Quasigroups and Related Systems **16** (2008), 1 – 12

Fuzzy Lie ideals of Lie algebras with interval-valued membership functions

Muhammad Akram

Abstract

The concept of interval-valued fuzzy sets was first introduced by Zadeh in 1975 as a generalization of fuzzy sets. In this paper we introduce the notion of interval-valued fuzzy Lie ideals in Lie algebras and investigate some of their properties. Using interval-valued fuzzy Lie ideals, characterizations of Noetherian Lie algebras are established. Construction of a quotient Lie algebra via interval-valued fuzzy Lie ideal in a Lie algebra is given. The interval-valued fuzzy isomorphism theorems are also established.

1. Introduction

Lie algebras were discovered by Sophus Lie (1842-1899) when he first attempted to classify certain "smooth" subgroups of general linear groups. The groups he considered are now called Lie groups. By taking the tangent space at the identity element of such a group, he obtained the Lie algebra and hence the problems on groups can be reduced to problems on Lie algebras so that it becomes more tractable. Lie algebra is applied in different domains such as physics, hyperbolic and stochastic differential equations. Lie algebra is also largely used by electrical engineers, mainly in the mobile robot control [5].

The notion of interval-valued fuzzy sets was first introduced by Zadeh [13] in 1975 as a generalization of fuzzy sets. An interval-valued fuzzy set is a fuzzy set whose membership function is many-valued and forms an interval with respect to the membership scale. This idea gives the simplest method

2000 Mathematics Subject Classification: 04A72
Keywords: Lie algebra, interval-valued fuzzy set, Lie ideal, Noetherian Lie algebra.
This research work was supported by PUCIT.

to capture the imprecision of the membership grades for a fuzzy set. It has been noted by Atansassov [3] that such fuzzy sets have some applications in the technological scheme of the functioning of a silo-farm with pneumatic transportation in a plastic products company and in medicine. The interval valued fuzzy sets provide a more adequate description of uncertainty than the traditional fuzzy sets, it is therefore important to use interval valued fuzzy sets in applications. One of the main applications of fuzzy sets is fuzzy control, and one of the most computationally intensive part of fuzzy control is the defuzzification. Since a transition to interval valued fuzzy sets usually increase the amount of computations, it is vitally important to design faster algorithms for the corresponding defuzzification. Fuzzy and anti fuzzy Lie ideals in Lie algebras have been studied in [1, 6, 7, 10, 11, 12]. In this paper, we apply the concept of interval-valued fuzzy sets to Lie algebras. We introduce the notion of interval-valued fuzzy Lie ideals in Lie algebras and investigate some of their properties. Using interval-valued fuzzy Lie ideals, characterizations of Noetherian Lie algebras are established. Construction of a quotient Lie algebra via interval-valued fuzzy Lie ideal in a Lie algebra is given. The interval-valued fuzzy isomorphism theorems are also established.

2. Preliminaries

In this paper by L will be denoted a *Lie algebra*, i.e., a vector space L over a field F (equal to $\mathbf{R}$ or $\mathbf{C}$) on which the operation $L \times L \to L$ denoted by $(x, y) \to [x, y]$ is defined and satisfies the following axioms:

(L_1) $[x, y]$ is bilinear,

(L_2) $[x, x] = 0$ for all $x \in L$,

(L_3) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in L$.

A subspace H of L closed under $[\ ,\ ]$ will be called a *Lie subalgebra.* A subspace I of L with the property $[I, L] \subseteq I$ will be called a *Lie ideal* of L. Obviously, any Lie ideal is a subalgebra.

A *fuzzy set* $\mu : L \to [0, 1]$ is called a *fuzzy Lie subalgebra* of L if

(a) $\mu(x + y) \geqslant \min\{\mu(x), \mu(y)\}$,

(b) $\mu(\alpha x) \geqslant \mu(x)$,

(c) $\mu([x, y]) \geqslant \min\{\mu(x), \mu(y)\}$

hold for all $x, y \in L$ and $\alpha \in F$.

According to [1] a fuzzy subset $\mu : L \to [0,1]$ satisfying (a), (b) and

(d) $\mu([x,y]) \geqslant \mu(x)$

is called a *fuzzy Lie ideal* of L. A fuzzy ideal of L is a fuzzy subalgebra [6] such that $\mu(-x) \geqslant \mu(x)$ holds for all $x \in L$.

By an *interval number* D we mean an interval $[a^-, a^+]$, where $0 \leqslant a^- \leqslant a^+ \leqslant 1$. The set of all interval numbers is denoted by $\mathcal{D}[0,1]$. For interval numbers $D_1 = [a_1^-, b_1^+]$, $D_2 = [a_2^-, b_2^+]$, we define

$\min(D_1, D_2) = \min([a_1^-, b_1^+], [a_2^-, b_2^+]) = [\min\{a_1^-, a_2^-\}, \min\{b_1^+, b_2^+\}]$,

$D_1 \leqslant D_2 \longleftrightarrow a_1^- \leqslant a_2^-$ and $b_1^+ \leqslant b_2^+$,

$D_1 = D_2 \longleftrightarrow a_1^- = a_2^-$ and $b_1^+ = b_2^+$.

An *interval-valued fuzzy set* (briefly, IF set) A on L is defined by

$$A = \{(x, [\mu_A^-, \mu_A^+]) : x \in L\},$$

where μ_A^- and μ_A^+ are fuzzy sets of L such that $\mu_A^-(x) \leqslant \mu_A^+(x)$ for all $x \in L$. Let $\widetilde{\mu}_A(x) = [\mu_A^-(x), \mu_A^+(x)]$, then

$$A = \{(x, \widetilde{\mu}_A(x)) : x \in L\},$$

where $\widetilde{\mu}_A : L \to \mathcal{D}[0,1]$. For $[s,t] \in \mathcal{D}[0,1]$, the set

$$U(\widetilde{\mu}; [s,t]) = \{x \in L : \widetilde{\mu}(x) \geq [s,t]\}$$

is called *upper level* of $\widetilde{\mu}$.

3. Interval-valued fuzzy Lie ideals in Lie algebras

Definition 3.1. An interval-valued fuzzy set $\widetilde{\mu}$ in a Lie algebra L is called an *interval-valued fuzzy Lie subalgebra* of L if

(1) $\widetilde{\mu}(x+y) \geqslant \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}$,

(2) $\widetilde{\mu}(\alpha x) \geqslant \widetilde{\mu}(x)$,

(3) $\widetilde{\mu}([x,y]) \geqslant \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}$

hold for all $x, y \in L$ and $\alpha \in F$.

Definition 3.2. An interval-valued fuzzy set $\widetilde{\mu}$ satisfying (1), (2) and

(4) $\widetilde{\mu}([x,y]) \geqslant \widetilde{\mu}(x)$

is called an *interval-valued fuzzy Lie ideal* of L.

From (2) it follows that

(5) $\widetilde{\mu}(0) \geqslant \widetilde{\mu}(x)$,

(6) $\widetilde{\mu}(-x) \geqslant \widetilde{\mu}(x)$

for all $x \in L$.

Example 3.3. The set $\Re^3 = \{(x,y,z) : x,y,z \in R\}$ with the operation $[x,y] = x \times y$, is a real Lie algebra. We define an IF set $\widetilde{\mu} : \Re^3 \to \mathcal{D}[0,1]$ by

$$\widetilde{\mu}(x,y,z) = \begin{cases} [s_1, s_2] & \text{if } x = y = z = 0, \\ [t_1, t_2] & \text{otherwise,} \end{cases}$$

where $[s_1, s_2] > [t_1, t_2]$ and $[s_1, s_2], [t_1, t_2] \in \mathcal{D}[0,1]$. By routine computations, we can see that it is an IF Lie subalgebra and Lie ideal of $\Re^3$.

Proposition 3.4. *Every interval-valued fuzzy Lie ideal is an interval-valued fuzzy Lie subalgebra.*

The converse of Proposition 3.4 is not true in general.

Example 3.5. Let $\Re^3$ and $[\ ,\ ]$ be as in the previous example. Putting

$$\widetilde{\mu}(x,y,z) = \begin{cases} [1,1] & \text{if } x = y = z = 0, \\ [0.5,\ 0.5] & \text{if } x \neq 0, y = z = 0, \\ [0,\ 0] & \text{otherwise,} \end{cases}$$

we obtain an example of an interval-valued fuzzy Lie subalgebra which is not an IF Lie ideal. Indeed,

$$\widetilde{\mu}([(1,0,0)\ (1,1,1)]) = \widetilde{\mu}(0,-1,1) = [0,0],$$

$$\widetilde{\mu}(1,0,0) = [0.5, 0.5].$$

That is,

$$\widetilde{\mu}([(1,0,0)\ (1,1,1)]) \ngeqslant \widetilde{\mu}(1,0,0).$$

Theorem 3.6. *An interval-valued fuzzy set $\widetilde{\mu} = [\mu^-, \mu^+]$ in L is an interval-valued fuzzy Lie ideal if and only if μ^- and μ^+ are fuzzy Lie ideals of L.*

Proof. Suppose that μ^- and μ^+ are fuzzy Lie ideals of L. Then

$$\begin{aligned}
\widetilde{\mu}(x+y) &= [\mu^-(x+y), \mu^+(x+y)] \\
&\geqslant [\min\{\mu^-(x)), \mu^-(y)\}, \min\{\mu^+(x)), \mu^+(y)\}] \\
&= [\min\{\mu^-(x), \mu^+(x)\}, \min\{\mu^-(y), \mu^+(y)\}] \\
&= \min\{\widetilde{\mu}(x)), \widetilde{\mu}(y)\}
\end{aligned}$$

for $x, y \in L$. The verification of (2) and (4) is analogous. Hence $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal of L.

Conversely, assume that $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal of L. Then

$$\begin{aligned}
[\mu^-(x+y), \mu^+(x+y)] &= \widetilde{\mu}(x+y) \geqslant \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\} \\
&= \min\{[\mu^-(x)), \mu^+(x)], [\mu^-(y), \mu^+(y)]\} \\
&= [\min\{\mu^-(x), \mu^-(y)\}, \min\{\mu^+(x), \mu^+(y)\}]
\end{aligned}$$

for $x, y \in L$. So,

$$\mu^-(x+y) \geqslant \min\{\mu^-(x), \mu^-(y)\} \text{ and } \mu^+(x+y) \geqslant \min\{\mu^+(x), \mu^+(y)\}.$$

In a similar way we can verify (2) and (4). This means that μ^- and μ^+ are fuzzy Lie ideals of L. □

Theorem 3.7. *All nonempty upper levels of interval-valued Lie ideals of a Lie algebra L are Lie ideals of L.*

Proof. Assume that $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal of L and let $[t_1, t_2] \in \mathcal{D}[0,1]$ be such that $U(\widetilde{\mu}; [t_1, t_2]) \neq \emptyset$. If $x \in U(\widetilde{\mu}; [t_1, t_2])$, and $y \in U(\widetilde{\mu}; [t_1, t_2])$, then $\widetilde{\mu}(x) \geqslant [t_1, t_2]$ and $\widetilde{\mu}(y) \geqslant [t_1, t_2]$. Hence

$$\widetilde{\mu}(x+y) \geqslant \min(\widetilde{\mu}(x), \widetilde{\mu}(y)) \geqslant [t_1, t_2],$$

$$\widetilde{\mu}(\alpha x) \geqslant \widetilde{\mu}(x) \geqslant [t_1, t_2],$$
$$\widetilde{\mu}([x, y]) \geqslant \widetilde{\mu}(x) \geqslant [t_1, t_2].$$

So, $x + y \in U(\widetilde{\mu}; [t_1, t_2])$, $\alpha x \in U(\widetilde{\mu}; [t_1, t_2])$ and $[x, y] \in U(\widetilde{\mu}; [t_1, t_2])$. This proves that $U(\widetilde{\mu}; [t_1, t_2])$ is a Lie ideal of L. □

Definition 3.8. Let $f : L_1 \to L_2$ be a homomorphism of Lie algebras. For any interval-valued fuzzy set $\widetilde{\mu}$ in a Lie algebra L_2, we define an interval-valued fuzzy set $\widetilde{\mu}^f$ in L by $\widetilde{\mu}^f(x) = \widetilde{\mu}(f(x))$ for all $x \in L_1$.

Lemma 3.9. *Let $f : L_1 \to L_2$ be a homomorphism of Lie algebras. If $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal of L_2, then $\widetilde{\mu}^f$ is an interval-valued fuzzy Lie ideal of L_1.*

Proof. Let $x, y \in L_1$ and $\alpha \in F$. Then

$$\begin{aligned}\widetilde{\mu}^f(x+y) = \widetilde{\mu}(f(x+y)) = \widetilde{\mu}(f(x)+f(y)) &\geqslant \min\{\widetilde{\mu}(f(x)), \widetilde{\mu}(f(y))\} \\ &= \min\{\widetilde{\mu}^f(x), \widetilde{\mu}^f(y)\},\end{aligned}$$

$$\widetilde{\mu}^f(\alpha x) = \widetilde{\mu}(f(\alpha x)) = \widetilde{\mu}(\alpha f(x)) \geqslant \widetilde{\mu}(f(x)) = \mu^f(x),$$

$$\widetilde{\mu}^f([x,y]) = \widetilde{\mu}(f([x,y])) = \widetilde{\mu}([f(x), f(y)]) \geqslant \widetilde{\mu}(f(x)) = \widetilde{\mu}^f(x),$$

which proves that $\widetilde{\mu}^f$ is an interval-valued fuzzy Lie ideal of L_1. □

Theorem 3.10. *Let $f : L_1 \to L_2$ be an epimorphism of Lie algebras. Then $\widetilde{\mu}^f$ is an interval-valued fuzzy Lie ideal of L_1 if and only if $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal of L_2.*

Proof. The sufficiency follows from Lemma 3.9. To prove the necessity observe that f is surjective, so for any $x, y \in L_2$ there are $x_1, y_1 \in L_1$ such that $x = f(x_1)$, $y = f(y_1)$. Thus $\widetilde{\mu}(x) = \widetilde{\mu}^f(x_1)$, $\widetilde{\mu}(y) = \widetilde{\mu}^f(y_1)$, whence

$$\begin{aligned}\widetilde{\mu}(x+y) = \widetilde{\mu}(f(x_1)+f(y_1)) = \widetilde{\mu}(f(x_1+y_1)) &= \widetilde{\mu}^f(x_1+y_1) \\ \geqslant \min\{\widetilde{\mu}^f(x_1), \widetilde{\mu}^f(y_1)\} &= \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\},\end{aligned}$$

$$\widetilde{\mu}(\alpha x) = \widetilde{\mu}(\alpha f(x_1)) = \widetilde{\mu}(f(\alpha x_1)) = \widetilde{\mu}^f(\alpha x_1) \geqslant \widetilde{\mu}^f(x_1) = \widetilde{\mu}(x),$$

$$\widetilde{\mu}([x,y]) = \widetilde{\mu}([f(x_1), f(y_1)]) = \widetilde{\mu}(f([x_1,y_1])) = \widetilde{\mu}^f([x_1,y_1]) \geqslant \widetilde{\mu}^f(x_1) = \widetilde{\mu}(x).$$

This proves that $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal of L_2. □

Definition 3.11. Two interval-valued fuzzy ideals $\widetilde{\mu}$ and $\widetilde{\lambda}$ of L have the *same type* if there exists $f \in Aut(L)$ such that $\widetilde{\mu}(x) = \widetilde{\lambda}(f(x))$ for all $x \in L$.

Theorem 3.12. *Let $\widetilde{\mu}$ and $\widetilde{\lambda}$ be interval-valued fuzzy Lie ideals of L. Then the following are equivalent:*

(*i*) *$\widetilde{\mu}$ and $\widetilde{\lambda}$ have the same type,*

(*ii*) *$\widetilde{\mu} \circ f = \widetilde{\lambda}$ for some $f \in Aut(L)$,*

(*iii*) *$g(\widetilde{\mu}) = \widetilde{\lambda}$ for some $g \in Aut(L)$,*

(*iv*) *$h(\widetilde{\lambda}) = \widetilde{\mu}$ for some $h \in Aut(L)$,*

(v) *there exist* $h \in Aut(L)$ *such that* $U(\widetilde{\mu};[t_1,t_2]) = h(U(\widetilde{\lambda};[t_1,t_2]))$ *for all* $[t_1,t_2] \in \mathcal{D}[0,1]$.

Proof. $(i) \rightarrow (ii)$: Proof follows immediately from the definition.

$(ii) \rightarrow (iii)$: Suppose that $\widetilde{\mu} \circ f = \widetilde{\lambda}$ for some $f \in Aut(L)$. Then $\widetilde{\mu}(f(x)) = \widetilde{\lambda}(x)$ and $f^{-1}(\widetilde{\mu})(x) = \sup_{y \in f(x)} \widetilde{\mu}(y) = \widetilde{\mu}(f(x)) = \widetilde{\lambda}(x)$ for all $x \in L$. If $g = f^{-1}$, then $g \in Aut(L)$ and $g(\widetilde{\mu}) = \widetilde{\lambda}$.

$(iii) \rightarrow (iv)$: Suppose that $g(\widetilde{\mu}) = \widetilde{\lambda}$ for some $g \in Aut(L)$. Then $\widetilde{\lambda}(x) = g(\widetilde{\mu}) = \sup_{y \in g^{-1}(x)} \widetilde{\mu}(y) = \widetilde{\mu}(g^{-1}(x))$. Hence $g^{-1}(x) = \sup_{y \in g(x)} \widetilde{\lambda}(y) = \widetilde{\lambda}(g(y)) = \widetilde{\mu}(g^{-1}(g(x))) = \widetilde{\mu}(x)$ for all $x \in L$. If $h = g^{-1}$, then $h \in Aut(L)$ and $h(\widetilde{\lambda}) = \widetilde{\mu}$.

$(iv) \rightarrow (v)$: If $h(\widetilde{\lambda}) = \widetilde{\mu}$ for some $h \in \mathrm{Aut}(L)$, then $\widetilde{\mu}(x) = h(\widetilde{\lambda})(x) = \sup_{y \in h^{-1}(x)} \widetilde{\lambda}(y) = \widetilde{\lambda}(h^{-1}(x))$ for all $x \in L$.

Let $[t_1,t_2] \in \mathcal{D}[0,1]$. We need to show $U(\widetilde{\mu};[t_1,t_2]) = h(U(\widetilde{\lambda};[t_1,t_2]))$. If $x \in U(\widetilde{\mu};[t_1,t_2])$, then $\widetilde{\lambda}(h^{-1}(x)) = \widetilde{\mu} \geqslant [t_1,t_2]]$ which implies that $h^{-1}(x) \in U(\widetilde{\lambda};[t_1,t_2])$, i.e., $x \in h(U(\widetilde{\lambda};[t_1,t_2]))$. Thus we obtain $U(\widetilde{\mu};[t_1,t_2]) \subseteq h(U(\widetilde{\lambda};[t_1,t_2]))$. On the other hand, let $x \in h(U(\widetilde{\lambda};[t_1,t_2]))$. Then $h^{-1}(x) \in U(\widetilde{\lambda};[t_1,t_2])$ and so $\widetilde{\mu}(x) = \widetilde{\lambda}(h^{-1}(x)) \geqslant [t_1,t_2]$. It follows that $x \in U(\widetilde{\mu};[t_1,t_2])$. Hence $h(U(\widetilde{\lambda};[t_1,t_2])) \subseteq U(\widetilde{\mu};[t_1,t_2])$ and (v) holds.

$(v) \rightarrow (i)$: Suppose that there exists $h \in \mathrm{Aut}(L)$ such that $U(\widetilde{\mu};[t_1,t_2]) = h(U(\widetilde{\lambda};[t_1,t_2]))$ for all $[t_1,t_2] \in \mathcal{D}[0,1]$. Let $\widetilde{\lambda}(h^{-1}(x)) = [s_1,s_2]$. Then $h^{-1}(x) \in U(\widetilde{\lambda};[s_1,s_2])$, hence $x \in h(U(\widetilde{\lambda};[s_1,s_2])) = U(\widetilde{\mu};[s_1,s_2])$. Thus $\widetilde{\mu}(x) \geqslant [s_1,s_2] = \widetilde{\lambda}(h^{-1}(x))$. Hence $\widetilde{\mu}(x) = \widetilde{\lambda}(h^{-1}(x))$ for all $x \in L$, which proves that $\widetilde{\mu}$ and $\widetilde{\lambda}$ have the same type. □

4. Characterizations of Noetherian Lie algebras

Definition 4.1. A Lie algebra L is said to be *Noetherian* if for every ascending sequence $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ of Lie ideals of L there exists a natural number n such that $I_n = I_k$ for all $n \geqslant k$.

Theorem 4.2. *A Lie algebra L is Noetherian if and only if the set of values of any its interval-valued fuzzy Lie ideal is well-ordered.*

Proof. Suppose that $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal whose set of values is not well-ordered subset of $\mathcal{D}[0,1]$. Then there exists a strictly decreasing sequence $\{[\alpha_n,\beta_n]\}$ such that $[\alpha_n,\beta_n] = \widetilde{\mu}(x_n)$ for some $x_n \in L$. Let $B_n := \{x \in L \,|\, \widetilde{\mu}(x) \geqslant [\alpha_n,\beta_n]\}$. Then $B_1 \subset B_2 \subset B_3 \subset \ldots$ form a strictly ascending chain of Lie ideals of L, contradicting the assumption that L is Noetherian.

Conversely, suppose that the set of values of any interval-valued fuzzy Lie ideal of L but L is not Noetherian. Then there exists a strictly ascending chain $A_1 \subset A_2 \subset A_3 \subset \ldots$ of Lie ideals of L. Suppose that $A = \bigcup\limits_{k=1}^{\infty} A_k$ is a Lie ideal of L. Define an interval-valued fuzzy set $\widetilde{\mu}$ in L by putting

$$\widetilde{\mu}(x) := \begin{cases} [\frac{1}{k+1}, \frac{1}{k}] & \text{for } x \in A_k \backslash A_{k-1}, \\ [0,\, 0] & \text{for } x \notin A. \end{cases}$$

We claim that $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideals of L. Let $x, y \in L$.

If $x, y \in A$ then there are m, n such that $x \in A_n \backslash A_{n-1}$, $y \in A_m \backslash A_{m-1}$. Obviously $x + y \in A_k \backslash A_{k-1} \subset A_p$, where $k \leqslant p = \max\{m, n\}$. So, $\widetilde{\mu}(x) = \left[\frac{1}{n+1}, \frac{1}{n}\right]$, $\widetilde{\mu}(y) = [\frac{1}{m+1}, \frac{1}{m}]$ and

$$\widetilde{\mu}(x+y) = [\frac{1}{k+1}, \frac{1}{k}] \geqslant [\frac{1}{p+1}, \frac{1}{p}] = \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}.$$

In the case $x \notin A$, $y \in A$ we have $y \in A_m \backslash A_{m-1}$ for some natural m. Hence $\widetilde{\mu}(x) = [0, 0]$, $\widetilde{\mu}(y) = [\frac{1}{m+1}, \frac{1}{m}]$, consequently

$$\widetilde{\mu}(x+y) \geqslant [0, 0] = \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}.$$

The case $x \in A$, $y \notin A$ is analogous. The case $x \notin A$, $y \notin A$ is obvious. The verification of (2) and (4) is analogous. Thus $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal of L. Consequently, $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal. Since the chain $A_1 \subset A_2 \subset A_3 \subset \ldots$ is not terminating, $\widetilde{\mu}$ has a strictly descending sequence of values. This contradicts that the value set of any interval-valued fuzzy Lie ideal is well-ordered. This completes the proof. □

We note that a set is well ordered if and only if it does not contain any infinite decreasing sequence.

Theorem 4.3. *Let $S = \{[s_1, t_1], [s_2, t_2], \ldots\} \cup \{[0, 0]\}$, where $\{[s_n, t_n]\}$ is a strictly decreasing sequence in $\mathcal{D}[0, 1]$. Then a Lie algebra L is Noetherian if and only if for each interval-valued fuzzy Lie ideal $\widetilde{\mu}$ of L, $Im(\widetilde{\mu}) \subseteq S$ implies that there exists a positive integer m such that $Im(\widetilde{\mu}) \subseteq \{[s_1, t_1], [s_2, t_2], \ldots,$ $[s_m, t_m]\} \cup \{[0, 0]\}$.*

Proof. If L is a Noetherian Lie algebra, then $Im(\widetilde{\mu})$ is a well ordered subset of $\mathcal{D}[0,1]$.

Conversely, if the above condition is satisfied and L is not Noetherian, then there exists a strictly ascending chain $A_1 \subset A_2 \subset A_3 \subset \ldots$ of Lie ideals of L. Define an interval-valued fuzzy set $\widetilde{\mu}$ by

$$\widetilde{\mu}(x) := \begin{cases} [s_1, t_1] & \text{if } x \in A_1, \\ [s_n, t_n] & \text{if } x \in A_n \backslash A_{n-1}, n = 2, 3, 4, \ldots \\ [0,\ 0] & \text{if } x \in G \backslash \bigcup_{n=1}^{\infty} A_n. \end{cases}$$

Let $x, y \in L$. If either x or y belongs to $G \backslash \bigcup_{n=1}^{\infty} A_n$, then either $\widetilde{\mu}(x) = [0,0]$ or $\widetilde{\mu}(y) = [0,0]$. Thus $\widetilde{\mu}(x+y) \geqslant \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}$.

If $x, y \in A_1$, then $x \in A_1$ and so $\widetilde{\mu}(x+y) = [s_1, t_1] \geqslant \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}$.

If $x, y \in A_n \backslash A_{n-1}$, then $x \in A_n$ and $\widetilde{\mu}(x+y) \geq [s_n, t_n] = \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}$. Assume that $x \in A_1$ and $y \in A_n \backslash A_{n-1}$ for $n = 2, 3, 4, \ldots$, then $x + y \in A_n$ and hence

$$\widetilde{\mu}(x+y) \geq [s_n, t_n] = \min\{[s_1, t_1], [s_n, t_n]\} = \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}.$$

Similarly for $x \in A_n \backslash A_{n-1}$ and $y \in A_1$ for $n = 2, 3, 4, \ldots$, we have

$$\widetilde{\mu}(x+y) \geq [s_n, t_n] = \min\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}.$$

Hence $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal of Lie algebra. This contradicts our assumption. The verification of (2) and (4) is analogous and we omit the details. This completes the proof. □

5. Quotient Lie algebra via IF Lie ideals

Theorem 5.1. *Let I be a Lie ideal of a Lie algebra L. If $\widetilde{\mu}$ is an interval-valued Lie ideal of L, then an interval-valued fuzzy set $\overline{\widetilde{\mu}}$ defined by*

$$\overline{\widetilde{\mu}}(a+I) = \sup_{x \in I} \widetilde{\mu}(a+x)$$

is an interval-valued Lie ideal of the quotient Lie algebra L/I.

Proof. Clearly, $\overline{\widetilde{\mu}}$ is well-defined. Let $x+I$, $y+I \in L/I$, then

$$\begin{aligned} \overline{\widetilde{\mu}}(x+I)+(y+I)) &= \overline{\widetilde{\mu}}_A((x+y)+I) = \sup\nolimits_{z \in I} \widetilde{\mu}((x+y)+z) \\ &= \sup\nolimits_{z=s+t \in I} \widetilde{\mu}((x+y)+(s+t)) \\ &\geqslant \sup\nolimits_{s,\ t \in I} \min\{\widetilde{\mu}(x+s), \widetilde{\mu}(y+t)\} \\ &= \min\{\sup\nolimits_{s \in I} \widetilde{\mu}(x+s), \sup\nolimits_{t \in I} \widetilde{\mu}(y+t)\} \\ &= \min\{\overline{\widetilde{\mu}}(x+I), \overline{\widetilde{\mu}}(y+I)\}, \end{aligned}$$

$$\overline{\widetilde{\mu}}(\alpha(x+I)) = \overline{\widetilde{\mu}}(\alpha x+I) = \sup_{z\in I}\widetilde{\mu}(\alpha x+z) \geqslant \sup_{z\in I}\widetilde{\mu}(x+z) = \overline{\widetilde{\mu}}(x+I),$$

$$\begin{aligned}\overline{\widetilde{\mu}}([x+I, y+I]) &= \overline{\widetilde{\mu}}([x,y]+I) = \sup_{z\in I}\widetilde{\mu}([x,y]+z)\\ &\geqslant \sup_{z\in I}\widetilde{\mu}(x+z) = \overline{\widetilde{\mu}}(x+I).\end{aligned}$$

Hence $\overline{\widetilde{\mu}}$ is an interval-valued fuzzy Lie ideal of L/I. □

Theorem 5.2. *Let $f : L_1 \to L_2$ be a homomorphism of a Lie algebra L_1 onto a Lie algebra L_2.*

(*i*) *If $\widetilde{\mu}$ is an interval-valued fuzzy Lie ideal of L_1, then $f(\widetilde{\mu})$ is an interval-valued fuzzy Lie ideal of L_2,*

(*ii*) *If $\widetilde{\lambda}$ is an interval-valued fuzzy Lie ideal of L_2, then $f^{-1}(\widetilde{\lambda})$ is an interval-valued fuzzy Lie ideal of L_1.*

Proof. Straightforward. □

For an interval-valued fuzzy Lie ideal $\widetilde{\mu}$ of a Lie algebra L we define a binary relation $\sim$ by putting

$$x \sim y \longleftrightarrow \widetilde{\mu}(x-y) = \widetilde{\mu}(0).$$

This relation is a congruence. The set of all its equivalence classes $\widetilde{\mu}[x]$ is denoted by $L/\widetilde{\mu}$. It is a Lie algebra under the following operations:

$$\widetilde{\mu}[x]+\widetilde{\mu}[y] = \widetilde{\mu}[x+y], \quad \alpha\widetilde{\mu}[x] = \widetilde{\mu}[\alpha x], \quad [\widetilde{\mu}[x], \widetilde{\mu}[y]] = \widetilde{\mu}[[x,y]],$$

where $x, y \in L$, $\alpha \in F$.

Theorem 5.3. (First IF isomorphism theorem)
Let $f : L_1 \to L_2$ be an epimorphism of Lie algebras and let $\widetilde{\mu}$ be an interval-valued fuzzy Lie ideal of L_2. Then $L_1/f^{-1}(\widetilde{\mu}) \cong L_2/\widetilde{\mu}$.

Proof. Define a map $\theta : L_1/f^{-1}(\widetilde{\mu}) \to L_2/\widetilde{\mu}$ by $\theta(f^{-1}(\widetilde{\mu})[x]) = \widetilde{\mu}[f(x)]$.

θ is well-defined since $f^{-1}(\widetilde{\mu})[x] = f^{-1}(\widetilde{\mu})[y]$ implies $f^{-1}(\widetilde{\mu})(x-y) = f^{-1}(\widetilde{\mu})(0)$. Whence $\widetilde{\mu}(f(x)-f(y)) = \widetilde{\mu}(f(0)) = \widetilde{\mu}(0)$. Thus $\widetilde{\mu}[f(x)] = \widetilde{\mu}[f(y)]$.

θ is one to one because $\widetilde{\mu}[f(x)] = \widetilde{\mu}[f(y)]$ gives $\widetilde{\mu}(f(x)-f(y)) = \widetilde{\mu}(0)$, i.e., $\widetilde{\mu}(f(x)-f(y)) = \widetilde{\mu}(f(0))$, which proves $f^{-1}(\widetilde{\mu})(x-y) = f^{-1}(\widetilde{\mu})(0)$. Thus $f^{-1}(\widetilde{\mu})[x] = f^{-1}(\widetilde{\mu})[y]$.

Since f is an onto, θ is an onto. Finally, θ is a homomorphism because

$$\begin{aligned}\theta(f^{-1}(\widetilde{\mu})[x]+f^{-1}(\widetilde{\mu})[y]) &= \theta(f^{-1}(\widetilde{\mu})[x+y]) = \widetilde{\mu}[f(x+y)] = \widetilde{\mu}[f(x)+f(y)]\\ &= \widetilde{\mu}[f(x)] + \widetilde{\mu}[f(y)] = \theta(f^{-1}(\widetilde{\mu})[x]) + \theta(f^{-1}(\widetilde{\mu})[y]),\end{aligned}$$

$$\theta(\alpha f^{-1}(\widetilde{\mu})[x]) = \theta(f^{-1}(\widetilde{\mu})[\alpha x]) = \widetilde{\mu}[f(\alpha x)] = \alpha\widetilde{\mu}[f(x)] = \alpha\theta(f^{-1}(\widetilde{\mu})[x]),$$

$$\begin{aligned}\theta([f^{-1}(\widetilde{\mu})[x], f^{-1}(\widetilde{\mu})[y]]) &= \theta([f^{-1}(\widetilde{\mu})[x,y]]) = \widetilde{\mu}[f([x,y])]\\ &= \widetilde{\mu}[[f(x), f(y)]] = [\widetilde{\mu}[f(x)], \widetilde{\mu}[f(y)]]\\ &= [\theta(f^{-1}(\widetilde{\mu})[x]), \theta(f^{-1}(\widetilde{\mu})[y])].\end{aligned}$$

Hence $L_1/f^{-1}(\widetilde{\mu}) \cong L_2/\widetilde{\mu}$. □

We state the following IF isomorphism Theorems without proofs.

Theorem 5.4. (Second IF isomorphism theorem)
Let $\widetilde{\mu}$ and $\widetilde{\lambda}$ be two interval-valued fuzzy subsets of the same Lie algebra. If $\widetilde{\mu}$ is a subalgebra and $\widetilde{\lambda}$ is a Lie ideal, then

(*i*) $\widetilde{\lambda}$ *is an interval-valued fuzzy Lie ideal of* $\widetilde{\mu}+\widetilde{\lambda}$,

(*ii*) $\widetilde{\mu}\cap\widetilde{\lambda}$ *is an interval-valued fuzzy ideal of* $\widetilde{\mu}$,

(*iii*) $(\widetilde{\mu}+\widetilde{\lambda})/\lambda \cong \widetilde{\mu}/(\widetilde{\mu}\cap\widetilde{\lambda})$.

Theorem 5.5. (Third IF isomorphism theorem)
Let $\widetilde{\mu}$ and $\widetilde{\lambda}$ be interval-valued fuzzy Lie ideals of the same Lie algebra such that $\widetilde{\mu} \leqslant \widetilde{\lambda}$. Then

(*i*) $\widetilde{\lambda}/\widetilde{\mu}$ *is an interval-valued fuzzy Lie ideal of* $L/\widetilde{\mu}$,

(*ii*) $(L/\widetilde{\mu})/(\widetilde{\lambda}/\widetilde{\mu}) \cong L/\widetilde{\lambda}$.

Theorem 5.6. (IF Zassenhaus lemma)
Let $\widetilde{\mu}$ and $\widetilde{\lambda}$ be interval-valued fuzzy subalgebras of a Lie algebra L and let $\widetilde{\mu}_1$ and $\widetilde{\lambda}_1$ be an interval-valued fuzzy Lie ideals of $\widetilde{\mu}$ and $\widetilde{\lambda}$ respectively. Then

(*a*) $\widetilde{\mu}_1+(\widetilde{\mu}\cap\widetilde{\lambda}_1)$ *is an interval-valued fuzzy Lie ideal of* $\widetilde{\mu}_1+(\widetilde{\mu}\cap\widetilde{\lambda})$,

(*b*) $\widetilde{\lambda}_1+(\widetilde{\mu}_1\cap\widetilde{\lambda})$ *is an interval-valued fuzzy ideal of* $\widetilde{\lambda}_1+(\widetilde{\mu}\cap\widetilde{\lambda})$,

(*c*) $\frac{\widetilde{\mu}_1+(\widetilde{\mu}\cap\widetilde{\lambda})}{\widetilde{\mu}_1+(\widetilde{\mu}\cap\widetilde{\lambda}_1)} \simeq \frac{\widetilde{\lambda}_1+(\widetilde{\mu}\cap\widetilde{\lambda})}{\widetilde{\lambda}_1+(\widetilde{\mu}_1\cap\widetilde{\lambda})}$.

References

[1] **M. Akram**: *Anti fuzzy Lie ideals of Lie algebras*, Quasigroups and Related Systems **14** (2006), 123 − 132.

[2] **M. Akram**: *Intuitionistic (S,T)-fuzzy Lie ideals of Lie algebras*, Quasigroups and Related Systems **15** (2007), 201 − 218.

[3] **K. T. Atanassov**: *Intuitionistic Fuzzy Sets: Theory and Applications*, Studies in fuzziness and soft computing, Heidelberg, Physica-Verl., 1999.

[4] **R. Biswas**: *Rosenfeld's fuzzy subgroups with interval-valued membership functions*, Fuzzy Sets and Systems **63** (1994), 87-90.

[5] **P. Coelho and U. Nunes**: *Lie algebra application to mobile robot control: a tutorial*, Robotica **21** (2003), 483 − 493.

[6] **B. Davvaz**: *Fuzzy Lie algebras*, Intern. J. Appl. Math. **6** (2001), 449 − 461.

[7] **B. Davvaz**: *A note on fuzzy Lie algebras*, Intern. JP J. Algebra Number Theory Appl. **2** (2002), 131 − 136.

[8] **W. A. Dudek**: *Fuzzy subquasigroups*, Quasigroups and Related Systems **5** (1998), 81 − 98.

[9] **A. K. Katsaras and D. B. Liu**: *Fuzzy vector spaces and fuzzy topological vector spaces*, J. Math. Anal. Appl. **58** (1977), 135 − 146.

[10] **Q. Keyun, Q. Quanxi and C. Chaoping**: *Some properties of fuzzy Lie algebras*, J. Fuzzy Math. **9** (2001), 985 − 989.

[11] **C. G. Kim and D. S. Lee**: *Fuzzy Lie ideals and fuzzy Lie subalgebras*, Fuzzy Sets and Systems **94** (1998), 101 − 107.

[12] **S. E. Yehia**: *The adjoint representation of fuzzy Lie algebras*, Fuzzy Sets and Systems **119** (2001), 409 − 417.

[13] **L. A. Zadeh**: *The concept of a lingusistic variable and its application to approximate reasoning*, Part 1, Information Sci. **8** (1975), 199 − 249.

[14] **J. M. Zhan and W. A. Dudek**: *Interval valued intuitionistic (S,T)-fuzzy H_v-submodules*, Acta Math. Sinica **22** (2006), 963 − 970.

Received May 7, 2007

Punjab University College of Information Technology, University of the Punjab, Old Campus, P. O. Box 54000, Lahore, Pakistan.
E-mail: m.akram@pucit.edu.pk

Quasigroups and Related Systems **16** (2008), 13 − 16

Counting loops with the inverse property

Asif Ali and John Slaney

Abstract

The numbers of isomorphism classes of IP loops of order up to 13 have been obtained by exhaustive enumeration, and are presented here along with some basic observations concerning IP loops.

1. Introduction

An *IP loop* is a set L and a binary operation $*$, where L contains an *identity* e such that $a * e = a = e * a$ for all $a \in L$, and where each $x \in L$ has a *two-sided inverse* x^{-1} such that for all $y \in L$

$$x^{-1} * (x * y) = y = (y * x) * x^{-1}.$$

For an account of the properties of IP loops, see Bruck's survey [3]). Clearly every group is an IP loop, but the converse is not the case. *Steiner loops* are also IP loops, satisfying the extra condition $x^{-1} = x$. IP loops form a very important class, not only in that they represent a strong generalization of both groups and Steiner loops, but also in that the Moufang nucleus (the set of $a \in L$ such that $a[(xy)a] = (ax)(ya)$ for all $x, y \in L$) of such loops behaves as a nilpotency function for this class. Moreover IP loops are exactly those groupoids whose power sets are the semiassociative relation algebras [7].

The present paper reports the numbers of non-isomorphic IP loops having order up to 13. Since these were obtained by exhaustive enumeration, they are available for inspection.

2000 Mathematics Subject Classification: 20N05
Keywords: loops, inverse property
This research was supported by National ICT Australia (NICTA). NICTA is funded through the Australian Government's *Backing Australia's Ability* initiative, in part through the Australian Research council.

2. History of counting loops

The number of non-isomorphic loops up to order 6 was found by Schönhardt [12] in 1930, but this was not noticed by Albert [1] or Sade [11] who obtained weaker results much later. Dénes and Keedwell [5] present counts of "quasigroups" up to order 6, but in fact count loops owing to their assumption that each "quasigroup" is isomorphic to a reduced square, which is obviously untrue of quasigroups in general. The loops of order 7 were counted in 1985 by Brant and Mullen [2]. In 2001, "QSCGZ" announced the number of loops of order 8 in an electronic forum [10], and the same value was found independently by Gujerin. For more on the history of counting loops, see McKay *et al* [9].

3. IP loops of small order

The smallest IP loop which is not a group is of order 7:

$*$	1	2	3	4	5	6	7
$e=1$	1	2	3	4	5	6	7
2	2	3	1	6	7	5	4
3	3	1	2	7	6	4	5
4	4	7	6	5	1	2	3
5	5	6	7	1	4	3	2
6	6	4	5	3	2	7	1
7	7	5	4	2	3	1	6

x	x^{-1}
1	1
2	3
3	2
4	5
5	4
6	7
7	6

This structure has proper subalgebras $\{1,2,3\}$, $\{1,4,5\}$ and $\{1,6,7\}$. Note that the order of these subloops does not divide the order of the loop, marking a significant difference between IP loops and groups.

Note also that the only element which is its own inverse is the identity e. This is a general feature of IP loops of odd order, as may be shown by a simple counting argument:

Observation 1. *IP loops of odd order have no subloops of even order.*

Proof. Let $(L,*)$ be an IP loop and let $(S,\underline{*})$ be a subloop of $(L,*)$ of even order. Clearly, S consists of e and some subset of elements of L along with their inverses. For this subset to be of even cardinality, some element in it other than e must be self-inverse and thus of order 2. Let $a \in L$ be such an element of order 2. Let $\dagger x$ be defined as $a * x$. Then the operation $\dagger$ is of period 2, because $\dagger\dagger x = a*(a*x) = a^{-1}*(a*x) = x$. Moreover, $\dagger$ has no fixed points, because if $\dagger x = x$ then $a * x = x$, so $a = e$, contradicting the assumption that a is of order 2. Hence $\dagger$ partitions L into pairs, so the cardinality of L must be even. □

The IP loops of small orders were counted by using a finite domain constraint solver to generate representatives of all isomorphism classes. The solver FINDER [13] has previously been used to generate results concerning the spectra of quasigroup identities [6]. It works by expressing each equation or other defining condition as the set of its ground instances on the domain of N elements, compiling these into constraints and then conducting a backtracking search for solutions to the constraint satisfaction problem using standard techniques such as forward checking and nogood learning [4].

Some symmetries were broken by enforcing conditions such as that e is always the first element. The remaining isomorphic copies were eliminated in a postprocessing phase. The results to order 11 were independently corroborated using the first order theorem prover PROVER9 and its associated propositional satisfiability solver MACE-4 [8]. In the cases of order 12 and order 13, the required searches are too hard for MACE and PROVER9, so we have only the results by FINDER in those cases.

size	groups	non − groups	total
1	1	0	1
2	1	0	1
3	1	0	1
4	2	0	2
5	1	0	1
6	2	0	2
7	1	1	2
8	5	3	8
9	2	5	7
10	2	45	47
11	1	48	49
12	5	2679	2684
13	1	10341	10342

Table 1. Numbers of IP loops of given order

The full list of these small IP loops, in a simple matrix format as for the order 7 example above, is available online.[1]

[1] `http://users.rsise.anu.edu.au/~jks/IPloops/`

References

[1] **A. A. Albert:** *Quasigroups. II*, Trans. Amer. Math. l Soc., **55** (1944), 401 – 409.

[2] **Brant and G. L. Mullen:** *A note on isomorphism classes of reduced latin squares of order* 7, Utilitas Math., **27** (1985), 261 – 263.

[3] **R. H. Bruck:** *A survey of binary systems*, Springer-Verlag, 1971.

[4] **R. Dechter:** *Constraint Processing*, Morgan Kaufmann, 2003.

[5] **J. Dénes and A. D. Keedwell:** *Latin squares and their applications*, Academic Press, 1974.

[6] **M. Fujita, J. Slaney, and F. Bennett:** *Automatic generation of some results in finite algebra*, Proc. 13th Internat. Joint Conference on Artificial Intelligence, 1993, 52 – 57.

[7] **R. Maddux:** *Some varieties containing relation algebras*, Trans. Amer. Math. Soc., **272** (1982), 501 – 526.

[8] **W. W. McCune:** *Prover9 Manual and Examples*, University of New Mexico, 2006. http://www.cs.unm.edu/ mccune/prover9/manual-examples.html.

[9] **B. D. McKay, A. Meynert, and W. Myrvold:** *Small latin squares, quasigroups and loops*, J. Combinatorial Designs, **15** (2007), 98 – 119.

[10] **QSCGZ** (pseudonym): *Anonymous electronic posting to Loopforum*, October 2001. http://groups.yahoo.com/group/loopforum/.

[11] **A. Sade:** *Morphismes de quasigroupes: Tables*, Revista da Faculdade de Ciências de Lisboa, 2: A – Ciências Matemáticas, **13** (1970/71), 149 – 172.

[12] **E. Schönhardt:** *Über lateinische quadrate und unionen*, J. für die reine und angewandte Mathematik, **163** (1930), 183 – 230.

[13] **J. Slaney:** *FINDER: Finite domain enumerator, system description*, Proc. 12th Confer. on Automated Deduction, 1994, 798 – 801.

Received October 12, 2007

Computer Sciences Laboratory
Research School of Infomation Sciences and Engineering
The Australian National University
Canberra, ACT 0200
Australia
e-mail: John.Slaney@anu.edu.au, dr_asif_ali@hotmail.com

Quasigroups and Related Systems **16** (2008), 17 − 24

On middle translations of finite quasigroups

Ivan I. Deriyenko

Abstract

We prove that a finite quasigroup is isotopic to a group if and only if some set of bijections induced by middle transformations of this quasigroup is a group.

1. Introduction

Let $Q = \{1, 2, 3, \dots, n\}$ be a finite set, φ and ψ permutations of Q. The multiplication (composition) of permutations is defined as $\varphi\psi(x) = \varphi(\psi(x))$.

Let $Q(\cdot)$ be a quasigroup. Permutations $L_a : x \to a \cdot x$, $R_a : x \to x \cdot a$ are called *left* and *right translations* of $Q(\cdot)$. Permutations λ_i, φ_i $(i \in Q)$ of Q such that

$$\lambda_i(x) \cdot x = i, \tag{1}$$

$$x \cdot \varphi_i(x) = i \tag{2}$$

for all $x \in Q$, are called *left* (respectively: *right*) *middle translations* of an element i in a quasigroup $Q(\cdot)$. Such translation were firstly studied by V. D. Belousov (cf. [1]) in connection with some groups associated with quasigroups. Next, the investigations of such translations were continued by many authors, see for example [3] or [5].

The above two conditions say that in a Latin square $n \times n$ connected with a quasigroup $Q(\cdot)$ of order n we select n cells, one in each row, one in each column, containing the same fixed element i. $\lambda_i(x)$ means that to find in the column x the cell containing an element i we must select the row $\lambda_i(x)$. Analogously, $\varphi_i(x)$ means that to find in the row x the cell containing i we must select the column $\varphi_i(x)$. Thus, λ_i is a selection of

2000 Mathematics Subject Classification: 05B15; 20N05
Keywords: Quasigroup, loop, group, isotopy, translation

rows, φ_i – a selection of columns, containing an element i. In connection with this fact λ_i will be called a *left track* (*l-track*), φ_i - a *right track* (*r-track*) of an element i. It is clear that for a quasigroup $Q(\cdot)$ of order n the set $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ uniquely determines its Latin square, and conversely, any Latin square $n \times n$ uniquely determines the set $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$. A similar situation holds for $\{\varphi_1, \varphi_2, \ldots, \varphi_n\}$.

More interesting facts on connections of translations with Latin squares one can find in [2].

As a simple consequence of the above definitions we obtain

Proposition 1.1. *In any quasigroup $Q(\cdot)$ the following identities hold:*

1) $\lambda_i = \varphi_i^{-1}$,

2) $\varphi_i^{-1}(x) \cdot x = i$,

3) $L_i(x) = (\lambda_i(x) \cdot x) \cdot x$,

4) $L_i(x) = (x \cdot \varphi_i(x)) \cdot x$,

5) $R_i(x) = x \cdot (\lambda_i(x) \cdot x)$,

6) $R_i(x) = x \cdot (x \cdot \varphi_i(x))$. □

Corollary 1.2. *In any group $G(\cdot)$ we have*

1) $\varphi_i(x) = x^{-1} \cdot i, \quad \lambda_i(x) = i \cdot x^{-1}$,

2) $\varphi_1(x) = \lambda_1(x) = x^{-1}$,

3) $L_i(x) = \lambda_i(x) \cdot x^2$,

4) $R_i(x) = x^2 \cdot \varphi_i(x)$,

where 1 is the identity element of the group $G(\cdot)$. □

2. Isotopy invariants in quasigroups

Two quasigroups $Q(\cdot)$ and $Q(\circ)$ are *isotopic* if there exists an ordered triple $T = (\alpha, \beta, \gamma)$ of bijections $\alpha, \beta, \gamma : Q \to Q$ such that

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

for all $x, y \in Q$.

For $y = \psi_i(x)$, where ψ_i is a r-track of a quasigroup $Q(\circ)$, this identity has the form

$$\gamma(x \circ \psi_i(x)) = \alpha(x) \cdot \beta\psi_i(x),$$

whence, according to (2), we obtain

$$\gamma(i) = \alpha(x) \cdot \beta\psi_i(x).$$

This for $z = \alpha(x)$ and $j = \gamma(i)$ gives

$$j = z \cdot \beta\psi_i\alpha^{-1}(z).$$

Since

$$j = z \cdot \varphi_j(z) = z \cdot \varphi_{\gamma(i)}(z)$$

for r-tracks φ_j and $\varphi_{\gamma(i)}$ of a quasigroup $Q(\cdot)$, the above implies

$$\varphi_{\gamma(i)} = \beta\psi_i\alpha^{-1}. \tag{3}$$

Remark 2.1. For l-tracks λ_i and μ_i of isotopic quasigroups $Q(\cdot)$ and $Q(\circ)$ we have

$$\lambda_{\gamma(i)} = \alpha\mu_i\beta^{-1}. \tag{4}$$

Definition 2.2. By a *spin* of a quasigroup $Q(\cdot)$ we mean the permutation

$$\varphi_{ij} = \varphi_i\varphi_j^{-1} = \varphi_i\lambda_j,$$

where φ_i and λ_j are tracks of $Q(\cdot)$. The spin φ_{ii} is called trivial.

The set of all spins of a quasigroup $Q(\cdot)$ is denoted by $\Phi_Q(\cdot)$.

Proposition 2.3. *Spins have the following properties*

1) $\varphi_{ij}(x) \neq x$ *for all* $x \in Q$ *and* $i \neq j$,

2) $\varphi_{pi}(x) \neq \varphi_{pj}(x)$ *for all* $x \in Q$ *and* $i \neq j$,

3) $\varphi_{ij} = \varphi_{ji}^{-1}$,

4) $\varphi_{ki}\varphi_{il} = \varphi_{kl}$,

5) $\varphi_{mk} = \varphi_{im}^{-1}\varphi_{ik}$.

Proof. (1) If $\varphi_{ij}(x) = x$ holds for some $i \neq j$ and $x \in Q$, then, according to the definition of φ_{ij}, we have $\varphi_i\varphi_j^{-1}(x) = x$. Whence, for $x = \varphi_j(y)$, we obtain $\varphi_i(y) = \varphi_j(y)$. Consequently $y \cdot \varphi_i(y) = y \cdot \varphi_j(y)$, i.e., $i = j$. This contradicts our assumption. So, $\varphi_{ij}(x) \neq x$ for all $x \in Q$ and $i \neq j$.

(2) Analogously as (1).

(3) $\varphi_{ij} = \varphi_i\varphi_j^{-1} = (\varphi_j\varphi_i^{-1})^{-1} = \varphi_{ji}^{-1}$.

(4) $\varphi_{ki}\varphi_{il} = (\varphi_k\varphi_i^{-1})(\varphi_i\varphi_l^{-1}) = \varphi_k(\varphi_i^{-1}\varphi_i)\varphi_l^{-1} = \varphi_{kl}$.

(5) $\varphi_{mk} = \varphi_m\varphi_k^{-1} = \varphi_m\varphi_i^{-1}\varphi_i\varphi_k^{-1} = (\varphi_i\varphi_m^{-1})^{-1}(\varphi_i\varphi_k^{-1}) = \varphi_{im}^{-1}\varphi_{ik}$. □

As it is well-known any permutation φ of the set Q of order n can be decomposed into $r \leqslant n$ cycles of the length $k_1, \ldots, k_r$ and $k_1 + \ldots + k_r = n$. We denote this fact by

$$Z(\varphi) = [k_1, k_2, \ldots, k_r] \, .$$

Since conjugate permutations are decomposable into cycles of the same length (see for example [4]), for any two conjugate permutations φ and ψ we have $Z(\varphi) = Z(\psi)$. Obviously $Z(\varphi) = Z(\varphi^{-1})$ for any permutation φ. So, $Z(\varphi_{ij}) = Z(\varphi_{ji})$ for all spins.

Definition 2.4. Let $\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ be a collection of permutations of the set Q. The set

$$Sp(\Phi) = [Z(\varphi_1), Z(\varphi_2), \ldots, Z(\varphi_n)]$$

is called the *spectrum* of Φ.

Two collections $\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ and $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ of permutations of Q have the same spectrum if and only if there exists a permutation γ of Q such that $Z(\varphi_i) = Z(\sigma_{\gamma(i)})$ for all $i = 1, 2, \ldots, n$.

The spectrum of all spins of a quasigroup $Q(\cdot)$, i.e., the set

$$[Z(\varphi_{11}), Z(\varphi_{12}), \ldots, Z(\varphi_{nn})]$$

is called the *spin-spectrum* of $Q(\cdot)$ and is denoted by $Ssp(Q, \cdot)$.

Theorem 2.5. *Finite isotopic quasigroups have the same spin-spectrum.*

Proof. Let $Q(\cdot)$ and $Q(\circ)$ be isotopic quasigroups. Then

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

for some permutations α, β, γ of Q.

In this case tracks of $Q(\cdot)$ and $Q(\circ)$ are connected by the formula (3). Spins of $Q(\cdot)$ and $Q(\circ)$ are pairwise conjugate. Namely

$$\varphi_{\gamma(i)\gamma(j)} = \beta\psi_{ij}\beta^{-1}.$$

Indeed,

$$\begin{aligned}\varphi_{\gamma(i)\gamma(j)} &= \varphi_{\gamma(i)}\varphi_{\gamma(j)}^{-1} = (\beta\psi_i\alpha^{-1})(\beta\psi_j\alpha^{-1})^{-1} \\ &= (\beta\psi_i\alpha^{-1})(\alpha\psi_j^{-1}\beta^{-1}) = \beta\psi_i\psi_j^{-1}\beta^{-1} = \beta\psi_{ij}\beta^{-1}.\end{aligned}$$

Since spins $\varphi_{\gamma(i)\gamma(j)}$ and ψ_{ij} are conjugate, we have $Z\left(\varphi_{\gamma(i)\gamma(j)}\right) = Z(\psi_{ij})$. This means that $Q(\cdot)$ and $Q(\circ)$ have the same spin-spectrum. □

Corollary 2.6. *If the isotopy of quasigroups $Q(\cdot)$ and $Q(\circ)$ has the form (α, α, γ), then also sets of all r-tracks (l-tracks) of these quasigroups have the same spectrum.*

Proof. Indeed, from (3) and (4), it follows that in this case l-tracks (respectively, r-tracks) of these quasigroups are pairwise conjugate. □

3. Spin-basis of quasigroups

Definition 3.1. Let Φ be a collection of all nontrivial spins of a quasigroup $Q(\cdot)$. A minimal subset B of Φ is called a *basis* of Φ if each spin from Φ can be written as a multiplication of spins (and their inverses) from B.

For example, the set

$$B_0 = \{\varphi_{12}, \varphi_{23}, \ldots, \varphi_{i(i+1)}, \ldots, \varphi_{(n-1)n}\}$$

containing $(n-1)$ spins is a basis since each spin φ_{pq}, where $p < q$, can be written in the form

$$\begin{aligned}\varphi_{pq} &= \varphi_p\varphi_q^{-1} = \varphi_p(\varphi_{p+1}^{-1}\varphi_{p+1}\varphi_{p+2}^{-1}\varphi_{p+2}\cdots\varphi_{q-1}^{-1}\varphi_{q-1})\varphi_q^{-1} \\ &= (\varphi_p\varphi_{p+1}^{-1})(\varphi_{p+1}\varphi_{p+2}^{-1})\ldots(\varphi_{q-1}\varphi_q^{-1}) = \varphi_{p(p+1)}\varphi_{(p+1)(p+2)}\cdots\varphi_{(q-1)q}.\end{aligned}$$

Also

$$B_i = \{\varphi_{i1}, \varphi_{i2}, \ldots, \varphi_{ik}, \ldots, \varphi_{in}\}, \quad i \neq k,$$

is a basis for every $i = 1, 2, \ldots, n$. Indeed, according to Proposition 2.3 (5), each spin φ_{pq} can be written in the form

$$\varphi_{pq} = \varphi_{ip}^{-1}\varphi_{iq}.$$

Definition 3.2. Let $Q(\cdot)$ be a quasigroup of order n. The set

$$\chi_i(Q,\cdot) = \{\varphi_{i1}, \varphi_{i2}, \dots, \varphi_{ii}, \dots, \varphi_{in}\} = B_i \cup \{\varphi_{ii}\}$$

is called the *ith spin-basis* of $Q(\cdot)$.

It coincides with the ith row of the matrix $[\varphi_{ij}]$. In general, it is not closed under multiplication of spins, but in some cases it is a group. Since $\varphi_{ki}\varphi_{ij} = \varphi_{kj}$, by Proposition 2.3, for all $i, k = 1, 2, \dots, n$ holds

$$\varphi_{ki}(\chi_i(Q,\cdot)) = \chi_k(Q,\cdot).$$

Proposition 3.3. *If one of the spin-basis of a quasigroup $Q(\cdot)$ is a group, then each of its spin-basis is a group and*

$$\chi_1(Q,\cdot) = \chi_2(Q,\cdot) = \ldots = \chi_n(Q,\cdot).$$

Proof. Let $\chi_i(Q,\cdot)$ be a group. Then $\chi_i(Q,\cdot)$ together with φ_{ik} contains also $\varphi_{ik}^{-1} = \varphi_{ki}$. This means that $\{\varphi_{1i}, \varphi_{2i}, \dots, \varphi_{ni}\} \subseteq \chi_i(Q,\cdot)$. Therefore each spin φ_{kj} belongs to $\chi_i(G,\cdot)$ because $\varphi_{kj} = \varphi_{ki}\varphi_{ij} \in \chi_i(G,\cdot)$ for all j, k. So, $\chi_k(Q,\cdot) \subseteq \chi_i(Q,\cdot)$ and $\varphi_{ki}(\chi_i(Q,\cdot)) = \chi_k(Q,\cdot)$ which completes the proof. □

Proposition 3.4. *Let quasigroups $Q(\cdot)$ and $Q(\circ)$ be isotopic. If one spin-basis of $Q(\cdot)$ is a group, then each spin-basis of $Q(\circ)$ is a group and for all $i = 1, \dots, n$ we have $\chi_i(Q,\cdot) \cong \chi_i(Q,\circ)$.*

Proof. Let $\gamma(x \circ y) = \alpha(x) \cdot \beta(y)$. Then, as in the proof of Theorem 2.5,

$$\varphi_{\gamma(i)\gamma(j)} = \beta\psi_{ij}\beta^{-1}.$$

Whence

$$\psi_{ij} = \beta^{-1}\varphi_{\gamma(i)\gamma(j)}\beta. \tag{5}$$

To prove that

$$\chi_i(G,\circ) = \{\psi_{i1}, \psi_{i2}, \dots, \psi_{in}\}$$

is a group observe that for all $\psi_{ip}, \psi_{iq} \in \chi_i(Q,\circ)$ we have

$$\psi_{ip}\psi_{iq} = \beta^{-1}\varphi_{\gamma(i)\gamma(p)}\varphi_{\gamma(i)\gamma(q)}\beta = \beta^{-1}\varphi_{\gamma(i)k}\beta = \psi_{it},$$

where $\gamma(t) = k$, since, by Proposition 3.3, each spin-basis of $Q(\cdot)$ is a group. Moreover, for every $\psi_{ik} \in \chi_i(Q,\circ)$, by (5) and Proposition 2.3, we obtain

$$\psi_{ik}^{-1} = \psi_{ki} = \beta^{-1}\varphi_{\gamma(k)\gamma(i)}\beta = \beta^{-1}\varphi_{\gamma(i)\gamma(k)}^{-1}\beta = \beta^{-1}\varphi_{\gamma(i)r}\beta = \psi_{is},$$

where $\gamma(s) = r$. This means that $\chi_i(Q, \circ)$ together with ψ_{ik} also contains ψ_{ik}^{-1}. So, it is a group. Clearly $\chi_i(Q, \circ) = \chi_k(Q, \circ)$ for all $k = 1, \dots, n$.

In view of (5) the isomorphism $h : \chi_{\gamma(i)}(Q, \cdot) \to \chi_i(Q, \circ) = \chi_{\gamma(i)}(Q, \circ)$ has the form $h(\varphi_{\gamma(i)\gamma(j)}) = \beta^{-1}\varphi_{\gamma(i)\gamma(j)}\beta$. □

Theorem 3.5. *A finite quasigroup which is a group is isomorphic to its spin-basis.*

Proof. Let $G(\cdot)$ be a group and $\chi_1(G, \cdot) = \{\varphi_{11}, \varphi_{12}, \dots, \varphi_{1n}\}$ its spin-basis. Then, according to the definition of spins, Proposition 1.1 and Corollary 1.2,

$$\varphi_{1i}(x) = \varphi_1(\lambda_i(x)) = \varphi_1(i \cdot x^{-1}) = (i \cdot x^{-1})^{-1} = x \cdot i^{-1} = R_{i^{-1}}(x),$$

which means that the spin-basis $\chi_1(G, \cdot)$ can be identified with the set of all right translations of $G(\cdot)$. So, $\chi_1(G, \cdot)$ and $G(\cdot)$ are isomorphic.

Proposition 3.3 completes the proof. □

Theorem 3.6. *A quasigroup for which the spin-basis is a group is isotopic to this group.*

Proof. Let $Q(\circ)$ be a quasigroup. Since it is isotopic to some loop $Q(\cdot)$ with the identity 1, in view of Propositions 3.3 and 3.4, it is sufficient to prove that $Q(\cdot)$ is isotopic to the group $\chi_1(Q, \cdot) = \{\varphi_{11}, \varphi_{12}, \varphi_{13}, \dots, \varphi_{1n}\}$.

For this we consider the mapping

$$h : \chi_1(Q, \cdot) \longrightarrow Q(\cdot) \quad \text{such that} \quad h(\varphi_{1i}) = i.$$

It is one-to-one and onto. We prove that it is an isomorphism, i.e.,

$$h(\varphi_{1k}\varphi_{1l}) = h(\varphi_{1k}) \cdot h(\varphi_{1l})$$

for all φ_{1k}, φ_{1l} from $\chi_i(Q, \cdot)$.

As $\chi_1(Q, \cdot)$ is a group, the product of φ_{1k} and φ_{1l} also belongs to $\chi_1(Q, \cdot)$. Let

$$\varphi_{1k}\varphi_{1l} = \varphi_{1p}.$$

By the definition of spins, the last equality is equivalent to

$$\varphi_1\varphi_k^{-1}\varphi_1\varphi_l^{-1} = \varphi_1\varphi_p^{-1},$$

i.e., to

$$\varphi_k^{-1}\varphi_1\varphi_l^{-1} = \varphi_p^{-1}$$

which can be written as

$$\varphi_p = \varphi_l \varphi_1^{-1} \varphi_k.$$

This means that

$$\varphi_p(x) = \varphi_l \varphi_1^{-1} \varphi_k(x)$$

holds for every $x \in Q$. Since $Q(\cdot)$ is a loop, the last identity is equivalent to

$$x \cdot \varphi_p(x) = x \cdot \varphi_l \varphi_1^{-1} \varphi_k(x),$$

whence, by (2), for $x = k$ we obtain

$$p = k \cdot \varphi_p(k) = k \cdot \varphi_l \varphi_1^{-1} \varphi_k(k) = k \cdot \varphi_l \varphi_1^{-1}(1) = k \cdot \varphi_l(1) = k \cdot l$$

because in any loop $\varphi_k(k) = 1$ and $\varphi_k(1) = k$.

So, $h(\varphi_{1k}\varphi_{1l}) = p = k \cdot l = h(\varphi_{1k}) \cdot h(\varphi_{1l})$, which completes the proof. $\square$

As a consequence of the above results we obtain

Theorem 3.7. *A finite quasigroup is isotopic to a group if and only if its spin-basis is a group.*

References

[1] **V. D. Belousov**: *On group associated with a quasigroup* (Russian), Mat. Issled. **4** (1969), no. 3, 21 − 39.

[2] **J. Dénes and A. D. Keedwell**: *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.

[3] **I. I. Deriyenko** (Derienko): *Necessary conditions of the isotopy of finite quasigroups*, (Russian) Mat. Issled. **120** (1991), 51 − 63.

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

[5] **V. A. Shcherbacov**: *Some properties of full associated group of IP-loop*, (Russian), Izvestia AN Mold. SSR. Ser. fiz.-techn. i mat. nauk **2** (1984), 51−52.

Received February 12, 2008

Kremenchuk State Polytechnical University
Pervomayskaya 20
39600 Kremenchuk
Ukraine
E-mail: ivan.deriyenko@gmail.com

Quasigroups and Related Systems **16** (2008), 25 − 29

Semigroup, monoid and group models of groupoid identities

Nick C. Fiala

Abstract

In this note, we characterize those groupoid identities that have a (finite) non-trivial (semigroup, monoid, group) model.

1. Introduction

Definition 1.1. A *groupoid* consists of a non-empty set equipped with a binary operation, which we simply denote by juxtaposition. A groupoid G is *non-trivial* if $|G| > 1$, otherwise it is *trivial*. A *semigroup* is a groupoid S that is *associative* ($(xy)z = x(yz)$ for all $x, y, z \in S$). A *monoid* is a semigroup M possessing a *neutral element* $e \in M$ such that $ex = xe = x$ for all $x \in M$ (the letter e will always denote the neutral element of a monoid). A *group* is a monoid G such that for all $x \in G$ there exists an *inverse* x^{-1} such that $x^{-1}x = xx^{-1} = e$. A *quasigroup* is a groupoid Q such that for all $a, b \in Q$, there exist unique $x, y \in Q$ such that $ax = b$ and $ya = b$. A *loop* is a quasigroup possessing a neutral element.

A *groupoid term* is a product of universally quantified variables. A *groupoid identity* is an equation, the left-hand side and right-hand side of which are groupoid terms. By the words *term* and *identity*, we shall always mean groupoid term and groupoid identity, respectively. The letters s and t will always denote terms. We will say that an identity $s = t$ has a (finite) non-trivial *model* if there exists a (finite) non-trivial groupoid G such that $s = t$ is valid in G. We will say that an identity $s = t$ has a (finite) non-trivial (semigroup, monoid, group, quasigroup, loop) model if $s = t$ has a

2000 Mathematics Subject Classification: 20N02
Keywords: groupoid, semigroup, monoid, group, quasigroup, loop, identity, model, non-trivial model, non-trivial finite model, undecidable, decidable

(finite) non-trivial model that is a (semigroup, monoid, group, quasigroup, loop).

The question of whether or not an identity has a (finite) non-trivial model is known to be *undecidable* (not answerable by an algorithm) [3]. In this note, we show that the question of whether or not an identity has a (finite) non-trivial (semigroup, monoid, group) model is *decidable*.

2. Results

Lemma 2.1. *An identity is valid in some non-trivial group if and only if it is valid in some non-trivial abelian group.*

Proof. Suppose that the identity $s = t$ is valid in some non-trivial group G. Let a be any non-neutral element of G. Then $s = t$ is valid in a non-trivial cyclic, and hence abelian, subgroup of G containing a. $\square$

Given a term t and a variable x_i, we denote by $o_i(t)$ the number of occurrences of x_i in t. Given an identity $s = t$ and a variable x_i, we denote by d_i the quantity $|o_i(s) - o_i(t)|$. Given an identity $s = t$ in the variables $x_1, x_2, \dots, x_n$, we denote by g the quantity $\gcd(d_1, d_2, \dots, d_n)$.

Proposition 2.2. *An identity $s = t$ in the variables $x_1, x_2, \dots, x_n$ has a non-trivial group model if and only if $g \neq 1$.*

Proof. Suppose $g = 1$. Suppose $s = t$ is valid in some non-trivial group G. By Lemma 2.1, $s = t$ is valid in some non-trivial abelian group H.

Now, in H, $s = t$ is equivalent to

$$x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n} = e.$$

Let $m_1, m_2, \dots, m_n \in \mathbb{Z}$ be such that $m_1 d_1 + m_2 d_2 + \cdots + m_n d_n = 1$. Then, in H,

$$\begin{aligned} x = x^1 &= x^{m_1 d_1 + m_2 d_2 + \cdots + m_n d_n} = x_1^{m_1 d_1} x_2^{m_2 d_2} \cdots x_n^{m_n d_n} \\ &= (x_1^{m_1})^{d_1} (x_2^{m_2})^{d_2} \cdots (x_n^{m_n})^{d_n} = e, \end{aligned}$$

a contradiction.

Finally, suppose $g \neq 1$. Then $s = t$ is valid in the non-trivial group $\mathbb{Z}_g$. $\square$

As was mentioned before, the question of whether or not an identity has a *finite* non-trivial model is also known to be undecidable [3]. In fact, there exist identities with no non-trivial finite models but that do have infinite models, such as the identity $(((yy)y)x)(((yy)((yy)y))z) = x$ [1].

Corollary 2.3. *An identity has a non-trivial group model if and only if it has a finite non-trivial group model.*

Proof. Suppose $s = t$ has a non-trivial group model. By Proposition 2.2, $g \neq 1$. Then $s = t$ is valid in the finite non-trivial group $\mathbb{Z}_g$. $\square$

Proposition 2.2 with "group" replaced by "loop" or "quasigroup" is false. Indeed, the identity $((xx)x)x = x(xx)$ is valid in the loop below (found with the model-generator Mace4 [2]).

$\cdot$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	5	0	6	4
2	2	4	5	1	6	3	0
3	3	0	6	4	2	1	5
4	4	3	0	6	5	2	1
5	5	6	1	0	3	4	2
6	6	5	4	2	1	0	3

It seems to be unknown if Corollary 2.3 with "group" replaced by "loop" or "quasigroup" is true.

Given the existence of a non-trivial idempotent ($x^2 = x$) monoid, Proposition 2.2 with "group" replaced by "monoid" is false. However, we now show that the question of whether or not an identity has a (finite) non-trivial monoid model is decidable.

Proposition 2.4. *An identity $s = t$ in the variables $x_1, x_2, \ldots, x_n$ has a non-trivial monoid model if and only if every variable occurs on both sides or $g \neq 1$.*

Proof. Suppose that there exists a variable x that occurs $n > 0$ times on one side of $s = t$ but not at all on the other side. Suppose $g = 1$. Suppose that $s = t$ is valid in some non-trivial monoid M. Substituting e for every variable in $s = t$ besides x results in $x^n = e$. Therefore, every element of M has an inverse and hence M is a group. By Proposition 2.2, M must be trivial, a contradiction.

Suppose that every variable in $s = t$ occurs on both sides. Then $s = t$ is valid in the non-trivial commutative idempotent monoid $(G, \cdot)$, where $G = \{0, 1\}$, $0 \cdot 0 = 0$ and $0 \cdot 1 = 1 \cdot 0 = 1 \cdot 1 = 1$.

Finally, suppose $g \neq 1$. Then $s = t$ is valid in the non-trivial group, and hence monoid, $\mathbb{Z}_g$. $\square$

Corollary 2.5. *An identity has a non-trivial monoid model if and only if it has a non-trivial finite monoid model.*

Proof. Suppose $s = t$ has a non-trivial monoid model. By Proposition 2.4, every variable that occurs in $s = t$ occurs on both sides or $g \neq 1$. If every variable that occurs in $s = t$ occurs on both sides, then $s = t$ is valid in the non-trivial commutative idempotent monoid above. If $g \neq 1$, then $s = t$ is valid in the finite non-trivial group, and hence monoid, $\mathbb{Z}_g$. □

Proposition 2.4 with "monoid" replaced by "semigroup" is false. Indeed, $xy = zu$ is valid in a non-trivial zero semigroup and $xy = x$ ($xy = y$) is valid in a non-trivial left-zero (right-zero) semigroup. Nevertheless, we now show that the question of whether or not an identity has a (finite) non-trivial semigroup model is decidable.

Proposition 2.6. *An identity $s = t$ in the variables $x_1, x_2, \ldots, x_n$ has a non-trivial semigroup model if and only if there are at least two variable occurrences on each side, one side is a variable which is also the left-most or right-most variable on the other side, or $g \neq 1$.*

Proof. Suppose one side of $s = t$ is a variable y. Suppose y is not the left-most or right-most variable on the other side. Suppose $g = 1$. Suppose $s = t$ is valid in some non-trivial semigroup S. Substituting x for every variable in $s = t$ besides y results in $xt(x, y)x = y$ for some (possibly empty) term $t(x, y)$ in the variables x and y.

Now, in S,

$$yt(y, x)(yt(y, z)y) = (yt(y, x)y)t(y, z)y.$$

Therefore,

$$yt(y, x)z = xt(y, z)y.$$

Substituting x for y in the above results in

$$xt(x, x)z = xt(x, z)x = z.$$

Thus, S is a monoid. By Proposition 2.4, S must be trivial, a contradiction.

Suppose that there are at least two variable occurrences on each side of $s = t$. Then $s = t$ is valid in the non-trivial zero semigroup $(G, \cdot)$, where $G = \{0, 1\}$ and $x \cdot y = 0$.

Suppose one side of $s = t$ is a variable which is also the left-most (right-most) variable on the other side. Then $s = t$ is valid in the non-trivial left-zero (right-zero) semigroup below.

$$\begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 1 & 1 \end{array} \quad \left(\begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 0 & 1 \end{array} \right)$$

Suppose $g \neq 1$. Then $s = t$ is valid in the non-trivial group, and hence semigroup, $\mathbb{Z}_g$. □

Corollary 2.7. *An identity has a non-trivial semigroup model if and only if it has a finite non-trivial semigroup model.*

Proof. Suppose $s = t$ has a non-trivial semigroup model. By Proposition 2.6, there are at least two variable occurrences on each side of $s = t$, one side of $s = t$ is a variable which is also the left-most or right-most variable on the other side, or $g \neq 1$. If there are at least two variable occurrences on each side of $s = t$, then $s = t$ is valid in the finite non-trivial zero semigroup above. If one side of $s = t$ is a variable which is also the left-most (right-most) variable on the other side, then $s = t$ is valid in the finite non-trivial left-zero (right-zero) semigroup above. If $g \neq 1$, then $s = t$ is valid in the finite non-trivial group, and hence semigroup, $\mathbb{Z}_g$. □

References

[1] **A. K. Austin**: *A note on models of identities*, Proc. Amer. Math. Soc. **16** (1965), 522 – 523.

[2] **W. McCune**: *Mace4* (`http://www.cs.unm.edu/~mccune/prover9/`).

[3] **R. McKenzie**: *On spectra, and the negative solution of the decision problem for identities having a finite nontrivial model*, J. Symbolic Logic **40** (1975), 186 – 196.

Received November 30, 2006
Revised May 8, 2007

Department of Mathematics, St. Cloud State University, St. Cloud, MN 56301
E-mail: ncfiala@stcloudstate.edu

Quasigroups and Related Systems **16** (2008), 31 − 36

Direct product of quasigroups and generalized diagonal subquasigroup

Tuval Foguel

Abstract

In this paper we look at when the direct product $\mathcal{P} \times \mathcal{Q}$ of two quasigroups contains a subquasigroup isomorphic to $\mathcal{P}$.

1. Introduction

The direct product $\mathcal{P} \times \mathcal{Q}$ of two groups (loops) clearly contains at least one subgroup (subloop) isomorphic to $\mathcal{P}$, namely $\mathcal{P} \times \{\mathbf{1}\}$. This is not the case for a direct product of two quasigroups. Bruck in [4] gives examples of finite nontrivial quasigroups $\mathcal{P}$ and $\mathcal{Q}$ whose direct product has no proper subquasigroups.

In this paper we will look at what we can say about the quasigroups $\mathcal{P}$ and $\mathcal{Q}$ if their direct product contains a subquasigroup isomorphic to $\mathcal{P}$.

2. Preliminaries

In this section, we review a few necessary notions from quasigroup theory and establish some notation conventions.

A *magma* $(\mathcal{Q}, \cdot)$ consists of a set $\mathcal{Q}$ together with a binary operation on $\mathcal{Q}$. For $x \in \mathcal{Q}$, define the left (resp., right) translation by x by $L(x)y = xy$ (resp., $R(x)y = yx$) for all $y \in \mathcal{Q}$. A magma with all left and right translations bijective is called a *quasigroup*. A quasigroup $\mathcal{Q}$ is an *idempotent quasigrop* if for all $x \in \mathcal{Q}$, $xx = x$. A quasigroup $\mathcal{L}$ with a two-sided identity element $\mathbf{1}$ such that for any $x \in \mathcal{L}$, $x\mathbf{1} = \mathbf{1}x = x$ is called a *loop*. A loop $\mathcal{L}$ is *power-associative*, if for any $x \in \mathcal{L}$, the subloop generated by x is a

2000 Mathematics Subject Classification: 20N05
Keywords: loop, quasigroup, direct product, covering.

group. For basic facts about loops and quasigroups, we refer the reader to [2], [3] and [7].

Notation 2.1. Given the direct product $\mathcal{P} \times \mathcal{Q}$ of two quasigroups, we will denote the i^{th} *projection homomorpishm* by π_i.

Notation 2.2. Given two quasigroups $\mathcal{K}$ and $\mathcal{Q}$, we will denote that $\mathcal{K}$ is a subquasigroup of $\mathcal{Q}$ by $\mathcal{K} \leq \mathcal{Q}$, and that $\mathcal{K}$ is a subquasigroup of $\mathcal{Q}$ but not equal to $\mathcal{Q}$ by $\mathcal{K} \lneq \mathcal{Q}$.

3. Generalized diagonal subquasigroup

Lemma 3.1. *If $\hat{\mathcal{Q}}$ is a homomorphic image of a quasigroup $\mathcal{P}$ and $\hat{\mathcal{Q}} \subseteq \mathcal{Q}$ a quasigroup, then $\hat{\mathcal{Q}}$ is a quasigroup.*

Proof. See [3]. $\square$

Lemma 3.2. *$\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups if and only if there exists a homomorphism $f : \mathcal{P} \to \mathcal{Q}$.*

Proof. Assume $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$. Then π_2 is a homomorphism from $\mathcal{K} \to \mathcal{Q}$ and since $\mathcal{P} \cong \mathcal{K}$ there exists a homomorphism $f : \mathcal{P} \to \mathcal{Q}$. Conversely, if there exists a homomorphism $f : \mathcal{P} \to \mathcal{Q}$, then $\mathcal{P} \cong \{(p, f(p)) | p \in \mathcal{P}\} \leq \mathcal{P} \times \mathcal{Q}$. $\square$

Corollary 3.3. *$\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups if and only if $\mathcal{Q}$ contains a subquasigroup that is a homomorphic image of $\mathcal{P}$.*

Proof. See Lemma 3.1 and Lemma 3.2. $\square$

Corollary 3.4. *$\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups with $\mathcal{Q}$ containing no subquasigroups except for itself if and only if $\mathcal{Q}$ is a homomorphic image of $\mathcal{P}$.*

Definition 3.5. Given $\mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups, we will call a subquasigroup $\mathcal{K}$ a *generalized diagonal subquasigroup* (*gd-subquasigroup*) if $\mathcal{K} = \{(p, f(p)) | p \in \mathcal{P}\} \leq \mathcal{P} \times \mathcal{Q}$ where f is a homomorphism from $\mathcal{P}$ to $\mathcal{Q}$.

Example 3.6. If $\mathcal{P}$ and $\mathcal{Q}$ are loops, then $\mathcal{K} = \mathcal{P} \times \{\mathbf{1}\} \leq \mathcal{P} \times \mathcal{Q}$ is a gd-subquasigroup.

Example 3.7. The diagonal-subquasigroup $\{(p, p) | p \in \mathcal{P}\}$ is a gd-subquasigroup of $\mathcal{P} \times \mathcal{P}$.

Theorem 3.8. *$\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups if and only if $\mathcal{P} \times \mathcal{Q}$ contains a gd-subquasigroup.*

Proof. By the definition of a gd-subquasigroup, it is isomorphic to $\mathcal{P}$.

If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$, then by Lemma 3.2 there is a homomorphism $f : \mathcal{P} \rightarrow \mathcal{Q}$. Thus $\{(p, f(p))|p \in \mathcal{P}\} \leq \mathcal{P} \times \mathcal{Q}$ is a gd-subquasigroup of $\mathcal{P} \times \mathcal{Q}$. □

Definition 3.9. A quasigroup is said to have a *covering* by subquasibgroups if it is the set-theoretic union of proper subquasigroups, and, if the set of subquasigroups is finite, we say the covering is finite. Such coverings have been widely studied in groups, and recently, analogous coverings for rings, semigroups, and loops have been discussed in [1], [6], and [5], respectively. A covering is disjoint if any two distinct subquasigroups in the covering are disjoint.

Lemma 3.10. *If $\mathcal{P}$ is a quasigroup and $\mathcal{Q}$ is an idempotent quasigroup, then $\mathcal{P} \times \mathcal{Q}$ has a disjoint covering $\mathcal{P} \times \mathcal{Q} = \bigcup\limits_{i \in \mathcal{Q}} (\mathcal{P} \times \{i\})$ where $\mathcal{P} \times \{i\} \cong \mathcal{P}$ for all $i \in \mathcal{Q}$.*

Proof. $\mathcal{P} \times \{i\} \cong \mathcal{P}$ since i is an idempotent for all $i \in \mathcal{Q}$. If $i, j \in \mathcal{Q}$ and $i \neq j$, then $\mathcal{P} \times \{i\} \bigcap \mathcal{P} \times \{j\} = \emptyset$ and if $h \in \mathcal{P} \times \mathcal{Q}$, then $h = (p, i)$ where $p \in \mathcal{P}$ and $i \in \{i\} \leq \mathcal{Q}$. □

Definition 3.11. A quasigroup is *homogeneous* if its automorphism group is transitive. A quasigroup is *doubly homogeneous* if its automorphism group is doubly transitive. A *two-quasigroup* is a nontrivial two generated doubly homogeneous quasigroup.

Remark 3.12. If $\mathcal{Q}$ is a two-quasigroup, then it is generated as a quasigroup by any two distinct elements, and by [8] $\mathcal{Q}$ is an idempotent quasigroup.

Example 3.13. Given $\mathcal{Q} = GF(p^n)$ (the Galois field of p^n elements), and α a primitive element in $GF(p^n)$. Then $(\mathcal{Q}, \odot)$ is a two-qusigroup under the binary operation

$$a \odot b = \alpha a + (\mathbf{1} - \alpha)b$$

for all $a, b \in \mathcal{Q}$.

Lemma 3.14. *If $\mathcal{P}$ is a quasigroup with no subquasigroups except for itself, and $\mathcal{Q}$ is a two-quasigroup, then every proper subquasigroup of $\mathcal{P} \times \mathcal{Q}$ is of the form $\mathcal{P} \times \{i\} \cong \mathcal{P}$ where $i \in \mathcal{Q}$.*

Proof. Assume $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$. Since $\pi_1(\mathcal{K}) \leq \mathcal{P}$ and $\mathcal{P}$ is a quasigroup with no proper subquasigroups, $\pi_1(\mathcal{K}) = \mathcal{P}$.

Let $k_1 = (p_1, i), k_2 = (p_2, j) \in \mathcal{K}$. If $i \neq j$, then since $\mathcal{Q}$ is a two-quasigroup $\pi_2(\mathcal{K}) = \mathcal{Q}$. Therefore given any $(p, t) \in \mathcal{P} \times \mathcal{Q}$ there exist $k = (\hat{p}, t) \in \mathcal{K}$, but some "power" of $\hat{p}$ is equal to p, and thus $\mathcal{K} = \mathcal{P} \times \mathcal{Q}$. So if $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$, then $\mathcal{K} = \mathcal{P} \times \mathcal{Q}$ or $\mathcal{K} = \mathcal{P} \times \{i\}$. $\square$

4. The non gd-subquasigroup

Lemma 3.1. *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups, then $\pi_1(\mathcal{K}) \leq \mathcal{P}$ and $\pi_1(\mathcal{K})$ is a homomrphic image of $\mathcal{P}$.*

Proof. $\pi_1(\mathcal{K}) \leq \mathcal{P}$ by definition. Since $\pi_1(\mathcal{K})$ is a homomrphic image of $\mathcal{K}$ it is a homomrphic image of $\mathcal{P} \cong \mathcal{K}$. $\square$

Corollary 3.2. *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a simple quasigroup and $\mathcal{Q}$ is a quasigroup, then $\pi_1(\mathcal{K}) \cong \mathcal{P}$ or $\{\mathbf{1}\}$.*

Corollary 3.3. *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a quasigroup with no subquasigroups except for itself, and $\mathcal{Q}$ is a quasigroup, then $\pi_1(\mathcal{K}) \cong \mathcal{P}$.*

Example 3.4. In $\mathbb{Z} \times \mathcal{L}$, where $\mathbb{Z}$ denotes the integers and $\mathcal{L}$ is any loop, $\mathcal{K} = 2\mathbb{Z} \times \{\mathbf{1}\} \cong \mathbb{Z} \cong \pi_1(\mathcal{K})$, but note that $\pi_1(\mathcal{K}) \neq \mathbb{Z}$.

Remark 3.5. Given $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups and $\mathcal{P}$ is finite, $\pi_1(\mathcal{K}) \cong \mathcal{P}$ if and only if $\pi_1(\mathcal{K}) = \mathcal{P}$.

Definition 3.6. Given nonempty subsets A and B of a quasigroup $\mathcal{P}$,we will denote by $AB = \{ab | \ a \in A, b \in B\}$.

The following deffinition is due to Bruck (see [4]).

Definition 3.7. Let $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups. For $p \in \mathcal{P}$ denote by $\mathcal{Q}_p = \{q \in \mathcal{Q} | \ (p, q) \in \mathcal{K}\} \subseteq \mathcal{Q}$.

Lemma 3.8. *If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups, then $\mathcal{Q}_p \mathcal{Q}_{\grave{p}} = \mathcal{Q}_{p\grave{p}}$ for $p, \grave{p} \in \pi_1(\mathcal{K})$.*

Proof. See [4] Lemma 15. Note that finiteness is not used in this part of the proof. $\square$

Remark 3.9. If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups and $p \in \mathcal{P} - \pi_1(\mathcal{K})$, then $\mathcal{Q}_p = \emptyset$.

Lemma 3.10. *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a loop and $\mathcal{Q}$ is a quasigroup, then $\mathcal{Q}_{\mathbf{1}}$ is isomorphic to a normal subloop of $\mathcal{P}$*

Proof. $\mathcal{Q}_{\mathbf{1}}$ is isomorphic to the kernel of π_1. $\square$

Lemma 3.11. *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a finite power associative loop and $\mathcal{Q}$ is a quasigroup, then $\underbrace{\mathcal{Q}_p \cdots \mathcal{Q}_p}_{|p|-times} = \mathcal{Q}_{\mathbf{1}}$ for any $p \in \pi_1(\mathcal{K})$.*

Proof. By Lemma 3.8 $\underbrace{\mathcal{Q}_p \cdots \mathcal{Q}_p}_{|p|-\text{times}} = \mathcal{Q}_{p^{|p|}} = \mathcal{Q}_{\mathbf{1}}$. $\square$

Definition 3.12. For a finite power associative loop $\mathcal{P}$, $\exp(\mathcal{P}) = n$ is the smallest positive integer such that given $p \in \mathcal{P}$ the identity $p^n = \mathbf{1}$ holds.

Corollary 3.13. *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a finite power associative loop and $\mathcal{Q}$ is a quasigroup, then for any $q \in \pi_2(\mathcal{K})$, $q^{\exp(\mathcal{P})} \in \mathcal{Q}_{\mathbf{1}}$.*

Proof. $q \in \mathcal{Q}_p$ for some $p \in \pi_1(\mathcal{K})$, and thus $q^{\exp(\mathcal{P})} \in \mathcal{Q}_{p^{\exp(\mathcal{P})}} = \mathcal{Q}_{\mathbf{1}}$. $\square$

Remark 3.14. If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups and $\mathcal{K}$ is finite, then $|\mathcal{K}| = \sum_{p \in \mathcal{P}} |\mathcal{Q}_p| = \sum_{p \in \pi_1(\mathcal{K})} |\mathcal{Q}_p|$.

Lemma 3.15. *If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups and $\mathcal{K}$ is finite, then $|\mathcal{Q}_p| = |\mathcal{Q}_{\grave{p}}|$ for $p, \grave{p} \in \pi_1(\mathcal{K})$ and $\mathcal{Q}_p$ and $\mathcal{Q}_{\grave{p}}$ are either disjoint or identical.*

Proof. By Remark 3.14 we see that $|\mathcal{Q}_p|$ is finite for each p, and thus by [4] Lemma 15, $|\mathcal{Q}_p| = |\mathcal{Q}_{\grave{p}}|$ for $p, \grave{p} \in \pi_1(\mathcal{K})$ where $\mathcal{Q}_p$ and $\mathcal{Q}_{\grave{p}}$ are either disjoint or identical. $\square$

Remark 3.16. *If $\mathcal{K} \cong \mathcal{P} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a finite quasigroup and $\mathcal{Q}$ is quasigroup, then $|\mathcal{P}| = \sum_{p \in \mathcal{P}} |\mathcal{Q}_p| = \sum_{p \in \pi_1(\mathcal{K})} |\mathcal{Q}_p|$.*

Lemma 3.17. *If $\mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups and $\mathcal{K}$ is finite, then $|\pi_1(\mathcal{K})| \, |\mathcal{Q}_p| = |\mathcal{K}|$ for any $p \in \pi_1(\mathcal{K})$.*
Proof. By Remarks 3.16 and Lemma 3.15 we get that

$$|\mathcal{K}| = \sum_{p \in \pi_1(\mathcal{K})} |\mathcal{Q}_p| = |\pi_1(\mathcal{K})| \, |\mathcal{Q}_p| \, . \qquad \square$$

Corollary 3.18. *If $\mathcal{P} \cong \mathcal{K} \leq \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a finit quasigroup and $\mathcal{Q}$ is quasigroup, then $|\pi_1(\mathcal{K})| \, |\mathcal{Q}_p| = |\mathcal{P}|$ for any $p \in \pi_1(\mathcal{K})$.*

Lemma 3.19. *If $\mathcal{K} \le \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups, $\pi_1(\mathcal{K}) \cong \mathcal{K}$ and $\mathcal{K}$ is finite, then $p \mapsto \mathcal{Q}_p$ for all $p \in \pi_1(\mathcal{K})$ is a homomorphism from $\pi_1(\mathcal{K})$ to $\mathcal{Q}$.*

Proof. By Lemma 3.17 we see that $|\mathcal{K}| = |\pi_1(\mathcal{K})|\,|\mathcal{Q}_p| = |\mathcal{K}|\,|\mathcal{Q}_p|$, and thus we get that $|\mathcal{Q}_p| = 1$ for all $p \in \pi_1(\mathcal{K})$. Therefore by Lemma 3.8 $p \mapsto \mathcal{Q}_p$ is a homomorphism for all $p \in \pi_1(\mathcal{K})$. □

Corollary 3.20. *If $\mathcal{P} \cong \mathcal{K} \le \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ is a finite quasigroup, $\mathcal{Q}$ is quasigroup, and $\pi_1(\mathcal{K}) \cong \mathcal{P}$, then $p \mapsto \mathcal{Q}_p$ for all $p \in \mathcal{P}$ is a homomorphism from $\mathcal{P}$ to $\mathcal{Q}$ and $\mathcal{K}$ is a gd-subquasigroup.*

Proof. Note that $\mathcal{K} = \{(p, \mathcal{Q}_p) | p \in \mathcal{P}\}$. □

Theorem 3.21. *If $\mathcal{P} \cong \mathcal{K} \le \mathcal{P} \times \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ are quasigroups with $\mathcal{P}$ finite, then $\pi_1(\mathcal{K}) \le \mathcal{P}$, $\pi_1(\mathcal{K})$ is a homomrphic image of $\mathcal{P}$, $|\mathcal{Q}_p|\,|\pi_1(\mathcal{K})| = |\mathcal{P}|$ for any $p \in \pi_1(\mathcal{K})$, and if $\mathcal{P} = \pi_1(\mathcal{K})$, then $\mathcal{K}$ is a gd-subquasigroup.*

Proof. This follows from Lemmas 3.1, Corollary 3.18 and Corollay 3.20. □

Example 3.22. Let $\mathcal{Q}$ be a finite quasigroup, $\mathcal{P} = \mathcal{Q} \times \mathcal{Q}$, and $\mathcal{K} = \{(q, q, \hat{q}) |\ q, \hat{q} \in \mathcal{Q}\} \subseteq \mathcal{P} \times \mathcal{Q}$. Then $\mathcal{K} \cong \mathcal{P}$ but $\pi_1(\mathcal{K}) \ncong \mathcal{P}$ and $\pi_2(\mathcal{K}) \ncong \mathcal{P}$.

Example 3.23. Let $\mathcal{P} = \mathcal{L} \times \mathbb{Z}_n = \mathcal{Q}$ where $\mathcal{L}$ is a loop, $\mathbb{Z}_n$ denotes the integers mod n, and let $\mathcal{K} = \{(l, 0, l, i) |\ l \in \mathcal{L}$ and $i \in \mathbb{Z}_n\}$. Then $\mathcal{Q}_{(l,0)} = \{(l, i) |\ i \in \mathbb{Z}_n\}$ is not a quasigroup if $l \neq \mathbf{1}$ and $\left|\mathcal{Q}_{(l,0)}\right| = n$.

References

[1] **H. Bell, A. Klein, L. C. Kappe:** *An analogue for rings of a group problem of P. Erdös and B.H. Neumann*, Acta Math. Hungar. **77** (1997), 57 – 67.

[2] **V. D. Belousov:** *Foundations of the Theory of Quasigroups and Loops*, Izdat. Nauka, Moscow, 1967 (Russian).

[3] **R. H. Bruck:** *A Survey of Binary Systems*, Springer Verlag, Berlin, 1971.

[4] **R. H. Bruck:** *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. **55** (1944), 19 – 52.

[5] **T. Foguel and L.C. Kappe:** *On loops covered by subloops*, Expositiones Math. **23**, (2005), 255 – 270.

[6] **L. C. Kappe, J.C. Lennox and J. Wiegold:** *An analogue for semigroups of a group problem of P. Erdös and B.H. Neumann*, Bull. Austral. Math. Soc. **63** (2001), 59 – 66.

[7] **H. O. Pflugfelder:** *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **7**, Heldermann Verlag, Berlin, 1990.

[8] **S. K. Stein:** *Homogeneous quasigroups*, *Pacific J. Math.* **14** (1964), 1091 – 1102.

Received June 25, 2007

Department of Mathematics, Auburn University Montgomery, PO Box 244023, Montgomery, AL 36124-4023 USA, E-mail: tfoguel@mail.aum.edu

Quasigroups and Related Systems **16** (2008), 37 − 54

Algebraic properties of some varieties of central loops

Tèmítọ́pẹ́ Gbọ́láhàn Jaiyéọlá and John Olúsọlá Adéníran

Abstract

Isotopes of C-loops with a unique non-identity squares are studied. It is proved that such loops are C-loops and A-loops. The relationship between C-loops and Steiner loops is further studied. Central loops with the weak and cross inverse properties are also investigated.

1. Introduction

C-loops are one of the least studied loops. Few publications that have considered C-loops include Fenyves [14], [15], Beg [7], [8], Phillips et. al. [24], [26], [21], [20], Chein [10] and Solarin et. al. [2], [30], [28], [27]. The difficulty in studying them is as a result of the nature of their identities when compared with other Bol-Moufang identities (the element occurring twice on both sides has no other element separating it from itself). Latest publications on the study of C-loops which has attracted fresh interest on the structure include [24], [26], and [21].

LC-loops, RC-loops and *C-loops* are loops that satisfies the identities

$$(xx)(yz) = (x(xy))z, \quad (zy)(xx) = z((yx)x), \quad x(y(yz)) = ((xy)y)z,$$

respectively. Fenyves' work in [15] was completed in [24]. Fenyves proved that LC-loops and RC-loops are defined by three equivalent identities. In [24] and [25], it was shown that LC-loops and RC-loops are defined by four equivalent identities. Solarin [28] named the fourth identities the *left middle* (LM) and *right middle* (RM) *identities* and loops that obey them are called

2000 Mathematics Subject Classification: 20N05, 08A05
Keywords: central loops, central square, weak inverse property, cross inverse property, unique non-identity commutator, associator, square, Osborn loop.

LM-loops and *RM-loops*, respectively. These terminologies were also used in [29]. Their basic properties are found in [26], [15] and [13].

The *right* and *left translation* on a loop $(L,\cdot)$ are bijections $R_x : L \to L$ and $L_x : L \to L$ defined as $yR_x = yx$.

Definition 1.1. Let $(L,\cdot)$ be a loop. The *left nucleus* of L is the set

$$N_\lambda(L,\cdot) = \{a \in L : ax \cdot y = a \cdot xy \ \forall\ x, y \in L\}.$$

The *right nucleus* of L is the set

$$N_\rho(L,\cdot) = \{a \in L : y \cdot xa = yx \cdot a \ \forall\ x, y \in L\}.$$

The *middle nucleus* of L is the set

$$N_\mu(L,\cdot) = \{a \in L : ya \cdot x = y \cdot ax \ \forall\ x, y \in L\}.$$

The *nucleus* of L is the set

$$N(L,\cdot) = N_\lambda(L,\cdot) \cap N_\rho(L,\cdot) \cap N_\mu(L,\cdot).$$

The *centrum* of L is the set

$$C(L,\cdot) = \{a \in L : ax = xa \ \forall\ x \in L\}.$$

The *center* of L is the set

$$Z(L,\cdot) = N(L,\cdot) \cap C(L,\cdot).$$

L is said to be a *centrum square loop* if $x^2 \in C(L,\cdot)$ for all $x \in L$. L is said to be a *central square loop* if $x^2 \in Z(L,\cdot)$ for all $x \in L$. L is said to be *left alternative* if for all $x, y \in L$, $x \cdot xy = x^2 y$ and is said to right alternative if for all $x, y \in L$, $yx \cdot x = yx^2$. Thus, L is said to be *alternative* if it is both left and right alternative. The triple (U, V, W) such that $U, V, W \in SYM(L,\cdot)$ is called an *autotopism* of L if and only if

$$xU \cdot yV = (x \cdot y)W \quad \forall\ x, y \in L.$$

$SYM(L,\cdot)$ is called the *permutation group* of the loop $(L,\cdot)$. The group of autotopisms of L is denoted by $AUT(L,\cdot)$. Let $(L,\cdot)$ and $(G,\circ)$ be two distinct loops. The triple $(U, V, W) : (L,\cdot) \to (G,\circ)$ such that $U, V, W : L \to G$ are bijections is called a *loop isotopism* if and only if

$$xU \circ yV = (x \cdot y)W \quad \forall\ x, y \in L.$$

We investigate central loops with the unique non-identity commutators, associators and squares. The relationship between C-loops and Steiner loops is studied. Central loops with the weak and cross inverse properties are also investigated.

For definition of concepts in theory of loops readers may consult [9], [29] and [23].

2. Preliminaries

Definition 2.1. (cf. [16]) Let a, b and c be three elements of a loop L. The *loop commutator* of a and b is the unique element (a, b) of L such that $ab = (ba)(a, b)$. The *loop associator* of a, b and c is the unique element (a, b, c) of L such that $(ab)c = \{a(bc)\}(a, b, c)$.

If X, Y, and Z are subsets of a loop L, we denote by (X, Y) and (X, Y, Z), respectively, the set of all commutators of the form (x, y) and all the associators of the form (x, y, z), where $x \in X, y \in Y, z \in Z$.

Definition 2.2. (cf. [16]) A *unique non-identity commutator* is an element $s \neq e$ (e is the identity element) in a loop L with the property that every commutator in L is e or s. A *unique non-identity commutator associator* is an element $s \neq e$ in a loop L with the property that every commutator in L is e or s and every associator is e or s. A *unique non-identity square* or *non-trivial square* is an element $s \neq e$ in a loop L with the property that every square in L is e or s.

Definition 2.3. A loop $(L, \cdot)$ is called a *weak inverse property loop* (W.I.P.L.) if and only if it satisfies the weak inverse property (W.I.P.): $y(xy)^\rho = x^\rho$ for all $x, y \in L$. L is called a *cross inverse property loop* (C.I.P.L.) if and only if it satisfies the cross inverse property (C.I.P.): $xy \cdot x^\rho = y$. $(L, \cdot)$ is a *left* (*right*) *inverse property loop* (L.I.P.L.) (resp. (R.I.P.L.)) if and only if it has the left (resp. right) inverse property (L.I.P) (resp. (R.I.P)): $x^\lambda(xy) = y$ (resp$(yx)x^\rho = y$. It is an *inverse property loop* (I.P.L.) if and only if it has the inverse property (I.P.) i.e., it has L.I.P. and R.I.P. property.

Most of our results and proofs, are written in dual form relative to RC-loops and LC-loops. That is, a statement like 'LC(RC)-loop... A(B)' where 'A' and 'B' are some equations or expressions means that 'A' is for LC-loops and 'B' is for RC-loops.

3. Inner mappings

Lemma 3.1. *Let L be a C-loop. Then for each $(A,B,C) \in AUT(L)$, there exists a unique pair $(S_1,T_1,R_1),(S_2,T_2,R_2) \in AUT(L,\cdot)$ such that $L_x^2 = S_2^{-1}S_1$, $R_x^2 = T_1^{-1}T_2$, $R_x^{-2}L_x^2 = R_2^{-1}R_1$, $R_1^{-1}R_2T_2^{-1}T_1S_2^{-1}S_1 = I$ for all $x \in L$.*

Proof. If L is a C-loop, then $(L_x^2, I, L_x^2), (I, R_x^2, R_x^2) \in AUT(L)$ for all $x \in L$. So, there exist $(S_1,T_1,R_1),(S_2,T_2,R_2) \in AUT(L)$ such that

$$(S_1,T_1,R_1) = (A,B,C)(L_x^2, I, L_x^2) \in AUT(L)$$
$$(S_2,T_2,R_2) = (A,B,C)(I, R_x^2, R_x^2) \in AUT(L).$$

Hence, the conditions hold although the identities do not depend on (A,B,C), but the uniqueness does. □

Theorem 3.1. *Let L be a C-loop and let there exist a unique pair of autotopisms $(S_1,T_1,R_1),(S_2,T_2,R_2)$ such that the conditions $L_x^2 = S_2^{-1}S_1$, $R_x^2 = T_1^{-1}T_2$ and $R_x^{-2}L_x^2 = R_2^{-1}R_1$ hold for each $x \in L$. If $\alpha_1 = S_1^{-1}$, $\alpha_2 = S_2^{-1}$, $\beta_1 = T_1^{-1}$, $\beta_2 = T_2^{-1}$, $\gamma_1 = R_1^{-1}$ and $\gamma_2 = R_2^{-1}$, then*

$$(x^2y)\alpha_1 = y\alpha_2, \qquad (yx^2)\beta_2 = y\beta_1, \qquad (x^2yx^{-2})\gamma_1 = y\gamma_2 \ \forall\ x,y \in L.$$

Proof. From Lemma 3.1 we have $L_x^2 = S_2^{-1}S_1$, $R_x^2 = T_1^{-1}T_2$, $R_x^{-2}L_x^2 = R_2^{-1}R_1$. Keeping in mind that a C-loop is power associative and nuclear square, we have the following:

1. $L_x^2 = S_2^{-1}S_1 \longleftrightarrow yL_x^2 = yS_2^{-1}S_1$ for all $y \in L \longleftrightarrow yL_{x^2} = yS_2^{-1}S_1 \longleftrightarrow x^2y = yS_2^{-1}S_1 \longleftrightarrow (x^2y)S_1^{-1} = yS_2^{-1} \longleftrightarrow x^2y\alpha_1 = y\alpha_2$.
2. $R_x^2 = T_1^{-1}T_2 \longleftrightarrow yR_x^2 = yT_1^{-1}T_2$ for all $y \in L \longleftrightarrow yx^2 = yT_1^{-1}T_2$ $\longleftrightarrow yx^2T_2^{-1} = yT_1^{-1} \longleftrightarrow yx^2\beta = y\beta_1$.
3. $R_x^{-2}L_x^2 = R_2^{-1}R_1 \longleftrightarrow yR_x^{-2}L_x^2 = yR_2^{-1}R_1$ for all $y \in L \longleftrightarrow x^2yx^{-2} = yR_2^{-1}R_1 \longleftrightarrow (x^2yx^{-2})R_1^{-1} = yR_2^{-1} \longleftrightarrow (x^2yx^{-2})\gamma_1 = y\gamma_2$. □

Corollary 3.1. *Let L be a C-loop. An autotopism of L can be constructed if there exists at least one $x \in L$ such that $x^2 \neq e$. In this case also the inverse can be constructed.*

Proof. We need Lemma 3.1 and Theorem 3.1. If $x^2 = e$, then the autotopism is trivial. Since L is a C-loop, using Lemma 3.1 and Theorem 3.1, it will be noticed that $(\alpha_1S_2, \beta_1T_2, \gamma_1R_2) \in AUT(L)$ and $(\alpha_2S_1, \beta_2T_1, \gamma_2R_1) = (\alpha_1S_2, \beta_1T_2, \gamma_1R_2)^{-1}$. Hence the proof. □

Lemma 3.2. *For a C-loop L the mapping $\gamma_2 R_1 \ : \ L \to L$ used in the autotopism $(\alpha_2 S_1, \beta_2 T_1, \gamma_2 R_1) \in AUT(L)$ and defined by the identity $y\gamma_2 R_1 = x^2 y x^{-2}$ for all $x \in L$ is:*

1. *an automorphism,*
2. *a semi-automorphism,*
3. *a middle inner mapping,*
4. *a pseudo-automorphism with companion x^2.*

Proof. 1. The map $\gamma_2 R_1$ is a bijection by the construction of the autotopism $(\alpha_2 S_1, \beta_2 T_1, \gamma_2 R_1) \in AUT(L)$. So we need only to show that it is an homomorphism. Let $y_1, y_2 \in L$, then: $(y_1 y_2)\gamma_2 R_1 = (x^2 y_1 x^{-2})(x^2 y_2 x^{-2}) = y_1\gamma_2 R_1 \cdot y_2 \gamma_2 R_1$. Whence, $\gamma_2 R_1$ is an automorphism.

2. We have $e\gamma_1 = e\gamma_2$, hence $e\gamma_2 R_1 = e$. Thus $(zy \cdot z)\gamma_2 R_1 = x^2(zy \cdot z)x^{-2} = x^2((zy \cdot z)x^{-2}) = (x^2 z x^{-2})(x^2 y x^{-2}) \cdot z\gamma_2 R_1 = (z\gamma_2 R_1 \cdot y\gamma_2 R_1) \cdot z\gamma_2 R_1$. So, $\gamma_2 R_1$ is a semi-automorphism.

3. Since $e\gamma_2 R_1 = e$, we hawe $y\gamma_2 R_1 = yR_{x^{-2}} L_{(x^{-2})^{-1}} = yT(x^{-2})$ for all $y \in L$, which implies $\gamma_2 R_1 = T(x^{-2}) \in Inn(L)$. Hence $\gamma_2 R_1$ is a middle inner mapping.

4. It is a consequence of the first property and the fact that any automorphism in a C-loop L is a pseudo-automorphism with companion x^2 for all $x \in L$. □

Lemma 3.3. *Let $(L, \cdot)$ be a C-loop. Then:*

1. $T(x^{-1}) = R_x T(x^{-2}) L_x^{-1}$, $T(x)^2 = R_x T(x^{-1})^{-1} L_x^{-1}$,
2. $T(x^n) = R_x^{n-1} T(x) L_x^{1-n}$, $T(x^{-n}) = R_x^{1-n} T(x^{-1}) L_x^{n-1}$ *for* $n \in \boldsymbol{Z}^+$,
3. $R(x, x) = I$, $L(x, x) = I$.

Proof. 1. For $\gamma_2 R_1$ from Lemma 3.2 we have $y\gamma_2 R_1 = x^2 y x^{-2} = yR_{x^{-2}} L_{x^2} = yR_x^{-1} R_x^{-1} L_x L_x = yR_x^{-1} T(x^{-1}) L_x$. Thus, $\gamma_2 R_1 = R_x^{-1} T(x^{-1}) L_x$. But $\gamma_2 R_1 = T(x^{-2})$ is the middle inner mapping, so, $T(x^{-2}) = R_x^{-1} T(x^{-1}) L_x$ implies $T(x^{-1}) = R_x T(x^{-2}) L_x^{-1}$. Therefore $T(x)^2 = R_x L_x^{-1} R_x L_x^{-1} = R_x (R_{x^{-1}} L_{x^{-1}}^{-1})^{-1} L_x^{-1} = R_x T(x^{-1})^{-1} L_x^{-1}$.

2. By induction.

$n = 1,\ T(x) = R_x^{1-1} T(x) L_x^{1-1} = R_{x^0} T(x) L_{x^0} = T(x)$ for $x \in L$,

$n = 2,\ T(x^2) = T(xx) = R_{x^2} L_{x^2}^{-1} = R_x R_x L_x^{-1} L_x^{-1} = R_x T(x) L_x^{-1}$ for $x \in L$,

$$n = 3,\ T(x^3) = T(x^2 x) = R_{x^2 x} L_{(x^2 x)^{-1}} = R_{x^2} R_x L_{x^{-1} x^{-2}} = R_{x^2} R_x L_{x^{-1}} L_{x^{-2}} = R_x^2 T(x) L_x^{-2} \text{ for all } x \in L.$$

Let $n = k,\ T(x^k) = R_x^{k-1} T(x) L_x^{1-k}$. Then for $n = k + 1$ we have

$T(x^{k+1}) = T(x^{k-1}x^2) = R_{x^{k-1}x^2}L^{-1}_{(x^{k-1}x^2)} = R_{x^{k-1}x^2}L_{x^{-2}x^{1-k}} =$
$R_{x^{k-1}}R_{x^2}L_{x^{-2}}L_{x^{1-k}} = R_{x^{k-1}}T(x^2)L_{x^{1-k}} = R_x^{k-1}R_xT(x)L_x^{-1}L_x^{1-k}$
$= R_x^kT(x)L_x^{-k}$.

Therefore $T(x^n) = R_x^{n-1}T(x)L_x^{1-n}$ for all $n \in \boldsymbol{Z}^+$. Replacing x by x^{-1} we obtain $T(x^{-n}) = T((x^{-1})^n) = R_{x^{-1}}^{n-1}T(x^{-1})L_{x^{-1}}^{1-n} = R_x^{1-n}T(x^{-1})L_x^{n-1}$. Thus, $T(x^{-n}) = R_x^{1-n}T(x^{-1})L_x^{n-1}$ for all $n \in \boldsymbol{Z}^+$.

3. $R(x,x) = R_x^2R_x^{-2} = I, L(x,x) = L_x^2L_x^{-2} = I$. □

Remark 3.1. Lemma 3.2 gives an example of a bijective mapping which is an automorphism, pseudo-automorphism, semi-automorphism and an inner mapping.

4. Relationship between C-loops and Steiner loops

For a loop $(L,\cdot)$, the bijection $J : L \to L$ is defined by $xJ = x^{-1}$. A *Steiner loop* is a loop satisfying the identities

$$x^2 = e, \quad yx \cdot x = y, \quad xy = yx.$$

Theorem 4.1. *A C-loop $(L,\cdot)$ in which $(I, L_z^2, JL_z^2J$ or (R_z^2, I, JR_z^2J) lies in $AUT(L)$ is a loop of exponent 4.*

Proof. 1. If $(I, L_z^2, JL_z^2J) \in AUT(L)$ for all $z \in L$, then $x \cdot yL_z^2 = (xy)JL_z^2J$ for all $x,y,z \in L$ implies $x \cdot z^2y = xy \cdot z^{-2}$. Whence $z^2y \cdot z^2 = y$. Then $y^4 = e$ for every $y \in L$.

2. If $(R_z^2, I, JR_z^2J) \in AUT(L)$ for all $z \in L$, then $xR_z^2 \cdot y = (xy)JR_z^2J$ for all $x,y,z \in L$ implies $(xz^2)\cdot y = [(xy)^{-1}z^2]^{-1}$. Whence $(xz^2)\cdot y = z^{-2}(xy)$, consequently $(xz^2)\cdot y = z^{-2}x \cdot y$. Thus $xz^2 = z^{-2}x$ which implies $z^4 = e$ for every $z \in L$. □

Theorem 4.2. *A C-loop $(L,\cdot)$ in which (I, L_z^2, JL_z^2J) and (R_z^2, I, JR_z^2J) lies in $AUT(L)$ is a central square C-loop of exponent 4.*

Proof. 1. If $(I, L_z^2, JL_z^2J) \in AUT(L)$ for all $z \in L$, then $x \cdot yL_z^2 = (xy)JL_z^2J$ for all $x,y,z \in L$ implies $x \cdot z^2y = xy \cdot z^{-2}$.

2. If $(R_z^2, I, JR_z^2J) \in AUT(L)$ for all $z \in L$, then $xR_z^2 \cdot y = (xy)JR_z^2J$ for all $x,y,z \in L$ implies $xz^2 \cdot y = z^{-2}(xy)$.

Therefore $x \cdot z^2y = xz^2 \cdot y$ if and only if $xy \cdot z^{-2} = z^{-2} \cdot xy$. Putting $t = xy$ we have $tz^{-2} = z^{-2}t$, i.e., $z^2t^{-1} = t^{-1}z^2$. Whence we conclude that

$z^2 \in C(L,\cdot)$ for all $z \in L$. Since C-loops are nuclear square (see [26]), we have $z^2 \in Z(L,\cdot)$. Hence L is a central square C-loop. By Theorem 4.1, $x^4 = e$. □

Corollary 4.1. *If $(I, L_z^2, JL_z^2J) \in AUT(L)$ and $(R_z^2, I, JR_z^2J) \in AUT(L)$ for a C-loop $(L,\cdot)$, then L is flexible, $(xy)^2 = (yx)^2$ for all $x, y \in L$ and $x \mapsto x^3$ is an anti-automorphism*

Proof. By Theorem 4.2, Lemma 5.1 and Corollary 5.2 of [21]. □

Theorem 4.3. *A central square C-loop of exponent 4 is a group.*

Proof. To prove this, it shall be shown that $R(x,y) = I$ for all $x, y \in L$. By Corollary 4.1, for $w \in L$ we get $wR(x,y) = wR_xR_yR_{xy}^{-1} = (wx)y \cdot (xy)^{-1} = (wx)(x^2yx^2) \cdot (xy)^{-1} = (wx^3)(yx^2) \cdot (xy)^{-1} = (w^2(w^3x^3))(yx^2) \cdot (xy)^{-1} = (w^2(xw)^3)(yx^2)\cdot(xy)^{-1} = w^2(xw)^3\cdot(yx^2)(xy)^{-1} = w^2(xw)^3\cdot[y\cdot x^2(xy)^{-1}] = w^2(xw)^3\cdot[y\cdot x^2(y^{-1}x^{-1})] = w^2(xw)^3\cdot[y(y^{-1}x^{-1}\cdot x^2)] = w^2(xw)^3\cdot[y(y^{-1}x)] = w^2(xw)^3 \cdot x = w^2(w^3x^3) \cdot x = w^2 \cdot (w^3x^3)x = w^2 \cdot (w^3x^{-1})x = w^2w^3 = w^5 = w$. So, $R(x,y) = I$, i.e., $R_xR_yR_{xy}^{-1} = I$. Thus $R_xR_y = R_{xy}$ and $zR_xR_y = zR_{xy}$. So, $zx \cdot y = z \cdot xy$. Therefore L is a group. □

Corollary 4.2. *A C-loop $(L,\cdot)$ in which for all $z \in L$ (I, L_z^2, JL_z^2J) and (R_z^2, I, JR_z^2J) are in $AUT(L)$ is a group.*

Proof. This follows from Theorem 4.2 and Theorem 4.3. □

Remark 4.1. Central square C-loops of exponent 4 are A-loops.

Theorem 4.4. *A C-loop is a central square loop if and only if $\gamma_2R_1 = I$.*

Proof. $\gamma_2R_1 = I \longleftrightarrow T(x^{-2}) = I$ for all $x \in L \longleftrightarrow R_{x^{-2}}L_{x^2} = I \longleftrightarrow yx^2 = x^2y \longleftrightarrow L$ is central square. □

Theorem 4.5. *Let L be a C-loop such that the mapping $x \mapsto T(x)$ is a bijection, then L is of exponent 2 if and only if $\gamma_2R_1 = I$.*

Proof. Indeed, $\gamma_2R_1 = I \longleftrightarrow T(x^{-2}) = I$ for all $x \in L \longleftrightarrow T(x^{-2}) = I = R_x^{-1}T(x^{-1})L_x \longleftrightarrow T(x^{-1}) = T(x) \longleftrightarrow x^{-1} = x$. Since $x \mapsto T(x)$ is a bijection L is a loop of exponent 2. □

Corollary 4.3. *A C-loop in which $x \mapsto T(x)$ is a bijection is a loop of exponent 2 if and only if it is central square.*

Proof. By Theorem 4.4 and Theorem 4.5. □

Corollary 4.4. *A central square C-loop in which the map $x \mapsto T(x)$ is a bijection is a Steiner loop.*

Proof. By the converse of Corollary 4.3, a C-loop in which $x \mapsto T(x)$ is a bijection, is of exponent 2 if it is central square. By the result of [26], an inverse property loop of exponent 2 is a Steiner loop. By the fact that C-loops are inverse property loops [26], it is a Steiner loop. □

Corollary 4.5. *A C-loop $(L,\cdot)$ in which $x \mapsto T(x)$ is a bijection and (I, L_z^2, JL_z^2J), (R_z^2, I, JR_z^2J) are in $AUT(L)$ for every $z \in L$, is a Steiner loop of exponent* 4.

Proof. According to Theorem 4.2, L is a central square loop. Since $x \mapsto T(x)$ is a bijection, by Corollary 4.4, L is a Steiner loop. By Theorem 4.1, it has a an exponent of 4. □

Corollary 4.6. *A C-loop L in which the mapping $x \mapsto T(x)$ is a bijection is a Steiner loop if and only if L is a central square C-loop.*

Proof. A Steiner loop L is a C-loop [26]. Steiner loops are loops of exponent two, hence by Corollary 4.3, L is central square since in L, the mapping $x \mapsto T(x)$ is a bijection. Conversely, by Corollary 4.3, a central square C-loop L in which the mapping $x \mapsto T(x)$ is a bijection is a loop of of exponent two. The fact that an inverse property loop of exponent two is a Steiner loop [26], completes the proof. □

4.1. Flexibility in C-loops

Lemma 4.1. *A C-loop is flexible if the mapping $x \mapsto x^2$ is onto.*

Proof. Let L be a C-loop . Then $yx^2 \cdot y = y \cdot x^2y$ for all $x, y \in L$. Thus, L is square flexible, hence by [12], it is flexible since the mapping $x \mapsto x^2$ is onto. □

Theorem 4.6. *A C-loop L is flexible if (I, L_z^2, JL_z^2J) and (R_z^2, I, JR_z^2J) are in $AUT(L)$ for all $z \in L$ and the middle inner mappings are of order* 2.

Proof. By Lemma 3.3, for every $x \in L$ we have $T(x)^2 = R_xT(x^{-1})^{-1}L_x^{-1} = R_x(R_xT(x^{-2})L_x^{-1})^{-1}L_x^{-1} = R_x(L_x(R_xT(x^{-2}))^{-1})L_x^{-1} = R_x(L_xT(x^{-2})^{-1}$ $R_x^{-1})L_x^{-1} = R_xL_xT(x^{-2})^{-1}R_x^{-1}L_x^{-1} = R_xL_xT(x^{-2})^{-1}(L_xR_x)^{-1}$. Therefore

$T(x)^2 = R_xL_xT(x^{-2})^{-1}(L_xR_x)^{-1} \longleftrightarrow T(x)^2L_xR_x = R_xL_xT(x^{-2})^{-1} = R_xL_x(\gamma_2R_1)^{-1} = R_xL_x\gamma_1R_2 \longleftrightarrow T(x)^2L_xR_x = R_xL_x\gamma_1R_2$. If $|T(x)| = 2$, $T(x)^2 = I$ and if $\gamma_1R_2 = I \longleftrightarrow L$ is central square, then $L_xR_x = R_xL_x \longleftrightarrow xy \cdot x = x \cdot yx$ is a flexible loop. □

Philips and Vojtěchovský [26] studied the close relationship between C-loops and Steiner loops. In [23], it is shown that Steiner loops are exactly commutative inverse property loops of exponent 2. But in [26], this fact was improved, so that commutativity is not a sufficient condition for an inverse property loop of exponent 2 to be a Steiner loop. So they said 'Steiner loops are exactly inverse property loops of exponent 2'. This result is general for inverse property loops among which are C-loops. They also proved that Steiner loops are C-loops.

The flexibility is possible in a C-loop if the loop is commutative or diassociative [23]. But C-loops naturally do not even satisfy the latter. Apart from the condition stated in Lemma 4.1, Theorem 4.6 when compared with Corollary 5.2 of [21] shows that some middle inner-mappings do not need to be of exponent of 2 for a C-loop to be flexible.

5. Unique non-identity commutator and associator

Lemma 5.1. *If s is a unique non-identity commutator in a C-loop L, then $|s| = 2$, $s \in C(L)$ and $s \in Z(L^2)$.*

Proof. $xy = (yx)(x, y) \longleftrightarrow (x, y) = (yx)^{-1}(xy) = (x^{-1}y^{-1})(xy)$. Therefore $(x, y)^{-1} = [(x^{-1}y^{-1})(xy)]^{-1} = (xy)^{-1}(x^{-1}y^{-1})^{-1} = (y^{-1}x^{-1})(yx) = (y, x)$. Thus, $s^{-1} = s$ or $s^{-1} = e$ implies $s^2 = e$ or $s = e$. So, $s^2 = e$.

If $xs \neq sx$, then $xs = (sx)s$ implies $x = sx$, whence $s = e$. So, $xs = sx$, i.e., $s \in C(L)$. Hence, $s \in Z(L^2)$. □

Lemma 5.2. *If s is a unique non-identity associator in a C-loop L, then $s \in N(L)$.*

Proof. If $(xy)s \neq x(ys)$, then $(xy)s = x(ys) \cdot s$ implies $xy = x \cdot ys$. Whence $y = ys$, i.e., $s = e$. So, $(xy)s = x(ys)$, that is, $s \in N(L)$. □

Lemma 5.3. *If a C-loop $(L, \cdot)$ has a unique non-identity commutator associator s, then s is a central element of order 2.*

Proof. We shall keep in mind that L as a C-loop has the inverse property. $s \in (L, L)$ implies $s^{-1} \in (L, L)$, whence $s^{-1} = s$. Since $s^{-1} \neq e$ if and only if $s \neq e$, we have $s^2 = e$. Let $xs \neq sx$ for some $x, y \in L$. Then $xs = (sx)s$ implies $x = sx$, i.e., $s = e$, which is a contradiction. Thus, $s \in C(L)$. If $(xy)s \neq x(ys)$ for some $x, y \in L$, then $(xy)s = (x \cdot ys)s$ implies $xy = x \cdot ys$. Thus $y = ys$, i.e, $s = e$, which is a contradiction. So, $s \in N(L)$. Therefore $s \in C(L)$, $s \in N(L)$ implies $s \in Z(L)$. □

Remark 5.1. The result of Lemma 5.3 is similar to the result proved in [16] for Moufang loops.

Lemma 5.4. *In $LC(RC)$-loops with a unique non-identity square s is $|s| = 2$, $|x| = 4$ or $|x| = 2$, $s \in N_\lambda$ or $s \in N_\rho$ and $s \in N_\mu$.*

Proof. For all $x \in L$ we have $x^2 = s$. Since $s^2 = s$ implies $s^{-1}s^2 = s^{-1}s$ or $s^2s^{-1} = ss^{-1}$, so $s = e$. This is a contradiction, thus $s^2 = e$ if and only if $|s| = 2$. Moreover, $x^2 = s$ implies $x^4 = x^2x^2 = s^2 = e$. Therefore $x^4 = e$ or $x^2 = e$. In any LC-loop, $x^2 \in N_\lambda$, N_μ, thus $s \in N_\lambda$, N_μ. In an RC-loop, $x^2 \in N_\rho, N_\mu$, thus $s \in N_\rho, N_\mu$. □

Lemma 5.5. *An $LC(RC)$-loop L has a unique non-identity square s if and only if $J = R_s^{-1} = R_{s^{-1}}^{-1}$ or $J = I$ (resp. $J = L_s^{-1} = L_{s^{-1}}^{-1}$ or $J = I$).*

Proof. Let L be a RC-loop. Then $x^2 = s \longleftrightarrow x^2x^{-1} = sx^{-1} \longleftrightarrow x = sx^{-1} \longleftrightarrow x = xJL_s \longleftrightarrow I = JL_s \longleftrightarrow J = L_s^{-1} = L_{s^{-1}}^{-1}$. Similarly, $x^2 = e \longleftrightarrow x = x^{-1} \longleftrightarrow x = xJ \longleftrightarrow J = I$.

For LC-loops the proof is analogous. □

Theorem 5.1. *For any L.I.P. (R.I.P.) $RC(LC)$-loop $(L, \cdot)$ with a unique non-identity square s,*

1. $s \in Z(L, \cdot)$, *i.e., L is centrum square,*
2. $J = L_s$ *(resp.* $J = R_s$*),*
3. $x^2y^2 \neq (xy)^2 \neq y^2x^2$, *i.e., $x \mapsto x^2$ is neither an automorphism nor an anti-automorphism,*
4. $(a, b, c) = (bc \cdot a)(ab \cdot c)$,
   - (a) $ab = a^{-1}b^{-1}$ *if and only if* $(J, J, I) \in AUT(L)$,
   - (b) $(a, b, a) = (bs)(ab \cdot a)$ *or* $(a, b, a) = b(ab \cdot a)$,
5. *L is a group or Steiner loop,*

6. *If L is a non-commutative C-loop, then s is its unique non-identity commutator.*

Proof. 1. $x^2 = s$ implies $x = sx^{-1}$, whence $x^{-1} = s^{-1}x$. This, by Lemma 2.1 from [1], gives $x^{-1} = (sx^{-1})^{-1} = (x^{-1})^{-1}s^{-1} = xs^{-1}$. Thus, $x^{-1} = s^{-1}x = xs^{-1}$, i.e., $sx = xs$. So, $s \in Z(L, \cdot)$.

2. This follows from Lemma 5.5.

3. If $(xy)^2 = x^2y^2$ or $(xy)^2 = y^2x^2$, then $s = s^2$ implies $s = e$ which is a contradiction.

4. $(a, b, c) = [a(bc)]^{-1} \cdot (ab)c = (bc)^{-1}a^{-1} \cdot (ab)c = (c^{-1}b^{-1})a^{-1} \cdot (ab \cdot c) = [s^{-1}(bc)](s^{-1}a) \cdot (ab \cdot c) = (bc \cdot s^{-1})(s^{-1}a) \cdot (ab \cdot c) = (bcs^{-2} \cdot a)(ab \cdot c) = (bc \cdot a)(ab \cdot c)$. So, $(a, b, c) = (bc \cdot a)(ab \cdot c)$.

4a. The above for $c = e$ gives $(a, b, e) = (ba)(ab) = e$, whence $ab = (ba)^{-1} = a^{-1}b^{-1}$. So, $(J, J, I) \in AUT(L)$.

4b. For $c = a$ we have $(a, b, a) = (ba \cdot a)(ab \cdot a) = (ba^2)(ab \cdot a) = (bs)(ab \cdot a)$. Thus $(a, b, a) = (bs)(ab \cdot a)$ or $(a, b, a) = b(ab \cdot a)$.

5. This follows from Lemma 5.4.

6. $(x, y) = x^{-1}y^{-1} \cdot xy = (x^{-1}y^{-1})(xy^{-1} \cdot y^2) = ((x^{-1}y^{-1})(xy^{-1}) \cdot y^2 = [x^{-2}(xy^{-1}) \cdot (xy^{-1})]y^2 = x^{-2}[(xy^{-1})(xy^{-1})]y^2 = e$ or $(x, y) = s$. Thus, L is either commutative or s is its unique non-identity commutator.

For $(x, s) = x^{-1}s^{-1} \cdot xs = s$ we have $x^{-1}R_s \cdot xR_s = s$, whence $xJ^2 \cdot x^{-1} = s$. Thus $xx^{-1} = s$, i.e., $s = e$, which is a contradiction. So. $(x, s) = e$ implies $s \in C(L, \cdot)$. □

Corollary 5.1. *A C-loop with a unique non-trivial square is a group.*

Proof. By Lemma 5.4 and Theorem 5.1, it is central square of exponent 4. By Theorem 4.3, it is a group. □

Remark 5.2. A C-loop with a unique non-trivial square is an A-loop.

Theorem 5.2. *Let $(G, \cdot)$ and $(H, \circ)$ be two distinct loop such that the triple $\alpha = (A, B, C)$ is an isotopism of G onto H.*

1. *If G is a central square C-loop of exponent 4, then H is a C-loop and an A-loop.*

2. *If G is a C-loop with a unique non-identity square, then H is a C-loop and an A-loop.*

Proof. 1. By Theorem 4.3, G is a group and since groups are G-loops, H is a group, i.e., it is a C-loop and an A-loop.

2. By Corollary 5.1. □

Remark 5.3. Some results for isotopes of central loops of the type (A, B, B) and (A, B, A) are obtained in [18].

Corollary 5.2. *Let $(G, \cdot)$ and $(H, \circ)$ be distinct loops. If the triple (A, B, C) is an isotopism of G onto H such that for every $z \in G$ (I, L_z^2, JL_z^2J) and (R_z^2, I, JR_z^2J) are in $AUT(G, \cdot)$, then H is a C-loop and an A-loop.*

Proof. It follows from Theorem 4.2 and Theorem 5.2. □

Theorem 5.3. *An isotopism (A, A, C) saves the property "unique non-identity square".*

Proof. Let $(A, A, C) : (G, \cdot) \to (H, \circ)$, where G and H are two distinct loops, be an isotopism. Then $xA \circ yA = (x \cdot y)C$. For $y = x$ we have $xA \circ xA = (xA)^2 = (x \cdot x)C = x^2C$. If s is the unique non-identity square in G, i.e $x^2 = s$ or $x^2 = e$ for all $x \in G$ then $s' = sC = (xA)^2 = y'^2$ or $y'^2 = (xA)^2 = x^2C = eC = e'$ for all $y' \in H$ with e' as the identity element in H. So, s' is the unique non-identity square element in H. □

Corollary 5.3. *Central loops with unique non-identity square are isotopic invariant.* □

6. Cross inverse property in central loops

According to [5], the W.I.P. is a generalization of the C.I.P. The latter was introduced and studied by R. Artzy [3] and [4], but from the formal point of view this property was introduced by J. M. Osborn [22]. Huthnance Jr. [17], proved that the holomorph of a W.I.P.L. is a W.I.P.L. A loop property is called *universal* (or universal relative to a given property) if every loop isotope of this loop is a loop with this property. A universal W.I.P.L. is called an *Osborn loop*. Huthnance Jr. [17] investigated the structure of some holomorph of Osborn loops. Basarab [6] studied Osborn loops which are G-loops.

Theorem 6.1. *An $LC(RC)$-loop of exponent 3 is centrum square if and only if it is a C.I.P.L.*

Proof. Let L be a LC-loop. Then $x^2y = yx^2 \longleftrightarrow x^{-1}y = yx^{-1} \longleftrightarrow x(x^{-1}y) = x(yx^{-1}) \longleftrightarrow y = x(yx^{-1})$, which holds if and only if the C.I.P. holds in L.

For RC-loops the proof is analogous. □

Corollary 6.1. *If L is a centrum square $LC(RC)$-loop of exponent 3, then*

1. *L has the A.I.P. and A.A.I.P.,*
2. *L has the W.I.P.,*
3. *$N = N_\lambda = N_\rho = N_\mu$,*
4. *$n \in N$ implies $n \in Z(L)$,*
5. *L is a commutative group.*

Proof. 1. By Theorem 6.1, L is a C.I.P.L. According to [4] and [5], a C.I.P.L. has the A.I.P. Thus, the first part is true. The second part follows from the fact that $x^2 = x^{-1}$.

2. This follows from the the fact that W.I.P. is a generalization of C.I.P. [23].

3. and 4. follows from [5] and [4]. The last statement is obvious. □

Lemma 6.1. *Any $LC(RC, C)$-loop of exponent 3 is a group.* □

Corollary 6.2. *A central square C-loop of exponent 3 has the W.I.P. and C.I.P. and it a commutative group.* □

The fact that central loops of exponent 3 are groups it will be interesting to study non-commutative central loops of exponent 3 with the C.I.P. since there exist groups that do not have the C.I.P. From Theorem 6.1, it follows that the study of LC(RC)-loops of exponent 3 with C.I.P. is equivalent to the study of centrum square LC(RC)-loops of exponent 3.

The existence of central loops of exponent 3 can be deduced from [15], [26] and [27]. According to [26] and [27], the order of every element in a finite LC(RC)-loop divides the order of the loop. Since $|x| = 3$ for all $x \in L$, then

$|L| = 2m$, $m \geqslant 3$ if L is a non-left (right) Bol LC(RC)-loop, or

$|L| = 4k$, $k > 2$ if L is a non-Moufang but both left (right)-Bol and LC(RC)-loop.

The possible orders of finite RC-loops were calculated in [27].

6.1. Osborn central-loops

Theorem 6.2. *An LC(RC)-loop has the R.I.P. (L.I.P.) if and only if has the W.I.P.*

Proof. Let $(L, \cdot)$ be a LC-loop with the W.I.P. Then for all $x, y \in L$, $y(xy)^\rho = x^\rho$. Let $xy = z$, then $x^\lambda(xy) = x^\lambda z$ implies $y = x^\lambda z$, thus $(x^\lambda z)z^\rho = x^\rho$ implies $(x^{-1}z)z^\rho = x^{-1}$. Replacing x^{-1} by x, we obtain $(xz)z^\rho = x$. So, L has the R.I.P.

Conversely, if L has the I.P., then $y(xy)^\rho = y(xy)^{-1} = y(y^{-1}x^{-1}) = x^{-1} = x^\rho$ hence it has the W. I. P. Let L be a RC-loop with the W.I.P. Then for all $x, y \in L$, $y(xy)^\rho = x^\rho$ if and only if $(xy)^\lambda \cdot x = y^\lambda$. Let $xy = z$, then $(xy)y^\rho = zy^\rho$ implies $x = zy^\rho$. Thus, $z^\lambda(zy^\rho) = y^\lambda$ implies $z^\lambda(zy^{-1}) = y^{-1}$. Replacing y^{-1} by y, we get $z^\lambda(zy) = y$. Thus, L has the L.I.P. □

Corollary 6.3. *Let $(L, \cdot)$ be an LC(RC)-loop with R.I.P. (L.I.P.). Then*

1. $N(L) = N_\lambda(L) = N_\rho(L) = N_\mu(L)$,
2. $(I, R_{x^2}, R_{x^2}) \in AUT(L)$ *(resp.* $(L_{x^2}, I, L_{x^2}) \in AUT(L)$*)*,
3. $(L_x^2, R_{x^2}, R_{x^2}L_x^2) \in AUT(L)$ *(resp.* $(L_{x^2}, R_x^2, L_{x^2}R_x^2) \in AUT(L)$*)*.

Proof. By Theorem 6.2, L has the W.I.P. According to [22], in a W.I.P.L., the three nuclei coincide, so the firs statement is true. Thus for an LC-loop, $x^2 \in N_\rho$ and for an RC-loop, $x^2 \in N_\lambda$. Hence for an LC-loop L, $(L_x^2, I, L_x^2), (I, R_{x^2}, R_{x^2}) \in AUT(L)$ implies that $(L_x^2, R_{x^2}, L_x^2 R_{x^2}) = (L_x^2, R_{x^2}, R_{x^2}L_x^2) \in AUT(L)$. For an RC-loop L, $(I, R_x^2, R_x^2), (L_{x^2}, I, L_{x^2}) \in AUT(L)$ implies $(L_{x^2}, R_x^2, R_x^2 L_{x^2}) = (L_{x^2}, R_x^2, L_{x^2}R_x^2) \in AUT(L)$. So, the last two statement are true, too. □

Remark 6.1. Corollary 6.3 is true for left (right) Bol loops (i.e., LB(RB)-loops). It follows from the fact that a RB(LB)-loop has the L.I.P. (R.I.P.) if and only if it is a Moufang loop [23], which is obviously a W.I.P.L. [19].

Theorem 6.3. *An LC(RC)-loop L is a C-loop if and only if one of the following equivalent statements holds:*

1. *L has the R.I.P. (L.I.P.),*
2. *L has the R.A.P. (L.A.P.),*
3. *L is a RC(LC)-loop,*
4. *L has the A.A.I.P. (i.e., $(xy)^{-1} = y^{-1}x^{-1}$),*

5. *L has the W.I.P.*

Proof. A C-loop satisfies 1 and 2. Conversely, if L is an LC-loop, then $(x{\cdot}xy)z = x(x{\cdot}yz)$, whence $[(x{\cdot}xy)z]^{-1} = [x(x{\cdot}yz)]^{-1}$. Thus $z^{-1}(x{\cdot}xy)^{-1} = (x \cdot yz)^{-1}x^{-1}$ and consequently $z^{-1}((xy)^{-1} \cdot x^{-1}) = ((yz)^{-1} \cdot x^{-1})x^{-1}$, i.e., $z^{-1}(y^{-1}x^{-1}{\cdot}x^{-1}) = (z^{-1}y^{-1}{\cdot}x^{-1})x^{-1}$, which means that $z(yx{\cdot}x) = (zy{\cdot}x)x$ for all $x, y, z \in L$. So, a RC-loop. Hence, L is a C-loop.

If L is an LC-loop, then according to [26], $x \cdot (y \cdot yz) = (x \cdot yy)z$ for all $x, y, z \in L$, while L is an RC-loop if and only if $(zy \cdot y)x = z(yy \cdot x)$ for all $x, y, z \in L$. Thus $x \cdot (y \cdot yz) = (x \cdot yy)z$, or equivalently $x \cdot zL_y^2 = xR_{y^2} \cdot z$. So, $(R_{y^2}, L_y^{-2}, I) \in AUT(L)$ for all $y \in L$. For $(zy \cdot y)x = z(yy \cdot x)$ we have $zR^2 \cdot x = z \cdot xL_{y^2}$, i.e., $(R_y^2, L_{y^2}^{-1}, I) \in AUT(L)$ for all $y \in L$.

If L has the right (left) alternative property, $(R_y^2, L_y^{-2}, I) \in AUT(L)$ for all $y \in L$ if and only if L is a C-loop.

3. This is shown in [15].

4. This is equivalent to 1. Indeed, if L has the L.I.P. (R.I.P.), then L has the R.I.P. (L.I.P.). so, L has the A.A.I.P. Conversely, if L.I.P. holds, then for $z = xy$, we have $y = x^{-1}z$ which gives $z^{-1} = (x^{-1}z)^{-1}x^{-1}$, whence $z^{-1} = (z^{-1}x)x^{-1}$. So, $z = (zx)x^{-1}$.

Similarly, if L has the R.I.P. (L.I.P.) then L has the L.I.P. (R.I.P.), i.e., it has the A.A.I.P. Conversely, if R.I.P. holds, then for $z = xy$, we have $x = zy^{-1}$. Thus, $z^{-1} = y^{-1}(zy^{-1})^{-1} = y^{-1}(yz^{-1})$, which proves the L.I.P.

5. This follows from 1 and Theorem 6.2. □

Theorem 6.4. (cf. [19]) *The following equivalent conditions define an Osborn loop $(L, \cdot)$.*

1. $x(yz \cdot x) = (x \cdot yE_x) \cdot zx$,
2. $(x \cdot yz)x = xy \cdot (zE_x^{-1} \cdot x)$,
3. $(A_x, R_x, R_xL_x) \in AUT(L)$,
4. $(L_x, B_x, L_xR_x) \in AUT(L)$,

where $A_x = E_xL_x$, $B_x = E_x^{-1}R_x$ and $E_x = R_xL_xR_x^{-1}L_x^{-1}$. □

Theorem 6.5. *If a RC(LC)-loop has the L.I.P. (R.I.P.), then it is an Osborn loop if every its element is a square.*

Proof. Let L be an RC-loop with L.I.P. Then, by Theorem 6.2, L has the W.I.P. Therefore $(A_{x^2}, I, L_{x^2}) \in AUT(L) \longleftrightarrow yA_{x^2} \cdot z = (yz)L_{x^2}$. But

$(yz)L_{x^2} = yE_{x^2}L_{x^2} \cdot z = yR_{x^2}L_{x^2}R_{x^2}^{-1}L_{x^2}^{-1}L_{x^2} \cdot z = yR_{x^2}L_{x^2}R_{x^2}^{-1} \cdot z = yR_x^2L_{x^2}R_{x^2}^{-1} \cdot z = yL_{x^2}R_x^2R_{x^2}^{-1} \cdot z = yL_{x^2} \cdot z$. This is equivalent to the fact that $(L_{x^2}, I, L_{x^2}) \in AUT(L)$ for all $x \in L$, which is true by Corollary 6.3.

Thus, $(I, R_x^2, R_x^2)(A_{x^2}, I, L_{x^2}) = (A_{x^2}, R_{x^2}, R_{x^2}L_{x^2}) \in AUT(L)$. Using Theorem 6.4, we see that L is an Osborn loop if every element in L is a square.

Now, let L be an LC-loop. If L has the R.I.P., then, by Theorem 6.2, L has the W.I.P. So, $(I, B_{x^2}, R_{x^2}) \in AUT(L)$ if and only if $y \cdot zB_{x^2} = (yz)R_{x^2}$. But $(yz)R_{x^2} = y \cdot zE_{x^2}^{-1}R_{x^2} = y \cdot z(R_{x^2}L_{x^2}R_{x^2}^{-1}L_{x^2}^{-1})^{-1}R_{x^2} = y \cdot zL_{x^2}R_{x^2}L_{x^2}^{-1}R_{x^2}^{-1}R_{x^2} = y \cdot zL_{x^2}R_{x^2}L_{x^2}^{-1} = y \cdot zR_{x^2}L_x^2L_{x^2}^{-1} = y \cdot zR_{x^2}$. This is equivalent to the fact that $(I, R_{x^2}, R_{x^2}) \in AUT(L)$ for all $x \in L$, which is true by Corollary 6.3.

Thus, $(L_x^2, I, L_x^2)(I, B_{x^2}, R_{x^2}) = (L_{x^2}, B_{x^2}, L_{x^2}R_{x^2}) \in AUT(L)$. Whence, as in previous case, we conclude that L is an Osborn loop if every element in L is a square. □

Corollary 6.4. *An LC(RC)-loop with R.I.P. (L.I.P.) is an Osborn loop if every its element is a square. Hence, this loop is a group.*

Proof. This follows from Theorem 6.5. The last conclusion is as a consequence of the fact that $x^2 \in N(L)$. □

Corollary 6.5. *A C-loop is an Osborn loop if every its element is a square. Hence, this loop is a group.* □

Question. *Does there exist a C-loop which is an Osborn loop but it is non-associative, non Moufang and non-conjugacy closed?*

Acknowledgement. J.O.Adéníran would like to express his profound gratitude to the Swedish International Development Cooperation Agency (SIDA) for the support for this research under the framework of the Associateship Scheme of the Abdus Salam International Centre for theoretical Physics, Trieste, Italy.

References

[1] **J. O. Adéníran and A. R. T. Solarin:** *A note on automorphic inverse property loops*, Collections of Scientific Papers of the Faculty of Science Krag., **20** (1998), 47 – 52.

[2] **J. O. Adéníran and A. R. T. Solarin:** *A note on generalized Bol identity*, Scientific Annals of Al.I.Cuza. Univ. **45** (1999), 99 – 102.

[3] **R. Artzy:** *On loops with special property*, Proc. Amer. Math. Soc. **6** (1955), 448 – 453.

[4] **R. Artzy:** *Crossed inverse and related loops*, Trans. Amer. Math. Soc. **91** (1959), 480 – 492.

[5] **R. Artzy:** *Relations between loops identities*, Proc. Amer. Math. Soc. **11** (1960), 847 – 851.

[6] **A. S. Basarab:** *Osborn's G-loop*, Quasigroups and Related Systems **1** (1994), 51 – 56.

[7] **A. Beg:** *A theorem on C-loops*, Kyungpook Math. J. **17** (1977), 91 – 94.

[8] **A. Beg:** *On LC-, RC-, and C-loops*, Kyungpook Math. J. **20** (1980), 211 – 215.

[9] **R. H. Bruck:** *A survey of binary systems*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1966.

[10] **O. Chein:** *A short note on supernuclear (central) elements of inverse property loops*, Arch. Math. **33** (1979), 131 – 132.

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

[12] **V. O. Chiboka:** *Conjugacy closed loops of Moufang type*, Riv. Mat. Pura Appl. **10** (1991), 89 – 93.

[13] **J. Dénes and A. D. Keedwell:** *Latin Squares and their Applications*, the English University press Lts, 1974.

[14] **F. Fenyves:** *Extra Loops I*, Publ. Math. Debrecen **15** (1968), 235 – 238.

[15] **F. Fenyves:** *Extra Loops II*, Publ. Math. Debrecen **16** (1969), 187 – 192.

[16] **E. G. Goodaire, E. Jespers and C. P. Milies:** *Alternative Loop Rings*, NHMS(184), Elsevier, 1996.

[17] **E. D. Huthnance Jr.:** *A theory of generalised Moufang loops*, Ph.D. thesis, Georgia Institute of Technology, 1968.

[18] **T. G. Jaiyéolá and J. O. Adéníran:** *On isotopic characterisation of C-loops*, Pre-Print.

[19] **M. K. Kinyon:** *A survey of Osborn loops*, Milehigh conference on loops, quasigroups and non-associative systems, University of Denver, Denver, Colorado, 2005.

[20] **M. K. Kinyon, K. Kunen and J. D. Phillips:** *A generalization of Moufang and Steiner loops*, Alg. Universalis **48** (2002), 81 – 101.

[21] **M. K. Kinyon, J. D. Phillips and P. Vojtěchovský:** *C-loops: Extensions and construction*, J. Algebra Appl. **6** (2007), 1 – 20.

[22] **J. M. Osborn:** *Loops with the weak inverse property*, Pac. J. Math. **10** (1961), 295 – 304.

[23] **H. O. Pflugfelder:** *Quasigroups and Loops: Introduction*, Sigma series in Pure Math. 7, Heldermann Verlag, Berlin, 1990.

[24] **J. D. Phillips and P. Vojtěchovský:** *The varieties of loops of Bol-Moufang type*, Alg. Universalis **53** (2005), 115 – 137.

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

[26] **J. D. Phillips and P. Vojtěchovský:** *On C-loops*, Publ. Math. Debrecen **68** (2006), 115 – 137.

[27] **V. S. Ramamurthi and A. R. T. Solarin:** *On finite right central loops*, Publ. Math. Debrecen, **35** (1988), 261 – 264.

[28] **A. R. T. Solarin:** *On the identities of Bol-Moufang type*, Koungpook Math. J., **28** (1998), 51 – 62.

[29] **A. R. T. Solarin:** *On certain Akivis algebra*, Italian J. Pure Appl. Math. **1** (1997), 85 – 90.

[30] **A. R. T. Solarin and V. O. Chiboka:** *A note on G-loops*, Collections of Scientific Papers of the Faculty of Science Krag., **17** (1995), 17 – 26.

Received September 17, 2006
Revised February 8, 2007

T. G. Jaiyéọlà
Department of Mathematics, Obafemi Awolowo University, Ilé Ifè, Nigeria
E-mail: jaiyeolatemitope@yahoo.com

J. O. Adéníran
Department of Mathematics, University of Abẹókùta, Abẹókùta 110101, Nigeria
E-mail: ekenedilichineke@yahoo.com

Quasigroups and Related Systems **16** (2008), 55 – 67

On reconstructing reducible n-ary quasigroups and switching subquasigroups

Denis S. Krotov, Vladimir N. Potapov, Polina V. Sokolova

Abstract

(1) We prove that, provided $n \geqslant 4$, a permutably reducible n-ary quasigroup is uniquely specified by its values on the n-ples containing zero. (2) We observe that for each $n, k \geqslant 2$ and $r \leqslant \lfloor k/2 \rfloor$ there exists a reducible n-ary quasigroup of order k with an n-ary subquasigroup of order r. As corollaries, we have the following: (3) For each $k \geqslant 4$ and $n \geqslant 3$ we can construct a permutably irreducible n-ary quasigroup of order k. (4) The number of n-ary quasigroups of order $k > 3$ has double-exponential growth as $n \to \infty$; it is greater than $\exp\exp(n \ln\lfloor k/3 \rfloor)$ if $k \geqslant 6$, and $\exp\exp(\frac{\ln 3}{3}n - 0.44)$ if $k = 5$.

1. Introduction

An n-ary operation $f : \Sigma^n \to \Sigma$, where Σ is a nonempty set, is called an *n-ary quasigroup* or *n-quasigroup* (*of order* $|\Sigma|$) iff in the equality $z_0 = f(z_1, \ldots, z_n)$ knowledge of any n elements of z_0, z_1, …, z_n uniquely specifies the remaining one [2].

An n-ary quasigroup f is *permutably reducible* iff

$$f(x_1, \ldots, x_n) = h\left(g(x_{\sigma(1)}, \ldots, x_{\sigma(k)}), x_{\sigma(k+1)}, \ldots, x_{\sigma(n)}\right)$$

where h and g are $(n-k+1)$-ary and k-ary quasigroups, σ is a permutation, and $1 < k < n$. In what follows we omit the word "permutably" because we consider only such type of reducibility.

2000 Mathematics Subject Classification: 20N15 05B15
Keywords: irreducible quasigroups, latin hypercubes, n-ary quasigroups, reducibility, subquasigroup
The first and the second authors were partially supported by the Russian Foundation for Basic Research (Grants 08-01-00673 and 08-01-00671 respectively)

We will use the following standard notation: x_i^j denotes $x_i, x_{i+1}, \ldots, x_j$.

In Section 2 we show that a reducible n-quasigroup can be reconstructed by its values on so-called 'shell'. 'Shell' means the set of variable values with at least one zero.

In Section 3 we consider the questions of imbedding n-quasigroups of order r into n-quasigroups of order $k \geqslant 2r$.

In Section 4 we prove that for all $n \geqslant 3$ and $k \geqslant 4$ there exists an irreducible n-quasigroup of order k. Before, the question of existence of irreducible n-quasigroups was considered by Belousov and Sandik [3] ($n = 3$, $k = 4$), Frenkin [5] ($n \geqslant 3$, $k = 4$), Borisenko [4] ($n \geqslant 3$, composite finite k), Akivis and Goldberg [7, 8, 1] (local differentiable n-quasigroups), Glukhov [6] ($n \geqslant 3$, infinite k).

In Sections 5 and 6 we prove the double-exponential ($\exp\exp(c(k)n)$) lower bound on the number $|Q(n,k)|$ of n-quasigroups of finite order $k \geqslant 4$. Before, the following asymptotic results on the number of n-quasigroups of fixed finite order k were known:

- $|Q(n,2)| = 2$.
- $|Q(n,3)| = 3 \cdot 2^n$, see, e.g., [13]; a simple way to realize this fact is to show by induction that the values on the shell uniquely specify an n-quasigroup of order 3.
- $|Q(n,4)| = 3^{n+1}2^{2^n+1}(1 + o(1))$ [15, 11].

Note that by the "number of n-quasigroups" we mean the number of mutually different n-ary quasigroup operations $\Sigma^n \to \Sigma$ for a fixed Σ, $|\Sigma| = k$ (sometimes, by this phrase one means the number of isomorphism classes). As we will see, for every $k \geqslant 4$ there is $c(k) > 0$ such that $|Q(n,k)| \geqslant 2^{2^{c(k)n}}$. More accurately (Theorem 3), if $k = 5$ then $|Q(n,5)| \geqslant 2^{3^{n/3-const}}$; for even k we have $|Q(n,k)| \geqslant 2^{(k/2)^n}$; for $k \equiv 0 \bmod 3$ we have $|Q(n,k)| \geqslant 2^{n(k/3)^n}$; and for every k we have $|Q(n,k)| \geqslant 2^{1.5\lfloor k/3\rfloor^n}$. Observe that dividing by the number (e.g., $(n+1)!(k!)^n$) of any natural equivalences (isomorphism, isotopism, paratopism,...) does not affect these values notably; so, for the number of equivalence classes almost the same bounds are valid. For the known exact numbers of n-quasigroups of order k with small values of n and k, as well as the numbers of equivalence classes for different equivalences, see the recent paper of McKay and Wanless [14].

2. On reconstructing reducible n-quasigroups

In what follows the constant tuples $\bar{o}$, $\bar{\theta}$ may be considered as all-zero tuples. From this point of view, the main result of this section states that a reducible n-quasigroup is uniquely specified by its values on the 'shell', where the 'shell' is the set of n-ples with at least one zero. Lemma 1 and its corollary concern the case when the groups of variables in the decomposition of a reducible n-quasigroup are fixed. In Theorem 1 the groups of variables are not specified; we have to require $n \geqslant 4$ in this case.

Lemma 1 (a representation of a reducible n-quasigroup by the superposition of retracts). *Let h and g be an $(n-m+1)$- and m-quasigroups, let $\bar{o} \in \Sigma^{m-1}$, $\bar{\theta} \in \Sigma^{n-m}$, and let*

$$f(x,\bar{y},\bar{z}) \stackrel{\text{def}}{=} h(g(x,\bar{y}),\bar{z}),$$
$$h_0(x,\bar{z}) \stackrel{\text{def}}{=} f(x,\bar{o},\bar{z}), \qquad g_0(x,\bar{y}) \stackrel{\text{def}}{=} f(x,\bar{y},\bar{\theta}), \qquad \delta(x) \stackrel{\text{def}}{=} f(x,\bar{o},\bar{\theta}) \quad (1)$$

where $x \in \Sigma$, $\bar{y} \in \Sigma^{m-1}$, $\bar{z} \in \Sigma^{n-m}$. Then

$$f(x,\bar{y},\bar{z}) \equiv h_0(\delta^{-1}(g_0(x,\bar{y})),\bar{z}). \qquad (2)$$

Proof. It follows from (1) that

$$h_0(\cdot,\bar{z}) \equiv h(g(\cdot,\bar{o}),\bar{z}), \quad g_0(x,\bar{y}) \equiv h(g(x,\bar{y}),\bar{\theta}), \quad \delta^{-1}(\cdot) \equiv g^{-1}(h^{-1}(\cdot,\bar{\theta}),\bar{o}).$$

Substituting these representations of h_0, g_0, δ^{-1} to (2), we can readily verify its validity. ☐

Corollary 1. *Let $q_{in}, q_{out}, f_{in}, f_{out} : \Sigma^2 \to \Sigma$ be some quasigroups, $q \stackrel{\text{def}}{=} q_{out}(x_1, q_{in}(x_2,x_3))$, $f \stackrel{\text{def}}{=} f_{out}(x_1, f_{in}(x_2,x_3))$, and $(o_1,o_2,o_3) \in \Sigma^3$. Assume that for all $(x_1,x_2,x_3) \in \Sigma^3$ it holds*

$$q(o_1,x_2,x_3) = f(o_1,x_2,x_3), \quad q(x_1,o_2,x_3) = f(x_1,o_2,x_3).$$

Then $q(\bar{x}) = f(\bar{x})$ for all $\bar{x} \in \Sigma^3$.

Theorem 1. *Let $q, f : \Sigma^n \to \Sigma$ be reducible n-quasigroups, where $n \geqslant 4$; and let $o_1^n \in \Sigma^n$. Assume that for all $i \in \{1,\ldots,n\}$ and for all $x_1^n \in \Sigma^n$ it holds*

$$q(x_1^{i-1}, o_i, x_{i+1}^n) = f(x_1^{i-1}, o_i, x_{i+1}^n). \qquad (3)$$

Then $q(x_1^n) = f(x_1^n)$ for all $x_1^n \in \Sigma^n$.

Proof. (*) We first proof the claim for $n = 4$. Without loss of generality (up to coordinate permutation and/or interchanging q and f), we can assume that one of the following holds for some quasigroups $q_{in}, q_{out}, f_{in}, f_{out}$:

Case 1) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3, x_4))$, $f(x_1^4) = f_{out}(x_1, f_{in}(x_2, x_3, x_4))$;
Case 2) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3, x_4))$, $f(x_1^4) = f_{out}(x_1, f_{in}(x_2, x_3), x_4)$;
Case 3) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3), x_4)$, $f(x_1^4) = f_{out}(x_1, f_{in}(x_2, x_3), x_4)$;
Case 4) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3, x_4))$, $f(x_1^4) = f_{out}(f_{in}(x_1, x_2, x_3), x_4)$;
Case 5) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3, x_4))$, $f(x_1^4) = f_{out}(f_{in}(x_1, x_4), x_2, x_3)$;
Case 6) $q(x_1^4) = q_{out}(x_1, x_2, q_{in}(x_3, x_4))$, $f(x_1^4) = f_{out}(x_1, f_{in}(x_2, x_3), x_4)$;
Case 7) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3), x_4)$, $f(x_1^4) = f_{out}(f_{in}(x_1, x_4), x_2, x_3)$.

1,2,3) Take an arbitrary x_4 and denote $q'(x_1, x_2, x_3) \stackrel{\text{def}}{=} q(x_1, x_2, x_3, x_4)$ and $f'(x_1, x_2, x_3) \stackrel{\text{def}}{=} f(x_1, x_2, x_3, x_4)$. Then, by Corollary 1, we have $q'(\bar{x}) = f'(\bar{x})$ for all $\bar{x} \in \Sigma^3$; this proves the statement.

4) Fixing $x_4 := o_4$ and applying (3) with $i = 4$, we have

$$f_{out}(f_{in}(x_1, x_2, x_3), o_4) = q_{out}(x_1, q_{in}(x_2, x_3, o_4)),$$

which leads to the representation $f_{in}(x_1, x_2, x_3) = h_{out}(x_1, h_{in}(x_2, x_3))$ where $h_{out}(x_1, \cdot) \stackrel{\text{def}}{=} f_{out}^{-1}(q_{out}(x_1, \cdot), o_4)$ and $h_{in}(x_2, x_3) \stackrel{\text{def}}{=} q_{in}(x_2, x_3, o_4)$. Using this representation, we find that f satisfies the condition of Case 2) for some f_{in}, f_{out}. So, the situation is reduced to the already-considered case.

5) Fixing $x_4 := o_4$ and using (3), we obtain the decomposition $f_{out}(\cdot, \cdot, \cdot) = h_{out}(\cdot, h_{in}(\cdot, \cdot))$ for some h_{in}, h_{out}. We find that q and f satisfy the conditions of Case 2).

6) Fixing $x_4 := o_4$ and using (3), we get the decomposition $q_{out}(\cdot, \cdot, \cdot) = h_{out}(\cdot, h_{in}(\cdot, \cdot))$. Then, we again reduce to Case 2).

7) Fixing $x_4 := o_4$ we derive the decomposition $f_{out}(\cdot, \cdot, \cdot) = h_{out}(\cdot, h_{in}(\cdot, \cdot))$, which leads to Case 3).

(**) Assume $n > 4$. It is straightforward to show that we always can choose four indexes $1 \leqslant i < j < k < l \leqslant n$ such that for all x_1^{i-1}, x_{i+1}^{j-1}, x_{j+1}^{k-1}, x_{k+1}^{l-1}, x_{l+1}^n the 4-quasigroups

$$q'_{x_1^{i-1} x_{i+1}^{j-1} x_{j+1}^{k-1} x_{k+1}^{l-1} x_{l+1}^n}(x_i, x_j, x_k, x_l) \stackrel{\text{def}}{=} q(x_1^n),$$
$$f'_{x_1^{i-1} x_{i+1}^{j-1} x_{j+1}^{k-1} x_{k+1}^{l-1} x_{l+1}^n}(x_i, x_j, x_k, x_l) \stackrel{\text{def}}{=} f(x_1^n)$$

are reducible. Since these 4-quasigroups satisfy the hypothesis of the lemma, they are identical, according to (*). Since they coincide for every values of the parameters, we see that q and f are also identical. $\square$

Remark 1. If $n = 3$ then the claim of Lemma 1 can fail. For example, the reducible 3-quasigroups $q(x_1^3) \stackrel{\mathrm{def}}{=} (x_1 * x_2) * x_3$ and $f(x_1^3) \stackrel{\mathrm{def}}{=} x_1 * (x_2 * x_3)$ where $*$ is a binary quasigroup with an identity element 0 (i. e., a loop) coincide if $x_1 = 0$, $x_2 = 0$, or $x_3 = 0$; but they are not identical if $*$ is nonassociative.

3. Subquasigroup

Let $q : \Sigma^n \to \Sigma$ be an n-quasirgoup and $\Omega \subset \Sigma$. If $g = q|_{\Omega^n}$ is an n-quasirgoup then we will say that g is a *subquasigroup* of q and q is Ω*-closed*.

Lemma 2. *For each finite Σ with $|\Sigma| = k$ and $\Omega \subset \Sigma$ with $|\Omega| \leqslant \lfloor k/2 \rfloor$ there exists a reducible n-quasigroup $q : \Sigma^n \to \Sigma$ with a subquasigroup $g : \Omega^n \to \Omega$.*

Proof. By Ryser theorem on completion of a Latin $s \times r$ rectangular up to a Latin $k \times k$ square (2-quasigroup) [16], there exists a Ω-closed 2-quasigroup $q : \Sigma^2 \to \Sigma$.

To be constructive, we suggest a direct formula for the case $\Sigma = \{0, \ldots, k-1\}$, $\Omega = \{0, \ldots, r-1\}$ where $k \geqslant 2r$ and $k - r$ is odd:

$$\begin{aligned}
q_{k,r}(i,j) &= (i+j) \bmod r, && i < r, j < r; \\
q_{k,r}(r+i,j) &= (i+j) \bmod (k-r) + r, && j < r; \\
q_{k,r}(i,r+j) &= (2i+j) \bmod (k-r) + r, && i < r; \\
q_{k,r}(r+i,r+j) &= \begin{cases} (i-j) \bmod (k-r) & \text{if } (i-j) \bmod (k-r) < r, \\ (2i-j) \bmod (k-r) + r & \text{otherwise.} \end{cases}
\end{aligned}$$

In the following four examples the second and the fourth value arrays correspond to $q_{5,2}$ and $q_{7,2}$:

$$4: \begin{array}{|cc|cc|} \hline 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ \hline \end{array} \qquad 5: \begin{array}{|cc|ccc|} \hline 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 3 & 4 & 2 \\ \hline 2 & 4 & 0 & 1 & 6 \\ 3 & 2 & 4 & 0 & 1 \\ 4 & 3 & 1 & 5 & 0 \\ \hline \end{array} \qquad 6: \begin{array}{|cc|cccc|} \hline 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 2 & 5 & 4 \\ \hline 4 & 5 & 0 & 1 & 2 & 3 \\ 5 & 4 & 1 & 0 & 3 & 2 \\ 2 & 3 & 4 & 5 & 0 & 1 \\ 3 & 2 & 5 & 4 & 1 & 0 \\ \hline \end{array} \qquad 7: \begin{array}{|cc|ccccc|} \hline 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 0 & 3 & 4 & 5 & 6 & 2 \\ \hline 2 & 4 & 0 & 1 & 6 & 3 & 5 \\ 3 & 5 & 6 & 0 & 1 & 2 & 4 \\ 4 & 6 & 5 & 2 & 0 & 1 & 3 \\ 5 & 2 & 4 & 6 & 3 & 0 & 1 \\ 6 & 3 & 1 & 5 & 2 & 4 & 0 \\ \hline \end{array} \tag{4}$$

Now, the statement follows from the obvious fact that a superposition of Ω-closed 2-quasigroups is an Ω-closed n-quasigroup. $\square$

The next obvious lemma is a suitable tool for obtaining a large number of n-quasigroups, most of which are irreducible.

Lemma 3 (switching subquasigroups). *Let $q : \Sigma^n \to \Sigma$ be an Ω-closed n-quasigroup with a subquasigroup $g : \Omega^n \to \Omega$, $g = q|_{\Omega^n}$, $\Omega \subset \Sigma$. And let $h : \Omega^n \to \Omega$ be another n-quasigroup of order $|\Omega|$. Then*

$$f(\bar{x}) \stackrel{\text{def}}{=} \begin{cases} h(\bar{x}) & \text{if } \bar{x} \in \Omega^n \\ q(\bar{x}) & \text{if } \bar{x} \notin \Omega^n \end{cases} \tag{5}$$

is an n-quasigroup of order $|\Sigma|$.

4. Irreducible n-quasigroups

Lemma 4. *A subquasigroup of a reducible n-quasigroup is reducible.*

Proof. Let $f : \Sigma^n \to \Sigma$ be a reducible Ω-closed n-quasigroup. Without loss of generality we assume that

$$f(x, \bar{y}, \bar{z}) \equiv h(g(x, \bar{y}), \bar{z})$$

for some $(n-m+1)$- and m-quasigroups h and g where $1 < m < n$. Take $\bar{o} \in \Omega^{m-1}$ and $\theta \in \Omega^{n-m}$. Then the quasigroups h_0, g_0, and δ defined by (1) are Ω-closed. Therefore, the representation (2) proves that $f|_{\Omega^n}$ is reducible. $\square$

Theorem 2. *For each $n \geqslant 3$ and $k \geqslant 4$ there exists an irreducible n-quasigroup of order k.*

Proof. (*) First we consider the case $n \geqslant 4$. By Lemma 2 we can construct a reducible n-quasigroup $q : \{0, \ldots, k-1\}^n \to \{0, \ldots, k-1\}$ of order k with a subquasigroup $g : \{0,1\}^n \to \{0,1\}$ of order 2. Let $h : \{0,1\}^n \to \{0,1\}$ be the n-quasigroup of order 2 different from g; and let f be defined by (5). By Theorem 1 with $\bar{o} = (2, \ldots, 2)$, the n-quasigroup f is irreducible.

(**) $n = 3$, $k = 4, 5, 6, 7$. In each of these cases we will construct an irreducible 3-quasigroup f, omitting the verification, which can be done, for example, using the formulas (1), (2). Let quasigroups $q_{4,2}$, $q_{5,2}$, $q_{6,2}$, and $q_{7,2}$ be defined by the value arrays (4). For each case $k = 4, 5, 6, 7$ we define the ternary quasigroup $q(x_1, x_2, x_3) \stackrel{\text{def}}{=} q_{k,2}(q_{k,2}(x_1, x_2), x_3)$, which have the subquasigroup $q|_{\{0,1\}^3}(x_1, x_2, x_3) = x_1 + x_2 + x_3 \bmod 2$. Using (5), we replace this subquasigroup by the ternary quasigroup $h(x_1, x_2, x_3) = x_1 + x_2 + x_3 + 1 \bmod 2$. The resulting ternary quasigroup f is irreducible.

(***) $n = 3$, $8 \leqslant k < \infty$. Using Lemma 2, Lemma 3, and (**), we can easily construct a ternary quasigroup of order $k \geqslant 8$ with an irreducible subquasigroup of order 4. By Lemma 4, such quasigroup is irreducible.

(****) The case of infinite order. Let $q : \Sigma_\infty^n \to \Sigma_\infty$ be an n-quasigroup of infinite order K and $g : \Sigma^n \to \Sigma$ be any irreducible n-quasigroup of finite order (say, 4). Then, by Lemma 4, their direct product $g{\times}q : (\Sigma \times \Sigma_\infty)^n \to (\Sigma \times \Sigma_\infty)$ defined as

$$g{\times}q\ \big([x_1, y_1], \ldots, [x_n, y_n]\big) \stackrel{\mathrm{def}}{=} \big[g(x_1, \ldots, x_n), q(y_1, \ldots, y_n)\big]$$

is an irreducible n-quasigroup of order K. $\square$

Remark 2. Using the same arguments, it is easy to construct for any $n \geqslant 4$ and $k \geqslant 4$ an irreducible n-quasigroup of order k such that fixing one argument (say, the first) by (say) 0 leads to an $(n-1)$-quasigroup that is also irreducible. This simple observation naturally blends with the following context. Let $\kappa(q)$ be the maximal number such that there is an irreducible $\kappa(q)$-quasigroup that can be obtained from q or one of its inverses by fixing $n - \kappa(q) > 0$ arguments. In this remark we observe that (for any n and k when the question is nontrivial) there is an irreducible n-quasigroup q with $\kappa(q) = n - 1$. In [10] for $k \vdots 4$ and even $n \geqslant 4$ an irreducible n-quasigroup with $\kappa(q) = n - 2$ is constructed. In [9, 12] it is shown that $\kappa(q) \leqslant n - 3$ (if k is prime then $\kappa(q) \leqslant n - 2$) implies that q is reducible.

5. On the number of n-quasigroups, I

We first consider a simple bound on the number of n-quasigroups of composite order.

Proposition 1. *The number $|Q(n, sr)|$ of n-quasigroups of composite order sr satisfies*

$$|Q(n, sr)| \geqslant |Q(n, r)| \cdot |Q(n, s)|^{r^n} > |Q(n, s)|^{r^n}. \tag{6}$$

Proof. Let $g : Z_r^n \to Z_r$ be an arbitrary n-quasigroup of order r; and let $\omega\langle\cdot\rangle$ be an arbitrary function from Z_r^n to the set $Q(n, s)$ of all n-quasigroups of order s. It is straightforward that the following function is an n-quasigroup of order sr:

$$f(z_1^n) \stackrel{\mathrm{def}}{=} g\left(y_1^n\right) \cdot s + \omega\left\langle y_1^n\right\rangle\left(x_1^n\right) \quad \text{where } y_i \stackrel{\mathrm{def}}{=} \lfloor z_i/s \rfloor, \quad x_i \stackrel{\mathrm{def}}{=} z_i \bmod s.$$

Moreover, different choices of $\omega\langle\cdot\rangle$ result in different n-quasigroups. So, this construction, which is known as the ω-product of g, obviously provides the bound (6). $\square$

If the order is divided by 2 or 3 then the bound (6) is the best known. Substituting the known values $|Q(n,2)| = 2$ and $|Q(n,3)| = 3 \cdot 2^n$, we get

Corollary 2. *If* $k\vdots 2$ *then* $|Q(n,k)| \geqslant 2^{(k/2)^n}$;

if $k\vdots 3$ *then* $|Q(n,k)| \geqslant (3 \cdot 2^n)^{(k/3)^n} > 2^{n(k/3)^n}$.

The next statement is weaker than the bound considered in the next section. Nevertheless, it provides simplest arguments showing that the number of n-quasigroup of fixed order k grows double-exponentially, even for prime $k \geqslant 8$. The cases $k = 5$ and $k = 7$ will be covered in the next section.

Proposition 2. *The number* $|Q(n,k)|$ *of* n*-quasigroups of order* $k \geqslant 8$ *satisfies*

$$|Q(n,k)| \geqslant 2^{\lfloor k/4 \rfloor^n}. \tag{7}$$

Proof. By Lemma 2, there is an n-quasigroup of order k with subquasigroup of order $2\lfloor k/4 \rfloor$. This subquasigroup can be switched (see Lemma 3) in $|Q(n, 2\lfloor k/4 \rfloor)|$ ways. By Proposition 1, we have

$$|Q(n, 2\lfloor k/4 \rfloor)| \geqslant |Q(n,2)|^{\lfloor k/4 \rfloor^n} = 2^{\lfloor k/4 \rfloor^n}.$$

Clearly, these calculations have sense only if $\lfloor k/4 \rfloor > 1$, i. e., $k \geqslant 8$. $\square$

6. On the number of n-quasigroups, II

In this section we continue using the same general switching principle as in previous ones: independent changing the values of n-quasigroups on disjoint subsets of Σ^n. We improve the lower bound in the cases when the order is not divided by 2 or 3; in particular, we establish a double-exponential lower bound on the number of n-quasigroups of orders 5 and 7.

We say that a nonempty set $\Theta \subset \Sigma^n$ is an *ab-component* or a *switching component* of an n-quasigroup q iff

(**a**) $q(\Theta) = \{a, b\}$ and

(**b**) the function $q\Theta : \Sigma^n \to \Sigma$ defined as follows is an n-quasigroup too:

$$q\Theta(\bar{x}) \stackrel{\mathrm{def}}{=} \begin{cases} q(\bar{x}) & \text{if } \bar{x} \notin \Theta \\ b & \text{if } \bar{x} \in \Theta \text{ and } q(\bar{x}) = a \\ a & \text{if } \bar{x} \in \Theta \text{ and } q(\bar{x}) = b. \end{cases}$$

For example, $\{(0,0),(0,1),(1,0),(1,1)\}$ and $\{(2,2),(2,3),(3,3),(3,4),(4,2),(4,4)\}$ are 01-components in (4.5).

Remark 3. From some point of view, it is naturally to require also Θ to be inclusion-minimal, i.e., (**c**) Θ does not have a nonempty proper subset that satisfies (a) and (b). Although in what follows all ab-components satisfy (c), formally we do not use it.

Lemma 5. *Let an n-quasigroup q have s pairwise disjoint switching components $\Theta_1, \dots, \Theta_s$ (note that we do not require them to be ab-components for common a, b). Then $|Q(n,|\Sigma|)| \geqslant 2^s$.*

Proof. Indeed, denoting $q\Theta^0 \stackrel{\text{def}}{=} q$ and $q\Theta^1 \stackrel{\text{def}}{=} q\Theta$, we have 2^s distinct n-quasigroups $q\Theta_1^{t_1}...\Theta_s^{t_s}$, $(t_1,\dots,t_s) \in \{0,1\}^s$. □

6.1. The order 5

In this section, we consider the n-quasigroups of order 5, the only case, when the other our bounds do not guarantee the double-exponential growth of the number of n-quasigroups as $n \to \infty$. Of course, the way that we use for the order 5 works for any other order $k > 3$, but the bound obtained is worse than (6) provided k is composite, worse than (7) provided $k \geqslant 8$, and worse than (8) provided $k \geqslant 6$. The bound is based on the following straightforward fact:

Lemma 6. *Let $\{0,1\}^n$ be a 01-component of an n-quasigroup q. For every $i \in \{1,\dots,n\}$ let q_i be an n_i-quasigroup and let Θ_i be its 01-component. Then $\Theta_1 \times \ldots \times \Theta_n$ is a 01-component of the $(n_1+\ldots+n_n)$-quasigroup*

$$f(x_{1,1},...,x_{1,n_1},x_{2,1},\dots,x_{n,n_n}) \stackrel{\text{def}}{=} q(q_1(x_{1,1},...,x_{1,n_1}),\dots,q_n(x_{n,1},...,x_{n,n_n})).$$

For a quasigroup $q : \Sigma^2 \to \Sigma$ denote $q^1 \stackrel{\text{def}}{=} q$, $q^2(x_1,x_2,x_3) \stackrel{\text{def}}{=} q(x_1,q^1(x_2,x_3))$, $\dots$, $q^i(x_1,x_2,\dots,x_{i+1}) \stackrel{\text{def}}{=} q(x_1,q^{i-1}(x_2,\dots,x_{i+1}))$.

Proposition 3. *If $n = 3m$ then $|Q(n,5)| \geqslant 2^{3^m}$; if $n = 3m+1$ then $|Q(n,5)| \geqslant 2^{4\cdot 3^{m-1}}$; if $n = 3m+2$ then $|Q(n,5)| \geqslant 2^{2\cdot 3^m}$. Roughly, for any n we have*

$$|Q(n,5)| > 2^{3^{n/3-0.072}} > e^{e^{\frac{\ln 3}{3}n-0.44}}.$$

Proof. Let q be the quasigroup of order 5 with value table (4.5). Then

(*) q has two disjoint 01-components $D_0 \stackrel{\text{def}}{=} \{(0,0),(0,1),(1,0),(1,1)\}$ and $D_1 \stackrel{\text{def}}{=} \{(2,2),(2,3),(3,3),(3,4),(4,2),(4,4)\}$;

(**) q^2 has three mutually disjoint 01-components $T_0 \stackrel{\text{def}}{=} \{0,1\} \times D_0$, $T_1 \stackrel{\text{def}}{=} \{0,1\} \times D_1$, and $T_2 \stackrel{\text{def}}{=} \{(x_1,x_2,x_3)|q^2(x_1,x_2,x_3) \in \{0,1\}\} \setminus (T_0 \cup T_1)$;

(***) $\{0,1\}^{m+1}$ is a 01-component of q^m.

By Lemma 6,

i. the $3m$-quasigroup defined as the superposition

$$q^{m-1}(q^2(\cdot,\cdot,\cdot),\ldots,q^2(\cdot,\cdot,\cdot))$$

has 3^m components $T_{t_1} \times \ldots \times T_{t_m}$, $(t_1,\ldots,t_m) \in \{0,1,2\}^m$;

ii. the $3m+1$-quasigroup defined as the superposition

$$q^m(q^2(\cdot,\cdot,\cdot),\ldots,q^2(\cdot,\cdot,\cdot),q(\cdot,\cdot),q(\cdot,\cdot))$$

has $3^{m-1}4$ components $T_{t_1}\times\ldots\times T_{t_{m-1}}\times D_{t_m}\times D_{t_{m+1}}$, $(t_1,\ldots,t_{m+1}) \in \{0,1,2\}^{m-1} \times \{0,1\}^2$;

iii. the $3m+2$-quasigroup defined as the superposition

$$q^m(q^2(\cdot,\cdot,\cdot),\ldots,q^2(\cdot,\cdot,\cdot),q(\cdot,\cdot))$$

has $3^m 2$ components $T_{t_1}\times\ldots\times T_{t_m}\times D_{t_{m+1}}$, $(t_1,\ldots,t_{m+1}) \in \{0,1,2\}^m \times \{0,1\}$.

By Lemma 5, the theorem follows. $\square$

Remark 4. If, in the proof, we consider the superposition $q^{n/2}(q(\cdot,\cdot),\ldots, q^2(\cdot,\cdot))$, then we obtain the bound $|Q(n,5)| \geqslant 2^{2^{n/2}}$ for even n, which is worse because $\frac{\ln 2}{2} < \frac{\ln 3}{3}$.

6.2. The case of order $\geqslant 7$

In this section, we will prove the following:

Proposition 4. *The number $|Q(n,k)|$ of n-quasigroups $\{0,1,\ldots,k-1\}^n \to \{0,1,\ldots,k-1\}$ satisfies*

$$|Q(n,k)| \geqslant 2^{\lfloor k/2\rfloor \lfloor k/3\rfloor^{n-1}} > e^{e^{\ln\lfloor k/3\rfloor n+\ln\lfloor k/2\rfloor-\ln\lfloor k/3\rfloor-0.37}} > e^{e^{\ln\lfloor k/3\rfloor n+0.038}}. \quad (8)$$

Note that this bound has no sense if $k < 6$; and it is weaker than (6) if $k\vdots 2$ or $k\vdots 3$. The proof is based on the following straightforward fact:

Lemma 7. *Let $\{c,d\} \times \{e,f\}$ be an ab-component of a quasigroup g. Then*

(a) $\{a,b\} \times \{e,f\}$ *is a cd-component of the quasigroup* g^- *defined by* $g(x,y) = z \Leftrightarrow g^-(z,y) = x$;

(b) *if* $\{a_1,b_1\} \times \ldots \times \{a_n,b_n\}$ *is a ef-component of an n-quasigroup q, then* $\{c,d\} \times \{a_1,b_1\} \times \ldots \times \{a_n,b_n\}$ *is an ab-component of the* $(n+1)$*-quasigroup defined as the superposition* $g(\cdot, q(\cdot,\ldots,\cdot))$.

Proof of Proposition 4. Taking into account Corollary 2, it is enough to consider only the cases of odd $k \not\equiv 0 \bmod 3$. Moreover, we can assume that $k > 6$ (otherwise the statement is trivial).

Define the 2-quasigroup q as

$$\begin{aligned} q(2j,i) &\stackrel{\text{def}}{=} i + 3j \bmod k; \\ q(2j+1,i) &\stackrel{\text{def}}{=} \pi(i) + 3j \bmod k; \\ q(2\lfloor k/3\rfloor + j, i) &\stackrel{\text{def}}{=} \tau(i) + 3j \bmod k;\ j = 0,\ldots,\lfloor k/3\rfloor - 1,\ i = 0,\ldots,k-1 \end{aligned}$$

where π, τ, and the remaining values of q are defined by the following value table (the fourth row is used only for the case $k \equiv 2 \bmod 3$):

i	0	1	2	3	4	$\ldots$	$k-5$	$k-4$	$k-3$	$k-2$	$k-1$
$\pi(i)$	1	0	3	2	5	$\ldots$	$k-4$	$k-5$	$k-2$	$k-1$	$k-3$
$\tau(i)$	$k-1$	2	1	4	3	$\ldots$		$k-3$	$k-4$	0	$k-2$
$q(k-2,i)$	$k-3$	$k-2$	$k-1$	0	1	$\ldots$		$k-7$	$k-6$	$k-4$	$k-5$
$q(k-1,i)$	$k-2$	$k-1$	0	1	2	$\ldots$		$k-6$	$k-5$	$k-3$	$k-4$

In what follows, the tables illustrate the cases $k = 7$ and $k = 11$.

$k = 7$:

0	1	2	3	4	5	6
1	0	3	2	5	6	4
3	4	5	6	0	1	2
4	3	6	5	1	2	0
6	2	1	4	3	0	5
2	5	4	0	6	3	1
5	6	0	1	2	4	3

$k = 11$:

0	1	2	3	4	5	6	7	8	9	10
1	0	3	2	5	4	7	6	9	10	8
3	4	5	6	7	8	9	10	0	1	2
4	3	6	5	8	7	10	9	1	2	0
6	7	8	9	10	0	1	2	3	4	5
7	6	9	8	0	10	2	1	4	5	3

For each $j = 0,\ldots,\lfloor k/3\rfloor - 1$ and $i = 0,\ldots,\lfloor k/2\rfloor - 2$ the set $\{2j, 2j+1\} \times \{2i, 2i+1\}$ is a $(2i+3j \bmod k)(2i+3j+1 \bmod k)$-component of such q. By Lemma 7(a), for the same pairs i,j the set $\{2i+3j \bmod k, 2i+3j+1 \bmod k\} \times \{2i, 2i+1\}$ is a $(2j)(2j+1)$-component of $g \stackrel{\text{def}}{=} q^-$; moreover, we can observe that for each j there is one more "non-square" $(2j)(2j+1)$-component of g which is disjoint with all considered "square" components, see the following examples (we omit the analytic description; indeed, we can ignore this component if we do not care about the constant in the bound $e^{e^{\ln\lfloor k/3\rfloor n+const}}$).

$k=7$:

0	1	6	5	2	4	3
1	0	4	6	3	2	5
5	4	0	1	6	3	2
2	3	1	0	4	5	6
3	2	5	4	0	6	1
6	5	2	3	1	0	4
4	6	3	2	5	1	0

$k=11$:

0	1	10	9	5	4	8	7	2	6	3
1	0	6	10	9	8	4	5	3	2	7
7	6	0	1	10	9	5	4	8	3	2
2	3	1	0	6	10	9	8	4	7	5
3	2	7	6	0	1	10	9	5	4	8
8	7	2	3	1	0	6	10	9	5	4
4	5	3	2	7	6	0	1	10	8	9
5	4	8	7	2	3	1	0	6	9	10
9	8	4	5	3	2	7	6	0	10	1
10	9	5	4	8	7	2	3	1	0	6
6	10	9	8	4	5	3	2	7	1	0

By induction, using Lemma 7(b), we derive that for every $j_1,\ldots,j_{n-1} \in \{0,\ldots,\lfloor k/3\rfloor-1\}$ and $i \in \{0,\ldots,\lfloor k/2\rfloor-2\}$ the set

$$\begin{array}{l}\{\quad 2j_2+3j_1 \bmod k, \quad 2j_2+3j_1+1 \bmod k\}\times \\ \qquad\qquad\qquad \ldots \\ \{2j_{n-1}+3j_{n-2} \bmod k,\ 2j_{n-1}+3j_{n-2}+1 \bmod k\}\times \\ \{\quad 2i+3j_{n-1} \bmod k, \quad 2i+3j_{n-1}+1 \bmod k\}\times\{2i,2i+1\}\end{array}$$

is a $(2j_1)(2j_1+1)$-component of the n-quasigroup g^{n-1}. Also, for every such $j_1,\ldots,j_{n-1}$ there is one more $(2j_1)(2j_1+1)$-component of g^{n-1}, which is generated by the "non-square" $(2j_{n-1})(2j_{n-1}+1)$-component of g. In summary, g^{n-1} has at least $\lfloor k/3\rfloor^{n-1}\lfloor k/2\rfloor$ pairwise disjoint switching components. By Lemma 5, the theorem is proved. □

Summarizing Corollary 2, Propositions 3 and 4, we get the following theorem.

Theorem 3. *Let a finite set Σ of size $k>3$ be fixed. The number $|Q(n,k)|$ of n-quasigroups $\Sigma^n\to\Sigma$ satisfies the following*:

(a) *If k is even, then $|Q(n,k)| \geqslant 2^{(k/2)^n}$.*

(b) *If k is divided by 3, then $|Q(n,k)| \geqslant 2^{n(k/3)^n}$.*

(c) *If $k=5$, then $|Q(n,k)| \geqslant 2^{3^{n/3-c}}$ where $c<0.072$ depends on $n \bmod 3$.*

(d) *In all other cases, $|Q(n,k)| \geqslant 2^{1.5\lfloor k/3\rfloor^n}$.*

References

[1] **M. A. Akivis, V. V. Goldberg**: *Solution of Belousov's problem*, Discuss. Math., Gen. Algebra Appl. **21** (2001), no. 1, 93 – 103.

[2] **V. D. Belousov**: *n-Ary Quasigroups*, (Russian), Shtiintsa, Kishinev, 1972.

[3] **V. D. Belousov, M. D. Sandik**: *n-Ary quasi-groups and loops*, Sib. Math. J. **7** (1966), 24 – 42 (translated from Sib. Mat. Zh. **7** (1966), 31 – 54).

[4] **V. V. Borisenko**: *Irreducible n-quasigroups on finite sets of composite order*, (Russian), Mat. Issled. **51** (1979), 38 – 42.

[5] **B. R. Frenkin**: *Reducibility and uniform reducibility in certain classes of n-groupoids, II*, (Russian), Mat. Issled., **7:1(23)** (1972), 150 – 162.

[6] **M. M. Glukhov**: *Varieties of (i, j)-reducible n-quasigroups*, (Russian), Mat. Issled., **39**, Shtiintsa, Kishinev, 1976, 67 – 72.

[7] **V. V. Goldberg**: *The invariant characterization of certain closure conditions in ternary quasigroups*, Sib. Math. J. **16** (1975), 23 – 34 (translated from Sib. Mat. Zh. **16** (1975), 29 – 43).

[8] **V. V. Goldberg**: *Reducible $(n+1)$-webs, group $(n+1)$-webs and $(2n+2)$-hedral $(n+1)$-webs of multidimensional surfaces*, Sib. Math. J. **17** (1976), 34 – 44 (translated from Sib. Mat. Zh. **17** (1976), 44 – 57).

[9] **D. S. Krotov**: *On reducibility of n-ary quasigroups*, Discrete Math., in press., 2007. DOI: 10.1016/j.disc.2007.08.099

[10] **D. S. Krotov**: *On irreducible n-ary quasigroups with reducible retracts*, Eur. J. Comb. **29** (2008), 507 – 513.

[11] **D. S. Krotov, V. N. Potapov**: *On the reconstruction of n-quasigroups of order 4 and the upper bounds on their number*, Proc. the Conference Devoted to the 90th Anniversary of Alexei A. Lyapunov, Novosibirsk, Russia, Oct. 2001, 323 – 327. Available at http://www.sbras.ru/ws/Lyap2001/2363

[12] **D. S. Krotov, V. N. Potapov**: *On reducibility of n-ary quasigroups, II*, Available at http://arxiv.org/abs/0801.0055

[13] **C. F. Laywine, G. L. Mullen**: *Discrete Mathematics Using Latin Squares*, Wiley, New York, 1998.

[14] **B. D. McKay, I. M. Wanless**: *A census of small Latin hypercubes*, SIAM J. Discrete Math., **22** (2008), 719 – 736.

[15] **V. N. Potapov, D. S. Krotov**: *Asymptotics for the number of n-quasigroups of order 4*, Sib. Math. J. **47** (2006), 720 – 731 (translated from Sib. Mat. Zh. 47 (2006), 873 – 887).

[16] **H. J. Ryser**: *A combinatorial theorem with an application to latin rectangles*, Proc. Am. Math. Soc. **2** (1951), 550 – 552.

Received September 23, 2007

Sobolev Institute of Mathematics
pr-t Ak. Koptyuga 4
Novosibirsk 630090
Russia
e-mail: {krotov;vpotapov}@math.nsc.ru; superpos@gorodok.net

Quasigroups and Related Systems **16** (2008), 69 – 76

Left almost semigroups defined by a free algebra

Qaiser Mushtaq and Muhammad Inam

Abstract

We have constructed LA-semigroups through a free algebra, and the structural properties of such LA-semigroups have been investegated. Moreover, the isomorphism theorems for LA-groups constructed through free algebra have been proved.

1. Introduction

A left almost semigroup, abbreviated as an LA-semigroup, is an algebraic structure midway between a groupoid and a commutative semigroup. The structure was introduced by M. A. Kazim and M. Naseeruddin [3] in 1972. This structure is also known as Abel-Grassmann's groupoid, abbreviated as an AG-groupoid [6] and as an invertive groupoid [1].

A groupoid G with *left invertive law*, that is: $(ab)\,c = (cb)\,a, \forall a, b, c \in G$, is called an *LA-semigroup.*

An LA-semigroup satisfies the medial law: $(ab)\,(cd) = (ac)\,(bd)$. An LA-semigroup with left identity is called an *LA-monoid.*

An LA-semigroup in which either $(ab)\,c = b\,(ca)$ or $(ab)\,c = b\,(ac)$ holds for all $a, b, c, d \in G$, is called an *AG^{*}-groupoid* [6].

Let G be an LA-semigroup and $a \in G$. A mapping $L_a : G \longrightarrow G$, defined by $L_a\,(x) = ax$, is called the *left translation* by a. Similarly, a mapping $R_a : G \longrightarrow G$, defined by $R_a\,(x) = xa$, is called the *right translation* by a. An LA-semigroup G is called *left* (*right*) *cancellative* if all the left (right) translations are injective. An LA-semigroup G is called *cancellative* if all translations are injective.

Let X be a non-empty set and W'_X denote the free algebra over X in the variety of algebras of the type $\{0, \alpha, +\}$, consisting of nullary, unary and

2000 Mathematics Subject Classification: 20M10, 20N99
Keywords: LA-semigroup, free algebra, Abel Grassmann's groupoid, medial law.

binary operations determined by the following identities:

$$(x+y)+z = x+(y+z)\,, \quad x+y = y+x, \quad x+0 = x,$$

$$\alpha\,(x+y) = \alpha x + \alpha y, \quad \alpha 0 = 0.$$

Every element $u \in W'_X$ has the form $u = \sum_{i=1}^{r} \alpha^{n_i} x_i$, where $r \geqslant 0$, and n_i are non-negative integers. This expression is unique up to the order of the summands. Moreover $r = 0$ if and only if $u = 0$.

Let us define a multiplication on W'_X by $u \circ v = \alpha u + \alpha^2 v$. Then the set W'_X is an LA-semigroup under this binary operation. We denote it by W_X. It is easy to see that W_X is cancellative.

If n is the smallest non-negative integer such that $\alpha^n x = x$, then n is called the *order* of α. The following examples show the existence of such LA-semigroups.

Example 1. Consider a field $F_5 = \{0,1,2,3,4\}$ and define $\alpha\,(x) = 3x$ for all $x \in F_5$. Then F_5 becomes an LA-semigroup under the binary operation defined by $u \circ v = \alpha u + \alpha^2 v$, $\forall\ u, v \in F_5$.

$\circ$	0	1	2	3	4
0	0	4	3	2	1
1	3	2	1	0	4
2	1	0	4	3	2
3	4	3	2	1	0
4	2	1	0	4	3

Example 2. Let $X = \{x, y\}$ and α be defined as $\alpha\,(a) = 2a$, for all $a \in X$ and $2 \in F_3$. Then the following table illustrates an LA-semigroup W_X.

$\circ$	0	x	$2x$	y	$2y$	$x+y$	$2x+y$	$x+2y$	$2x+2y$
0	0	x	$2x$	y	$2y$	$x+y$	$2x+y$	$x+2y$	$2x+2y$
x	$2x$	0	x	$2x+y$	$2x+2y$	y	$x+y$	$2y$	$x+2y$
$2x$	x	$2x$	0	$x+y$	$x+2y$	$2x+y$	y	$x+2y$	$2y$
y	$2y$	$x+2y$	$2x+2y$	0	y	x	$2x$	$x+y$	$2x+y$
$2y$	y	$x+y$	$2x+y$	$2y$	0	$x+2y$	$2x+2y$	x	$x+y$
$x+y$	$2x+2y$	$2y$	$x+2y$	$2x$	$2x+y$	0	x	y	$x+y$
$2x+y$	$x+2y$	$2x+2y$	$2y$	x	$x+y$	$2x$	0	$2x+2y$	y
$x+2y$	$2x+y$	y	$x+y$	$2x+2y$	$2x$	$2y$	$x+2y$	0	x
$2x+2y$	$x+y$	$2x+y$	y	$x+2y$	x	$2x+2y$	$2y$	$2x+2y$	0

An LA-semigroup is called an *LA-band* [6], if all of its elements are idempotents. An LA-band can easily be constructed from a free algebra by choosing a unary operation α such that $\alpha + \alpha^2 = Id_X$, where Id_X denotes the identity map on X.

Example 3. Define a unary operation α as $\alpha(x) = 2x$, where $x \in F_5$. Then under the binary operation $\circ$ defined as above, F_5 is an LA-band.

$\circ$	0	1	2	3	4
0	0	4	3	2	1
1	2	1	0	4	3
2	4	3	2	1	0
3	1	0	4	3	2
4	3	2	1	0	4

An LA-semigroup $(G, \cdot)$ is called an *LA-group* [5], if
(i) there exists $e \in G$ such that $ea = a$ for every $a \in G$,
(ii) for every $a \in G$ there exists $a' \in G$ such that $a'a = e$.

A subset I of an LA-semigroup $(G, \cdot)$ is called a *left* (*right*) *ideal* of G, if $GI \subseteq I$ $(IG \subseteq I)$, and I is called a *two sided ideal* of G if it is left and right ideal of G. An LA-semigroup is called *left* (*right*) *simple*, if it has no proper left (right) ideals. Consequently, an LA-semigroup is *simple* if it has no proper ideals.

Theorem 1. *A cancellative LA-semigroup is simple.*

Proof. Let G be a cancellative LA-semigroup. Suppose that G has a proper left ideal I. Then by definition $GI \subseteq I$ and so I being its proper ideal, is a proper LA-subsemigroup of G. If $g \in G \backslash I$, then $gi \in GI$, for all $i \in I$. But $GI \subseteq I$, so there exists an $i' \in I$, such that $gi = i'$. Since G is cancellative so is then I. This implies that all the right and left translations are bijective. Therefore there exists $i_1 \in I$, such that $L_{i_1}(i) = i'$. This implies that $gi = i_1 i$. By applying the right cancellation, we obtain $g = i_1$. This implies that $g \in I$, which contradicts our supposition. Hence G is simple. $\square$

Corollary 1. *An LA-semigroup defined by a free algebra is simple.*

Theorem 2. *If G is a right* (*left*) *cancellative LA-semigroup, then $G^2 = G$.*

Proof. Let G be a right (left) cancellative LA-semigroup. Then all the right (left) translations are bijective. This implies that for each $x \in G$, there exist some $y, z \in G$ such that $R_y(z) = x$ $(L_y(z) = x)$. Hence $G^2 = G$. $\square$

Corollary 2. *An AG^*-groupoid cannot be defined by a free algebra.*

Proof. It has been proved in [6], that if G is an AG*-groupoid then G^2 is a commutative semigroup. Moreover, if G is a right (left) cancellative LA-semigroup, then $G^2 = G$. $\square$

We now define a subset T_x of W_X such that $T_x = \{\sum_{i=1}^{r} \alpha^{n_i} x \mid x \in X\}$.

Theorem 3. *T_x is an LA-subsemigroup of W_X.*

Proof. It is sufficient to show that T_x is closed under the operation $\circ$. Let $u, v \in T_x$. Then $u = \sum_{i=1}^{n} \alpha^{n_i} x$, $v = \sum_{i=1}^{m} \alpha^{n_i} x$, and so

$$\begin{aligned} u \circ v &= \alpha(u) + \alpha^2(v) = \alpha\left(\textstyle\sum_{i=1}^{n} \alpha^{n_i} x\right) + \alpha^2\left(\textstyle\sum_{i=1}^{m} \alpha^{n_i} x\right) \\ &= \left(\textstyle\sum_{i=1}^{n} \alpha^{n_i+1} + \sum_{i=1}^{m} \alpha^{n_i+2}\right) x = \textstyle\sum_{i=1}^{r} \alpha^{m_i} x, \end{aligned}$$

where $r = n + m$, $m_i = n_i + 1$ for $i \leqslant n$ and $m_i = n_i + 2$ for $i > n$. $\square$

Theorem 4. *If $X = \{x_1, x_2, \dots, x_n\}$, then $W_X = T_{x_1} \oplus T_{x_2} \oplus \dots \oplus T_{x_n}$.*

Proof. Every element $u \in W_X$ is of the form $u = \sum_{i=1}^{r} \alpha^{n_i} x_i$, where r and n_i are non-negative integers. This expression is unique up to the order of the summands. This implies that $W_X = T_{x_1} + T_{x_2} + \dots + T_{x_n}$. To complete the proof it is sufficient to show that $T_{x_i} \cap T_{x_j} = \{0\}$, for $i \neq j$. Let $u \in T_{x_i} \cap T_{x_j}$, such that $u \neq 0$. Then $u \in T_{x_i}$ and $u \in T_{x_j}$. This is possible only if $x_i = x_j$. Which is a contradiction to the fact that $x_i \neq x_j$. Hence the proof. $\square$

Proposition 1. *The direct sum of any T_{x_i} and T_{x_j} for $i \neq j$ is an LA-subsemigroup of W_X.*

Proof. The proof is straightforward. $\square$

Theorem 5. *The direct sum of any finite number of T_{x_i}'s is an LA-subsemigroup of W_X.*

Proof. The proof follows directly by induction. $\square$

Theorem 6. *The set W_X / T_x of all right (left) cosets of T_x in W_X is an LA-semigroup.*

Proof. Let $W_X / T_x = \{u \circ T_x \mid u \in W_X\}$, and $u \circ T_x$, $v \circ T_x \in W_X / T_x$. Then by the medial law $(u \circ T_x) \circ (v \circ T_x) = (u \circ v) \circ T_x \circ T_x$. But $T_x \circ T_x = T_x$. Hence $(u \circ T_x) \circ (v \circ T_x) = (u \circ v) \circ T_x \in W_X / T_x$.

Let $u \circ T_x, v \circ T_x, w \circ T_x \in W_X \diagup T_x$. Then

$$\begin{aligned}((u \circ T_x) \circ (v \circ T_x)) \circ (w \circ T_x) &= ((u \circ v) \circ T_x) \circ w \circ T_x \\ &= ((u \circ v) \circ w) \circ T_x = ((w \circ v) \circ u) \circ T_x \\ &= ((w \circ T_x) \circ (v \circ T_x)) \circ (u \circ T_x)\end{aligned}$$

implies that $W_X \diagup T_x$ is an LA-simigroup. □

Remark 1. $\alpha(T_x) = T_x$.

Proposition 2. *For any* $T_x \leq W_X$ *and* $v \in W_X$ *we have*

(a) $T_x \circ v = (\alpha(v)) \circ T_x$,
(b) $T_x \circ (T_x \circ v) = \alpha^2(T_x \circ v) = \alpha^3(v \circ T_x)$,
(c) $(T_x \circ v) \circ T_x = \alpha(T_x \circ v) = \alpha^2(v \circ T_x)$,
(d) $T_x \circ v = \alpha(v \circ T_x)$.

Proof. The proof is straightforward. □

Theorem 7. $W_X \diagup T_{x_i} = \{v \circ T_{x_i} : v \in W_X\}$ *forms a partition of* W_X.

Proof. We shall show that $u \circ T_{x_i} \cap v \circ T_{x_i} = \emptyset$ for $u \neq v$, and $W_X = \cup_{v \in W_X} v \circ T_{x_i}$. Let $w \in v \circ T_{x_i} \cap u \circ T_{x_i}$. Then $w \in v \circ T_{x_i}$ and $w \in u \circ T_{x_i}$. This implies that $w = v \circ t_1$ and $w = u \circ t_2$, where $t_1, t_2 \in T_{x_i}$. This implies $v \circ t_1 = u \circ t_2$. Hence $\alpha(v) + \alpha^2(t_1) = \alpha(u) + \alpha^2(t_2)$, which further gives $\alpha(v) = \alpha(u) + \alpha^2(t_2) - \alpha^2(t_1)$ where $\alpha^2(t_2) - \alpha^2(t_1) \in T_{x_i}$.

Now $\alpha(v) \in \alpha(u) + T_{x_i}$ yields $\alpha(v) + T_{x_i} \subseteq \alpha(u) + T_{x_i}$, i.e., $v \circ T_{x_i} \subseteq u \circ T_{x_i}$. Similarly, $u \circ T_{x_i} = v \circ T_{x_i}$. Hence $v \circ T_{x_i} \cap u \circ T_{x_i} = \emptyset$. Obviously, $\cup_{v \in W_X} v \circ T_{x_i} \subseteq W_X$.

Conversely, let $t \in W_X$. Then $t = \sum_{i=1}^{r} \alpha^{n_i} x_i$ implies that

$$\begin{aligned}t &= \alpha^{n_1} x_1 + \alpha^{n_2} x_2 + \ldots + \alpha^{n_r} x_r \\ &= \alpha^{n_i} x_i + \alpha^{n_1} x_1 + \alpha^{n_2} x_2 + \ldots + \alpha^{n_{i-1}} x_{i-1} + \alpha^{n_{i+1}} x_{i+1} + \ldots + \alpha^{n_r} x_r.\end{aligned}$$

If $\alpha^{n_1} x_1 + \alpha^{n_2} x_2 + \ldots + \alpha^{n_{i-1}} x_{i-1} + \alpha^{n_{i+1}} x_{i+1} + \ldots + \alpha^{n_r} x_r = u$, then $t = \alpha^{n_i} x_i + u$, $\alpha^{n_i} x_i \in T_{x_i}$. Now $t = \alpha^{n_i} x_i + u \in T_{x_i} + u = \alpha(u) + T_{x_i} = \alpha(u) + \alpha^2(T_{x_i}) = u \circ T_{x_i} \in \cup_{v \in W_X} v \circ T_{x_i}$ implies $W_X \subseteq \cup_{v \in W_X} v \circ T_{x_i}$. Hence $W_X = \cup_{v \in W_X} v \circ T_x$. □

Theorem 8. *The order of* T_{x_i} *divides the order of* W_X.

Proof. If X is a finite non-empty set then W_X is also finite. This implies that the set of all the right (left) cosets of T_{x_i} in W_X is finite.

Let $W_X \diagup T_{x_i} = \{v_1 \circ T_{x_i}, v_2 \circ T_{x_i}, \ldots, v_r \circ T_{x_i}\}$. Then by virtue of Theorem 7, $W_X = v_1 \circ T_{x_i} \cup v_2 \circ T_{x_i} \cup \ldots \cup v_r \circ T_{x_i}$. This implies that $|W_X| = |v_1 \circ T_{x_i}| + |v_2 \circ T_{x_i}| + \ldots + |v_r \circ T_{x_i}|$. Thus $|W_X| = r\,|T_{x_i}|$. Hence $|W_X| = [T_{x_i}, W_X]\,|T_{x_i}|$, where $[T_{x_i}, W_X]$ denotes the number of cosets of T_{x_i} in W_X. □

Theorem 9. *If X is a non-empty finite set having r number of elements and the order of T_{x_i} is n, then $|W_X| = n^r$.*

Proof. Since it has already been proved that $W_X = T_{x_1} \oplus T_{x_2} \oplus \ldots \oplus T_{x_r}$ for $X = \{x_1, x_2, \ldots, x_r\}$, it is sufficient to show that $|T_{x_1} \oplus T_{x_2} \oplus \ldots \oplus T_{x_r}| = n^r$. We apply induction on r. Let $r = 2$, that is, $W_X = T_{x_1} \oplus T_{x_2}$. Construct the multiplication table of T_{x_1} and write all the elements of T_{x_2} except 0 in the index row and in the index column. Then the number of elements in the index row or column row is $2n-1$. We see from the multiplication table that when the elements of T_{x_1} are multiplied by the elements of T_{x_2} some new elements appear in the table, which are of the form $u \circ v = \alpha(u) + \alpha^2(v)$, where $u \in T_{x_1}$ and $v \in T_{x_2}$ and they are $(n-1)^2$ in number. We write all such elements in index row and column and complete the multiplication table of $T_{x_1} \oplus T_{x_2}$. We see that no new element appear in the table. Then the number of elements in the index row or column is $2n-1+(n-1)^2 = n^2$. We now consider $n = 3$. Take the multiplication table of $T_{x_1} \oplus T_{x_2}$, and write all elements of T_{x_3} except 0 in the index row and column. The number of elements in the index row and column are $n^2 + n - 1$. Multiply the elements of $T_{x_1} \oplus T_{x_2}$ and T_{x_3}. Then in the table, some new elements of the form $t \circ w = \alpha(t) + \alpha^2(w)$ appear, where $t \in T_{x_1} \oplus T_{x_2}$, $w \in T_{x_3}$ which are $n^2(n-1)$ in number. Now we write all these elements in the index row and column of the table of $T_{x_1} \oplus T_{x_2} \oplus T_{x_3}$. We see that no new element appears in the table. The number of elements in the index row or column is $n^2 + n^2(n-1) = n^3$. Continuing in this way we finally get $|T_{x_1} \oplus T_{x_2} \oplus \ldots \oplus T_{x_r}| = n^r$. □

Theorem 10. *Let p be prime and F_P a finite field. Let E denote the r-th extension of F_P. Then there exists a unique epimorphism between LA-semigroups formed by E and F_p.*

Proof. Let α be a unary operation. Suppose that β is a root of an irreducible polynomial with respect to F_p. It is not difficult to prove that the mapping

$\varphi : E \to F_P$ defined by $\varphi\left(a_0 + a_1\beta + ... + a_{r-1}\beta^{r-1}\right) = a_0 + a_1 + ... + a_r$ is a unique epimorphism. $\square$

Theorem 11. *T_x is simple.*

Proof. Suppose that T_x has a proper left (right) ideal of S. Then by definition $ST_x \subseteq S$ ($T_xS \subseteq S$) and S is proper LA-subsemigroup of T_x. We know that the order of T_x is either prime or power of a prime. So, if it has a proper LA-subsemigroup S, then the order of S will be prime. Since S is embedded into T_x, so there exists a monomorphism between T_x and S. But by Theorem 10, there exists a unique epimorphism between T_x and S. This implies that there exists an isomorphism between T_x and S. This is a contradiction. Hence the proof. $\square$

Theorem 12. *If K is a kernel of a homomorphism h between LA-groups W and W', then*

(*a*) $K \leq W$,
(*b*) W / K *is an LA-group,*
(*c*) $W / K \cong Im\,(h)$.

Proof. (*a*) and (*b*) are obvious. For (*c*) define a mapping $\varphi : W / K \to Im(h)$ by $\varphi(u \circ K) = h(u)$ for $u \in W$. Then φ is an isomorphism. $\square$

Theorem 13. *If $T_1 = T_{x_1} \oplus T_{x_2} \oplus \ldots \oplus T_{x_n}$, $T_2 = T_{x_1} \oplus T_{x_2} \oplus \ldots \oplus T_{x_m}$, where $n \neq m$, then*

(1) $T_1 \leq T_1 \oplus T_2$ *and* $T_1 \cap T_2 \leq T_2$,
(2) $T_1 \oplus T_2 / T_1$ *and* $T_2 / T_1 \cap T_2$ *are LA-semigroups,*
(3) $T_1 \oplus T_2 / T_1 \cong T_2 / T_1 \cap T_2$.

Proof. (1) and (2) are obvious. For (3) define a mapping $\varphi : T_2 / T_1 \cap T_2 \longrightarrow T_1 \oplus T_2 / T_1$ by $\varphi(v \circ (T_1 \cap T_2)) = v \circ T_1$ for all $v \in T_1 \cap T_2$. Then ϕ is an isomorphism. $\square$

Theorem 14. *If W_X is an LA-group, and $T = T_{x_1} \oplus T_{x_2} \oplus \ldots \oplus T_{x_n}$, then $(W_X / T_{x_i}) / (T / T_{x_i})$ is isomorphic to W_X / T, where $1 \leqslant i \leqslant n$.*

Proof. Define a mapping $\varphi : W_X / T_{x_i} \longrightarrow W_X / T$, by $\varphi\,(v \circ T_{x_i}) = v \circ T$, where $v \in W_X$. Then φ is an epimorphism. By Theorem 12,

$$(W_X / T_{x_i}) / (Ker\,\varphi) \cong W_X / T$$

and $Ker\varphi = T / T_{x_i}$. Hence the proof. $\square$

References

[1] **P. Holgate**: *Groupoids satisfying a simple invertive law*, The Math. Student **61** (1992), 101 – 106.

[2] **J. Jezek and T. Kepka**: *Free entropic groupoids*, Comm. Math. Univ. Carolinae **22** (1981), 223 – 233.

[3] **M. Kazim and M. Naseeruddin**: *On almost semigroups*, Alig. Bull. Math. **2** (1972), 1 – 7.

[4] **T. Kepka and P. Nemec**: *A note on left distributive groupoids*, Coll. Math. Soc. J. Bolyai **29** (1977), 467 – 471.

[5] **Q. Mushtaq and M. S. Kamran**: *On left almost groups*, Proc. Pak. Acad. Sci. **331** (1996), 53 – 55.

[6] **V. Protič and N. Stevanović**: *AG-test and some general properties of Abel-Grassmann's groupoids*, PU. M. A **4** (1995), 371 – 383.

Department of Mathematics
Quaid-i-Azam University
Islamabad
Pakistan
E-mail: qmushtaq@isb.apollo.net.pk

Received February 11, 2007

Quasigroups and Related Systems **16** (2008), 77 – 88

Quasi union hyper K-algebras

Mohammad A. Nasr-Azadani and Mohammad M. Zahedi

Abstract

We give a method of construction of a hyper K-algebra on a set of order α, where α is a fixed cardinal number. Then we introduce the notion of quasi union hyper K-algebra and prove that any quasi union hyper K-algebra is implicative and whenever $0 \circ 0 = \{0\}$, it is strong implicative hyper K-algebra. Also a quasi union hyper K-algebra is positive implicative if and only if it is a hyper BCK-algebra. Finally we prove that any hyper K-algebra $H \overset{C}{=} \oplus_{i\in\Lambda} A_i$ (closed set), where $|A_i| = 2$ under some conditions is a quasi union hyper K-algebra or a quasi union hyper BCK-algebra.

1. Introduction

The study of BCK-algebra was initiated by Imai and Iséki [6] in 1966 as a generalization of the concept of set-theoretic difference and propositional calculi. The hyper structure theory (called also multi algebras) was introduced in 1934 by Marty [8] at the 8th congress of Scandinavian Mathematicians. Hyper structures have many applications to several sectors of both pure and applied sciences. Borzooei, et.al. [4, 7] applied the hyper structure to BCK-algebras and introduced the concept of hyper BCK-algebra and hyper K-algebra in which, each of them is a generalization of BCK-algebra. Borzooei and Harizavi [3] introduced a decomposition for a hyper BCK-algebra. Nasr-Azadani and Zahedi [9] study S-absorbing (P)-decomposable hyper K-algebras as a generalization of decomposition for hyper BCK-algebras. Now, we follow [9] and obtain some results as mentioned in the abstract.

2000 Mathematics Subject Classification: 06F35, 03G25
Keywords: S-absorbing set, (P)-decomposition, (P)-closed union, positive implicative hyper K-algebra, quasi union hyper K-algebra.

2. Preliminaries

Let H be a non-empty set, the set of all non-empty subset of H is denoted by $\mathcal{P}^*(H)$. A *hyperoperation* on H is a map $\circ : H \times H \to \mathcal{P}^*(H)$, where $(a, b) \to a \circ b$ for all $a, b \in H$. A set H, endowed with a hyperoperation, "$\circ$", is called a *hyperstructure*. If $A, B \subseteq H$, then $A \circ B = \bigcup_{a \in A, b \in B} a \circ b$.

Definition 1. [4, 7] Let H be a non-empty set containing a constant "0" and "$\circ$" be a hyperoperation on H. Then H is called a *hyper K-algebra* (*hyper BCK-algebra*) if it satisfies K1 – K5 (respectively: HK1 – HK4).

K1: $(x \circ z) \circ (y \circ z) < x \circ y$,	HK1: $(x \circ z) \circ (y \circ z) \ll x \circ y$,
K2: $(x \circ y) \circ z = (x \circ z) \circ y$,	HK2: $(x \circ y) \circ z = (x \circ z) \circ y$,
K3: $x < x$,	HK3: $x \circ H \ll x$,
K4: $x < y,\ y < x$, then $x = y$,	HK4: $x \ll y,\ y \ll x$, then $x = y$,
K5: $0 < x$	

for all $x, y, z \in H$, where $x < y$ ($x \ll y$) means $0 \in x \circ y$. Moreover for any $A, B \subseteq H$, $A < B$ if $\exists\, a \in A$, $\exists\, b \in B$ such that $a < b$ and $A \ll B$ if $\forall\, a \in A$, $\exists\, b \in B$ such that $a \ll b$.

For briefly the readers could see some definitions and results about hyper K-algebra and hyper BCK-algebra in [4, 7]. In the sequel H always denotes a hyper K-algebra. If $I \subset H$, then $I' = H \setminus I$ and $I^* = I' \cup \{0\}$.

Definition 2. [5] An element $b \in H$ is called a *left* (*right*) *scalar* if $|b \circ x| = 1$ ($|x \circ b| = 1$) for all $x \in H$. An element is called *scalar* if it is a left and a right scalar.

Theorem 1. [10] *Let $(H_i, \circ_i, 0)$, $i \in \Omega$ be a family of hyper K-algebras such that $H_i \cap H_j = \{0\}$, $i \neq j \in \Omega$, 0 be a left scalar in each H_i, $i \in \Omega$, $H = \bigcup_{i \in \Omega} H$ and "$\circ$" on H is defined as follows:*

$$x \circ y := \begin{cases} x \circ_i y & \text{if } x, y \in H_i, \\ \{x\} & \text{if } x \in H_i,\ y \notin H_i. \end{cases}$$

Then $(H, \circ, 0)$ is hyper K-algebra denoted by $H = \oplus_{i \in \Omega} H_i$. □

Definition 3. [1, 2] A hyper K-algebra H is called

(*i*) *weak implicative* if $x < x \circ (y \circ x)$,

(*ii*) *implicative* if $x \in x \circ (y \circ x)$,

(*iii*) *strong implicative* if $x \circ 0 \subseteq x \circ (y \circ x)$,

(*iv*) *positive implicative* if $(x \circ y) \circ z = (x \circ z) \circ (y \circ z)$

holds for all $x, y, z \in H$.

Definition 4. [9, 4, 11] A non-empty subset I of H is said to be *closed* if $x < y$ and $y \in I$ imply $x \in I$, and it is said to be a *hyper K-ideal* of H if $x \circ y < I$ and $y \in I$ imply $x \in I$.

Theorem 2. [9] *Any hyper K-ideal of H is closed.* $\square$

Definition 5. [9] Let I and S be non-empty subsets of H. Then we say that I is *S-absorbing* if $x \in I$ and $y \in S$ imply $x \circ y \subseteq I$. In the case $S = I'$ or $S = I^*$ we say that I is *C-absorbing* or *C^*-absorbing*, respectively.

Theorem 3. [9] *Let H be a hyper BCK-algebra and I be a hyper BCK-ideal or closed set. Then I is H-absorbing.* $\square$

Definition 6. [9] A hyper K-algebra H is called *(P)-decomposable* if there exists a non-trivial family $\{A_i\}_{i\in\Lambda}$ of subsets of H with P-property such that $H \neq \{A_i\}$ for all $i \in \Lambda$, $H = \bigcup_{i\in\Lambda} A_i$ and $A_i \cap A_j = \{0\}$, $i \neq j$.

In this case, we write $H = \oplus_{i\in\Lambda} A_i(\mathrm{P})$ and say that $\{A_i\}_{i\in\Lambda}$ is a (P)-decomposition for H. If each A_i, $i \in \Lambda$, is S-absorbing we write $H \overset{\mathrm{S}}{=} \oplus_{i\in\Lambda} A_i(\mathrm{P})$. Moreover, we say that this decomposition is *closed union*, in short (P)-CUD, if $\cup_{i\in\Delta} A_i$ has P-property for any non-empty subset Δ of Λ. If there exists a (P)-CUD for H, then we say that H is a (P)-CUD.

Theorem 4. [9] *Let $H \overset{\mathrm{H}}{=} A \oplus B$. Then 0 is a left scalar element.* $\square$

Theorem 5. [9] *Let $H \overset{\mathrm{C}^*}{=} \oplus_{i\in\Lambda} A_i$(hyper K-ideal). Then H is (hyper K-ideal)-CUD and $H \overset{\mathrm{C}^*}{=} I \oplus I^*$(hyper K-ideal), where $I = \cup_{i\in\Delta} A_i$ for any non-empty subset Δ of Λ.* $\square$

Theorem 6. [10] *Let $(H, \circ, 0)$ be a hyper BCK-algebra. Then $H = \oplus_{i\in\Omega} H_i$ (hyper BCK-algebra) if and only if $H = \oplus_{i\in\Omega} H_i$(hyper BCK-ideal).* $\square$

3. Quasi union hyper K-algebra

In this section we give a method to construct a hyper K-algebra of order α where α is a given cardinal number. Also we introduce the concept of quasi union hyper K-algebra and investigate some properties of it.

Remark 1. Let H be a set containing "0", $\mathcal{P}_0(H) = \{A \subseteq H : 0 \in A\}$ and $\mathcal{S} = \{f | f : H \to \mathcal{P}_0(H) \text{ is a function}\}$. For convenience we use F^x instead of $f(x)$ for any $f \in \mathcal{S}$. Clearly $\mathcal{S} \neq \emptyset$, because the functions $f, g : H \to \mathcal{P}_0(H)$, where $f(x) = \{0\}$ and $g(x) = \{0, x\}$ for all $x \in H$, are members of $\mathcal{S}$.

Theorem 7. *Let $H = X \cup \{0\}$, where X is a non-empty set. Then for any $f \in \mathcal{S}$ we can define the hyperoperation $\circ_f : H \times H \longrightarrow \mathcal{P}^*(H)$ by putting:*

$$x \circ_f y := \begin{cases} F^x & \text{if } x = y, \\ \{x\} & \text{otherwise.} \end{cases}$$

Moreover, the following statements are equivalent

(i) $(H, \circ_f, 0)$ *is a hyper K-algebra,*

(ii) $F^x \circ_f y = F^x$ *for all* $y \neq x, y \in H$,

(iii) $x \neq y$ *and* $y \in F^x$ *imply* $y \in F^y$ *and* $F^y \subseteq F^x$.

Proof. By Remark 1, $u = v$ implies $f(u) = F^u = f(v) = F^v$. This yields that "$\circ_f$" is well-defined and hence it is a hyperoperation on H.

$(i) \Rightarrow (ii)$. Let $(H, \circ_f, 0)$ be a hyper K-algebra and $y \neq x, y \in H$. Then by definition of "$\circ_f$" and K2 we have:

$$F^x \circ_f y = (x \circ_f x) \circ_f y = (x \circ_f y) \circ_f x = (x \circ_f x) = F^x.$$

$(ii) \Rightarrow (i)$. To do this, we show that H satisfies K1 – K5. Since $0 \in F^x = x \circ_f x$, hence $x < x$ for all $x \in H$ and K3 holds. Moreover by definition of $\circ_f$ we have $0 \circ_f x = \{0\}$ for all $x \neq 0$, that is $0 < x$. Thus K5 holds.

To check K1, K2 and K4, we consider the following five cases:
(I) $x \neq y$, $x \neq z$ and $y \neq z$, (II) $x = y \neq z$, (III) $x = z \neq y$,
(IV) $x \neq y = z$, (V) $x = y = z$.

K1: $(x \circ_f z) \circ_f (y \circ_f z) < x \circ_f y$.
For convenience, we put $(x \circ_f z) \circ_f (y \circ_f z) = A$ and $x \circ_f y = B$. If (I) holds, then $A = \{x\} = B$ and by K3, $A < B$. If (II) holds, then $A = F^x = B$, therefore $A < B$. If (III) holds, then by (ii), $A = F^x \circ_f y = F^x$ and $B = \{x\}$. Since $0 \in F^x$ and K5 holds, then $A < B$. If (IV) holds, then $A = x \circ_f F^y$ and $B = \{x\}$. Since $0 \in F^y$ and K3 holds, thus $x \in x \circ_f 0 \subseteq x \circ_f F^y$ and it yields that $A < B$. If (V) holds, then $A = F^x \circ_f F^x$ and $B = F^x$. Since $0 \in F^x$ and K5 holds, then $A < B$. Therefore K1 holds in all cases.

K2: $(x \circ_f y) \circ_f z = (x \circ_f z) \circ_f y$.
We put $A = (x \circ_f y) \circ_f z$ and $B = (x \circ_f z) \circ_f y$ and show that $A = B$ for all cases (I) – (V). If (I) holds, then $A = \{x\} = B$. If (II) holds, then by (ii) we have $A = F^x \circ_f z = F^x$ and $B = F^x$, so $A = B$. If (III) holds, similar to the proof of case (II) we have $A = B$. If (IV) holds, then $A = \{x\} = B$. If (V) holds, then $A = B$. Finally we show that K4 holds, i.e., $x < y,\ y < x \Rightarrow x = y$. Suppose $x < y,\ y < x$ and $x \neq y$. Then we

have $0 \in x \circ_f y = \{x\}$ and $0 \in y \circ_f x = \{y\}$. Hence $x = y = 0$ which is a contradiction to $x \neq y$. Thus $(\mathrm{H}, \circ_f, 0)$ is hyper K-algebra.

$(ii) \Rightarrow (iii)$. Let $y \neq x$ and $y \in F^x$. Then, according to the definition, $u \circ_f y = \{u\}$ where $u \neq y$. Therefore

$$F^x \circ_f y = \cup_{u \neq y, u \in F^x} (u \circ_f y) \cup y \circ y = (F^x - \{y\}) \cup F^y. \tag{1}$$

By (ii), $F^x \circ_f y = F^x$. So equality (1) yields that $y \in F^y$ and $F^y \subseteq F^x$, that is, (iii) holds.

$(iii) \Rightarrow (ii)$. Suppose $x \neq y$. We consider two cases (a): $y \notin F^x$ and (b): $y \in F^x$. If (a) holds , then $u \neq y$ for all $u \in F^x$. Thus by definition of $\circ_f$ we have $F^x \circ_f y = F^x$, hence (ii) holds. If (b) holds, then by equality (1) and hypothesis $(F^y \subseteq F^x)$ we get that $F^x \circ_f y = F^x$. □

Definition 7. The hyperoperation and hyper K-algebra which have been introduced in Theorem 7 are called a *quasi union hyper operation* and a *quasi union hyper K-algebra*, respectively.

Corollary 1. *For any set X such that $0 \notin X$ and $f(x) \in \{\{0\}, \{0, x\}\}$ for all $f \in \mathcal{S}$ and $x \in H$ there is a quasi union hyper K-algebra on $H = X \cup \{0\}$ with the hyperoperation defined as follows:*

$$x \circ y := \begin{cases} F^x = \{0\} \text{ or } F^x = \{0, x\} & \text{if } x = y \\ \{x\} & \text{otherwise.} \end{cases}$$

Proof. Since $F^x \circ y = F^x$, for all $x \neq y \in H$, thus by Theorem 7 (ii) and Definition 7, $(H, \circ, 0)$ is a quasi union hyper K-algebra. □

Example 1. Let $X = \{1, 2\}$. Then according to Corollary 1, each of the following tables are quasi union hyper K-algebra on $H = \{0, 1, 2\}$.

$\circ_1$	0	1	2
0	{0}	{0}	{0}
1	{1}	{0}	{1}
2	{2}	{2}	{0}

$\circ_2$	0	1	2
0	{0}	{0}	{0}
1	{1}	{0,1}	{1}
2	{2}	{2}	{0}

$\circ_3$	0	1	2
0	{0}	{0}	{0}
1	{1}	{0}	{1}
2	{2}	{2}	{0,2}

$\circ_4$	0	1	2
0	{0,1}	{0}	{0}
1	{1}	{0,1}	{1}
2	{2}	{2}	{0,1,2}

Corollary 2. *Let H be a quasi union hyper K-algebra and $x \neq y$. If $y \in F^x$ and $x \in F^y$, then $F^y = F^x$.*

The proof follows from Theorem 7 (iii).

4. Some results on quasi union hyper K-algebras

Theorem 8. *Let H be a quasi union hyper K-algebra. Then the following statements are equivalent:*

(i) *H is positive implicative hyper K-algebra,*

(ii) *$F^x = \{0\}$ or $F^x = \{0, x\}$ for all $x \in H$,*

(iii) *H is a hyper BCK-algebra.*

Proof. $(i) \Rightarrow (ii)$. Let H be positive implicative, i.e., $(x \circ y) \circ z = (x \circ z) \circ (y \circ z)$ for all $x, y, z \in H$ and $u \in F^x$. If $u \neq x$, since $(u \circ x) \circ x = (u \circ x) \circ (x \circ x)$ we get that $\{u\} = \{u\} \circ (x \circ x)$. From $u \in F^x = x \circ x$, we conclude that $0 \in \{u\} \circ (x \circ x) = \{u\}$. So $u = 0$ and $F^x = \{0\}$ or $F^x = \{0, x\}$ for all $x \in H$.

$(ii) \Rightarrow (i)$. Suppose $F^x = \{0\}$ or $F^x = \{0, x\}$ for all $x \in H$. We show that H is a positive implicative hyper K-algebra, i.e., H satisfies the following identity:

$$(x \circ y) \circ z = (x \circ z) \circ (y \circ z). \tag{2}$$

We prove it by considering the following cases: (I) $x \circ x = \{0\}$, (II) $x \circ x = \{0, x\}$.

Case 1. $x \neq y,\ x \neq z,\ y \neq z$.

$$(x \circ y) \circ z = \{x\} \circ z = \{x\} \text{ and } (x \circ z) \circ (y \circ z) = \{x\} \circ \{y\} = \{x\}.$$

Case 2. $x = y \neq z$. If (I) holds, then

$$(x \circ y) \circ z = \{0\} \circ z = \{0\} \text{ and } (x \circ z) \circ (y \circ z) = \{x\} \circ \{x\} = \{0\}.$$

If (II) holds, then

$$(x \circ y) \circ z = \{0, x\} \circ z = \{0, x\} \text{ and } (x \circ z) \circ (y \circ z) = \{x\} \circ \{x\} = \{0, x\}.$$

Case 3. $x = z \neq y$. By K2 and the proof of Case 2, (2) holds.

Case 4. $x \neq y = z$. By considering $F^0 = 0 \circ 0 = \{0\}$, if (I) holds then

$$(x \circ y) \circ z = \{x\} \circ z = \{x\} \text{ and } (x \circ z) \circ (y \circ z) = \{x\} \circ \{0\} = \{x\}.$$

If (II) holds, then

$$(x \circ y) \circ z = \{x\} \circ z = \{x\} \text{ and } (x \circ z) \circ (y \circ z) = \{x\} \circ \{0, y\} = \{x\}.$$

Case 5. $x = y = z$. By considering $F^0 = 0 \circ 0 = \{0\}$, if (I) holds then

$$(x \circ y) \circ z = \{0\} \circ x = \{0\} \text{ and } (x \circ z) \circ (y \circ z) = \{0\} \circ \{0\} = \{0\}.$$

If (II) holds, then $(x \circ y) \circ z = \{0, x\} \circ x = \{0, x\}$ and $(x \circ z) \circ (y \circ z) = \{0, x\} \circ \{0, x\} = \{0, x\}$. These cases imply that the identity (2) is satisfied, thus H is a positive implicative hyper K-algebra.

$(ii) \Rightarrow (iii)$. Let $F^x = \{0\}$ or $F^x = \{0, x\}$ for all $x \in H$. We show that H is a hyper BCK-algebra. To do this, since each hyper K-algebra satisfies HK2 and HK4, it is sufficient to prove H satisfies HK1 and HK3. Now we show that HK1 holds, i.e., $(x \circ z) \circ (y \circ z) \ll x \circ y$ for all $x, y \in H$. We prove it by considering the following cases:

$$\text{(I) } x \circ x = \{0\}, \qquad \text{(II) } x \circ x = \{0, x\}.$$

Case 1. $x \neq y,\ x \neq z,\ y \neq z$.

$$(x \circ z) \circ (y \circ z) = \{x\} \ll x \circ y = \{x\}.$$

Case 2. $x = y \neq z$.

$$(x \circ z) \circ (y \circ z) = \{x\} \circ \{x\} = x \circ x \ll x \circ y = x \circ x.$$

Case 3. $x = z \neq y$. By considering $F^0 = 0 \circ 0 = \{0\}$, if (I) holds then

$$(x \circ z) \circ (y \circ z) = \{0\} \circ \{y\} = \{0\} \ll x \circ y = \{x\}.$$

If (II) holds, then $(x \circ z) \circ (y \circ z) = \{0, x\} \circ \{y\} = \{0, x\} \ll x \circ y = \{x\}$.

Case 4. $x \neq y = z$. If (I) holds, then $(x \circ z) \circ (y \circ z) = \{x\} \circ \{0\} = \{x\} \ll \{x\}$. If (II) holds, then $(x \circ z) \circ (y \circ z) = \{x\} \circ \{0, y\} = \{x\} \ll x \circ y = \{x\}$.

Case 5. $x = y = z$. If (I) holds, then $(x \circ z) \circ (y \circ z) = \{0\} \ll x \circ y = \{0\}$. If (II) holds, then $(x \circ z) \circ (y \circ z) = \{0, x\} \ll x \circ y = \{0, x\}$.

Therefore HK1 holds. Finally since $0 \ll x$, $x \ll x$, hence $\{0, x\} \ll x$. Therefore by considering "$\circ$" of H we have $x \circ y \ll x$ for all $x, y \in H$, i.e., HK3 holds. Thus H is a hyper BCK-algebra.

$(iii) \Rightarrow (ii)$. Let H be a quasi union hyper BCK-algebra. Then $F^0 = 0 \circ 0 = \{0\}$. So, let $u \in F^x$ and $u \neq x$. Then, since $x \circ x \ll x$, we have $u \ll x$ or $0 \in u \circ x = \{u\}$. This implies that $u = 0$, hence $F^x = \{0\}$ or $F^x = \{0, x\}$ for all $x \in H$. □

Theorem 9. *Any quasi union hyper K-algebra H is implicative.*

Proof. Let H be a quasi union hyper K-algebra. By considering Definition 3, it is enough to show that $x \in x \circ (y \circ x)$ for all $x, y \in H$. Let $x, y \in H$. Then if $x \neq y$, we have $x \circ (y \circ x) = \{x\}$ and if $x = y$, then $x \in x \circ (x \circ x)$. Because $0 \in x \circ x$. Hence we have $x \in x \circ (y \circ x)$, for any $x, y \in H$. □

Theorem 10. *Let H be a quasi union hyper K-algebra. Then H is strong implicative if and only if $F^0 = \{0\}$.*

Proof. Let H be a strong implicative quasi union hyper K-algebra. Then $x \circ 0 \subseteq x \circ (y \circ x)$ for all $x, y \in H$. If $x = 0$ and $y \neq 0$ we have $0 \circ 0 \subseteq 0 \circ (y \circ 0) = \{0\}$. Hence $0 \circ 0 = F^0 = \{0\}$. Conversely, suppose $F^0 = \{0\}$. We prove that $x \circ 0 \subseteq x \circ (y \circ x)$ for all $x, y \in H$. By considering $F^0 = 0 \circ 0 = \{0\}$, if $x \neq y$, then we have $x \circ 0 = \{x\} = x \circ (y \circ x)$. If $x = y$, then we have $x \circ 0 = \{x\} \subseteq x \circ (x \circ x)$, because $0 \in x \circ x$ and $x \circ 0 = \{x\}$. Therefore H is a strong implicative hyper K-algebra. □

Theorem 11. *If $(H, \circ, 0)$ is a quasi union hyper K-algebra, then for any $x \in H \setminus \{0\}$, $A_x = \{0, x\}$ is a hyper K-ideal of H.*

Proof. Suppose $v \circ y < A_x$ and $y \in A_x$. We show that $v \in A_x$. If $v \in \{0, x\}$, then we are done. Otherwise, we have $v \circ y = \{v\} < \{0, x\}$. This implies that $v < 0$ or $v < x$. Since $v \neq 0, x$, from these we conclude that $0 \in v \circ 0 = \{v\}$ or $0 \in v \circ x = \{v\}$. Hence $v = 0$, which is a contradiction. Therefore $v \in \{0, x\}$ and hence A_x is a hyper K-ideal of H. □

Theorem 12. *Let H be a quasi union hyper K-algebra. Then $H \overset{\mathrm{C}}{=} \oplus_{x \in H \setminus \{0\}} A_x$ (hyper K-ideal).*

Proof. By considering Definition 6 and Theorem 11, it is enough to show that for all $x \in H \setminus \{0\}$, $A_x = \{0, x\}$ is C-absorbing. Suppose $t \notin \{0, x\}$, since $u \circ t = \{u\} \subseteq A_x$ for all $u \in \{0, x\}$, we conclude that A_x is C-absorbing. □

Corollary 3. *Let H be a quasi union hyper K-algebra and $0 \circ 0 = \{0\}$. Then $H \overset{\mathrm{C}^*}{=} \oplus_{x \in H \setminus \{0\}} A_x$(hyper K-ideal).*

Proof. The proof follows from Definition 5 and Theorem 12. □

By the following example we show that there is a quasi union hyper K-algebra such that $A_x = \{0, x\}$ is not C^*-absorbing.

Example 2. Consider $H = \{0, 1, 2\}$ with the following structure:

$\circ$	0	1	2
0	{0,1}	{0}	{0}
1	{1}	{0,1}	{1}
2	{2}	{2}	{0,1,2}

Then $(H, \circ, 0)$ is a quasi hyper K-algebra and $A_2 = \{0, 2\}$ is not C^*-absorbing, because $0 \circ 0 = \{0, 1\} \nsubseteq A_2$.

Corollary 4. *Let H be a quasi union hyper K-algebra. Then $H \stackrel{\text{C}}{=} \oplus_{x \in H \setminus \{0\}} A_x$ (closed set).*

Proof. Since any hyper K-ideal is closed set, the proof follows from Theorem 12. □

Lemma 1. *Any hyper K-ideal I of hyper BCK-algebra H is a hyper BCK-ideal too.*

Proof. Let $x \circ y \ll I$ and $y \in I$. Then $x \circ y < I$. Since I is a hyper K-ideal and $y \in H$, we conclude that $x \in I$. Hence I is a hyper BCK-ideal of H. □

Corollary 5. *Let H be a quasi union hyper BCK-algebra. Then $H \stackrel{\text{H}}{=} \oplus_{x \in H \setminus \{0\}} A_x$(hyper BCK-ideal).*

Proof. Since by Theorem 3 any hyper BCK-ideal is H-absorbing, then by using Lemma 1 and Theorem 12 we get that $H \stackrel{\text{H}}{=} \oplus_{x \in H} \{0, x\}$(hyper BCK-ideal). □

Corollary 6. *Let H be a quasi union hyper BCK-algebra. Then $H \stackrel{\text{H}}{=} \oplus_{x \in H \setminus \{0\}} A_x$ (hyper BCK-algebra), i.e., it is a union of family of hyper BCK-algebras.*

Proof. The proof follows from Corollary 5 and Theorem 6. □

Theorem 13. *Any quasi union hyper K-algebra H is (hyper K-ideal)-CUD.*

Proof. By Theorem 12, $H \stackrel{\text{C}}{=} \oplus_{x \in H \setminus \{0\}} A_x$(hyper K-ideal). By Theorem 1, we must show that for any non-empty subset B of $H \setminus \{0\}$, $\cup_{x \in B} A_x$ is a hyper K-ideal of H. Suppose $u \circ y < \cup_{x \in B} A_x$ and $y \in \cup_{x \in B} A_x$. If $u \neq y$ then $u \circ y = \{u\} < \cup_{x \in B} A_x$. This yields that for some $x \in B$, $u < A_x$. Since A_x is a hyper K-ideal and by Theorem 2 it is a closed set, we conclude that $u \in A_x$. Therefore $u \in \cup_{x \in B} A_x$. If $u = y$, then $u \in \cup_{x \in B} A_x$. Thus $\cup_{x \in B} A_x$ is a hyper K-ideal of H, i.e., H is a (hyper K-ideal)-CUD. □

Theorem 14. *Let H be a quasi union hyper K-algebra and I be a subset of H containing 0. Then I is a hyper K-ideal of H.*

Proof. By Theorem 12 we have $H \overset{\mathrm{C}}{=} \oplus_{x\in H\setminus\{0\}} A_x$(hyper K-ideal). Since $I = \cup_{x\in I}\{0, x\}$, by Theorem 13, I is a hyper K-ideal of H. □

Now, we proceed to find some relations between a quasi union hyper K-algebra and a family of hyper K-algebras of type $H \overset{\mathrm{C}}{=} \oplus_{i\in\Lambda} A_i$(hyper K-ideal) where, $|A_i| = 2$. In particular, we show that whenever $|H| \geqslant 4$, any type of these hyper K-algebras is a quasi union hyper K-algebra.

Remark 2. Let $H \overset{\mathrm{C}}{=} \oplus_{i\in\Lambda} A_i$(hyper K-ideal) where, $|A_i| = 2$. Since $|A_i| = 2$, we have $A_i = \{0, x\}$ for a nonzero element $x \in H$. Hence for convenience we write A_x instead of A_i and hence $H \overset{\mathrm{C}}{=} \oplus_{x\in H\setminus\{0\}} A_x$(hyper K-ideal).

Theorem 15. *Let $H \overset{\mathrm{C}}{=} \oplus_{x\in H\setminus\{0\}} A_x$(hyper K-ideal) and $|H| \geqslant 4$. Then H is a quasi union hyper K-algebra.*

Proof. Since by K3, we have $0 \in x \circ x = F^x$, according to Theorem 7, it is sufficient to show that $x \circ y = \{x\}$ for all $x \neq y$. Suppose $u \in x \circ y$ and $x \neq y$. Then by considering the following three cases we prove $u = x$.

$$\text{(I) } y = 0, \quad \text{(II) } x \neq 0 \text{ and } y \neq 0, \quad \text{(III) } x = 0.$$

If (I) holds, then since $x \circ 0 < A_u$ and A_u is a hyper K-ideal, we conclude that $x \in A_u$. Since $x \neq y = 0$, then $x = u$. If (II) holds, since $y \notin A_x$ and A_x is C-absorbing, we get that $x \circ y \subseteq A_x$. Thus $u \in A_x$. We show that $u \neq 0$. If $u = 0$, then $x < y$ and $x \in A_y$, because any hyper K-ideal is closed set. This yields that $x = y$, which is a contradiction. Therefore $u = x$. If (III) holds, then since $|H| \geqslant 4$ we have at least two nonzero elements $t, z \in H$ different from y. Therefore $0 \circ y \subseteq A_t \cap A_z = \{0\}$, because A_x and A_t are C-absorbing. This yield that $0 \circ y = \{0\}$, or $u = x = 0$. Therefore $x \circ y = \{x\}$, where $x \neq y \in H$. □

Theorem 15 is not true in general.

Example 3. Let $H = \{0, 1, 2\}$ with the following structure:

$\circ$	0	1	2
0	{0}	{0,2}	{0,1}
1	{1}	{0,1}	{1}
2	{2}	{2}	{0,2}

Then H= $(H, \circ, 0)$ is a hyper K-algebra such that $H \overset{\mathrm{C}}{=} \{0, 1\} \oplus \{0, 2\}$(hyper K-ideal) and $0 \circ y \neq \{0\}$ where $y \neq 0$. Also this example shows that even if each A_x in Theorem 15 is C^*-absorbing, then H may not be a quasi union hyper K-algebra, whenever $|H| = 3$.

Lemma 2. *Let* $H \overset{\mathrm{H}}{=} \oplus_{x\in H\setminus\{0\}} A_x$*(closed set) and* $|H| \geqslant 3$*. Then 0 is a left scalar.*

Proof. Since $|H| \geqslant 3$ the proof follows from Theorems 5 and 4. $\square$

Theorem 16. *Let* $H \overset{\mathrm{H}}{=} \oplus_{x\in H\setminus\{0\}} A_x$*(closed set) and* $|H| \geqslant 3$*. Then* $x \circ y$ $=\{x\}$ *for* $x \neq y$*.*

Proof. By Lemma 2 we conclude that $0 \circ y = \{0\}$ for all $y \in H$. Now let $0 \neq x \neq y$. On the contrary, suppose $x \circ y \neq \{x\}$. Since A_x is H-absorbing we have $x \circ y \subseteq A_x = \{0, x\}$. If $x \circ y = \{0, x\}$ or $\{0\}$, then $x < y$. In this case if $y = 0$ we conclude that $x = 0$, which is a contradiction. Otherwise, $y \neq 0$, we get that $x \in A_y$, because A_y is a closed set and $y \in A_y$. This yields that $x = y$ which is also a contradiction. Hence $x \circ y = \{x\}$. So, $x \neq y$. $\square$

Theorem 16 is not true in general.

Example 4. Let $H = \{0, 1\}$ with the following structure:

$\circ$	0	1
0	{0}	{0,1}
1	{1}	{0,1}

Then $H=$ $(H, \circ, 0)$ is a hyper K-algebra such that $0 \circ 1 \neq \{0\}$.

Theorem 17. *Let* $H \overset{\mathrm{H}}{=} \oplus_{x\in H\setminus\{0\}} A_x$ *(closed set) and* $|H| \geqslant 3$*. Then* 0 *is a scalar and* $x \circ y$ $=\{x\}$ *for* $x \neq y$*.*

Proof. By Theorem 16, $a \circ 0 = \{a\}$ and $0 \circ a = \{0\}$ while $a \neq 0$. Also by Lemma 2 we have $0 \circ 0 = \{0\}$. Hence 0 is scalar. The remaining of the proof follows from Theorem 16. $\square$

Corollary 7. *Let* $H \overset{\mathrm{H}}{=} \oplus_{x\in H\setminus\{0\}} A_x$*(hyper K-ideal) and* $|H| \geqslant 3$*. Then* 0 *is a scalar and* $x \circ y$ $=\{x\}$ *for* $x \neq y$*.*

The proof follows from Theorems 2 and 17.

Theorem 18. *Let* $H \overset{\mathrm{H}}{=} \oplus_{x\in H\setminus\{0\}} A_x$*(closed set) and* $|H| \geqslant 3$*. Then H is a positive (strong) implicative quasi union hyper BCK-algebra.*

Proof. By hypothesis and Theorem 17, we have $0 \circ 0 = \{0\}$ and $x \circ y = \{x\}$, where $x \neq y$. Since A_x is H-absorbing we have $x \circ x \subseteq A_x$, for all $x \in H$. Hence $x \circ x = \{0\}$ or $x \circ x = \{0, x\}$. Therefore these imply that

$$x \circ y = \begin{cases} \{0\} \ or \ \{0, x\} & \text{if } x = y, \\ \{x\} & \text{otherwise.} \end{cases}$$

So the proof follows from Corollary 1 and Theorems 8 and 10. □

References

[1] **R. A. Borzooei, A. Borumand Saeid and M. M. Zahedi**: (*Strong, Weak) implicative hyper K-algebra*, 8th In. Conference on AHM (Greece) (2002), 103 – 114.

[2] **R. A. Borzooei, P. Corsini and M. M. Zahedi**: *Some kinds of positive implicative hyper K-ideals*, J. Discrete Math. and Crypyography **6** (2003), 113 – 121.

[3] **R. A. Borzooei and H. Harizavi**: *On decomposable hyper BCK-algebras*, Quasigroups and Related Systems **13** (2005), 193 – 202.

[4] **R. A. Borzooei, A. Hasankhani, M. M. Zahedi and Y. B. Jun**: *On hyper K-algebras*, Math. Japon. **52** (2000), 113 – 121.

[5] **P. Corsini**: *Prolegomena of hypergroup theory*, Aviani Editore, Italy, 1993.

[6] **Y. Imai and K. Isêki**: *On axiom systems of propositional calculi XIV*, Proc. Japan Academy **42** (1966), 19 – 22.

[7] **Y. B. Jun, M. M. Zahedi, X. L. Xin and R. A. Borzooei**: *On hyper BCK-algebra*, Italian J. Pure Appl. Math. **10** (2000), 127 – 136.

[8] **F. Marty**: *Sur une generalization de la notion de groups*, 8th congress Math. Scandinavies, Stockhholm, 1934, 45 – 49.

[9] **M. A. Nasr-Azadani and M. M. Zahedi**: *S-absorbing set and (P)-decomposition in hyper algebras*, (in preparation).

[10] **M. A. Nasr-Azadani and M. M. Zahedi**: *A note on union of hyper K-algebras*, (in preparation).

[11] **M. M. Zahedi, R. A. Borzooei, Y. B. Jun and A. Hasankhani**: *Some results on hyper K-algebra*, Scientiae Math. **3** (2000), 53 – 59.

Department of Mathematics
Shahid Bahonar University of Kerman
Kerman
Iran
E-mail: nasr@shahed.ac.ir, zahedi_mm@mail.uk.ac.ir

Received April 17, 2007

Quasigroups and Related Systems **16** (2008), 89 − 96

A note on a union of hyper K-algebras

Mohammad A. Nasr-Azadani and Mohammad M. Zahedi

Abstract

In this paper, at first by some examples we show that the Theorem 3.7 of [1] is not true in general. Then we give a correct version of it. Moreover we give the notion of a union of a family of hyper K-algebras and investigate some of its properties. Finally by considering the concept of (closed set)-decomposable, we show that a hyper BCK-algebra is (closed set)-decomposable if and only if it is the union of a family of hyper BCK-algebras.

1. Introduction and Preliminaries

The study of BCK-algebra was initiated by Imai and Iséki [2] in 1966 as a generalization of the concept of set-theoretic difference and propositional calculi. Borzooei, et.al. [1, 3] applied the hyper structure to BCK-algebras and introduced the concept of hyper BCK-algebra and K-algebra in which each of them is a generalization of BCK-algebra. They have defined the notion of a union of two hyper K-algebra as an extension of a union of BCK-algebra [1]. Now we follow them and obtain some results such as mentioned in the abstract.

Definition 1. [1, 4] Let H be a non-empty set containing a constant 0 and $\mathcal{P}^*(H)$ be the set of all non-empty subset of H. Then H with hyperoperation $\circ : H \times H \to \mathcal{P}^*(H)$, where $(a, b) \mapsto a \circ b$, is called a *hyper K-algebra* (*hyper BCK-algebra*) if it satisfies $K1 - K5$ (respectively: $HK1 - HK4$)

$K1$: $(x \circ z) \circ (y \circ z) < x \circ y$,	$HK1$: $(x \circ z) \circ (y \circ z) \ll x \circ y$,
$K2$: $(x \circ y) \circ z = (x \circ z) \circ y$,	$HK2$: $(x \circ y) \circ z = (x \circ z) \circ y$,
$K3$: $x < x$,	$HK3$: $x \circ H \ll x$,
$K4$: $x < y,\ y < x$ then $x = y$,	$HK4$: $x \ll y,\ y \ll x$ then $x = y$,
$K5$: $0 < x$,	

2000 Mathematics Subject Classification: 06F35, 03G25
Keywords:(P)-closed union decomposition, union hyper K-algebra, positive implicative and implicative hyper K-algebra, S-absorbing, (P)-Decomposition

for all $x, y, z \in H$, where $x < y (x \ll y)$ means $0 \in x \circ y$. Moreover for any $A, B \subseteq H$, $A < B$ if $\exists\, a \in A$, $\exists\, b \in B$ such that $a < b$ and $A \ll B$ if $\forall\, a \in A$, $\exists\, b \in B$ such that $a \ll b$.

The readers could see some definitions and results about hyper K-algebra and hyper BCK-algebra in [1, 4, 5].

Definition 2. [6] Let I and S be non-empty subsets of H. Then we say that I is *S-absorbing* if $x \in I$ and $y \in S$ then $x \circ y \subseteq I$.

Theorem 1. [6] *Let H be a hyper BCK-algebra and I be a hyper BCK-ideal or closed set. Then I is H-absorbing.*

Definition 3. [6] A hyper K-algebra H is called *(P)-decomposable* if there exists a family $\{A_i\}_{i \in \Omega}$ of subsets of H with *P-property* such that:
(i) $H \neq \{A_i\}$ for all $i \in \Omega$, (ii) $H = \cup_{i \in \Omega} A_i$, (iii) $A_i \cap A_j = \{0\}, i \neq j$.

In this case, we write $H = \oplus_{i \in \Omega} A_i(\mathrm{P})$ and say that $\{A_i\}_{i \in \Omega}$ is a (P)-decomposition for H. If each A_i, $i \in \Omega$, is S-absorbing we write $H \stackrel{\mathrm{S}}{=} \oplus_{i \in \Omega} A_i(\mathrm{P})$. Moreover we say that this decomposition is a *closed union*, in short (P)-CUD, if $\cup_{i \in \Delta} A_i$ has P-property for any non-empty subset Δ of Ω. If there exists a (P)-CUD for H, then we say that H is (P)-CUD.

Theorem 2. [6] *Let $H \stackrel{\mathrm{H}}{=} \oplus_{i \in \Omega} A_i$ (a hyper K-ideal). Then H is (hyper K-ideal)-CUD.*

2. Union hyper K-algebras

In this section at first we show that Theorem 3.7 [1] as follows is not true in general, then we give a correct version of it.

Theorem 3.7 of [1]: *Let$(H_1, \circ_2, 0)$ and $(H_2, \circ_2, 0)$ be hyper K-algebras (resp. hyper BCK-algebras) such that $H_1 \cap H_2 = \{0\}$ and $H = H_1 \cup H_2$. Then $(H, \circ, 0)$ is hyper K-algebra (resp. hyper BCK-algebras), where the hyperoperation $\circ$ on H is defined as follows:*

$$x \circ y := \begin{cases} x \circ_1 y & \text{if } x, y \in H_1, \\ x \circ_2 y & \text{if } x, y \in H_2, \\ \{x\} & \text{otherwise,} \end{cases}$$

for all $x, y \in H$.

Remark 1. This theorem is not true in general. Because we have $0 \circ 0$ is a subset of H_1 and H_2. Hence $0 \circ 0$ must be $\{0\}$ in any H_i, $i = 1, 2$, but the authors have not considered this fact, this yields that $\circ$ is not well-defined. To see this, consider the following example.

Example 1. Let $H_1 = \{0, 1, 2\}$ and $H_2 = \{0, 3, 4\}$. Then $(H_1, \circ_1, 0)$ and $(H_2, \circ_2, 0)$ with hyperoperations $\circ_1$ and $\circ_2$ as follows are hyper K-algebras.

$\circ_1$	0	1	2
0	{0,1}	{0}	{0}
1	{1}	{0,1}	{1}
2	{2}	{2}	{0,1,2}

$\circ_2$	0	3	4
0	{0,3,4}	{0}	{0}
3	{1}	{0,3,4}	{3}
4	{4}	{4}	{0,3,4}.

By the definition of hyper operation $\circ$ for the union of two hyper K-algebras in theorem 3.7 of [1] we have: (i): $0 \circ 0 = \{0, 1\}$, because $0 \in H_1$. (ii): $0 \circ 0 = \{0, 3, 4\}$, because $0 \in H_2$. (iii): $0 \circ 0 = \{0\}$, because $0 \in H_1 \cap H_2$. Thus $\circ$ is not well-defined.

Theorem 3.7 [1] is not correct even if we assume $0 \circ 0 = \{0\}$. For this, consider the following example.

Example 2. Let $H_1 = \{0, 1, 2\}$, $H_2 = \{0, 3, 4\}$ with hyperoperation $\circ_1$ and $\circ_2$ respectively as follows:

$\circ_1$	0	1	2
0	{0}	{0,1}	{0,1,2}
1	{1}	{0,1,2}	{0,1}
2	{2}	{2}	{0,1,2}

$\circ_2$	0	3	4
0	{0}	{0,3}	{0,4}
3	{3}	{0,3,4}	{0,3,4}
4	{4}	{3,4}	{0,3,4}

Then $H_1 = (H, \circ_1, 0)$ and $H_2 = (H, \circ_2, 0)$ are hyper K-algebras and $H_1 \cap H_2 = \{0\}$. Thus by considering the hyperoperation $\circ$ of the theorem 3.7 of [1] we have $H = H_1 \cup H_2 = \{0, 1, 2, 3, 4\}$ with hyperoperation $\circ$ as follows:

$\circ$	0	1	2	3	4
0	{0}	{0,1}	{0,1,2}	{0,3}	{0,4}
1	{1}	{0,1,2}	{0,1}	{1}	{1}
2	{2}	{2}	{0,1,2}	{2}	{2}
3	{3}	{3}	{3}	{0,3,4}	{0,3,4}
4	{4}	{4}	{4}	{3,4}	{0,3,4}

But $(H, \circ, 0)$ is not hyper K-algebra. Since $(1 \circ 1) \circ 3 = \{0, 1, 2, 3\} \neq (1 \circ 3) \circ 1 = \{0, 1, 2\}$, i.e., K2 does not hold.

Now we give not only a correct version of it, but also we extend it.

Theorem 3. *Let $(H_i, \circ_i, 0), i \in \Omega$ be a family of hyper K-algebras such that $H_i \cap H_j = \{0\}, i \neq j \in \Omega$ and 0 be a left scalar in each H_i, $i \in \Omega$. Then $(H, \circ, 0)$ is hyper K-algebra where, $H = \cup_{i\in\Omega} H$ and $\circ$ on H is defined as follows:*

$$x \circ y := \begin{cases} x \circ_i y & \text{if } x, y \in H_i, \\ \{x\} & \text{if } x \in H_i, y \notin H_i. \end{cases}$$

Proof. Since 0 is a left scalar in H_i for all $i \in \Omega$, then $0 \circ 0 = \{0\}$ and $\circ$ is well-defined. Now we prove H satisfies K1-K5. If $x, y, z \in H_i$ for some $i \in \Omega$ then, by hypothesis, H satisfies $K1 - K5$, otherwise we consider the following cases:

(I) $x \in H_i$ and $y, z \notin H_i$,

(II) $x, y \in H_i$ and $z \notin H_i$,

(III) $x, z \in H_i$ and $y \notin H_i$.

K1: $(x \circ z) \circ (y \circ z) < x \circ y, \forall x, y, z \in H$.

If (I) holds and $0 \notin y \circ z$, then $(x \circ z) \circ (y \circ z) = x \circ (y \circ z) = \{x\} < x \circ y = \{x\}$. Otherwise $(x \circ z) \circ (y \circ z) = x \circ (y \circ z) = x \circ 0 < x \circ y = \{x\}$, since $x \in x \circ 0$. If (II) holds, then $(x \circ z) \circ (y \circ z) = x \circ_i y < x \circ_i y$. If (III) holds, by considering $x \circ z \subseteq H_i$ and 0 is a left scalar, then $(x \circ z) \circ (y \circ z) = (x \circ_i z) \circ y = x \circ_i z < x \circ y = \{x\}$.

K2: $(x \circ y) \circ z = x \circ y = (x \circ z) \circ y, \forall x, y, z \in H$.

If (I) holds, then $(x \circ y) \circ z = x \circ z = \{x\} = (x \circ z) \circ y$. If (II) holds, then $(x \circ y) \circ z = x \circ_i y = (x \circ z) \circ y$, even if $0 \in x \circ y$. Since 0 is a left scalar and $x \circ y \subseteq H_i$, so we have $(x \circ y) \circ z = x \circ_i y$ and K2 holds. If (III) holds, then as proof (II) we have $(x \circ y) \circ z = x \circ_i z = (x \circ_i z) \circ y$, and K2 holds.

The proof of **K3** and **K5** are straightforward.

K4: If $x < y$ and $y < x$, then $x = y$. Let $x, y \in H$ be such that $x < y$ and $y < x$. We consider two cases (i): $x \in H_i$, $y \notin H_i$ and (ii): $x, y \in H_i$. If (i) holds, then $0 \in x \circ y = \{x\}$ and $0 \in y \circ x = \{y\}$, hence $x = y = 0$. If (ii) holds, then H satisfies K4. Therefore $(H, \circ, 0)$ is a hyper K-algebra. □

Definition 4. Let $(H_i, \circ_i, 0), i \in \Omega$ be hyper K-algebras such that $H_i \cap H_j = \{0\}$, $i \neq j \in \Omega$ and 0 be a left scalar in each H_i, $i \in \Omega$. Then the hyper K-algebra $(H, \circ, 0)$ which has been defined in Theorem 3 is called the *union* of a family $\{H_i : i \in \Omega\}$ of hyper K-algebras and it is denoted by $H = \oplus_{i\in\Omega} H_i$(hyper K-algebra).

Now we consider some properties of H_i's, $i \in \Omega$ in which they can be extended to $H = \oplus_{i\in\Omega} H_i$ (hyper K-algebra).

Theorem 4. *Let $H = \oplus_{i\in\Omega} H_i$ (hyper K-algebra). Then*

(i) *whenever 0 is a right scalar, the hyper K-algebra H is positive implicative if and only if each H_i, $i \in \Omega$ is positive implicative;*

(ii) *whenever 0 is a right scalar, the hyper K-algebra H is strong implicative if and only if each H_i, $i \in \Omega$ is strong implicative;*

(iii) *the hyper K-algebra H is weak implicative (implicative) if and only if each H_i, $i \in \Omega$ is weak implicative (implicative).*

Proof. Since the proof of $(\Rightarrow)$ is clear, we prove only $(\Leftarrow)$.

(i) Let each H_i, $i \in \Omega$ satisfies the identity:

$$(x \circ y) \circ z = (x \circ z) \circ (y \circ z). \tag{1}$$

We have to show that H satisfies (1) for all $x, y, z \in H$. For briefly, we denote $(x \circ y) \circ z$ by A and $(x \circ z) \circ (y \circ z)$ by B and proceed the proof by following cases.

Case 1: If $x, y, z \in H_i$ for some $i \in \Omega$, then the proof is clear.

Case 2: If $x, y \in H_i$ and $z \in H_j$ where $i \neq j \in \Omega$, then from the definition of $\circ$ and the fact that 0 is a left scalar in each H_i, we have $A = x \circ_i y = B$.

Case 3: If $x, z \in H_i$ and $y \in H_j$ where $i \neq j$, then by K2 and Case 2 the proof is obvious.

Case 4: If $x \in H_i$ and $y, z \in H_j$ where $i \neq j$, then $A = \{x\}$. Since $y \circ z \subseteq H_j$ and 0 is a right scalar, so we have B$=$ $x \circ (y \circ z) = \{x\}$, hence A=B.

Case 5: If $x \in H_i$, $y \in H_j$ and $z \in H_k$ where $i \neq j$, $i \neq k$, $j \neq k$ and $i, j, k \in \Omega$, then $A = \{x\} = B$, which completes the proof of (i).

(ii) We know H is strong implicative if $x \circ 0 \subseteq x \circ (y \circ x)$. Let $x, y \in H$. For $x, y \in H_i$, $i \in \Omega$, the proof is obvious. For $x \in H_i$, $y \in H_j$, where $i \neq j \in \Omega$, the fact that 0 is a right scalar implies $x \circ 0 = \{x\} \subseteq x \circ (y \circ x) = \{x\}$, which completes the proof.

(iii) If H is weak implicative (implicative) then $x < x \circ (y \circ x)$ (resp. $x \in x \circ (y \circ x)$). Thus the case $x, y \in H_i$, $i \in \Omega$, is obvious. In the case $x \in H_i$, $y \in H_j$, $i \neq j \in \Omega$, we have $x \circ (y \circ x) = \{x\}$. Hence $x < x \circ (y \circ x)$ (resp. $x \in x \circ (y \circ x)$). $\square$

Theorem 5. *Let $H = \oplus_{i\in\Omega} H_i$ (hyper K-algebra). Then $H \overset{\mathrm{H}}{=} \oplus_{i\in\Omega} H_i$ (hyper K-ideal), moreover H is (hyper K-ideal)-CUD.*

Proof. It is sufficient to prove that each H_i, $i \in \Omega$, is an H-absorbing hyper K-ideal in H. By Theorem 2, H is (hyper K-ideal)-CUD. Let $x \neq 0$, $x \circ y <$

H_i and $y \in H_i$. If $x \notin H_i$, then we have $0 \in (x \circ y) \circ t = \{x\}$, for some $t \in H_i$, hence $x = 0$ which is a contradiction. So, $x \in H_i$ and H_i is a hyper K-ideal of H. Since $H_i \cap H_j = \{0\}$, $i \neq j$, and $H = \cup H_{i\in\Omega}$, by Definition 3 we conclude that $H = \oplus_{i\in\Omega} H_i$ (hyper K-ideal). Also H_i, $i \in \Omega$ is H-absorbing. Indeed, for $x, y \in H_i$ we have $x \circ y = x \circ_i y \subseteq H_i$. For $x \in H_i$, $y \notin H_i$, we have $x \circ y = \{x\} \subset H_i$. Hence each H_i is H-absorbing. □

Corollary 1. *Let* $H = \oplus_{i\in\Omega} H_i$ (*hyper K-algebra*). *Then* $H \overset{\mathrm{H}}{=} \oplus_{i\in\Omega} H_i$ (*closed set*), *moreover* H *is* (*closed set*)*-CUD*

Proof. Since a hyper K-ideal is closed set, the proof follows from Theorem 5. □

Now we show that there exists a (hyper K-ideal)-decomposable hyper K-algebra such that it is not a union of any family of hyper K-algebras. Hence the converse of Theorem 5, is not true in general. In the next section we show that if H is (hyper BCK-ideal)-decomposable, then it is a union of a family of hyper BCK-algebras.

Example 3. Let $H = \{0, 1, 2, 3\}$ and consider the following table:

$\circ$	0	1	2	3
0	{0}	{0}	{0}	{0}
1	{1}	{0,1}	{0,1}	{1,2}
2	{2}	{2}	{0,2}	{2}
3	{3}	{3}	{3}	{0,3}

Then $(H, \circ, 0)$ is a hyper K-algebra and $H = \{0, 1, 2\} \oplus \{0, 3\}$. It is clear that $\{0, 1, 2\}$ and $\{0, 3\}$ are hyper K-subalgebras of H, but H is not the union of $H_1 = \{0, 1, 2\}$ and $H_2 = \{0, 3\}$ because $1 \circ 3 = \{1, 2\} \neq \{1\}$.

3. Union hyper BCK-algebras

In this section we show that a hyper BCK-algebra is (closed set)-decomposable if and only if it is the union of a family of hyper BCK-algebras.

Lemma 1. *Let* $(H, \circ, 0)$ *be a hyper BCK-algebra. If* $0 \in (x \circ u) \circ 0$ *where* $x, u \in H$, *then* $x \ll u$.

Proof. Suppose $0 \in (x \circ u) \circ 0$, then there is an element $t \in x \circ u$ in which $0 \in t \circ 0$, that is, $t \ll 0$. Since $0 \ll t$ and HK4 holds, we conclude that $t = 0$. Since $t \in x \circ u$, thus $0 \in x \circ u$ or $x \ll u$. □

Theorem 6. *In any hyper BCK-algebra 0 is a scalar.*

Proof. In any hyper BCK-algebra we have $0 \circ x = \{0\}$, i.e., 0 is a left scalar. Now we show that 0 is a right scalar, i.e., $x \circ 0 = \{x\}$. We know $x \in x \circ 0$. Now let $u \in x \circ 0$. Then we show that $u = x$. From $0 \in u \circ u$ and HK2 we get that $0 \in (x \circ 0) \circ u = (x \circ u) \circ 0$. Hence by Lemma 1, $x \ll u$. On the other hand we have $x \circ 0 \ll x$, so $u \ll x$. By considering HK4, from $u \ll x$ and $x \ll u$ we conclude that $u = x$. Thus $x \circ 0 = \{x\}$. $\square$

Theorem 7. *Let $(H_i, \circ_i, 0), i \in \Omega$ be hyper BCK-algebras such that $H_i \cap H_j = \{0\}$, $i \neq j \in \Omega$. Then $(H, \circ, 0)$, where $H = \cup_{i\in\Omega} H$ and*

$$x \circ y := \begin{cases} x \circ_i y & \textit{for} \ \ x, y \in H_i \\ \{x\} & \textit{for} \ \ x \in H_i,\ y \notin H_i, \end{cases}$$

is a hyper BCK-algebra. We denote it by $H = \oplus_{i\in\Omega} H_i$ (hyper BCK-algebra).

Proof. By Lemma 6, the element 0 is a scalar in any hyper BCK-algebra, hence the proof follows from Theorem 3. $\square$

Theorem 8. *Let $H = \oplus_{i\in\Omega} H_i$ (hyper BCK-algebra). Then each H_i, $i \in \Omega$ is weak implicative (implicative, strong implicative) if and only if H is weak implicative (implicative, strong implicative).*

Proof. Since 0 is a scalar, the proof follows from Theorem 4. $\square$

Lemma 2. *Any closed subset of a hyper BCK-algebra is a hyper BCK-subalgebra.* $\square$

Theorem 9. ***(Main Theorem)*** *Let $(H, \circ, 0)$ be a hyper BCK-algebra. Then $H = \oplus_{i\in\Omega} A_i$ (closed set) if and only if $H = \oplus_{i\in\Omega} A_i$ (hyper BCK-algebra).*

Proof. ($\Rightarrow$) Let $H = \oplus_{i\in\Omega} A_i$ (closed set). Then by Lemma 2, A_i is a hyper BCK-subalgebra for any $i \in \Omega$. Now, suppose $0 \neq x \in A_i$ and $y \notin A_i$. In view of Theorem 7, we must show $x \circ y = \{x\}$. We assume that $y \in A_j$ where $i \neq j \in \Omega$. If $0 \in x \circ y$, i.e., $x \ll y$ then $x \in A_j$, because $y \in A_j$ and A_j is a closed set. This is a contradiction to $A_i \cap A_j = \{0\}$. So, let $0 \notin x \circ y$. We know $x \circ y \ll x$. Let $u \in x \circ y$. Then $u \ll x$, and $0 \in (x \circ y) \circ u = (x \circ u) \circ y$. Therefore $0 \in (x \circ u) \circ y$. Hence there exists $t \in x \circ u$ in which, $0 \in t \circ y$, i.e., $t \ll y$. Since $y \in A_j$ and A_j is a closed set we get that $t \in A_j$. By Theorem 1, as A_i is H-absorbing, we have $t \in x \circ u \subseteq A_i$ and consequently

$t \in A_i \cap A_j$. This implies that $t = 0$ and hence $0 \in x \circ u$, i.e., $x \ll u$. On the other hand we had $u \ll x$, these imply that $x = u$. Therefore $x \circ y = \{x\}$.

($\Leftarrow$) The proof follows from Corollary 1. $\square$

Corollary 2. *Let* $(H, \circ, 0)$ *be a hyper BCK-algebra. Then* $H = \oplus_{i \in \Omega} H_i$ *(hyper BCK-algebra) if and only if* $H = \oplus_{i \in \Omega} H_i$ *(hyper BCK-ideal).* $\square$

Corollary 3. *Let* $(H, \circ, 0)$ *be a hyper BCK-algebra. Then* $H = \oplus_{i \in \Omega} H_i$ *(hyper BCK-ideal) if and only if* $H = \oplus_{i \in \Omega} H_i$ *(closed set).* $\square$

References

[1] **R. A. Borzooei, A. Hasankhani, M. M. Zahedi, and Y.B. Jun**: *On hyper K-algebras*, Math. Japonicae **52** (2000), 113 – 121.

[2] **Y. Imai and K. Iséki**: *On axiom systems of propositional calculi xiv*, Proc. Japan Academy **42** (1966), 19 – 22.

[3] **Y. B. Jun, X. L. Xin, E. H. Roh, and M. M. Zahedi**: *Strong on hyper BCK-ideals of hyper BCK-algebras*, Math. Japonicae **51** (2000), 493 – 498.

[4] **Y. B. Jun, M. M. Zahedi, X. L. Xin, and R. A. Borzooei**: *On hyper BCK-algebra*, Italian J. Pure and Appl Math. **10** (2000), 127 – 136.

[5] **M. A. Nasr-Azadani and M. M. Zahedi**: *Quasi union on hyper K-algebras*, Quasigroups and Related Systems **16** (2008), 65 – 74.

[6] **M. A. Nasr-Azadani and M. M. Zahedi**: *S-absorbing set and (P)-decommposition in hyper algebras*, Italian J. Pure and Appl. Math. (2008), (to appear).

Received October 10, 2007

Department of Mathematics, Shahid Bahonar University of Kerman, Kerman, Iran
E-mail: nasr@shahed.ac.ir, zahedi_mm@mail.uk.ac.ir

Quasigroups and Related Systems **16** (2008), 97 – 101

On decomposition of commutative Moufang groupoids

Boris V. Novikov

Abstract

We prove that every commutative Moufang groupoid is a semilattice of Archimedean subgroupoids.

It is well-known that the multiplicative groupoid of an alternative/Jordan algebra satisfies Moufang identities [1, 4]. Therefore it seems interesting to study the structure of such groupoids. In this note we apply to Moufang groupoids an approach which is widespread in semigroup theory – decomposition into a semilattice of subsemigroups [3].

We shall call a groupoid with the identity

$$(xy)(zx) = (x(yz))x \tag{1}$$

a Moufang groupoid. **Everywhere in this article M denotes a commutative Moufang groupoid.**

Theorem 1. *If M consists of idempotents, then it is a semilattice.*

Proof. Under assumption of the theorem it follows from (1) for $y = z$

$$(xy)x = xy \tag{2}$$

Applying (2) to the right part of (1), we get:

$$x(yz) = (xy)(xz) \tag{3}$$

Now define a binary relation $\leqslant$ on M :

$$a \leqslant b \Longleftrightarrow ab = a$$

2000 Mathematics Subject Classification: 20N05
Keywords: Moufang groupoid, semilattice, Archimedean groupoid

and show that it is a partial order.

Indeed, the reflexivity follows from idempotentness, the antisymmetry follows from commutativity. Let $a \leqslant b \leqslant c$. Then

$$ac = (ab)c = (ac)(bc) = (ac)b = (ab)(bc) = ab = a,$$

i.e., $a \leqslant c$.

Further, ab is a greatest lower bound for the pair $\{a, b\}$. Really, $ab \leqslant a$, $ab \leqslant b$ by (2). Suppose that $x \leqslant a$, $x \leqslant b$. Then $(ab)x = (ax)(bx) = x \cdot x = x$, i.e., $x \leqslant ab$. □

Lemma 2. *M is a groupoid with associative powers.*

Proof. For $a \in M$ we shall denote by $a^{(n)}$ an arbitrary term of the length $n \geq 1$, all letters of which are a. If all such terms coincide in M, we denote them by a^n.

We use the induction on length of the term. Let $a^{(k)} = a^k$ for any $k < n$ (for $k = 3$ this follows from commutativity). Consider some term $a^{(n)}$. It can be written in the form $a^{(n)} = a^{(k)}a^{(l)}$, where $k, l \geqslant 1$ and $k + l = n$; in view of commutativity one can assume that $k \leqslant l$.

Suppose that $k \geqslant 2$. Then under hypothesis of the induction

$$a^{(n)} = a^k a^l = (aa^{k-1})(aa^{l-1}) = (a(a^{k-1}a^{l-1}))a = (aa^{n-2})a = aa^{n-1}.$$

Hence all terms of the form $a^{(n)}$ are equal. □

We denote by L_a the left translation corresponding to an element a: $L_a b = ab$. From (1) we have:

$$(xy)^2 = L_x^2 y^2.$$

We generalize this identity:

Lemma 3. $(ab)^{2^n} = L_a^{2^n} b^{2^n}$ *for any* $a, b \in M$, $n \geqslant 0$ (*here powers are defined correctly in view of Lemma* 2).

Proof. Assume that for n the statement is faithful and prove it for $n+1$:

$$(ab)^{2^{n+1}} = [(ab)^2]^{2^n} = [a(ab^2)]^{2^n} = L_a^{2^n}(ab^2)^{2^n} = L_a^{2^n} L_a^{2^n} b^{2^{n+1}} = L_a^{2^{n+1}} b^{2^{n+1}}$$

□

Corollary 4. $(L_{a_1} \dots L_{a_{k-1}} a_k)^{2^n} = L_{a_1}^{2^n} \dots L_{a_{k-1}}^{2^n} a_k^{2^n}$.

Further we shall need one more equality for translations:

Lemma 5. *$L_a^{2n}L_b = L_{L_a^n b}L_a^n$ for any $a, b \in M$, $n \geqslant 1$.*

Proof. For $n = 1$ this statement coincides with (1). The general case is obtained by induction on n. □

Let I_a be denoted the principal ideal, generated by $a \in M$. It is clear that each element from I_a can be written in the form $L_{x_1} \dots L_{x_{k-1}} L_{x_k} a$.

Define relations ρ and σ:

$$a\rho b \Longleftrightarrow \exists n \geqslant 1 \quad a^n \in I_b, \tag{4}$$

$$a\sigma b \Longleftrightarrow a\rho b \quad \& \quad b\rho a. \tag{5}$$

Lemma 6. *σ is a congruence.*

Proof. Reflexivity and symmetry are obvious, it is enough to check transitivity and stability of ρ. Note that one can assume in the definition of ρ that n is the power of the two.

Let $a\rho b$, $b\rho c$, i.e.,

$$a^{2^m} = L_{x_1} \dots L_{x_k} b, \quad b^{2^n} = L_{y_1} \dots L_{y_l} c.$$

By Corollary 4

$$a^{2^{m+n}} = L_{x_1}^{2^n} \dots L_{x_k}^{2^n} b^{2^n} = L_{x_1}^{2^n} \dots L_{x_k}^{2^n} L_{y_1} \dots L_{y_l} c \in I_c,$$

so ρ is transitive.

Now let $a\rho b$, i.e., $a^{2^n} = L_{x_1} \dots L_{x_k} b$, and $c \in M$.

1) Suppose that $k \leqslant n$. Then using several times Lemma 5, we get for some $u_1, \dots, u_k \in M$:

$$(ca)^{2^n} = L_c^{2^n} a^{2^n} = L_c^{2^n} L_{x_1} \dots L_{x_k} b = L_{u_1} \dots L_{u_k} L_c^{2^{n-k}} b \in I_{cb}.$$

2) Let $k > n$. Then $a^{2^{n+k+1}} = L_y L_{x_1} \dots L_{x_k} b$, where $y = a^{2^{n+k+1} - 2^n}$. Since $k + 1 < n + k + 1$, we get the case 1). Consequently, $ca\rho cb$. □

Lemma 7. *M/σ is a semilattice.*

Proof. Obviously, $a\sigma a^2$ for any $a \in M$. So M/σ is an idempotent groupoid. By Theorem 1 it is a semilattice. □

Now let us to consider the structure of σ-classes (of course, they are subgroupoids).

Like to theory of semigroups, we call a groupoid M *Archimedean* if $a\sigma b$ for any $a, b \in M$, where σ is defined by the conditions (4) and (5). It is clear that an Archimedean groupoid is indecomposable into a semilattice of subgroupoids.

Lemma 8. *Let σ be a congruence on M, defined by conditions* (4) *and* (5). *Then each σ-class is Archimedean.*

Proof. Let N is a σ-class, $a, b \in N$. Then

$$a^n = L_{x_1} \dots L_{x_k} b \tag{6}$$

for some $n > 0$, $x_1, \dots, x_k \in M$. We need to prove that in the equality (6) elements $x_1, \dots, x_k$ can be chosen from N.

From (6) and Lemma 5 we have:

$$a^{n+2^k} = L_a^{2^k} L_{x_1} \dots L_{x_k} b = L_{L_a^{2^{k-1}} x_1} L_{L_a^{2^{k-2}} x_2} \dots L_{L_a x_k} b.$$

Show that for any $i \leqslant k$ the element $y_i = L_a^{2^{k-i}} x_i$ is contained in N. Indeed, since $y_i = a(L_a^{2^{k-i}-1} x_i)$ then $y_i \rho a$. On the other hand,

$$a^{n+2^k} = L_{y_1} \dots L_{y_k} b = L_{y_1} \dots L_{y_{i-1}} [(L_{y_{i+1}} \dots L_{y_k} b) y_i],$$

whence $a \rho y_i$. Thereby, $a \sigma y_i$, i.e., $y_i \in N$. □

The final result:

Theorem 9. *A commutative Moufang groupoid is a semilattice of Archimedean groupoids.*

Example. Let a finite semigroup S satisfy the identity $ab = a$ (*a left zero semigroup*), F be a field, $\operatorname{char} F \neq 2$, $A = FS$ be the semigroup algebra. A is a Jordan algebra with respect to the operation $x * y = \frac{1}{2}(xy + yx)$. Denote by A^* its multiplicative groupoid (as is well-known it is Moufang and commutative [4]).

The operation in A^* can be written as follows. For $x = \sum_{a \in S} \alpha_a a \in A^*$, $\alpha_a \in F$, denote $|x| = \sum_{a \in S} \alpha_a$. Then

$$x * y = \frac{1}{2}(|x| y + |y| x)$$

From here $x^{*n} = |x|^{n-1}x$ and $|xy| = |x||y|$. In particular, $x \in \operatorname{Rad} A^*$ iff $|x| = 0$.

Evidently, all elements from $\operatorname{Rad} A^*$ constitute one σ-class. On the other hand, if $x, y \notin \operatorname{Rad} A^*$ then they divide one another. To make sure that, it is enough to put

$$t = \frac{1}{|x|^2}(2|x|y - |y|x);$$

then $y = x * t$. Thus $A^* = \operatorname{Rad} A^* \cup (A^* \setminus \operatorname{Rad} A^*)$ is the decomposition of A^* into Archimedean components.

Finally we discuss some problems which arise here.

1. For loops the identity (1) (*central Moufang identity*) is equal to each of ones $x(y(xz)) = ((xy)x)z$ and $((zx)y)x = z(x(yx))$ (*left and right Moufang identities*). This is valid for multiplicative groupoids of Jordan algebras as well, but not in the general case. So we can consider left and right Moufang (commutative) groupoids. Are there similar decompositions for them?

2. Is there Archimedean decomposition in noncommutative situation? This is the case for semigroups [2].

3. What can one say about the structure of an Archimedean component? For instance, can it contain more than one idempotent (cf. [3], Ex.4.3.2)?

References

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

[2] **S. Bogdanović and M. Ćirić**: *Semigroups*, (Serbian), Prosveta, Niš, 1993.

[3] **A. H. Clifford and G. B. Preston**: *Algebraic theory of semigroups*, Amer. Math. Soc., Providence, 1964.

[4] **N. Jackobson**: *Structure and representations of Jordan algebras*, Amer. Math. Soc. Colloq. Publ., Providence, 1968.

Department of Mechanics and Mathematics
Kharkov National University
Svobody sq. 4
61077 Kharkov
Ukraine
e-mail: boris.v.novikov@univer.kharkov.ua

Received August 16, 2007

Quasigroups and Related Systems **16** (2008), 103 − 118

Greedy quasigroups

Theodore A. Rice

Abstract

The paper investigates the quasigroup Q_s constructed on the well-ordered set of natural numbers by placing a number s known as the *seed* in the top left-hand corner of the body of the multiplication table, and then completing the Latin square using the greedy algorithm that chooses the least possible entry at each stage. The initial motivation comes from the theory of combinatorial games, where Q_0 gives the usual nim sum, while Q_1 gives the corresponding sums for positions in misère nim. The multiplication groups of these quasigroups are analyzed. The alternating group of the natural numbers is a subgroup of the multiplication groups. It is shown that these so-called *greedy quasigroups* Q_s are mutually non-isomorphic. The quasigroup Q_1 is subdirectly irreducible. For $s > 1$, the greedy quasigroups Q_s are simple, and for $s > 2$ they are rigid, possessing no non-trivial automorphisms. Indeed in this case the endomorphism monoid contains just the identity and a single constant. The subquasigroup structures of the Q_s are also determined. While Q_0, Q_1 have uncountably many subquasigroups, and Q_2 has just one proper, non-trivial subquasigroup, Q_s has none for $s > 2$.

1. Introduction

In this paper, quasigroups motivated by combinatorial games, nim in particular, are examined. They form a countably infinite family of infinite quasigroups with some curious properties. The underlying set Q of the quasigroups is taken to be the well-ordered set of natural numbers including 0. A quasigroup is constructed by filling in the multiplication table in a greedy fashion with the rows and columns labelled by the elements of Q in their natural order. For each proper subset S, of Q, define the *minimal*

2000 Mathematics Subject Classification: 20N05, 91A46
Keywords: quasigroup, combinatorial game

excluded number mex S of S to be the least element of the (non-empty) complement of S in Q. (This element is uniquely defined by the well-ordering principle.) Fix a natural number s, known as the *seed*. Define

$$0 \cdot 0 := s. \tag{1}$$

One may then use the following greedy algorithm to define the remaining products of natural numbers l and m inductively:

$$l \cdot m := \operatorname{mex}(\{i \cdot m \mid i < l\} \cup \{l \cdot j \mid j < m\}). \tag{2}$$

The algorithm guarantees that the body of the multiplication table will be a (infinite) Latin square, and therefore that $(Q, \cdot)$ becomes a quasigroup Q_s, known as the *greedy quasigroup* seeded by s. As an illustration, the following table

	0	1	2	3	4	5	6	7	8	9	10
0	5	0	1	2	3	4	6	7	8	9	10
1	0	1	2	3	4	5	7	6	9	8	11
2	1	2	0	4	5	3	8	9	6	7	12
3	2	3	4	0	1	6	5	8	7	10	9
4	3	4	5	1	0	2	9	10	11	6	7
5	4	5	3	6	2	0	1	11	10	12	8
6	6	7	8	5	9	1	0	2	3	4	13
7	7	6	9	8	10	11	2	0	1	3	4
8	8	9	6	7	11	10	3	1	0	2	5
9	9	8	7	10	6	12	4	3	2	0	1
10	10	11	12	9	7	8	13	4	5	1	0

Table 1. Part of the multiplication table of Q_5.

gives the first few entries of the multiplication table of Q_5.

Seeding with 0, one obtains Q_0 as a countable elementary abelian 2-group. In the theory of combinatorial games, the multiplication of Q_0 is known as *nim sum* [5]. Greedy quasigroups will be seen as a generalization of nim. Each position X in the game of nim is assigned a natural number value x, and the nim sum $x \oplus y$ denotes the value of the nim position $X + Y$ obtained by juxtaposing X with a second position Y of value y. Seeding with 1, the quasigroup Q_1 gives a comparable description of the juxtaposition of positions in the game of misère nim – nim played to lose. Section discusses elementary properties of the greedy quasigroups: commutativity, associativity, total symmetry, and the existence of identity, idempotent, and nilpotent elements. The next two sections (which may be skipped at first reading) comprise a number of technical lemmas about the multiplication by 2 and 3 in Q_s for $s > 0$. These lemmas drive the theorems regarding the multiplication groups in Section . Section examines the subquasigroup structure of the greedy quasigroups. It transpires that while Q_0, Q_1 have uncountably many subquasigroups, Q_2 has just one proper, non-trivial subquasigroup, and Q_s has none for $s > 2$ (Theorem 6.2). It is also shown that for $s > 2$, the quasigroup Q_s is simple. The congruences of Q_0 correspond directly to its subgroups, essentially forming a projective geometry of countable dimension over the 2-element field. For $s > 1$, the greedy quasigroups Q_s are shown to be simple in Theorem 6.3. Section considers homomorphisms between greedy quasigroups. It is shown that the greedy quasigroups are mutually non-isomorphic (Theorem 7.1), and indeed that for distinct positive seeds s, t, the only homomorphism from Q_s to Q_t is the constant map taking the value 1 (Theorem 7.11). Finally, Theorem 7.12 shows that for $s > 2$, the only endomorphisms of Q_s are the constant and the identity. In particular, Q_s is *rigid* in the sense of having a trivial automorphism group. It may be worth noting that the properties of the greedy quasigroups Q_s for $s > 2$, namely simplicity, rigidity, and lack of proper, non-trivial subalgebras, are reminiscent of the Foster-Pixley characterization of (necessarily finite) primal algebras [7]. The paper concludes with a brief characterization of greedy quasigroups in terms of combinatorial game theory. For algebraic concepts and conventions that are not otherwise explained here, especially involving quasigroups, readers are referred to [8]. Note that mappings are usually placed to the right of their arguments, allowing composition in natural order, and minimizing the number of brackets that otherwise proliferate in the study of non-associative structures such as quasigroups.

2. Elementary properties

Recall that a quasigroup $(Q, \cdot, /, \backslash)$ is said to be *commutative* or *associative* respectively if its multiplication $\cdot$ is commutative or associative.

Proposition 2.1. *For each seed s, the quasigroup Q_s is commutative.*

Proof. By induction, using (2):

$$\begin{aligned} l \cdot m &= \operatorname{mex}(\{i \cdot m \mid i < l\} \cup \{l \cdot j \mid j < m\}) \\ &= \operatorname{mex}(\{m \cdot i \mid i < l\} \cup \{j \cdot l \mid j < m\}) \\ &= \operatorname{mex}(\{i \cdot l \mid i < m\} \cup \{m \cdot j \mid j < l\}) = m \cdot l. \end{aligned}$$

(The induction hypothesis is used for the second equality.) □

Proposition 2.2. *Suppose $s > 0$.*

1. $\forall\ 0 < x \leqslant s,\ 0 \cdot x = x \cdot 0 = x - 1.$
2. $\forall\ x > s,\ 0 \cdot x = x \cdot 0 = x.$
3. $\forall\ 0 \leqslant x \leqslant s,\ 1 \cdot x = x \cdot 1 = x.$

Proof. (1) Since $0 \cdot 0 = s$, $1 \cdot 0 = 0$, and applying (2) to each successive term, one has $x \cdot 0 = \operatorname{mex}\{s, 0, 1, \ldots, (x-1) \cdot 0 = (x-2)\} = x - 1$.

(2) For $x = s+1$, (2) gives $0 \cdot x = \operatorname{mex}\{s, 0, 1, \ldots, s-1\} = s+1$. Then $0 \cdot x = x$ for $x > s$ by induction.

(3) Note $0 \cdot 1 = 0$. Then for $x \leqslant s$, induction yields

$$x \cdot 1 = \operatorname{mex}\{0, 1, \ldots, x-1, 0 \cdot x = x - 1\} = x.$$ □

Corollary 2.3. *For $s > 0$, the quasigroup Q_s is not associative.*

Proof. $(0 \cdot 0) \cdot (s+1) = s \cdot (s+1) \neq 0 \cdot (s+1) = 0 \cdot (0 \cdot (s+1))$. □

Definition 2.4. The *hub* of a greedy quasigroup Q_s is defined to be the subset $H_s = \{0, \ldots, s\}$.

In Table 1, the hub H_5 is marked off by separating lines.

Remark 2.5. The element 0 is the identity element of the group Q_0. For $s > 0$, the quasigroup Q_s does not have a universal identity element. However, the later parts of Proposition 2.2 may be interpreted as saying that 1 is an identity for the hub, while 0 is an identity outside the hub. In particular, 1 is the only idempotent element of Q_s, i.e., the only element x forming a singleton subquasigroup $\{x\}$.

A quasigroup $(Q, \cdot, /, \backslash)$ is said to be *totally symmetric* if its three binary operations agree, i.e., if the implication

$$x_1 \cdot x_2 = x_3 \Rightarrow x_{1\pi} \cdot x_{2\pi} = x_{3\pi} \tag{3}$$

holds for all permutations π of the index set $\{1, 2, 3\}$. (Commutativity means that (3) holds for $\pi = (12)$.) Note that Q_0, like any elementary abelian 2-group, is totally symmetric. Now outside the hub, the multiplication on Q_1 is constructed exactly as in Q_0. Furthermore, the hub of Q_1 is totally symmetric, being isomorphic to the subgroup $\{0, 1\}$ of Q_0. Thus Q_1 is also totally symmetric.

Lemma 2.6. *Suppose $s > 0$. For $x > s$,*

$$x \cdot 1 = \begin{cases} x+1, & x-s \equiv_2 1 \\ x-1, & x-s \equiv_2 0. \end{cases}$$

Proof. As an induction basis, note:

$$(s+1) \cdot 1 = \operatorname{mex}\{0, 1, \ldots, s, (s+1) \cdot 0 = s+1\} = s+2;$$
$$(s+2) \cdot 1 = \operatorname{mex}\{0, 1, \ldots, s, s+2, (s+2) \cdot 0\} = s+1.$$

Consider $x > s$. By induction, for $x - s \equiv_2 1$,

$$x \cdot 1 = \operatorname{mex}\{0, 1, \ldots, x-1, x \cdot 0\} = x+1,$$

and for $x - s \equiv_2 0$,

$$x \cdot 1 = \operatorname{mex}\{0, 1, 2, \ldots, x-3+1, x-2-1, x-1+1, x \cdot 0\} = x-1. \quad \square$$

Recall that in any quasigroup $(Q, \cdot, /, \backslash)$, the *square* x^2 of an element x is $x \cdot x$. An element of a greedy quasigroup is described as *nilpotent* if its square is 0. All but at most two elements of a greedy quasigroup are nilpotent, and 0 is the only square of infinitely many elements.

Theorem 2.7. *For $x > 1$ in any greedy quasigroup, $x^2 = 0$.*

Proof. The result is immediate in Q_0, so suppose $s > 0$. Recall $0 \cdot 1 = 0 = 1 \cdot 0$. Thus the first place 0 can appear in the 2-column of the Latin square is the 2-row, so it must appear there. Then the first place 0 can and must appear in the 3-column is the 3-row. Fill in the first n columns (labelled $0, \ldots, n-1$) by induction. The first place 0 can appear in the n-column is in the n-row. Thus by induction $n \cdot n = 0$ for all $n > 1$. $\square$

Corollary 2.8. *Consider the greedy quasigroup Q_s.*

1. *If $s = 1$, then $0^2 = 1^2 = 1$.*
2. *For $s \neq 1$, the element 0 is the only square of more than one element.*

3. Multiplication by 2

Throughout the next two technical sections, which may be skipped at first reading, assume $s > 0$. (Later, it will be implicitly necessary to assume that s is "sufficiently large.") Consider the inductive construction of the Latin square that forms the body of the multiplication table of Q_s. There is a critical dependence on the congruence class of the seed to certain moduli. A column is said to be *complete at entry* n if its first $n+1$ elements are precisely the numbers $0, 1, \ldots, n$. The proofs are by induction and can be done by hand in a similar fashion to those above.

Lemma 3.1. *For $x < s$,*

$$x \cdot 2 = \begin{cases} x+1, & x \equiv_3 0, 1; \\ x-2, & x \equiv_3 2. \end{cases}$$

The post-hub behavior of the 2-column depends on the congruence class of the seed modulo 3. We consider each class in turn.

Lemma 3.2. *For $s \equiv_3 0$ and $s \equiv_3 1$ and $x > s+1$:*

$$x \cdot 2 = \begin{cases} x+1, & x-s \equiv_2 0; \\ x-1, & x-s \equiv_2 1. \end{cases}$$

Lemma 3.3. *For $s \equiv_3 2$, and $x > s$,*

$$x \cdot 2 = \begin{cases} x+2, & x-s \equiv_4 1, 2; \\ x-2, & x-s \equiv_4 3, 0. \end{cases}$$

4. Multiplication by 3

Multiplication by 3 is the last detailed case that is analyzed in this paper. Its structure is slightly more difficult than in the earlier cases. For each of the following lemmas, suppose that the seed is sufficiently large. The first lemma collects some preliminary calculations.

Lemma 4.1. $0 \cdot 3 = 2,\ 1 \cdot 3 = 3,\ 2 \cdot 3 = 4,\ 3 \cdot 3 = 0,\ 4 \cdot 3 = 1.$

Lemma 4.2. *For* $5 \leqslant x \leqslant s$:

$$x \cdot 3 = \begin{cases} x+1, & x \equiv_9 5, 8; \\ x+2, & x \equiv_9 6, 1, 2; \\ x-2, & x \equiv_9 7, 0, 4; \\ x-1, & x \equiv_9 3. \end{cases}$$

After each ninth step, the column becomes complete.

In the remainder of this section, only the 3-column of the multiplication table for $s \equiv_3 2$ is considered, since this is the only case needed for the subsequent results. Note that $s \equiv_9 2, 5, 8$. Each case yields a different pattern after the row labelled by the seed.

Lemma 4.3. *For* $x > s \equiv_9 2$:

$$x \cdot 3 = \begin{cases} x-2, & x-s \equiv_4 1, 2; \\ x+2, & x-s \equiv_4 3, 0. \end{cases}$$

Lemma 4.4. *For* $x > s \equiv_9 5$:

$$x \cdot 3 = \begin{cases} x-1, & x-s \equiv_2 1; \\ x+1, & x-s \equiv_2 0. \end{cases}$$

Lemma 4.5. *For* $s \equiv_9 8$, $(s+1) \cdot 3 = s-1$. *For* $x \geqslant s+2$:

$$x \cdot 3 = \begin{cases} x+1, & x-s \equiv_2 0; \\ x-1, & x-s \equiv_2 1. \end{cases}$$

5. Multiplication groups

In this section, the multiplication groups for each Q_s are analyzed. The analysis yields easy proofs of some later theorems.

Consider

$$G = \langle R(0), R(1), R(2) \rangle < \mathrm{Mlt}(Q_s).$$

$$R(0) = (0, s, s-1, s-2, \ldots, 1)$$
$$R(1) = (s+1, s+2)(s+3, s+4) \ldots (s+2n+1, s+2n+2) \ldots$$
$$R(2) = (0, 2, 1)(3, 5, 4) \ldots$$

But one has to consider the seed mod 3.

- For $s \equiv_3 0$, one has $(0,2,1)\dots(s-3,s-1,s-2)\cdot(s,s+1)(s+2,s+3)\dots$
- For $s \equiv_3 1$, one has $(0,2,1)\dots(s,s+1,s-1)\cdot(s+2,s+3)\dots$
- For $s \equiv_3 2$, one has $(0,2,1)\dots(s-1,s,s-2)\cdot(s+1,s+3)(s+2,s+4)(s+5,s+7)(s+6,s+8)\dots$

Consider $R(0), R(1), R(2)$ in $S_{\mathbb{N}}$. A natural question is whether or not the groups

$$G = \langle R(0), R(1), R(2)\rangle$$

and

$$F = \langle R(0), R(1), R(2), R(3)\rangle$$

have transitive actions on Q_s. If so, are the groups multiply transitive?

5.1. Transitivity

Lemma 5.1. *For all s, $\langle R(0)\rangle$ acts transitively on the hub.*

Proof. By Lemma 2.2, $0 \cdot x = x - 1$ for $0 < x \leqslant s$ and $0 \cdot 0 = s$. Thus $xR(0)^x = 0$, and $0R(0)^{y+1} = s - y$. Therefore for $x, z = s - y \in H$, there is an n such that $xR(0)^n = z$. □

Lemma 5.2. *For $s \equiv_3 0, 1$, $Q_s \setminus H_s$ is in one orbit of the action of G on Q_s. Moreover, one can choose $g \in G$ so that $x_1 g = x_2$ for any $x_1, x_2 \in Q_s \setminus H_s$ and g stabilizes 1.*

Proof. Let $x = s+2n-i$, $y = s+2m-j$, where $n, m \in \mathbb{N}$ and $i, j \in \{0,1\}$. Let $\tau = R(1)^i(R(2)R(1))^{m-n}R(1)^j$. Now it is shown that $x\tau = y$. The initial multiplication by $R(1)^i$ sends both $s+2n-i$ to $s+2n$. Now by Lemmas 2.6 and 3.1 an application of $R(2)R(1)$ sends $s+2n$ to $s+2n+2$. So $(R(2)R(1))^t$ sends $s+2n$ to $s+2n+2t$. Therefore $R(1)^i(R(2)R(1))^t$ sends $s+2n-i$ to $s+2n+2t$. Finally $R(1)^j$ sends this to to $s+2n+2t-j$. Therefore $(s+2n-i)\tau = s+2n+2(m-n)-j = s+2m-j$. To stabilize 1, use $\sigma = R(1)^i R_1(2,0)^{m-n}R(1)^j$. Note that since $R_1(2,0) = R(2)R(0)R(1)^{-1}$, on $Q_s \setminus H_s$, $R_1(2,0)$ behaves like $R(2)R(1)$, since $xR(0) = x$ and $xR(1)^2 = x$ for $x \in Q_s \setminus H_s$. Thus $x\sigma = xR(1)^i(R(2)R(1))^{n-m}R(1)^j = y$ as above. □

Theorem 5.3. *The group G acts transitively on Q_s for $s \equiv_3 0, 1$.*

Proof. Using Lemmas 5.1 and 5.2, it remains to show that a hub element can be sent to a non-hub element. Note that $s \cdot 2 = s + 1$ in this case. So to send a hub element h to a non-hub element $s + 2n - j$, use $\sigma = R(0)^{h+1}R(2)R(1)\left(R(2)R(1)\right)^{n-1}R(1)^j$. □

For $s \equiv_3 2$ the situation is more complex.

Lemma 5.4. *Let $\sigma_{k,i} = R(2)^k R(1)^i$ for $k, i \in \{0, 1\}$. Then in Q_s for $s \equiv_3 2$, $\sigma_{k,i}$ sends $s + 4n - 2k - i$ to $s + 4n$.*

Proof. Since multiplication by 2 adds or subtracts 2, $R(2)^k$ sends $s + 4n - 2k - i$ to $s + 4n - i$. Now multiplication by 1 adds or subtracts 1. So $R(1)^i$ sends $s + 4n - i$ to $s + 4n$. □

Lemma 5.5. *For $s \equiv_9 5, 8$, $\tau = R(3)R(2)R(1)$ sends $s + 4n$ to $s + 4n + 4$.*

Proof. First, $(s + 4n)R(3) = s + 4n + 1$ by Lemmas 4.4 and 4.5. Then $(s+4n+1)R(2) = s+4n+3$ by Lemma 3.3 and $(s+4n+3)R(1) = s+4n+4$ by Lemma 2.6. Thus $(4n)\tau = (4n)R(3)R(2)R(1) = 4n + 4$. □

Lemma 5.6. *For $s \equiv_9, 2$ $\tau = R(3)R(2)$ sends sends $s + 4n$ to $s + 4n + 4$*

Proof. First $(s + 4n)R(3) = (s + 4n + 2)$ by Lemma 4.3. Then $(s + 4n)$ $(R(3)R(2)) = s + 4n + 4$ by Lemma 3.3. □

Lemma 5.7. *For $s \equiv_3 2$, $Q_s \setminus H_s$ is in one orbit of the action of G on Q_s. Moreover, one can choose $g \in G$ so that $x_1 g = x_2$ for any $x_1, x_2 \in Q_s \setminus H_s$ and g stabilizes 1.*

Proof. We show that any $x \in Q_s \setminus H_s$ can be sent to $y \in Q_s \setminus H_s$. Let $x = 4n - 2k - i$ and $y = 4m - 2k' - i'$, where $k, k', i,' i \in \{0, 1\}$. Then for $\varphi = \sigma_{k,i}\tau^{m-n}\sigma k', i'^{-1}$, $x\varphi = y$:

$$\begin{aligned}
(s + 4n - 2k - i)\varphi &= (s + 4n - 2k - i)\sigma_{k,i}\tau^{m-n}\sigma_{k',i'} \\
&= (s + 4n)\tau^{m-n}\sigma_{k',i'} \\
&= (s + 4m)\sigma_{k',i'} \\
&= s + 4m - k' - i'
\end{aligned}$$

Thus $x\varphi = y$. Note that outside the hub $R(0)$ stabilizes x. So $\alpha = R_1(3, 0)R_1(2, 0)R(1)$ behaves like $R(3)$ and stabilizes 1 while $\beta = R_1(2, 0)R(1)$ behaves like $R(2)$ and stabilizes 1. Now apply Lemma 5.7 with α in place of $R(3)$ and β in place of $R(2)$ □

Theorem 5.8. *For $s \equiv_3 2$, F acts transitively on Q_s.*

Proof. It remains to be shown that one can send a hub element to a non-hub element as before. Let $h \in H_s$ and $x = s + 4n - 2k - i$. First, let $\psi = R(0)^{h+1}R(3)\sigma_{1,1}\tau^{n-1}\sigma_{k,i}$. Then $h\psi = x$ by the above lemmas. □

5.2. 2-transitivity

The goal of this section is to prove that $Mlt(Q_s)$ is 2-transitive.

Lemma 5.9. *Let $H = \langle R(0), R(2)\rangle$. Then H_s is in one orbital of the action of H on Q_s for $s \equiv_3 0, 1$.*

Proof. Given $h_1, h_2, x_1, x_2 \in H_s$, there is an n so that $h_1R(0)^n = s$ (by Lemma 5.1). So $h_1R(0)^nR(2) = s + 1$. Let $h_2R(0)^nR(2) = k$. Now choose m so that $kR(0)^m = x_2R(0)^{-(s-x_1)}R(2)^{-1}$. Thus $h_1\sigma = x_1$ and $h_2\sigma = x_2$ for $\sigma = R(0)^nR(2)R(0)^mR(2)^{-1}R(0)^{s-x_1}$. □

Lemma 5.10. *Let $H = \langle R(0), R(3)\rangle$. Then H_s is in one orbital of the action of H on Q_s for $s \equiv_3 2$.*

Proof. Given $h_1, h_2, x_1, x_2 \in H_s$, there is an n so that $h_1R(0)^n = s$ (by Lemma 5.1). So $h_1R(0)^nR(3) = s + 1$. Let $h_2R(0)^nR(3) = k$. Now choose m so that $kR(0)^m = x_2R(0)^{-(s-x_1)}R(3)$. Thus $h_1\sigma = x_1$ and $h_2\sigma = x_2$ for $\sigma = R(0)^nR(3)R(0)^mR(3)^{-1}R(0)^{s-x_1}$. □

Remark 5.11. The above two lemmas, along with the fact that $hR(1) = h\ \forall h \in H_s$ show that the hub is in one orbital of the action of F.

Lemma 5.12. *For $x_1 \in Q_s \setminus H_s$ and h_1, h_2, h_3 there is a σ so that $x_1\sigma = h_2$ and $h_1\sigma = h_3$.*

Proof. Use $R(0)^n$ for some n so send h_1 to 1. By Lemmas 5.2 and 5.7, there is a β so that $1\beta = 1$ and $x_1\beta = s+1$. Then for $s \equiv_3 0, 1$ $\gamma = R(0)^n\beta R(2)^{-1}$ is such that $x_1\gamma, h_1\gamma \in H_s$. For $s \equiv_3 2$ use $\gamma = R(0)^n\beta R(3)^{-1}$. Now since H_s is in one orbital of the action of $\langle R(0), R(2), R(3)\rangle$ (Remark 5.11), the proof is complete. □

Lemma 5.13. *For $x_1, x_2 \in Q_s \setminus H_s$ and $h_1, h_2 \in H_s$, there is a σ so that $x_i\sigma = h_i$.*

Proof. Let α be so that $x_1\alpha = 1$. Then perhaps $x_2\alpha = h \in H_s$. Then by Lemma 5.9, there is a β, so that $1\beta = h_1, h\beta = h_2$. Thus $\sigma = \alpha\beta$. If $x_2\alpha = x \notin H_s$ apply Lemma 5.12. □

Theorem 5.14. *F acts 2-transitively on Q_s.*

Proof. We find a σ that sends $(x_1, x_2) \in Q_s^2$ to (y_1, y_2). First by the above three lemmas, there is a map α so that $(x_1, x_2)\alpha = (0, 1)$, and a map β so that $(y_1, y_2)\beta = (0, 1)$. Then $(x_1, x_2)\alpha\beta^{-1} = (y_1, y_2)$ □

5.3. High transitivity

It has been shown how to construct permutations in $F \leqslant \mathrm{Mlt}(Q_s)$ that are 2-transitive. The question is whether one can go farther.

First note that since F is 2-transitive it is primitive (Lemma 4.10 in [3]). Therefore we can apply Lemma 10.8 in [3] with the hub as the Jordan set. This theorem says that if a permutation group on Ω is primitive on an infinite set with a subgroup H that is transitive on a set, X, and fixes the complement of X, the multiplication group is highly transitive. Moreover, if X is finite, $\mathrm{Alt}(\Omega) \leqslant F$. Thus $\mathrm{Alt}(\mathbb{N}) \leqslant F \leqslant \mathrm{Mlt}(Q_s)$.

6. Subquasigroups

As noted in Remark 2.5, each greedy quasigroup has a unique singleton subquasigroup: $\{0\}$ in the elementary 2-group Q_0, and $\{1\}$ in Q_s for $s > 0$. We refer to the singleton subquasigroup and the empty subquasigroup as the *trivial* subquasigroups of the greedy quasigroups. The group Q_0 has uncountably many subquasigroups, since for each of the uncountably many subsets S of $\mathbb{N}$, the vector

$$(0\chi_S, 1\chi_S, \dots, n\chi_S, \dots) \tag{4}$$

of values of the characteristic function of S generates a distinct subgroup of the isomorphic copy $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ of Q_0.

Proposition 6.1. *The greedy quasigroup Q_1 has uncountably many subquasigroups.*

Proof. Outside the hub $\{0, 1\}$, the multiplication on Q_1 is constructed exactly as in Q_0. Thus for each subgroup P of Q_0 with $\{0, 1\} \leqslant P$, the subset P of $\mathbb{N}$ forms a subquasigroup of Q_1. But Q_0 has uncountably many such subgroups P. □

The respective hubs H_1 and H_2 of Q_1 and Q_2 form cyclic groups, with 1 as the identity element (Remark 2.5). These cases are exceptional.

Proposition 6.2. *For $s > 2$, there are no non-trivial subquasigroups of Q_s.*

Proof. Note that F is transitive for all $s \geqslant 3$. Thus if a subquasigroup, H, contains $0, 1, 2, 3$ then $H = Q_s$. Let H be a subquasigroup. If $0 \in H$, then $H_s \subset H$. In particular for $s \geqslant 3$, $0, 1, 2, 3 \in H$ and $H = Q_s$. Suppose $x \neq 0, 1 \in H$, then $x \cdot x = 0 \in H$, so as above $H = Q_s$. Thus the only subquasigroup is the trivial subquasigroup $\{1\}$. □

Proposition 6.3. *For $s \geqslant 2$, Q_s is simple.*

Proof. This follows immediately since $\mathrm{Mlt}(Q_s)$ is 2-transitive. □

7. Homomorphisms

Theorem 7.1. *For $i \neq j$, $Q_i \ncong Q_j$.*

Proof. In both Q_i, Q_j, 0 is the unique element that fixes infinitely many elements. So for any isomorphism φ, $\varphi : 0 \mapsto 0$. In $\mathrm{Mlt}(Q_i)$, $R(0)$ is an $i+1$-cycle, but in Q_j $R(0)$ is a $j+1$-cycle. Thus $Q_i \ncong Q_j$. □

One can actually prove stronger results.

Lemma 7.2. *Let $\varphi : Q_i \to Q_j$.*

(*a*) *If φ is injective then there is a $k \in Q_i$ such that $k, k\varphi$ are both nilpotent.*

(*b*) *If φ is surjective then there is a $k \in Q_i$ such that $k, k\varphi$ are both nilpotent.*

Proof. There are only two elements $k \in Q_i$ such that $k \cdot k \neq 0$, namely $0, 1$, and similarly for Q_j.

(*a*) Let φ be injective. Suppose that $x\varphi, y\varphi$ are not nilpotent. Let z be nilpotent, then $z\varphi$ is not $x\varphi, y\varphi$ and these are the only non-nilpotent elements in Q_j. Thus both $z, z\varphi$ are nilpotent.

(*b*) Since φ is surjective, at most two of the nilpotent elements of Q_j can be the image of non-nilpotent elements of Q_i. There must be nilpotent elements on Q_i that are mapped to nilpotent elements of Q_j.

□

In what follows, the notations q_i, q_j are used for an element $q \in Q_i$ to distinguish it from $q \in Q_j$.

Lemma 7.3. *Let $\varphi : Q_i \to Q_j$ be a homomorphism and $0_i\varphi = 0_j$. If $x \cdot x = 0$, then $x\varphi \cdot x\varphi = 0$.*

Proof. $0_j = 0_i\varphi = (x \cdot x)\varphi = x\varphi \cdot x\varphi$. □

Lemma 7.4. *Let $\varphi : Q_i \to Q_j$ be a homomorphism. If there is an element $x \in Q_i$ such that $x \cdot x = 0$ and $x\varphi \cdot x\varphi = 0$, then $0_i\varphi = 0_j$.*

Proof. Let k be one such element. Then $0_j = 0_i\varphi = (k \cdot k)\varphi = k\varphi \cdot k\varphi$. □

Remark 7.5. In particular, Lemma 7.3 and Lemma 7.4 are true for surjective and injective homomorphisms.

Lemma 7.6. *For any homomorphism $\varphi : Q_i \to Q_j$ and $i, j \neq 0, 1$, $1_i\varphi = 1_j$.*

Proof. This follows from the fact that 1_i is the only idempotent element of Q_i. (Everything else other than 0_i is nilpotent). □

Lemma 7.7. *For any surjective (injective) homomorphism $\varphi : Q_i \to Q_j$, $s_i\varphi = s_j$.*

Proof. $s_i\varphi = (0_i \cdot_i 0_i)\varphi = 0_i\varphi \cdot_j 0_i\varphi = 0_j \cdot_j 0_j = s_j$. □

Remark 7.8. In fact, this is true if $0_i\varphi = 0_j$.

Theorem 7.9 (Homomorphism Theorem). *Suppose $i, j > 1$.*

(*a*) *There is no injective homomorphism $\varphi : Q_i \to Q_j$.*

(*b*) *There is no surjective homomorphism $\varphi : Q_i \to Q_j$.*

Proof. Note that by looking at the multiplication table for Q_j, that $s_jL(0_j)^{s_j} = s_j$ and $s_jL(0_i)^i \neq s_j$ for $i < s_j$. Since $s_i\varphi = s_j$, then $s_j = s_i\varphi = s_iR(0_i)^i = s_i\varphi R(0_i\varphi)^i = s_jR(0_j)^i$. Thus $j + 1|i + 1$. Perhaps one can "loop" several times, but the loop must be completed. Thus there is no injective or surjective homomorphism $\varphi : Q_i \to Q_j$, if $i < j$. So, suppose that $j + 1|i + 1$, but $j \neq i$. Note that $s_iR(0)^{j-1}$ is nilpotent. Then $s_iR(0)^{j-1}\varphi = s_i\varphi R(0\varphi)^{j-1} = s_jR(0_j)^{j-1} = 1_j$. This is contradicts Lemma 7.3, since a nilpotent must be mapped to a nilpotent and 1_j is idempotent. □

Remark 7.10. Theorem 7.1 can be seen as a corollary to the Homomorphism Theorem.

Not only are the Q_i's are not isomorphic, there is no injective or surjective homomorphism between them. It is natural to ask whether there is any non-trivial homomorphism between them. Of course, there is the trivial homomorphism $x\varphi = 1, \forall x \in Q_i$ for any Q_i, Q_j. It turns out that this is the only homomorphism $\varphi : Q_i \to Q_j$ for $i \neq j$.

Theorem 7.11. *The only homomorphism $\varphi : Q_i \to Q_j$ for $i \neq j$ is the trivial homomorphism.*

Proof. Let $\varphi : Q_i \to Q_j$. If there is a nilpotent element x such that $x\varphi$ is also nilpotent, by Lemma 7.4 $0_i\varphi = 0_j$, so then by Lemma 7.7 $s_i\varphi = s_j$. Then the homomorphism fails as in Theorem 7.9. Thus for any nilpotent x, $x\varphi$ is either 0 or 1. If $x \neq 0$ and $x\varphi = 0$, then $0\varphi = (x\cdot x)\varphi = x\varphi x\varphi = 0_j \cdot 0_j = s_j$. Then for any nilpotent y, $s_j = 0\varphi = (y \cdot y)\varphi = y\varphi \cdot y\varphi$. So s_j is the square of $y\varphi$. Thus $y\varphi = 0_j$ for any nilpotent y. Now, $s_i\varphi = (0_i \cdot 0_i)\varphi = 0_i\varphi 0_i\varphi = s_j \cdot s_j = 0_j$. However, in any Q_i there are nilpotent elements x, y such that $xy = s_i$. Then $s_i\varphi = (xy)\varphi = x\varphi y\varphi = 0_j \cdot 0_j = s_j$. This is a contradiction, so there is no x so that $x\varphi = 0_j$. Thus $x\varphi = 1_j$ for all nilpotent x. In particular $s_i\varphi = 1$, so $0_i\varphi = (s_i \cdot s_i)\varphi = s_i\varphi \cdot s_i\varphi = 1_j \cdot 1_j = 1$. Thus φ is trivial. □

Theorem 7.12. *For $s > 2$, there are only two endomorphisms of Q_s, the constant and the identity. In particular, Q_s is rigid.*

Proof. Suppose that $f : Q_s \to Q_s$ is an endomorphism. Since Q_s is simple by Theorem 6.3, the kernel congruence of f is either trivial (the equality relation) or improper. If it is improper, then f is constant, its image being the unique singleton subquasigroup $\{1\}$ of Q_s. Otherwise, f injects. Now 0 is the only element that is the square of more than one element, so $0f = 0$. The image $sf = (0 \cdot 0)f = 0^f \cdot 0^f$ of the seed is a square, namely $1, 0$ or s. If $sf = 1$, then $0^f \cdot 0^f = 1$, yielding the contradiction $0f = 1$. Again, $sf = 0$ would contradict the injectivity of f. Thus $sf = s$. By Lemma 5.2, $s - r = sR(0)^r$ for $0 \leqslant r < s$. Then $(s - r)f = sR(0)^r f = sR(0)^r = s - r$, so the hub is fixed. Since the hub generates all of Q_s, it follows that Q_s is fixed, and f is the identity. □

8. Game theory applications

Greedy quasigroups are motivated in part by combinatorial games, in particular by nim. Nim is a game played with several piles, or heaps of counters. A player selects a pile and removes some, or possibly all the counters in the pile. The player to make the last move wins. With only two piles, the strategy is simple: equalize the piles, and then when your opponent removes n counters from one pile, remove n from the other. In this way, a player will never be at a loss for a move. With three or more non-empty piles, the strategy is a little more elusive. One must compute the *nim-sum*. The nim-sum is a way of reducing a collection of piles to a single value. This value represents the size of a single pile that is equivalent to the original position. If this pile were included in the original position, the resulting game would be a win for the first player. For details, see [1]. An alternative characterization of nim is that of a Rook on a quarter-infinite chessboard. Place a Rook on the board and make legal Rook moves up and left of the board. A player wins by placing the Rook on the upper-left corner. Now, greedy quasigroups have the following characterization as a game: place a nim-heap of size n, $n \geqslant 0$ on a chessboard. Move the heap as a Rook. Once the heap reaches the upper-left square, players may play in the nim heap. Clearly, with a single non-empty nim-heap on the board, one can win by forcing the other player to place the heap on the upper-left square and then removing the entire nim-heap. These game are examples of the sequential compounds in [9]. The difficulty arises when several heaps of different sizes are placed on the board. To play correctly, one must compute the value of each heap, with is a function of its size and its location. In this way, one can compute the nim-value of the position, and using combinatorial game theory, make the correct move. Suppose heaps of sizes $n_1, n_2, \ldots, n_k$ at locations $(x_1, y_1), \ldots, (x_n, y_n)$. The value of each heap is $x_i \cdot_i y_i$ where $\cdot_i$ is the multiplication in Q_{n_i}. The total value of the game is then:

$$\bigoplus_{i=1}^{k} x_i \cdot y_i$$

where $\oplus$ is nim-addition. A natural generalization is to place an entire game of nim on a square. This does not produce any new games, since each game of nim is equivalent to a single nim heap; so one might as well simply put the single nim-heap on the square.

References

[1] **E. Berlekamp, J. H. Conway and R. K. Guy:** *Winning Ways for your Mathematical Plays*, A K Peters, Ltd, 2001.

[2] **E. Berlekamp, J. H. Conway and R. K. Guy:** *Winning Ways for your Mathematical Plays*, A K Peters, Ltd, 2002.

[3] **M. Bhattacharjee et. al.:** *Notes on Infinite Permutation Groups*, Lecture Notes in Mathematics, 1998.

[4] **G. Birkhoff:** *Lattice Theory*, American Mathematical Society, 1967.

[5] **J. H. Conway:** *On Numbers and Games*, A K Peters, Ltd, 2002.

[6] **T. Evans:** *Homomorphisms of non-associative systems*, J. London Math. Soc. **24** (1949), 254 – 260.

[7] **A. L. Foster and A. F. Pixley:** *Semi-categorical algebras I: semi-primal algebras*, Math. Z. **83** (1964), 147 – 169.

[8] **J. D. H. Smith and A. B. Romanowska:** *Post-Modern Algebra*, Wiley, 1999.

[9] **W. Stromquist and D. Ullman:** *Sequential compounds of combinatorial games*, Theoretical Computer Science **(119)** (1993), 311 – 321.

Iowa State University
Department of Mathematics
Ames, IA 50011
USA
E-mail: tarice@iastate.edu

Received November 2, 2006