Quasigroups and Related Systems **29** (2021), 157 − 170

Annihilator graph of a commutative semigroup whose zero-divisor graph is a refinement of a star graph

Mojgan Afkhami, Kazem Khashyarmanesh

and Seyed Mohammad Sakhdari

Abstract. Suppose that G is a refinement of a star graph with center c and G^* is the subgraph of G induced on the vertices $V(G) \setminus \{x \in V(G) \mid x = c$ or x is an end vertex adjacent to $c\}$. Let S be a commutative semigroup with zero and $\Gamma(S)$ be the zero-divisor graph of S. In this paper, we determine the structure of the annihilator graph of S by using the zero-divisor graph $\Gamma(S)$, which is a refinement of a star graph with center c, and $\Gamma(S)^*$ has at least two components or $\Gamma(S)^*$ is isomorphic to a cycle graph or a path.

1. Introduction

Throughout the paper S is a commutative semigroup with zero whose operation is written multiplicatively. The set of all zero-divisors of S is denoted by $Z(S)$ and $Z(S)^* = Z(S) \setminus \{0\}$.

There are many papers which interlink graph theory and ring theory. Several classes of graphs associated with algebraic structures have been actively investigated (see for example, [2, 3, 4, 5, 6, 7, 8, 11, 12, 18, 19]).

For any commutative semigroup S with zero element 0, there is a simple undirected graph, which is called the zero-divisor graph and is denoted by $\Gamma(S)$ (cf. [17]). The vertex set of $\Gamma(S)$ is $Z(S)^*$ and x is adjacent to y in $\Gamma(S)$ if and only if $xy = 0$, for each two distinct elements x and y in $Z(S)^*$. It was proved that $\Gamma(S)$ is connected and the diameter of $\Gamma(S)$ is less than or equal to three. Also if $\Gamma(S)$ contains a cycle, then its girth is less than or equal to four. For more details on zero-divisor graphs see [9], [13], [15], [16], [17], [21].

In [10], A. Badawi introduced the concept of the annihilator graph for a commutative ring R, denoted by $AG(R)$, with vertices $Z(R)^*$ and $x \sim y$ is an edge in $AG(R)$ if and only if $\mathrm{ann_R}(xy) \neq \mathrm{ann_R}(x) \cup \mathrm{ann_R}(y)$, where $\mathrm{ann_R}(x) = \{r \in R \mid xr = 0\}$.

In [1], the present authors introduced the annihilator graph for a commutative semigroup S, which is denoted by $AG(S)$. The graph $AG(S)$ is an undirected

2010 Mathematics Subject Classification: 05C99, 20M14
Keywords: Zero-divisor graph, annihilator graph, isolated vertex, star graph.

graph with vertex set $Z(S)^*$ and two distinct vertices x and y are adjacent if and only if $\mathrm{ann_S}(xy) \neq \mathrm{ann_S}(x) \cup \mathrm{ann_S}(y)$, where $\mathrm{ann_S}(x) = \{s \in S \mid xs = 0\}$. Some basic properties of $AG(S)$ are investigated in [1]. For example, it was proved that if $Z(S) \neq S$, then $\Gamma(S)$ is a subgraph of $AG(S)$, and so $AG(S)$ is connected. Also if $Z(S) = S$ and there exists $x \in S^* = S \setminus \{0\}$ such that $\mathrm{ann_S}(x) \supseteq Z(S) \setminus \{x\}$, then x is an isolated vertex in $AG(S)$.

Recall that a graph G with $n+1$ vertices is called a star graph, and is denoted by $K_{1,n}$, if there exists a vertex $x \in V(G)$ such that $\mathrm{d}(x) = n$, and for each vertex $y \in V(G) \setminus \{x\}$, we have $\mathrm{d}(y) = 1$. The vertex x is called the center of $K_{1,n}$. Suppose that G and H are two graphs. H is called a *refinement* of G if $V(G) = V(H)$ and each edge in G is an edge in H. The subgraph induced on vertices $V(G) \setminus \{x \in V(G) \mid x = c \text{ or } x \text{ is an end vertex adjacent to } c\}$ is denoted by G^*.

In this paper, we study the annihilator graph associated to a commutative semigroup with zero by using the zero-divisor graph $\Gamma(S)$, where $\Gamma(S)$ is a refinement of a star graph with center c, and $\Gamma(S)^*$ has at least two components or $\Gamma(S)^*$ is isomorphic to a cycle graph or a path.

2. Preliminaries

Now we recall some definitions and notations of graphs. We use the standard terminology of graphs is contained in [14]. Let G be a graph with vertex set $V(G)$ and edge set $E(G)$. We use the notation $x \sim y$ to denote that x is adjacent to y in G and edge between x and y will denote by $\{xy\}$. Also the *distance* between two distinct vertices a and b, denoted by $\mathrm{d}(a,b)$, is the length of the shortest path connecting a and b, if such a path exists; otherwise, we use $\mathrm{d}(a,b) := \infty$. The *diameter* of a graph G is $\mathrm{diam}(G) = \sup\{\mathrm{d}(a,b) : a \text{ and } b \text{ are distinct vertices of } G\}$. The *girth* of G, denoted by $\mathrm{gr}(G)$, is the length of the shortest cycle in G, if such a cycle exists; otherwise, we use $\mathrm{gr}(G) := \infty$. A graph G is said to be *connected* if there exists a path between any two distinct vertices, and it is *complete* if it is connected with diameter one. We use K_n to denote a complete graph with n vertices. Also, we say that G is *totally disconnected* if no two vertices of G are adjacent. We use nK_1 to denote the totally disconnected graph with n vertices. For a vertex x of a graph G, the *neighborhood* of x, denoted by $\mathrm{N}(x)$, is the set of vertices which are adjacent to x, moreover the *degree* of x, denoted by $\mathrm{d}(x)$, is the cardinality of $\mathrm{N}(x)$. Also, a vertex u is an end vertex, if there is only one edge incident to u, and it is an *isolated* vertex if $\mathrm{d}(u) = 0$. Let G and H be two graphs. We use the notation $H \leqslant G$ (resp, $H \cong G$) to denote that H is a subgraph of G (resp, H is isomorphic to G). Also we use $G \setminus \{\{x_1y_1\}, \{x_2y_2\}, \{x_3y_3\}, ..., \{x_ny_n\}\}$ to denote a graph G, such that the edges $\{x_1y_1\}, \{x_2y_2\}, \{x_3y_3\}, ..., \{x_ny_n\}$ are deleted.

As usual P_n and C_n will denote the path of length n and the cycle of length n, respectively. Suppose that G is a graph with m components such that each component of G is isomorphic to K_n. Then we will denote G by mK_n. Let H and G be two graphs such that $V(G) \cap V(H) = \emptyset$ and $E(G) \cap E(H) = \emptyset$. Then the union of the graphs H and G, which is denoted by $H \cup G$, is a graph with vertex set $V(G) \cup V(H)$ and edge set $E(H) \cup E(G)$.

Throughout the paper, we assume that $|Z(S)^*| \geqslant 3$. The case that $|Z(S)^*| \leqslant 2$ is easy. Indeed, if $|Z(S)^*| = 1$, then $AG(S) \cong \Gamma(S) \cong K_1$. Let $|Z(S)^*| = 2$. Then $\Gamma(S) \cong K_2$. Now if $Z(S) = S$, then clearly $AG(S) \cong 2K_1$, and if $Z(S) \neq S$, then $AG(S) \cong \Gamma(S) \cong K_2$. Moreover, in [1, Section 4], the case that $|Z(S)^*| = 3$ and in [20] the case that $|Z(S)^*| = 4$, have been discussed.

3. Properties of $AG(S)$

In this section, we determine the structure of the annihilator graph of a commutative semigroup S whose $\Gamma(S)$ is a refinement of a star graph with center c and $\Gamma(S)^*$ satisfies one of the properties: (1) $\Gamma(S)^*$ has at least two components, (2) $\Gamma(S)^*$ is a cycle graph, (3) $\Gamma(S)^*$ is a path. Also since $\Gamma(S)$ is a refinement of a star graph with center c, if $c^2 = 0$, then $\mathrm{ann_S}(c) = Z(S)$. Moreover, in this section, we show that if $Z(S) = S$, then 5 is sharp for the girth of $AG(S)$, while if $Z(S) \neq S$, then $\mathrm{gr}(AG(S)) \leqslant 4$.

Proposition 3.1. [22, Corollary 2.4] *Suppose that $\Gamma(S)$ is a refinement of a star graph with center c, and $\Gamma(S)^*$ has at least two components. Then $S^2 = \{0, c\}$, where $S^2 = \{xy | x, y \in S\}$.*

By Proposition 3.1, it is clear that if $\Gamma(S)$ is a refinement of a star graph and $\Gamma(S)^*$ has at least two components, then if there exists a vertex z which is not adjacent to some vertices x and y in $\Gamma(S)$, then x and y are adjacent in $AG(S)$. Also, note that if $\Gamma(S)$ is a refinement of a star graph with center c and $S^2 = \{0, c\}$, then $\mathrm{ann_S}(xy) = Z(S)$, for all $x, y \in Z(S)$. Now, the proof of the next theorem follows from [1, Theorems 3.1 and 3.8].

Theorem 3.2. *Suppose that $\Gamma(S)$ is a refinement of a star graph with center c. Also assume that $\Gamma(S)^*$ has at least three components and $|V(\Gamma(S))| = n+1$. Then the following statements hold.*

1. *If x and y are two distinct non adjacent vertices in $\Gamma(S)$, then $x \sim y$ in $AG(S)$.*
2. *If $Z(S) \neq S$, then $AG(S) \cong K_{n+1}$.*
3. *$Z(S) = S$, then $AG(S) \cong K_n \cup K_1$, where c is an isolated vertex in $AG(S)$.*

A graph G is called a *friendship graph* (or a *fan graph*) if G is a refinement of a star graph with center c such that $G \setminus \{c\} \cong nK_2$ and it is denoted by F_n. Clearly $|V(F_n)| = 2n + 1$.

Corollary 3.3. *Suppose that $\Gamma(S) \cong F_n$ with center c and $n \geqslant 3$. Then the following statements hold.*

1. *If $Z(S) \neq S$, then $AG(S) \cong K_{2n+1}$.*
2. *If $Z(S) = S$, then $AG(S) \cong K_{2n} \cup K_1$, where c is an isolated vertex in $AG(S)$.*

Proof. Since $\Gamma(S) \cong F_n$ with center c and $n \geqslant 3$, we have $\Gamma(S)^* \cong nK_2$, and so $\Gamma(S)^*$ has at least three components. Therefore, by Theorem 3.2, the results hold. □

Lemma 3.4. *Suppose that $\Gamma(S)$ is a refinement of a star graph with center c such that $\Gamma(S)^*$ has exactly two components A and B. Then the following statements hold.*

1. *If $x, y \in A$, then $x \sim y$ in $AG(S)$. Similarly, if $x, y \in B$, then $x \sim y$ in $AG(S)$.*
2. *Suppose that x, $y \in Z(S)^* \setminus \{c\}$. Then $x \nsim y$ in $AG(S)$ if and only if there exists no end vertex adjacent to c in $\Gamma(S)$ and $x \in A$, $\mathrm{ann}_{\mathrm{S}}(x) = A \cup \{0, c\}$ and $y \in B$, $\mathrm{ann}_{\mathrm{S}}(y) = B \cup \{0, c\}$.*

Proof. (1). It follows by Proposition 3.1.

(2). First suppose that $x, y \in Z(S)^* \setminus \{c\}$ and $x \nsim y$ in $AG(S)$. Then, by (i), $x \in A$, $y \in B$, and so $xy \neq 0$ and, by Proposition 3.1, we have $xy = c$ which follows that $c^2 = (xy)c = x(yc) = 0$, and hence $\mathrm{ann}_{\mathrm{S}}(c) = Z(S)$. Since $x \nsim y$ in $AG(S)$, we see that $\mathrm{ann}_{\mathrm{S}}(x) \cup \mathrm{ann}_{\mathrm{S}}(y) = \mathrm{ann}_{\mathrm{S}}(xy) = \mathrm{ann}_{\mathrm{S}}(c) = Z(S)$. If there exists u such that u is an end vertex adjacent to c in $\Gamma(S)$, then $u \notin \mathrm{ann}_{\mathrm{S}}(x) \cup \mathrm{ann}_{\mathrm{S}}(y) = Z(S)$, which is impossible. Thus there exists no end vertex adjacent to c in $\Gamma(S)$. Now if $x^2 \neq 0$ or $y^2 \neq 0$, then $x \notin \mathrm{ann}_{\mathrm{S}}(x) \cup \mathrm{ann}_{\mathrm{S}}(y) = Z(S)$, or $y \notin \mathrm{ann}_{\mathrm{S}}(x) \cup \mathrm{ann}_{\mathrm{S}}(y) = Z(S)$, which is impossible. Therefore $x^2 = y^2 = 0$. Finally, if there exists $a \in A$ such that $x \nsim a$ in $\Gamma(S)$, then $a \notin \mathrm{ann}_{\mathrm{S}}(x) \cup \mathrm{ann}_{\mathrm{S}}(y) = \mathrm{ann}_{\mathrm{S}}(xy) = \mathrm{ann}_{\mathrm{S}}(c) = Z(S)$, which is impossible. Hence for each $a \in A$, we have $x \sim a$ in $\Gamma(S)$, and so $\mathrm{ann}_{\mathrm{S}}(x) = A \cup \{0, c\}$. Similarly, $\mathrm{ann}_{\mathrm{S}}(y) = B \cup \{0, c\}$.

Conversely, since $x \in A$ and $y \in B$, which implies that $xy \neq 0$ and, by Proposition 3.1, we have $xy = c$. So $\mathrm{ann}_{\mathrm{S}}(xy) = \mathrm{ann}_{\mathrm{S}}(c) = Z(S)$. Since there exists no end vertex adjacent to c in $\Gamma(S)$ and $\mathrm{ann}_{\mathrm{S}}(x) = A \cup \{0, c\}$ and $\mathrm{ann}_{\mathrm{S}}(y) = B \cup \{0, c\}$, we have $\mathrm{ann}_{\mathrm{S}}(x) \cup \mathrm{ann}_{\mathrm{S}}(y) = A \cup B \cup \{0, c\} = Z(S) = \mathrm{ann}_{\mathrm{S}}(xy)$. Therefore $x \nsim y$ in $AG(S)$. □

The next theorem follows from Lemma 3.4.

Theorem 3.5. *Suppose that $\Gamma(S)$ is a refinement of a star graph with center c such that there exists no end vertex adjacent to c in $\Gamma(S)$ and $|V(\Gamma(S)^*| = n$. Also assume that $\Gamma(S)^*$ has exactly two components A and B. Then the following statements hold.*

1. *If $Z(S) \neq S$, then $AG(S) \cong K_{n+1} \setminus \{\{xy\} \mid x \in A,\ y \in B$ and $\mathrm{ann}_{\mathrm{S}}(x) = A \cup \{0, c\}$ and $\mathrm{ann}_{\mathrm{S}}(y) = B \cup \{0, c\}\}$.*

2. *If* $Z(S) = S$, *then* $AG(S) \cong K_1 \cup K_n \setminus \{\{xy\} |\ x \in A,\ y \in B$ *and* $\mathrm{ann}_S(x) = A \cup \{0, c\}$ *and* $\mathrm{ann}_S(y) = B \cup \{0, c\}\}$, *where* c *is an isolated vertex in* $AG(S)$.

The next two corollaries immediately follows from Theorem 3.5 and [1, Theorems 3.1 and 3.8].

Corollary 3.6. *Suppose that* $\Gamma(S) \cong F_2$ *with center* c. *Also assume that* $Z(S) \neq S$ *and* $V(\Gamma(S)^*) = \{x, y, z, w\}$ *with* $x \sim y$ *and* $w \sim z$. *Then the following statements hold.*

1. $AG(S) \cong F_2$ *if and only if* $x^2 = y^2 = z^2 = w^2 = 0$.
2. $AG(S) \cong K_5 \setminus \{\{wy\}, \{wx\}\}$ *if and only if* $z^2 = c$ *and* $y^2 = w^2 = x^2 = 0$.
3. $AG(S) \cong K_5 \setminus \{\{yz\}\}$ *if and only if* $x^2 = w^2 = c$ *and* $y^2 = z^2 = 0$.
4. $AG(S) \cong K_5$ *if and only if* $x^2 = y^2 = c$ *or* $w^2 = z^2 = c$.

Corollary 3.7. *Suppose that* $\Gamma(S) \cong F_2$ *with center* c. *Also assume that* $Z(S) = S$ *and* $V(\Gamma(S)^*) = \{x, y, z, w\}$ *with* $x \sim y$ *and* $w \sim z$. *Then the following statements hold.*

1. $AG(S) \cong K_1 \cup 2K_2$, *where* c *is an isolated vertex in* $AG(S)$, *if and only if* $x^2 = y^2 = z^2 = w^2 = 0$.
2. $AG(S) \cong K_1 \cup K_4 \setminus \{\{wy\}, \{wx\}\}$, *where* c *is an isolated vertex in* $AG(S)$, *if and only if* $z^2 = c$ *and* $y^2 = w^2 = x^2 = 0$.
3. $AG(S) \cong K_1 \cup K_4 \setminus \{\{yz\}\}$, *where* c *is an isolated vertex in* $AG(S)$, *if and only if* $x^2 = w^2 = c$ *and* $y^2 = z^2 = 0$.
4. $AG(S) \cong K_1 \cup K_4$, *where* c *is an isolated vertex in* $AG(S)$, *if and only if* $x^2 = y^2 = c$ *or* $w^2 = z^2 = c$.

Theorem 3.8. *Suppose that* $\Gamma(S)$ *is a refinement of a star graph with center* c *and* $T = \{u \mid u$ *is an end vertex adjacent to* c *in* $\Gamma(S)\}$ *and* $|\ T\ | = m \geqslant 1$. *Also assume that* $\Gamma(S)^*$ *has exactly two components* A *and* B *and* $|V(\Gamma(S)^*)| = n$. *Then the following statements hold.*

1. *If* $x \in A$ *and* $y \in B$, *then* $x \sim y$ *in* $AG(S)$.
2. *If* $x \in A$, $y \in B$ *and* $u \in T$, *then* $u \sim x$ *and* $u \sim y$ *in* $AG(S)$.
3. *If* $u, v \in T$, *then* $u \sim v$ *in* $AG(S)$.

The next corollary immediately follows from Theorem 3.8 and [1, Theorems 3.1 and 3.8].

Corollary 3.9. *Suppose that* $\Gamma(S)$ *is a refinement of a star graph with center* c *and* $T = \{u \mid u$ *is an end vertex adjacent to* c *in* $\Gamma(S)\}$ *and* $|\ T\ | = m \geqslant 1$. *Also assume that* $\Gamma(S)^*$ *has exactly two components and* $|V(\Gamma(S)^*)| = n$. *Then the following statements hold.*

1. *If* $Z(S) \neq S$, *then* $AG(S) \cong K_{m+n+1}$.
2. *If* $Z(S) = S$, *then* $AG(S) \cong K_{m+n} \cup K_1$, *where* c *is an isolated vertex in* $AG(S)$.

Proposition 3.10. [22, Theorem 2.5] *Suppose that* $\Gamma(S)$ *is a refinement of a star graph with center* c *such that* $\Gamma(S)^*$ *is isomorphic to* C_n*, where* $n \geqslant 5$*. Then* $S^2 = \{0, c\}$*.*

Lemma 3.11. *Suppose that* $\Gamma(S)$ *is a refinement of a star graph with center* c *such that there exists no end vertex adjacent to* c *in* $\Gamma(S)$*. Also assume that* $\Gamma(S)^* \cong C_n$*, where* $n \geqslant 5$ *and* $x, y \in Z(S)^* \setminus \{c\}$*. Then the following statements hold.*

1. *If* $x \sim y$ *in* $\Gamma(S)$*, then* $x \sim y$ *in* $AG(S)$*.*
2. *If* $x \nsim y$ *in* $\Gamma(S)$ *and* $x^2 \neq 0$ *or* $y^2 \neq 0$*, then* $x \sim y$ *in* $AG(S)$*.*
3. *If* $x \nsim y$ *in* $\Gamma(S)$ *and* $n \geqslant 7$*, then* $x \sim y$ *in* $AG(S)$*.*
4. $x \nsim y$ *in* $AG(S)$ *if and only if* $x^2 = y^2 = 0$*,* $xy = c$ *and* $n = 5$*, or* $x^2 = y^2 = 0$*,* $\mathrm{d}(x, y) = 3$ *in* $\Gamma(S)$ *and* $n = 6$*.*

Proof. The proof of (1) and (2) is clear.

(3). Since $\Gamma(S) \cong C_n$ and $n \geqslant 7$, we have $|V(\Gamma(S)^*)| \geqslant 7$, and so $|Z(S)| \geqslant 9$, since $Z(S) = C_n \cup \{0, c\}$. On the other hand, for each two distinct vertices x and y in $\Gamma(S)^*$, we see that $|\mathrm{ann}_S(x) \cup \mathrm{ann}_S(y)| \leqslant 8$. Since $x \nsim y$ in $\Gamma(S)$, by Proposition 3.10, we have $xy = c$, and so $\mathrm{ann}_S(xy) = Z(S)$. Hence $\mathrm{ann}_S(x) \cup \mathrm{ann}_S(y) \neq \mathrm{ann}_S(xy)$, and therefore $x \sim y$ in $AG(S)$.

(4). First suppose that $x \nsim y$ in $AG(S)$. Then, by (i), (ii), (iii) and Proposition 3.10, we have $x^2 = y^2 = 0$, $xy = c$ and $n = 5$, or $n = 6$. If $n = 6$ and $\mathrm{d}(x, y) = 2$ in $\Gamma(S)$, then there exists a vertex z, such that $z \notin \mathrm{ann}_S(x) \cup \mathrm{ann}_S(y)$, and so $\mathrm{ann}_S(x) \cup \mathrm{ann}_S(y) \neq Z(S) = \mathrm{ann}_S(c) = \mathrm{ann}_S(xy)$. Thus $x \sim y$ in $AG(S)$, which is impossible. Also if $\mathrm{d}(x, y) = 1$ in $\Gamma(S)$, then $x \sim y$ in $\Gamma(S)$ and, by (i), $x \sim y$ in $AG(S)$, which is again impossible. Therefore $\mathrm{d}(x, y) = 3$ in $\Gamma(S)$.

Conversely, first suppose that $n = 5$, $x^2 = y^2 = 0$ and $xy = c$. Then, since $x \nsim y$ in $\Gamma(S)$ and $x, y \in C_5$, we have $\mathrm{ann}_S(x) \cup \mathrm{ann}_S(y) = Z(S) = \mathrm{ann}_S(c) = \mathrm{ann}_S(xy)$. Thus $x \nsim y$ in $AG(S)$.
Now suppose that $x^2 = y^2 = 0$, $\mathrm{d}(x, y) = 3$ in $\Gamma(S)$ and $n = 6$. Then $Z(S) = C_6 \cup \{0, c\}$, and so $|Z(S)| = 8$. Also since $\mathrm{d}(x, y) = 3$, we see that $\mathrm{ann}_S(x) \cap \mathrm{ann}_S(y) = \{0, c\}$ and $|\mathrm{ann}_S(x)| = |\mathrm{ann}_S(y)| = 5$, and so $|\mathrm{ann}_S(x) \cup \mathrm{ann}_S(y)| = 8 = |Z(S)| = |\mathrm{ann}_S(c)| = |\mathrm{ann}_S(xy)|$. Thus $\mathrm{ann}_S(x) \cup \mathrm{ann}_S(y) = \mathrm{ann}_S(xy)$. Therefore $x \nsim y$ in $AG(S)$. □

The following three theorems immediately follows from Lemma 3.11, [1, Theorems 3.1 and 3.8].

Theorem 3.12. *Assume that all the hypothesis of Lemma 3.11 hold and* $n \geqslant 7$*. Then we have the following statements.*

1. *If* $Z(S) \neq S$*, then* $AG(S) \cong K_{n+1}$*.*
2. *If* $Z(S) = S$*, then* $AG(S) \cong K_n \cup K_1$*, where* c *is an isolated vertex in* $AG(S)$*.*

Theorem 3.13. *Suppose that all the hypothesis of Lemma 3.11 hold and* $n = 6$*. Then we have the following statements.*

1. *If* $Z(S) \neq S$*, then* $AG(S) \cong K_7 \setminus \{\{xy\} | x^2 = y^2 = 0, \mathrm{d}(x,y) = 3$ *in* $\Gamma(S)\}$.
2. *If* $Z(S) = S$*, then* $AG(S) \cong K_1 \cup K_6 \setminus \{\{xy\} | x^2 = y^2 = 0, \mathrm{d}(x,y) = 3$ *in* $\Gamma(S)\}$*, where* c *is an isolated vertex in* $AG(S)$.

Theorem 3.14. *Suppose that all the hypothesis of Lemma 3.11 hold and* $n = 5$*. Then we have the following statements.*

1. *If* $Z(S) \neq S$*, then* $AG(S) \cong K_6 \setminus \{\{xy\} | x^2 = y^2 = 0, xy = c\}$.
2. *If* $Z(S) = S$*, then* $AG(S) \cong K_1 \cup K_5 \setminus \{\{xy\} | x^2 = y^2 = 0, xy = c\}$*, where* c *is an isolated vertex in* $AG(S)$.

If $Z(S) \neq S$, then, by [1, Theorem 3.1], $\Gamma(S) \leqslant AG(S)$, and since $\mathrm{gr}(\Gamma(S)) \leqslant 4$, we have $\mathrm{gr}(AG(S)) \leqslant 4$. But if $Z(S) = S$, then the following example shows that 5 is sharp for the girth of $AG(S)$.

Example 3.15. Suppose that $S = \{0, c, a_1, a_2, a_3, a_4, a_5\}$, with $a_1a_2 = a_2a_3 = a_3a_4 = a_4a_5 = a_5a_1 = 0$, $cS = 0$ and $a_i^2 = c^2 = 0$, for each $1 \leqslant i \leqslant 5$. Otherwise $a_ia_j = c$. Then $Z(S) = S$ and, by [22, Theorem 2.5], S is a semigroup and $\Gamma(S)$ is a refinement of a star graph with center c such that there exists no end vertex adjacent to c in $\Gamma(S)$ and $\Gamma(S)^* \cong C_5$.

Now, by Theorem 3.14 (ii), $AG(S) \cong K_1 \cup C_5$ which means that $gr(AG(S)) = 5$.

Theorem 3.16. *Suppose that all the hypothesis of Lemma 3.11 hold and* $n = 3$*. Then we have the following statements.* 1. *If* $Z(S) \neq S$*, then* $AG(S) \cong K_4$.

2. *If* $Z(S) = S$*, then* $AG(S) \cong 4K_1$.

Proof. Since there exists no end vertex adjacent to c in $\Gamma(S)$ and $\Gamma(S)^* \cong C_3 \cong K_3$, we have $\Gamma(S) \cong K_4$. Now, by [1, Theorems 3.1 and 3.9], the results hold. □

For the case $n = 4$, we have the following lemma.

Lemma 3.17. *Suppose that all the hypothesis of Lemma 3.11 hold and* $n = 4$*. Also assume that* $V(\Gamma(S)^*) = \{x, y, z, w\}$ *with* $x \sim y \sim z \sim w \sim x$*. Then we have the following statements.*

1. $\mathrm{ann_S}(x) \cup \mathrm{ann_S}(y) = \mathrm{ann_S}(y) \cup \mathrm{ann_S}(z) = \mathrm{ann_S}(z) \cup \mathrm{ann_S}(w) = \mathrm{ann_S}(w) \cup \mathrm{ann_S}(x) = Z(S)$.
2. $xz \in \{x, z, c\}$ *and* $wy \in \{w, y, c\}$.
3. $x \nsim z$ *in* $AG(S)$ *if and only if* $xz = x$*, or* $xz = z$*, or* $xz = c$ *and* $x^2 = z^2 = 0$*. Also* $w \nsim y$ *in* $AG(S)$ *if and only if* $wy = w$*, or* $wy = y$*, or* $wy = c$ *and* $w^2 = y^2 = 0$.
4. $x \sim z$ *in* $AG(S)$ *if and only if* $xz = c$ *and* $x^2 \neq 0$ *or* $z^2 \neq 0$*. Also* $w \sim y$ *in* $AG(S)$ *if and only if* $wy = c$ *and* $w^2 \neq 0$ *or* $y^2 \neq 0$.

Proof. (1). Since $V(\Gamma(S)^*) = \{x, y, z, w\}$ with $x \sim y \sim z \sim w \sim x$, we have $Z(S) = \{0, c, x, y, z, w\}$, and $\mathrm{ann_S}(x) \supseteq \{0, c, y, w\}$ and $\mathrm{ann_S}(y) \supseteq \{0, c, x, z\}$.

Thus $\mathrm{ann_S}(x) \cup \mathrm{ann_S}(y) = Z(S)$. Similarly, $\mathrm{ann_S}(y) \cup \mathrm{ann_S}(z) = \mathrm{ann_S}(z) \cup \mathrm{ann_S}(w) = \mathrm{ann_S}(w) \cup \mathrm{ann_S}(x) = Z(S)$.

(2). Since $x \nsim z$ and $w \nsim y$ in $\Gamma(S)$, we have $xz \neq 0$ and $wy \neq 0$. If $xz = y$, then $wy = w(xz) = (wx)z = 0$, which is impossible. So $xz \neq y$. Similarly $xz \neq w$. Thus $xz \in \{x, z, c\}$. By a similar argument, $wy \in \{w, y, c\}$.

(3). Suppose that $x \nsim z$ in $AG(S)$, $xz \neq x$ and $xz \neq z$. Then, by (ii), $xz = c$. If $x^2 \neq 0$, then $x \notin \mathrm{ann_S}(x) \cup \mathrm{ann_S}(z)$, and so $\mathrm{ann_S}(x) \cup \mathrm{ann_S}(z) \neq Z(S) = \mathrm{ann_S}(c) = \mathrm{ann_S}(xz)$. This implies that $x \sim z$ in $AG(S)$, which is impossible. Therefore $x^2 = 0$, and similarly $z^2 = 0$.

Conversely, if $xz = x$ or $xz = z$, then $x \nsim z$ in $AG(S)$. Now suppose that $xz = c$ and $x^2 = z^2 = 0$. Then $\mathrm{ann_S}(x) = \{0, c, x, y, w\}$ and $\mathrm{ann_S}(z) = \{0, c, y, z, w\}$, and so $\mathrm{ann_S}(x) \cup \mathrm{ann_S}(z) = \{0, c, x, y, z, w\} = Z(S) = \mathrm{ann_S}(c) = \mathrm{ann_S}(xz)$. Therefore $x \nsim z$ in $AG(S)$. In the same manner we can see that $w \nsim y$ in $AG(S)$ if and only if $wy = w$, or $wy = y$, or $wy = c$ and $w^2 = y^2 = 0$.

(4) By (3), it is clear. □

The following two corollaries follow from Lemma 3.17 and [1, Theorems 3.1 and 3.8].

Corollary 3.18. *Suppose that all the hypothesis of Lemma* 3.17 *hold and* $Z(S) \neq S$. *Then one of the following statements hold.*

1. $AG(S) \cong K_5$ *if and only if the conditions:*
   (1) $xz = wy = c$,
   (2) $x^2 \neq 0$ *or* $z^2 \neq 0$,
   (3) $w^2 \neq 0$ *or* $y^2 \neq 0$ *hold.*
2. $AG(S) \cong K_5 \setminus \{\{xz\}\}$ *if and only if the conditions:*
   (1) $wy = c$, *and* $w^2 \neq 0$ *or* $y^2 \neq 0$,
   (2) $xz = x$, *or* $xz = z$, *or* $xz = c$ *and* $x^2 = z^2 = 0$ *hold.*
3. $AG(S) \cong K_5 \setminus \{\{xz\}, \{wy\}\}$ *if and only if the conditions:*
   (1) $wy = w$, *or* $wy = y$, *or* $wy = c$ *and* $w^2 = y^2 = 0$,
   (2) $xz = x$, *or* $xz = z$, *or* $xz = c$ *and* $x^2 = z^2 = 0$ *hold.*

Corollary 3.19. *Suppose that all the hypothesis of Lemma* 3.17 *hold and* $Z(S) = S$. *Then one of the following statements holds.*

1. $AG(S) \cong 2K_2 \cup K_1$, *where* c *is an isolated vertex and* $x \sim z$ *and* $y \sim w$, *if and only if the conditions:*
   (1) $xz = wy = c$,
   (2) $x^2 \neq 0$ *or* $z^2 \neq 0$,
   (3) $w^2 \neq 0$ *or* $y^2 \neq 0$ *hold.*
2. $AG(S) \cong K_2 \cup 3K_1$, *where* c, x, z *are isolated vertices and* $w \sim y$ *if and only if the conditions:*
   (1) $wy = c$,
   (2) $w^2 \neq 0$ *or* $y^2 \neq 0$,
   (3) $xz = x$, *or* $xz = z$, *or* $xz = c$ *and* $x^2 = z^2 = 0$ *hold.*

3. $AG(S) \cong 5K_1$ *if and only if the conditions:*
   (1) $wy = w$, *or* $wy = y$, *or* $wy = c$ *and* $w^2 = y^2 = 0$,
   (2) $xz = x$, *or* $xz = z$, *or* $xz = c$ *and* $x^2 = z^2 = 0$ *hold.*

The next theorem follows from [1, Theorems 3.1 and 3.8].

Theorem 3.20. *Suppose that* $\Gamma(S)$ *is a refinement of a star graph with center* c *and* $\Gamma(S)^* \cong C_n$, *where* $n \geqslant 5$. *Also assume that*

$$T = \{u \mid u \text{ is an end vertex adjacent to } c \text{ in } \Gamma(S)\}$$

and $\mid T \mid = m \geqslant 1$. *Then the following statements hold.*

1. *If* $x,\, y \in V(\Gamma(S)^*)$, *then* $x \sim y$ *in* $AG(S)$.
2. *If* $x \in V(\Gamma(S)^*)$ *and* $u \in T$, *then* $x \sim u$ *in* $AG(S)$.
3. *If* $u,\, v \in T$, *then* $u \sim v$ *in* $AG(S)$.
4. *If* $Z(S) \neq S$, *then* $AG(S) \cong K_{n+m+1}$.
5. *If* $Z(S) = S$, *then* $AG(S) \cong K_{n+m} \cup K_1$, *where* c *is an isolated vertex in* $AG(S)$.

Proposition 3.21. [22, Theorem 2.6] *Suppose that* $\Gamma(S)$ *is a refinement of a star graph with center* c *and* $\Gamma(S)^* \cong P_n$, *where* $n \geqslant 5$. *Then* $S^2 = \{0, c\}$ *and* $c^2 = 0$.

Theorem 3.22. *Suppose that* $\Gamma(S)$ *is a refinement of a star graph with center* c *and* $\Gamma(S)^* \cong P_n$, *where* $n \geqslant 6$. *Also assume that*

$$T = \{u \mid u \text{ is an end vertex adjacent to } c \text{ in } \Gamma(S)\}$$

and $\mid T \mid = m \geqslant 0$. *Then we have the following statements.*

1. *If* $x,\, y \in V(\Gamma(S)^*)$, *then* $x \sim y$ *in* $AG(S)$.
2. *If* $x \in V(\Gamma(S)^*)$ *and* $u \in T$, *then* $x \sim u$ *in* $AG(S)$.
3. *If* $u,\, v \in T$, *then* $u \sim v$ *in* $AG(S)$.
4. *If* $Z(S) \neq S$, *then* $AG(S) \cong K_{n+m+2}$.
5. *If* $Z(S) = S$, *then* $AG(S) \cong K_{n+m+1} \cup K_1$, *where* c *is an isolated vertex in* $AG(S)$.

Proof. The proof follows from Proposition 3.21 and [1, Theorems 3.1 and 3.8]. □

Lemma 3.23. *Suppose that* $\Gamma(S)$ *is a refinement of a star graph with center* c *and* $\Gamma(S)^* \cong P_5$, *with* $a_1 \sim a_2 \sim a_3 \sim a_4 \sim a_5 \sim a_6$. *Also assume that there exists no end vertex adjacent to* c *in* $\Gamma(S)$. *Then* $a_2 \sim a_5$ *in* $AG(S)$ *if and only if* $a_2^2 \neq 0$ *or* $a_5^2 \neq 0$. *Otherwise,* $a_i \sim a_j$ *in* $AG(S)$, *for each* $1 \leqslant i < j \leqslant 6$.

Proof. By proposition 3.15, for each $1 \leqslant i < j \leqslant 6$, we have $a_i a_j = 0$ or $a_i a_j = c$ and $c^2 = 0$, which follows that $\mathrm{ann_S}(a_i a_j) = Z(S)$. Now if $a_2^2 \neq 0$ or $a_5^2 \neq 0$, then $ann_S(a_2) \cup \mathrm{ann_S}(a_5) \neq Z(S) = \mathrm{ann_S}(a_2 a_5)$, which implies that $a_2 \sim a_5$ in $AG(S)$.

Conversely, suppose on the contrary that $a_2 \sim a_5$ in $AG(S)$ and $a_2^2 = a_5^2 = 0$. Then $ann_S(a_2) \cup \mathrm{ann_S}(a_5) = Z(S) = \mathrm{ann_S}(a_2 a_5)$, which is a contradiction. Thus $a_2^2 \neq 0$ or $a_5^2 \neq 0$.

Finally, since $\Gamma(S)^* \cong P_5$, it implies that, for each $1 \leqslant i < j \leqslant 6$, other than the case $i = 2$ and $j = 5$, we have $\mathrm{ann}_S(a_i) \cup \mathrm{ann}_S(a_j) \neq Z(S) = \mathrm{ann}_S(a_i a_j)$, which implies that $a_i \sim a_j$ in $AG(S)$. □

Theorem 3.24. *Suppose that all the hypothesis of Lemma 3.23 hold. Then we have the following statements.*

1. *If $Z(S) \neq S$, then $AG(S) \cong K_7$ if and only if $a_2^2 \neq 0$ or $a_5^2 \neq 0$. Otherwise $AG(S) \cong K_7 \setminus \{a_2 a_5\}$.*
2. *If $Z(S) = S$, then $AG(S) \cong K_1 \cup K_6$ if and only if $a_2^2 \neq 0$ or $a_5^2 \neq 0$. Otherwise $AG(S) \cong K_1 \cup K_6 \setminus \{a_2 a_5\}$, where c is an isolated vertex in $AG(S)$.*

Proof. By Lemma 3.23 and [1, Theorems 3.1 and 3.8], it is clear. □

Lemma 3.25. *Suppose that $\Gamma(S)$ is a refinement of a star graph with center c and $\Gamma(S)^* \cong P_5$, with $a_1 \sim a_2 \sim a_3 \sim a_4 \sim a_5 \sim a_6$. Also assume that $T = \{u \mid u$ is an end vertex adjacent to c in $\Gamma(S)\}$ and $\mid T \mid = m \geqslant 1$. Then we have the following statements.*

1. *If $Z(S) \neq S$, then $AG(S) \cong K_{7+m}$.*
2. *If $Z(S) = S$, then $AG(S) \cong K_{6+m} \cup K_1$, where c is an isolated vertex in $AG(S)$.*

For the case $n \leqslant 4$, Proposition 3.21 doesn't hold. For the case $n = 4$, we have the following two lemmas.

Lemma 3.26. *Suppose that $\Gamma(S)$ is a refinement of a star graph with center c and $\Gamma(S)^* \cong P_4$, with $a_1 \sim a_2 \sim a_3 \sim a_4 \sim a_5$. Then the following statements hold.*

1. *$\Gamma(S)^* \leqslant AG(S)$.*
2. *$a_1 a_3 \in \{a_3, c\}$, $a_1 a_4 = c$, $a_1 a_5 \in \{a_3, c\}$, $a_2 a_4 = c$, $a_2 a_5 = c$ and $a_3 a_5 \in \{a_3, c\}$.*

Proof. (1). Since $a_5 \notin \mathrm{ann}_S(a_1) \cup \mathrm{ann}_S(a_2) \cup \mathrm{ann}_S(a_3)$ and $a_1 \notin \mathrm{ann}_S(a_3) \cup \mathrm{ann}_S(a_4) \cup \mathrm{ann}_S(a_5)$, which follows that $\Gamma(S)^* \cong P_4 \leqslant AG(S)$.
(2). Since $a_1 \nsim a_3$ in $\Gamma(S)$, we have $a_1 a_3 \neq 0$. If $a_1 a_3 = a_1$, then $a_1 a_4 = (a_1 a_3) a_4 = a_1 (a_3 a_4) = 0$, and if $a_1 a_3 = a_2$, then $a_2 a_4 = 0$, which are impossible. Also if $a_1 a_3 = a_4$, then $a_2 a_4 = 0$, and if $a_1 a_3 = a_5$, then $a_2 a_5 = 0$, which are again impossible. Thus $a_1 a_3 \in \{a_3, c\}$. The similar arguments applies to the other cases. □

If $a_1 a_3 = a_3$, then $a_1 \nsim a_3$ in $AG(S)$, and if $a_1 a_3 = c$, then $a_1 \sim a_3$ in $AG(S)$, since $a_5 \notin \mathrm{ann}_S(a_1) \cup \mathrm{ann}_S(a_3)$. Also if $a_1^2 = 0$ and $a_4^2 = 0$, then $\mathrm{ann}_S(a_1) \cup \mathrm{ann}_S(a_4) = \{a_1, a_2, a_3, a_4, a_5, c, 0\} = \mathrm{ann}_S(c) = \mathrm{ann}_S(a_1 a_4)$. Thus $a_1 \sim a_4$ in $AG(S)$ if and only if $a_1^2 \neq 0$ or $a_4^2 \neq 0$. Since $a_3 \notin \mathrm{ann}_S(a_1) \cup \mathrm{ann}_S(a_5)$ and $a_3 \in \mathrm{ann}_S(c) = \mathrm{ann}_S(a_1 a_5)$, if $a_1 a_5 = c$, then $a_1 \sim a_5$ in $AG(S)$. If $a_1 a_5 = a_3$, then $a_1^2a_5 = a_1a_3 \neq 0$ and $a_5^2a_1 = a_5a_3 \neq 0$, and so $a_1^2 \neq 0$ and $a_5^2 \neq 0$. Now if $a_3^2 \neq 0$, then $\mathrm{ann_S}(a_1) \cup \mathrm{ann_S}(a_5) = \{a_2, a_4, c, 0\} = \mathrm{ann_S}(a_3) = \mathrm{ann_S}(a_1a_5)$. Hence if $a_1a_5 = a_3$, then $a_1 \sim a_5$ in $AG(S)$ if and only if $a_3^2 = 0$. Similarly, $a_2 \sim a_4$ in $AG(S)$ if and only if $a_2^2 \neq 0$ or $a_4^2 \neq 0$, and $a_2 \sim a_5$ in $AG(S)$ if and only if $a_2^2 \neq 0$ or $a_5^2 \neq 0$. Clearly, if $a_3a_5 = a_3$, then $a_3 \nsim a_5$ in $AG(S)$, and since $a_1 \notin \mathrm{ann_S}(a_3) \cup \mathrm{ann_S}(a_5)$, if $a_3a_5 = c$, then $a_3 \sim a_5$ in $AG(S)$.

For example, suppose that $S = \{0, c, a_1, a_2, a_3, a_4, a_5\}$, with $a_1a_2 = a_2a_3 = a_3a_4 = a_4a_5 = 0$, $a_1a_3 = a_1a_5 = a_3a_5 = a_3$, $a_1a_4 = a_2a_4 = a_2a_5 = c$, $a_1^2 = a_3^2 = a_5^2 = a_3$ and $a_2^2 = c$, $a_4^2 = 0$. Then, by [22, Exampe 2.7], S is a commutative semigroup and $\Gamma(S)$ is a refinement of a star graph with center c and $\Gamma(S)^* \cong P_4$, with $a_1 \sim a_2 \sim a_3 \sim a_4 \sim a_5$. Also there exists no end vertex adjacent to c in $\Gamma(S)$. See Figure 1.

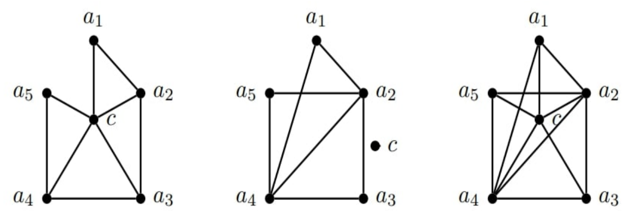

Figure 1. $\Gamma(S)$ $\qquad$ $AG(S)$, $Z(S) = S$ $\qquad$ $AG(S)$, $Z(S) \neq S$

Lemma 3.27. *Suppose that $\Gamma(S)$ is a refinement of a star graph with center c and $\Gamma(S)^* \cong P_4$, with $a_1 \sim a_2 \sim a_3 \sim a_4 \sim a_5$. Also assume that*

$$T = \{u \mid u \text{ is an end vertex adjacent to } c \text{ in } \Gamma(S)\}$$

and $\mid T \mid = m \geqslant 1$. Then the following statements hold.

1. *For each u, $v \in T$, if $uv \notin T$, or $uv = t \in T \setminus \{u, v\}$ and $t^2 = 0$, then $u \sim v$ in $AG(S)$. Otherwise $u \nsim v$ in $AG(S)$.*
2. *For each $a_i \in V(\Gamma(S)^*)$ and $u \in T$, we have $a_iu \notin T$ and $a_i \sim u$ in $AG(S)$ if and only if $a_iu \neq a_i$, for $1 \leqslant i \leqslant 5$.*

Proof. (1). If $uv \notin T$, then $uv = c$ or $uv = a_i$, $(1 \leqslant i \leqslant 5)$. If $uv = c$, then $c^2 = 0$ and clearly $u \sim v$ in $AG(S)$. Assume that $uv = a_i$, $(1 \leqslant i \leqslant 5)$. Then there exists a_j, $(1 \leqslant j \leqslant 5$ and $j \neq i)$ such that $a_ia_j = 0$, $ua_j \neq 0$ and $va_j \neq 0$. Thus $a_j \in \mathrm{ann_S}(a_i) = \mathrm{ann_S}(uv)$ and $a_j \notin \mathrm{ann_S}(u) \cup \mathrm{ann_S}(v)$, and hence $u \sim v$ in $AG(S)$.

Now suppose that $uv = t \in T \setminus \{u, v\}$ and $t^2 = 0$. Then $u^2v = ut \neq 0$, and so $u^2 \neq 0$ also $v^2 \neq 0$. Thus $\mathrm{ann_S}(u) \cup \mathrm{ann_S}(v) = \{0, c\} \neq \{0, c, t\} = \mathrm{ann_S}(t)$, which implies that $u \sim v$ in $AG(S)$. Otherwise if $uv = u$, or $uv = v$, or $uv = t$ and $t^2 \neq 0$, then clearly $u \nsim v$ in $AG(S)$.

(2). If $a_iu = t \in T$, then there exists $a_j \in \mathrm{ann_S}(a_i)$, $j \neq i$, such that $a_jt = a_j(a_iu) = (a_ja_i)u = 0$, which is impossible. Thus $a_iu \notin T$, and so $a_iu = c$ or $a_iu = a_j$ and $1 \leqslant j \leqslant 5$. If $a_iu = c$, then clearly $a_i \sim u$ in $AG(S)$, since there exists a_j, $(1 \leqslant j \leqslant 5$ and $j \neq i)$, such that $a_ia_j \neq 0$, $ua_j \neq 0$ and $ca_j = 0$.

Now if $a_1u = a_4$, then $a_2a_4 = a_2(a_1u) = (a_2a_1)u = 0$, and if $a_1u = a_5$, then $a_2a_5 = 0$, which are impossible. Thus $a_1u \in \{c, a_1, a_2, a_3\}$. Similarly we have $a_5u \in \{c, a_3, a_4, a_5\}$, $a_2u \in \{c, a_2\}$, $a_3u \in \{c, a_3\}$, and $a_4u \in \{c, a_4\}$.

Now by the above discussion the statement (2) holds. □

In this case, by Lemma 3.26, $\Gamma(S)^* \leqslant AG(S)$ and we have $a_1 \sim a_4 \sim a_2 \sim a_5$ in $AG(S)$ and $a_1 \sim a_3$ in $AG(S)$ if and only if $a_1a_3 = c$ and $a_3 \sim a_5$ in $AG(S)$ if and only if $a_3a_5 = c$. Also $a_1 \sim a_5$ in $AG(S)$ if and only if $a_1a_5 = c$, or $a_1a_5 = a_3$ and $a_3^2 = 0$.

For the case $n = 3$, we have the following two lemmas.

Lemma 3.28. *Suppose that $\Gamma(S)$ is a refinement of a star graph with center c and $\Gamma(S)^* \cong P_3$, with $a_1 \sim a_2 \sim a_3 \sim a_4$. Also assume that there exists no end vertex adjacent to c in $\Gamma(S)$. Then the following statements hold.*

1. *$a_1 \sim a_2$ and $a_3 \sim a_4$ in $AG(S)$, but if $Z(S) = S$, then $a_2 \nsim a_3$ in $AG(S)$.*
2. *$a_1a_3 \in \{a_3, c\}$, $a_1a_4 \in \{a_2, a_3, c\}$, $a_2a_4 \in \{a_2, c\}$. Also if $a_1a_4 = a_2$, then $a_2^2 = 0$, and $a_4^2 \neq 0$, and if $a_1a_4 = a_3$, then $a_3^2 = 0$ and $a_1^2 \neq 0$.*

Proof. (1). Since $a_4 \notin \mathrm{ann}_S(a_1) \cup \mathrm{ann}_S(a_2)$ and $a_1 \notin \mathrm{ann}_S(a_3) \cup \mathrm{ann}_S(a_4)$, we have $a_1 \sim a_2$ and $a_3 \sim a_4$ in $AG(S)$. Also we see that $\mathrm{ann}_S(a_2) \cup \mathrm{ann}_S(a_3) = Z(S)$ and $\mathrm{ann}_S(a_2a_3) = S$, and so if $Z(S) = S$, then $a_2 \nsim a_3$ in $AG(S)$.

(2). Since $a_1 \nsim a_3$ in $\Gamma(S)$, we have $a_1a_3 \neq 0$. If $a_1a_3 = a_1$, then $a_1a_4 = (a_1a_3)a_4 = a_1(a_3a_4) = 0$, and if $a_1a_3 = a_2$, then $a_2a_4 = 0$, which are impossible. Also if $a_1a_3 = a_4$, then $a_2a_4 = 0$, which is again impossible. Thus $a_1a_3 \in \{a_3, c\}$. Since $a_1 \nsim a_4$ in $\Gamma(S)$, we have $a_1a_4 \neq 0$. If $a_1a_4 = a_1$, then $a_1a_3 = (a_1a_4)a_3 = a_1(a_4a_3) = 0$, and If $a_1a_4 = a_4$, then $a_2a_4 = 0$, which are again impossible. Thus $a_1a_4 \in \{a_2, a_3, c\}$. Similarly, $a_2a_4 \in \{a_2, c\}$. Also if $a_1a_4 = a_2$, then $a_2^2 = a_2(a_1a_4) = (a_2a_1)a_4 = 0$, and since $a_1a_4^2 = a_2a_4 \neq 0$, we have $a_4^2 \neq 0$. Similarly, if $a_1a_4 = a_3$, then $a_3^2 = 0$ and $a_1^2 \neq 0$. □

If $a_1a_3 = a_3$, then $a_1 \nsim a_3$ in $AG(S)$, and if $a_1a_3 = c$, then $a_1 \sim a_3$ in $AG(S)$ if and only if $a_1^2 \neq 0$ or $a_3^2 \neq 0$. If $a_1a_4 = c$, then $a_1 \sim a_4$ in $AG(S)$ if and only if $a_1^2 \neq 0$ or $a_4^2 \neq 0$. Assume that $a_1a_4 = a_2$. Then $a_2^2 = 0$ and $a_4^2 \neq 0$. If $a_1^2 = 0$, then $\mathrm{ann}_S(a_1) \cup \mathrm{ann}_S(a_4) = \{0, c, a_1, a_2, a_3\} = \mathrm{ann}_S(a_2)$, and so $a_1 \nsim a_4$ in $AG(S)$. Thus if $a_1a_4 = a_2$, then $a_1 \sim a_4$ in $AG(S)$ if and only if $a_1^2 \neq 0$. Similarly, if $a_1a_4 = a_3$, then $a_1 \sim a_4$ in $AG(S)$ if and only if $a_4^2 \neq 0$. Moreover $a_2 \sim a_4$ in $AG(S)$ if and only if $a_2a_4 = c$ and $a_2^2 \neq 0$ or $a_4^2 \neq 0$. Clearly, if $a_2a_4 = a_2$, then $a_2 \nsim a_4$ in $AG(S)$.

Lemma 3.29. *Suppose that $\Gamma(S)$ is a refinement of a star graph with center c and $\Gamma(S)^* \cong P_3$, with $a_1 \sim a_2 \sim a_3 \sim a_4$. Also assume that*

$T = \{u \mid u$ *is an end vertex adjacent to c in $\Gamma(S)$*$\}$

and $\mid T \mid = m \geqslant 1$. Then the following statements hold.

1. *$\Gamma(S)^* \leqslant AG(S)$.*
2. *$a_1a_3 \in \{a_3, c\}$, $a_1a_4 \in \{a_2, a_3, c\}$, $a_2a_4 \in \{a_2, c\}$. Also if $a_1a_4 = a_2$, then*

$a_2^2 = 0$, *and also if* $a_1a_4 = a_2$, *then* $a_2^2 = 0$ *and* $a_4^2 \neq 0$, *and if* $a_1a_4 = a_3$, *then* $a_3^2 = 0$ *and* $a_1^2 \neq 0$.

3. *For each* $u, v \in T$, *if* $uv \notin T$, *or* $uv = t \in T \setminus \{u, v\}$ *and* $t^2 = 0$, *then* $u \sim v$ *in* $AG(S)$. *Otherwise* $u \nsim v$ *in* $AG(S)$.
4. *For each* $a_i \in V(\Gamma(S)^*)$ *and* $u \in T$, *we have* $a_iu \notin T$ *and* $a_i \sim u$ *in* $AG(S)$ *if and only if* $a_iu \neq a_i$, *for* $1 \leqslant i \leqslant 5$.

Proof. Since $a_2a_3 = 0$, $ua_2 \neq 0$ and $ua_3 \neq 0$, we have $u \notin \mathrm{ann_s}(a_2) \cup \mathrm{ann_s}(a_3)$ and $u \in \mathrm{ann_s}(a_2a_3)$. Thus $a_2 \sim a_3$ in $AG(S)$. Now, by using argument similar to that we used in the proof of Lemmas 3.27 and 3.28, the results hold. □

In this case, $a_1 \sim a_3$ in $AG(S)$ if and only if $a_1a_3 = c$, and if $a_1a_4 = c$, then $a_1 \sim a_4$ in $AG(S)$. Also if $a_1a_4 = a_2$, then $a_1 \sim a_4$ in $AG(S)$ if and only if $a_1^2 \neq 0$. Similarly, if $a_1a_4 = a_3$, then $a_1 \sim a_4$ in $AG(S)$ if and only if $a_4^2 \neq 0$. Moreover $a_2 \sim a_4$ in $AG(S)$ if and only if $a_2a_4 = c$ and $a_2^2 \neq 0$ or $a_4^2 \neq 0$

Assume that $\Gamma(S)$ is a refinement of a star graph with center c and $\Gamma(S)^* \cong P_2$, with $a_1 \sim a_2 \sim a_3$ such that there exists no end vertex adjacent to c in $\Gamma(S)$. Then $\Gamma(S) \cong K_4 \setminus \{a_1a_2\}$ and we can see [20, Lemmas 3.11, 3.15, 4.12, 4.16]. Also for the case $n = 1$, we can see [20, Lemmas 3.17, 3.12, 3.21, 4.9, 4.17] and [1, Section 4].

Acknowledgments. The authors are deeply grateful to the referee for careful reading of the manuscript and helpful suggestions.

References

[1] **M. Afkhami, K. Khashyarmanesh and M. Sakhdari,** *On the annihilator graphs of semigroups,* J. Algebra Appl., **14** (2015), 1550015 – 1550029.

[2] **M. Afkhami and K. Khashyarmanesh,** *The cozero-divisor graph of a commutative ring,* Southeast Asian Bull. Math., **35** (2011), 753 – 762.

[3] **S. Akbari, H.R. Maimani and S. Yassemi,** *When a zero-divisor graph is planar or a complete r-partite graph,* J. Algebra, **270** (2003), 169 – 180.

[4] **D.F. Anderson and A. Badawi,** *On the zero-divisor graph of a ring,* Comm. Algebra, **36** (2008), 3073 – 3092.

[5] **D.F. Anderson and A. Badawi,** *The total graph of a commutative ring,* J. Algebra, **320** (2008), 2706 – 2719.

[6] **D.F. Anderson and A. Badawi,** *The total graph of a commutative ring without the zero element,* J. Algebra Appl., **11** (2012), 12500740 – 12500758.

[7] **D.F. Anderson and A. Badawi,** *The generelized total graph of a commutative ring,* J. Algebra Appl., **12** (2013), 1250212 – 1250230.

[8] **D.F. Anderson, A. Frazier, A. Lauve and P.S Livingston,** *The zero-divisor graph of a commutative ring. II,* Ideal Theoretic Methods in Comm. Algebra (Columbia, MO, 1999) 61 – 72.

[9] **D.F. Anderson and P.S. Livingston,** *The zero-divisor graph of a commutative ring,* J. Algebra, **217** (1999), 434 – 447.

[10] **A. Badawi,** *On the annihilator graph of a commutative ring,* Commun. Algebra, **42** (2014), 1 – 14.

[11] **A. Badawi,** *On dot-product graph of a commutative ring,* Commun. Algebra, **43** (2015), 43 – 50.

[12] **Z. Barati, K. Khashyarmanesh, F. Mohammadi and Kh. Nafar,** *On the associated graphs to a commutative ring,* J. Algebra Appl., **11** (2012), 1250037 – 1250054.

[13] **I. Beck,** *Coloring of commutative rings,* J. Algebra, **116** (1998), 208 – 226.

[14] **J.A. Bondy and U.S.R. Murty,** *Graph Theory with Applications,* American Elsevier, New York, (1976).

[15] **F.R. DeMeyer and L. DeMeyer,** *Zero-divisor graphs of semigroups,* J. Algebra, **283** (2005), 190 – 198.

[16] **L. DeMeyer, M. Dsa, I. Epstein, A. Geiser and K. Smith,** *Semigroups and the zero-divisor graph,* Bull. Inst. Comb. Appl., **57** (2009), 60 – 70.

[17] **L. Demeyer, T. Mckenzie and K. Schneider,** *The zero-divisor graph of a commutative semigroup,* Semigroup Forum, **65** (2002), 206 – 214.

[18] **A.V. Kelarev and C.E. Praeger,** *On transitive Cayley graphs of groups and semigroups,* European J. Combin., **24** (2003), 59 – 72.

[19] **K. Khashyarmanesh and M.R. Khorsandi,** *A generalization of the unit and unitary Cayley graphs of a commutative ring,* Acta Math. Hungar., **137** (2012), 242 – 253.

[20] **M. Sakhdari, K. Khashyarmanesh and M. Afkhami,** *Annihilator graphs with four vertices,* Semigroup Forum. **94** (2017), 139 – 166.

[21] **T. S. Wu and D.C. Lu,** *Subsemigroups determined by the zero-divisor graph,* Discrete Math., **308** (2008), 5122 – 5135.

[22] **T.S. Wu, Q. Liu and L. Chen,** *Zero-divisor semigroups and refinement of a star graph,* Discrete Math., **309** (2009), 2510 – 2518.

Received March 2, 2021

M. Afkhami
Department of Mathematics, University of Neyshabur, P.O.Box 91136-899, Neyshabur, Iran
e-mail: mojgan.afkhami@yahoo.com

K. Khashyarmanesh
Department of Pure Mathematics, Ferdowsi University of Mashhad, P.O.Box 1159-91775, Mashhad, Iran
e-mail:khashyar@ipm.ir

M. Sakhdari
Department of Basic Sciences, Sabzevar Branch, Islamic Azad University, Sabzevar, Iran
e-mail:sakhdari85@yahoo.com

Quasigroups and Related Systems **29** (2021), 171 − 176

On the torsion in multiplicatively closed subsets of power associative algebras

Evgenii L. Bashkirov

Abstract. Let A be a commutative ring with 1, M an ideal of A, E a power associative algebra over A having a basis and a unit element e. In the paper, the torsion in the multiplicatively closed subset $e + ME$ of E has been studied when A is an integral domain of characteristic 0 with a theory of divisors. The main theorem of the paper generalizes a result concerning the torsion in the congruence subgroup of the general linear group over A.

One of the most useful way to study an algebraic system with a single binary operation is to ask whether or not a property satisfied by some class of groups is valid for the system in question. The present short note has its origin in the observation that the results of [4] concerning the torsion in the congruence subgroups of the general linear groups over rings can not only be proved for matrix groups over commutative integral domains that have a theory of divisors (this kind of commutative rings is more general than that considered in [4]) but also can be carried over to some multiplicatively closed sets in power associative algebras over rings belonging to the family indicated. In particular, this features to investigate the torsion in Moufang loops because these are power associative by Moufang's theorem ([3], p. 117). To pose the problem properly as well as to formulate the main result one must, first, introduce and recall some terminology and notation.

Let A be a commutative ring with 1. Let E be an algebra over A with unit element e. If M is an ideal of A, then ME denotes the set of all finite sums $\sum_i a_i x_i$ with $a_i \in M, x_i \in E$. Define $S(M)$ to be the set of all elements $e+x$ where $x \in ME$. Since ME is a two-sided ideal of E, the subset $S(M)$ is multiplicatively closed, that is, the product uv is in $S(M)$ whenever u and v are in $S(M)$.

Hereafter A is assumed to be an integral domain. Recall that the requirement A to have a theory of divisors means that there is a commutative semigroup D with identity and with unique factorization such that there exists a homomorphism $a \mapsto (a)$ of the semigroup $A^* = A \setminus \{0\}$ into D satisfying conditions (1)–(3) listed on p. 171 [2]. In particular, an element $a \in A^*$ is divisible by $b \in A^*$ in the ring A if and only if (a) is divisible by (b) in the semigroup D. Also an element $a \in A^*$ is said to be divisible by an element $\mathfrak{a} \in D$, in symbols $\mathfrak{a}|a$, if (a) is divisible by $\mathfrak{a}$ in

2010 Mathematics Subject Classification: 20N02, 20N05, 17A05, 17D05
Keywords: Power associative algebras; Moufang loops; alternative algebras; commutative rings; congruence subgroups

the semigroup D. Accordingly, the notation $\mathfrak{a} \nmid a$ means that (a) is not divisible by $\mathfrak{a}$ in D. The set of all elements of A that are divisible by $\mathfrak{a}$ form an ideal of A, written $I(\mathfrak{a})$. Under the settings established, the following result is valid.

Theorem. *Let A be a commutative integral domain of characteristic 0 with an identity 1. Suppose that A has a theory of divisors $A^* \to D$ such that D contains a prime element $\mathfrak{P}$ satisfying the following conditions: $\mathfrak{P} \nmid 2$ and $\mathfrak{P}^2 \nmid p$ for every prime rational integer p. Let E be a power associative algebra over A with unit element e. Suppose that the underlying A-module of E is free. Then the set $S(I(\mathfrak{P}))$ contains no element of finite order.*

Proof. Suppose that $S(I(\mathfrak{P}))$ contains an element of finite order other than e. Then it contains an element a of prime order p. Let $a = e + b$ with $b \in I(\mathfrak{P})E$. By the condition of the theorem, the module E admits a basis, say $(e_\lambda)_{\lambda\in\Lambda}$ where Λ is an index set which need not be finite. Write $b = \sum_{\lambda\in\Lambda} b_\lambda e_\lambda$ with all b_λ in A, only a finite number of b_λ being nonzero. Moreover, since $b \in I(\mathfrak{P})E$, all b_λ must be in the ideal $I(\mathfrak{P})$. Now due to the power associativity of the algebra E, one gets

$$a^p = (e+b)^p = e + bp + \frac{p(p-1)}{2!}b^2 + \ldots + b^p = e,$$

whence it follows that

$$pb + \frac{p(p-1)}{2!}b^2 + \ldots + b^p = 0. \tag{1}$$

For any integer $t \geqslant 1$, write

$$b^t = \sum_{\lambda\in\Lambda} b_\lambda^{(t)} e_\lambda, \quad b_\lambda^{(t)} \in A, \tag{2}$$

where certainly $b_\lambda^{(1)} = b_\lambda$ for each $\lambda \in \Lambda$. If t ranges from 1 through p, then equations (2) contains only a finite number of nonzero coefficients $b_\lambda^{(t)}$ and, in fact, a finite number of basis elements e_λ. Therefore the set of all indices λ occurring in (2) with t ranging from 1 through p is finite and so it can be identified with the set of positive integers $\{1, 2, \ldots, n\}$ for an appropriate n. Thus equations (2) with $t \in \{1, 2, \ldots, p\}$ can be rewritten as

$$b^t = \sum_{i=1}^{n} b_i^{(t)} e_i. \tag{3}$$

Since each $b_i = b_i^{(1)}$ is divisible by $\mathfrak{P}$ (it should be kept in mind that the zero element of A is supposed to be divisible by all elements of D), one can find an integer $l \geqslant 1$ such that $\mathfrak{P}^l$ divides all $b_1, \ldots, b_n$ while $\mathfrak{P}^{l+1}$ does not divide some $b_j (j \in \{1, 2, \ldots, n\})$. This means that

$$(b_j) = \mathfrak{P}^l \mathfrak{p}_1^{m_1} \ldots \mathfrak{p}_r^{m_r}, \tag{4}$$

where $r \geqslant 0$, m_i are positive integers and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are prime elements of D such that

$$\mathfrak{P} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}. \tag{5}$$

On substituting (3) into (1), one obtains

$$p\sum_{i=1}^{n} b_i e_i + \frac{p(p-1)}{2!}\sum_{i=1}^{n} b_i^{(2)} e_i + \ldots + \sum_{i=1}^{n} b_i^{(p)} e_i = 0.$$

Matching the coefficients of e_j gives the equation

$$pb_j = -\sum_{i=2}^{p-1} \frac{p(p-1)\ldots(p-i+1)}{i!} b_j^{(i)} - b_j^{(p)}. \tag{6}$$

There are two possibilities to consider: (a) $\mathfrak{P} \nmid p$; (b) $\mathfrak{P} | p$.

Consider (a). Assume first that $\mathfrak{P}^{l+1} | pb_j$. This assumption means that

$$(pb_j) = \mathfrak{P}^{l+u} \mathfrak{q}_1^{k_1} \ldots \mathfrak{q}_s^{k_s}. \tag{7}$$

for some integers $u \geqslant 1, s \geqslant 0$, some positive integers k_i and some prime elements $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \in D$ different from $\mathfrak{P}$. In view of (4),

$$(pb_j) = (p)\mathfrak{P}^l \mathfrak{p}_1^{m_1} \ldots \mathfrak{p}_r^{m_r}. \tag{8}$$

Equations (8) and (7) are combined to yield

$$(p)\mathfrak{p}_1^{m_1} \ldots \mathfrak{p}_r^{m_r} = \mathfrak{P}^u \mathfrak{q}_1^{k_1} \ldots \mathfrak{q}_s^{k_s}. \tag{9}$$

Here $u \geqslant 1$, so $\mathfrak{P}$ arises on the right-hand side of (9) and consequently it must coincide with some of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ which is false by (5). This shows that $\mathfrak{P}^{l+1} \nmid pb_j$. On the other hand for each $i = 2, \ldots, p$, $\mathfrak{P}^{li}$ divides $b_j^{(i)}$, and hence $\mathfrak{P}^{l+1}$ divides all $b_j^{(2)}, \ldots, b_j^{(p)}$. Thus $\mathfrak{P}^{l+1}$ divides each summand on the right-hand side of (6), and therefore $\mathfrak{P}^{l+1} | pb_j$. This contradiction shows that possibility (a) is in fact impossible.

Consider (b). Assume first that $\mathfrak{P}^{l+2} | pb_j$. In other words,

$$(pb_j) = \mathfrak{P}^{l+v} \mathfrak{r}_1^{d_1} \ldots \mathfrak{r}_t^{d_t}, \tag{10}$$

where $v \geqslant 2$, all d_i are positive integers and $\mathfrak{r}_1, \ldots, \mathfrak{r}_t (t \geqslant 0)$ are prime elements of D different from $\mathfrak{P}$. By the condition of the theorem, $\mathfrak{P}^2 \nmid p$, and hence

$$(p) = \mathfrak{P} \mathfrak{q}_1^{k_1} \ldots \mathfrak{q}_s^{k_s}, \tag{11}$$

where k_i are positive integers and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s (s \geqslant 0)$ are prime elements of D such that

$$\mathfrak{P} \notin \{\mathfrak{q}_1, \ldots, \mathfrak{q}_s\}. \tag{12}$$

Further, by (4) and (11),

$$(p)(b_j) = \mathfrak{P}^{1+l}\mathfrak{q}_1^{k_1}\dots\mathfrak{q}_s^{k_s}\mathfrak{p}_1^{m_1}\dots\mathfrak{p}_r^{m_r},$$

and comparing the last relation with (10), one concludes, after cancelling $\mathfrak{P}^l$, that

$$\mathfrak{P}^v\mathfrak{r}_1^{d_1}\dots\mathfrak{r}_t^{d_t} = \mathfrak{P}\mathfrak{q}_1^{k_1}\dots\mathfrak{q}_s^{k_s}\mathfrak{p}_1^{m_1}\dots\mathfrak{p}_r^{m_r}.$$

Since $v \geqslant 2$, the last equation can be rewritten as

$$\mathfrak{P}^{v-1}\mathfrak{r}_1^{d_1}\dots\mathfrak{r}_t^{d_t} = \mathfrak{q}_1^{k_1}\dots\mathfrak{q}_s^{k_s}\mathfrak{p}_1^{m_1}\dots\mathfrak{p}_r^{m_r},$$

where $v-1 \geqslant 1$, and so $\mathfrak{P}$ must occur on the right-hand side of the last equality which is impossible in view of (12) and (5). Thus the assumption $\mathfrak{P}^{l+2}|pb_j$ has led to a contradiction, and therefore, $\mathfrak{P}^{l+2} \nmid pb_j$, or, to put it another way, $\mathfrak{P}^{l+2}$ is not a divisor of the left-hand side of (6). On the other hand, if $2 \leqslant i \leqslant p-1$, the element

$$\frac{p(p-1)\dots(p-i+1)}{i!}b_j^{(i)}$$

of A has $\mathfrak{P}(\mathfrak{P}^l)^i = \mathfrak{P}^{1+li}$ as a divisor, and so $\mathfrak{P}^{l+2}$ is its divisor too. Also $\mathfrak{P}^{lp}|b_j^{(p)}$. Now notice that $p > 2$ due to the assumption $\mathfrak{P}|p$ defining possibility (b) and in view of the relation $\mathfrak{P} \nmid 2$ which is true by the condition of the theorem. Therefore, one has $lp \geqslant l+2$, and consequently $\mathfrak{P}^{l+2}|b_j^{(p)}$. Thus every term on the right-hand side of (6) has $\mathfrak{P}^{l+2}$ as a divisor, and hence $\mathfrak{P}^{l+2}$ divides the entire expression on the right-hand side of (6). This final contradiction completes the proof. □

As a special case of the preceding theorem, the following assertion dealing with general alternative algebras deserves to be formulated.

Corollary 1. *Let A, E and $\mathfrak{P}$ be as in Theorem. Suppose that the algebra E is alternative. Then the set of invertible elements of E that are contained in $S(I(\mathfrak{P}))$ is a Moufang loop without torsion.*

Proof. By [1], p. 81, the set of invertible elements in E is a Moufang loop. So having in view Theorem, it suffices to show that for any invertible $x \in S(I(\mathfrak{P}))$, its inverse x^{-1} is also in $S(I(\mathfrak{P}))$. Now one can write $x^{-1} = e+b$ with $b \in E$. Recalling that $x = e+a$ with $a \in I(\mathfrak{P})E$, one has $e = xx^{-1} = (e+a)(e+b) = e+a+b+ab$, whence $b = -a-ab$. But $I(\mathfrak{P})E$ is a two-sided ideal of E, and so b must lie in $I(\mathfrak{P})E$ as required. □

To obtain an application of Theorem in a more concrete situation of the split Cayley-Dickson algebra $O(A)$ as well as in the case of associative matrix algebras, the following portion of notation is needed.

The set $O(A)$ is formed by all symbols $\left(\begin{smallmatrix} a & \alpha \\ \beta & b \end{smallmatrix}\right)$ such that $a, b \in A$ and $\alpha, \beta \in A^3$, where A^3 is the rank 3 free A-module of length 3 columns with components in A. In $O(A)$, equality, addition and multiplication by elements of A are fulfilled componentwise so that $O(A)$ is a free A-module of rank 8. The operation of multiplication in $O(A)$ is defined by

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + \alpha d - \beta \times \delta \\ \beta c + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}$$
$$(a, b, c, d \in A, \alpha, \beta, \gamma, \delta \in A^3),$$

where $\cdot$ and $\times$ denote the usual dot product and crossed product, respectively, in A^3. This makes $O(A)$ a non-associative alternative algebra over A. The algebra $O(A)$ is called the (split) octonion (or Cayley–Dickson) algebra over A, and its elements $\left(\begin{smallmatrix} a & \alpha \\ \beta & b \end{smallmatrix}\right)$ are called octonions. The identity of the algebra $O(A)$ is the octonion $\left(\begin{smallmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 1 \end{smallmatrix}\right)$, where $\mathbf{0}$ denotes the element of A^3 all of whose components are zeros. The Moufang loop of invertible elements of $O(A)$ is denoted $G(A)$.

Now let M be an ideal of A. It is a straightforward verification that the canonical homomorphism $f_M \colon A \to A/M = B$ can be extended to an epimorphism of alternative rings $h_M \colon O(A) \to O(B)$,

$$\left(\begin{array}{c|c} a_1 & \begin{bmatrix} a_2 \\ a_3 \\ a_4 \end{bmatrix} \\ \hline \begin{bmatrix} a_5 \\ a_6 \\ a_7 \end{bmatrix} & a_8 \end{array}\right) \mapsto \left(\begin{array}{c|c} f_M(a_1) & \begin{bmatrix} f_M(a_2) \\ f_M(a_3) \\ f_M(a_4) \end{bmatrix} \\ \hline \begin{bmatrix} f_M(a_5) \\ f_M(a_6) \\ f_M(a_7) \end{bmatrix} & f_M(a_8) \end{array}\right).$$

This h_M determines, in turn, a loop homomorphism $g_M \colon G(A) \to G(B) \colon x \mapsto h_M(x)$. The kernel of g_M, denoted $CL(A, M)$, will be termed the *M-congruence subloop* by analogy with the corresponding concept in the theory of matrix groups (see [4], p. 65) and it is appropriate to recall this concept here.

First, if $n \geqslant 2$ and R is an associative ring with identity, then the group of all invertible $n \times n$ matrices over R is denoted by $GL(n, R)$ and called the general linear group (of degree n over R). Now the canonical homomorphism f_M determines the group homomorphism $\beta_M \colon GL(n, A) \to GL(n, B)$ which sends a matrix $a \in GL(n, A)$ whose element in row i, column j is denoted $a_{ij} (1 \leqslant i, j \leqslant n)$ to the matrix of $GL(n, B)$ whose element in row i, column j is equal to $f_M(a_{ij})$. The kernel of β_M is just the M-congruence subgroup $GL(n, A, M)$.

Corollary 2. *Let A and $\mathfrak{P}$ be such as in Theorem. Let n be an integer, $n \geqslant 3$. Then the $I(\mathfrak{P})$-congruence subloop $C(A, I(\mathfrak{P}))$ as well as the $I(\mathfrak{P})$-congruence subgroup $CL(n, A, I(\mathfrak{P}))$ are torsion free.*

Proof. Note that the subloop $C(A, I(\mathfrak{P}))$ (the subgroup $CL(n, A, I(\mathfrak{P}))$, respectively) coincides with the set of invertible elements in the multiplicatively closed subset $S(I(\mathfrak{P}))$ of the algebra $O(A)$ (the algebra of $n \times n$ matrices over A, respectively). Using Corollary 1 completes the proof. $\square$

References

[1] *Alternative loop rings*, Edited by E.G. Goodaire, E. Jespers, C.P. Milies, North Holland Math. Studies, (1996).

[2] **Z.I. Borevich, I.R. Shafarevich**, *Number theory*, Academic Press, New York, (1966).

[3] **R.H. Bruck**, *A survey of binary systems*, Springer, New York, (1971).

[4] **D.A. Suprunenko**, *Matrix groups*, Transl. Math. Monographs, **45**, Amer. Math. Soc., Providence, Rhode Island, (1976).

Received July 29, 2021

Kalinina str 25, ap. 24
220012 Minsk
Belarus
e-mail: zh.bash@mail.ru

Quasigroups and Related Systems **29** (2021), 177 – 192

Mal'cev classes of left quasigroups and quandles

Marco Bonatto and Stefano Fioravanti

Abstract. In this paper we investigate some Mal'cev classes of varieties of left quasigroups. We prove that the weakest non-trivial Mal'cev condition for a variety of left quasigroups is having a Mal'cev term and that every congruence meet-semidistributive variety of left quasigroups is congruence arithmetic. Then we specialize to the setting of quandles for which we prove that the congruence distributive varieties are those which have no non-trivial finite models.

1. Introduction

Starting from Mal'cev's description of congruence permutability as in [18], the problem of characterizing properties of classes of varieties as *Mal'cev conditions* has led to several results. Mal'cev conditions turned out to be extremely useful, for instance to capture lattice theoretical properties of the congruence lattices of the algebras of classes of variety. In [24] A. Pixley found a strong Mal'cev condition defining the class of varieties with distributive and permuting congruences. In [15] B. Jónsson shows a Mal'cev condition characterizing congruence distributivity, in [10] A. Day shows a Mal'cev condition characterizing the class of varieties with modular congruence lattices.

These results are examples of a more general theorem obtained independently by Pixley [25] and R. Wille [28] that can be considered as a foundational result in the field. They proved that if $p \leqslant q$ is a lattice identity, then the class of varieties whose congruence lattices satisfy $p \leqslant q$ is the intersection of countably many Mal'cev classes. [25] and [28] include an algorithm to generate Mal'cev conditions associated with congruence identities.

Furthermore, the class of varieties satisfying a non-trivial idempotent Mal'cev condition (i.e. any idempotent Mal'cev condition which is not satisfied by any projection algebra) is known to be a Mal'cev class [27]. This class of varieties was characterized by the existence of a *Taylor* term, namely an idempotent n-ary term t that for every coordinate $i \leqslant n$ satisfies an identity as

$$t(x_1, \dots, x_n) \approx t(y_1, \dots, y_n)$$

where $x_1, \dots, x_n, y_1, \dots, y_n \in \{x, y\}$, $x_i = x$ and $y_i = y$.

Recently this class of varieties was proven to be a strong Mal'cev class [22], i.e. there exists the weakest strong idempotent Mal'cev condition.

2010 Mathematics Subject Classification: 20N02, 57M27, 08A30, 20N05.
Keywords: Mal'cev conditions, quandles, quasigroups:

A variety $\mathcal{V}$ is *meet-semidistributive* if the implication

$$\alpha \wedge \beta = \alpha \wedge \gamma \implies \alpha \wedge \beta = \alpha \wedge (\beta \vee \gamma),$$

holds for every triple of congruences of any algebra in $\mathcal{V}$. It is still unknown if the class of meet-semidistributivity varieties is defined by a strong Mal'cev condition, nevertheless it can be characterized in several different ways [23]. On the other hand, we are going to use the characterization of meet-semidistributive varieties in terms of *commutator of congruences* as defined in [11].

Theorem 1.1. [17, Theorem 8.1 items (1), (3), (4)]
Let $\mathcal{V}$ be a variety. The following are equivalent:

(*i*) *$\mathcal{V}$ is a congruence meet-semidistributive variety.*

(*ii*) *No member of $\mathcal{V}$ has a non-trivial abelian congruence.*

(*iii*) $[\alpha, \beta] = \alpha \wedge \beta$ *for every* $\alpha, \beta \in \mathrm{Con}(A)$ *and every* $A \in \mathcal{V}$.

Let A be an algebra, let $\alpha \in \mathrm{Con}(A)$, and let $a \in A$. We denote by $[a]_\alpha$ the congruence class of a in α. The algebra A is said to be:

(*i*) *coherent* if every subalgebra of A which contains a block of a congruence $\alpha \in \mathrm{Con}(A)$ is a union of blocks of α.

(*ii*) *Congruence regular* if whenever $[a]_\alpha = [a]_\beta$ for some $a \in A$ and α, β in $\mathrm{Con}(A)$ then $\alpha = \beta$.

(*iii*) *Congruence uniform* if the blocks of every congruence $\alpha \in \mathrm{Con}(A)$ have all the same cardinality.

A variety $\mathcal{V}$ is *coherent* (resp. *congruence uniform*, *congruence regular*) if all the algebras in $\mathcal{V}$ are coherent (resp. congruence uniform, congruence regular). Because for varieties regularity is equivalent to the condition that no non-zero congruence has a singleton congruence class, every congruence uniform variety is congruence regular. Congruence regularity and coherency are weak Mal'cev classes (see [9] and [12]). On the other hand, it is known that congruence uniformity is not defined by a Mal'cev condition [26].

Some of the most studied Mal'cev classes of varieties are displayed in Figure 1. We refer the reader to [2] for further informations about such classes and to [3] for a more exhaustive poset of Mal'cev classes.

The main goal of this paper is to investigate Mal'cev conditions for racks and quandles. In particular, this paper is concerned with certain Mal'cev classes of varieties, namely, the varieties having a Taylor term, a Mal'cev term and congruence meet semi-distributive varieties.

Left quasigroups are rather combinatorial objects, nevertheless Mal'cev classes of varieties of left quasigroups behave in a pretty rigid way. A characterization of Mal'cev varieties of left quasigroups is provided in Theorem 3.2: they are the varieties for which every left quasigroup is connected, (a left quasigroup is connected

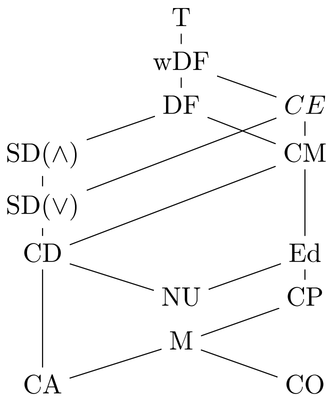

Figure 1: Mal'cev classes: T = Taylor term, wDF = weak difference term, CE = non trivial congruence equation, DF = difference term, CM = congruence modularity, Ed = edge term, CP = congruence permutability, M = Mal'cev term, CO = congruence coherency, SD($\wedge$) = meet semidistributivity, SD($\vee$) = join semidistributivity, CD = congruence distributivity, NU = CD $\bigcap$ Ed = near unanimity term, CA = CD $\bigcap$ M = congruence arithmeticity.

if the action of its left multiplication group is transitive). Moreover, we show that several Mal'cev conditions are equivalent for varieties of left quasigroups. In particular, all the classes in the interval between the class of Taylor varieties and the class of coherent varieties in Figure 1 collapse into the strong Mal'cev class of varieties with a Mal'cev term. Moreover, we prove that the weakest non-trivial (not necessarily idempotent) Mal'cev condition for left quasigroups is having a Mal'cev term, and all such varieties are congruence uniform. In Corollary 3.3 we characterize finite Mal'cev idempotent left quasigroups as the superconnected idempotent left quasigroups (i.e. left quasigroups such that all the subalgebras are connected) using a general result given in [1].

In Theorem 3.5 we show that a congruence meet-semidistributive variety of left quasigroups is congruence arithmetic.

As a consequence of our two main theorems, the poset of Mal'cev classes of left quasigroups in Figure 2 turns into the one in Figure 2.

$$\begin{array}{c} \mathrm{T} = \mathrm{CO} = \mathrm{M} \\ | \\ \mathrm{NU} = \mathrm{SD}(\wedge) = \mathrm{CA} \end{array}$$

Figure 2: Mal'cev classes of varieties of left quasigroups.

Then we turn our attention to quandles, i.e. idempotent left distributive left quasigroups. Quandles are of interest since they provide knot invariants [16, 19]. The class of quandles used for such topological applications is the class of connected quandles. According to the characterization of Mal'cev varieties of left quasigroups, connectedness is actually a relevant property also algebraically. Some of the contents of the paper are formulated for *semimedial* left quasigroups, a class that contain racks and medial left quasigroups [5].

A characterization of distributive varieties of semimedial left quasigroup is given by the properties of the displacement group in Theorem 4.3 where we take advantage of the adaptation of the commutator theory in the sense of [11] developed first for racks in [8] and then extended to semimedial left quasigroups in [5].

In Theorem 4.9 we prove that a variety of quandles is distributive if and only if it has no finite models, making use of the characterization of strictly simple and simple abelian quandles [4]. We also prove that there is no distributive variety of involutory quandles. The problem of finding an example of non-trivial distributive variety of quandles (resp. left quasigroups) is still open.

Examples of non-trivial Mal'cev varieties of quandles (which members are not just left quasigroup reducts of quasigroups) are provided in Table 1.

Notation and terminology. We refer to [2] for basic concepts of universal algebra. Let A be an algebra and t be an n-ary term. Then we say that A satisfies the identity $t_1(x_1,\dots,x_n) \approx t_2(x_1,\dots,x_n)$ if $t_1(a_1,\dots,a_n) = t_2(a_1,\dots,a_n)$ for every $a_i \in A$.

We denote by $\mathbf{H}(A)$, $\mathbf{S}(A)$ and $\mathbf{P}(A)$ respectively the set of homomorphic images, subalgebras and powers of the algebra A and $\mathcal{V}(\mathcal{K})$ denotes the variety generated by the class of algebras $\mathcal{K}$. We denote by $\mathrm{Con}(A)$ the congruence lattice of A, the block of $a \in A$ with respect to a congruence α is denoted by $[a]_\alpha$ (or simply by $[a]$) and the factor algebra by A/α. We denote by $1_A = A \times A$ and $0_A = \{(a,a) : a \in A\}$ respectively the top and bottom element in the congruence lattice of A

Through all the paper, concrete examples of left quasigroups are computed using the software Mace4 [20] and examples of quandles are taken from the library of connected quandles of GAP [13].

2. Left quasigroups

A left quasigroup is a binary algebraic structure $(Q, *, \backslash)$ such that the following identities hold:

$$x * (x\backslash y) \approx y \approx x\backslash(x * y).$$

Hence, a left quasigroup is a set Q endowed with a binary operation $*$ such that the mapping $L_x \colon y \mapsto x * y$ is a bijection of Q for every $x \in Q$. The right multiplication mappings $R_x \colon y \mapsto y * x$ need not to be bijections. Clearly the left division is defined by $x\backslash y = L_x^{-1}(y)$, so we usually denote left quasigroups just as a pair $(Q, *)$. Nevertheless, if $(Q, *)$ is a left quasigroup and $(R, *)$ is a binary algebraic structure and $f \colon Q \to R$ is a homomorphism with respect to $*$, the image of f is not necessarily a left quasigroup. We define the *left multiplication group of* Q as $\mathrm{LMlt}(Q) = \langle L_a,\, a \in Q\rangle$.

Let α be a congruence of a left quasigroup Q. The map

$$\mathrm{LMlt}(Q) \longrightarrow \mathrm{LMlt}(Q/\alpha), \quad L_a \mapsto L_{[a]}$$

can be extended to a surjective morphism of groups with kernel denoted by LMlt^α. The *displacement group relative to* α, denoted by Dis_α, is the normal closure in $\mathrm{LMlt}(Q)$ of $\{L_a L_b^{-1} \,:\, a\,\alpha\, b\}$. In particular, we denote by $\mathrm{Dis}(Q)$ the displacement group relative to 1_Q and we simpy call it the *displacement group of* Q. The maps defined above clearly restrict and corestrict to the displacement groups of Q and Q/α and we denote by Dis^α the intersection between LMlt^α and $\mathrm{Dis}(Q)$.

Lemma 2.1. *Let $\mathcal{K}$ be a class of left quasigroups and $Q \in \mathcal{V}(\mathcal{K})$. Then:*

(i) $\mathrm{Dis}(Q) \in \mathcal{V}(\{\mathrm{Dis}(R) \,:\, R \in \mathcal{K}\})$.

(ii) $\mathrm{LMlt}(Q) \in \mathcal{V}(\{\mathrm{LMlt}(R) \,:\, R \in \mathcal{K}\})$.

Proof. (i). Let $\{Q_i \,:\, i \in I\} \subseteq \mathcal{K}$. The group $\mathrm{Dis}(Q_i/\alpha) \in \mathbf{H}(\mathrm{Dis}(Q_i))$. Let S be a subalgebra of Q_i and $H = \langle L_a,\, a \in S\rangle$. Then

$$\mathrm{Dis}(S) \cong \langle h L_a L_b^{-1} h^{-1}|_S,\, a, b \in S,\, h \in H\rangle \in \mathbf{HS}(\mathrm{Dis}(Q_i)).$$

Let $Q = \prod_{i\in I} Q_i$ and α_i the kernel of the canonical homomorphism onto Q_i. Then $\bigcap_{i\in I} \mathrm{Dis}^{\alpha_i} = 1$ and so we have a canonical embedding

$$\mathrm{Dis}(Q) \hookrightarrow \prod_{i\in I} \mathrm{Dis}(Q)/\mathrm{Dis}^{\alpha_i} = \prod_{i\in I} \mathrm{Dis}(Q_i),$$

i.e. $\mathrm{Dis}(Q) \in \mathbf{SP}(\{\mathrm{Dis}(Q_i) \,:\, i \in I\})$. The same argument can be used for (ii). $\square$

In [5, Section 1] we introduced the lattice of *admissible subgroups* of a left quasigroup Q. Given $N \leqslant \mathrm{LMlt}(Q)$ we have two equivalence relations on the underlying set of the left quasigroup Q:

(i) the orbit decomposition with respect to the action of N, denoted by $\mathcal{O}_N$.

(ii) The equivalence con_N defined as

$$a \,\mathrm{con}_N\, b \text{ if and only if } L_a L_b^{-1} \in N.$$

The assignments $\alpha \mapsto \mathrm{Dis}_\alpha$ (resp. Dis^α) and $N \mapsto \mathrm{con}_N$ (resp. $\mathcal{O}_N$) are monotone and $\mathrm{Dis}_\alpha \leqslant \mathrm{Dis}^\alpha$ (see the characterization of congruences in terms of the properties of subgroups provided in [5, Lemma 1.5]), whereas in general no containment between the equivalences con_N and $\mathcal{O}_N$ holds.

We define the lattice of admissible subgroups as

$$\mathrm{Norm}(Q) = \{N \trianglelefteq \mathrm{LMlt}(Q) \,:\, \mathcal{O}_N \subseteq \mathrm{con}_N\}.$$

In particular, $\mathcal{O}_N$ is a congruence of Q whenever N is admissible and $\mathrm{Dis}_\alpha, \mathrm{Dis}^\alpha \in \mathrm{Norm}(Q)$ for every congruence α. The assignments $N \mapsto \mathcal{O}_N$ and $\alpha \mapsto \mathrm{Dis}^\alpha$ provide a monotone Galois connection between $\mathrm{Norm}(Q)$ and the congruence lattice of Q [5, Theorem 1.10].

The *Cayley kernel* of a left quasigroup Q is the equivalence relation λ_Q defined by

$$a \,\lambda_Q\, b \text{ if and only if } L_a = L_b.$$

Such a relation is not a congruence in general. We say that:

(i) Q is a *Cayley* left quasigroup if λ_Q is a congruence. A class of left quasigroups is Cayley if all its members are Cayley left quasigroups.

(ii) Q is *faithful* if $\lambda_Q = 0_Q$ and Q is *superfaithful* if all the subalgebras of Q are faithful.

(iii) Q is *permutation* if $\lambda_Q = 1_Q$, i.e. there exists $f \in \mathrm{Sym}(Q)$ such that $a*b = f(b)$ for every $a, b \in Q$. If $f = 1$ we say that Q is a *projection* left quasigroup (we denote by $\mathcal{P}_n$ the projection left quasigroup of size n). Note that, permutation left quasigrouops are unary algebras and that projection left quasigroups are also called right zero semigroups.

According to [7, Theorem 5.3], the *strongly abelian* congruences of left quasigroups (in the sense of [21]) are exactly those below the Cayley kernel. Equivalently, if α is a congruence of a left quasigroup Q, then $\alpha \leqslant \lambda_Q$ if and only if $\mathrm{Dis}_\alpha = 1$.

A left quasigroup Q is *connected* if its left multiplication group is transitive on Q. We say that Q is *superconnected* if all the subalgebras of Q are connected. We investigated superconnected left quasigroups in [6].

Proposition 2.2. [6, Corollary 1.6] *A left quasigroup Q is superconnected if and only if $\mathcal{P}_2 \notin \boldsymbol{HS}(Q)$.*

The property of being (super)connected is also reflected by the properties of congruences.

Lemma 2.3. *Connected left quasigroups are congruence uniform and congruence regular.*

Proof. Let Q be a connected left quasigroup and assume that $[a]_\alpha = [a]_\beta$ for some $a \in Q$. For every $b \in Q$ there exists $h \in \mathrm{LMlt}(Q)$ with $b = h(a)$. The blocks of congruences are blocks with respect to the action of $\mathrm{LMlt}(Q)$. Then

$$[b]_\alpha = [h(a)]_\alpha = h([a]_\alpha) = h([a]_\beta) = [h(a)]_\beta = [b]_\beta,$$

and so $\alpha = \beta$. In particular, the mapping h is a bijection between $[a]_\alpha$ and $[b]_\alpha$ for every $\alpha \in \mathrm{Con}(Q)$. □

Lemma 2.4. *Superconnected left quasigroups are coherent.*

Proof. Let Q be a superconnected left quasigroup, M be a subalgebra of Q and $\alpha \in \mathrm{Con}(Q)$ with $[a]_\alpha \subseteq M$ for some $a \in M$. For every $b \in M$ there exists $h \in \mathrm{LMlt}(M)$ such that $b = h(a)$. The blocks of α are blocks with respect to the action of $\mathrm{LMlt}(Q)$ and M is a subalgebra, then $h([a]_\alpha) = [b]_\alpha \subseteq M$. Therefore, $M = \bigcup_{b\in M}[b]_\alpha$. □

A *quasigroup* is a binary algebra $(Q, *, \backslash, /)$ such that $(Q, *, \backslash)$ is a left quasigroup (the *left quasigroup reduct* of Q) and $(Q, *, /)$ is a right quasigroup. The left quasigroups obtained as reducts of quasigroups are called *latin* (note that congruence and subalgebras of a quasigroup and its left quasigroup reduct might be different due to the different signature considered for the two structures). Latin left quasigroups are superfaithful and connected.

The *squaring mapping* for a left quasigroup is the map $\mathfrak{s} : Q \longrightarrow Q,\ a \mapsto a * a$. We denote the set of *idempotent elements of* Q by

$$E(Q) = Fix(\mathfrak{s}) = \{a \in Q \,:\, a * a = a\}.$$

We say that:

(i)] Q is *idempotent* if $Q = E(Q)$, i.e. the identity $x * x \approx x$ holds in Q.

(ii) Q is 2-*divisible* if $\mathfrak{s}$ is a bijection.

(iii) Q is n-*multipotent* if $|\mathfrak{s}^n(Q)| = 1$ (here $\mathfrak{s}^n = \mathfrak{s} \circ \mathfrak{s}^{n-1}$ denotes the usual composition of maps). If $n = 1$ we say that Q is *unipotent*.

3. Mal'cev classes of left quasigroups

In this section we turn our attention to Mal'cev classes of left quasigroups. According to [17, Theorem 3.13] a variety with a Taylor term does not contain any strongly abelian congruence, so in particular Taylor varieties of left quasigroup do not contain permutation left quasigroups (if Q is permutation, then $1_Q = \lambda_Q$ is strongly abelian).

Proposition 3.1. *Let $\mathcal{V}$ be a Taylor variety of left quasigroups. Then* $\mathrm{Dis}(Q)$ *is transitive on Q for every $Q \in \mathcal{V}$.*

Proof. Let $Q \in \mathcal{V}$. According to [5, Corollary 1.9], $P = Q/\mathcal{O}_{\mathrm{Dis}(Q)}$ is a permutation left quasigroup and so P is trivial, i.e. $\mathrm{Dis}(Q)$ is transitive on Q. □

For left quasigroups, the interval of Mal'cev classes between the class of Taylor varieties and the class of coherent varieties collapses into the class of varieties with a Mal'cev term.

Theorem 3.2. *Let $\mathcal{V}$ be a variety of left quasigroups. The following are equivalent:*

(i) $\mathcal{V}$ has a Mal'cev term.

(ii) $\mathcal{V}$ has a Taylor term.

(iii) $\mathcal{V}$ satisfies a non-trivial idempotent Mal'cev condition.

(*iv*) *$\mathcal{V}$ satisfies a non-trivial Mal'cev condition.*

(*v*) $\mathcal{P}_2 \notin \mathcal{V}$.

(*vi*) *Every algebra in $\mathcal{V}$ is superconnected.*

(*vii*) *$\mathcal{V}$ is coherent.*

In particular, every Mal'cev variety of left quasigroup is congruence uniform.

Proof. The implications $(i) \Rightarrow (ii)$ and $(vii) \Rightarrow (i)$ hold in general as represented in Figure 1, (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (iv) clearly hold.

$(v) \Rightarrow (vi)$. According to Proposition 2.2, if $\mathcal{P}_2 \notin \mathcal{V}$ then every left quasigroup in $\mathcal{V}$ is connected and then superconnected since $\mathcal{V}$ is closed under taking subalgebras.

$(vi) \Rightarrow (vii)$. By Lemma 2.4 every superconnected left quasigroup is coherent, i.e. $\mathcal{V}$ is coherent.

According to Lemma 2.3, connected left quasigroups are congruence uniform, therefore so is any Mal'cev variety of left quasigroup. □

Corollary 3.3. *Let Q be a finite idempotent left quasigroup. Then $\mathcal{V}(Q)$ has a Mal'cev term if and only if Q is superconnected.*

Proof. Let Q be a finite idempotent left quasigroup. According to [1, Theorem 1.1], $\mathcal{V}(Q)$ has Taylor term if and only if $\mathcal{P}_2 \notin \mathbf{HS}(Q)$. Thus, $\mathcal{V}(Q)$ has Taylor term if and only if Q is superconnected by Proposition 2.2. □

Proposition 3.4. *Let $\mathcal{V}$ be a Cayley* (*resp. idempotent*) *Mal'cev variety of left quasigroups and $Q \in \mathcal{V}$. Then:*

(*i*) *every left quasigroups in $\mathcal{V}$ is superfaithful.*

(*ii*) *The* Dis *operator is injective and the* con *operator is surjective and* $\alpha = \mathrm{con}_{\mathrm{Dis}_\alpha} = \mathrm{con}_{\mathrm{Dis}^\alpha}$ *for every $\alpha \in \mathrm{Con}(Q)$.*

Proof. (*i*). Idempotent superconnected left quasigroups are superfaithful according to [6, Lemma 1.9], so the claim follows if $\mathcal{V}$ is idempotent.

Assume that $\mathcal{V}$ is a Cayley variety. The Cayley kernel is a strongly abelian congruence for Cayley left quasigroups (see [7, Proposition 5.1]), therefore the left quasigroups in $\mathcal{V}$ are superfaithful.

(*ii*). All the left quasigroups in $\mathcal{V}$ are superfaithful by (i). According to [5, Proposition 1.6] we have that

$$\alpha \leqslant \mathrm{con}_{\mathrm{Dis}_\alpha} \leqslant \mathrm{con}_{\mathrm{Dis}^\alpha} = \alpha.$$

and so the operator $\mathrm{con}_{\mathrm{Dis}}$ is the identity on $\mathrm{Con}(Q)$. □

Let us turn our attention to congruence distributive varieties of left quasigroups. We have already proved that every Taylor variety of left quasigroups is also Mal'cev. Therefore, the left branch of the poset in Figure 1 also collapses into the Mal'cev class of distributive varieties.

Theorem 3.5. *Let $\mathcal{V}$ be a variety of left quasigroups. The following are equivalent:*

(i) $\mathcal{V}$ is congruence meet-semidistributive.

(ii) $\mathcal{V}$ is congruence distributive.

(iii) $\mathcal{V}$ is congruence arithmetic.

According to Theorems 3.2 and 3.5, for left quasigroups the poset of Mal'cev classes in Figure 1 turns into the one in Figure 2.

A term $t(x_1, \dots, x_n)$ in the language of left quasigroups is a well-formed formal expression using the variables $x_1, \dots, x_n$ and the operations $\{*, \backslash\}$. It is easy to see that the term t is either a variable or can be expressed by

$$t(x_1, \dots x_n) = u(x_1, \dots, x_n) \bullet r(x_1, \dots, x_n) \tag{1}$$

where $\bullet \in \{*, \backslash\}$ and u and r are suitable subterms. Let u be a n-ary term. We define

$$\begin{aligned} L^0_{u(x_1,\dots,x_n)}(y) &= y \\ L^{k+1}_{u(x_1,\dots,x_n)}(y) &= u(x_1, \dots, x_n) * L^k_{u(x_1,\dots,x_n)}(y), \\ L^{k-1}_{u(x_1,\dots,x_n)}(y) &= u(x_1, \dots, x_n) \backslash L^k_{u(x_1,\dots,x_n)}(y), \end{aligned}$$

for $k \in \mathbb{Z}$. Using this notation we have that every term t can be written as

$$t(x_1, \dots, x_n) = L^{k_1}_{u_1(x_1,\dots,x_n)} \dots L^{k_m}_{u_m(x_1,\dots,x_n)}(x_R)$$

where u_i is a subterm, $k_i = \pm 1$ for $1 \leqslant i \leqslant m$ and $x_R \in \{x_i : i = 1, \dots, n\}$. We say that x_R is the *rightmost variable of* t.

Every identity in the language of left quasigroups $t_1 \approx t_2$ has the form

$$L^{k_1}_{w_1(x_1,\dots,x_n)} \dots L^{k_m}_{w_m(x_1,\dots,x_n)}(x_R) \approx L^{r_1}_{u_1(y_1,\dots,y_l)} \dots L^{r_l}_{u_l(y_1,\dots,y_l)}(y_R),$$

or equivalently,

$$L^{-r_l}_{u_l(y_1,\dots,y_l)} \dots L^{-r_1}_{u_1(y_1,\dots,y_l)} L^{k_1}_{w_1(x_1,\dots,x_n)} \dots L^{k_m}_{w_m(x_1,\dots,x_n)}(x_R) \approx y_R. \tag{2}$$

The projection left quasigroup $\mathcal{P}_2$ satisfies (2) if and only if $x_R = y_R$. So a variety of left quasigroups $\mathcal{V}$ has a Mal'cev term if and only if it satisfies an identity as in (2) with $x_R \neq y_R$.

Note that, an identity as in (2) might have just the trivial model. For instance if $\mathcal{V}$ is a variety of idempotent left quasigroups satisfying such an identity and the variable y_R does not appear in the left handside then $\mathcal{V}$ is trivial. Indeed, identifying all the variables $x_1, \dots, x_n, y_1, \dots, y_l$ we have $L^{k_1+\dots+k_m}_{x_R}(x_R) = x_R \approx y_R$.

Example 3.6. A variety axiomatized by some identities as in (2) might be made up of latin left quasigroups. For instance, Mal'cev varieties of left quasigroups are provided by varieties of quasigroup in which every member is *term equivalent* to its left quasigroup reduct. This is the case of the following examples (for an example of a Mal'cev variety of latin left quasigroups not arising from quasigroups see Proposition 4.2).

(i) The variety of commutative left quasigroups defined by the identity

$$x * y \approx y * x.$$

(ii) Let $n \in \mathbb{N}$. The variety of left quasigroups satisfying the identity

$$(\dots((x * \underbrace{y) * y) \dots) * y}_{n} \approx x.$$

(iii) The variety of paramedial left quasigroups, identified by the identity

$$(x * y) * (z * t) \approx (t * y) * (z * x).$$

Example 3.7. Mal'cev varieties of left quasigroups are not limited to varieties of latin left quasigroups, as witnessed by the following examples.

(i) Let $\mathcal{V}_n$ be the variety of left quasigroups satisfying $L_x^n(x) \approx L_y^n(y)$ where $n \in \mathbb{Z}$. Then

$$m(x, y, z) = L_x^{-n} L_y^n(z)$$

is a Mal'cev term. Let $n > 0$, Q be a set and e be a fixed element in Q. We define $L_e = 1$ and L_a to be any cycle $(a, \dots, e)$ of length n for every $a \in Q$, $a \neq e$ (if $n < 0$ we define L_a^{-1} in the same way). Then $(Q, *) \in \mathcal{V}_n$.

(ii) The variety of n-multipotent left quasigroups is axiomatized by the identity

$$\mathfrak{s}^n(x) = L_{\mathfrak{s}^{n-1}(x)} L_{\mathfrak{s}^{n-2}(x)} \dots L_{\mathfrak{s}(x)} L_x(x) \approx L_{\mathfrak{s}^{n-1}(y)} L_{\mathfrak{s}^{n-2}(y)} \dots L_{\mathfrak{s}(y)} L_y(y) = \mathfrak{s}^n(y).$$

A Mal'cev term for n-multipotent left quasigroups is

$$m(x, y, z) = \left(L_{\mathfrak{s}^{n-2}(x)} \dots L_{\mathfrak{s}(x)} L_x\right)^{-1} L_{\mathfrak{s}^{n-2}(y)} \dots L_{\mathfrak{s}(y)} L_y(z).$$

Example 3.8. Let $\mathfrak{G}$ be a variety of groups. We denote the class of left quasigroups such that the left multiplication group (resp. displacement group) belongs to $\mathfrak{G}$ by $L(\mathfrak{G})$ (resp. $D(\mathfrak{G})$). According to Lemma 2.1 such classes are varieties. Since $\mathrm{LMlt}(\mathcal{P}_2) = \mathrm{Dis}(\mathcal{P}_2) = 1$ then $\mathcal{P}_2$ belongs to $L(\mathfrak{G})$ and to $D(\mathfrak{G})$ and so they have no Mal'cev term.

4. Semimedial left quasigroups

Semimedial left quasigroups are defined by the semimedial law:

$$(x * y) * (x * z) \approx (x * x) * (y * z).$$

The projection left quasigroup $\mathcal{P}_2$ satisfies the semimedial law and so the whole variety of semimedial left quasigroups is not Mal'cev.

A relevant subvariety of 2-divisible semimedial left quasigroups is the variety of *racks*, axiomatized by the identity

$$x * (y * z) \approx (x * y) * (x * z).$$

Idempotent semimedial left quasigroups are racks and they are called *quandles*. If Q is semimedial then the squaring map $\mathfrak{s}$ is a homomorphism and so if $h = L_{a_1}^{k_1} \dots L_{a_n}^{k_n} \in \mathrm{LMlt}(Q)$ we have

$$\mathfrak{s}h = \underbrace{L_{\mathfrak{s}(a_1)}^{k_1} \dots L_{\mathfrak{s}(a_n)}^{k_n}}_{=h^{\mathfrak{s}}} \mathfrak{s}$$

and the subset $E(Q) = \{a \in Q \,:\, a * a = a\}$ is a subquandle of Q. *Medial* left quasigroups, i.e. those for which

$$(x * y) * (z * t) \approx (x * z) * (y * t)$$

holds are also semimedial.

For a semimedial left quasigroup Q, the admissible subgroups are

$$\mathrm{Norm}(Q) = \{N \trianglelefteq \mathrm{LMlt}(Q) \,:\, N^{\mathfrak{s}} \leqslant N\}$$

where $N^{\mathfrak{s}} = \{h^{\mathfrak{s}} \,:\, h \in N\}$. Note that $[g,h]^{\mathfrak{s}} = [g^{\mathfrak{s}}, h^{\mathfrak{s}}]$ for every $g, h \in \mathrm{LMlt}(Q)$. Thus, if $N \in \mathrm{Norm}(Q)$ then $[\mathrm{LMlt}(Q), N] \in \mathrm{Norm}(Q)$ (see [5, Lemma 3.1]).

The relation con_N is a congruence for every admissible subgroup N and the assignments $\alpha \mapsto \mathrm{Dis}_\alpha$ and $N \mapsto \mathrm{con}_N$ provide a second monotone Galois connection between the lattice of congruences and the admissible subgroups [5, Theorem 3.5]. Such a Galois connection is also well-behaved with respect to the commutator of congruences. Indeed, in a Mal'cev variety the commutator of congruences in the sense of [11] is completely determined by such Galois connection.

Lemma 4.1. *Let $\mathcal{V}$ be a Mal'cev variety of semimedial left quasigroups and $Q \in \mathcal{V}$. Then*

$$[\alpha, \beta] = \mathrm{con}_{[\mathrm{Dis}_\alpha, \mathrm{Dis}_\beta]}$$

for every $\alpha, \beta \in \mathrm{Con}(Q)$.

Proof. The variety $\mathcal{V}$ is Cayley ([5, Proposition 3.6]), and so the left quasigroups in it are superfaithful by Proposition 3.4(i). Therefore we can apply directly [5, Proposition 3.10] □

Let us show that unipotent semimedial left quasigroups are latin, providing an example of variety of latin left quasigroups that is not term equivalent to a variety of quasigroups. Recall that a group G acting on a set Q is *regular* if for every $a, b \in Q$ there exists a unique $g \in G$ such that $b = g \cdot a$. Equivalently the action is transitive and the pointwise stabilizers are trivial.

Proposition 4.2. *Let Q be a unipotent semimedial left quasigroup and $\mathfrak{s}(Q) = \{e\}$. Then:*

(*i*) *the group* $\mathrm{Dis}(Q)$ *is regular and* $\mathrm{Dis}(Q) = \{L_a L_e^{-1} \,:\, a \in Q\}$.

(*ii*) *Q is latin.*

Proof. (i). Let $h = L_{a_1}^{k_1} \dots L_{a_n}^{k_n} \in \mathrm{Dis}(Q)$. According to [5, Lemma 1.4] $k_1 + \dots + k_n = 0$ and so $h^{\mathfrak{s}} = L_{\mathfrak{s}(a_1)}^{k_1} \dots L_{\mathfrak{s}(a_n)}^{k_n} = L_e^{k_1+\dots+k_n} = 1$. If $h \in \mathrm{Dis}(Q)_a$, then $L_a = L_{h(a)} = h^s L_a h^{-1} = L_a h^{-1}$, i.e. $h = 1$ and so $\mathrm{Dis}(Q)$ is regular. On the other hand, $e = (e\backslash a) * (e\backslash a) = L_{e\backslash a} L_e^{-1}(a)$, and so we have $\mathrm{Dis}(Q) = \{L_a L_e^{-1} : a \in Q\}$.

(ii). Let $a, b \in Q$. According to (i) $\mathrm{Dis}(Q) = \{L_c L_e^{-1} : c \in Q\}$ and it is regular. Thus, there exists a unique c such that

$$a = L_c L_e^{-1}(b) = c * (e\backslash b)$$

and so the right multiplication $R_{e\backslash b}$ is bijective for every $b \in Q$. □

4.1. Congruence distributive varieties

According to Theorem 3.5 we have that congruence meet-semidistributive varieties of left quasigroups are congruence distributive. For semimedial left quasigroups congruence distributivity is determined by the properties of the relative displacement groups and of the admissible subgroups.

Proposition 4.3. *Let $\mathcal{V}$ be a variety of semimedial left quasigroups. The following are equivalent:*

(i) *$\mathcal{V}$ is distributive.*

(ii) $\mathrm{Dis}_\alpha = [\mathrm{Dis}_\alpha, \mathrm{Dis}_\alpha]$ *for every $Q \in \mathcal{V}$ and $\alpha \in \mathrm{Con}(Q)$.*

(iii) *If $N \in \mathrm{Norm}(Q)$ is solvable then $N = 1$ for every $Q \in \mathcal{V}$.*

Proof. It is enough to prove the equivalence for meet-semidistributive varieties thanks to Theorem 3.5.

Let $Q \in \mathcal{V}$ and $\alpha \in \mathrm{Con}(Q)$. By Lemma 4.1 we have

$$\mathrm{Dis}_{[\alpha,\alpha]} = \mathrm{Dis}_{\mathrm{con}_{[\mathrm{Dis}_\alpha, \mathrm{Dis}_\alpha]}} \leqslant [\mathrm{Dis}_\alpha, \mathrm{Dis}_\alpha] \leqslant \mathrm{Dis}_\alpha.$$

$(i) \Rightarrow (ii)$. By Theorem 1.1 we have $[\alpha, \alpha] = \alpha$ and so $\mathrm{Dis}_\alpha = \mathrm{Dis}_{[\alpha,\alpha]} = [\mathrm{Dis}_\alpha, \mathrm{Dis}_\alpha]$.

$(ii) \Rightarrow (iii)$. Let $N \in \mathrm{Norm}(Q)$ be solvable of length n and let D be the non-trivial $(n-1)$th element of the derived series of N. So D is abelian and it is in $\mathrm{Norm}(Q)$. Hence, according to [5, Lemma 2.6], $\beta = \mathcal{O}_D$ is a non-trivial abelian congruence of Q. Therefore Dis_β is abelian and we have $\mathrm{Dis}_\beta = [\mathrm{Dis}_\beta, \mathrm{Dis}_\beta] = 1$. Hence, $\beta \leqslant \lambda_Q = 0_Q$, contradiction.

$(iii) \Rightarrow (i)$. If α is abelian then Dis_α is abelian [8, Corollary 5.4]. Hence $\mathrm{Dis}_\alpha = [\mathrm{Dis}_\alpha, \mathrm{Dis}_\alpha] = 1$, i.e. $\alpha \leq \lambda_Q = 0_Q$. □

If Q is a 2-divisible semimedial left quasigroup then

$$\mathrm{Norm}(Q) = \{N \trianglelefteq \mathrm{LMlt}(Q) : \mathfrak{s} N \mathfrak{s}^{-1} \leqslant N\}$$

since $\mathfrak{s}$ is bijective. In particular, $Z(N)$ is a characteristic subgroup of N, and so it is normal in $\mathrm{LMlt}(Q)$ and $\mathfrak{s} Z(N) \mathfrak{s}^{-1} \leqslant Z(N)$. Thus, $Z(N) \in \mathrm{Norm}(Q)$.

Proposition 4.4. *Let $\mathcal{V}$ be a variety of* 2*-divisible semimedial left quasigroups. The following are equivalent*

(*i*) *$\mathcal{V}$ is distributive*

(*ii*) *$Z(N) = 1$ for every $Q \in \mathcal{V}$ and every $N \in \mathrm{Norm}(Q)$.*

Proof. We are using the characterization of distributive varieties given in Proposition 4.3(*iii*).

(*i*) $\Rightarrow$ (*ii*). If $N \in \mathrm{Norm}(Q)$, then $Z(N) \in \mathrm{Norm}(Q)$ is solvable and so $Z(N) = 1$.

(*ii*) $\Rightarrow$ (*i*). If $Z(N) = 1$ for every $N \in \mathrm{Norm}(Q)$ then there are no abelian subgroups in $\mathrm{Norm}(Q)$. Since $[N, N] \in \mathrm{Norm}(Q)$ for every $N \in \mathrm{Norm}(Q)$ then there are no solvable subgroup in $\mathrm{Norm}(Q)$. $\square$

Corollary 4.5. *Let $\mathcal{V}$ be a distributive variety of semimedial left quasigroups. Then:*

(*i*) *$\mathcal{V}$ does not contain any non-trivial medial left quasigroup.*

(*ii*) *$\mathcal{V}$ does not contain any non-trivial finite* 2*-divisible latin left quasigroup.*

In particular, there is no distributive variety of medial left quasigroups.

Proof. The variety $\mathcal{V}$ omits solvable algebras. Medial left quasigroups are nilpotent [5, Corollary 4.4] and finite 2-divisible latin semimedial left quasigroups are solvable [5, Corollary 3.20]. $\square$

4.2. Mal'cev varieties of quandles

In this Section we focus on quandles. A remarkable construction of quandles is the following.

Example 4.6. (cf. [16]) Let G be a group, $f \in \mathrm{Aut}(G)$ and a subgroup $H \leqslant Fix(f) = \{a \in G : f(a) = a\}$. Let G/H be the set of left cosets of H and the multiplication defined by

$$aH * bH = af(a^{-1}b)H.$$

Then $\mathcal{Q}(G, H, f) = (G/H, *, \backslash)$ is a quandle, called a *coset* quandle. A coset quandle $\mathcal{Q}(G, H, f)$ is called *principal* if $H = 1$ and in such case it is denoted by $\mathcal{Q}(G, f)$. A principal quandle is called *affine* if G is abelian and in such case it is denoted by $\mathrm{Aff}(G, f)$.

Connected quandles can be represented as coset quandles over their displacement group.

Proposition 4.7. [14, Theorem 4.1] *Let Q be a connected quandle Q. Then Q is isomorphic to $\mathcal{Q}(\mathrm{Dis}(Q), \mathrm{Dis}(Q)_a, \widehat{L_a})$ for every $a \in Q$, where $\widehat{L}_a : \mathrm{Dis}(Q) \longrightarrow \mathrm{Dis}(Q)$ is defined by setting $x \mapsto L_a x L_a^{-1}$ for every $x \in \mathrm{Dis}(Q)$.*

The class of latin quandles is not a subvariety of the variety of quandles. Indeed the non-connected quandle $\mathrm{Aff}(\mathbb{Z}, -1)$ embeds into the latin quandle $\mathrm{Aff}(\mathbb{Q}, -1)$. On the other hand, the class of principal quandles of a Mal'cev variety is a subvariety.

Theorem 4.8. *The class of principal quandles of a Mal'cev variety $\mathcal{V}$ is a subvariety of $\mathcal{V}$.*

Proof. The product of principal quandles is principal [4, Corollary 2.3]. By virtue of [6, Proposition 2.11] subquandles and factors of principal Mal'cev quandles are principal. Hence the class of principal quandles of $\mathcal{V}$ is a subvariety. $\square$

`SmallQuandle`(28,i) for $i = 3, 4, 5, 6$ are the smallest examples of non-latin superconnected quandles in the [13] library of GAP. The identities in Table 1 provide Mal'cev varieties of quandles that contain such minimal examples.

Table 1: Examples of Mal'cev varieties of quandles

Identity	Witness in the RIG library
$L_x L_y^2 L_x L_y L_x^2 L_y L_x L_y^2(x) \approx y$	`SmallQuandle`(28,3)
$L_x^2 L_y L_x L_y^2 L_x L_y L_x^2 L_y^2(x) \approx y$	`SmallQuandle`(28,4)
$L_x L_y^2 L_x L_y L_x^2 L_y L_x L_y^2(x) \approx y$	`SmallQuandle`(28,5)
$L_x L_y^2 L_x L_y L_x^2 L_y L_x L_y^2(x) \approx y$	`SmallQuandle`(28,6)

Distributive varieties of quandles have the following characterization.

Theorem 4.9. *Let $\mathcal{V}$ be a variety of quandles. The following are equivalent:*

(i) $\mathcal{V}$ contains a non-trivial abelian quandle.

(ii) $\mathcal{V}$ has a non-trivial finite model.

In particular, $\mathcal{V}$ is distributive if and only if $\mathcal{V}$ has no non-trivial finite model.

Proof. $(i) \Rightarrow (ii)$. According to [4, Theorem 3.21] simple abelian quandles are finite. Let $Q \in \mathcal{V}$ be a non-trivial abelian quandle. According to the main result of [**?**], $\mathcal{V}(Q) \subseteq \mathcal{V}$ contains a simple abelian quandle which is finite.

$(ii) \Rightarrow (i)$. Let assume that $\mathcal{V}$ contains a non-trivial finite quandle Q. According to [4, Theorem 4.7], the minimal subquandles of Q with respect to inclusion are abelian.

The variety $\mathcal{V}$ is idempotent, and so it contains an abelian congruence if and only if it contains an abelian algebra. Thus, the last claim follows. $\square$

Corollary 4.10. *Let $\mathcal{V}$ be a distributive variety of semimedial left quasigroups and $Q \in \mathcal{V}$. If $E(Q)$ is finite then $|E(Q)| = 1$.*

Proof. According to Theorem 4.9 if $E(Q)$ is finite then $\mathcal{V}(E(Q))$ contains an abelian algebra. $\square$

Involutory quandles are the quandles that satisfy the identity $x(xy) \approx y$. A direct consequence of the contents of [6, Section 3] is that connected involutory quandles on two generators are finite, so we have the following Corollary of Theorem 4.9.

Corollary 4.11. *There is no distributive variety of involutory quandles.*

Acknowledgements. The first author would like to thank Professor David Stanovský for introducing him to the topic and Professor Paolo Aglianò for the useful discussions and remarks about the present paper.

References

[1] **L. Barto, M. Kozik, and D. Stanovský**, Mal'tsev conditions, lack of absorption, and solvability, Algebra Universalis, **74** (2015), 185–206.

[2] **C. Bergman**, *Universal algebra, Pure and Applied Mathematics (Boca Raton)*, Fundamentals and selected topics. CRC Press, Boca Raton, FL, **301**(2012). Fundamentals and selected topics.

[3] **M. Bodirski**, *Mal'cev condition figure*, https://www.math.tu-dresden.de/ bodirsky/Maltsev-Conditions/(2021).

[4] **M. Bonatto**, *Principal and doubly homogeneous quandles*, Monatshefte für Mathematik, **191** (2020), no. 4, 691–717.

[5] **M. Bonatto**, *Medial and semimedial left quasigroups*, J. Algebra, available as 10.1142/S0219498822500219 (2021).

[6] **M. Bonatto**, *Superconnected left quasigroups and involutory quandles*, arXiv e-prints (2021).

[7] **M. Bonatto and D. Stanovský**, *A universal algebraic approach to rack coverings*, arXiv:1910.09317 (2019).

[8] **M. Bonatto and D. Stanovský**, *Commutator theory for racks and quandles*, J. Math. Soc. Japan, **73** (2021), 41–75.

[9] **B. Csakany**, *Characterizations of regular varieties*, Acta Sci. Math. (Szeged), **31** (1970), 187–189.

[10] **A. Day**, *A characterization of modularity for congruence lattices of algebras*, Canad. Math. Bull., **12** (1969), 167–173.

[11] **R. Freese and R. McKenzie**, *Commutator theory for congruence modular varieties*, London Math. Soc. Lecture Note Series, Cambridge, **125** (1987).

[12] **D. Geiger**, *Coherent algebras*, Notices Amer. Math. Soc., **21** (1974).

[13] **M. Graña and L. Vendramin**, Rig, a GAP package for racks, quandles and Nichols algebras.

[14] **A. Hulpke, D. Stanovský, and P. Vojtěchovský**, *Connected quandles and transitive groups*, J. Pure Appl. Algebra, **220** (2016), no. 2, 735–758.

[15] **B. Jonnson**, *Algebras whose congruence lattices are distributive*, Math. Scandinav., **21** (1967), 110–121.

[16] **D. Joyce**, *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra, **23** (1982), no. 1, 37–65.

[17] **K.A. Kearnes and E.W. Kiss**, *The shape of congruence lattices*, Mem. Amer. Math. Soc., **222** (2013).

[18] **A.I. Mal'cev**, *On the general theory of algebraic systems*, Amer. Math. Soc. Transl. (2), **27** (1963), 125–142.

[19] **S.V. Matveev**, *Distributive groupoids in knot theory*, Mat. Sb. (N.S.), **119** (1982), no. 1, 78–88.

[20] **W. McCune**, Prover9 and mace4. `http://www.cs.unm.edu/~mccune/prover9/`, 2005–2010.

[21] **R. McKenzie and D. Hobby**, *The structure of finite algebras*, Contemporary Math., **76** (1988).

[22] **M. Olšák**, *The weakest nontrivial idempotent equations*, Bull. Lond. Math. Soc., **49** (2017), no. 6, 1028–1047.

[23] **M. Olšák**, *Maltsev conditions for general congruence meet-semidistributive algebras*, arXiv:1810.03178(2018).

[24] **A.F. Pixley**, *Distributivity and permutability of congruence relations in equational classes of algebras*, Proc. Amer. Math. Soc., **14** (1963), 105–109.

[25] **A.F. Pixley**, *Local Mal'cev conditions*, Canad. Math. Bull., **15** (1972), 559–1568.

[26] **W. Taylor**, *Uniformity of congruences*, Algebra Universalis, **4** (1974), 342–360.

[27] **W. Taylor**, *Varieties obeying homotopy laws*, Canad. J. Math., **29** (1977), no. 3, 498–527.

[28] **R. Wille**, *Kongruenzklassengeometrien*, Lecture Notes Math., Springer, **113** (1970).

Received March 25, 2021

M. Bonatto
Dipartimento di matematica e informatica - UNIFE
Ferrara, Italy
e-mail: marco.bonatto.87@gmail.com

S. Fioravanti
DIISM
Università degli Studi di Siena
Siena, Italy
e-mail: stefano.fioravanti66@gmail.com

Quasigroups and Related Systems **29** (2021), 193 − 208

Translatable isotopes of finite groups

Wieslaw A. Dudek and *Robert A. R. Monzo*

Abstract. We prove the main result, that if $(Q, *)$ is a k-translatable isotope of a finite group $(Q, \oplus)$ of order n then $(Q, \oplus)$ is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n. Given a k-translatable ordering of a left cancellative groupoid Q of order n, we determine all k-translatable orderings of Q. We also prove that a left-cancellative, k-translatable groupoid Q is translatable for a single value of k. Finally, we prove that a left (or right) linear isotope of $\mathbb{Z}_n$ is linear and we give examples of k-translatable isotopes of $\mathbb{Z}_4$ that are neither left nor right linear.

1. Introduction

We assume that all sets considered in this note are finite and have form $Q = \{1, 2, \ldots, n\}$ with the *natural ordering* $1, 2, \ldots, n$.

A groupoid $(Q, *)$ of order n is called *k-translatable*, where $1 \leqslant k < n$, if its Cayley table is obtained by the following rule: If the first row of the Cayley table is $a_1, a_2, \ldots, a_n$, then the q-th row is obtained from the $(q-1)$-st row by taking the last k entries in the $(q-1)-$st row and inserting them as the first k entries of the q-th row and by taking the first $n-k$ entries of the $(q-1)$-st 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 ordering $1, 2, \ldots, n$. A groupoid of order n is called *translatable* if it has a k-translatable sequence for some $k \in \{1, 2, \ldots, n-1\}$. A quasigroup of order n may be k-translatable only for k relatively prime to n. A group of order n is translatable if and only if it is cyclic. It is $(n-1)$-translatable.

It is important to note that a k-translatable sequence depends on the ordering of the elements in the Cayley table. A groupoid may be k-translatable for one ordering but not for another (see Example 2.4 below). Unless otherwise stated we will assume that the ordering of the Cayley table is $1, 2, \ldots, n$ and the first row of the table is $a_1, a_2, \ldots, a_n$.

The concept of translatability was first explored in [1] and [2]. It arose through the examination of the fine structure of quadratical quasigroups. Translatability determines the structure of certain types of quasigroups [3]. The question of when quadratical quasigroups, which are idempotent, are translatable was answered in [4] and [5]. There it was proved that a naturally ordered groupoid $(Q, *)$ is

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

idempotent and k-translatable if and only if for all $i, j \in Q$ there exist $a, b \in \mathbb{Z}_n$ such that $i*j = (ai+bj)(\bmod n)$, where $(a+b) = 1(\bmod n)$ and $(a+bk) = 0(\bmod n)$.

Now we are interested in the k-translatability of (α,β)-*isotopes* of a group $(Q,\oplus)$, i.e. quasigroups $(Q,*)$ with product $x * y = \alpha x \oplus \beta y$, where α, β are bijections of Q. We will prove our main result in Theorem 5.1, that if an isotope of a group $(Q,\oplus)$ is k-translatable then $(Q,\oplus)$ is isomorphic to the additive group $\mathbb{Z}_n$ of integers modulo n. Then, for a given a bijection α of $\mathbb{Z}_n$, for particular values of k and n we will determine all possible bijections β for which $(Q,*)$ is k-translatable.

2. Preliminaries

For simplicity instead of $i \equiv j(\bmod n)$ we will write $[i]_n = [j]_n$. Additionally, in calculations of modulo n, we assume that $0 = n$. Also the neutral element of a group $(Q,\oplus)$ will be denoted by 0. The inverse elements in $(Q,\oplus)$ and $\mathbb{Z}_n$ will be denoted by the same symbol; namely, as $-x$. The set $\{1, 2, \ldots, n\}$ will be denoted by $\overline{\{1,n\}}$. For $k \in \overline{\{1,n\}}$, $(k,n) = 1$ denotes that k and n are relatively prime.

With this convention a naturally ordered groupoid $(Q,*)$ is k-translatable if and only if $i * j = [i+1]_n * [j+k]_n$ for all $i, j \in Q$. Then $a_1, a_2, \ldots, a_n$, where $a_i = 1 * i$, is a k-translatable sequence.

We will need the following results proven in our previous publications.

Lemma 2.1. (cf. [4, Lemma 9.1]) *The quasigroup $(\mathbb{Z}_n,*)$ with the operation $i * j = [ai + c + bj]_n$, where $a, b, c \in \mathbb{Z}_n$ and $(a,n) = (b,n) = 1$ is k-translatable if and only if $[a+kb]_n = 0$.*

Lemma 2.2. (cf. [2, Lemma 2.5]) *Let $a_1, a_2, \ldots, a_n$ be the first row of the Cayley table of a quasigroup $(Q,*)$ of order n. Then $(Q,*)$ is k-translatable if and only if for all $i, j \in Q$ the following (equivalent) conditions are satisfied.*

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

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

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

Lemma 2.3. (cf. [2, Lemma 2.7]) *If a quasigroup $(Q,*)$ of order n is k-translatable with respect to the ordering $a_1, a_2, \ldots, a_n$ then it is k-translatable with respect to the ordering $a_n, a_1, a_2, \ldots, a_{n-1}$.*

Example 2.4. Consider the following tables:

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

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

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

These tables define the same quasigroup isomorphic to the additive group $\mathbb{Z}_4$. The first table shows that with respect to the natural ordering this quasigroup is 3-translatable. The second table is an example of Lemma 2.3. The third table shows that in another ordering this quasigroup is not translatable.

Lemma 2.5. *Let $(Q,*)$ be a k-translatable groupoid with respect to the natural ordering $1,2,\ldots,n$, with k-translatable sequence $a_1,a_2,\ldots,a_n$. Then $(Q,*)$ is k-translatable with respect to the ordering $n,n-1,\ldots,2,1$, with k-translatable sequence $a_k,a_{k-1},\ldots,a_1,a_n,a_{n-1},\ldots,a_{k+1}$.*

Proof. The ordering $n,n-1,n-2,\ldots,2,1$ can be expressed as $1',2',3',\ldots,n'$, where $i'=[1-i]_n$. Then, by Lemma 2.2(ii) we have $i'*j'=[1-i]_n*[1-j]_n=[(1-i)-1]_n*[(1-j)-k]_n=[-i]_n*[1-(j+k)]_n=(i+1)'*(j+k)'$. So, $1',2',\ldots,n'$ is a k-translatable ordering on $(Q,*)$. Since $n*j=a_{k-kn+j}=a_{k+j}$, this ordering has the k-translatable sequence $a_k,a_{k-1},\ldots,a_1,a_n,a_{n-1},\ldots,a_{k+1}$. □

Lemma 2.6. *Let $(Q,*)$ be a k-translatable groupoid with respect to the natural ordering with k-translatable sequence $a_1,a_2,\ldots,a_n$ and suppose that $(s,n)=1$. Then $(Q,*)$ is k-translatable with respect to the ordering $1,[1+s]_n,[1+2s]_n,\ldots,[1+(n-1)s]_n$ with k-translatable sequence $a_1,a_{1+s},a_{1+2s},\ldots,a_{1+(n-1)s}$.*

Proof. Since $(s,n)=1$, we can introduce the new ordering $1',2',\ldots,n'$ where $i'=[1+(i-1)s]_n$. Then, using Lemma 2.2(ii), we obtain $i'*j'=[1+(i-1)s]_n*[1+(j-1)s]_n=[(1+is)-s]_n*[(1+js)-s]_n=[1+is]_n*[(1+js)-s+ks]_n=[1+is]_n*[1+((j+k)-1)s]_n=(i+1)'*(j+k)'$. So, $1',2',\ldots,n'$ is a k-translatable ordering on $(Q,*)$. Since $1'*j'=1*[1+(j-1)s]_n=a_{[1+(j-1)s]_n}$ the corresponding k-translatable sequence for this order is $a_1,a_{1+s},a_{1+2s},\ldots,a_{1+(n-1)s}$. □

3. Translatable left cancellative groupoids

A groupoid $(Q,*)$ is *left cancellative* if for all $a,b,c\in Q$ $a*b=a*c$ implies $b=c$.

Note that if $a_1,a_2,\ldots,a_n$ is a k-translatable sequence of a left cancellative groupoid Q then for all $i\in\overline{\{1,n\}}$, $a_i=a_j$ if and only if $i=j$.

Definition 3.1. Let $Q=\{1,2,\ldots,n\}$ be a groupoid of order n, with $a_1,a_2,\ldots,a_n$ an ordering of Q. For $i\in\overline{\{1,n\}}$ we define the set A_i as the set consisting of the sequence $a_i,a_{i+1},\ldots,a_n,a_1,a_2,\ldots,a_{i-1}$ and B_j as the set consisting of the sequence $a_i,a_{i-1},\ldots,a_1,a_n,a_{n-1},\ldots,a_{i+1}$. Then we call $\bigcup(A_i\cup B_i)$, $i\in\overline{\{1,n\}}$, the *set of cyclic versions of the ordering* $a_1,a_2,\ldots,a_n$.

Note that by Lemmas 2.3 and 2.5, a cyclic version of a k-translatable ordering is k-translatable.

Henceforth, $-j'$ will denote $-(j')$ and not $(-j)'$. Similarly $[x]'_n$ denotes $([x]_n)'$.

Theorem 3.2. *Let a left cancellative groupoid* $(Q,*)$ *be* k*-translatable with respect to the natural ordering, with* k*-translatable sequence* $a_1, a_2, \ldots, a_n$*. Then an ordering is* k*-translatable on* $(Q,*)$ *if and only if it is a cyclic version of the ordering* $1, [1+s]_n, [1+2s]_n, \ldots, [1+(n-1)s]_n$ *for some* $s \in \overline{\{1,n\}}$*, where* $(s,n)=1$.

Proof. ($\Leftarrow$). This follows from Lemma 2.6 and the fact that a cyclic version of a k-translatable ordering is k-translatable.

($\Rightarrow$). By Lemma 2.2(ii) we can choose a k-translatable ordering $1', 2', \ldots, n'$ on $(Q,*)$, with $1'=1$ and with k-translatable sequence $a_1, a_2, \ldots, a_n$ say. Then, by Lemma 2.6(i), the first two rows of the multiplication table are as follows, with all subscripts of the entries being calculated modulo n.

	1	$2'$	$\ldots$	$(-k)'$	$(1-k)'$	$\ldots$	$(n-1)'$	n'
1	a_{1}	$a_{2'}$	$\ldots$	$a_{(-k)'}$	$a_{(1-k)'}$	$\ldots$	$a_{(n-1)'}$	$a_{n'}$
$2'$	$a_{k-k2'+1}$	$a_{k-k2'+2'}$	$\ldots$	$a_{k-k2'+(-k)'}$	$a_{k-k2'+(1-k)'}$	$\ldots$	$a_{k-k2'+(n-1)'}$	$a_{k-k2'+n'}$

Then, since the groupoid $(Q,*)$ is left cancellative and k-translatable, modulo n we have $k-k2' = (1-k)'-1 = (2-k)'-2' = \ldots = (n-1)'-(k-1)' = n'-k' = 1-(k+1)' = 2'-(k+2)' = \ldots = (-1-k)'-(n-1)' = (-k)'-n'$, which implies the following n identities:

$$
\begin{array}{cl}
(1) & (1-k)'-1 = (2-k)'-2' \\
(2) & (2-k)'-2' = (3-k)'-3' \\
\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
(k) & n'-k' = 1-(k+1)' \\
(k+1) & 1-(k+1)' = 2'-(k+2)' \\
(k+2) & 2'-(k+2)' = 3'-(k+3)' \\
\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
(n-1) & (-1-k)'-(n-1)' = (-k)'-n' \\
(n) & (-k)'-n' = (1-k)'-1.
\end{array}
$$

We note that in any one of these n identities

(A) If j' is the first term on the left-hand side of the identity then $(j+1)'$ is the first term on the right-hand side of that identity.

(B) If $-(j')$ is the second term on the left-hand side of the identity then $-(j+1)'$ is the first term on the right-hand side of that identity.

(C) If j' is the first term on the left (right)-hand side of the identity the second term on the left (right)-hand side of the identity is $-(j+k)'$.

It follows that for all $j = 1, 2, \ldots, n$,

(D) $j'-(j+k)' = (j+1)'-(j+1+k)'$.

Now $n'-1 \overset{(k)}{=} k'-(k+1)'$. But (D) implies $k'-(2k)'=(k+1)'-(2k+1)'$. So, $k'-(k+1)'=(2k)'-(2k+1)'$ and $n'-1=k'-(k+1)'=(2k)'-(2k+1)'$. Continuing in this manner we get $n'-1=k'-(k+1)'=(2k)'-(2k+1)'=(3k)'-(3k+1)'=\ldots=(-2k)'-(-2k+1)'=(-k)'-(1-k)'$.

Since $(k,n)=1$, the elements $k',(2k)',\ldots,(-2k)',(-k)'$ are all different. Therefore $n'-1=1-2'=2'-3'=\ldots=(n-1)'-n'$ and this implies $j'=(j+1)'+n'-1$. Hence, $j'=1+(1-j)(n'-1)$, $(n'-1,n)=1$ and $1',2',3',\ldots,n'$ is the order $1,1-(n'-1),1-2(n'-1),\ldots,1-(n-1)(n'-1)$, a cyclic version of which returns us to the original k-translatable ordering, as required. □

Theorem 3.3. *If a left cancellative groupoid $(Q,*)$ is k-translatable then it is k-translatable for a single value of k.*

Proof. Suppose that $1,2,3,\ldots,n$ is a k-translatable ordering on $(Q,*)$, with k-translatable sequence $a_1,a_2,a_3,\ldots,a_n$ and that $1',2',3',\ldots,n'$ is a k^*-translatable ordering on $(Q,*)$, with the k^*-translatable sequence $b_1,b_2,b_3,\ldots,b_n$. By Lemma 2.5, there is a k^*-translatable ordering $1'',2'',3'',\ldots,n''$ with a k^*-translatable sequence $c_1,c_2,c_3,\ldots,c_n$ and with $1''=1$. Then, $1*j''=a_{k-k+j''}=c_{k^*-k^*+j''}$. Therefore, $a_j=c_j$ for all $j\in\overline{\{1,n\}}$. Then, $2*n=a_{[k-2k+n]_n}=c_{[k^*-2k^*+n]_n}=a_{[k^*-2k^*+n]_n}$ and, since $(Q,*)$ is left cancellative, $-k=-(k^*)$ and $k=k^*$, completing the proof. □

Note that the condition of left cancellation is necessary in the previous theorem. For example, a constant groupoid of order $n>1$ is k-translatable for all $k=1,2,\ldots,n-1$. Similarly, the groupoid $(Q,*)$ of order $2m$, with $x*y=1$ for all odd y and $x*y=2$ for all even y, is $2k$-translatable for every $k=1,\ldots,m-1$.

4. Translatable T-quasigroups

A quasigroup $(Q,*)$ is called a *T-quasigroup* if there exist an abelian group $(Q,\oplus)$ and its automorphisms φ,ψ such that $x*y=\varphi(x)\oplus\psi(y)\oplus c$ for all $x,y\in Q$ and some fixed $c\in Q$. Obviously, each T-quasigroup induced by $(Q,\oplus)$ is (α,β)-isotope of $(Q,\oplus)$.

By the Toyoda theorem (cf. for example [6] or [7]) a quasigroup $(Q,*)$ is medial if and only if it is a T-quasigroup with $\varphi\psi=\psi\varphi$.

Theorem 4.1. *A translatable T-quasigroup $(Q,*)$ of order n is isomorphic to a translatable medial quasigroup induced by the group $\mathbb{Z}_n$.*

Proof. Let $(Q,*)$ be a finite quasigroup of order n induced by the group $(Q,+)$, Then $x*y=\varphi(x)+\psi(y)+c$ for some fixed $c\in Q$ and automorphisms φ,ψ of $(Q,+)$. Denote the k-translatable ordering of Q by $1,2,3,\ldots,n$. By Lemma 2.2(*ii*), $(Q,*)$ is k-translatable $(1\leqslant k<n)$ with respect to the ordering $1,2,\ldots,n$

if and only if $\varphi(i)+\psi(j)+c = i*j = [i+1]_n*[j+k]_n = \varphi([i+1]_n)+\psi([j+k]_n)+c$, i.e. if and only if $\varphi(i)+\psi(j) = \varphi([i+1]_n)+\psi([j+k]_n)$ for all $i,j \in \{1,2,\ldots,n\}$.

By Lemma 2.3, we can choose the ordering such that the group element in the n-th position in this ordering is 0, the identity element of $(Q,+)$. We define $t_i = \overline{i}-\overline{1}$, where $\overline{i}$ is the group element of $(Q,+)$ located in the i^{th} position of the ordering $1,2,\ldots,n$. Note that $t_1 = 0$ and $t_n = -\overline{1}$. Then, $\varphi(i)+\psi(j) = \varphi([i+1]_n)+\psi([j+k]_n) \Leftrightarrow \varphi(\overline{i})+\psi(\overline{j}) = \varphi(\overline{[i+1]_n})+\psi(\overline{[j+k]_n}) \Leftrightarrow \psi(\overline{j}-\overline{[j+k]_n}) = \varphi(\overline{[i+1]_n}-\overline{i}) \Leftrightarrow \psi((\overline{1}+t_j)-(\overline{1}+t_{[j+k]_n})) = \varphi((\overline{1}+t_{[i+1]_n})-(\overline{1}-t_i)) \Leftrightarrow \psi(t_j-t_{[j+k]_n}) = \varphi(t_{[i+1]_n}-t_i)$ for all $i,j \in \overline{\{1,n\}}$.

For $j=1$ and $i \in \overline{\{1,n\}}$, $\psi(-t_{[1+k]_n}) = \varphi(t_{[i+1]_n}-t_i)$. So, $\psi(-t_{[1+k]_n}) = \varphi(t_{[s+1]_n}-t_s)$ for all $s \in \overline{\{1,n\}}$. Hence, $t_n-t_{n-1} = t_{n-1}-t_{n-2} = \ldots = t_2-t_1 = t_1-t_n = 0-(-\overline{1}) = \overline{1}$. Thus, $t_2 = \overline{1}$, $t_i = (i-1)\overline{1}$ and $\overline{i} = i\overline{1}$. This means that $\overline{1}$ generates the group $(Q,+)$ and so $(Q,+)$ is a cyclic group isomorphic to $\mathbb{Z}_n$. Hence, by Lemma 2.1, $(Q,*)$ is isomorphic to a translatable medial quasigroup $i \diamond j = [ai+bj+c]_n$, where $(a,n) = 1 = (b,n)$ and $[a+bk]_n = 0$. □

Corollary 4.2. *A medial quasigroup of order n is translatable if and only if it is induced by a group isomorphic to the additive group $\mathbb{Z}_n$.*

Proof. The necessity follows from Theorem 4.1. To prove the sufficiency observe that a medial quasigroup of order n induced by the group $\mathbb{Z}_n$ has the form $x*y = [ax+by+c]_n$, where $a,b,c \in \mathbb{Z}_n$ and $(a,n) = (b,n) = 1$. By Lemma 2.1 this quasigroup is k-translatable if and only if $[a+bk]_n = 0$. This equation is always uniquely solvable with $k = [-a\overline{b}\,]_n$, where $[b\overline{b}\,]_n = 1$. □

5. Translatability of isotopes of a finite group

Theorem 5.1. *If an (α,β)-isotope $(Q,*)$ of a group $(Q,\oplus)$ of order n is k-translatable then there is an ordering $1,2,\ldots,n$ on Q such that for some $s \in \overline{\{1,n\}}$ and all $i,j \in \overline{\{1,n\}}$*

(i) $\alpha n = 0 = \beta s$,

(ii) $\alpha[i+1]_n = \alpha i \oplus \alpha 1$,

(iii) $\alpha i = \underbrace{\alpha 1 \oplus \alpha 1 \oplus \ldots \oplus \alpha 1}_{i\ times} = i(\alpha 1)$,

(iv) *$(Q,\oplus)$ is isomorphic to the group $\mathbb{Z}_n$,*

(v) $\beta[j+k]_n = \beta j - \alpha 1$ *and* $\beta[s+jk]_n = j(-\alpha 1)$.

Proof. From Lemma 2.3, there is a k-translatable ordering $1,2,\ldots,n$ on Q such that $\alpha n = 0$ and, since β is a bijection, $\beta s = 0$ for some $s \in Q$.

Then, using k-translatability and Lemma 2.2(ii), $0 = n * s = 1 * [s+k]_n = \alpha 1 \oplus \beta[s+k]_n$. Hence, $\beta[s+k]_n = -\alpha 1$.

Thus, $\alpha i = \alpha i \oplus 0 = i * s = [i+1]_n * [s+k]_n = \alpha[i+1]_n \oplus \beta[s+k]_n = \alpha[i+1]_n - \alpha 1$, which implies

$$\alpha[i+1]_n = \alpha i \oplus \alpha 1. \tag{1}$$

Then, by induction on i, it is easy to prove that for all $i \in \overline{\{1,n\}}$, $\alpha i = \alpha 1 \oplus \alpha 1 \oplus \ldots \oplus \alpha 1$, (with i number of summands). Consequently, $\alpha i \oplus \alpha j = \alpha[i+j]_n$. We then define a bijection $\varphi : Q \to \mathbb{Z}_n$ as $\varphi \alpha i = i$ and so, we have $\varphi(\alpha i \oplus \alpha j) = \varphi(\alpha[i+j]_n) = [i+j]_n = [\varphi\alpha i + \varphi\beta j]_n$. Hence, φ is an isomorphism.

Finally, $\beta j = 0 \oplus \beta j = n * j = 1 * [j+k]_n = \alpha 1 \oplus \beta[j+k]_n$ and, since the groups $(Q, \oplus)$ and $(\mathbb{Z}, +)$ are isomorphic, the operation $\oplus$ is commutative, for all $j \in \overline{\{1,n\}}$ we have $\beta[j+k]_n = \beta j - \alpha 1$. By induction on j it is then easy to prove that for all $j \in \overline{\{1,n\}}$, $\beta[s+jk]_n = -\alpha 1 - \alpha 1 - \ldots - \alpha 1$ (j times). □

Proposition 5.2. *If an (α,β)-isotope $(Q,*)$ of the commutative group $(Q,\oplus)$ satisfies (ii) and (v) of Theorem* 5.1*, then it is k-translatable.*

Proof. $[i+1]_n * [j+k]_n = \alpha[i+1]_n \oplus \beta[j+k]_n \overset{(ii),(v)}{=} \alpha i \oplus \alpha 1 \oplus \beta j - \alpha 1 = \alpha i \oplus \beta j = i * j$, for all $i, j \in \overline{\{1,n\}}$. By Lemma 2.2($ii$), $(Q,*)$ is k-translatable. □

The following Corollary follows readily from Theorem 5.1 and Proposition 5.2. The proof is omitted.

Corollary 5.3. *The quasigroup $(\mathbb{Z}_n, *)$ with $i * j = [\alpha i + \beta j]_n$, where α, β are bijections of $\mathbb{Z}_n$ is k-translatable for some k if and only if there is an ordering $1', 2', \ldots, n'$ of $\mathbb{Z}_n$ such that for some $s \in \overline{\{1,n\}}$ and all $i \in \overline{\{1,n\}}$*

(i) $\alpha n' = 0 = \beta s'$,

(ii) $\alpha([i+1]'_n) = [\alpha i' + \alpha 1']_n$,

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

(iv) $\beta([i+k]'_n) = \beta i' - \alpha 1'$ *and* $\beta([s+ik]'_n) = [i(-\alpha 1')]_n$,

(v) $(\alpha 1', n) = 1$.

Corollary 5.4. *For a given ordering on $\mathbb{Z}_n$ and any $k, t \in \overline{\{1,n\}}$ such that $(k,n) = (t,n) = 1$ there are bijections α_t and β_s ($s \in \overline{\{1,n\}}$) on $\mathbb{Z}_n$ such that the quasigroup $(\mathbb{Z}_n, *_s)$ defined by $i *_s j = [\alpha_t i + \beta_s y]_n$ is k-translatable with respect to this ordering.*

Proof. Suppose that $1', 2', \ldots, n'$ is a fixed ordering on $\mathbb{Z}_n$ and that $k, t \in \overline{\{1,n\}}$ be such that $(k,n) = (t,n) = 1$. Then, we define the bijection α_t on $\mathbb{Z}_n$ by putting $\alpha_t i' = [it]_n$ for any $i \in \overline{\{1,n\}}$. It is easy to see that $\alpha_t[i+t]'_n = [\alpha_t i' + t]_n$ for any $i \in \overline{\{1,n\}}$. Now for any $s \in \overline{\{1,n\}}$ we define the bijection β_s by putting $\beta_s[s+ik]_n = [-it]_n$ for any $i \in \overline{\{1,n\}}$. Since $(k,n) = 1$, we have $\{1, 2, \ldots, n\} =$

$\{[s+k]_n, [s+2k]_n, \ldots, [s+nk]_n = s\}$. It follows that $\beta_s([i+k]'_n) = [\beta_s i' - t]_n$ for any $i \in \overline{\{1,n\}}$. Then $[i+1]'_n *_s [j+k]'_n = [\alpha_t([i+1]'_n) + \beta_s([j+k]'_n)]_n = [\alpha_t i' + t + \beta_s j' - t]_n = [\alpha_t i' + \beta_s j']_n = i' *_s j'$. So, by Lemma 2.2($ii$). $(\mathbb{Z}_n, *_s)$ is k-translatable with respect to this ordering. □

Note that, as a result of Theorem 5.1 and Corollary 5.4, a finite group of order n is isomorphic to $\mathbb{Z}_n$ if and only if it has a k-translatable isotope for some $k \in \overline{\{1, n-1\}}$. In fact, a finite group of order n either has no k-translatable isotope or it has k-translatable isotopes for all values of $k \in \overline{\{1, n-1\}}$.

Example 5.5. Let $n = 8$. Then $(t, 8) = 1$ for $t \in \{1,3,5,7\}$. Then for $t = 5$, $s = 1$, $k = 3$ and the given ordering $4,6,1,3,2,8,5,7$ we see that $\alpha_5 = (1,7,8,6,2)(3,4,5)$ and $\beta_1 = (1,2,4,8,5,6)(3)(7)$. The Cayley table of $i' *_1 j' = [\alpha_5 i' + \beta_1 j']_8$ follows.

$*_1$	4	6	1	3	2	8	5	7
$1' = 4$	5	6	7	8	1	2	3	4
$2' = 6$	2	3	4	5	6	7	8	1
$3' = 1$	7	8	1	2	3	4	5	6
$4' = 3$	4	5	6	7	8	1	2	3
$5' = 2$	1	2	3	4	5	6	7	8
$6' = 8$	6	7	8	1	2	3	4	5
$7' = 5$	3	4	5	6	7	8	1	2
$8' = 7$	8	1	2	3	4	5	6	7

Example 5.6. For $t = 5$ we want to determine all the k-translatable quasigroups $(\mathbb{Z}_8 .*)$ of the form $i * j = [\alpha i + \beta j]_8$, where α is an automorphism of the group $\mathbb{Z}_8$. Such automorphisms are of the form $\alpha i = [mi]_8$, where $m \in \{1,3,5,7\}$. Then $\alpha_5 1' = 5$, $\alpha_5 2' = 2$, $\alpha_5 3' = 7$, $\alpha_5 4' = 4$, $\alpha_5 5' = 1$, $\alpha_5 6' = 6$, $\alpha_5 7' = 3$, $\alpha_5 8' = 8$.

Now let $\alpha = \alpha_5$ be an automorphism of $\mathbb{Z}_8$. If $\alpha i = 1i = i$, then $i' = 5i$. If $\alpha i = 3i$, then $i' = 7i$. If $\alpha i = 5i$, then $i' = i$. If $\alpha i = 7i$, then $i' = 3i$. These automorphisms, respectively, give the following orderings: $\alpha i = i$ gives the ordering $5,2,7,4,1,6,3,8$; $\alpha i = 3i$ gives the ordering $7,6,5,4,3,2,1,8$; $\alpha i = 5i$ gives $1,2,3,4,5,6,7,8$; $\alpha i = 7x$ gives $3,6,1,4,7,2,5,8$.

By Corollary 5.4, for each $s \in \{1,2,\ldots,8\}$ and each $k \in \{1,3,5,7\}$ we can calculate β_s. It turns out that β_s is an automorphism of $\mathbb{Z}_8$ if and only if $s = 8$ (as long as α is an automorphism of $\mathbb{Z}_8$). These calculations give: for $\alpha_5 i = i$ and $k = 1$, $\beta_8 i = 7i$; for $\alpha_5 i = 3i$ and $k = 1$, $\beta_8 i = 5i$; for $\alpha_5 i = 5x$ and $k = 1$, $\beta_8 i = 3i$ and for $\alpha_5 i = 7i$ and $k = 1$, $\beta_8 i = i$, which matches Lemma 2.1.

For $s \neq 8$, $i *_s j = [\alpha_t i + \beta_s j]_n$ is a 1-translatable, left linear quasigroup. For example, in the case when $\alpha_5 i = i$, $k = 1$, the ordering $5,2,7,4,1,6,3,8$ and $s = 1$, $\beta_1 = (1,4)(2,3)(5,8)(6,7)$ is not an automorphism of $\mathbb{Z}_8$. This quasigroup has the following Cayley table that is clearly 1-translatable. It has a right neutral element; namely, 5, and it is unipotent.

$*_1$	5	2	7	4	1	6	3	8
5	5	8	3	6	1	4	7	2
2	2	5	8	3	6	1	4	7
7	7	2	5	8	3	6	1	4
4	4	7	2	5	8	3	6	1
1	1	4	7	2	5	8	3	6
6	6	1	4	7	2	5	8	3
3	3	6	1	4	7	2	5	8
8	8	3	6	1	4	7	2	5

An (α,β)-isotope $(Q,*)$ of the group $(Q,\oplus)$ is *left* (*right*) *linear* over $(Q,\oplus)$ if α (respectively, β) is an automorphism of $(Q,\oplus)$. If an (α,β)-isotope can be written as $x*y=\hat{\alpha}x\oplus c\oplus\hat{\beta}y$ for automorphisms $\hat{\alpha},\hat{\beta}$ of $(Q,\oplus)$ and some $c\in Q$, then the quasigroup $(Q,*)$ is called *linear* over $(Q,\oplus)$.

The following Theorem finds all k-translatable quasigroups that are left linear over $\mathbb{Z}_n$.

Theorem 5.7. *If an (α,β)-isotope $(\mathbb{Z}_n,*)$ of the group $\mathbb{Z}_n$ is left linear over $\mathbb{Z}_n$, then it is k-translatable if and only if there exist $m,s,t\in\overline{\{1,n\}}$ such that $(t,n)=1=(m,n)$ and $\beta_s j=[\overline{k}(st-mj)]_n$ for all $j\in\overline{\{1,n\}}$, where $\alpha i=[mi]_n$ and $[\overline{k}k]_n=1$.*

Proof. ($\Rightarrow$): Since α is an automorphism of the group $\mathbb{Z}_n$, $\alpha i=[mi]_n$ for some $(m,n)=1$. Using Corollary 5.3, there exists an ordering $1',2',\ldots,n'$ on $\mathbb{Z}_n$ and $s\in\overline{\{1,n\}}$ such that $\alpha n'=0=\beta s'$ and, for all $i\in\overline{\{1,n\}}$, $\alpha i'=[i(\alpha 1')]_n$, $(\alpha 1',n)=1$ and $\beta_s([s+ik]'_n)=-[i(\alpha 1')]_n$. Thus for $t=\alpha 1'$ we obtain $[mi']_n=\alpha i'=[i(\alpha 1')]_n=[it]_n$. Hence, for $(m,\overline{m})=1$ $i'=[\overline{m}ti]_n$ and $[s+ik]'_n=[\overline{m}t(s+ik)]_n=[\overline{m}ts+\overline{m}tki]_n$. Therefore, $-[it]_n=$ $beta_s([s+ik]'_n)=\beta_s[\overline{m}ts+\overline{m}tki]_n$. This for $i=[-\overline{k}s+\overline{k}\overline{t}mj]_n$ gives $\beta_s j=[-(-\overline{k}s+\overline{k}\overline{t}mj)t]_n=[\overline{k}(st-mj)]_n$.

($\Leftarrow$): For all $i,j\in\mathbb{Z}_n$, $[i+1]_n*[j+k]_n=[mi+m+\overline{k}(st-m(j+k))]_n=[mi+m+\overline{k}(st-mj)-m]_n=[mi+\overline{k}(st-mj)]_n=i*j$. So, k-translatability follows from Lemma 2.2(ii). □

Theorem 5.8. *If a k-translatable quasigroup $(Q,*)$ is an (α,β)-isotope of the group $(Q,\oplus)$, then there is an ordering $1,2,\ldots,n$ on Q such that*

(i) $\alpha s=0=\beta n$ *for some* $s\in\overline{\{1,n\}}$,

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

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

(iv) $(Q,\oplus)$ *is isomorphic to* $(\mathbb{Z}_n,+)$,

(v) $\beta[jk]_n=j(-\alpha[s+1]_n)$ *for all* $j\in\overline{\{1,n\}}$.

Proof. From Lemma 2.3, there is a k-translatable sequence $1, 2, \ldots, n$ on Q such that $\beta n = 0$ and, since α is a bijection, $\alpha s = 0$ for some $s \in \overline{\{1, n\}}$. Then, using k-translatability and Lemma 2.2, $0 = s * n = [s+1]_n * k = \alpha[s+1]_n \oplus \beta k$. Hence,

$$\beta k = -\alpha[s+1]_n. \tag{2}$$

Also, $\alpha i = i * n = [i+1]_n * k = \alpha[i+1]_n \oplus \beta k = \alpha[i+1]_n - \alpha[s+1]_n$, which implies $\alpha[i+1]_n = \alpha i \oplus \alpha[s+1]_n$. This proves (ii). Then, by induction on i, we can prove (iii).

Now, $\beta j = s * j = [s+1]_n * [j+k]_n = \alpha[s+1]_n \oplus \beta[j+k]_n$. Therefore $\alpha[s+1]_n = \beta j - \beta[j+k]_n$, which together with (2) implies $\beta j - \beta[j+k]_n = -\beta k$. From this, by induction, we obtain $\beta[jk]_n = \beta k \oplus \beta k \oplus \ldots \oplus \beta k$ (with j number of summands). This, by (2), proves (v).

Since α is a bijection $Q = \{\alpha[s+i]_n : i \in \overline{\{1, n\}}\}$. So we can define a bijection $\varphi : Q \to \mathbb{Z}_n$ as $\varphi\alpha[s+i]_n = i$. Then we have $\varphi(\alpha[s+i]_n \oplus \alpha[s+j]_n) = \varphi(i\alpha[s+1]_n \oplus j\alpha[s+1]_n) = \varphi([i+j]_n\alpha[s+1]_n) = \varphi\alpha[s+[i+j]_n]_n = [i+j]_n = [\varphi\alpha[s+i]_n + \varphi\alpha[s+j]_n]_n$. Hence, φ is an isomorphism between $(Q, \oplus)$ and $(\mathbb{Z}_n, +)$. This completes the proof of Theorem 5.8. □

Proposition 5.9. *If an (α, β)-isotope of the commutative group $(Q, \oplus)$ satisfies (ii), (iii) and (v) of Theorem 5.8 then it is a k-translatable quasigroup.*

Proof. Suppose that $i, j \in Q$. By (ii), (iii) and (v) of Theorem 5.8 we see that $Q = \{i\alpha[s+1]_n : i \in \overline{\{1, n\}}\} = \{[ik]_n : i \in \overline{\{1, n\}}\}$ and so $j = [\hat{j}k]_n$ for some $\hat{j} \in \overline{\{1, n\}}$. Then, $[i+1]_n * [j+k]_n = \alpha[i+1]_n \oplus \beta[(\hat{j}+1)k]_n = \alpha i \oplus \alpha[s+1]_n \oplus [\hat{j}+1]_n(-\alpha[s+1]_n) = \alpha i \oplus \hat{j}(-\alpha[s+1]_n) = \alpha i \oplus \beta[\hat{j}k]_n = \alpha i \oplus \beta j = i * j$ and k-translatability follows from Lemma 2.2. □

The following Corollary follows directly from Theorem 5.8.

Corollary 5.10. *An (α, β)-isotope of the group $\mathbb{Z}_n$ is k-translatable if and only if there is an ordering $1', 2', \ldots, n'$ on $\mathbb{Z}_n$ such that for some $s \in \overline{\{1, n\}}$ and all $i \in \overline{\{1, n\}}$*

(i) $\alpha s' = n = \beta n'$,

(ii) $(\alpha([s+1]'_n), n) = 1$,

(iii) $\alpha([i+1]'_n) = \alpha i' + \alpha([s+1]'_n)$,

(iv) $(\alpha([s+i]'_n) = i\alpha([s+1]'_n)$,

(v) $\beta([ik]'_n) = -i\alpha([s+1]'_n)$.

Theorem 5.11. *If an (α, β)-isotope $(\mathbb{Z}_n, *)$ of the group $\mathbb{Z}_n$ is right linear over $\mathbb{Z}_n$, then it is k-translatable if and only if there exist $m, s.t \in \overline{\{1, n\}}$ such that $(t, n) = 1 = (m, n)$ and $\alpha i = [-st - mki]_n$ for all $i \in \overline{\{1, n\}}$, where $\beta j = [mj]_n$.*

Proof. ($\Rightarrow$): Since β is an automorphism of the group $\mathbb{Z}_n$, $\beta j = [mj]_n$ for some $(m,n) = 1$. Using Corollary 5.10(ii) with $t = \alpha([s+1]'_n)$ and $\alpha s' = n$, for all $i \in \overline{\{1,n\}}$ we have $[m([ik]'_n)]_n = [-it]_n$ and so $[i']_n = -[\overline{m}\overline{k}it]_n$, where $[\overline{m}m]_n = 1$. By Corollary 5.10(iv), $[jt]_n = \alpha([\overline{m}\overline{k}t(s+j)]_n$, which for $j = [-s - mk\overline{t}i]_n$ gives $\alpha i = [-st - mki]_n$.

($\Leftarrow$): For all $i,j \in \overline{\{1,n\}}$ we have $[i+1]_n * [j+k]_n = [-st - mki + mj]_n = [\alpha i + \beta j]_n = i * j$. Therefore, by Lemma 2.2(ii), $(\mathbb{Z}_n, *)$ is k-translatable. □

Corollary 5.12. *For any ordering $1', 2', \ldots, n'$ on $\mathbb{Z}_n$ and any $k, t \in \overline{\{1,n\}}$ such that $(k,n) = (t,n) = 1$ there is a bijection β_t on $\mathbb{Z}_n$ and bijections α_s, $s \in \overline{\{1,n\}}$, such that the quasigroups $(\mathbb{Z}_n, *_s)$ defined by $i *_s j = [\alpha_s i + \beta_t j]_n$ are k-translatable with respect to this ordering.*

Proof. Suppose that $1', 2', \ldots, n'$ is an order on $\mathbb{Z}_n$ and that $k, t \in \overline{\{1,n\}}$, with $(k,n) = 1 = (t,n)$. Then, we define $\alpha_s([s+i]'_n) = [it]_n$. It follows that for all $i \in \overline{\{1,n\}}$, $\alpha([i+1]'_n) = [\alpha i' + t]_n$. Then, we define $\beta_t([ik]'_n) = [-it]_n$. It follows that for all $i \in \overline{\{1,n\}}$, $\beta_t[j+k]'_n = [\beta_t j' - t]_n$. Then, $[i+1]'_n *_s [j+k]'_n = [\alpha_s([i+1]'_n) + \beta_t([j+k]'_n)]_n = [\alpha_s i' + t + \beta_t j - t]_n = i' *_s j'$. The required result then follows from Lemma 2.2(ii). □

Theorem 5.13. *A k-translatable quasigroup left or right linear over $\mathbb{Z}_n$ is medial and linear over $\mathbb{Z}_n$. If $[k^2]_n = 1$ then it is also paramedial.*

Proof. By Theorem 5.7 a k-translatable quasigroup left linear over $\mathbb{Z}_n$ has the operation $i * j = [\alpha i + \overline{k}st + \delta j]_n$, where $\alpha i = [mi]_n$ and $\delta j = [-\overline{k}mj]_n$. A k-translatable quasigroup right linear over $\mathbb{Z}_n$ has, by Theorem 5.11, the operation $i * j = [\gamma i - st + \beta j]_n$, where $\gamma i = [-mki]_n$ and $\beta j = [mj]_n$. Since $(k,n) = (m,n) = 1$, $\alpha, \beta, \delta, \gamma$ are automorphisms of the group $\mathbb{Z}_n$. If $[k^2]_n = 1$ then $\alpha^2 = \delta^2$ and $\gamma^2 = \beta^2$. This means (cf. [6, Theorem 9]) that this quasigroup is paramedial. □

We have seen in Theorem 5.13 that k-translatable left linear and k-translatable right linear quasigroups over $\mathbb{Z}_n$ are linear. This leads to the question of whether there are k-translatable isotopes over $\mathbb{Z}_n$ of the form $x * y = [\alpha x + \beta y]_n$ where both α and β are not automorphisms of $\mathbb{Z}_n$ and $(\mathbb{Z}_n, *)$ cannot be written as $x * y = [\hat{\alpha} x + c + \hat{\beta} y]_n$, where either $\hat{\alpha}$ or $\hat{\beta}$ are automorphisms of $\mathbb{Z}_n$. (That is, the k-translatable quasigroup $(\mathbb{Z}_n, *)$ has no representation as a linear, k-translatable quasigroup over $\mathbb{Z}_n$.) In fact, there are many such k-translatable quasigroups over $\mathbb{Z}_4$, as we show in the example below.

The proofs of Theorem 5.14 and Corollary 5.15 are similar to the proofs of Theorems 5.1 and 5.8 and Corollaries 5.3 and 5.10 and are therefore omitted. Corollary 5.15 will be applied to give the examples just referred to in the preceding paragraph.

Theorem 5.14. *If an (α, β)-isotope $(Q, *)$ of a group $(Q, \oplus)$ of order n is k-translatable then there is an ordering $1, 2, \ldots, n$ on Q such that for some $r, s \in \overline{\{1,n\}}$ and all $i, j \in \overline{\{1,n\}}$*

(*i*) $\alpha r = 0 = \beta s$,

(*ii*) $\alpha[i+1]_n = \alpha i \oplus \alpha[r+1]_n$,

(*iii*) $\alpha[r+i]_n = \underbrace{\alpha[r+1]_n \oplus \alpha[r+1]_n \oplus \ldots \oplus \alpha[r+1]_n}_{i\ times} = i(\alpha[r+1]_n)$,

(*iv*) $(Q, \oplus)$ *is isomorphic to the group* $\mathbb{Z}_n$,

(*v*) $\beta[j+k]_n = \beta j \oplus \beta[s+k]_n$ *and* $\beta[s+jk]_n = j(-\alpha[r+1]_n)$.

Corollary 5.15. *An* (α,β)*-isotope of the group* $\mathbb{Z}_n$ *is* k*-translatable for some* k *if and only if there is an ordering* $1', 2', \ldots, n'$ *of* $\mathbb{Z}_n$ *such that for some* $r, s \in \overline{\{1,n\}}$ *and all* $i \in \overline{\{1,n\}}$

(*i*) $\alpha r' = n = \beta s'$,

(*ii*) $\alpha([i+1]'_n) = [\alpha i' + \alpha([r+1]'_n)]_n$,

(*iii*) $\alpha([r+i]'_n) = [i\alpha([r+1])'_n]_n$,

(*iv*) $\beta([i+k]'_n) = [\beta i' + \beta([s+k]'_n)]_n$ *and* $\beta([s+ik]'_n) = [i(-\alpha([r+1]'_n)]_n$,

(*v*) $(\alpha([r+1]'_n), n) = 1$.

Theorem 5.16. *If an* (α,β)*-isotope of the group* $\mathbb{Z}_n$ *is* $(n-1)$*-translatable for some ordering* $1', 2', \ldots, n'$ *with* $\beta s' = n$*, then* $\beta i' = [\alpha i' - \alpha s']_n$ *for all* $i \in \overline{\{1,n\}}$.

Proof. An $(n-1)$-translatable quasigroup of order n is commutative. Hence in an $(n-1)$-translatable (α,β)-isotope of the group $\mathbb{Z}_n$ we have $[\alpha i + \beta j]_n = [\alpha j + \beta j]_n$. In particular, $\alpha i' = [\alpha i' + \beta s']_n = [\alpha s' + \beta i']_n$. So, $\beta i' = [\alpha i' - \alpha s']_n$. □

6. 3-translatable isotopes of $\mathbb{Z}_4$

We proceed to calculate the 3-translatable (α,β)-isotopes of the group $\mathbb{Z}_4$. By Theorem 5.16, for all $i \in \overline{\{1,4\}}$, $\beta i' = [\alpha i' - \alpha s']_4$. Using Corollary 5.15, there is a 3-translatable ordering $1', 2', 3', 4'$ on $\mathbb{Z}_4$ and $r, s \in \overline{\{1,4\}}$ such that $\alpha r' = 4 = \beta s'$, $(\alpha([r+1]'_4), 4) = 1$ and $\alpha([r+i]'_4) = i\alpha([r+1]'_4)$ for all $i \in \overline{\{1,4\}}$. So, $\alpha([r+1]_4)' \in \{1,3\}$. If we choose $\alpha([r+1]'_4) = 1$ then $\alpha([r+i]'_4) = i\alpha([r+1]'_4) = i$ for all $i \in \overline{\{1,4\}}$. Therefore, $\beta([r+i]'_4) = [\alpha([r+i]'_4) - \alpha s']_4 = [i - \alpha s']_4$. Since $\alpha s' = \alpha([r-(r-s)]'_4) = [s-r]_4$ we have $\beta([r+i]'_4) = [i - \alpha s']_4 = [i+r-s]_4$.

Note that since $1', 2', 3', 4'$ is a 3-translatable ordering, by Lemma 2.3 so is the ordering $[r+1]'_4, [r+2]'_4, [r+3]'_4, r'$. If we define $x_i = [r+i]'_4$ then we obtain the following 3-translatable Cayley table for $\mathbb{Z}_4$, where $d = [r - s]_4$ and each entry is calculated modulo 4.

$*$	x_1	x_2	x_3	x_4
x_1	$2+d$	$3+d$	d	$1+d$
x_2	$3+d$	d	$1+d$	$2+d$
x_3	d	$1+d$	$2+d$	$3+d$
x_4	$1+d$	$2+d$	$3+d$	d

Note that in the Cayley table above, changing the ordering to $x_3x_4x_1x_2$ in the leftmost column and also in the top row gives exactly the same quasigroup. That is, not only is the main body of the Cayley table the same, all the products are the same. For a fixed value of d, any other ordering gives a different quasigroup.

Note also that, given a fixed r, s and $t = \alpha([r+1]'_n)$, any chosen ordering $x_1x_2x_3x_4$ determines precisely one bijection α which in turn by Corollary 5.15 and Theorem 5.16 determines the bijection β, as indicated in the table below, the entries of which are calculated modulo 4.

There are all 24 possible orderings listed in the table below, twelve pairs of which give 12 distinct 3-translatable quasigroups induced by $\mathbb{Z}_4$. The first 4 pairs of those are linear over $\mathbb{Z}_4$, namely, the quasigroups determined by the orderings 1234, 3412, 2341, 4123, 4321, 2143, 1432 and 3214, as will be shown below. None of the quasigroups determined by the eight other pairs of orderings is linear over $\mathbb{Z}_4$.

$x_1x_2x_3x_4$	α	$\beta 1$	$\beta 2$	$\beta 3$	$\beta 4$
1234	ε	$1+d$	$2+d$	$3+d$	d
3412	(13)(24)	$3+d$	d	$1+d$	$2+d$
2341	(1432)	d	$1+d$	$2+d$	$3+d$
4123	(1234)	$2+d$	$3+d$	d	$1+d$
4321	(14)(23)	d	$3+d$	$2+d$	$1+d$
2143	(12)(34)	$2+d$	$1+d$	d	$3+d$
1432	(24)	$1+d$	d	$3+d$	$2+d$
3214	(13)	$3+d$	$2+d$	$1+d$	d
1243	(34)	$1+d$	$2+d$	d	$3+d$
4312	(1324)	$3+d$	d	$2+d$	$1+d$
1321	(23)	$1+d$	$3+d$	$2+d$	d
2413	(1342)	$3+d$	$1+d$	d	$2+d$

1342	(243)	$1+d$	d	$2+d$	$3+d$
4213	(134)	$3+d$	$2+d$	d	$1+d$
1423	(234)	$1+d$	$3+d$	d	$2+d$
2314	(132)	$3+d$	$1+d$	$2+d$	d
2134	(12)	$2+d$	$1+d$	$3+d$	d
3421	(1423)	d	$3+d$	$1+d$	$2+d$
2431	(142)	d	$1+d$	$3+d$	$2+d$
3124	(123)	$2+d$	$3+d$	$1+d$	d
3142	(1243)	$2+d$	d	$1+d$	$3+d$
4231	(14)	d	$2+d$	$3+d$	$1+d$
3241	(143)	d	$2+d$	$1+d$	$3+d$
4132	(124)	$2+d$	d	$3+d$	$1+d$

Given that the only automorphisms of $\mathbb{Z}_4$ are of the form $\varphi i = i$ and $\varphi i = 3i$, using Lemma 2.1 it is easy to calculate that the only 3-translatable quasigroups linear over $\mathbb{Z}_4$ are of the form $i*j = [\varphi i+\varphi j+c]_4$, where $c \in \mathbb{Z}_4$ is fixed. Examining the Cayley table of the quasigroups determined by the first eight pairs in the table, in their natural ordering, shows that they each are of one of these linear forms.

In particular, the orderings 1234 and 3412 give $i * j = [i + j - d]_4$, 2341 and 4123 give $i * j = [i + j + 2 - d]_4$, 4321 and 2143 give $i * j = [3i + 3j + 2 - d]_4$ and 1432 and 3214 give $i * j = [3i + 3j - d]_4$.

Any of the other quasigroups determined by the remaining 8 pairs of orderings is not of a linear form because, in their natural ordering, there is always an increase in the value of a particular two consecutive, increasing entries by a value of 2. This is not possible for a 3-translatable quasigroup linear over $\mathbb{Z}_4$, where the values of two consecutive, increasing entries always increases by a value of 1 or 3.

If we had chosen $\alpha([r+1]'_4) = 3$ then by Corollary 5.15, for all $i \in \overline{\{1,4\}}$, $(\alpha[r+1]'_4) = [3i]_4$ and $\beta([s+3i]'_4) = [-3i]_4 = i = \beta([s-i]'_4)$. Therefore, $\beta([r+i]'_4) = [s-r-i]_4$. As previously, if we define $x_i = [r+i]'_4$ then any ordering $x_1x_2x_3x_4$ gives the following 3-translatable Cayley table.

$*$	x_1	x_2	x_3	x_4
x_1	$2-d$	$1-d$	$-d$	$3-d$
x_2	$1-d$	$-d$	$3-d$	$2-d$
x_3	$-d$	$3-d$	$2-d$	$1-d$
x_4	$3-d$	$2-d$	$1-d$	$-d$

The first eight orderings of the table below give different values of the mapping α, but for each ordering the value of βi, $i \in \overline{\{1,4\}}$ is the additive inverse of the corresponding entries in the table on the previous page.

$x_1x_2x_3x_4$	α	$\beta 1$	$\beta 2$	$\beta 3$	$\beta 4$
1234	(13)	$-d-1$	$-d-2$	$-d-3$	$-d$
3412	(24)	$-d-3$	$-d$	$-d-1$	$-d-2$
2341	(14)(23)	$-d$	$-d-1$	$-d-2$	$-d-3$
4123	(12)(34)	$-d-2$	$-d-3$	$-d$	$-d-1$
4321	(1432)	$-d$	$-d-3$	$-d-2$	$-d-1$
2143	(1234)	$-d-2$	$-d-1$	$-d$	$-d-3$
1432	(13)(24)	$-d-1$	$-d$	$-d-3$	$-d-2$
3214	ε	$-d-3$	$-d-2$	$-d-1$	$-d$

In particular, the orderings 1234 and 3412 give $i*j=[3i+3j-d]_4$, 2341 and 4123 give $i*j=[3i+3j+2-d]_4$, 4321 and 2143 give $i*j=[i+j+2-d]_4$ and 1432 and 3214 give $i*j=[i+j-d]_4$.

Note that, whether $\alpha([r+1]_4')=1$ or $\alpha([r+1]_4')=3$, since $[r-s]_4\in\overline{\{1,4\}}$ every possible 3-translatable linear isotope appears for any of the first eight orderings in Tables 2 or 4. The remainder of the non-linear, 3-translatable isotopes are of one of the following 8 forms in their natural ordering.

$*_1$	1	2	3	4
1	2	1	3	4
2	1	4	2	3
3	3	2	4	1
4	4	3	1	2

$*_2$	1	2	3	4
1	2	4	1	3
2	4	2	3	1
3	1	3	4	2
4	3	1	2	4

$*_3$	1	2	3	4
1	2	3	1	4
2	3	4	2	1
3	1	2	4	3
4	4	1	3	2

$*_4$	1	2	3	4
1	2	4	3	1
2	4	2	1	3
3	3	1	4	2
4	1	3	2	4

$*_5$	1	2	3	4
1	4	1	3	2
2	1	2	4	3
3	3	4	2	1
4	2	3	1	4

$*_6$	1	2	3	4
1	4	3	1	2
2	3	2	4	1
3	1	4	2	3
4	2	1	3	4

$*_7$	1	2	3	4
1	4	2	1	3
2	2	4	3	1
3	1	3	2	4
4	3	1	4	2

$*_8$	1	2	3	4
1	4	2	3	1
2	2	4	1	3
3	3	1	2	4
4	1	3	4	2

The quasigroups $(\mathbb{Z}_4,*_1)$, $(\mathbb{Z}_4,*_3)$, $(\mathbb{Z}_4,*_7)$ and $(\mathbb{Z}_4,*_8)$ are isomorphic to each other, as are the quasigroups $(\mathbb{Z}_4,*_2)$, $(\mathbb{Z}_4,*_4)$, $(\mathbb{Z}_4,*_5)$ and $(\mathbb{Z}_4,*_6)$.

References

[1] **W.A. Dudek and R.A.R. Monzo**, *The fine structure of quadratical quasigroups*, Quasigroups and Related Systems, **24** (2016), 205 – 218.

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

[3] **W.A. Dudek and R.A.R. Monzo**, *Translatability determines the structure of certain types of idempotent quasigroups*, Quasigroups and Related Systems, **28** (2020), 53 – 76.

[4] **W.A. Dudek and R.A.R. Monzo**, *Translatable quadratical quasigroups*, Quasigroups and Related Systems, **28** (2020), 203 – 228.

[5] **W.A. Dudek and R. A. R. Monzo**, *The structure of idempotent translatable quasigroups*, Bull. Malays. Math. Sci. Soc., **43** (2020), 1603 – 1621.

[6] **P. Němec, T. Kepka**, *T-quasigroups I*, Acta Univ. Carolin. Math. Phys., **12** (1971), no. 1, 39˘49.

[7] **V. Shcherbacov**, *Elements of quasigroup theory and applications*, CRC Press, Boca Raton, 2017.

Received 17 September, 2021

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 **29** (2021), 209 − 212

On quasi-cancellative AG-groupoids

Muhammad Iqbal and Imtiaz Ahmad

Abstract. We proved the analog of the Burmistrovich's theorem for semigroups: a cyclic-associative AG-groupoid is quasi-cancellative if and only if it is a semilattice of cancellative cyclic-associative AG-subgroupoids. We also proved that an AG-groupoid in which all elements are 3-potent is quasi-cancellative.

1. Introduction

A magma is a fundamental type of an algebraic structure, consist of a non-empty set together with one binary operation. Abel-Grassmann's groupoids (abbreviated as AG-groupoids) [9] (also known as left almost semigroups (LA-semigroups) [5]) can be considered as the non-empty set H with the binary operation satisfying the identity $xy \cdot z = zy \cdot x$. This structures was introduced by Kazim and Naseeruddin in [5].

Protić and Stevanović introduced in [10] the concept of 3-potent elements, AG-3-bands, AG-bands and anti-rectangular AG-bands. The notion of cyclic-associative AG-groupoids (AC-AG-groupoids) was introduced by Iqbal et al. in [4]. Dudek and Gigoń [2, 3] studied some fundamental properties of completely inverse AG**-groupoids and determine certain fundamental congruences on it. Mushtaq and Yusuf proved in [7] that a left cancellative AG-groupoid is right cancellative. Shah et al. proved in [12] that in AG-monoids the set of all cancellative elements is an AG-subgroupoid. They further proved that a finite AG-monoid has at least one non-cancellative element and the set of non-cancellative elements form a maximal ideal.

In this note we will prove the Burmistrovich theorem for AG-groupoids: a cyclic-associative AG-groupoid is quasi-cancellative if and only if it is a semilattice of cancellative cyclic-associative AG-subgroupoids. Also we will prove that any AG-groupoid H in which $xx \cdot x = x \cdot xx = x$ for all $x \in H$ is quasi-cancellative.

2. Results

A groupoid $(H, \cdot)$, or simply H, satisfying the identity $xy \cdot z = zy \cdot x$ (known as the left invertive law (L.I.Law) [5]) is called an *AG-groupoid.* Every AG-groupoid satisfies the *medial law* (M.Law): $xy \cdot zt = xz \cdot yt$. An AG-groupoid contains at most one left identity [7]. An AG-groupoid having a left identity satisfies the *paramedial law* (P.Law): $xy \cdot zt = ty \cdot zx$.

An element $h \in H$ is called an *idempotent* if $h^2 = h$. The set of all idempotent elements of H is denoted by $E(H)$. An AG-groupoid containing only idempotent elements is called an *AG-band* [13]. A commutative AG-band is called a *semilattice.* An element $h \in H$ is *3-potent* if $(hh)h = h(hh) = h$. If all elements of an AG-groupoid H are 3-potents, then H is called an *AG-3-band.* An AG-groupoid H is called an *AG*-groupoid* [6] if $xy \cdot z = y \cdot xz$ for all $x, y, z \in H$ (known as a weak associative law); an *AG**-groupoid* [8] if $x \cdot yz = y \cdot xz$ and a *cyclic-associative AG-groupoid* (CA-AG-groupoid) if $x \cdot yz = z \cdot xy$ [4]. Every CA-AG-groupoid is paramedial [4]. An element h of an AG-groupoid H is *right* (*left*) *cancellative* if for all $x, y \in H$, $xh = yh$ ($hx = hy$) implies $x = y$. The element h is *cancellative* if it is simultaneously right and left

2010 Mathematics Subject Classification: 20N02, 20N99, 08A30.
Keywords: AG-groupoid; LA-semigroup; CA-AG-groupoid; AG-band; quasi-cancellative; Burmistrovich's Theorem.

cancellative. H is (right/left) cancellative if all elements of H are (right/left) cancellative. H is *quasi-cancellative* [11] if for all $x, y \in H$: (i) $x^2 = xy$ and $y^2 = yx$ imply $x = y$, (ii) $x^2 = yx$ and $y^2 = xy$ imply $x = y$.

Lemma 1. *If a quasi-cancellative AG-groupoid is cyclic-associative, then*
(A) $xa = xb \Longleftrightarrow ax = bx$,
(B) $x^2a = x^2b \Rightarrow ax = bx$,
(C) $x^2a = x^2b \Rightarrow xa = xb$,
(D) $xy \cdot a = xy \cdot b \Rightarrow a \cdot yx = b \cdot yx$,
(E) $xy \cdot a = xy \cdot b \Rightarrow yx \cdot a = yx \cdot b$,
(F) $a \cdot xy = b \cdot xy \Rightarrow a \cdot yx = b \cdot yx$,
(G) $a \cdot xy = b \cdot xy \Rightarrow yx \cdot a = yx \cdot b$,
(H) $xy \cdot a = xy \cdot b \Longleftrightarrow a \cdot yx = b \cdot yx$.

Proof. (A). Assume $xa = xb$, then $xa \cdot xa = xb \cdot xa$ and $xa \cdot xb = xb \cdot xb$. Now by the cyclic-associativity and M.Law we get

$$xa \cdot xa = a(xa \cdot x) = x(a \cdot xa) = x(a \cdot ax) = x(x \cdot aa) = aa \cdot xx = ax \cdot ax = (ax)^2.$$

Analogously,

$$\begin{aligned} xb \cdot xa &= a(xb \cdot x) = x(a \cdot xb) = x(b \cdot ax) = x(x \cdot ba) = ba \cdot xx = bx \cdot ax = x(bx \cdot a) \\ &= x(ax \cdot b) = b(x \cdot ax) = ax \cdot bx. \end{aligned}$$

Thus $(ax)^2 = ax \cdot bx$. Similarly, we obtain $xa \cdot xb = ba \cdot xx = bx \cdot ax$. Thus $(bx)^2 = bx \cdot ax$.
By quasi-cancellativity, from $(ax)^2 = ax \cdot bx$ and $(bx)^2 = bx \cdot ax$, we have $ax = bx$.
The converse implication follows by symmetry.

(B). Let $x^2a = x^2b$. Then $x^2a \cdot a = x^2b \cdot a \Rightarrow aa \cdot xx = ab \cdot xx \Rightarrow ax \cdot ax = ax \cdot bx \Rightarrow (ax)^2 = ax \cdot bx$.
Similarly from $x^2a = x^2b$ we have $x^2a \cdot b = x^2b \cdot b$, which gives $(bx)^2 = bx \cdot ax$. This together with $(ax)^2 = ax \cdot bx$ implies $ax = bx$.

(C). Follows from (A) and (B).

(D). Assume $xy \cdot a = xy \cdot b$. Then $a^2 \cdot xy = (xy \cdot a)a = (xy \cdot b)a = ab \cdot xy$. So, $a^2 \cdot xy = ab \cdot xy$. Thus, $(a^2 \cdot xy) \cdot xy = (ab \cdot xy) \cdot xy$. But $(xy \cdot xy)a^2 = (yy \cdot xx)a^2 = (yx \cdot yx)a^2 = (a \cdot yx)(a \cdot yx) = (a \cdot yx)^2$. Similarly, $(ab \cdot xy) \cdot xy = (xy \cdot xy) \cdot ab = (yy \cdot xx) \cdot ab = (yx \cdot yx) \cdot ab = (b \cdot yx)(a \cdot yx) = (b \cdot yx)(a \cdot yx)$. Therefore $(a \cdot yx)^2 = (b \cdot yx)(a \cdot yx)$.
In the same way from $xy \cdot a = xy \cdot b$ we obtain $(a \cdot yx)(b \cdot yx) = (b \cdot yx)^2$, which together with the previous equality implese $a \cdot yx = b \cdot yx$.

(E). Follows from (D) and (A); (F) – from (A) and (D); (G) – from (F) and (A); (H) – from (D) and (G). □

The following theorem is an analog of the Burmistrovich's theorem for semigroups from [1].

Theorem 1. *A cyclic-associative AG-groupoid is quasi-cancellative if and only if it is a semilattice of cancellative cyclic-associative AG-subgroupoids.*

Proof. Necessity. Let a cyclic-associative AG-groupoid be quasi-cancellative. Let σ by the relation on H such that $x \,\sigma\, y$ if for any $p, q \in H$, $xp = xq \Longleftrightarrow yp = yq$. It is an equivalence relation. To prove that σ is a congruence, let $x \,\sigma\, y$ and $z \in H$. If $xz \cdot p = xz \cdot q$, then $pz \cdot x = qz \cdot x$. Thus, $x \cdot pz = x \cdot qz$, by Lemma 1 (A). Hence $z \cdot xp = z \cdot xq$, which by our assumption gives $z \cdot yp = z \cdot yq$. So, $p \cdot zy = q \cdot zy$, i.e. $y \cdot pz = y \cdot qz$. The last, by Lemma 1 (A), gives $pz \cdot y = qz \cdot y$. Consequently, $yz \cdot p = yz \cdot q$. By symmetry $yz \cdot p = yz \cdot q$ implies $xz \cdot p = xz \cdot q$. Hence $xz \,\sigma\, yz$. Therefore, σ is right compatible.

Now if $zx \cdot p = zx \cdot q$, then $xz \cdot p = xz \cdot q$, by Lemma 1 (E). So, as it is proved above, $yz \cdot p = yz \cdot q$. This, by Lemma 1 (E), implies $zy \cdot p = zy \cdot q$. By symmetry $zy \cdot p = zy \cdot q$ implies $zx \cdot p = zx \cdot q$. Hence, $zx \,\sigma\, zy$, therefore σ is left compatible. Consequently, σ is a congruence.

Then H/σ, by Lemma 1 (A) and (B), is an AG-band, By Lemma 1 (E), it is commutative. Consequently, σ is a semilattice congruence.

Suppose $zx = zy$, $x\,\sigma\,z$ and $y\,\sigma\,z$. Since $x\,\sigma\,z$, $zx = zy$ implies that $x^2 = xy$ and since $y\sigma z$, thus $yx = y^2$. This, by quasi-cancellativity, gives $x = y$. If $xz = yz$ with $x\,\sigma\,z$ and $y\,\sigma\,z$, then $zx = zy$, by Lemma 1 (A), and this reduces to the case just considered before. Hence, each σ-class is cancellative.

Sufficiency. Let H is a semilattice of cancellative cyclic-associative AG-subgroupoids and x, y are elements such that $x^2 = yx$ and $y^2 = xy$. Suppose η be the component of H that contains yx. As H is semilattice, consequently H is commutative, thus $xy \in \eta$ as well. Hence, $x^2, y^2 \in \eta$. As η is a cyclic-associative AG-groupoid, thus by the closure property in η we have $x, y \in \eta$. But η is cancellative and therefore the equality $xx = xy$ implies $x = y$. By similar argument if $x^2 = xy$ and $y^2 = yx$, then $x = y$. Hence, H is quasi-cancellative. □

The following example illustrate Theorem 1.

Example 1. The Cayley table given below defines a quasi-cancellative cyclic-associative AG-groupoid H that is a semilattice of cancellative cyclic-associative AG-subgroupoids $I = \{1\}$ and $J = \{2, 3, 4, 5\}$ such thst I, J commute and $I^2 = I$, $J^2 = J$.

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

Theorem 2. *Every AG-3-band is quasi-cancellative.*

Proof. Suppose H is AG-3-band and $x, y \in H$.

To prove that $x^2 = xy$ and $y^2 = yx$ imply $x = y$ suppose $x^2 = xy$ and $y^2 = yx$. then, by the definition of AG-3-band, supposition, L.I.Law and M.Law we obtain

$$\begin{aligned}
x &= x^2x = xy \cdot x = ((xx \cdot x)y)x = (yx \cdot xx)x = (x \cdot xx) \cdot yx = x \cdot yx = xy^2 \\
&= (xx \cdot x) \cdot yy = (xx \cdot y) \cdot xy = (yx \cdot x) \cdot xy = (y^2x) \cdot xy = (yy \cdot x) \cdot xy \\
&= (xy \cdot y) \cdot xy = (xy \cdot x) \cdot yy = (((xx \cdot x)y)x) \cdot yy = ((yx \cdot xx)x) \cdot yy \\
&= ((x \cdot xx) \cdot yx) \cdot yy = (x \cdot yx) \cdot yy = xy^2 \cdot yy = xy \cdot y^2y = xy \cdot y \\
&= yy \cdot x = yy \cdot (x \cdot xx) = yx \cdot (y \cdot xx) = y^2 \cdot yx^2 = y^2\left((yy \cdot y) \cdot xx\right) \\
&= y^2\left((yy \cdot x) \cdot yx\right) = y^2\left((xy \cdot y) \cdot yx\right) = y^2\left(x^2y \cdot yx\right) = y^2\left((xx \cdot y) \cdot yx\right) \\
&= y^2\left((yx \cdot x) \cdot yx\right) = y^2\left((yx \cdot y) \cdot xx\right) = y^2\left((((yy \cdot y)x)y) \cdot xx\right) \\
&= y^2\left(((xy \cdot yy)y) \cdot xx\right) = y^2\left(((y \cdot yy) \cdot xy) \cdot xx\right) = y^2\left((y \cdot xy) \cdot xx\right) \\
&= y^2\left(yx^2 \cdot xx\right) = y^2\left(yx \cdot x^2x\right) = y^2\left(yx \cdot x\right) = y^2(y^2x) = y^2\left(yy \cdot x\right) \\
&= y^2\left(xy \cdot y\right) = y^2(xy \cdot y^2y) = y^2\left(xy^2 \cdot yy\right) = y^2\left((x \cdot yx) \cdot yy\right) \\
&= y^2(((x \cdot xx) \cdot yx) \cdot yy) = y^2\left(((yx \cdot xx)x) \cdot yy\right) = y^2\left((((xx \cdot x)y)x) \cdot yy\right) \\
&= y^2\left((xy \cdot x) \cdot yy\right) = y^2\left((xy \cdot y) \cdot xy\right) = y^2\left((yy \cdot x) \cdot xy\right) = y^2\left(y^2x \cdot xy\right) \\
&= y^2\left((yx \cdot x) \cdot xy\right) = y^2\left((xx \cdot y) \cdot xy\right) = y^2\left((xx \cdot x) \cdot yy\right) = y^2 \cdot xy^2 \\
&= yy \cdot xy^2 = yx \cdot yy^2 = y^2y = y.
\end{aligned}$$

This shows that $x^2 = xy$ and $y^2 = yx$ imply $x = y$.

To prove that $x^2 = yx$ and $y^2 = xy$ imply $x = y$ suppose $x^2 = yx$ and $y^2 = xy$. Then, as in the previous case,

$$\begin{aligned} x &= x^2x = yx \cdot x = xx \cdot y = x^2y = yx \cdot y = (y^2y \cdot x)y \\ &= ((xy \cdot y)x)y = ((yy \cdot x)x)y = (xx \cdot yy)y = (xy \cdot xy)y \\ &= (y^2 \cdot y^2)y = (yy \cdot yy)y = ((yy \cdot y)y)y = yy \cdot y = y. \end{aligned}$$

Hence $x = y$. This completes the proof. □

Acknowledgements. This research work is financially supported by the HEC funded project NRPU-3509.

References

[1] **I.E. Burmistrovich**, *The commutative bands of cancellative semigroups*, Sib. Mat. Zh. (Russian) **6** (1965), 284 − 299.

[2] **W.A. Dudek and R.S. Gigoń**, *Congruences on completely inverse AG**-groupoids*, Quasigroups Related Systems **20** (2012), 203 − 209.

[3] **W.A. Dudek and R.S. Gigoń**, *Completely inverse AG**-groupoid*, Semigroup Forum **87** (2013), 201 − 229.

[4] **M. Iqbal, I. Ahmad, M. Shah and M. Irfan Ali**, *On cyclic associative Abel-Grassman groupoids*, British J. Math. Comp. Sci. **12**(5) (2016), 1 − 16.

[5] **M.A. Kazim and M. Naseeruddin**, *On almost semigroups*, Portugaliae Math. **2** (1972), 1 − 7.

[6] **Q. Mushtaq and M.S. Kamran**, *On LA-semigroups with weak associative law*, Scientific Khyber **1**(11) (1989), 69 − 71.

[7] **Q. Mushtaq and S.M. Yusuf**, *On LA-semigroups*, Alig. Bull. Math. **8** (1978), 65 − 70.

[8] **P.V. Protić and M. Božinović**, *Some congruences on an AG**-groupoid*, Algebra Logic Discrete Math. **9**(3) (1995), 879 − 886.

[9] **P.V. Protić and N. Stevanović**, *On Abel-Grassmann's groupoids* (*exposition*), In: Proc. Math. Conf. Priština pp. 27 − 29 (1994).

[10] **P.V. Protić and N. Stevanović**, *Abel-Grassmann's bands*, Quasigroups Related Systems **11** (2004), 95 − 101.

[11] **M. Shah, I. Ahmad and A. Ali**, *On quasi-cancellativity of AG-groupoids*, Int. J. Contemp. Math. Sci. **7**(42) (2012), 2065 − 2070.

[12] **M. Shah, T. Shah and A. Ali**, *On the cancellativity of AG-groupoids*, Int. Math. Forum **6**(44) (2011), 2187 − 2194.

[13] **N. Stevanović and P.V. Protić**, *Some decompositions on Abel-Grassmann's groupoids*, Pure Math. Appl. **8** (1997), 355 − 366.

Received December 4, 2020

Department of Mathematics, University of Malakand, Khyber Pakhtunkhwa, Pakistan

E-mail: iqbalmuhammadpk78@yahoo.com (M.Iqbal), iahmad@uom.edu.pk (I.Ahmad)

Quasigroups and Related Systems **29** (2021), 213 – 222

Semigroups in which 2-absorbing ideals are prime and maximal

Biswaranjan Khanra and Manasi Mandal

Abstract. We characterize commutative semigroups in which 2-absorbing ideals are maximal. We introduce the concept of 2-AB semigroups in which 2-absorbing ideals are prime and characterize 2-AB semigroups in terms of minimal prime ideal over a 2-absorbing ideal and study some properties of these semigroups.

1. Introduction

Throughout this paper all semigroups are commutative, prime ideals are proper and whenever speaking about maximal ideals we suppose, of course, it exists.

The notion of 2-absorbing ideals for commutative ring was introduced as a generalization of prime ideals by Badwai [1] and later extended to commutative semigroup by [5] and [3] as follows: A proper ideal I of a semigroup S is said to be a 2-*absorbing* ideal of S if for any elements $s_1, s_2, s_3 \in S$, $s_1s_2s_3 \in I$ implies $s_1s_2 \in I$ or $s_1s_3 \in I$ or $s_2s_3 \in I$. Clearly, every prime ideal is 2-absorbing but the converse is not true (see Lemma 2.1 and Example 2.2).

In this paper, we prove that every maximal ideal of a commutative semigroup is 2-absorbing but converse is not true (see Theorem 2.3). In [2], D. Bennis characterize commutative rings in which 2-absorbing ideals are prime. These observations prompted us to solve the following two natural questions:

(1) In which class of semigroups 2-absorbing ideals are maximal?

(2) In which class of semigroups 2-absorbing ideals are prime?

We establish an analogues result of Theorem 2.3 in a commutative ring (Theorem 2.4). Then we characterize the class of semigroups with unity (Theorem 2.7) and without unity (Theorem 2.11), in which 2-absorbing ideals are maximal. Next, we define the notion of 2-AB semigroup, in which 2-absorbing ideals are prime and an example of this semigroup is given (Definition 3.1 and Example 3.2). We study many properties of a 2-AB semigroup S such as 2-absorbing ideals are linearly ordered, S has atmost one maximal ideal, S is semiprimary and prime ideals of S are idempotent (Theorem 3.3). Then we characterize 2-AB semigroup in terms of minimal prime ideal over a 2-absorbing ideal (Theorem 3.5), some other characterizations have also been established (Theorem 3.6, Theorem 3.7 and

2010 Mathematics Subject Classification: 20M12, 20M14.
Keywords: Commutative semigroup, Prime ideal, Maximal ideal, 2-absorbing ideal.

Theorem 3.9). We study some equivalent conditions for a regular semigroup S to be 2-AB semigroup (Theorem 3.11). Finally, we prove that a semigroup S will be 2-AB if S is with unity and having no essential congrurence (Corollary 3.12) or every 2-absorbing ideal of S generated by idempotent (Theorem 3.13).

Before going to the main work we recall some preliminaries which are necessary:

A non-empty ideal P of a semigroup S is said to be *prime* if $AB \subseteq P$ implies that $A \subseteq P$ or $B \subseteq P$, A, B being ideals of S. An ideal P is said to be *completely prime* if $ab \in P$ implies $a \in P$ or $b \in P$, a, b being elements of S. The concepts of prime and completely prime ideal are coincide if S is commutative.

For an ideal A of a semigroup S, a *radical* of A, denoted as $\sqrt{A}$, is the set of all $x \in S$ such that some power of x is in A. An ideal A of S is called *primary* if $ab \in A$ implies either $a \in A$ or $b \in \sqrt{A}$. An ideal I of a semigroup S is said to be *semiprimary* ideal if $\sqrt{I}$ is a prime ideal of S. A commutative semigroup S is called *fully prime semigroup* if every ideal of S is prime and *primary* if every ideal of S is primary. Also a semigroup S is said to be *semiprimary* if every ideal of S is a semiprimary ideal of S. A semigroup in which every ideal is idempotent is called a *fully idempotent semigroup.*

Theorem 1.1. (cf. [7]) *A commutative semigroup S is semiprimary if and only if prime ideals of S are linearly ordered.*

A commutative semigroup S is said to be *Archimedian* if, for any two elements of S, each divides some power of the other. In [10] it is proved that a commutative semigroup is archimedian if and only if S has no proper prime ideals.

We will use the following theorems proved in [11].

Theorem 1.2. *If I and J are any two ideals of a commutative semigroup S, then the following statements are true;*

(1) $IJ \subseteq I \cap J \subseteq I$.

(2) $I \subseteq \sqrt{I}$.

(3) $I \subseteq J \Rightarrow \sqrt{I} \subseteq \sqrt{J}$,

(4) $\sqrt{IJ} = \sqrt{(I \cap J)} = \sqrt{I} \cap \sqrt{J}$,

(5) *If A is a prime ideal of S, then $\sqrt{A} = A$ and if A is a primary ideal of S, then $\sqrt{A}$ is a prime ideal of S.*

Theorem 1.3. *Let A be an ideal of a commutative semigroup S with unity. If $\sqrt{A} = M$, where M is a maximal ideal of S, then A is a primary ideal of S.*

Theorem 1.4. *In a commutative semigroup S with unity, the unique maximal ideal M is prime, which is the union of all proper ideals of S; $\sqrt{M^n} = M$ for every positive integer n and M^n is a primary ideal for every positive integer n.*

Theorem 1.5. *The radical of an ideal I in a commutative semigroup is the intersection of all prime ideals containing I.*

Theorem 1.6. *Any prime ideal containing an ideal I in a semigroup contains a minimal prime ideal belonging to I.*

Also the following theorem will be used.

Theorem 1.7. (cf. [12]) *If M is a maximal ideal of a semigroup S such that the complement of M contains either more than one element, or an idempotent, then M is a prime ideal of S.*

2. The case when 2-absorbing ideals are maximal

Lemma 2.1. *In a commutative semigroup every prime ideal is 2-absorbing.*

Proof. Let I be a prime ideal of S and $abc \in I$ with $ab \notin I$ for some $a, b, c \in S$. Since I is prime, so $c \in I$, which implies $ac \in I$ and $bc \in I$. So I is a 2-absorbing ideal of S. □

The following example shows that the converse of the above lemma is not true:

Example 2.2. *The principal ideal $I = (6)$ in the semigroup $S = (\mathbb{N}, \cdot)$ is 2-absorbing but not prime as $2 \cdot 3 \in (6)$ but neither $2 \in (6)$ nor $3 \in (6)$.*

A commutative semigroup with unity has a unique maximal ideal, which is prime and 2-absorbing. But in a commutative semigroup without unity maximal ideal need not be prime. For example, the ideal $I = \{m \in \mathbb{N} : m \geqslant 2\}$ in the semigroup $S = (\mathbb{N}, +)$ is maximal but not prime.

Theorem 2.3. *In a commutative semigroup without unity every maximal ideal is 2-absorbing.*

Proof. Let M be a maximal ideal of a semigroup S without unity and $abc \in M$ with $ab \notin M$ for some $a, b, c \in S$.

1. If $c \in M$ then $ac \in M$ and $bc \in M$, since M is an ideal of S. Hence M is a 2-absorbing ideal of S.

2. Let $c \notin M$. Since $ab \notin M$, then both a, b belongs to $S - M$. Now if $c \neq ab$, then $S - M$ contains two distinct elements c and ab. Again if $c = ab$ and $a \neq b$ then $S - M$ contains two distinct elements a and b and if $a = b$ then $\{a, a^2\}$ belongs to $S - M$, moreover if $a = a^2$, then a is an idempotent element of S. Thus in either case $S - M$ contains more than one elemenet or an idempotent, hence M is a prime ideal of S by Theorem 1.7. Consequently, M is a 2-absorbing ideal of S by Lemma 2.1. □

The converse is not true if S has unity. Indeed, the ideal $I = \{m \in S : m \geqslant 2\}$ in $S = (\mathbb{N} \cup \{0\}, +)$ is 2-absorbing but not maximal.

Theorem 2.4. *In a commutative ring every maximal ideal is 2-absorbing.*

Proof. Let M be a maximal ideal of a commutative ring R and $abc \in M$ with $ab \notin M$, for some $a, b, c \in R$. If $c \notin M$, then $M + (c) = R = M + (ab)$, where (c) and (ab) denotes respectively the principal ideal generated by c and ab.

Since $a, b \in R$, so there exist $r, s \in R$ and $p, q \in \mathbb{Z}$ such that $a = m+rc+pc$ and $b = n+sab+qab$, for some $m, n \in M$. Therefore $ab = (m+rc+pc)(n+sab+qab) = mn+msab+qmab+nrc+rsabc+qrabc+pnc+psabc+pqabc \in M$, a contradiction. Hence $c \in M$ implies $ac, bc \in M$ and consequently M is 2-absorbing. $\square$

The converse is not true. In the commutative ring $\mathbb{Z}[x]$ with unity the principal ideal (x) is 2-absorbing but it is not maximal.

Lemma 2.5. *The intersection of any two prime ideals is a* 2*-absorbing ideal.*

Proof. Let $abc \in P_1 \cap P_2$ for some $a, b, c \in S$. Then $abc \in P_1$ and $abc \in P_2$. Since P_1 and P_2 are prime ideals so either $a \in P_1$ or $b \in P_1$ or $c \in P_1$ and also either $a \in P_2$ or $b \in P_2$ or $c \in P_2$. Thus in either ab or bc or ac belongs to $P_1 \cap P_2$. $\square$

Theorem 2.6. *If in a semigroup S all* 2*-absorbing ideals are maximal, then S has at most one prime ideal. This ideal is maximal.*

Proof. By Lemma 2.5 the intersection of two prime ideals P_1 and P_2 is a 2-absorbing ideal. It is maximal and it is contained in both ideal P_1 and P_2. Hence $P_1 = P_2$. $\square$

Theorem 2.7. *In a semigroup S with unity every* 2*-absorbing ideal is maximal if and only if S is either a group or S has a unique* 2*-absorbing ideal A such that $S = A \cup H$, where H is the group of units and A is an archimedian subsemigroup of S.*

Proof. Let S be a semigroup with unity in which every 2-absorbing ideal is maximal. If S is not group, then S has a unique maximal ideal A which is the only prime as well as 2-absorbing ideal of S. Therefore $S = A \cup H$, where A is unique 2-absorbing ideal of S and H is the group of units. Since A is the unique prime ideal in S, for any p,$q \in A$, $\sqrt{(p)} = \sqrt{(q)} = A$. Then there exist positive integers m and n such that $p^m = qx$ and $q^n = py$ for some x, $y \in S$. So $p^{m+1} = q(px)$ and $q^{n+1} = p(qy)$, where $px, qy \in M$. Hence A is an archimedian subsemigroup of S.

Conversely, let A be the unique 2-absorbing ideal of S. Since in a semigroup with unity has unique maximal ideal and maximal ideals are 2-absorbing, therefore A is maximal, as desired. $\square$

Theorem 2.8. *Let S be a regular semigroup with unity such that every* 2*-absorbing ideal is of the form M^n, where n is any positive integer and M is the unique maximal ideal of S. Then an ideal I of S is a primary if and only if I is a* 2*-absorbing ideal of S.*

Proof. Let I be a 2-absorbing ideal of a semigroup S with unity, which is of the form M^n, where n is any positive integer and M is the unique maximal ideal of S. Then $\sqrt{I} = \sqrt{M^n} = M$ by Theorem 1.4. Hence I is a primary ideals of S.

Conversely, let I be a primary ideal of S. Since S is regular so $I = \sqrt{I}$. Cosequently I is prime and hence I is 2-absorbing ideal of S. $\square$

As a consequence of the above theorem and Theorem 2.1 of [9] we obtain

Corollary 2.9. *If in a regular semigroup S with zero and identity every 2-absorbing ideal has the form M^n, where $n \in \mathbb{N}$ and M is the maximal ideal of S, then every non-zero 2-absorbing ideal of S is maximal if and only if*

(i) *S is the union of two groups with adjoined zero, or*

(ii) *$S = H \cup M$, where $M = \{0, xh : h \in H, x^2 = 0, x \in M\}$ and H is the group of units.*

Theorem 2.10. *If in a semigroup S with unity all 2-absorbing ideals are maximal, then*

(1) *S is a primary semigroup,*

(2) *$M^2 = M$, where M is the maximal ideal of S,*

(3) *S has atmost one idempotent different from identity.*

Proof. (1). Let S be a semigroup with unity in which all 2-absorbing ideals are maximal. Then S has a unique maximal ideal, say M, which is the union of all proper ideals of S and it is also the unique prime ideal of S. Then for any ideal I of S, $\sqrt{I} = M$, hence I is a primary ideal of S. Therefore S is a primary semigroup.

(2). Let $abc \in M^2 \subseteq M$ for some $a, b, c \in S$. Since M is a prime ideal of S either a or b or c belongs to M. Let $a \in M$. Then $bc \in M$, implies $b \in M$ or $c \in M$. Hence ac or ab belongs to M^2 and so M^2 is a 2-absorbing ideal of S. Since every 2-absorbing ideal of S is maximal so M^2 is a maximal ideal of S. Therefore $M^2 = M$.

(3). If e and f are idempotents different from the identity, then $\sqrt{(eS)} = \sqrt{(fS)} = M$, where M is the unique prime as well as unique maximal ideal of S. Therefore $e = ef = f$. □

Theorem 2.11. *Let S be a semigroup without unity. Then 2-absorbing ideals of S are maximal if and only if complement of each 2-absorbing ideals contains exactly one non-idempotent element or is a subgroup of S.*

Proof. Let S be a semigroup without unity in which 2-absorbing ideals are maximal. Then S has at most one prime ideal (Theorem 2.6). Let I be a 2-absorbing ideal of S but not prime. Now if complement of I in S contains more than one element or an idempotent, then I is prime (Theorem 1.7), a contradiction. Hence in this case complement of a 2-absorbing ideal contains exactly one non-idempotent element of S. Again, let a 2-absorbing ideal J is prime. Then $a, b \in S - I$ implies $ab \in S - I$, since I is a prime ideal of S. We know that complement of a maximal ideal in a commutative semigroup is a $\mathcal{H}$-class (Green's), and a, b, ab all belong to same $\mathcal{H}$-class $S - I$ of the semigroup S. Hence $S - I$ is a subgroup of S (Theorem 2.16, [4]), as desired.

Conversely, if complement of a 2-absorbing ideal contains exactly one element then clearly it is maximal. Now let complement of a 2-absorbing ideal J forms a subgroup of S. If J is not maximal, then J is contained in a proper ideal K of S.

Let i be the identity element of $S - J$. Since $J \neq K$, there exists $p \in K - J$ such that $pq = i$ for some $q \in S$. Hence $i \in K$. Since $K \neq S$, there exists $m \in S - K$ such that $m = mi \in K$, a contradiction. Thus, J is a maximal ideal of S. $\square$

Since in an archimedian semigroup has no prime ideal, we have

Corollary 2.12. *In an archimedian semigroup S without unity all 2-absorbing ideals are maximal if and only if complement of every 2-absorbing ideal contains exactly one non-idempotent element.*

Corollary 2.13. *In a semigroup S without unity all 2-absorbing ideals are prime as well as maximal if and only if the complement of each 2-absorbing ideal is a subgroup of S.*

3. The case when 2-absorbing ideals are prime

In this section we characterize the class of semigroups in which 2-absorbing ideals are prime and study some properties of this semigroup.

Definition 3.1. A commutative semigroup S is said to be a 2-*AB semigroup* if every 2-absorbing ideal of S is prime.

Example 3.2. In a semigroup $S = \{a, b\}$ with the multiplication determined by $a^2 = a$, $b^2 = b$, $ab = ba = a$, $\{a\}$ is a 2-absorbing ideal which also is prime. Hence S is a 2-AB semigroup.

Theorem 3.3. *Let S be a 2-AB semigroup. Then*

(1) *2-absorbing ideals of S are linearly ordered,*

(2) *prime ideals of S are linearly ordered,*

(3) *S has at most one maximal ideal, if exists then it is prime,*

(4) *S is a semiprimary semigroup,*

(5) *idempotents in S form a chain under natural ordering,*

(6) *$P = P^2$ for every prime ideal P of S,*

(7) *semiprime ideals of S are prime.*

Proof. (1). Let A and B be any two distinct 2-absorbing ideals of a 2-AB semigroup S. So $A \cap B$ is 2-absorbing (Lemma 2.5) and hence prime, which implies either $A \subseteq B$ or $B \subseteq A$.

(2) Clearly prime ideals of S are linearly ordered.

(3) Let M_1 and M_2 be two maximal ideal of S. Since every maximal ideal of S is 2-absobing (Theorem 2.3), so $M_1 \subseteq M_2$ or $M_2 \subseteq M_1$ which implies $M_1 = M_2$. Hence S has atmost one maximal ideal and if exists clearly it is prime.

(4) By Theorem 1.1, a commutative semigroup is semiprimary if and only if prime ideals are linearly ordered. Hence S is a semiprimary semigroup.

(5) Since S is a semiprimary semigroup, then for any ideal A of S, $\sqrt{A}$ is prime. Let e and f are any two idempotents of S. Then $\sqrt{eS}$ and $\sqrt{fS}$ are prime ideals, so either $\sqrt{eS} \subseteq \sqrt{fS}$ or $\sqrt{fS} \subseteq \sqrt{eS}$, which proves that the idempotents form a chain under natural ordering.

(6) Let P be a prime ideal of S and $abc \in P^2 \subseteq P$ for some $a, b, c \in S$. Since P is a prime ideal of S, either $a \in P$ or $b \in P$ or $c \in P$. Let $a \in P$. Then $bc \in P$, implies b or c belogs to P and so ac or ab belongs to P^2. Hence P^2 is a 2-absorbing ideal of S and so P^2 is a prime ideal of S. Let $x \in P$. Then $x^2 \in P^2$ implies $x \in P^2$ so $P \subseteq P^2$. Therefore $P = P^2$.

(7) Let I be a semiprime ideal of S. Then $I = \sqrt{I}$ is a prime ideal of S, since prime ideals of S are linearly ordered, as desired. $\square$

Lemma 3.4. *Let S be a semigroup with unity and unique maximal ideal M. Then for every prime ideal P, PM is a 2-absorbing ideal of S. Moreover, PM is prime if and only if $PM = P$.*

Proof. Let $xyz \in PM \subseteq P$. Since P is prime, either $x \in P$ or $y \in P$ or $z \in P$. Let $x \in P$. Then either $y \in M$ or $z \in M$, since M is also prime. Hence $xy \in PM$ or $xz \in PM$. Consequently, PM is a 2-absorbing ideal of S. Clearly, PM is prime if and only if $PM = P$. $\square$

The following is a characterization of a 2-AB semigroup in terms of minimal prime ideal over a 2-absorbing ideal, which is analogous to (Theorem 2.3, [2]).

Theorem 3.5. *A semigroup S with unity is a 2-AB semigroup if and only if prime ideals of S are linearly ordered and if P is a minimal prime ideal over a 2-absorbing ideal I, then $IM = P$, where M is the unique maximal ideal of S.*

Proof. Let I be a 2-absorbing ideal of a 2-AB semigroup S with unity. Then prime ideals of S are linearly ordered (Theorem 3.3) and I is prime by hypothesis. Then $IM = I$ (Lemma 3.4).

Conversely, let I be a 2-absorbing ideal of S. Since prime ideals are linearly ordered and $P = IM$, where P is a minimal prime ideal over I, $P = IM \subseteq I \cap M = I \subseteq P$ implies $I = P$, as desired. $\square$

Theorem 3.6. *A commutative semigroup S is a 2-AB semigroup if and only if $P = P^2$ for every prime ideal P of S and every 2-absorbing ideal of S is of the form A^2, where A is a prime ideal of S.*

Proof. Let P be a 2-absorbing ideal of a 2-AB semigroup. Then P is prime and so $P = P^2$ (Theorem 3.3(6)).

Conversely, let I be a 2-absorbing ideal of S. Then $I = A^2 = A$, where A is a prime ideal of S. $\square$

Theorem 3.7. *A commutative semigroup S is a 2-AB semigroup if and only if its prime ideals are linearly ordered and $A = A^2$ for every 2-absorbing ideal A of S.*

Proof. Let S be a 2-AB semigroup. Let P_1 and P_2 be two prime ideals of S. Then $P_1 \cap P_2$ is 2-absorbing ideal of S (Lemma 2.5) and so prime, which implies either $P_1 \subseteq P_2$ or $P_2 \subseteq P_1$. Again let A be a 2-absorbing ideal of S and so prime. Therefore $A = A^2$ (Theorem 3.3).

Conversely, let A be any 2-absorbing ideal of S and $x \in \sqrt{A}$. Then $x^2 \in A = A^2$, since A is 2-absorbing ideal of S. This implies $x \in A$, so $A = \sqrt{A}$. Since prime ideals are linearly ordered so A is prime and hence S is a 2-AB semigroup. □

Since in a fully idempotent semigroup S, $A = A^2$ for every ideal A of S, the following is a simple consequence of above theorems:

Corollary 3.8. *A fully idempotent semigroup S is a 2-AB semigroup if and only if one of the following conditions hols:*

(1) *Prime ideals are linearly ordered.*

(2) *Every 2-absorbing ideal is of the form P^2, where P is a prime ideal of S.*

Theorem 3.9. *A semigroup S is a 2-AB semigroup if and only if its prime ideals are linearly ordered and $A = \sqrt{A}$ for every 2-absorbing ideal A of S.*

Proof. Let S be a 2-AB semigroup. Then prime ideals of S are linearly ordered (Theorem 3.3). Again any 2-absorbing ideal A of S is prime so $A = \sqrt{A}$.

Conversely, let A be a 2-absorbing ideal of S. Then $A = \sqrt{A} = \bigcap P_i = P_\beta$, for some $\beta \in \Lambda$ and where $\{P_i : i \in \Lambda\}$ are prime ideals containing A. Hence S is a 2-AB semigroup. □

Since in a semiprimary semigroup prime ideals are linearly ordered (Theorem 1.1), the following corollary is an obvious consequence of the above theorem:

Corollary 3.10. *A semiprimary semigroup S is a 2-AB semigroup if and only if $A = \sqrt{A}$ for every 2-absorbing ideal A of S.*

Theorem 3.11. *For a commutative regular semigroup S the following statements are equivalent:*

(1) *S is 2-AB semigroup.*

(2) *2-absorbing (prime) ideals are linearly ordered.*

(3) *Idempotents in S form a chain under natural ordering.*

(4) *All ideals of S are linearly ordered.*

(5) *S is a fully prime semigroup.*

(6) *S is a primary semigroup.*

(7) *S is a semiprimary semigroup.*

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) by Theorem 3.3.

(3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (6) $\Rightarrow$ (7) follows from Theorem 2.4 of [11].

(7) $\Rightarrow$ (1). Let A be a 2-absorbing ideal of a commutative regular semigroup S. Then $A = \sqrt{A} = \bigcap P_\alpha$, where $\{P_\alpha : \alpha \in \Lambda\}$ are the prime ideals of S contaning

A. Since S is semiprimary, so prime ideals are linearly ordered, which implies $A = \sqrt{A} = P_\beta$ for some $\beta \in \Lambda$. Therefore S is a 2-AB semigroup. $\square$

Let $\mathcal{D}$ be the class of commutative semigroups with an identity element and having no proper essential congruences, i.e. congruences δ such that $\alpha \cap \delta \neq i$ for every congruence $\alpha \neq i$, where i is the identity relation on S. Oehmke [8], proved that if $S \in \mathcal{D}$, then the set of ideals of S are linearly ordered by inclusion and hence the set of prime ideals of S are linearly ordered. Again Khaksari [6], proved that if $S \in \mathcal{D}$, then S is regular i.e. $A = \sqrt{A}$ for every ideal A of S. So as a simple consequence of Theorem 3.9, we have the following result:

Corollary 3.12. *If $S \in \mathcal{D}$, then S is a 2-AB semigroup.*

Theorem 3.13. *If every 2-absorbing ideal of a semigroup S has an idempotent generator, then S is a 2-AB semigroup.*

Proof. Let I be a 2-absorbing ideal of S generated by the idempotent e i.e. $I = (e) = eS$. Since S is commutative so $I = I^2$. It is clear that $I \subseteq \sqrt{I}$. Let $x \in \sqrt{I}$. Then $x^2 \in I = I^2$, since I is 2-absorbing. This implies $x \in I$, so $\sqrt{I} \subseteq I$. Hence $I = \sqrt{I}$. Again, let P, Q be two prime ideals of S. Then the prime ideal $P \cup Q$ is 2-absorbing, has an idempotent generator e, i.e. $P \cup Q = eS$. But then $e \in P$ or $e \in Q$. This implies either $P = eS$ or $Q = eS$ and either $P \subseteq Q$ or $Q \subseteq P$. Hence by Theorem 3.9, S is a 2-AB semigroup. $\square$

Since every principal ideal of a commutative regular semigroup has an idempotent generator, the following is an obvious consequence of the above theorem:

Corollary 3.14. *If every 2-absorboing ideal of a commutative regular semigroup S is principal, then S is a 2-AB semigroup.*

Acknowledgements. The authors are grateful to prof. Sujit Kumar Sardar of Jadavpur University for constant encouragement and active guidence throughout the preparation of the paper. We are also thankful to the anonymous referee for making some valuable suggesitions.

References

[1] **A. Badawi**, *On 2-absorbing ideals of commutative rings,* Bull. Austral. Math. Soc. **75** (2007), 417–429.

[2] **D. Bennis and B. Fahid**, *Rings in which every 2-absorbing ideal is prime,* Beitr. Algebra Geom. **59** (2017), 391–396..

[3] **H. Cay, H. Mostafanasab, G. Ulucak and U. Tekir**, *On 2-absorbing and strongly 2-absorbing ideals of commutative semigroups,* An. Ştiinţ. Univ. Al. I. Cuza Iaşi. Math. **62** (2016), 871–881.

[4] **A.H. Clifford and G.B. Preston**, *The algebric theory of semigroup,* Vol I, Am. Math. Soc. (1961).

[5] **A.Y. Darani and E.R. Puczylowski**, *On 2-absorbing commutative semigroups and their application to rings,* Semigroup Forum **86** (2013), 83–91.

[6] **A. Khaksari, S.J. Bavaryani and Gh. Moghimi**, *Fully prime semigroup,* Pure Math. Sci. **1** (2012), 25–27.

[7] **H. Lal**, *Commutative semi-primary semigroups,* Czechoslovak Math. J. **25** (1975), 1–3.

[8] **R.H. Oehmke**, *On essential right congrurences of a semigroup,* Acta Math. Hungar. **57** (1991), 73–83.

[9] **M. Satyanarayana**, *Commutative semigroups in which primary ideals are prime,* Math. Nachr. **48** (1971), 107–111.

[10] **M. Satyanarayana**, *A class of commutative semigroups in which idempotents are linearly ordered,* Czechoslovak Math. J. **21** (1971), 633–637.

[11] **M. Satyanarayana**, *Commutative primary semigroups,* Czechoslovak Math. J. **22** (1972), 509–516.

[12] **S. Schwartz**, *Prime ideals and maximal ideals in semigroups,* Czechoslovak Math. J. **19** (1969), 72–79.

Received December 10, 2020

Department of Mathematics, Jadavpur University, Kolkata-700032, India
Emails: biswaranjanmath91@gmail.com (B. Khanra), manasi_ju@yahoo.in (M. Mandal)

Quasigroups and Related Systems **29** (2021), 223 – 242

Semisymmetric quasigroups as alignments on abstract polyhedra

Kyle M. Lewis

Abstract. A quasigroup satisfying the identity $x(yx) = y$ is called semisymmetric; if a semisymmetric quasigroup is commutative, then it is totally symmetric. We demonstrate a bijection between totally symmetric quasigroups and directed graphs satisfying certain specifications. Further, we demonstrate a bijection between semisymmetric quasigroups and certain mappings between abstract polyhedra and directed graphs, termed alignments.

1. Introduction

As a class, the semisymmetric quasigroups arguably warrant particular interest due to both their algebraic and their combinatorial properties – commutative semisymmetric i.e. totally symmetric quasigroups have been an object of study for almost as long as quasigroups themselves [1]. There is a well-known bijection between idempotent totally symmetric quasigroups and the combinatorial block designs known as Steiner triple systems [2]; this further links totally symmetric quasigroups to finite geometry, as the Steiner triple system of order 7 is equivalent to the finite projective plane of order 2, and the Steiner triple system of order 9 is equivalent to the finite affine plane of order 3 [11]. Notably, via the semisymmetrization functor described by Smith [16], as well as the similar Mendelsohnization functor described by Krapež and Petrić [12], [17], it is possible to reduce homotopisms between arbitrary quasigroups to homomorphisms between semisymmetric quasigroups.

In this paper, we first lay groundwork by establishing a novel bijection between totally symmetric quasigroups and directed graphs meeting certain specifications. There have been several graph theoretic approaches applied to the study of quasigroups in the past [3], [9]; the main advantages of the schema implemented here are that the diagrams remain relatively simple, yet we are still able to fully recover the structure of any given (totally symmetric) quasigroup from its associated directed graph, even such that new quasigroups can be constructed starting only with a set of rules for constructing digraphs. Then, we expand this result to demonstrate a link between semisymmetric quasigroups and abstract polytopes, which are a combinatorial generalization of more traditional, geometric polytopes [5], [13].

2010 Mathematics Subject Classification: 05B07, 05C25, 20N05
Keywords: quasigroup, semisymmetric quasigroup, totally symmetric quasigroup, abstract polytope

Specifically, we demonstrate a bijection between semisymmetric quasigroups and objects we will refer to as *alignments*, which represent mappings between abstract polyhedra and directed graphs. Likewise, up to isomorphism the full structure of a semisymmetric quasigroup will be shown to be recoverable from its associated alignment and vice versa.

2. Preliminaries

A *partial quasigroup* $(Q, \cdot)$ is a set Q with a binary operation $(\cdot)$ such that for some $a, b \in Q$ there exist (at most) unique elements $x, y \in Q$ such that $a \cdot x = b, y \cdot a = b$; if this relation is satisfied for all $a, b \in Q$, then it is *complete* or simply a *quasigroup* [2]. For brevity, we will denote $x \cdot y$ by juxtaposition xy. An *isomorphism* between partial quasigroups is a bijection $f : Q \to Q'$ such that $f(x) \cdot f(y) = f(xy)$ for all $x, y \in Q$, in which case Q and Q' are said to be *isomorphic*.

Given a quasigroup $(Q, \cdot)$, it is possible to define 5 conjugate or *parastrophic* operations [6], [15] such that:

$$x \cdot y = z \Leftrightarrow z/y = x \tag{1}$$

$$x \cdot y = z \Leftrightarrow x\backslash z = y \tag{2}$$

$$x \cdot y = z \Leftrightarrow y \circ x = z \tag{3}$$

$$x \cdot y = z \Leftrightarrow y//z = x \tag{4}$$

$$x \cdot y = z \Leftrightarrow z\backslash\backslash x = y \tag{5}$$

If Q satisfies any of the equivalent [16] identities:

$$y \cdot xy = x \tag{6}$$

$$yx \cdot y = x \tag{7}$$

$$x/y = yx \tag{8}$$

$$x\backslash y = yx \tag{9}$$

then it is said to be *semisymmetric*. If Q is both semisymmetric and commutative, then it is *totally symmetric*, abbreviated as a *TS-quasigroup*. Equivalently, Q is totally symmetric iff all of its parastrophic operations coincide with one another.

A *partial Steiner triple system of order n* is a pair (V, B) where V is an n-element set and B is a set of 3-element subsets of V, referred to as *Steiner triples*, where any 2-element subset of V is contained in at most 1 triple. A partial Steiner triple system is *complete* if every 2-element subset of N is contained in exactly 1 triple in B, in which case it is referred to as simply a *Steiner triple system* [2].

A *cyclic order* on 3 elements is a ternary relation θ such that for distinct elements x, y, z then $\theta(x, y, z) \Leftrightarrow \theta(z, x, y) \Leftrightarrow \neg\theta(z, y, x)$ [7]. We call a pair of cyclic orders of the form $\theta_1(x, y, a), \theta_2(y, x, b)$ *partial opposites*; that is, to say, they share $\geqslant 2$ common elements which are in reversed order in regards to each other. If partial opposites share all 3 elements, then they are simply *opposites*. The scope of this paper is limited to cyclic orders on 3 elements, and so we need not consider cyclic orders on larger sets.

A *partial Mendelsohn triple system* (W, C) is a generalization of a Steiner triple system where W is a set and C is set of 3-element subsets of W with some cyclic order, referred to as *Mendelsohn triples*, such that $(\{x, y, z\}, \theta) = (x, y, z)$ contains the ordered pairs (x, y),(y, z),(z, x), and no others. Likewise, any ordered pair of distinct elements $(x, y) : x, y \in W$ can be contained in at most 1 triple in C; if every possible ordered pair of distinct elements in W is contained in exactly 1 triple in C, then the system is *complete* and simply a *Mendelsohn triple system* [3].

A *multiset* is a generalization of a set allowing for multiple instances of each element. Similarly, an *extended Steiner system of order* n is a pair (V, B) where V is an n-element set and B is a set of 3-element submultisets of V, called *extended Steiner triples* wherein each 2-element multisubset of V is contained in exactly 1 extended Steiner triple. An *extended Mendelsohn system* is a pair (W, C) where W is a set and C is a set of *extended Mendelsohn triples* such that any ordered pair of not necessarily distinct elements $(a, b) : a, b \in M$ is contained within exactly 1 triple in C. That is to say, extended Steiner and Mendelsohn triple systems are simply triple systems that allow for the repetition of elements [3]. From hereon, we will assume all Steiner and Mendelsohn systems are extended, and as such we can safely use just *triples* and *triple systems* when there is no chance of confusion. Cyclic orders also extend to multisets – note that any cyclic order of the form $\theta(x, x, y)$ or $\theta(x, x, x)$ is opposite to itself.

Suppose some graded partially ordered set $(P, \leqslant)$ with strictly monotone rank function $\rho : P \to \{-1, 0, 1, 2, ..., n\}$ sending elements $f_i \in P$, called *faces*, to integer values such that there is some unique least face f_{-1} and some unique greatest face f_n such that $\rho(f_{-1}) = -1$ and $\rho(f_n) = n$. Faces of rank n are *n-faces* – we call 0-faces *vertices* and 1-faces *edges*. Faces f_1, f_2 are *incident* if $f_1 \leqslant f_2$ or $f_2 \leqslant f_1$. Any maximal totally ordered subset $F_i \subset P$ is a *flag*; each flag contains exactly $n + 2$ faces. 2 flags are *adjacent* if they differ by exactly 1 face. P is *strongly flag-connected* if for any 2 flags F_x, F_y in P, there is some sequence of flags $(F_0, F_1, ..., F_n)$ such that any 2 successive F_i, F_{i+1} are adjacent to each other, where $F_x = F_0, F_y = F_n$ and $F_x \cap F_y \subseteq F_i$ for all i. If for any pair of faces $f_x \leqslant f_z$ in P where $\rho(f_x) = i - 1, \rho(f_z) = i + 1$, there are exactly 2 faces f_{y1}, f_{y2} such that $f_x \leqslant f_{y1,2} \leqslant f_z$ and $\rho(f_{y1,2}) = i$, then P is said to satisfy the *diamond condition*; that is to say, any pair of incident faces that differ in rank by 2 have exactly 2 incident faces strictly between them.

A graded poset $(P, \leqslant)$ is an *abstract n-polytope* [5], [13], [14] if it has a unique least face of rank -1 and a unique greatest face of rank n, is strongly flag-connected, all flags contain exactly $n + 2$ faces, and it satisfies the diamond condition. An abstract 3-polytope is an *abstract polyhedron*. We will call a polyhedron *cubic* if its graph is 3-regular – that is to say, each vertex is incident to exactly 3 edges.

An *automorphism* on an abstract polytope P is an order-preserving bijection

$\varphi : P \to P$. From hereon, all polytopes will be assumed to be abstract and all quasigroups will be assumed to be finite.

3. Totally symmetric quasigroups and digraphs

3.1 Constructing didgraphs from quasigroups

There is a natural bijection between Steiner triple systems and totally symmetric quasigroups given by $S : Q \to S(Q)$ where Q is some partial TS-quasigroup and $S(Q) = (V, B)$ is the partial Steiner system over the same underlying set such that for $x, y, z \in Q$ then $\{x, y, z\} \in B$ if and only if $xy = z, yx = z, xz = y$. We will refer to partial Steiner systems as *isomorphic* to each other iff their corresponding partial quasigroups are isomorphic to each other, and likewise for individual Steiner triples.

Lemma 3.1. *There are exactly* 3 *isomorphism classes of Steiner triples: triples of the form* $\{x, x, x\}$ *(type* 1*), of the form* $\{x, x, y\}$ *(type* 2*), and of the form* $\{x, y, z\}$ *(type* 3*), where* $x \neq y \neq z$.

Proof. Any 2 triples $\{x, x, x\}, \{a, a, a\}$ are isomorphic by $\varphi(x) = a, \varphi(a) = x$. Any 2 triples $\{x, x, y\}, \{a, a, b\}$ are isomorphic by $\varphi(x) = a, \varphi(a) = x, \varphi(y) = b, \varphi(b) = y$. Any 2 triples $\{x, y, z\}, \{a, b, c\}$ are isomorphic by $\varphi(x) = a, \varphi(a) = x, \varphi(y) = b, \varphi(b) = y, \varphi(z) = c, \varphi(c) = z$. No isomorphism between triples of different types is possible because any mapping would necessarily either map unique values x, y to the same value a or map the a single value x to different values a, b. □

A partial triple system can be constructed through the union of any 2 triples with less than 2 elements in common. Necessarily then, said triples must either have exactly 1 element in common, in which case we will refer to them as *intersecting*, or they have no elements in common, making them *disjoint*. If 2 triples t_1, t_2 are intersecting such that t_1 has more instances of the intersecting element than t_2, we will say that t_2 *binds* to t_1 e.g. $\{1, 2, 3\}$ binds to $\{1, 1, 4\}$.

Proposition 3.2. *A partial Steiner triple system is uniquely determined up to isomorphism by the types of its constituent triples and the intersection between them.*

Proof. Given partial triple systems (V_1, B_1) where $B_1 = \{\{x_1, y_1, z_1\}, \{a_1, b_1, c_1\}\}$ and (V_2, B_2) where $B_2 = \{\{x_2, y_2, z_2\}, \{a_2, b_2, c_2\}\}$ there exists an isomorphism $\varphi(x_1) = x_2, \varphi(x_2) = x_1, \varphi(a_1) = a_2, \varphi(a_2) = a_1$ et cetera iff $\forall d_1, e_1 \in \cup B_1 \exists d_2, e_2 \in \cup B_2((d_1 = e_1) \Rightarrow (d_2 = e_2))$. This process can be continued inductively for the union of triple systems of arbitrarily greater (finite) order. □

Corollary 3.3. *Any given totally symmetric quasigroup is uniquely determined up to isomorphism by the types of its corresponding triples and the intersection between them.*

In light of this, we can devise a schema to represent totally symmetric quasigroups as directed graphs: for given partial totally symmetric quasigroup Q, let $D : Q \to D(Q)$ take it to the directed graph $D(Q)$ such that for every Steiner triple $t_i \in S(Q)$ there is exactly 1 vertex $v_i \in D(Q)$ and where for any $t_1, t_2 \mapsto v_1, v_2$ then v_1 directly succeeds v_2 if and only if t_2 binds to t_1. For example, given an example quasigroup Q_4 of order 4 with the Cayley table:

	1	**2**	**3**	**4**
1	1	2	4	3
2	2	1	3	4
3	4	3	2	1
4	3	4	1	2

we can derive the corresponding triples: $\{1{,}1{,}1\}, \{2, 2{,}1\}, \{3, 3, 2\}, \{4, 4, 2\}, \{1, 3, 4\}$, producing the directed graph:

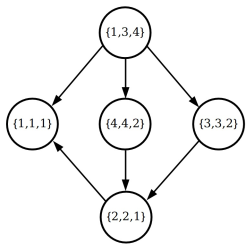

Figure 1: Labeled digraph of Q_4

The labels in figure 1 are purely for illustrative purposes; the final, unlabeled digraph is:

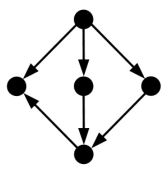

Figure 2: Unlabeled digraph $D(Q_4)$

We will refer to vertices in $D(Q)$ as being of the same *type* as the triples in $S(Q)$ they correspond to e.g. a type 1 vertex represents some triple of the form $\{x, x, x\}$. In general, if there is little chance for confusion we will use the same terminology between vertices in $D(Q)$ and the triples in $S(Q)$ which they represent.

Proposition 3.4. *Up to isomorphism, the full structure of any TS-quasigroup Q can be recovered from its directed graph D(Q).*

Proof. It is clear from the definition of an extended Steiner triple system that in any complete system (V, B) each element of its underlying set $x \in V$ must occur in exactly 1 triple either of the form $\{x, x, x\}$ or of the form $\{x, x, y\}$. It follows then that for given triples t_1, t_2 the only possible case in which t_2 can contain less instances of some shared element $x \in t_1, t_2$ is if t_2 contains exactly 1 instance of x and t_1 contains either 2 or 3 instances of x. That is to say, a given triple binds exactly once for each element it contains exactly 1 instance of. Therefore, the type of triple each vertex represents can be inferred from its outdegree: vertices with outdegree 0 map to type 1 triples, outdegree 1 to type 2 triples, and outdegree 3 to type 3 triples.

Given the digraph $D(Q)$, once the type of each vertex is identified, we may arbitrarily assign some bijective mapping between the type 1 and 2 vertices of the digraph and the elements of Q; that is to say, we label each type 1 and 2 vertex with a unique element of Q. Now, each vertex can be mapped to some triple as follows: type 1 vertices with label x are sent to $\{x, x, x\}$, type 2 vertices with label x binding to some vertex with label y are sent to $\{x, x, y\}$, type 3 vertices binding to some vertices with labels x, y, z (respectively) are sent to $\{x, y, z\}$. The union of these triples forms a triple system and thus a totally symmetric quasigroup. For example:

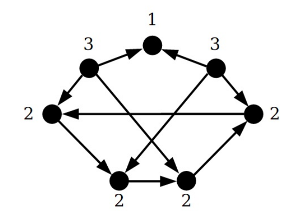

Figure 3: The type of each vertex in example diagram $D(Q_5)$

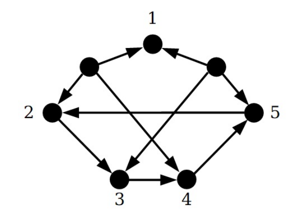

Figure 4: Arbitrary labeling of type 1 and type 2 vertices of $D(Q_5)$

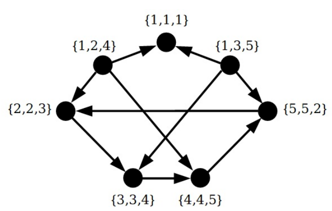

Figure 5: Deriving the corresponding triples for each vertex of $D(Q_5)$

Our choice in assigning type 1 and 2 vertices to elements of Q does not matter, because the type of each triple and the intersection between them are preserved and so by Corollary 3.3 any quasigroup produced by this method will be isomorphic to Q. In fact, every quasigroup isomorphic to Q on the same underlying set can be produced via permutations on the labels of the type 1 and 2 vertices of its digraph $D(Q)$. □

Corollary 3.5. *Every automorphism of a given TS-quasigroup Q corresponds to some graph isomorphism between permutations of labelings on the type 1 and 2 vertices of its directed graph $D(Q)$.*

3.2 Constructing quasigroups from digraphs

A complete extended Steiner triple system of order n contains:

$$\binom{n+2-1}{2} = \frac{1}{2}n(n+1) \tag{10}$$

(unordered) pairs of elements. As shown by Johnson and Mendelsohn in Section 3 of [8], given a triple system of order n, fixing the number of triples of any type also fixes the number of triples of each of the other 2 types. More specifically, where i is the number of type 1 triples, the number of type 3 triples must be equal to:

$$\frac{\frac{1}{2}n(n+1) - (i + 2(n-i))}{3} = n^2/6 - n/2 + i/3 \tag{11}$$

and therefore the number of type 1 triples i in a given triple system of order n must be such that:

$$3 \mid \frac{1}{2}n^2 - \frac{3}{2}n + i \tag{12}$$

A given element of a quasigroup $x \in Q$ such that $xx = x$ is called an *idempotent element* or simply an *idempotent* [3]; a quasigroup wherein all elements are idempotent is an *idempotent quasigroup.* It is readily apparent that each type 1 triple in a Steiner system specifies an element of its corresponding TS-quasigroup to be idempotent, and that each type 2 triple specifies an element not to be idempotent. By definition:

$$xx = y \Leftrightarrow xy = x \Leftrightarrow yx = x \tag{13}$$

and so these triples define not only the squares for each element $x^2 = y$ but also the local identities for each element $xy = x$. Let us define the subset: $U = \{y \in Q \mid x^2 = y, x \in Q\}$ as the *unique squares* of Q. On $D(Q)$, the unique squares correspond to the type 1 vertices together with the type 2 vertices which have at least 1 other type 2 vertex bound to them – this is equivalent to saying the unique squares are the elements that are either their own squares or the square of some other element.

Lemma 3.6. *For a TS-quasigroup of odd order n, $|U| = n$; all elements are unique squares.*

Proof. For elements of a TS-quasigroup $x, y, z \in Q$, by definition $xy = z \Leftrightarrow xz = y$. Then for any fixed x, we can define an involution $\varphi : Q \to Q$ sending $y \mapsto xy$. If n is odd, because φ is an involution there then must be some element z for which $\varphi(z) = z$ i.e. $xz = z$. Because Q is a quasigroup, there can be no y such that $xz = z, yz = z, x \neq y$; that is to say, if x acts as a local identity element for z, then it must be the only identity element for z. There being exactly n elements in Q, if some x were to act as an identity for more than 1 element, then there must be some y that cannot be an identity for any element – but as we established, every element of Q must be an identity for some other element. Therefore, each z maps uniquely to some local identity x, or alternatively, every element x is the unique square of some z. □

In informal terms, every row and column of the Cayley table for Q is some involution on the underlying set of Q, which means each row can be represented as the product of disjoint transpositions, but because n is odd for any row x there always must be some cell left over that cannot be swapped with any other cell. This defines the local identity for x and thus it also defines x^2; this must be unique because if another row had the same local identity for x there would be multiple instances of the same element in a single column.

Corollary 3.7. *For any TS-quasigroup Q of odd order, all type 2 vertices in $D(Q)$ are partitioned into cycles of length $\geqslant 3$.*

Proof. If all elements are unique squares, then each type 2 vertex must have at least 1 other type 2 vertex bound to it. Given that type 2 vertices have outdegree 1, they all must bind to other type 2 vertices, else there necessarily would be some type 2 vertex left over with no type 2 vertex bound to it. Assuming the number of vertices is finite, they will therefore be partitioned into cycles. There can be no 2-cycles as that would imply $\{\{x, x, y\}, \{y, y, x\}\}$, thus the pair $\{x, y\}$ would occur in more than 1 triple. □

Lemma 3.8. *For a TS-quasigroup of even order n, $1 \leqslant |U| \leqslant n/2$.*

Proof. As above, on TS-quasigroup Q we define an involution $\varphi : y \mapsto xy$ for some fixed x where $x, y \in Q$. If n is even, because φ is an involution for every y such that $\varphi(y) = y$ there must also be another distinct element $z \in Q$ where $\varphi(z) = z$; that is, any x must act as a local identity for an even number of elements in Q (0 being even). Conversely, every x must be the square of an even number of elements. It follows then that the maximum possible number of unique squares is $n/2$; trivially, there must be at least 1 unique square. □

Informally, because n is even there cannot be an odd number of unswapped cells in a given row of the Cayley table for Q.

Corollary 3.9. *In the digraph $D(Q)$ for a TS-quasigroup Q of even order, every type 1 vertex must have an odd number of type 2 vertices bound to it and every* *type* 2 *vertex must have an even number of type* 2 *vertices bound to it* (0 *being even*).

To summarize, for a TS-quasigroup Q of order n: the number of type 1 vertices i must be such that $3 \mid \frac{1}{2}n^2 - \frac{3}{2}n + i$. The number of type 2 vertices must be $n - i$. If n is odd, the type 2 vertices are partitioned into cycles of length $\geqslant 3$. If n is even, every type 1 vertex must have an odd number of type 2 vertices bound to it and every type 2 vertex must have an even number of type 2 vertices bound to it. We will refer to a given configuration of type 1 and 2 vertices meeting the aforementioned specifications as a *diagonal subgraph*.

Proposition 3.10. *For any TS-quasigroup Q, $D(Q)$ contains a diagonal subgraph as an induced subgraph. Further, up to isomorphism every diagonal subgraph can be mapped to some unique partial TS-quasigroup.*

Proof. By Corollaries 3.7 and 3.9, the induced subgraph containing only the type 1 and type 2 vertices of the digraph of a TS-quasigroup will always be a diagonal subgraph. Using the method specified in Proposition 3.4, we can always produce a partial Steiner system and therefore a partial TS-quasigroup with any arbitrary labeling of the vertices bijective with some set. Because this method preserves the types of triples and the intersections between them, by Corollary 3.3 this partial quasigroup is unique up to isomorphism for each unique diagonal subgraph. Triples in a diagonal subraph are all either of the form $\{x, x, x\}$ or $\{x, x, y\}$, and thus the only way for a given pair to show up more than once would be to label more than 1 vertex with the same element, which goes against the definition. □

However, not every diagonal subgraph can be made into a complete TS-quasigroup. There must be $n^2/6 - n/2 + i/3$ type 3 triples in a complete Steiner system, and each corresponding type 3 vertex must bind to exactly 3 type 1 or type 2 vertices. Further, no 2 type 3 vertices may bind to more than 1 shared vertex, as this would imply 2 triples that shared more than 1 common element. Finally, no type 3 vertex may bind to 2 vertices a, b where a is bound to b; this would imply some $\{\{x, y, z\}, \{x, x, y\}, \{y, y, w\}\}$ and thus the pair $\{x, y\}$ is contained in more than 1 triple. A directed graph composed (solely) of a diagonal subgraph and a set of type 3 vertices meeting the aforementioned specifications is *complete*.

Theorem 3.11. *Up to isomorphism, there exists a bijection between complete digraphs and totally symmetric quasigroups such that the full structure of a unique totally symmetric quasigroup can be recovered from any complete digraph and vice versa.*

Proof. Given any diagonal subgraph and some bijective labeling from some set to the vertices, it is readily apparent that any completion via the addition of bound type 3 vertices is equivalent to the specification of a set of triples, each containing exactly 3 distinct elements of the set. If any 2 of these type 3 triples shared more than 1 common element between them, they would necessarily bind to more than

1 shared vertex and thus violate the definition of a complete digraph. If any of these type 3 triples shared more than 1 common element with some type 2 triple, it would also necessarily bind to the triple said type 2 binds to and thus violate the definition of a complete digraph. Clearly, a type 3 triple cannot share more than 1 common element with a type 1 triple. There being $n^2/6 - n/2 + i/3$ type 3 triples ensures by the pigeonhole principle that every possible pair of elements of the set is accounted for in some triple. By Corollary 3.3, any 2 digraphs corresponding to isomorphic quasigroups are necessarily isomorphic to each other. By Proposition 3.4, every totally symmetric quasigroup corresponds to a directed graph, and thus the bijection is complete. □

Corollary 3.12. *Every subquasigroup of any TS-quasigroup Q appears as an induced subgraph of $D(Q)$.*

The methodology described here for constructing digraphs from TS-quasigroups is compatible with that of Khatirinejad et al. in [10] for constructing digraphs from Mendelsohn triple systems, which are equivalent to idempotent, semisymmetric quasigroups [17]. Specifically, given any idempotent TS-quasigroup Q, we can construct a Khatirinejad et al. digraph from $D(Q)$ by replacing each type 3 vertex with a set of 6 vertices arranged into 2 cyclically ordered triangles (as each Steiner triple is equivalent to 2 Mendelsohn triples).

Remark 3.13. There is known to exist a bijection between idempotent TS-quasigroups of order n and TS-quasigroups of order $n + 1$ with a (global) identity element [4]. This can be represented graphically as follows: given the digraph of some idempotent, TS-quasigroup, add 1 additional type 1 vertex, then bind every other type 1 vertex to the added vertex, converting them to type 2 vertices.

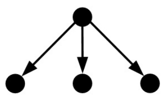

Figure 6: Example idempotent quasigroup Q_3

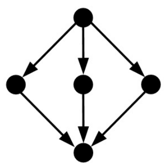

Figure 7: Derived quasigroup with identity V_4 (the Klein 4-group)

Note that 1 of the arrows in Figure 2 is in the opposite orientation to that of its counterpart in Figure 7, distinguishing Q_4 and V_4 as nonisomorphic quasigroups.

4. Quasigroups and abstract polyhedra

4.1 Constructing polyhedra from quasigroups

Similarly to Steiner systems and totally symmetric quasigroups, there exists a natural bijection between Mendelsohn triple systems and semisymmetric quasigroups given by $M : Q \to M(Q)$ where Q is a given partial semisymmetric quasigroup and $M(Q) = (W, C)$ is the partial Mendelsohn system over the same underlying set such that for elements $x, y, z \in Q$ then $(x, y, z) \in C$ if and only if $xy = z, yz = x, zx = y$; note that because semisymmetric quasigroups are not necessarily commutative, this does not necessarily imply $yx = z, zy = x, xz = y$.

Lemma 4.1. *There exist exactly* 3 *isomorphism classes of extended Mendelsohn triples.*

Proof. The same reasoning applied to Steiner systems in Lemma 3.1 equally applies to Mendelsohn systems. □

Indeed, type 1 and type 2 Mendelsohn triples behave similarly to their Steiner counterparts in that they specify squares and local identities and are also commutative: type 1 triples (x, x, x) trivially imply $xx = x$, type 2 triples (x, x, y) imply $xx = y, yx = x, xy = x$. Type 3 Mendolsohn triples, however, have a more complex structure in that $(x, y, z) \neq (z, y, x)$. As such, we will need to devise a new schema to represent type 3 Mendelsohn triples.

For given partial semisymmetric quasigroup Q, let $G : Q \to G(Q)$ take it to the (undirected) multigraph $G(Q)$ such that for every type 3 Mendelsohn triple $t_i \in M(Q)$ there is exactly 1 vertex $v_i \in G(Q)$ and where for any $t_1, t_2 \mapsto v_1, v_2$ then there is exactly 1 edge linking v_1 to v_2 for every pair of elements t_1 and t_2 have in common. Thus, 2 vertices are adjacent if and only if the triples they represent share at least 2 elements in common e.g. $(1, 2, 3)$ is adjacent to $(2, 1, 4)$ but not to $(1, 5, 6)$. As above, we will use the same terminology between vertices in $G(Q)$ and the triples they represent in $M(Q)$ when expedient.

To illustrate, from an example semisymmetric quasigroup Q_{4s} with Cayley table:

	1	**2**	**3**	**4**
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

we can derive 4 type 1 triples $\{(1, 1, 1), (2, 2, 2), (3, 3, 3), (4, 4, 4)\}$ and 4 type 3 triples $\{(1, 2, 3), (1, 3, 4), (1, 4, 2), (2, 4, 3)\}$. This would produce the graph:
or unlabeled:

For given semisymmetric quasigroup Q, let us define a relation $\rightleftharpoons$ on the type 3 triples of $M(Q)$ such that $a \rightleftharpoons b$ for $a, b \in M(Q)$ if and only if their corresponding

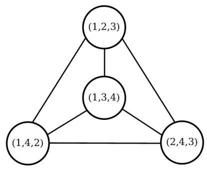

Figure 8: Labelled graph of Q_{4s}

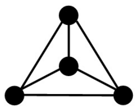

Figure 9: Unlabeled graph $G(Q_{4s})$

vertices in $G(Q)$ are connected. Because connectivity is reflexive, symmetric, and transitive, $\rightleftharpoons$ is then an equivalence relation; we will refer to the partial quasigroups corresponding to the equivalence classes of type 3 triples in $M(Q)$ under $\rightleftharpoons$ as the *components* of Q. A partial quasigroup q such that any $t_1, t_2 \in M(q)$ are type 3 triples corresponding to vertices of degree 3 in $G(q)$ and $t_1 \rightleftharpoons t_2$ we will call a *free component*. That is to say, a free component q is a partial quasigroup composed of type 3 triples where $G(q)$ is connected and where adding any further type 3 triple to $M(q)$ would make $G(q)$ disconnected.

Lemma 4.2. *Given a complete semisymmetric quasigroup Q, $G(Q)$ will be 3-regular; further, $G(q)$ will be 3-regular for every component q of Q.*

Proof. Each type 3 Mendelsohn triple contains exactly 3 ordered pairs of elements, and because Q is complete then for each ordered pair (x, y) in a type 3 triple there also must be some triple containing (y, x). If there were some type 2 triple containing (y, x), then necessarily (y, x, x) or (y, y, x), which would make (x, y) appear in more than 1 triple, and trivially no type 1 triple can contain (y, x), so (y, x) must be contained in some other type 3 triple, which will be adjacent by definition. Therefore, every vertex must be incident to exactly 3 edges, each edge corresponding to an unordered pair $\{x, y\}$. By definition any vertices in $G(Q)$ connected to any vertex in $G(q)$ of any component q are also within $G(q)$, thus $G(q)$ for every component of Q must also be 3-regular. $\square$

Corollary 4.3. *Every component of a complete semisymmetric quasigroup is isomorphic to some free component.*

In some cases, $M(Q)$ may contain triples of the form $\{(x, y, z), (z, y, x)\}$, that is to say, pairs of triples containing the same elements but in opposite order; we will call these *commutative pairs*. In $G(Q)$, these pairs correspond to the multigraph:

Figure 10: Multigraph of a commutative pair

Remark 4.4. A semisymmetric quasigroup is totally symmetric if and only if all of its components are commutative pairs.

Lemma 4.5. *For any free component q, if q is not a commutative pair, then $G(q)$ is a simple graph.*

Proof. By definition, any vertex $v \in G(q)$ must have 3 incident edges. If all edges connect to 1 other vertex, then their corresponding triples in $M(q)$ have all 3 pairs of elements in common and thus q is a commutative pair. If v were linked to some other vertex by exactly 2 edges, this would imply there are 2 triples that have 2 pairs of elements in common, but not the 3rd, which is clearly combinatorially impossible. Then if q is not a commutative pair, any $v \in G(q)$ will have 3 edges linking to 3 separate vertices, thus $G(q)$ is a simple graph. □

For a given free component q, let a cycle $c_x \in G(q)$ be an *element-cycle* for x iff for every vertex in c_x, its corresponding triple in $M(q)$ contains x. Define a *cycle structure* on q to be a surjection $C : G(q) \to q$ sending each element-cycle in $G(q)$ to an element of q such that if $c_x \mapsto x$ then c_x is an element-cycle for x.

Lemma 4.6. *For any commutative pair q, up to isomorphism there exists exactly* 1 *cycle structure on q.*

Proof. All vertices in $G(q)$ represent triples in $M(q)$ containing all elements of q, so all cycles qualify as element-cycles. There are 3 elements of q and there are 3 cycles in $G(q)$, so any surjection must assign 1 cycle to each element. $G(q)$ is vertex transitive and edge transitive, therefore any such assignment will be equivalent up to isomorphism. □

Proposition 4.7. *For any free component q, if q is not a commutative pair, then there exists exactly* 1 *cycle structure on q.*

Proof. For a given triple $t_1 = (x, y, z) \in M(q)$, consider an element x; by definition, $G(q)$ is 3-regular, therefore there exist edges linking t_1 to vertices containing (y, x) and (x, z). $G(q)$ is simple, therefore these edges link to distinct vertices $t_2 = (y, x, a)$ and $t_3 = (x, z, b)$ where $a \neq b$. The 3rd edge must link to some vertex containing (z, y), and this vertex cannot contain x, else the pairs (y, x) or (x, z) would appear in more than 1 triple. Now, t_2 must be adjacent to t_1, some vertex $t_4 = (x, d, a)$, and some 3rd vertex which also cannot contain x else (x, a) or (a, x) would appear in more than 1 triple. Likewise, t_3 is adjacent to t_1, some vertex $t_5 = (x, b, e)$, and a 3rd vertex not containing x. So then t_4 must be adjacent to some vertex containing (d, x), and t_5 must be adjacent to a vertex containing

(x, e), and so on. Assuming the number of triples and therefore vertices is finite, there must eventually be some vertex (x, e, d) linking these 2 trails into a closed cycle c_x.

All vertices in c_x contain x, so then c_x is an element-cycle for x; thus for any triple in $M(q)$ and any element contained in that triple, there exists an element-cycle in $G(q)$ for that element. Further, as demonstrated, any vertex adjacent to a vertex in c_x which is not contained in c_x cannot contain x, so c_x is the only possible element cycle for x for any vertex in c_x. If there were some element $f \in q$ such that c_x was also an element cycle for f, then there would be multiple triples containing (x, f) or (f, x). Therefore, any cycle structure C has only 1 possible mapping from cycles to elements. By definition, any element in q must be represented in some vertex of $G(q)$, so then C is a surjection. □

Given that for any free component q there always exists a cycle structure on $G(q)$ unique up to isomorphism for commutative pairs and fully unique for simple $G(q)$, from hereon we can safely assume the cycle structure on any free component. It is therefore meaningful to speak of *the* element-cycles of a given q.

Corollary 4.8. *Each vertex of $G(q)$ is contained within exactly 3 element-cycles.*

Lemma 4.9. *For some free component q, any 2 element-cycles in $G(q)$ either share exactly 2 common vertices that are adjacent to each other, or they share no common vertices.*

Proof. Given graph $G(q)$ containing element-cycles c_x, c_y for elements $x, y \in q$, if they share a common vertex it must be representative of some triple containing the pair (x, y) or the pair (y, x). The existence of a triple containing (x, y) necessarily implies the existence of some triple containing (y, x) and vice versa, and because they share 2 common elements by definition they are adjacent. There cannot be any more triples containing (x, y) or (y, x) and thus there are no more common vertices shared by c_x and c_y. □

Lemma 4.10. *For some free component q, each edge in $G(q)$ is contained within exactly 2 element-cycles.*

Proof. By definition, every edge in $G(q)$ links 2 vertices representing triples containing 2 shared elements, and by Proposition 4.7 there can be no adjacent vertices sharing a common element not contained within a shared element-cycle. An edge cannot be in more than 2 element-cycles for any graph with > 2 vertices because that would imply 2 triples sharing more than 2 common elements, and it cannot be in more than 2 element cycles for any graph with 2 vertices because that would necessitate a cycle with length > 2. □

Proposition 4.11. *The graph of any free component is isomorphic to the graph of some cubic abstract polyhedron.*

Proof. We use the work of Murty in [13]: Lemmas 4.9 and 4.10 satisfy Murty's Lemmas 2.2 (i) and (ii), therefore by Murty's Theorem 2.11, the graph of any free component satisfies the necessary and sufficient conditions to be that of a cubic abstract 3-polytope i.e. an abstract polyhedron, where each element-cycle is equivalent to some 2-face. □

Further, by Murty's Theorem 2.8, any 2 abstract polytopes with the same 2 dimensional skeleton are isomorphic, thus we can specify the polyhedron associated with any given free component via its element-cycles. Define $P : q \to P(q)$ taking some free component q to the cubic polyhedron $P(q)$ such that each element-cycle $c_i \in G(q)$ is sent to its equivalent 2-face in $P(q)$. For any cubic polyhedron p, we define a *labeling* on p to be a function $L : p \to X$ sending each 2-face of p to an element of some set X such that for every edge in p incident to 2-faces f_1, f_2, the (unordered) pair $\{L(f_1), L(f_2)\}$ is unique.

4.2 Constructing quasigroups from polyhedra

For quasigroup $(Q, \cdot)$ we will refer to the parastrophic quasigroup $(Q, \circ)$ such that $x \cdot y = z \Leftrightarrow y \circ x = z$ as the *transpose* of $(Q, \cdot)$; or alternatively, Q^T is the transpose of Q. A totally symmetric quasigroup and its transpose are exactly identical (indeed, this is true for any commutative quasigroup). By definition, a strictly semisymmetric quasigroup and its transpose are not identical, but sometimes they are isomorphic. This is somewhat problematic, as heretofore our procedure cannot distinguish between a semisymmetric quasigroup and its transpose – both will produce the same graph, even if they are not isomorphic to each other. We must devise a way to differentiate between parastrophes, but also a way to identify when they are essentially the same.

Conveniently, because we can now map components of semisymmetric quasigroups to polyhedra, we can also assign them an orientation. Define an *oriented vertex* to be the pair $\hat{v} = (v, \theta)$, where v is a vertex of some polyhedron p and θ is some cyclic order on the 2-faces incident to v, called an *orientation* on v. Let an *oriented polyhedron* be the pair $\hat{p} = (p, \Theta)$ where p is some cubic polyhedron and $\Theta : V \to \Theta(V)$ is a function on the vertices $V \subset P$ sending each vertex $v_i \mapsto \hat{v_i}$ to an oriented vertex such that the orientation for any $\hat{v_1}$ is a partial opposite that of any adjacent vertex $\hat{v_2}$. We will refer to Θ as an *orientation* on p.

Lemma 4.12. *There are at most* 2 *possible orientations on any given polyhedron* p.

Proof. Suppose we fix the orientation for some vertex $\hat{v_1}$ such that $\theta_1(f_1, f_2, f_3)$. Then any adjacent vertex $\hat{v_2}$ sharing incident 2-faces f_1, f_2 must be partial opposite such that $\theta_2(f_2, f_1, -)$, and likewise for all other adjacent vertices. So fixing a single vertex therefore fixes all connected vertices, and since all vertices in p are connected and there are only 2 possible cyclic orders on a set of 3 elements, there are at most 2 possible orientations on p. □

Proposition 4.13. *Given some oriented polyhedron $\hat{p}$, any labeling on $\hat{p}$ specifies a unique free component q_p.*

Proof. A labeling on $\hat{p}$ identifies each 2-face with some set element such that every edge is incident to a unique pair of elements, and each oriented vertex $\hat{v_i} \in \hat{p}$ specifies a cyclic order on its incident 2-faces, thus each $\hat{v_i}$ specifies a cyclic order on 3 distinct set elements and is therefore equivalent to a type 3 Mendelsohn triple. By the definition of a cubic polyhedron, there are exactly 2 vertices $\hat{v_1}, \hat{v_2}$ incident to any pair of 2-faces $\{f_1, f_2\}$, and by the definition of an orientation on p then $\hat{v_1}$ and $\hat{v_2}$ must have opposite orientations relative to f_1 and f_2; therefore no ordered pair (f_1, f_2) occurs in $\hat{p}$ more than once. The graph of $\hat{p}$ is connected and 3-regular so necessarily the partial quasigroup q_p it defines is a free component. Any other polyhedron that defines the same q_p would necessarily have the same faces, labels, and orientation as $\hat{p}$ and thus be identical to $\hat{p}$; therefore q_p is unique. □

For given free component q, define $\hat{P} : q \to \hat{P}(q)$ as the function taking q to the oriented polyhedron $\hat{P}(q)$ such that for each triple $t_i \in M(q)$ is sent to a corresponding oriented vertex $t_i \mapsto \hat{v_i}$.

For given cubic polyhedron p, consider the action of its automorphism group $\mathrm{Aut}\,(p)$ on its 2-faces; let us denote the orbit of a 2-face f_i under this action as $\mathrm{Aut}\,(p) \cdot f_i$. Given any 2 vertices $v_1, v_2 \in p$ with incident 2-faces $\{f_1, f_2, f_3\}$ and $\{f_4, f_5, f_6\}$, respectively, then by definition if there is some $\varphi \in \mathrm{Aut}\,(p)$ sending $v_1 \mapsto v_2$ then necessarily

$$\{\mathrm{Aut}\,(p)\cdot f_1, \mathrm{Aut}\,(p)\cdot f_2, \mathrm{Aut}\,(p)\cdot f_3\} = \{\mathrm{Aut}\,(p)\cdot f_4, \mathrm{Aut}\,(p)\cdot f_5, \mathrm{Aut}\,(p)\cdot f_6\} \quad (14)$$

that is to say, for any vertices in the same orbit, the set of orbits of their incident 2-faces must also be the same. However, given some orientation on p, the order of incident 2-faces relative to $\hat{v_1}$ and $\hat{v_2}$ may be different. If some $\varphi \in \mathrm{Aut}\,(p) : v_1 \mapsto v_2$ and the orbits of the faces incident to corresponding oriented vertices $\hat{v_1}$ and $\hat{v_2}$ are in opposite order, we will call them *opposite vertices*. Any vertex which is opposite to itself is a *self-opposite vertex*.

Proposition 4.14. *A free component q is isomorphic to its transpose q^T if and only if there exists some automorphism $\varphi : P(q) \to P(q)$ taking every vertex in $\hat{P}(Q)$ to some opposite vertex.*

Proof. By definition, q and q^T are identical in all respects except for the order of the elements in their constituent triples in $M(q), M(q^T)$, so as the (unordered) sets of elements and their intersections are preserved, $P(q) = P(q^T)$ without some orientation to distinguish between them. Therefore $\hat{P}(q^T)$ is simply $\hat{P}(q)$ with its orientation reversed. If there exists some $\varphi \in \mathrm{Aut}\,(P(q))$ taking every vertex to some opposite, it follows that $\hat{P}(q)$ is isomorphic to itself with reversed orientation i.e. $\hat{P}(q^T)$; then by Proposition 4.13 q is isomorphic to q^T. □

Let $D : Q \to D(Q)$ take semisymmetric quasigroup Q to directed graph $D(Q)$ such that for every type 1 or 2 triple in $t_i \in M(Q)$ there is exactly 1 vertex $v_i \in D(Q)$ and where for any $t_1, t_2 \mapsto v_1, v_2$ then v_1 directly succeeds v_2 if and only if t_2 binds to t_1. That is to say, D applies to the type 1 and 2 triples of semisymmetric quasigroups in the same way it does for totally symmetric quasigroups; as above, the number of type 1 and 2 vertices is equal to $|Q|$. Let any digraph such that each vertex has outdegree $\leqslant 1$ be a *semisymmetric diagonal subgraph.*

For a given oriented polyhedron $\hat{p}$ and a given semisymmetric diagonal subgraph d, let $\psi : \hat{p} \to d$ be any function taking each 2-face of $\hat{p}$ to some vertex of d such that for every edge in $\hat{p}$ incident to 2-faces f_1, f_2, the (unordered) pair $\{\psi(f_1), \psi(f_2)\}$ is unique and $\psi(f_1)$ does not bind to $\psi(f_2)$ or vice versa.

Lemma 4.15. *Given some oriented polyhedron $\hat{p}$ and some semisymmetric diagonal subgraph d, any ψ_i from $\hat{p}$ to d specifies a unique partial semisymmetric quasigroup q up to isomorphism.*

Proof. Suppose some bijective mapping between the vertices of d and the elements of some set X – it is clear that this is equivalent to a labeling on $\hat{p}$ given by $L : \hat{p} \to X$ maps each face of $\hat{p}$ to an element of X iff ψ_i sends that face to the vertex in d mapped to X. Therefore by Proposition 4.13 we now have a unique free component, and we derive all type 1 and 2 triples from d in the same way as we did for TS-quasigroups to produce a unique partial semisymmetric quasigroup q. The derived type 3 triples in $M(q)$ are self-consistent by Proposition 4.13 and the type 1 and 2 triples are self-consistent by Proposition 3.10. Supposing, then, there were some pair (x, y) contained in a type 3 triple (x, y, a) and a type 2 triple (x, x, y) – necessarily there would then be some other type 3 triple (y, x, b) forming an edge in $\hat{p}$ incident to faces f_x, f_y such that $\psi_i(f_x) = (x, x, y), \psi_i(f_y) = (y, y, -)$, meaning $\psi_i(f_x)$ binds to $\psi_i(f_y)$, which would violate the definition of the ψ function. It follows then that for any ψ_j that specifies a quasigroup isomorphic to q then the image of $\hat{p}$ under ψ_j must be isomorphic to the image of $\hat{p}$ under ψ_i; therefore, the mapping ψ_i is unique up to isomorphism. □

Suppose some diagonal subgraph d; each vertex of d represents an element of some semisymmetric quasigroup Q, and for every element $x \in Q$ there must be $|Q|$ unordered pairs $\{x, y\}$ represented within $M(Q)$. Each type 1 triple contains 1 pair and each type 2 triple contains 2 pairs, so we shall say that a type 1 vertex starts with a *bound weight* of 1 and a type 2 vertex starts with a bound weight of 2. Every type 2 triple bound to a given vertex corresponds to another pair of elements, so we add +1 bound weight to a vertex for every other type 2 vertex bound to it. Finally, for each face of a polyhedron 1 pair is represented for every edge, so we add the number of edges mapped to a vertex in d to its bound weight.

Define an *alignment* to be the ordered triple (d, O, Ψ) where d is some semisymmetric diagonal subgraph, $O = \{\hat{p_1}, \hat{p_2}, ..., \hat{p_n}\}$ some set of oriented polyhedra, and $\Psi = \{\psi_1, \psi_2, ..., \psi_n\}$ some set of functions $\psi_i : \hat{p_i} \to d$ taking each 2-face of its respective $\hat{p_i} \in O$ to some vertex in d such that for every edge in $\hat{p_i}$ incident to 2-faces f_1, f_2, the unordered pair $\{\Psi^{-1}(\psi_i(f_1)), \Psi^{-1}(\psi_i(f_2))\}$ is unique, where $\Psi^{-1}(v_i) = \{f_x|\psi_x(f_x) = v_i\}$, that is to say Ψ^{-1} is the preimage of $v_i \in d$ across all $\psi_x \in \Psi$. Further, there is no v_1 binding to v_2 such that some face $f_1 \in \Psi^{-1}(v_1)$ shares an incident edge with some $f_2 \in \Psi^{-1}(v_2)$, and the total bound weight for each $v_i \in d$ across all of Ψ is equal to $|d|$, the number of vertices in d. We will call 2 alignments A_1, A_2 *isomorphic* iff their sets of polyhedra O_1, O_2 are isomorphic to each other and the image of Ψ_1 in d_1 is isomorphic to the image of Ψ_2 in d_2.

Theorem 4.16. *Up to isomorphism, there exists a bijection between alignments and semisymmetric quasigroups such that the full structure of a unique semisymmetric quasigroup can be recovered from any alignment and vice versa.*

Proof. Suppose some alignment $A = (d, O, \Psi)$: by Lemma 4.15 each $\psi_i \in \Psi$ yields a unique partial semisymmetric quasigroup, so then the union of these partial quasigroups also produces a semisymmetric quasigroup Q. Because the bound weight of each $v_i \in d$ is equal to $|d|$, every possible pair of elements in Q must be represented and therefore Q is complete. If there were 2 type 3 triples $t_1, t_2 \in M(Q)$ both containing some ordered pair of elements (x, y), then this would imply there are faces $f_{1-4} \in \cup O$ such that f_1, f_2 share an incident edge and f_3, f_4 share an incident edge and there are some $\psi_i, \psi_j \in \Psi$ where $\psi_i(f_1) = \psi_j(f_3), \psi_i(f_2) = \psi_j(f_4)$, but this would violate the definition of an alignment because for any edge in $\cup O$ the image of its pair of incident faces must be unique across all Ψ. If there were a type 3 triple t_1 and a type 2 triple t_2 in $M(Q)$ both containing some ordered pair of elements (x, y), then this would imply some faces $f_1, f_2 \in \cup O$ such that $\psi_i(f_1)$ binds to $\psi_j(f_2)$, which also violates the definition of an alignment. Any alignment that yields a quasigroup isomorphic to Q would necessarily have a set of oriented polyhedra isomorphic to O mapping to an image isomorphic to $\Psi(O)$ and therefore be equivalent to A, thus A corresponds to a unique Q up to isomorphism.

Conversely, suppose some semisymmetric quasigroup Q': the diagonal subgraph is given by $D(Q')$. For each component $q'_i \in Q'$, we can derive an oriented polyhedron $\hat{P}(q'_i)$; let the set of all such $\hat{P}(q'_i)$ be $\hat{P}(Q')$. Finally, ψ_i for each $\hat{P}(q'_i)$ is given by simply mapping each 2-face corresponding to an element $x \in Q'$ to the vertex in $D(Q')$ corresponding to x; let the set of all such ψ_i be $\Psi_{Q'}$. Now we can define function $\alpha : Q' \to A' = (D(Q'), \hat{P}(Q'), \Psi_{Q'})$ taking any given semisymmetric quasigroup Q' to a unique alignment A' up to isomorphism, thus, the bijection is complete. □

For example, given an alignment A_5 on a triangular prism:

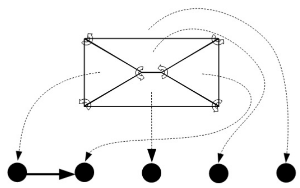

Figure 11: Diagram of alignment A_5

We can assign an arbitrary labeling to the type 1 and 2 vertices:

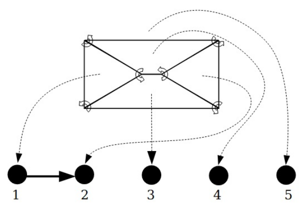

Figure 12: Arbitrary labeling on A_5

And derive the Mendelsohn triples corresponding to each vertex:

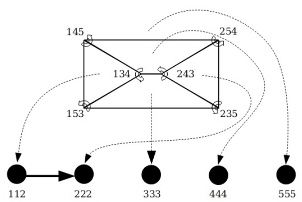

Figure 13: A_5 with derived triples

Yielding a semisymmetric quasigroup with the Cayley table:

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

Remark 4.17. Any labeling on a triangular prism produces a free component isomorphic to its transpose, so in the previous example the orientations on the vertices could have been omitted, but we retain them for illustrative purposes.

Acknowledgment. The author is very grateful to Wieslaw A. Dudek and Jonathan D. H. Smith for answering the author's questions via email, as well as to the reviewer for their helpful remarks.

References

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

[2] **D. Bryant**, *Completing partial commutative quasigroups constructed from partial Steiner triple systems is NP-complete*, Discrete Math., **309** (2009), 4700 − 4704.

[3] **V.E. Castellana and M.E. Raines**, *Embedding extended Mendelsohn triple systems*, Discrete Math., **252** (2002), 47 − 55.

[4] **C.J. Colbourn, M.L. Merlini-Giuliani, A. Rosa, and I. Stuhl**, *Steiner loops satisfying Moufang's theorem*, Austr. J. Combin., **63** (2015), 170 − 181.

[5] **G. Cunningham and M. Mixer**, *Internal and external duality in abstract polytopes*, Contrib. Discrete Math., **12 (2)** (2016). 187 − 21.

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

[7] **S. Haar**, *Cyclic ordering through partial orders*, J. Multiple-Valued Logic Soft Comput., **27 (2-3)** (2016), 209 − 228.

[8] **D.M. Johnson and N.S. Mendelsohn**, *Extended triple systems*, Aequationes Math., **8** (1972), 291 − 298.

[9] **B. Kerby and J.D.H. Smith**, *A graph-theoretic approach to quasigroup cycle numbers*, J. Combinatorial Theory (A), **118** (2011), 2232 − 2245.

[10] **M. Khatirinejad, P.R.J. Östergård, and A. Popa**, *The Mendelsohn triple systems of order 13*, J. Combinatorial Designs, **22** (2014), 1 − 11.

[11] **D. Král', E. Máčajová, A. Pór, and J.S. Sereni**, *Characterization results for Steiner triple systems and their application to edge-colorings of cubic graphs*, Canadian J. Math., **62** (2010), 335 − 381.

[12] **A. Krapež and Z. Petrić** *A note on semisymmetry*, Quasigroups and Related Systems, **25** (2017), 269 − 278.

[13] **K.G. Murty**, *The graph of an abstract polytope*, Math. Programming, **4** (1973), 336 − 346.

[14] **E. Schulte and G.I. Williams**, *Polytopes with preassigned automorphism groups*, Discrete and Computational Geometry, **54** (2015), 444 − 458.

[15] **V.A. Shcherbacov**, *On the structure of left and right F-, SM-, and E-quasigroups*, J. Generalized Lie Theory Appl.„ **3** (2009), 197 − 259.

[16] **J.D.H. Smith**, *Homotopy and semisymmetry of quasigroups*, Algebra Univers., **38** (1997), 175 − 184.

[17] **J.D.H. Smith**, *Semisymmetrization and Mendelsohn quasigroups*, Comment. Math. Univ. Carolin., **61** (2020), 553 − 566.

Received March 25, 2021

Boston, Massachusetts
United States
e-mail: KML112358@gmail.com

Quasigroups and Related Systems **29** (2021), 243 – 254

On transiso-class graphs

Surendra Kumar Mishra and *Ravindra Prasad Shukla*

Abstract. In this paper, we have determined the number of isomorphism classes of transversals of subgroups of order 2 and 5 of $Alt(5)$. Further, we have introduced two new graphs $\Gamma_{tic}(G)$ and $\Gamma_{d,tic}(G)$ on a finite group G, where d is the order of a subgroup of G and studied some properties of these graphs.

1. Introduction

Let G be a finite group and H be a subgroup of G. We say that a subset S of G is a normalized right transversal (NRT) of H in G, if S is obtained by choosing one and only one element from each right coset of H in G and $1 \in S$. For $x,\ y \in S$, define $\{x \circ y\} = S \cap Hxy$. Then with respect to this binary operation, S is a right loop with identity 1, that is, a right-quasigroup with both-sided identity (see [12, Proposition 4.3.3]). Conversely, every right loop can be embedded as an NRT in a group with some universal property (see [8, Theorem 3.4]).

Let S be an NRT of H in G. Let $\langle S\rangle$ be the subgroup of G generated by S and H_S be the subgroup $\langle S\rangle \cap H$. Then $H_S = \langle\{xy(x \circ y)^{-1} \,|\, x, y \in S\}\rangle$ and $H_S S = \langle S\rangle$ (see [8, Corollary 3.7]). Identifying S with the set $H \setminus G$ of all right cosets of H in G, we get a transitive permutation representation $\chi_S : G \to \mathrm{Sym}(S)$ defined by $\{\chi_S(g)(x)\} = S \cap Hxg, g \in G, x \in S$. The kernel $\ker\chi_S$ of this action is $\mathrm{Core}_G(H)$, the core of H in G. Let $G_S = \chi_S(H_S)$, the group torsion of the right loop S (see [8]). The group G_S depends only on the right loop structure $\circ$ on S and not on the subgroup H. Since χ_S is injective on S and if we identify S with $\chi_S(S)$, then $\chi_S(\langle S\rangle) = G_S S$ which also depends only on the right loop S and S is an NRT of G_S in $G_S S$. One can also verify that $\ker(\chi_S|_{H_S S} : H_S S \to G_S S) = \ker(\chi_S|_{H_S} : H_S \to G_S) = \mathrm{Core}_{H_S S}(H_S)$ and $\chi_S|_S =$ the identity map on S. Also, G_S is trivial if and only if $(S, \circ)$ is a group (see [8]).

We denote the set of all normalized right transversals (NRTs) of H in G by $\mathcal{T}(G, H)$. We say that S and $T \in \mathcal{T}(G, H)$ are isomorphic (denoted by $S \cong T$), if their induced right loop structures are isomorphic. Let $\mathcal{I}(G, H)$ denote the set of isomorphism classes of NRTs of H in G. It has been proved in [10] as well as in [7] that $|\mathcal{I}(G, H)| = 1$ if and only if $H \trianglelefteq G$. It has been shown in [4] that there is no pair (G, H) such that $|\mathcal{I}(G, H)| = 2$. It is easy to observe that if H is a non-normal subgroup of G of index 3, then $|\mathcal{I}(G, H)| = 3$. The converse of this statement is

2010 Mathematics Subject Classification: 20N05, 20D06, 20D60, 97K30
Keywords: Transversals; right loops; complete graphs.

proved in [5]. Also, it has been proved in [6] that there is no pair (G, H) such that $|\mathcal{I}(G, H)| = 4$. The integers 5, 6 also realized in this way (see [6]). It is easy to observe that if H is a subgroup of order 3 of $Alt(4)$, then $|\mathcal{I}(G, H)| = 7$. Therefore it seems an interesting problem to know that which integer appears as $|\mathcal{I}(G, H)|$ for some pair $(G,\ H)$.

In the Section 2, we have determined $|\mathcal{I}(G, H)|$, where $G = Alt(5)$ and H be a non-normal subgroup of G of order 2 or 5. In the Section 3, we have defined two new graphs associated to the isomorphism classes of transversal of a subgroup in a finite group and studied some properties of these graphs.

2. Isomorphism classes of transversals in $Alt(5)$

Now, we state the following proposition whose proof is essentially the same proof of the Proposition 2.7 in [10].

Proposition 2.1. *Let G be a finite group and H be a corefree subgroup of G. Let $T \in \mathcal{T}(G, H)$ such that $\langle T \rangle = G$. Let $\mathcal{O} = \{L \in \mathcal{T}(G, H) | T \cong L\}$. Then $Aut_H(G)$ acts transitively on the set $\mathcal{O}$.*

Remark 2.2. If G is a finite group and H a subgroup of G such that $Core_G(H)$ is nontrivial, then the number $|\mathcal{I}(G, H)|$ may be different from the number of $Aut_H(G)$-orbits in $\mathcal{T}(G, H)$. For example, let $G = \langle x, y | x^6 = 1 = y^2, yxy^{-1} = x^{-1} \rangle \cong D_{12}$, the dihedral group of order 12 and $H = \{1, x^3, y, yx^3\}$, where 1 is the identity of G. Then H is non-normal in G and $[G : H] = 3$. Hence $|\mathcal{I}(G, H)| = 3$. However, NRTs $\{1, x, x^2\}$, $\{1, yx, x^2\}$, $\{1, x, yx^2\}$ and $\{1, yx, yx^2\}$ to H in G, lie in different $Aut_H(G)$-orbits (as the set of orders of group elements in any two NRTs are not same).

Lemma 2.3. *Let L be a subgroup of $G = Alt(5)$ of order 12. Then $L \cong Alt(4)$, the alternating group of degree 4.*

Proof. Up to isomorphism, there are only 5 groups of order 12 (see [1, Theorem 5.1]),

1. $\mathbb{Z}_{12}$;
2. $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$;
3. D_{12}, the dihedral group of order 12;
4. $\langle x, y | x^4 = y^3 = 1, xy = y^2 x \rangle$;
5. $Alt(4)$.

Since G does not contain an element of order 12 or order 6 or order 4, hence it is not isomorphic to either of the groups in (1)-(4). Thus $L \cong Alt(4)$. □

Lemma 2.4. *Let K be a subgroup of $Sym(5)$ of order 20. Then K is isomorphic to the group $\langle x, y \mid x^5 = y^4 = 1, yxy^{-1} = x^2 \rangle$, which is the one dimensional affine group over $\mathbb{Z}_5$.*

Proof. Up to isomorphism, there are only five non-isomorphic groups of order 20 (see [3]),

1. $\mathbb{Z}_{20}$;
2. $\mathbb{Z}_{10} \times \mathbb{Z}_2$;
3. D_{20}, the dihedral group of order 20;
4. $M = \langle x, y \mid x^5 = y^4 = 1, yxy^{-1} = x^{-1} \rangle$;
5. $\langle x, y \mid x^5 = y^4 = 1, yxy^{-1} = x^2 \rangle$.

Since $Sym(5)$ does not contain an element of order 10, K cannot be isomorphic to the either of the groups $\mathbb{Z}_{20}$, $\mathbb{Z}_{10} \times \mathbb{Z}_2$, D_{20} and M. This implies that K is not isomorphic to either of the groups in (1) - (4) (we observe that $Z(M) = \langle y^2 \rangle$). Thus K is isomorphic to the group $\langle x, y \mid x^5 = y^4 = 1, yxy^{-1} = x^2 \rangle$. □

Remark 2.5. Let $G = Alt(5)$. Then $Aut(G) = Inn(Sym(5))$ (see [13, 2.17, p.299]). Since $Z(Sym(5)) = \{I\}$, we may identify $Aut(G)$ with $Sym(5)$ by identifying each $g \in Sym(5)$ with i_g, the inner automorphism of $Sym(5)$, determined by g ($x \mapsto gxg^{-1}$). Thus for a subgroup H of G, $Aut_H(G) = N_{Sym(5)}(H)$.

Proposition 2.6. *Let $G = Alt(5)$. Let H be a subgroup of G of order 5. Then $Aut_H(G)$ is isomorphic to $\langle x, y \mid x^5 = y^4 = 1, yxy^{-1} = x^2 \rangle$, the one dimensional affine group over $\mathbb{Z}_5$.*

Proof. Let H be a subgroup of G of order 5. Then by Remark 2.5, $Aut_H(G) = N_{Sym(5)}(H)$. Since there are 6 Sylow 5-subgroups in $Sym(5)$, $[Sym(5) : N_{Sym(5)}(H)] = 6$. This implies that $|N_{Sym(5)}(H)| = 20 = |Aut_H(G)|$. Now, the proposition follows from the Lemma 2.4. □

Proposition 2.7. *Let $G = Alt(5)$ and $H = \langle a = (12345) \rangle$. Let $S \in \mathcal{T}(G, H)$. Then $H \nsubseteq Stab_K(S)$, the stabilizer of S in K, where $K = N_{Sym(5)}(H)$ and the action of K is by conjugation.*

Proof. Let $S_0 = \{\alpha \in G : \alpha(5) = 5\}$. Then $S_0 \cong Alt(4)$ and $S_0 \in \mathcal{T}(G, H)$. Let $S_0 = \{I = a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}\}$, where $a_1 = (12)(34)$, $a_2 = (13)(24)$, $a_3 = (14)(23)$, $a_4 = (123)$, $a_5 = (132), a_6 = (124)$, $a_7 = (142), a_8 = (134)$, $a_9 = (143)$, $a_{10} = (234)$, $a_{11} = (243)$. Then there exists a unique map $\sigma : S_0 \to H$, with $\sigma(a_0) = a_0$ such that $S = S_\sigma = \{\sigma(a_i)a_i \mid 0 \leqslant i \leqslant 11\} \in \mathcal{T}(G, H)$. Assume that $Stab_K(S) \supseteq H$. Then

$$aSa^{-1} = S. \tag{1}$$

Now, $a\sigma(a_3)a_3a^{-1} = \sigma(a_3)aa_3a^{-1} = \sigma(a_3)a^2a_3$. Since $a\sigma(a_3)a_3a^{-1} \in S_\sigma$ $(= S)$, by (1), $\sigma(a_3)a^2a_3 \in S$. This gives $\sigma(a_3)a^2 = \sigma(a_3)$. This implies that $a^2 = I$, a contradiction. Thus $Stab_K(S) \not\supseteq H$. □

Corollary 2.8. *Let G, H, K and S be as in the Proposition* 2.7. *Then $Stab_K(S) \ncong D_{10}$, the dihedral group of order* 10. *Further, $Stab_K(S) \neq K$.*

Proof. We observe that K has only one subgroup L of order 10 isomorphic to the dihedral group D_{10}. Since L contains the subgroup H of K, by Proposition 2.7, $Stab_K(S) \neq L$. Since $H \subseteq K$, by Proposition 2.7 $Stab_K(S) \neq K$. □

Proposition 2.9. *Let $G = Alt(5)$ and $H = \langle(12345)\rangle$. Let $S \in \mathcal{T}(G,H)$ such that $\langle S\rangle = S$. Then $S = hS_0h^{-1}$, where $h \in H$ and $S_0 = \{\alpha \in G : \alpha(5) = 5\} \in \mathcal{T}(G,H)$.*

Proof. We observe that $S_0 = \langle(123),(124)\rangle \cong Alt(4)$. Let $S \in \mathcal{T}(G,H)$ such that $\langle S\rangle = S$. By Lemma 2.3, $S \cong S_0$. This implies that $S = \langle(abc),(def)\rangle$, where $a,b,c,d,e,f \in \{1,2,3,4,5\}$. Since $S \cong S_0$ and $|(123)(124)| = 2$, $|(abc)(def)| = 2$. This implies that $d = a$, $e = b$ and hence $S = \langle(abc),(abf)\rangle$, where a,b,c and f are distinct. Thus we have a permutation $\alpha \in Sym(5)$ with $\alpha(1) = a$, $\alpha(2) = b$, $\alpha(3) = c$, $\alpha(4) = f$ and $\alpha(5) = d_0$, where $d_0 \in \{1,2,3,4,5\} \setminus \{a,b,c,f\}$. Thus

$$\alpha S_0\alpha^{-1} = \big\langle\big(\alpha(1)\alpha(2)\alpha(3)\big),\big(\alpha(1)\alpha(2)\alpha(4)\big)\big\rangle = \big\langle(abc),(abf)\big\rangle = S. \qquad (2)$$

Next, since $\alpha \in Sym(5)$, either $\alpha \in Alt(5)$ or $(12)\alpha \in Alt(5)$. First, assume that $\alpha \in Alt(5)$. Then there exists $h_1 \in H$ and $\beta_1 \in S_0$ such that $\alpha = h_1\beta_1$. Thus $h_1 = \alpha{\beta_1}^{-1} \in H$. Since $\beta_1 \in S_0$, by (2) $h_1S_0h_1^{-1} = \alpha\beta_1^{-1}S_0(\alpha\beta_1^{-1})^{-1} = S$.

Next, assume that $(12)\alpha \in Alt(5)$. Then there exists $h_2 \in H$ and $\beta_2 \in S_0$ such that $(12)\alpha = h_2\beta_2$. Thus $h_2 = (12)\alpha\beta_2^{-1}$. Now, since $\big((12)\alpha\big)(123)\big((12)\alpha\big)^{-1} = \big(\alpha(2)\alpha(1)\alpha(3)\big)$ and $\big((12)\alpha\big)(124)\big((12)\alpha\big)^{-1} = \big(\alpha(2)\alpha(1)\alpha(4)\big)$, therefore

$$\big((12)\alpha\big)S_0\big((12)\alpha\big)^{-1} = \big\langle\big(\alpha(2)\alpha(1)\alpha(3)\big),\big(\alpha(2)\alpha(1)\alpha(4)\big)\big\rangle = \alpha S_0\alpha^{-1}. \qquad (3)$$

Since $\beta_2 \in S_0$, by (3) $h_2S_0h_2^{-1} = S$. Thus in either cases, we have $S = hS_0h^{-1}$, for some $h \in H$. □

Remark 2.10. *Let G be a finite group. If H and K are subgroups of G such that $f(H) = K$ for some $f \in$Aut(G), then $|\mathcal{I}(G,H)| = |\mathcal{I}(G,K)|$.*

Proposition 2.11. *Let $G = Alt(5)$, the alternating group of degree 5 and H be a subgroup of G of order 5. Then $|\mathcal{I}(G,H)| = 5^2 \cdot (13 + 5^2 + 5^3 + 5^4 + 5^5 + 5^6 + 5^7)$.*

Proof. Since any two subgroups of order 5 of G are conjugate, by Remark 2.10, we may take $H = \langle a = (12345)\rangle$. Let $S_0 \in \mathcal{T}(G,H)$, where $S_0 = \{a_0 = I,\ a_1 = (12)(34),\ a_2 = (13)(24),\ a_3 = (14)(23),\ a_4 = (123),\ a_5 = (132), a_6 = (124),\ a_7 =$

$(142), a_8 = (134),\ a_9 = (143),\ a_{10} = (234),\ a_{11} = (243)\}$. Then $S_0 \cong Alt(4)$. We observe that for each $S \in \mathcal{T}(G,H)$, there exists a unique map $\sigma : S_0 \to H$ such that $\sigma(a_0) = a_0$ and $S = S_\sigma = \{\sigma(a_i)a_i : 0 \leqslant i \leqslant 11\}$. Let $S \in \mathcal{T}(G,H)$. Then $S = S_\sigma$ for a unique map $\sigma : S_0 \to H$ with $\sigma(a_0) = a_0$. Further, since $|H| = 5$, a prime number, either $\langle S\rangle = S$ or $\langle S\rangle = G$. Assume that $\langle S\rangle = S$. Then by Lemma 2.3, $S \cong S_0 \cong Alt(4)$. By Proposition 2.9 all non-generating NRTs of H in G are conjugate, all non-generating NRTs of H in G forms a single $Aut_H(G)$-orbit in $\mathcal{T}(G,H)$, where $Aut_H(G)$ is identified with the subgroup $K = N_{Sym(5)}(H)$ of $Sym(5)$ and the action of K on $\mathcal{T}(G,H)$ is by conjugation (see also Remark 2.5). If $\langle S\rangle = G$, then by Proposition 2.1, the isomorphism class of S on $\mathcal{T}(G,H)$ forms a single $Aut_H(G)$-orbit. Thus $\mathcal{I}(G,H)$ is precisely the orbits of K in $\mathcal{T}(G,H)$. Now, we describe the orbits of K in $\mathcal{T}(G,H)$. Since $H = \langle a = (12345)\rangle$, we have

$$N_{Sym(5)}(H) = K = \left\langle a, b = (1342) \mid a^5 = b^4 = 1, bab^{-1} = a^2 \right\rangle,$$

K is isomorphic to one dimensional affine group over $\mathbb{Z}_5$ (see Proposition 2.6). Further, by Proposition 2.7 and Corollary 2.8, $|Stab_K(S)| \in \{1, 2, 4\}$.

Assume that $|Stab_K(S)| = 4$. Since a subgroup of K of order 4 is a Sylow 2-subgroup of K, we may assume that $Stab_K(S) = \langle b = (1342)\rangle = K_1$. Since $bab^{-1} = a^2$, we obtain the following relations:

$$\left.\begin{array}{c} \sigma(a_0) \;=\; \sigma(a_1) \;=\; \sigma(a_2) \;=\; \sigma(a_3) \;=\; I \\ \sigma(a_6) = (\sigma(a_4))^2,\ \sigma(a_9) = (\sigma(a_4))^3,\ \sigma(a_{11}) = (\sigma(a_4))^4, \\ \sigma(a_7) = (\sigma(a_5))^2,\ \sigma(a_8) = (\sigma(a_5))^3,\ \sigma(a_{10}) = (\sigma(a_5))^4. \end{array}\right\} \tag{4}$$

Conversely, if $\sigma_1 : S_0 \to H$ is a map satisfying the relations (4), then $Stab_K(S_{\sigma_1}) = K_1$, for if $g \in K \setminus K_1$, then $a_3 \notin gS_{\sigma_1}g^{-1}$ (note that $a_3 \in S_{\sigma_1}$) and $K_1 \subseteq Stab_K(S_{\sigma_1})$. Let $\sigma_1 : S_0 \to H$ be a map satisfying (4). Then $S_{\sigma_1} = \{\sigma_1(a_i)a_i \mid 0 \leqslant i \leqslant 11\} \in \mathcal{T}(G,H)$ and $Stab_K(S_{\sigma_1}) = K_1$. Assume that $T \in \mathcal{T}(G,H)$ lies in the K-orbit of S_{σ_1}. Then there exists $g \in K$ such that $gS_{\sigma_1}g^{-1} = T$. This implies that $Stab_K(T) = gK_1g^{-1}$. Since $N_K(K_1) = K_1$, if $g \notin K_1$, then $Stab_K(T) \neq K_1$. Further, if $g \in K_1$, then $S_{\sigma_1} = gS_{\sigma_1}g^{-1} = T$. This implies that S_{σ_1} lies in the unique K-orbit of size 5. From the relations (4), we observe that a map $\sigma : S_0 \to H$ satisfying (4) can be completely determined by assigning values of $\sigma(a_4)$ and $\sigma(a_5)$. Since each of $\sigma(a_4)$ and $\sigma(a_5)$ can take five distinct values, we have 25 $Aut_H(G) = K$-orbits in $\mathcal{T}(G,H)$ each of size $\frac{|K|}{|K_1|} = 5$.

Next, assume that $|Stab_K(S)| = 2$. Since a Sylow 2-subgroup of K is cyclic, any two subgroups of K of order 2 are conjugate. Thus we may assume that $Stab_K(S) = \langle b^2 = (14)(23)\rangle = L_1$. Since $b^2ab^{-2} = a^4$, we obtain the following relations:

$$\left.\begin{array}{l} \sigma(a_0) = \sigma(a_1) = \sigma(a_2) = \sigma(a_3) = 1, \\ \sigma(a_8) = (\sigma(a_7))^4,\quad \sigma(a_9) = (\sigma(a_6))^4, \\ \sigma(a_{10}) = (\sigma(a_5))^4,\quad \sigma(a_{11}) = (\sigma(a_4))^4. \end{array}\right\} \tag{5}$$

Conversely, let $\sigma_1 : S_0 \to H$ be a map satisfying (5). Then $Stab_K(S_{\sigma_1}) \supseteq L_1$. From the relations (5), we observe that σ_1 satisfying (5) can be completely determined by assigning values of $\sigma_1(a_4)$, $\sigma_1(a_5)$, $\sigma_1(a_6)$ and $\sigma_1(a_7)$. Since each of $\sigma_1(a_i)$'s $(4 \leqslant i \leqslant 7)$ can take five distinct values, there are 625 choices of σ_1 satisfying (5). Further, from the relations (4) and (5), we observe that if a map from S_0 to H satisfies the relations (4), then it also satisfies (5). Further, since there are 25 choices of maps $\sigma : S_0 \to H$ satisfying (4), there are 600 choices of maps from $S_0 \to H$ which satisfies (5) but not (4). Let $\sigma_1 : S_0 \to H$ be a map which satisfies the relations (5) but not (4). Then $S_{\sigma_1} = \{\sigma_1(a_i)a_i \mid 0 \leqslant i \leqslant 11\} \in \mathcal{T}(G,H)$ and $Stab_K(S_{\sigma_1}) = L_1$. Assume that $T \in \mathcal{T}(G,H)$ lies in the K-orbit of S_{σ_1}. Then there exists $g \in K$ such that $gS_{\sigma_1}g^{-1} = T$. This implies that $Stab_K(T) = gL_1g^{-1}$. Since $N_K(L_1) = K_1$, if $g \notin K_1$, then $Stab_K(T) \neq L_1$. Next, if $g \in K_1 \setminus L_1$, then $gS_{\sigma_1}g^{-1} = T(\neq S_{\sigma_1})$. Since $[K_1 : L_1] = 2$, there exists a unique $T \in \mathcal{T}(G,H)$, different from S_{σ_1} which lies in the K-orbit of S_{σ_1} and $Stab_K(T) = L_1$. Thus by the discussion made above, there are 300 K-orbits in $\mathcal{T}(G,H)$ each of size $\frac{|K|}{|L_1|} = 10$.

Lastly, assume that $|Stab_K(S)| = 1$. As argued in the above paragraphs there are 125 NRTs in $\mathcal{T}(G,H)$ whose stabilizer are of order 4 and there are 3000 NRTs in $\mathcal{T}(G,H)$ whose stabilizer are of order 2, there are $5^{11} - 5^5 = 5^5(5^6 - 1)$ NRTs whose stabilizer are trivial. Hence, we have $5^4 \cdot (1+5+5^2+5^3+5^4+5^5)$, K-orbits in $\mathcal{T}(G,H)$ each of size 20. Thus $|\mathcal{I}(G,H)| = 5^2 + 3\cdot4\cdot5^2 + 5^4\cdot(1+5+5^2+5^3+5^4+5^5) = 5^2 \cdot (13 + 5^2 + 5^3 + 5^4 + 5^5 + 5^6 + 5^7)$. ☐

Corollary 2.12. *There are at least,* $5^2 \cdot (13 + 5^2 + 5^3 + 5^4 + 5^5 + 5^6 + 5^7)$ *non-isomorphic right loops of order 12.*

Proof. Let $G = Alt(5)$, the alternating group of degree 5 and H be a subgroup of G of order 5. If $S \in \mathcal{T}(G,H)$, then S is a right loop of order 12 (see [12, Proposition 4.3.3, p.102]). By Proposition 2.11, $|\mathcal{I}(G,H)|$ is precisely the number of $\mathrm{Aut}_H(G)$-orbits in $\mathcal{T}(G,H)$. Thus if $S_1, S_2 \in \mathcal{T}(G,H)$ belongs to different $\mathrm{Aut}_H(G)$-orbits, then $S_1 \ncong S_2$. This completes the proof. ☐

Lemma 2.13. *Let L be a subgroup of $Sym(5)$ of order 8. Then L is isomorphic to D_8, the dihedral group of order 8.*

Proof. Since $|Sym(5)| = 2^3 \cdot 3 \cdot 5$, if L is a subgroup of $Sym(5)$ of order 8, then it is a Sylow 2-subgroup of $Sym(5)$. Let $N = \langle (13), (1234) \rangle$. Then N is a subgroup of $Sym(5)$ of order 8 isomorphic to D_8. Since any two Sylow 2-subgroups of $Sym(5)$ are conjugate, the lemma follows. ☐

Proposition 2.14. *Let $G = Alt(5)$, the alternating group of degree 5 and H be a subgroup of G of order 2. Then $|\mathcal{I}(G,H)| = 2^{26} + 10$.*

Proof. Let H be a subgroup of G of order 2. Since any two elements of G of order 2 are conjugate, by Remark 2.10, we may assume that $H = \{I, x = (12)(34)\}$, where I is the identity element of G. Let $K = Aut_H(G)$. By Remark 2.5, we identify K with the group $N_{Sym(5)}(H) = C_{Sym(5)}(H)$, the centralizer of H in $Sym(5)$. Since there are 15 conjugates of (12)(34) in $Sym(5)$, $|C_{Sym(5)}(H)| = 8$. By Lemma 2.13, $C_{Sym(5)}(H) \cong D_8$. Since $H = \{I, x = (12)(34)\}$, we have

$$K = \{I, (1324), (12)(34), (1423), (14)(23), (34), (13)(24), (12)\}.$$

Consider the subgroups $V_4 = \{I, (12)(34), (13)(24), (14)(23)\}$ (isomorphic to the Klein's four group) and $L = \{g \in G : g(5) = 5\}$ of G. Let $T_1 = \{b_0 = I,\ b_1 = (13)(24)\}$, $T_2 = \{c_0 = I, c_1 = (134), c_2 = (143)\}$ and $T_3 = \{d_0 = I, d_1 = (12345), d_2 = (13524), d_3 = (14253), d_4 = (15432)\}$. Then $T_1 \in \mathcal{T}(V_4, H)$, $T_2 \in \mathcal{T}(L, V_4)$ and $T_3 \in \mathcal{T}(G, L)$. Thus $S_0 = T_1T_2T_3 = \{b_ic_jd_k\ :\ 0 \leqslant i \leqslant 1,\ 0 \leqslant j \leqslant 2, 0 \leqslant k \leqslant 4\} \in \mathcal{T}(G, H)$.

Since G is a simple group and H is of order 2, $\langle S \rangle = G$, for every $S \in \mathcal{T}(G, H)$. Thus by Proposition 2.1, $\mathcal{I}(G, H)$ is precisely the orbits of K in $\mathcal{T}(G, H)$, where the action of K is by conjugation.

Let $S \in \mathcal{T}(G, H)$. Then there exists a unique map $\sigma\ :\ S_0 \to H$ such that $\sigma(b_0c_0d_0 = I) = I$ and $S = S_\sigma = \{\sigma(b_ic_jd_k)b_ic_jd_k\ :\ 0 \leqslant i \leqslant 1,\ 0 \leqslant j \leqslant 2, 0 \leqslant k \leqslant 4\}$. Let $g \in \{(1324), (1423), (12), (34)\} \subseteq K$. Then $g \notin Stab_K(S)$, for if $g \in Stab_K(S)$, then $g\sigma(b_1c_0d_0)b_1c_0d_0g^{-1} = \sigma(b_1c_0d_0)xb_1c_0d_0$, a contradiction as $x = (12)(34) \in H$ and $\sigma(b_1c_0d_0)b_1c_0d_0 \in S$. Let $g = (13)(24) \in K$. Then $g \notin Stab_K(S)$, for if $g \in Stab_K(S)$, then $g\sigma(b_0c_1d_0)b_0c_1d_0g^{-1} = \sigma(b_0c_1d_0)xb_0c_1d_0 \in S$ and so we have a contradiction as $x = (12)(34) \neq I$. Next, let $g = (14)(23) \in K$. Then $g \notin Stab_K(S)$, for if $g \in Stab_K(S)$, then $g\sigma(b_0c_2d_0)b_0c_2d_0g^{-1} = \sigma(b_0c_2d_0)xb_0c_2d_0 \in S$, $\sigma(b_0c_2d_0)x = \sigma(b_0c_2d_0)$, again a contradiction. The above arguments imply that stabilizer in K of an NRT of H in G is either H or $\{I\}$. Thus a K-orbit in $\mathcal{T}(G, H)$ is either of size 4 or of size 8.

Now, assume that $Stab_K(S) = H$. Then σ satisfies the following relations:

$$\left.\begin{array}{l}
\sigma(b_1c_0d_0) = I \text{ or } x,\ \sigma(b_0c_1d_4)x = \sigma(b_1c_0d_3),\ \sigma(b_0c_2d_1)x = \sigma(b_0c_1d_2)\\
\sigma(b_1c_1d_1)x = \sigma(b_1c_0d_2), \sigma(b_1c_2d_2)x = \sigma(b_1c_0d_1), \sigma(b_0c_2d_3) = \sigma(b_0c_0d_4)\\
\sigma(b_0c_2d_0) = \sigma(b_1c_2d_0),\ \sigma(b_0c_1d_3) = \sigma(b_1c_2d_4),\ \sigma(b_0c_2d_2)x = \sigma(b_0c_0d_1)\\
\sigma(b_1c_1d_2)x = \sigma(b_1c_2d_1),\ \sigma(b_1c_0d_4) = \sigma(b_1c_2d_3),\ \sigma(b_0c_1d_1)x = \sigma(b_oc_0d_2)\\
\sigma(b_0c_1d_0)x = \sigma(b_1c_1d_0),\ \sigma(b_0c_2d_4) = \sigma(b_1c_1d_3),\ \sigma(b_1c_1d_4)x = \sigma(b_0c_0d_3)
\end{array}\right\} \quad (6)$$

Conversely, if a map $\sigma_1 : S_0 \to H$ with $\sigma_1(I) = I$ satisfies (6), then $Stab_K(S_{\sigma_1}) = H$. From the relations (6), we find that there are 20 K-orbits in $\mathcal{T}(G, H)$ each of size 4. Hence we have $\frac{2^{29}-80}{8} = 2^{26} - 10$, K-orbits in $\mathcal{T}(G, H)$ each of size 8. Therefore $|\mathcal{I}(G, H)| = 2^{26} - 10 + 20 = 2^{26} + 10$. □

Corollary 2.15. *There are at least,* $2^{26} + 10$ *non-isomorphic right loops of order 30.*

Proof. Let $G = Alt(5)$, the alternating group of degree 5 and H be a subgroup of G of order 2. If $S \in \mathcal{T}(G, H)$, then S is a right loop of order 30 (see [12, Proposition 4.3.3, p.102]). By Proposition 2.14, $|\mathcal{I}(G, H)|$ is precisely the number of $\mathrm{Aut}_H(G)$-orbits in $\mathcal{T}(G, H)$. Thus if $S_1, S_2 \in \mathcal{T}(G, H)$ belongs to different $\mathrm{Aut}_H(G)$-orbits, then $S_1 \ncong S_2$. This completes the proof. □

3. Graphs and isomorphism classes of transversals

In this section, we have introduced two graphs associated to the isomorphism classes of transversals of a subgroup of a finite group and studied some properties of these graphs.

Definition 3.1. Let G be a finite group and X be the set of all nontrivial proper subgroups of G. We define a graph $\Gamma_{tic}(G)$ on G whose vertex set is X and two distinct vertices H and K are adjacent in $\Gamma_{tic}(G)$ if and only if $|\mathcal{I}(G,H)| = |\mathcal{I}(G,K)|$. We will call this graph the *transiso-class* graph.

It is easy to observe that $\Gamma_{tic}(G)$ is complete if and only if $|\mathcal{I}(G,H)| = |\mathcal{I}(G,K)|$ for every $H,\ K \in X$.

Definition 3.2. Let G be a finite group. Let d be the order of a subgroup of G and X_d be the set of all subgroups of G of order d. We define a graph $\Gamma_{d,tic}(G)$ on G with vertex set X_d and two distinct vertices are adjacent in $\Gamma_{d,tic}(G)$ if and only if $|\mathcal{I}(G,H)| = |\mathcal{I}(G,K)|$. We call the graph $\Gamma_{d,tic}(G)$ as *d-transiso-class* graph.

We observe that $\Gamma_{d,tic}(G)$ is complete if and only if $|\mathcal{I}(G,H)| = |\mathcal{I}(G,K)|$ for any $H,\ K \in X_d$.

Remark 3.3. In the definitions 3.1 and 3.2, we observe that $\Gamma_{tic}(G)$ and $\Gamma_{d,tic}(G)$ both are connected if and only if they are complete.

Definition 3.4. ([11], p.143)A group G is said to be a *Dedekind* group if all the subgroups of G are normal in G.

Example 3.5. Let G be a finite Dedekind group. Since each subgroup of G is normal in G, $|\mathcal{I}(G,H)| = 1$ (see [10, Main Theorem, p.643]), for every subgroup H of G. Thus both $\Gamma_{tic}(G)$ and $\Gamma_{d,tic}(G)$ are complete, where d is the order of subgroup of G.

Proposition 3.6. *Let $G = Sym(3)$. Then $\Gamma_{d,tic}(G)$ is complete, d is the order of a subgroup of G.*

Proof. Let $X_d = \{H \leqslant G : \ |H| = d\}$. Obviously, $d \in \{1,2,3,6\}$. If $d = 1$ or $d = 3$ or $d = 6$, then $H \in X_d$ is normal in G and so $|\mathcal{I}(G,H)| = 1$. Thus $\Gamma_{d,tic}(G)$ is complete. Next, assume that $d = 2$. Since all 2-cycles in G are conjugate, any two members of X_2 are conjugate. Hence by Remark 2.10, $|\mathcal{I}(G,H)| = |\mathcal{I}(G,K)|$ for every $H,\ K \in X_2$. Thus $\Gamma_{2,tic}(G)$ is complete. □

Remark 3.7. It is easy to observe that if H is a subgroup of $G = Sym(3)$ of order 2, then $|\mathcal{I}(G,H)| = 3$. However, if $H = Alt(3)$, the alternating group of degree 3, then $|\mathcal{I}(G,H)| = 1$ (see [10]). Consequently, $\Gamma_{tic}(Sym(3))$ is not complete.

Proposition 3.8. *Let $G = Alt(4)$. Then $\Gamma_{d,tic}(G)$ is complete for every d, where d is the order of a subgroup of G.*

Proof. Let $G = Alt(4)$. Let X_d denote the set of all subgroups of G of order d. Then any two members of X_d are conjugate. By Remark 2.10, $|\mathcal{I}(G,H)| = |\mathcal{I}(G,K)|$ for every $H,\ K \in X_d$. Thus $\Gamma_{d,tic}(G)$ is complete for every d. □

Proposition 3.9. *Let $G = Alt(4)$. Then $\Gamma_{tic}(G)$ is not complete.*

Proof. Let $G = Alt(4)$. If H is a subgroup of G of order 2, then $|\mathcal{I}(G,H)| = 5$ (see [6]). Also, It is easy to observe that if K is a subgroup of order 3 of $Alt(4)$, then $|\mathcal{I}(G,K)| = 7$. Thus H and K are not adjacent in $\Gamma_{tic}(G)$. Hence $\Gamma_{tic}(G)$ is not complete. □

Lemma 3.10. *Let $G = Alt(5)$. Let X_d be the set of all subgroups of G of order d. Then any two members of X_d are conjugate.*

Proof. Let X_d be the set of all subgroups of G of order d. Since G is simple, if $H \in X_d$, then $[G : H] \geqslant 5$ (see [13, p. 308]). Hence $d \in \{1, 2, 3, 4, 5, 6, 10, 12, 60\}$. If $d = 1$ or $d = 60$, then the proof is over. Assume that $d = 2$. Let $H \in X_2$. Then H is of the form $\{I, \sigma\}$, where $\sigma \in Alt(5)$ is product of two distinct transpositions. Since all permutations of the form σ are conjugate in $Alt(5)$, any two members of X_2 are conjugate. Further, if $d \in \{3, 4, 5\}$, then any member of X_d is a Sylow d-subgroup of G. Hence any two members of X_d are conjugate.

Next, assume that $d = 6$. Since G has no permutation of order 6, a subgroup of order 6 in G is isomorphic to $Sym(3)$. If K is a subgroup of G of order 6, then $N_G(K) = K$. Hence there are 10 conjugates of K in G. Since there are exactly 10 subgroups of G of order 6, all members of X_6 form a complete conjugacy class. Now, assume that $d = 10$. Again, since G has no permutation of order 10, a subgroup of G of order 10 is isomorphic to D_{10}. If $L \in X_{10}$, then it is easy to observe that $N_G(L) = L$. Thus there are 6 conjugates of L in G. Since there are exactly 6 subgroups of G of order 10, any two subgroups of G of order 10 are conjugate. Lastly, assume that $d = 12$. By Proposition 2.9 any two subgroups of G of order 12 are conjugate. □

Proposition 3.11. *Let $G = Alt(5)$. Then $\Gamma_{d,tic}(G)$ is complete, for every d, where d is the order of a subgroup of G.*

Proof. Let $G = Alt(5)$. Let X_d denote the set of all subgroups of G of order d. Then by Lemma 3.10, any two members of X_d are conjugate. By Remark 2.10, $|\mathcal{I}(G,H)| = |\mathcal{I}(G,K)|$, for any $H,\ K \in X_d$. Hence $\Gamma_{d,tic}(G)$ is complete for every d. □

Remark 3.12. In the above proposition, we observe that $\Gamma_{d,tic}(Alt(5))$ is complete for every d, where d is the order of a subgroup of $Alt(5)$. However, $Alt(5)$ is not a Dedekind group.

Proposition 3.13. *Let $G = Alt(5)$. Then $\Gamma_{tic}(G)$ is not complete.*

Proof. Let $G = Alt(5)$. Let X be the set of all nontrivial proper subgroups of G. Let H be a subgroup of G of order 2. Then by Proposition 2.14, $|\mathcal{I}(G,H)| = 2^{26} + 10$.

Let K be a subgroup of G of order 5. Then by Proposition 2.11, $|\mathcal{I}(G,K)| \neq |\mathcal{I}(G,H)|$. Thus both H and K are in X, however they are not adjacent in $\Gamma_{tic}(G)$. Hence $\Gamma_{tic}(G)$ is not complete. $\square$

Proposition 3.14. *Let G be a finite p-group, p is a prime. Then $\Gamma_{d,tic}(G)$ is complete if and only if each member of X_d is normal in G, where X_d is the set of all subgroups of G of order d.*

Proof. Let G be a finite p-group. Then for each divisor d of $|G|$, G contains a normal subgroup H of order d (see [9, Proposition 9.1.23]). Thus $\Gamma_{d,tic}(G)$ is complete if $|\mathcal{I}(G,K)| = 1$ for every $K \in X_d$. Consequently, each $K \in X_d$ is normal in G (see [10]). Conversely, assume that each member of X_d is normal in G. Then $|\mathcal{I}(G,H)| = 1$, for any $H \in X_d$. Hence $\Gamma_{d,tic}(G)$ is complete. $\square$

Corollary 3.15. *Let G be a nonabelian group of order order p^3, p is a prime. Then $\Gamma_{p,tic}(G)$ is complete if and only if $G \cong Q_8$.*

Proof. Assume that $\Gamma_{p,tic}(G)$ is complete. By the above proposition each subgroup of G of order p is normal in G. Since a subgroup of G of order p^2 is maximal in G, it is normal in G. Thus if $\Gamma_{p,tic}(G)$ is complete, then all subgroups of G are normal in G. Hence G is a Dedekind group. Thus by [11, p.143], $G \cong Q_8$. Conversely, if $G = Q_8$, then $\Gamma_{2,tic}(G)$ is complete follows from the Example 3.5. $\square$

Proposition 3.16. *Let $G = D_{2n}$. If n is even, then $\Gamma_{2,tic}(G)$ is not complete.*

Proof. Let X_2 be the set of all subgroups of G of order 2. Since the center $Z(G)$ of G is of order 2, $|\mathcal{I}(G,Z(G))| = 1$. Again if $H \in X_2$ and H is non-normal, then $|\mathcal{I}(G,H)| \neq 1$ (see [10, Main Theorem, p.643]). Thus $Z(G)$ and H are not adjacent in $\Gamma_{2,tic}(G)$. Consequently, $\Gamma_{2,tic}(G)$ is not complete. $\square$

Let $G = D_8 = \langle a, b : a^2 = b^4 = 1,\ aba = b^{-1}\rangle$. Let $X_2 = \{H_1 = \langle a\rangle, H_2 = \langle ba\rangle, H_3 = \langle b^2a\rangle, H_4 = \langle b^3a\rangle, H_5 = \langle b^2\rangle\}$ be the set of all subgroups of G of order 2 and let $X_4 = \{K_1 = \langle b\rangle, K_2 = \langle b^2, a\rangle, K_3 = \langle b^2, ba\rangle\}$ be the set of all subgroups of G of order 4. Then the connectivity of subgroups in $\Gamma_{2,tic}(D_8)$ and $\Gamma_{4,tic}(D_8)$ can be shown in following pictorial form:

(a) Γ_1 (b) Γ_2

Figure 1: $\Gamma_{2,tic}(D_8) = \Gamma_1 \cup \Gamma_2$

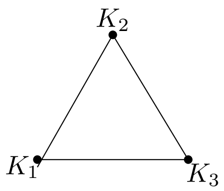

Figure 2: $\Gamma_{4,tic}(D_8)$

Proposition 3.17. *Let G be a finite group containing a nontrivial proper normal subgroup. Assume that $\Gamma_{tic}(G)$ is complete. Then G is a Dedekind group.*

Proof. Let X be the set of all nontrivial proper subgroups of G. Then there exists $H \in X$ such that $H \trianglelefteq G$ and hence $|\mathcal{I}(G,H)| = 1$ (see [10, Main Theorem, p.643]). Assume that $\Gamma_{tic}(G)$ is complete. Then $|\mathcal{I}(G,K)| = 1$, for every $K \in X$. Thus each subgroup of G is normal in G (see [10]). Hence G is a Dedekind group. $\square$

In the Proposition 3.17, we saw that if $\Gamma_{tic}(G)$ is complete and G has a nontrivial proper normal subgroup, then G is Dedekind. Then, we may ask the following questions:

Question 1. *Does there exists a finite non-abelian simple group G such that $\Gamma_{tic}(G)$ complete ?*

Question 2. *Let G be a finite group. Let X_d be the set of all subgroups of G of order d. Assume that $\Gamma_{d,tic}$ is complete. Then what can we say about the members of X_d ?*

Acknowledgement. The authors are grateful to the anonymous referee for the valuable suggestions for adding the Corollary 2 and 3. During the work of this paper the first author was supported (financially) by CSIR, Government of India.

References

[1] **M. Artin**, *Algebra*, PHI Learning Private Limited, New Delhi, 2003.

[2] **R. Diestel**, *Graph Theory*, Springer-Verlag, New York, 2005.

[3] **D. Dummit and R. Foote**, *Abstract Algebra*, J. Wiley & Sons, New Delhi, 2004.

[4] **V.K. Jain and R.P. Shukla**, *On the isomorphism classes of transversals*, Comm. Alg., **36** (2008), 1717–1725.

[5] **V.K. Jain and R.P. Shukla**, *On the isomorphism classes of transversals II*, Comm. Alg., **39** (2011), 2024–2036.

[6] **V. Kakkar and R.P. Shukla**, *On the number of isomorphism classes of transversals*, Proc. Indian Acad. Sci. (Math. Sci.), **123** (2013), 345–359.

[7] **V. Kakkar and R.P. Shukla**, *Some characterizations of a normal subgroups of a group and isotopic classes of transversals*, Algebra Colloq., **23** (2106), 409-422.

[8] **R. Lal**, *Transversals in groups.* J. Algebra, **181** (1996), 70–81.

[9] **R. Lal**, *Algebra* 1, Infosys Sci. Found. Ser. Math. Sci., Singapore, 2017.

[10] **R. Lal and R.P. Shukla**, *Perfectly stable subgroups of finite groups*, Comm. Alg., **24** (1996), 643–657.

[11] **D.J.S. Robinson,** *A Course in the Theory of Groups*, Springer-Verlag, 1996.

[12] **J.D.H. Smith and A.B. Romanowska**, *Post-Modern Algebra*, J. Wiley & Sons, New York, 1991.

[13] **M. Suzuki**, *Group Theory I*, Springer-Verlag, 1982.

Received February 14, 2021

Department of Mathematics,
University of Allahabad,
Prayagraj, 211002, India.
e-mails: surendramishra557@gmail.com (S.K. Mishra), shuklarp@gmail.com (R.P. Shukla)

Quasigroups and Related Systems **29** (2021), 255 − 268

Menger algebras of terms induced by transformations with restricted range

Sarawut Phuapong and Thodsaporn Kumduang

Abstract. In this paper, a special kind of n-ary terms of type τ_n, which are called $T(\bar{n}, Y)$-full terms, are introduced. They are derived by applying transformations on the set $\bar{n} = \{1, 2, \ldots, n\}$ with restricted range. Under the superposition operation S^n, the algebra of such terms called the clone of $T(\bar{n}, Y)$-full terms is constructed. We prove that the superassociative law is satisfied in the clone of $T(\bar{n}, Y)$-full terms and the freeness is investigated using a generating set and a suitable homomorphism. Based on the theory of hypervariety, we study $T(\bar{n}, Y)$-full hypersubstitutions which are maps taking all operation symbols to our obtained terms. These lead us to provide the classes of $T(\bar{n}, Y)$-full hyperidentities and $T(\bar{n}, Y)$-full solid varieties. A connection between identities in $clone_{T(\bar{n},Y)}(\tau_n)$ and $T(\bar{n}, Y)$-full hyperidentities is established.

1. Introduction

It is commonly known that the idea of terms is one of fundamental tools in study of universal algebra. It is also connect with various fields of science, for instance, graph theory and automata theory. Normally, terms are formal expression defined from variables and operation symbols. Let $X := \{x_1, x_2, \ldots\}$ be a countably infinite set of symbols called *variables*. We often refer to these variables as letters to X as an alphabet, and also refer to the set $X_n := \{x_1, x_2, \ldots, x_n\}$ as an n-element alphabet. Let $(f_i)_{i\in I}$ be an indexed set which is disjoint from X. Each f_i is called an *n_i-ary operation symbol*, where $1 \leqslant n_i \leqslant n$ is a natural number. Let τ be a function which assigns to every f_i the number n_i as its arity. The sequence of the values of function τ, written as $(n_i)_{i\in I}$, is called a *type*. An *n-ary term of type τ* is defined inductively as follows: (i) Every variable $x_j \in X_n$ is an n-ary term of type τ. (ii) $f_i(t_1, \ldots, t_{n_i})$ is an n-ary term of type τ where $t_1, \ldots, t_{n_i}$ are n-ary terms of type τ and f_i is an n_i-ary operation symbol. The set of all n-ary terms of type τ, closed under finite number of applications of (ii), is denoted by $W_\tau(X_n)$. The symbol $W_\tau(X) := \bigcup_{n=1}^{\infty} W_\tau(X_n)$ stands for the set of all terms of type τ. See [13, 14, 15, 21, 22, 24] for example of current trands in the study of terms.

2010 Mathematics Subject Classification: 08A62; 08B15; 20M10
Keywords: term, Menger algebra, clone, hypersubstitution, hyperidentity, transformations with restricted range.

The set of all terms of type τ can be used as the universe of an algebra of type τ. For every $i \in I$, an n_i-ary operation $\bar{f}_i : W_\tau(X)^{n_i} \longrightarrow W_\tau(X)$ is defined by

$$\bar{f}_i\left(t_1, \ldots, t_{n_i}\right) := f_i\left(t_1, \ldots, t_{n_i}\right).$$

The algebra $\mathcal{F}_\tau(X) := (W_\tau(X); (\bar{f}_i)_{i \in I})$ is called the *absolutely free algebra* of type τ over the set X.

There is another way to consider the operation on the set of terms. Now, we recall the concept of superposition operation of terms. For each natural numbers $m, n \geqslant 1$, the superposition operation is a many-sorted mapping

$$S^n_m : W_\tau(X_n) \times (W_\tau(X_m))^n \to W_\tau(X_m)$$

defined by

(i) $S^n_m(x_j, t_1, \ldots, t_n) := t_j$, if $x_j \in X_n$,

(ii) $S^n_m(f_i(s_1, \ldots, s_{n_i}), t_1, \ldots, t_n) := f_i(S^n_m(s_1, t_1, \ldots, t_n), \ldots, S^n_m(s_{n_i}, t_1, \ldots, t_n))$.

Then the many-sorted algebra can be defined by

$$\text{clone } \tau := ((W_\tau(X_n))_{n \in \mathbb{N}^+}; (S^n_m)_{n,m \in \mathbb{N}^+}, (x_i)_{i \leqslant n \in \mathbb{N}^+}),$$

which is called *the clone of all terms of type* τ. For recent developments in this way, see [3].

Let $\tau_n = (n, n, \ldots, n)$ be a type consisting of the same values equal to n, i.e. $\tau_n = (n_i)$ with $n_i = n$ for all $i \in I$. The concept of full terms is used in [6] to study the depth of terms and full hypersubstitutions, and solid varieties. The composed full terms are derived by operation symbols and terms in which all input variables occur. Thus the resulting subterms in each step of composition, content whole set of the input variables, which can be permuted, only.

In 2004, Denecke and Jampachon [5] inductively defined n-ary full terms of type τ_n, based on the full transformations (mappings) instead of the permutations, as follows:

(i) $f_i(x_{\alpha(1)}, \ldots, x_{\alpha(n)})$ is an n-ary full term of type τ_n if f_i is an n-ary operation symbol and $\alpha \in T_n$ where T_n is the set of all full transformation on $\{1, 2, \ldots, n\}$;

(ii) $f_i\left(t_1, \ldots, t_n\right)$ is an n-ary full term of type τ_n if f_i is an n-ary operation symbol and $t_1, \ldots, t_n$ are n-ary full terms of type τ_n.

The set of all n-ary full terms of type τ_n, closed under finite application of (ii), is denoted by $W^F_{\tau_n}(X_n)$. If T_n is replaced by the submonoid $\{1_n\}$, then $W^F_{\tau_n}(X_n)$ is denoted by $W^{SF}_{\tau_n}(X_n)$ called the set of all *strongly full terms* of type τ_n [4]. Actually, there are many generalizations of full terms as in [4, 18, 19, 27, 28].

Beginning with the notions of terms, we define $T(\bar{n}, Y)$-full terms through transformations with restricted range. The Menger algebea of $T(\bar{n}, Y)$-full terms is presented. In Section 3, we construct the monoid of $T(\bar{n}, Y)$-full hypersubstitution of type τ_n which consists of a mapping from the set of operation sysmbols to the set of all $T(\bar{n}, Y)$-full terms. These mappings preserve the arity of operation symbols and the arity of $T(\bar{n}, Y)$-full terms, together with one binary associative operation and the identity element. Finally, the $T(\bar{n}, Y)$-full solid varieties of type τ_n are charaterized.

2. The algebra of $T(\bar{n}, Y)$-full terms

The first aim of our main results is to propose the new concept of a specific term, based on full transformation mappings and the original notions of terms. For this, we recall the concept of the full transformations.

Let X be a nonempty set and let $T(X)$ denote the semigroup of the full transformations from X into itself under composition of mappings and let Y be a nonempty subset of X. Then $T(X, Y)$ was introduced by Symons [26] to be the set of all transformations from X to Y called the *full transformation semigroup with restricted range*, that means

$$T(X, Y) := \{\alpha \in T(X) \mid X\alpha \subseteq Y\}.$$

Clearly, $T(X, Y)$ is a subsemigroup of $T(X)$ and if $X = Y$ then $T(X, Y) = T(X)$. For more information about $T(X, Y)$, we refer to[1, 11, 25].

Let $\tau_n = (n_i)_{i\in I}$ be a type and let $(f_i)_{i\in I}$ be an indexed set of operation symbols of type τ. The *full transformation semigroup* T_n consists of the set of all maps $\alpha : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ and the usual composition of mappings. Indeed, T_n is a monoid and identity map 1_n acts as its identity. Let $\bar{n} := \{1, 2, \ldots, n\}$. For a fixed nonempty subset Y of $\bar{n}$, it is well-known that the set

$$T(\bar{n}, Y) := \{\alpha \in T_n \mid \operatorname{Im}\alpha \subseteq Y\} \cup \{1_n\}$$

is a submonoid of T_n.

Then we introduce the definition of n-ary $T(\bar{n}, Y)$-full term of type τ_n.

Definition 2.1. Let f_i be an n-ary operation symbol and $\alpha \in T(\bar{n}, Y)$. An n-ary $T(\bar{n}, Y)$-full term of type τ_n is defined in the following way:

(i) $f_i(x_{\alpha(1)}, \ldots, x_{\alpha(n)})$ is an n-ary $T(\bar{n}, Y)$-full term of type τ_n;

(ii) if $t_1, \ldots, t_n$ are n-ary $T(\bar{n}, Y)$-terms of type τ_n, then $f_i(t_1, \ldots, t_n)$ is an n-ary $T(\bar{n}, Y)$-full term of type τ_n.

Let $W_{\tau_n}^{T(\bar{n},Y)}(X_n)$ be the set of all n-ary $T(\bar{n}, Y)$-full terms of type τ_n.

Now we give an example of Definition 2.1.

Example 2.2. Let $\tau_n = (n)$ be a type with one operation symbol f and let us consider the following examples:

(i) Let $n = 2$, and $Y = \{2\}$, then
$$f(x_1, x_2), f(x_2, x_2), f(f_1(x_2, x_2), f(x_2, x_2)) \in W_{\tau_2}^{T(\bar{2},Y)}(X_2).$$

(ii) Let $n = 3$, and $Y = \{1, 3\}$, then
$$f(x_1,x_2, x_3), f(x_3, x_3, x_3), f(f_2(x_3, x_3, x_1), f(x_1, x_1, x_1), f(x_1,x_3, x_3)) \in W_{\tau_3}^{T(\bar{3},Y)}(X_3).$$

(iii) Let $n = 4$, and $Y = \{2, 3, 4\}$, then
$$f(x_1, x_2, x_3, x_4), f(x_2, x_2, x_4, x_2), f(x_2, x_4, x_2, x_4) \in W_{\tau_4}^{T(\bar{4},Y)}(X_4).$$

Let us note that if $Y = \bar{n}$ then the set $W_{\tau_n}^{T(\bar{n},Y)}(X_n)$ of all $T(\bar{n}, Y)$-full terms is equal to the set $W_{\tau_n}^{F}(X_n)$ of all n-ary full terms of type τ_n, as defined in [5]. This means that $T(\bar{n}, Y)$-full terms of type τ_n are natural generalization of the full terms of type τ_n, discussed in [5] and [6]. By the definition of $T(\bar{n}, Y)$-full terms of type τ_n we have that $\left(W_{\tau_n}^{T(\bar{n},Y)}(X_n); (\bar{f}_i)_{i\in I}\right)$ is a subalgebra of $\left(W_{\tau}(X); (\bar{f}_i)_{i\in I}\right)$.

Normally, terms have many measures of their complexity, see [23]. As a result, there is a possibility to measure a complexity of $T(\bar{n}, Y)$-full terms. The depth of a $T(\bar{n}, Y)$-full term t, denoted by $Depth(t)$, is the longest distance from a first operation symbol that appears in a term (from the left) to variables. It can be inductively defined by

(i) $Depth(t) = 1$ if $t = f_i(x_{\alpha(1)}, \ldots, x_{\alpha(n)})$ and $\alpha \in T(\bar{n}, Y)$;

(ii) $Depth(t) = 1 + max\{Depth(t_j) \mid 1 \leqslant j \leqslant n\}$ if $t = f_i(t_1, \ldots, t_n)$.

On the set $W_{\tau_n}^{T(\bar{n},Y)}(X_n)$, we define an $(n + 1)$-ary operation S^n,
$$S^n : \left(W_{\tau_n}^{T(\bar{n},Y)}(X_n)\right)^{n+1} \longrightarrow W_{\tau_n}^{T(\bar{n},Y)}(X_n)$$
for all $t_1, \ldots, t_n, s_1, \ldots, s_n \in W_{\tau_n}^{T(\bar{n},Y)}(X_n)$ by

(i) $S^n\left(f_i\left(x_{\alpha(1)}, \ldots, x_{\alpha(n)}\right), t_1, \ldots, t_n\right) := f_i\left(t_{\alpha(1)}, \ldots, t_{\alpha(n)}\right)$;

(ii) $S^n(f_i(t_1, \ldots, t_n), s_1, \ldots, s_n) := f_i\left(S^n(t_1, s_1, \ldots, s_n), \ldots, S^n(t_n, s_1, \ldots, s_n)\right)$.

Then we form the algebra
$$clone_{T(\bar{n},Y)}(\tau_n) := \left(W_{\tau_n}^{T(\bar{n},Y)}(X_n), S^n\right)$$
which is called *the clone of all $T(\bar{n}, Y)$-full terms of type τ_n*. Theorem 2.3, presented below, shows that the algebra $\left(W_{\tau_n}^{T(\bar{n},Y)}(X_n), S^n\right)$ satisfies the superassociative law (SASS):
$$\begin{aligned} &S^n(X_0, S^n(Y_1, Z_1, \ldots, Z_n), \ldots, S^n(Y_n, Z_1, \ldots, Z_n)) \\ &\qquad \approx S^n(S^n(X_0, Y_1, \ldots, Y_n), Z_1, \ldots, Z_n) \end{aligned} \tag{1}$$

where S^n is an $(n+1)$-ary operation symbol and X_0, Y_j, Z_j are variables for all $1 \leqslant j \leqslant n$.

Next, we shall show that the superassociative law is satisfied in the clone of all $T(\bar{n}, Y)$-full terms.

Theorem 2.3. *The algebra $clone_{T(\bar{n},Y)}(\tau_n)$ satisfies the superassociative law.*

Proof. We give a proof by induction on the depth of an n-ary $T(\bar{n}, Y)$-full term t which is substituted for X_0 from (1). If we substitute for X_0 from (1) by a $T(\bar{n}, Y)$-full term $t = f_i(x_{\alpha(1)}, \ldots, x_{\alpha(n)})$ where $\alpha \in T(\bar{n}, Y)$, and $Depth(t) = 1$, then we have

$$\begin{aligned}
&S^n(f_i(x_{\alpha(1)}, \ldots, x_{\alpha(n)}), S^n(t_1, s_1, \ldots, s_n), \ldots, S^n(t_n, s_1, \ldots, s_n)) \\
&\qquad = f_i(S^n(x_{\alpha(1)}, S^n(t_1, s_1, \ldots, s_n), \ldots, S^n(t_n, s_1, \ldots, s_n)), \ldots, \\
&\qquad\quad S^n(x_{\alpha(n)}, S^n(t_1, s_1, \ldots, s_n), \ldots, S^n(t_n, s_1, \ldots, s_n))) \\
&\qquad = f_i(S^n(t_{\alpha(1)}, s_1, \ldots, s_n), \ldots, S^n(t_{\alpha(n)}, s_1, \ldots, s_n)) \\
&\qquad = S^n(f_i(t_{\alpha(1)}, \ldots, t_{\alpha(n)}), s_1, \ldots, s_n) \\
&\qquad = S^n(S^n(f_i(x_{\alpha(1)}, \ldots, x_{\alpha(n)}), t_1, \ldots, t_n), s_1, \ldots, s_n).
\end{aligned}$$

If we substitute for X_0 from (1) by a $T(\bar{n}, Y)$-full term $t = f_i(r_1, \ldots, r_n)$ where $r_1, \ldots, r_n \in W_{\tau_n}^{T(\bar{n},Y)}(X_n)$ and assume that

$$S^n(r_k, S^n(t_1, s_1, \ldots, s_n), \ldots, S^n(t_n, s_1, \ldots, s_n)) = S^n(S^n(r_k, t_1, \ldots, t_n), s_1, \ldots, s_n)$$

for all $1 \leqslant k \leqslant n$, and $max_{1 \leqslant k \leqslant n} Depth(r_k) = m$, then $Depth(t) = m + 1$ and we have

$$\begin{aligned}
&S^n(f_i(r_1, \ldots, r_n), S^n(t_1, s_1, \ldots, s_n), \ldots, S^n(t_n, s_1, \ldots, s_n)) \\
&\quad = f_i(S^n(r_1, S^n(t_1, s_1, \ldots, s_n), \ldots, S^n(t_n, s_1, \ldots, s_n)), \ldots, \\
&\quad\quad S^n(r_n, S^n(t_1, s_1, \ldots, s_n), \ldots, S^n(t_n, s_1, \ldots, s_n))) \\
&\quad = f_i\left(S^n\left(S^n(r_1, t_1, \ldots, t_n), s_1, \ldots, s_n\right), \ldots, \left(S^n(r_n, t_1, \ldots, t_n), s_1, \ldots, s_n\right)\right) \\
&\quad = S^n(f_i(S^n(r_1, t_1, \ldots, t_n), \ldots, S^{n_i}(r_n, t_1, \ldots, t_n)), s_1, \ldots, s_n) \\
&\quad = S^n(S^n(f_i(r_1, \ldots, r_n), t_1, \ldots, t_n), s_1, \ldots, s_n).
\end{aligned}$$

□

An algebra $\mathcal{M} := (M, S^n)$ of type $\tau = (n+1)$ is called a *Menger algebra* of rank n if $\mathcal{M}$ satisfies the condition (SASS) [2]. It follows immediately from Theorem 2.3 that $clone_{T(\bar{n},Y)}(\tau_n)$ is a Menger algebra of rank n. For basics and some advanced developments of Menger algebras can be found in the works of W.A. Dudek and V.S. Trokhimenko, for example, see [8, 9, 10].

It is clear that $clone_{T(\bar{n},Y)}(\tau_n)$ is generated by

$$F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)} := \left\{ f_i\left(x_{\alpha(1)}, \ldots, x_{\alpha(n)}\right) \mid i \in I, \alpha \in T(\bar{n}, Y) \right\}.$$

Let $V^{T(\bar{n},Y)}$ be the variety of type $\tau = (n+1)$ generated by the superassociative law (SASS). Now let $\mathcal{F}_{V^{T(\bar{n},Y)}}(\{Y_l \mid l \in J\})$ be the free algebra with respect to $V^{T(\bar{n},Y)}$, freely generated by an alphabet $\{Y_l \mid l \in J\}$ where $J = \{(i,\alpha) \mid i \in I\ , \alpha \in T(\bar{n},Y)\}$. The operation of $\mathcal{F}_{V^{T(\bar{n},Y)}}(\{Y_l \mid l \in J\})$ is denoted by $\tilde{S}^n$. Next, we are going to prove that the clone of all $T(\bar{n},Y)$-full terms is a free algebra with respect to the variety $V^{T(\bar{n},Y)}$.

Theorem 2.4. *The algebra* $clone_{T(\bar{n},Y)}(\tau_n)$ *is isomorphic to* $\mathcal{F}_{V^{T(\bar{n},Y)}}(\{Y_l \mid l \in J\})$ *and therefore it is free with respect to the variety* $V^{T(\bar{n},Y)}$*, and freely generated by the set*

$$\{f_i(x_{\alpha(1)},\ldots,x_{\alpha(n)}) \mid i \in I, \alpha \in T(\bar{n},Y)\}.$$

Proof. We define the mapping $\varphi : W_{\tau_n}^{T(\bar{n},Y)}(X_n) \longrightarrow \mathcal{F}_{V^{T(\bar{n},Y)}}(\{Y_l \mid l \in J\})$ inductively as follows:

(i) $\varphi(f_i(x_{\alpha(1)},\ldots,x_{\alpha(n)}) = y_{(i,\alpha)}$;

(ii) $\varphi(f_i(t_{\alpha(1)},\ldots,t_{\alpha(n)})) = \tilde{S}^n(y_{(i,\alpha)},\varphi(t_1),\ldots,\varphi(t_n))$.

Since φ maps the generating system of $clone_{T(\bar{n},Y)}(\tau_n)$ onto the generating system of $\mathcal{F}_{V^{T(\bar{n},Y)}}(\{Y_l \mid l \in J\})$, it is surjective. We prove the homomorphism property

$$\varphi(S^n(t_0,t_1,\ldots,t_n)) = \tilde{S}^n(\varphi(t_0),\varphi(t_1),\ldots,\varphi(t_n))$$

by induction on the depth of an n-ary $T(\bar{n},Y)$-full term t_0.If $t_0 = f_i(x_{\alpha(1)},\ldots,x_{\alpha(n)})$ where $\alpha \in T(\bar{n},Y)$, and $Depth(t) = 1$, then we have

$$\begin{aligned}
&\varphi(S^n(f_i(x_{\alpha(1)},\ldots,x_{\alpha(n)}),t_1,\ldots,t_n)) \\
&\qquad = \varphi(f_i(t_{\alpha(1)},\ldots,t_{\alpha(n)})) \\
&\qquad = \tilde{S}^n(y_{(i,\alpha)},\varphi(t_1),\ldots,\varphi(t_n)) \\
&\qquad = \tilde{S}^n(\varphi(f_i(x_{\alpha(1)},\ldots,x_{\alpha(n)})),\varphi(t_1),\ldots,\varphi(t_n)).
\end{aligned}$$

If $t_0 = f_i(r_1,\ldots,r_n)$ and assume that

$$\varphi(S^n(r_k,t_1,\ldots,t_n)) = \tilde{S}^n(\varphi(r_k),\varphi(t_1),\ldots,\varphi(t_n))$$

for all $1 \leqslant k \leq n$ and $max_{1\leqslant k\leqslant n}Depth(r_k) = m$, then $Depth(t) = m+1$ and we have

$$\begin{aligned}
&\varphi(S^n(f_i(r_1,\ldots,r_n),t_1,\ldots,t_n)) \\
&\quad = \varphi(f_i(S^n(r_1,t_1,\ldots,t_n),\ldots,S^n(r_n,t_1,\ldots,t_n))) \\
&\quad = \tilde{S}^n(y_{(i,1_n)},\varphi(S^n(r_1,t_1,\ldots,t_n)),\ldots,\varphi(S^n(r_n,t_1,\ldots,t_n))) \\
&\quad = \tilde{S}^n(y_{(i,1_n)},\tilde{S}^n(\varphi(r_1),\varphi(t_1),\ldots,\varphi(t_n)),\ldots, \\
&\qquad \tilde{S}^n(\varphi(r_n),\varphi(t_1),\ldots,\varphi(t_n))) \\
&\quad = \tilde{S}^n(\tilde{S}(y_{(i,1_n)},\varphi(r_1),\ldots,\varphi(r_n)),\varphi(t_1),\ldots,\varphi(t_n)) \\
&\quad = \tilde{S}^n(\varphi(f_i(r_1,\ldots,r_n)),\varphi(t_1),\ldots,\varphi(t_n)).
\end{aligned}$$

Thus φ is a homomorphism. The mapping φ is clearly bijective since the set $\{y_{(i,\alpha)} \mid i \in I,\ \alpha \in T(\bar{n},Y)\}$ is free independent. Therefore we have

$$y_{(i,\alpha)} = y_{(j,\beta)} \Longrightarrow (i,\alpha) = (j,\beta) \Longrightarrow i = j,\ \alpha = \beta.$$

So $f_i(x_{\alpha 1}), \ldots, x_{\alpha(n)}) = f_j(x_{\beta(1)}, \ldots, x_{\beta(n)})$. Thus φ is a bijection between the generating sets of $clone_{T(\bar{n},Y)}(\tau_n)$ and $\mathcal{F}_{V^{T(\bar{n},Y)}}(\{Y_l \mid l \in J\})$ and therefore φ is an isomorphism. $\square$

3. $T(\bar{n}, Y)$-full hypersubstitutions

The concept of a hypersubstitution is the main tool used to study hyperidentities and hypervarieties, see, for instance, in [7, 16, 17, 20] for more background. In this section, the monoid of hypersubstitution will be studied. First, we recall the definition and notation of hypersubstitutions.

A hypersubstitution of type τ is a mapping $\sigma : \{f_i \,|\, i \in I\} \longrightarrow W_\tau(X)$ which maps each operation symbol f_i to an n_i-ary term $\sigma(f_i)$ of type τ. Any hypersubstitution $\sigma : \{f_i \,|\, i \in I\} \longrightarrow W_\tau(X)$ can be uniquely extended to a mapping $\hat{\sigma} : W_\tau(X) \longrightarrow W_\tau(X)$ as follows:

(i) $\hat{\sigma}[t] := t$ if $t \in X$; and

(ii) $\hat{\sigma}[t] := S^{n_i}\left(\sigma(f_i), \hat{\sigma}[t_1], \ldots, \hat{\sigma}[t_{n_i}]\right)$ if $t = f_i(t_1, \ldots, t_{n_i}) \in W_\tau(X_{n_i})$.

The set $Hyp(\tau)$ of all hypersubstitutions of type τ forms a monoid under the binary operation $\circ_h$, defined by

$$\sigma_1 \circ_h \sigma_2 := \hat{\sigma_1} \circ \sigma_2$$

where $\circ$ denotes the usual composition of mappings.

The identity is $\sigma_{id} : \{f_i \mid i \in I\} \longrightarrow W_\tau(X)$ such that $\sigma_{id}(f_i) = f_i(x_1, ..., x_{n_i})$.

Now, we call mapping

$$\sigma : \{f_i \mid i \in I\} \longrightarrow W_{\tau_n}^{T(\bar{n},Y)}(X_n).$$

$T(\bar{n}, Y)$-*full hypersubstitution* of type τ_n.

For a $T(\bar{n}, Y)$-full term t we need the $T(\bar{n}, Y)$-full term t_β derived from t by replacement a variable $x_{\alpha(j)}$ in t by a variable $x_{\beta(\alpha(j))}$ for a mapping $\beta \in T(\bar{n}, Y)$. This can be defined as follows.

Let $t, t_1, \ldots, t_n \in W_{\tau_n}^{T(\bar{n},Y)}(X_n)$ and $\alpha, \beta \in T(\bar{n}, Y)$. Then we define the $T(\bar{n}, Y)$-full term t_β in the following steps:

(i) If $t = f_i(x_{\alpha(1)}, \ldots, x_{\alpha(n)})$, then $t_\beta := f_i(x_{\beta\alpha(1)}, \ldots, x_{\beta\alpha(n)})$.

(ii) If $t = f_i(t_1, \ldots, t_n)$, then $t_\beta := f_i((t_1)_\beta, \ldots, (t_n)_\beta)$.

It is observed that if t is an $T(\bar{n}, Y)$-full term of type τ_n, then t_β is an $T(\bar{n}, Y)$-full term of type τ_n for all $\beta \in T(\bar{n}, Y)$. Then an $T(\bar{n}, Y)$-full hypersubstitution $\sigma : \{f_i \mid i \in I\} \longrightarrow W_{\tau_n}^{T(\bar{n},Y)}(X_n)$ of type τ_n can be extended to a mapping

$$\hat{\sigma} : W_{\tau_n}^{T(\bar{n},Y)}(X_n) \longrightarrow W_{\tau_n}^{T(\bar{n},Y)}(X_n)$$

as follows:

(i) $\hat{\sigma}[f_i(x_{\alpha(1)},\ldots,x_{\alpha(n)})] := (\sigma(f_i))_\alpha$,

(ii) $\hat{\sigma}[f_i(t_1,\ldots,t_n)] := S^n\left(\sigma(f_i),\hat{\sigma}[t_1],\ldots,\hat{\sigma}[t_{n_i}]\right)$.

The set of all $T(\bar{n},Y)$-full hypersubstitutions of type τ_n will be denoted by $Hyp^{T(\bar{n},Y)}(\tau_n)$. It is easy to see that $\left(Hyp^{T(\bar{n},Y)}(\tau_n);\circ_h,\sigma_{id}\right)$ is a submonoid of $(Hyp(\tau_n);\circ_h,\sigma_{id})$.

The following lemma shows the property of a term t_α and the extension $\hat{\sigma}$.

Lemma 3.1. *Let* $t,t_1,...,t_n \in W_{\tau_n}^{T(\bar{n},Y)}(X_n)$. *Then*

$$S^n(t,\hat{\sigma}[t_{\alpha(1)}],\ldots,\hat{\sigma}[t_{\alpha(n)}]) = S^n(t_\alpha,\hat{\sigma}[t_1],\ldots,\hat{\sigma}[t_n])$$

for all $\alpha \in T(\bar{n},Y)$.

Proof. We begin with the case when $t = f_i(x_{\alpha(1)},x_{\alpha(2)},\ldots,x_{\alpha(n)})$, which is the first claim of the first step of the induction $Depth(t) = 1$. In fact, we have
$S^n(f_i(x_1,x_2,\ldots,x_n),\hat{\sigma}[t_{\alpha(1)}],\ldots,\hat{\sigma}[t_{\alpha(n)}]) = f_i(\hat{\sigma}[t_{\alpha(1)}],\hat{\sigma}[t_{\alpha(2)}],\ldots,\hat{\sigma}[t_{\alpha(n)}]) = S^n(f_i(x_{\alpha(1)},\ldots,x_{\alpha(n)}),\hat{\sigma}[t_1],\ldots,\hat{\sigma}[t_n]) = S^n(f_i(x_1,x_2,\ldots,x_n)_\alpha,\hat{\sigma}[t_1],\ldots,\hat{\sigma}[t_n])$.

If $t = f_i(s_1,\ldots,s_n)$ and assume that

$$S^n(s_k,\hat{\sigma}[t_{\alpha(1)}],\ldots,\hat{\sigma}[t_{\alpha(n)}]) = S^n((s_k)_{\alpha_i},\hat{\sigma}[t_{\alpha(1)}],\ldots,\hat{\sigma}[t_{\alpha(n)}])$$

for all $1 \leqslant k \leqslant n$ and $\alpha \in T(\bar{n},Y)$ then

$$\begin{aligned}
&S^n(t,\hat{\sigma}[t_{\alpha(1)}],\ldots,\hat{\sigma}[t_{\alpha(n)}])\\
&\quad = S^n(f_i(s_1,\ldots,s_n),\hat{\sigma}[t_{\alpha(1)}],\ldots,\hat{\sigma}[t_{\alpha(n)}])\\
&\quad = f_i(S^n(s_1,\hat{\sigma}[t_{\alpha(1)}],\ldots,\hat{\sigma}[t_{\alpha(n)}]),\ldots,S^n(s_n,\hat{\sigma}[t_{\alpha(1)}],\ldots,\hat{\sigma}[t_{\alpha(n)}]))\\
&\quad = f_i(S^n((s_1)_\alpha,\hat{\sigma}[t_1],\ldots,\hat{\sigma}[t_n]),\ldots,S^n((s_n)_\alpha,\hat{\sigma}[t_1],\ldots,\hat{\sigma}[t_n]))\\
&\quad = S^n(f_i((s_1)_\alpha,\ldots,(s_n)_\alpha),\hat{\sigma}[t_1],\ldots,\hat{\sigma}[t_n])\\
&\quad = S^n(t_\alpha,\hat{\sigma}[t_1],\ldots,\hat{\sigma}[t_n]).
\end{aligned}$$
□

Using Lemma 3.1 we show that the extension $\hat{\sigma}$ of each $T(\bar{n},Y)$-full hypersubstitution σ preserves the operation S^n on the set $W_{\tau_n}^{T(\bar{n},Y)}(X_n)$.

Theorem 3.2. *For* $\sigma \in Hyp^{T(\bar{n},Y)}(\tau_n)$, *the extension*

$$\hat{\sigma} : W_{\tau_n}^{T(\bar{n},Y)}(X_n) \longrightarrow W_{\tau_n}^{T(\bar{n},Y)}(X_n)$$

is an endomorphism on the algebra $clone_{T(\bar{n},Y)}(\tau_n)$.

Proof. It is clear that $\hat{\sigma} : W_{\tau_n}^{T(\bar{n},Y)}(X_n) \longrightarrow W_{\tau_n}^{T(\bar{n},Y)}(X_n)$. Let $t_0,t_1,\ldots,t_n \in W_{\tau_n}^{T(\bar{n},Y)}(X_n)$. We will show by induction on the depth of t_0 that

$$\hat{\sigma}[S^n(t_0,t_1,\ldots,t_n)] = S^n(\hat{\sigma}[t_0],\hat{\sigma}[t_1],\ldots,\hat{\sigma}[t_n]).$$

If $t_0 = f_i(x_{\alpha(1)},\ldots,x_{\alpha(n)})$ where $\alpha \in T(\bar{n},Y)$, and $Depth(t) = 1$, then we have

$$\begin{aligned}
\hat{\sigma}[S^n(t_0,t_1,\ldots,t_n)] &= \hat{\sigma}[S^n(f_i(x_{\alpha(1)},\ldots,x_{\alpha(n)}),t_1,\ldots,t_n)]\\
&= \hat{\sigma}[f_i(t_{\alpha 1)},\ldots,t_{\alpha(n)})]
\end{aligned}$$

$$\begin{aligned}&= S^n(\sigma(f_i), \hat{\sigma}[t_{\alpha(1)}], \ldots, \hat{\sigma}[t_{\alpha(n)}])\\ &= S^n(\hat{\sigma}[t_0], \hat{\sigma}[t_1], \ldots, \hat{\sigma}[t_n]).\end{aligned}$$

If $t_0 = f_i(r_1, \ldots, r_n)$ and we assume that

$$\hat{\sigma}[S^n(r_k, t_1, \ldots, t_n)] = S^n(\hat{\sigma}[r_k], \hat{\sigma}[t_1], \ldots, \hat{\sigma}[t_n])$$

for all $1 \leqslant k \leqslant n$ and $max_{1\leqslant k\leqslant n}Depth(r_k) = m$, then $Depth(t) = m + 1$ and we have

$$\begin{aligned}&\hat{\sigma}[S^n(t_0, t_1, \ldots, t_n)]\\ &\quad= \hat{\sigma}[S^n(f_i(r_1, \ldots, r_n), t_1, \ldots, t_n)]\\ &\quad= \hat{\sigma}[f_i(S^n(r_1, t_1, \ldots, t_n), \ldots, S^{n_i}(r_n, t_1, \ldots, t_n))]\\ &\quad= S^n(\sigma(f_i), \hat{\sigma}[S^n(r_1, t_1, \ldots, t_n)], \ldots, \hat{\sigma}[S^n(r_{n_i}, t_1, \ldots, t_n)])\\ &\quad= S^n(\sigma(f_i), S^n(\hat{\sigma}[r_1], \hat{\sigma}[t_1], \ldots, \hat{\sigma}[t_n]), \ldots, S^n(\hat{\sigma}[r_n], \hat{\sigma}[t_1], \ldots, \hat{\sigma}[t_n]))\\ &\quad= S^n(S^n(\sigma(f_i), \hat{\sigma}[r_1], \ldots, \hat{\sigma}[r_n]), \hat{\sigma}[t_1], \ldots, \hat{\sigma}[t_n])\\ &\quad= S^n(\hat{\sigma}[t_0], \hat{\sigma}[t_1], \ldots, \hat{\sigma}[t_n]). \qquad \square\end{aligned}$$

We complete this section by studying the connection between $T(\bar{n}, Y)$-full terms and the extension of a mapping which maps fundamental term to any $T(\bar{n}, Y)$-full terms.

As mentioned, the algebra $clone_{T(\bar{n},Y)}(\tau_n)$ is generated by the set

$$F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)} := \left\{ f_i\left(x_{\alpha(1)}, \ldots, x_{\alpha(n)}\right) \mid i \in I, \alpha \in T(\bar{n}, Y) \right\}.$$

Thus, any mapping

$$\eta : F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)} \longrightarrow W_{\tau_n}^{T(\bar{n},Y)}(X_n)$$

called $T(\bar{n}, Y)$-*full clone substitution*, can be uniquely extended to endomorphism

$$\bar{\eta} : W_{\tau_n}^{T(\bar{n},Y)}(X_n) \longrightarrow W_{\tau_n}^{T(\bar{n},Y)}(X_n).$$

Let $Subst_{T(\bar{n},Y)}(\tau_n)$ be the set of all $T(\bar{n}, Y)$-full clone substitutions. On the set $Subst_{T(\bar{n},Y)}(\tau_n)$, a binary operation $\odot$ can be defined by

$$\eta_1 \odot \eta_2 := \bar{\eta_1} \circ \eta_2$$

where $\circ$ denotes the usual composition of mappings. Furthermore, the identity mapping with respect to $\odot$ is denoted by $id_{F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}}$.

Then clearly, $\left(Subst_{T(\bar{n},Y)}(\tau); \odot, id_{F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}}\right)$ forms a monoid.

Consider $\sigma \in Hyp^{T(\bar{n},Y)}(\tau_n)$ and by Theorem 3.2,

$$\hat{\sigma} \colon W_{\tau_n}^{T(\bar{n},Y)}(X_n) \longrightarrow W_{\tau_n}^{T(\bar{n},Y)}(X_n)$$

is an endomorphism. Since $F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}$ generates $clone_{T(\bar{n},Y)}(\tau_n)$, $\hat{\sigma}\big|_{F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}}$ is an $T(\bar{n}, Y)$-full clone substitution with

$$\overline{\hat{\sigma}\big|_{F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}}} = \hat{\sigma}.$$

Define a mapping $\psi : Hyp^{T(\bar{n},Y)}(\tau_n) \longrightarrow Subst_{T(\bar{n},Y)}(\tau_n)$ by

$$\psi(\sigma) = \hat{\sigma}\big|_{F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}}.$$

We have that ψ is a homomorphism. In fact: Let $\sigma_1, \sigma_2 \in Hyp^{T(\bar{n},Y)}(\tau_n)$. Then

$$\begin{aligned}\psi(\sigma_1 \circ_h \sigma_2) &= (\sigma_1 \circ_h \sigma_2)^{\wedge}\big|_{F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}} = (\hat{\sigma_1} \circ \hat{\sigma_2})\big|_{F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}} \\ &= \overline{\hat{\sigma_1}\big|_{F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}}} \circ \hat{\sigma_2}\big|_{F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}} = \overline{\psi(\sigma_1)} \circ \psi(\sigma_2) \\ &= \psi(\sigma_1) \odot \psi(\sigma_2).\end{aligned}$$

Clearly, ψ is an injection. Hence we have proved, the following corollary.

Corollary 3.3. *The monoid* $\left(Hyp^{T(\bar{n},Y)}(\tau_n); \circ_h, \sigma_{id}\right)$ *can be embedded into* $(Subst_{T(\bar{n},Y)}(\tau_n); \odot, id_{F_{W_{\tau_n}^{T(\bar{n},Y)}(X_n)}})$.

4. $T(\bar{n}, Y)$-full hyperidentities and clone identities

In this section we examine the relationship between a variety V of type τ_n and the identity in the $clone_{T(\bar{n},Y)}(\tau_n)$.

Let V be a variety of type τ_n and let IdV be the set of all identities of V. Let $Id^{T(\bar{n},Y)}V$ be the set of all $s \approx t$ of V such that s and t are both $T(\bar{n}, Y)$-full term of type τ_n; that is

$$Id^{T(\bar{n},Y)}V := \left(W_{\tau_n}^{T(\bar{n},Y)}(X_n)\right)^2 \cap IdV.$$

It is well-known that IdV is a congruence on the free algebra $\mathcal{F}_\tau(X)$. However, in general this is not true for $Id^{T(\bar{n},Y)}V$. The following theorem shows that $Id^{T(\bar{n},Y)}V$ is a congruence on $clone_{T(\bar{n},Y)}(\tau_n)$.

Theorem 4.1. *Let* V *be a variety of type* τ_n. *Then* $Id^{T(\bar{n},Y)}V$ *is a congruence on the algebra* $clone_{T(\bar{n},Y)}(\tau_n)$.

Proof. We will prove that if $t \approx r$, $t_k \approx r_k \in Id^{T(\bar{n},Y)}V$, $k = 1, 2, \ldots, n$, then $S^n(t, t_1, \ldots, t_n) \approx S^n(r, r_1, \ldots, r_n) \in Id^{T(\bar{n},Y)}V$. Firstly, we give a proof by induction on the depth of a term $t \in W_{\tau_n}^{T(\bar{n},Y)}(X_n)$ that for every $i \in I$ from $t_k \approx r_k \in Id^{T(\bar{n},Y)}V$, $k = 1, 2, \ldots, n$, there follows $S^n(t, t_1, \ldots, t_n) \approx S^n(t, r_1, \ldots, r_n) \in Id^{T(\bar{n},Y)}V$. If $t = f_i(x_{\alpha(1)}, \ldots, x_{\alpha(n)})$, where $\alpha \in T(\bar{n}, Y)$, and $Depth(t) = 1$, then we have

$$\begin{aligned}S^n(f_i(x_{\alpha(1)}, \ldots, x_{\alpha(n)}), t_1, \ldots, t_n) &= f_i(t_{\alpha(1)}, \ldots, \overline{t_{\alpha(n)})} \\ &\approx f_i(r_{\alpha(1)}, \ldots, r_{\alpha(n)}) = \overline{\psi(\sigma_1)} \circ \psi(\sigma_2) \\ &= S^n(f_i(x_{\alpha(1)}, \ldots, x_{\alpha(n)}), r_1, \ldots, r_n) \in Id^{T(\bar{n},Y)}V,\end{aligned}$$

since IdV is compatible with the operation $\overline{f_i}$ of the absolutely free algebra $\mathcal{F}_\tau(X)$ and by the definition of $T(\bar{n}, Y)$-full terms.

If $t = f_i(l_1, \ldots, l_n) \in W_{\tau_n}^{T(\bar{n},Y)}(X_n)$ and assume that

$$S^n(l_k, t_1, ..., t_n) \approx S^n(l_k, r_1, ..., r_n) \in Id^{T(\bar{n},Y)}V.$$

for all $1 \leqslant k \leqslant n$ and $max_{1\leqslant k\leqslant n}Depth(r_k) = m$, then $Depth(t) = m + 1$ and we obtain

$$\begin{aligned} S^n(f_i(l_1, \ldots, l_n), t_1, \ldots, t_n) &= f_i(S^n(l_1, t_1, \ldots, t_n), \ldots, S^n(l_n, t_1, \ldots, t_n)) \\ &\approx f_i(S^n(l_1, r_1, \ldots, r_n), \ldots, S^{n_i}(l_n, r_1, \ldots, r_n)) \\ &= S^n(f_i(l_1, \ldots, l_n), r_1, \ldots, r_n) \in Id^{T(\bar{n},Y)}V. \end{aligned}$$

This means

$$S^n(t, t_1, \ldots, t_n) \approx S^n(t, r_1, \ldots, r_n) \in Id^{T(\bar{n},Y)}V.$$

This is a consequence of the fact that IdV is a fully invariant congruence on the absolutely free algebra $\mathcal{F}_\tau(X)$. Assume now that $t \approx r, t_k \approx r_k \in Id^{T(\bar{n},Y)}V$. Then

$$S^n(t, t_1, \ldots, t_n) \approx S^n(r, t_1, \ldots, t_n) \approx S^n(r, r_1, \ldots, r_n) \in Id^{T(\bar{n},Y)}V. \qquad \square$$

By using the concepts of $T(\bar{n}, Y)$-full hypersubstitution as we presented in Section 3. We shall define $T(\bar{n}, Y)$-full hyperidentities in a variety of typer τ_n.

Let V be a variety of type τ_n. An identity $s \approx t \in Id^{T(\bar{n},Y)}V$ is called a $T(\bar{n}, Y)$-*full hyperidentity* of V if $\hat{\sigma}[s] \approx \hat{\sigma}[t] \in IdV$ for all $\sigma \in Hyp^{T(\bar{n},Y)}(\tau_n)$. Moreover, the variety V is called $T(\bar{n}, Y)$-*full solid* if the following holds:

$$\forall s \approx t \in Id^{T(\bar{n},Y)}V \; \forall \sigma \in Hyp^{T(\bar{n},Y)}(\tau_n) \; \hat{\sigma}[s] \approx \hat{\sigma}[t] \in IdV.$$

Next theorem characterizes the $T(\bar{n}, Y)$-full solid variety.

Theorem 4.2. *Let V be a variety of type τ_n. If $Id^{T(\bar{n},Y)}V$ is a fully invariant congruence on $clone_{T(\bar{n},Y)}(\tau_n)$, then V is $T(\bar{n}, Y)$-full solid.*

Proof. Assume that $Id^{T(\bar{n},Y)}V$ is a fully invariant congruence on $clone_{T(\bar{n},Y)}(\tau_n)$. Let $s \approx t \in Id^{T(\bar{n},Y)}V$ and $\sigma \in Hyp^{T(\bar{n},Y)}(\tau_n)$. By Theorem 3.2, $\hat{\sigma}$ is an endomorphism of $clone_{T(\bar{n},Y)}(\tau_n)$. Hence $\hat{\sigma}[s] \approx \hat{\sigma}[t] \in Id^{T(\bar{n},Y)}V$, which shows that V is $T(\bar{n}, Y)$-full solid. $\square$

For a variety V of type τ_n, $Id^{T(\bar{n},Y)}V$ is a congruence on $clone_{T(\bar{n},Y)}(\tau_n)$ by Theorem 4.1. We can form the quotient algebra

$$clone_{T(\bar{n},Y)}(V) := clone_{T(\bar{n},Y)}(\tau_n)/Id^{T(\bar{n},Y)}V.$$

This quotient algebra belongs to the class of a Menger algebra of rank n. Note that we have a natural homomorphism

$$nat_{Id^{T(\bar{n},Y)}V} : clone_{T(\bar{n},Y)}(\tau_n) \longrightarrow clone_{T(\bar{n},Y)}(V)$$

such that

$$nat_{Id^{T(\bar{n},Y)}V}(t) = [t]_{Id^{T(\bar{n},Y)}V}.$$

Finally, we prove the following connection between $T(\bar{n}, Y)$-full hyperidentities of a variety V and clone identities.

Theorem 4.3. *Let V be a variety of type τ_n. If $s \approx t \in Id^{T(\bar{n},Y)}V$ is an identity in $clone_{T(\bar{n},Y)}(V)$, then $s \approx t$ is $T(\bar{n},Y)$-full hyperidentity of V.*

Proof. Assume that $s \approx t \in Id^{T(\bar{n},Y)}V$ is an identity in $clone_{T(\bar{n},Y)}(V)$. Let $\sigma \in Hyp^{T(\bar{n},Y)}(\tau_n)$. Then $\hat{\sigma} : clone_{T(\bar{n},Y)}(\tau_n) \longrightarrow clone_{T(\bar{n},Y)}(\tau_n)$ is an endomorphism by Theorem 3.2. Thus

$$nat_{Id^{T(\bar{n},Y)}V} \circ \hat{\sigma} : clone_{T(\bar{n},Y)}(\tau_n) \longrightarrow clone_{T(\bar{n},Y)}(V)$$

is a homomorphism. By assumption,

$$\left(nat_{Id^{T(\bar{n},Y)}V} \circ \hat{\sigma}\right)(s) = \left(nat_{Id^{T(\bar{n},Y)}V} \circ \hat{\sigma}\right)(t).$$

That is

$$nat_{Id^{T(\bar{n},Y)}V}(\hat{\sigma}[s]) = nat_{Id^{T(\bar{n},Y)}V}(\hat{\sigma}[t]).$$

Thus

$$[\hat{\sigma}[s]]_{Id^{T(\bar{n},Y)}V} = [\hat{\sigma}[t]]_{Id^{T(\bar{n},Y)}V},$$

and hence

$$\hat{\sigma}[s] \approx \hat{\sigma}[t] \in Id^{T(\bar{n},Y)}V.$$

Therefore, $s \approx t$ is a $T(\bar{n},Y)$-full hyperidentity of V. □

5. Open Problems

Finally, we give three problems and suggestions for the future research in this area.

(1) Determine the semigroup properties of the monoid $\left(Hyp^{T(\bar{n},Y)}(\tau_n); \circ_h, \sigma_{id}\right)$. Find the order of its elements for the particular type. Describe the idempotency and several kinds of regularity of the $T(\bar{n},Y)$-full hypersubstitutions.

(2) Use some difference definions of transformation semigroup, for instance transformations with invariant subset to define new generalizations of full terms. Study the connection between the different kinds of full terms.

(3) Based on [12], define the set of all formulas induced by $T(\bar{n},Y)$-full terms and study this set.

Acknowledgment. The research was supported by Rajamangala University of Technology Lanna and Chiang Mai University, Chiang Mai, Thailand. The authors are thankful to the referees for their valuable comments.

References

[1] **R. Chinram, S. Baupradist**, *Magnifying elements in a semigroup of transformations with restricted range*, Missouri J. Math. Sci., **30** (2018), No. 1, 54-58.

[2] **K. Denecke**, *Menger algebra and clones of terms*, East-West J. Math., **5** (2003), 179-193.

[3] **K. Denecke**, *Partial clones*, Asian-Eur. J. Math., **18** (2020), Article ID: 2050161.

[4] **K. Denecke, L. Freiberg**, *The algebra of strongly full terms*, Novi Sad J. Math., **34** (2004), 87-98.

[5] **K. Denecke, P. Jampachon**, *Clones of full terms*, Algebra Discrete Math., **4** (2004), 1-11.

[6] **K. Denecke, J. Koppitz, S. Shtrakov**, *The depth of a hypersubstitution*, J. Automata, Languages and Combinatorics, **6** (2001), No. 3, 253-262.

[7] **K. Denecke, J. Koppitz, S. Shtrakov**, *Multi-hypersubstitutions and colored solid varieties*, Int. J. Algebra Comput., **16** (2006), 797-815.

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

[9] **W.A. Dudek, V.S. Trokhimenko**, *Menger algebras of associative and self-distributiven-ary operations*, Quasigroups Related Syst., **26** (2018),45-52.

[10] **W.A. Dudek, V.S. Trokhimenko**, *Menger algebras of idempotent n-ary operations*, Stud. Sci. Math. Hung., **55** (2019), 260-269.

[11] **V.H. Fernandes, J. Sanwong**, *On the ranks of semigroups of transformations on a finite set with restricted range*, Algebra Colloq., **21** (2014), No. 3, 497-510.

[12] **J. Joomwong, D. Phusanga**, *Deterministic and Non-deterministic hypersubstitutions for algebraic systems*, Asian-Eur. J. Math., **9** (2016), No. 2, Article ID: 1650047.

[13] **T. Kumduang, S. Leeratanavalee**, *Monoid of linear hypersubstitutions for algebraic systems of type $((n),(2))$ and its regularity*, Songklanakarin J. Sci. Technol., **41** (2019), 1248-1259.

[14] **T. Kumduang, S. Leeratanavalee**, *Regularity of linear hypersubstitutions for algebraic systems of type $((n),(m))$*, Communications in Mathematics and Applications, **10** (2019), No. 1, 1-18.

[15] **T. Kumduang, S. Leeratanavalee**, *Semigroups of terms, tree languages, Menger algebra of n-ary functions and their embedding theorems*, Symmetry, **13** (2021), No. 4, 558.

[16] **S. Leeratanavalee**, *Outermost-strongly solid variety of commutative semigroups*, Thai J. Math., **14** (2016), No. 2, 305-313.

[17] **Yu. M. Movsisyan**, *Hyperidentities and related concepts, I*, Armen. J. Math., **10** (2018), 1-85.

[18] **S. Phuapong**, *Some algebraic properties of generalized clone automorphisms*, Acta Univ. Apulensis Math. Inform., **41** (2015), 165-175.

[19] **S. Phuapong, S. Leeratanavalee**, *The algebra of generalized full terms*, Int. J. Open Problems Compt. Math., **4** (2011), 54-65.

[20] **S. Phuapong, C. Pookpienlert**, *Fixed variables generalized hypersubstitutions*, Int. J. Math. Comput. Sci., **16** (2021), 133-142.

[21] **D. Phusanga, J. Koppitz**, *The semigroup of linear terms*, Asian-Eur. J. Math., **13** (2020), Article ID: 2050005.

[22] **S. Shtrakov**, *Essential variables and positions in terms*, Algebra Univers., **61** (2009), 381-397.

[23] **S. Shtrakov, K. Denecke**, *Essential variables and separable sets in universal algebra*, Multiple Valued Logic, An International Journal., **8** (2002), No. 2, 165-181.

[24] **S. Shtrakov, J. Koppitz**, *Stable varieties of semigroups and groupoids*, Algebra Univers., **75** (2016), 85-106.

[25] **R.P. Sullivan**, *Semigroups of Linear Transformations with Restricted Range*, Bull. Austral. Math. Soc., **77** (2008), 441-453.

[26] **J.S.V. Symons**, *Some results concerning a transformation semigroup*, J. Aust. Math. Soc., **19A(4)** (1975), 413-425.

[27] **K. Wattanatripop, T. Changphas**, *The clone of $K^*(n,r)$-full terms*, Discuss. Math. Gen. Algebra Appl., **39** (2019), 277-288.

[28] **K. Wattanatripop, T. Changphas**, *The Menger algebra of terms induced by order-decreasing transformations*, Commun. Algebra, (2021) DOI: 10.1080/00927872.2021.1888385

Received March 18, 2021

S. Phuapong
Department of Mathematics, Faculty of Science and Agricultural Technology
Rajamangala University of Technology Lanna, Chiang Mai, Thailand
e-mail: Phuapong.sa@gmail.com

T. Kumduang
Department of Mathematics, Faculty of Science, Chiang Mai University, Chiang Mai, Thailand
e-mail: Kumduang01@gmail.com

Quasigroups and Related Systems **29** (2021), 269 − 282

Some applications of the independence to the semigroup of all binary systems

Akbar Rezaei, Hee Sik Kim and Joseph Neggers

Abstract. We extend the notions of *right (left) independency* and *absorbent* from groupoids to $Bin(X)$ as a semigroup of all the groupoids on a set X and study and investigate many of their properties. We show that these new concepts are different by presenting several examples. In general, the concept of right (left) independence is a generalization and alternative of classical concept of the converse of *injective function*.

1. Introduction

Bruck [2] published a book, *A survey of binary systems* discussed in the theory of groupoids, loops and quasigroups, and several algebraic structures. Borůvka [3] stated the theory of decompositions of sets and its application to binary systems. Nebeský [12] introduced the notion of a travel groupoid by adding two axioms to a groupoid, and he described an algebraic interpretation of the graph theory. Allen et al. [1] introduced the concept of several types of groupoids related to semigroups, viz., twisted semigroups for which twisted versions of the associative law hold. Kim et al. [7] showed that every selective groupoid induced by a fuzzy subset is a pogroupoid, and they discussed several properties in quasi ordered sets by introducing the notion of a framework. Liu et al. [11] extended the theory of groupoids already developed for semigroups $(Bin(X), \square)$ in a growing number of research papers with X a set and $Bin(X)$ the set of groupoids defined on X to the generalizations: fuzzy (sub)groupoids and hyperfuzzy (sub)groupoids. Hwang et al. [8] generalized the notion of an implicativity discussed in BCK-algebras, and applied it to some groupoids and BCK-algebras. Also, they discussed the notion of the locally finiteness and convolution products in groupoids [9]. Fayoumi introduced the notions of locally zero groupoids and the center of $Bin(X)$ of all binary systems on a set X [4]. Also, she introduced two methods of factorization for this binary system under the binary groupoid product in the semigroup $(Bin(X), \square)$ and showed that a strong non-idempotent groupoid can be represented as a product of its similar- and signature- derived factors. Moreover, she showed that a groupoid with the orientation property is a product of its orient- and skew-factors [5]. Feng et al. discussed on some relations among axioms in groupoids, and

2010 Mathematics Subject Classification: 20N02, 06F35.
Keywords: groupoid, (right , left) independence, (right , left) absorbent.

obtained some useful properties [6].

The motivation of this study came from the idea of the converse of "injective function". We applied this concepts to $Bin(X)$, and obtained several properties. Moreover, we discuss the right (left) absorbent subsets of $Bin(X)$. We provide several (counter-) examples to describe the concepts.

2. Preliminaries

A groupoid $(X, *)$ is said to be a *right zero semigroup* if $x * y = y$ for any $x, y \in X$, and a groupoid $(X, *)$ is said to be a *left zero semigroup* if $x * y = x$ for any $x, y \in X$. A groupoid $(X, *)$ is said to be a *right oid* for $f : X \to X$ if $x * y = f(y)$ for any $x, y \in X$. Similarly, a groupoid $(X, *)$ is said to be a *leftoid* for $f : X \to X$ if $x * y = f(x)$ for any $x, y \in X$. Note that a right (left, resp.) zero semigroup is a special case of a right oid(leftoid, resp.) (see [10]). A groupoid $(X, *)$ is said to be *right cancellative* (or *left cancellative*, resp.) if $y * x = z * x$ $(x * y = x * z$, resp.) implies $y = z$. A groupoid $(X, *)$ is said to be *locally zero* [4] if

(i) $x * x = x$ for all $x \in X$,

(ii) for any $x \neq y \in X$, $(\{x, y\}, *)$ is either a left zero semigroup or a right zero semigroup.

Given a groupoid $(X, *)$ (i.e., $(X, *) \in Bin(X)$), a non-empty subset E of X is said to be *right independence* if $x \neq y \in E$, then $x * u \neq y * u$ for all $u \in X$. Also E is said to be *left independence* if $x \neq y \in E$, then $u * x \neq u * y$ for all $u \in X$. E is said to be *independence* if it both right and left independence [13].

The notion of the semigroup $(Bin(X), \Box)$ was introduced by Kim and Neggers [10]. Given binary operations "$*$" and "$\bullet$" on a set X, they defined a product binary operation "$\Box$" as follows: $x \Box y = (x * y) \bullet (y * x)$. This in turn yields a binary operation on $Bin(X)$, the set of all groupoids, defined on X turning $(Bin(X), \Box)$ into a semigroup with identity $(x * y = x)$, the left zero semigroup, and an analog of negative one in the right zero semigroup [10].

Example 2.1. Let $X := \{a, b\}$ be a set. Then we have 16 groupoids $(X, *_i)$ for $i \in \{1, \ldots, 16\}$ with the following tables.

$*_1$	a	b
a	a	a
b	a	a

$*_2$	a	b
a	b	a
b	a	a

$*_3$	a	b
a	a	b
b	b	a

$*_4$	a	b
a	b	b
b	a	a

$*_5$	a	b
a	a	a
b	b	a

$*_6$	a	b
a	b	a
b	b	a

$*_7$	a	b
a	a	b
b	a	b

$*_8$	a	b
a	b	b
b	b	a

$*_9$	a	b
a	a	a
b	b	b

$*_{10}$	a	b
a	b	a
b	a	b

$*_{11}$	a	b
a	a	b
b	b	b

$*_{12}$	a	b
a	b	b
b	a	b

$*_{13}$	a	b
a	a	a
b	a	b

$*_{14}$	a	b
a	b	a
b	b	b

$*_{15}$	a	b
a	a	b
b	a	a

$*_{16}$	a	b
a	b	b
b	b	b

It follows that $Bin(X) = \{(X, *_i)\}_{i \in \{1, \ldots, 16\}}$. We see that $(Bin(X), \Box)$, where $\Box$ is defined by $x \Box y = (x *_i y) *_j (y *_i x)$ for all $i, j \in \{1, \ldots, 16\}$, forms a semigroup.

For example, $(X,*_1)\Box(X,*_2)$ and $(X,*_2)\Box(X,*_1)$ are groupoids with the following tables:

$\Box$	a	b
a	b	b
b	b	b

$\Box$	a	b
a	a	a
b	a	a

It is seen that $(X,*_1)\Box(X,*_2) = (X,*_{16}) \neq (X,*_2)\Box(X,*_1) = (X,*_1)$. Also, for example, in $(X,*_6)\Box(X,*_7)$, we have $a\Box b = (a *_6 b) *_7 (b *_6 a) = a *_7 b = b$, but $b\Box a = (b *_6 a) *_7 (a *_6 b) = b *_7 a = a$, and so $a\Box b \neq b\Box a$. Further, $(Bin(X),\Box)$ it is not a left cancellative semigroup, since $(X,*_2)\Box(X,*_3) = (X,*_2)\Box(X,*_5) = (X,*_1)$, but $(X,*_3) \neq (X,*_5)$. Also, it is not a right cancellative semigroup, since $(X,*_{13})\Box(X,*_{14}) = (X,*_1)\Box(X,*_{14}) = (X,*_{16})$, but $(X,*_{13}) \neq (X,*_1)$.

3. right (left) independence in $Bin(X)$

Definition 3.1. A non-empty subset $\mathbb{A} \subseteq Bin(X)$ is said to be *right independence* if $(X,*) \neq (X,\bullet)$ in $\mathbb{A}$, then $(X,*)\Box(X,\diamond) \neq (X,\bullet)\Box(X,\diamond)$ for all $(X,\diamond) \in Bin(X)$. Also $\mathbb{A}$ is said to be *left independence* if $(X,*) \neq (X,\bullet) \in \mathbb{A}$, then $(X,\diamond)\Box(X,*) \neq (X,\diamond)\Box(X,\bullet)$ for all $(X,\diamond) \in Bin(X)$. $\mathbb{A}$ is said to be *independence* if it both right and left independence.

Example 3.2. (a). Let $(R,+,\cdot,0,1)$ be a commutative ring with identity 1, 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 $a,b,c \in R$. Such a groupoid is said to be a *linear groupoid.* Notice that $a = 1$, $b = c = 0$ yields $x * y = 1 \cdot x = x$, and thus the left zero semigroup on R is a linear groupoid. Now, suppose that $(R,*)$ and $(R,\bullet)$ are linear groupoids where $x * y = ax + by + c$ and $x \bullet y = dx + ey + f$. Then

$$x\Box y = d(ax+by+c) + e(ay+bx+c) + f = (da+cb)x + (db+ca)y + (d+e)c + f,$$

whence $(R,\Box) = (R,*)\Box(R,\bullet)$ is also a linear groupoid (i.e., $(L(R),\Box)$ is a semigroup with identity (cf. [5])).

Let $L(A)$ denote the collection of all groupoids $(R,*)$ such that for all $x,y \in R$,

$$x * y = ax,$$

where $a \in R$. Now, suppose that $(R,*) \neq (R,\bullet) \in L(A)$ where $x * y = a_1x$ and $x \bullet y = a_2x$, for some $a_1 \neq a_2 \in R$. Let $(R,\diamond) \in L(R)$, where $x \diamond y := ax + by + c$ for some $a,b,c \in R$ with $abc \neq 0$. Hence

$x\Box y = (x * y) \diamond (y * x) = a_1x \diamond a_1y = aa_1x + ba_1y + c$ in $(R,*)\Box(R,\diamond)$ and

$x\Box y = (x \bullet y) \diamond (y \bullet x) = a_2x \diamond a_2y = aa_2x + ba_2y + c$ in $(R,\bullet)\Box(R,\diamond)$.

Assume $(R,*)\Box(R,\diamond) = (R,\bullet)\Box(R,\diamond)$. Then $aa_1x + ba_1y + c = aa_2x + ba_2y + c$ and hence $a(a_1 - a_2)x + b(a_1 - a_2)y = 0$. Since $a_1 \neq a_2$, we obtain $a = b = 0$, a contradiction. Thus, $(R,*)\Box(R,\diamond) \neq (R,\bullet)\Box(R,\diamond)$, and hence $L(A)$ is a right independence subset of $L(R)$. Moreover, $x\Box y = (x\diamond y)*(y\diamond x) = (ax+by+c)*(ay+bx+c) = a_1(ax+by+c) = a_1ax+a_1by+a_1c$ in $(R,\diamond)\Box(R,*)$ and $x\Box y = (x\diamond y)\bullet(y\diamond x) = (ax+by+c)\bullet(ay+bx+c) = a_2(ax+by+c) = a_2ax+a_2by+a_2c$ in $(R,\diamond)\Box(R,\bullet)$. It is easy to see that $a_1ax+a_1by+a_1c \neq a_2ax+a_2by+a_2c$. Thus, $(R,\diamond)\Box(R,*) \neq (R,\diamond)\Box(R,\bullet)$, and so $L(A)$ is a left independence subset of $L(R)$. Therefore $L(A)$ is an independence subset of $L(R)$.

(b). Let $\mathbb{R}$ denote the real numbers. Let $\mathbb{R}^* := \mathbb{R}\setminus\{0\}$, and let $L(\mathbb{R}^*)$ denote the collection of all groupoids on $\mathbb{R}^*$ (e.g., $(\mathbb{R}^*,\cdot)$, $(\mathbb{R}^*,+)$, $(\mathbb{R}^*,-)$, $(\mathbb{R}^*,\div)$ and $(\mathbb{R}^*,\bullet)$ where $\bullet : \mathbb{R}^*\times\mathbb{R}^* \longrightarrow \mathbb{R}^*$ is an arbitrary binary relation on $\mathbb{R}^*$. Take $A = \{(\mathbb{R}^*,+),(\mathbb{R}^*,\cdot)\}$. Then A is not a right independence subset of $L(\mathbb{R}^*)$. Since $(\mathbb{R}^*,+) \neq (\mathbb{R}^*,\cdot) \in A$ and $(\mathbb{R}^*,\div) \in L(\mathbb{R}^*)$, for all $x,y \in \mathbb{R}^*$, we get $x\Box y = (x+y)\div(y+x) = 1$ in $(\mathbb{R}^*,+)\Box(\mathbb{R}^*,\div)$ and $x\Box y = (x\cdot y)\div(y\cdot x) = 1$ in $(\mathbb{R}^*,\cdot)\Box(\mathbb{R}^*,\div)$. Thus, $(\mathbb{R}^*,+)\Box(\mathbb{R}^*,\div) = (\mathbb{R}^*,\cdot)\Box(\mathbb{R}^*,\div)$.

Note that the singleton set $\{(X,*)\} \subseteq Bin(X)$ is right (left) independence, since $\{(X,*)\}$ has no element $(X,\bullet) \in Bin(X)$ such that $(X,*) \neq (X,\bullet)$. Also, if $(Bin(X),\Box)$ is a group, then every subset of $Bin(X)$ is both right and left independence, and so it is an independence subset of $Bin(X)$. By routine calculation we can see that if $A_i \subseteq Bin(X)$ for $i\in\Lambda$ are right (left) independence, then $\bigcap_{i\in\Lambda} A_i$ and $\bigcup_{i\in\Lambda} A_i$ are right (left) independence. Note that if $\mathbb{B}$ and $\mathbb{D}$ are not right (left) independence subsets of $Bin(X)$, then $\mathbb{B}\cap\mathbb{D}$, $\mathbb{B}\cup\mathbb{D}$, $\mathbb{D}\setminus\mathbb{B}$ and $\mathbb{B}\triangle\mathbb{D}$ are not right (left) independence subsets of $Bin(X)$.

The following example shows that there exists a right (left) independence subset $\mathbb{A}$ of $Bin(X)$ such that $\mathbb{A}' = Bin(X)\setminus\mathbb{A}$ is not a right (left) independence subset of $Bin(X)$.

Example 3.3. Consider groupoid $(X,*_1)$ at Example 2.1. Then $\mathbb{A} = \{(X,*_1)\}$ is a right independence subset of $Bin(X)$ and

$$\mathbb{A}' = Bin(X)\setminus\{(X,*_1)\} = \{(X,*_i)\}_{i\in\{2,\ldots,16\}}.$$

The subset $\mathbb{A}'$ is not a right independence subset of $Bin(X)$, since $(X,*_{11}) \neq (X,*_{12}) \in \mathbb{A}'$, but $(X,*_{11})\Box(X,*_{16}) = (X,*_{12})\Box(X,*_{16})$. Moreover, it is not a left independence subset of $Bin(X)$, since $(X,*_{16})\Box(X,*_{11}) = (X,*_{16})\Box(X,*_{12}) = \{b\}$. Thus, $\mathbb{A}'$ is not an independence subset of $Bin(X)$.

Proposition 3.2. *Let $\mathbb{A},\mathbb{B} \subseteq Bin(X)$ and $\mathbb{A}$ be a right (left) independence subset of $Bin(X)$. Then $\mathbb{A}\cap\mathbb{B}$ a right (left) independence subset of $Bin(X)$.*

Proof. Assume $\mathbb{A}$ is a right (left) independence subset of $Bin(X)$ and $\mathbb{B}$ is an arbitrary subset of $Bin(X)$. Let $(X,*) \neq (X,\bullet)$ in $\mathbb{A}\cap\mathbb{B}$. Since $\mathbb{A}\cap\mathbb{B} \subseteq \mathbb{A}$, we get $(X,*) \neq (X,\bullet)$ in $\mathbb{A}$. Since $\mathbb{A}$ is a right (left) independence subset of $Bin(X)$, for all $(X,\diamond) \in Bin(X)$, we have $(X,*)\Box(X,\diamond) \neq (X,\bullet)\Box(X,\diamond)$, and hence $\mathbb{A}\cap\mathbb{B}$ is a right (left) independence subset of $Bin(X)$. $\Box$

Corollary 3.3. *Let $\mathbb{A}, \mathbb{B} \subseteq Bin(X)$ and $\mathbb{A}$ be a right (left) independence subset of $Bin(X)$. Then $\mathbb{A} \setminus \mathbb{B}$ a right (left) independence subset of $Bin(X)$.*

Proof. Since $\mathbb{A} \setminus \mathbb{B} = \mathbb{A} \cap \mathbb{B}'$, using Proposition 3.2, we obtain that $\mathbb{A} \setminus \mathbb{B}$ is a right (left) independence subset of $Bin(X)$. $\square$

Corollary 3.4. *Let $\mathbb{A}, \mathbb{B} \subseteq Bin(X)$ and $\mathbb{A}$ be a right (left) independence subset of $Bin(X)$. If $\mathbb{B} \subseteq \mathbb{A}$, then $\mathbb{B}$ is a right (left) independence subset of $Bin(X)$.*

Corollary 3.5. *Let $Bin(X)$ be right (left) independence and let $\mathbb{A} \subseteq Bin(X)$. Then $\mathbb{A}$ is a right (left) independence subset of $Bin(X)$.*

Proof. It follows immediately from Corollary 3.4. $\square$

The following example shows that there exists a right (left) independence subset $\mathbb{A}$ of $Bin(X)$ such that $\mathbb{A} \cup \mathbb{B}$ is not a right (left) independence subset of $Bin(X)$ for some $\mathbb{B} \subseteq Bin(X)$.

Example 3.4. Consider Example 3.3, and take $\mathbb{B} := \mathbb{A}'$, the complement of $\mathbb{A}$ in $Bin(X)$. Then $\mathbb{B}$ is not an independence subset of $Bin(X)$. Then $\mathbb{A} \cup \mathbb{B} = \mathbb{A} \cup \mathbb{A}' = Bin(X)$, which is not a right (left) independence subset of $Bin(X)$, since $(X, *_{11}) \neq (X, *_{12}) \in Bin(X)$, but $(X, *_{11})\square(X, *_{16}) = (X, *_{12})\square(X, *_{16})$. Moreover, it is not a left independence subset of $Bin(X)$, since $(X, *_{16})\square(X, *_{11}) = (X, *_{16})\square(X, *_{12}) = \{b\}$. Thus, $Bin(X)$ itself is not an independence subset of $Bin(X)$. Also, $\mathbb{A} \triangle \mathbb{B} = \mathbb{A} \triangle \mathbb{A}' = (\mathbb{A} \cup \mathbb{A}') \setminus (\mathbb{A} \cap \mathbb{A}') = Bin(X) \setminus \emptyset = Bin(X)$, which is not a right (left) independence subset of $Bin(X)$.

Theorem 3.6. *Let $Bin(X) := \mathbb{A} \cup \mathbb{B}$, where $\mathbb{B} \subseteq Bin(X)$ is a non-trivial group and A be a right (left) independence subset of $Bin(X)$. Then $Bin(X)$ is independence.*

Proof. Assume $\mathbb{B}$ is a non-trivial group and $\mathbb{A}$ is a right independence subset of $Bin(X)$ satisfying $Bin(X) = \mathbb{A} \cup \mathbb{B}$. Let $(X, *) \neq (X, \bullet)$ in $Bin(X)$.

Case 1. if $(X, *) \neq (X, \bullet)$ in $Bin(X) \cap \mathbb{A}$, since $\mathbb{A}$ is a right independence subset of $Bin(X)$, we get $(X, *)\square(X, \diamond) \neq (X, \bullet)\square(X, \diamond)$ for all $(X, \diamond) \in Bin(X)$.

Case 2. if $(X, *) \neq (X, \bullet)$ in $Bin(X) \cap \mathbb{B}$. We claim that

$$(X, *)\square(X, \diamond) \neq (X, \bullet)\square(X, \diamond) \text{ for all } (X, \diamond) \in Bin(X).$$

Assume $(X, *)\square(X, \diamond) = (X, \bullet)\square(X, \diamond)$ for some $(X, \diamond) \in Bin(X)$. Since $\mathbb{B}$ is a non-trivial group, we have $|\mathbb{B}| \geqslant 2$. Hence there is at least one element $(X, \circ) \in \mathbb{B}$, and so there is $(X, \circ)^{-1} \in \mathbb{B}$ as an inverse of $(X, \circ)$ (i.e., $(X, \circ)\square(X, \circ)^{-1} = (X, \star)$ and $(X, \star)$ is the left zero semigroup). Thus,

$$((X, *)\square(X, \circ))\square(X, \circ)^{-1} = (X, *)\square((X, \circ)\square(X, \circ)^{-1}) = (X, *)\square(X, \star) = (X, *)$$

and

$$((X, \bullet)\square(X, \circ))\square(X, \circ)^{-1} = (X, \bullet)\square((X, \circ)\square(X, \circ)^{-1}) = (X, \bullet)\square(X, \star) = (X, \bullet).$$

Therefore, $(X,*) = (X,\bullet)$, which is a contradiction.

CASE 3. Let $(X,*) \in \mathbb{A}$ and $(X,\bullet) \in \mathbb{B}$ such that $(X,*) \neq (X,\bullet)$. We claim that $(X,*)\Box(X,\diamond) \neq (X,\bullet)\Box(X,\diamond)$ for all $(X,\diamond) \in Bin(X)$.

Assume $(X,*)\Box(X,\diamond) = (X,\bullet)\Box(X,\diamond)$ for some $(X,\diamond) \in Bin(X)$. Since $(X,\bullet) \in \mathbb{B}$ and $\mathbb{B}$ is a non-trivial group, there is $(X,\bullet)^{-1} \in \mathbb{B}$ as an inverse of $(X,\bullet)$ (i.e., $(X,\bullet)\Box(X,\bullet)^{-1} = (X,\star)$ and $(X,\star)$ is the left zero semigroup). Thus,

$$\begin{aligned}((X,*)\Box(X,\bullet)^{-1})\Box(X,\bullet) &= ((X,\bullet)\Box(X,\bullet)^{-1})\Box(X,\bullet)\\ &= (X,\star)\Box(X,\bullet) = (X,\bullet) \in \mathbb{B}.\end{aligned}$$

Since $(X,\star)$ is a left zero semigroup, we get $(X,*)\Box(X,\bullet)^{-1} = (X,\star)$, and so $(X,*) = (X,\bullet)$, which is a contraction.

Similarly, we prove the theorem for the case of a left independence subset in $Bin(X)$. $\Box$

Corollary 3.7. *If $Bin(X) = \bigcup_{i\in\Lambda} \mathbb{A}_i$ is a right (left) independence, $\mathbb{A}_i \neq \emptyset$ for all $i \in \Lambda$, and $\mathbb{A}_j$ is a non-trivial group for some $j \in \Lambda$. Then every $\mathbb{A}_i$ $(i \neq j \in \Lambda)$ is a right (left) independence subset of $Bin(X)$.*

Proposition 3.8. *Let $(\mathbb{A},\Box_1)$ and $(\mathbb{B},\Box_2)$ be right (left, respectively) independence subsets of $(Bin(X),\Box_1)$ and $(Bin(Y),\Box_2)$ respectively. Then $\mathbb{A}\times\mathbb{B}$ is a right (left, respectively) independence subset of $(Bin(X)\times Bin(Y),\Box)$, where $\Box$ is defined by $(x,u)\Box(y,v) := (x\Box_1 y, u\Box_2 v)$.*

Proof. Assume $(\mathbb{A},\Box_1)$ and $(\mathbb{B},\Box_2)$ are right independence subsets of $Bin(X)$ and $Bin(Y)$ respectively. Let $(X,*_1)\times(Y,\circ_1) \neq (X,*_2)\times(Y,\circ_2)$, where $(X,*_i) \in \mathbb{A}$ and $(Y,\circ_i) \in \mathbb{B}$ for $i \in \{1,2\}$. Then either $(X,*_1) \neq (X,*_2)$ or $(Y,\circ_1) \neq (Y,\circ_2)$. Since $\mathbb{A}$ and $\mathbb{B}$ are right independence subsets of $Bin(X)$ and $Bin(Y)$ respectively, we obtain either $(X,*_1)\Box_1(X,\bullet) \neq (X,*_2)\Box_1(X,\bullet)$ or $(Y,\circ_1)\Box_2(Y,\diamond) \neq (Y,\circ_2)\Box_2(Y,\diamond)$ for all $(X,\bullet) \in Bin(X)$ and $(Y,\diamond) \in Bin(Y)$. It follows that

$$((X,*_1)\times(Y,\circ_1))\Box((X,\bullet)\times(Y,\diamond)) \neq ((X,*_2)\times(Y,\circ_2))\Box((X,\bullet)\times(Y,\diamond))$$

for all $(X,\bullet)\times(Y,\diamond) \in \mathbb{A}\times\mathbb{B}$. Therefore, $\mathbb{A}\times\mathbb{B}$ is a right independence subset of $Bin(X)\times Bin(Y)$. Similarly, we can prove the case of the left independence, and we omit it. $\Box$

Let $\emptyset \neq \mathbb{A} \subseteq Bin(X)$, and let $(X,*) \in Bin(X)$. Define two sets $(X,*)\Box\mathbb{A}$ and $\mathbb{A}\Box(X,*)$ as follows:

$$(X,*)\Box\mathbb{A} = \{(X,*)\Box(X,\circ) : (X,\circ) \in \mathbb{A}\}$$

and

$$\mathbb{A}\Box(X,*) = \{(X,\circ)\Box(X,*) : (X,\circ) \in \mathbb{A}\}.$$

Note that if $\mathbb{A} = \{(X,\diamond)\}$ (i.e., $|\mathbb{A}| = 1$), then $\{(X,*)\Box(X,\diamond)\}$ and $\{(X,\diamond)\Box(X,*)\}$ are also singleton sets, and so these are independence subsets of $Bin(X)$.

Proposition 3.9. *Let $Bin(X)$ be a right (left) zero semigroup, and $(X,*) \in Bin(X)$. Then $A\Box(X,*)$ (resp., $(X,*)\Box A$) is an independence subset of $Bin(X)$.*

Proof. Assume $Bin(X)$ is a right (left) zero semigroup. Then $A\Box(X,*) = \{(X,*)\}$ (resp., $(X,*)\Box A = \{(X,*)\}$). Thus, the proof is complete. $\Box$

Proposition 3.10. *If $Bin(X)$ is a right (left) zero semigroup, $A \subseteq Bin(X)$ is a right (left) independence subset, and $(X,*) \in Bin(X)$, then $(X,*)\Box A$ (resp., $A\Box(X,*)$) is a right (left) independence subset of $Bin(X)$.*

Proof. Assume $Bin(X)$ is a right (left) zero semigroup, $A \subseteq Bin(X)$ is a right (left) independence and $(X,*) \in Bin(X)$. Then $A\Box(X,*) \subseteq A$ (resp., $(X,*)\Box A \subseteq A$). Using Proposition 3.2, we get $(X,*)\Box A \subseteq A$ (resp., $A\Box(X,*) \subseteq A$) is a right (left) independence subset of $Bin(X)$. $\Box$

Proposition 3.11. *If $Bin(X)$ is a right cancellative, and $A \subseteq Bin(X)$ (right (left) independence or not), where $|A| > 1$ and $(X,*) \in Bin(X)$, then $(X,*)\Box A$ and $(X,*)\Box A$ are independence subsets of $Bin(X)$.*

Proof. Assume $(X,*)\Box(X,*_1) \neq (X,*)\Box(X,*_2) \in (X,*)\Box A$ for some $(X,*_i) \in A$ for $i \in \{1,2\}$, and let $(X,\diamond) \in Bin(X)$.

On the contrary, if $((X,*)\Box(X,*_1))\Box(X,\diamond) = ((X,*)\Box(X,*_2))\Box(X,\diamond)$ for some $(X,\diamond) \in Bin(X)$, then using cancellative laws we get $(X,*)\Box(X,*_1) = (X,*)\Box(X,*_2)$, which is a contradiction. Thus, $(X,*)\Box A$ is an independence subset of $Bin(X)$.

Similarly, if $Bin(X)$ is a left cancellative, then $(X,*)\Box A$ is an independence subset of $Bin(X)$.

By a similar argument for the set $A\Box(X,*)$ the result is valid. $\Box$

Let $\mathbb{E} \subseteq Bin(X)$, and $(X,*) \in Bin(X)$. Define

$$(X,*)\mathbb{E} := \{(X,\bullet) \in \mathbb{E} : (X,*)\Box(X,\bullet) = (X,\bullet)\},$$

$$\mathbb{E}(X,*) := \{(X,\bullet) \in \mathbb{E} : (X,\bullet)\Box(X,*) = (X,\bullet)\}$$

and

$$(X,*)\mathbb{E}(X,*) := \{(X,\bullet) \in \mathbb{E} : (X,*)\Box(X,\bullet) = (X,\bullet)\Box(X,*) = (X,\bullet)\}.$$

(a) If $\mathbb{E} = \emptyset$, then $(X,*)\mathbb{E} = \mathbb{E}(X,*) = (X,*)\mathbb{E}(X,*) = \emptyset$, for all $(X,*) \in Bin(X)$.

(b) For all $(X,*) \in Bin(X)$, $(X,*)\mathbb{E}$, $\mathbb{E}(X,*)$ and $(X,*)\mathbb{E}(X,*)$ are subsets of $Bin(X)$ and we have:

(i) $(X,*)\mathbb{E} \cap \mathbb{F} = (X,*)\mathbb{E} \cap (X,*)\mathbb{F}$,
$\mathbb{E} \cap \mathbb{F}(X,*) = \mathbb{E}(X,*) \cap \mathbb{F}(X,*)$,
$(X,*)\mathbb{E} \cap \mathbb{F}(X,*) = (X,*)\mathbb{E}(X,*) \cap (X,*)\mathbb{F}(X,*)$.

(ii) $(X,*)\mathbb{E}\cup\mathbb{F}\subseteq(X,*)\mathbb{E}\cap(X,*)\mathbb{F}$,
$\mathbb{E}\cap\mathbb{F}(X,\cup)\subseteq\mathbb{E}(X,*)\cup\mathbb{F}(X,*)$,
$(X,*)\mathbb{E}\cup\mathbb{F}(X,*)\subseteq(X,*)\mathbb{E}(X,*)\cup(X,*)\mathbb{F}(X,*)$.

(iii) $(X,*)\mathbb{E}\cap Bin(X)=(X,*)\mathbb{E}$.

(iv) $(X,*)\mathbb{E}\cup Bin(X)=(X,*)Bin(X)$.

(v) if $\mathbb{E}\subseteq\mathbb{F}$, then $(X,*)\mathbb{E}\subseteq(X,*)\mathbb{F}$, $\mathbb{E}(X,*)\subseteq\mathbb{F}(X,*)$, and so $(X,*)\mathbb{E}(X,*)\subseteq(X,*)\mathbb{F}(X,*)$.

(vi) $(X,*)\mathbb{E}(X,*)=(X,*)\mathbb{E}\cap\mathbb{E}(X,*)$,

(vii) $(X,*)(\mathbb{E}\setminus\mathbb{F})=(X,*)\mathbb{E}\setminus(X,*)\mathbb{F}$,
$(\mathbb{E}\setminus\mathbb{F})(X,*)=\mathbb{E}(X,*)\setminus\mathbb{F}(X,*)$,
$(X,*)(\mathbb{E}\setminus\mathbb{F})(X,*)=(X,*)\mathbb{E}(X,*)\setminus(X,*)\mathbb{F}(X,*)$.

(viii) If $\mathbb{E}$ is a group in $Bin(X)$, then for all $(X,\bullet)\in(X,*)\mathbb{E}$ (resp., $(X,\bullet)\in\mathbb{E}(X,*)$ or $(X,\bullet)\in(X,*)\mathbb{E}(X,*)$) we have $(X,*)=(X,\star)$, as a zero element.

(ix) If $(X,*)\in(X,*)\mathbb{E}$ (resp., $(X,*)\in\mathbb{E}(X,*)$ or $(X,*)\in(X,*)\mathbb{E}(X,*)$), then $(X,*)\square(X,*)=(X,*)$, and so $(X,*)$ is an idempotent element in $Bin(X)$,

(x) If $Bin(X)$ is commutative, then $(X,*)\mathbb{E}=\mathbb{E}(X,*)=(X,*)\mathbb{E}(X,*)$,

(c) If $(X,*)\mathbb{E}\neq\emptyset$, then it is a closed subset. Let $(X,\bullet)$ and $(X,\diamond)$ be elements in $(X,*)\mathbb{E}$, we get $(X,*)\square(X,\bullet)=(X,\bullet)$ and $(X,*)\square(X,\diamond)=(X,\diamond)$. Hence

$$(X,*)\square((X,\bullet)\square(X,\diamond))=((X,*)\square(X,\bullet))\square(X,\diamond)=(X,\bullet)\square(X,\diamond).$$

Thus, $(X,\bullet)\square(X,\diamond)\in(X,*)\mathbb{E}$, and so $(X,*)\mathbb{E}$ is a subsemigroup of $Bin(X)$.

If $\mathbb{E}(X,*)\neq\emptyset$, then it is a closed subset. Let $(X,\bullet)$ and $(X,\diamond)$ be elements in $\mathbb{E}(X,*)$. So $(X,\bullet)\square(X,*)=(X,\bullet)$ and $(X,\diamond)\square(X,*)=(X,\diamond)$. Hence

$$((X,\bullet)\square(X,\diamond))\square(X,*)=(X,\bullet)\square((X,\diamond)\square(X,*))=(X,\bullet)\square(X,\diamond).$$

Thus, $(X,\bullet)\square(X,\diamond)\in\mathbb{E}(X,*)$, and so $\mathbb{E}(X,*)$ is a subsemigroup of $Bin(X)$.

Similarly, $(X,*)\mathbb{E}(X,*)$ is a closed set.

(d) If $Bin(X)$ is a monoid or group and $(X,\star)$ is a unique right (left) zero semigroup, then $(X,\star)Bin(X)=Bin(X)(X,\star)=(X,\star)Bin(X)(X,\star)=Bin(X)$, and so the cancellation law is valid.

(e) Let $\mathbb{E}$ be the set of all right zero semigroups. Then $(X,*)Bin(X)=Bin(X)$ for all $(X,*)\in\mathbb{E}$, and so the left cancellation law is valid in $\mathbb{E}$.

(f) Let $\mathbb{E}$ be the set of all left zero semigroups. Then $Bin(X)(X,*)=Bin(X)$ for all $(X,*)\in\mathbb{E}$, and so the right cancellation law is valid in $\mathbb{E}$.

(g) If for all $(X,*) \in \mathbb{E}$ the set $(X,*)\mathbb{E}(X,*) = \{(X,\bullet)\}$ for some $(X,\bullet) \in Bin(X)$ (i.e., $(X,*)\mathbb{E}(X,*)$ is a singleton set), then $\mathbb{E}$ is a group in semigroup $Bin(X)$.

(h) If there exists $(X,*) \in Bin(X)$ such that $(X,*)\mathbb{E} \cap \mathbb{E}(X,*) = \emptyset$, then $\mathbb{E}$ is not a group.

(i) If there exists $(X,*) \in Bin(X)$ such that $((X,*)\mathbb{E})' = \mathbb{E}(X,*)$, then $Bin(X) = (X,*)\mathbb{E} \cup \mathbb{E}(X,*)$ and $\mathbb{E}$ is not a group.

(j) If $(X,*) \in Bin(X)$ is an idempotent element (i.e., $(X,*)\Box(X,*) = (X,*)$), then $(X,*) \in (X,*)Bin(X)(X,*)$.

(k) Let $(X,*) \in Bin(X)$. If there exists $\emptyset \neq \mathbb{E} \subseteq Bin(X)$, where $(X,*) \in (X,*)\mathbb{E} \cup \mathbb{E}(X,*)$, then $(X,*)$ is an idempotent element.

Theorem 3.12. *Let $\emptyset \neq \mathbb{E} \subseteq Bin(X)$. Then*

(*a*) *if $\mathbb{F} = \bigcap_{(X,*)\in Bin(X)} \mathbb{E}(X,*) \neq \emptyset$, then $\mathbb{F}$ is a right independence subset of $Bin(X)$,*

(*b*) *if $\mathbb{F} = \bigcap_{(X,*)\in Bin(X)} \mathbb{E} \neq \emptyset$, then $\mathbb{F}$ is a left independence subset of $Bin(X)$,*

(*c*) *if $\mathbb{F} = \bigcap_{(X,*)\in Bin(X)} (X,*)\mathbb{E}(X,*) \neq \emptyset$, then $\mathbb{F}$ is an independence subset of $Bin(X)$.*

Proof. (a). Assume $\emptyset \neq \mathbb{E} \subseteq Bin(X)$, $\mathbb{F} = \bigcap_{(X,*)\in Bin(X)} \mathbb{E}(X,*)$ and $(X,\bullet) \neq (X,\circ) \in \mathbb{F}$. Hence $(X,\bullet) \in \bigcap_{(X,*)\in Bin(X)} \mathbb{E}(X,*)$, and so we get $(X,\bullet)\Box(X,*) = (X,\bullet)$.

On the other hand, from $(X,\circ) \in \bigcap_{(X,*)\in Bin(X)} \mathbb{E}(X,*)$, we have $(X,\circ)\Box(X,*) = (X,\circ)$. Thus, $(X,\bullet)\Box(X,*) = (X,\bullet) \neq (X,\circ) = (X,\circ)\Box(X,*)$. Therefore, $\mathbb{F}$ is a right independence subset of $Bin(X)$.

(b). Assume $\emptyset \neq \mathbb{E} \subseteq Bin(X)$, $\mathbb{F} = \bigcap_{(X,*)\in Bin(X)} (X,*)\mathbb{E}$ and $(X,\bullet) \neq (X,\circ) \in \mathbb{F}$. Hence $(X,\bullet) \in \bigcap_{(X,*)\in Bin(X)} (X,*)\mathbb{E}$, and so we get $(X,*)\Box(X,\bullet) = (X,\bullet)$.

On the other hand, from $(X,\circ) \in \bigcap_{(X,*)\in Bin(X)} (X,*)\mathbb{E}$, we have $(X,*)\Box(X,\circ) = (X,\circ)$. Thus, $(X,*)\Box(X,\bullet) = (X,\bullet) \neq (X,\circ) = (X,*)\Box(X,\circ)$. Therefore, $\mathbb{F}$ is a left independence subset of $Bin(X)$.

(c). It follows immediately from (a) and (b). $\Box$

Suppose that $\mathbb{A}$ and $\mathbb{B}$ are two arbitrary subsets of $Bin(X)$. Define $\mathbb{A}\Box\mathbb{B}$ as follows:

$$\begin{aligned}\mathbb{A}\Box\mathbb{B} &= \{(X,*)\Box(X,\circ) : (X,*) \in \mathbb{A} \text{ and } (X,\circ) \in \mathbb{A}\}\\ &= \bigcup_{(X,*)\in\mathbb{A}} ((X,*)\Box\mathbb{B}) = \bigcup_{(X,\circ)\in\mathbb{B}} (\mathbb{A}\Box(X,\circ)).\end{aligned}$$

Note that $\emptyset\Box\mathbb{A} = \mathbb{A}\Box\emptyset = \emptyset\Box\emptyset = \emptyset$, $Bin(X)\Box Bin(X) = Bin(X)$, $\mathbb{A}\Box\mathbb{A} \neq \mathbb{A}$ and $\mathbb{A}\Box\mathbb{B} \neq \mathbb{B}\Box\mathbb{A}$.

Also, let $\mathbb{A}$, $\mathbb{B}$, and $\mathbb{C}$ be subsets of $Bin(X)$. Then one can see that:

- if $\mathbb{A} \subseteq \mathbb{B}$, then $\mathbb{A}\Box\mathbb{C} \subseteq \mathbb{B}\Box\mathbb{C}$ and $C\Box\mathbb{A} \subseteq \mathbb{C}\Box\mathbb{B}$,
- $(\mathbb{A}\cap\mathbb{B})\Box\mathbb{C} \subseteq (\mathbb{A}\Box\mathbb{C}) \cap (\mathbb{B}\Box\mathbb{C})$,
- $\mathbb{C}\Box(\mathbb{A}\cap\mathbb{B}) \subseteq (\mathbb{C}\Box\mathbb{A}) \cap (\mathbb{C}\Box\mathbb{B})$,
- $(\mathbb{A}\cup\mathbb{B})\Box\mathbb{C} = (\mathbb{A}\Box\mathbb{C}) \cup (\mathbb{B}\Box\mathbb{C})$,
- $\mathbb{C}\Box(\mathbb{A}\cup\mathbb{B}) = (\mathbb{C}\Box\mathbb{A}) \cup (\mathbb{C}\Box\mathbb{B})$.

Corollary 3.13.
(a) *If $Bin(X)$ is a right (left) zero semigroup and either $\mathbb{A}$ or $\mathbb{B}$ is a right (left) independence subset of $Bin(X)$, then $\mathbb{A}\Box\mathbb{B}$ is also a right (left) independence subset of $Bin(X)$.*
(b) *If $|\mathbb{A}| = 1$ or $|\mathbb{B}| = 1$, then $\mathbb{A}\Box\mathbb{B}$ is a right (left) independence subset of $Bin(X)$.*
(c) *If $Bin(X)$ is a right (left) cancellative semigroup, then $\mathbb{A}\Box\mathbb{B}$ is an independence subset of $Bin(X)$.*

Consider Example 2.1, and put $\mathbb{A} := \{(X,*_1),(X,*_2)\}$. Then $Bin(X)\,\Box\mathbb{A} \neq \mathbb{A}$, since $(X,*_3)\Box(X,*_2) = (X,*_{10}) \notin \mathbb{A}$. Also, $\mathbb{A}\Box Bin(X) \neq \mathbb{A}$, since $(X,*_2)\Box(X,*_5) = (X,*_5) \notin \mathbb{A}$. If take $\mathbb{B} := \{(X,*_{16})\}$, then $Bin(X)\Box\mathbb{B} = \mathbb{B} \neq Bin(X)$. Also, $\mathbb{B}\Box Bin(X) = \{(X,*_1),(X,*_{16})\} \neq \{(X,*_{16})\}$ and $\mathbb{B}\Box Bin(X) \neq Bin(X)\Box\mathbb{B}$.

Now, we can rewrote the definitions of right (left) zero semigruops as the follows:
A semigroup $(Bin(X),\Box)$ is said to be a *right zero semigroup* if

$$Bin(X)\Box(X,*) = \{(X,*)\}$$

and a groupoid $(Bin(X),\Box)$ is said to be a *left zero semigroup* if

$$(X,*)\Box Bin(X) = \{(X,*)\}$$

for any $(X,*) \in Bin(X)$.

4. right (left) absorbent in $Bin(X)$

Definition 4.1. A non-empty subset $\mathbb{A}$ of $Bin(X)$ is said to be *right absorbent* (resp., *left absorbent*) if $Bin(X)\Box\mathbb{A} = \mathbb{A}$ (resp., $\mathbb{A}\Box Bin(X) = \mathbb{A}$). It is *absorbent* if it is both right and left absorbent (i.e., $Bin(X)\Box\mathbb{A} = \mathbb{A}\Box Bin(X) = \mathbb{A}$).

Example 4.5. Consider Example 2.1.
(a) If $\mathbb{C} := \{(X, *_1)\}$, then $Bin(X)\Box\mathbb{C} = \mathbb{C}$, and so $\mathbb{C}$ is a right absorbent of $Bin(X)$, but not a left absorbent, since

$$\mathbb{C}\Box Bin(X) = \{(X, *_1), (X, *_{16})\} \neq \mathbb{C} \neq Bin(X).$$

(b) If $\mathbb{B} := \{(X, *_3\}$, then $\mathbb{B}\Box Bin(X) = \mathbb{B}$, and so $\mathbb{B}$ is a left absorbent of $Bin(X)$, but not a right absorbent, since

$$(X, *_7) = (X, *_6)\Box(X, *_3) \in Bin(X)\Box\mathbb{B}, \text{ but } (X, *_7) \notin \{(X, *_3)\}.$$

(c) If $\mathbb{D} := \{(X, *_1), (X, *_{16})\}$, then $Bin(X)\Box\mathbb{D} = \mathbb{D}$ and $\mathbb{D}\Box Bin(X) = \mathbb{D}$. Thus, $\mathbb{D}$ is an absorbent subset of $Bin(X)$.

Proposition 4.2. *If $Bin(X)$ is a right (left) zero semigroup, then every subset of $Bin(X)$ is a right (left) absorbent subset of $Bin(X)$.*

Proof. Straightforward. □

The converse of Proposition 4.2, may not be true in general. For this, consider Example 2.1, and take $\mathbb{A} := \{(X, *_1)\}$, so $\mathbb{A}$ is a right absorbent subset, but $Bin(X)$ is neither a right zero semigroup nor a left zero semigroup, since $(X, *_2)\Box(X, *_{14}) = (X, *_{16}) \notin \{(X, *_2), (X, *_{14})\}$.

Proposition 4.3. *Let $\mathbb{A}$ be a right (left) absorbent subset of $Bin(X)$. Then $\mathbb{A}$ is closed under $\Box$ (i.e., $\mathbb{A}$ is a subsemigroup of $Bin(X)$).*

Proof. Assume $\mathbb{A}$ is a right absorbent subset of $Bin(X)$ and $(X, *)$, $(X, \circ) \in \mathbb{A}$. Then $(X, *)\Box(X, \circ) \in \mathbb{A}\Box\mathbb{A} \subseteq Bin(X)\Box\mathbb{A} = \mathbb{A}$. Thus, $(X, *)\Box(X, \circ) \in \mathbb{A}$. Now, suppose that $\mathbb{A}$ is a left absorbent subset of $Bin(X)$, and let $(X, *), (X, \circ) \in \mathbb{A}$. Then $(X, *)\Box(X, \circ) \in \mathbb{A}\Box\mathbb{A} \subseteq \mathbb{A}\ \Box Bin(X) = \mathbb{A}$. Thus, $(X, *)\Box(X, \circ) \in \mathbb{A}$. □

Proposition 4.4. *Let $\mathbb{A}_1$ and $\mathbb{A}_2$ be two right (left) absorbent subsets of $Bin(X)$. Then $\mathbb{A}_1 \cup \mathbb{A}_2$ is also a right (left) absorbent subset of $Bin(X)$.*

Proof. Assume $\mathbb{A}_1$ and $\mathbb{A}_2$ are two right absorbent subsets of $Bin(X)$. Then $Bin(X)\Box\mathbb{A} = \mathbb{A}$ and $Bin(X)\Box\mathbb{B} = \mathbb{B}$. It follows that

$$Bin(X)\Box(\mathbb{A} \cup \mathbb{B}) = (Bin(X)\Box\mathbb{A}) \cup (Bin(X)\Box\mathbb{B}) = \mathbb{A} \cup \mathbb{B}.$$

Similarly, the assertion holds for the left absorbent subsets. □

Corollary 4.5. *Let $\{\mathbb{A}_i\}_{i\in\Lambda}$ be a family of right (left) absorbent subsets of $Bin(X)$. Then $\bigcup_{i\in\Lambda} \mathbb{A}_i$ is a right (left) absorbent subset of $Bin(X)$.*

Let $\mathbb{A} \subseteq Bin(X)$. Define $\mathbb{A}_{(X,*)}$ and ${}_{(X,*)}\mathbb{A}$ as follows:

$$\mathbb{A}_{(X,*)} = \{(X,\bullet) \in Bin(X) : (X,*)\Box(X,\bullet) \in \mathbb{A}\},$$

$${}_{(X,*)}\mathbb{A} = \{(X,\bullet) \in Bin(X) : (X,\bullet)\Box(X,*) \in \mathbb{A}\}.$$

Also, we can define:

$${}_{(X,*)}\mathbb{A}_{(X,*)} = \{(X,\bullet) \in Bin(X) : (X,\bullet)\Box(X,*) \text{ and } (X,*)\Box(X,\bullet) \in \mathbb{A}\}.$$

Proposition 4.6. *Let $\mathbb{A}$ be a right independence subset of a left cancellative semigroup $Bin(X)$. If $\mathbb{A}_{(X,*)} \neq \emptyset$ for some $(X,*) \in Bin(X)$, then $\mathbb{A}_{(X,*)}$ is a right independence subset of $Bin(X)$.*

Proof. Assume $\mathbb{A}$ is a right independence subset of the left cancellative semigroup $Bin(X)$. If $(X,\bullet_1) \neq (X,\bullet_2)$ in $\mathbb{A}_{(X,*)}$, then $(X,*)\Box(X,\bullet_1) \in \mathbb{A}$ and $(X,*)\Box(X,\bullet_2) \in \mathbb{A}$. We claim $(X,*)\Box(X,\bullet_1) \neq (X,*)\Box(X,\bullet_2)$. If we assume $(X,*)\Box(X,\bullet_1) = (X,*)\Box(X,\bullet_2)$, since $Bin(X)$ is left cancellative, we obtain $(X,\bullet_1) = (X,\bullet_2)$, a contradiction. Now, since $\mathbb{A}$ is right independence, we have $[(X,*)\Box(X,\bullet_1)]\Box(X,\diamond) \neq [(X,*)\ \Box(X,\bullet_2)]\Box(X,\diamond)$ for all $(X,\diamond) \in Bin(X)$. Since $Bin(X)$ is left cancellative, by the associativity, we obtain $(X,*)\Box[(X,\bullet_1)\Box(X,\diamond)] \neq (X,*)\Box[(X,\bullet_2)\Box(X,\diamond)]$, and so $(X,\bullet_1)\Box(X,\diamond) \neq (X,\bullet_2)\Box(X,\diamond)$ for all $(X,\diamond) \in Bin(X)$. Thus, $\mathbb{A}_{(X,*)}$ is a right independence subset of $Bin(X)$. □

Proposition 4.7. *Let $\mathbb{A}$ be a left independence subset of a right cancellative semigroup $Bin(X)$. Then ${}_{(X,*)}\mathbb{A}$ is a left independence subset of $Bin(X)$ for any $(X,*) \in Bin(X)$.*

Proof. Assume $\mathbb{A}$ is a left independence subset of the right cancellative semigroup $Bin(X)$. Let $(X,\bullet_1) \neq (X,\bullet_2)$ in $\mathbb{A}$. Then $(X,\bullet_1)\Box(X,*) \in \mathbb{A}$ and $(X,\bullet_2)\Box(X,*) \in \mathbb{A}$. Since $Bin(X)$ is right cancellative, we obtain $(X,\bullet_1)\Box(X,*) \neq (X,\bullet_2)\Box(X,*)$. Now, since $\mathbb{A}$ is a left independence subset of $Bin(X)$, we obtain $(X,\diamond)\Box[(X,\bullet_1)\Box(X,*)] \neq (X,\diamond)\Box[(X,\bullet_2)\Box(X,*)]$ for all $(X,\diamond) \in Bin(X)$. Since $Bin(X)$ is a right cancellative semigroup, by using the associative laws, we obtain $[(X,\diamond)\Box(X,\bullet_1)]\Box(X,*) \neq [(X,\diamond)\Box(X,\bullet_2)]\Box(X,*)$, and hence $(X,\diamond)\Box(X,\bullet_1) \neq (X,\diamond)\Box(X,\bullet_2)$ for all $(X,\diamond) \in Bin(X)$. Thus, ${}_{(X,*)}\mathbb{A}$ is a left independence subset of $Bin(X)$. □

Corollary 4.8. *Let $\mathbb{A}$ be an independence subset of a cancellative semigroup $Bin(X)$. Then ${}_{(X,*)}\mathbb{A}_{(X,*)}$ is an independence subset of $Bin(X)$ for any $(X,*) \in Bin(X)$.*

Proof. It follows immediately from Propositions 4.6 and 4.7. □

Theorem 4.9. *Let $\mathbb{A}$ be a right (left) absorbent subset of $Bin(X)$, and let $(X,*) \in \mathbb{A}$. Then $Bin(X) = \mathbb{A}_{(X,*)}$ (resp., $Bin(X) =_{(X,*)} \mathbb{A}$).*

Proof. Assume $\mathbb{A}$ is a right absorbent subset of $Bin(X)$ and $(X,*) \in \mathbb{A}$. Then $(X,*)\Box(X,\bullet) \in \mathbb{A}\Box Bin(X) = \mathbb{A}$ for all $(X,\bullet) \in Bin(X)$. Thus, $(X,\bullet) \in \mathbb{A}_{(X,*)}$, and so $Bin(X) \subseteq \mathbb{A}_{(X,*)}$. Thus, $Bin(X) = \mathbb{A}_{(X,*)}$.

Assume $\mathbb{A}$ is a left absorbent subset of $Bin(X)$ and $(X,*) \in \mathbb{A}$. Hence $(X,\bullet)\Box(X,*) \in Bin(X)\Box\mathbb{A} = \mathbb{A}$ for all $(X,\bullet) \in Bin(X)$. Thus, $(X,\bullet) \in {}_{(X,*)}\,\mathbb{A}$, and so $Bin(X) \subseteq \mathbb{A}_{(X,*)}$. Thus, $Bin(X) = {}_{(X,*)}\,\mathbb{A}$. □

Corollary 4.10. *Let $\mathbb{A}$ be an absorbent subset of $Bin(X)$. Then for $(X,*) \in \mathbb{A}$ we have $Bin(X) =_{(X,*)} \mathbb{A} = \mathbb{A}_{(X,*)}$.*

Theorem 4.11. *Let $\{A_i\}_{i\in\Lambda}$ be a family of disjoint right (left) absorbent subsets, $Bin(X) = \bigcup\limits_{i\in\Lambda} A_i$ and $|A_i| = 1$ for $i \in \Lambda$. Then the following hold:*

(a) *$Bin(X)$ is not a commutative semigroup,*

(b) *$Bin(X)$ is an independence.*

Proof. (a). Assume $\{\mathbb{A}_i\}_{i\in\Lambda}$ be a partition of right (resp., left) absorbent subsets of $Bin(X)$. Then $Bin(X) = \bigcup\limits_{i\in\Lambda} \mathbb{A}_i$. Let $(X,*) \neq (X,\bullet) \in Bin(X)$. Then there exist $i \neq j \in \Lambda$ such that $(X,*) \in \mathbb{A}_i$ and $(X,\bullet) \in \mathbb{A}_j$. It follows that $(X,*)\Box(X,\bullet) \in Bin(X)\Box\mathbb{A}_j = \mathbb{A}_j$ (resp., $(X,*)\Box(X,\bullet) \in \mathbb{A}_i\Box Bin(X) = \mathbb{A}_i$), since $\mathbb{A}_j$ is a right (resp., $\mathbb{A}_i$ is a left) absorbent subset of $Bin(X)$. On the other hand, since $\mathbb{A}_i$ is a right (resp., $\mathbb{A}_j$ is a left) absorbent subset of $Bin(X)$, $(X,\bullet)\Box(X,*) \in Bin(X)\Box\mathbb{A}_i = \mathbb{A}_i$ (resp., $(X,\bullet)\Box(X,*) \in \mathbb{A}_j\Box Bin(X) = \mathbb{A}_j$), Since $\mathbb{A}_i \cap \mathbb{A}_j = \emptyset$, we get $(X,*)\Box(X,\bullet) \neq (X,\bullet)\Box(X,*)$. This proves ($a$).

(b). Assume $(X,*) \neq (X,\bullet) \in Bin(X)$. Hence there are $i \neq j \in \Lambda$ such that $(X,*) \in \mathbb{A}_i$ and $(X,\bullet) \in \mathbb{A}_j$. Then for all $(X,\diamond) \in Bin(X)$, since $\mathbb{A}_i$ and $\mathbb{A}_j$ are right absorbent subsets of $Bin(X)$, we get $(X,\diamond)\Box(X,*) \in Bin(X)\Box\mathbb{A}_i = \mathbb{A}_i$ and $(X,\diamond)\Box(X,\bullet) \in Bin(X)\Box\mathbb{A}_j = \mathbb{A}_j$. Since $\mathbb{A}_i \cap \mathbb{A}_j = \emptyset$, we get $(X,\diamond)\Box(X,*) \neq (X,\diamond)\Box(X,\bullet)$, and so $Bin(X)$ is a left independence.

Also, since $\mathbb{A}_i$ and $\mathbb{A}_j$ are left absorbent subsets of $Bin(X)$, $(X,*)\Box(X,\diamond) \in \mathbb{A}_i\Box Bin(X) = \mathbb{A}_i$ and $(X,\bullet)\Box(X,\diamond) \in \mathbb{A}_j\Box Bin(X) = \mathbb{A}_j$. Since $\mathbb{A}_i \cap \mathbb{A}_j = \emptyset$, we get $(X,*)\Box(X,\diamond) \neq (X,\bullet)\Box(X,\diamond)$, and so $Bin(X)$ is a right independence. □

5. Open problem

There is a partition $\{\mathbb{A}_i\}_{i\in\Lambda}$ of right (left) independence subsets of $Bin(X)$ (i.e., $Bin(X) = \bigcup\limits_{i\in\Lambda} \mathbb{A}_i$, $|\mathbb{A}_i| = 1$ and $\mathbb{A}_i \bigcap \mathbb{A}_j = \emptyset$ for $i,j \in \Lambda$).

Is there another partition of $Bin(X)$, where there is at least $i \in \Lambda$ such that $|\mathbb{A}_i| > 1$?

References

[1] **P.J. Allen, H.S. Kim and J. Neggers**, *Several types of groupoids induced by two-variables functions*, Springer Plus **5** (2016), 1715–1725.

[2] **R.H. Bruck**, *A survey of binary systems*, Springer: New York, 1971.

[3] **O. Borůvka**, *Foundations of the theory of groupoids and groups*, John Wiley & Sons: New York, NY, USA, 1976.

[4] **H.F. Fayoumi**, *Locally-Zero groupoids and the center of $Bin(X)$*, Commun. Korean Math. Soc. **26** (2011), 163–168, no. 2.

[5] **H.F. Fayoumi**, *Groupoid factorizations in the semigroup of binary systems*, arXiv:2010.09229

[6] **F. Feng, H.S. Kim and J. Neggers**, *General implicativity in groupoids*, Mathematics **6** (2018), 235.

[7] **Y.H. Kim, H.S. Kim and J. Neggers**, *Selective groupoids and frameworks induced by fuzzy subsets*, Iran. J. Fuzzy Syst. **14** (2017), 151–160.

[8] **I.H. Hwang, H.S. Kim and J. Neggers**, *Some implicativies for groupoids and BCK-algebras*, Mathematics **7** (2019), 973–980.

[9] **I.H. Hwang, H.S. Kim and J. Neggers**, *Locally finiteness and convolution products in groupoids*, AIMS Mathematics **5** (2020), 7350–358, no. 6.

[10] **H.S. Kim and J. Neggers**, *The semigroups of binary systems and some perspectives*, Bull. Korean Math. Soc. **45** (2008), 651–661.

[11] **Y.L. Liu, H.S. Kim and J. Neggers**, *Hyper fuzzy subsets and subgroupoids*, J. Intell. Fuzzy Syst. **33** (2017), 1553–1562.

[12] **L. Nebeský**, *Travel groupoids*, Czech. Math. J. **56** (2006), 659–675.

[13] **A. Rezaei, J. Neggers and H.S. Kim**, *Independence concepts for groupoids*, submitted.

Received March 08, 2021

A. Rezaei
Department of Mathematics, Payame Noor University, P. O. Box 19395-3697, Tehran, Iran
e-mail: rezaei@pnu.ac.ir

H.S. Kim
Research Institute for Natural Sci., Department of Mathematics, Hanyang University, Seoul, 04763, Korea
e-mail: heekim@hanyang.ac.kr

J. Neggers
Department of Mathematics, University of Alabama, Tuscaloosa, AL 35487-0350, U.S.A
e-mail: jneggers@ua.edu

Quasigroups and Related Systems **29** (2021), 283 − 302

Four halves of the inverse property in loop extensions

Uzi Vishne

Abstract. Any two of the left, right, weak and antiautomorphic inverse properties of a loop imply the full inverse property. Considering these properties in the context of nuclear loop extensions $1 \to K \to L \to Q \to 1$, we discover an action of the infinite dihedral group on $\mathrm{C}^2(Q, K)$ whose subspaces fixed under odd subgroups precisely correspond to these classical loop properties.

When in doubt, look for the group!
(André Weil)

1. Introduction

A set equipped with a (nonassociative) binary operation is called a *loop* if it has a unit element, and left and right multiplications are invertible. Thus every element has a unique left inverse and a unique right inverse. A loop has the *inverse property* if the left and right inverses coincide, and the identities $x^{-1}(xy) = (yx)x^{-1} = y$ hold. Any group has the inverse property, but there are plenty of other examples (see [4]). This paper is concerned with a cohomological structure governing various generalizations of the inverse property.

Let L be a loop. The actions on L by left and right multiplication by $x \in L$ are denoted ℓ_x and r_x, respectively. The left and right inverses of x are denoted x^λ and x^ρ, respectively. The maps $\lambda, \rho : L \to L$ satisfy $\lambda\rho = \rho\lambda = \mathrm{id}$. We consider the following properties of loops, all studied by multiple authors before.

(LI) $x^\lambda(xy) = y$ (the *left inverse property*).

(RI) $(yx)x^\rho = y$ (the *right inverse property*).

(WI) $(xy)z = 1$ precisely when $x(yz) = 1$ (the *weak inverse property*).

(AI) $(xy)^\lambda = y^\lambda x^\lambda$, equivalently $(xy)^\rho = y^\rho x^\rho$ (the *antiautomorphic inverse property*).

2020 Mathematics Subject Classification: 20N05
Keywords: Inverse property, weak inverse, antiautomorphic inverse loops, loop extensions.
Partially supported by an Israeli Science Foundation, grant number 1623/16.

(IP) both left and right inverse properties (the *inverse property*).

(Inv) All elements are invertible ($\lambda = \rho$).

(H) The map λ^2 (equivalently ρ^2) is a loop homomorphism.

The logical dependencies are given in Figure 1 (up-side down, anticipating the refinement given in Figure , see Section). We call (LI), (RI), (WI) and (AI) the "*four halves*" of the inverse property, because, as we show below, any two of these conditions imply the inverse property (IP) and thus all the others.

We study these properties for loops arising as nuclear extensions of a group Q by an abelian group K. Let $\mathrm{C}^2(Q,K) = \{c\colon Q \times Q \to K\}$ be the function space parameterizing the extensions via the classical factor set construction. We say that a subspace $X \subseteq \mathrm{C}^2(Q,K)$ "is" the loop property P if the extension (K,Q,c) has P precisely when $c \in X$. The purpose of this paper is to exhibit an action of the infinite dihedral group, which was discovered by Artzy [5, Prop. 3.2], in the cohomological context. Let D_∞ denote the infinite dihedral group, and C_∞ its cyclic subgroup of index 2. We say that a subgroup is *even* if it is contained in C_∞, and *odd* otherwise.

Theorem 1.1. *There is an action of D_∞ on the space $\mathrm{C}^2(Q,K)$, such that the subspaces fixed under subgroups of D_∞ are:*

- (LI), (RI), (AI) *and* (IP) (*for odd subgroups*) *and*
- (W_{2n+1}) *and* (H^n) (*for even subgroups*).

A loop has the property (H^n) if λ^{2n} is a homomorphism; thus (H^1) = (H). The m-inverse properties (W_m), defined in Section , are variations on the weak inverse property, which is (WI) = (W_{-1}).

The action of D_∞ in the theorem preserves the coboundaries $\mathrm{B}^2(Q,K)$ elementwise, and is in particular well-defined on the quotient space $\mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K)$ which classifies extensions up to equivalence.

As we see below, any two of the four halves define the group action, and in this sense could have defined the other properties. Notice that there are infinitely many odd subgroups, a-priori each with its own fixed subspace. The fact that our action has finitely many fixed subspaces under odd subgroups indicates a strong connection between the four halves and places (W_{2n+1}) and (H^n) as their conceptual derivatives.

Section provides a brief sketch of the properties of loops we encounter in this paper. The proofs follow standard arguments, and are given here for completeness. In Section we define loop extensions arising from an action of a group Q on an abelian group K, and characterize the four properties (LI), (RI), (WI) and (AI) of the extension (K,Q,c) in terms of conditions on the factor set $c \in \mathrm{C}^2(Q,K)$. Further details are given in Section , where we find similar characterization for (Inv) and (H).

$$\begin{tikzcd}
 & \text{(H)} & & \\
 & \text{(Inv)} \arrow[u] & & \\
\text{(AI)} \arrow[ur] & \text{(LI)} \arrow[u] & \text{(RI)} \arrow[ul] & \text{(WI)} \arrow[uull] \\
 & \text{(IP)} \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

Figure 1: Logical dependencies of loop properties

In Section we introduce the action of the infinite dihedral group D_∞ on $\mathrm{C}^2(Q, K)$; the action preserves equivalence classes of extensions. Proposition 6.1 ties the loop properties with the dihedral action, and Theorem 7.1 proves the odd part of Theorem 1.1. Section studies the m-inverse properties, denoted here (W_m), which include the k-fold weak inverse properties $(\mathrm{W}^k\mathrm{IP})$. Theorem 8.8 covers the even part of Theorem 1.1. Finally, in Section we specialize to the case $Q = \mathbb{Z}_4$ and provide some examples and counterexamples.

We thank the referee for helpful remarks on an earlier version of this paper, which in particular led to the current Section .

2. Four halves of the inverse property

In this section we provide equivalent formulations for each of the four halves of (IP), and prove:

Proposition 2.1. *Any two of the properties* (LI), (RI), (WI) *and* (AI) *imply the* (*full*) *inverse property.*

Counterexamples, showing that none of the four halves implies (IP) on its own, are given in Corollary 9.3.

2.1. The left and right inverse properties

Let L be a loop. If the inverse of ℓ_x has the form ℓ_y for some y, then necessarily $\ell_x^{-1} = \ell_{x^\lambda}$. Indeed, if $xy = \ell_x \ell_y(1) = 1$ then $y = x^\lambda$. Likewise if the inverse of r_x has the form r_y, then $r_x^{-1} = r_{x^\rho}$.

Proposition 2.2.

a The left inverse property is equivalent to $\ell_x^{-1} = \ell_{x^\lambda}$ *for every* x.

b. The right inverse property is equivalent to $r_x^{-1} = r_{x^\rho}$ *for every* x.

c. Each of the properties (LI) *and* (RI) *implies* (Inv).

Proof. The identity $x^\lambda(xy) = y$ is equivalent to $\ell_{x^\lambda}\ell_x = \mathrm{id}$ so $\ell_x^{-1} = \ell_{x^\lambda}$. Now suppose $\ell_{x^\lambda} = \ell_x^{-1}$ for all x. Then $\ell_{x^{\lambda^2}} = \ell_{x^\lambda}^{-1} = \ell_x$, implying $x^{\lambda^2} = x$, and so $\lambda^2 = \mathrm{id}$. But then $\rho = \lambda^{-1} = \lambda$, so all elements are invertible. The proof for right inverse is similar. □

The left (resp. right) inverse property holds for all isotopes of a loop L, if and only if L satisfies the left (resp. right) Bol axiom $\ell_x\ell_y\ell_x = \ell_{x(yx)}$ (resp. $r_xr_yr_x = r_{(xy)x}$), [12, Thm 3.1].

2.2. The antiautomorphic inverse property

Proposition 2.3. *The following properties of a loop are equivalent.*

- (a) $(xy)^\lambda = y^\lambda x^\lambda$ (*namely antiautomorphic inverse*).
- (a') $(xy)^\rho = y^\rho x^\rho$.
- (b) $r_y = \rho\ell_{y^\lambda}\lambda$.
- (b') $r_y = \lambda\ell_{y^\rho}\rho$.
- (c) $r_{x^\lambda} = \lambda\ell_x\rho$.
- (c') $r_{x^\rho} = \rho\ell_x\lambda$.

Proof. Condition (a) is equivalent to (b) by the action on x, and to (c) by the action on y. Condition (a') is equivalent to (b') by the action on x, and to (c') by the action on y. Taking $x = y^\lambda$ in (c') we get (b). □

Proposition 2.4. *(IP) $\Longrightarrow$ (AI) $\Longrightarrow$ (Inv).*

Proof. Assuming (IP) we have $(xy)^{-1} = ((xy)^{-1}x)x^{-1} = ((xy)^{-1}(xy\cdot y^{-1}))x^{-1} = y^{-1}x^{-1}$. Assuming (AI), we have $xx^\lambda = (x^\rho)^\lambda x^\lambda = (xx^\rho)^\lambda = 1^\lambda = 1$, so $x^\lambda = x^\rho$. □

For example, every automorphic loop (=all inner maps are automorphisms) has the antiautomorphic inverse property [8, Cor. 6.6]. Artzy proved that an (IP) loop all of whose isotopes satisfy (AI) is a Moufang loop [2] (see also [1]).

2.3. The weak inverse property

Weak inverse loops are of interest mostly due to Osborn's theorem that their one-sided nuclei coincide [11].

Proposition 2.5. *The following properties of a loop are equivalent.*

- $(a)'$ $x(yz) = 1$ *if and only if* $(xy)z = 1$ *(namely weak inverse).*
- $(b)'$ *if* $x(yz) = 1$ *then* $(xy)z = 1$.

(b') *if* $(xy)z = 1$ *then* $x(yz) = 1$.

(c)$'$ $(yz)^\lambda y = z^\lambda$.

(c') $y(xy)^\rho = x^\rho$.

(d)$'$ $r_y = \lambda \ell_y^{-1} \rho$.

Proof. Condition $(b)'$ says that if $x = (yz)^\lambda$ then $xy = z^\lambda$, namely $(yz)^\lambda y = z^\lambda$, which is condition $(c)'$. Action on z interprets this condition as $r_y \lambda \ell_y = \lambda$, which is condition $(d)'$. Similarly (b') is equivalent to (c') and to $(d)'$; and $(a)' = (b)' + (b')$. □

Proposition 2.6. *The property* (AI)*, together with either* (LI) *or* (RI)*, implies* (WI)*.*

Proof. If $(xy)z = 1$ then $z = (xy)^{-1} = y^{-1}x^{-1}$ by (AI) and then $x(yz) = x(y(y^{-1}x^{-1})) = xx^{-1} = 1$ by (LI). Similarly if $x(yz) = 1$ then $x = (yz)^{-1} = z^{-1}y^{-1}$ by the (AI) and then $(xy)z = (z^{-1}y^{-1} \cdot y)z = z^{-1}z = 1$ by (RI). □

Osborn [11, p. 296] notes that (WI) $\Longrightarrow$ (H) (but (WI)$\not\Longrightarrow$(Inv), see Example 9.5).

2.4. Any two suffice

We move to prove Proposition 2.1.

Proof. The inverse property clearly implies both (LI), (RI), and by Proposition 2.4 it also implies (AI). By Proposition 2.6, (WI) follows as well.

1. Assume (LI) and (RI). The inverse property holds by Proposition 2.2.(c).

2. Assume (WI) and either (LI) or (RI). All elements are invertible. Now Proposition 2.5.$(d)'$ gives $r_y = \lambda \ell_y^{-1} \lambda^{-1}$, so taking y^{-1} for y we get $r_{y^{-1}} = \lambda \ell_{y^{-1}}^{-1} \lambda^{-1}$, implying that $r_y r_{y^{-1}} = \lambda(\ell_{y^{-1}} \ell_y)^{-1} \lambda^{-1}$, so the left inverse property $r_y r_{y^{-1}} = \mathrm{id}$ is equivalent to the right inverse property $\ell_{y^{-1}} \ell_y = \mathrm{id}$; but we assume one of them holds, so both do.

3. Assume (AI) and either (LI) or (RI). Then by Proposition 2.3.(b'), $r_y = \lambda \ell_{y^{-1}} \lambda^{-1}$, so taking y^{-1} for y we get $r_{y^{-1}} = \lambda \ell_y \lambda^{-1}$, implying once more $r_y r_{y^{-1}} = \lambda(\ell_{y^{-1}} \ell_y)^{-1} \lambda^{-1}$. The argument continues as in 2.

4. Finally if (WI) and (AI) hold, then $\lambda \ell_{y^\lambda} \rho = r_y = \lambda \ell_y^{-1} \rho$ by Propositions 2.3.(b') and 2.5.$(d)'$, implying $\ell_{y^\lambda} = \ell_y^{-1}$ which is the left inverse property, and we are done by 2. or 3.

□

3. Loop extensions

Let L' and L'' be loops. A loop L is an *extension* of L' by L'' if there is a short exact sequence of loop homomorphisms $1 \longrightarrow L'' \longrightarrow L \longrightarrow L' \longrightarrow 1$. This classical construction is systematically studied in the recent paper [9] (also see the references therein). The extension is *nuclear* if the image of L'' is contained in the nucleus of L. Our focus here is on loops obtained as nuclear extensions of a group by an abelian group.

Let Q be a group acting on an abelian group K. We denote the action by $q : k \mapsto k^q$, so that $k^{qq'} = (k^{q'})^q$. For a function $c : Q \times Q \to K$ satisfying $c_{1,q} = c_{q,1} = 1$ for all $q \in Q$, let (K, Q, c) denote the set $K \times Q = \{kq : k \in K, q \in Q\}$ with the binary operation

$$kq \cdot k'q' = kk'^q c_{q,q'}(qq').$$

We always have that K is a normal nuclear subgroup of the loop (K, Q, c). It is well known that (K, Q, c) is a group if and only if c satisfies the 2-cocycle condition

$$c_{q,q'} c_{qq',q''} = c^q_{q',q''} c_{q,q'q''}. \tag{1}$$

The semidirect extension $L = K \rtimes Q$ with respect to the given action corresponds to the trivial co-cycle $c = 1$.

We say that c, c' are *equivalent* (and write $c \approx c'$) if there are $a_q \in K$, $a_1 = 1$, such that $c'_{q,q'} = a_q a^q_{q'} a^{-1}_{qq'} c_{q,q'}$. There is an extension isomorphism $(K, Q, c) \to (K, Q, c')$, namely a loop isomorphism preserving K elements-wise and each of the cosets Kq, if and only if $c \approx c'$.

The "diagonal" entries $c_{q,q^{-1}}$ of the function $c : Q \times Q \to K$ play a special role in the computations to follow. We thus denote

$$\gamma_q = c_{q,q^{-1}}, \tag{2}$$

always understood as depending on c. Writing $k^{-q} = (k^{-1})^q = (k^q)^{-1}$, we have in (K, Q, c) that

$$(kq)^\lambda = k^{-q^{-1}} \gamma^{-1}_{q^{-1}} q^{-1}, \tag{3}$$

$$(kq)^\rho = k^{-q^{-1}} \gamma_q^{-q^{-1}} q^{-1}. \tag{4}$$

Proposition 3.1. *The loop (K, Q, c) satisfies the property:*

(LI) *if* $c_{p,q} c^p_{p^{-1},pq} = \gamma^p_{p^{-1}}$.

(RI) *if* $c_{p,q} c_{pq,q^{-1}} = \gamma^p_q$.

(WI) *if* $c_{p,q} c^{-p}_{q,(pq)^{-1}} = \gamma_p \gamma^{-1}_{pq}$.

(AI) *if* $c_{p,q} c^{pq}_{q^{-1},p^{-1}} = \gamma^p_{p^{-1}} \gamma^{pq}_{q^{-1}} \gamma^{-pq}_{(pq)^{-1}}$, *equivalently if* $c_{p,q} c^{pq}_{q^{-1},p^{-1}} = \gamma_p \gamma^p_q \gamma^{-1}_{pq}$.

Proof. Computation with the defining identities, based on Equations (3) and (4). For the antiautomorphic inverse property we used both (a) and (a') of Proposition 2.3 (so each of the conditions $c_{p,q}c^{pq}_{q^{-1},p^{-1}} = \gamma^{p}_{p^{-1}}\gamma^{pq}_{q^{-1}}\gamma^{-pq}_{(pq)^{-1}}$ and $c_{p,q}c^{pq}_{q^{-1},p^{-1}} = \gamma_p\gamma^p_q\gamma^{-1}_{pq}$ suffices). □

4. Detecting (Inv) and (H)

Recall that $\mathrm{C}^1(Q,K) = \{a : Q \to K\}$ and $\mathrm{C}^2(Q,K) = \{c : Q \times Q \to K\}$ are the spaces of unary and binary functions from Q to the abelian group K. The differential map $\delta^1 : \mathrm{C}^1(Q,K) \to \mathrm{C}^2(Q,K)$, defined by

$$(\delta^1 a)_{p,q} = a_p a^p_q a^{-1}_{pq},$$

gives rise to the groups of cocycles

$$\mathrm{Z}^1(Q,K) = \mathrm{Ker}(\delta^1)$$

and coboundaries

$$\mathrm{B}^2(Q,K) = \mathrm{Im}(\delta^1)$$

(see [3]). The loop extensions (K,Q,c), up to equivalence, are in correspondence with the quotient $\mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K)$. The properties listed in Proposition 3.1 are well-defined up to equivalence of c because they are preserved by loop isomorphism; alternatively by direct computation.

For any $k \in K$ and $q \in Q$, we have in (K,Q,c) that

$$(kq)(kq)^{\lambda} = (kq^{-1})^{\rho}(kq^{-1}) = \gamma^{-q}_{q^{-1}}\gamma_q,$$

which is independent of k (compare to [6, Lemma 4.2], that every element of a Buchsteiner loop satisfies $x^{\rho}x = xx^{\lambda}$). Motivated by this quantity, we define a function $\psi : \mathrm{C}^2(Q,K) \to \mathrm{C}^1(Q,K)$ by

$$(\psi c)_q = c^{-q}_{q^{-1},q}c_{q,q^{-1}} = \gamma^{-q}_{q^{-1}}\gamma_q.$$

Proposition 4.1. *The function ψ is a well-defined group homomorphism*

$$\psi : \mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K) \to \mathrm{C}^1(Q,K).$$

Proof. Verify that $(\psi\delta^1 a) = a^{-q}_{q^{-1}}a^{-1}_q \cdot a^1_q a^q_{q^{-1}} = 1$ for every $a \in \mathrm{C}^1(Q,K)$, showing that ψ is trivial on $\mathrm{B}^2(Q,K)$. □

In particular, ψc is defined in terms of the equivalence class of the loop (K,Q,c). Complementing Proposition 3.1, we have:

Proposition 4.2. *The loop (K,Q,c) satisfies the property:*

(Inv) *if* $\psi c = 1$.

(H) *if* $\delta^1\psi c = 1$.

Proof. The first statement follows from the computation $(kq)(kq)^\lambda = (\psi c)_q$ (for any $k \in K$ and $q \in Q$). By (3) we find that $(kq)^{\lambda^2} = k\gamma_{q^{-1}}^q\gamma_q^{-1}q$ and $(kq)^{\rho^2} = k\gamma_q\gamma_{q^{-1}}^{-q}q$, namely

$$(kq)^{\lambda^2} = (\psi c)_q^{-1} \cdot kq; \tag{5}$$

$$(kq)^{\rho^2} = (\psi c)_q \cdot kq. \tag{6}$$

This proves the first claim. One can then verify that λ^2 is a homomorphism if and only if $(\delta^1\psi c)_{q,q'} = \gamma_{q^{-1}}^q\gamma_q^{-1}(\gamma_{q'^{-1}}^{q'}\gamma_{q'}^{-1})^q(\gamma_{(qq')^{-1}}^{qq'}\gamma_{qq'}^{-1})^{-1} = 1$. $\square$

Taking $q = p^{-1}$ in the condition for (AI) given in Proposition 3.1, we obtain the condition of (Inv) as stated in Proposition 4.2, consistently with the implication (AI) $\implies$ (Inv) of Proposition 2.4.

4.1. Extensions of $\mathbb{Z}_2$

As an illustration we consider extensions with the largest nucleus, namely the case when $Q = \langle\sigma\rangle$ is the cyclic group of order 2. (The case $Q = \mathbb{Z}_4$ is described in Section). Since $|Q| = 2$, the factor set c is determined by the single value $\gamma_\sigma = c_{\sigma,\sigma} \in K$. Let us describe the properties of (K, Q, c) in this case.

Example 4.3. Suppose $L = (K, Q, c)$ is a nuclear loop extension of $Q = \mathbb{Z}_2$ by an abelian group. Then:

a. (WI) always holds.

b. (Inv) implies associativity.

Indeed, the conditions in Proposition 3.1 hold trivially when $p = 1$ or $q = 1$, so it remains to substitute $p = q = \sigma$. We find that (WI) holds trivially. Also, $(\psi c)_\sigma = \gamma_\sigma^{-1}\gamma_\sigma^\sigma$, so $\psi c = 1$ if and only if $\gamma_\sigma \in K^\sigma$, which is equivalent to associativity.

We also note that the loops in this subsection are all conjugacy closed, see [7].

5. A dihedral action

We use the conditions for (LI) and (RI) in Proposition 3.1 to define operators

$$\alpha, \beta : \mathrm{C}^2(Q, K) \to \mathrm{C}^2(Q, K)$$

as follows:

$$(\alpha c)_{p,q} = \gamma_{p^{-1}}^{p}\, c_{p^{-1},pq}^{-p},$$
$$(\beta c)_{p,q} = \gamma_{q}^{p}\, c_{pq,q^{-1}}^{-1},$$

where tautologically $\gamma_q = c_{q,q^{-1}}$ by (2).

Remark 5.1. The maps α, β are built on top of the involutorial maps $(p,q) \mapsto (p^{-1}, pq)$ and $(p,q) \mapsto (pq, q^{-1})$, generating an action of the symmetric group S_3 on the space of pairs Q^2. In fact, if $Q = \mathbb{Z}$ we obtain the irreducible representation $S_3 \hookrightarrow \mathrm{GL}_2(\mathbb{Z})$ generated by the involutions $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$.

Proposition 5.2. *The operators α, β define an action of the infinite dihedral group D_∞ on $\mathrm{C}^2(Q,K)$; namely $\alpha^2 = \beta^2 = \mathrm{id}$.*

Proof. We have that

$$(\alpha^2 c)_{p,q} = (\alpha c)_{p^{-1},p}^{p} (\alpha c)_{p^{-1},pq}^{-p} = (c_{p,p^{-1}}^{p^{-1}} c_{p,1}^{-p^{-1}})^{p} (c_{p,p^{-1}}^{p^{-1}} c_{p,q}^{-p^{-1}})^{-p} = c_{p,q};$$

and

$$(\beta^2 c)_{p,q} = (\beta c)_{q,q^{-1}}^{p} (\beta c)_{pq,q^{-1}}^{-1} = (c_{q^{-1},q}^{q} c_{1,q}^{-1})^{p} (c_{q^{-1},q}^{pq} c_{p,q}^{-1})^{-1} = c_{p,q};$$

thus $\langle \alpha, \beta \rangle$ is a dihedral group (which by Proposition 5.6 below is infinite for a generic K). $\square$

Remark 5.3. Both α and β act trivially on $\mathrm{B}^2(Q,K)$, so $\langle \alpha, \beta \rangle$ acts on the quotient space $\mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K)$. (However, see Example 9.7 below.)

Indeed, we also have that

$$\begin{aligned}(\alpha \delta^1 a)_{p,q} &= (\delta^1 a)_{p^{-1},p}^{p} (\delta^1 a)_{p^{-1},pq}^{-p} = (a_{p^{-1}} a_p^{p^{-1}} a_1^{-1})^{p} (a_{p^{-1}} a_{pq}^{p^{-1}} a_q^{-1})^{-p} \\ &= a_p a_{pq}^{-1} a_q^{p} = (\delta^1 a)_{p,q},\end{aligned}$$

and likewise $\beta \delta^1 a = \delta^1 a$.

Remark 5.4. We point out some useful computations.

1. The diagonal entries of α and β are

$$(\alpha c)_{p,p^{-1}} = (\beta c)_{p,p^{-1}} = c_{p^{-1},p}^{p};$$

   and therefore

$$(\alpha\beta c)_{p,p^{-1}} = (\beta\alpha c)_{p,p^{-1}} = c_{p,p^{-1}}.$$

2. Define $\Gamma : \mathrm{C}^2(Q,K) \to \mathrm{C}^1(Q,K)$ by $\Gamma c = \gamma$, namely $(\Gamma c)_p = c_{p,p^{-1}}$; then $\Gamma \alpha\beta = \Gamma$.

3. We have that $\psi\alpha c = \psi\beta c = \psi c^{-1}$. Therefore $\psi\alpha\beta = \psi$.

Proof. Taking $q = p^{-1}$ in the definition of α, β gives (1). (2) follows from the definition of $\Gamma c = \gamma$. Since ψc can be computed from $\Gamma c = \gamma$, we conclude (3) from (2). □

Let us compute some elements in the orbit of $c \in \mathrm{C}^2(Q, K)$ under the action.

Proposition 5.5. *The following formulas hold:*

$$(\alpha\beta c)_{p,q} = \gamma_p \gamma_{pq}^{-1} \, c^p_{q,(pq)^{-1}}; \tag{7}$$

$$(\beta\alpha c)_{p,q} = \gamma^{pq}_{q^{-1}} \gamma^{-pq}_{(pq)^{-1}} \, c^{pq}_{(pq)^{-1},p}; \tag{8}$$

$$(\alpha\beta\alpha c)_{p,q} = \gamma^{p}_{p^{-1}} \gamma^{pq}_{q^{-1}} \gamma^{-pq}_{(pq)^{-1}} \, c^{-pq}_{q^{-1},p^{-1}}; \tag{9}$$

$$(\beta\alpha\beta c)_{p,q} = \gamma_p \gamma^p_q \gamma^{-1}_{pq} \, c^{-pq}_{q^{-1},p^{-1}}. \tag{10}$$

Proof. Direct computation, aided by Proposition 5.4.(1). □

Careful substitution then proves:

Proposition 5.6. *We have the equality $(\alpha\beta)^3 c = c \cdot \delta^1 \psi c$.*

We write $X^G = \{x \in X : (\forall g \in G)\, gx = x\}$ for the subspace of X fixed under the action of a group G.

Corollary 5.7. *We have that*

$$\mathrm{C}^2(Q, K)^{\left\langle (\alpha\beta)^3 \right\rangle} = \psi^{-1} \mathrm{Z}^1(Q, K).$$

Proof. By Proposition 5.6, the elements fixed under $(\alpha\beta)^3$ are those c for which $\delta^1 \psi c = 1$, namely $\psi c \in \mathrm{Z}^1(Q, K) = \mathrm{Ker}(\delta^1)$. □

Notice that while the dihedral group D_∞ acts on the full space $\mathrm{C}^2(Q, K)$ (in a free manner, if K has elements of infinite order), there is an action of its quotient $\langle \alpha, \beta \rangle / \left\langle (\alpha\beta)^3 \right\rangle \cong S_3$ on the fixed subspace $\mathrm{C}^2(Q, K)^{\left\langle (\alpha\beta)^3 \right\rangle}$.

6. Loops and the dihedral action

We now interpret the loop properties from the introduction in terms of the dihedral action introduced in Section .

Proposition 6.1. *Let $c \in \mathrm{C}^2(Q, K)$. The loop (K, Q, c) has the property:*

(LI) *if and only if $\alpha c = c$.*

(RI) *if and only if $\beta c = c$.*

(WI) *if and only if* $\alpha\beta c = c$.

(AI) *if and only if* $\alpha\beta\alpha c = c$, *if and only if* $\beta\alpha\beta c = c$.

(IP) *if and only if* $\alpha c = \beta c = c$.

Proof. This is an interpretation of the conditions of Proposition 3.1, in the language of the operators as spelled out in Proposition 5.5. For example, (K, Q, c) has (LI) when $c_{p,q} = \gamma^p_{p^{-1}} c^{-p}_{p^{-1},pq} = (\alpha c)_{p,q}$. □

The dual description of (AI) in Proposition 6.1 allows us to extract a curious fact (especially in light of $\alpha\beta\alpha$ and $\beta\alpha\beta$ not being conjugate in the group, see Remark 7.3):

Corollary 6.2. $\mathrm{C}^2(Q,K)^{\langle\alpha\beta\alpha\rangle} = \mathrm{C}^2(Q,K)^{\langle\beta\alpha\beta\rangle}$.

Even more surprising, the loop theoretic description of the fixed subspaces gives the following inclusions:

Corollary 6.3. *We have that*

$$\mathrm{C}^2(Q,K)^{\langle\alpha\rangle},\quad \mathrm{C}^2(Q,K)^{\langle\beta\rangle},\quad \mathrm{C}^2(Q,K)^{\langle\alpha\beta\alpha\rangle} \;\subseteq\; \mathrm{Ker}(\psi) \;\subseteq\; \mathrm{C}^2(Q,K)^{\left\langle(\alpha\beta)^3\right\rangle}.$$

Proof. If $c \in \mathrm{C}^2(Q,K)$ is fixed under α, β or $\alpha\beta\alpha$, then (K,Q,c) has the properties (LI), (RI) or (AI) respectively, implying (Inv) in each case; but (Inv) means $\psi c = 1$ by Proposition 4.2. This proves the first statement. Likewise if $\psi c = 1$ then clearly $\delta^1\psi c = 1$, and by Corollary 5.7 we then get that $(\alpha\beta)^3 c = c$. □

We also note the trivial inclusion $\mathrm{C}^2(Q,K)^{\langle\alpha\beta\rangle} \subseteq \mathrm{C}^2(Q,K)^{\left\langle(\alpha\beta)^3\right\rangle}$, which in the same manner encodes the implication (WI) $\implies$ (H).

7. The fixed subspaces

The element $\alpha\beta$ of D_∞ is well defined up to inversion, as the generator of the unique subgroup C_∞ of index 2. Moreover, C_∞ contains all the non-torsion elements of D_∞, and these are the elements of even length in terms of the generators α, β (or any other pair of generating involutions). Recall that a subgroup is even if it is contained in C_∞, and odd otherwise. We analyze odd subgroups in this section, and even subgroups in Section .

Theorem 7.1. *Any fixed subspace* $\mathrm{C}^2(Q,K)^H$*, under an odd subgroup* $H \le D_\infty$*, is one of the subspaces*

$$\textit{(LI)} = \mathrm{C}^2(Q,K)^{\langle\alpha\rangle},\qquad \textit{(RI)} = \mathrm{C}^2(Q,K)^{\langle\beta\rangle},\qquad \textit{(AI)} = \mathrm{C}^2(Q,K)^{\langle\alpha\beta\alpha\rangle}$$

and

$$\textit{(IP)} = \mathrm{C}^2(Q,K)^{\langle\alpha,\beta\rangle}.$$

Proof. For $g, g' \in D_\infty$, let us write that $g \approx g'$ if $\mathrm{C}^2(Q,K)^{\langle g\rangle} = \mathrm{C}^2(Q,K)^{\langle g'\rangle}$. Since $\mathrm{C}^2(Q,K)^{\langle ghg^{-1}\rangle} = g(\mathrm{C}^2(Q,K)^{\langle h\rangle})$, this equivalence relation is stable under joint conjugation. Corollary 6.2 tells us that $\alpha\beta\alpha \approx \beta\alpha\beta$. Conjugation by α gives $\beta \approx \alpha\beta\alpha\beta\alpha$. These facts can be restated as $(\alpha\beta)^i\alpha \approx (\alpha\beta)^{i-3}\alpha$ for $i = 1, 2$. We have that $(\alpha\beta)^j(\alpha\beta)^k\alpha(\alpha\beta)^{-j} = (\alpha\beta)^{k+2j}\alpha$, which now implies $(\alpha\beta)^i\alpha \approx (\alpha\beta)^{i-3}\alpha$ for any $i \in \mathbb{Z}$. It follows that every odd element has the same fixed subspace as one of the three elements $\alpha, \beta, \alpha\beta\alpha$ (corresponding to $i = 0, -1, 1$).

Now let $H \leq D_\infty$ be an odd subgroup. Since the intersection with $\langle\alpha\beta\rangle$ is cyclic, we may write $H = \langle g, (\alpha\beta)^k\rangle$ where g is an odd element and $k \in \mathbb{Z}$. Then $\mathrm{C}^2(Q,K)^H = \mathrm{C}^2(Q,K)^{\langle g\rangle} \cap \mathrm{C}^2(Q,K)^{\langle(\alpha\beta)^k\rangle}$, so by the previous paragraph g can be replaced by one of the elements $\alpha, \beta, \alpha\beta\alpha$. By Corollary 6.3 we conclude that $\mathrm{C}^2(Q,K)^H \subseteq \mathrm{C}^2(Q,K)^{\langle(\alpha\beta)^3,(\alpha\beta)^k\rangle}$. If k is divisible by 3 it follows that $\mathrm{C}^2(Q,K)^H = \mathrm{C}^2(Q,K)^{\langle g\rangle}$; and otherwise $\mathrm{C}^2(Q,K)^H = \mathrm{C}^2(Q,K)^{\langle g,\alpha\beta\rangle} = \mathrm{C}^2(Q,K)^{\langle\alpha,\beta\rangle}$. □

Recall that $\mathrm{Z}^2(Q,K)$ is the space of elements $c \in \mathrm{C}^2(Q,K)$ satisfying the 2-cocycle condition (1); namely those c for which (K,Q,c) is a group. Since every group has the inverse property (IP), we proved:

Corollary 7.2. $\mathrm{Z}^2(Q,K) \subseteq \mathrm{C}^2(Q,K)^{\langle\alpha,\beta\rangle}$.

In other words, our group D_∞ acts trivially on the cohomology group $\mathrm{H}^2(Q,K) = \mathrm{Z}^2(Q,K)/\mathrm{B}^2(Q,K)$, which explains why it went unobserved in the classical theory of group extensions. The facts proved in Sections – are summarized in Figure 2.

$\mathrm{C}^2(Q,K)$

(H)$=\mathrm{C}^2(Q,K)^{\langle(\alpha\beta)^3\rangle}$

(Inv)$=\mathrm{Ker}(\psi)$

(AI)$=\mathrm{C}^2(Q,K)^{\langle\alpha\beta\alpha\rangle}$ (LI)$=\mathrm{C}^2(Q,K)^{\langle\alpha\rangle}$ (RI)$=\mathrm{C}^2(Q,K)^{\langle\beta\rangle}$ (WI)$=\mathrm{C}^2(Q,K)^{\langle\alpha\beta\rangle}$

(IP)$=\mathrm{C}^2(Q,K)^{\langle\alpha,\beta\rangle}$

(Associative)$=\mathrm{Z}^2(Q,K)$

(Trivial)$=\mathrm{B}^2(Q,K)$

Figure 2. Subgroups of $\mathrm{C}^2(Q,K)$, ordered by inclusion, and the respective properties of the loops (K,Q,c)

7.1. The opposite loop

The opposite serves as a left-right mirror, explaining expected symmetries. Recall that the opposite loop L^{op} has the same underlying set as L, with the reverse multiplication.

Remark 7.3. We have that $(K,Q,c)^{\mathrm{op}} \cong (K,Q,\tau c)$ via the map $(kq)^{\mathrm{op}} \mapsto k^{q^{-1}} q^{-1}$, where $\tau : \mathrm{C}^2(Q,K) \to \mathrm{C}^2(Q,K)$ is defined by $(\tau c)_{p,q} = c^{pq}_{q^{-1},p^{-1}}$. (This is an isomorphism of loops, even if not an equivalence of extensions since K is not fixed elementwise). We have that $\tau^2 = 1$ and $\tau\alpha = \beta\tau$ by computation. Consequently, the group $\langle \alpha, \beta, \tau \rangle = \langle \tau, \alpha \rangle$, which is by itself infinite dihedral, acts by conjugation on its subgroup $\langle \alpha, \beta \rangle$ as the full group of automorphisms. The action of $\langle \tau, \alpha \rangle$ on loops is discussed in [5].

It follows that a-priori

$$\begin{aligned} \mathrm{C}^2(Q,K)^{\langle\beta\rangle} &= \tau(\mathrm{C}^2(Q,K)^{\langle\alpha\rangle}), \\ \mathrm{C}^2(Q,K)^{\langle\beta\alpha\beta\rangle} &= \tau(\mathrm{C}^2(Q,K)^{\langle\alpha\beta\alpha\rangle}), \\ \mathrm{C}^2(Q,K)^{\langle\alpha\beta\rangle} &= \tau(\mathrm{C}^2(Q,K)^{\langle\alpha\beta\rangle}); \end{aligned}$$

indeed (LI) and (RI) are dual with respect to the opposite, while the other properties are left-right symmetric.

We also have that $\psi\tau = \psi$, in line with the fact that (Inv) is invariant to taking the opposite.

8. Generalizations of the weak inverse property

Following an insightful suggestion by the referee, we show in this section how the "doubly weak inverse property" and some of its generalizations fall under the framework of fixed subgroups of $\mathrm{C}^2(Q,K)$.

8.1. The m-inverse properties

For $m \in \mathbb{Z}$, a loop is said to have the *m-inverse property*, which we denote here by (W_m), if it satisfies the equivalent conditions

$$(xy)^{\rho^m} x^{\rho^{m+1}} = y^{\rho^m}; \tag{11}$$

$$x^{\lambda^{m+1}} (yx)^{\lambda^m} = y^{\lambda^m}; \tag{12}$$

$$\rho^m \ell_x \rho^{-m} = r^{-1}_{x^{\rho^{m+1}}}; \tag{13}$$

$$\lambda^m r_x \lambda^{-m} = \ell^{-1}_{x^{\lambda^{m+1}}}. \tag{14}$$

Indeed, (11)=(13) and (12)=(14) by the action on y, and (14) is obtained from (13) by taking $x^{\lambda^{m+1}}$ for x.

These properties were introduced by Karkliňš and Karkliň [10], see [6, Section 3]. By Proposition 2.5$(c)'$the weak inverse property is (WI)=(W_{-1}). One of the key facts on this sequence, proven in [6, Lemma 3.1], is that

$$(W_m) \implies (W_{-2m-1}), \tag{15}$$

resulting in the chain

$$(\mathrm{WI}) = (\mathrm{W}^1\mathrm{IP}) \Rightarrow (\mathrm{W}^2\mathrm{IP}) \Rightarrow (\mathrm{W}^3\mathrm{IP}) \Rightarrow (\mathrm{W}^4\mathrm{IP}) \Rightarrow \cdots$$

where ($\mathrm{W}^k\mathrm{IP}$) is defined for $k \geq 1$ as (W_m) for $m = \frac{(-2)^k-1}{3}$. The "doubly weak inverse property" ($\mathrm{W}^2\mathrm{IP}$)=(W_1) holds in any Buchsteiner loop, where (WI) does not necessarily hold.

Before characterizing the possible m-inverse properties of any given loop, we propose a change of indices, and write (W'_{1+3m}) instead of (W_m). Although hard to justify in terms of the defining identities (11)–(14), the formulation of various facts becomes cleaner in this manner. For example (15) reads $(W'_\ell) \implies (W'_{-2\ell})$, and $(\mathrm{W}^k\mathrm{IP}) = (W'_{(-2)^k})$.

We call a subset of $1 + 3\mathbb{Z}$ a *principal ideal* if it is has the form $(1 + 3\mathbb{Z})\ell$ for some $\ell \in 1 + 3\mathbb{Z}$. Notice that every two numbers $\ell, \ell' \in 1 + 3\mathbb{Z}$ have a unique greatest common divisor in $1 + 3\mathbb{Z}$, which we denote by $\gcd(\ell, \ell')$. For example, $\gcd(40, 100) = -20$.

Proposition 8.1.
1. $(W_{m'})+(W_{m''})+(W_{m'''}) \implies (W_{m'-m''+m'''})$.
2. *If* $1 + 3m \mid 1 + 3m'$ *then* $(W_m) \implies (W_{m'})$.
3. $(W'_\ell) + (W'_{\ell'}) \implies (W'_{\gcd(\ell,\ell')})$.

Proof. For completeness we copy the proof of the case $p = -1$ from [6, Lemma 3.1]: assuming (W_m), we have that $x^{\lambda^{-2m}}(yx)^{\lambda^{-(2m+1)}} = x^{\rho^{2m}}(yx)^{\rho^{2m+1}} \overset{(11)}{=} ((yx)^{\rho^m} \cdot y^{\rho^{m+1}})^{\rho^m} \cdot ((yx)^{\rho^m})^{\rho^{m+1}} \overset{(11)}{=} (y^{\rho^{m+1}})^{\rho^m} = y^{\lambda^{-2m-1}}$, proving ($W_{-2m-1}$).

1. Assume ($W_{m'}$), ($W_{m''}$) and ($W_{m'''}$) hold. Applying (13) and (14) alternatively, we have that

$$\begin{aligned}
\rho^{m'-m''+m'''}\ell_x\rho^{-(m'-m''+m''')} &= \rho^{m'''}\lambda^{m''}\rho^{m'}\ell_x\rho^{-m'}\lambda^{-m''}\rho^{-m'''} \\
&= \rho^{m'''}\lambda^{m''}r^{-1}_{x^{\rho^{m'+1}}}\lambda^{-m''}\rho^{-m'''} \\
&= \rho^{m'''}\ell_{x^{\rho^{m'-m''}}}\rho^{-m'''} \\
&= r^{-1}_{x^{\rho^{m'-m''+m'''+1}}},
\end{aligned}$$

which is ($W_{m'-m''+m'''}$).

2. Taking m', m'' in the previous claim to be m and $-2m-1$, it now follows that $(\mathrm{W}'_{1+3m}) + (\mathrm{W}'_{(1+3p)(1+3m)}) = (\mathrm{W}'_{1+3m}) + (\mathrm{W}'_{(4+3p)(1+3m)})$, and we are done by induction on p.

3. Let $I \subseteq 1+3\mathbb{Z}$ be the set of integers p for which (W'_p) is a consequence of the pair (W'_ℓ) and $(\mathrm{W}'_{\ell'})$. Let $a \in I$ be minimal in terms of absolute value. Assuming a does not divide $\gcd(\ell, \ell')$, let b be a minimal element of I, in terms of absolute value, not divisible by a. By (15) we have that $-2a \in I$. If a, b have different signs, then $-a-b = a-b+(-2a) \in I$ by the first part, but $|-a-b| < |b|$. If a, b have the same sign, then again $2a-b = a-b+a \in I$, but $|2a-b| = \left|2\frac{a}{b}-1\right||b| < |b|$ because $|a| < |b|$. In either case we have a contradiction. □

Corollary 8.2. *Let L be any loop. The set of integers $p \in 1+3\mathbb{Z}$ for which L satisfies (W'_p), if nonempty, is a principal ideal.*

Thus, if L satisfies any of the m-inverse properties, there is a minimal one, of which all of the others are formal consequences of. This may be called the "inverse level" of L. Corollary 8.2 is shown in [5] by using isotrophisms.

8.2. m-inverse for loop extensions

As always, let Q be a group acting on an abelian group K.

Proposition 8.3. *Let m be an odd integer. For $c \in \mathrm{C}^2(Q, K)$, $L = (K, Q, c)$ satisfies (W_m) if and only if*

$$(\alpha\beta)^{(3m+1)/2} c = c.$$

Proof. Write $m = 2n+1$. By (5)–(6) we have that

$$(kq)^{\rho^{2n}} = (\psi c)^n_q \cdot kq, \tag{16}$$

regardless of the sign of n. Taking $x = kp$ and $y = k'q$ in (11), acting by pq on the resulting equality and rearranging, we find that (K, Q, c) is has the property (W_m) if and only

$$c_{p,q} = (\delta^1\gamma)_{p,q} (\delta^1\psi c)^n_{p,q} \gamma^{-p}_{p^{-1}} c^{pq}_{(pq)^{-1},p}.$$

Next, we compute by Equation (7) that $((\alpha\beta)^2 c)_{p,q} = (\delta^1\gamma)_{p,q} \gamma^{-p}_{p^{-1}} c^{pq}_{(pq)^{-1},p}$. Applying Proposition 5.6 to $(\alpha\beta)^2 c$ in place of c, we then find that

$$((\alpha\beta)^{3n+2} c)_{p,q} = (\delta^1\gamma)_{p,q} (\delta^1\psi c)^n_{p,q} \gamma^{-p}_{p^{-1}} c^{pq}_{(pq)^{-1},p},$$

and the result follows. □

Remark 8.4. In terms of n, Proposition 8.3 reads that $L = (K, Q, c)$ satisfies (W_{2n+1}) if and only if $(\alpha\beta)^{3n+2} c = c$. To cover the other non-zero residue of 3 substitute $-n-1$ for n, to find that $(\mathrm{W}_{-(2n+1)})$ holds if and only if $(\alpha\beta)^{-(3n+1)} c = c$, which is equivalent to $(\alpha\beta)^{3n+1} c = c$.

Taking $m = -1$ in Proposition 8.3 recaptures the fact that $\mathrm{C}^2(Q,K)^{\langle\alpha\beta\rangle}$ corresponds to the weak inverse property, (WI). For $m = 1$ we obtain that $\mathrm{C}^2(Q,K)^{\left\langle(\alpha\beta)^2\right\rangle}$ is the doubly weak inverse property (W^2IP). More generally, taking $m = \frac{(-2)^k-1}{3}$, we obtain:

Corollary 8.5. *The extension $L = (K,Q,c)$ satisfies the property* (W^kIP) *if and only if $c \in \mathrm{C}^2(Q,K)^{\left\langle(\alpha\beta)^{2^{k-1}}\right\rangle}$.*

8.3. Generalizations of (H)

Let (H^m) denote the property of a loop that ρ^{2m}, equivalently λ^{2m}, are homomorphisms. Here m is allowed to be negative. By [6, Lemma 3.1],

$$(\mathrm{W}'_{2\ell}) \implies (\mathrm{H}^\ell)$$

for any $\ell \equiv 2 \pmod 3$; for example, (W^kIP) $\implies$ ($\mathrm{H}^{2^{k-1}}$); and in particular (WI)= (W^1IP) $\implies$ (H^1) = (H).

The following proposition complements Proposition 8.3, as we see in the theorem below.

Proposition 8.6. *The following are equivalent for the loop (K,Q,c):*

1. (H^n) *(namely λ^{2n} and ρ^{2n} are homomorphisms)*
2. $(\delta^1\psi c)^n = 1$.
3. $(\alpha\beta)^{3n}c = c$.

Proof. Since $(kq)^{\rho^{2n}} = (\psi c)^n_q \cdot kq$ by Example 16, it immediately follows that ρ^{2n} is a homomorphism if and only if $(\delta^1\psi(c^m) = 1$. But by Proposition 5.6 we also have that $(\alpha\beta)^{3n}c = (\delta^1\psi c)^n \cdot c$. □

The same computation yields the following observation, concerning weak versions of (Inv):

Proposition 8.7. *The following are equivalent for $c \in \mathrm{C}^2(Q,K)$:*

1. $\lambda^{2n} = 1$ *holds in* (K,Q,c).
2. $(\psi c)^n = 1$.

8.4. Invariants of even subgroups

Theorem 8.8. *The subspaces of $\mathrm{C}^2(Q,K)$ fixed under subgroups of $C_\infty = \langle\alpha\beta\rangle$ are*

$$(W_{2n+1}) = \mathrm{C}^2(Q,K)^{\left\langle(\alpha\beta)^{3n+2}\right\rangle}$$

and

$$(H^n) = \mathrm{C}^2(Q,K)^{\left\langle(\alpha\beta)^{3n}\right\rangle}.$$

Proof. Combine Remark 8.4 and Proposition 8.6, noting that any nontrivial subgroup of $\langle\alpha\beta\rangle$ can be uniquely represented in one of the forms $\langle(\alpha\beta)^{3n+2}\rangle$ (for $n \in \mathbb{Z}$) and $\langle(\alpha\beta)^{3n}\rangle$ (for $n > 0$). □

Proof of Theorem 1.1. The action of D_∞ on $\mathrm{C}^2(Q, K)$ is defined in Proposition 5.2. The subspaces fixed under odd subgroups are given in Theorem 7.1. The subspaces fixed under even subgroups are given in Theorem 8.8. □

9. Extensions of $\mathbb{Z}_4$

In this final section we describe the extensions (K, Q, c) for $Q = \langle\sigma\rangle$ the cyclic group of order 4, acting on an arbitrary abelian group K. This is a case of interest in light of the fact that any Buchsteiner loop is a nuclear extension of an abelian group of exponent 4 (see [6, Theorem 7.14]).

For brevity we denote $c_{\sigma^i,\sigma^j} = c_{ij}$ (and $a_{\sigma^i} = a_i$), and write c in a 3×3 matrix form, omitting the trivial row and column corresponding to the identity element of Q.

We are interested in c up to equivalence, so we may multiply c by $\delta^1 a$ for some $a \in \mathrm{C}^1(Q, K)$. Note that $(\delta^1 a)_2 = a_1 a_1^\sigma a_2^{-1}$ and $(\delta^1 a)_3 = a_1 a_2^\sigma a_3^{-1}$, so choosing a_2 and then a_3 properly, we may henceforth assume $c_{11} = c_{12} = 1$. Equivalence under this reduction amounts to entry-wise multiplication by $\delta^1 a = \begin{pmatrix} 1 & 1 & N(a_1) \\ 1 & N(a_1) & N(a_1) \\ N(a_1) & N(a_1) & N(a_1) \end{pmatrix}$ where $N(k) = kk^\sigma k^{\sigma^2} k^{\sigma^3}$ and $a_1 \in K$ is arbitrary. Solving the equations in Proposition 3.1 for $c_{ij} \in K$, we find:

Proposition 9.1. *The conditions for the loop $(K, \mathbb{Z}_4, c)$ to satisfy the respective properties are as follows:*

(LI) *if* $c \approx \begin{pmatrix} 1 & 1 & k \\ k' & \pi & \pi k'^{-\sigma^2} \\ k^{\sigma^3} & k^{\sigma^3} & k^{\sigma^3} \end{pmatrix}$ *for* $k, k', \pi \in K$ *with* $\pi^{\sigma^2} = \pi$.

(RI) *if* $c \approx \begin{pmatrix} 1 & 1 & k \\ k' & \pi & k^\sigma \\ k^{\sigma^3} & \pi^\sigma & k^{\sigma^2} k'^{-1} \end{pmatrix}$ *for* $k, k', \pi \in K$ *with* $\pi^{\sigma^2} = \pi$.

(WI) *if* $c \approx \begin{pmatrix} 1 & 1 & k \\ \pi & k & k' \\ \pi^{-1} k & \pi^{-1} k'^{\sigma^3} & k'^{\sigma^2} \end{pmatrix}$ *for* $k, k', \pi \in K$ *with* $\pi^\sigma = \pi^{-1}$.

(AI) *if* $c \approx \begin{pmatrix} 1 & 1 & k \\ k' & \pi & \pi k^\sigma k^{-1} \\ k^{\sigma^3} & \pi^\sigma k^{\sigma^3} k^{-1} k'^{-\sigma} & \pi^{-1} k^{\sigma^2} k^{\sigma^3} \end{pmatrix}$ *for* $k, k', \pi \in K$ *with* $\pi^{\sigma^2} = \pi$.

(Inv) *if* $c_{13} = c_{31}^{\sigma}$ *and* $c_{22}^{\sigma^2} = c_{22}$.

(H) *if there is* $\mu \in K$ *such that* $c_{13} = \mu^{-1}c_{31}^{\sigma}$ *and* $c_{22}^{\sigma^2} = \mu\mu^{\sigma}c_{22}$.

Intersecting any two of the conditions for (LI), (RI), (AI) and (WI), we obtain:

Proposition 9.2. (K, Q, c) *has* (IP) *when* $c \approx \begin{pmatrix} 1 & 1 & \pi \\ \pi\pi^{-\sigma} & \pi & \pi^{\sigma} \\ \pi^{\sigma} & \pi^{\sigma} & \pi^{\sigma} \end{pmatrix}$ *for* $\pi \in K$ *satisfying* $\pi^{\sigma^2} = \pi$. *This loop is a group when* $\pi \in K^{\sigma}$.

Letting $N : K \to K$ denote the function $N(k) = kk^{\sigma}k^{\sigma^2}k^{\sigma^3}$, Proposition 9.2 gives a 1-to-1 correspondence between $K^{\sigma^2}/N(K)$ and extensions of $\mathbb{Z}_4$ satisfying (IP), extending the well known correspondence between $\mathrm{H}^2(\mathbb{Z}_4, K) = K^{\sigma}/N(K)$ and group extensions.

As a complement to Proposition 2.1, we now give counterexamples for each of the implications (LI), (RI), (AI), (WI) + (Inv) $\implies$ (IP).

Corollary 9.3. *For each of the four halves, there is a loop of order* 8*, in fact an extensions of* $Q = \mathbb{Z}_4$ *by* $K = \mathbb{Z}_2$*, satisfying this property as well as* (Inv)*, but not any of the other three.*

Proof. In any of the formulas of Proposition 9.1 take $\pi = k' = 1$ and $k \neq 1$ to avoid the form of Proposition 9.2. □

Let $K_{(2)}$ denote the 2-torsion subgroup of K.

Proposition 9.4. *Let* K *be an abelian group on which* $Q = \mathbb{Z}_4$ *acts. The following are equivalent:*

1. *(WI)* $\implies$ *(Inv) for loops of the form* $L = (K, \mathbb{Z}_4, c)$*;*
2. *(H)* $\implies$ *(Inv) for loops of the form* $L = (K, \mathbb{Z}_4, c)$*;*
3. $K_{(2)} = 1$ *and the action is trivial.*

Proof. 2. $\implies$ 1. because (WI) $\implies$ (H).

1. $\implies$ 3. By Proposition 9.1, the condition for (Inv) is that $c_{31} = c_{13}^{\sigma^3}$ and $c_{22}^{\sigma^2} = c_{22}$. For the function c given in the same proposition for (WI), this holds when $k^{\sigma^2} = k$ and $\pi = kk^{-\sigma}$ (which imply $\pi^{\sigma} = \pi^{-1}$). If the action is nontrivial these conditions are countered by taking $\pi = 1$ and $k \notin K^{\sigma}$. If the action is trivial and there are elements of order 2, take π to be such an element and $k = 1$. It follows that the action is trivial and $K_{(2)} = 1$.

3. $\implies$ 2. Again by Proposition 9.1, (H) $\implies$ (Inv) if $\mu\mu^{\sigma} = \pi^{\sigma^2}\pi^{-1}$ implies $\mu = 1$. This condition can be written as $(\mu\pi^{\sigma}\pi^{-1})(\mu\pi^{\sigma}\pi^{-1})^{\sigma} = 1$, or equivalently $\mu \in \mathrm{Ker}(1+\sigma)\mathrm{Im}(1-\sigma)$, viewing K as a $\mathbb{Z}[Q]$-module, written multiplicatively. If the action is trivial and there are no elements of order 2, we have that $\mathrm{Im}(1-\sigma) = 1$ and $\mathrm{Ker}(1+\sigma) = \mathrm{Ker}(2) = 1$. □

Recall that (LI), (RI) and (AI) each imply (Inv). Following the recipe in the first part of Proposition 9.4, we construct an example showing that (WI)$\not\Longrightarrow$(Inv) for loop extensions.

Example 9.5. Let $L = \{\epsilon^i\sigma^j\}_{i\in\mathbb{Z}_3,\, j\in\mathbb{Z}_4}$ be the (monogenic) loop of order 12 with multiplication rule $\epsilon^i\sigma^j\cdot\epsilon^{i'}\sigma^{j'} = \epsilon^{i+(-1)^j i'+\delta_{j,-j'}(1-\delta_{j,0})}\sigma^{j+j'}$. Then L satisfies (WI) but not (Inv). (This is the loop $(\mathbb{Z}_3, \mathbb{Z}_4, c)$ where $\mathbb{Z}_4$ acts by inversion and c is taken from the formula for (WI) in Proposition 9.1 with $k = \epsilon$ and $k' = \pi = 1$.)

Remark 9.6. An extension $L = (K, Q, c)$ is commutative if Q is commutative, its action on K is trivial, and $c_{p,q} = c_{q,p}$ for all p, q. When $Q = \mathbb{Z}_4$, assuming commutativity means that either (LI) or (RI) implies associativity. On the other hand the examples for (AI)$\not\Longrightarrow$(IP) and (WI)$\not\Longrightarrow$(IP) in Corollary 9.3 are commutative. Example 9.5 for (WI)$\not\Longrightarrow$(Inv) is flexible, but not commutative.

As noted in Remark 5.3, $\langle\alpha,\beta\rangle$ acts on the quotient space $\mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K)$, namely on extensions up to equivalence. Clearly,

$$\mathrm{C}^2(Q,K)^{\langle\alpha\rangle}/\mathrm{B}^2(Q,K) \leq (\mathrm{C}^2(Q,K)/\mathrm{B}^2(Q,K))^{\langle\alpha\rangle},$$

and likewise for β (or any group action). If $K_2 = 1$ this is an equality, because $\alpha c = c\cdot\delta^1 a$ implies $(\delta^1 a)^2 = 1$. However, when K has 2-torsion the situation is more delicate:

Example 9.7. Let $Q = \mathbb{Z}_4$ act on $K = \langle t_0, t_1, t_2, t_3\rangle \cong (\mathbb{Z}_2)^4$ by permuting the indices. Consider the cocycle $c = \begin{pmatrix} 1 & 1 & 1 \\ 1 & t_0t_1 & t_0t_1 \\ t_0t_1t_2t_3 & t_0t_1t_2t_3 & t_0t_1t_2t_3 \end{pmatrix}$.

Then $(K,Q,c) \cong (K,Q,\alpha c)$ because $\alpha c\cdot c^{-1} \in \mathrm{B}^2(Q,K)$, but $\alpha c \neq c$, and indeed (K,Q,c) does not satisfy (LI): $t_0t_1t_2t_3\sigma^2 = (\sigma^2)^\lambda\cdot(\sigma^2\cdot\sigma^2) \neq \sigma^2$.

Similar examples can be constructed for the other properties.

References

[1] **R. Artzy**, *Contributions to the theory of loops*, Trans. AMS, **60** (1946), 245–354.

[2] **R. Artzy**, *On automorphic-inverse proerties in loops*, Proc. AMS, **10** (1959), 588–591.

[3] **K.S. Brown**, *Cohomology of groups*, Graduate Texts in Math., **87**, Springer, 1982.

[4] **R.H. Bruck**, *A survey of binary systems*, Berlin-Heidelberg, 1958.

[5] **A. Drápal and V.A. Shcherbakov**, *Identities and the group of isostrophisms*, Comm. Math. Univ. Carolinae, **53** (2012), 347–374.

[6] **P. Csörgő, A. Drápal, M.K. Kinyon**, *Buchsteiner loops*, Intern. J. Algebra Comput., **19** (2007), 1044–1088..

[7] **E.G. Goodaire and D.A. Robinson**, *A class of loops which are isomorphic to all loop isotopes*, Canad. J. Math., **34** (1982), 662–672.

[8] **K.W. Johnson, M.K. Kinyon, G.P. Nagy and P. Vojtěchovský**, *Searching for small simple automorphic loops*, LMS J. Comput. Math., **14** (2011), 200–213.

[9] **P. Nagy**, *Nuclear properties of loop extensions*, Results Math., **74** (2019), no.100.

[10] **B.B. Karkliňš and V.B. Karkliň**, *Inversnyje lupy*, Mat. Issled., **39** (1976), 87–101.

[11] **J. Marshall Osborn**, *Loops with the weak inverse property*, Pacific J Math., **10** (1960), 205–304..

[12] **D.A. Robinson**, *Bol loops*, Trans. AMS, **123**(2) (1966), 341–354.

Received November 10, 2020

Department of Mathematics,
Bar Ilan University,
Ramat Gan,
Israel
e-mail: vishne@math.biu.ac.il