N:M)$, we have $rs \in \sqrt{(N:M)}$, which is a contradiction with ϕ-triple-zero of N. Therefore, $r(N:M)x \subseteq \phi(N)$. Similarly, $s(N:M)x \subseteq \phi(N)$.

(2). Suppose that there exists $t, k \in (N:M)$ such that $tkx \notin \phi(N)$. Since (r,s,x) is a ϕ-triple-zero of N, we have $rsx \in \phi(N)$. By part (1), we have $stx, rkx \in \phi(N)$. Thus, $(t+r)(k+s)x \notin \phi(N)$. Then $(t+r)(k+s)x \in N \backslash \phi(N)$. Since N is a ϕ-2-absorbing primary subsemimodule of M and $rx, sx \notin N$, we have $(t+r)(k+s) \in \sqrt{(N:M)}$. By Lemma 2.6, we obtain $rs \in \sqrt{(N:M)}$, which is a contradiction with ϕ-triple-zero of N. Hence, $(N:M)^2x \subseteq \phi(N)$.

(3). Suppose that there exists $y \in N$ such that $rsy \notin \phi(N)$. Since (r,s,x) is a ϕ-triple-zero of N, we have $rsx \in \phi(N)$. So, $rs(x+y) \notin \phi(N)$. Then $rs(x+y) \in N \backslash \phi(N)$ because $\phi(N) \subseteq N$. Since N is a ϕ-2-absorbing primary subsemimodule, $r(x+y) \in N$ or $s(x+y) \in N$ or $rs \in \sqrt{(N:M)}$. Since N is a subtractive subsemimodule and $y \in N$, we obtain $rx \in N$ or $sx \in N$ or $rs \in \sqrt{(N:M)}$, which is a contradiction with ϕ-triple-zero of N. Therefore, $rsN \subseteq \phi(N)$.

(4). Suppose that there exists $t \in (N:M)$ and $y \in N$ such that $rty \notin \phi(N)$. Since (r,s,x) is a ϕ-triple-zero of N, we obtain $rsx \in \phi(N)$. By parts (1) and (3), we have $rtx, rsy \in \phi(N)$. So, $r(s+t)(x+y) \notin \phi(N)$. Since $\phi(N) \subseteq N$ and $y \in N$, we get $r(s+t)(x+y) \in N \backslash \phi(N)$. Since N is a ϕ-2-absorbing primary subsemimodule, $r(x+y) \in N$ or $(s+t)(x+y) \in N$ or $r(s+t) \in \sqrt{(N:M)}$. Since N is a subtractive subsemimodule and Lemma 2.6, we have $rx \in N$ or $sx \in N$ or $rs \in \sqrt{(N:M)}$, which is a contradiction with ϕ-triple-zero of N. Hence, $r(N:M)N \subseteq \phi(N)$. Similarly, $s(N:M)N \subseteq \phi(N)$. □

Corollary 3.6. *Let M be an R-semimodule, $\boldsymbol{\phi} : S(M) \longrightarrow S(M) \cup \{\emptyset\}$ a function, and let N be a subtractive subsemimodule of M such that $\phi(N) \subseteq N$. Assume that N is a ϕ-2-absorbing primary subsemimodule of M and is not a 2-absorbing primary subsemimodule. Then $(N:M)^2N \subseteq \phi(N)$.*

Proof. Since N is a ϕ-2-absorbing primary subsemimodule of M and is not a 2-absorbing primary subsemimodule, we have (r,s,x) is a ϕ-triple-zero of N. Assume that $t, k \in (N:M)$, $y \in N$ and $tky \notin \phi(N)$. So, $tky \in N \backslash \phi(N)$. Consider $(r+t)(s+k)(x+y) \notin \phi(N)$ because N is a ϕ-triple zero and Theorem 3.5 and $\phi(N) \subseteq N$ is subtractive subsemimodule. Then $(r+t)(s+k)(x+y) \in N \backslash \phi(N)$. Since N is a ϕ-2-absorbing primary subsemimodule, we have $(r+t)(x+y) \in N$ or $(s+k)(x+y) \in N$ or $(r+t)(s+k) \in \sqrt{(N:M)}$. Since N is a subtractive subsemimodule and Lemma 2.6, we have $rx \in N$ or $sx \in N$ or $rs \in \sqrt{(N:M)}$, which is a contradiction with ϕ-triple-zero of N. Therefore, $(N:M)^2N \subseteq \phi(N)$. $\square$

To illustrate Theorem 3.16(3), consider the following example. We define a function $\phi : S(\mathbb{Z}_0^+) \to S(\mathbb{Z}_0^+) \cup \{\emptyset\}$ by $\phi(A) = 2A$ where $A \in S(\mathbb{Z}_0^+)$. In this context, $15\mathbb{Z}_0^+$ is demonstrably a ϕ-2-absorbing primary subsemimodule and a subtractive subsemimodule of $\mathbb{Z}_0^+$. Interestingly, $30\mathbb{Z}_0^+ = \phi(15\mathbb{Z}_0^+) \subseteq 15\mathbb{Z}_0^+$. Furthermore, the triplet $(3, 10, 2)$ qualifies as a ϕ-triple-zero of $15\mathbb{Z}_0^+$. In this case, $(3 \cdot 10) \cdot 15\mathbb{Z}_0^+ = 450\mathbb{Z}_0^+ \subseteq 30\mathbb{Z}_0^+$, which aligns with the concept outlined in Theorem 3.16(3).

In 2017, the concept of weakly ϕ-2-absorbing primary submodules was introduced by Moradi and Ebrahimpour [12]. In the current study, we will extend this idea and provide a definition for weakly ϕ-2-absorbing primary subsemimodules.

Definition 3.7. Let M be an R-semimodule, $\phi : S(M) \to S(M) \cup \{\emptyset\}$ be a function, where $S(M)$ is the set of $R-$module M. They said that a proper submodule N of M is a *weakly ϕ-2-absorbing primary submodule* if $0 \neq rsx \in N \setminus \phi(N)$ implies $rx \in N$, or $sx \in N$, or $rs \in \sqrt{(N:M)}$, where $r, s \in R$ and $x \in M$.

Proposition 3.8. *Let M be an R-semimodule, $\boldsymbol{\phi} : S(M) \longrightarrow S(M) \cup \{\emptyset\}$ a function, and let N be subtractive subsemimodule of M such that $\phi(N) \subseteq N$ that is not 2-absorbing primary subsemimodule of M. If N is a weakly 2-absorbing primary subsemimodule of M, then $(N:M)^2N = \{0\}$.*

Proof. Assume that N is a weakly 2-absorbing primary subsemimodule of M but N is not 2-absorbing primary subsemimodule of M. Then N is a ϕ_0-2-absorbing primary subsemimodule of M. By Corollary 3.6, we obtain $(N:M)^2N \subseteq \phi_0(N) = \{0\}$. Clearly, $\{0\} \subseteq (N:M)^2N$. Thus, $(N:M)^2N = \{0\}$. $\square$

Subsequently, we analyze the function ϕ_n, as defined in Definition 2.7, for cases where $n \leqslant 4$. We also explore the function ϕ_ω, also defined in Definition 2.7, which establishes a connection with ϕ-2-absorbing primary subsemimodules.

Proposition 3.9. *Let M be an R-semimodule, $\boldsymbol{\phi} : S(M) \longrightarrow S(M) \cup \{\emptyset\}$ a function, and let N be subtractive subsemimodule of M such that*

$\phi(N) \subseteq N$ that is not 2-absorbing primary subsemimodule of M. If N is a ϕ-2-absorbing primary subsemimodule of M for some ϕ with $\phi \leqslant \phi_4$, then $(N : M)^2N = (N : M)^3N$.

Proof. Assume that N is a ϕ-2-absorbing primary subsemimodule of M with $\phi \leqslant \phi_4$ and N is not 2-absorbing primary subsemimodule. By Corollary 3.6, we obtain $(N : M)^2N \subseteq \phi(N)$. Since $\phi \leqslant \phi_4$, then $\phi(N) \subseteq \phi_4(N) = (N : M)^3N$. Now, we have $(N : M)^2N \subseteq (N : M)^3N$. Since N is an R-semimodule, we have $(N : M)^3N = (N : M)(N : M)^2N \subseteq (N : M)^2N$. Therefore, $(N : M)^2N = (N : M)^3N$. □

Corollary 3.10. *Let M be an R-semimodule, $\phi : S(M) \longrightarrow S(M) \cup \{\emptyset\}$ a function, and let N be subtractive subsemimodule of M such that $\phi(N) \subseteq N$. If N is a ϕ-2-absorbing primary subsemimodule of M with $\phi \leqslant \phi_4$, then N is a ϕ_ω-2-absorbing primary subsemimodule of M.*

Proof. Assume that N is a ϕ-2-absorbing primary subsemimodule of M with $\phi \leqslant \phi_4$. It's clear that N is a ϕ_ω-2-absorbing primary subsemimodule of M if N is a 2-absorbing primary subsemimodule. Now, we consider in case that N is not 2-absorbing primary, then $(N : M)^2N = (N : M)^3N$, by Proposition 3.9. Since N is a ϕ-2-absorbing primary subsemimodule of M with $\phi \leqslant \phi_4$, we have N is ϕ_4-2-absorbing primary. So, $\phi_\omega(N) = \bigcap_{m=0}^{\infty}(N : M)^mN = (N : M)^3N = \phi_4$. Thus, N is a ϕ_ω-2-absorbing primary subsemimodule of M. □

Lemma 3.11. *Let N be a subtractive ϕ-2-absorbing primary subsemimodule of an R-semimodule M and $a, b \in R$. Suppose that $abK \subseteq N\backslash\phi(N)$ for some subsemimodule K of M. Then $ab \in \sqrt{(N : M)}$ or $aK \subseteq N$ or $bK \subseteq N$.*

Proof. Let $abK \subseteq N \setminus \phi(N)$ for some subsemimodule K of M. Assume that $ab \notin \sqrt{(N : M)}$, $aK \nsubseteq N$ and $bK \nsubseteq N$. Then $ak_1 \notin N$ and $bk_2 \notin N$ for some $k_1, k_2 \in K$. Since $abk_1 \in N\backslash\phi(N)$, $ab \notin \sqrt{(N : M)}$, $ak_1 \notin N$ and N is a ϕ-2-absorbing primary subsemimodule, we have $bk_1 \in N$. Since $abk_2 \in N\backslash\phi(N), ab \notin \sqrt{(N : M)}, bk_2 \notin N$ and N is a ϕ-2-absorbing primary subsemimodule, we obtain $ak_2 \in N$. We know that $ab(k_1 + k_2) \in N\backslash\phi(N)$ and $ab \notin \sqrt{(N : M)}$. Since N is a ϕ-2-absorbing primary subsemimodule, we have $a(k_1 + k_2) \in N$ or $b(k_1 + k_2) \in N$. If $a(k_1 + k_2) \in N$, then $ak_1 \in N$ (as N is a subtractive), which is a contradiction. If $b(k_1+k_2) \in N$, then $bk_2 \in N$ (as N is a subtractive), which is a contradiction. Hence, $ab \in \sqrt{(N : M)}$ or $aK \subseteq N$ or $bK \subseteq N$. □

Theorem 3.12. *Let K be a subtractive subsemimodule of M and $\sqrt{(K:M)}$ be a subtractive ideal of R. If K is a ϕ-2-absorbing primary subsemimodule of M, then whenever $IJN \subseteq K\backslash\phi(K)$ for some ideals I, J of R and a subsemimodule N of M, then $IJ \subseteq \sqrt{(K:M)}$ or $IN \subseteq K$ or $JN \subseteq K$.*

Proof. Let K be a ϕ-2-absorbing primary subsemimodule of M. Assume that $IJN \subseteq K\backslash\phi(K)$ for some ideals I, J of R and a subsemimodule N of M. Suppose that $IJ \nsubseteq \sqrt{(K:M)}$, $IN \nsubseteq K$ and $JN \nsubseteq K$. Then $a_1N \nsubseteq K$ and $b_1N \nsubseteq K$ for some $a_1 \in I$ and $b_1 \in J$. Since $a_1b_1N \subseteq K\backslash\phi(K), a_1N \nsubseteq K, b_1N \nsubseteq K$ and Lemma 3.11, we have $a_1b_1 \in \sqrt{(K:M)}$. Since $IJ \nsubseteq \sqrt{(K:M)}$, we have $a_2b_2 \notin \sqrt{(K:M)}$ for some $a_2 \in I$ and $b_2 \in J$. Since $a_2b_2N \subseteq K\backslash\phi(K)$ and $a_2b_2 \notin \sqrt{(K:M)}$, we have $a_2N \subseteq K$ or $b_2N \subseteq K$ by Lemma 3.11. Here three cases arise.

Case I: When $a_2N \subseteq K$ but $b_2N \nsubseteq K$. Since $a_1b_2N \subseteq K\backslash\phi(K)$, $b_2N \nsubseteq K$ and $a_1N \nsubseteq K$, then by Lemma 3.11, $a_1b_2 \in \sqrt{(K:M)}$. We know that $a_2N \subseteq K$ but $a_1N \nsubseteq K$, so $(a_1+a_2)N \nsubseteq K$ (as K is subtractive). Since $(a_1+a_2)b_2N \subseteq K\backslash\phi(K)$, $b_2N \nsubseteq K$ and $(a_1+a_2)N \nsubseteq K$, we have $(a_1+a_2)b_2 \in \sqrt{(K:M)}$ by Lemma 3.11. Since $a_1b_2 \in \sqrt{(K:M)}$ and $\sqrt{(K:M)}$ is subtractive, we have $a_2b_2 \in \sqrt{(K:M)}$, which is a contradiction.

Case II: When $b_2N \subseteq K$ but $a_2N \nsubseteq K$. We can conclude similary to Case I.

Case III: When $a_2N \subseteq K$ and $b_2N \subseteq K$. Since $b_2N \subseteq K$ and $b_1N \nsubseteq K$, we have $(b_1+b_2)N \nsubseteq K$. Since $a_1(b_1+b_2)N \subseteq K\backslash\phi(K)$, $(b_1+b_2)N \nsubseteq K$ and $a_1N \nsubseteq K$, we get that $a_1(b_1+b_2) \in \sqrt{(K:M)}$ by Lemma 3.11. Since $a_1b_1 \in \sqrt{(K:M)}$ and $\sqrt{(K:M)}$ is subtractive, we conclude that $a_1b_2 \in \sqrt{(K:M)}$. Since $a_2N \subseteq K$, $a_1N \nsubseteq K$ and K is subtractive implies $(a_1+a_2)N \nsubseteq K$. Since $(a_1+a_2)b_1N \subseteq K\backslash\phi(K)$, $(a_1+a_2)N \nsubseteq K$ and $b_1N \nsubseteq K$, we have $(a_1+a_2)b_1 \in \sqrt{(K:M)}$ by Lemma 3.11. Since $a_1b_1 \in \sqrt{(K:M)}$, $(a_1+a_2)b_1 \in \sqrt{(K:M)}$ and $\sqrt{(K:M)}$ is subtractive, we have $a_2b_1 \in \sqrt{(K:M)}$. Since $(a_1+a_2)(b_1+b_2)N \subseteq K\backslash\phi(K)$, $(a_1+a_2)N \nsubseteq K$ and $(b_1+b_2)N \nsubseteq K$, by Lemma 3.11, $(a_1+a_2)(b_1+b_2) \in \sqrt{(K:M)}$. Since $a_2b_1, a_1b_2, a_1b_1 \in \sqrt{(K:M)}$ and $\sqrt{(K:M)}$ is subtractive, then $a_2b_2 \in \sqrt{(K:M)}$, which is a contradiction.

Hence, $IJ \subseteq \sqrt{(K:M)}$ or $IN \subseteq K$ or $JN \subseteq K$. □

Theorem 3.13. *Let M an R-semimodule, and let $\phi : S(M) \longrightarrow S(M) \cup \{\emptyset\}$ be a function. Assume that N is a subsemimodule of M such that $\phi(N)$ is a*

2-absorbing primary subsemimodule of M and $\phi(N) \subseteq N$. Then N is a ϕ-2-absorbing primary subsemimodule of M if and only if N is a 2-absorbing primary subsemimodule of M.

Proof. First, assume that N is a ϕ-2-absorbing primary subsemimodule of M and $\phi(N)$ is a 2-absorbing primary subsemimodule of M. Let $r, s \in R$ and $x \in M$ with $rsx \in N$. Suppose that neither rx nor sx is in N. Here two cases arise.

Case I: $rsx \in \phi(N)$. Then $rs \in \sqrt{(\phi(N) : M)} \subseteq \sqrt{(N : M)}$ because $\phi(N)$ is a ϕ-2-absorbing primary subsemimodule, $\phi(N) \subseteq N$ and $rx, sx \notin N$.

Case II: $rsx \notin \phi(N)$. Since N is a ϕ-2-absorbing primary subsemimodule and $rx, sx \notin N$, we obtain $rs \in \sqrt{(N : M)}$.

Conversely, it's clearly. $\square$

Let M be an R-semimodule, N be a Q-subsemimodule of M. For a function $\boldsymbol{\phi} : S(M) \longrightarrow S(M) \cup \{\emptyset\}$ we define the function $\boldsymbol{\phi_N} : S(M/N_{(Q)}) \longrightarrow S(M/N_{(Q)}) \cup \{\emptyset\}$ by $\phi_N(K/N) = \phi(K)/N_{(\phi(K)\cap Q)}$ if $\phi(K) \neq \emptyset$, and $\phi_N(K/N) = \emptyset$ if $\phi(K) = \emptyset$, for every subsemimodule K of M with $N \subseteq K$.

Theorem 3.14. *Let M be an R-semimodule, N a Q-subsemimodule of M and $P, \phi(P)$ are subtractive subsemimodules of M with $N \subseteq P$. Then P is a ϕ-2-absorbing primary subsemimodule of M if and only if $P/N_{(Q\cap P)}$ is a ϕ_N-2-absorbing primary subsemimodule of $M/N_{(Q)}$.*

Proof. First, assume that P is a ϕ-2-absorbing primary subsemimodule of M. Then we have $P/N_{(Q\cap P)}$ is a subsemimodule of $M/N_{(Q)}$. Now let $r, s \in R$ and $q_1 + N \in M/N_{(Q)}$ where $q_1 \in Q$ be such that $rs \odot (q_1 + N) \in P/N_{(Q\cap P)} \setminus \phi_N(P/N_{(Q\cap P)})$. Then there existe unique $q_2 \in Q \cap P$ such that $rs \odot (q_1 + N) = q_2 + N$ where $rsq_1 + N \subseteq q_2 + N$. Since $q_2 \in P$ and $N \subseteq P$, we have $rsq_1 + N \subseteq P$. Since $N \subseteq P$ and P is a subtractive subsemimodule, $rsq_1 \in P$. Since $rsq_1 + N \subseteq q_2 + N \notin \phi_N(P/N_{(Q\cap P)})$, we obtain $rsq_1 + N \subseteq q_2 + N \notin \phi(P)/N_{(Q\cap\phi(P))}$. Thus, we have $rsq_1 = q_2 + x$ for some $x \in N \subseteq \phi(P)$. Since $q_2 \notin Q \cap \phi(P)$, we get $q_2 \notin \phi(P)$. Then $rsq_1 = q_2 + x \notin \phi(P)$ because $\phi(P)$ is subtractive. Now, we have $rsq_1 \in P \setminus \phi(P)$. Since P is a ϕ-2-absorbing subsemimodule of M, it can be concluded that $rq_1 \in P$ or $sq_1 \in P$ or $rs \in \sqrt{(P : M)}$. We claim that $r \odot (q_1 + N) \in P/N_{(Q\cap P)}$ or $s \odot (q_1 + N) \in P/N_{(Q\cap P)}$ or $rs \in \sqrt{(P/N_{(Q\cap P)} : M/N_{(Q)}}$.

Case I: $rq_1 \in P$. Since $q_1 \in Q$, we have $rq_1 \in Q$. Then $rq_1 \in Q \cap P$. So, $rq_1 + N \in P/N_{(Q\cap P)}$. Moreover, $r \odot (q_1 + N) = q_3 + N$ where $q_3 \in Q$ is unique such that $rq_1 + N \subseteq q_3 + N$. Then $rq_1 = q_3 + x_1$ for some $x_1 \in N \subseteq P$. Since P is subtractive, we have $q_3 \in P$. Thus, $r \odot (q_1 + N) = q_3 + N \in P/N_{(Q\cap P)}$.

Case II: $sq_1 \in P$. We can conclude similarly to Case I that $s \odot (q_1 + N) \in P/N_{(Q\cap P)}$.

Case III: $rs \in \sqrt{(P : M)}$. Then there exists $k \in \mathbb{N}$ such that $(rs)^k \in (P : M)$. So, $(rs)^k M \subseteq P$. Let $q + N \in M/N_{(Q)}$ where $q \in Q$. Consider $(rs)^k \odot (q + N) = q_4 + N$ where $q_4 \in Q$ is unique such that $(rs)^k + N \subseteq q_4 + N$. So, $(rs)^k q = q_4 + x_2$ for some $x_2 \in N \subseteq P$. Since $(rs)^k \in (P : M)$, we have $(rs)^k q \in P$. Hence, $q_4 \in P$ because P is subtractive. Then $q_4 \in Q \cap P$. Thus, $(rs)^k \odot (q + N) = q_4 + N \in P/N_{(Q\cap P)}$. Hence, $rs \in \sqrt{(P/N_{(Q\cap P)} : M/N_{(Q)}}$.

Therefore, $P/N_{(Q\cap P)}$ is a ϕ_N-2-absorbing primary subsemimodule of $M/N_{(Q)}$.

Conversely, assume that $P/N_{(Q\cap P)}$ is a ϕ_N-2-absorbing primary subsemimodule of M. Let $r, s \in R$ and $x \in M$ such that $rsx \in P \setminus \phi(P)$. Since N is a Q-subsemimodule of M and $x \in M$, we have $x \in q_1 + N$ where $q_1 \in Q$. So, $rsx \in rs \odot (q_1 + N)$. Let $rs \odot (q_1 + N) = q_2 + N$ where q_2 is the unique element of Q such that $rsq_1 + N \subseteq q_2 + N$. Then $rsx \in q_2 + N$. So there is $y \in N$ such that $q_2 + y = rsx \in P$. Since $y \in N \subseteq P$ and P is subtractive, we obtain $q_2 \in P$. Then $q_2 \in Q \cap P$. Thus, $rs \odot (q_1 + N) = q_2 + N \in P/N_{(Q\cap P)}$. Consider $rsx \notin \phi(P)$ and $y \in N \subseteq \phi(P)$. Since $rsx = q_2 + y$ and $\phi(P)$ is subsemimodule, we have $q_2 \notin \phi(P)$ so that $q_2 + N \notin \phi(P)/N_{(Q\cap\phi(P))} = \phi_N(P/N)$. Now, we have $rs \odot (q_1 + N) = q_2 + N \notin P/N_{(Q\cap P)} \setminus \phi_N(P/N)$. Since $P/N_{(Q\cap P)}$ is a ϕ_N-2-absorbing primary subsemimodule of $M/N_{(Q)}$, we get $r \odot (q_1 + N) \in P/N_{(Q\cap P)}$ or $s \odot (q_1 + N) \in P/N_{(Q\cap P)}$ or $rs \in \sqrt{(P/N_{(Q\cap P)} : M/N_{(Q)})}$. Here three cases arise.

Case I: $r \odot (q_1 + N) \in P/N_{(Q\cap P)}$. Then $r \odot (q_1 + N) = q_2 + N$ where q_2 is the unique element of $Q \cap P$ such that $rq_1 + N \subseteq q_2 + N$. Thus, $rq_1 + N \subseteq q_2 + N \subseteq P$ because $N \subseteq P$ and $q_2 \in Q \cap P$. So, $x \in q_1 + N$ that $rx \in r(q_1 + N) \subseteq rq_1 + N \subseteq q_2 + N \subseteq P$. Thus, $rx \in P$.

Case II: $s \odot (q_1 + N) \in P/N_{(Q\cap P)}$. We can conclude similarly to Case I that $sx \in P$.

Case III: $rs \in \sqrt{(P/N_{(Q\cap P)} : M/N_{(Q)})}$. Then $(rs)^k \odot M/N_{(Q)} \subseteq P/N_{(Q\cap P)}$ for some $k \in \mathbb{N}$. Let $m \in M$. So, there is unique $q_3 \in Q$ such that $m \in q_3 + N$ and $(rs)^k m \in (rs)^k(q_3 + N) \subseteq (rs)^k \odot (q_3 + N) = q_4 + N$ where q_4 is the unique element of Q such that $(rs)^k q_3 + N \subseteq q_4 + N$. Now, $q_4 + N = (rs)^k \odot (q_3 + N) \in P/N_{(Q\cap P)}$. Then $(rs)^k m \in q_4 + N \subseteq P$. So, $(rs)^k M \subseteq P$. Thus, $(rs)^k M \subseteq P$. Therefore, $rs \in \sqrt{(P : M)}$.

Hence, P is a ϕ-2-absorbing primary subsemimodule of M. □

Corollary 3.15. *Let M be an R-semimodule, N a Q-subsemimodule of M, and let P and $\phi(P)$ be subtractive subsemimodules of M with $N \subseteq P$. If $\phi(P) = N$ and P is a ϕ-2-absorbing primary subsemimodule of M, then $P/N_{(Q\cap P)}$ is a weakly 2-absorbing primary subsemimodule of $M/N_{(Q)}$.*

Proof. Since $\phi(P) = N$, we have $\phi_N(P/N) = \phi(P)/N = \{0\}$. By Theorem 3.14, we conclude that $P/N_{(Q\cap P)}$ is a weakly 2-absorbing primary subsemimodule of $M/N_{(Q)}$. □

References

[1] **D.D. Anderson and M. Batanieh**, *Generalizations of prime ideals*, Comm. Algebra, **36** (2008), 686 − 696.

[2] **R.E. Atani, and S.E. Atani**, *On subsemimodules of semimodules*, Bul. Acad. Siinte Repub. Mold. Mat., **63** (2010), no. 2, 20 − 30.

[3] **A. Badawi**, *On 2-absorbing ideals of commutative rings*, Bull. Aust. Math. Soc., **75** (2007), no. 3, 417 − 429.

[4] **J.N. Chaudhari and B.R. Bonde**, *On partitioning and subtractive subsemimodules of semimodules over semirings*, Kyungpook Math. J., **50** (2010), 329 − 336.

[5] **J.N. Chaudhari and B.R. Bonde**, *Weakly prime subsemimodules of semimodules over semirings*, Int. J. Algebra, **5** (2011), no. 4, 167 − 174.

[6] **J.N. Chaudhari**, *2-absorbing ideals in semirings*, Int. J. Algebra, **6** (2012), no. 6, 265 − 270.

[7] **A.Y. Darani, and F. Soheilnia**, *2-absorbing and weakly 2-absorbing submodules*, Thai. J. Math., **9** (2011), no. 3, 577 − 584.

[8] **M.K. Dubey and P. Sarohe**, *On 2-absorbing semimodules*, Quasigroups Related Syst., **21** (2013), 175 − 184.

[9] **M. K. Dubey and P. Sarohe**, *On 2-absorbing primary subsemimodules over commutative semirings*, Bul. Acad. Stiinte Repub. Mold., Mat., **78** (2015), no. 2, 27 – 35.

[10] **J.S. Golan**, *Semirings and their Applications*, Kluwer Academic Publishers, Dordrecht, (1999).

[11] **P. Kumar, M.K. Dubey and P. Sarohe**, *On 2-absorbing ideals in commutative semiring*, Quasigroups Related Syst. **24** (2016), 67 – 74.

[12] **R. Moradi and M. Ebrahimpour**, *On ϕ-2-absorbing primary submodule*, Acta Math. Vietnam, **42** (2017), 27 – 35.

[13] **P. Petchkaew, A. Wasanawichit, and S. Pianskool**, *Generalizations of n-absorbing ideals of commutative semirings*, Thai. J. Math., **14** (2016), no. 2, 477 – 489.

Received August 13, 2023

I. Thongsomnuk
Division of Mathematics, Faculty of Science and Technology, Phetchaburi Rajabhat University, Na Wung, Muang, Phetchaburi 76000, Thailand
E-mail: issaraporn.tho@mail.pbru.ac.th

R. Chinram
Division of Computational Science, Faculty of Science, Prince of Songkla University, Hat Yai, Songkhla, 90110 Thailand
E-mail: ronnason.c@psu.ac.th

P. Singavanada
Program in Mathematics, Faculty of Science and Technology, Songkhla Rajabhat University, Khoa-Roob-Chang, Muang, Songkhla 90000, Thailand
pattarawan.pe@skru.ac.th

P. Chumket
Division of Mathematics, Faculty of Science Technology and Agriculture, Yala Rajabhat University, Tambol Sateng, Mueang, Yala 95000, Thailand
E-mail: patipat.c@yru.ac.th