Quasigroups and Related Systems **30** (2022), 181 – 191

Applications of $\bigcap$-large pseudo N-injective acts in quasi-Frobenius monoid theory and its relationship with some classes of injectivity

Shaymaa Amer Abdul-Kareem and Ahmed A. Abdulkareem

Abstract. The aim of this paper is to review thoroughly the applications of $\bigcap$-large pseudo N-injective acts in quasi-Frobenius monoid theory, and therefore, the relationship of $\bigcap$-large pseudo N-injective acts with some class of injectivity is studied. Applications of the properties of $\bigcap$-large pseudo injective acts in quasi-Frobenius monoid theory are proven. Also, it's proved that the subsequent parity, every union (direct sum) of the two $\bigcap$-large pseudo injective acts is a $\bigcap$-large pseudo injective act if and only if every $\bigcap$-large pseudo injective act is injective under Noetherian condition for a right monoid S. Additionally, we proved that the category of strongly $\bigcap$-large pseudo N-injective right S-acts are going to be egalitarian to the category of projective right S-acts under monoid conditions. The connections between quasi injective and $\bigcap$-large pseudo injective acts are investigated.

1. Introduction

Acts over semigroups appeared and were utilized in a spread of applications like graph theory, combinatorial problems, algebraic automata theory, mathematical linguistics, the theory of machines, and theoretical computing. In a semigroup theory, it represents semigroups as semigroups of functions from a set to itself such it's almost like to Cayley's theorem [10]. This suggests that a semigroup action consists of a semigroup S, a set A, and a mapping of the elements of the semigroup S to functions from the set A to itself. Thereby in any mathematical structure on a set, the collection gathering of structure-preserving maps of the set to itself is an example

2010 Mathematics Subject Classification: 20M30, 20M99, 08B30.
Keywords: $\bigcap$-large pseudo injective acts,$\bigcap$-reversible acts, mutually pseudo injective acts, quasi-Frobenius monoid, Noetherian monoid.

of an abstract algebraic object called a semigroup. On the opposite hand, if you're given an abstractly defined semigroup, when can it's represented as a semigroup of maps of a mathematical structure? One can say that it's represented by actions. As for the monoid, the action is a functor from that category to an arbitrary category. It's well-known that a really natural concept and important tool within the study of monoids is that the idea of getting monoids working on certain (finite) sets. This provides how to show any monoid into a (finite) transformation monoid. Additionally, a monoid action is in contrast to group operations where a monoid action often comes with a natural grading which will be wont to perform certain calculations more efficiently. Due to the importance of the unit, it's rather thought of a semigroup as a "monoid apart from unit," instead of the standard way of a monoid as a "semigroup with unit" [10].

Now, during this paper, S means a monoid with zero elements 0 and each right S-act M is unitary with zero elements Θ which is denoted by M_S. It's possible to seek out the S-act in many names mentioned as S-acts, S-sets, S-operands, S-polygons, transition acts, S-automata [10]. Note that we'll use terminology and notations from [1, 2, 3, 4, 5, 8, 13, 15] freely. For more information about S-act we refer the reader for [9, 10, 12, 17].

A *right S-act* M_S with zero is a non-empty set with a function f from $M \times S$ into M such $(m, s) \mapsto ms$ and therefore, the following conditions hold

(1) $m(st) = (ms)t$ for all $m \in M$ and $s, t \in S$,

(2) $m1 = m$, where 1 is that the identity element of S,

(3) $m.0 = 0$, where 0 is the zero element of S.

A *subact* N of an S-act M_S is a non-empty subset of M such that $xs \in N$ for all $x \in N$ and $s \in S$. A subact N of M_S is called large (or essential) in M_S if and only if any homomorphism $f : M_S \longrightarrow H_S$, where H_S is any S-act with restriction to N is one to at least one, then f is itself one to at least one. During this case, we are saying that M_S is an important extension of N. A non-zero subact N of M_S is *intersection large* if for all non-zero subact A of M_S, $A \bigcap N \neq \Theta$, and will be denoted by N is $\bigcap$-large in M_S [7]. A non-zero S-act M_S over a monoid S is called $\bigcap$-*reversible* if every non-zero subact of M_S is $\bigcap$-large. A monoid S is called $\bigcap$-*reversible* if S_S is $\bigcap$-reversible S-act [19]. An equivalence relation ρ on a right S-act M_S is a congruence relation if and only if aρb implies that $as\rho bs$ for all $a, b \in M_S$ and $s \in S$.

An S-act A_S is called *injective* if for every monomorphism $\alpha : C_S \longrightarrow B_S$ and every S-homomorphism $\beta : C_S \longrightarrow A_S$, there exists an S-homomorphism

$\sigma : \mathrm{B_S} \longrightarrow \mathrm{A_S}$ such $\sigma\alpha = \beta$ [11]. Let $\mathrm{M_S}$, $\mathrm{N_S}$ be S-acts. $\mathrm{N_S}$ is *pseudo M-injective* if for each S-subact A of $\mathrm{M_S}$, each S-monomorphism $f : A \longrightarrow N_{\mathrm{S}}$ is often extended to an S-homomorphism $g : M_{\mathrm{S}} \longrightarrow N_{\mathrm{S}}$. An S-act $\mathrm{N_S}$ is *pseudo injective* if it's pseudo N-injective. An S-act $\mathrm{M_S}$ is $\bigcap$*-large pseudo N-injective* if for any $\bigcap$-large subact X of N, any monomorphism $f : X \longrightarrow M_{\mathrm{S}}$ is often extended to some $g : N \longrightarrow M_{\mathrm{S}}$. $\mathrm{M_S}$ is $\bigcap$*-large pseudo injective* if M is $\bigcap$-large pseudo M–injective.

2. Applications of $\bigcap$-large pseudo injective acts

Let N be a simple subact of an S-act $\mathrm{M_S}$. Then $\mathrm{Soc_N(M_S)}$ is called a *homogeneous component* of $\mathrm{Soc(M_S)}$ containing N. Thus

$$\mathrm{Soc}_N\,(M_S) \;:= \bigcup \big\{X \textit{ be subact of } M_S : X \cong N\big\}.$$

Definition 2.1. Let S be a moniod and A be a class of S-acts, A is called *socle fine* whenever for any $M_{\mathrm{S}}, N_{\mathrm{S}} \in A$, we have $\mathrm{Soc(M_S)} \cong \mathrm{Soc(N_S)}$ if and only if $\mathrm{M_S} \cong \mathrm{N_S}$.

An S-act $\mathrm{M_S}$ is *Noetherian* if every subact of $\mathrm{M_S}$ is finitely generated. A monoid S is a *right Noetherian* if $\mathrm{S_S}$ is Noetherian. Equivalently, S is a right Noetherian if and only if S satisfies the ascending chain condition for right ideals.

An S-act $\mathrm{M_S}$ is *projective* if for every S-epimorphism g from S-act $\mathrm{A_S}$ into S-act $\mathrm{B_S}$ and each homomorphism h from $\mathrm{M_S}$ into $\mathrm{B_S}$, there's a homomorphism f from $\mathrm{M_S}$ into $\mathrm{A_S}$ such that $g \circ h = f$.

Definition 2.2. A monoid S is quasi-Frobenius if and only if S satisfies any of the following equivalent conditions:

1. S is Noetherian on one side and self-injective on one side.
2. S is Artinian on a side and self-injective on a side.
3. All right (or all left) S-acts that are projective are also injective.
4. All right (or all left) S-acts that are injective are also projective.

For example, every semisimple monoid is quasi-Frobenius, since all acts are projective and injective. We denote by SL the category of strongly $\bigcap$-large pseudo N-injective right S-acts, by PR the category of projective right S-acts and E is the injective hull.

Theorem 2.3. *The following conditions are equivalent for a monoid S.*

(1) *S is quasi-Frobenius.*

(2) *The class PR* $\bigcup$ *SL is socle fine.*

Proof. (1)⇒(2). If S is quasi-Frobenius, then projective S-acts are injective. Thus, PR $\bigcup$ SL=SL.

Let $M_S, N_S \in$ SL with $Soc(M_S) \cong Soc(N_S)$.Then $E(Soc(M_S)) \cong E(Soc(N_S))$. Since S is right Artinian, $Soc(M_S)$ is a $\bigcap$-large subact of M_S and $Soc(N_S)$ is a $\bigcap$-large subact of N_S. Hence, $E(M) \cong E(N)$. Then, by Proposition 2.7 in [6], we obtain $M_S \cong N_S$. Thus the class PR $\bigcup$ SL is socle fine.

(2)⇒(1). Let P be a projective right S-act. Then P ∈ PR, E(P) ∈ SL and Soc(P)=Soc(E(P)). By (2), we get P≅ E(P) and hence, P is injective. It follows that S is quasi-Frobenius. □

Theorem 2.4. *The following conditions are equivalent for a monoid S.*

(1) *S is semisimple.*

(2) *The class of all* $\bigcap$*-large pseudo injective acts is socle fine.*

(3) *The class SE is the socle fine.*

Proof. (1)⇒(2) since over every semisimple monoid S in the class of all S-acts is socle fine.

(2)⇒(3). It is clear.

(3)⇒(1). Clearly Soc $(E(S_S))$=$Soc(Soc(S_S))$. Since E (S_S) and $Soc(S_S)$ are $\bigcap$-large pseudo injective, we obtain $E(S_S)=Soc(S_S)$ by (3). It implies that $E(S_S)$ is semisimple and so S is semisimple. □

3. $\bigcap$-large pseudo N-injective and injective acts

Recall that $Soc(M_S)$ represents all $\bigcap$-large subacts of M_S and it's mentioned as $Soc(M_S) := \bigcap\{X \mid X \text{ is } \bigcap\text{−large subact of } M_S\}$. Also, $Soc_N(M_S)$ represents the homogeneous component of $Soc(M_S)$ containing N where N is a simple subact of an S-act M_S. Thus,

$$Soc_N(M_S) := \bigcup\{X \text{ be subact of } M_S : X \cong N\}.$$

Definition 3.1. An S-act M_S is referred to as *strongly* $\bigcap$*-large pseudo injective* if, M_S is $\bigcap$-large pseudo N-injective for all right S-act N_S.

Recall that an ordered groupoid S is called *Artinian* if S satisfies the descending chain condition for ideals.

Lemma 3.2. *Let M_S and N_S be S-acts and M_S be $\bigcap$-reversible. Then, N_S is an injective S-act if and only if N_S is $\bigcap$-large pseudo M-injective for all M_S.*

Proof. By Proposition 2.10(3) in [13], if N_S is $\bigcap$-large pseudo M-injective for all M_S, then every S-monomorphism $f : N_S \to M_S$ is essential since $f(N)$ is $\bigcap$-large in M_S. So, it's split for all S-acts M_S, thus N_S is injective. □

Recall that a proper subact N of an S-act M_S is *maximal* if for every subact K of M_S with $N \subseteq K \subseteq M_S$ implies either K = N or K = M_S.

Definition 3.3. M_S is called a *V-act* (or *cosemisimple*) if every proper subact of M_S is an intersection of maximal subacts. S is called a *V-monoid* if the right act S_S is a V-act.

It is well known that M_S is a V-act if and only if every simple act is M-injective.

Theorem 3.4. *Let S is a right Noetherian monoid. Then*

(1) *Every direct sum of two $\bigcap$-large pseudo injective acts is $\bigcap$-large pseudo injective if and only if every $\bigcap$-large pseudo injective is injective.*

(2) *Essential extensions of semisimple right S-acts are $\bigcap$-large pseudo injective if and only if S is right V-monoid.*

Proof. (1). Assume that the act M_S is $\bigcap$-large pseudo injective(this means that M_S is $\bigcap$-large pseudo M-injective), S is a right Noetherian monoid and E(M) is injective envelope of M_S. Then, since E(M) is injective, so, it's $\bigcap$-large pseudo injective and by assumption (Every direct sum of two $\bigcap$-large pseudo injective acts is $\bigcap$-large pseudo injective) N_S=$M_S\bigoplus$E(M) is $\bigcap$-large pseudo injective. Consider the injection maps j_1:$M_S \longrightarrow$E(M), j_2 : E(M)$\longrightarrow M_S\bigoplus$E(M), $j_3 : M_S \longrightarrow M_S\bigoplus$E(M) and the identity map I_M : $M_S \longrightarrow M_S$. Let π_M: $M_S\bigoplus$E(M)$\longrightarrow M_S$ be the projection map such that $\pi_M \circ j_3 = I_M$. Now $M_S\bigoplus$E(M) is $\bigcap$-large pseudo injective, so this implies there exists an S-homomorphism $g : M_s\bigoplus$E(M) $\longrightarrow M_s\bigoplus$E(M) such that $g \circ j_2 \circ j_1 = j_3 \circ I_M$, then $\pi_M \circ g \circ j_2 \circ j_1 = \pi_M \circ j_3 \circ I_M$.

Thus, $I_M = \pi_M \circ g \circ j_2 \circ j_1$, so that f $= \pi_M \circ g \circ j_2$ and then $I_M = f \circ j_1$. Therefore, M_S is a retract of E(M) and then it is injective. For the converse, let M_S and N_S be two $\bigcap$-large pseudo injective S-act. By hypothesis M_S and N_S are injective which implies that the direct sum of any two injective S-acts is

injective whence S is Noetherian monoid [15] and then every injective act is $\bigcap$-large pseudo injective. Therefore, the direct sum of two $\bigcap$-large pseudo injective is $\bigcap$-large pseudo injective.

(2). Let M_S be a semisimple act. Then $M_S \oplus E(M)$ is an essential extension of a semisimple act. It follows that $M_S \oplus E(M)$ is an $\bigcap$-large pseudo injective act and so by (1) M_S is injective. Thus, S is a right V-monoid and a right Noetherian monoid. The converse is obvious because every semisimple right S-act is injective. □

Proposition 3.5. *Let M_S be an S-act and $\{N_i \mid i \in I\}$ be a family of S-acts. Then $\prod_{i\in I} N_i$ is $\bigcap$-large pseudo M-injective if and only if N_i is $\bigcap$-large pseudo M-injective for every $i \in I$.*

Proof. ($\Rightarrow$). Assume that $N_S = \prod_{i\in I} N_i$ is $\bigcap$-large pseudo M-injective, where M_S is an S-act. Let X be a $\bigcap$-large subact of M_S and f be S-monomorphism from X to N_i. Since N_S is a $\bigcap$-large pseudo M-injective act then there exists an S-homomorphism $g : M_S \longrightarrow N_S$ such that $g \circ i = j_i \circ f$, where i is the inclusion map of X into M_S and j_i is the injection map of N_i into N_S. Define $h : M_S \longrightarrow N_i$ such that $h = \pi_i \circ g$ where π_i is the projection map from N_S onto N_i. Then $h \circ i = \pi_i \circ g \circ i = \pi_i \circ j_i \circ f = f$. That is for all $x \in X$, $h(x) = h(i(x)) = \pi_i(g(x)) = \pi_i(g(i(x))) = \pi_i(j_i(f(x))) = (\pi_i \circ j_i)(f(x)) = f(x)$. Figure 1 illustrates this:

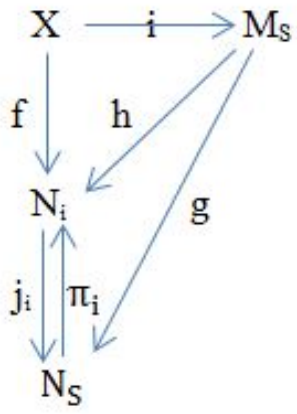


Figure 1: Illustrate that N_S is a $\bigcap$-large pseudo M-injective.

($\Leftarrow$). Assume that N_i is $\bigcap$-large pseudo M-injective for each $i \in I$, where

M_S is an S-act. Let A be a $\bigcap$-large subact of M_S, f be S-monomorphism from A to $N_S = \prod_{i\in I} N_i$. Since N_i is $\bigcap$-large pseudo M-injective, there exists an S-homomorphism $\beta_i : M_S \longrightarrow N_i$, such that $\beta_i \circ i = \pi_i \circ f$. Then, we claim that there exists an S-homomorphism $\beta : M_S \longrightarrow N_S$ such that $\beta_i = \pi_i \circ \beta$. We claim that $\beta \circ i = f$. Since $\beta_i \circ i = \pi_i \circ \beta \circ i$, then $\pi_i \circ f = \pi_i \circ \beta \circ i$, so we obtain $f = \beta \circ i$. Figure 2 explains this:

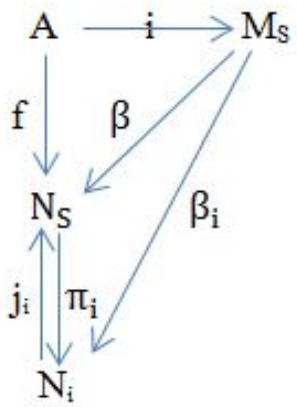


Figure 2: Clarifies that N_i is $\bigcap$-large pseudo M-injective act.

Therefore N_S is $\bigcap$-large pseudo M-injective. □

Corollary 3.6. *Let M_S and N_i be S-acts, where $i \in I$ and I is a finite index set. Then, for every i, N_i is $\bigcap$-large M-pseudo injective if and only if $\bigoplus_{i=1}^{n} N_i$ is $\bigcap$-large M-pseudo injective.*

Proposition 3.7. *Let M_S be a $\bigcap$-large subact of M_s^n. M_S^n is $\bigcap$-large pseudo injective for any finite integer n, if and only if M_S is $\bigcap$-large pseudo M-injective (this means M_S is $\bigcap$-large pseudo injective).*

Proof. Let M_S^n be $\bigcap$-large pseudo injective. Since M_S is a $\bigcap$-large subact of M_S^n, so by Proposition 3.4 in [15], M_S^n is $\bigcap$-large pseudo M-injective. As M_S is retract of M_S^n, for this reason, and by Lemma 3.3 in [15], M_S is $\bigcap$-large pseudo M-injective. Conversely, if M_S is $\bigcap$-large pseudo M-injective, then by Proposition 3.5, M_S^n is $\bigcap$-large pseudo M-injective. □

Every pseudo N-injective act is $\bigcap$-large pseudo N-injective. The subsequent proposition answers the question: When the converse is true?

Proposition 3.8. *For a $\bigcap$-reversible act N_S the following conditions are equivalent:*

(a) *M_S is pseudo N-injective;*

(b) *M_S is $\bigcap$-large pseudo N-injective.*

Proof. $(a) \Rightarrow (b)$. Follows from the definition.

$(b) \Rightarrow (a)$. Let $\mathrm{M_S}$ be $\bigcap$-large pseudo N-injective, A be any subact of $\mathrm{N_S}$. Let $f : A \longrightarrow M_{\mathrm{S}}$ be any monomorphism and $\alpha : \mathrm{A} \longrightarrow \mathrm{N_S}$ be the inclusion map. $\mathrm{N_S}$ being $\bigcap$-reversible implies α is an essential monomorphism. Since $\mathrm{M_S}$ is $\bigcap$-large pseudo N-injective, there exists $h \in Hom(N, M)$ such that $f = h \circ \alpha$. Hence $\mathrm{M_S}$ is pseudo N-injective. □

Each quasi injective act is $\bigcap$-large pseudo injective, but the converse is not true in general. The subsequent theorem gives the condition for the converse to be correct.

An S-act $\mathrm{H_S}$ is called *cog-reversible* if each congruence ρ on $\mathrm{H_S}$ with $\rho \neq I_H$ is large on $\mathrm{H_S}$.

Theorem 3.9. *Let M_S be a cog-reversible nonsingular S-act with $\updownarrow_M(s) = \Theta$ for each $s \in S$ and M_S be $\bigcap$-reversible. Then M_S is $\bigcap$-large pseudo injective if and only if M_S is quasi injective act.*

Proof. Let A be a subact of an S-act $\mathrm{M_S}$ and f be a nonzero S-homomorphism from A into $\mathrm{M_S}$. Since $\mathrm{M_S}$ is $\bigcap$-reversible, so A is $\bigcap$-large subact of $\mathrm{M_S}$. If f is an S-monomorphism, then there is nothing to prove. So assume f is not an S-monomorphism. Since E(M) is injective, then E(M) is an M (respectively E(M))-injective. Thus, there is an S-homomorphism $h : M_{\mathrm{S}} \longrightarrow E(M)$ such that $h \circ \omega_A = \omega_M \circ f$, where ω_A (respectively ω_M) is the inclusion mapping of A (respectively $\mathrm{M_S}$) into $\mathrm{M_S}$ (respectively E(M)). Again there is an S-homomorphism $g : E(M) \longrightarrow E(M)$ such that $g \circ \omega_M = h$. Then either $\ker(h) = I_M$ or $\ker(h) \neq I_M$. If $\ker(h) = I_M$, then h is an S-monomorphism. The Largeness of $\mathrm{M_S}$ in E(M) implies that g is an S-monomorphism, so $g(M_{\mathrm{S}}) \subseteq M_{\mathrm{S}}$ by Theorem 3.6 in [13]. Thus, $h(M_{\mathrm{S}}) \subseteq M_{\mathrm{S}}$ which is extension of f, since $h(A) = h \circ \omega_A(A) = \omega_M \circ f(A) = f(A)$. If $\ker(h) \neq I_M$, then $\ker(h)$ is large on $\mathrm{M_S}$, so $\mathrm{M_S}/\ker(h)$ is singular. But $\mathrm{M_S}/\ker(h) \cong h(M) \subseteq M_{\mathrm{S}}$, so $\mathrm{M_S}/\ker(h)$ is nonsingular. These two cases imply that $\ker(h) = M \times M$. This implies that h (and hence f) is a zero map. □

The subsequent theorem illustrates that M_1 and M_2 are quasi injective acts whence the direct sum is $\bigcap$-large pseudo injective by using some conditions.

Theorem 3.10. *Let M_1 and M_2 be $\bigcap$-reversible S-acts such that M_i is $\bigcap$-large in $M_1 \bigoplus M_2$ for each $i = 1, 2$. If $M_1 \bigoplus M_2$ is $\bigcap$-large pseudo injective, then M_1 and M_2 are quasi injective acts.*

Proof. Let A be a subact of M_1 and $f : A \longrightarrow M_1$ be an S-homomorphism. Then, by assumption M_1 is $\bigcap$-reversible S-act, so A is $\bigcap$-large in M_1 and then in $M_1 \bigoplus M_2$. Define $\alpha : A \longrightarrow M_1 \bigoplus M_2$ by $\alpha(a) = (f(a), a)$, $\forall a \in A$. Then α is an S-monomorphism. By Theorem 3.4, $M_1 \bigoplus M_2$ is $\bigcap$-large M_1-pseudo injective, so there exists an S-homomorphism $\beta : M_1 \longrightarrow M_1 \bigoplus M_2$ such that $\beta \circ i = \alpha$. Now, let j_1 and π_1 be the injection and projection map of M_1 into $M_1 \bigoplus M_2$ and $M_1 \bigoplus M_2$ onto M_1. Then, $\sigma = \pi_1 \beta L)$ $M_1 \longrightarrow M_1$ be an S-homomorphism that extends f, this means $\sigma i = \pi_1 \ \beta i = \pi_1 \ j_1 f \ = I_{M_1} f = f$, which implies $\sigma i = f$. □

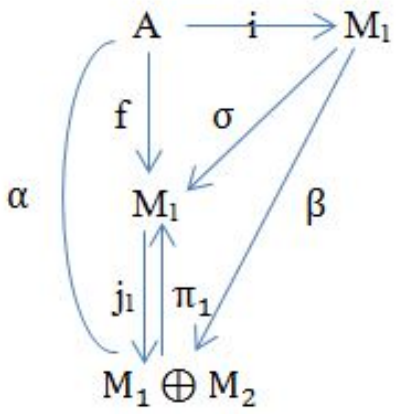


Figure 3: Explains that $M_1 \bigoplus \mathbf{M_2}$ **is $\bigcap$-large $\mathbf{M_1}$-pseudo injective act.**

Proposition 3.11. (cf. [6]) *Let M_S be an S-act and $\{N_i \mid i \in I\}$ be a family of S-acts. Then $\prod_{i \in I} N_i$ is M-injective if and only if N_i is M-injective for all $i \in I$.*

Corollary 3.12. *For any integer $n \geqslant 2$, let M_S be $\bigcap$-reversible and a cog-reversible nonsingular S-act with $\updownarrow_M(s) = \Theta$ for each $s \in S$. Then M_S^n is $\bigcap$-large pseudo M-injective if and only if M_S is quasi injective.*

Proof. If M_S^n is $\bigcap$-large pseudo injective, then by Theorem 3.4 M_S^n is $\bigcap$-large pseudo M-injective. Then, by Lemma 2.3 in [13], $\mathrm{M_S}$ is $\bigcap$-large pseudo M-injective. Since $\mathrm{M_S}$ is a cog-reversible nonsingular S-act, so by Theorem 3.10, $\mathrm{M_S}$ is quasi injective act. Conversely, if $\mathrm{M_S}$ is quasi injective act, then by Proposition 3.11, M_S^n is quasi injective and in particular, is $\bigcap$-large pseudo M-injective. □

Proposition 3.13. *Let M_S=$\bigoplus_{i\in I} M_i$ be a direct sum of a cog-reversible non-singular with $\updownarrow_M(s) = \Theta$ for each $s \in S$ and $\bigcap$-reversible S-acts M_i. An S-act M_S is quasi injective if and only if it is $\bigcap$-large pseudo injective.*

Proof. Let $\mathrm{M_S}$ be a $\bigcap$-large pseudo injective S-act. This means that $\mathrm{M_S}$ is $\bigcap$-large pseudo M-injective, so by Proposition 2.4 in [13], $\mathrm{M_j}$ is $\bigcap$-large pseudo M-injective, Now, each $\mathrm{M_j}$ is $\bigcap$-large pseudo M-injective act, so by Theorem 3.9, each $\mathrm{M_j}$ is quasi injective. Therefore, by Proposition 3.11 $\mathrm{M_S}$ is quasi injective. The rest is obvious. □

Acknowledgement. The authors thank the editor and anonymous reviewers for their useful comments and suggestions. Also, the first author would like to thank Mustansiriyah University Baghdad-Iraq for its support in the present work.

References

[1] **M.S. Abbas and A.Shaymaa**, *Pseudo injective and pseudo QP-injective S-acts over monoids*, Intern. J. Pure Engin. Math., **3** (2015), no.2, 33 − 49.

[2] **M.S. Abbas and A.Shaymaa**, *Pseudo PQ-injective acts over monoids,* J. Progressive Research Math., **4** (2015), no.2, 321 − 327.

[3] **S.A. Abdul-Kareem**, *Dual of extending acts*, Iraqi J. Sci., Special Issue, (2020), 64 − 71.

[4] **S.A. Abdul-Kareem**, *Minimal quasi injective S-acts*, Intern. J. Math. Computer Sci., **15** (2020), 515 − 524.

[5] **J. Ahsan**, *Monoids characterized by their quasi injective S-acts*, Semigroup froum, **36** (1987), 285 − 292.

[6] **J. Ahsan and L. Zhongkui**, *On relative quasi-projective acts over monoids*, Arabian J. Sci. Engin., **35** (2010), 225 − 233.

[7] **P. Berthiaume**, *The injective envelope of S-sets*, Canad. Math. Bull., **10** (1967), 261 − 272.

[8] **C.V. Hinkle**, *The extended centralizer of an S-set*, Pacific J. Math., **53** (1974), 163 – 170.

[9] **K. Jupil**, *PI-S-acts*, J. Chungcheong Math. Soc., **21** (2008), 591 – 599.

[10] **M. Kilp and et al.**, *Monoids sets and categories with applications to wreath products and graphs*, Walter de Gruyter, Berlin, 2000.

[11] **N. Kehayopulu and M. Tsingelis**, *Noetherian and Artinian ordered semigroups*, Intern. J. Math. and Math. Sci., **13** (2005), 2041 – 2051.

[12] **A.M. Lopez, Jr. and J.K. Luedeman**, *Quasi-injective S-acts and their S-endomorphism semigroup*, Czechoslovak Math .J., **29** (1979), 97 – 104.

[13] **A.Shaymaa and A.A. Abdulkareem**, $\bigcap$-*large pseudo injective acts*, J. Discr. Math. Sci. Cryptography, **25** (2022), 511 – 522.

[14] **A. Shaymaa**, *About the generalizations in acts over monoids*, (Handbook), LAP LAMBERT Academic Publishing, Germany, 2018.

[15] **A. Shaymaa**, *On finitely generated in S-acts over monoids*, (Handbook), Noor Publishing, Germany, 2018.

[16] **A.V. Skorokhodov**, *Generalization of the reachability problem on directed graphs*, Math. Statistics, **8** (2020), 699 – 704.

[17] **T. Yan**, *Generalized injective S-acts on a monoid*, Adva. Math., **40** (2011), 421 – 432.

Received November 12, 2021

S.A. Abdul Kareem
Department of Mathematics, College of Basic Education, Mustansiriyah University, Baghdad, Iraq
E-mail: Shaymma_amer.edbs@uomustansiriyah.edu.iq

A.A.Abdulkareem
Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq
E-mail: ahmed.amer.abdulkareem@gmail.com

Quasigroups and Related Systems **30** (2022), 193 – 208

Translatable isotopes of translatable quasigroups

Wieslaw A. Dudek and Robert A. R. Monzo

Abstract. We determine the structure of translatable isotopes of translatable quasigroups. Necessary and sufficient conditions are found for a bijection between two such isotopes to be an isomorphism. It is also proved that in a left cancellative, k-translatable magma, the value of k is unique.

1. Introduction

This paper is motivated by the following question: *What is the structure of translatable isotopes of a left cancellative translatable magma?* In Theorem 3.1 below we start with a quasigroup that is k-translatable with respect to the natural order. The elements of a quasigroup $(Q, \cdot)$ that is translatable with respect to a particular ordering of Q can be re-labelled so that $(Q, \cdot)$ is translatable with respect to the natural ordering, so that starting with the natural ordering is no limitation. We then determine all bijections α and β on Q such that $(Q, *)$, defined by $l' * m' = \alpha l' \cdot \beta m'$, is h-translatable with respect to the ordering $1', 2', 3', \ldots, n'$ of Q. This ordering is arbitrary, except for the fact that $1' = 1$, the first element of the natural ordering. Using perhaps repeated applications of Lemma 2.6 below, such an ordering is always possible.

That is, we have determined the form of all h-translatable isotopes of any k-translatable quasigroup. As a Corollary, it follows that a k-translatable quasigroup of order n has h-translatable isotopes of every value relatively prime to n. In addition, such translatable isotopes exist for every possible ordering of Q.

We also give a correct proof of the fact that a left cancellative k-translatable magma is translatable for a unique value of k and explain why the proof of this given in [4], Theorem 3.3, is not valid.

2010 Mathematics Subject Classification: 20N02
Keywords: Magma, quasigroups, translatable quasigroups, isotopes.

2. Preliminary results, definitions and notation

.

All magmas (groupoids) considered here are of finite order n. That is, $Q = \{1, 2, \ldots, n\}$ and $1, 2, 3, \ldots, n$ is the natural ordering. We denote $\{1, 2, \ldots, n\}$ by $\overline{\{1, n\}}$. The value of t modulo n is denoted by $[t]_n$. If $i \equiv j (\mathrm{mod}\, n)$ we write $[i]_n = [j]_n$. Recall that $t \in \overline{\{1, n\}}$ is relatively prime to n if and only if there exists $\tilde{t} \in \overline{\{1, n\}}$ such that $[\tilde{t}t]_n = 1$, if and only if $[tx]_n = [ty]_n$ implies $x = y$ for all $x, y \in \overline{\{1, n\}}$. We denote this by $(t, n) = 1$.

Definition 2.1. (cf. [2]) A finite magma is called *k-translatable* (for fixed k, $1 \leqslant k < n$) if its Cayley table is obtained by the following rule: If the first row of the table is $a_1, a_2, \ldots, a_n$ then the q^{th} row is obtained from the $(q-1)^{th}$ row by taking the last k entries in the $(q-1)^{th}$ row and inserting them as the first k entries of the q^{th} row and by taking the first $(n-k)$ entries from the $(q-1)^{th}$ row and inserting them as the last $(n-k)$ entries of the q^{th} row, where $q \in \{2, 3, \ldots, n\}$. Then, the (ordered) sequence $a_1, a_2, \ldots, a_n$ is called a *k-translatable sequence of Q* with respect to the natural ordering $1, 2, 3, \ldots, n$. A magma is called *translatable* if it has a k-translatable sequence for some $k \in \{1, 2, \ldots, n-1\}$.

Example 2.2. Consider the following magma represented by three Cayley tables with different orderings.

	1	2	3	4	5
1	2	5	3	4	1
2	3	4	1	2	5
3	1	2	5	3	4
4	5	3	4	1	2
5	4	1	2	5	3

	4	2	3	1	5
4	1	3	4	5	2
2	2	4	1	3	5
3	3	2	5	1	4
1	4	5	3	2	1
5	5	1	2	4	3

	4	2	5	3	1
4	1	3	2	4	5
2	2	4	5	1	3
5	5	1	3	2	4
3	3	2	4	5	1
1	4	5	1	3	2

Notice that $(Q, \cdot)$ is 3-translatable with respect to the natural ordering and with respect to the ordering $4, 2, 5, 3, 1$. But it is not translatable with respect to the ordering $4, 2, 3, 1, 5$.

Example 2.3. *The magma $(Q, \cdot)$, where $Q = \{1, 2, 3, 4\}$ and $x \cdot y = 1$, is k-translatable for every $k \in \{1, 2, 3, 4\}$. Its k-translatable sequence has the form* $1, 1, 1, 1$.

The following lemmas are stated without proof, as the proofs are elsewhere, as referenced.

Lemma 2.4. (cf. [2, Lemma 2.5]) *Let $a_1, a_2, \ldots, a_n$ be the first row of the Cayley table of the magma $(Q, \cdot)$ of order n. Then $(Q, \cdot)$ is k-translatable with respect to the natural ordering if and only if for all $i, j \in \overline{\{1, n\}}$ one of the following (equivalent) conditions is satisfied:*

(*i*) $i \cdot j = a_{[k-ki+j]_n}$,

(*ii*) $i \cdot j = [i+1]_n \cdot [j+k]_n$,

(*iii*) $i \cdot [j-k]_n = [i+1]_n \cdot j$.

Lemma 2.5. *Suppose that $Q = \{1', 2', \ldots, n'\}$ is a set of order n. In the magma $(Q, \cdot)$, let $a_i = 1' \cdot i'$ for all $i \in \overline{\{1, n\}}$. Then $(Q, \cdot)$ is k-translatable with respect to the ordering $1', 2', \ldots, n'$ if and only if for all $i, j \in \overline{\{1, n\}}$ one of the following (equivalent) conditions is satisfied:*

(*i*) $i' \cdot j' = a_{[k-ki+j]_n}$,

(*ii*) $i' \cdot j' = [i+1]'_n \cdot [j+k]'_n$,

(*iii*) $i' \cdot [j-k]'_n = [i+1]'_n \cdot j'$.

Note that in Lemma 2.5, $i' \cdot j' \neq a_{[k-ki'+j']_n}$. This is because $[k-ki+j]_n$ marks the position of the entry $a_{[k-ki+j]_n}$. For example, in the third Cayley table in Example 2.2, $(Q, \cdot)$ is 3-translatable with respect to the ordering $1', 2', 3', 4', 5'$ where $1' = 4$, $2' = 2$, $3' = 5$, $4' = 3$ and $5' = 1$. Then, $1' \cdot 2' = 4 \cdot 2 = 3 = 4' \neq 2 = a_3 = a_{[-2]_5} = a_{[3-(3\cdot 4)+2]_5} = a_{[3-3(1')+2']_5}$ while $1' \cdot 2' = 3 = a_2 = a_{[3-3(1)+2]_5}$.

Lemmas 2.4 and 2.5 above will be applied throughout the rest of the paper, at times without reference. Lemma 2.5 accounts, in part, for the error in the proof of the fact that the value of the translatability of a left cancellative translatable magma is unique, in [4], Theorem 3.3. An error in the proof there is that $a_{j''} = 1 \cdot j'' = 1'' \cdot j'' = c_j \neq c_{j''}$, because as we have just seen, j'' is not necessarily equal to j for all $j \in \overline{\{1, n\}}$, except in the natural ordering.

We now list some previously proved results that, along with the proof of the converse of Lemma 2.7 from [2] will be used as lemmas to give a valid proof that the value of translatability of left cancellative magmas is unique.

Lemma 2.6. (cf. [2, Lemma 2.7]) *Let $(Q, \cdot)$ be a k-translatable magma with respect to the natural ordering $1, 2, \ldots, n$, with k-translatable sequence*

$a_1, a_2, \ldots, a_n$. *Then* $(Q, \cdot)$ *is* k*-translatable with respect to the ordering* $n, 1, 2, \ldots, n-2, n-1$*, with* k*-translatable sequence*

$$a_k, a_{k+1}, \ldots, a_{n-1}, a_n, a_1, a_2, \ldots, a_{k-1}.a_{k-1}.$$

Lemma 2.7. (cf. [4, Lemma 2.6]) *Let* $(Q, \cdot)$ *be a naturally ordered* k*-translatable magma of order* n *with* k*-translatable sequence* $a_1, a_2, \ldots, a_n$ *and suppose that* $(t, n) = 1$*. Then* $(Q, \cdot)$ *is* k*-translatable with respect to the ordering*

$$1, [1+t]_n, [1+2t]_n, [1+3t]_n, \ldots, [1-2t]_n, [1-t]_n$$

with k*-translatable sequence*

$$a_1, a_{[1+t]_n}, a_{[1+2t]_n}, \ldots, a_{[1-2t]_n}, a_{[1-t]_n}.$$

The following result, the converse of Lemma 2.7, is new.

Lemma 2.8. *A magma* $(Q, \cdot)$ *of order* n *is a* k*-translatable with respect to the natural ordering if and only if it is* k*-translatable with respect to the ordering* $1, [1+t]_n, [1+2t]_n, \ldots, [1-2t]_n, [1-t]_n$ *for any* t *relatively prime to* n*.*

Proof. ($\Rightarrow$). This is Lemma 2.7.

($\Leftarrow$). Let the magma $(Q, \cdot)$ be k-translatable with respect to the ordering $1', 2', 3', \ldots, n'$, where $i' = [1 + (i-1)t]_n$ for all $i \in \overline{\{1, n\}}$ and where $(t, n) = 1$.

Define $t_q = [(q-1)\tilde{t}\,]_n$ for any $q \in \overline{\{1, n\}}$. Note that $[1 + t_q t\,]_n = q = [t_q + 1]'_n$. Then, for all $i, j \in \overline{\{1, n\}}$, by Lemma 2.5($iii$)

$$\begin{aligned}
[i+1]_n \cdot [j+k]_n &= [1 + (t_i + \tilde{t}\,)t]_n \cdot [1 + (t_j + \tilde{t} + t_k)t]_n \\
&= [t_i + \tilde{t} + 1]'_n \cdot [t_j + \tilde{t} + t_k + 1]'_n \\
&= [t_i + 1]'_n \cdot [t_j + \tilde{t} + t_k + 1 - \tilde{t}k]'_n \\
&= i \cdot [1 + (t_j + \tilde{t} + t_k - \tilde{t}k)t]_n = i \cdot j.
\end{aligned}$$

So, by Lemma 2.4(ii), $(Q, \cdot)$ is k-translatable with respect to the natural ordering. □

From Lemma 2.5 (i) it follows that if a k-translatable magma $(Q, \cdot)$ of order n is left cancellative, then all elements of its k-translatable sequence (consequently, elements in each row of its Cayley table) are different because $\varphi_i(x) = i \cdot x$ is a bijection. But, in general, such a magma is not a quasigroup. It is a quasigroup if and only if $(k, n) = 1$. A quasigroup of order n can be k-translatable only for $(k, n) = 1$ [2, Lemma 2.15].

Corollary 2.9. *If $(Q,\cdot)$ is a k-translatable quasigroup, then $(k,n)=1$.*

Theorem 2.10. *A left cancellative magma $(Q,\cdot)$ can be k-translatable only for one value of k.*

Proof. Suppose that $(Q,\cdot)$ is k-translatable of order n. Then, by a renumeration of the elements of Q, we can consider $(Q,\cdot)$ as k-translatable with respect to the natural ordering. Suppose that $(Q,\cdot)$ is h-translatable with respect to some ordering. Then using Lemma 2.6, perhaps repeatedly, $(Q,\cdot)$ is h-translatable with respect to some ordering $1',2',\dots,n'$, where $1'=1$. Suppose that $(Q,\cdot)$ has the k-translatable sequence $a_1,a_2,\dots,a_n$ with respect to the natural ordering and that $(Q,\cdot)$ has the h-translatable sequence $c_1,c_2,\dots,c_n$ with respect to the ordering $1,2',3',\dots,n'$. Then, for any $i\in Q$, by Lemma 2.4 (i) and Lemma 2.5 (i),

$$a_{i'}=1\cdot i'=1'\cdot i'=c_i. \tag{1}$$

For $i\in Q$, define $s_i=i'$. Then, $s_1=1'=1$ and for any $i,j\in Q$, by the definition of h-translatability $i'\cdot j'=s_i\cdot s_j=a'_{[k-ks_i+s_j]_n}=c_{[h-hi+j]_n}\overset{(1)}{=}a'_{[h-hi+j]_n}$, and, since $(Q,\cdot)$ is left cancellative, we have

$$[k-ks_i+s_j]_n=[h-hi+j]'_n. \tag{2}$$

Then, for any $i\in Q$, $[h+i]'_n=[h-h\tilde{h}+i+1]'_n\overset{(2)}{=}[k-ks_{\tilde{h}}+s_{i+1}]_n=[h-hn+i]'_n\overset{(2)}{=}[k-ks_n+s_i]_n$. So, for all $i\in\overline{\{1,n\}}$,

$$[s_{[i+1]_n}-s_i]_n=[k(s_{\tilde{h}}-s_n)]_n. \tag{3}$$

It is then straightforward to prove by induction on i that

$$s_i=[1+(i-1)k(s_{\tilde{h}}-s_n)]_n. \tag{4}$$

Since $\{s_1,s_2,\dots,s_n\}=\{1',2',\dots,n'\}=\{1,2,\dots,n\}$, $(k(s_{\tilde{h}}-s_n),n)=1$ and the ordering $1',2',\dots,n'$ is of the form in our Lemma 2.8, with $t=[k(s_{\tilde{h}}-s_n)]_n$. Therefore, by Lemma 2.8, $(Q,\cdot)$ is both h and k-translatable with respect to the natural ordering. Applying Lemma 2.3 from [2] we obtain $h=k$. □

3. Translatable isotopes of a translatable magma

A magma $(Q,*)$ is an *isotope* of the magma $(Q,\cdot)$ if there are bijections α,β and γ of Q such that $\gamma(i*j)=\alpha i\cdot\beta j$. If γ is the identity map, then $(Q,*)$ is called a *principal isotope* of $(Q,\cdot)$. One can prove (see for example [1]) that every isotope of the magma $(Q,\cdot)$ is isomorphic to a principal isotope of this magma. Therefore, although our results on isotopes of translatable magma are actually results on the principal isotopes of a translatable magma, up to isomorphism they are results on all isotopes.

Theorem 3.1. *Suppose that a quasigroup $(Q,\cdot)$ of order n is k-translatable with respect to the natural ordering of Q. Then $(Q,*)$ is an isotope of $(Q,\cdot)$ and is h-translatable with respect to the ordering $1,2',3',\dots,n'$ if and only if there exist bijections α and β of Q and $c,d\in\overline{\{1,n\}}$ such that $\alpha c'=n=\beta d'$ and*

(i) $l'*m'=\alpha l'\cdot\beta m'$ *for all* $l,m\in\overline{\{1,n\}}$,

(ii) $\alpha([c+i]'_n)=i\alpha([c+1]'_n)$ *for all* $i\in\overline{\{1,n\}}$,

(iii) $\beta([d+ih]'_n)=ki\alpha([c+1]'_n)$ *for all* $i\in\overline{\{1,n\}}$, *and*

(iv) $(\alpha([c+1]'_n),n)=1$.

Proof. ($\Rightarrow$). Let $a_1,a_2,\dots,a_n$ be the k-translatable sequence of a quasigroup $(Q,\cdot)$. Then since $(Q,\cdot)$ is left cancellative,

$$a_l=a_m \text{ if and only if } l=m. \tag{5}$$

Also, by Lemma 2.4 (i), $l\cdot m=a_{[k-kl+m]_n}$ for all $l,m\in\overline{\{1,n\}}$. Since $(Q,*)$ is an isotope of $(Q,\cdot)$, by definition there exist bijections α and β of Q such that (i) is valid. Hence, $l'*m'=\alpha l'\cdot\beta m'=a_{[k-k(\alpha l')+\beta m']_n}$ for all $l,m\in\overline{\{1,n\}}$.

Since α and β are bijections of Q there exist $c,d\in\overline{\{1,n\}}$ such that $\alpha c'=n=\beta d'$. Thus, for all $i\in\overline{\{1,n\}}$, using h-translatability of $(Q,*)$, by Lemma 2.5(ii) we obtain

$$a_k=n\cdot n=\alpha c'\cdot\beta d'=c'*d'=[c+i]'_n*[d+ih]'_n=\alpha([c+i]'_n)\cdot\beta([d+ih]'_n)$$
$$=a_{[k-k\alpha([c+i]'_n)+\beta([d+ih]'_n)]_n}$$

and so by (5),

$$k\alpha([c+i]'_n)=\beta([d+ih]'_n) \tag{6}$$

for all $i \in \overline{\{1,n\}}$.

Also,

$$[c+1]'_n * d' = \alpha([c+1]'_n) \cdot \beta d' = a_{[k-k\alpha([c+1]'_n)]_n} = [c+1+i]'_n * [d+ih]'_n \\ = a_{[k-k\alpha([c+1+i]'_n)+\beta([d+ih]'_n)}$$

and so by (5),

$$k\alpha([c+1+i]'_n) - k\alpha([c+1]'_n) = \beta([d+ih]'_n) \overset{(6)}{=} k\alpha([c+i]'_n). \qquad (7)$$

By induction on i we now prove (ii), that $\alpha([c+i]'_n) = i\alpha([c+1]'_n)$ for all $i \in \overline{\{1,n\}}$. Clearly, the statement is true for $i = 1$. If the statement is true for all $t \leqslant i-1$ then $\alpha([c+i-1]'_n) = (i-1)\alpha([c+1]'_n)$. Then by (7) for $i-1$ we have that

$$k\alpha([c+i]'_n) - k\alpha([c+1]'_n) = k\alpha([c+i-1]'_n)$$

and so $k\alpha([c+i]'_n) = ki\alpha([c+1]'_n)$. Since $(k,n) = 1$,

$$\alpha([c+i]'_n) = i\alpha([c+1]'_n) \qquad (8)$$

for all $i \in \overline{\{1,n\}}$.

Now (iii) follows from (6) and (8), and (iv) follows from (8), the fact that α is a bijection of Q and the fact that $Q = \{1, 2', 3', \ldots, n'\}$.

($\Leftarrow$). Clearly, $(Q,*)$ is an isotope of $(Q,\cdot)$. We need only prove therefore that $(Q,*)$ is h-translatable with respect to the ordering $1, 2', 3', \ldots, n'$.

For any $l, m \in \overline{\{1,n\}}$, $l = [c+i_l]_n$ and $m = [d+i_m h]_n$ for some $i_l, i_m \in \overline{\{1,n\}}$. Then, $[l+1]'_n * [m+h]'_n = \alpha([c+i_l+1]'_n) \cdot \beta([d+(i_m+1)h]'_n) = a_w$, where,

$$\begin{aligned} w &= [k - k\alpha([c+i_l+1]'_n) + \beta([d+(i_m+1)h]'_n]_n \\ &= [k - k(i_l+1)\alpha([c+1]'_n) + k(i_m+1)\alpha([c+1]'_n)]_n && \text{by } (ii),\ (iii) \\ &= [k - ki_l\alpha([c+1]'_n) + ki_m\alpha([c+1]'_n)]_n \\ &= [k - ki_l\alpha([c+1]'_n) + \beta([d+i_m h]'_n)]_n) && \text{by } (iii) \\ &= [k - k\alpha l' + \beta m']_n. && \text{by } (ii) \end{aligned}$$

So,

$$[l+1]'_n * [m+h]'_n = a_w = a_{[k-k\alpha l'+\beta m']_n} = \alpha l' \cdot \beta m' = l' * m'$$

and, by Lemma 2.5 (ii), $(Q,*)$ is h-translatable with respect to the ordering $1, 2', 3', \ldots, n'$. □

Corollary 3.2. *A k-translatable quasigroup of order n has h-translatable isotopes for all values of h relatively prime to n. It has such isotopes for every ordering.*

Corollary 3.3. *$(\mathbb{Z}_n, *)$ is an h-translatable isotope of $(\mathbb{Z}_n, +)$ with respect to the ordering $1, 2', 3', \ldots, n'$ if and only if there exist bijections α and β of $\mathbb{Z}_n$ and $c, d \in \mathbb{Z}_n$ such that $\alpha c' = 0 = \beta d'$, $\alpha([c+i]'_n) = i\alpha([c+1]'_n) = -\beta([d+ih]'_n)$ for all $i \in \overline{\{1,n\}}$, $(\alpha([c+1]'_n), n) = 1 = (h, n)$ and $l' * m' = \alpha l' \cdot \beta m'$ for all $l, m \in \mathbb{Z}_n$.*

Corollary 3.4. *Suppose that $(Q, \cdot)$ is a k-translatable quasigroup with respect to the natural ordering, with k-translatable sequence $a_1, a_2, \ldots, a_n$. Suppose also that $(Q, *)$ is an h-translatable quasigroup with respect to the ordering $1, 2', 3', \ldots, n'$. Then $(Q, *)$ is an h-translatable isotope of $(Q, \cdot)$ if and only if there exist $c, d, t \in \overline{\{1,n\}}$ with $(t, n) = 1$ and for all $q \in \overline{\{1,n\}}$, $1 * q' = a_{x_q}$, where $x_q = [r+(q-1)\tilde{h}kt]_n$ and $r = [k+kct-kt+(1-d)\tilde{h}kt]_n$. Also, $(Q, *)$ is an h-translatable idempotent isotope of $(Q, \cdot)$ if and only if there exist $c, d, t \in \overline{\{1,n\}}$ with $(t, n) = 1$ such that $q = a_{[k-kct+(q-d)\tilde{h}kt-ktq]_n}$ for all $q \in \overline{\{1,n\}}$.*

Proof. ($\Rightarrow$). By Theorem 3.1, there exist bijections α and β of Q and $c, d \in \overline{\{1,n\}}$ such that $\alpha c' = n = \beta d'$ and (i), (ii), (iii) and (iv) of Theorem 3.1 are valid. Let $t = \alpha([c+1]'_n)$.

For any $m \in \overline{\{1,n\}}$ there exists $i_m \in \overline{\{1,n\}}$ such that $m = [d + i_m h]_n$ and $[m+1]_n = [d + (i_m + \tilde{h})h]_n$. Therefore,

$$\beta([m+1]'_n) \overset{(iii)}{=} [k(i_m + \tilde{h})t]_n = [ki_m t]_n + [k\tilde{h}t]_n = \beta m' + [k\tilde{h}t]_n.$$

By Theorem 3.1 again, for all $l, m \in \overline{\{1,n\}}$, we have $l' * m' = \alpha l' \cdot \beta m' = a_{[k-k(\alpha l')+\beta m']_n}$. Therefore, for any $q \in \overline{\{1,n\}}$, $1 * q' = 1' * q' = \alpha 1 \cdot \beta q' = a_{x_q}$, where

$$x_q = [k - k\alpha 1 + \beta q']_n = [k - k\alpha 1 + \beta 1 + (q-1)\tilde{h}kt]_n = [r + (q-1)\tilde{h}kt]_n$$

for $r = [k - k\alpha 1 + \beta 1]_n$, whence, applying (ii) and (iii), we obtain

$$r = [k - k(1-c)t + (1-d)\tilde{h}kt]_n = [k + kct - kt + (1-d)\tilde{h}kt]_n.$$

($\Leftarrow$). For all $i \in \overline{\{1,n\}}$ we define $\alpha([c+i]'_n) = [it]_n$ and $\beta([d+i]'_n) = [i\tilde{h}kt]_n$. Then α and β are bijections of Q. For any $q \in \overline{\{1,n\}}$, define $b_q = a_w$, where $w = [r + (q-1)\tilde{h}kt]_n$. That is, $b_1, b_2, \ldots, b_n$ is the h-translatable sequence of $(Q, *)$ with respect to the ordering $1, 2', 3', \ldots, n'$.

By Lemma 2.5 (i), for all $l, m \in \overline{\{1,n\}}$, $l' * m' = b_{[h-hl+m]_n} = a_x$, where $x = [r + (h - hl + m - 1)\tilde{h}kt]_n$. Since $r = [k + kct - kt + (1 - d)\tilde{h}kt]_n$, $x = [k + kct - ktl - d\tilde{h}kt + m\tilde{h}kt]_n$ and $l' * m' = b_{[h-hi+m]_n} = a_x$. Then, since for any $m \in \overline{\{1,n\}}$, $\beta m' = \beta([d + (m - d)]'_n) = [(m - d)\tilde{h}kt]_n$ we have $\alpha l' \cdot \beta m' = a_y$, where $y = [k - k\alpha l' + \beta m']_n = [k - k(l - c)t + (m - d)\tilde{h}kt]_n = x$. Hence, $l' * m' = a_x = a_y = \alpha l' \cdot \beta m'$ and $(Q, *)$ is an h-translatable isotope of $(Q, \cdot)$.

The last sentence in the statement of Corollary 3.4 follows from the fact that $(Q, *)$ is idempotent if and only if $q = q * q = a_{x_{[h-hq+q]_n}}$. □

Example 3.5. The set $Q_8 = \{1, 2, 3, 4, 5, 6, 7, 8\}$ with the operation defined by table

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

is a 5-translatable quasigroup. We can re-label the elements of Q_8 as follows: 4 becomes 1, 8 becomes 2, 1 becomes 3, 3 becomes 4, 2 becomes 5, 5 becomes 6, 7 stays as 7 and 6 becomes 8. Then, with this new labelling, $(Q_8, \cdot)$ is 5-translatable with respect to the natural ordering, as follows.

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

Its translatable sequence has the form $8, 6, 3, 2, 5, 1, 4, 7$.

Using Corollary 3.4, we now construct an isotope $(Q_8, *)$ of $(Q_8, \cdot)$ that is 3-translatable with respect to the ordering $1, 2', 3', \ldots, n'$.

We have $k = 5$ and $h = 3 = \tilde{h}$. We choose $c = 4$ and $d = 7 = t = \alpha([4+1]'_8)$. Then we calculate that $r = [k + kct - kt + (1-d)\tilde{h}kt]_8 = 8$. Then, as in the proof of Corollary 3.4 ($\Leftarrow$), for all $l, m \in \overline{\{1,8\}}$ is $l' * m' = b_{[3-3l+m]_8} = a_{[8+(3-3l+m-1)(105)]_8} = a_{[3-3l+m-1]_8}$. This gives the following 3-translatable sequence for $(Q_8, *)$, with respect to the ordering $1, 2', 3', \ldots, 8'$: $a_8, a_7, a_6, a_5, a_4, a_3,\ a_2, a_1$ or $7, 8, 6, 3, 2, 5, 1, 4$. This gives the following Cayley table for the 3-translatable isotope $(Q_8, *)$ of $(Q_8, \cdot)$.

$*$	1	$2'$	$3'$	$4'$	$5'$	$6'$	$7'$	$8'$
1	7	8	6	3	2	5	1	4
$2'$	5	1	4	7	8	6	3	2
$3'$	6	3	2	5	1	4	7	8
$4'$	4	7	8	6	3	2	5	1
$5'$	2	5	1	4	7	8	6	3
$6'$	8	6	3	2	5	1	4	7
$7'$	1	4	7	8	6	3	2	5
$8'$	3	2	5	1	4	7	8	6

According to Theorem 3.1, the mappings α and β that satisfy $l' * m' = \alpha l' \cdot \beta m'$, for all $l, m \in \overline{\{1,8\}}$, are: $\alpha 1' = \alpha 1 = 3$, $\alpha 2' = 2$, $\alpha 3' = 1$, $\alpha 4' = 8$, $\alpha 5' = 7$, $\alpha 6' = 6$, $\alpha 7' = 5$, $\alpha 8' = 4$, and $\beta 1' = 2$, $\beta 2' = 3$, $\beta 3' = 4$, $\beta 4' = 5$, $\beta 5' = 6$, $\beta 6' = 7$, $\beta 7' = n$, $\beta 8' = 1$.

Using Lemma 2.6 we can see that 3-translatable isotopes of $(Q_8, \cdot)$ exist for every ordering of Q_8.

Example 3.6. Consider again the 5-translatable quasigroup of Example 3.5, with the following Cayley table:

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

Consider also a quasigroup $(Q_8, \star)$ with ordering $5, 3, 8, 1, 7, 2, 6, 4$ and Cayley table as follows:

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

Is the quasigroup $(Q_8, \star)$ a translatable isotope of $(Q_8, \cdot)$? If it is translatable then it must be 7-translatable, as all other possible values of translatability, $1, 3$ and 5, do not yield commutative quasigroups.

By (perhaps repeated) application of Lemma 2.6, if $(Q_8, \star)$ is 7-translatable then it is 7-translatable with respect to an ordering $1, 2', 3', 4', 5', 6', 7', 8'$, with 7-translatable sequence $2, b_2, b_3, b_4, b_5, b_6, b_7, b_8$ with $\{b_3, b_5, b_7\} = \{6, 7, 8\}$.

Assuming that $2' = 6$ and using Lemma 2.4 (ii) and (iii), we can calculate that $3' = 3$, $4' = 5$, $5' = 2$, $6' = 4$, $7' = 7$ and $8' = 8$. Using this ordering, $1, 6, 3, 5, 2, 4, 7, 8$ and the Cayley table given above for $(Q_8, \star)$, we can calculate that, in fact $(Q_8, \star)$, is 7-translatable, with 7-translatable sequence $2, 4, 6, 5, 7, 3, 8, 1$ or $a_4, a_7, a_2, a_5, a_8, a_3, a_1, a_6$. Then, by Corollary 3.4, we see that $(Q_8, \star)$ is not a 7-translatable isotope of $(Q_8, \cdot)$. That is because the subscripts of the a's in its translatable sequence must increase successively by the same value of $[\tilde{7} \cdot 5t]_8 = [35t]_8 = [3t]_8$. Although the subscripts start increasing by a value of 3, this does not continue when moving from b_6 to b_7.

4. Translatability and isomorphism

It is known that isomorphism preserves k-translatability; that is, if $(Q, \cdot)$ is k-translatable and isomorphic to $(Q, *)$ then $(Q, *)$ is k-translatable (cf. [3, Theorem 8.14]). However, k-translatable quasigroups of the same order are not necessarily isomorphic. An example of such quasigroups are 3-translatable quasigroups defined by the following tables. The first is without idempotents, in the second - all elements are idempotent. So, they cannot be isomorphic.

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

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

So, when are two translatable quasigroups of the same order isomorphic? As already mentioned, we know by [3, Theorem 8.14] that if they are isomorphic then they must have equal value of translatability. Two idempotent, k-translatable quasigroups of the same order are isomorphic [2, Theorem 2.12]. The general problem remains. If $(Q,\cdot)$ and $(S,*)$ are both k-translatable quasigroups of the same order then when are they isomorphic?

Theorem 4.1. *Suppose that $(Q,\cdot)$ and $(S,*)$ are k-translatable quasigroups of the same order n. If $(Q,\cdot)$ is k-translatable with respect to the natural ordering, with k-traslatable sequence $a_1,a_2,a_3,\ldots,a_n$ and $(S,*)$ is k-translatable with respect to the ordering $1',2',3',\ldots,n'$, with k-translatable sequence $b'_1,b'_2,b'_3\ldots,b'_n$. Then $\Psi: Q\to S$ defined by $\Psi i=(s_i)'$, $i\in\overline{\{1,n\}}$, is an isomorphism if and only if*

(i) $s_i=[s_n+it]_n$ for all $i\in\overline{\{1,n\}}$, where $t=[k(s_1-s_{[1-\tilde{k}]_n})]_n$, $(t,n)=1$ and

(ii) $s'_{a_j}=b'_{[r+jt]_n}$ for all $j\in\overline{\{1,n\}}$, where $r=[k(1-s_n-t)+s_n]_n$.

Proof. ($\Rightarrow$). By Lemma 2.4 (i) and Lemma 2.5 (i), $i\cdot j=a_{[k-ki+j]_n}$ and $i'*j'=b'_{[k-ki+j]_n}$ for all $i,j\in\overline{\{1,n\}}$. Since Ψ is an isomorphism, for all $i,j\in\overline{\{1,n\}}$, $\Psi a_{[k-ki+j]_n}=\Psi(i\cdot j)=\Psi i*\Psi j=s'_i*s'_j=b_{[k-ks_i+s_j]_n}$. But $1\cdot[k-ki+j]_n=a_{[k-ki+j]_n}$, $\Psi a_{[k-ki+j]_n}=b'_{[[k-ks_i+s_j]_n}=\Psi(1\cdot[k-ki+j]_n)=\Psi 1*\Psi[k-ki+j]_n=s'_1*s'_{[k-ki+j]_n}=b'_{[k-ks_1+s_{[k-ki+j]_n}]_n}$ and so

$$[k(s_1-s_i)]_n=[s_{[k-ki+j]_n}-s_j]_n,$$

which for $i=[1-\tilde{k}]_n$ gives

$$[k(s_1-s_{[1-\tilde{k}]_n})]_n=[s_{[j+1]_n}-s_j]_n,$$

for all $j\in\overline{\{1,n\}}$.

The last equation for $t=[k(s_1-s_{[1-\tilde{k}]_n})]_n$ implies $t=[s_1-s_n]_n=[s_2-s_1]_n=\ldots=[s_n-s_{n-1}]_n$. Hence

$$s_i=[s_n+it]_n \tag{9}$$

and $S = \{s_1, s_2, \ldots, s_n\}$ for $(t, n) = 1$.

Also, $\Psi(i \cdot j) = \Psi a_{[k-ki+j]_n} = s'_{a_{[k-ki+j]_n}}$ and $\Psi i * \Psi j = s'_i * s'_j = b'_{[k-ks_i+s_j]_n} \overset{(9)}{=} b'_{[k-ks_n-kit+s_n+jt]_n}$. Therefore, $s'_{a_{[k-ki+j]_n}} = b'_{[k-ks_n-kit+s_n+jt]_n}$. Hence, when $i = 1$, we have

$$s'_{a_j} = b'_{[k-ks_n-kt+s_n+jt]_n} = b'_{[k(1-s_n-t)+s_n+jt]_n} = b'_{[r+jt]_n}$$

for all $j \in \overline{\{1, n\}}$, where $r = [k((1 - s_n - t) + s_n]_n$. So, we have proved (i) and (ii), thereby proving necessity.

$(\Leftarrow)$. Assume that (i) and (ii) are valid. Let $j = [k - kl + m]_n$ for any $l, m \in \overline{\{1, n\}}$. By (ii), $s'_{a_{[k-ki+m]_n}} = b'_{[r+(k-kl+m)t]_n}$. Since $r = [k(1 - s_n - t) + s_n]_n$, $[r + (k - kl + m)t]_n = [k - ks_n + s_n - klt + mt]_n = [k - k(s_n + lt) + (s_n + mt)]_n \overset{(i)}{=} [k - ks_l + s_m]_n$ and so $s'_{a_{[k-kl+m]_n}} = b'_{[k-ks_l+s_m]_n}$ and $\Psi(l \cdot m) = \Psi a_{[k-kl+m]_n} = s'_{a_{[k-kl+m]_n}} = b'_{[k-ks_l-s_m]_n} = s'_l * s'_m = \Psi l * \Psi m$ for any $l, m \in \overline{\{1, n\}}$. Hence $(Q, \cdot)$ and $(S, *)$ are isomorphic. □

Notice that, given the k-translatable quasigroups $(Q, \cdot)$ and $(Q, *)$, given the k-translatable sequence $a_1, a_2, \ldots, a_n$ of Q and a given t relatively prime to n, by (i) and (ii) every $s_n \in Q$ determines a k-translatable sequence $b'_1, b'_2, \ldots, b'_n$ for which $(Q.\cdot)$ and $(Q, *)$ are isomorphic.

Example 4.2. Let $(Q, \cdot)$, where $Q = \{1, 2, 3, 4, 5\}$, be a 2-translatable quasigroup with respect to the natural ordering, with 2-translatable sequence $3, 1, 5, 2, 4$. Let a quasigroup $(S, *)$ be 2-translatable with respect to the ordering $b'_1, b'_2, b'_3, b'_4, b'_5$. Let $s_5 = 5$ and $t = 3$, with $\Psi i = (s_i)'$, $i \in \overline{\{1, 5\}}$ and $s_1 = 3$, $s_2 = 1$, $s_3 = 4$, $s_4 = 2$, $s_5 = 5$. Suppose that $b_1 = 3$, $b_2 = 1$,$b_3 = 2$, $b_4 = 4$, $b_5 = 5$ Then, by Theorem 4.1, Ψ is not an isomorphism because although (i) is satisfied, $s_{a_5} = s_4 = 2 \neq b_x$, where $x = [k(1 - s_5 - t) + s_6 + 5t]_5 = 1$ and so, $2 \neq b_1 = 3$. Thus, (ii) is not satisfied and Ψ is not an isomorphism. However, if we consider the mapping when $s_5 = 2$ and $t = 3$, then $s_1 = 5$, $s_2 = 3$, $s_3 = 1$, $s_4 = 4$ and this satisfies (i) and (ii). So, $(Q, \cdot)$ and $(S, *)$ are isomorphic, with that mapping as the isomorphism; namely, $1 \mapsto 5'$, $2 \mapsto 3'$, $3 \mapsto 1'$, $4 \mapsto 4'$, $5 \mapsto 2'$.

Example 4.3. Here are the Cayley tables of the 2-translatable quasigroups of Example 4.2.

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

$*$	$1'$	$2'$	$3'$	$4'$	$5'$
$1'$	b'_1	b'_2	b'_3	b'_4	b'_5
$2'$	b'_4	b'_5	b'_1	b'_2	b'_3
$3'$	b'_2	b'_3	b'_4	b'_5	b'_1
$4'$	b'_5	b'_1	b'_2	b'_3	b'_4
$5'$	b'_3	b'_4	b'_5	b'_1	b'_2

Using Theorem 4.1, we can determine all 2-translatable sequences $b'_1, b'_2, b'_3, b'_4, b'_5$ of $(S, *)$ such that $(Q, \cdot)$ and $(Q, *)$ are isomorphic.

Since $s_5 \in \overline{\{1, 5\}}$ and $t \in \overline{\{1, 4\}}$ there are 20 such 2-translatable sequences. Below we present these sequences for $t = 2$.

s_5	t	r	s_1	s_2	s_3	s_4	b_1	b_2	b_3	b_4	b_5	$\Psi 1$	$\Psi 2$	$\Psi 3$	$\Psi 4$	$\Psi 5$
1	2	2	3	5	2	4	3	4	1	2	5	$3'$	$5'$	$2'$	$4'$	$1'$
2	2	1	4	1	3	5	5	2	3	1	4	$4'$	$1'$	$3'$	$5'$	$2'$
3	2	5	5	2	4	1	3	4	2	5	1	$5'$	$2'$	$4'$	$1'$	$3'$
4	2	4	1	3	5	2	5	3	1	2	4	$1'$	$3'$	$5'$	$2'$	$4'$
5	2	3	2	4	1	3	4	2	3	5	1	$2'$	$4'$	$1'$	$3'$	$5'$

We can check that the quasigroups in the table above are actually isomorphic to $(Q, \cdot)$ by using the mapping Ψ and re-ordering $(S, *)$ accordingly. In this sense, Ψ can be considered to be a mapping that re-orders S, giving it a 2-translatable Cayley table that is more clearly isomorphic to $(Q, \cdot)$. For example, for $s_5 = 3$, $t = 2$ and $r = 5$ we have the following:

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

$*$	$1'$	$2'$	$3'$	$4'$	$5'$
$1'$	$3'$	$4'$	$2'$	$5'$	$1'$
$2'$	$5'$	$1'$	$3'$	$4'$	$2'$
$3'$	$4'$	$2'$	$5'$	$1'$	$3'$
$4'$	$1'$	$3'$	$4'$	$2'$	$5'$
$5'$	$2'$	$5'$	$1'$	$3'$	$1'$

$*$	$5'$	$2'$	$4'$	$1'$	$3'$
$5'$	$4'$	$5'$	$3'$	$2'$	$1'$
$2'$	$2'$	$1'$	$4'$	$5'$	$3'$
$4'$	$5'$	$3'$	$2'$	$1'$	$4'$
$1'$	$1'$	$4'$	$5'$	$3'$	$2'$
$3'$	$3'$	$2'$	$1'$	$4'$	$5'$

It is not at all obvious that the first and second quasigroups above are isomorphic. Whereas, using the mapping ψ that takes $1 \mapsto 5'$, $2 \mapsto 2'$, $3 \mapsto 4'$, $4 \mapsto 1'$ and $5 \mapsto 3'$, it is clear that the first and third Cayley tables are exactly the same, except for this re-labelling.

Definition 4.4. Suppose that $(Q, \cdot)$ is a k-translatable quasigroup with respect to the natural ordering, with k-translatable sequence $a_1, a_2, \ldots, a_n$. If $(Q, *)$ is an h-translatable quasigroup with respect to the ordering $1, 2', \ldots, n'$ and is also an isotope of $(Q, \cdot)$, then we write

$$(Q, *) = (Q, *, h, i', \cdot, k, c, d, t, a_1, a_2, \ldots, a_n),$$

where c, d and t are as in Corollary 3.4. If $(Q, *)$ is h-translatable with respect to the natural ordering then we write

$$(Q, *) = (Q, *, h, i' = i, \cdot, k, c, d, t, a_1, a_2, \ldots, a_n).$$

Corollary 4.5. *Suppose that* $(Q, *) = (Q, *, h, i' = i, \cdot, k, c, d, t, a_1, a_2, \ldots, a_n)$, $(Q, \bullet) = (Q, \bullet, h, i', \cdot, k, e, f, u, a_1, a_2, \ldots, a_n)$ *and* $\Phi : (Q, *) \to (Q, \bullet)$ *is defined by* $\Psi i = (s_i)'$, $i \in \overline{\{1, n\}}$. *Then* Ψ *is an isomorphism if and only if*

(1) $s_i = [s_n + iv]_n$ *for all* $i \in \overline{\{1, n\}}$, *where* $v = [h(s_1 - s_{[1-\tilde{h}]_n})]_n$ *and* $(v, n) = 1$, *and*

(2) $\Psi\, a_{[x+(j-d)\tilde{h}kt]_n} = a_{[y+(r+jv-f)\tilde{h}ku]_n}$ *for all* $j \in \overline{\{1, n\}}$, *where* $x = [k + kct - kt]_n$, $y = [k + keu - ku]_n$ *and* $r = [h(1 - s_v - v) + s_n]_n$.

Proof. ($\Rightarrow$). By Theorem 4.1, (i) of Corollary 4.5 is valid. By Corollary 3.4, the j^{th} entry in the h-translatable sequences of $(Q, *)$ and $(Q, \bullet)$ is $a_{[x+(j-d)\tilde{h}kt]_n}$ and $a_{[y+(j-f)\tilde{h}ku]_n}$ respectively, where $x = [k + kct - kt]_n$ and $y = [k + keu - ku)]_n$. Note that the h-translatable sequence of $(Q, \bullet)$, $b'_1, b'_2, \ldots, b'_n$, satisfies $b'_j = a_{[y+(j-f)\tilde{h}ku]_n}$. Then, Theorem 4.1 (ii) implies $(s_{a_{[x+(j-d)\tilde{h}kt]_n}})' = (b_{[r+jn]_n})'$, where $r = [h(1 - s_v - v) + s_v]_n$. Therefore, (ii) of Corollary 4.5 is valid.

($\Leftarrow$). This follows from ($\Leftarrow$) of Theorem 4.1. □

Example 4.6. Let $(Q, \cdot)$ be the quasigroup determined by the following Cayley table.

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

Then $(Q, \cdot)$ is 3-translatable with respect to the natural ordering, with 3-translatable sequence $a_1 = 3$, $a_2 = 1$, $a_3 = 4$, $a_3 = 5$ and $a_5 = 2$. Using Corollary 3.4, we now construct a quasigroup $(Q, *)$ that is 3-translatable with respect to the natural ordering, is an isotope of $(Q, \cdot)$ and is not isomorphic to $(Q, \cdot)$.

Firstly, we want $5 * 5 = 5$. This ensures that $(Q, *)$ and $(Q, \cdot)$ are not isomorphic, because $(Q, \cdot)$ has no idempotent elements. Now, since we want $(Q, *)$ to be 3-translatable with respect to the natural ordering, in Corollary 3.4 we have $q' = q$ for all $q \in \overline{\{1, 5\}}$.

Then, since we want $h = k$, $1 * q' = 1 * q = a_{x_q}$, where $x_q = [r + (q - 1)\tilde{k}kt]_5 = [r + (q - 1)t]_5$ and $r = [k - kct - kt + (1 - d)\tilde{k}kt]_5$. Choosing $c = 5$ and $d = 1$ we get $r = [3 - 3t]_5$ and $x_q = [3 - 3t + (q - 1)t] - 5$. But, since $(Q, *)$ is 3-translatable and $5 * 5 = 5$, by Corollary 3.4, we have $1 * 3' = 1 * 3 = a_{x_3} = 5 = a_4$. Hence, $x_3 = 4 = [3 - 3t + (3 - 1)t]_5 = [3 - t]_5$ and $t = [-1]_5 = 4$ and $r = [3 - 3t]_5 = 1$.

This gives $x_q = [1 + (q - 1)4]_5$ and so, $x_1 = 1$, $x_2 = 5$, $x_4 = 3$ and $x_5 = 2$. Therefore, by Corollary 3.4 again, the 3-translatable sequence of $Q, *)$ is a_1, a_5, a_4, a_3, a_2 or $3, 2, 5, 4, 1$. This gives the following Cayley table for $(Q, *)$.

$*$	1	2	3	4	5
1	3	2	5	4	1
2	5	4	1	3	2
3	1	3	2	5	4
4	2	5	4	1	3
5	4	1	3	2	5

Using ($\Leftarrow$) of Corollary 3.4, we see that $\alpha([c + i]'_5) = \alpha i' = \alpha i = [it]_5 = [4i]_5 = \beta([1 + i]'_5) = \beta[i + 1]_5$. This gives $\alpha 1 = 4 = \beta 2$, $\alpha 2 = 3 = \beta 3$, $\alpha 3 = 2 = \beta 4$, $\alpha 4 = 1 = \beta 5$ and $\alpha 5 = 5 = \beta 1$. One easily checks that $i * j = \alpha i \cdot \beta j$ for all $i, j \in \overline{\{1, 5\}}$. Therefore, $(Q, *)$ is the required 3-translatable isotope of $(Q, \cdot)$.

References

[1] **R.H. Bruck**, *A survey of Binary Systems*, Springer-Verlag, New York, 1966.

[2] **W.A. Dudek and R.A.R. Monzo**, *Translatability and translatable semigroups*, Open Mathematics **16** (2018), 1266-1282.

[3] **W.A. Dudek and R.A.R. Monzo**, *Translatable quadratical quasigroups*, Quasigroups and Related Systems, **28** (2021), 209-223.

[4] **W.A. Dudek and R.A.R. Monzo**, *Translatable isotopes of finite groups*, Quasigroups and Related Systems, **29** (2021), 209-223.

Received March 10, 2022

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

R.A.R. Monzo
Flat 10, Albert Mansions, Crouch Hill, London N8 9RE, United Kingdom
E-mail: bobmonzo@talktalk.net

Quasigroups and Related Systems **30** (2022), 209 – 218

On right bases of partially ordered ternary semigroups

Wichayaporn Jantanan, Natee Raikham and Ronnason Chinram

Abstract. We investigate the results of a partially ordered ternary semigroup containing right bases and characterize when a non-empty subset of a partially ordered ternary semigroup is a right base. Moreover, we give a characterization of a right base of a partially ordered ternary semigroup to be a ternary subsemigroup and we show that the right bases of a partially ordered ternary semigroup have same cardinality. Finally, we show that the complement of the union of all right bases of a partially ordered ternary semigroup is a maximal proper left ideal.

1. Introduction

A ternary semigroup is a particular case of n-ary semigroup introduced by Kasner [5], i.e. it is a non-empty set T with an operation $T \times T \times T \to T$, written as $(a, b, c) \to [abc]$, such that $[[abc]de] = [a[bcd]e] = [ab[cde]]$ for all $a, b, c, d, e \in T$. Any ternary semigroup can be embedded into some binary semigroup (called a covering semigroup) in this way that $[abc] = abc$ for $a, b, c \in T$ [1]. Based on the notion of one-sided ideals of a semigroup generated by a non-empty set, the notion of one-sided bases of a semigroup was first introduced by Tamura [6]. Later, this concept was studied by Fabrici [2]. Moreover, the concept of one-sided bases were introduced and discussed in ternary semigroups by Changphas and Kummon [7]. In this paper, we introduce the concept of right bases of a partially ordered ternary semigroup. We study the structure of a partially ordered ternary semigroup containing right bases and extend the conclusions obtained by Thongkam and Changphas [7] to the results in partially ordered ternary semigroups, where by a *partially ordered ternary semigroup* (shortly: *ternary po-semigroup*) is mean

2010 Mathematics Subject Classification: 20N10, 06F05.
Keywords: partially ordered ternary semigroup, right base, right singular.

a ternary semigroup with a partial order such that

$$a \leqslant b \Rightarrow [axy] \leqslant [bxy], \quad [xay] \leqslant [xby] \text{ and } [xya] \leqslant [xyb]$$

for all $a, b, x, y \in T$. In the last years ternary semigroups (also partially ordered) were studied by many authors (see for example [3, 4]).

We shall assume throughout this paper that T stands for a ternary po-semigroup. For non-empty subsets A, B and C of a ternary po-semigroup T, we denote

$[ABC] := \{[abc] \mid a \in A, b \in B, c \in C\}$ and

$(A] := \{t \in T \mid t \leqslant a \text{ for some } a \in A\}$.

If $A = \{a\}$, we write $[\{a\}BC]$ as $[aBC]$ and $(\{a\}]$ as $(a]$. For any other cases can be defined analogously. For the sake of simplicity, we write $[ABC]$ as ABC and $[abc]$ as abc.

A non-empty subset A of a ternary po-semigroup T is called a *left* (resp. *right*) *ideal* if (1) $TTA \subseteq A$ (resp. $ATT \subseteq A$) (2) if $x \in A$ and $y \in T$ such that $y \leqslant x$, then $y \in A$. A left ideal A of T is said to be *proper* if $A \subset T$. A proper left ideal A of T is said to be *maximal* if there is no a proper left ideal B of A such that $A \subset B$. Note that the union of left ideals of T is a left ideal of T, and the intersection of left ideals of T is a left ideal of T, if it is non-empty. By $L(A)$ we denote the smallest left ideal of T containing A, that is $L(A) = (A \cup TTA]$. In particular case, for $a \in T$, we write $L(a)$ instead of $L(\{a\})$, called the *principal left ideal* of T generated by a, and it is the from $L(a) = (a \cup TTa]$.

As in [7], we define the *quasi-ordering* on a partially ordered ternary semigroup T by for any $a, b \in T$,

$$a \leqslant_L b \text{ if and only if } L(a) \subseteq L(b).$$

The symbol $a <_L b$ stands for $a \leqslant_L b$ and $a \neq b$ i.e., $L(a) \subset L(b)$.

Let A, B, C be non-empty subsets of T. Then

(1) $A \subseteq (A]$ and $((A]] = (A]$.

(2) If $A \subseteq B$, then $(A] \subseteq (B]$.

(3) $(A](B](C] \subseteq (ABC]$.

(4) $(A] \cup (B] = (A \cup B]$.

(5) $(TTA]$ is a left ideal of T.

(6) For any $a \in T$, $(TTa]$ is a left ideal of T.

2. Main results

In this section we characterize right bases of a ternary po-semigroup and extend the results from [7].

Definition 2.1. A non-empty subset A of a ternary po-semigroup T is called a *right base* of T if:

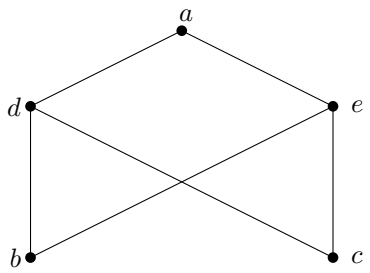
(1) $T = (A \cup TTA]$, i.e., $T = L(A)$;

(2) if B is a subset of A such that $T = L(B)$, then $B = A$.

Example 2.2. Let $T = \{a, b, c, d, e\}$ be a ternary po-semigroup with the operation $xyz = z$ and the partial order $a \leqslant c \leqslant e \leqslant b$ where d is a separate element. Then $\{b, d\}$ is a right base of T, but $\{b\}$ and $\{d\}$ are not right bases of T.

Example 2.3. Let $T = \{a, b, c, d, e\}$ be a ternary po-semigroup with the operation $abc = a * (b * c)$, where $(T, *, \leqslant)$ is a po-semigroup defined by the following table and graph:

$*$	a	b	c	d	e
a	a	e	e	a	e
b	d	b	b	d	b
c	d	b	b	d	b
d	d	b	b	d	b
e	a	e	e	a	e



The right bases of T are $\{a\}$ and $\{d\}$. But $\{a, d\}$ is not a right base.

Lemma 2.4. Let T be a ternary po-semigroup. For any $a, b \in T$, if $a \leqslant b$, then $a \leqslant_L b$.

Lemma 2.5. Let A be a right base of a ternary po-semigroup T, and $a, b \in A$. If $a \in (TTb]$, then $a = b$.

Proof. Let $a, b \in A$ be such that $a \in (TTb]$. Suppose that $a \neq b$. Let $B = A \setminus \{a\}$. Then $B \subset A$. We claim that $L(B) = T$. Clearly, $L(B) \subseteq T$. Next, let $x \in T$. Then, by $L(A) = T$, we have $x \in (A \cup TTA]$. Thus, $x \leqslant y$ for some $y \in A \cup TTA$. There are two cases to consider:

Case 1: $y \in A$. We have $y \neq a$ or $y = a$. If $y \neq a$, then $y \in B \subseteq L(B)$. If $y = a$, then

$$y = a \in (TTb] \subseteq (TTB] \subseteq L(B).$$

Case 2: $y \in TTA$. We set $y = t_1t_2a_1$ for some $t_1, t_2 \in T$ and $a_1 \in A$. If $a_1 \neq a$, then

$$y = t_1t_2a_1 \in TTB \subseteq L(B).$$

If $a_1 = a$, then

$$y = t_1t_2a_1 \in TT(TTb] \subseteq (T](T](TTB] \subseteq ([TTT]TB] \subseteq (TTB] \subseteq L(B).$$

From both cases, we obtain that $y \in L(B)$. Since $x \leqslant y$ and $y \in L(B)$, then $x \in (L(B)] = L(B)$. Thus, $T \subseteq L(B)$. Hence $L(B) = T$. This is a contradiction. Therefore, $a = b$. □

Theorem 2.6. *A non-empty subset A of a ternary po-semigroup T is a right base of T if and only if*

(1) *for any $x \in T$ there exists $a \in A$ such that $x \leqslant_L a$;*

(2) *for any $a, b \in A$, if $a \neq b$, then neither $a \leqslant_L b$ nor $b \leqslant_L a$.*

Proof. Assume that A is a right base of T. We have $L(A) = T$. First, to show that (1) holds. Let $x \in T$. Then $x \in (A \cup TTA]$. Thus, $x \leqslant y$ for some $y \in A \cup TTA$. If $y \in A$ and $x \leqslant y$, by Lemma 2.4, we obtain $x \leqslant_L y$. If $y \in TTA$, then $y = t_1t_2a$ for some $t_1, t_2 \in T$ and $a \in A$. Since $x \leqslant y$ and $y = t_1t_2a \in TTa \subseteq L(a)$, we obtain $x \in (L(a)] = L(a)$. It follows that $L(x) \subseteq L(a)$. Thus, $x \leqslant_L a$ where $a \in A$. This shows that (1) holds.

To prove (2) let $a, b \in A$ be such that $a \neq b$. Suppose that $a \leqslant_L b$. We set $B = A \setminus \{a\}$. Then $b \in B$ and $B \subset A$. Let $x \in T$, by (1), there exists $c \in A$ such that $x \leqslant_L c$ i.e., $L(x) \subseteq L(c)$. Since $c \in A$, we have $c \neq a$ or $c = a$. If $c \neq a$, then $c \in B$. We obtain $x \in L(x) \subseteq L(c) \subseteq L(B)$. If $c = a$, then $x \leqslant_L c = a \leqslant_L b$ and so $x \leqslant_L b$. We obtain $x \in L(x) \subseteq L(b) \subseteq L(B)$. Hence, $T \subseteq L(B)$ and so $T = L(B)$. This is a contradiction. The case $b \leqslant_L a$ can be proved similarly. Thus, $a \leqslant_L b$ and $b \leqslant_L a$ are false.

Conversely, assume that the conditions (1) and (2) hold. We will show that A is a right base of T. Clearly, $L(A) \subseteq T$. By (1), we obtain $T \subseteq L(A)$. Thus, $T = L(A)$. Next, suppose that $T = L(B)$ for some $B \subset A$. Let $a \in A \setminus B$. We have $a \in A \subseteq T = L(B) = (B] \cup (TTB]$. If $a \in (B]$, then $a \leqslant b$ for some $b \in B$. By Lemma 2.4, we obtain $a \leqslant_L b$ where $a, b \in A$. This contradicts to (2). If $a \in (TTB]$, then $a \leqslant t_1t_2b_1$ for some $t_1, t_2 \in T$ and $b_1 \in B$. Since $a \leqslant t_1t_2b_1$ and $t_1t_2b_1 \in TTb_1$, we have $a \in (TTb_1] \subseteq L(b_1)$. It follows that $L(a) \subseteq L(b_1)$. Thus, $a \leqslant_L b$ where $a, b_1 \in A$. This contradicts to (2). Hence, A is a right base of T. □

Definition 2.7. A ternary po-semigroup T is said to be *right singular* if $xyz = z$ for all $x, y, z \in T$.

In general, a right base of a ternary po-semigroup need not be a ternary subsemigroup. Thus, the following theorem is a requirement for a right base to be a ternary subsemigroup.

Theorem 2.8. *Let A be a right base of a ternary po-semigroup T. Then A is a ternary subsemigroup of T if and only if A is right singular.*

Proof. Assume that A is a ternary subsemigroup of T. Let $a, b, c \in A$. By assumption, we have $abc \in A$. Since $abc \in A$, then there exists $x \in A$ such that $x = abc$. Then $x = abc \in TTc \subseteq (TTc]$. By Lemma 2.5, $x = c$. Thus, $abc = c$. Therefore, A is right singular. The converse statement is obvious. □

In Example 2.2 and Example 2.3, it is observed that the cardinality of right bases are the same. However, it turns out that this is true in general, and we will prove in the following theorem.

Theorem 2.9. *Let A and B be any right bases of a ternary po-semigroup T. Then A and B have the same cardinality.*

Proof. Let $a \in A$. Since B is a right base of T, by Theorem 2.6(1), we have $a \leqslant_L b$ for some $b \in B$. Similarly, since A is a right base of T, we have $b \leqslant_L a^*$ for some $a^* \in A$. Thus, $a \leqslant_L b \leqslant_L a^*$ and so $a \leqslant_L a^*$. By Theorem 2.6(2), we obtain $a = a^*$. Hence, $a \leqslant_L b \leqslant_L a$ and so $L(a) = L(b)$. Define a mapping

$$f : A \to B \quad \text{by} \quad f(a) = b \quad \text{for all } a \in A.$$

If $a_1, a_2 \in A$ be such that $a_1 = a_2$, $f(a_1) = b_1$ and $f(a)_2 = b_2$ for some $b_1, b_2 \in B$, we have $L(a_1) = L(a_2)$, $L(a_1) = L(b_1)$ and $L(a_2) = L(b_2)$. Thus, $L(a_1) = L(a_2) = L(b_1) = L(b_2)$ i.e., $b_1 \leqslant_L b_2$ and $b_2 \leqslant_L b_1$. By Theorem 2.6(2), we obtain $b_1 = b_2$. Hence, f is well-defined. Next, to show that f is one-to-one. Let $a_1, a_2 \in A$ be such that $f(a_1) = f(a_2) = b$ for some $b \in B$. Then $a_1 \leqslant_L b$ and $a_2 \leqslant_L b$. Since A is a right base of T, we have $b \leqslant_L a$ for some $a \in A$. Thus, $a_1 \leqslant_L b \leqslant_L a$, $a_2 \leqslant_L b \leqslant_L a$ and so $a_1 \leqslant_L a$, $a_2 \leqslant_L a$. By Theorem 2.6(2), we obtain $a_1 = a = a_2$. Hence, f is one-to-one. Finally, we will show that f is onto. Let $b \in B$. To show that $f(a) = b$ for all $a \in A$, it suffices to show $L(a) = L(b)$ for all $a \in A$. Since A is a right base of T, by Theorem 2.6(1), we have $b \leqslant_L a$ for some $a \in A$. Similarly, since B is

a right base of T, we have $a \leqslant_L b^*$ for some $b^* \in B$. Thus, $b \leqslant_L a \leqslant_L b^*$ and so $b \leqslant_L b^*$. By Theorem 2.6(2), $b = b^*$. This implies that $L(a) = L(b)$. Therefore, f is onto. □

Theorem 2.10. *Let A be a right base of a ternary po-semigroup T, and $a \in A$. If $L(a) = L(b)$ for some $b \in T$ and $a \neq b$, then b is an element of a right base of T which is distinct from A.*

Proof. Assume that $L(a) = L(b)$ for some $b \in T$ and $a \neq b$. Let $B = (A \setminus \{a\}) \cup \{b\}$. Then $B \neq A$. We will show that B is a right base of T, it suffices to show that B satisfies the conditions (1) and (2) of Theorem 2.6. First, let $x \in T$. Since A is a right base of T, we have $x \leqslant_L c$ for some $c \in A$. If $c \neq a$, then $c \in B$. If $c = a$, then $L(c) = L(a) = L(b)$. Thus, $L(x) \subseteq L(c) = L(b)$. Hence, $x \leqslant_L b$ where $b \in B$. This means that satisfies the condition (1) of Theorem 2.6. Next, let $b_1, b_2 \in B$ be such that $b_1 \neq b_2$. We consider four cases:

Case 1: $b_1 \neq b$ and $b_2 \neq b$. Then $b_1, b_2 \in A$. This implies neither $b_1 \leqslant_L b_2$ nor $b_2 \leqslant_L b_1$.

Case 2: $b_1 \neq b$ and $b_2 = b$. Then $L(b_2) = L(b)$. If $b_1 \leqslant_L b_2$, we have

$$L(b_1) \subseteq L(b_2) = L(b) = L(a).$$

Thus, $b_1 \leqslant_L a$ where $b_1, a \in A$. This is a contradiction. If $b_2 \leqslant_L b_1$, we have

$$L(a) = L(b) = L(b_2) \subseteq L(b_1).$$

Thus, $a \leqslant_L b_1$ where $b_1, a \in A$. This is a contradiction.

Case 3: $b_1 = b$ and $b_2 \neq b$. Then $L(b_1) = L(b)$. If $b_1 \leqslant_L b_2$, we have

$$L(a) = L(b) = L(b_1) \subseteq L(b_2).$$

Thus, $a \leqslant_L b_2$ where $b_2, a \in A$. This is a contradiction. If $b_2 \leqslant_L b_1$, we have

$$L(b_2) \subseteq L(b_1) = L(b) = L(a).$$

Thus, $b_2 \leqslant_L a$ where $b_2, a \in A$. This is a contradiction.

Case 4: $b_1 = b$ and $b_2 = b$. Then $b_1 = b_2$. This contradicts to $b_1 \neq b_2$. This means that B satisfies the condition (2) of Theorem 2.6. Therefore, B is a right base of T. □

The following corollary follows directly from Theorem 2.10.

Corollary 2.11. *Let A be a right base of a ternary po-semigroup T, and $a \in A$. If $L(a) = L(b)$ for some $b \in T$ and $a \neq b$, then T contains at least two right bases.*

Theorem 2.12. *Let R be the union of all right bases of a ternary po-semigroup T. If $T \setminus R$ is non-empty, then it is a left ideal of T.*

Proof. Assume that $T \setminus R$ is non-empty. Let $x, y \in T$ and $a \in T \setminus R$. Suppose that $xya \notin T \setminus R$. Then $xya \in R$. Thus, $xya \in A$ for some a right base A of T. We set $xya = b$ for some $b \in A$. Then $b = xya \in TTa \subseteq L(a)$. This implies that $L(b) \subseteq L(a)$. Thus, $b \leqslant_L a$. If $L(b) = L(a)$, by Theorem 2.10, $a \in R$. This contradicts to $a \in T \setminus R$. Hence, $L(b) \neq L(a)$. Since A is a right base of T, we have $a \leqslant_L c$ for some $c \in A$. If $c = b$, then $L(a) \subseteq L(c) = L(b) \subseteq L(a)$. Thus, $L(a) = L(b)$. This is a contradiction. Hence, $c \neq b$. Since $b \leqslant_L a$ and $a \leqslant_L c$, we have $b \leqslant_L c$ where $b \neq c$ and $b, c \in A$. This contradicts to the condition (2) of Theorem 2.6. Thus, $xya \in T \setminus R$. Next, let $x \in T \setminus R$ and $y \in T$ such that $y \leqslant x$. By Lemma 2.4, $y \leqslant_L x$. To show that $y \in T \setminus R$, suppose that $y \notin T \setminus R$. Then $y \in R$ and so $y \in B$ for some a right base B of T. Since B is a right base of T, we have $x \leqslant_L z$ for some $z \in B$. Since $y \leqslant_L x$ and $x \leqslant_L z$, then $y \leqslant_L z$ where $y, z \in B$. If $y = z$, we have $x \leqslant_L z = y \leqslant_L x$. By Theorem 2.6(2), $x = y$. This is a contradiction. Thus, $y \neq z$ and $y \leqslant_L z$. This contradicts to the condition (2) of Theorem 2.6. Hence, $y \in T \setminus R$. Therefore, $T \setminus R$ is a left ideal of T. □

Theorem 2.13. *Let R be the union of all right bases of a ternary po-semigroup T such that $R \neq \varnothing$. Then $T \setminus R$ is a maximal proper left ideal of T if and only if $R \neq T$ and $R \subseteq L(a)$ for all $a \in R$.*

Proof. Assume that $T \setminus R$ is a maximal proper left ideal of T. We have $T \setminus R \subset T$ and so $R \neq T$. Let $a \in R$. Suppose that $R \nsubseteq L(a)$. Then there exists $x \in R$ such that $x \notin L(a)$. Since $x \notin T \setminus R$ and $x \notin L(a)$, then $(T \setminus R) \cup L(a) \subset T$. So, we have $(T \setminus R) \cup L(a)$ is a proper left ideal of T, and $(T \setminus R) \subset (T \setminus R) \cup L(a)$. This contradicts to the maximality of $T \setminus R$. Thus, $R \subseteq L(a)$.

Conversely, assume that $R \neq T$ and $R \subseteq L(a)$ for all $a \in R$. We will show that $T \setminus R$ is a maximal proper left ideal of T. Since $\varnothing \neq R \subset T$, then $\varnothing \neq T \setminus R \subset T$. By Theorem 2.12, $T \setminus R$ is a proper left ideal of T. Next, let L is a proper left ideal of T such that $T \setminus R \subset L \subset T$. Then there exists $x \in L$ such that $x \notin T \setminus R$ i.e., $x \in R$. Thus, $R \cap L \neq \varnothing$. Let $a \in R \cap L$.

Then $a \in R$ and $a \in L$. So, we have $R \subseteq L(a)$ and $L(a) \subseteq L$. Hence, $R \subseteq L$ and so

$$T = (T \setminus R) \cup R \subseteq L \subset T.$$

Thus, $T = L$. This is a contradiction. Therefore, $T \setminus R$ is a maximal proper left ideal of T. □

Theorem 2.14. *Let R be the union of all right bases of a ternary po-semigroup T such that $\varnothing \neq R \subset T$, and let L^* be a proper left ideal of T containing every proper left ideal of T. Then the following statements are equivalent:*

(1) *$T \setminus R$ is a maximal proper left ideal of T;*

(2) *$R \subseteq L(a)$ for all $a \in R$;*

(3) *$T \setminus R = L^*$;*

(4) *every right base of T is singleton set.*

Proof. (1) $\Leftrightarrow$ (2). This follows from Theorem 2.13.

(3) $\Leftrightarrow$ (4). Assume that $T \setminus R = L^*$. Then $T \setminus R$ is a maximal proper left ideal of T. Let $a \in R$. By Theorem 2.13, we have $R \subseteq L(a)$. If $T \setminus R \nsubseteq L(a)$ for some $a \in R$, we have $L(a) \neq T$ and so $L(a)$ is a proper left ideal of T. Thus, $a \in L(a) \subseteq L^* = T \setminus R$ and so $a \in T \setminus R$. This contradicts to $a \in R$. Hence, $T \setminus R \subseteq L(a)$. Since $R \subseteq L(a)$ and $T \setminus R \subseteq L(a)$ for all $a \in R$, it follows that

$$T = (T \setminus R) \cup R \subseteq L(a) \subseteq T.$$

Thus, $T = L(a)$ for all $a \in R$. Hence, $\{a\}$ is a right base of T. Next, let A be a right base of T. To show that $a = b$ for all $a, b \in A$ suppose that there exists $a, b \in A$ such that $a \neq b$. Then $a, b \in A \subseteq R$. So, we obtain $T = L(a)$. Since $b \in T = L(a) = (a \cup TTa]$ we have $b \leqslant a$ or $b \in (TTa]$. If $b \leqslant a$, by Lemma 2.4, $b \leqslant_L a$. This contradicts to the condition (2) of Theorem 2.6. Thus, $b \in (TTa]$. By Lemma 2.5, $b = a$. This is a contradiction. Hence, $a = b$ for all $a, b \in A$. Therefore, every right base of T is singleton set. Conversely, assume that every right base of T is singleton set. To show that $T \setminus R = L^*$, it suffices to show $A \subseteq T \setminus R$ for all a proper left ideal A of T. Suppose that A is a proper left ideal of T such that $A \nsubseteq T \setminus R$. Then there exists $x \in A$ such that $x \notin T \setminus R$ i.e., $x \in R$. Since $x \in A$, it follows that $L(x) \in A$. Since $x \in R$, by assumption, $T = L(x)$ and so $T = L(x) \subseteq A \subset T$. Thus, $T = A$. This is a contradiction. Hence, $A \subseteq T \setminus R$. Therefore, $T \setminus R = L^*$.

(1) $\Leftrightarrow$ (3). Assume that $T \setminus R$ is a maximal proper left ideal of T. To show that $T \setminus R = L^*$. Let A be a left ideal of T such that $A \nsubseteq T \setminus R$. Then there exists $x \in A \cap R$. By Theorem 2.13, we have $R \subseteq L(x) \subseteq A$. Thus, $A = R \cup B$ for some $B \subseteq T \setminus R$. For any $a \in T$, there exists $b \in R$ such that $a \leqslant_L b$. Since $b \in R$, then $L(b) \in R$. Thus, $a \in L(a) \subseteq L(b) \subseteq R \subseteq A$. Hence, $T = A$. Therefore, $T \setminus R = L^*$. The converse statement is obvious. □

Theorem 2.15. *Let R be the union of all right bases of a ternary po-semigroup T such that $\varnothing \neq R \subset T$. If $T \setminus R$ is a maximal proper left ideal of T, then one of the following conditions holds:*

(1) $(TTA] = T$ *(i.e., $L(A) = (TTA]$) for every right base A of T;*

(2) *there is unique a right base A of T such that $A \subseteq T \setminus (TTA]$.*

Proof. Assume that $T \setminus R$ is a maximal proper left ideal of T and suppose that the condition (1) is false. By Theorem 2.14, we have a right base $A = \{a\}$ of T and $(TTA] \neq T$. If $a \in (TTa]$, then $(a] \subseteq ((TTa]] = (TTa]$. So, we have $(TTa] = (a] \cup (TTa] = (a \cup TTa] = T$. This is a contradiction. Thus, $a \notin (TTa]$. Hence, $A \subseteq T \setminus (TTA]$. Next, suppose that T contains at least two right bases, $A_1 = \{a_1\}$, $A_2 = \{a_2\}$ such that $a_1 \notin (TTa_1]$,$a_2 \notin (TTa_2]$ and $a_1, a_2 \in R$. We claim that $\{a_1\} = (a_1]$. Suppose that $b \in T \setminus A_1$ such that $b \in (a_1]$. Then $b \leqslant a_1$, by Lemma 2.4, we have $b \leqslant_L a_1$. Thus, $b \in L(b) \subseteq L(a_1) \subseteq L(A_1)$. Clearly, if $x \in T \setminus A_1$ such that $x \notin (a_1]$, then $x \in L(A_1)$. So, we obtain $T \setminus A_1 \subseteq L(A_1)$. Since $A_1 \subseteq L(A_1)$ and $T \setminus A_1 \subseteq L(A_1)$, we have $T \setminus L(A_1) \subseteq T \setminus A_1 \subseteq L(A_1)$. This is a contradiction. Thus, $\{a_1\} = (a_1]$. Since $A_1 \subseteq R$, we have

$$T \setminus R \subseteq T \setminus A_1 = (a_1 \cup TTa_1] \setminus \{a_1\} = ((a_1] \cup (TTa_1]) \setminus (a_1] = (TTa_1].$$

Since $a_2 \in T = (a_1 \cup TTa_1]$, then $a_2 \in (TTa_1]$. Thus, $T \setminus R \subset (TTa_1]$. This contradicts to the maximality of $T \setminus R$. Hence, there is unique a right base A of T such that $A \subseteq T \setminus (TTA]$. □

Acknowledgment. The authors would like to thank the referees for their valuable suggestions which lead to an improvement of this paper.

References

[1] **G. Čupona and N. Celakoski**, *On representation of n-associatives into semigroups*, Maced. Acad. Sci. and Arts, Contribution, **VI-2** (1974), 23 – 34.

[2] **I. Fabrici**, *One-sided bases of semigroups*, Matematicky Casopis, **22** (1972), no. 4, 286 – 290.

[3] **A. Iampan**, *Characterizing the minimality and maximality of ordered lateral ideals in ordered ternary semigroups*, J. Korean Math. Soc., **46** (2009), no. 4, 775 – 784.

[4] **S. Kar, A. Roy and I. Dutta**, *On regularities in po-ternary semigroups*, Quasigroups Related Syst., **28** (2020), 149 – 158.

[5] **E. Kasner**, *An extension of the group concept* (repoted by L.G. Weld) Bull. Amer. Math. Soc., **10** (1904), 290 – 291.

[6] **T. Tamura**, *One sided-bases and translation of a semigroup*, Math. Japan., **3** (1955), 137 – 141.

[7] **B. Thongkam and T. Changphas**, *On one-sided bases of a ternary semigroup*, Int. J. Pure Appl. Math., **103** (2015), no. 3, 429 – 437.

Received November 23, 2021

W. Jantanan and N. Raikham
Department of Mathematics, Faculty of Science, Buriram Rajabhat University, Muang, Buriram, 31000 Thailand
E-mail: wichayaporn.jan@bru.ac.th (W. Jantanan), nateeraikham04@gmail.com (N. Raikham)

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

Quasigroups and Related Systems **30** (2022), 219 – 240

Projective finitely supported M-sets

Khadijeh Keshvardoost and Mahdieh Haddadi

Abstract. The purpose of this paper is to provide simple characterizations of the projective objects in the category of finitely supported M-sets. To do so, first, we introduce the notion of zero-retraction monoid and then characterize projective finitely supported M-sets where M contains a zero-retraction monoid.

1. Introduction

Take $\mathbb{D}$ to be a countable infinite set. A permutation over $\mathbb{D}$ is said to be finite if it changes only a finite number of elements of $\mathbb{D}$. Let $G = \mathrm{Perm}(\mathbb{D})$ be the group of finite permutations. A nominal set is a G-set such that for each element x one can find a finite set of $\mathbb{D}$ supporting x.

The notion of nominal sets (finitely supported G-sets) was introduced by Fraenkel in 1922, and developed by Mostowski in the 1930s in order to prove the independence of the axiom of choice and other axioms in classical Zermelo-Fraenkel set theory. In computer science, nominal sets were used in order to properly model the syntax of formal systems involving variable-binding operations (cf. [5]). Nominal sets also have been used in game theory [1], Logic [10], topology [9] and in proof theory [13].

Pitts [12] generalized finite permutations to finite substitutions and introduced the monoid Cb. He has shown that this category is equivalent to a particular category of presheaves named cubical sets.

The question of projectivity, as the dual notion of injectivity, is one which arises in many areas of mathematics, and concerns the possibility of lifting a given morphism defined in to a structure through the epimorphisms.

A projective M-set, a set equipped with an action of a monoid (or a group) M, generalizes the concept of the free M-set (cf. [8]). In fact, a projective M-set is a retract of a free M-set. Indecomposable projective

2010 Mathematics Subject Classification: 20M30, 20B30, 20M35, 18B20, 18G05
Keywords: Finitely supported M-sets, nominal sets, projective S-sets, S-sets.

M-sets are cyclic (cf. Proposition 17.7.III, [8]). Also a characterization of a projective M-set in terms of indecomposable projective M-sets is given by Knauer (cf. Theorem 17.8.III, [8]).

Throughout the paper, $\mathbb{D}$ and $\mathrm{End}(\mathbb{D})$ are both fixed. The set $\mathbb{D}$ is an infinite countable set and $\mathrm{End}(\mathbb{D})$ is the monoid of all maps from $\mathbb{D}$ to itself with respect to composition. As we mentioned, a projective M-set is a retract of a free M-set. However in categories of finitely supported M-sets there exists no free finitely supported M-sets over sets (see Theorem 3.1). Here, we observe that although the category of nominal sets has no projective object (see Corollary 3.4), but projective finitely supported M-sets exist, in which M is a submonoid of $\mathrm{End}(\mathbb{D})$. In [8], it is proved that every singleton M-set is projective if and only if M contains some zero elements. This result fails in the category of finitely supported Cb-sets. The monoid Cb has no zero element (see Lemma 2.15) while every singleton Cb-set (which is also a finitely supported Cb-set) in the category of finitely supported Cb-sets is projective, by Proposition 3.5.

These facts motivate us to study projective finitely supported M-sets where M is a submonoid of $\mathrm{End}(\mathbb{D})$. We introduce the notion of zero-retraction monoids (Definition 3.6) and then we characterize projective finitely supported M-sets where M is a zero-retraction monoid. In fact, we consider those monoids to behave almost like Cb. Finally, using the functor introduced in [6], we characterize projective finitely supported N-sets where N contains a zero-retraction monoid M.

2. Preliminaries

In this section, the preliminary facts about (finitely supported) M-sets are given where $M \leqslant \mathrm{End}(\mathbb{D})$. For more information see [2, 3, 8, 12].

2.1 M-sets

An (left) *M-set* for a monoid M with identity $id_{\mathbb{D}}$ is a set X equipped with a map $M \times X \to X, (m, x) \rightsquigarrow mx$, called an *action* of M on X, such that $id_{\mathbb{D}}x = x$ and $m(m'x) = (mm')x$, for all $x \in X$ and $m, m' \in M$.

The set $\mathbb{D}$ is an M-set with the action given by $md = m(d)$ for all $m \in M$ and $d \in \mathbb{D}$.

The set $\mathbb{D}^k = \{(d_1, \ldots, d_k) : d_1, \ldots, d_k \in \mathbb{D}\}$ is an M-set with the action $m(d_1, \ldots, d_k) = (md_1, \ldots, md_k)$.

An *equivariant map* from an M-set X to an M-set Y is a map $f : X \to Y$ with $f(mx) = mf(x)$, for all $x \in X, m \in M$.

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

A subset Y of an M-set X is an *M-subset* of X if $my \in Y$, for all $m \in M$ and $y \in Y$. Given an M-set X, the set $\mathcal{Z}(X)$ is in fact an M-subset of X.

For the family $\{X_i\}_{i\in I}$ of M-sets, the cartesian product $\prod_{i\in I} X_i$ with the component wise action, $m(x_i)_{i\in I} = (mx_i)_{i\in I}$, is the product of X_i's in the category of M-sets. The coproduct of the family $\{X_i\}_{i\in I}$ is their disjoint union $\coprod_{i\in I} X_i = \bigcup_{i\in I}(X_i \times \{i\})$ with the action of M defined by $m(x, i) = (mx, i)$, for every $m \in M$ and $x \in X_i$.

An element $m \in M$ is called *idempotent* if $mm = m$.

An M-set X is *decomposable* if there exist two M-subsets Y, Z of X with $X = Y \cup Z$ and $Y \cap Z = \emptyset$. In this case $X = Y \cup Z$ is called a *decomposition* of X. An M-set X is called *indecomposable* if it has no decomposition.

Every M-set has a decomposition into indecomposable M-subsets (cf. Theorem 5.10.I, [8]).

A cyclic M-set X is an M-set which is generated by only one element. That is $X = Mx$, for some $x \in X$.

2.2 Projective M-sets

The following facts about projective M-sets are needed in the sequel. For more details see [8].

An M-set P is said to be *projective* if for each epimorphism (equivariant surjective map) $h : A \twoheadrightarrow B$ and each equivariant map $f : P \to B$, there exists an equivariant map $\varphi : P \to A$ with $h\varphi = f$.

Also, an M-subset A of an M-set B is called a *retract* of B if there exists an equivariant map $f : B \to A$ with $fi = id_A$, in this case, f is said to be a *retraction*.

Remark 2.1. (cf. Proposition 17.2.III, [8])

(1) A free M-set is projective.

(2) Any retract of a projective M-set is projective.

(3) Any monoid M is a free M-set.

Proposition 2.2. (cf. [8]) *Let X be an M-set. Then,*

(i) (Proposition 17.1.III) *X is projective if and only if $X = \coprod_{i\in I} X_i$, where X_i's are projective M-sets.*

(ii) (Theorem 17.8.III) *X is projective if and only if $X = \coprod_{i\in I} X_i$ with $X_i \cong Me$, where Me is a cyclic M-subset of M, and $e \in M$ is an idempotent element.*

(iii) (Proposition 17.4.III) *X is projective if and only if it is a retract of a free M-set.*

2.3 Finitely supported M-sets

In this subsection, we give some needed facts about finitely supported M-sets. For more information see [2, 12].

Definition 2.3. (cf. [12]) Suppose X is an M-set and $x \in X$.

(a) A subset $C \subseteq \mathbb{D}$ *supports* x if, for every $m, m' \in M$,

$$(m(c) = m'(c), (\forall c \in C)) \Rightarrow mx = m'x.$$

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

(b) If every element of X has a finite support, then X is called a *finitely supported M-set*.

(c) A subset $C \subseteq \mathbb{D}$ *strongly supports* x if, for every $m, m' \in M$,

$$(m(c) = m'(c), (\forall c \in C)) \Leftrightarrow mx = m'x.$$

We denote the category of all M-sets with equivariant maps between them by M-**Set**, and its full subcategory of all finitely supported M-sets by $(M\text{-}\mathbf{Set})_{\text{fs}}$.

Remark 2.4. Suppose $C \subseteq \mathcal{Z}(\mathbb{D})$ is a finite subset. If X is a finitely supported M-set and $x \in X$, then

(1) $B \subseteq \mathbb{D}$ supports x if and only if $B - C$ supports x.

(2) $B \subseteq C$ supports x if and only if x is a zero element.

Example 2.5. (1) A discrete M-set is a finitely supported M-set, because the empty set is a finite support for each element.

(2) For each M-set X, the set

$$X_{\text{fs}} = \{x \in X : x \text{ has a finite support in } X\},$$

is a finitely supported M-subset of X. Also, $\mathcal{Z}(X) = \mathcal{Z}(X_{\mathrm{fs}})$.

(3) The sets $\mathbb{D}$ and

$$\mathbb{D}^k = \{(d_1, \ldots, d_k) : d_1, \ldots, d_k \in \mathbb{D}\}$$

are finitely supported M-sets. In fact, $\{d\}$ is a finite support of d and $\{d_1, \ldots, d_k\}$ is a finite support for $(d_1, \ldots, d_k)$.

The following example shows that there exists an M-set which is not a finitely supported M-set.

Example 2.6. (Exercise 2.4, [11]) For each natural number k, let $X_k = \mathbb{D}$. Take the element $(x_k)_{k\in\mathbb{N}}$ in $A = \prod_{k\in\mathbb{N}} X_k$ such that for every $d \in \mathbb{D}$ there exists $k \in \mathbb{N}$ with $d = x_k$. Then, this element has no finite support. So, $A_{\mathrm{fs}} \neq A$.

Remark 2.7. (1) The product of a family of finitely supported M-sets X_i's is $(\prod_{i\in I} X_i)_{\mathrm{fs}}$.

(2) Coproducts in the category of finitely supported M-sets are constrcuted just as in the catgeory of M-sets. Hence, for a family of finitely supported M-sets X_i indexed by a set I, disjoint union of X_i's is the coproduct of them, and denoted by $\coprod_{i\in I} X_i$. For each element $t \in \coprod_{i\in I} X_i$, there exists $j \in I$ with $t \in X_j$. Hence, if S is a finite support of t in X_j, then S is a finite support of t in $\coprod_{i\in I} X_i$. For more details cf. Section 2.2, [12] and Chapter II, [8].

Definition 2.8. (cf. [2, 12]) Let X be a finitely supported M-set and $x \in X$. Then,

(a) x admits least support if the set $\bigcap\{C : C \text{ is a finite support of } x\}$ supports x. We denote the least support of $x \in X$ with $\operatorname{supp} x$.

(b) X admits least support if every $x \in X$ has the least support.

Remark 2.9. (1) For the given M-set X and $x \in X$, if C (strongly) supports x, then $m(C)$ (strongly) supports mx.

(2) Suppose $f : X \to Y$ is an equivariant map and $x \in X$. If C is a finite support of x, then C is a finite support of $f(x)$.

Definition 2.10. (a) A permutation (bijection map) $\pi : \mathbb{D} \to \mathbb{D}$ is said to be *finite* if $\{d \in \mathbb{D} \mid \pi(d) \neq d\}$ is finite. The set $\mathrm{Perm}(\mathbb{D})$ is the group of all finite permutations on $\mathbb{D}$.

(b) A finitely supported $\mathrm{Perm}(\mathbb{D})$-set X is called a *nominal set*.

Example 2.11. The set $\mathbb{D}^{(k)} = \{(d_1, \ldots, d_k) \in \mathbb{D}^k : (\forall i \neq j),\ d_i \neq d_j\}$ is a nominal set.

2.4 Finitely supported Cb-sets

We give some basic facts about the monoid Cb and finitely supported Cb-sets. For more information one can see [4, 7, 12].

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

Definition 2.12. (a) A map $\sigma : \mathbb{D} \to \mathbb{D} \cup \mathsf{2}$ is called an *injective finite substitution* if $\{d \in \mathbb{D} \mid \sigma(d) \neq d\}$ is finite and

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

(b) If $d \in \mathbb{D}$ and $b \in \mathsf{2}$, a basic substitution (b/d) maps d to b, and is the identity mapping on all the other elements of $\mathbb{D}$.

(c) If $d, d' \in \mathbb{D}$ then each transposition $(d\ d')$ is called a *transposition substitution.*

Definition 2.13. (a) The monoid Cb is the monoid whose elements are injective finite substitutions with the monoid operation given by $\sigma \cdot \sigma' = \hat{\sigma}\sigma'$, where $\hat{\sigma} : \mathbb{D} \cup \mathsf{2} \to \mathbb{D} \cup \mathsf{2}$ maps 0 to 0, 1 to 1, and on $\mathbb{D}$ is defined the same as σ. The identity element of Cb is the inclusion $\iota : \mathbb{D} \hookrightarrow \mathbb{D} \cup \mathsf{2}$.

(b) The subsemigroup of Cb generated by basic substitutions is denoted by S. Each element of S is of the form $\delta = (b_1/d_1) \cdots (b_k/d_k) \in S$ for some $d_i \in \mathbb{D}$ and $b_i \in \mathsf{2}$, and we denote the set $\{d_1, \ldots, d_k\}$ by $\mathbb{D}_\delta$.

Theorem 2.14. (Theorem 2.4, [7]) *For the monoid Cb, we have*

$$Cb = \mathrm{Perm}(\mathbb{D})(S \cup \{\iota\}).$$

Lemma 2.15. *The monoid Cb (as a Cb-set) has no zero element.*

Proof. On the contrary, assume that there exists a zero element $\sigma' \in Cb$. We must show that $\sigma\sigma' = \sigma'$, for all $\sigma \in Cb$. By Theorem 2.14, $\sigma' \in \mathrm{Perm}(\mathbb{D})$ or $\sigma' \in \mathrm{Perm}(\mathbb{D})S$. For the first case, let $\sigma = (\mathsf{0}/d)$. Then,

$$d = \sigma'(\sigma'^{-1}d) = \sigma\sigma'(\sigma'^{-1}d) = \sigma d = (\mathsf{0}/d)d = \mathsf{0},$$

which is a contradiction. Now, suppose $\sigma' \in \mathrm{Perm}(\mathbb{D})S$. So, there exist $\pi' \in \mathrm{Perm}(\mathbb{D})$ and $\delta' \in S$ with $\sigma' = \pi'\delta'$. Let $\sigma = (\mathsf{0}/d)\pi'^{-1}$ with $d \notin \mathbb{D}_{\delta'}$. Then,

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

which is impossible. □

Proposition 2.16. (i) (Lemma 2.4, [12]) *Suppose X is a Cb-set, $x \in X$ and $b \in 2$. Also, let C be a finite subset of $\mathbb{D}$. Then, C is a support of x if and only if*

$$(\forall d \in \mathbb{D}) \quad d \notin C \Rightarrow (b/d)x = x.$$

(ii) *The set $\{d \in \mathbb{D} : (0/d)x \neq x\}$ is the least finite support of x.*

Lemma 2.17. (cf. Lemma 3.4, [4]) *Let X be a Cb-set and $x \in X$. Then,*

(i) *$S_x = \{\delta \in S \mid \delta x \neq x\}$ and $S'_x = S - S_x$ are two subsemigroups of S.*

(ii) *If x has the least finite support, then $\operatorname{supp} \delta x \subseteq (\operatorname{supp} x) \setminus \mathbb{D}_\delta$, for all $\delta \in S'_x$.*

(iii) *Let $\delta \in S$. Then, $\delta x \neq x$ if and only if $\mathbb{D}_\delta \cap \operatorname{supp} x \neq \emptyset$.*

Remark 2.18. Let $\delta, \delta' \in S$. Then, $\delta = \delta'$ if and only if $\mathbb{D}_\delta = \mathbb{D}_{\delta'}$ with $\delta(d) = \delta'(d)$, for all $d \in \mathbb{D}_\delta$.

Lemma 2.19. (Lemma 4.5, [4]) *Let Cbx be a cyclic finitely supported Cb-set. Then, $Cbx = \operatorname{Perm}(\mathbb{D})S'_x x \cup \operatorname{Perm}(\mathbb{D})x$.*

3. Projective finitely supported M-sets

In this section, we give a characterization of projective finitely supported M-sets, where M is a zero-retraction monoid. To do so, first we show that although free objects over sets do not exist in the categories of finitely supported Cb-sets and nominal sets, but this is not true about projectivity. In fact, we show that the singleton finitely supported Cb-sets are projective while no nominal sets are projective. This fact happens because of a property of finite substitutions in Cb. So then we generalize this property and introduce the notion of zero-retraction monoids. Then, using this notion we find the projective finitely supported M-sets when M is a zero-retraction monoid or contains a zero-retraction monoid.

Let us begin this section with the following theorem which shows that, analogous to the categories nominal sets and Cb-sets, the forgetful functor

$$V : (M\text{-}\mathbf{Set})_{\text{fs}} \to \mathbf{Set}$$

has no left adjoint and so free finitely supported M-sets over sets do not exist.

Theorem 3.1. *The forgetful functor $V : (M\text{-}\mathbf{Set})_{\text{fs}} \to \mathbf{Set}$ has no left adjoint.*

Proof. Let L be a left adjoint of V. Then, since right adjoints preserves limits, we get that V preserves arbitrary products. Consider the finitely supported M-set A_{fs} in Example 2.6. So, $V(A_{\text{fs}}) = A_{\text{fs}}$ is the product of the family of X_k's. But, the product of X_k's is A. □

Corollary 3.2. *No free finitely supported M-sets exists over sets.*

Lemma 3.3. *No indecomposable nominal set is projective.*

Proof. Let X be indecomposable. Then $X = \text{Perm}(\mathbb{D})x$, for some $x \in X$. Notice that, indecomposable nominal sets are cyclic. Take k to be a natural number with $k > |\text{supp}\, x|$, $h : \mathbb{D}^{(k)} \to \{\theta\}$ to be a surjective constant equivariant map, and $f : X \to \{\theta\}$ is an equivariant map. If X is projective, then there exists an equivariant map $\varphi : X \to \mathbb{D}^{(k)}$ with $h\varphi = f$. Now, we have $\varphi(x) = (d_1, \ldots, d_k) \in \mathbb{D}^{(k)}$. Since φ is equivariant, we get that $\text{supp}\, \varphi(x) \subseteq \text{supp}\, x$. Thus, $k = |\{d_1, \ldots, d_l\}| \leqslant |\text{supp}\, x|$ which is a contradiction. □

Corollary 3.4. *No nominal set is projective.*

Proof. Follows from Proposition 2.2(i). □

Proposition 3.5. *The singleton finitely supported Cb-set $\{\theta\}$ is projective.*

Proof. Suppose $h : A \to B$ is a surjective equivariant map. Take $f : \{\theta\} \to B$ to be an equivariant map with $f(\theta) = \theta' \in \mathcal{Z}(B)$. Notice that, finitely supported Cb-sets have zero elements. We show that there exists an equivariant map $\varphi : \{\theta\} \to A$ with $h\varphi = f$. Since h is surjective, there exists $a \in A$ with $h(a) = \theta'$. If $a \in \mathcal{Z}(A)$, then define $\varphi(\theta) = a$, and so, $h\varphi(\theta) = h(a) = \theta' = f(\theta)$. If $\text{supp}\, a \neq \emptyset$, then take $\delta \in S$ with $\mathbb{D}_\delta = \text{supp}\, x$. Now, by Lemma 2.17(ii), $\text{supp}\, \delta x = \emptyset$, and so, taking $\varphi(\theta) = \delta a$, we get that $h\varphi(\theta) = h(\delta a) = \delta h(a) = \delta\theta' = \theta' = f(\theta)$. □

3.1 Retraction-monoid

Definition 3.6. (a) Let A and B be two finite subsets of $\mathbb{D}$ with $A \subseteq B$. Then, A is called an *M-zero-retraction* of B if $A \cup \mathcal{Z}(\mathbb{D})$ is a retraction of B; that is there exists $m \in M$ with $m(B) \subseteq A \cup \mathcal{Z}(\mathbb{D})$ and $m|_A = id|_A$.

(b) A is an *absolutely M-zero-retraction* if A is an M-zero-retraction of every B that contains A; that is $A \subseteq B$.

The monoid M is called *zero-retraction*, if every finite subset A of $\mathbb{D}$ is an absolutely M-zero-retraction.

Proposition 3.7. *Let M be a zero-retraction monoid. Then,*

(i) *$\mathcal{Z}(\mathbb{D})$ is non-empty.*

(ii) *There exists $C \subseteq \mathcal{Z}(\mathbb{D})$ such that $m|_C = id|_C$, for every $m \in M$. In other words, M is a submonoid of M_C where*

$$M_C = \{m \in \mathrm{End}(\mathbb{D}) : m|_C = id|_C\},$$

for some $C \subseteq \mathcal{Z}(\mathbb{D})$.

Proof. (i). Suppose $B \subseteq \mathbb{D}$ is a non-empty finite subset. Notice that, $m(B) \neq \emptyset$, for every $m \in M$. Since M is zero-retraction and $\emptyset \subseteq B$, there exists $m_0 \in M$ with $m_0(B) \subseteq \mathcal{Z}(\mathbb{D})$. Now, since $m_0(B) \neq \emptyset$, we get $\mathcal{Z}(\mathbb{D}) \neq \emptyset$.

(ii). By (i), $C = m_0(B) \subseteq \mathcal{Z}(\mathbb{D})$. Let $m \in M$. Then, $m|_C = id|_C$ and so $m \in M_C$. □

Remark 3.8. (1) The nominal set $\mathbb{D}$ has no zero elements.

(2) The group $G = \mathrm{Perm}(\mathbb{D})$ is not a zero-retraction monoid. This is because, if $A \subsetneq B$ finite subsets of $\mathbb{D}$ and there exists $\pi \in G$ with $\pi(B) \subseteq A$, then $A = B$ which is a contradiction.

(3) The monoid Cb is a zero-retraction monoid (cf. Lemma 4.1). Notice that, $\mathcal{Z}(\mathbb{D}) = 2$.

3.2 Finitely supported $\mathbb{D}^A$

The following example plays an important role in characterizing projective finitely supported M-sets.

For a finite subset A of $\mathbb{D}$, the set $\mathbb{D}^A = \{m|_A : m \in M\}$ is an M-set with the action defined by $m' * m|_A := (m'm)|_A$, for all $m, m' \in M$, where $* : M \times \mathbb{D}^A \to \mathbb{D}^A$ (cf. Example 2.4, [2]).

Lemma 3.9. *Let A be a finite subset of $\mathbb{D}$. Then, $\mathbb{D}^A$ is a cyclic finitely supported M-set.*

Proof. First we show that $m(A)$ is a finite support of $m|_A$. Indeed, if $m_1, m_2 \in M$ and $m_1(a) = m_2(a)$, for all $a \in m(A)$, then $m_1 m(d) = m_2 m(d)$, for all $d \in A$. Hence $(m_1 m)|_A = (m_2 m)|_A$, and so $m_1 * m|_A = m_2 * m|_A$.

Now we note that $\mathbb{D}^A = Mid|_A$. That is $\mathbb{D}^A$ is cyclic and we are done. □

Corollary 3.10. *The map $\varphi : M \to \mathbb{D}^A$ defined by $\varphi(m) = m|_A$ is a surjective equivariant map.*

Proposition 3.11. *Given a finitely supported M-set Y and a finite subset $A \subseteq \mathbb{D}$, there exists an equivariant map from $\mathbb{D}^A$ to Y if and only if A is a finite support of some $y \in Y$.*

Proof. Suppose $\varphi : \mathbb{D}^A \to Y$ is an equivariant map. Then, we consider $\varphi(id|_A) = y \in Y$. Since φ is equivariant, we get that A is a finite support of y, by Remark 2.9.

To prove the other part, it is sufficient to define $\varphi : \mathbb{D}^A \to Y$ by $\varphi(m|_A) = my$, where A is a finite support of y. □

Lemma 3.12. *Let $X = Mx$ be a cyclic finitely supported M-set and A be a finite support of x. Then, Mx is isomorphic to $\mathbb{D}^A$ if and only if A strongly supports x.*

Proof. First notice that if $A = \emptyset$, then $X \cong \mathbb{D}^\emptyset$. Let x be non-zero. Then, $\varphi : \mathbb{D}^A \to Mx$ defined by $\varphi(m|_A) = mx$ is a surjective equivariant map using Proposition 3.11. Now, φ is an injective map if and only if

$$(\forall m, m' \in M)\,(mx = m'x \Leftrightarrow m|_A = m'|_A)$$

if and only if A strongly supports x. □

3.3 Projective finitely supported M-sets

In this subsection, we take M to be a zero-retraction monoid and then characterize projective finitely supported M-sets.

Proposition 3.13. *If X is a finitely supported M-set, then X has some zero elements.*

Proof. First, notice that M is a submonoid of M_C, for some finite subset C of $\mathbb{D}$, by Proposition 3.7. Now suppose $x \in X$ and B is a finite support of x. The set $B - C$ is a support of x, by Remark 2.4(2). If $B - C = \emptyset$, then x is zero. If $\emptyset \subsetneq B - C$, then there exists $m_0 \in M$ with $m_0(B - C) \subseteq \mathcal{Z}(\mathbb{D})$. By Remark 2.9(1), $m_0(B - C)$ is a finite support of $m_0 x$. Thus, $m_0 x \in \mathcal{Z}(X)$, by Remark 2.4(2). □

The following lemma is the key to show that cyclic finitely supported M-sets $\mathbb{D}^A$ are projective (see Lemma 3.16).

Lemma 3.14. *Suppose $f : X \to Y$ is an equivariant map between finitely supported M-sets, and A is a finite support of $f(x)$, for some $x \in X$. Then, there exists $m \in M$ with $f(mx) = f(x)$ such that A is a finite support of mx.*

Proof. Let A be a finite support of $y = f(x)$. Then, by Remark 2.4(2), $A_1 = A - \mathcal{Z}(\mathbb{D})$ supports y. If A_1 supports x, then taking $m = id$ we get the result. Otherwise, take $B_1 = B - \mathcal{Z}(\mathbb{D})$ to be a finite support of x. So, $A_1 \subseteq A_1 \cup B_1$ and since M is a zero-retraction monoid, there exists $m \in M$ with $[m(A_1 \cup B_1)] \subseteq A_1 \cup \mathcal{Z}(\mathbb{D})$ and $m|_{A_1} = id|_{A_1}$. Since $m(A_1 \cup B_1)$ supports mx, we have $A_1 \cup \mathcal{Z}(\mathbb{D})$ supports mx and so A_1 supports mx, by Remark 2.4(2). Also, $m|_{A_1} = id|_{A_1}$ implies that $f(mx) = mf(x) = f(x) = y$. □

As a result of Lemma 3.14, we have the following corollary for finitely supported M-sets admit least supports.

Corollary 3.15. *Let $f : X \to Y$ be an equivariant map between finitely supported M-sets admit least supports. Then, for every $y \in f(X)$ there exist $x \in X$ and $m \in M$ with $f(mx) = y$ and $\operatorname{supp} y = \operatorname{supp} mx$.*

Proof. Let $y = f(x)$, for some $x \in X$. Since f is equivariant, we have $\operatorname{supp} y \subseteq \operatorname{supp} x$. Since M is zero-retraction, there exists $m_0 \in M$ with $m_0(\operatorname{supp} x) \subseteq \operatorname{supp} y \cup \mathcal{Z}(\mathbb{D})$ and $m_0|_{\operatorname{supp} y} = id|_{\operatorname{supp} y}$. Now, $f(m_0 x) = m_0 y = y$. Also, $\operatorname{supp} y \subseteq \operatorname{supp} m_0 x \subseteq [m_0(\operatorname{supp} x) - \mathcal{Z}(\mathbb{D})] \subseteq \operatorname{supp} y$ implies that $\operatorname{supp} m_0 x = \operatorname{supp} y$. □

Lemma 3.16. *If A is a finite subset of $\mathbb{D}$, then $\mathbb{D}^A$ is a projective finitely supported M-set.*

Proof. Let $f : X \to Y$ be a surjective equivariant map and $g : \mathbb{D}^A \to Y$ be an equivariant map. Then, we show that there exists an equivariant map $\varphi : \mathbb{D}^A \to X$ with $f\varphi = g$. To do so, applying Proposition 3.11, we find an element in X such that A supports it. We have $g(id|_A) \in Y$ and f is surjective. So, there exists $x \in X$ with $f(x) = g(id|_A)$. Since g is equivariant and $A = id(A)$ is a finite support of $id|_A$, we get that A is a finite support of $g(id|_A)$. Hence, by Lemma 3.14, there exists $m_0 \in M$ with $f(m_0 x) = g(id|_A)$ and A supports $m_0 x$. Therefore, $\varphi(m|_A) = m m_0 x$ is a required equivariant map by Proposition 3.11. Also,

$$f\varphi(m|_A) = f(m m_0 x) = m f(m_0 x) = m g(id|_A) = g(m|_A).$$

This completes the proof. □

Corollary 3.17.

(i) *Every singleton finitely supported M-set is projective.*

(ii) *Every discrete finitely supported M-set is projective.*

Proof. (i). $\mathbb{D}^{\emptyset}$ is isomorphic to a singleton finitely supported M-set.

(ii). Follows from (i) and Proposition 2.2(i). □

Theorem 3.18. *Suppose X is a finitely supported M-set. Then, there exists a surjective equivariant map from $P = \coprod_{x\in X} \mathbb{D}^{A_x}$ to X, where A_x is a finite support of x.*

Proof. For each element $x \in X$, take A_x to be a finite support of x. Then, by Proposition 3.11 there exists an equivariant map $\varphi_x : \mathbb{D}^{A_x} \to X$ with $\varphi_x(m|_{A_x}) = mx$. Now, the universal property of coproduct, ensures that there exists a unique equivariant map $\varphi : P \to X$ by $\varphi(a) = \varphi_x(a)$, for every $a \in \mathbb{D}^{A_x}$. Also, for each $x \in X$, there exists an element $id|_{A_x} \in \mathbb{D}^{A_x}$ with $\varphi(id|_{A_x}) = \varphi_x(id|_{A_x}) = x$ which means that φ is surjective. □

Lemma 3.19. *Let X be a finitely supported M-set. Then, there exists a projective finitely supported M-set P such that X is a surjective equivariant image of P.*

Proof. If $X = Z(X)$, then by Corollary 3.17(ii), X is projective, and so, in this case $P = X$. If X is non-discrete, then applying Lemma 3.16, Proposition 2.2(i), and Theorem 3.18 we get the result. □

Lemma 3.20. *Let X be a finitely supported M-set. Then, X is indecomposable and projective if and only if X is cyclic and $X \cong \mathbb{D}^A$, for some finite subset $A \subseteq \mathbb{D}$.*

Proof. Necessity. First, notice that, applying Theorem 3.18 there exists a surjective equivariant map $\varphi : P \to X$, where $P = \coprod_{x\in X} \mathbb{D}^{A_x}$ and $\varphi|_{\mathbb{D}^{A_x}} = \varphi_x : \mathbb{D}^{A_x} \to X$. Now since X be projective, there exists an equivariant map $\psi : X \to P$ such that $\varphi\psi = id_X$, where $id_X : X \to X$. Thus, $\varphi\psi(X) = X$. Since X is indecomposable, we have $\psi(X) \subseteq \mathbb{D}^{A_x}$, for some $x \in X$. Now, $X = \varphi\psi(X) \subseteq \varphi(\mathbb{D}^{A_x}) \subseteq X$, and so, $M\varphi(id|_{A_x}) = \varphi(\mathbb{D}^{A_x}) = X$ which means that X is cyclic. Notice that, $X = M\varphi(id|_{A_x}) = M\varphi_x(id|_{A_x}) = \mathbb{D}^{A_x}$. Also, since ψ is an injective equivariant map, we get that

$$X \cong \psi(X) = \psi(\mathbb{D}^{A_x}) = M\psi\varphi(id|_{A_x}) = M\psi(id|_{A_x}) = \mathbb{D}^{A_x}.$$

Sufficiency. Follows from Lemma 3.9 and Lemma 3.16. □

Theorem 3.21. *Let X be a finitely supported M-set. Then, X is projective if and only if $X = \coprod_{i\in I} X_i$, where every X_i is isomorphic to $\mathbb{D}^A$, for some finite subset A.*

Proof. Suppose X is projective. Take $X = \coprod X_i$ to be a coproduct of indecomposable finitely supported M-sets X_i. Then, since each X_i has a zero element, it is a retract of X. So, by Remark 2.1(2), we get that X_i's are projective. Now, applying Theorem 3.20, every X_i is isomorphic to $\mathbb{D}^A$, for some finite subset A.

To prove the other side, by Lemma 3.16, cyclic $\mathbb{D}^A$'s are projective, and so, every X_i is projective. Now, applying Proposition 2.2(i), any coproduct of projective finitely supported M-sets is projective. □

Corollary 3.22. *Every projective finitely supported M-set is a surjective equivariant image of a free M-set.*

Proof. Let X be a projective finitely supported M-set. Then, by Theorem 3.21, we get that $X \cong \coprod_{x\in X} \mathbb{D}^{A_x}$, where A_x supports x. On the other hand, by Corollary 3.10, for every $x \in X$ there exists a surjective equivariant map $\varphi_x : M \to \mathbb{D}^{A_x}$. Now, the map $\varphi : \coprod_{x\in X} M \to \coprod_{x\in X} \mathbb{D}^{A_x}$ defined by $\varphi(m) = \varphi_x(m)$ for some $x \in X$ and $m \in M$ is a required surjective equivariant map. □

4. Projective finitely supported Cb-sets

The monoid Cb is isomorphic to a submonoid of $\mathrm{End}(\mathbb{D})$. It is sufficient to take two fixed elements $a, b \in \mathbb{D}$ instead of $\mathsf{0}$ and $\mathsf{1}$ and replace $\mathbb{D}$ with $\mathbb{D} - \{a, b\}$. Then, by the same scheme of Pitts, one can get a submonoid of $\mathrm{End}(\mathbb{D})$ isomorphic to Cb. As an example of a zero-retraction monoid, we can mention the monoid Cb.

Lemma 4.1. *The monoid Cb is a zero-retraction monoid.*

Proof. Suppose $A \subseteq B$ are two finite subsets of $\mathbb{D}$. If $A = B$ or $B = \emptyset$, then $\iota(B) - \mathsf{2} = \iota(B) = \iota(A) = A$.

If $A \subsetneq B$ and $A = \emptyset$, then take $\delta \in S$ with $\mathbb{D}_\delta = B$. So, $\delta(B) - \mathsf{2} = \emptyset = A$.

If $A \subsetneq B$ and $A \neq \emptyset$, then take $\delta \in S$ with $\mathbb{D}_\delta = B - A$. Hence $\delta(B) = A \cup \mathsf{2}$ and so $\delta(B) - \mathsf{2} = A$ and $\delta|_A = id|_A$. □

Lemma 3.15 holds in the category of finitely supported Cb-sets. In the following proposition we prove it more specifically.

Proposition 4.2. *Suppose X and Y are two finitely supported Cb-set. If $f : X \to Y$ is an equivariant map, then for every $y \in f(X)$ there exists $x \in X$ with* $\operatorname{supp} x = \operatorname{supp} y$.

Proof. Let $y \in f(X)$. Then, there exists $x \in X$ with $y = f(x)$. If $\operatorname{supp} x = \emptyset$, then $\operatorname{supp} y = \emptyset$. Suppose $x \in X$ with $\operatorname{supp} x \neq \emptyset$. If $\operatorname{supp} x = \operatorname{supp} y$, then we get the result. If $\operatorname{supp} x \subsetneq \operatorname{supp} y$, then take $\delta_0 \in S$ with $\mathbb{D}_{\delta_0} = (\operatorname{supp} y) - \operatorname{supp} x$. Thus $\delta_0 x = x$ and so $\operatorname{supp} x \subseteq \operatorname{supp} \delta_0 y$. On the other hand, $\operatorname{supp} y = (\operatorname{supp} y - \operatorname{supp} x) \cup \operatorname{supp} x = \mathbb{D}_{\delta_0} \cup \operatorname{supp} x$. So, $\operatorname{supp} \delta_0 y \subseteq \operatorname{supp} y - \mathbb{D}_{\delta_0} = \operatorname{supp} x$. □

4.1 Max-zero cyclic finitely supported Cb-sets

In this subsection, we construct a particular cyclic finitely supported Cb-set, and show that it is isomorphic to a finitely supported Cb-set $\mathbb{D}^A$, for some finite subset $A \subseteq \mathbb{D}$.

First, we give the following needed remark and lemma.

Remark 4.3. Let Cbx be a non-singleton cyclic finitely supported Cb-set. Then,

(1) The Cb-subset $\mathcal{Z}(Cbx)$ of Cbx is a subset of $S'_x x$. This is because, by Lemma 2.19, we have $\mathcal{Z}(Cbx) \cap \operatorname{Perm}(\mathbb{D})x = \emptyset$.

(2) If $\delta \in S'_x$ with $\mathbb{D}_\delta = \operatorname{supp} x$, then, by Lemma 2.17(ii), we get that $\operatorname{supp} \delta x \subseteq (\operatorname{supp} x) - \mathbb{D}_\delta = \emptyset$. So, $\delta x \in \mathcal{Z}(Cbx)$.

(3) If $\delta \in S'_x$, then there exists $\delta' \in S'_x$ such that $\mathbb{D}_{\delta'} \subseteq \operatorname{supp} x$ and $\delta x = \delta' x$. Furthermore, $\operatorname{supp} x \setminus \mathbb{D}_\delta = \operatorname{supp} x - \mathbb{D}_{\delta'}$. To show this, let $\delta \in S'_x$. Then, $\mathbb{D}_\delta \cap \operatorname{supp} x \neq \emptyset$. Suppose $\delta = \delta_1 \delta_2$ with $\mathbb{D}_{\delta_2} = \mathbb{D}_\delta \cap \operatorname{supp} x \subseteq \operatorname{supp} x$ and $\mathbb{D}_{\delta_1} \cap \operatorname{supp} x = \emptyset$. Then, $\delta x = \delta_2 x$. Now, we show that $\operatorname{supp} x - \mathbb{D}_\delta = \operatorname{supp} x - \mathbb{D}_{\delta'}$. Notice that, since $\mathbb{D}_{\delta_1} \cap \operatorname{supp} x = \emptyset$, we get that $\operatorname{supp} x - \mathbb{D}_{\delta_1} = \operatorname{supp} x$. So,

$$\operatorname{supp} x - \mathbb{D}_\delta = \operatorname{supp} x - (\mathbb{D}_{\delta_1} \cup \mathbb{D}_{\delta_2}) = (\operatorname{supp} x - \mathbb{D}_{\delta_1}) - \mathbb{D}_{\delta_2} = \operatorname{supp} x - \mathbb{D}_{\delta_2}.$$

Proposition 4.4. *Suppose X is a finitely supported Cb-set and $x \in X$. Let $\sigma, \sigma' \in Cb$ with $\sigma x = \sigma' x$. Then,*

(i) $\sigma, \sigma' \in \operatorname{Perm}(\mathbb{D}) \cup \operatorname{Perm}(\mathbb{D}) S_x$ *or* $\sigma, \sigma' \in \operatorname{Perm}(\mathbb{D}) S'_x$.

(ii) *there exists* $\pi \in \operatorname{Perm}(\mathbb{D})$ *with* $\pi x = x$ *or there exist* $\delta, \delta' \in S'_x$ *and* $\pi \in \operatorname{Perm}(\mathbb{D})$ *with* $\pi \delta x = \delta' x$.

Proof. (i). Since $S_x \cap S'_x = \emptyset$, it is sufficient to prove if $\sigma \in \mathrm{Perm}(\mathbb{D})S'_x$, then $\sigma' \in \mathrm{Perm}(\mathbb{D})S'_x$ and vice versa. Let $\sigma x = \sigma' x$ with $\sigma \in \mathrm{Perm}(\mathbb{D})S'_x$. Then, $\sigma = \pi\delta$, and so, by Lemma 2.17, we get that

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

Now, if $\sigma' \in \mathrm{Perm}(\mathbb{D}) \cup \mathrm{Perm}(\mathbb{D})S_x$, then $|\mathrm{supp}\,\sigma' x| = |\mathrm{supp}\,x|$, which is impossible.

(ii). By (i), we get $\sigma, \sigma' \in \mathrm{Perm}(\mathbb{D}) \cup \mathrm{Perm}(\mathbb{D})S_x$ or $\sigma, \sigma' \in \mathrm{Perm}(\mathbb{D})S'_x$. If $\sigma, \sigma' \in \mathrm{Perm}(\mathbb{D})S'_x$, then $\sigma = \pi_1\delta$ and $\sigma' = \pi_2\delta'$, and so, we get that $\pi_1\delta x = \pi_2\delta' x$. In this case, taking $\pi_2^{-1}\pi_1 = \pi$, we have $\pi\delta x = \delta' x$.

Notice that, if $\sigma \in \mathrm{Perm}(\mathbb{D})S_x$, then $\sigma x = \pi\delta x = \pi x$. So, if both $\sigma, \sigma' \in \mathrm{Perm}(\mathbb{D}) \cup \mathrm{Perm}(\mathbb{D})S_x$, then $\sigma x = \pi x$, and $\sigma' x = \pi' x$ which means that $\pi x = \pi' x$. Thus, $\pi_1 x = x$ where $\pi_1 = \pi'^{-1}\pi$. □

Remark 4.5. (1) For given $c_1, \ldots, c_k \in \{0, 1\}$, the decimal number is denoted by $(c_k c_{k-1} \cdots c_1)_2$ and computed as $c_k \times 2^{k-1} + c_{k-1} \times 2^{k-2} + \cdots + c_2 \times 2^1 + c_1 \times 2^0$.

(2) If $(c_k c_{k-1} \cdots c_1)_2 = (c'_k c'_{k-1} \cdots c'_1)_2$, then $c_i = c'_i$, for all $i = 1, \ldots, k$.

Note. The substitutions $\mathsf{0} \neq \mathsf{1}$ are just symbols, and they do not belong to $\mathbb{D}$. In the following lemma, if b_i is the substitution $\mathsf{1}$, then take c_i to be the natural number 1, and if $b_i = \mathsf{0}$, then take c_i to be the zero number 0, for all $i = 1, \ldots, k$.

Lemma 4.6. *Suppose X is a finitely supported Cb-set with $x \in X$. Let* $\mathrm{supp}\,x = \{d_1, \ldots, d_k\}$ *and* $b_1, \ldots, b_k \in \mathsf{2}$. *Take* $A = \{0, 1, 2, 3, \ldots, 2^{k-1}, x\}$ *to be a set with* 2^{k+1} *elements. Define map* $g_x : Cb \to A$ *by*

$$g_x(\sigma) = \begin{cases} (c_k c_{k-1} \cdots c_1)_2, & \text{if} \quad \sigma \in Cb(b_1/d_1) \cdots (b_k/d_k) \\ x, & \text{if} \qquad\qquad\qquad \text{otherwise.} \end{cases}$$

Then, $\mathrm{supp}\,g_x = \mathrm{supp}\,x$.

Proof. First applying Proposition 2.16, we show that $(0/d)\,g_x = g_x$, for all $d \notin \mathrm{supp}\,x$. In fact, we show that $((0/d)g_x)(\sigma) = g_x(\sigma)$, for all $\sigma \in Cb$. Suppose $\sigma \in Cb$.

If $\sigma \notin Cb(b_1/d_1) \cdots (b_k/d_k)$, then $\sigma(0/d) \notin Cb(b_1/d_1) \cdots (b_k/d_k)$, because otherwise if $\sigma(0/d) = \sigma'(b_1/d_1) \cdots (b_k/d_k)$, then

$$\hat{\sigma}(d_i) = (\hat{\sigma}(0/d))(d_i) = \hat{\sigma'}(b_1/d_1) \cdots (b_k/d_k)(d_i) \in \mathsf{2},$$

for all $d_i \in \{d_1, \ldots, d_k\}$. This implies that $\sigma \in Cb(b_1/d_1)\cdots(b_k/d_k)$, which is impossible. Thus, in this case, for all $\sigma \in Cb$, we get that

$$((0/d)g_x)(\sigma) = g_x(\sigma(0/d)) = x = g_x(\sigma).$$

Now, let $\sigma \in Cb(b_1/d_1)\cdots(b_k/d_k)$. Then, for some $\sigma_1 \in Cb$, we have $\sigma = \sigma_1(b_1/d_1)\cdots(b_k/d_k)$. Hence,

$$\begin{aligned}\sigma(0/d) &= \sigma_1(b_1/d_1)\cdots(b_k/d_k)(0/d)\\ &= \sigma_1(0/d)(b_1/d_1)\cdots(b_k/d_k) \in Cb(b_1/d_1)\cdots(b_k/d_k),\end{aligned}$$

and so, $g_x(\sigma(0/d)) = g_x(\sigma)$.

Therefore, $g_x \in (A^{Cb})_{\text{fs}}$, and so $\operatorname{supp} g_x \subseteq \operatorname{supp} x$.

Now, we show that $\operatorname{supp} x \subseteq \operatorname{supp} g_x$. To prove this, by Proposition 2.16, first, we prove that $(0/d)\, g_x \neq g_x$, for all $d \in \operatorname{supp} x$.

Let $\alpha = (0/d_1)\cdots(0/d_{i-1})(1/d_i)(0/d_{i+1})\cdots(0/d_k)$, and $d = d_i$. Then,

$$\begin{aligned}((0/d_i)g_x)(\alpha) &= g_x(\alpha(0/d_i))\\ &= g_x((0/d_1)\cdots(0/d_{i-1})(0/d_i)(0/d_{i+1})\cdots(0/d_k))\\ &= (0\cdots0)_2 = 0\\ &\neq 2^{i-1} = (0\cdots1\cdots0)_2\\ &= g_x(\alpha).\end{aligned}$$

Thus, $(0/d_i)g_x \neq g_x$. □

Remark 4.7. The element g_x in Lemma 4.6 belongs to $(A^{Cb})_{\text{fs}}$. Thus, Cbg_x is a Cb-subset of $(A^{Cb})_{\text{fs}}$.

In the following proposition, we give all needed information about Cbg_x.

Proposition 4.8. *Consider Cbg_x constructed in Lemma 4.6. The following statements hold:*

(i) *Suppose $\delta, \delta' \in S'_{g_x}$ with $\mathbb{D}_\delta = \mathbb{D}_{\delta'} = \operatorname{supp} g_x$. Then $\delta(d) = \delta'(d)$, if $\delta g_x = \delta' g_x$, for all $d \in \operatorname{supp} g_x$.*

(ii) *For all $\delta \in S'_{g_x}$, we have $\operatorname{supp} \delta g_x = (\operatorname{supp} g_x) - \mathbb{D}_\delta$.*

(iii) *For all $\delta \in S'_{g_x}$ with $\mathbb{D}_\delta \subsetneq \operatorname{supp} g_x$, we have $\delta g_x \notin Z(Cbg_x)$.*

(iv) *$\mathcal{Z}(Cbg_x) = \{\delta g_x : \mathbb{D}_\delta = \operatorname{supp} g_x\}$.*

(v) *Cbg_x has exactly 2^k zero elements.*

Proof. (i). On the contrary, suppose there exists some $d \in \operatorname{supp} g_x$ with $\delta(d) = 0 \neq 1 = \delta'(d)$. We show that $\delta g_x \neq \delta' g_x$. Let $\delta = (b_1/d_1)\cdots(0/d_k)$ and $\delta' = (b'_1/d_1)\cdots(b'_{k-1}/d_{k-1})(1/d_k)$. Then,

$$\delta g_x(\iota) = g_x(\iota\delta) = (0c_{k-1}\cdots c_0)_2 \neq (1c'_{k-1}\cdots c'_0)_2 = g_x(\iota\delta') = \delta' g_x(\iota).$$

(ii). Let $\delta \in S'_{g_x}$. Then, by Remark 4.3(3), there exists $\delta_1 \in S'_{g_x}$ with $\mathbb{D}_{\delta_1} \subseteq \operatorname{supp} g_x$ and $\delta g_x = \delta_1 g_x$. Also, $\operatorname{supp} g_x \setminus \mathbb{D}_\delta = \operatorname{supp} g_x - \mathbb{D}_{\delta_1}$. If $\mathbb{D}_{\delta_1} = \operatorname{supp} g_x$, then by Lemma 2.17(ii), $\operatorname{supp} \delta_1 g_x \subseteq (\operatorname{supp} g_x) - \mathbb{D}_{\delta_1} = \emptyset$. So, in this case, $\operatorname{supp} \delta g_x = \operatorname{supp} \delta_1 g_x = (\operatorname{supp} g_x) - \mathbb{D}_{\delta_1} = \operatorname{supp} g_x - \mathbb{D}_\delta$. Let $\mathbb{D}_{\delta_1} \subsetneq \operatorname{supp} g_x$. In this case, we also show that $\operatorname{supp} \delta g_x = (\operatorname{supp} g_x) - \mathbb{D}_\delta$. To prove this, it is sufficient to show that $\operatorname{supp} \delta_1 g_x = (\operatorname{supp} g_x) - \mathbb{D}_{\delta_1}$. On the contrary, suppose the equality does not hold. Take $\delta'_1, \delta'_2 \in S$ with $\mathbb{D}_{\delta'_1} = \mathbb{D}_{\delta'_2} = [(\operatorname{supp} g_x) - \mathbb{D}_{\delta_1})] - \operatorname{supp} \delta_1 g_x$, and $\delta'_1(d) \neq \delta'_2(d)$, for some $d \in \mathbb{D}_{\delta'_1}$. Then, $\delta'_1\delta_1 g_x = \delta_1 g_x = \delta'_2\delta_1 g_x$. We have the following cases;

Case (1): Suppose $\operatorname{supp} \delta_1 g_x \neq \emptyset$. Let $\delta_0 \in S$ with $\mathbb{D}_{\delta_0} = \operatorname{supp} \delta_1 g_x$. Then, $\mathbb{D}_{\delta_0\delta'_1\delta_1} = \operatorname{supp} g_x = \mathbb{D}_{\delta_0\delta'_2\delta_1}$. Now, since there exists some $d \in \mathbb{D}_{\delta'_1}$ with $\delta'_1(d) \neq \delta'_2(d)$, we get that $\delta_0\delta'_1\delta_1(d) \neq \delta_0\delta'_2\delta_1(d)$. So applying (i), we get that $\delta_0\delta'_1\delta_1 g_x \neq \delta_0\delta'_2\delta_1 g_x$ which is a contradiction. This is because the equality of $\delta'_1\delta_1 g_x = \delta_1 g_x = \delta'_2\delta_1 g_x$ implies that $\delta_0\delta'_1\delta_1 g_x = \delta_0\delta_1 g_x = \delta_0\delta'_2\delta_1 g_x$.

Case (2): Let $\operatorname{supp} \delta_1 g_x = \emptyset$. Then, $\mathbb{D}_{\delta'_1\delta_1} = \operatorname{supp} g_x = \mathbb{D}_{\delta'_2\delta_1}$. Now, since there exists some $d \in \mathbb{D}_{\delta'_1}$ with $\delta'_1(d) \neq \delta'_2(d)$, we get that $\delta'_1\delta_1(d) \neq \delta'_2\delta_1(d)$. So, applying (i), we get that $\delta'_1\delta_1 g_x \neq \delta'_2\delta_1 g_x$ which is a contradiction. This is because $\delta'_1\delta_1 g_x = \delta_1 g_x = \delta'_2\delta_1 g_x$.

(iii). Since $\mathbb{D}_\delta \subsetneq \operatorname{supp} g_x$, we get that $\operatorname{supp} g_x - \mathbb{D}_\delta \neq \emptyset$. Now, applying (ii), we have $\operatorname{supp} \delta g_x \neq \emptyset$, and so, $\delta g_x \notin \mathcal{Z}(Cbg_x)$.

(iv). Let $\mathcal{Z} = \{\delta g_x : \mathbb{D}_\delta = \operatorname{supp} g_x\}$. Then, we show that $\mathcal{Z} = \mathcal{Z}(Cbg_x)$. Let $a \in \mathcal{Z}$. Then, $a = \delta g_x$ with $\mathbb{D}_\delta = \operatorname{supp} g_x$. Thus, by Lemma 2.17(ii), $\operatorname{supp} \delta g_x \subseteq (\operatorname{supp} g_x) - \mathbb{D}_\delta = \emptyset$, and so, $\delta g_x \in \mathcal{Z}(Cbg_x)$. Now, let $a \in \mathcal{Z}(Cbg_x)$. Then, $a = \sigma g_x$ for some $\sigma \in Cb$. By Remark 4.3(1), $\sigma \in S'_{g_x}$. Thus, $a = \delta g_x$ where $\delta \in S'_{g_x}$. First, we show that $\mathbb{D}_\delta \subseteq \operatorname{supp} g_x$. Notice that, since $\delta \in S'_{g_x}$, applying Remark 4.3(3), there exists $\delta_1 \in S'_{g_x}$ with $\mathbb{D}_{\delta_1} \subseteq \operatorname{supp} g_x$ and $\delta g_x = \delta_1 g_x$. Also, $\operatorname{supp} g_x - \mathbb{D}_\delta = \operatorname{supp} g_x - \mathbb{D}_{\delta_1}$. If $\mathbb{D}_{\delta_1} \subsetneq \operatorname{supp} g_x$, then by part (iii), $\delta_1 g_x \notin \mathcal{Z}(Cbg_x)$. So, $\delta g_x \notin \mathcal{Z}(Cbg_x)$. Thus, $\mathbb{D}_{\delta_1} = \operatorname{supp} g_x$, and so, $\operatorname{supp} g_x - \mathbb{D}_\delta = \operatorname{supp} g_x - \mathbb{D}_{\delta_1} = \emptyset$. Therefore,

$\mathbb{D}_\delta \subseteq \operatorname{supp} g_x$. Now, if $\mathbb{D}_\delta \subsetneq \operatorname{supp} g_x$, then using part (iii) we get that $\delta g_x \notin \mathcal{Z}(Cbg_x)$ which is impossible. So, $\mathbb{D}_\delta = \operatorname{supp} g_x$.

(v). This follows by (iv). □

Lemma 4.9. *Let $\pi\delta_1 g_x = \delta_2 g_x$ where $\mathbb{D}_{\delta_1}, \mathbb{D}_{\delta_2} \subseteq \operatorname{supp} g_x$ and $\pi \in \operatorname{Perm}(\mathbb{D})$. Then,*

(i) $|\mathbb{D}_{\delta_1}| = |\mathbb{D}_{\delta_2}|$.

(ii) $\mathbb{D}_{\delta_1} = \mathbb{D}_{\delta_2}$.

(iii) $\delta_1 = \delta_2$.

Proof. (i). Notice that, by Proposition 4.8(ii), $\operatorname{supp} \delta_1 g_x = (\operatorname{supp} g_x) - \mathbb{D}_{\delta_1}$, and $\operatorname{supp} \delta_2 g_x = (\operatorname{supp} g_x) - \mathbb{D}_{\delta_2}$. Now, since $|\operatorname{supp} \delta_1 g_x| = |\operatorname{supp} \delta_2 g_x|$, we get that $|\mathbb{D}_{\delta_1}| = |\mathbb{D}_{\delta_2}|$.

(ii). On the contrary, suppose $\mathbb{D}_{\delta_1} \neq \mathbb{D}_{\delta_2}$. So, there exists some $d \in \mathbb{D}_{\delta_1} - \mathbb{D}_{\delta_2}$ or $d \in \mathbb{D}_{\delta_2} - \mathbb{D}_{\delta_1}$. Assuming $d \in \mathbb{D}_{\delta_2} - \mathbb{D}_{\delta_1}$, we prove the result. The other case is proved similarly. Notice that, $d \in \mathbb{D}_{\delta_2}$ implies that $\delta_2(d) \in \mathsf{2}$, say, $\delta_2(d) = \mathsf{0}$. Take $\delta \in S$ with $\mathbb{D}_\delta = \operatorname{supp} \delta_1 g_x$ and $\delta(d) = \mathsf{1}$. Now, $\pi\delta\delta_1 g_x = \delta''\pi\delta_1 g_x = \delta''\delta_2 g_x$. Applying Proposition 4.8(ii), since $\operatorname{supp} \delta\delta_1 g_x = (\operatorname{supp} \delta_1 g_x) - \mathbb{D}_\delta = \emptyset$, we get that $\delta\delta_1 g_x \in \mathcal{Z}(Cbg_x)$. Thus, by Proposition 4.8(i), we have $\delta\delta_1(d) = \delta''\delta_2(d)$ for all $d \in \operatorname{supp} g_x$ which is a contradiction. This is because $\delta''\delta_2(d) = \mathsf{0}$ while $\delta\delta_1(d) = \delta(d) = \mathsf{1}$.

(iii). By part (ii), we have $\mathbb{D}_{\delta_1} = \mathbb{D}_{\delta_2}$. Now, we show that $\delta_1(d) = \delta_2(d)$, for all $d \in \mathbb{D}_{\delta_1}$. Similar to the proof of (ii), take $\delta \in S$ with $\mathbb{D}_\delta = \operatorname{supp} \delta_1 g_x$. Then, we get that $\pi\delta\delta_1 g_x = \delta''\delta_2 g_x$, and so, $\delta\delta_1(d) = \delta''\delta_2(d)$ for all $d \in \operatorname{supp} g_x$. Let $d \in \mathbb{D}_{\delta_1}$. Then, $\delta_1(d) \in \mathsf{2}$, say $\delta_1(d) = \mathsf{0}$. So, $\delta''\delta_2(d) = \delta\delta_1(d) = \mathsf{0}$. Now, since $\mathbb{D}_{\delta_1} = \mathbb{D}_{\delta_2}$, we get that $d \in \mathbb{D}_{\delta_2}$, and so, $\delta_2(d) = \mathsf{0}$. Thus, $\delta_1 = \delta_2$. □

The following lemma shows that g_x is a strongly finitely supported element of Cbg_x.

Lemma 4.10. *Let $\sigma g_x = \sigma' g_x$ where $\sigma, \sigma' \in Cb$. Then, $\sigma|_{\operatorname{supp} g_x} = \sigma'|_{\operatorname{supp} g_x}$.*

Proof. Let $\sigma g_x = \sigma' g_x$. Then, by Proposition 4.4, we have the following cases:

Case (1): Suppose $\pi g_x = g_x$. In this case, for all $d \in \operatorname{supp} g_x$, we show that $\pi(d) = d$. We have $\pi(\operatorname{supp} g_x) = \operatorname{supp} \pi g_x = \operatorname{supp} g_x$. Take $d \in \operatorname{supp} g_x$. Since $\pi g_x = g_x$, we get that $\pi(0/d)g_x = (0/\pi d)g_x$. Now, by Lemma 4.9, $\pi d = d$.

Case (2): If $\pi\delta g_x = \delta' g_x$, then applying Lemma 4.9, we have $\delta = \delta'$. So, $\pi\delta g_x = \delta g_x$. Notice that, by Proposition 4.8(ii), $\operatorname{supp}\delta g_x = (\operatorname{supp} g_x) - \mathbb{D}_\delta$. If $\operatorname{supp}\delta g_x = \emptyset$, then $\operatorname{supp} g_x = \mathbb{D}_\delta$. So, in this case, it s clear that $\pi\delta(d) = \delta(d)$ for all $d \in \operatorname{supp} g_x$. Suppose $\operatorname{supp}\delta g_x \neq \emptyset$. First, we show $\pi|_{\operatorname{supp}\delta g_x} = \iota|_{\operatorname{supp}\delta g_x}$. Let $d \in \operatorname{supp}\delta g_x$ Then, $\pi d \in \operatorname{supp}\delta g_x$, and so, $\pi(0/d)\delta g_x = (0/\pi d)\delta g_x$. Applying Lemma 4.9, $\pi d = d$. Therefore, for all $d \in \operatorname{supp}\delta g_x$, we have $\pi d = d$. Now, we prove the result. Take $d \in \operatorname{supp} g_x$. If $d \in \mathbb{D}_\delta$, then the result holds. If $d \notin \mathbb{D}_\delta$, then $\sigma d = \pi\delta d = \pi d$ and $\delta' d = \delta d = d$. On the other hand, since $d \in (\operatorname{supp} g_x - \mathbb{D}_\delta) = \operatorname{supp}\delta g_x$, we get that $\pi d = d$. □

Corollary 4.11. *Max-zero cyclic finitely supported Cb-sets are projective.*

Proof. If $X = Cbx$ is a max-zero cyclic finitely supported Cb-sets, then X is isomorphic to $\mathbb{D}^{\operatorname{supp} x}$, by Lemma 3.12 and Lemma 4.10. So, applying Lemma 3.16 we get that X is projective. □

5. Conclusions

In this section, we assume that M and N are two submonoids of $\mathrm{End}(\mathbb{D})$ such that M is a submonoid of N.

Note. An N-equivariant (M-equivariant) map is an equivariant map between finitely supported N-sets (M-sets). (cf. Example 2.4, [2])

In [6], we proved that free finitely supported N-sets exist over finitely supported M-sets (Theorem 5.1). By Theorem 5.1, we show that the functor F preserves projective objects and then we characterize projective finitely supported N-sets in which N contains a zero-retraction submonoid M.

Theorem 5.1. (cf. [6]) *The forgetful functor* $U : (N\text{-}\mathbf{Set})_{\text{fs}} \to (M\text{-}\mathbf{Set})_{\text{fs}}$ *has a left adjoint* $F : (M\text{-}\mathbf{Set})_{\text{fs}} \to (N\text{-}\mathbf{Set})_{\text{fs}}$.

Remark 5.2. (cf. [6]) (1) Since $M \leqslant N$, every finitely supported N-set can be considered as a finitely supported M-set.

(2) The set $N \times X$ together with the action $(n, (n', x)) \mapsto (nn', x)$ is an N-set, for each finitely supported M-set X.

(3) $F(X) = (N \times X)/\sim$ is a finitely supported N-set where X is a finitely supported M-set and the relation $\sim$ over $N \times X$ is the smallest equivariant equivalence relation generated by R defined as follows:

$$(n, x)R(n', x') \Leftrightarrow \exists m \in M;\ mx = x' \text{ and } n'm|_S = n|_S,$$

where S is a finite support of x.

The equivalence class of (n, x) denoted by $[n, x]$.

(4) If X is a finitely supported M-set, then $\eta_X : X \longrightarrow F(X)$ defined by $\eta_X(x) = [id, x]$ is an equivariant map.

(5) Using (1), for every finitely supported N-set, there exists a surjective equivariant map $\varphi : F(U(X)) = F(X) \longrightarrow X$ defined by $\varphi([n, x]) = nx$.

Now, by Theorem 5.1, we can characterize projective finitely supported N-sets.

Proposition 5.3. *If X is a projective finitely supported M-set, then $F(X)$ is a projective finitely supported N-set.*

Proof. Let $g : Y \longrightarrow Z$ be a surjective N-equivariant map and $f : F(X) \longrightarrow Z$ be an N-equivariant map. Then, $f\eta_X : X \longrightarrow Z$ is an M-equivariant map, since $\eta_X : X \longrightarrow F(X)$ is an M-equivariant map. Now, since X is projective, there exists an M-equivariant map $h : X \longrightarrow Y$ with $gh = f\eta_X$. On the other hand, since $F(X)$ is free over X, there exists an N-equiavriant map $\bar{f} : F(X) \longrightarrow Y$ with $\bar{f}\eta_X = h$. Now, we show that $g\bar{f} = f$. We have

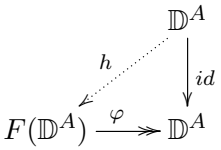
$$g\bar{f}[n, x] = ng\bar{f}[id, x] = ng\bar{f}\eta_X(x) =$$
$$ngh(x) = nf\eta_X(x) = nf([id, x]) = f([n, x]). \qquad \square$$

Corollary 5.4. *If M is a zero-retraction submonoid of N and $A \subseteq \mathbb{D}$ is a finite subset, then $F(\mathbb{D}^A)$ is a projective finitely supported N-set.*

Proof. Follows from Lemma 3.16 and Proposition 5.3. $\square$

Lemma 5.5. *Let $\mathbb{D}^A$ be a finitely supported N-set where A is a finite subset of $\mathbb{D}$. Then, $\mathbb{D}^A$ is a retract of $F(\mathbb{D}^A)$.*

Proof. First, notice that, by Remark 5.2(2), there exists a surjective N-equivariant $\varphi : F(\mathbb{D}^A) \longrightarrow \mathbb{D}^A$ defined by $\varphi[n, id|_A] = nid|_A = n|_A$. Suppose $n \in N$. Define $h(n|_A) = [n, id|_A]$. We show that h is an N-equivariant and commutes the following diagram; that is, $\varphi h = id$.



To do so, let $n, n' \in N$ with $n|_A = n'|_A$. Then, since A is a finite support of $id|_A$, by Remark 5.2(2), we get that $(n, id|_A)R(n', id|_A)$. Now, since $R \subseteq \sim$, we get that $[n, id|_A] = [n', id|_A]$. If $n_1 \in N$, then

$$n_1 h(n|_A) = n_1[n, id|_A] = [n_1 n, id|_A] = h(n_1 n|_A).$$

Also, $\varphi h(n|_A) = \varphi([n, id|_A] = n|_A = id(n|_A)$. □

Corollary 5.6. *For every finite subset $A \subseteq \mathbb{D}$, finitely supported N-set $\mathbb{D}^A$ is projective.*

Proof. Follows from Proposition 5.3 and Lemma 5.5. □

Theorem 5.7. *Let X be a finitely supported N-set. Then,*

(i) *X is indecomposable and projective if and only if it is cyclic and isomorphic to $\mathbb{D}^A$ for some finite subset $A \subseteq \mathbb{D}$.*

(ii) *X is projective if and only if $X = \coprod_{i \in I} X_i$, where every X_i is isomorphic to $\mathbb{D}^A$ for some finite $A \subseteq \mathbb{D}$.*

Proof. (i). Follows from Lemma 3.20 and Corollary 5.6.
(ii). Follows from (i), Proposition 2.2 and Corollary 5.6. □

Acknowledgement. The authors gratefully thank to Referees for the careful reading and constructive suggestions which definitely help to improve the readability and quality of the paper.

References

[1] **S. Abramsky, D.R. Ghica, A.S. Murawski, C.H. Luke Ong, I.D.B. Stark**, *Nominal games and full abstraction for the ν-calculus*, In: 19th IEEE Symposium on Logic in Computer Science, IEEE Computer Society Press (2004), 150 – 159.

[2] **M. Bojanczyk, B. Klin, S. Lasota**, *Automata theory in nominal sets*, Log. Methods Comput. Sci. **10**(3:4) (2014), 1 – 44.

[3] **M.M. Ebrahimi, M. Mahmoudi**, *The category of M-sets*, Ital. J. Pure Appl. Math. **9** (2001), 123 – 132.

[4] **M.M. Ebrahimi, Kh. Keshvardoost, M. Mahmoudi**, *Simple and subdirectly irreducible finitely supported Cb-sets*, Theort. Comput. Sci. **706** (2018), 1 – 21.

[5] **M. Gabbay, A. Pitts**, *A new approach to abstract syntax with variable binding*, Form. Asp. Comput. **13**(3-5) (2002), 341 – 363.

[6] **M. Haddadi, Kh. Keshvardoost, A. Hosseinabadi**, *Finitely presentable objects in* $(Cb\text{-}Sets)_{fs}$, submitted.

[7] **Kh. Keshvardoost, M. Mahmoudi**, *Separated finitely supported Cb-sets*, Categ. Gen. Algebr. Struct. Appl. **13**(1) (2020), 55 – 81.

[8] **M. Kilp, U. Knauer, A. Mikhalev**, Monoids, Acts and Categories, Walter de Gruyter, Berlin, New York, 2000.

[9] **D. Petrisan**, *Investigations into algebra and topology over nominal sets*, Ph. D. Thesis, University of Leicester, Leicester, (2011).

[10] **A. Pitts**, *Nominal logic, a first order theory of names and binding*, Inf. Comput. **186**(2) (2003), 165 – 193.

[11] **A. Pitts**, Nominal sets, Names and Symmetry in Computer Science, Cambridge University Press, 2013.

[12] **A. Pitts**, *Nominal presentations of the cubical sets model of type theory*, LIPIcs. Leibniz Int. Proc. Inform. (2015), 202 – 220.

[13] **C. Urban**, *Nominal techniques in Isabelle/HOL*, J. Autom. Reason. **40**(4)(2008), 327˘356.

Received November 15, 2021

Kh. Keshvardoost
Faculty of Mathematics, Statistics and Computer Sciences, Velayat University, Iranshahr, Sistan and Balouchestan, Iran

E-mail: khadijeh.keshvardoost@gmail.com, kh.keshvardoost@velayat.ac.ir

M. Haddadi
Faculty of Mathematics, Statistics and Computer Sciences, Semnan University, Semnan, Iran

E-mail: m.haddadi@semnan.ac.ir, haddadi_1360@yahoo.com

Quasigroups and Related Systems **30** (2022), 241 – 256

A note on 2-prime and n-weakly 2-prime ideals of semirings

Biswaranjan Khanra, Manasi Mandal and Sampad Das

Abstract. We introduce and study the concepts of 2-prime and n-weakly 2-prime (resp. weakly 2-prime) ideals in a commutative semiring. We prove that an integral semidomain S is a valuation semiring if and only if every proper ideal of S is 2-prime and in a principal ideal semidomain the concepts of primary, quasi-primary and 2-prime ideals coincide. We characterize semirings where 2-prime ideals are prime and also characterize semirings where every proper ideal is n-weakly 2-prime (resp. weakly 2-prime).

1. Introduction

A commutative semiring is a commutative semigroup $(S, \cdot)$ and a commutaive monoid $(S, +, 0_S)$ in which 0_S is the additive identity and $0_S.x = x.0_S = 0_S$ for all $x \in S$, both are connected by ring like distribuitivity. We say S is a semiring with identity if the multiplicative semigroup $(S, \cdot)$ has identity element. Throughout this paper, unless otherwise mentioned, all semirings are commutative with identity element $1 \neq 0$, in particular S will denote such a semiring.

A nonempty subset I of S is called an ideal of S if a, $b \in I$ and $r \in S$, then $a + b \in I$ and $ra \in I$. We define radical of an ideal I as $\sqrt{I} = \{x \in S : x^n \in I\}$ and residual of I by $a \in S$ as $(I : a) = \{s \in S : sa \in I\}$. Annihilator of an element a in a semiring S is defined as $\mathrm{Ann}(a) = \{x \in S : ax = 0\}$. For an element x of S, $(x) = Sx$ is the principal ideal of S generated by x. An ideal I of a semiring S is said to be subtructive (or k-ideal) if a, $a+b \in I$, $b \in S$ then $b \in I$. A nonzero element a of S is said to be a zero divisor if $ab = 0$ for some nonzero $b \in S$. For an ideal I of S, $Zd_S(I) = \{s \in S : sr \in I$ for some $r \notin I\}$ and $\sqrt[2]{I} = \{x \in S : x^2 \in I\}$. An ideal I of a semiring S

2010 Mathematics Subject Classification: 16Y60.
Keywords: Prime ideal, maximal ideal, 2-prime ideal, weakly 2-prime ideal

is said to be proper if $I \neq S$ and an ideal generated by nth powers of elements of I is denoted as $I_n = (\{x^n : x \in I\})$ [?]. A semiring S is called a semidomain if $ab = ac$ implies $b = c$ for any $b, c \in S$ and for all nonzero $a \in S$. Similarly to the concept of field of fractions in ring theory, one can define the semifield of fractions $F(S)$ of a semidomain S ([5], p. 22). Let A be a multiplicatively closed subset of a semiring S. The relation is defined on the set $S \times A$ by $(s, a) \sim (t, b) \Leftrightarrow xsb = xat$ for some $a \in A$ is an equivalence relation and the equivalence class of $(s, a) \in S \times A$ denoted by s/a. The set of all equivalence classes of $S \times A$ under "$\sim$" denoted by $A^{-1}S$. The addition and multiplication are defined $s/a + t/b = (sb + ta)/ab$ and $(s/a)(t/b) = st/ab$. The semiring $A^{-1}S$ is called quotient semiring S by A. Suppose that S is a commutative semiring, A be a multiplicatively closed subset and I be an ideal. The set $A^{-1}I = \{a/b : a \in I, b \in A\}$ is an ideal of $A^{-1}S$. A proper ideal I of a semiring is said to be prime (resp. weakly prime) if for $a, b \in S$ such that $ab \in I$ (resp. $0 \neq ab \in I$) implies either $a \in I$ or $b \in I$. An ideal I of S is said to be primary if $ab \in I$ for some $a, b \in S$ implies $a \in I$ or $b \in \sqrt{I}$ and quasiprimary if $\sqrt{I}$ is a prime ideal of S. The notion of 2-prime (resp. weakly 2-prime ideal) as a generalisations of prime (resp. weakly prime) ideals in a commutative ring was introduced in [2, 7] and in a commutative semigroup in [6]. Moreover, rings in which concept of 2-prime, primary ideals coincide and rings in which 2-prime ideals are prime has been studied in [13]. These observations tempted us to study 2-prime (resp. weakly 2-prime) ideals in a commutative semiring.

In this article, firstly we define 2-prime ideals in a commutative semiring and state its relations with prime and quasi-primary ideals. Then we prove that every maximal ideal of a semiring without unity is 2-absorbing (Theorem 2.6). We define valuation ideal in a semiring and prove that a semidomain is a valuation semiring if and only if every proper ideal of the semidomain is 2-prime (Theorem 2.11). Also we prove that in a principal ideal semidomain the concepts of 2-prime, primary, quasi-primary ideals coincide (Theorem 2.15). In section 3, we characterize semirings in which 2-prime ideals are prime, defined as 2-P-semiring. In section 4, we define n-weakly 2-prime (resp. weakly 2-prime) ideals in a semiring. Then we characterize semirings in which every proper ideal is weakly 2-prime (Theorem 4.5) (resp. n-weakly 2-prime) (Theorem 4.6) and also studied some further properties of these ideals.

Before going to main work, we discuss some necessary preliminaries.

Theorem 1.1. (cf. [8]) *Let $I \subseteq P$ be ideals of a semiring S, where P is*

prime. Then the following statements are equivalent:

(1) *P is a minimal prime ideal of I.*
(2) *For each $x \in P$, there is a $y \notin P$ and a nonnegative integer i such that $yx^i \in I$.*

2. 2-prime ideals

Definition 2.1. A proper ideal I of a semiring S is said to be a 2-*prime ideal* if $xy \in I$ for some $x, y \in S$ implies either $x^2 \in I$ or $y^2 \in I$.

The following lemmas are obvious, hence we omit the proof.

Lemma 2.2.

(1) *Every prime ideal of S is a 2-prime ideal of S.*
(2) *Every 2-prime ideal of S is a quasi-primry ideal of S. Therefore if I is a 2-prime ideal of S, then $\sqrt{I} = P$ is a prime ideal of S.*

Remark 2.3. For a 2-prime ideal I of a semiring S, we refer to the prime ideal $P = \sqrt{I}$ as the associated prime ideal of I and I is referred to as a *P-2-prime ideal of S.*

The following examples show that converses of above lemmas are not true.

Example 2.4. Consider the ideal $I = \{m \in \mathbb{N} \cup \{0\} : m \geqslant 3\}$ in the semiring $S = \{\mathbb{N} \cup \{0\}, +, \cdot\}$. Clearly, I is 2-prime but not a prime ideal of S, since $2.2 \in I$ but $2 \notin I$.

Example 2.5. Consider the ideal $I = (\{X_n^n\}_{n=1}^{\infty})$ in the semiring $S = \mathbb{Z}_2[\{X_i\}_{i=1}^{\infty}]$. Clearly I is quasiprimary ideal of S, since $\sqrt{I}$ is a prime ideal of S. But I is not a 2-prime ideal of S, as $X_6^2 \cdot X_6^4 = X_6^6 \in I$ and neither $(X_6^2)^2 \notin I$ nor $(X_6^4)^2 \notin I$.

If S is a semiring with unity, then every maximal ideal of S is prime ([1], Theorem 11) and hence 2-prime. If S is a semiring without unity then maximal ideal of S need not be prime for example see ([1], Example 12) but there is a relation between maximal and 2-prime ideal of S, as follows

Theorem 2.6. *Let S be semiring without unity and assume maximal ideal exists. Then every maximal ideal of S is a 2-prime ideal of S.*

Proof. Let $xy \in M$ with $x^2 \notin M$ for some $x, y \in S$, where M is a maximal ideal of S. If $y^2 \notin M$, then clearly $x, y \in S - M$. Hence $M + (x) = M + (y) = S$. Since $x \in S$, $x^2 = (p + s_1x + n_1x)(q + s_2y + n_2y)$ for some $p, q \in M$, $s_1, s_2 \in S$ and $n_1, n_2 \in \mathbb{Z}$, implies $x^2 \in M$, a contradiction. Consequently, $y^2 \in M$. Hence M is a 2-prime ideal of S. □

Proposition 2.7. *Let I be an ideal of a semiring S.*

(1) *If I is a 2-prime ideal of S, then there is exactly one prime ideal of S that is minimal over I.*

(2) *If I is a prime ideal of S, then I^2 is a 2-prime ideal of S.*

(3) *An ideal I of S is prime if and only if it is both 2-prime and semiprime.*

(4) *If I is a 2-prime ideal of S and $J_1, J_2, \ldots, J_n$ are ideals of S such that $\bigcap J_i \subseteq \sqrt{I}$, then $J_i \subseteq \sqrt{I}$ for some $i \in \{1, 2, \ldots, n\}$.*
In particular, if $\bigcap J_i = \sqrt{I}$, then $J_i = \sqrt{I}$ for some $i \in \{1, 2, \ldots, n\}$.

(5) *If I is a P-2-prime ideal of S, then $(I : a^2)$ is a 2-prime ideal of S, for all $a \in S$ such that $a^2 \notin I$.*
In particular $(I : a^2)$ is a P-2-prime ideal of S for all $a \in S - \sqrt{I}$.

(6) *If I is a 2-prime ideal of S and $(I : a) = (I : a^2)$ for all $a \in S - I$, then $(I : a)$ is a 2-prime ideal of S.*

(7) *I is a proper ideal of S and A be a multiplicatively closed subset of S, then the following statements hold.*
   (*i*) *If I is a 2-prime ideal of S such that $I \cap A = \phi$, then $A^{-1}I$ is a 2-prime ideal of $A^{-1}S$.*
   (*ii*) *If $A^{-1}I$ is a 2-prime ideal of $A^{-1}S$ with $Zd_S(I) \cap S = \phi$, then I is a 2-prime ideal of S.*

(8) *If I is a P-primary ideal for some prime ideal P of S such that $P^2 \subseteq I$. Then I is a 2-prime ideal of S.*

Proof. (1). If possible, let J_1 and J_2 be two distinct prime ideal that are minimal over I. Hence there exists $j_1 \in J_1 - J_2$ and $j_2 \in J_2 - J_1$. By Theorem 1.1 there is $a_1 \notin J_1$ and $a_2 \notin J_2$ such that $a_1 j_1^n \in I$ and $a_2 j_2^m \in I$ for some integer m, $n \geqslant 1$. Since $j_1, j_2 \notin I \subseteq J_1 \cap J_2$ and I is 2-prime , hence $a_1^2 \in I \subseteq J_1 \cap J_2$ and $a_2^2 \in I \subseteq J_1 \cap J_2$. Therefore $a_1^2 \in J_1$. Since J_1 is prime so $a_1 \in J_1$, a contradiction. Similarly if $a_2^2 \in J_2$ then $a_2 \in J_2$, a contradiction. Hence there is exactly one prime ideal minimal over I.

(2). Since $I^2 \subseteq I$ for any ideal I of S, it is clear.

(3). If an ideal I is prime, then clearly it is 2-prime and semiprime.

Conversely, let $ab \in I$ for some $a, b \in S$. Since I is 2-prime we have $a^2 \in I$ or $b^2 \in I$, which implies $a \in I$ or $b \in I$, since I is semprime also. Consequently I is a prime ideal of S.

(4). Let $J_i \nsubseteq \sqrt{I}$ for all $i \in \{1, 2, \ldots, n\}$. Then there exists $a_i \in J_i$ but $a_i \notin \sqrt{I}$ for all $i \in \{1, 2, \ldots, n\}$. Let $x = a_1 a_2 \cdots a_n$. Then $x \in \bigcap J_i$ but $x \notin \sqrt{I}$, since $\sqrt{I}$ is a prime ideal of S, a contradiction . Hence $J_i \subseteq \sqrt{I}$ for some $i \in \{1, 2, \ldots, n\}$.
Again if, $\bigcap J_i = \sqrt{I}$, then $\sqrt{I} \subseteq J_i$ for all $i \in \{1, 2, \ldots, n\}$. Hence $J_i = \sqrt{I}$ for some $i \in \{1, 2, \ldots, n\}$.

(5). Let $xy \in (I : a^2)$ with $x^2 \notin (I : a^2)$ for $x, y \in S$. Then $xya^2 = (xa)(ya) \in I$. Hence $(ya)^2 = y^2a^2 \in I$, since I is a 2-prime ideal of S and $x^2a^2 \notin I$. Consequently $(I : a^2)$ is a 2-prime ideal of S.
Again let $a \in S - P$ and $x \in (I : a^2)$. Then $a^2x \in I \subseteq P$. Hence $x^2 \in I$, since $a \notin P$ and I is a 2-prime ideal of S. Thus $I \subseteq (I : a^2) \subseteq P$, which implies $P = \sqrt{I} \subseteq \sqrt{(I : a^2)} \subseteq \sqrt{P} = P$. Consequently $(I : a^2)$ is a P-2-prime ideal of S.

(6). Clearly follows from (5).

(7). (i) Let $(a/s)(b/t) \in A^{-1}I$ for some $a, b \in S$ and $s, t \in A$. Then there exists $u \in A$ such that $abu \in I$. Then $a^2 \in I$ or $b^2u^2 \in I$, since I is a 2-prime ideal of S. If $a^2 \in I$, then $(a/s)^2 = (ua^2/us^2) \in A^{-1}I$ and if $b^2u^2 \in I$ then $(b/s)^2 = (b^2u^2/s^2u^2) \in A^{-1}I$. Therefore $A^{-1}I$ is a 2-prime ideal of $A^{-1}S$.

(ii) Let $xy \in I$ for some $x, y \in S$. Then $\frac{x}{1}\frac{y}{1} \in A^{-1}I$ implies $\frac{x^2}{1} \in A^{-1}I$ or $\frac{y^2}{1} \in A^{-1}I$. Hence $ax^2 \in I$ or $by^2 \in I$ for some $a, b \in S$. Since $A \cap Zd_S(I) = \phi$, we have either $x^2 \in I$ or $y^2 \in I$, as desired.

(8). Let $ab \in I$ for some $a, b \in S$, where I is a P-primary ideal of S such that $P^2 \subseteq I$. Then either $a \in I$ or $b \in \sqrt{I} = P$. If $a \in I$ then $a^2 \in I^2$ and if $b \in P$ then $b^2 \in P^2 \subseteq I$. Consequently I is a 2-prime ideal of S. □

Theorem 2.8. *Let P be a proper ideal of a semiring S. Then the following statements are equivalent:*

(1) *P is a 2-prime ideal of S.*

(2) *for any ideals J, K of S with $JK \subseteq P$ implies either $J_2 \subseteq P$ or $K_2 \subseteq P$, where $J_2 = (\{x^2 : x \in J\})$ and $K_2 = (\{k^2 : k \in K\})$.*

(3) *For every $s \in S$, either $(s) \subseteq (P : s)$ or $(P : s) \subseteq \sqrt[2]{P}$.*

(4) *For any ideals A and B of S with $AB \subseteq P$ implies either $A_2 \subseteq P$ or $B \subseteq \sqrt[2]{P}$.*

(5) *For every $s \in S$, either $s^2 \in P$ or $(P : s)_2 \subseteq P$.*

Proof. (1) $\Rightarrow$ (2). Let P be a 2-prime ideal of a semiring S and $JK \subseteq P$ for some ideal J, K of S with $J_2 \nsubseteq P$. Then there exists an element $p \in J$ such that $p^2 \notin P$. Since $pK \subseteq P$ and $p^2 \notin P$, we conclude $K_2 \subseteq P$ (Proposition 2.7 ????).

(2) $\Rightarrow$ (1). Let $ab \in P$ for some a,$b \in S$ and $a^2 \notin P$. Let $J = (a)$ and $K = (b)$. Then $JK \subseteq P$ and $J_2 \nsubseteq P$, otherwise $a^2 \in P$. Hence $K_2 \subseteq P$ implies $b^2 \in P$. Consequently, P is a 2-prime ideal of S.

(1) $\Rightarrow$ (3) Let $s \in S$. If $s^2 \in P$, then $s \in (P : s)$ implies $(s) \subseteq (P : s)$. Let $s^2 \notin P$ and $r \in (P : s)$ for some $r \in S$. Hence $rs \in P$ implies $r^2 \in P$, since P is 2-prime and $s^2 \notin P$. Consequently, $(P : s) \subseteq \sqrt[2]{P}$.

(3) $\Rightarrow$ (4). Let $AB \subseteq P$ for some ideals A, B of S. Let $B \nsubseteq \sqrt[2]{P}$. Then there exists $b \in B - \sqrt[2]{P}$ and $ab \in P$ for all $a \in A$. Since $b \in (P : a) - \sqrt[2]{P}$, we have $(P : a) \nsubseteq \sqrt[2]{P}$. Hence by hypothesis, $(a) \subseteq (P : a)$ implies $a^2 \in P$. Consequently $A_2 \subseteq P$.

(4) $\Rightarrow$ (5). Let $s \in S$. If $s^2 \in P$, there is nothing to prove. So let $s^2 \notin P$ and $A = (P : s)$, $B = (s)$. Then $AB = (P : s)(s) \subseteq P$. Since $B \nsubseteq \sqrt[2]{P}$, we have $A_2 = (P : s)_2 \subseteq P$.

(5) $\Rightarrow$ (1). Let $xy \in P$ with $x^2 \notin P$ for some x, $y \in S$. Then $y \in (P : x)$. Hence by hypothesis, $y^2 \in (P : s)_2 \subseteq P$, as desired. □

The concept of valuation semiring has been defined by P. Nasehpour in [10], here we define valuation ideal of a semiring, as follows

Definition 2.9. Let S be a semidomain and K be its semifield of fractions. Then an ideal I in S is a *valuation ideal* if I is the intersection of S with an ideal of a valuation semiring S_v containing S. Moreover if v is the corresponding M-valuation we say I is a *valuation ideal associated with the M-valuation v* or I is a *v-ideal*.

Lemma 2.10. *Let v be an M-valuation on K and I an ideal of a semidomain S. Then the followings are equivalent*

(1) *I is a valuation ideal.*

(2) *For each $x \in S$, $y \in I$, the inequality $v(x) \geqslant v(y)$ implies $x \in I$.*

(3) *I is of the form $I = S_v I \cap S$.*

Proof. The proof is similar to ([15], page 340). □

Theorem 2.11. *Let S be a semidomain. Then the following are equivalent*

(1) *Every ideal of S is 2-prime.*

(2) *Every principal ideal of S is 2-prime.*

(3) *S is a valuation semiring.*

Proof. (1) $\Rightarrow$ (2). It is clear.

(2) $\Rightarrow$ (3). Let $x \in K - \{0\}$, where K is the semifield of fractions of S. Then $x = \frac{a}{b}$ for some $a, b \in S - \{0\}$. Let $I = (ab)$ be a principal ideal of S so 2-prime and since $ab \in (ab) = I$, we have $a^2 \in I$ or $b^2 \in I$. If $a^2 \in I$, then there exists an element $c \in S$ such that $a^2 = cab$, hence $x = \frac{a}{b} = c \in S$. Similarly, if $b^2 \in I$, we have $x^{-1} \in S$. Consequently, S is a valuation semiring ([10], Theorem 2.4).

(3) $\Rightarrow$ (1). Let I be a v-ideal on S where v is a valuation on S. Let $xy \in I$ for some $x, y \in S$. If $v(x) \geqslant v(y)$, we get $v(x^2) \geqslant v(xy)$ and as I is a v-ideal we have $x^2 \in I$. Similarly, $v(y) \geqslant v(x)$ implies $y^2 \in I$. Consequently I is a 2-prime ideal of S. □

The following lemmas are obvious, hence we omit the proof

Lemma 2.12. *Let S be a semidomain and $a, b \in S - \{0\}$. Then a and b are associates if and only if $(a) = (b)$.*

Lemma 2.13. *Let S be a semidomain and $p \in S - \{0\}$. Then p is an irreducible element of S if and only if (p) is a maximal ideal of S.*

Lemma 2.14. *Let I be a P-primary ideal of a semiring S. Then P is the unique minimal prime ideal of I in S.*

Proof. Let Q be another minimal prime of I in S. Then $I \subseteq Q$ implies $P = \sqrt{I} \subseteq \sqrt{Q} = Q$. Hence P is the unique minimal prime ideal of I in S. □

Theorem 2.15. *Let I be a proper ideal of a principal ideal semidomain S. Then the followings are equivalent*

(1) *I is a quasi-primary ideal of S.*

(2) *I is a primary ideal of S.*

(3) *I is of the form (p^n), where n is a postitive integer and $p = 0$ or an irreduicible element of S.*

(4) *I is a 2-prime ideal of S.*

Proof. (1) $\Rightarrow$ (2). Since every nonzero prime ideal of a principal ideal semidomain S is a maximal ideal ([11], Proposition 2.1), it follows claerly from ([1], Theorem 40).

(2) $\Rightarrow$ (1). It is obvious.

(2) $\Rightarrow$ (3). Let I be a nonzero primary ideal of S. Then $I = (a)$ for some nonzero nonunit element $a \in S$. Since every principal ideal semidomain is a unique factorization semidomain ([11], Theorem 3.2), a can written as a product of irreduicible elements of S. If a were divisible by two irreduicible elements x and y of S, which are not associates, then by Lemma 2.12 and 2.13 (x) and (y) would be distinct maximal ideal of S, they would both minimal prime ideal of (a), which contradicts Lemma 2.14. Hence $I = \{(p^n) : p = 0$ or p is an irreduicible elements of S and $n \in \mathbb{N}\}$.

(3) $\Rightarrow$ (2). Since S is a semidomain, $\{0\}$ is prime and hence primary. Let p be an irreduicible element of S and $n \in \mathbb{N}$, then by Lemma 2.13 (p^n) is a power of a maximal ideal so is a primary ideal of S ([1], Theorem 40).

(3) $\Leftrightarrow$ (4) The proof is similar as that of ([13], Theorem 2.3). □

Example 2.16. Let I be an ideal of a von neuman regular semiring S. Then $I = I^2 = \sqrt{I}$ ([14], Proposition 1). Hence the concepts of prime, primary, 2-prime and quasiprimary ideal coincide in a regular semiring S.

If R and S are semirings then a function $f : R \longrightarrow S$ is said to be a morphism of semirings ([4], p. 105) if (i) $f(0_R) = 0_S$, (ii) $f(1_R) = 1_S$ and (iii) $f(r_1 + r_2) = f(r_1) + f(r_2)$ and $f(r_1 r_2) = f(r_1)f(r_2)$ for all $r_1, r_2 \in R$.

Theorem 2.17. *Let $f : S_1 \to S_2$ be a morphism of semirings. Then the following statements holds:*

(1) *If J is a 2-prime ideal of S_2, then $f^{-1}(J)$ is a 2-prime ideal of S_1.*

(2) *If f is onto steady morphism such that $kerf \subseteq I$ and I is a 2-prime k-ideal of S_1, then $f(I)$ is a 2-prime k-ideal of S_2.*

Proof. (1). Let $ab \in f^{-1}(J)$ for some $a, b \in S_1$. Then $f(ab) \in J$, hence $f(a^2) \in J$ or $f(b^2) \in J$, since f is a morphism and J is a 2-prime of S_2. Therefore $a^2 \in f^{-1}(J)$ or $b^2 \in f^{-1}(J)$. Consequently, $f^{-1}(J)$ is a 2-prime ideal of S_1.

(2). Let $xy \in f(I)$ for some $x, y \in S_2$. Then there exists $a, b \in S_1$ such that $f(a) = x$ and $f(b) = y$. Then $xy = f(a)f(b) = f(ab) \in f(I)$. Hence $f(ab) = f(r)$ for some $r \in I$. So we have $ab + s = r + t$ for some s, $t \in I$, since f is steady. Hence $ab \in I$, since $\ker f \subseteq I$ and I is a k-ideal of S_1. Hence either $a^2 \in I$ or $b^2 \in I$, since I is a 2-prime ideal of S_1. Thus either $f(a^2) \in f(I)$ or $f(b^2) \in f(I)$. Consequently, $f(I)$ is a 2-prime k-ideal of S_2. □

Corollary 2.18. *If $S \subseteq R$ is an extension of semiring and I is a 2-prime ideal of R, then $I \cap S$ is a 2-prime ideal of S.*

Theorem 2.19. *Let $S = S_1 \times S_2$ and $I = I_1 \times I_2$, where I_i are ideals of S_i for $i = 1, 2$. Then the following are equivalent*

(1) *I is a 2-prime ideal of S.*

(2) *$I_1 = S_1$ and I_2 is a 2-prime ideal of S_2 or $I_2 = S_2$ and I_1 is a 2-prime ideal of S_1.*

Proof. (1) $\Rightarrow$ (2). Let I be a 2-prime ideal of S. Then $\sqrt{I} = \sqrt{I_1} \times \sqrt{I_2}$, is a prime ideal of S. Hence either $I_1 = S_1$ or $I_2 = S_2$. Let $I_2 = S_2$ and $ab \in I_1$ for some a, $b \in S_1$. Then $(a, 1)(b, 1) \in I$. Hence $(a, 1)^2 \in I$ or $(b, 1)^2 \in I$, since I is a 2-prime ideal of S. This implies $a^2 \in I_1$ or $b^2 \in I_1$. Consequently, I_1 is a 2-prime of S_1. Similarly, if $I_1 = S_1$, we can show that I_2 is a 2-prime ideal of S_2.

(2) $\Rightarrow$ (1). Assume $I_1 = S_1$ and I_2 is a 2-prime ideal of S_2. Let $(a, x)(b, y) \in I$ for some a, $b \in S_1$ and x, $y \in S_2$. Then $xy \in I_2$ and this implies $x^2 \in I_2$ or $y^2 \in I_2$. Hence $(a, x)^2 \in I$ or $(b, y)^2 \in I$, as desired. In a similar way, one can prove the other case. □

Corollary 2.20. *Let $S = S_1 \times S_2 \times \ldots \times S_n$ and $I = I_1 \times I_2 \times \ldots \times I_n$, where I_i are ideals of S_i and $n \in \mathbb{N}$. Then the following are equivalent*

(1) *I is a 2-prime ideals of S.*

(2) *I_i is a 2-prime ideal of S_i for some $i \in \{1, 2, \ldots, n\}$ and $I_j = S_j$ for all $j \neq i$.*

Proof. By using Theorem 2.19 and induction on n, the proof is straightforward. □

Let S be a semiring and M an S-semimodule. Then $S \times M$ equipped with the following two operations $(s_1, m_1) + (s_2, m_2) = (s_1 + s_2, m_1 + m_2)$ and $(s_1, m_1)(s_2, m_2) = (s_1 s_2, s_1 m_2 + s_2 m_1)$, forms a semiring, denoted by $S\tilde{\bigoplus}M$, is called the expectation semiring of the S-semimodule M ([12], Proposition 1.1).

If I is an ideal of S and N is an S-subsemimodule of M, then $I\tilde{\bigoplus}N$ is an ideal of $S\tilde{\bigoplus}M$ if and only if $IM \subseteq N$ ([12], Theorem 1.6(2)).

Theorem 2.21. *Let M be a S-semimodule, I a proper ideal of S and $N \neq M$ an S-subsemimodule of M. Then*

(1) *If $I\tilde{\bigoplus}N$ is a 2-prime ideal of $S\tilde{\bigoplus}M$, then I is a 2-prime ideal of S.*

(2) *If the ideal I of S is 2-prime and $\sqrt[2]{I}M \subseteq N$, then $I\tilde{\bigoplus}N$ is a 2-prime ideal of $S\tilde{\bigoplus}M$.*

Proof. (1). Let $ab \in I$ with $a^2 \notin I$ for some a, $b \in S$. Then $(a,0)(b,0) \in I\tilde{\bigoplus}N$ while $(a,0)^2 \notin I\tilde{\bigoplus}N$. Hence $(b,0)^2 \in I\tilde{\bigoplus}N$, since $I\tilde{\bigoplus}N$ is a 2-prime ideal of $S\tilde{\bigoplus}M$. Consequently, $b^2 \in I$, as desired.

(2). Let $(a,m)(b,n) \in I\tilde{\bigoplus}N$ for some a, $b \in S$, m, $n \in M$. This implies $ab \in I$ implies $a^2 \in I$ or $b^2 \in I$. If $a^2 \in I$, then $am \in \sqrt[2]{I}M \subseteq N$ and this yields $(a,m)^2 = (a^2, 2am) \in I\tilde{\bigoplus}N$. Again if $b^2 \in I$ we have $(b,m)^2 \in I\tilde{\bigoplus}N$. Consequently, $I\tilde{\bigoplus}N$ is a 2-prime ideal of $S\tilde{\bigoplus}N$. □

3. 2-P-semiring

Definition 3.1. A semiring S is said to be a 2-*P-semiring* if 2-prime ideals of S are prime.

Example 3.2. Clearly every idempotent semiring is a 2-P-semiring.

Theorem 3.3. *A semiring S is 2-P-semiring if and only if one of the following conditions holds:*

(1) *2-prime ideals are semiprime.*

(2) *Prime ideals are idempotent and every 2-prime ideal is of the form A^2, where A is a prime ideal of S.*

Proof. (1). If S is a 2-P-semiring, clearly 2-prime ideals are semiprime. Converse follows easily from Proposition 2.7(3).

(2). Let P be a prime ideal of a 2-P-semiring S. Then P^2 is a prime ideal of S (Proposition 2.7(2)) and hence $P \subseteq P^2$. Clearly $P^2 \subseteq P$. Therefore prime ideals of S are idempotent. Again, let I be a 2-prime ideal of S. Then I is prime and hence $I = I^2$.

Conversely, let I be a 2-prime ideal of S. Then $I = P^2 = P$ for some prime ideal P of S. Consequently, S is a 2-P semiring. □

Lemma 3.4. *Let (S,M) be a local semiring. Then for every prime ideal I of S, IM is a 2-prime ideal of S. Furthermore, IM is prime if and only if $IM = I$*

Proof. Let $xy \in IM \subseteq I$. Then either $x \in I$ or $y \in I$, since I is a prime ideal of S. Let $x \in I$ implies $x^2 \in IM$, since $I \subseteq M$. Hence IM is a 2-prime ideal of S. □

Definition 3.5. Let I be an ideal of a semiring S. We define a 2-prime ideal P to be a *minimal 2-prime ideal over* I if there is not a 2-prime ideal K of S such that $I \subseteq K \subset P$. We denote the set of minimal 2-prime ideals over I by 2-$\text{Min}_S(I)$.

Theorem 3.6. *Let S be a subtructive semiring with unique maximal ideal M such that $(\sqrt{I})^2 \subseteq I$ for every 2-prime ideal I of S. Then the following statements are equivalent.*

(1) *S is a 2-P-semiring.*

(2) *If P is the minimal prime ideal over a 2-prime ideal I, then $IM = P$.*

(3) *For every prime ideal P of S, 2-$Min_S(P^2) = \{P\}$.*

Proof. (1) $\Rightarrow$ (2). Let P be the minimal prime ideal over a 2-prime ideal I of a 2-P-semiring S. Then clearly $IM = P$ (Lemma 3.4).

(2) $\Rightarrow$ (1). Let I be a 2-prime ideal of a subtructive semiring S with unique maximal ideal M and P is the minimal prime ideal over I such that $IM = P$. Then $I \subseteq P = IM \subseteq I \cap M = I$ implies $I = P$. Hence S is a 2-P-semiring.

(2) $\Rightarrow$ (3) Let P be a prime ideal of S and I be a 2-prime ideal of S such that $I \in$ 2-$\text{Min}_S(P^2)$. Let J be a prime ideal of S such that $I \subseteq J \subseteq P$. Clearly, $P^2 \subseteq I \subseteq J \subseteq P$. Let $a \in P$ then $a^2 \in P^2$. Therefore $a^2 \in J$ implies $a \in J$, since J is prime. Hence $J = P$. Now by hypothesis, $IM = P$ implies $P = IM \subseteq I \subseteq P$. Consequently, 2-$\text{Min}_S(P^2) = \{P\}$.

(3) $\Rightarrow$ (2). Let P is the minimal prime ideal over a 2-prime ideal I of S. Then $\sqrt{I} = P$. Hence by hypothesis $P^2 \subseteq I \subseteq P$. Therefore 2-$\text{Min}_S(P^2) = \{P\}$. Clearly $I = P$ implies IM is 2-prime (Lemma 3.4). Now $P^2 \subseteq PM \subseteq P$ so $IM = PM = P$. □

Theorem 3.7. *Let $S \subseteq R$ be an extension of semiring and spec(S)=spec(R), where spec(S) and spec(R) denotes set of all prime ideals of S and R respectively. If S is a 2-P-semiring, then R is 2-P-semiring.*

Proof. Let I be a 2-prime ideal of R. Then $\sqrt{I} = P \in spec(R) = spec(S)$. Clearly $I \subseteq P$. Also $I \cap S$ is a 2-prime ideal of S (Corollary 2.18), hence prime, since S is 2-P-semiring. Therefore $I \cap S = \sqrt{I \cap S} = P$ and $P^2 \subseteq I \cap S$. Let $x \in P$. Then $x^2 \in P^2 \subseteq I \cap S \in spec(A)$. Hence $x \in I \cap S \subseteq I$. Consequently, $I = P$, as desired. □

4. n-weakly 2-prime ideal

Definition 4.1. A proper ideal I of a semiring S is said to be *n-weakly 2-prime* if for $a, b \in S$, $ab \in I - I^n$ implies that $a^2 \in I$ or $b^2 \in I$.

Definition 4.2. A proper ideal I of a semiring S is said to be a *weakly 2-prime ideal* of S if $0 \neq xy \in I$ for some $x, y \in S$ implies $x^2 \in I$ or $y^2 \in I$.

The following lemmas are obvious, hence we omit the proof.

Lemma 4.3.

(1) *Every 2-prime ideal of S is a weakly 2-prime ideal of S.*

(2) *Every weakly prime ideal of S is a weakly 2-prime ideal of S.*

(3) *Every weakly 2-prime ideal of S is a n-weakly 2-prime ideal of S.*

(4) *An n-weakly 2-prime is a $(n-1)$-weakly 2-prime ideal, for all $n \geqslant 3$.*

Proposition 4.4. *Let I be a subtructive ideal of a semiring S. Then*

(1) *If I is weakly 2-prime but not a 2-prime ideal of S, then*
   (i) $I^2 = 0$.
   (ii) $\sqrt{I} = \sqrt{0}$.

(2) *Let (S, M) be a local semiring with $M^2 = 0$. Then every proper subtructive ideal of S is a weakly prime and hence weakly 2-prime ideal of S.*

(3) *Let P be a weakly prime ideal of S and Q be an ideal of S containg P, then PQ is a weakly 2-prime ideal of S. In particular, for every weakly prime ideal P of S, P^2 is a weakly 2-prime ideal of S.*

(4) *$\sqrt{I}$ is a prime (resp. weakly prime) ideal of S if and only if $\sqrt{I}$ is a 2-prime (resp. weakly 2-prime) ideal of S.*

(5) *Let I be a n-weakly 2-prime ideal of S and A be a multiplicatively closed subset of S with $A \cap I = \phi$ and $A^{-1}I^n \subseteq (A^{-1}I)^n$. Then $A^{-1}I$ is a n-weakly 2-prime ideal of $A^{-1}S$.*

Proof. (1)(i). We first show that if $ab = 0$ for some $a, b \in S - I$, then we have $aI = bI = 0$. Let $ai \neq 0$ for some $i \in I$. Then $0 \neq a(b + i) \in I$. Since I is a subtructive weakly 2-prime ideal of S, either $a^2 \in I$ or $b^2 \in I$, a contradiction. Therefore $aI = 0$. Similarly we can show $Ib = 0$. Now let $xy \neq 0$ for some $x, y \in I$ and $ab = 0$ for some $a, b \notin I$. Then we have

$(a+x)(b+y) = xy \neq 0$. Since I is subtructive weakly 2-prime ideal of S, either $a^2 \in I$ or $b^2 \in I$, a contradiction. Hence $I^2 = 0$.

(ii). By (i), $I^2 = \{0\}$. So we have $I \subseteq \sqrt{0}$ implies $\sqrt{I} \subseteq \sqrt{0}$. Also we have $\sqrt{0} \subseteq \sqrt{I}$. Therefore $\sqrt{I} = \sqrt{0}$.

(2). Let I be a proper ideal of a local semiring (S, M) such that $M^2 = 0$ and $0 \neq ab \in I$ for some $a, b \in S$. Then either $a \in M$ or $b \in M$ but both a, b does not belongs to M, otherwise $ab \in M^2 = 0$, a contradiction. Hence a or b must be semi-unit, let a be a semi-unit of S. Then there exists p, $q \in S$ such that $1 + pa = qa$ implies $b + pab = qab \in I$. Also $pab \in I$ implies $b \in I$, since I is a subtructive ideal of S. Similarly if b is a semi-unit then $a \in I$. Consequently I is a weakly 2-prime ideal of S, as desired.

(3). Let $0 \neq ab \in PQ$ for some $a, b \in I$. Since $PQ \subseteq P$ and P is weakly prime ideal of S, we have either $a \in P \subseteq Q$ or $b \in P \subseteq Q$. Hence either $a^2 \in PQ$ or $b^2 \in PQ$. Consequently, PQ is a weakly 2-prime ideal of S, in particular, P^2 is a weakly 2-prime ideal of S.

(4). Since $\sqrt{\sqrt{I}} = I$ for any ideal I of S, it is clear.

(5). Let $a, b \in S$ and $x, y \in A$ such that $\frac{a}{x}\frac{b}{y} \in A^{-1}I - (A^{-1}I)^n$. Then there exists $u \in A$ such that $uab \in I$. Again $vab \notin I^n$ for any $v \in A$ because if $vab \in I^n$ then $\frac{a}{x}\frac{b}{y} \in A^{-1}I \subseteq (A^{-1}I)^n$, a contradiction. So $abu \in I - I^n$, implies $a^2 \in I$ or $b^2u^2 \in I$, since I is a n-weakly 2-prime ideal of S. Hence $(\frac{a}{x})^2 \in A^{-1}I$ or $(\frac{b}{y})^2 \in A^{-1}I$. Thus $A^{-1}I$ is a n-weakly 2-prime ideal of $A^{-1}S$. □

The following is a characterization of a semiring in which every proper ideal is weakly 2-prime.

Theorem 4.5. *Let S be a semiring. Then every proper ideal of S is weakly 2-prime if and only if $(a^2) \subseteq (ab)$ or $(b^2) \subseteq (ab)$ or $ab = 0$, for any $a, b \in S$ such that $(ab) \neq S$.*

Proof. Let every proper ideal of a semiring S is weakly 2-prime and $a, b \in S$ such that $(ab) \neq S$. If $ab \neq 0$, then $0 \neq ab \in (ab)$ and (ab) is weakly 2-prime, hence $a^2 \in (ab)$ or $b^2 \in (ab)$. Consequently, $(a^2) \subseteq (ab)$ or $b^2 \subseteq (ab)$.

Conversely, let I be a proper ideal of a semiring S and $0 \neq ab \in I$ for some $a, b \in S$. Then $0 \neq ab \in (ab) \subseteq I$ implies $a^2 \in (a^2) \subseteq (ab) \subseteq I$ or $b^2 \in (b^2) \subseteq (ab) \subseteq I$. Hence, I is weakly 2-prime ideal of S, as desired. □

Theorem 4.6. *Let I be a subtructive ideal of a semiring S with $I^2 \nsubseteq I^n$. Then I is a 2-prime ideal of S if and only if I is a n-weakly 2-prime ideal.*

Proof. Let I be a subtructive n-weakly 2-prime ideal of S such that $I^2 \subseteq I^n$ and $ab \in I$ for some $a, b \in S$. If $ab \notin I^n$, then $a^2 \in I$ or $b^2 \in I$, since I is n-weakly 2-prime. So we assume $ab \in I^n$. First we suppose $aI \nsubseteq I^n$. Then for some $i \in I$, $ai \notin I^n$ implies $a(b+i) \notin I^n$, since I is subtructive and $ab \in I^n$. Hence $a(b+i) \in I - I^n$ implies $a^2 \in I$ or $b^2 \in I$. So we can assume $aI \subseteq I^n$. Similarly we can assume $Ib \subseteq I^n$. Now since $I^2 \nsubseteq I^n$, there exists $a_1, b_1 \in I$ such that $a_1b_1 \notin I^n$. Hence $(a+a_1)(b+b_1) \in I - I^n$ because if $(a+a_1)(b+b_1) \in I^n$ then $a_1b_1 = (a+a_1)(b+b_1) = (ab+aa_1+bb_1+a_1b_1) \in I^n$, which contradicts that $a_1b_1 \notin I^n$. Hence $(a+a_1)^2 \in I$ or $(b+b_1)^2 \in I$, since I is n-weakly 2-prime ideal of S. Therefore $a^2 \in I$ or $b^2 \in I$, since I is subtructive ideal of S, as desired. The other part is obvious. □

Proposition 4.7. *Let S be a semiring and $x \in S$. Then the following statements holds.*

(1) *If Sx is a subtructive ideal of S and $Ann(x) \subseteq Sx$. Then Sx is a 2-prime ideal of S if and only if Sx is a n-weakly 2-prime ideal.*

(2) *If Sx is a subtructive ideal of S and $Ann(x) \subseteq xI$ for some subtrative ideal I of S. Then xI is a 2-prime ideal of S if and only if xI is a n-weakly 2-prime ideal of S.*

Proof. (1). Let Sx be a subtructive n-weakly 2-prime ideal of S and $ab \in Sx$ for some $a, b \in S$. If $ab \notin (Sx)^n$, then I is 2-prime ideal, since Sx is n-weakly 2-prime ideal of S. So we assume $ab \in (Sx)^n$. Clearly $a(b+x) \in Sx$. If $a(b+x) \notin (Sx)^n$, then $a^2 \in Sx$ or $b^2 \in Sx$, since Sx is n-weakly 2-prime ideal of S. So we assume $a(b+x) \in (Sx)^n$. Since $ab \in (Sx)^n$ and $(Sx)^n$ is subtructive, we have $ax \in (Sx)^n$ implies $ax = tx$ for some $t \in (Sx)^n \subseteq Sx$. Hence $a - t \subseteq Ann(x) \subseteq Sx$ implies $a^2 \in Sx$. Consequently, Sx is a 2-prime ideal of S. The converse part is obvious.

(2). Let xI be a subtructive n-weakly 2-prime ideal of S and $ab \in xI$ for some $a, b \in S$. If $ab \in (xI)^n$, then xI is a 2-prime ideal of S. Hence we assume $ab \in (xI)^n$. Clearly, $a(b+x) \in xI$. If $a(b+x) \notin (xI)^n$, then $a^2 \in xI$ or $b^2 \in xI$, since xI is subtructive n-weakly 2-prime ideal of S. Hence xI is n-weakly 2-prime ideal of S. Now suppose $a(b+x) \in (xI)^n$. Since $ab \in (xI)^n$, we have $ax = yx$ for some $y \in (aI)^n \subseteq aI$. This implies $(a-y)x = 0$. Hence $a-y \in Ann(x) \subseteq xI$. Therefore $a^2 \in xI$. Consequently, xI is a 2-prime ideal of S. □

Definition 4.8. A proper ideal I of a semiring S is said to be a *strong ideal*, if for each $a \in I$ there exists $b \in I$ such that $a + b = 0$.

Proposition 4.9. *Let $f : S \to S_1$ be an epimorphism of semirings such that $f(0) = 0$ and I be a subtructive strong ideal of S. Then*

(1) *If I is a weakly 2-prime ideal of S such that $kerf \subseteq I$, then $f(I)$ is a weakly 2-prime ideal of S_1.*

(2) *If I is a 2-prime ideal of S such that $kerf \subseteq I$, then $f(I)$ is a 2-prime ideal of S_1.*

Proof. (1). Let a_1, $b_1 \in S_1$ be such that $0 \neq a_1b_1 \in f(I)$. So there exists an element $p \in I$ such that $0 \neq a_1b_1 = f(p)$. Also there exist a, $b \in S$ such that $f(a) = a_1$, $f(b) = b_1$, since f is an epimorphism. Since I is a strong ideal of S and $p \in I$, there exists $q \in I$ such that $p + q = 0$. This implies $f(p + q) = 0$, that is, $f(ab + q) = 0$, implies $ab + q \in kerf \subseteq I$, Hence $0 \neq ab \in I$, as I is a subtructive ideal of S and if $ab = 0$, then $f(p) = 0$, a contradiction. Thus $a^2 \in I$ or $b^2 \in I$, since I is a weakly 2-prime ideal of S. Thus $a_1^2 \in f(I)$ or $b_1^2 \in f(I)$. Hence, $f(I)$ is a weakly 2-prime ideal of S.

(2). It is clear from (1). □

Proposition 4.10. *Let S_1 and S_2 be two semirings and I be a proper ideal of S_1. Then the followings are equivalent:*

(1) *I is a 2-prime ideal of S_1.*

(2) *$I \times S_2$ is a 2-prime ideals of $S_1 \times S_2$.*

(3) *$I \times S_2$ is a weakly 2-prime ideals of $S_1 \times S_2$.*

Proof. (1) $\Rightarrow$ (2). Let $(a_1, b_1)(c_1, d_1) \in I \times S_2$ for some $(a_1, b_1) \in S_1 \times S_2$ and $(c_1, d_1) \in S_1 \times S_2$. Then $(a_1c_1, b_1d_1) \in I \times S_2$ implies $a_1^2 \in I$ or $c_1^2 \in I$, since I is a 2-prime ideal of S_1. Now if $a_1^2 \in I$, then $(a_1, b_1)^2 = (a_1^2, b_1^2) \in I \times S_2$. Similarly if $c_1^2 \in I$, then $(c_1, d_1)^2 = (c_1^2, d_1^2) \in I \times S_2$. Consequently, $I \times S_2$ is a 2-prime ideal of $S_1 \times S_2$.

(2) $\Rightarrow$ (3) It is clear.

(3) $\Rightarrow$ (1). Let $ab \in I$ for some a, $b \in S$. Then $(0, 0) \neq (a, 1)(b, 1) \in I \times S_2$. This implies $(a^2, 1) \in I \times S_2$ or $(b^2, 1) \in I \times S_2$, since $I \times S_2$ is a 2-prime ideal of $S_1 \times S_2$. Hence, $a^2 \in I$ or $b^2 \in I$, as desired. □

Acknowledgments. We are thankful to the referee for several valuable suggestions which improve the presentation of the paper.

References

[1] **Allen, P.J., Neggers, J.**, *Ideal theory in commutative A-semirings*, Kyngpook Math. J., **46**(2006), 261 – 271. 5

[2] **Beddani, C., and Messirdi, W.**, 2-*Prime ideals and their applications*, J. Algebra Appl., **15**(3)(2016), 1650051(11 pages). 5

[3] **Dubey, M. K., and Aggarwal, P.**, *On* 2-*absorbing ideals in a commutative rings with unity*, Lobachevskii J. Math., **39**(2)(2018), 185 − 190.

[4] **Golan, J.S.**, *Semirings and their applications*, Dordrecht: Kluwer Academic Publ., (1999).

[5] **Golan, J. S.**, *Power algebras over semirings*. With applications in mathematics and computer science, Dordrecht: Kluwer Academic Publ., (1999).

[6] **Khanra, B., and Mandal, M.**, *On* 2-*prime ideals in commutative semigroups*, An. Ştiinţ. Univ. Al. I. Cuza Iasi. Mat., **68** (2022), 49 − 60.

[7] **Koc, S.**, *On weakly* 2-*prime ideals in commutative rings*, Commun. Algebra, **(**2021), 1 − 17.

[8] **Nasehpour, P.**, *Pseudocomplementation and minimal prime ideals in semirings*, Algebra Universalis, **79**(1)(2018), Paper No. 11.

[9] **Nasehpour, P.**, *Some remarks on ideals of commutative semirings*, Quasigroups Relat. Syst., **26** (2018), 281 − 298.

[10] **Nasehpour, P.**, *Valuation semiring*, J. Algebra Appl., **17** (2018) 1850073.

[11] **Nasehpour, P.**, *Some remarks on semirings and their ideals*, Asian-Eur. J. Math., **13**(1)(2020), Article ID 2050002 (14 pages).

[12] **Nasehpour, P.**, *Algebraic properties of expectation semirings*, Afrika Mathematika **31**(2020), 903 − 915.

[13] **Nikandish, R., Nikmehr, M. J. and Yassine, A.**, *More on the* 2-*prime ideals of commutative rings*, Bull. Korean Math. Soc., **57**(1)(2020), 117 − 126.

[14] **Subramanian, H.**, *Von Neumann regularity in semirings*, Math. Nachrichten, **45** (1970), 73 − 76.

[15] **Zariski, O., and Samuel, P.**, *Commutative Algebra*, Vol II, Van Nostrand, New York, 1960.

Received October 14, 2021

Department of Mathematics, Jadavpur University, Kolkata-700032, India
E-mails: biswaranjanmath91@gmail.com (B. Khanra)
m.haddadi@semnan.ac.ir, haddadi_1360@yahoo.com M. (Mandal)
jumathsampad@gmail.com (S. Das)

Quasigroups and Related Systems **30** (2022), 257 – 262

Left twisted rings

Hee Sik Kim and Jae Hee Kim

Abstract. We introduce the notion of a left-twisted ring, and we construct a left-zero ring which is not a ring. We show that such a left-twisted ring does not have an identity. Also, we show that every non-zero element of the left-twisted ring is a pseudo unit of it.

1. Introduction

The concept of several types of groupoids related to semigroups, viz., twisted semigroups for which twisted versions of the associative law hold was introduced by Allen et al. in [1]. Thus, if $(X, *)$ is a groupoid and if $\varphi : X^2 \to X^2$ is a function $\varphi(a, b) = (u, v)$, then $(X, *)$ is a *left-twisted semigroup* with respect to φ if for all $a, b, c \in X$, $a * (b * c) = (u * v) * c$. Moreover, right-twisted, middle-twisted and their duals, a dual left-twisted semigroup were also discussed. The class of groupoids defined over a field $(X, +, \cdot)$ via a formula $x * y = \lambda x + \mu y$, with $\lambda, \mu \in X$, fixed structure constants as twisted semigroups are discussed.

The basic idea came from the following observations. Let $X = \mathbf{R}$ be the set of all real numbers. We consider a binary operation $(\mathbf{R}, -)$ where "$-$" is the usual subtraction. Then $(x - y) - z \neq x - (y - z) = x - y + z$ in general, i.e., $(\mathbf{R}, -)$ is not a semigroup. Since $(x - y) - z = x - (y - (-z))$, if we define $u := x, v := -z$, then we have $(x - y) - z = u - (y - v)$, which looks like that "$-$" satisfies a version of the associative law in $\mathbf{R}$, i.e., there exists a map $\varphi : \mathbf{R}^2 \to \mathbf{R}^2$ such that $\varphi(x, z) = (x, -z) = (u, v)$. Thus, we obtain a "twisted" associated law for $(\mathbf{R}, -)$, with the function φ defining the "nature" of the "twisted semigroup" of a particular type.

Kim and Neggers introduced in [2] the notion of $Bin(X)$, the collection of all groupoids defined on a non-empty set X. They showed that $(Bin(X), \square)$ is a semigroup and the left zero semigroup on X acts as an identity in $(Bin(X), \square)$. Let $(R, +, \cdot)$ be a commutative ring with identity

2010 Mathematics Subject Classification: 16Y99, 20N02, 20M10.
Keywords: left-twisted ring, right-zero-divisor, pseudo unit.

and let $L(R)$ denote the collection of all groupoids $(R, *)$ such that, for all $x, y \in R$, $x * y := ax + by + c$, where $a, b, c \in R$ are fixed constants. Such a groupoid $(R, *)$ is said to be a *linear groupoid*. They showed that $(L(R), \square)$ is a semigroup with identity. Neggers et al. introduced in [3] the notion of a Q-algebra, and showed that every quadratic Q-algebra $(X, *, e), e \in X$, has of the form $x * y = x - y + e$ when X is a field with $|X| \geqslant 3$.

In this paper, we construct a left-twisted ring which is not a ring on the basis of left-twisted semigroups on a field K, where $char(K) = p$, $K > p$, p is a prime by defining a binary operation $a * b := a^p b$ for all $a, b \in K$, and by defining an associator function φ, where $\varphi(a, b) := (a^{\frac{1}{p}}, b)$. We prove that such a left twisted ring $(K, +, \cdot, 0, 1)$ does not have an identity, but its non-zero element is a pseudo unit of it.

2. Preliminaries

Let $(X, *)$ be a groupoid for which there exists a function $\varphi : X^2 \to X^2$ such that, for all $a, b, c \in X$,

$$a * (b * c) = (u * v) * c, \tag{1}$$

where $\varphi(a, b) = (u, v)$, i.e., $u = u(a, b), v = v(a, b)$ are functions of two variables. We call $(X, *)$ a *left-twisted semigroup* with respect to the map φ. Such a map φ is called an *associator function* of the groupoid $(X, *)$.

Example 2.1. (cf. [1]) Let $\mathbf{R} = (\mathbf{R}, +, \cdot)$ be a real field and $\lambda \neq 0, \mu \in \mathbf{R}$. We define a binary operation "$*$" on $\mathbf{R}$ as follows: $x * y := \lambda x + \mu y$ for any $x, y \in \mathbf{R}$. If we define a map $\varphi(a, b) := (\frac{a}{\lambda}, b)$ and $\mu^2 = \mu$, then $(\mathbf{R}, *)$ is a left-twisted semigroup with respect to φ.

We may think of changing the equation (1) as follows:

$$(a * b) * c = a * (u * v), \tag{2}$$

where $\varphi(a, b) = (u, v)$, i.e., $u = u(a, b), v = v(a, b)$ are functions of two variables. We call $(X, *)$ a *right-twisted semigroup* with respect to φ.

Example 2.2. (cf. [1]) Consider $X := 2^A$ where $A \neq \emptyset$. If we define $a * b := a - b$ for any $a, b \in X$, then $(a * b) * c \neq a * (b * c)$. On the other hand, if we let $\varphi(b, c) := (b \cup c, \emptyset)$, then $(a * b) * c = (a - b) - c = a - (b \cup c)$, and $a * (u * v) = a - (b \cup c - \emptyset) = a - (b \cup c)$, proving that $(X, *)$ is a right-twisted semigroup with respect to φ.

Note that Example 2.2 is a typical example of a BCK-algebra which is also a right-twisted semigroup.

3. Left-twisted rings

An algebraic system $(X, +, *, 0, \varphi)$ is said to be a *left-twisted ring* if

(tr1) $(X, +, 0)$ is an abelian group,

(tr2) $(X, *, \varphi)$ is a left-twisted semigroup,

(tr3) for all $a, b, c \in X$,

$$a * (b + c) = a * b + a * c,$$
$$(a + b) * c = a * c + b * c.$$

Note that we can provide many examples of a left-twisted ring which are not a ring by applying Theorem 4.1 below using the change of prime number p.

Proposition 3.1. *Let $(X, +, *, 0, \varphi)$ be a left-twisted ring. Then*

(i) $a * 0 = a = 0 * a$ *for all* $a \in X$,

(ii) $a * (-b) = (-a) * b = -(a * b)$ *for all* $a, b \in X$.

Proof. (i). If $(X, +, *, 0, \varphi)$ is a left-twisted ring, then $a * 0 = a * (0 + 0) = a*0+a*0$ for all $a \in X$. Since $(X, +)$ is an abelian group, we have $a*0 = 0$ for all $a \in X$. Similarly, $0 * a = (0 + 0) * a = 0 * a + 0 * a$ implies $0 * a = 0$ for all $a \in X$.
(ii). By applying (i), we obtain

$$0 = a * 0 = a * (b + (-b)) = a * b + a * (-b).$$

It follows that $a*(-b) = -(a*b)$. Similarly, we obtain $(-a)*b = -(a*b)$. □

When we defined left-(resp., right-) twisted semigroup, we used the associator function $\varphi(a, b) = (u, v)$, i.e., $u = u(a, b), v = v(a, b)$ are functions of two variables. Since u and v are represented by a and b, we may define $u * v := \xi(a, b)$ for some $\xi : X^2 \to X^2$. We denote such a function ξ by $\widehat{\varphi}$, i.e., $u * v = \widehat{\varphi}(a, b)$.

Proposition 3.2. *Let $(X, +, *, 0, \varphi)$ be a left-twisted ring. Then, for all $a, b, c, d \in X$, we have*

$$\widehat{\varphi}(a+b, c) * d = \widehat{\varphi}(a, c) * d + \widehat{\varphi}(b, c) * d. \tag{3}$$

Proof. Given $a, b, c, d \in X$, since X is a left-twisted ring, there exist u, v in X such that $(a+b) * (c+d) = (u * v) * d$ where $\varphi(a+b, c) = (u, v)$. It follows that $u * v = \widehat{\varphi}(a+b, c)$, and hence we obtain

$$(a+b) * (c+d) = \widehat{\varphi}(a+b, c) * d. \tag{4}$$

Now, by applying (tr3), we obtain

$$\begin{aligned} (a+b) * (c * d) &= a * (c * d) + b * (c * d) \\ &= \widehat{\varphi}(a, c) * d + \widehat{\varphi}(b, c) * d. \end{aligned} \tag{5}$$

By (4) and (5), we prove the proposition. □

Corollary 3.3. *Let $(X, +, *, 0, \varphi)$ be a left-twisted ring. If $d(\in X)$ is right cancellative, then*

$$\widehat{\varphi}(a+b, c) = \widehat{\varphi}(a, c) + \widehat{\varphi}(b, c). \tag{6}$$

Proof. Straightforward. □

Corollary 3.4. *Let $(X, +, *, 0, \varphi)$ be a left-twisted ring. Then*

$$\widehat{\varphi}(0, c) * d = 0 \tag{7}$$

for all $c, d \in X$.

Proof. If we let $a = b = 0$ in Proposition 3.2, then

$$\widehat{\varphi}(0, c) * d = [\widehat{\varphi}(0, c) + \widehat{\varphi}(0, c)] * d = \widehat{\varphi}(0, c) * d + \widehat{\varphi}(0, c) * d.$$

This shows that $\widehat{\varphi}(0, c) * d = 0$. □

Let $(X, +, *, 0, \varphi)$ be a left-twisted ring. An element d in X is said to be a *right-non-zero-divisor* if $a * d = 0$ then $a = 0$.

Corollary 3.5. *Let $(X, +, *, 0, \varphi)$ be a left-twisted ring. If d in X is a right-non-zero-divisor, then $\widehat{\varphi}(0, c) = 0$ for all $c \in X$.*

Proof. It follows immediately from Corollary 3.4. □

Proposition 3.6. *Let $(X, +, *, 0, \varphi)$ be a left-twisted ring. If b in X is a right-non-zero-divisor, then $\widehat{\varphi}(a, 0) = 0$ for all $a \in X$.*

Proof. Given $a \in X$, we have $0 = a * 0 = a * (0 * b) = \widehat{\varphi}(a, 0) * b$. Since b is a right-non-zero-divisor, we obtain $\widehat{\varphi}(a, 0) = 0$ for all $a \in X$. □

4. Constructions of a left twisted ring

In this section, we construct a left twisted ring which is not a ring.

Theorem 4.1. *Let $(K, +, \cdot, 0, 1)$ be a field where $char(K) = p$, $|K| > p$, p is a prime. Define a binary operation $a * b := a^p b$ for all $a, b \in K$, and define a map $\varphi(a, b) := (a^{\frac{1}{p}}, b)$. Then $(K, +, *, 0, \varphi)$ is a left-twisted ring which is not a ring.*

Proof. We claim that $(K, *, \varphi)$ is a left-twisted semigroup. Given $a, b, c \in K$, we have $a * (b * c) = a^p(b * c) = a^p(b^p c) = (ab)^p c$. It follows that $(u * v) * c = \widehat{\varphi}(a, b) * c = (a^{\frac{1}{p}} * b) * c = (a^{\frac{1}{p}})^p b * c = ab * c = (ab)^p c = a * (b * c)$, proving the claim.

We claim that $(K, *)$ is not a semigroup. Let $a \notin GF(p)$. Then $a^p \neq a$ and hence $a \neq a^{\frac{1}{p}}$. Hence $a * (b * c) = (u * v) * c = ab * c = (a^{\frac{1}{p}} * b) * c$, which shows that $(K, *)$ is not a semigroup.

Finally, we show that (tr3) condition holds. Given $a, b, c \in K$, we have $a * (b + c) = a^p(b + c) = a^p b + a^p c = a * b + a * c$. Since $char(K) = p$, we obtain $(a + b) * c = (a + b)^p c = (a^p + b^p)c = a^p c + b^p c = a * c + b * c$. Hence $(K, +, *, 0, \varphi)$ is a left-twisted ring which is not a ring. □

Proposition 4.2. *Let $(X, +, *, 0, \varphi)$ be a left-twisted ring. Then*

(i) *if $a * c \neq b * c$ and $c \neq 0$, then $a = b$,*

(ii) *if $a * c \neq a * d$ and $a \neq 0$, then $c = d$.*

Proof. (i). Suppose $a * c = b * c$. Then $a^p c = b^p c$ and hence $(a - b)^p c = (a^p - b^p)c = 0$. Since $c \neq 0$ and K is a field, we obtain $(a - b)^p = 0$, proving that $a = b$.
(ii). Similar to (i), and we omit it. □

Theorem 4.3. *Let $(K, +, \cdot, 0, 1)$ be a field where $|K| > p$, $char(K) = p$, where p is a prime. Then a left-twisted ring $(K, +, *, 0, \varphi)$ does not have an identity.*

Proof. Assume that there exists $e \in K$ such that $a * e = a = e * a$ for all $a \in K$. It follows that $a^p e = a$. Since $a \neq 0$, we obtain $e = a^{1-p} = (\frac{1}{a})^{p-1} = \alpha^{p-1}$ where $\alpha = \frac{1}{a}$. This shows that $|K| = p$, i.e., $K = GF(p)$, a contradiction. Since $e * a = a$ and $a \neq 0$, we have $e^p a = a$, and hence $e^p = 1$. Hence e is a root of an equation $x^p - 1 = 0$. Since $x^p - 1 = 0$ has at most p such elements, $|K| = p$, a contradiction. □

Let $(K, +, *, 0, \varphi)$ be a left-twisted ring described in Theorem 4.3. An element $u \in K$ is said to be a *pseudo unit* if $x \in X$, there exist $x_L, x_R \in K$ such that $x_L * u = x, u * x_R = x$, i.e., $(x_L)^p u = x, u^p x_R = x$. It follows that $x_L = (\frac{x}{u})^{\frac{1}{p}}$ and $x_R = \frac{x}{u^p}$. Clearly, the identity 1 is a pseudo unit of K. For any $x \in K$, if we take $x_L := x^{\frac{1}{p}}$ and $x_R := x$, then 1 becomes a pseudo unit of K.

Proposition 4.4. *Let $(K, +, *, 0, \varphi)$ be a left-twisted ring as in Theorem* 4.3. *Let $P(*) := \{u \in K \mid u : a \ \ pseudo\ unit\ of\ K\}$. Then $(P(*), *)$ is a subsemigroup of $(K, *)$ containing 1.*

Proof. Clearly, $1 \in P(*)$. If $u, v \in X$, then $u * v = u^p v$. Given $x \in K$, we let $\alpha \in K$ such that $\alpha * (u^p v) = x$. It follows that $\alpha = (\frac{x}{u^p v})^{\frac{1}{p}} \in K$. Let $\beta \in K$ such that $(u * v) * \beta = x$. It follows that $(u^p v)^p \beta = x$, and hence $\beta = \frac{x}{(u^p v)^p} \in K$. If we take $x_L := \alpha, x_R := \beta$, then $u * v$ is a pseudo unit. □

Theorem 4.5. *Every non-zero element of K as in Theorem* 4.3 *is a pseudo unit of K.*

Proof. Let $u \notin P(*)$ with $u \neq 0$. Then there exists $x \in K$ such that $\alpha * u = x$ or $u * \beta = x$ is impossible for some $\alpha, \beta \in K$. It follows that $\alpha^p u = x$ or $u^p \beta = x$ is impossible. Since $u \neq 0$, we obtain $\alpha = (\frac{x}{u})^{\frac{1}{p}}$ or $\beta = \frac{x}{u^p}$ is impossible, a contradiction, since $\alpha, \beta \in K$. □

References

[1] **P.J. Allen, H.S. Kim and J. Neggers**, *Several types of groupoids induced by two-variable functions*, Springer Plus **5** (2016), 1715 – 1725.

[2] **H.S. Kim and J. Neggers**, *The semigroups of binary systems and some perspectives*, Bull. Korean Math. Soc. **45** (2008), 651 – 661.

[3] **J. Neggers, S.S. Ahn and H.S. Kim**, *On Q-algebras*, Int. J. Math & Math. Sci. **27** (2001), 749 – 757.

Received March 08,2022

H. S. Kim
Research Institute for Natural Science, Department of Mathematics, Hanyang University Seoul 04763, Korea
E-mail: heekim@hanyang.ac.kr

J. H. Kim
Center for Innovation in Engineering Education, College of Engineering, Hanyang University, Seoul 04763, Korea
E-mail: jaehee86@hanyang.ac.kr

Quasigroups and Related Systems **30** (2022), 263 – 274

Menger hypercompositional algebras represented by medial n-ary hyperoperations

Thodsaporn Kumduang

Dedicated to the memory of Professor Valentin S. Trokhimenko

Abstract. The necessary and sufficient conditions under which a Menger algebra can be isomorphically represented by medial n-ary operations are proposed. Since a Menger hypercompositional algebra can be regarded as a generalization of a Menger algebra, for this reason, the situation for medial hyperoperations is further examined and a representation theorem of Menger hypercompositional algebras by such concepts is proved.

1. Introduction and preliminaries

It is widely accepted that Professor V.S. Trokhimenko, who is a Ukrainian mathematician, has a great contribution in the developments of Menger algebras and algebras of multiplace functions for a long time. Many papers concerning various classes of multiplace functions and their structural properties have been extensively studied in the past few decades, for instance, idempotent n-ary operations [10] and k-commutative n-place functions [11]. See [8, 9, 12, 13, 14, 15] for more related topics in this direction. It turned out that these works can be considered as nice connections between the study of algebra and the theory of functions. Unfortunately, V.S. Trokhimenko passed away in 2020 due to the pandamic of COVID-19. However, the paper that mentioned his personal life and scientific works was commemoratively collected by W.A. Dudek in [6].

Basically, for a fixed positive integer n, a Menger algebra of rank n is a pair of a nonempty set G and an $(n+1)$-ary operation on G which

2010 Mathematics Subject Classification: 20N05; 20N15; 08A05
Keywords: Menger algebra, mediality, algebra of multiplace function

satisfies the superassociative law. Nowadays, Menger algebras were investigated in different aspects, for example, partial Menger algebras of terms [5], power Menger algebras of terms defined by order-decreasing transformations [28]. For other, see [4, 20, 23]. Fundamental properties of Menger algebras concerning quotient Menger algebras and isomorphism theorems for Menger algebras were recently examined in [18]. Now two elementary examples of Menger algebras are provided. The first one is the set $\mathbb{R}^+$ of all positive real numbers with the operation $\circ : (\mathbb{R}^+)^{n+1} \to \mathbb{R}^+$, defined by $\circ(x_0, \ldots, x_n) = x_0 \sqrt[n]{x_1 \cdots x_n}$. Another one is the set of all real numbers $\mathbb{R}$ with the following $(n+1)$-ary operation $\circ$, which is defined by $\circ(x, y_1 \ldots, y_n) = x + \frac{y_1 + \ldots + y_n}{n}$ for all $x, y_1 \ldots, y_n \in \mathbb{R}$. In a view of extensions, a Menger algebra of rank $n = 1$ is a semigroup. This means that a Menger algebra of rank n is a generalized structure of semigroups too.

Normally, semigroups and groups can be isomorphically represented by functions of one variables. Representations of other structures, for example, see [1, 22, 27]. Analogously, Menger algebras of some types are also studied in the same direction. It turned out that some types of Menger algebras of rank n can be represented by n-ary functions. In fact, let A^n be the n-th Cartesian product of a nonempty set A. Any mapping from A^n to A is called a *full n-ary function* or an *n-ary operation* if it is defined for all elements of A^n. The set of all such mappings is denoted by $T(A^n, A)$. One can consider the *Menger's superposition* on the set $T(A^n, A)$, i.e., an $(n+1)$-ary operation $\mathcal{O} : T(A^n, A)^{n+1} \to T(A^n, A)$ defined by

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

where $f, g_1, \ldots, g_n \in T(A^n, A), a_1, \ldots, a_n \in A$. A Menger algebra of all full n-ary functions, or a Menger algebra of all n-ary operations, is a pair of the set $T(A^n, A)$ of all full n-ary functions defined on A and the Menger composition of full n-ary functions satisfying the superassociative law. For an extensive information on functions, see [7, 21].

It is commonly seen that the study of hypercompositional algebra has become famous topics among mathematicians. One of outstanding classes of its is a semihypergroup, a hyperstructure that generalized semigroups but the composition of two elements is a nonempty set. There are several possibilities to construct generalizations of semihypergroups. Recall from [19] that a Menger hypercomposition algebra or a Menger hyperalgebra is a cuple $(G, \diamond)$ of a nonempty set G and one $(n+1)$-ary hyperoperation $\diamond$ on G satisfying the identity of the superassociativity. It can be noticed that a

Menger hyperalgebra can be reduced to a semihypergroup if we set $n = 1$. Furthermore, every Menger algebra is a Menger hypercomposition algebra. Normally, a representation is an essential part of the study of algebra, so representation theorems for Menger hyperalgebras are now recalled. Let A^n be the n-th Cartesian product of a nonempty set A. The symbol $P^*(A)$ stands for a power set of A without emptyset. On the set $T(A^n, P^*(A))$ of all *multivalued full n-ary functions* or *n-ary hyperoperations* $\alpha : A^n \to P^*(A)$, one can define the following $(n+1)$-ary operation $\bullet : T(A^n, P^*(A))^{n+1} \to T(A^n, P^*(A))$, called the *Menger superposition* $\bullet$, defined by

$$\bullet(f, g_1, \ldots, g_n)(x_1, \ldots, x_n) = \bigcup_{\substack{y_i \in g_i(x_1,\ldots,x_n) \\ i \in \{1,\ldots,n\}}} f(y_1, \ldots, y_n),$$

for all $i = 1, \ldots, n$ where $f, g_1, \ldots, g_n \in T(A^n, P^*(A))$, $x_1, \ldots, x_n \in A$. As a consequence, the set $T(A^n, P^*(A))$ of all multivalued full n-ary functions on A together with an $(n+1)$-ary operation $\bullet$ forms a Menger algebra.

This papar aims to apply a specific class of functions which are called medial operations (the formal definition will be recalled in the next section) into the study of Menger algebras and to describe properties of Menger hypercomposition algebras by such tools. In Section 2, the idea of medial operations is mainly presented and a representation theroem for Menger algebras via such concepts is mentioned. These lead us to generalized our study in Menger hypercompositional algebras. In addition, the conditions under which hyperstructure can be isomorphically represented by medial hyperoperations are found. Finally, some interesting remarks and some potential problems are given.

2. Results

This section begins with recalling some basic definitions of medial properties. An n-ary algebra (A, g) is said to be *medial* if it satisfies the identity

$$g(g(x_{11}, ..., x_{n1}), \ldots, g(x_{1n}, ..., x_{nn})) = g(g(x_{11}, ..., x_{1n}), \ldots, g(x_{n1}, ..., x_{nn})),$$

and an n-ary operation g on A is called medial. Furthermore, it has been studied by many authors under different names, such as Abelian, entropy, and bisymmetric algebras. On the other hand, if g satisfies the identity

$$g(g(x_{11}, ..., x_{n1}), \ldots, g(x_{1n}, ..., x_{nn})) = g(g(x_{nn}, ..., x_{n1}), \ldots, g(x_{1n}, ..., x_{11})),$$

then an algebra (A, g) is called *paramedial*. For more information about medial and paramedial properties can be found, for instance, in [2, 3, 16, 17, 24, 25, 26].

Example 2.1. Two interesting examples of mediality are collected.

(1) Every left (right) zero semigroup is a medial semigroup.

(2) Let (A, g) be an n-ary algebra. By an antiendomorphism on A we mean a mapping $\alpha : A \to A$, $\alpha(g(a_1, \ldots, a_n)) = g(\alpha(a_n), \ldots, \alpha(a_1))$. As a result if (A, g) is a paramedial n-ary algebra and $\gamma_1, \ldots, \gamma_n$ are pair wise commuting antiendomorphisms of A, then an n-ary operation g^* on A, which is defined by

$$g^*(x_1, \ldots, x_n) = g(\gamma_1(x_1), \ldots, \gamma_n(x_n)),$$

is a medial n-ary operation.

By a_1^n, we mean the sequence $a_1, \ldots, a_n$ for a positive integer n. However, it is not difficult to verify that the superassociativity does not valid for every medial n-ary operations. In order to state necessary and sufficient conditions representing an abstract Menger hypercompisitonal algebra by medial n-ary operations, we need a technical lemma.

Lemma 2.2. *For any medial n-ary operations f, g_{ij} on A, $i, j = 1, 2, \ldots, n$, we have*

$$\begin{aligned}\mathcal{O}(f, \mathcal{O}(f, g_{11}, \ldots, g_{n1}), \ldots, \mathcal{O}(f, g_{1n}, \ldots, g_{nn})) \\ = \mathcal{O}(f, \mathcal{O}(f, g_{11}, \ldots, g_{1n}), \ldots, \mathcal{O}(f, g_{n1}, \ldots, g_{nn})).\end{aligned}$$

Proof. Let $a_1, \ldots, a_n$ be elements in A. Then we obtain

$$\begin{aligned}&\mathcal{O}(f, \mathcal{O}(f, g_{11}, \ldots, g_{n1}), \ldots, \mathcal{O}(f, g_{1n}, \ldots, g_{nn}))(a_1^n) \\ =\ & f(\mathcal{O}(f, g_{11}, \ldots, g_{n1})(a_1^n), \ldots, \mathcal{O}(f, g_{1n}, \ldots, g_{nn})(a_1^n)) \\ =\ & f(f(g_{11}(a_1^n), \ldots, g_{n1}(a_1^n)), \ldots, f(g_{1n}(a_1^n), \ldots, g_{nn}(a_1^n))) \\ =\ & f(f(g_{11}(a_1^n), \ldots, g_{1n}(a_1^n)), \ldots, f(g_{n1}(a_1^n), \ldots, g_{nn}(a_1^n))) \\ =\ & f(\mathcal{O}(f, g_{11}, \ldots, g_{1n})(a_1^n), \ldots, \mathcal{O}(f, g_{n1}, \ldots, g_{nn})(a_1^n)) \\ =\ & \mathcal{O}(f, \mathcal{O}(f, g_{11}, \ldots, g_{1n}), \ldots, \mathcal{O}(f, g_{n1}, \ldots, g_{nn}))(a_1^n).\end{aligned}$$

The proof is completed. □

As a consequence, we have

Theorem 2.3. *A Menger algebra $(G, \circ)$ of rank n is isomorphically represented by medial n-ary operations defined on some set if and only if $(G, \circ)$ satisfies the equation*

$$\circ(y, \circ(y, x_{11}^{n1}), \ldots, \circ(y, x_{1n}^{nn})) = \circ(y, \circ(y, x_{11}^{1n}), \ldots, \circ(y, x_{n1}^{nn}))$$

for all $y, x_{ij} \in G$ and $i, j \in \{1, \ldots, n\}$.

Proof. The necessity follows directly from the result of Lemma 2.2. Conversely, let $(G, \circ)$ be an arbitrary Menger algebra satisfying the equation

$$\circ(y, \circ(y, x_{11}^{n1}), \ldots, \circ(y, x_{1n}^{nn})) = \circ(y, \circ(y, x_{11}^{1n}), \ldots, \circ(y, x_{n1}^{nn})).$$

We now prove that there exists an n-ary operation induced by an element g of G. For this construction, consider the set $G' = G \cup \{e, c\}$ where e and c are different elements not containing in G. For every element $g \in G$, we assign an n-ary operation $\eta_g : (G')^n \to G'$ by setting

$$\eta_g(a_1^n) = \begin{cases} \circ(g, a_1^n) & \text{if } a_i \in G \text{ for all } 1 \leqslant i \leqslant n, \\ g & \text{if } a_i = e \text{ for all } 1 \leqslant i \leqslant n, \\ c & \text{otherwise.} \end{cases}$$

Firstly, we show that the n-ary operation η_g defined above is medial. For this, let $a_{ij} \in G'$ for $i, j = 1, \ldots, n$.

If all $a_{ij} \in G$, then according to the assumption, we have

$$\begin{aligned} \eta_g(\eta_g(a_{11}^{n1}), \ldots, \eta_g(a_{1n}^{nn})) &= \circ(g, \eta_g(a_{11}^{n1}), \ldots, \eta_g(a_{1n}^{nn})) \\ &= \circ(g, \circ(g, a_{11}^{n1}), \ldots, \circ(g, a_{1n}^{nn})) \\ &= \circ(g, \circ(g, a_{11}^{1n}), \ldots, \circ(g, a_{n1}^{nn})) \\ &= \eta_g(\eta_g(a_{11}^{1n}), \ldots, \eta_g(a_{n1}^{nn})). \end{aligned}$$

In the second case, if $a_{ij} = e$ for all $i, j \in \{1, \ldots, n\}$, then we obtain

$$\eta_g(\eta_g(a_{11}^{n1}), \ldots, \eta_g(a_{1n}^{nn})) = \eta_g(g, \ldots, g) = \circ(g, g, \ldots, g).$$

Moreover, $\eta_g(\eta_g(a_{11}^{1n}), \ldots, \eta_g(a_{n1}^{nn})) = \eta_g(g, \ldots, g) = \circ(g, g, \ldots, g)$.

In other case,

$$\eta_g(\eta_g(a_{11}^{n1}), \ldots, \eta_g(a_{1n}^{nn})) = \eta_g(c, \ldots, c) = c = \eta_g(\eta_g(a_{11}^{1n}), \ldots, \eta_g(a_{n1}^{nn})).$$

So, the n-ary operation η_g is medial.

Define a mapping $\phi : (G, \circ) \to (T(G^n, G), \mathcal{O})$ by $\phi(g) = \eta_g$ for all $g \in G$. To prove the injectivity of ϕ, let $g_1, g_2 \in G$. Suppose that $\phi(g_1) = \phi(g_2)$. Then for all $a_1, \ldots, a_n \in G$, we have $\eta_{g_1}(a_1, \ldots, a_n) = \eta_{g_2}(a_1, \ldots, a_n)$. In

particular, $\eta_{g_1}(e,\dots,e) = \eta_{g_2}(e,\dots,e)$, which implies that $g_1 = g_2$. So, ϕ is injective. Finally, we show that the identity

$$\eta_{\circ(x,y_1,\dots,y_n)} = \mathcal{O}(\eta_x, \eta_{y_1}, \dots, \eta_{y_n})$$

holds for all $x, y_1, \dots, y_n \in G$. For this, let $a_1, \dots, a_n$ be arbitrary elements in G'. If $a_i \in G$ for all $1 \leqslant i \leqslant n$, then for $x, y_1, \dots, y_n \in G$, applying the superassociativity of $(n+1)$-ary operation $\circ$ on G, we have

$$\begin{aligned}
\eta_{\circ(x,y_1,\dots,y_n)}(a_1,\dots,a_n) &= \circ(\circ(x,y_1,\dots,y_n),a_1,\dots,a_n)\\
&= \circ(x,\circ(y_1,a_1,\dots,a_n),\dots,\circ(y_n,a_1,\dots,a_n))\\
&= \eta_x(\eta_{y_1}(a_1,\dots,a_n),\dots,\eta_{y_n}(a_1,\dots,a_n))\\
&= \mathcal{O}(\eta_x,\eta_{y_1},\dots,\eta_{y_n})(a_1,\dots,a_n).
\end{aligned}$$

If $(a_1,\dots,a_n) = (e,\dots,e)$, then $\eta_{\circ(x,y_1,\dots,y_n)}(e,\dots,e) = \circ(x,y_1,\dots,y_n)$. On the other hand, we get $\eta_x(y_1,\dots,y_n) = \eta_x(\eta_{y_1}(e,\dots,e),\dots,\eta_{y_n}(e,\dots,e)) = \mathcal{O}(\eta_x,\eta_{y_1},\dots,\eta_{y_n})(e,\dots,e)$. Now, if $(a_1,\dots,a_n) \in (G')^n \backslash (G^n \cup \{(e,\dots,e)\})$, then we get $\eta_{\circ(x,y_1,\dots,y_n)}(a_1,\dots,a_n) = c$ and $\mathcal{O}(\eta_x,\eta_{y_1},\dots,\eta_{y_n})(a_1,\dots,a_n) = \eta_x(\eta_{y_1}(c,\dots,c),\dots,\eta_{y_n}(c,\dots,c)) = \eta_x(c,\cdots,c) = c$, which implies

$$\eta_{\circ(x,y_1,\dots,y_n)}(a_1,\dots,a_n) = c = \mathcal{O}(\eta_x,\eta_{y_1},\dots,\eta_{y_n})(a_1,\dots,a_n).$$

This completes the proof of this theorem. □

Applyig the same construction of the n-ary operation η_g, we can prove a representation theorem of any Menger algebra by paramedial operations. So, we obtain the following corollary.

Corollary 2.4. *A Menger algebra $(G,\circ)$ of rank n is isomorphically represented by paramedial n-ary operations defined on some set if and only if $(G,\circ)$ satisfies the equation*

$$\circ(y,\circ(y,x_{11}^{n1}),\dots,\circ(y,x_{1n}^{nn})) = \circ(y,\circ(y,x_{nn},\dots,x_{n1}),\dots,\circ(y,x_{1n},\dots,x_{11}))$$

for all $y, x_{ij} \in G$ and $i,j \in \{1,\dots,n\}$.

Now the investigation in Menger algebras is finished. We continue our study on Menger hypercompositional algebras. In our conjecture, the situation for Menger hypercompositional algebras is different. To attain this purpose, the concept of medial hyperoperations is now introduced. An n-ary hyperoperation f on A is said to be *medial* if

$$f(f(x_{11}^{n1}),\dots,f(x_{1n}^{nn})) = f(f(x_{11}^{1n}),\dots,f(x_{n1}^{nn})).$$

For convenience, we may rewrite the above identity in the following form:

$$\bigcup_{\substack{y_i\in f(x_{1i}^{ni})\\ i\in\{1,\dots,n\}}} f(y_1^n) = \bigcup_{\substack{y_i\in f(x_{i1}^{in})\\ i\in\{1,\dots,n\}}} f(y_1^n).$$

The following theorem presents a mediality of medial hyperoperations in a connection with permutations.

Theorem 2.5. *Let f be a medial n-ary hyperoperation on a nonempty set A and π be a permutation on $\{1,\dots,n\}$. Then the n-ary hyperoperation $\widehat{f}$ on A, which is defined by $\widehat{f}(a_1,\dots,a_n) = f(a_{\pi(1)},\dots,a_{\pi(n)})$, is medial.*

Proof. For every $i,j\in\{1,\dots,n\}$, let $a_{ij}\in A$. Then we obtain

$$\begin{aligned}\bigcup_{\substack{b_i\in\widehat{f}(a_{1i},\dots,a_{ni})\\ i\in\{1,\dots,n\}}} \widehat{f}(b_1,\dots,b_n) &= \bigcup_{\substack{b_{\pi(i)}\in f(a_{\pi(1)\pi(i)},\dots,a_{\pi(n)\pi(i)})\\ i\in\{1,\dots,n\}}} f(b_{\pi(1)},\dots,b_{\pi(n)})\\ &= \bigcup_{\substack{b_{\pi(i)}\in f(a_{\pi(i)\pi(1)},\dots,a_{\pi(i)\pi(n)})\\ i\in\{1,\dots,n\}}} f(b_{\pi(1)},\dots,b_{\pi(n)})\\ &= \bigcup_{\substack{b_i\in\widehat{f}(a_{i1},\dots,a_{in})\\ i\in\{1,\dots,n\}}} \widehat{f}(b_1,\dots,b_n).\end{aligned}$$

This shows that the n-ary hyperoperation $\widehat{f}$ is medial. □

Theorem 2.6. *A Menger hypercompositonal algebra $(G,\diamond)$ of rank n is isomorphically represented by medial n-ary hyperoperations defined on some set if and only if $(G,\diamond)$ satisfies the equation*

$$\bigcup_{\substack{y_i\in\diamond(y,x_{1i}^{ni})\\ i\in\{1,\dots,n\}}} \diamond(y,y_1^n) = \bigcup_{\substack{y_i\in\diamond(y,x_{i1}^{in})\\ i\in\{1,\dots,n\}}} \diamond(y,y_1^n)$$

for all $y,x_{ij}\in G$ and $i,j\in\{1,\dots,n\}$.

Proof. Let $j=1,\dots,n$ and f,g_{1j}^{nj} be arbitrary medial n-ary hyperoperations. Then we have

$$\bullet(f,\bullet(f,g_{11}^{n1}),\dots,\bullet(f,g_{1n}^{nn}))(a_1^n) = \bigcup_{\substack{y_i\in\bullet(f,g_{1i}^{ni})(a_1^n)\\ i\in\{1,\dots,n\}}} f(y_1^n) = \bigcup_{\substack{y_i\in f(g_{1i}(a_1^n),\dots,g_{ni}(a_1^n))\\ i\in\{1,\dots,n\}}} f(y_1^n)$$

$$= \bigcup_{\substack{y_i \in f(g_{i1}(a_1^n),\ldots,g_{in}(a_1^n)) \\ i\in\{1,\ldots,n\}}} f(y_1^n) = \bigcup_{\substack{y_i \in \bullet(f,g_{i1},\ldots,g_{in})(a_1^n) \\ i\in\{1,\ldots,n\}}} f(y_1^n)$$
$$= \bullet(f, \bullet(f, g_{11}^{1n}), \ldots, \bullet(f, g_{n1}^{nn}))(a_1^n).$$

For the converse, let $G' = G \cup \{e, c\}$ where $e, c \notin G$ and $e \neq c$. Firstly, we now construct an n-ary hyperoperation G'. For each element $g \in G'$, an n-ary hyperoperation on G' can be defined by setting

$$\mu_g(a_1, \ldots, a_n) = \begin{cases} \diamond(g, a_1^n) & \text{if } a_1^n \in G; \\ \{g\} & \text{if } a_1 = \cdots = a_n = e; \\ \{c\} & \text{otherwise}. \end{cases}$$

Moreover, the extension of the multivalued full n-ary function is needed. For any nonempty subset A of G', the function μ_A is defined by

$$\mu_A(a_1^n) = \begin{cases} \diamond(A, a_1^n) & \text{if } a_1, \ldots, a_n \in G; \\ A & \text{if } a_1 = \cdots = a_n = e; \\ \{c\} & \text{otherwise}. \end{cases}$$

To show that μ_g is a medial n-ary hyperoperation, let $a_{ij} \in G'$ for every $i, j = 1, \ldots, n$. We first consider in the case when $a_{1j}^{nj} \in G$. Then we obtain

$$\bigcup_{\substack{b_i \in \mu_g(a_{1i}^{ni}) \\ i\in\{1,\ldots,n\}}} \mu_g(b_1^n) = \bigcup_{\substack{b_i \in \diamond(g,a_{1i}^{ni}) \\ i\in\{1,\ldots,n\}}} \diamond(g, b_1^n) = \bigcup_{\substack{b_i \in \diamond(g,a_{i1}^{in}) \\ i\in\{1,\ldots,n\}}} \diamond(g, b_1^n) = \bigcup_{\substack{b_i \in \mu_g(a_{i1}^{in}) \\ i\in\{1,\ldots,n\}}} \mu_g(b_1^n).$$

In the second case, if $a_{1j} = \cdots = a_{nj} = e$ for all $j = 1, \ldots, n$, we have

$$\bigcup_{\substack{b_i \in \mu_g(a_{1i}^{ni}) \\ i\in\{1,\ldots,n\}}} \mu_g(b_1^n) = \bigcup_{\substack{b_i \in \mu_g(e,\ldots,e) \\ i\in\{1,\ldots,n\}}} \mu_g(b_1^n) = \bigcup_{\substack{b_i \in \{g\} \\ i\in\{1,\ldots,n\}}} \mu_g(b_1^n) = \mu_g(g, \ldots, g)$$
$$= \diamond(g, g, \ldots, g) = \bigcup_{\substack{b_i \in \mu_g(e,\ldots,e) \\ i\in\{1,\ldots,n\}}} \mu_g(b_1^n) = \bigcup_{\substack{b_i \in \mu_g(a_{i1}^{in}) \\ i\in\{1,\ldots,n\}}} \mu_g(b_1^n).$$

In other case, by the construction of μ_g, we have

$$\bigcup_{\substack{b_i \in \mu_g(a_{1i}^{ni}) \\ i\in\{1,\ldots,n\}}} \mu_g(b_1^n) = \bigcup_{\substack{b_i \in \{c\} \\ i\in\{1,\ldots,n\}}} \mu_g(b_1^n) = \{c\} = \bigcup_{\substack{b_i \in \mu_g(a_{i1}^{in}) \\ i\in\{1,\ldots,n\}}} \mu_g(b_1^n).$$

As a result, the hyperoperation μ_g with respect to each element g is medial.

Now we show that the mapping $\varphi : G \to \Lambda'$, which is defined by $\varphi(g) = \mu_g$ for all $g \in G$, is a strong isomorphism between $(G, \diamond)$ and

$(T(G^n, P^*(G)), \bullet)$ where $\Lambda' = \{\mu_g \mid g \in G\}$. In order to prove this property, we show

$$\mu_{\diamond(a,b_1,\dots,b_n)} = \bullet(\mu_a, \mu_{b_1}, \dots, \mu_{b_n})$$

for any $a, b_1, \dots, b_n \in G'$.

Let $x_1, \dots, x_n \in G$. Then we first show that the equation

$$\mu_{\diamond(a,b_1,\dots,b_n)}(x_1^n) = \bullet(\mu_a, \mu_{b_1}, \dots, \mu_{b_n})(x_1^n).$$

holds. For this, let $a, b_1, \dots, b_n, x_1, \dots, x_n$ be arbitrary elements in G. Then

$$\begin{aligned}\mu_{\diamond(a,b_1,\dots,b_n)}(x_1^n) &= \diamond(\diamond(a, b_1^n), x_1^n) = \diamond(a, \diamond(b_1, x_1^n), \dots, \diamond(b_n, x_1^n)) \\ &= \diamond(a, \mu_{b_1}(x_1^n), \dots, \mu_{b_n}(x_1^n)) = \bigcup_{\substack{y_i \in \mu_{b_i}(x_1^n) \\ i \in \{1,\dots,n\}}} \diamond(a, y_1^n) \\ &= \bigcup_{\substack{y_i \in \mu_{b_i}(x_1^n) \\ i \in \{1,\dots,n\}}} \mu_a(y_1^n) = \bullet(\mu_a, \mu_{b_1}, \dots, \mu_{b_n})(x_1^n).\end{aligned}$$

Now let $x_1 = \cdots = x_n = e$, then according to the definition of μ_A, we have

$$\begin{aligned}\mu_{\diamond(a,b_1,\dots,b_n)}(x_1^n) &= \mu_{\diamond(a,b_1^n)}(e, \dots, e) = \diamond(a, b_1^n) = \mu_a(b_1^n) = \bigcup_{\substack{y_i \in \{b_i\} \\ i \in \{1,\dots,n\}}} \mu_a(y_1^n) \\ &= \bigcup_{\substack{y_i \in \mu_{b_i}(e,\dots,e) \\ i \in \{1,\dots,n\}}} \mu_a(y_1^n) = \bullet(\mu_a, \mu_{b_1}, \dots, \mu_{b_n})(e, \dots, e) \\ &= \bullet(\mu_a, \mu_{b_1}, \dots, \mu_{b_n})(x_1^n),\end{aligned}$$

which implies $\mu_{\diamond(a,b_1,\dots,b_n)}(e, \dots, e) = \bullet(\mu_a, \mu_{b_1}, \dots, \mu_{b_n})(e, \dots, e)$.

Otherwise, we have $\mu_{\diamond(a,b_1,\dots,b_n)}(z_1^n) = \{c\}$ and

$$\begin{aligned}\bullet(\mu_a, \mu_{b_1}, \dots, \mu_{b_n})(z_1^n) &= \bigcup_{\substack{y_i \in \mu_{b_i}(z_1^n) \\ i \in \{1,\dots,n\}}} \mu_a(y_1^n) = \bigcup_{\substack{y_i \in \{c\} \\ i \in \{1,\dots,n\}}} \mu_a(y_1, \dots, y_n) \\ &= \mu_a(c, \dots, c) = \{c\},\end{aligned}$$

which shows $\mu_{\diamond(a,b_1,\dots,b_n)}(z_1^n) = \bullet(\mu_a, \mu_{b_1}, \dots, \mu_{b_n})(z_1^n)$. This completes the proof of the homomorphism property.

In order to prove that μ_g is injective, suppose $\mu_a = \mu_b$. Since e is an element in the domian of μ_a and μ_b, then $\mu_a(e, \dots, e) = \mu_b(e, \dots, e)$, and $\{a\} = \{b\}$. Hence, $a = b$. So the mapping $\varphi : g \mapsto \mu_g$ is an isomorphism. □

Corollary 2.7. *A Menger hypercompositional algebra $(G, \diamond)$ of rank n is isomorphically represented by paramedial n-ary hyperoperations defined on some set if and only if $(G, \diamond)$ satisfies the equation*

$$\diamond(y, \diamond(y, x_{11}^{n1}), \ldots, \diamond(y, x_{1n}^{nn})) = \diamond(y, \diamond(y, x_{nn}, \ldots, x_{n1}), \ldots, \diamond(y, x_{1n}, \ldots, x_{11}))$$

for all $y, x_{ij} \in G$ *and* $i, j \in \{1, \ldots, n\}$.

3. Concluding remarks

In the given paper, applying medial operations in the study of medial algebras, a representation theorem for Menger algebras via such operations was proved. Several results connecting Menger hypercompositional algebras and medial hyperoperations were developed. The main goals of these studies were to introduce a novel concept of operations and hyperoperations that generated by a certain classes of mediality and to generalize the investigation in Menger algebras to Menger hypercompositional algebras. To achieve these two aims, some technical tools that derived from the idea of W.A. Dudek and V.S. Trokhimenko were applied.

Finally, two problems for the future research in this area are collected.

(1) Describe algebraic properties of medial operations and medial hyperoperations.

(2) According to Chapter 6 in the monograph [7], systems of multiplace functions are described. It is possible to generalize Menger systems to Menger hypercompsitional systems and try to discuss a construction of a mapping λ_g with repect to each element g in a family of Menger hypercompositonal system $(G_n)_{n\in I}$. Find necessary and sufficient conditions under which a Menger hypercompositional system can be represented by medial hyperoperations.

Acknowledgment. This work was supported by Rajamangala University of Technology Rattanakosin, Thailand.

References

[1] **M. Al Tahan, B. Davvaz**, *A class of representations of Artin braid hypergroups*, Asian-Eur. J. Math., **13** (2020), no. 3, Article ID: 2050056.

[2] **S.S. Davidov**, *On the structure of medial divisible n-ary groupoids*, Math. Notes, **104** (2018), no. 1, 33 – 44.

[3] **S.S. Davidov**, *Regular medial division algebras*, Quasigroups Related Systems, **21** (2013), no. 2, 155-164.

[4] **K. Denecke**, *Partial clones*, Asian-Eur. J. Math., **13** (2020), no. 8, Article ID: 2050161.

[5] **K. Denecke and H. Hounnon**, *Partial Menger algebras of terms*, Asian-Eur. J. Math., **15** (2021), no. 6, Article ID: 2150092.

[6] **W.A. Dudek**, *In memoriam: Valentin S. Trokhimenko*, Quasigroups Related Systems, **28** (2020), 171 – 176.

[7] **W.A. Dudek and V.S. Trokhimenko**, *Algebras of multiplace functions*, De Gruyter, Berlin, (2012), 389 pp.

[8] **W.A. Dudek and V.S. Trokhimenko**, *De Morgan* $(2, n)$*-semigroups of* n*-place functions*, Comm. Algebra, **44** (2016), 4430-4437.

[9] **W.A. Dudek and V.S. Trokhimenko**, *Menger algebras of associative and self-distributiven-ary operations*, Quasigroups Related Systems, **26** (2018), 45 – 52.

[10] **W.A. Dudek and V.S. Trokhimenko**, *Menger algebras of idempotent* n*-ary operations*, Stud. Sci. Math. Hung., **55** (2019), 260 – 269.

[11] **W.A. Dudek and V.S. Trokhimenko**, *Menger algebras of* k*-commutative* n*-place functions*, Georgian Math. J., **28** (2021), no. 3, 355 – 361.

[12] **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.

[13] **W.A. Dudek and V.S. Trokhimenko**, *On some subtraction Menger algebras of multiplace functions*, Semigroup Forum, **93** (2016), 375 – 386.

[14] **W.A. Dudek and V.S. Trokhimenko**, *Stabilizers of functional Menger systems*, Comm. Algebra, **37** (2009), 985 – 1000.

[15] **W.A. Dudek and V.S. Trokhimenko**, *The relations of semiadjacency and semicompatibility in* n*-semigroups of transformations*, Semigroup Forum, **90** (2015), 113 – 125.

[16] **A. Ehsani and Yu. M. Movsisyan**, *A representation of paramedial* n*-ary groupoids*, Asian-Eur. J. Math., **7** (2014), no. 1, Article ID: 1450020.

[17] **A. Ehsani and Yu. M. Movsisyan**, *Linear representation of medial-like algebras*, Comm. Algebra, **41** (2013), no.9, 3429 – 3444.

[18] **T. Kumduang and S. Leeratanavalee**, *Left translations and isomorphism theorems for Menger algebras of rank* n, Kyungpook Math. J., **61** (2021), no. 2, 223 – 237.

[19] **T. Kumduang and S. Leeratanavalee**, *Menger hyperalgebras and their representations*, Comm. Algebra, **49** (2021), no. 4, 1513 – 1533.

[20] **T. Kumduang and S. Leeratanavalee**, *Semigroups of terms, tree languages, Menger algebra of n-ary functions and their embedding theorems*, Symmetry, **13** (2021), no. 4, Article 558.

[21] **D. Lau**, *Function algebras on finite sets. A basic course on many-valued logic and clone theory*. Springer-Verlag, Berlin, Heidelberg, (2006)

[22] **A. Molkhasi**, *Representations of Sheffer stroke algebras and Visser algebras*, Soft Computing, **25** (2021), 8533 – 8538.

[23] **A. Nongmanee and S. Leeratanavalee**, *Ternary Menger algebras: a generalization of ternary semigroups*, Mathematics, **9** (2021), no. 5, Article 553.

[24] **N. Sawatraksa and C. Namnak**, *Some remarks on paramedial semigroups and medial semigroups*, Thai J. Math., Special Issue: Annual Meeting in Mathematics (2019), 167 – 176.

[25] **V. Shcherbacov**, *On structure of finite n-ary medial quasigroups and automorphism groups of these quasigroups*, Quasigroups Related Systems, **13** (2005), 125 – 156.

[26] **Z. Stojalović**, *Medial cyclic n-quasigroups*, Novi Sad J. Math., **28** (1998), no. 1, 47 – 54.

[27] **T. Suksumran**, *Complete reducibility of gyrogroup representations*, Comm. Algebra, **48** (2020), no. 2, 847 – 856.

[28] **K. Wattanatripop, T. Kumduang, S. Leeratanavalee, and T. Changphas**, *Power Menger algebra of terms induced by order-decreasing transformations and superpositions*, Int. J. Math. Comput. Sci., **16** (2021), no. 4, 1697 – 1707.

Received July 8, 2021

School of General Science, Faculty of Liberal Arts, Rajamangala University of Technology Rattanakosin, Thailand

E-mail: Kumduang01@gmail.com

Quasigroups and Related Systems **31** (2023), 275 – 286

Topological S-act congruence

Sunil Kumar Maity and Monika Paul

Abstract. In this paper, we establish the necessary and sufficient condition for an equivalence relation ρ on an S-act A endowed with a topology such that A/ρ becomes a Hausdorff topological S-act. Also, we show that if A_1 and A_2 be two topological S-acts, then for any homomorphism $\varphi : A_1 \to A_2$, $A_1/\ker\varphi$ is a topological S-act if and only if φ is φ-saturated continuous. Moreover, we establish for any two congruences θ_1 and θ_2 on an S-act A endowed with a topology, $\theta_1 \cap \theta_2$ is a topological S-act congruence on A if and only if the mapping $\varphi : A \to A/\theta_1 \times A/\theta_2$, defined by $\varphi(a) = (a\theta_1, a\theta_2)$, for all $a \in A$, is φ-saturated continuous, where S is a topological semigroup.

1. Introduction and preliminaries

Analogous to topological group actions, topological semigroup actions plays an important role in the study of semigroup action theory. There are wide application of topological semigroup action in many fields like manifold, topological vector space etc. Properties of topological semigroup actions have been recently studied by many authors, for example, P. Normak, B. Khosravi and others (see [8], [4]). In [4], the author established a necessary and sufficient conditions for a congruence on a topological S-act to be topological S-act congruence.

Recall that a semigroup $(S, \cdot)$ is a nonempty set together with a binary operation on S satisfying the associative law, i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in S$. Let S be a semigroup and A be a nonempty set. Then A is said to be a left S-act if there is an action $\lambda : S \times A \to A$ defined by $\lambda(s, a) = sa$ such that $(st)a = s(ta)$, for all $s, t \in S$ and $a \in A$. Throughout this paper, by an S-act, we always mean a left S-act. An equivalence relation θ on an S-act A is said to be a congruence on A if, for all $a, b \in A$ and $s \in S$, $(a, b) \in \theta$

2010 Mathematics Subject Classification: 22A20, 20M30
Keywords: Topological semigroup, S-act topological congruence, topological S-act congruence

implies $(sa, sb) \in A$. For any two S-acts A and B, a mapping $f : A \to B$ is said to be a homomorphism if $f(sa) = sf(a)$, for all $s \in S, a \in A$.

A semigroup S endowed with a topology τ is said to be a topological semigroup if the binary operation $\mu : \begin{smallmatrix} S\times S\to S \\ (x,y)\mapsto xy \end{smallmatrix}$ is continuous. Let S be a semigroup endowed with a topology τ and A be a nonempty set endowed with a topology $\tau_{_A}$. Then A is said to be an S-act topological space if the action $\lambda : S \times A \to A$ is continuous. Now an S-act topological space A is said to be a topological S-act if S is a topological semigroup.

Let S be a semigroup endowed with a topology τ and A be an S-act endowed with a topology $\tau_{_A}$. Also, let θ be an equivalence relation on A. Consider the natural mapping $\pi : A \to A/\theta$ defined by $\pi(a) = a\theta$, for all $a \in A$. Define a topology on A/θ as follows : a subset U of A/θ is open in A/θ if and only if $\pi^{-1}(U)$ is open in A. With this topology, π is a quotient map and A/θ is called a quotient space. Two S-acts A and B endowed with topologies $\tau_{_A}$ and $\tau_{_B}$ respectively are said to be topologically isomorphic if there exists a homomorphism $\varphi : A \to B$ which is also a homeomorphism. Moreover, for a semigroup S endowed with a topology, a congruence θ on an S-act A endowed with a topology τ is said to be a S-act topological congruence if A/θ is an S-act topological space. In addition, for a topological semigroup S, a congruence θ on an S-act A endowed with a topology τ is said to be a topological S-act congruence if A/θ is a topological S-act.

2. Congruence on a topological S-act

Let S be a semigroup endowed with a topology τ, A be an S-act endowed with a topology $\tau_{_A}$ and θ be an equivalence relation on A. Consider the natural map $\pi : A \to A/\theta$ defined by $\pi(a) = a\theta$ and the set $\tau_{_\theta} = \{B \in \tau_{_A} : \pi^{-1}\pi(B) = B\}$. It can easily be shown that $\tau_{_\theta}$ is a topology on A. We first state a very useful result from [4].

Theorem 2.1. *Let A be a topological S-act and θ be a congruence on A. Then A/θ is a topological S-act if and only if $(A, \tau_{_\theta})$ is a topological S-act.*

From Theorem 2.1, we have the following two corollaries which will be very useful in our discussion.

Corollary 2.2. *Let S be a semigroup endowed with a topology τ and A be an S-act endowed with a topology $\tau_{_A}$. Then for any congruence θ on A,*

A/θ is an S-act topological space if and only if (A, τ_θ) is an S-act topological space.

Corollary 2.3. *Let S be a topological semigroup and A be an S-act endowed with a topology τ_A. Then for any congruence θ on A, A/θ is a topological S-act if and only if (A, τ_θ) is a topological S-act.*

We now present a necessary and sufficient condition for an equivalence relation ρ on an S-act A endowed with a topology to be an S-act topological congruence.

Theorem 2.4. *Let S be a semigroup endowed with a topology τ and A be an S-act endowed with a topology τ_A. Then for any equivalence relation θ on A such that A/θ is a Hausdorff space, A/θ is an S-act topological space if and only if (A, τ_θ) is an S-act topological space.*

Proof. Let A/θ be an S-act topological space. Then θ is a congruence on A. Hence by Corollary 2.2, (A, τ_θ) is an S-act topological space. Conversely, let (A, τ_θ) be an S-act topological space. Let $(a, b) \in \theta$ and $s \in S$. If possible, let $(sa, sb) \notin \theta$. Then $[sa] \neq [sb]$, where by $[x]$ we mean the θ-equivalence class containing the element $x \in X$. Since S/θ is Hausdorff, there exist disjoint open sets G and H containing $[sa]$ and $[sb]$ respectively in A/θ. Then $sa \in \pi^{-1}(G)$ and $sb \in \pi^{-1}(H)$. Since π is continuous, it follows that $\pi^{-1}(G)$ and $\pi^{-1}(H)$ are open in (A, τ_θ). Now (A, τ_θ) being S-act topological space, there exist open sets U_1 and V_1 in (S, τ) and (A, τ_θ) respectively such that $s \in U_1$, $a \in V_1$ and $U_1V_1 \subseteq \pi^{-1}(G)$. Similarly, there exist open sets U_2 and V_2 in (S, τ) and (A, τ_θ) respectively such that $s \in U_2$, $b \in V_2$ and $U_2V_2 \subseteq \pi^{-1}(H)$. Let $U = U_1 \cap U_2$. Then $s \in U$. As $(a, b) \in \theta$, we have $[a] = [b] \in \pi(V_1) \cap \pi(V_2)$ and thus $a, b \in V_1 \cap V_2 = V$ (say). This implies $sa, sb \in UV \subseteq \pi^{-1}(G) \cap \pi^{-1}(H)$ which implies that $G \cap H \neq \emptyset$, a contradiction. Therefore, $[sa] = [sb]$ and hence θ is a congruence on S. Consequently, by Corollary 2.2, it follows that A/θ is an S-act topological space. □

Using Theorem 2.4, we at once have the following corollary.

Corollary 2.5. *Let (S, τ) be a topological semigroup and A be an S-act endowed with a topology τ_A. Then for any equivalence relation θ such that A/θ is Hausdorff, A/θ is a topological S-act if and only if (A, τ_θ) is a topological S-act.*

It is well known that image of an S-act is an S-act. But continuous image of a topological S-act need not be a topological S-act. This follows from the following examples.

Example 2.6. Consider the topological semigroup $S = (\mathbb{Z}_6, \tau_{dis})$, where τ_{dis} is the discrete topology on $\mathbb{Z}_6$. Also, let $A = S$ and $B = (\mathbb{Z}_6, \tau_1)$, where $\tau_1 = \{\mathbb{Z}_6, \emptyset, \{\bar{4}\}\}$. Then A is a topological S-act. Consider the map $\varphi : A \to B$ defined by $\varphi(\bar{x}) = \overline{2x}$. Then $\varphi(A) = \{\bar{0}, \bar{2}, \bar{4}\}$ and the subspace topology on $\varphi(A)$ is given by $\tau_{\varphi(A)} = \{\varphi(A), \emptyset, \{\bar{4}\}\}$. It is easy to verify that φ is continuous and $\varphi(A)$ is an S-act. Now, for the open set $\{\bar{4}\}$ in $\varphi(A)$ with $s \cdot a \in \{\bar{4}\}$, where $s = \bar{2} \in S$ and $a = \bar{2} \in \varphi(A)$, there is no open set U containing a in $\varphi(A)$ such that $\{s\} \cdot U \subseteq \{\bar{4}\}$, where $\{s\}$ is open in S. Hence $\varphi(A)$ is not a topological S-act.

We now establish some sufficient conditions for which continuous image of a topological S-act will be a topological S-act. For this purpose, we first define φ-saturated continuity of between two S-acts A and B.

Definition 2.7. Let S be a semigroup endowed with a topology τ. Let A_1 and A_2 be S-acts endowed with topologies τ_1 and τ_2 respectively. Then a mapping $\varphi : A_1 \to A_2$ is said to be *φ-saturated continuous* if for any subset W of A_2 with $\varphi^{-1}(W)$ is open in A_1 and $s \in S$, $a \in A_1$ with $sa \in \varphi^{-1}(W)$, there exist open sets U and V in (S, τ) and $(A_1, \tau_{\ker \varphi})$ containing s and a respectively such that $UV \subseteq \varphi^{-1}(W)$, where $\ker \varphi = \{(a, b) \in A_1 \times A_1 : \varphi(a) = \varphi(b)\}$.

Now we characterize φ-saturated continuous map between two topological S-acts.

Proposition 2.8. *Let S be a topological semigroup. Any injective mapping $\varphi : A \to B$ between two topological S-acts A and B is always φ-saturated continuous.*

Proof. Let $\varphi : A \to B$ be an injective mapping between two topological S-acts A and B. Let W be a subset of B with $\varphi^{-1}(W)$ is open in A and $s \in S$, $a \in A$ with $sa \in \varphi^{-1}(W)$. Now A being a topological S-act, there exist open sets U and V in S and A containing s and a respectively such that $UV \subseteq \varphi^{-1}(W)$. Now φ being injective, $\varphi^{-1}(\varphi(V)) = V$ and this implies that $V \in \tau_{\ker \varphi}$. Hence the result. □

By a counter-example below, we conclude that the converse of the Proposition 2.8 may not be true.

Example 2.9. Let $S = A = B = (\mathbb{Z}_6, \cdot_6, \tau)$, where $\tau = \{\mathbb{Z}_6, \emptyset, \{\bar{0}, \bar{3}\}, \{\bar{1}, \bar{2}, \bar{4}, \bar{5}\}\}$. Then S is a topological semigroup where A and B can be thought of as a topological S-acts. Consider the mapping $\varphi : A \to B$ defined by $\varphi(a) = 2a$, for all $a \in A$. Clearly, φ is not injective. But it can be easily verify that φ is φ-saturated continuous.

By the following example, we prove that any φ-saturated continuous map φ between two topological S-acts may not be continuous.

Example 2.10. Let $S = B = (\mathbb{Z}_6, \cdot_6, \tau_{discrete})$ and $A = (\mathbb{Z}_6, \cdot_6, \tau_{indiscrete})$. Then S is a topological semigroup where A and B are topological S-acts. Consider the identity map $id_{_A} : A \to B$. Now $id_{_A}$ being injective, $id_{_A}$ is a $id_{_A}$-saturated continuous map. But it can be easily check that $id_{_A}$ is not a continuous map.

Now we discuss the topological influence of a φ-saturated continuous image of a S-act endowed with a topology.

Theorem 2.11. *Let S be a topological semigroup. Let A and B be two S-acts endowed with topologies $\tau_{_A}$ and $\tau_{_B}$ respectively such that $(A, \tau_{_A})$ is a topological S-act. Also, assume that $\varphi : A \to B$ be a homomorphism which is a quotient map. Then B is a topological S-act if any one of the following two conditions holds:*

(i) φ is an open map.

(ii) φ is φ-saturated continuous.

Proof. (i). Let φ be open. Let W be open in B with $s\varphi(a) \in W$, where $s \in S$ and $a \in A$. Then $sa \in \varphi^{-1}(W)$. Because of the continuity of φ, $\varphi^{-1}(W)$ is open in A. Now, A being a topological S-act, there exit open sets U in S and V in A containing s and a respectively such that $UV \subseteq \varphi^{-1}(W)$. Since φ is open, we must have $\varphi(V)$ is open in B with $\varphi(a) \in \varphi(V)$. Moreover, $U\varphi(V) \subseteq W$ and thus B is a topological S-act.

(ii). Let φ be φ-saturated continuous. Let W_1 be open in B with $t\varphi(a) \in W_1$, where $t \in S$ and $a \in A$. Then $ta \in \varphi^{-1}(W_1)$. Because of the continuity of φ, $\varphi^{-1}(W_1)$ is open in A. Now, φ being φ-saturated continuous, there exist open sets U_1 and V_1 in S and $(A, \tau_{\ker\varphi})$ containing t and a respectively such that $U_1V_1 \subseteq \varphi^{-1}(W_1)$. One can easily verify that $\varphi^{-1}(\varphi(V_1)) = V_1$. Now φ being a quotient map, $\varphi(V_1)$ is open in B with $\varphi(a) \in \varphi(V_1)$. Also, $U_1\varphi(V_1) \subseteq W_1$. Hence B is a topological S-act. □

We know that the kernel of a homomorphism between two S-acts is always a congruence. But the kernel of a homomorphism between two topological S-acts need not be a topological S-act congruence. Using Theorem 2.11, we have the following corollary which ensures that the kernel of a homomorphism between two topological S-acts is a topological S-act congruence.

Corollary 2.12. *Let S be a topological semigroup. Let A and B be two S-acts endowed with topologies τ_1 and τ_2 respectively such that (A, τ_1) is a topological S-act. Also, assume that $\varphi : A \to B$ is a homomorphism which is also a quotient map. If φ is φ-saturated continuous, then B is topologically isomorphic to $A/\ker\varphi$ and hence $A/\ker\varphi$ is a topological S-act.*

Remark 2.13. For any two S-acts A and B, any homomorphism $\varphi : A \to B$ induces an S-act $A/\ker\varphi$. But for any two topological S-acts A and B, any homomorphism $\varphi : A \to B$ need not induce topological S-act $A/\ker\varphi$, i.e., $A/\ker\varphi$ need not be a topological S-act. Now, we establish a necessary and sufficient condition on the homomorphism $\varphi : A \to B$ so that $A/\ker\varphi$ will be a topological S-act.

Theorem 2.14. *Let S be a semigroup endowed with a topology τ. Also, let A_1 and A_2 be S-acts endowed with topologies τ_1 and τ_2 respectively. Then for any mapping $\varphi : A_1 \to A_2$ such that $\ker\varphi$ is a congruence on A_1, $A_1/\ker\varphi$ is an S-act topological space if and only if φ is φ-saturated continuous.*

Proof. Let us define a map $f : A_1/\ker\varphi \to A_2$ by $f(a\ker\varphi) = \varphi(a)$, for all $a\ker\varphi \in A_1/\ker\varphi$. Then $f \circ \pi = \varphi$, where $\pi : A_1 \to A_1/\ker\varphi$ is defined by $\pi(a) = a\ker\varphi$, for all $a \in A_1$.

First suppose that $A_1/\ker\varphi$ is an S-act topological space. Let W be a subset of A_2 such that $\varphi^{-1}(W)$ is open in A_1. Let $s \in S$, $a \in A_1$ with $sa \in \varphi^{-1}(W)$. Then $sa \in \pi^{-1}(f^{-1}(W))$. Now, $A_1/\ker\varphi$ being an S-act topological space, by Corollary 2.2, $(A_1, \tau_{\ker\varphi})$ is an S-act topological space. So, there exist open sets U and V containing s and a in (S, τ) and $(A_1, \tau_{\ker\varphi})$ respectively such that $UV \subseteq \pi^{-1}(f^{-1}(W))$. This implies that $UV \subseteq \varphi^{-1}(W)$ and hence φ is φ-saturated continuous.

Conversely, let φ be φ-saturated continuous. Let $G \in \tau_{\ker\varphi}$ and $t \in S$, $a \in A_1$ with $ta \in G$. Then $ta \in G = \pi^{-1}(\pi(G))$. Since f is injective, $G = \pi^{-1}(\pi(G)) = \varphi^{-1}(f(f^{-1}(\varphi(G))))$. Now, φ being φ-saturated continuous, there exist open sets U_1 and V_1 containing t and a in S and $(A_1, \tau_{\ker\varphi})$

respectively such that $U_1V_1 \subseteq \varphi^{-1}(f(f^{-1}(\varphi(G)))) = G$. So, $(A_1, \tau_{\ker\varphi})$ is an S-act topological space and hence by Corollary 2.2, $A_1/\ker\varphi$ is an S-act topological space. □

Corollary 2.15. *Let S be a topological semigroup. Also, let A_1 and A_2 be two S-acts endowed with topologies τ_1 and τ_2 respectively. Then for any mapping $\varphi : A_1 \to A_2$ such that $\ker\varphi$ is a congruence on A_1, $A_1/\ker\varphi$ is a topological S-act if and only if φ is φ-saturated continuous.*

Corollary 2.16. *Let S be a semigroup endowed with a topology τ. Also, let A_1 and A_2 be two S-acts endowed with topologies τ_1 and τ_2 respectively. Then for any homomorphism $\varphi : A_1 \to A_2$, $A_1/\ker\varphi$ is an S-act topological space if and only if φ is φ-saturated continuous.*

Corollary 2.17. *Let S be a topological semigroup. Also, let A_1 and A_2 be two topological S-acts. Then for any homomorphism $\varphi : A_1 \to A_2$, $A_1/\ker\varphi$ is a topological S-act if and only if φ is φ-saturated continuous.*

Using Corollary 2.15, we will prove that for any mapping $\varphi : A_1 \to A_2$ between two topological S-acts, the continuity of φ does not imply the φ-saturated continuity of φ. By the following example, we will prove this fact.

Example 2.18. [6, Example 2.7] We consider the topological semigroup $S = \{(a, b) \in \mathbb{Q} \times \mathbb{R} : b \geqslant 0\}$ with respect to the binary operation $((x, y), (a, b)) \mapsto (x + a, min(y, b))$. Let $I = \{(a, b) \in S : b = 0\}$. Then from [6], it follows that S/ρ_I is not a topological semigroup, where ρ_I is the Rees congruence induced by the ideal I on the semigroup S. Let us define a mapping $\varphi : S \to S$ by for all $(a, b) \in S$,

$$\varphi((a, b)) = \begin{cases} (a, b) & b > 0 \\ (0, 0) & b = 0. \end{cases}$$

Then it can be easily shown that φ is a continuous mapping with $\ker\varphi = \rho_I$. We claim that φ is not φ-saturated continuous. Because if so, then by Corollary 2.15, it follows that $S/\ker\varphi = S/\rho_I$ is a topological semigroup which is not true. Hence φ is not φ-saturated continuous.

Theorem 2.19. *Let S be a semigroup endowed with a topology τ. Also, let A_1 and A_2 be two S-acts endowed with topologies τ_1 and τ_2 respectively. Then for any mapping $\varphi : A_1 \to A_2$, if $A_1/\ker\varphi$ is Hausdorff, then $A_1/\ker\varphi$ is an S-act topological space if and only if φ is φ-saturated continuous.*

Proof. Let $A_1/\ker\varphi$ is an S-act topological space. Then $\ker\varphi$ is a congruence on A and hence by Theorem 2.14, φ is φ-saturated continuous.

Conversely, let φ be φ-saturated continuous. First we show that $\ker\varphi$ is a congruence on A_1. For this, let $(a,b)\in\ker\varphi$ and $s\in S$. If possible, let $(sa,sb)\notin\ker\varphi$. Then $[sa]\neq[sb]$. Since $A_1/\ker\varphi$ is Hausdorff, there exist disjoint open sets U and V in $A_1/\ker\varphi$ containing $[sa]$ and $[sb]$ respectively. Then $sa\in\pi^{-1}(U)$ and $sb\in\pi^{-1}(V)$. Since π is continuous, we have $\pi^{-1}(U)$ and $\pi^{-1}(V)$ are open in (A_1,τ_1). Then $sa\in\pi^{-1}(U)=\varphi^{-1}(f(U))$ and $sb\in\pi^{-1}(V)=\varphi^{-1}(f(V))$, where the mapping $f:A_1/\ker\varphi\to A_2$, defined by $f(a\ker\varphi)=\varphi(a)$, is a continuous injective homomorphism. Now, φ being φ-saturated continuous, there exist open sets U_1, U_2 in (S,τ) and V_1, V_2 in $(A_1,\tau_{\ker\varphi})$ such that $U_1V_1\subseteq\varphi^{-1}(f(U))=\pi^{-1}(U)$, $U_2V_2\subseteq\varphi^{-1}(f(V))=\pi^{-1}(V)$, where $s\in U_1\cap U_2$ and $a\in V_1, b\in V_2$. Set $G=U_1\cap U_2$. Then $s\in G$. Moreover, $(a,b)\in\ker\varphi$ implies $[a]=[b]\in\pi(V_1)\cap\pi(V_2)$ and hence $a,b\in V_1\cap V_2=H$ (say). Therefore, $sa,sb\in GH\subseteq\pi^{-1}(U)\cap\pi^{-1}(V)$ and thus $U\cap V\neq\emptyset$, a contradiction. Therefore, $[sa]=[sb]$ and thus $\ker\varphi$ is a congruence on A_1. Consequently, by Theorem 2.14, it follows that $A_1/\ker\varphi$ is an S-act topological space. □

Corollary 2.20. *Let S be a topological semigroup. Also, let A_1 and A_2 be two S-acts endowed with topologies τ_1 and τ_2 respectively. Then for any mapping $\varphi:A_1\to A_2$, if $A_1/\ker\varphi$ is Hausdorff, then $A_1/\ker\varphi$ is a topological S-act if and only if φ is φ-saturated continuous.*

3. Intersection and join of S-act congruences

It is well known that the intersection of finite number of congruences on an S-act A is again a congruence on A. But for a topological semigroup S, intersection of two topological S-act congruences on a topological S-act A may not be a topological S-act congruence. In this section, we establish a necessary and sufficient condition so that intersection of two topological S-act congruences on a topological S-act A to be a topological S-act congruence.

Before going to this result, we give a counter example to show that intersection of any S-act topological congruences on an S-act endowed with a topology τ may not be a S-act topological congruence.

Example 3.1. Consider the semigroup $S=(\mathbb{Z}_6,\cdot_6,\tau)$, where $\tau=\{\mathbb{Z}_6,\emptyset,\{\bar{0},\bar{3}\},\{\bar{1},\bar{2},\bar{4},\bar{5}\},\{\bar{4}\}\}$. Let $S=A$. Then A is an S-act endowed with

topology τ. It is clear that A is not a S-act topological space. Now let $\theta_1 = \{(x,x) : x \in A\} \cup \{(\bar{2},\bar{4}),(\bar{4},\bar{2}),(\bar{1},\bar{5}),(\bar{5},\bar{1})\}$ and $\theta_2 = \{(x,x) : x \in A\} \cup \{(\bar{2},\bar{5}),(\bar{5},\bar{2})(\bar{1},\bar{4}),(\bar{4},\bar{1}),(\bar{0},\bar{3}),(\bar{3},\bar{0})\}$. Then θ_1 and θ_2 are congruences on A. Clearly, $\theta_1 \cap \theta_2 = \{(x,x); x \in A\}$. Now $\tau_{\theta_1} = \tau_{\theta_2} = \{\mathbb{Z}_6, \emptyset, \{\bar{0},\bar{3}\}, \{\bar{1},\bar{2},\bar{4},\bar{5}\}\}$. It follows that (A,τ_{θ_1}) and (A,τ_{θ_2}) are S - act topological spaces. But $\tau_{\theta_1\cap\theta_2} = \tau$ and this implies that $\theta_1 \cap \theta_2$ is not an S-act topological congruence.

Now we establish some sufficient conditions for the intersection of two S-act topological congruences on an S-act A endowed with a topology τ to be a S-act topological congruence.

Theorem 3.2. *Let S be a semigroup endowed with a topology τ and A be an S-act endowed with a topology τ_A. Let θ_1 and θ_2 be two S-act topological congruences on A. If $\tau_{\theta_1} \cup \tau_{\theta_2}$ is a basis for $\tau_{\theta_1\cap\theta_2}$, then $\theta_1 \cap \theta_2$ is an S-act topological congruence on A.*

Proof. Let $\theta = \theta_1 \cap \theta_2$. We first show that $\tau_{\theta_1} \cup \tau_{\theta_2} \subseteq \tau_\theta$. Consider the natural epimorphisms $\pi : A \to A/\theta$, $\pi_1 : A \to A/\theta_1$ and $\pi_2 : A \to A/\theta_2$. Let $U \in \tau_{\theta_1}$. Then $\pi_1^{-1}(\pi_1(U)) = U$. Clearly, $U \subseteq \pi^{-1}(\pi(U))$. Let $x \in \pi^{-1}(\pi(U))$. Then $\pi(x) = \pi(u)$, for some $u \in U$. This implies that $(x,u) \in \theta \subseteq \theta_1$ and so $\pi_1(x) = \pi_1(u)$. From this, we have $x \in \pi_1^{-1}(\pi_1(U)) = U$ and thus $\pi^{-1}(\pi(U)) = U$. Therefore, $U \in \tau_\theta$ and hence $\tau_{\theta_1} \subseteq \tau_\theta$. Similarly, one can show that $\tau_{\theta_2} \subseteq \tau_\theta$. Therefore, $\tau_{\theta_1} \cup \tau_{\theta_2} \subseteq \tau_\theta$. Let $G \in \tau_\theta$ and $s \in S$, $a \in A$ with $sa \in G$. Then there exists a basic open set $W \in \tau_{\theta_1} \cup \tau_{\theta_2}$ such that $sa \in W \subseteq G$. Without any loss of generality, we assume that $W \in \tau_{\theta_1}$. Since θ_1 is an S-act topological congruence, there exist open sets U_1 and V_1 containing s and a in (S,τ) and (A,τ_{θ_1}) respectively such that $U_1V_1 \subseteq W$. As $\tau_{\theta_1} \subseteq \tau_\theta$, $V_1 \in \tau_\theta$. Hence $U_1V_1 \subseteq W \subseteq G$. Therefore, (A,τ_θ) is an S-act topological space and hence by Corollary 2.2, it follows that $\theta = \theta_1 \cap \theta_2$ is an S-act topological congruence on A. □

Corollary 3.3. *Let S be a topological semigroup and A be an S-act endowed with a topology τ_A. Let θ_1 and θ_2 be two topological S-act congruences on A. If $\tau_{\theta_1} \cup \tau_{\theta_2}$ is a basis for $\tau_{\theta_1\cap\theta_2}$, then $\theta_1 \cap \theta_2$ is a topological S-act congruence on A.*

Now, we come to the part where we talk about the join of two topological S-act congruences on a topological S-act A. In the following results, we establish a necessary and sufficient condition for the join of two topological

S-act congruences on a topological S-act to be again a topological S-act congruence.

Theorem 3.4. *Let S be a semigroup endowed with a topology τ and A be an S-act endowed with a topology τ_A. For any two S-act topological congruences θ_1 and θ_2 on A, $\theta_1 \vee \theta_2$ is an S-act topological congruence on A if and only if $(A, \tau_{\theta_1} \cap \tau_{\theta_2})$ is an S-act topological space.*

Proof. Let $\theta = \theta_1 \vee \theta_2$. Then by Corollary 2.2, θ is an S-act topological congruence on A if and only if (A, τ_θ) is an S-act topological space. For this, it suffices to show that $\tau_\theta = \tau_{\theta_1} \cap \tau_{\theta_2}$. Consider the natural epimorphisms $\pi : A \to A/\theta$, $\pi_1 : A \to A/\theta_1$ and $\pi_2 : A \to A/\theta_2$. Let $U \in \tau_\theta$. Then $\pi^{-1}(\pi(U)) = U$. Clearly, $U \subseteq \pi_1^{-1}(\pi_1(U))$. Let $x \in \pi_1^{-1}(\pi_1(U))$. Then $\pi_1(x) = \pi_1(u)$, for some $u \in U$. This implies that $(x, u) \in \theta_1 \subseteq \theta$ and so $\pi(x) = \pi(u)$. Then $x \in \pi^{-1}(\pi(U)) = U$. So, $\pi_1^{-1}(\pi_1(U)) = U$. This implies that $U \in \tau_{\theta_1}$. Thus, we have $\tau_\theta \subseteq \tau_{\theta_1}$. Similarly, $\tau_\theta \subseteq \tau_{\theta_2}$. Therefore, $\tau_\theta \subseteq \tau_{\theta_1} \cap \tau_{\theta_2}$. For the reverse inclusion let, $W \in \tau_{\theta_1} \cap \tau_{\theta_2}$. Then $\pi_1^{-1}(\pi_1(W)) = W$ and $\pi_2^{-1}(\pi_2(W)) = W$. Let $y \in \pi^{-1}(\pi(W))$. Then $\pi(y) = \pi(w)$, for some $w \in W$. This implies that $(y, w) \in \theta_1 \vee \theta_2$. Then by [2, Proposition 5.14], for some $n \in \mathbb{N}$, there exist elements $x_1, x_2, \ldots, x_{2n-1}$ in A such that $(y, x_1) \in \theta_1, (x_1, x_2) \in \theta_2, (x_2, x_3) \in \theta_1, \ldots, (x_{2n-1}, w) \in \theta_2$. Then $\pi_2(x_{2n-1}) = \pi_2(w)$ for some $w \in W$ and so $x_{2n-1} \in \pi_2^{-1}(\pi_2(W)) = W$. Now, $(x_{2n-2}, x_{2n-1}) \in \theta_1$ implies $x_{2n-2} \in \pi_1^{-1}(\pi_1(W)) = W$. Continuing in this way, we have $x_1 \in W$ and this implies that $y \in \pi_1^{-1}(\pi_1(W)) = W$. Therefore, $\pi^{-1}(\pi(W)) = W$ and so $W \in \tau_\theta$. Hence $\tau_\theta = \tau_{\theta_1} \cap \tau_{\theta_2}$. □

Corollary 3.5. *Let S be a topological semigroup and A be an S-act endowed with a topology τ_A. For any two topological S-act congruences θ_1 and θ_2 on A, $\theta_1 \vee \theta_2$ is a topological S-act congruence on A if and only if $(S, \tau_{\theta_1} \cap \tau_{\theta_2})$ is a topological S-act.*

We now establish necessary and sufficient conditions for the intersection of two topological S-act congruences on a topological S-act to be a topological S-act congruence.

Theorem 3.6. *Let S be a semigroup endowed with a topology τ and A be an S-act endowed with a topology τ_A. For any two congruences θ_1 and θ_2 on A, $\theta_1 \cap \theta_2$ is an S-act topological congruence on A if and only if the mapping $\varphi : A \to A/\theta_1 \times A/\theta_2$ defined by $\varphi(a) = (a\theta_1, a\theta_2)$, for all $a \in A$, is φ-saturated continuous.*

Proof. Since $\ker\varphi = \theta_1 \cap \theta_2$, the result follows from Theorem 2.14. □

Corollary 3.7. *Let S be a topological semigroup and A be an S-act endowed with a topology τ_A. Then for any two congruences θ_1 and θ_2 on A, $\theta_1 \cap \theta_2$ is a topological S-act congruence on A if and only if the mapping $\varphi : A \to A/\theta_1 \times A/\theta_2$ defined by $\varphi(a) = (a\theta_1, a\theta_2)$, for all $a \in A$, is φ-saturated continuous.*

Definition 3.8. *Let X and Y be topological spaces. A mapping $\varphi : X \to Y$ is said to be a weakly quotient mapping if for any subset A of Y, $\varphi^{-1}(A)$ is open in X implies A is open in Y.*

Theorem 3.9. *Let S be a semigroup endowed with a topology τ, A be an S-act endowed with a topology τ_A and θ_1, θ_2 be two S-act topological congruences on A. If the mapping $\varphi : A \to A/\theta_1 \times A/\theta_2$ defined by $\varphi(a) = (a\theta_1, a\theta_2)$, for all $a \in A$, is weakly quotient, then $\theta_1 \cap \theta_2$ is an S-act topological congruence on A.*

Proof. Clearly, $\ker\varphi = \theta_1 \cap \theta_2$. Consider the natural semigroup epimorphisms $\pi : A \to A/(\theta_1 \cap \theta_2)$, $\pi_1 : A \to A/\theta_1$ and $\pi_2 : A \to A/\theta_2$. To show $\theta_1 \cap \theta_2$ is an S-act topological congruence on A, it is suffices to show that φ is φ-saturated continuous. Let G be a subset of $A/\theta_1 \times A/\theta_2$ such that $\varphi^{-1}(G)$ is open in A and $s \in S$, $a \in A$ with $sa \in \varphi^{-1}(G)$. Since φ is weakly quotient, G is open in $A/\theta_1 \times A/\theta_2$. As $sa \in \varphi^{-1}(G)$, we have $(sa\theta_1, sa\theta_2) \in G$ and hence there exists a basic open set $U \times V$ in $A/\theta_1 \times A/\theta_2$ such that $(sa\theta_1, sa\theta_2) \in U \times V \subseteq G$, where U is open in A/θ_1 and V is open in A/θ_2. This implies that $sa \in \pi_1^{-1}(U) \cap \pi_2^{-1}(V)$. Since A/θ_1 is an S-act topological space, (A, τ_{θ_1}) is an S-act topological space. So there exist open sets U_1 containing s and V_1 containing a in (S, τ) and (A, τ_{θ_1}) respectively such that $U_1V_1 \subseteq \pi_1^{-1}(U)$. Similarly, there exist open sets U_2 containing s and V_2 containing a in (S, τ) and (A, τ_{θ_2}) respectively such that $U_2V_2 \subseteq \pi_2^{-1}(V)$. Let $U_3 = U_1 \cap U_2$ and $V_3 = V_1 \cap V_2$. Then U_3 and V_3 are open sets containing s and a in (S, τ) and (A, τ_A) respectively. We now show that $\pi^{-1}(\pi(V_3)) = V_3$. For this, let $z \in \pi^{-1}(\pi(V_3))$. Then $\pi(z) \in \pi(V_3)$ and so $\pi(z) = \pi(v)$, for some $v \in V_3$. Now, $v \in V_3$ implies $v \in V_1 \cap V_2$ and $\pi(z) = \pi(v)$ implies $(z, v) \in \theta_1 \cap \theta_2 \subseteq \theta_1$. This implies $\pi_1(z) = \pi_1(v)$ and $v \in V_1$. Therefore, $z \in \pi_1^{-1}(\pi_1(V_1)) = V_1$. Similarly, we can show that $z \in V_2$. Thus, $z \in V_1 \cap V_2 = V_3$ and hence $\pi^{-1}(\pi(V_3)) = V_3$. Therefore, $V_3 \in \tau_{\theta_1 \cap \theta_2}$ and $U_3V_3 \subseteq U_1V_1 \subseteq \pi_1^{-1}(U)$ and $U_3V_3 \subseteq U_2V_2 \subseteq \pi_2^{-1}(V)$. Let $t \in U_3$ and $c \in V_3$. Then $(tc\theta_1, tc\theta_2) \in U \times V \subseteq G$

implies $\varphi(tc) \in G$, i.e., $tc \in \varphi^{-1}(G)$. Therefore, $U_3V_3 \subseteq \varphi^{-1}(G)$ and hence φ is φ-saturated continuous. Consequently, $\theta_1 \cap \theta_2$ is an S-act topological congruence on A. □

Corollary 3.10. *Let S be a topological semigroup, A be an S-act endowed with a topology τ_A and θ_1, θ_2 be two topological S-act congruences on A. If the mapping $\varphi : A \to A/\theta_1 \times A/\theta_2$ defined by $\varphi(a) = (a\theta_1, a\theta_2)$, for all $a \in A$, is weakly quotient, then $\theta_1 \cap \theta_2$ is a topological S-act congruence on A.*

Acknowledgement. The authors are thankful to the Referee for valuable suggestions which have definitely improved the presentation of this article. The presented research was supported by CSIR, India. CSIR Award no.: 09/028(1001)/2017-EMR-1.

References

[1] **A.H. Clifford and G.B. Preston**, The Algebraic Theory of Semigroup (Vol-I), Math. Surveys, 7, Amer. Math. Soc., (1961).

[2] **J.M. Howie**, *An Introduction to Semigroup Theory*, London, New York, 1976.

[3] **T. Husain**, *Introduction to Topological Groups*, W. B. Saunders company, (1966).

[4] **B. Khosravi**, *Congruence on topological S-acts and topological semigroups*, J. Appl. Sci., **10**(2010), no. 9, 766 – 771.

[5] **R.J. Koch, J.A. Hildebrant and J.H. Carruth**, *The Theory of Topological Semigroups*, Marcel Dekker, Inc., (1983).

[6] **J. Lawson and B. Madison**, *On congruences and cones*, Math. Z. **120**(1971), 18 – 24.

[7] **J.R. Munkress**, *Topology*, 2nd edition, PHI Learning Private Limited, Delhi, (2014).

[8] **P. Normak**, *Topological S-acts: preliminaries and problems*, Transformation Semigroups, Univ. Essex, Colchester, (1993), 60 – 69.

[9] **M. Petrich and N.R. Reilly**, *Completely Regular Semigroups* Wiley, New York, (1999).

Received June 16, 2022

Department of Pure Mathematics, University of Calcutta, 35, Ballygunge Circular Road, Kolkata - 700019, India
E-mail: skmpm@caluniv.ac.in (Maity), paulmonika007@gmail.com (Paul)

Quasigroups and Related Systems **30** (2022), 287 – 298

Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations

Nikolay A. Moldovyan

Abstract. A new-type algebraic digital signature schemes on non-commutative associative algebras are developed using technique of performing exponentiation operations in a hidden group. The signature contains two elements: a randomization integer e and a vector S. The used verification equations are characterized in multiple entries of the signature element S. The post-quantum security of the introduced signature algorithms is provided by the computational difficulty of solving a system of many quadratic equations in many variables, like in the public-key multivariate cryptosystems. However in the former case the quadratic equations are set over the finite fields having the order of significantly larger size.

1. Introduction

One of current challenges in the area of post-quantum cryptography reates to the development of practical digital signature algorithms [15, 2]. Recently [6, 10, 13] several signature schemes on finite non-commutative associative algebras (FNAAs) had been propsed. In that schemes, which are based on computational complexity of so called hidden discrete logarithm problem (HDLP), the exponentiation operations in a hidden group are performed, when generating the public key and the signature. Since there is a discrete logarithm problem, although in a hidden group, there are certain

2010 Mathematics Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: non-commutative algebra, finite associative algebra, hidden group, post-quantum cryptography, multivariate cryptography, public-key cryptoscheme, signature scheme.
This work was partially supported by RFBR (project No. 21-57-54001-Viet_a) and by the budget theme No. FFZF-2022-0007.

difficulties in justifying post-quantum security. The latter are associated with the potential opportunity to find algebraic methods for reducing the HDLP to the usual discrete logarithm problem that can be solved in polynomial time on a quantum computer [4, 17].

Multivariate cryptography [3, 18] suggests various public-key cryptosystems that are based on the hardness of solving systems of many quadratic equations in many variables. The hypothetic quantum computer is not efficient to solve the latter type problems, therefore the multivariate public-key cryptographic algorithms are post-quantum. However, the maltivariate signature algorithms are not practical because of very large sizes of public and seret keys.

The present paper introduces a new signature algorithms with a hidden group in which the exponentiation operations are executed. However, the proposed signature algorithm is not attributed to the HDLP-based cryptoschemes, since its security is based on the computational hardness of solving the systems of many quadratic equations with many unknowns.

2. The used FNAAs

Suppose in a finite m-dimensional vector space over the field $GF(p)$ an additional operation, namely, the vector multiplication that is distributive at the right and at the left relatively the addition operation, is defined. Then one gets a finite m-dimensional algebra. Some algebra element (m-dimensional vector) A can be denoted in the following two forms: $A = (a_0, a_1, \ldots, a_{m-1})$ and $A = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, where $a_0, a_1, \ldots, a_{m-1} \in GF(p)$ are called coordinates; $\mathbf{e}_0$, $\mathbf{e}_1$, ... $\mathbf{e}_{m-1}$ are basis vectors.

The vector multiplication operation of two m-dimensional vectors A and B is defined as follows:

$$AB = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i b_j (\mathbf{e}_i \mathbf{e}_j),$$

where every of the products $\mathbf{e}_i \mathbf{e}_j$ is to be replaced by a 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 so called basis vector multiplication table (BVMT) like Tables 1 and 2. To define associative vector multiplication operation the BVMT should define associative multiplication of all possible triples of the basis vectors $(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$:

$$(\mathbf{e}_i \mathbf{e}_j)\, \mathbf{e}_k = \mathbf{e}_i\, (\mathbf{e}_j \mathbf{e}_k)\,.$$

Table 1: The BVMT for defining the 4-dimensional FNAA ($\lambda \neq 1$).

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\lambda\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\lambda\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_3$

In the developed signature algorithms, the FNAAs defined by Tables 1 and 2 are used as algebraic supports. The 4-dimensional FNAA had been used earlier in [12] as algebraic support of a HDLP-based signature scheme. This algebra contains the two-sided global unit

$$E = \left(\frac{1}{1-\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{1}{\lambda-1}\right).$$

A 4-dimensional vector A of the algebra, coordinates of which satisfy the condition

$$a_0 a_1 \neq a_2 a_3, \tag{1}$$

is invertible, i.e., for a vector of such a kind there exists the vector A^{-1} such that the condition $A \circ A^{-1} = A^{-1} \circ A = E$ holds true. If $a_0 a_1 = a_2 a_3$, then the vector A is non-invertible.

The 6-dimensional FNAA is obtained as a particular case defined by the unified method for constructing the FNAAs of arbitrary even dimensions, which had been proposed in [5]. The used 6-dimensional FNAA contains the global two-sided unit $E = (1, 0, 0, 0, 0, 0)$. The scalar vectors have the form $(j, 0, 0, 0, 0, 0)$, where $j = 1, 2, \ldots p-1$. A vector $G = (g_0, g_1, g_2, g_3, g_4, g_5)$ is invertible, if its coordinates satisfy the following invertibility condition [5]:

$$\begin{aligned} &\frac{1}{4}((g_0 + g_2 + g_4)^2 - \lambda\,(g_1 + g_3 + g_5)^2)\times \\ &\times ((g_0 - g_2)^2 + (g_0 - g_4)^2 + (g_2 - g_4)^2 - \\ &- \lambda\,(g_1 - g_3)^2 - \lambda\,(g_1 - g_5)^2 - \lambda\,(g_3 - g_5)^2)^2 \neq 0. \end{aligned} \tag{2}$$

Each of the used FNAAs contains sufficiently large number of commutative groups of orders $(p-1)^2$, $p^2 - 1$, and $p(p-1)$. The developed signature schemes are not based on the HDLP, therefore, the existance of a prime divisor of the order of the hidden group is not a strict requirement that is

Table 2: The BVMT setting the used 6-dimensional FNAA ($\lambda \neq 0$).

$\cdot$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_5$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$

critical for providing security. However, to have possibility to reduce the computational complexity of the signature generation procedure the used FNAAs are defined over the ground finite field $GF(p)$ with the prime order $p = 2q+1$, where q is also a prime. In the case $m = 4$ ($m = 6$) it is supposed to use the prime q having the size 128 bits (96 bits).

In each of two developed signature algorithms selection of a commutative hidden group is performed as generation of a random minimum generator system $<G, H>$, which includes two mutually permutable vectors of the same order equal to q, as follows:

1. Using the invertibility condition (1) in the case $m = 4$ or (2) in the case $m = 6$, select at random an invertible vector R.

2. Compute the vector $G' = R^{p(p+1)}$.

3. If the vector G' is a scalar vector, then go to step1.

4. Select a random non-negative integer k ($k < q$) and generate a primitive element α modulo p. Then compute the scalar vector $L = \alpha E$ and the vector $H' = G'^k L$.

5. Compute the vectors $G = G'^2$ and $H = H'^2$ each of which has order q.

6. Output the pair of vectors $<G, H>$ as a minimum generator system of a hidden group possessing 2-dimensonal cyclicity and having order q^2.

3. The first signature scheme

The public key is generated as a set of four 4-dimensional vectors Y, Z, U, and W as follows:

1. Generate at random a minimum generator system $<G, H>$ of a hidden group $\Gamma_{<G,H>}$ of the order q^2.

2. Using the invertibility condition (1), generate random invertible vectors A and B satisfying the following inequalities $AB \neq BA$, $AG \neq GA$, and $BG \neq GB$. Then calculate the vectors A^{-1} and B^{-1}.

3. Generate random integers $x_1, x_2 \in GF(p)$ and calculate the vectors Y, Z, U, and W as follows:

$$\begin{aligned} Y &= AGB, \quad & Z &= AG^{x_1}B; \\ U &= AHB, \quad & W &= AH^{x_2}A^{-1}. \end{aligned} \tag{3}$$

Since the size of the prime p equals to 129 bits, the size of public key is equal to ≈ 2064 bits (258 bytes). The integers x_1, and x_2 and the vectors G, H, A^{-1}, and B^{-1} represent a private key having the size equal to ≈ 2320 bits (≈ 290 bytes).

Using the private key $\left(x_1, x_2, G, H, A^{-1}, B^{-1}\right)$ and some specified 384-bit hash-function f, one can generate a signature to the electronic document M as follows:

The signature generation procedure.

1. Generate a random natural numbers k ($k < q$) and t ($t < q$). Then calculate the vector

$$R = AG^kH^tA^{-1}.$$

2. Compute the hash-function value $e = e_1||e_2||e_3$ (the first signature element), where $||$ denotes the concatenation operation, from the document M to which the vector R is concatenated: $e = e_1||e_2||e_3 = f\left(M, R\right)$, where e_1, e_2, and e_3 are 128-bit integers.

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:

$$S = B^{-1}G^nH^uA^{-1}.$$

The size of the output signature (e, S) is equal to ≈ 900 bits (≈ 113 bytes). Computational difficulty w of the signature generation procedure is roughly equal to four exponentiation operations in the 4-dimensional FNAA used as algebraic support of the signature scheme, i. e., to $w \approx 12,288$ multiplications modulo a 129-bit prime. The verification of the signature (e, S) to the document M is performed using the public key (Y, Z, U, W) as folows:

The signature verification procedure.

1. Calculate the vector R':

$$R' = (YS\,(US)^{e_1}\,(ZSW)^{e_2})^{e_3}\,.$$

2. Compute the hash-function value e' from the document M to which the vector R' is concatenated: $e' = f\,(M, R')\,.$

3. If $e' = e$, then the signature is genuine. Otherwise reject the signature.

At the first step of the signature verification algorithm the computations are performed in accordance with a verification equation with 3 entries of the signature element S. The computational complexity w' of the signature verification procedure is roughly equal to three exponentiation operations in the 4-dimensional FNAA used as algebraic support of the signature scheme, i. e., we have $w' \approx 9,216$ multiplications modulo a 129-bit prime.

Correctness proof.
Taking into account that the vectors G and H are permutable and have order q, one can show that the correctly computed signature (e, S) passes the verification procedure as genuine signature:

$$\begin{aligned}
&R'_1 = (YS\,(US)^{e_1}\,(ZSW)^{e_2})^{e_3} = \\
&= \left(AGBB^{-1}G^nH^uA^{-1}\left(AHBB^{-1}G^nH^uA^{-1}\right)^{e_1}\times\right. \\
&\qquad \left.\times\left(AG^{x_1}BB^{-1}G^nH^uA^{-1}AH^{x_2}A^{-1}\right)^{e_2}\right)^{e_3} = \\
&= \left(AGG^nH^uA^{-1}\left(AHG^nH^uA^{-1}\right)^{e_1}\left(AG^{x_1}G^nH^uH^{x_2}A^{-1}\right)^{e_2}\right)^{e_3} = \\
&= \left(AG^{n+1}H^uA^{-1}AH^{e_1(u+1)}G^{e_1n}A^{-1}AG^{e_2(x_1+n)}H^{e_2(u+x_2)}A^{-1}\right)^{e_3} = \\
&= \left(AG^{n+1+e_1n+e_2(x_1+n)}H^{u+e_1(u+1)+e_2(u+x_2)}A^{-1}\right)^{e_3} = \\
&= AG^{e_3n+e_3+e_3e_1n+e_3e_2(x_1+n)}H^{e_3u+e_3e_1(u+1)+e_3e_2(u+x_2)}A^{-1} = \\
&= AG^{n(e_3+e_1e_3+e_2e_3)+e_3+x_1e_2e_3}H^{u(e_3+e_1e_3+e_2e_3)+e_1e_3+x_2e_2e_3}A^{-1} = \\
&= AG^{\frac{k-x_1e_2e_3-e_3}{e_3+e_1e_3+e_2e_3}(e_3+e_1e_3+e_2e_3)+e_3+x_1e_2e_3}\times \\
&\qquad \times H^{\frac{t-x_2e_2e_3-e_1e_3}{e_3+e_1e_3+e_2e_3}(e_3+e_1e_3+e_2e_3)+e_1e_3+x_2e_2e_3}A^{-1} = \\
&= AG^kH^tA^{-1} = R \;\;\Rightarrow\;\; f(M,R') = f(M.R) \;\Rightarrow\; e' = e.
\end{aligned}$$

4. The second signature scheme

The public key is calculted as a set of three 6-dimensional vectors Y, Z, and U in accordance with the public-key generation procedure of the first signature scheme (see Section 3) with exception that at step 3 only the following three vectors are computed:

$$Y = AGB, \quad Z = AG^{x_1}B, \quad U = AHB. \tag{4}$$

Since in the case $m = 6$ we use a 97-bit (96-bit) prime p (prime q) The size of public key is equal to ≈ 1746 bits (≈ 219 bytes). The integer x_1 and the vectors G, H, A^{-1}, and B^{-1} represent a private key having the size equal to ≈ 2424 bits (≈ 303 bytes).

Using the private key $\left(x_1, G, H, A^{-1}, B^{-1}\right)$ and some specified 384-bit hash-function f, one can generate a signature to the electronic document M as follows:

The signature generation procedure.

1. Generate random natural numbers k ($k < q$) and t ($t < q$). Then calculate the vector

$$R = B^{-1}G^kH^tB.$$

2. Compute the hash-function value $e = e_1||e_2||e_3||e_4$ (the first signature element) from the document M to which the vector R is concatenated: $e = e_1||e_2||e_3||e_4 = f\left(M, R\right)$, where e_1, e_2, e_3, and e_3 are 96-bit integers.

3. Calculate the integers n and u:

$$n = \frac{k - e_4 - e_1e_4 - x_1e_3e_4}{e_1e_4 + e_2e_4 + e_3e_4 + e_4} \bmod q; \quad u = \frac{t - e_2e_4}{e_1e_4 + e_2e_4 + e_3e_4 + e_4} \bmod q.$$

4. Calculate the second signature element S:

$$S = B^{-1}G^nH^uA^{-1}.$$

The size of the output signature (e, S) is equal to ≈ 966 bits (≈ 121 bytes). Computational difficulty w of the signature generation procedure is roughly equal to four exponentiation operations in the 6-dimensional FNAA used as algebraic support of the signature scheme, i. e., $w \approx 20,736$ multiplications modulo a 97-bit prime or $w \approx 11,720$ multiplications modulo a 129-bit prime. The verification of the signature (e, S) to the document M is performed using the public key (Y, Z, U) as folows:

The signature verification procedure.

1. Calculate the vector R':

$$R' = \left((SY)^{e_1}\, S\, (US)^{e_2}\, (ZS)^{e_3}\, Y\right)^{e_4}.$$

2. Compute the hash-function value e' from the document M to which the vector R' is concatenated: $e' = f\left(M, R'\right)$.

3. If $e' = e$, then the signature is genuine. Otherwise reject the signature.

At the first step of the signature verification algorithm the computations are performed in accordance with a verification equation with 4 entries of the signature element S. The computational complexity w' of the signature verification procedure is roughly equal to four exponentiation operations in the 6-dimensional FNAA used as algebraic support of the signature scheme, i. e., we have $w' \approx 20,736$ multiplications modulo a 97-bit prime or $w' \approx 11,720$ multiplications modulo a 129-bit prime.

Correctness proof.
Taking into account that the vectors G and H are permutable and have order q, one can show that the correctly computed signature (e, S) passes the verification procedure as genuine signature:

$$
\begin{aligned}
R'_1 &= ((SY)^{e_1} S (US)^{e_2} (ZS)^{e_3} Y)^{e_4} = \\
&= \left(\left(B^{-1}G^nH^uA^{-1}AGB\right)^{e_1} B^{-1}G^nH^uA^{-1} \left(AHBB^{-1}G^nH^uA^{-1}\right)^{e_2} \times \right. \\
&\qquad \left. \times \left(AG^{x_1}BB^{-1}G^nH^uA^{-1}\right)^{e_3} AGB\right)^{e_4} = \\
&= \left(\left(B^{-1}G^nH^uGB\right)^{e_1} B^{-1}G^nH^uA^{-1} \left(AHG^nH^uA^{-1}\right)^{e_2} \times \right. \\
&\qquad \left. \times \left(AG^{x_1}G^nH^uA^{-1}\right)^{e_3} AGB\right)^{e_4} = \\
&= \left(B^{-1}G^{e_1(n+1)}H^{e_1u}G^nH^uH^{e_2(1+n)}G^{e_2n}A^{-1}AG^{e_3(x_1+n)}H^{e_3u}GB\right)^{e_4} = \\
&= \left(B^{-1}G^{e_1(n+1)+n+e_2n+e_3(x_1+n)+1}H^{e_1u+u+e_2(1+n)+e_3u}B\right)^{e_4} = \\
&= B^{-1}G^{e_4e_1(n+1)+e_4n+e_4e_2n+e_4e_3(x_1+n)+e_4}H^{e_4e_1u+e_4u+e_4e_2(1+n)+e_4e_3u}B = \\
&= B^{-1}G^{n(e_1e_4+e_2e_4+e_3e_4+e_4)+e_4+e_1e_4+e_3e_4x_1}H^{u(e_1e_4+e_2e_4+e_3e_4+e_4)+e_2e_4}B = \\
&= B^{-1}G^{\frac{k-e_4-e_1e_4-x_1e_3e_4}{e_1e_4+e_2e_4+e_3e_4+e_4}(e_1e_4+e_2e_4+e_3e_4+e_4)+e_4+e_1e_4+e_3e_4x_1} \times \\
&\qquad \times H^{\frac{t-e_2e_4}{e_1e_4+e_2e_4+e_3e_4+e_4}(e_1e_4+e_2e_4+e_3e_4+e_4)+e_2e_4}B = \\
&= B^{-1}G^kH^tB = R \quad \Rightarrow \quad f(M,R') = f(M.R) \;\Rightarrow\; e' = e.
\end{aligned}
$$

5.Disscussion

In each of the two introduced signature algorithms with a hidden group, the used exponentiation operations are a part of the technique that provides possibility (when using the private key) to compute the randomization vector R and the signature element S that satisfy the verification equation. It can be noted that the knowledge of the x_1 and x_2 values does not make it possible to develop a polynomial algorithm for computing a signature

until the secret vectors G and H are also known. Actually, the values x_1 and x_2 are used only to select some random vectors from the hidden group and to reduce the computational complexity of the signature generation procedure. It is easy to show that using a precomputed large set of the vectors contained in the group $\Gamma_{<G,H>}$ allows one to compute the public key, for example, in the first signature algorithm in the form of four vectors $Y = AG_1B$, $Z = AG_2B$, $U = AG_3B$, and $W = AG_4A^{-1}$, where $G_1, G_2, G_3, G_4 \in \Gamma_{<G,H>}$ are random vectors selected from the said set of pairwise permutable vectors. For this method of generating a public key, a modified signature generation procedure (computational complexity of which is roughly equal to eight exponentiation operations) can be used , while the source signature verification procedure is saved. Thus, the developed sihnature algorithms with a hidden group are not HDLP-based schemes.

We suppose that the most efficient attack on the proposed first algorithm is to find the vectors A', B', G_1, G_2, G_3, and G_4 which express the public-key in the form of formulas (3). The formulas (3) define the following system of seven quadratic vector equations with the said six unknowns:

$$\begin{cases} A'^{-1}Y = G_1B', & A'^{-1}Z = G_2B'; & A'^{-1}U = G_3B', & WA'^{-1} = A'G_4 \\ G_1G_2 = G_2G_1, & G_1G_3 = G_3G_1, & G_1G_4 = G_4G_1. \end{cases} \tag{5}$$

The last three vector equations in (5) reflect the requirement of pairwise permutability of the vectors G_1, G_2,G_3, and G_4. Thus we have a system of 7 quadratic vector equations with 6 unknowns. The system (5) reduces to the system of 28 equations with 24 unknowns over the field $GF(p)$ of 129-bit order.

A similar attack on the second proposed signature algorithm leads to the system of 5 quadratic vector equations with 5 unknowns, which reduces to the system of 30 quadratic equations with 30 unknowns, which is set over the field $GF(p)$ of 97-bit order.

From the multivariate cryptography [1, 3, 18] it is known that finding a solution of such systems is a computationally hard problem and the quantum computer is not efficient to solve it. Like the multivariate public-key cryptosystems, the developed algorithms are attributed to the post-quantum signature schemes. The latter represent significant practical interest due to significantly lower sizes of the public key, private key, and signature. A merit of the introduced algorithms is a significantly higher order of the finite field over which the system of quadratic equations is set.

Table 3: Comparison of the proposed and known multivariate signature schemes.

Signature scheme	signature size, bytes	public-key size, bytes	η	ρ	ω
[18]	–	–	27	27	2^{16}
Rainbow [1]	33	16,065	27	33	2^8
Rainbow [16] (3 versions)	66... 204	>150,000... >1,900,000	64... 128	96... 204	$2^4, 31,$ 2^8
QUARTZ [3]	16	72,704	100	107	2^4
Proposed ($m = 4$)	160	768	28	24	$>2^{128}$
Proposed ($m = 6$)	112	576	30	30	$>2^{96}$

Table 3 (where η (ρ) is the number of equations (unknowns) in the system of quadratic equations; ω is the order of the finite field) provides some comparison of the introduced post-quantum signature algorithms with some multivariate sinature algorithms. Table 4, where a procedure execution time* is estimated in multiplications in $GF(p)$ with 129-bit characteristic, compares the introduced signature algorithms with some HDLP-base ones.

6. Conclusion

The proposed two post-quantum signature algorithms, using FNAAs as algebraic support, can be attributed to the cryptoschemes with a hidden group and to the multivariate public key cryptosystems, however not to the HDLP-based signature algorithms. For the first time it is proposed a method for development of the signature schemes on FNAAs, which are based on the computational difficulty of solving systems of many quadratic equations with many unknowns. The introduced post-quantum signature algorithms are more practical than the known multivariate signature algorithms and can serve as an attractive starting point for preparing a new proposal for participating in the NIST competition on developing a standard on a post-quantum signature algorithm (NIST is going to consider new proposals at the fourth round of its competition [14]).

Table 4: Comparison of the proposed and known HDLP-based signature schemes.

Signature scheme	signature size, bytes	public-key size, bytes	signature generation time*	signature verification time*
[7]	96	384	$\approx 49,200$	$\approx 36,800$
[9]	96	384	$\approx 12,400$	$\approx 24,800$
[8]	192	768	$\approx 221,200$	$\approx 221,200$
[11]	96	576	$\approx 221,200$	$\approx 165,900$
Proposed ($m = 4$)	113	290	$\approx 12,288$	$\approx 9,216$
Proposed ($m = 6$)	121	219	$\approx 27,648$	$\approx 13,824$

References

[1] **J. Ding, D. Schmidt**, *Rainbow, a new multivariable polynomial signature scheme*, Lecture Notes in Computer Sci., **3531** (2005), 164 – 175.

[2] Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms, (2016) [on line] https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (May 10, 2022)

[3] **D. Jintai, S. Dieter**, *Multivariable Public Key Cryptosystems*, (2004) https://eprint.iacr.org/2004/350.pdf (May 10, 2022)

[4] **R. Jozsa**, *Quantum algorithms and the fourier transform*, Proc. Roy. Soc. London Ser A, **454** (1998), 323 – 337.

[5] **N.A. Moldovyan**, *Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions*, Quasigroups and Related Systems, **26** (2020), 263 – 270.

[6] **N.A. Moldovyan**, *Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security*, Bull. Acad. Sci. Moldova, Math., **2(93)** (2020), 62 – 67.

[7] **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.

[8] **N.A. Moldovyan, A.A. Moldovyan**, *Candidate for practical post-quantum signature scheme*, Vestnik of Saint Petersburg Univ. Applied Math., Computer Sci., Control Processes, **16** (2020), 455 – 464.

[9] **N.A. Moldovyan, A.A. Moldovyan**, *Digital signature scheme on the 2x2 matrix algebra*, Vestnik of Saint Petersburg Univ. Applied Math., Computer Sci., Control Processes, **17** (2021), 254 – 261.

[10] **D.N. Moldovyan, A.A. Moldovyan, N.A. Moldovyan**, *Digital signature scheme with doubled verification equation*, Computer Sci. J. Moldova, **28** (2020), no. 1(82), 80 – 103.

[11] **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, **29** (2021), 97 – 106.

[12] **A.A. Moldovyan, N.A. Moldovyan**, *Post-quantum signature algorithms based on the hidden discrete logarithm problem*, Computer Sci. J. Moldova, **26** (2018), no. 3(78), 301 – 313.

[13] **A.A. Moldovyan, N.A. Moldovyan**, *Finite Non-commutative Associative Algebras as Carriers of Hidden Discrete Logarithm Problem*, Bull. South Ural State Univ., Ser. Mathematical Modelling, Programming & Computer Software, **12** (2019), no. 1, 66 – 81.

[14] **D. Moody**, *NIST Status Update on the 3rd Round*, (2021). Available at: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf (May 10, 2022).

[15] *Post-Quantum Cryptography*, Lecture Notes in Computer Sci., **11505**, (2019).

[16] Rainbow Signature. One of three NIST Post-quantum Signature Finalists [on line] 2021. https://www.pqcrainbow.org/ (May 10, 2022)

[17] **P.W. Shor**, *Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer*, SIAM J. Computing, **26** (1997), 1484 – 1509.

[18] **Q. Shuaiting, H. Wenbao, Li Yifa, J. Luyao**, *Construction of Extended Multivariate Public Key Cryptosystems*, Intern. J. Network Security, **18** (2016), 60 – 67.

Received November 22, 2021

St. Petersburg Federal Research Center
of the Russian Academy of Sciences
14-th line 39, 199178, St. Petersburg, Russia
e-mail: nmold@mail.ru

Quasigroups and Related Systems **30** (2022), 299 – 306

On the weight of finite groups

Mohammad Amin Morshedlo and Mohammad Mehdi Nasrabadi

Abstract. For a finite group G, let $W(G)$ denotes the set of the orders of the elements of G. In this paper we study $|W(G)|$ and show that the cyclic group of order n has the maximum value of $|W(G)|$ among all groups of the same order. Furthermore we study this notion in nilpotent and non-nilpotent groups and state some inequality for it. Among the result we show that the minimum value of $|W(G)|$ is power of 2 or it pertains to a non-nilpotent group.

1. Introduction

Let G be a finite group. The connection between structure and the set of the orders of the elements of G, has been studied in several works. In 1932, Levi and Waerden [4] showed that under some conditions the groups with weight 2 are nilpotent of class at most 3. Later in 1937, Neumann [6] proved that if $W(G) = \{1, 2, 3\}$, then G is an elementary abelian-by-prime order group. Sanov [9] showed that, when $W(G) \subseteq \{1, 2, 3, 4\}$ G is a locally finite group. Novikov and Adjan [7] in 1968 answered negatively to the following question. Does the finiteness of $W(G)$ imply G to be locally finite? In the same line of research Gupta et. al, [3] proved if $W(G) \subseteq \{1, 2, 3, 4, 5\}$ and $W(G) \neq \{1, 5\}$, then G is locally finite. In 2007, D. V. Lytkina [5] showed that for the group G, with $W(G) = \{1, 2, 3, 4\}$, either G is an extension of an elementary abelian 3-group by a cyclic or a quaternion group, or it is an extension of a nilpotent 2-group of class 2 by a subgroup of S_3. The sum of element orders in finite groups is studied by Amiri, Jafarian Amiri and Isaacs [1]. We denote by $|W(G)|$, the number of element orders of G. The group G is m-weight group, if $|W(G)| = m$. It is easy to see that if G is trivial, then $|W(G)| = 1$. If G be a non-trivial group then, the weight of G is at least 2. In the following lemma, we state a result about 2-weight

2010 Mathematics Subject Classification: Primary 20D15; Secondary 20K01.
Keywords: Weight of group, finite p-group, non-nilpotency property.

group.

Lemma 1.1. *Let G be a group, then G is a 2-weight group if and only if* $\exp(G) = p$.

Proof. First assumethat, G is a 2-weight group. If $\exp(G) = p$ has two distinct prime divisors p and q, then $\{1, p, q\} \subseteq W(G)$, so $exp(G)$ must be a p-number for some prime p. Now, if $exp(G) = p^n$, for some $n \geqslant 2$, then, $\{1, p, p^2\} \subseteq W(G)$. The converse is trivial. □

2. Preliminary results

This section contains some basic properties on the weight of a finite group. The following proposition shows the relation of the weight of a direct product of a finite number of finite groups with the weights of its factors.

Proposition 2.1. *Let H and K be two arbitrary finite groups, then*

$$|W(H \times K)| \leqslant |W(H)| \times |W(K)|,$$

and the equality holds if $(exp(H), exp(K)) = 1$.

Proof. Let $m \in W(H \times K)$ then, there exists $(h, k) \in H \times K$, such that $m = o(h, k) = [o(h), o(k)] = \dfrac{o(h)}{g_1} \times \dfrac{o(k)}{g_2} = rs$. Since $[o(h), o(k)]$ is the least common multiple of $o(h)$ and $o(k)$ and $g_1 g_2 = gcd(o(h), o(k))$, on the other hand $r = \dfrac{o(h)}{g_1}, s = \dfrac{o(k)}{g_2}$. So we have $r \in W(H)$ and $s \in W(K)$. Hence $|W(H \times K)| \leqslant |W(H)| \times |W(K)|$. Now, if $(exp(H), exp(K)) = 1$ and $(r, s) \in W(H) \times W(K)$, then there exsit $h \in H$ and $k \in K$ of orders r and s, respectively. Therefore, (h, k) is an element of $H \times K$ of order rs, so the result holds. □

Now, using induction in order to prove the following corollary.

Corollary 2.2. *Let $G_i{}_{i=1}^{n}$ be a family of finite groups. Then, $|W(\prod_{i=1}^{n} G_i)| \leqslant \prod_{i=1}^{n} |W(G_i)|$. Furthermore, the equality holds if the exponent of distinct direct factors are mutully coprime.*

It is easy to see that the cyclic group of order p^{m-1}, $C_{p^{m-1}}$ is an m-weight group, in which p is an arbitrary prime number, so for every natural number n, there exists a finite group (in fact a finite p-group) of weight m.

The following theorem gives an upper bound for the weight of a finite group in terms of its order.

Theorem 2.3. *Let G be a finite group of order n, then $|W(G)| \leqslant |W(C_n)|$ and the equality holds if and only if $G \cong C_n$.*

Proof. Since the order of each element of G is a divisor of n and $|W(C_n)| = d(n)$, in which $d(n)$ is the number of natural divisors of n, it is trivial, such that $|W(G)| \leqslant |W(C_n)|$. Now, if $|W(G)| = |W(C_n)|$, then $n \in W(G)$ and hence $G \cong C_n$. □

3. Nilpotent groups

In this section, we state some facts on $W(G)$, when G is a nilpotent group. The following proposition gives the upper and lower bound for $W(G)$, when G is a finite nilpotent group.

Proposition 3.1. *Let $\aleph$ be class of nilpotent groups of order n, then for each $G \in \aleph$ we have*

$$2^{|\pi(n)|} \leqslant |W(G)| \leqslant d(n),$$

and equality in the first inequality holds if and only if all Sylow subgroups of G has prime exponent.

Proof. Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $d(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$. Let G be a nilpotent group of order n, so $G \cong \prod_{i=1}^{k} S_i$, in which S_i is the Sylow p_i-subgroup of G of order $p_i^{\alpha_i}$ $(1 \leqslant i \leqslant k)$. Now, by Proposition 2.1, we have $|W(G)| = \prod_{i=1}^{k} |W(S_i)|$. Applying, Theorem 2.3, thus $2 \leqslant |W(S_i)| \leqslant \alpha_i + 1$, for all i, $1 \leqslant i \leqslant k$. So $2^{|\pi(n)|} \leqslant |W(G)| \leqslant \prod_{i=1}^{k} (\alpha_i + 1) = d(n)$. Hence, $|W(G)| = 2^{|\pi(n)|}$ if and only if $\alpha_i = 1$, for all i, $1 \leqslant i \leqslant k$ which is equal to $\exp(S_i) = p_i$, for all i, $1 \leqslant i \leqslant k$. □

As an immediate result we have.

Corollary 3.2. *Let G be a finite group of order n, if $|W(G)| < 2^{|\pi(n)|}$ then G is non-nilpotent.*

Theorem 3.3. *Let G be a group of prime weight then G is nilpotent if and only if G is a p-group.*

Proof. Since G is a nilpotent group we have $G = P_1 \times \cdots \times P_k$ so $W(G) = W(P_1) \cdots W(P_k)$ this implies $k = 1$ hence G is a p-group □

Immediate consequence of Theorem 3.3, we get the following corollary.

Corollary 3.4. *In the class of all finite groups of prime weight, each group is either a p-group or non-nilpotent.*

Proposition 3.5. (See [8, Theorem 1]) *Suppose that* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, *in which* p_i*'s are distinct prime numbers. Then, every finite group of order* n *is a nilpotent group if and only if* $p_i \nmid p_j^{\beta_j} - 1$, *for each* j, $0 < \beta_j \leqslant \alpha_j$ *and* $i \neq j$.

In above proposition such these numbers are called nilpotent numbers. Now in order to prove our main result, we need the following results.

Lemma 3.6. *Every finite nilpotent group of order* n *is cyclic if and only if* n *is square free.*

Proof. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be decomposition of n into prime factors and G be a nilpotent group of order n. By Proposition 3.1, we have $2^k \leqslant |W(G)| \leqslant |W(C_n)|$, since every nilpotent group of order n is cyclic, so both inequalities are in fact equality and hence $\alpha_i = 1$, for all i, $1 \leqslant i \leqslant k$. Conversely, let G be a nilpotent group of order $n = p_1 \cdots p_k$. Applying, Proposition 3.1 again, so we have $|W(G)| = 2^k = d(n) = |W(C_n)|$, it implies that $G \cong C_n$. □

Using, the above lemma we can prove the following theorem.

Theorem 3.7. *Every finite group of order* n *is cyclic if and only if* $n = p_1 \cdots p_k$, *in which* $p_1 < \ldots < p_k$ *and* $p_i \nmid p_{i+s} - 1$, *where* $1 \leqslant i \leqslant k-1$ *and* $1 \leqslant s \leqslant k - i$.

Proof. If every finite group of order n is cyclic, then by Lemma 3.6 and Proposition 3.5, the result holds. If $n = p_1 \cdots p_k$, in which $p_1 < \ldots < p_k$ and $p_i \nmid p_{i+s} - 1$, where $1 \leqslant i \leqslant k-1$ and $1 \leqslant s \leqslant k-i$, then every group of order n is nilpotent, so we have $|W(G)| = 2^k = d(n) = |W(C_n)|$ and hence $G \cong C_n$. □

4. Non-nilpotent groups

This section is devoted to some results on non-nilpotent groups.

Let $\mathcal{K}_{(n)}$ denote the class of all groups of order n.

Definition 4.1. *We say that* $\mathcal{K}_{(n)}$ *has non-nilpotency property if there exists a non-nilpotent group* T *in* $\mathcal{K}_{(n)}$, *such that* $\min\{|W(G)| \mid G \in \mathcal{K}_{(n)}\} = |W(T)|$.

Theorem 4.2. *If $\mathcal{K}_{(n)}$ has non-nilpotency property, then $\mathcal{K}_{(nm)}$, has also non-nilpotency property, for any natural number m, such that $(n, m) = 1$.*

Proof. Let H be a nilpotent group of order nl, since $(n, l) = 1$ and H is nilpotent, there exist normal subgroups N and L of H, such that $|L| = l$, $|N| = n$ and $H = N \times L$. Now, as $N \in \mathcal{K}_{(n)}$ and $\mathcal{K}_{(n)}$ has non-nilpotency property, so there is a non-nilpotent group T in $\mathcal{K}_{(n)}$ such that

$$|W(T)| = \min\{|W(G)| \mid G \in \mathcal{K}_{(n)}\}$$

so

$$|W(T)| \leqslant |W(N)|.$$

If $E = T \times L$, then E is also a non-nilpotent group, and clearly $|T| = |N| = n$ and $|L| = l$. Now, we have

$$|W(E)| = |W(T \times L)| = |W(T)||W(L)| \leqslant W(N)||W(L)| = |W(N \times L)| = |W(H)|.$$

So, as E is a non-nilpotent group, and H is nilpotent group in$\mathcal{K}_{(nl)}$ and $|W(E)| \leqslant W(H)|$, then $\mathcal{K}_{(nl)}$ has non-nilpotency property. □

Example 4.3. It is easy to see that $\mathcal{K}_{(6)}$ has the non-nilpotency property, so $\mathcal{K}_{(30)}$ has the non-nilpotency property, we know that

$$\mathcal{K}_{(30)} = \{C_{30}, C_3 \times D_{10}, C_5 \times D_6, D_{30}\}$$

and

$$\omega(C_{30}) = 8, \omega(C_3 \times D_{10}) = 6, \omega(C_6 \times D_6) = 6 \text{ and } \omega(D_{30}) = 5.$$

Therefore, the minimum weight occurs at the non-nilpotent group D_{30} .

In the following lemma, we construct non-nilpotent groups with small enough weights.

Lemma 4.4. *Let p and q be two distinct prime numbers and $\alpha \in Aut(C_q^r)$ be of order p. If $\{a_1, \ldots, a_m\}$ be the standard generating set for C_p^m, then the semidirect product C_p^m and C_q^r, by the homomorphism $\mu : C_p^m \to Aut(C_q^r)$, such that $\mu(a_i) = \alpha$, for each i, $i = 1, \ldots, m$, is a non-nilpotent group with weight at most 4.*

Proof. Let $b \neq 0$ and $(0, b) \in C_p^m \ltimes C_q^r$. Clearly $(0, b)^q = (0, b^q) = (0, 0)$ and hence $o(0, b) = q$. So, if $a \neq 0$ and $(a, 0) \in C_p^m \ltimes C_q^r$, we have $(a, 0)^p = (a^p, 0) = (0, 0)$, it implies that $o(a, 0) = p$

Now, assume that $a \neq 0$ and $b \neq 0$, as $(a,b)^{pq} = (0,0)$ and $o(a,b) \leqslant pq$, it follows that

$$W(C_p^m \ltimes C_q^r) \subseteq \{1, p, q, pq\},$$

therefore $C_p^m \ltimes C_q^r$ is a non-nilpotent group with maximum weight 4.

□

We use the following useful result in the next theorem.

Proposition 4.5. (See [2]) *For a finite p-group G, $\mathrm{Aut}(G) \cong Gl(n,p)$ if and only if G is an elementary abelian p-group of order p^n.*

Theorem 4.6. *The class of $\mathcal{K}_{(n)}$ has non-nilpotency property, for any non-nilpotent natural number n.*

Proof. As n is not a nilpotent number according to Proposition 3.5, there exist distinct and prime divisors p and q of n such that

$$p \mid q^i - 1$$

Now, we consider $n = p^m q^r k$ that $(pq, k) = 1$. By Proposition 4.5, we have

$$\left|Aut(C_q^r)\right| = (q^r - 1)(q^r - q)(\ldots(q^r - q^{r-1})$$

As

$$p \mid q^i - 1,$$

thus

$$p \mid (q^i - 1)q^{r-i} = q^r - q^{r-i}.$$

Therefore, $p \mid \left|Aut(C_q^r)\right|$ and hence there exists $\alpha \in Aut(C_q^r)$ with $o(\alpha) = p$. Now, if $\{a_1, \ldots, a_m\}$ is standard generator set of C_p^m, we consider homomorphism μ, such that

$$\mu : C_p^m \to Aut(C_q^r)$$

given by $\mu(a_i) = \alpha$ for $i = 1, \ldots, m$. We get semidirect product C_p^m and C_q^r, by homomorphism μ. Then, $C_p^m \ltimes C_q^r$ is a non-nilpotent group of order $p^m q^r$. On the other hand by Lemma 4.4, we have

$$\left|W(C_p^m \ltimes C_q^r)\right| \leqslant 4$$

So, if G is a nilpotent group of order $p^m q^r$, then we have

$$|W(G)| \geqslant 2^2 = 4$$

Thus, we conclude that $\mathcal{K}_{(p^m q^r)}$ has nonnilpotency property. Since $(pq, k) = 1$ and $p^m q^r k = n$, by Theorem 4.2, $\mathcal{K}_{(n)}$ has non-nilpotency property. □

Theorem 4.7. *Let n be an even number, such that n is not a power of 2, then $\mathcal{K}_{(n)}$ has the non-nilpotency property.*

Proof. Suppose that $n = 2^{\alpha_1}p^{\alpha_2}q_3^{\alpha_3}\cdots q_r^{\alpha_r}$, for some $r \geq 2$. Since 2 is a divisor of $\left|Aut\left(Z_p^{\alpha_2}\right)\right|$, we have $\omega\left(\mathbb{Z}_2^{\alpha_1} \ltimes \mathbb{Z}_p^{\alpha_2}\right) \subseteq \{1, 2, p, 2p\}$. Now, let G be a nilpotent group of order n, thus $\omega(G) \geqslant 2^r$, also we have

$$\omega\left(\left(\mathbb{Z}_2^{\alpha_1} \ltimes \mathbb{Z}_p^{\alpha_2}\right) \times \mathbb{Z}_{q_3}^{\alpha_3} \times ... \times \mathbb{Z}_{q_r}^{\alpha_r}\right) \leqslant 4(2^{r-2}) = 2^r$$

Therefore

$$\omega\left(\left(\mathbb{Z}_2^{\alpha_1} \ltimes \mathbb{Z}_p^{\alpha_2}\right) \times \mathbb{Z}_{q_3}^{\alpha_3} \times ... \times \mathbb{Z}_{q_r}^{\alpha_r}\right) \leqslant \omega(G)$$

and the results hold. □

Example 4.8. $\mathcal{K}_{(12)}$, $\mathcal{K}_{(22)}$ and $\mathcal{K}_{(30)}$ has the non-nilpotency property. We know that $\mathcal{K}_{(12)} = \{A_4, D_{12}, T, C_{12}, C_3 \times C_2 \times C_2\}$ in which

$$T =< a, b \mid a^4 = b^3 = 1; a^{-1}ba = b^{-1} >.$$

We have $\omega(T) = \omega(D_{12}) = \omega(C_2 \times C_2 \times C_3) = 4$ also $\omega(A_4) = 3$ and $\omega(C_{12}) = 6$.

$\mathcal{K}_{(22)} = \{C_{22}, D_{22}\}$, $\omega(C_{22}) = 4$ and $\omega(D_{22}) = 3$.

$\mathcal{K}_{(30)} = \{C_{30}, C_3 \times D_{10}, C_5 \times D_6, D_{30}\}$(see Theorem 4.2).

Here, we can prove the main theorem.

Theorem 4.9. *Let G be a finite group of order n, then $|W(G)| \leqslant |W(C_n)|$. If $\min\{|W(G)| \mid |G| = n\} = m$, then $m = 2^{|\pi(n)|}$ or there is a nonnilpotent group T that $|T| = n$ and $|W(T)| = m$. In other words, the class of groups of order n, cyclic group C_n has the most weight and if the least weight on the above groups equals m, then m is a power of 2, such that the power equals to numbers of distinct prime factors of n. Therefore m is the weight of a non-nilpotent group.*

Proof. Let C_n be a cyclic group of order n. If m is a divisor of n, then $m \in W(G)$ and it follows that

$$\{m \in \mathbb{Z} \mid m > 0, m \mid n\} \subseteq W(C_n).$$

Now, if G is a group of order n and $m \in W(G)$, then $m \mid n$ and hence

$$W(G) \subseteq \{m \in \mathbb{Z} \mid m > 0, m \mid n\}.$$

Thus, $W(G) \subseteq W(C_n)$, and so we have

$$|W(G)| \leqslant |W(C_n)|.$$

For the finite group G if n is a nilpotent number, then

$$|W(G)| \geqslant 2^{|\pi(n)|},$$

If n is not a nilpotent number, then $\mathcal{K}_{(n)}$ has nonnilpotency property. So, there exists a nonnilpotent group T in $\mathcal{K}_{(n)}$, such that for every group G in $\mathcal{K}_{(n)}$, we have

$$|W(T)| \leqslant |W(G)|\,.$$

Hence

$$|W(T)| = \min\left\{|W(G)| \mid G \in \mathcal{K}_{(n)}\right\},$$

Therefore, the proof is completed □

References

[1] **H. Amiri, S.M. Jafarian Amiri and I.M. Isaacs**, *Sums of element orders in finite groups*, Commun. Algebra, **37** (2009), no. 9, 2978 – 2980.

[2] **S. Fouladi, R. Orfi**, *General linear groups as automorphism groups*, Intern. J. Algebra, **5** (2011), no. 27, 1327 – 1335.

[3] **N.D. Gupta and V.B. Mazurov**, *On groups with small orders of elements*, Bull. Australian Math. Soc., **6** (1999), 197 – 205.

[4] **F. Levi, B.L. Waerden**, *Uber eine besondere Klasse von Gruppen*, Abhandlungen Math. Seminar Univ. Hamburg, **9** (1932), 154 – 158.

[5] **D.V. Lytkina**, *Structure of a group with elements of order at most*, Siberian Math. J., **48** (2007), 283 – 287.

[6] **B.H. Neumann**, *Groups whose elements have bounded orders*, J. London Math. Soc., **12** (1937), 195 – 198.

[7] **P.S. Novikov, S.I. Adjan**, *Infinite periodic groups I*, Mathematics of the USSR-Izvestiya., **2** (1968), no. 1, 209 – 236.

[8] **J. Pakianathan, K. Shankar**, *Nilpotent numbers*, Amer. Math. Monthly, **107** (2000), no. 7, 631 – 634.

[9] **I.N. Sanov**, *Solution of Burnside's problem for exponent* 4, Leningrad Math. J., **10** (1940), 166 – 170.

Received December 23, 2021

Department of Mathematics and Statistics
University of Birjand
Birjand, Iran
E-mail: mnasrabadi@birjand.ac.ir

Quasigroups and Related Systems **30** (2022), 307 – 315

The relationship between EQ algebras and equality algebras

Akbar Paad

Abstract. It is proved that every involutive equivalential equality algebra $(E, \wedge, \sim, 1)$, is an involutive residualted lattice EQ-algebra, which operation $\otimes$ is defined by $x \otimes y = (x \to y')'$. Moreover, it is showen that by an involutive residualted lattice EQ-algebra we have an involutive equivalential equality algebra.

1. Introduction

Fuzzy type theory (FTT) has been developed by Novák as a fuzzy logic of higher order, the fuzzy version of the classical type theory of the classical logic of higher order. BL-algebras, MTL-algebras, MV-algebras are the best known classes of residuated lattices [4, 5] and since the algebra of truth values is no longer a residuated lattice, a specific algebra called an EQ-algebra [7] by Novák and De Baets was introduced. EQ-algebras generalize the residuated lattices that have three binary operations meet, multiplication, fuzzy equality and a unit element. If the product operation in EQ-algebras is replaced by another binary operation smaller or equal than the original product we still obtain an EQ-algebra, and this fact might make it difficult to obtain certain algebraic results. For this reason, equality algebras were introduced by Jeni [6], which the motivation cames from EQ-algebras [7]. These algebras are assumed for a possible algebraic semantics of fuzzy type theory. It was proved [1, 6], that any equality algebra has a corresponding BCK-meet-semilattice and any BCK(D)-meet-semilattice (with distributivity property) has a corresponding equality algebra. Since equality algebras could also be candidates for a possible algebraic semantics for fuzzy type theory, their study is highly motivated. In [9], by considering the notion of

2010 Mathematics Subject Classification: 08A72, 06E99, 03G25.
Keywords: EQ-algebra, Equality algebra

equality algebra, it is shown that there are relations among equality algebras and some of other logical algebras such as residuated lattice, MTL-algebra, BL-algebra, MV-algebra, Hertz-algebra, Heyting-algebra, Boolean-algebra, EQ-algebra and hoop-algebra. Specially, it was proved that every good EQ-algebra is equality algebra but the converse is open problem which means how multiplication operation, $\otimes$, on equality algebra $(E, \wedge, \sim, 1)$ should be defined such that $(E, \wedge, \otimes, \sim, 1)$ is an EQ-algebra?

2. Preliminaries

In this section, we give some fundamental definitions and results. For more details, refer to the references.

Definition 2.1. (cf. [6]) An algebra $(E, \wedge, \sim, 1)$ of the type $(2, 2, 0)$ is called an *equality algebra* if it satisfies the following conditions, for all $x, y, z \in E$:
$(E1)$ $(E, \wedge, 1)$ is a meet-semilattice with top element 1,
$(E2)$ $x \sim y = y \sim x$,
$(E3)$ $x \sim x = 1$,
$(E4)$ $x \sim 1 = x$,
$(E5)$ $x \leqslant y \leqslant z$ implies $x \sim z \leqslant y \sim z$ and $x \sim z \leqslant x \sim y$,
$(E6)$ $x \sim y \leqslant (x \wedge z) \sim (y \wedge z)$,
$(E7)$ $x \sim y \leqslant (x \sim z) \sim (y \sim z)$.

The operation $\wedge$ is called *meet* (infimum) and $\sim$ is an equality operation. We write $x \leqslant y$ if and only if $x \wedge y = x$, for all $x, y \in E$. Also, other two operations are defined, called *implication* and *equivalence operation*, respectively:

$$x \to y = x \sim (x \wedge y). \tag{I}$$
$$x \leftrightarrow y = (x \to y) \wedge (y \to x). \tag{II}$$

An equality algebra $(E, \sim, \wedge, 1)$ is bounded if there exists an element $0 \in E$ such that $0 \leq x$, for all $x \in E$. In a bounded equality algebra E, we define the negation " $'$ " on E by, $x' = x \to 0 = x \sim 0$, for all $x \in E$. If $x'' = x$, for all $x \in E$, then the bounded equality algebra E is called involutive. A lattice equality algebra is an equality algebra which is a lattice. Equality algebra E (and as well as its equality operation $\sim$) called *equivalential*, if $\sim$ coincides with the equivalence operation of a suitably chosen equality algebra.

Theorem 2.2. (cf. [6]) *An equality algebra* $(E, \sim, \wedge, 1)$ *is equivalential if and only if for all* $x, y \in E$, $x \sim y = (x \sim (x \wedge y)) \wedge (y \sim (x \wedge y))$.

Proposition 2.3. (cf. [6]) *Let* $(E, \wedge, \sim, 1)$ *be an equality algebra. Then the following properties hold, for all* $x, y, z \in E$*:*

(i) $x \to y = 1$ *if and only if* $x \leqslant y$,
(ii) $1 \to x = x$, $x \to 1 = 1$, $x \to x = 1$,
(iii) $x \leqslant (x \sim y) \sim y$,
(iv) $x \leqslant y$ *implies* $y \to z \leqslant x \to z$, $z \to x \leqslant z \to y$,
(v) $x \sim y \leqslant x \leftrightarrow y \leqslant x \to y$,
(vi) $x \to (y \to z) = y \to (x \to z)$.
(vii) $x \to y \leqslant (y \to z) \to (x \to z.)$

Definition 2.4. (cf. [7]) An *EQ-algebra* is an algebra $(E, \wedge, \otimes, \sim, 1)$ of type $(2, 2, 2, 0)$ satisfying the following axioms:

$(EQ1)$ $(E, \wedge, 1)$ is a $\wedge$-semilattice with top element 1. We set $x \leqslant y$ if and only
if $x \wedge y = x$,
$(EQ2)$ $(E, \otimes, 1)$ is a commutative monoid and $\otimes$ is isotone with respect to $\leq$,
$(EQ3)$ $x \sim x = 1$ (reflexivity axiom),
$(EQ4)$ $((x \wedge y) \sim z) \otimes (s \sim x) \leqslant z \sim (s \wedge y)$ (substitution axiom),
$(EQ5)$ $(x \sim y) \otimes (s \sim t) \leqslant (x \sim s) \sim (y \sim t)$ (congruence axiom),
$(EQ6)$ $(x \wedge y \wedge z) \sim x \leqslant (x \wedge y) \sim x$ (monotonicity axiom),
$(EQ7)$ $x \otimes y \leqslant x \sim y$ (boundedness axiom),
For all $s, t, x, y, z \in E$.

Let E be an EQ-algebra. Then for all $x, y \in E$, we put

$$x \to y = (x \wedge y) \sim x, \qquad \tilde{x} = x \sim 1.$$

The derived operation $\to$ is called *implication*. If an EQ-algebra E contains a bottom element 0, then we may define the unary operation $\neg$ on E by $\neg x = x \sim 0 = x \to 0$.

Definition 2.5. (cf. [7]) Let E be an EQ-algebra. We say that it is

(i) *good*, if $\tilde{x} = x$ for all $x \in E$.
(ii) *residuated*, if $(x \otimes y) \wedge z = x \otimes y$ if and only if $x \wedge ((y \wedge z) \sim y) = x$ for all
$x, y, z \in E$
(iii) *envolutive* (*IEQ-algebra*), if $\neg\neg x = x$, for all $x \in E$.

(*iv*) *lattice-ordered EQ-algebra* if it has a lattice reduct.
(*v*) *lattice EQ-algebra* (*lEQ-algebra*) if it is a lattice-ordered EQ-algebra in which the following substitution axiom holds forall $x, y, z, w \in E$:

$$((x \vee y) \sim z) \otimes (w \sim x) \leqslant ((w \vee y) \sim z)$$

Proposition 2.6. (cf. [3]) *For an EQ-algebra E the following are equivalent:*
(*i*) *E is residuated,*
(*ii*) *E is good and $x \leqslant y \to (x \otimes y)$ holds for all $x, y \in E$.*

Proposition 2.7. (cf. [2, 7]) *Let E be an EQ-algebra. Then for any $x, y, z \in E$:*
(*i*) *$x = 1 \to x$ and $x \to (y \to z) = y \to (x \to z)$, where E is residuated.*
(*ii*) *$x \otimes y \leqslant z$ if and only if $x \leqslant y \to z$, where E is good.*

Theorem 2.8. (cf. [7]) *Any IEQ-algebra E is a good, spanned and separated lattice EQ-algebra.*

Definition 2.9. (cf. [8]) A *residuated lattice* is an algebra $(E, \vee, \wedge, \otimes, \to, 0, 1)$ of type $(2, 2, 2, 2, 0, 0)$ satisfying the following axioms:
(*i*) $(E, \vee, \wedge, 0, 1)$ is a bounded lattice,
(*ii*) $(E, \otimes, 1)$ is a commutative monoid,
(*iii*) $x \otimes y \leqslant z$ if and only if $x \leqslant y \to z$, for any $x, y, z \in E$.

Theorem 2.10. (cf. [9]) *The algebraic structure $(E, \vee, \wedge, \otimes, \to, 0, 1)$ is a residuated lattice if and only if*
(*RL*1) *$(E, \vee, \wedge, 0, 1)$ is a bounded lattice,*
(*RL*2) *$(E, \to, 1)$satisfies $x = 1 \to x$ and $x \to (y \to z) = y \to (x \to z)$,*
(*RL*3) *$x \otimes y \leqslant z$ if and only if $x \leqslant y \to z$, for any $x, y, z \in E$.*

Theorem 2.11. (cf. [9]) *For any residuated lattice $\mathcal{E} = (E, \vee, \wedge, \to, 0, 1)$, the structure $\psi(\mathcal{E}) = (E, \vee, \wedge, \leftrightarrow, 0, 1)$ is a bounded lattice equality algebra, where $\leftrightarrow$ denotes the equivalence operation of E. Moreover, the implication of $\psi(\mathcal{E})$ coincides with $\leftrightarrow$, that is, $x \to y = x \leftrightarrow (x \wedge y)$.*

3. Relation between algebras

Theorem 3.1. (cf. [9]) *Every good EQ-algebra $(E, \wedge, \sim, \otimes, 1)$ is an equality algebra.*

Open problem. Under what suitable conditions the converse of Theorem 3.1 is correct? Which means how multiplication operation, $\otimes$, on equality algebra $(E, \wedge, \sim, 1)$ should be defined such that $(E, \wedge, \otimes, \sim, 1)$ is an EQ-algebra?

In the following, by adding some conditions to an equality algebra, we answer to this open problem as follow:

Theorem 3.2. *Let $(E, \wedge, \sim, 1)$ be an involutive equivalential equality algebra. Then $(E, \wedge, \sim, \otimes, 1)$ is an involutive residualted lattice EQ-algebra, which operation $\otimes$ is defined by $x \otimes y = (x \to y')'$.*

Proof. Let $(E, \wedge, \sim, 1)$ be an involutive equivalential equality algebra. Then $(E, \wedge, 1)$ is a meet semilattice with top element 1 and so $(EQ1)$ holds. For $x, y \in E$, we define $x \otimes y = (x \to y')'$ and we prove that $(E, \otimes, 1)$ is a commutative monoid and $\otimes$ is isotone with respect to $\leqslant$. By Proposition 2.3(vi), for $x, y \in E$, we have

$$x \otimes y = (x \to y')' = (x \to (y \to 0))' = (y \to (x \to 0))' = (y \to x')' = y \otimes x.$$

Hence, operation $\otimes$ is commutative.

Let $x, y, z \in E$. Then by Proposition 2.3(vi), we have

$$\begin{aligned} x \otimes (y \otimes z) &= (x \to (y \otimes z)'))' = (x \to (y \to z')'')' = (x \to (y \to z'))' \\ &= (x \to (y \to (z \to 0)))' = (x \to (z \to (y \to 0)))' \\ &= (z \to (x \to (y \to 0)))' = (z \to (x \to (y \to 0)'')')' \\ &= (z \to (x \otimes y)')' = z \otimes (x \otimes y) = (x \otimes y) \otimes z. \end{aligned}$$

Hence, operation $\otimes$ is associative. Now, let $x \leqslant y$. Then by Proposition 2.3(iv), $y' = y \to 0 \leqslant x \to 0 = x'$ and so $z \to y' \leqslant z \to x'$. Hence, $x \otimes z = z \otimes x = (z \to x')' \leqslant (z \to y')' = z \otimes y = y \otimes z$. Thus, the operation $\otimes$ is isotone respect to $\leqslant$. Moreover, $x \otimes 1 = (x \to 1')' = x''' = x$ and so $(E, \otimes, 1)$ is a commutative monoid which proves the $(EQ2)$. Since by $(E3)$, $x \sim x = 1$, for any $x \in E$, we conclude that $(EQ3)$. In the follow, we prove $x \otimes y \leqslant z$ if and only if $x \leqslant y \to z$, for any $x, y, z \in E$. Since E is involutive and by Proposition 2.3(i) and (iv), for any $x, y, z \in E$, we have $x \otimes y \leqslant z$ if and only if $(x \to y')' \leqslant z$ if and only if $z' \leqslant (x \to y')''$ if and only if $z' \leqslant x \to y'$ if and only if $x \leqslant z' \to y'$ if and only if $x \leqslant y \to z''$ if and only if $x \leqslant y \to z$. Now, we prove $(EQ4)$. Let $x, y, z, w \in E$. Then

$$((x \wedge y) \sim z) \otimes (w \sim x) \leqslant z \sim (w \wedge y)$$

if and only if

$$(((x \wedge y) \sim z) \to (w \sim x)')' \leqslant z \sim (w \wedge y)$$

if and only if

$$(z \sim (w \wedge y))' \leqslant (((x \wedge y) \sim z) \to (w \sim x)')''$$

if and only if

$$(z \sim (w \wedge y))' \leqslant ((x \wedge y) \sim z) \to (w \sim x)'$$

if and only if

$$(z \sim (w \wedge y))' \otimes ((x \wedge y) \sim z) \leqslant (w \sim x)'$$

if and only if

$$(w \sim x)'' \leqslant ((z \sim (w \wedge y))' \otimes ((x \wedge y) \sim z))'$$

if and only if

$$(w \sim x) \leqslant ((z \sim (w \wedge y))' \otimes ((x \wedge y) \sim z))'$$

if and only if

$$(w \sim x) \leqslant ((z \sim (w \wedge y))' \to ((x \wedge y) \sim z)')''$$

if and only if

$$(w \sim x) \leqslant (z \sim (w \wedge y))' \to ((x \wedge y) \sim z)'.$$

Now, since by $(E6)$ and Proposition 2.3(v), for any $x, y, z, w \in E$, we have

$$\begin{aligned}(w \sim x) &\leqslant (x \wedge y) \sim (w \wedge y)\\ &\leqslant ((w \wedge y) \sim z) \sim ((x \wedge y) \sim z)\\ &\leqslant ((w \wedge y) \sim z)' \sim ((x \wedge y) \sim z)'\\ &\leqslant ((w \wedge y) \sim z)' \to ((x \wedge y) \sim z)'\\ &= (z \sim (w \wedge y))' \to (z \sim (x \wedge y))'.\end{aligned}$$

Now, since the inequality $(w \sim x) \leqslant (z \sim (w \wedge y))' \to (z \sim (x \wedge y))'$, holds for any $x, y, z, w \in E$, we conclude that $((x \wedge y) \sim z) \otimes (w \sim x) \leqslant z \sim (w \wedge y)$, for any $x, y, z, w \in E$ and so $(EQ4)$ holds.

For $(EQ5)$, we must prove $(x \sim y) \otimes (s \sim t) \leqslant (x \sim s) \sim (y \sim t)$, for any $x, y, s, t \in E$. Since for any $x, y, s, t \in E$, by $(E7)$ and Proposition 2.3(v) and (vi), we have:

$$\begin{aligned}(s \sim t) &\leqslant (x \sim s) \sim (x \sim t) \leqslant (x \sim s) \to (x \sim t)\\ &\leqslant (x \sim s) \to ((x \sim y) \sim (y \sim t))\\ &\leqslant (x \sim s) \to ((x \sim y) \to (y \sim t))\\ &= (x \sim y) \to ((x \sim s) \to (y \sim t)).\end{aligned}$$

So, we conclude that $(s \sim t) \otimes (x \sim y) \leqslant (x \sim s) \to (y \sim t)$. Moreover, since by Proposition 2.3(iv) and (v), for any $x, y, s, t \in E$,

$$\begin{aligned}(s \sim t) &\leq (t \sim y) \sim (s \sim y)\\ &\leq (y \sim t) \to (y \sim s)\\ &\leq (y \sim t) \to ((x \sim y) \sim (x \sim s))\\ &\leq (y \sim t) \to ((x \sim y) \to (x \sim s))\\ &= (x \sim y) \to ((y \sim t) \to (x \sim s)).\end{aligned}$$

We conclude that $(s \sim t) \otimes (x \sim y) \leqslant (y \sim t) \to (x \sim s)$ and so we have

$$(s \sim t) \otimes (x \sim y) \leqslant ((x \sim s) \to (y \sim t)) \wedge ((y \sim t) \to (x \sim s))$$

and since E is equivalential, we get that

$$((x \sim s) \to (y \sim t)) \wedge ((y \sim t) \to (x \sim s)) = (x \sim s) \sim (y \sim t)$$

Hence,

$$(s \sim t) \otimes (x \sim y) \leqslant (x \sim s) \sim (y \sim t).$$

Therefore, $(EQ5)$ is established.

For $(EQ6)$, assume that $x, y, z \in E$. Then by $x \wedge y \wedge z \leqslant x \wedge y \leqslant x$ and $(E5)$, we get that

$$(x \wedge y \wedge z) \sim x \leqslant (x \wedge y) \sim x.$$

Hence, $(EQ6)$ holds. Finally, let $x, y \in E$. Then by Proposition 2.3(iii) and (v),

$$x \leqslant (x \sim y) \sim y = y \sim (x \sim y) \leq y \to (x \sim y).$$

Hence, $x \otimes y \leqslant x \sim y$ and so $(EQ7)$ is established. Therefore, $(E, \wedge, \sim, \otimes, 1)$ is an EQ-algebra and since $x = x'' = (x \to 0) \to 0 = \neg\neg x$ and by $(E4)$,

$1 \sim x = x$, for any $x \in E$, by Theorem 2.8, we conclude that $(E, \wedge, \sim, \otimes, 1)$ is an involutive good lattice EQ-algebra. Moreover, since by Proposition 2.3(iii), $x \leqslant (x \sim y) \sim y$, for any $x, y \in E$ and by $x \otimes y \leqslant x \otimes y$, we have $x \leqslant y \to (x \otimes y)$, for any $x, y \in E$, by Proposition 2.6, we conclude that $(E, \wedge, \sim, \otimes, 1)$ is a residuated EQ-algebra. Therefrore, $(E, \wedge, \sim, \otimes, 1)$ is an involutive residualted lattice EQ-algebra. □

Theorem 3.3. *Let $(E, \wedge, \sim, \otimes, 1)$ be an involutive residualted lattice EQ-algebra. Then $(E, \vee, \wedge, \otimes, \leftrightarrow, 0, 1)$ be an involutive equivalential equality algebra.*

Proof. Let $(E, \wedge, \sim, \otimes, 1)$ be an involutive residualted lattice EQ-algebra. Then $(E, \vee, \wedge, 0, 1)$ is a bounded lattice and by Theorem 2.8, E is a good EQ-algebra and so by Proposition 2.7(i), $x = 1 \to x$ and $x \to (y \to z) = y \to (x \to z)$, for any $x, y \in E$. Moreover, since E is a residuated EQ-algebra, by Proposition 2.7(ii), we get that $x \otimes y \leqslant z$ if and only if $x \leqslant y \to z$, for any $x, y, z \in E$. Hence, by Theorem 2.10, $(E, \vee, \wedge, \otimes, \to, 0, 1)$ is a residuated lattice and so by Theorem 2.11, $(E, \vee, \wedge, \otimes, \leftrightarrow, 0, 1)$ is a bounded lattice equality algebra, where $\leftrightarrow$ denote the equivalence operation of E and $x \to y = x \leftrightarrow (x \wedge y)$ and since

$$x \leftrightarrow y = (x \to y) \wedge (y \to x) = (x \leftrightarrow (x \wedge y)) \wedge (y \leftrightarrow (y \wedge x))$$

by Theorem 2.2, we conclude that $(E, \wedge, \leftrightarrow, 1)$ is an equvalential equality algebra. Now, we prove $(E, \wedge, \leftrightarrow, 0, 1)$ is an involutive equality algebra. For $x, y \in E$, we have

$$x \leftrightarrow 0 = (x \to 0) \wedge (0 \to x) = (x \to 0) \wedge 1 = x \to 0$$

and since $(E, \wedge, \sim, \otimes, 1)$ an involutive EQ-algebra we get that

$$(x \leftrightarrow 0) \leftrightarrow 0 = (x \to 0) \leftrightarrow 0 = (x \to 0) \to 0 = x.$$

Therefore, $(E, \vee, \wedge, \otimes, \leftrightarrow, 0, 1)$ is an involutive equivalential equality algebra. □

4. Conclusion

The main result of this paper is devoted to solution of open problem which is about relation between EQ-algebras and equality algebras. In [9], it is proved that every good EQ-algebra is a equality algebra and it is asked

under what suitable conditions the converse is correct? We proved that every involutive equivalential equality algebra $(E, \wedge, \sim, 1)$, is an involutive residualted lattice EQ-algebra, which operation $\otimes$ is defined by $x \otimes y = (x \to y')'$. Moreover, we showed that by an involutive residualted lattice EQ-algebra we have an involutive equivalential equality algebra.

References

[1] **L.C. Ciungu**, *Internal states on equality algebras*, Soft Comput., **19** (2015), 939 – 953.

[2] **M. El-Zekey**, *Representable good EQ-algebras*, Soft Comput., **14** (2010), 1011 – 1023.

[3] **M. El-Zekey, V. Novák, R. Mesiar**, *On good EQ-algebras*, Fuzzy Sets and Systems, **178** (2011), 1 – 23.

[4] **F. Esteva, L. Godo**, *Monoidal t-normbased logic: towards a logic for left-continuous t-norms*, Fuzzy Sets and Systems, **124** (2001) no. 3, 271 – 288.

[5] **P. Hájek**, *Metamathematics of Fuzzy Logic*, Springer Science and Business Media, 1998.

[6] **S. Jenei**, *Equality algebras, Studia Logica*, **100** (2012) no. 6, 1201 – 1209.

[7] **V. Novák, B. De Baets**, *EQ-algebras, Fuzzy Sets and Systems*, **160** (2009) no. 20, 2956 – 2978.

[8] **M. Ward, R.P. Dilworth**, *Residuated lattices, Trans. Am. Math. Soc.* **45** (1939), 335˘354.

[9] **F. Zebardast, R.A. Borzooei, M. Aaly Kologani**, *Results on Equality algebras*, Information Sciences, **381** (2017), 270 – 282.

Received Jun 20, 2021

Department of Mathematics
University of Bojnord
Bojnord
Iran
e-mail: akbar.paad@gmail.com, a.paad@ub.ac.ir

Quasigroups and Related Systems **30** (2022), 317 – 327

Normal filter in quasi-ordered residuated systems

Daniel A. Romano

Abstract. The concept of quasi-ordered residuated systems was introduced by Bonzio and Chajda in 2018. The author introduced the concept of filters in such systems as well as some types of filters in them such as implicative and comparative filters. This article introduces the concept of a normal filter in a quasi-ordered residuated system and relates it to some other filters in such algebraic systems.

1. Introduction

Residuated lattices were introduced by Ward and Dilworth in [15]. The filter theory of residuated lattice has been widely studied, and some important results have been obtained. Normal filters in BL-algebra were defined in paper [13]. Borzooei and Paad studied the normal filter in BL-algebras (cf. [4]) by comparing it with other types of filters in residuated lattices. Ahadpanah and Torkzadeh are studied normal filters in residuated lattices (cf. [1]). Wang et al. also dealt with normal filters in some logical algebras (cf. [14]).

The concept of residuated relational systems ordered under a quasi-order relation, or quasi-ordered residuated systems (briefly, QRS), was introduced in 2018 by S. Bonzio and I. Chajda (cf. [3]). Previously, this concept was discussed in [2]. It should be noted that this algebraic system differs from the commutative residuated lattice ordered under a quasi-order (see Example 2.13):

- QRS does not have to be limited from below: and
- QRS, in the general case, does not have to be a lattice.

The author introduced and developed the concepts of filters (cf. [7]) in this algebraic structure as well as several types of filters such as implicative (cf.

2010 Mathematics Subject Classification: 08A02, 06A11
Keywords: Quasi-ordered residuated system, filter in quasi-ordered residuared system, implicative filter, comparative filter, normal filter.

[9]), associated (cf. [8]) and comparative filters (cf. [10]). In [9], it is shown that every comparative filter of a quasi-ordered residuated system $\mathfrak{A}$ is an implicative filter of $\mathfrak{A}$ and the reverse it need not be valid.

In the following, some preliminary claims and terms about quasi-ordered residuated systems are taken from the literature [2, 3, 7, 9, 10]. In Section 3, we define the concept of normal filters in a quasi-ordered residuated system and we prove some theorems that accurately describe the relationship between this notion and the other types of filters in such an algebraic structure.

2. Preliminaries

2.1. Concept of quasi-ordered residuated systems

In article [3], S. Bonzio and I. Chajda introduced and analyzed the concept of residual relational systems.

Definition 2.1. [[3], Definition 2.1] A *residuated relational system* is a structure $\mathfrak{A} = \langle A, \cdot, \to, 1, R\rangle$, where $\langle A, \cdot, \to, 1\rangle$ is an algebra of type $\langle 2, 2, 0\rangle$ and R is a binary relation on A and satisfying the following properties:

(1) $(A, \cdot, 1)$ is a commutative monoid;
(2) $(\forall x \in A)((x, 1) \in R)$;
(3) $(\forall x, y, z \in A)((x \cdot y, z) \in R \Longleftrightarrow (x, y \to z) \in R)$.

We will refer to the operation $\cdot$ as multiplication, to $\to$ as its residuum and to condition (3) as residuation.

The basic properties for residuated relational systems are subsumed in the following

Theorem 2.2 ([3], Proposition 2.1)**.** *Let $\mathfrak{A} = \langle A, \cdot, \to, 1, R\rangle$ be a residuated relational system. Then*

(4) $(\forall x, y \in A)(x \to y = 1 \Longrightarrow (x, y) \in R)$;
(5) $(\forall x \in A)((x, 1 \to 1) \in R)$;
(6) $(\forall x \in A)((1, x \to 1) \in R)$;
(7) $(\forall x, y, z \in A)(x \to y = 1 \Longrightarrow (z \cdot x, y) \in R)$;
(8) $(\forall x, y \in A)((x, y \to 1) \in R)$.

Recall that a *quasi-order relation* $' \preccurlyeq '$ on a set A is a binary relation which is reflexive and transitive.

Definition 2.3. [[3], Definition 3.1] A *quasi-ordered residuated system* is a residuated relational system $\mathfrak{A} = \langle A, \cdot, \to, 1, \preccurlyeq \rangle$, where $\preccurlyeq$ is a quasi-order relation in the monoid $(A, \cdot)$

Example 2.4. Let $A = \{1, a, b, c, d\}$ and operations '$\cdot$' and '$\to$' defined on A as follows:

$\cdot$	1	a	b	c	d
1	1	a	b	c	d
a	a	a	d	c	d
b	b	d	b	d	d
c	c	c	d	c	d
d	d	d	d	d	d

and

$\to$	1	a	b	c	d
1	1	a	b	c	d
a	1	1	b	c	d
b	1	a	1	c	c
c	1	1	b	1	b
d	1	1	1	1	1

Then $\mathfrak{A} = \langle A, \cdot, \to, 1 \rangle$ is a quasi-ordered residuated systems where the relation '$\preccurlyeq$' is defined as follows $\preccurlyeq := \{(1,1), (a,1), (b,1), (c,1), (d,1), (b,b), (a,a), (c,c), (d,d), (c,a), (d,a), (d,b), (d,c)\}$.

Example 2.5. For a commutative monoid A, let $\mathfrak{P}(A)$ denote the powerset of A ordered by set inclusion and '$\cdot$' the usual multiplication of subsets of A. Then $\langle \mathfrak{P}(A), \cdot, \to, A, \subseteq \rangle$ is a quasi-ordered residuated system in which the residuum are given by

$$(\forall X, Y \in \mathfrak{P}(A))(Y \to X := \{z \in A : Yz \subseteq X\}).$$

Example 2.6. Let $\mathbb{R}$ be a field of real numbers. Define a binary operations '$\cdot$' and '$\to$' on $A = [0,1] \subset \mathbb{R}$ by

$$(\forall x, y \in [0,1])(x \cdot y := max\{0, x+y-1\}) \text{ and } x \to y := min\{1, 1-x+y\}).$$

Then, A is a commutative monoid with the identity 1 and $\langle A, \cdot, \to, \leqslant, 1 \rangle$ is a quasi-ordered residuated system.

Example 2.7. Any commutative residuated lattice $\langle A, \cdot, \to, 0, 1, \sqcap, \sqcup, R \rangle$ where R is a lattice quasi-order is a quasi-ordered residuated system.

The following proposition shows the basic properties of quasi-ordered residuated systems.

Proposition 2.8 ([3], Proposition 3.1)**.** *Let A be a quasi-ordered residuated system. Then*

(9) $(\forall x, y, z \in A)(x \preccurlyeq y \implies (x \cdot z \preccurlyeq y \cdot z \wedge z \cdot x \preccurlyeq z \cdot y))$;

(10) $(\forall x, y, z \in A)(x \preccurlyeq y \implies (y \to z \preccurlyeq x \to z \wedge z \to x \preccurlyeq z \to y))$;

(11) $(\forall x, y \in A)(x \cdot y \preccurlyeq x \wedge x \cdot y \preccurlyeq y)$.

It is generally known that a quasi-order relation $\preccurlyeq$ on a set A generates an equivalence relation $\equiv_{\preccurlyeq} := \preccurlyeq \cap \preccurlyeq^{-1}$ on A. Due to properties (9) and (10), this equivalence is compatible with the operations in $\mathfrak{A}$. Thus, $\equiv_{\preccurlyeq}$ is a congruence on $\mathfrak{A}$. The concept of a strong quasi-ordered residuated system is given by the following definition:

Definition 2.9. [[11], Definition 6] For a quasi-ordered residuated system $\mathfrak{A}$ it is said to be a *strong quasi-ordered residuated system* if the following holds

$$(\forall u, v \in A)((u \to v) \to v \equiv_{\preccurlyeq} (v \to u) \to u).$$

Example 2.10. Let $A = \{1, a, b, c\}$ and operations '$\cdot$' and '$\to$' defined on A as follows:

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	a	a	a
b	b	a	b	a
c	c	a	a	c

and

$\to$	1	a	b	c
1	1	a	b	c
a	1	1	1	1
b	1	c	1	c
c	1	b	b	1

Then $\mathfrak{A} = \langle A, \cdot, \to, 1\rangle$ is a quasi-ordered residuated systems where the relation '$\preccurlyeq$' is defined as follows

$$\preccurlyeq := \{(1,1), (a,1), (b,1), (c,1), (a,a), (b,b), (c,c), (a,b), (a,c)\}.$$

Direct verification it can prove that $\mathfrak{A}$ is a strong quasi-ordered residuated system.

2.2. Concept of filters

In this subsection we give some notions that will be used in this article.

Definition 2.11. [[7], Definition 3.1] For a non-empty subset F of a quasi-ordered residuated system $\mathfrak{A}$ we say that it is a *filter* of $\mathfrak{A}$ if it satisfies conditions

$(F2)$ $(\forall u, v \in A)((u \in F \wedge u \preccurlyeq v) \implies v \in F)$, and

$(F3)$ $(\forall u, v \in A)((u \in F \wedge u \to v \in F) \implies v \in F)$.

It is shown (cf. [7], Proposition 3.4 and Proposition 3.2), that if a non-empty subset F of a quasi-ordered system $\mathfrak{A}$ satisfies the condition (F2), then it also satisfies the conditions

(F-0) $1 \in F$ and

(F-1) $(\forall u, v \in A)((u \cdot v \in F \implies (u \in F \wedge v \in F))$.

If $\mathfrak{F}(A)$ is the family of all filters in a QRS $\mathfrak{A}$, then $\mathfrak{F}(A)$ is a complete lattice (cf. [7], Theorem 3.1).

Remark 2.12. In implicative algebras, the term 'implicative filter' is used instead of the term 'filter' we use (see, for example [5, 12]) because in the structure we study the concept of filter is determined more complexly than requirements (F3). It is obvious that our filter concept is also a filter in the sense of [5, 6, 12]. The term 'special implicative filter' is also used in the aforementioned sources if the implicative filter in the sense of [12] satisfies some additional condition.

Example 2.13. Let $A = \langle -\infty, 1] \subset \mathbb{R}$ (the real numbers field). If we define '$\cdot$' and '$\to$' as follows, $(\forall y, v \in A)(u \cdot v := min\{u, v\})$ and $u \to v := 1$ if $u \leqslant v$ and $u \to v := v$ if $v < u$ for all $u, v \in A$, then $\mathfrak{A} := \langle A, \cdot, \to, 1, \leqslant \rangle$ is a quasi-ordered residuated system. All filters in $\mathfrak{A}$ are in the form of $\langle x, 1]$, for $x \in \langle -\infty, 1]$.

Terms covering some of the requirements used herein to identify various types of filters in the observed algebraic structure are mostly taken from papers on UP-algebras. In some other algebraic systems, different terms are used to cover the concepts of implicative and comparative filters mentioned herein.

Definition 2.14. [[9], Definition 3.1] For a non-empty subset F of a quasi-ordered residuated system $\mathfrak{A}$ we say that an *implicative filter* of $\mathfrak{A}$ if (F2) and the following condition

(IF) $(\forall u, v, z \in A)((u \to (v \to z) \in F \wedge u \to v \in F) \implies u \to z \in F)$

are valid.

Definition 2.15. [[10], Definition 3.1] For a non-empty subset F of a quasi-ordered residuated system $\mathfrak{A}$ we say that a *comparative filter* of $\mathfrak{A}$ if (F2) and the following condition

(CF) $(\forall u, v, z \in A)((u \to ((v \to z) \to v) \in F \wedge u \in F) \implies v \in F)$

are valid.

Example 2.16. *Let $\mathfrak{A}$ be a quasi-ordered residuated system as in Example 2.4. Then the set $F := \{1, a, b\}$ is a comparative filter in $\mathfrak{A}$.*

In [9] (Theorem 3.4), it is shown that every comparative filter in a quasi-ordered residuated system is an implicative filter and that the reverse does not have to be.

Example 2.17. (cf. [9], Example 3.3) Let $\mathfrak{A}$ be a quasi-ordered residuated system as in Example 2.4. Then the subset $F := \{1, b\}$ is an implicative filter but it is not a comparative filter.

Notions and notations that are used but not previously determined in this paper can be found in ([2, 3, 7, 8, 9, 10]).

3. Normal filters in QRS

In this section, which is the main part of this paper, the concept of a normal filter in a quasi-ordered residuated system is presented and some of its important features are shown. Some of the assertions used in this article, although shown in our paper [9], will be shown again due to the consistency of the material presented in this paper.

Definition 3.1. A filter F of a quasi-ordered residuated system $\mathfrak{A}$ is called *normal* if the following holds

(NF) $(\forall x, y, z \in A)((z \to ((y \to x) \to x) \in F \wedge z \in F) \Rightarrow (x \to y) \to y \in F)$.

In the general case, the filter in a quasi-ordered residuated system does not have to be a normal filter.

Theorem 3.2. *If $\mathfrak{A}$ is a strong quasi-ordered residuated system, then any filter of $\mathfrak{A}$ is a normal filter of $\mathfrak{A}$.*

Proof. Let F be a filter of a strong quasi-ordered residuated system $\mathfrak{A}$. Suppose that $x, y, z \in A$ are elements such that $z \in F$ and $z \to ((y \to x) \to x) \in F$. Then $(y \to x) \to x \in F$ by (F-3). Since $(y \to x) \to x = (x \to y) \to y$ because $\mathfrak{A}$ is a strong quasi-ordered residuated system, we conclude that $(x \to y) \to y \in F$ is valid. So, F is a normal filter. □

Example 3.3. Let $\mathfrak{A}$ be as in Example 2.13. We will show that $\mathfrak{A}$ does not have any proper normal filter. Let $u, v \in A$ be such that $u < v < x$ and let $F := \langle x, 1]$ be a filter in $\mathfrak{A}$ where $x < 1$. Then $(v \to u) \to u = 1 \in F$ and $(u \to v) \to v = u \to v = u \notin F$. So, F is not a normal filter in $\mathfrak{A}$. Thus, F is not a normal filter in A according to Theorem 3.2.

In what follows, we need the following lemma

Lemma 3.4 ([9], Lemma 3.1)**.** *Let a subset F of a quasi-ordered residuated system $\mathfrak{A}$ satisfies the condition (F2). Then the following holds*

$$(\forall u \in A)(u \in F \iff 1 \to u \in F).$$

Proof. Since $(\forall x \in A)(1 \to x \preccurlyeq x)$ and $(\forall x \in A)(x \preccurlyeq 1 \to x)$, by Proposition 2.3 (d) in [3], the proof of this lemma follows from (F2). □

Theorem 3.5. *Let F be a filter of a quasi-ordered residuated system $\mathfrak{A}$. F is a normal filter of $\mathfrak{A}$ if and only if the followings holds*

(12) $(\forall x, y, z \in A)((y \to x) \to x \in F \implies (x \to y) \to y \in F)$.

Proof. Let F be a normal filter of a quasi-ordered residuated system $\mathfrak{A}$ and let $x, y, z \in A$ be elements such that $(y \to x) \to x \in F$. Since $(y \to x) \to x \in F$ is equivalent with $1 \to ((y \to x) \to x) \in F$ by Lemma 3.4 and since $1 \in F$, thus $(x \to y) \to y \in F$ because F is a normal filter of $\mathfrak{A}$.

Suppose that the filter F of a quasi-ordered residuated system $\mathfrak{A}$ satisfies the condition (12). Let $z \to ((y \to x) \to x) \in F$ and $z \in F$ be holds for all $x, y, z \in A$. Since F is a filter of $\mathfrak{A}$, then $(y \to x) \to x \in F$ by (F-3). Thus we get that $(x \to y) \to y \in F$ by the hypothesis (12). Hence, F is a normal filter of $\mathfrak{A}$. □

In proving the following result that connects comparative and normal filters in a quasi-ordered residuated system we need the following lemma

Lemma 3.6 ([9], Proposition 3.1)**.** *For any comparative filter F in a quasi-ordered residuated system $\mathfrak{A}$ holds*

(13) $(\forall v, z \in A)((v \to z) \to v \in F \implies v \in F)$.

Theorem 3.7. *Any comparative filter in a quasi-ordered residuated sustem $\mathfrak{A}$ is a normal filter in $\mathfrak{A}$.*

Proof. Let F be a filter in $\mathfrak{A}$ and let $x, y, z \in A$ be such $(x \to y) \to y \in F$. By the clain (11) of Proposition 2.8, we conclude

$$x \preccurlyeq (y \to x) \to x.$$

Then

$$((y \to x) \to x) \to y \preccurlyeq x \to y$$

by (10) and by repeated procedure, we have

$$(x \to y) \to y \preccurlyeq (((y \to x) \to x) \to y) \to y.$$

Thus $(((y \to x) \to x) \to y) \to y \in F$ by (F2).

On the other hand, since $y \to x \preccurlyeq y \to x$ is equivalent to $(y \to x) \cdot y \preccurlyeq x$ according to (3) and $y \cdot (y \to x) \preccurlyeq x$, respectively, because the multiplication in A is commutative operation, we have

$$y \preccurlyeq (y \to x) \to x.$$

If we treat this inequality with $((y \to x) \to x) \to y$ using procedure (10) on the right, we get

$$(((y \to x) \to x) \to y) \to y \preccurlyeq (((y \to x) \to x) \to y) \to ((y \to x) \to x).$$

Since $(((y \to x) \to x) \to y) \to y \in F$, we obtain

$$(((y \to x) \to x) \to y) \to ((y \to x) \to x) \in F$$

according to (F2). If we denote $v =: (y \to x) \to x$, $z =: y$, then we recognize the previous condition as the hypothesis in Lemma 3.6. Therefore $(y \to x) \to x \in F$, since F is a comparative filter in $\mathfrak{A}$. So, F is a normal filter in $\mathfrak{A}$. □

Example 3.8. Let $A = \{1, a, b, c\}$ and operations '$\cdot$' and '$\to$' defined on A as follows:

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	a	a	a
b	b	a	a	a
c	c	a	a	1

and

$\to$	1	a	b	c
1	1	a	b	c
a	1	1	1	1
b	1	b	1	b
c	1	b	1	1

Then $\mathfrak{A} = \langle A, \cdot, \to, 1\rangle$ is a quasi-ordered residuated systems where the relation '$\preccurlyeq$' is defined as follows

$$\preccurlyeq := \{(1,1), (a,1), (b,1), (c,1), (a,a), (a,b), (a,c), (b,b), (c,b), (c,c)\}.$$

Subset $\{1\}$ is a normal filter of $\mathfrak{A}$ but it is not a comparative filter in $\mathfrak{A}$ because it does not satisfy the condition (13) since, for example, for $v = b$ and $u = a$, we have $(b \to a) \to b = 1 \in F$ while $b \notin F$.

Example 3.9. Let $\mathfrak{A}$ be as in Example 3.8. $F = \{1\}$ is a normal filter in $\mathfrak{A}$ but it is not an implicative filter in $\mathfrak{A}$ since it does not satisfy the condition (14). For example, for $u = b$ and $v = c$ we have $u \to (u \to v) = b \to (b \to c) = b \to b = 1 \in F$ but $u \to v = b \to c = b \notin F$.

We first express the following theorem:

Theorem 3.10. *Every comparative filter in a quasi-ordered residuated system is an implicative and a normal filter in it.*

Proof. The proof is obtained by combining Theorem 3.4 in [9] and Theorem 3.7. □

To demonstrate the following statement we need the following lemma

Lemma 3.11 ([9], Proposition 3.1)**.** *Let F be an implicative filter of a quasi-ordered residuated system A. Then the following holds*

(14) $(\forall u, v \in A)(u \to (u \to v) \in F \implies u \to v \in F)$.

Proof. If we put $v = u$ in (IF), we immediately obtain the claim of this proposition, since for every $u \in A$ always $u \to u \in F$ holds for every non-empty set F satisfying condition (F2). Indeed, $u \to u \in F$ follows from $u \preccurlyeq u$; whence $1 \preccurlyeq (u \to u)$ by $1 \in F$ and (F2). □

Theorem 3.12. *If F is an implicative and normal filter in a quasi-ordered residuated system $\mathfrak{A}$, then F is a comparative filter in $\mathfrak{A}$.*

Proof. Let F be an implicative and normal filter of a quasi-ordered residuated system $\mathfrak{A}$. Let us prove that F is a comparative filter in $\mathfrak{A}$. For this purpose, according to Theorem 3.2 in [9], it suffices to prove that (13) holds. Assume $(x \to y) \to x \in F$. Since

$$(x \to y) \to x \preccurlyeq (x \to y) \to ((x \to y) \to y)$$

is valid according to (10), from this inequality and from $(x \to y) \to x \in F$ we get $(x \to y) \to ((x \to y) \to y) \in F$ by (F2). Hence it follows $(x \to y) \to y \in F$ according to Lemma 3.11 because F is an implicative filter in A. So, $(y \to x) \to x \in F$, since F is a normal filter in $\mathfrak{A}$.

On the other hand, by the claim (11) of Proposition 2.8 we have $y \preccurlyeq x \to y$. Thus $(x \to y) \to x \preccurlyeq y \to x$ by (10). From this and from the hypothesis $(x \to y) \to x \in F$, it follows that $y \to x \in F$ in accordance with (F2). Finally, $(y \to x) \to x \in F$ and $y \to x \in F$ implies that $x \in F$ by (F3). We have shown that condition (13) is a valid formula and, therefore, F is a comparative filter in $\mathfrak{A}$. □

The notion of MV-filters in residuated lattices was introduced in [1] as follows: A subset F of a residuated lattice L is called an MV-filter of L if it is a filter of L that satisfies in the condition

(MVF) $(\forall u, v \in L)(((u \to v) \to v) \to ((v \to u) \to u) \in F)$.

Also, in [1] it is shown (Theorem 3.10) that every MV-filter of L is a normal filter of L. It has been shown there that the reverse need not be true (Example 3.11). In our case, the relationships between conditions (MVF) and (NF) are similar.

Theorem 3.13. *Any filter in a quasi-ordered residuated system $\mathfrak{A}$ which satisfies the condition (MVF), is a normal filter in $\mathfrak{A}$.*

Proof. Let F be a filter in $\mathfrak{A}$ and let $x, y \in A$ be such $(x \to y) \to y \in F$. By the hypothesis (MVF) we have $((x \to y) \to y) \to ((y \to x) \to x) \in F$. Since F is a filter in $\mathfrak{A}$, we conclude that $(y \to x) \to x \in F$. So, F is a normal filter in $\mathfrak{A}$ by Theorem 3.5. □

Example 3.14. Consider the quasi-ordered residuated system $\mathfrak{A}$ as in Example 3.8. The filter $F = \{1\}$ in $\mathfrak{A}$ is a normal filter in $\mathfrak{A}$ while it does not satisfy the condition (MVF), since $((c \to a) \to a) \to ((a \to c) \to x) = a \notin F$ holds.

4. Conclusion and further work

The condition (NF), taken from the theory of residual lattices and BL-algebras, is placed here in the context of a specific principle-logical environment. Notwithstanding these specificities, it is shown that the substructure of the normal filtera in a quasi-ordered residuated system, determined by the requirement (NF), have similar properties as that substructure in the mentioned algebraic structures. It is quite reasonable to assume that the requirement (NF) by which it is determined substructure of the normal filter and its properties do not depend much on the environment in which they are observed. It seems that a deeper understanding of requirements (NF) in different principle-logical environments could offer some answer to the aforementioned dilemma.

References

[1] **A. Ahadpanah and L. Torkzadeh**, *Normal filters in reiduated lattices*, Le Matematiche, **70** (2005), 81–92.

[2] **S. Bonzio**, *Algebraic structures from quantum and fuzzy logics.* Ph.D Thesis. Cagliari: Universit'a degli studi di Cagliari, 2015.

[3] **S. Bonzio and I. Chajda**, *Residuated relational systems*, Asian-European J. Math., **11** (2018), 1850024

[4] **R.A. Borzooei and A. Paad**, *Some new types of stabilizers in BL-algebras and their applications*, Indian J. Sci. and Technology, **5** (2012), 1910–1915.

[5] **J.M. Font**, *On special implicative filters*, Math. Log. Q. **45** (1999), 117–126.

[6] **J.M. Font**, *Abstract algebraic logic: An introductory textbook.*, College Publ., London, 2016.

[7] **D.A. Romano**, *Filters in residuated relational system ordered under quasi-order*, Bull. Int. Math. Virtual Inst., **10** (2020), 529–534.

[8] **D.A. Romano**, *Associated filters in quasi-ordered residuated systems*, Contributions to Math., **1** (2020), 22–26.

[9] **D.A. Romano**, *Implicative filters in quasi-ordered residuated system*, Proyecciones J. Math., **40** (2021), 417–424.

[10] **D.A. Romano**, *Comparative filters in quasi-ordered residuated system*, Bull. Int. Math. Virtual Inst., **11** (2021), 177–184.

[11] **D.A. Romano**, *Strong quasi-ordered residuated system*, Open J. Math. Sci., **5** (2021), 73–79.

[12] **H. Rasiowa**, *An algebraic approach to non-classical logics*, North-Holland Publ. Comp., Amsterdam, 1974.

[13] **A.B. Saeid and S. Motamed**, *Normal filters in BL-Algebras*, World Appl. Sci. J., **7** (2009), 70-–76.

[14] **W. Wang, P. Yang and Y. Xu**, *Further complete solutions to four open problems on filter of logical algebras*, Intern. J. Computat. Intell. Systems, **12** (2009), 359–366.

[15] **M. Ward and R.P. Dilworth**, *Residueted lattices*, Trans. Am. Math. Soc., **45** (1939), 335–354.

Received July 19, 2021
Revised November 13, 2021

International Mathematical Virtual Institute
Kordunaška Street 6
78000 Banja Luka
Bosnia and Herzegobina
e-mail: bato49@hotmail.com

Quasigroups and Related Systems **30** (2022), 329 – 338

On the finite loop algebra $F[M(C_p^m \rtimes C_2, 2)]$

Swati Sidana

Abstract. Let $G = C_p^m \rtimes C_2$ be a generalized dihedral group for an odd prime p and a natural number m, $L = M(G, 2)$ be the $RA2$ loop obtained from G and F be a finite field of characteristic 2. For the loop algebra $F[L]$, we determine the Jacobson radical $J(F[L])$ of $F[L]$ and the Wedderburn decomposition of $F[L]/J(F[L])$. The structure of $1 + J(F[L])$ is also determined.

1. Introduction

The problem of determining the structure of the unit loop of the loop ring is of great interest to many authors. Goodaire in [4], Jespers and Leal in [5] determined the unit loops of integral loop rings of RA loops. Ferraz, Goodaire and Milies [3] studied some classes of semisimple loop algebras of RA loops over finite fields. Sidana and Sharma have characterized the structure of the unit loops of the finite loop algebras of many RA and $RA2$ loops in [7, 8, 9]. In [1], Chein and Goodaire studied the loops whose loop rings over the field of characteristic 2 are alternative. In this paper, we study the structure of the unit loop of the loop algebra $F[L]$ of $RA2$ loop $L = M(G, 2)$ obtained from the group

$$G = C_p^m \rtimes C_2 = \langle a_1, a_2, \ldots, a_m, b \mid a_i^p, b^2, a_i a_j a_i^{-1} a_j^{-1}, b a_i b a_i,\ i, j = 1, 2, \ldots, m \rangle,$$

p an odd prime and m a natural number, over the finite field F of characteristic 2 which contains a primitive p^{th} root of unity. The structure of $1 + J(F[L])$ is also determined.

Following is the main theorem of this paper.

Theorem 1.1. *Let p be an odd prime, $m \in \mathbb{N}$, F be a finite field with $|F| = 2^n$ containing a primitive p^{th} root of unity and $L = M(C_p^m \rtimes C_2, 2)$. Then*

$$\mathcal{U}(F[L]/J(F[L])) \cong F^* \times GLL(2, F)^{\frac{p^m - 1}{2}}$$

2010 Mathematics Subject Classification: 20N05, 17D05
Keywords: Loop algebra, $RA2$ loop, Zorn's algebra, unit loop, general linear loop.

and $1 + J(F[L]) \cong C_2^{3n}$, *an elementary abelian* 2*-group of order* 2^{3n}.

Throughout the paper, p is an odd prime, F denotes the finite field of characteristic 2 containing a primitive p^{th} root of unity, $F^* = F\backslash\{0\}$, C_m the cyclic group of order m, $\Phi_n(x)$ the n^{th} cyclotomic polynomial and ξ_p a primitive p^{th} root of unity.

2. Preliminaries

A loop L is said to be a *Moufang Loop* if it satisfies any of the following three equivalent identities:

$$\begin{aligned} ((xy)x)z &= x(y(xz)), && \text{the left Moufang identity,} \\ ((xy)z)y &= x(y(zy)), && \text{the right Moufang identity,} \\ (xy)(zx) &= (x(yz))x, && \text{the middle Moufang identity} \end{aligned}$$

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

Let G be a non-abelian group, $g_0 \in \mathcal{Z}(G)$, the center of G and $g \mapsto g^*$ be an involution of G such that $g_0^* = g_0$ and $gg^* \in \mathcal{Z}(G)$ for every $g \in G$. For an indeterminate u, let $L = G \dot\cup Gu$ and extend the binary operation from G to L by the rules

$$g(hu) = (hg)u, \quad (gu)h = (gh^*)u, \quad (gu)(hu) = g_0h^*g, \quad \text{for all } g, h \in G.$$

The loop L so constructed is a Moufang loop denoted by $M(G, *, g_0)$ and its order is twice the order of the group G. If the involution '$*$' is the inverse map on G and $g_0 = 1$, the identity element of G, then $M(G, -1, 1)$ is denoted as $M(G, 2)$.

A loop whose loop ring in characteristic 2 is alternative but not associative is known as *RA*2 *loop*.

Theorem 2.1. [1, Theorem 5.4] *The loop* $M(G, -1, g_0)$ *is an RA*2 *loop if and only if either* $G = Dih(A)$ *is the generalized dihedral group of some abelian group* A *of exponent* > 2*, or* G *is a non-abelian group of exponent* 4 *having exactly* 2 *squares.*

The Zorn's vector matrix algebra is an 8-dimensional alternative algebra and is a generalization of the matrix algebra over an associative ring. For any commutative and associative ring R (with unity), let R^3 denotes the

set of ordered triples over R. Consider the set of 2×2 matrices of the form $\begin{bmatrix} a & x \\ y & b \end{bmatrix}$, where $a, b \in R$ and $x, y \in R^3$ with the usual addition

$$\begin{bmatrix} a & x \\ y & b \end{bmatrix} + \begin{bmatrix} c & z \\ w & d \end{bmatrix} = \begin{bmatrix} a+c & x+z \\ y+w & b+d \end{bmatrix}$$

and the multiplication defined by

$$\begin{bmatrix} a & x \\ y & b \end{bmatrix} \begin{bmatrix} c & z \\ w & d \end{bmatrix} = \begin{bmatrix} ac + x \cdot w & az + dx - y \times w \\ cy + bw + x \times z & bd + y \cdot z \end{bmatrix},$$

where $\cdot$ and $\times$ denote the dot product and the cross product respectively in R^3. By this construction, we obtain an alternative algebra called as *Zorn's vector matrix algebra* denoted by $\mathfrak{Z}(R)$.

The loop of the invertible elements of the Zorn's vector matrix algebra,

$$GLL(2, R) = \{A \in \mathfrak{Z}(R) \mid \det A \text{ is a unit in } R\}$$

is a Moufang loop called the *General Linear Loop*. This loop is a generalization of the General Linear group for associative algebras.

For any abelian group A, the *generalized dihedral group* of A is the semidirect product of A and C_2, with C_2 acting on A by inverting the elements and is written as $Dih(A) = A \rtimes C_2$.

If G is a non-abelian group with a faithful two dimensional matrix representation, then we can find a matrix representation of Moufang loop $M(G, 2)$ with the help of the following remark.

Remark 2.2. [10, §2.3] Let G be a non-abelian group with a faithful, two-dimensional representation over a commutative ring R with identity. That is, there exists an embedding $\phi : G \to GL(2, R)$. If we choose two orthogonal unit vectors v, w in R^3 such that $||v \times w|| = 1$ and consider the map $\psi : GL(2, R) \to \mathfrak{Z}(R)$ defined as $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & bv \\ cv & d \end{bmatrix}$. Then $\psi\phi : G \to \mathfrak{Z}(R)$ and $u \mapsto \begin{bmatrix} 0 & w \\ w & 0 \end{bmatrix}$ give the matrix representation of L.

The following lemma will be used repeatedly in this article.

Lemma 2.3. *Let p be an odd prime and ξ_p be a primitive p^{th} root of unity. If $\xi_p, \xi_p^2, \ldots, \xi_p^{p-1}$ are the roots of a polynomial $f(x) = a_{p-1}x^{p-1} + a_{p-2}x^{p-2} + \ldots + a_1x + a_0$ over F, then the coefficients of $f(x)$ are all the same, that is, $a_{p-1} = a_{p-2} = \ldots = a_1 = a_0 = a(say)$.*

Proof. Since the factor $1+x+x^2+\ldots+x^{p-1}$ of p^{th} cyclotomic polynomial $\Phi_p(x)$ divides $f(x)$, therefore all the coefficients of the polynomial $f(x)$ must be the same. □

An element $a \in R$ is said to be *quasiregular* if there exists $b \in R$ such that $a+b=ab=ba$ and b is called the *quasi-inverse* of a. An ideal is said to be *quasiregular ideal* if all its elements are quasiregular elements. The *Jacobson radical* $J(R)$ of an alternative ring R is the largest quasiregular ideal of R. If the ring R has unity, this ideal is also the intersection of all the maximal left ideals of R. Let θ be an onto ring homomorphism from a ring R_1 to a ring R_2. Then $\theta(J(R_1)) \subseteq J(R_2)$.

3. Irreducible matrix representations of $C_p^m \rtimes C_2$

In this section, we determine the irreducible and inequivalent representations of the group $C_p^m \rtimes C_2$ over F induced from the irreducible representations of its subgroup C_p^m over F. In [6, §3], the irreducible and inequivalent representations of $C_p^2 \rtimes C_2$ over F have been discussed. Here we extend this to $C_p^m \rtimes C_2$. Since $H = C_p^m$ is an abelian group, therefore, all the irreducible representations of H are of degree 1.

For $1 \leqslant k \leqslant m$, $0 \leqslant i_k \leqslant p-1$, let

$$\rho_{(i_1,i_2,\ldots,i_m)} : H \to F$$

be defined by

$$a_k \mapsto \xi_p^{i_k}.$$

Using [2, Ch 1, §10], we get the induced representations of G as

$$\theta_{(i_1,i_2,\ldots,i_m)} : G \to M(2,F)$$

defined by

$$a_k \mapsto \begin{bmatrix} \xi_p^{i_k} & 0 \\ 0 & \xi_p^{-i_k} \end{bmatrix}, \quad b \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ for all } 0 \leqslant i_k \leqslant p-1, 1 \leqslant k \leqslant m.$$

All these representations of G need not be irreducible and inequivalent.

For each $(i_1, i_2, \ldots, i_m) \in \{0, 1, \ldots, p-1\}$, the representation $\theta_{(i_1,i_2,\ldots,i_m)}$ is similar to the representation $\theta_{(-i_1,-i_2,\ldots,-i_m)}$. Also it is clear that the representation $\theta_{(0,0,\ldots,0)}$ is not irreducible. Thus, for each $1 \leqslant k \leqslant m$, if we

define

$$\mathcal{J}_k^m = \left\{ (i_1, i_2, \ldots, i_m) \;\middle|\; \begin{array}{ll} 1 \leqslant i_j \leqslant \frac{p-1}{2}, & \text{if } j = k \\ 0 \leqslant i_j \leqslant p-1, & \text{if } j < k \\ i_j = 0, & \text{if } j > k \end{array} \right\}$$

and

$$S^m = \big\{ (i_1, i_2, \ldots, i_m) \mid (i_1, i_2, \ldots, i_m) \in \mathcal{J}_k^m, \;\; 1 \leqslant k \leqslant m \big\},$$

then the representations $\theta_{(i_1,i_2,\ldots,i_m)}$ for all $(i_1, i_2, \ldots, i_m) \in S^m$ are irreducible and inequivalent over F.

Hence the total number of 2-degree irreducible and inequivalent representations of G are

$$\frac{p-1}{2} + p.\frac{p-1}{2} + p^2.\frac{p-1}{2} + \ldots + p^{m-1}.\frac{p-1}{2} = \frac{p^m - 1}{2}.$$

4. The unit loop $\mathcal{U}(F[L]/J(F[L]))$ for $L = M(C_p^m \rtimes C_2, 2)$

In this section, we determine the Wedderburn decomposition of $F[L]/J(F[L])$ for $L = M(C_p^m \rtimes C_2, 2)$ and prove the main theorem. Consider the following loop homomorphisms:

1. $\phi_0 : L \to F^*$ defined by

$$a_j \mapsto 1, \;\; \forall\; j = 1, 2, \ldots, m, \qquad b \mapsto 1, \qquad u \mapsto 1.$$

2. For each $(i_1, i_2, \ldots, i_m) \in S^m$, define

$$\phi_{(i_1,i_2,\ldots,i_m)} : L \to GLL(2, F)$$

by

$$a_j \mapsto \begin{bmatrix} \xi_p^{i_j} & (0,0,0) \\ (0,0,0) & \xi_p^{-i_j} \end{bmatrix} \text{ for all } j = 1, 2, \ldots, m,$$

$$b \mapsto \begin{bmatrix} 0 & (0,1,0) \\ (0,1,0) & 0 \end{bmatrix}, \qquad u \mapsto \begin{bmatrix} 0 & (0,0,1) \\ (0,0,1) & 0 \end{bmatrix}.$$

Then

$$T_m : L \to F^* \times (GLL(2,F))^{\frac{p^m-1}{2}}$$

defined as

$$T_m := \phi_0 \ \times \prod_{(i_1,i_2,\ldots,i_m)\in S^m} \phi_{(i_1,i_2,\ldots,i_m)}$$

is a well defined loop homomorphism.

Let $\phi^*_{(i_1,i_2,\ldots,i_m)} : F[L] \to \mathfrak{Z}(F)$ be the loop algebra homomorphism obtained by extending $\phi_{(i_1,i_2,\ldots,i_m)}$ linearly over F and

$$T^*_m : F[L] \to F \bigoplus (\mathfrak{Z}(F))^{\frac{p^m-1}{2}}$$

be defined as

$$T^*_m := \phi^*_0 \bigoplus \ \underset{(i_1,i_2,\ldots,i_m)\in S^m}{\oplus} \phi^*_{(i_1,i_2,\ldots,i_m)}.$$

Now we shall calculate the kernel of T^*_m.

Let

$$\begin{aligned} X_m = & \sum_{i_1=0}^{p-1}\sum_{i_2=0}^{p-1}\cdots\sum_{i_m=0}^{p-1} \alpha_{i_1,i_2,\ldots,i_m} a_1^{i_1}a_2^{i_2}\ldots a_m^{i_m} \\ & + \sum_{i_1=0}^{p-1}\sum_{i_2=0}^{p-1}\cdots\sum_{i_m=0}^{p-1} \beta_{i_1,i_2,\ldots,i_m} a_1^{i_1}a_2^{i_2}\ldots a_m^{i_m} b \\ & + \sum_{i_1=0}^{p-1}\sum_{i_2=0}^{p-1}\cdots\sum_{i_m=0}^{p-1} \gamma_{i_1,i_2,\ldots,i_m} a_1^{i_1}a_2^{i_2}\ldots a_m^{i_m} u \\ & + \sum_{i_1=0}^{p-1}\sum_{i_2=0}^{p-1}\cdots\sum_{i_m=0}^{p-1} \delta_{i_1,i_2,\ldots,i_m} a_1^{i_1}a_2^{i_2}\ldots a_m^{i_m} bu \\ = & \ X_{m1} + X_{m2} + X_{m3} + X_{m4} \in Ker\ T^*_m. \end{aligned}$$

For $(i_1, i_2, \ldots, i_m) \in \mathcal{J}^m_k$, on applying $\phi^*_{(i_1,i_2,\ldots,i_m)}$ on X_m, we get

$$\phi^*_{(i_1,i_2,\ldots,i_m)}(X_{m1}) = \begin{bmatrix} Y_{11} & (0,0,0) \\ (0,0,0) & Y_{12} \end{bmatrix},$$

$$\phi^*_{(i_1,i_2,\ldots,i_m)}(X_{m2}) = \begin{bmatrix} 0 & (0,Y_{21},0) \\ (0,Y_{22},0) & 0 \end{bmatrix},$$

$$\phi^*_{(i_1,i_2,\ldots,i_m)}(X_{m3}) = \begin{bmatrix} 0 & (0,0,Y_{31}) \\ (0,0,Y_{32}) & 0 \end{bmatrix},$$

$$\phi^*_{(i_1,i_2,\ldots,i_m)}(X_{m4}) = \begin{bmatrix} 0 & (Y_{41},0,0) \\ (Y_{42},0,0) & 0 \end{bmatrix}$$

for some $Y_{11}, Y_{12}, Y_{21}, Y_{22}, Y_{31}, Y_{32}, Y_{41}$ and $Y_{42} \in F$.

That is,

$$\phi^*_{(i_1,i_2,\ldots,i_m)}(X_m) = \begin{bmatrix} Y_{11} & (Y_{41},Y_{21},Y_{31}) \\ (Y_{42},Y_{22},Y_{32}) & Y_{12} \end{bmatrix}.$$

Thus $\phi^*_{(i_1,i_2,\ldots,i_m)}(X_m) = 0$ gives that $Y_{11} = Y_{12} = Y_{21} = Y_{22} = Y_{31} = Y_{32} = Y_{41} = Y_{42} = 0$. This means that for all $(i_1, i_2, \ldots, i_m) \in \mathcal{J}_k^m$,

$\phi^*_{(i_1,i_2,\ldots,i_m)}(X_m) = 0$ implies that $\phi^*_{(i_1,i_2,\ldots,i_m)}(X_{mj}) = 0$ for all $j = 1, 2, 3, 4$.

Firstly, consider $\phi^*_{(i_1,i_2,\ldots,i_m)}(X_{m1}) = 0$. For a fixed $(i_1, i_2, \ldots, i_m) \in \mathcal{J}_k^m$, define

$$\mathcal{A}_k^m = \left\{ (j_1, j_2, \ldots, j_m) \;\middle|\; \begin{array}{ll} j_l \in \{i_l, 0\}, & \text{if } 1 \leqslant l < k \\ j_k = i_k, & \\ i_j = 0, & \text{if } l > k \end{array} \right\}.$$

Let us start with $k = m$, for $(j_1, j_2, \ldots, j_m) \in \mathcal{A}_m^m$, $\phi^*_{(j_1,j_2,\ldots,j_m)}(X_{m1}) = 0$ and using Lemma 2.3, we get that

$$\alpha_{i_1,i_2,\ldots,i_{m-1},i_m} = \alpha_{i_1,i_2,\ldots,i_{m-1}}(say) \text{ for all } i_1, \ldots, i_m = 0, 1, \ldots, m.$$

Then $\phi^*_{(j_1,j_2,\ldots,j_m)}(X_{m1}) = 0$ for $(j_1, j_2, \ldots, j_m) \in \mathcal{A}_{m-1}^m$ gives

$$\alpha_{i_1,i_2,\ldots,i_{m-2},i_{m-1}} = \alpha_{i_1,i_2,\ldots,i_{m-2}}(say) \text{ for all } i_1, \ldots, i_{m-1} = 0, 1, \ldots, m.$$

Continuing the same process, $\phi^*_{(j_1,j_2,\ldots,j_m)}(X_{m1}) = 0$ for $(j_1, \ldots, j_m) \in \mathcal{A}_2^m$, implies that $\alpha_{i_1,i_2} = \alpha_{i_1}(\text{say})$ for all $i_1, i_2 = 0, 1, \ldots, m$.

Finally, $\phi^*_{(j_1,j_2,\ldots,j_m)}(X_{m1}) = 0$ for $(j_1, j_2, \ldots, j_m) \in \mathcal{A}_1^m$ gives that $\alpha_{i_1} = \alpha(\text{say})$ for all $i_1 = 0, 1, \ldots, m$. Hence $\alpha_{i_1,i_2,\ldots,i_m} = \alpha$ for all $i_1, i_2, \ldots, i_m = 0, 1, \ldots, m$. By repeating the same procedure for $\phi^*_{(j_1,j_2,\ldots,j_m)}(X_{m2}) = 0$, $\phi^*_{(j_1,j_2,\ldots,j_m)}(X_{m3}) = 0$ and for $\phi^*_{(j_1,j_2,\ldots,j_m)}(X_{m4}) = 0$, we get $\beta_{i_1,i_2,\ldots,i_m} = \beta$, $\gamma_{i_1,i_2,\ldots,i_m} = \gamma$ and $\delta_{i_1,i_2,\ldots,i_m} = \delta$ for all $i_1, i_2, \ldots, i_m = 0, 1, \ldots, m$.

Next, $\phi_0^*(X_m) = 0$ implies that $\alpha + \beta + \gamma + \delta = 0$. Thus

$$\begin{aligned} X_m &= \beta \left(\sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \dots \sum_{i_m=0}^{p-1} a_1^{i_1} a_2^{i_2} \dots a_m^{i_m} \; + \; \sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \dots \sum_{i_m=0}^{p-1} a_1^{i_1} a_2^{i_2} \dots a_m^{i_m} b \right) \\ &+ \gamma \left(\sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \dots \sum_{i_m=0}^{p-1} a_1^{i_1} a_2^{i_2} \dots a_m^{i_m} \; + \; \sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \dots \sum_{i_m=0}^{p-1} a_1^{i_1} a_2^{i_2} \dots a_m^{i_m} u \right) \\ &+ \delta \left(\sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \dots \sum_{i_m=0}^{p-1} a_1^{i_1} a_2^{i_2} \dots a_m^{i_m} \; + \; \sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \dots \sum_{i_m=0}^{p-1} a_1^{i_1} a_2^{i_2} \dots a_m^{i_m} bu \right) \\ &= \beta f_{m1} + \gamma f_{m2} + \delta f_{m3}. \end{aligned}$$

We have few observations to note, which will be used here:

In the group $G = C_p^m \rtimes C_2$, $(a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})^2 = p(a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})$ and $(a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})b = b(a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})$, since $a_i^k b = b a_i^{-k}$ (a presenting relator of G).

Further, the definition of the loop gives $ug = g^{-1}u$, which implies $(a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})u = u(a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})$.

Also we can write
$\sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \dots \sum_{i_m=0}^{p-1} a_1^{i_1} a_2^{i_2} \dots a_m^{i_m} = \prod_{i=1}^{m} (a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})$.

Consequently, we have $f_{m1} = \prod_{i=1}^{m} (a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1}) + \prod_{i=1}^{m} (a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})b$. This gives
$f_{m1}^2 = 2 \prod_{i=1}^{m} (a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1}) \; + \; 2 \prod_{i=1}^{m} (a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})b = 0$, since the characteristic of F is 2. Similarly, we can prove $f_{m2}^2 = 0$, and $f_{m3}^2 = 0$.

Also for $1 \leqslant r, s \leqslant 3$, f_{mr} and f_{ms} commute, as

$$\begin{aligned} f_{mr} f_{ms} &= \prod_{i=1}^{m} (a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1}) + \prod_{i=1}^{m} (a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})b \\ &+ \prod_{i=1}^{m} (a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})u + \prod_{i=1}^{m} (a_i^0 + a_i^1 + a_i^2 + \ldots + a_i^{p-1})bu \\ &= \sum_{l \in L} l. \end{aligned}$$

It follows that every element of $ker\ T_m^*$ is a nilpotent element of nilpotency

index 2 and hence is quasiregular with quasi-inverse as itself. Thus $ker\ T_m^*$ is a quasiregular ideal of $F[L]$, which implies that $ker\ T_m^* \subseteq J(F[L])$.

Since

$$dim_F\ (F \oplus \mathfrak{Z}(F)^{\frac{p^m-1}{2}}) = 4p^m - 3 = dim_F\ (F[L]/\ker\ T_m^*)$$

therefore, T_m^* is onto. This implies $J(F[L]) \subseteq ker\ T_m^*$. Consequently, $ker\ T_m^* = J(F[L])$. Hence

$$F[L]/J(F[L]) \cong F \oplus \mathfrak{Z}(F)^{\frac{p^m-1}{2}}$$

which further gives

$$\mathcal{U}(F[L]/J(F[L])) \cong F^* \times GLL(2,F)^{\frac{p^m-1}{2}}.$$

Consider $1 + J(F[L])$. An element h of $1 + J(F[L])$ is of the form $h = 1 + c_1 f_{m1} + c_2 f_{m2} + c_3 f_{m3}$, where $c_i' s \in F$. As f_{mr} and f_{ms} commute for all $1 \leqslant r, s \leqslant 3$, we get that $1 + J(F[L])$ is a commutative loop.

Further, for all $r, s, t = 1, 2, 3$,

$$(f_{mr} f_{ms}) f_{mt} = 2\sum_{l \in L} l = 0 \quad \text{and } f_{mr}(f_{ms} f_{mt}) = 2\sum_{l \in L} l = 0.$$

Thus $1 + J(F[L])$ is an abelian group and $h^2 = 1$ for all $h \in 1 + J(F[L])$, which gives $1 + J(F[L]) \cong (C_2 \times C_2 \times C_2)^n$.

Acknowledgments. The author is thankful to the anonymous referees and Professor Petr Vojtěchovský for their useful comments and suggestions, which have greatly improved the presentation of the paper.

References

[1] **O. Chein and E. G. Goodaire**, *Loops whose loop rings in characteristic* 2 *are alternative*, Comm. Algebra, **18** (1990), no. 3, 659 – 688.

[2] **Ch.W. Curtis and I. Reiner**, *Methods of representation theory. Vol. I*, John Wiley & Sons, Inc., New York (1990).

[3] **R.A. Ferraz, E.G. Goodaire and C.P. Milies**, *Some classes of semisimple group* (*and loop*) *algebras over finite fields*, J. Algebra, **324** (2010), no. 12, 3457 – 3469.

[4] **E.G. Goodaire**, *Six Moufang loops of units*, Canad. J. Math., **44** (1992), no. 5, 951 – 973.

[5] **E. Jespers and G. Leal**, *A characterization of the unit loop of the integral loop ring* $\mathbf{Z}M_{16}(Q, 2)$, J. Algebra, **155** (1993), no. 1, 95 – 109.

[6] **S. Sidana**, *On units in loop algebra* $F[M(Dih(C_p^2), 2)]$, Beitr. Algebra Geom., **58** (2017), no. 4, 765 – 774.

[7] **S. Sidana and R.K. Sharma**, *Finite semisimple loop algebras of indecomposable RA loops*, Canad. Math. Bull., **58** (2015), no. 2, 363 – 373.

[8] **S. Sidana and R.K. Sharma**, *On the finite loop algebra of the smallest Moufang loop* $M(S_3, 2)$, Armenian J. Math., **8** (2016), no. 1, 68 – 76.

[9] **S. Sidana and R.K. Sharma**, *Units in finite loop algebras of RA*2 *loops*, Asian-Eur. J. Math., **9** (2016), no. 1, 1650026.

[10] **A.T. Wells**, *Zorn vector matrices over commutative rings and the loops arising from their construction*, Thesis (Ph.D.)–Iowa State University (2010).

Received November 22, 2021
Revised July 20, 2022

Post Graduate Department of Mathematics
Mehr Chand Mahajan DAV College for Women
Sector 36-A
Chandigarh
India 160036
E-mail: swatisidana@gmail.com