Quasigroups and Related Systems **15** (2007), 191 – 200

On central loops and the central square property

John Olúsọlá Adéníran and Tèmítọ́pẹ́ Gbọ́láhàn Jaiyéọlà

Abstract

The representation sets of a central square C-loop are investigated. Isotopes of central square C-loops of exponent 4 are shown to be both C-loops and A-loops.

1. Introduction

C-loops are one of the least studied loops. Few publications that have considered C-loops include Fenyves [10], [11], Beg [3], [4], Phillips et. al. [17], [19], [15], [14], Chein [7] and Solarin et. al. [2], [23], [21], [20]. 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 [17], [19], and [15].

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 [11] was completed in [17]. Fenyves proved that LC-loops and RC-loops are defined by three equivalent identities. In [17] and [18], it was shown that LC-loops and RC-loops are defined by four equivalent identities. Solarin [21] named the fourth identities the *left middle* (LM) and *right middle* (RM) *identities* and loops that obey them are called *LM-loops* and *RM-loops*, respectively. These terminologies were also used in [22]. Their basic properties are found in [19], [11] and [9].

Definition 1.1. A set Π of permutations on a set L is the *representation* of a loop $(L, \cdot)$ if and only if

2000 Mathematics Subject Classification: 20N05, 08A05
Keywords: central loops, isotopes, central square.

(*i*) $I \in \Pi$ (identity mapping),

(*ii*) Π is transitive on L (i.e., for all $x, y \in L$, there exists a unique $\pi \in \Pi$ such that $x\pi = y$),

(*iii*) if $\alpha, \beta \in \Pi$ and $\alpha\beta^{-1}$ fixes one element of L, then $\alpha = \beta$.

The left (right) representation of a loop L is denoted by $\Pi_\lambda(L)$ (resp. $\Pi_\rho(L)$) or Π_λ (resp. Π_ρ) and is defined as the set of all left (right) translation maps on the loop i.e., if L is a loop, then $\Pi_\lambda = \{L_x : L \to L \mid x \in L\}$ and $\Pi_\rho = \{R_x : L \to L \mid x \in L\}$, where $R_x : L \to L$ and $L_x : L \to L$ are defined as $yR_x = yx$ and $yL_x = xy$ are bijections.

Definition 1.2. 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 $x, y \in L$, $x \cdot xy = x^2y$ 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 $AUT(L)$. 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

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

In [13], the three identities stated in [11] were used to study finite central loops and the isotopes of central loops. It was shown that in a finite RC(LC)-loop L, $\alpha\beta^2 \in \Pi_\rho(L)\big(\Pi_\lambda(L)\big)$ for all $\alpha,\beta \in \Pi_\rho(L)\big(\Pi_\lambda(L)\big)$ while in a C-loop L, $\alpha^2\beta \in \Pi_\rho(L)\big(\Pi_\lambda(L)\big)$ for all $\alpha,\beta \in \Pi_\rho(L)\big(\Pi_\lambda(L)\big)$. A C-loop is both an LC-loop and an RC-loop [11], hence it satisfies the formal. Here, it will be shown that LC-loops and RC-loops satisfy the later formula.

Also in [13], under triples of the form (A,B,B), (A,B,A), alternative centrum square loop isotopes of centrum square C-loops were shown to be C-loops.

It is shown that a finite loop is a central square central loop if and only if its left and right representations are closed relative to some left and right translations. Central square C-loops of exponent 4 are groups, hence their isotopes are both C-loops and A-loops.

For other definitions see [5], [22] and [16].

2. Preliminaries

Definition 2.1. (cf. [16]) Let $(L,\cdot)$ be a loop and $U,V,W \in SYM(L,\cdot)$. If $(U,V,W) \in AUT(L)$ for some U,V,W, then U is called an *autotopism*. If there exists $V \in SYM(L,\cdot)$ such that $xU \cdot y = x \cdot yV$ for all $x,y \in L$, then U is called *μ-regular*, while $U' = V$ is called its *adjoint*.

The set of autotopic bijections in a loop $(L,\cdot)$ is denoted by $\Sigma(L,\cdot)$, the set of all μ-regular bijections by $\Phi(L)$, the set of all adjoints by $\Phi^*(L)$.

Theorem 2.1. ([16]) *Groups of autotopisms of isotopic quasigroups are isomorphic.* □

Theorem 2.2. ([16]) *The set of all μ-regular bijections of a quasigroup $(Q,\cdot)$ is a subgroup of the group $\Sigma(Q,\cdot)$ of all autotopic bijections of $(Q,\cdot)$.* □

Corollary 2.1. ([16]) *If two quasigroups Q and Q' are isotopic, then the corresponding groups Φ and Φ' [Φ^* and Φ'^*] are isomorphic.* □

Definition 2.2. A loop $(L, \cdot)$ is called a *left inverse property loop* or *right inverse property loop* (L.I.P.L. or R.I.P.L.) if and only if it satisfies the left inverse property (resp. right inverse property): $x^{\lambda}(xy) = y$ (resp. $(yx)x^{\rho} = y$. Hence, it is called an *inverse property loop* (I.P.L.) if and only if it has the inverse property (I.P.) i.e., it has a left inverse property (L.I.P.) and right inverse property (R.I.P.).

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. Finite central loops

Lemma 3.1. *Let L be a loop. L is an LC(RC)-loop if and only if $\beta \in \Pi_{\rho}$ (Π_{λ}) implies $\alpha\beta \in \Pi_{\rho}$ (Π_{λ}) for some $\alpha \in \Pi_{\rho}$ (Π_{λ}).*

Proof. L is an LC-loop if and only if $x \cdot (y \cdot yz) = (x \cdot yy)z$ for all $x, y, z \in L$. 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, L is an LC-loop if and only if $xR_{y \cdot yz} = xR_{y^2}R_z$ if and only if $R_{y^2}R_z = R_{y \cdot yz}$ for all $y, z \in L$ and L is an RC-loop if and only if $xL_{zy \cdot y} = xL_{y^2}L_z$ if and only if $L_{zy \cdot y} = L_{y^2}L_z$. With $\alpha = R_{y^2}$ (L_{y^2}) and $\beta = R_z(L_z)$, $\alpha\beta \in \Pi_{\rho}$ (Π_{λ}). □

Lemma 3.2. *A loop L is an LC(RC)-loop if and only if $\alpha^2\beta = \beta\alpha^2$ for all $\alpha \in \Pi_{\lambda}$ (Π_{ρ}) and $\beta \in \Pi_{\rho}$ (Π_{λ}).*

Proof. L is an LC-loop if and only if $x(x \cdot yz) = (x \cdot xy)z$ while L is an RC-loop if and only if $(zy \cdot x)x = z(yx \cdot x)$. Thus, when L is an LC-loop, $yR_zL_x^2 = yL_x^2R_z$ if and only if $R_zL_x^2 = L_x^2R_z$, while when L is an RC-loop, $yL_zR_x^2 = yR_x^2L_z$ if and only if $L_zR_x^2 = R_x^2L_z$. Thus, replacing L_x (R_x) and R_z (L_z) respectively by α and β, We obtain our result. The converse statement can be proved analogously. □

Theorem 3.1. *A loop L is an LC(RC)-loop if and only if $\alpha, \beta \in \Pi_{\lambda}$ (Π_{ρ}) implies $\alpha^2\beta \in \Pi_{\lambda}$ (Π_{ρ}).*

Proof. L is an LC-loop if and only if $x \cdot (y \cdot yz) = (x \cdot yy)z$ 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 when L is an LC-loop, $zL_{x \cdot yy} = zL_y^2 L_x$ if and only if $L_y^2 L_x = L_{x \cdot yy}$ while when L is an RC-loop, $zR_y^2 R_x = zR_{yy \cdot x}$ if and only if $R_y^2 R_x = R_{yy \cdot x}$. Replacing $L_y(R_y)$ and $L_x(R_x)$ with α and β respectively, we have $\alpha^2\beta \in \Pi_\lambda(\Pi_\rho)$ when L is an LC(RC)-loop. The converse follows by reversing the procedure. □

Theorem 3.2. *Let L be an LC(RC)-loop. L is centrum square if and only if $\alpha \in \Pi_\rho$ (Π_λ) implies $\alpha\beta \in \Pi_\rho$ (Π_λ) for some $\beta \in \Pi_\rho(\Pi_\lambda)$.*

Proof. By Lemma 3.1, $R_{y^2}R_z = R_{y \cdot yz}$ $(L_{y^2}L_z = L_{zy \cdot y})$. Using Lemma 3.2, if L is centrum square, $R_{y^2} = L_{y^2}$ $(L_y^2 = R_{y^2})$. So, when L is an LC-loop, $R_{y^2}R_z = L_y^2 R_z = R_z L_y^2 = R_z R_{y^2} = R_{y \cdot yz}$, while when L is an RC-loop, $L_{y^2}L_z = R_y^2 L_z = L_z R_{y^2} = L_z L_{y^2} = L_{zy \cdot y}$. Let $\alpha = R_z$ (L_z) and $\beta = R_{y^2}$ (L_{y^2}), then $\alpha\beta \in \Pi_\rho$ (Π_λ) for some $\beta \in \Pi_\rho$ (Π_λ).

Conversely, if $\alpha\beta \in \Pi_\rho$ (Π_λ) for some $\beta \in \Pi_\rho$ (Π_λ) such that $\alpha = R_z$ (L_z) and $\beta = R_{y^2}$ (L_{y^2}) then $R_z R_{y^2} = R_{y \cdot yz}$ $(L_z L_{y^2} = L_{zy \cdot y})$. By Lemma 3.1, $R_{y^2}R_z = R_{y \cdot yz}$ $(L_{zy \cdot y} = L_{y^2}L_z)$, thus $R_z R_{y^2} = R_{y^2}R_z$ $(L_z L_{y^2} = L_{y^2}L_z)$ if and only if $xz \cdot y^2 = xy^2 \cdot z$ $(y^2 \cdot zx = z \cdot y^2 x)$. Let $x = e$, then $zy^2 = y^2 z$ $(y^2 z = zy^2)$ implies L is centrum square. □

Corollary 3.1. *Let L be a loop. L is a centrum square LC(RC)-loop if and only if*

1. *$\alpha\beta \in \Pi_\rho$ (Π_λ) for all $\alpha \in \Pi_\rho$ (Π_λ) and for some $\beta \in \Pi_\rho$ (Π_λ),*
2. *$\alpha\beta \in \Pi_\rho$ (Π_λ) for all $\beta \in \Pi_\rho$ (Π_λ) and for some $\alpha \in \Pi_\rho$ (Π_λ).*

Proof. This follows from Lemma 3.1 and Theorem 3.2. □

4. Isotopes of central loops

In [23] is concluded that central loops are not CC-loops. This means that the study of the isotopic invariance of C-loops will be trivial. This is, because if C-loops are CC-loops, then commutative C-loops would be groups since commutative CC-loops are groups. But from the constructions in [19], it follows that there are commutative C-loops which are not groups. The conclusion in [23] is based on the fact that the authors considered a loop of units in a central algebra.

Theorem 4.1. *A loop L is an LC(RC)-loop if and only if $(R_{y^2}, L_y^{-2}, I) \in AUT(L)$ (resp. $(R_y^2, L_{y^2}^{-1}, I) \in AUT(L)$) for all $y \in L$.*

Proof. According to [19], L is an LC-loop if and only if $x\cdot(y\cdot yz)=(x\cdot yy)z$ 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 $x,y,z\in L$. $x\cdot(y\cdot yz)=(x\cdot yy)z$ if and only if $x\cdot zL_y^2=xR_{y^2}\cdot z$ if and only if $(R_{y^2},L_y^{-2},I)\in AUT(L)$ for all $y\in L$, while $(zy\cdot y)x=z(yy\cdot x)$ if and only if $zR^2\cdot x=z\cdot xL_{y^2}$ if and only if $(R_y^2,L_{y^2}^{-1},I)\in AUT(L)$ for all $y\in L$. □

Corollary 4.1. *Let $(L,\cdot)$ be an LC(RC)-loop, then $(R_{y^2}L_x^2,L_y^{-2},L_x^2)$ (resp. $(R_y^2,L_{y^2}^{-1}R_x^2,R_x^2)$) belongs to $AUT(L)$ for all $x,y\in L$.*

Proof. In an LC-loop L, $(L_x^2,I,L_x^2)\in AUT(L)$ while in an RC-loop L we have $(I,R_x^2,R_x^2)\in AUT(L)$. Thus, by Theorem 4.1, for any LC-loop, $(R_{y^2},L_y^{-2},I)(L_x^2,I,L_x^2)=(R_{y^2}L_x^2,L_y^{-2},L_x^2)\in AUT(L)$ and for any RC-loop, $(R_y^2,L_{y^2}^{-1},I)(I,R_x^2,R_x^2)=(R_y^2,L_{y^2}^{-1}R_x^2,R_x^2)\in AUT(L)$. □

Theorem 4.2. *A loop L is a C-loop if and only if L is a right (left) alternative LC(RC)-loop.*

Proof. If $(L,\cdot)$ is an LC(RC)-loop, then by Theorem 4.1, (R_{y^2},L_y^{-2},I) (resp. $(R_y^2,L_{y^2}^{-1},I)$) $\in AUT(L)$ for all $y\in L$. If L has the right (left) alternative property, then $(R_y^2,L_y^{-2},I)\in AUT(L)$ for all $y\in L$ if and only if L is a C-loop. □

Lemma 4.1. *A loop L is an LC(RC,C)-loop if and only if $R_{y^2}\in\Phi(L)$ (resp. R_y^2, $R_y^2\in\Phi(L)$) and $(R_{y^2})^*=L_y^2\in\Phi^*(L)$ (resp. $(R_y^2)^*=L_{y^2}\in\Phi^*(L)$, $(R_y^2)^*=L_y^2\in\Phi^*(L)$) for all $y\in L$.*

Proof. This can be deduced from Theorem 4.1. □

Theorem 4.3. *Let $(G,\cdot)$ and $(H,\circ)$ be two distinct loops. If G is a central square LC(RC)-loop, H an alternative central square loop and the triple $\alpha=(A,B,B)$ (resp. $\alpha=(A,B,A)$) is an isotopism of G onto H, then H is a C-loop.*

Proof. G is a LC(RC)-loop if and only if R_{y^2} $(R_y^2)\in\Phi(G)$ and $(R_{y^2})^*=L_y^2$ (resp. $(R_y^2)^*=L_{y^2})\in\Phi^*(G)$ for all $x\in G$. Using the idea of [6], $L'_{xA}=B^{-1}L_xB$ and $R'_{xB}=A^{-1}R_xA$ for all $x\in G$. Using Corollary 2.1, for the case when G is an LC-loop: let $h:\Phi(G)\to\Phi(H)$ and $h^*:\Phi^*(G)\to\Phi^*(H)$ be defined as $h(U)=B^{-1}UB$ for all $U\in\Phi(G)$ and $h^*(V)=B^{-1}VB$ for all $V\in\Phi^*(G)$. This mappings are isomorphisms. Using the hypothesis, $h(R_{y^2})=h(L_{y^2})=h(L_y^2)=B^{-1}L_y^2B=$

$B^{-1}L_yBB^{-1}L_yB = L'_{yA}L'_{yA} = L'^2_{yA} = L'_{(yA)^2} = R'_{(yA)^2} = R'^2_{(yA)} \in \Phi(H)$. $h^*[(R_{y^2})^*] = h^*(L_y^2) = B^{-1}L_y^2B = B^{-1}L_yL_yB = B^{-1}L_yBB^{-1}L_yB = L'_{yA}L'_{yA} = L'^2_{yA} \in \Phi^*(H)$. So, $R'^2_y \in \Phi(H)$ and $(R'^2_y)^* = L'^2_y \in \Phi^*(H)$ for all $y \in H$ if and only if H is a C-loop.

For the case of RC-loops, using h and h^* as above, but now defined as: $h(U) = A^{-1}UA$ for all $U \in \Phi(G)$ and $h^*(V) = A^{-1}VA$ for all $V \in \Phi^*(G)$. This mappings are still isomorphisms. Using the hypotheses, $h(R_y^2) = A^{-1}R_y^2A = A^{-1}R_yAA^{-1}R_yA = R'_{yB}R'_{yB} = R'^2_{yB} \in \Phi(H)$. $h^*[(R_y^2)^*] = h^*(L_{y^2}) = h^*(R_{y^2}) = A^{-1}R_y^2A = A^{-1}R_yR_yB = B^{-1}R_yBB^{-1}R_yB = R'_{yA}R'_{yA} = R'^2_{yA} = R'_{(yA)^2} = L'_{(yA)^2} = L'^2_{yA} \in \Phi^*(H)$. So, $R'^2_y \in \Phi(H)$ and $(R'^2_y)^* = L'^2_y \in \Phi^*(H)$ if and only if H is a C-loop. □

Corollary 4.2. *Let $(G,\cdot)$ and $(H,\circ)$ be two distinct loops. If G is a central square left (right) RC(LC)-loop, H an alternative central square loop and the triple $\alpha = (A,B,B)$ (resp. $\alpha = (A,B,A)$) is an isotopism of G onto H, then H is a C-loop.*

Proof. By Theorem 4.2, G is a C-loop in each case. The rest of the proof follows by Theorem 4.3. □

Remark 4.1. Corollary 4.2 was proved in [13].

5. Central square C-loops of exponent 4

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

Theorem 5.1. *If for a C-loop $(L,\cdot)$ (I, L_z^2, JL_z^2J) or (R_z^2, I, JR_z^2J) lies in $AUT(L)$, then L is a loop of exponent 4.*

Proof. 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 $y^4 = e$. Hence L is a C-loop of exponent 4.

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 $x,y,z \in L \longrightarrow (xz^2) \cdot y = [(xy)^{-1}z^2]^{-1} \longrightarrow (xz^2) \cdot y = z^{-2}(xy) \longrightarrow (xz^2) \cdot y = z^{-2}x \cdot y \longrightarrow xz^2 = z^{-2}x \longrightarrow z^4 = e$. Hence L is a C-loop of exponent 4. □

Theorem 5.2. *If in a C-loop L for all $z \in L$ (I, L_z^2, JL_z^2J) or (R_z^2, I, JR_z^2J) is in $AUT(L)$, then L is a central square C-loop of exponent 4.*

Proof. 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 $x, y, z \in L$, whence $x \cdot z^2y = xy \cdot z^{-2}$.

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 $x, y, z \in L$, whence $xz^2 \cdot y = z^{-2} \cdot xy$.

So, in both these cases we have $x \cdot z^2y = xz^2 \cdot y \longleftrightarrow xy \cdot z^{-2} = z^{-2} \cdot xy$. For $t = xy$, we get $tz^{-2} = z^{-2}t \longleftrightarrow z^2t^{-1} = t^{-1}z^2$, which implies $z^2 \in C(L, \cdot)$ for all $z \in L$.

Since C-loops arenuclear square (cf. [19]), we have $z^2 \in Z(L, \cdot)$. Hence L is a central square C-loop. By Theorem 5.1, $x^4 = e$. □

Remark 5.1. In [19], C-loops of exponent 2 were found. In [19] and [11] i is proved that C-loops are naturally nuclear square. Our Theorem 5.2 gives some conditions under which a C-loop can be naturally central square.

Theorem 5.3. *If $A = (U, V, W) \in AUT(L)$ for a C-loop $(L, \cdot)$, then $A_\rho = (V, U, JWJ) \notin AUT(L)$, but $A_\mu = (W, JVJ, U), A_\lambda = (JUJ, W, V)$ are in $AUT(L)$.*

Proof. The fact that $A_\mu, A_\lambda \in AUT(L)$ has been shown in [5] and [16] for an I.P.L. L. Let L be a C-loop. Since C-loops are inverse property loops, $A_\mu = (W, JVJ, U)$, $A_\lambda = (JUJ, W, V) \in AUT(L)$. A C-loop is both an RC-loop and an LC-loop. So, $(I, R_x^2, R_x^2), (L_x^2, I, L_x^2) \in AUT(L, \cdot)$ for all $x \in L$. Thus, if $A_\rho \in AUT(L)$ when $A = (I, R_x^2, R_x^2)$ and $A = (L_x^2, I, L_x^2)$, $A_\rho = (I, L_x^2, JL_x^2J) \in AUT(L)$ and $A_\rho = (R_x^2, I, JR_x^2J) \in AUT(L)$ hence by Theorem 5.1 and Theorem 5.2, all C-loops are central square and of exponent 4 (in fact it will soon be seen in Theorem 5.4 that central square C-loops of exponent 4 are groups), which is false. So, $A_\rho = (V, U, JWJ) \notin AUT(L)$. □

Corollary 5.1. *If $(I, L_z^2, JL_z^2J) \in AUT(L)$, and $(R_z^2, I, JR_z^2J) \in AUT(L)$ for all $z \in L$, where $(L, \cdot)$ is a C-loop, then*

1. *L is flexible,*
2. *$(xy)^2 = (yx)^2$ for all $x, y \in L$,*
3. *$x \mapsto x^3$ is an anti-automorphism.*

Proof. This is a consequence of Theorem 5.2, Lemma 5.1 and Corollary 5.2 of [15]. □

Theorem 5.4. *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 $x, y \in L$.

Using Corollary 5.1 we see that for any $w \in L$ will be $wR(x,y) = wR_xR_yR_{xy}^{-1} = (wx)y\cdot(xy)^{-1} = (wx)(x^2yx^2)\cdot(xy)^{-1} = (wx^3)(yx^2)\cdot(xy)^{-1} = (w^2(w^3x^3))(yx^2)\cdot(xy)^{-1} = (w^2(xw)^3)(yx^2)\cdot(xy)^{-1} = w^2(xw)^3\cdot(yx^2)(xy)^{-1} = w^2(xw)^3\cdot[y\cdot x^2(xy)^{-1}] = w^2(xw)^3\cdot[y\cdot x^2(y^{-1}x^{-1})] = w^2(xw)^3\cdot[y(y^{-1}x^{-1}\cdot x^2)] = w^2(xw)^3\cdot[y(y^{-1}x)] = w^2(xw)^3\cdot x = w^2(w^3x^3)\cdot x = w^2\cdot(w^3x^3)x = w^2\cdot(w^3x^{-1})x = w^2w^3 = w^5 = w \longleftrightarrow R(x,y) = I \longleftrightarrow R_xR_yR_{xy}^{-1} = I \longleftrightarrow R_xR_y = R_{xy} \longleftrightarrow zR_xR_y = zR_{xy} \longleftrightarrow zx\cdot y = z\cdot xy \longleftrightarrow L$ is a group. □

Corollary 5.2. *If $(I, L_z^2, JL_z^2J) \in AUT(L)$ and $(R_z^2, I, JR_z^2J) \in AUT(L)$ for all $z \in L$, where L is a C-loop, then L is a group.*

Proof. This follows from Theorem 5.2 and Theorem 5.4. □

Remark 5.2. Central square C-loops of exponent 4 are A-loops. □

Acknowledgement. The first author 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:** *The study of properties of certain class of loops via their Bryant-Schneider groups*, Ph.D. thesis, University of Agriculture, Abeokuta, Nigeria, 2002.

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

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

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

[6] **R. Capodaglio Di Cocco:** *On isotopism and pseudo-automorphism of the loops*, Bollettino U. M. I. **7** (1993), 199 – 205.

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

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

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

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

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

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

[13] **T. G. Jaiyéọlá:** *An isotopic study of properties of central loops*, M.Sc. thesis, University of Agriculture, Abeokuta, Nigeria, 2005.

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

[15] **M. K. Kinyon, J. D. Phillips and P. Vojtěchovský:** *C-loops: Extensions and construction*, J. Algebra and its Appl. (to appear).

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

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

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

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

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

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

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

[23] **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

J. O. Adéníran: Department of Mathematics, University of Abẹ́ókùta, Abẹ́ókùta 110101, Nigeria
E-mail: ekenedilichineke@yahoo.com
T. G. Jaiyéọlà: Department of Mathematics, Obafemi Awolowo University, Ilé Ifè, Nigeria
E-mail: jaiyeolatemitope@yahoo.com

Quasigroups and Related Systems **15** (2007), 201 – 218

Intuitionistic (S, T)-fuzzy Lie ideals of Lie algebras

Muhammad Akram

Abstract

In this paper we introduce the notion of an intuitionistic (S,T)-fuzzy Lie ideal of a Lie algebra and investigate some related properties. Nilpotency of intuitionistic (S,T)-fuzzy Lie ideals is introduced. Intuitionistic (S,T)-fuzzy of adjoint representation of Lie algebras is introduced and the relation between this representation and nilpotent intuitionistic (S,T)-fuzzy Lie ideals is discussed. Killing form in the intuitionistic (S,T)-fuzzy case is defined and some of its properties are studied.

1. Introduction

Lie algebras were first discovered by Sophus Lie (1842-1899) when he 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 of physics and mathematics, such as spectroscopy of molecules, atoms, nuclei, hadrons, hyperbolic and stochastic differential equations.

After the introduction of fuzzy sets by L. Zadeh [14], various notions of higher-order fuzzy sets have been proposed. Among them, intuitionistic fuzzy sets, introduced by K. Atanassov [2, 3], have drawn the attention of many researchers in the last decades. This is mainly due to the fact that intuitionistic fuzzy sets are consistent with human behavior, by reflecting and modeling the hesitancy present in real-life situations. In fact, the fuzzy

2000 Mathematics Subject Classification: 04A72, 17B99
Keywords: Lie ideal, nilpotent Lie ideal, adjoint representation, Killing form.
This research work is supported by PUCIT.

sets give the degree of membership of an element in a given set, while intuitionistic fuzzy sets give both a degree of membership and a degree of non-membership. As for fuzzy sets, the degree of membership is a real number between 0 and 1. This is also the case for the degree of nonmembership, and furthermore the sum of these two degrees is not greater than 1. Fuzzy and anti fuzzy Lie ideals in Lie algebras have been studied in [1, 4, 7, 8, 9, 12].

In this paper, we introduce the notion of an intuitionistic (S,T)-fuzzy Lie ideal of a Lie algebra and investigate some of related properties. Nilpotency of intuitionistic (S,T)-fuzzy Lie ideals is introduced. Intuitionistic (S,T)-fuzzy of adjoint representation of Lie algebras is introduced and the relation between this representation and nilpotent intuitionistic (S,T)-fuzzy Lie ideals is proved. Killing form in the intuitionistic (S,T)-fuzzy case is defined and some of its properties are studied.

2. Preliminaries

A *Lie algebra* is a vector space L over a field F (equal to $\mathbf{R}$ or $\mathbf{C}$) on which $L \times L \to L$ denoted by $(x,y) \to [x,y]$ is defined satisfying 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 $x,y,z \in L$ (Jacobi identity).

In this paper by L will be denoted a Lie algebra. We note that the multiplication in a Lie algebra is not associative, i.e., it is not true in general that $[[x,y],z] = [x,[y,z]]$. But it is *anti commutative*, i.e., $[x,y] = -[y,x]$.

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. Let γ be a *fuzzy set* on L, i.e., a map $\gamma : L \to [0,1]$. A *fuzzy set* $\gamma : L \to [0,1]$ is called a *fuzzy Lie subalgebra* of L if

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

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

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

hold for all $x, y \in L$ and $\alpha \in F$. A fuzzy subset $\gamma : L \to [0,1]$ satisfying (a), (b) and

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

is called a *fuzzy Lie ideal* of L. The addition and the commutator $[\ ,\ ]$ of L are extended by Zadeh's extension principle [15], to two operations on I^L in the following way:

$$(\mu \oplus \lambda)(x) = \sup\{\min\{\mu(y), \lambda(z)\} \,|\, y, z \in L,\ y + z = x\},$$

$$\ll \mu, \lambda \gg (x) = \sup\{\min\{\mu(y), \lambda(z)\} \,|\, y, z \in L,\ [y,z] = x\},$$

where μ, λ are fuzzy sets on I^L and $x \in L$. The scalar multiplication αx for $\alpha \in F$ and $x \in L$ is extended to an action of the field F on I^L denoted by $\odot$ as follows for all $\mu \in I^L$, $\alpha \in F$ and $x \in L$:

$$(\alpha \odot \mu)(x) = \begin{cases} \mu(\alpha^{-1}x) & \text{if } \alpha \neq 0, \\ 1 & \text{if } \alpha = 0,\ x = 0, \\ 0 & \text{if } \alpha = 0,\ x \neq 0. \end{cases}$$

The two operations of the field F can be extended to two operations on I^F in the same way. The operations are denoted by $\oplus$ and $\circ$ as well [15]. The zeros of L and F are denoted by the same symbol 0. Obviously $0 \odot \mu = 1_0$ for every $\mu \in I^L$ and every $\mu \in I^F$, where 1_x is the fuzzy subset taking 1 at x and 0 elsewhere.

Let L be a Lie algebra. A fuzzy subset γ of L is called an *anti fuzzy Lie ideal* of L if the following axioms are satisfied:

(AF_1) $\gamma(x+y) \leqslant \max(\gamma(x), \gamma(y))$,

(AF_2) $\gamma(\alpha x) \leqslant \gamma(x)$,

(AF_3) $\gamma([x,y]) \leqslant \gamma(x)$

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

A *t-norm* is a mapping $T : [0,1] \times [0,1] \to [0,1]$ such that

(T_1) $T(x,1) = x$,

(T_2) $T(x,y) = T(y,x)$,

(T_3) $T(x, T(y,z)) = T(T(x,y), z)$,

(T_4) $T(x,y) \leqslant T(x,z)$ whenever $y \leqslant z$,

where $x, y, z \in [0,1]$. Replacing 1 by 0 in condition (T_1), we obtain the concept of *s-norm* S.

A mapping $A = (\mu_A, \lambda_A) : L \to [0,1] \times [0,1]$ is called an *intuitionistic fuzzy set* (IFS, in short) in L if $\mu_A(x) + \lambda_A(x) \leqslant 1$, for all $x \in L$, where the mappings $\mu_A : L \to [0,1]$ and $\lambda_A : L \to [0,1]$ denote the *degree of membership* (namely $\mu_A(x)$) and the *degree of non-membership* (namely $\lambda_A(x)$) of each element $x \in L$ to A respectively. In particular, $0_\sim$ and $1_\sim$ denote the *intuitionistic fuzzy empty set* and the *intuitionistic fuzzy whole set* in a set L defined by $0_\sim(x) = (0,1)$ and $1_\backsim(x) = (1,0)$ for each $x \in L$ respectively.

3. Intuitionistic (S,T)-fuzzy Lie ideals

Definition 3.1. An intuitionistic fuzzy set $A = (\mu_A, \lambda_A)$ on L is called an *intuitionistic fuzzy Lie ideal* of L with respect to the t-norm T and the s-norm S (shortly, intuitionistic (S,T)-fuzzy Lie ideals of L) if

(1) $\mu_A(x+y) \geqslant T(\mu_A(x), \mu_A(y))$ and $\lambda_A(x+y) \leqslant S(\lambda_A(x), \lambda_A(y))$,

(2) $\mu_A(\alpha x) \geqslant \mu_A(x)$ and $\lambda_A(\alpha x) \leqslant \lambda_A(x)$,

(3) $\mu_A([x,y]) \geqslant \mu_A(x)$ and $\lambda_A([x,y]) \leqslant \lambda_A(x)$

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

From (2) it follows that

(4) $\mu_A(0) \geqslant \mu_A(x)$ and $\lambda_A(0) \leqslant \lambda_A(x)$,

(5) $\mu_A(-x) = \mu_A(x)$ and $\lambda_A(-x) = \lambda_A(x)$

for all $x \in L$.

Example 3.2. Let $\Re^2 = \{(x,y) \,|, x, y \in R\}$ be the set of all 2-dimensional real vectors. Then $\Re^2$ with the bracket $[\ ,\ ]$ defined as usual cross product, i.e., $[x,y] = x \times y$, is a real Lie algebra. We define an intuitionistic fuzzy set $A = (\mu_A, \lambda_A) : L \to [0,1] \times [0,1]$ as follows:

$$\mu_A(x,y) = \begin{cases} m_1 & \text{if } x = y = 0, \\ m_2 & \text{otherwise,} \end{cases} \qquad \lambda_A(x,y) = \begin{cases} m_2 & \text{if } x = y = 0, \\ m_1 & \text{otherwise,} \end{cases}$$

where $m_1 > m_2$ and $m_1, m_2 \in [0,1]$. Let T be a t-norm which is defined by $T(x,y) = \max\{x+y-1, 0\}$ and S an s-norm which is defined by $S(x,y) = \min\{x+y, 1\}$ for all $x, y \in [0,1]$. Then by routine computation, we see that $A = (\mu_A, \lambda_A)$ is an intuitionistic (S,T)-fuzzy Lie ideal of L.

The following proposition is obvious.

Proposition 3.3. *If A is an intuitionistic (S,T)-fuzzy Lie ideal of L, then*

(i) $\mu_A([x,y]) \geqslant S(\mu_A(x),\mu_A(y))$,

(ii) $\lambda_A([x,y]) \leqslant T(\lambda_A(x),\lambda_A(y))$

for all $x,y \in L$. □

Theorem 3.4. *Let $G_0 \subset G_1 \subset G_2 \subset \ldots G_n = L$ be a chain of Lie ideals of a Lie algebra L. Then there exists an intuitionistic (S,T)-fuzzy Lie ideal A of L for which level subsets $U(\mu_A,\alpha)$ and $L(\lambda_A,\beta)$ coincide with this chain.*

Proof. Let $\{\alpha_k \,|\, k = 0,1,\ldots,n\}$ and $\{\beta_k \,|\, k = 0,1,\ldots,n\}$ be finite decreasing and increasing sequences in $[0,1]$ such that $\alpha_i+\beta_i \leqslant 1$, for $i = 0,1,\ldots,n$. Let $A = (\mu_A,\lambda_A)$ be an intuitionistic fuzzy set in L defined by $\mu_A(G_0) = \alpha_0$, $\lambda_A(G_0) = \beta_0$, $\mu_A(G_k \setminus G_{k-1}) = \alpha_k$ and $\lambda_A(G_k \setminus G_{k-1}) = \beta_k$ for $0 < k \leqslant n$. Let $x,y \in L$. If $x,y \in G_k \setminus G_{k-1}$, then $x+y, \alpha x, [x,y] \in G_k$ and

$$\begin{aligned}
\mu_A(x+y) &\geqslant \alpha_k = T(\mu_A(x),\mu_A(y)),\\
\lambda_A(x+y) &\leqslant \beta_k = S(\lambda_A(x)),\lambda_A(y)),\\
\mu_A(\alpha x) \geqslant \alpha_k = \mu_A(x), &\quad \lambda_A(\alpha x) \leqslant \beta_k = \lambda_A(x),\\
\mu_A([x,y]) \geqslant \alpha_k = \mu_A(x), &\quad \lambda_A([x,y]) \leqslant \beta_k = \lambda_A(x).
\end{aligned}$$

For $i > j$, if $x \in G_i \setminus G_{i-1}$ and $y \in G_j \setminus G_{j-1}$, then $\mu_A(x) = \alpha_i = \mu_A(y)$, $\lambda_A(x) = \beta_j = \lambda_A(y)$ and $x+y, \alpha x, [x,y] \in G_i$. Thus

$$\begin{aligned}
\mu_A(x+y) &\geqslant \alpha_i = T(\mu_A(x),\mu_A(y)),\\
\lambda_A(x+y) &\leqslant \beta_j = S(\lambda_A(x)),\lambda_A(y)),\\
\mu_A(\alpha x) \geqslant \alpha_i = \mu_A(x), &\quad \lambda_A(\alpha x) \leqslant \beta_j = \lambda_A(x),\\
\mu_A([x,y]) \geqslant \alpha_i = \mu_A(x), &\quad \lambda_A([x,y]) \leqslant \beta_j = \lambda_A(x).
\end{aligned}$$

So, $A = (\mu_A,\lambda_A)$ is an intuitionistic (S,T)-fuzzy Lie ideal of a Lie algebra L and all its nonempty level subsets are Lie ideals. Since $\mathrm{Im}(\mu_A) = \{\alpha_0,\alpha_1,\ldots,\alpha_n\}$, $\mathrm{Im}(\lambda_A) = \{\beta_0,\beta_1,\ldots,\beta_n\}$, level subsets of A form chains:

$$U(\mu_A,\alpha_0) \subset U(\mu_A,\alpha_1) \subset \ldots \subset U(\mu_A,\alpha_n) = L$$

and

$$L(\lambda_A,\beta_0) \subset L(\lambda_A,\beta_1) \subset \ldots \subset L(\lambda_A,\beta_n) = L,$$

respectively. Indeed,

$$U(\mu_A, \alpha_0) = \{x \in L \,|\, \mu_A(x) \geqslant \alpha_0\} = G_0,$$

$$L(\lambda_A, \beta_0) = \{x \in L \,|\, \lambda_A(x) \leqslant \beta_0\} = G_0.$$

We now prove that

$$U(\mu_A, \alpha_k) = G_k = L(\lambda_A, \beta_k) \text{ for } 0 < k \leqslant n.$$

Clearly, $G_k \subseteq U(\mu_k, \alpha_k)$ and $G_k \subseteq L(\lambda_A, \beta_k)$. If $x \in U(\mu_A, \alpha_k)$, then $\mu_A(x) \geqslant \alpha_k$ and so $x \notin G_i$ for $i > k$. Hence

$$\mu_A(x) \in \{\alpha_0, \alpha_1, \ldots, \alpha_k\},$$

which implies $x \in G_i$ for some $i \leqslant k$. Since $G_i \subseteq G_k$, it follows that $x \in G_k$. Consequently, $U(\mu_A, \alpha_k) = G_k$ for some $0 < k \leqslant n$. Now if $y \in L(\lambda_A, \beta_k)$, then $\lambda_A(x) \leqslant \beta_k$ and so $y \notin G_i$ for $j \leqslant k$. Thus

$$\lambda_A(x) \in \{\beta_0, \beta_1, \ldots, \beta_k\},$$

which implies $x \in G_j$ for some $j \leqslant k$. Since $G_j \subseteq G_k$, it follows that $y \in G_k$. Consequently, $L(\lambda_A, \beta_k) = G_k$ for some $0 < k \leqslant n$. This completes the proof. □

Definition 3.5. Let $f : L_1 \to L_2$ be a homomorphism of Lie algebras. Let $A = (\mu_A, \lambda_A)$ be an IFS of L_2. Then we can define an IFS $f^{-1}(A)$ of L_1 by

$$f^{-1}(A)(x) = A(f(x)) = (\mu_A(f(x)), \lambda_A(f(x))) \ \ \forall\, x \in L_1.$$

Proposition 3.6. *Let $f : L_1 \to L_2$ be an epimorphism of Lie algebras. Then A is an intuitionistic (S,T)-fuzzy Lie ideal of L_2 if and only if $f^{-1}(A)$ is an intuitionistic (S,T)-fuzzy Lie ideal of L_1.*

Proof. Straightforward. □

Definition 3.7. Let $f : L_1 \to L_2$ be a homomorphism of Lie algebras. Let $A = (\mu_A, \lambda_A)$ be an intuitionistic fuzzy set of L_1. Then IFS $f(A) = (f(\mu_A), f(\lambda_A))$ in L_2 is defined by

$$f(\mu_A)(y) = \begin{cases} \sup\{\mu_A(t) \mid t \in L_1, f(t) = y\}, & \text{if } f^{-1}(y) \neq \emptyset\ , \\ 0, & \text{otherwise,} \end{cases}$$

$$f(\lambda_A)(y) = \begin{cases} \inf\{\lambda_A(t) \mid t \in L_1, f(t) = y\}, & \text{if } f^{-1}(y) \neq \emptyset\ , \\ 1, & \text{otherwise.} \end{cases}$$

Definition 3.8. Let L_1 and L_2 be any sets and $f : L_1 \to L_2$ any function. Then, we call an intuitionistic fuzzy set $A = (\mu_A, \lambda_A)$ of L_1 *f-invariant* if $f(x) = f(y)$ implies $A(x) = A(y)$, i.e., $\mu_A(x) = \mu_A(y)$, $\lambda_A(x) = \lambda_A(y)$ for $x, y \in L_1$.

Theorem 3.9. *Let $f : L_1 \to L_2$ be an epimorphism of Lie algebras. Then $A = (\mu_A, \lambda_A)$ is an f-invariant intuitionistic (S,T)-fuzzy Lie ideal of L_1 if and only if $f(A)$ is an intuitionistic (S,T)-fuzzy ideal of L_2.*

Proof. Let $x, y \in L_2$. Then there exist $a, b \in L_1$ such that $f(a) = x$, $f(b) = y$ and $x + y = f(a + b)$, $\alpha x = \alpha f(a)$. Since A is f-invariant, by straightforward verification, we have

$$\begin{aligned}
f(\mu_A)(x+y) = \mu_A(a+b) &\geqslant T(\mu_A(a), \mu_A(b)) = T(f(\mu_A)(x), f(\mu_A)(y)),\\
f(\lambda_A)(x+y) = \lambda_A(a+b) &\leqslant S(\lambda_A(a), \lambda_A(b)) = S(f(\lambda_A)(x), f(\lambda_A)(y)),\\
f(\mu_A)(\alpha x) = \mu_A(\alpha a) &\geqslant \mu_A(a) = f(\mu_A)(x),\\
f(\lambda_A)(\alpha x) = \lambda_A(\alpha a) &\leqslant \lambda_A(a) = f(\lambda_A)(x),\\
f(\mu_A)([x,y]) = \mu_A([a,b]) = [\mu_A(a), \mu_A(b)] &\geqslant \mu_A(a) = f(\mu_A)(x),\\
f(\lambda_A)([x,y]) = \lambda_A([a,b]) = [\lambda_A(a), \lambda_A(b)] &\leqslant \lambda_A(a) = f(\lambda_A)(x).
\end{aligned}$$

Hence $f(A)$ is an intuitionistic (S,T)-fuzzy Lie ideal of L_2.

Conversely, if $f(A)$ is an intuitionistic (S,T)-fuzzy Lie ideal of L_2, then for any $x \in L_1$

$$\begin{aligned}
f^{-1}(f(\mu_A))(x) &= f(\mu_A)(f(x)) = \sup\{\mu_A(t) \mid t \in L_1, f(t) = f(x)\}\\
&= \sup\{\mu_A(t) \mid t \in L_1, \mu_(t) = \mu_A(x)\} = \mu_A(x),\\
f^{-1}(f(\lambda_A))(x) &= f(\lambda_A)(f(x)) = \inf\{\lambda_A(t) \mid t \in L_1, f(t) = f(x)\}\\
&= \inf\{\lambda_A(t) \mid t \in L_1, \lambda_(t) = \lambda_A(x)\} = \lambda_A(x).
\end{aligned}$$

Hence $f^{-1}(f(A)) = A$ is an intuitionistic (S,T)-fuzzy Lie ideal. □

Lemma 3.10. *Let $A = (\mu_A, \lambda_A)$ be an intuitionistic (S,T)-fuzzy Lie ideal of a Lie algebra L and let $x \in L$. Then $\mu_A(x) = t$, $\lambda_A(x) = s$ if and only if $x \in U(\mu_A, t)$, $x \notin U(\mu_A, s)$ and $x \in L(\lambda_A, s)$, $x \notin L(\lambda_A, t)$, for all $s > t$.*

Proof. Straightforward. □

Definition 3.11. A Lie ideal A of Lie algebra L is said to be *characteristic* if $f(A) = A$, for all $f \in Aut(L)$, where Aut(L) is the set of all automorphisms of a Lie algebra L. An intuitionistic (S,T)-fuzzy Lie ideal $A = (\mu_A, \lambda_A)$ of a Lie algebra L is called *characteristic* if $\mu_A(f(x)) = \mu_A(x)$ and $\lambda_A(f(x)) = \lambda_A(x)$ for all $x \in L$ and $f \in Aut(L)$.

Theorem 3.12. *An intuitionistic (S,T)-fuzzy Lie ideal is characteristic if and only if each its level set is a characteristic Lie ideal.*

Proof. Let an intuitionistic (S,T)-fuzzy Lie ideal $A = (\mu_A, \lambda_A)$ be characteristic, $t \in Im(\mu_A)$, $f \in Aut(L)$, $x \in U(\mu_A, t)$. Then $\mu_A(f(x)) = \mu_A(x) \geqslant t$, which means that $f(x) \in U(\mu_A, t)$. Thus $f(U(\mu_A, t)) \subseteq U(\mu_A, t)$. Since for each $x \in U(\mu_A, t)$ there exists $y \in L$ such that $f(y) = x$ we have $\mu_A(y) = \mu_A(f(y)) = \mu_A(x) \geqslant t$, whence we conclude $y \in U(\mu_A, t)$. Consequently $x = f(y) \in f(U(\mu_A, t))$. Hence $f(U(\mu_A, t)) = U(\mu_A, t)$. Similarly, $f(L(\lambda_A, s)) = L(\lambda_A, s)$. This proves that $U(\mu_A, t)$-and $L(\lambda_A, s)$ are characteristic.

Conversely, if all levels of $A = (\mu_A, \lambda_A)$ are characteristic Lie ideals of L, then for $x \in L$, $f \in Aut(L)$ and $\mu_A(x) = t < s = \lambda_A(x)$, by Lemma 3.10, we have $x \in U(\mu_A, t)$, $x \notin U(\mu_A, s)$ and $x \in L(\lambda_A, s)$, $x \notin L(\lambda_A, t)$. Thus $f(x) \in f(U(\mu_A, t)) = U(\mu_A, t)$ and $f(x) \in f(L(\lambda_A, s)) = L(\lambda_A, s)$, i.e., $\mu_A(f(x)) \geqslant t$ and $\lambda_A(f(x)) \leqslant s$. For $\mu_A(f(x)) = t_1 > t$, $\lambda_A(f(x)) = s_1 < s$ we have $f(x) \in U(\mu_A, t_1) = f(U(\mu_A, t_1))$, $f(x) \in L(\lambda_A, s_1) = f(L(\lambda_A, s_1))$, whence $x \in U(\mu_A, t_1)$, $x \in L(\mu_A, s_1)$. This is a contradiction. Thus $\mu_A(f(x)) = \mu_A(x)$ and $\lambda_A(f(x)) = \lambda_A(x)$. So, $A = (\mu_A, \lambda_A)$ is characteristic. □

Using the same method as in the proof of Theorems 4.6 in [5] we can prove the following theorem.

Theorem 3.13. *Let $\{C_\alpha \mid \alpha \in \Lambda \subseteq [0, \frac{1}{2}]\}$ be a collection of Lie ideals of a Lie algebra L such that $L = \bigcup_{\alpha \in \Lambda} C_\alpha$, and for every $\alpha, \beta \in \Lambda$, $\alpha < \beta$ if and only if $C_\beta \subset C_\alpha$. Then an intuitionistic fuzzy set $A = (\mu_A, \lambda_A)$ defined by*

$$\mu_A(x) = \sup\{\alpha \in \Lambda \mid x \in C_\alpha\} \quad \text{and} \quad \lambda_A(x) = \inf\{\alpha \in \Lambda \mid x \in C_\alpha\}$$

is an intuitionistic (S,T)-fuzzy Lie ideal of L. □

Theorem 3.14. *Let $A = (\mu_A, \lambda_A)$ be an intuitionistic (S,T)-fuzzy Lie ideal of Lie algebra L. Define a binary relation $\sim$ on L by*

$$x \sim y \longleftrightarrow \mu_A(x - y) = \mu_A(0) \text{ and } \lambda_A(x - y) = \lambda_A(0).$$

Then $\sim$ is a congruence on L.

Proof. The reflexivity and symmetry is obvious. To prove transitivity let $x \sim y$ and $y \sim z$. Then $\mu_A(x-y) = \mu_A(0)$, $\mu_A(y-z) = \mu_A(0)$ and $\lambda_A(x-y) = \lambda_A(0)$, $\lambda_A(y-z) = \lambda_A(0)$, by (5). Thus

$$\mu_A(x-z) = \mu_A(x-y+y-z) \geqslant T(\mu_A(x-y), \mu_A(y-z)) = \mu_A(0),$$
$$\lambda_A(x-z) = \lambda_A(x-y+y-z) \leqslant S(\lambda_A(x-y), \lambda_A(y-z)) = \lambda(0),$$

whence, by (4), we conclude $x \sim z$.

If $x_1 \sim y_1$ and $x_2 \sim y_2$, then

$$\begin{aligned}\mu_A((x_1+x_2)-(y_1+y_2)) &= \mu_A((x_1-y_1)+(x_2-y_2)) \\ &\geqslant T(\mu_A(x_1-y_1), \mu_A(x_2-y_2)) = \mu_A(0),\end{aligned}$$
$$\begin{aligned}\lambda_A((x_1+x_2)-(y_1+y_2)) &= \lambda_A((x_1-y_1)+(x_2-y_2)) \\ &\leqslant S(\lambda_A(x_1-y_1), \lambda_A(x_2-y_2)) = \lambda_A(0),\end{aligned}$$
$$\mu_A((\alpha x_1 - \alpha y_1) = \mu_A(\alpha(x_1-y_1)) \geqslant \mu_A(x_1-y_1) = \mu(0),$$
$$\lambda_A((\alpha x_1 - \alpha y_1) = \lambda_A(\alpha(x_1-y_1)) \leqslant \lambda_A(x_1-y_1) = \lambda_A(0),$$
$$\mu_A([x_1,x_2]-[y_1,y_2]) = \mu_A([x_1-y_1],[x_2-y_2]) \geqslant \mu_A(x_1-y_1) = \mu_A(0),$$
$$\lambda_A([x_1,x_2]-[y_1,y_2]) = \lambda_A([x_1-y_1],[x_2-y_2]) \leqslant \lambda_A(x_1-y_1) = \lambda_A(0).$$

Now, applying (4), it is easily to see that $x_1+x_2 \sim y_1+y_2$, $\alpha x_1 \sim \alpha y_1$ and $[x_1,x_2] \sim [y_1,y_2]$. So, $\sim$ is a congruence. □

4. Nilpotency of intuitionistic (S,T)-fuzzy Lie ideals

Definition 4.1. Let $A = (\mu_A, \lambda_A) \in I^L$, an intuitionistic fuzzy subspace of L generated by A will be denoted by $[A]$. It is the intersection of all intuitionistic fuzzy subspaces of L containing A. For all $x \in L$, we define:

$$[\mu_A](x) = \sup\{\min \mu_A(x_i) : \mid x = \sum \alpha_i x_i, \alpha_i \in F, x_i \in L\},$$
$$[\lambda_A](x) = \inf\{\max \lambda_A(x_i) \mid x = \sum \alpha_i x_i, \alpha_i \in F, x_i \in L\}.$$

Definition 4.2. Let $f : L_1 \to L_2$ be a homomorphism of Lie algebras which has an extension $f : I^{L_1} \to I^{L_2}$ defined by:

$$f(\mu_A)(y) = \sup\{\mu_A(x), x \in f^{-1}(y)\},$$
$$f(\lambda_A)(y) = \inf\{\lambda_A(x), x \in f^{-1}(y)\},$$

for all $A = (\mu_A, \lambda_A) \in I^{L_1}$, $y \in L_2$. Then $f(A)$ is called the *homomorphic image* of A.

The following two propositions are obvious.

Proposition 4.3. *Let $f : L_1 \to L_2$ be a homomorphism of Lie algebras and let $A = (\mu_A, \lambda_A)$ be an intuitionistic (S,T)-fuzzy Lie ideal of L_1. Then*
(i) $f(A)$ is an intuitionistic (S,T)-fuzzy Lie ideal of L_2,
(ii) $f([A]) \supseteq [f(A)]$.

Proposition 4.4. *If A and B are intuitionistic (S,T)-fuzzy Lie ideals in L, then $[A,B]$ is an intuitionistic (S,T)-fuzzy Lie ideal of L.*

Theorem 4.5. *Let A_1, A_2, B_1, B_2 be intuitionistic (S,T)-fuzzy Lie ideals in L such that $A_1 \subseteq A_2$ and $B_1 \subseteq B_2$, then $[A_1, B_1] \subseteq [A_2, B_2]$.*

Proof. Indeed,

$$\begin{aligned}
\ll \mu_{A_1}, \mu_{B_1} \gg (x) &= \sup\{T(\mu_{A_1}(a), \mu_{B_1}(b)) \mid a, b \in L_1, [a,b] = x\} \\
&\geqslant \sup\{T(\mu_{A_2}(a), \mu_{B_2}(b)) \mid a, b \in L_1, [a,b] = x\} \\
&= \ll \mu_{A_2}, \mu_{B_2} \gg (x), \\
\ll \lambda_{A_1}, \lambda_{B_1} \gg (x) &= \inf\{S(\lambda_{A_1}(a), \lambda_{B_1}(b)) \mid a, b \in L_1, [a,b] = x\} \\
&\leqslant \inf\{S(\lambda_{A_2}(a), \lambda_{B_2}(b)) \mid a, b \in L_1, [a,b] = x\} \\
&= \ll \lambda_{A_2}, \lambda_{B_2} \gg (x).
\end{aligned}$$

Hence $[A_1, B_1] \subseteq [A_2, B_2]$. □

Let $A = (\mu_A, \lambda_A)$ be an intuitionistic (S,T)-fuzzy Lie ideal in L. Putting

$$A^0 = A,\ A^1 = [A, A_0],\ A^2 = [A, A_1],\ \ldots,\ A^n = [A, A^{n-1}]$$

we obtain a descending series of an intuitionistic (S,T)-fuzzy Lie ideals

$$A^0 \supseteq A^1 \supseteq A^2 \supseteq \ldots \supseteq A^n \supseteq \ldots$$

and a series of intuitionistic fuzzy sets $B^n = (\mu_B^n, \lambda_B^n)$ such that

$$\mu_B^n = \sup\{\mu_A^n(x) \,|\, 0 \neq x \in L\}, \quad \lambda_B^n = \inf\{\lambda_A^n(x) \,|\, 0 \neq x \in L\}.$$

Definition 4.6. An intuitionistic (S,T)-fuzzy Lie ideal $A = (\mu_A, \lambda_A)$ is called *nilpotent* if there exists a positive integer n such that $B^n = 0_\sim$.

Theorem 4.7. *A homomorphic image of a nilpotent intuitionistic (S,T)-fuzzy Lie ideal is a nilpotent intuitionistic (S,T)-fuzzy Lie ideal.*

Proof. Let $f : L_1 \to L_2$ be a homomorphism of Lie algebras and let $A = (\mu_A, \lambda_A)$ be a nilpotent intuitionistic (S,T)-fuzzy Lie ideal in L_1. Assume that $f(A) = B$. We prove by induction that $f(A^n) \supseteq B^n$ for every natural n. First we claim that $f([A,A]) \supseteq [f(A), f(A)] = [B,B]$. Let $y \in L_2$, then

$$\begin{aligned}
&f(\ll \mu_A, \mu_A \gg)(y) = \sup\{\ll \mu_A, \mu_A \gg)(x) \mid f(x) = y\} \\
&= \sup\{\sup\{T(\mu_A(a), \mu_A(b)) \mid a,b \in L_1, [a,b] = x, f(x) = y\}\} \\
&= \sup\{T(\mu_A(a), \mu_A(b)) \mid a,b \in L_1, [a,b] = x, f(x) = y\} \\
&= \sup\{T(\mu_A(a), \mu_A(b)) \mid a,b \in L_1, [f(a), f(b)] = x\} \\
&= \sup\{T(\mu_A(a), \mu_A(b)) \mid a,b \in L_1, f(a) = u, f(b)] = v, [u,v] = y\} \\
&\geqslant \sup\{T(\sup_{a \in f^{-1}(u)} \mu_A(a), \sup_{b \in f^{-1}(v)} \mu_A(b)) \mid [u,v] = y\} \\
&= \sup\{T(f(\mu_A)(u), f(\mu_A)(v)) \mid [u,v] = y\} = \ll f(\mu_A), f(\mu_A) \gg (y),
\end{aligned}$$

$$\begin{aligned}
&f(\ll \lambda_A, \lambda_A \gg)(y) = \inf\{\ll \lambda_A, \lambda_A \gg)(x) \mid f(x) = y\} \\
&= \inf\{\inf\{S(\lambda_A(a), \lambda_A(b)) \mid a,b \in L_1, [a,b] = x, f(x) = y\}\} \\
&= \inf\{S(\lambda_A(a), \lambda_A(b)) \mid a,b \in L_1, [a,b] = x, f(x) = y\} \\
&= \inf\{S(\lambda_A(a), \lambda_A(b)) \mid a,b \in L_1, [f(a), f(b)] = x\} \\
&= \inf\{S(\lambda_A(a), \lambda_A(b)) \mid a,b \in L_1, f(a) = u, f(b)] = v, [u,v] = y\} \\
&\leqslant \inf\{S(\inf_{a \in f^{-1}(u)} \lambda_A(a), \inf_{b \in f^{-1}(v)} \lambda_A(b)) \mid [u,v] = y\} \\
&= \inf\{S(f(\lambda_A)(u), f(\lambda_A)(v)) \mid [u,v] = y\} = \ll f(\lambda_A), f(\lambda_A) \gg (y).
\end{aligned}$$

Thus

$$f([A,A]) \supseteq f(\ll A, A \gg) \supseteq \ll f(A), f(A) \gg = [f(A), f(A)].$$

For $n > 1$, we get

$$f(A^n) = f([A, A^{n-1}]) \supseteq [f(A), f(A^{n-1})] \supseteq [B, B^{n-1}] = B^n.$$

Let m be a positive integer such that $A^m = 0_\sim$. Then for $0 \neq y \in L_2$ we have

$$\mu_B^m(y) \leqslant f(\mu_A^m)(y) = f(0)(y) = \sup\{0(a) \,|\, f(x) = y\} = 0,$$

$$\lambda_B^m(y) \geqslant f(\lambda_A^m)(y) = f(1)(y) = \inf\{1(a) \,|\, f(x) = y\} = 1.$$

Thus $B^m = 0_\sim$. This completes the proof. □

Let $A = (\mu_A, \lambda_A)$ be an intuitionistic (S,T)-fuzzy Lie ideal in L. Putting

$$A^{(0)} = A,\ A^{(1)} = [A^{(0)}, A^{(0)}],\ A^{(2)} = [A^{(1)}, A^{(1)}], \ldots, A^{(n)} = [A^{(n-1)}, A^{(n-1)}]$$

we obtain series

$$A^{(0)} \subseteq A^{(1)} \subseteq A^{(2)} \subseteq \ldots \subseteq A^{(n)} \subseteq \ldots$$

of intuitionistic (S,T)-fuzzy Lie ideals and a series of intuitionistic fuzzy sets $B^{(n)} = (\mu_B^{(n)}, \lambda_B^{(n)})$ such that

$$\mu_B^{(n)} = \sup\{\mu_A^{(n)}(x) \,|\, 0 \neq x \in L\}, \quad \lambda_B^{(n)} = \inf\{\lambda_A^{(n)}(x) \,|\, 0 \neq x \in L\}.$$

Definition 4.8. An intuitionistic (S,T)-fuzzy Lie ideal $A = (\mu_A, \lambda_A)$ is called *solvable* if there exists a positive integer n such that $B^{(n)} = 0_\sim$.

Theorem 4.9. *A nilpotent intuitionistic (S,T)-fuzzy Lie ideal is solvable.*

Proof. It is enough to prove that $A^{(n)} \subseteq A^n$ for all positive integers n. We prove it by induction on n and by the use of Theorem 4.5:

$$A^{(1)} = [A, A] = A^1, \qquad A^{(2)} = [A^{(1)}, A^{(1)}] \subseteq [A, A^{(1)}] = A^2.$$

$$A^{(n)} = [A^{(n-1)}, A^{(n-1)}] \subseteq [A, A^{(n-1)}] \subseteq [A, A^{(n-1)}] = A^n.$$

This completes the proof. □

Definition 4.10. Let $A = (\mu_A, \lambda_A)$ and $B = (\mu_B, \lambda_B)$ be two intuitionistic (S,T)-fuzzy Lie ideals of a Lie algebra L. The sum $A \oplus B$ is called a *direct sum* if $A \cap B = 0_\sim$.

Theorem 4.11. *The direct sum of two nilpotent intuitionistic (S,T)-fuzzy Lie ideals is also a nilpotent intuitionistic (S,T)-fuzzy Lie ideal.*

Proof. Suppose that $A = (\mu_A, \lambda_A)$ and $B = (\mu_B, \lambda_B)$ are two intuitionistic (S,T)-fuzzy Lie ideals such that $A \cap B = 0_\sim$. We claim that $[A, B] = 0_\sim$. Let $x(\neq 0) \in L$, then

$$\ll \mu_A, \mu_B \gg (x) = \sup\{T(\mu_A(a), \mu_B(b)) \mid [a,b] = x\} \leqslant T(\mu_A(x), \mu_B(x)) = 0$$

and

$$\ll \lambda_A, \lambda_B \gg (x) = \inf\{S(\lambda_A(a), \lambda_B(b)) \mid [a,b] = x\} \geqslant S(\lambda_A(x), \lambda_B(x)) = 1.$$

This proves our claim. Thus we obtain $[A^m, B^n] = 0_\sim$ for all positive integers m, n. Now we again claim that $(A \oplus B)^n \subseteq A^n \oplus B^n$ for positive integer n. We prove this claim by induction on n. For $n = 1$,

$$(A \oplus B)^1 = [A \oplus B, A \oplus B] \subseteq [A, A] \oplus [A, B] \oplus [B, A] \oplus [B, B] = A^1 \oplus B^1.$$

Now for $n > 1$,

$$\begin{aligned}(A \oplus B)^n &= [A \oplus B, (A \oplus B)^{n-1}] \subseteq [A \oplus B, A^{n-1} \oplus B^{n-1}] \\ &\subseteq [A, A^{n-1}] \oplus [A, B^{n-1}] \oplus [B, A^{n-1}] \oplus [B, B^{n-1}] = A^n \oplus B^n.\end{aligned}$$

Since there are two positive integers p and q such that $A^p = B^q = 0_\sim$, we have $(A \oplus B)^{p+q} \subseteq A^{p+q} \oplus B^{p+q} = 0_\sim$. □

In a similar way we can prove the following theorem.

Theorem 4.12. *The direct sum of two solvable intuitionistic (S,T)-fuzzy Lie ideals is a solvable intuitionistic (S,T)-fuzzy Lie ideal.*

Definition 4.13. For any $x \in L$ we define the function $adx : L \to L$ putting $adx(y) = [x, y]$. It is clear that this function is a linear homomorphism with respect to y. The set $H(L)$ of all linear homomorphisms from L into itself is made into a Lie algebra by defining a commutator on it by $[f, g] = f \circ g - g \circ f$. The function $ad : L \to H(L)$ defined by $ad(x) = adx$ is a Lie homomorphism (see [6]) which is called the *adjoint representation* of L.

The adjoint representation $adx : L \to L$ is extended to $\overline{ad}x : I^L \to I^L$ by putting

$$\overline{ad}x(\gamma)(y) = \sup\{\gamma(a) : [x, a] = y\}$$

for all $\gamma \in I^L$ and $y \in L$.

Theorem 4.14. *Let $A = (\mu_A, \lambda_A)$ be an intuitionistic (S,T)-fuzzy Lie ideal in a Lie algebra L. Then $A^n \subseteq [A_n]$ for any $n > 0$, where an intuitionistic fuzzy subset $[A_n] = ([\mu_{A_n}], [\lambda_{A_n}])$ is defined by*

$$[\mu_{A_n}](x) = \sup\{\mu_A(a) \mid [x_1, [x_2, [\ldots, [x_n, a]\ldots]]] = x, \quad x_1, \ldots, x_n \in L\},$$
$$[\lambda_{A_n}](x) = \inf\{\lambda_A(a) \mid [x_1, [x_2, [\ldots, [x_n, a]\ldots]]] = x, \quad x_1, \ldots, x_n \in L\}.$$

Proof. It is enough to prove that $\ll A, A^{n-1} \gg \subseteq [A_n]$. We prove it by induction on n. For n=1 and $x \in L$, we have

$$\begin{aligned}\ll \mu_A, \mu_A \gg (x) &= \sup\{T(\mu_A(a), \mu_A(b)) \mid [a, b] = x\} \\ &\geqslant \sup\{\mu_A(b) \mid [a, b] = x, a \in L\} = [\mu_{A_1}](x),\end{aligned}$$

$$\ll \lambda_A, \lambda_A \gg (x) = \inf\{S(\mu_A(a), \mu_A(b)) \mid [a,b] = x\}$$
$$\leqslant \inf\{\lambda_A(b) : [a,b] = x, a \in L\} = [\lambda_{A_1}](x).$$

For $n > 1$,

$$\ll \mu_A, \mu_A^{n-1} \gg (x) = \sup\{T(\mu_A(a), \mu_A^{n-1}(b)) \mid [a,b] = x\}$$
$$= \sup\{T(\mu_A(a), [\mu_A(b), \mu_A^{n-2}(b)]) \mid [a,b] = x\}$$
$$\geqslant \sup\{T(\mu_A(a), \sup\{\ll \mu_A, \mu_A^{n-2} \gg (b_i) \mid b = \textstyle\sum \alpha_i b_i\}) \mid [a,b] = x\}$$
$$\geqslant \sup\{T(\mu_A(a), \sup\{[\mu_{A_{n-1}}](b_i) \mid b = \textstyle\sum \alpha_i b_i\}) \mid [a,b] = x\}$$
$$\geqslant \sup\{T(\mu_A(a), [\mu_{A_{n-1}}](b_i)) \mid \textstyle\sum \alpha_i [a,b_i] = x\}$$
$$\geqslant \sup\{T(\mu_A(a), \sup\{\mu_{A_{n-1}}(c_i) \mid b_i = \textstyle\sum \beta_i c_i\}) \mid \sum \alpha_i [a,b_i] = x\}$$
$$\geqslant \sup\{T(\mu_A(a), \mu_{A_{n-1}}(c_i)) \mid \textstyle\sum \gamma_i [a,c_i] = x\}$$
$$\geqslant \sup\{T(\mu_A(a), \sup\{\mu_A(d_i)) \mid [x_1, [x_2, [\ldots, [x_{n-1}, d_i] \ldots]]] = c_i\} \mid \textstyle\sum \gamma_i [a,c_i] = x\}$$
$$\geqslant \sup\{T(\mu_A(a), \mu_A(d_i)) \mid \textstyle\sum \gamma_i [a, [x_1, [x_2, [\ldots, [x_{n-1}, d_i] \ldots]]]] = x\}$$
$$\geqslant \sup\{\mu_{A_n}(d_i) \mid \textstyle\sum \gamma_i [a, [x_1, [x_2, [\ldots, [x_{n-1}, d_i] \ldots]]]] = x\} \geqslant [\mu_{A_n}](x),$$

$$\ll \lambda_A, \lambda_A^{n-1} \gg (x) = \inf\{S(\lambda_A(a), \lambda_A^{n-1}(b)) \mid [a,b] = x\}$$
$$= \inf\{S(\lambda_A(a), [\lambda_A(b), \lambda_A^{n-2}(b)]) \mid [a,b] = x\}$$
$$\leqslant \inf\{S(\lambda_A(a), \inf\{\ll \lambda_A, \lambda_A^{n-2} \gg (b_i) \mid b = \textstyle\sum \alpha_i b_i\}) \mid [a,b] = x\}$$
$$\leqslant \inf\{S(\lambda_A(a), \inf\{[\lambda_{A_{n-1}}](b_i) \mid b = \textstyle\sum \alpha_i b_i\}) \mid [a,b] = x\}$$
$$\leqslant \inf\{S(\lambda_A(a), [\lambda_{A_{n-1}}](b_i)) \mid \textstyle\sum \alpha_i [a,b_i] = x\}$$
$$\leqslant \inf\{S(\lambda_A(a), \inf\{\lambda_{A_{n-1}}(c_i) \mid b_i = \textstyle\sum \beta_i c_i\}) \mid \sum \alpha_i [a,b_i] = x\}$$
$$\leqslant \inf\{S(\lambda_A(a), \lambda_{A_{n-1}}(c_i)) \mid \textstyle\sum \gamma_i [a,c_i] = x\}$$
$$\leqslant \inf\{S(\lambda_A(a), \inf\{\lambda_A(d_i)) \mid [x_1, [x_2, [\ldots, [x_{n-1}, d_i] \ldots]]] = c_i\} \mid \textstyle\sum \gamma_i [a,c_i] = x\}$$
$$\leqslant \inf\{S(\lambda_A(a), \lambda_A(d_i)) \mid \textstyle\sum \gamma_i [a, [x_1, [x_2, [\ldots, [x_{n-1}, d_i] \ldots]]]] = x\}$$
$$\leqslant \inf\{\lambda_{A_n}(d_i) \mid \textstyle\sum \gamma_i [a, [x_1, [x_2, [\ldots, [x_{n-1}, d_i] \ldots]]]] = x\} \leqslant [\lambda_{A_n}](x).$$

This complete the proof. □

Theorem 4.15. *If for an intuitionistic (S,T)-fuzzy Lie ideal $A = (\mu_A, \lambda_A)$ there exists a positive integer n such that*

$$(a\bar{d}x_1 \circ a\bar{d}x_2 \circ \cdots \circ a\bar{d}x_n)(\mu_A) = 0,$$
$$(a\bar{d}x_1 \circ a\bar{d}x_2 \circ \cdots \circ a\bar{d}x_n)(\lambda_A) = 1,$$

for all $x_1, \ldots, x_n \in L$, then A is nilpotent.

Proof. For $x_1,\ldots,x_n \in L$ and $x(\neq 0) \in L$, we have

$$(a\overline{d}x_1 \circ \cdots \circ a\overline{d}x_n)(\mu_A)(x) = \sup\{\mu_A(a) \,|\, [x_1,[x_2,[\ldots,[x_n,a]\ldots]]] = x\} = 0,$$

$$(a\overline{d}x_1 \circ \cdots \circ a\overline{d}x_n)(\lambda_A)(x) = \inf\{\lambda_A(a) \,|\, [x_1,[x_2,[\ldots,[x_n,a]\ldots]]] = x\} = 1.$$

Thus $[A_n] = 0_\sim$. From Theorem 4.14, it follows that $A^n = 0_\sim$. Hence $A = (\mu_A, \lambda_A)$ is a nilpotent intuitionistic (S,T)-fuzzy Lie ideal. □

5. The intuitionistic (S,T)-fuzzy Killing form

The mapping $K : L \times L \to F$ defined by $K(x,y) = Tr(adx \circ ady)$, where Tr is the *trace* of a linear homomorphism, is a symmetric bilinear form which is called the *Killing form*. It is not difficult to see that this form satisfies the identity $K([x,y],z) = K(x,[y,z])$. The form K can be naturally extended to $\overline{K} : I^{L\times L} \to I^F$ defined by putting

$$\overline{K}(\mu_A)(\beta) = \sup\{\mu_A(x,y) \,|\, Tr((adx \circ ady)) = \beta\},$$
$$\overline{K}(\lambda_A)(\beta) = \inf\{\lambda_A(x,y) \,|\, Tr((adx \circ ady)) = \beta\}$$

The Cartesian product of two intuitionistic (S,T)-fuzzy sets $A = (\mu_A, \lambda_A)$ and $B = (\mu_B, \lambda_B)$ is defined as

$$(\mu_A \times \mu_B)(x,y) = T(\mu_A(x), \mu_B(y)),$$
$$(\lambda_A \times \lambda_B)(x,y) = S(\lambda_A(x), \lambda_B(y)).$$

Similarly we define

$$\overline{K}(\mu_A \times \mu_B)(\beta) = \sup\{T(\mu_A(x), \mu_B(y)) \,|\, Tr((adx \circ ady)) = \beta\},$$
$$\overline{K}(\lambda_A \times \lambda_B)(\beta) = \inf\{S(\lambda_A(x), \lambda_B(y)) \,|\, Tr((adx \circ ady)) = \beta\}.$$

Proposition 5.1. *Let $A = (\mu_A, \lambda_A)$ be an intuitionistic (S,T)-fuzzy Lie ideal of Lie algebra L. Then*

(*i*) $1_{\sim(x+y)} = 1_{\sim x} \oplus 1_{\sim y}$,

(*ii*) $1_{\sim(\alpha x)} = \alpha \odot 1_{\sim x}$

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

Proof. Straightforward. □

Theorem 5.2. *Let $A = (\mu_A, \lambda_A)$ be an intuitionistic (S,T)-fuzzy Lie ideal of Lie algebra L. Then $\overline{K}(\mu_A \times 1_{(\alpha x)}) = \alpha \odot \overline{K}(\mu_A \times 1_x)$ and $\overline{K}(\lambda_A \times 0_{(\alpha x)}) = \alpha \odot \overline{K}(\lambda_A \times 0_x)$ for all $x \in L$, $\alpha \in F$.*

Proof. If $\alpha = 0$, then for $\beta = 0$ we have

$$\begin{aligned}\overline{K}(\mu_A \times 1_0)(0) &= \sup\{T(\mu_A(x), 1_0(y)) \,|\, Tr(adx \circ ady) = 0\} \\ &\geqslant T(\mu_A(0), 1_0(0)) = 0, \\ \overline{K}(\lambda_A \times 0_0)(0) &= \inf\{S(\lambda_A(x), 0_0(y)) : Tr(adx \circ ady) = 0\} \\ &\leqslant S(\lambda_A(0), 0_0(0)) = 1.\end{aligned}$$

For $\beta \neq 0$ $Tr((adx \circ ady) = \beta$ means that $x \neq 0$ and $y \neq 0$. So,

$$\begin{aligned}\overline{K}(\mu_A \times 1_0)(\beta) &= \sup\{T(\mu_A(x), 1_0(y)) \,|\, Tr((adx \circ ady) = \beta\} = 0, \\ \overline{K}(\lambda_A \times 0_0)(\beta) &= \inf\{S(\lambda_A(x), 0_0(y)) \,|\, Tr((adx \circ ady) = \beta\} = 1.\end{aligned}$$

If $\alpha \neq 0$, then for arbitrary β we obtain

$$\begin{aligned}\overline{K}(\mu_A \times 1_{\alpha x})(\beta) &= \sup\{T(\mu_A(y), 1_{\alpha x}(z)) \,|\, Tr((ady \circ adz) = \beta\} \\ &= \sup\{T(\mu_A(y), \alpha \odot 1_x(z)) \,|\, Tr((ady \circ adz) = \beta\} \\ &= \sup\{T(\mu_A(y), 1_x(\alpha^{-1}z)) \,|\, \alpha Tr((ady \circ ad(\alpha^{-1}z)) = \beta\} \\ &= \sup\{T(\mu_A(y), 1_x(\alpha^{-1}z)) \,|\, Tr((ady \circ ad(\alpha^{-1}z)) = \alpha^{-1}\beta\} \\ &= \overline{K}(\mu_A \times 1_x)(\alpha^{-1}\beta) = \alpha \odot \overline{K}(\mu_A \times 1_x)(\beta),\end{aligned}$$

$$\begin{aligned}\overline{K}(\lambda_A \times 0_{\alpha x})(\beta) &= \inf\{S(\lambda_A(y), 0_{\alpha x}(z)) \,|\, Tr((ady \circ adz) = \beta\} \\ &= \inf\{S(\lambda_A(y), \alpha \odot 0_x(z)) \,|\, Tr((ady \circ adz) = \beta\} \\ &= \inf\{S(\lambda_A(y), 0_x(\alpha^{-1}z)) \,|\, \alpha Tr((ady \circ ad(\alpha^{-1}z)) = \beta\} \\ &= \inf\{S(\lambda_A(y), 0_x(\alpha^{-1}z)) \,|\, Tr((ady \circ ad(\alpha^{-1}z)) = \alpha^{-1}\beta\} \\ &= \overline{K}(\lambda_A \times 1_x)(\alpha^{-1}\beta) = \alpha \odot \overline{K}(\lambda_A \times 0_x)(\beta).\end{aligned}$$

This completes the proof. □

Theorem 5.3. *Let $A = (\mu_A, \lambda_A)$ be an intuitionistic (S,T)-fuzzy Lie ideal of a Lie algebra L. Then $\overline{K}(\mu_A \times 1_{(x+y)}) = \overline{K}(\mu_A \times 1_x) \oplus \overline{K}(\mu_A \times 1_y)$ and $\overline{K}(\mu_A \times 0_{(x+y)}) = \overline{K}(\mu_A \times 0_x) \oplus \overline{K}(\mu_A \times 0_y)$ for all $x, y \in L$.*

Proof. Indeed,

$$\begin{aligned}\overline{K}(\mu_A \times 1_{(x+y)})(\beta) &= \sup\{T(\mu_A(z), 1_{x+y}(u)) \,|\, Tr((adz \circ adu) = \beta\} \\ &= \sup\{\mu_A(z) \,|\, Tr(adz \circ ad(x+y)) = \beta\} \\ &= \sup\{\mu_A(z) \,|\, Tr(adz \circ adx) + Tr(adz \circ ady) = \beta\}\end{aligned}$$

$$= \sup\{T(\mu_A(z), T(1_x(v), 1_y(w))) \,|\, Tr(adz \circ adv) + Tr(adz \circ adw) = \beta\}$$
$$= \sup\{T(\sup\{T(\mu_A(z), 1_x(v)) \,|\, Tr(adz \circ adv) = \beta_1\},$$
$$\sup\{T(\mu_A(z), 1_y(w)) \,|\, Tr(adz \circ adw) = \beta_2\} \,|\, \beta_1 + \beta_2 = \beta)\}$$
$$= \sup\{T(\overline{K}(\mu_A \times 1_x)(\beta_1),\ \overline{K}(\mu_A \times 1_y)(\beta_2)) \,|\, \beta_1 + \beta_2 = \beta\}$$
$$= \overline{K}(\mu_A \times 1_x) \oplus \overline{K}(\mu_A \times 1_y)(\beta),$$

$$\overline{K}(\lambda_A \times 0_{(x+y)})(\beta) = \inf\{S(\lambda_A(z), 0_{x+y}(u)) \,|\, Tr((adz \circ adu) = \beta\}$$
$$= \inf\{\lambda_A(z) \,|\, Tr(adz \circ ad(x+y)) = \beta\}$$
$$= \inf\{\lambda_A(z) \,|\, Tr(adz \circ adx) + Tr(adz \circ ady) + \beta\}$$
$$= \inf\{S(\lambda_A(z), S(0_x(v), 0_y(w))) \,|\, Tr(adz \circ adv) + Tr(adz \circ adw) = \beta\}$$
$$= \inf\{S(\inf\{S(\lambda_A(z), 0_x(v)) \,|\, Tr(adz \circ adv) = \beta_1\},$$
$$\inf\{S(\lambda_A(z), 0_y(w) \,|\, Tr(adz \circ adw) = \beta_2\} \,|\, \beta_1 + \beta_2 = \beta)\}$$
$$= \inf\{S(\overline{K}(\lambda_A \times 0_x)(\beta_1),\ \overline{K}(\lambda_A \times 0_y)(\beta_2)) \,|\, \beta_1 + \beta_2 = \beta\}$$
$$= \overline{K}(\lambda_A \times 0_x) \oplus \overline{K}(\lambda_A \times 0_y)(\beta).$$

This completes the proof. □

As a consequence of the above two theorems we obtain

Corollary 5.4. *For each intuitionistic (S,T)-fuzzy Lie ideal $A = (\mu_A, \lambda_A)$ and all $x, y \in L$, $\alpha, \beta \in F$ we have*

$$\overline{K}(\mu_A \times 1_{(\alpha x + \beta y)}) = \alpha \odot \overline{K}(\mu_A \times 1_x) \oplus \beta \odot \overline{K}(\mu_A \times 1_y),$$
$$\overline{K}(\lambda_A \times 0_{(\alpha x + \beta y)}) = \alpha \odot \overline{K}(\lambda_A \times 0_x) \oplus \beta \odot \overline{K}(\lambda_A \times 0_y).$$

References

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

[2] **K. T. Atanassov:** *Intuitionistic fuzzy sets*, Fuzzy Sets and Systems **20** (1986), 87 – 96.

[3] **K. T. Atanassov:** *New operations defined over the intuitionistic fuzzy sets*, Fuzzy Sets and Systems **61** (1994), 137 – 142.

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

[5] **W. A. Dudek:** *Intuitionistic fuzzy approach to n-ary systems*, Quasigroups and Related Systems **13** (2005), 213 – 228.

[6] **J. E. Humphreys:** *Introduction to Lie Algebras and Representation Theory*, Springer, New York 1972.

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

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

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

[10] **B. Schweizer and A. Sklar:** *Statistical metric spaces*, Pacific J. Math. **10** (1960), 313 – 334.

[11] **B. Schweizer and A. Sklar:** *Associative functions and abstract semigroups*, Publ. Math. Debrecen **10** (1963), 69 – 81.

[12] **S. E. Yehia:** *Fuzzy ideals and fuzzy subalgebras of Lie algebras*, Fuzzy Sets and Systems **80** (1996), 237 – 244.

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

[14] **L. A. Zadeh:** *Fuzzy sets*, Information Control **8** (1965), 338 – 353.

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

Received March 30, 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 **15** (2007), 219 – 232

Fuzzy (strong) congruence relations on hypergroupoids and hyper BCK-algebras

Reza Ameri, Mahmoud Bakhshi, Seyyed A. Nematollah Zadeh and Rajabali Borzooei

Abstract

We define the concept of fuzzy (strong) congruence relations on hypergroupoids and hyper BCK-algebras and construct a quotient hyperstructure on a hypergroupoid. In particular, we prove that if H is a (semi) hypergroup and R is a fuzzy (strong) congruence relation on H, then H/R is a (semi) group. Finally, by considering the notion of a hyper BCK-algebra, we construct a quotient hyper BCK-algebra.

1. Introduction

The notion of a hyperstructure was introduced by F. Marty [13] in 1934 at the 8^{th} congress of Scandinavian Mathematicians and the notion of a fuzzy set was introduced by Zadeh [16] in 1965. The study of BCK-algebras was initiated by Y. Imai and K. Iséki [7] in 1966 as a generalization of the concept of the set-theoretic difference and propositional calculi. In this paper, we use the notion of a fuzzy set and define the concept of a fuzzy (strong) congruence relation on hypergroupoids and hyper BCK-algebras and we obtain some results as mentioned in the abstract.

2. Fuzzy (strong) congruence relations

Definition 1. By a *hypergroupoid* we mean a nonempty set H endowed with a binary hyperoperation "$\circ$" (i.e., a function $\circ : H \times H \longrightarrow P(H)$,

2000 Mathematics Subject Classification: 06F35, 03G25.
Keywords: Fuzzy (strong) congruence, hypergroup, hyper BCK-algebra.
This research partially is supported by the "Fuzzy Systems and it's Applications" Center of Excelence, Shahid Bahonar University of Kerman, Iran".

where $P(H)$ is the set of all nonempty subsets of H.)

Let Θ be a binary relation on a hypergroupoid H and $A, B \subseteq H$. Then:

(a) $A\Theta B$ means that there exist $a \in A$ and $b \in B$ such that $a\Theta b$,

(b) $A\overline{\Theta}B$ means that for $a \in A$ there exists $b \in B$ and for $b \in B$ there exists $a \in A$ such that $a\Theta b$,

(c) $A\overline{\overline{\Theta}}B$ means that $a\Theta b$ for each $a \in A$ and for $b \in B$,

(d) Θ is *left* (*resp. right*) *compatible* if $x\Theta y$ implies $a \circ x\overline{\Theta}a \circ y$ (resp. $x \circ a\overline{\Theta}y \circ a$) for all $x, y, a \in H$,

(e) Θ is *strong left* (resp. *right*) *compatible* if $x\Theta y$ implies $a \circ x\overline{\overline{\Theta}}a \circ y$ (resp. $x \circ a\overline{\overline{\Theta}}y \circ a$),

(f) Θ is (resp. *strong*) *compatible* if it is both (resp. strong) left and right compatible,

(g) Θ is a (resp. *strong*) *congruence* relation on H if it is a (resp. strong) compatible equivalence relation on H.

Definition 2. Let H be a nonempty set and R be a fuzzy relation on H. We say that R satisfies the *sup property* if for every subset T of H there exists $(u, v) \in T^2$ such that $\sup\limits_{(x,y)\in T^2} R(x, y) = R(u, v)$. R is said to be a *fuzzy equivalence relation* if

$$R(x, x) = \bigvee_{(y,z)\in H^2} R(y, z), \text{ (\textit{fuzzy reflexive})}$$

$$R(y, x) = R(x, y), \text{ (\textit{fuzzy symmetric})}$$

$$R(x, y) \geqslant \bigvee_{z\in H} (R(x, z) \wedge R(z, y)), \text{ (\textit{fuzzy transitive}).}$$

Definition 3. Let H be a nonempty set and R be a fuzzy relation on H. Then, for all $\alpha \in [0, 1]$, the *α-level subset* and *strong α-level subset* of R respectively, is defined as follows:

$$R^{\alpha} = \{(x, y) \in H^2 : R(x, y) \geqslant \alpha\}$$
$$R^{\alpha^{>}} = \{(x, y) \in H^2 : R(x, y) > \alpha\}$$

Lemma 1. *Let R be a fuzzy relation on a nonempty set H. Then:*

$$R^{\alpha} = \bigcap_{\beta\in[0,\alpha)} R^{\beta^{>}} \quad \textit{and} \quad R^{\alpha^{>}} = \bigcup_{\beta\in(\alpha,1]} R^{\beta}$$

for all $\alpha \in [0, 1]$.

Proof. Let $\alpha \in [0,1]$ and $\beta < \alpha$. Then $R^\alpha \subseteq R^\beta$ and so $R^\alpha \subseteq \bigcap_{\beta\in[0,\alpha)} R^\beta$. Conversely, let $\varepsilon > 0$ be given and $(x,y) \in \bigcap_{\beta\in[0,\alpha)} R^\beta$. Then $R(x,y) \geqslant \alpha - \varepsilon$, which implies that $R(x,y) \geqslant \alpha$ and hence $(x,y) \in R^\alpha$. Similarly, the other part can be proved. □

Theorem 1. (cf. [3]) *Let R be a fuzzy relation on nonempty set H. Then the following properties are equivalent:*

(*i*) *R is a fuzzy equivalence relation on H,*

(*ii*) *$R^\alpha \neq \emptyset$ is an equivalence relation on H for all $\alpha \in [0,1]$,*

(*iii*) *$R^{\alpha^>} \neq \emptyset$ is an equivalence relation on H for all $\alpha \in [0,1]$.* □

Definition 4. Fuzzy relation R on hypergroupoid H is said to be

(*i*) *fuzzy left compatible* iff

$$\Big(\bigwedge_{u\in c\circ a}\bigvee_{v\in c\circ b} R(u,v)\Big) \wedge \Big(\bigwedge_{v\in c\circ b}\bigvee_{u\in c\circ a} R(u,v)\Big) \geqslant R(a,b) \quad \forall a,b,c \in H,$$

and *fuzzy right compatible* iff

$$\Big(\bigwedge_{u\in a\circ c}\bigvee_{v\in b\circ c} R(u,v)\Big) \wedge \Big(\bigwedge_{v\in b\circ c}\bigvee_{u\in a\circ c} R(u,v)\Big) \geqslant R(a,b) \quad \forall a,b,c \in H,$$

(*ii*) *fuzzy strong left compatible* iff

$$\bigwedge_{u\in c\circ a, v\in c\circ b} R(u,v) \geqslant R(a,b) \quad \forall a,b,c \in H.$$

and *fuzzy strong right compatible* iff

$$\bigwedge_{u\in a\circ c, v\in b\circ c} R(u,v) \geqslant R(a,b), \ \forall a,b,c \in H$$

Clearly, every fuzzy strong left (resp. right) compatible relation is a fuzzy left (resp. right) compatible relation, but the converse is not true.

Theorem 2. *Let R be a fuzzy relation on a hypergroupoid H that satisfies the sup property. Then the following statements are equivalent:*

(*i*) *R is fuzzy left (resp. right) compatible,*

(*ii*) $R^{\alpha} \neq \emptyset$ *is left (resp. right) compatible, for all* $\alpha \in [0,1]$,

(*iii*) $R^{\alpha^>} \neq \emptyset$ *is left (resp. right) compatible, for all* $\alpha \in [0,1]$.

Proof. We prove only for "left" compatible, the other cases can be proved in a similar way.

$(i) \Longrightarrow (ii)$ Let $R^{\alpha} \neq \emptyset$. For $\alpha \in [0,1]$ and $x, y, a \in H$ let $xR^{\alpha}y$ and $u \in x \circ a$. Since by (i), R is fuzzy left compatible, then

$$\Big(\bigwedge_{u \in a \circ x} \bigvee_{v \in a \circ y} R(u,v) \Big) \wedge \Big(\bigwedge_{v \in a \circ y} \bigvee_{u \in a \circ x} R(u,v) \Big) \geqslant R(x,y) \geqslant \alpha$$

and so

$$\bigwedge_{u \in a \circ x} \bigvee_{v \in a \circ y} R(u,v) \geqslant \alpha \quad \text{and} \quad \bigwedge_{v \in a \circ y} \bigvee_{u \in a \circ x} R(u,v) \geqslant \alpha.$$

Hence, for all $u \in a \circ x$, $\bigvee_{v \in a \circ y} R(u,v) \geqslant \alpha$ and for all $v \in a \circ y$, $\bigvee_{u \in a \circ x} R(u,v) \geqslant \alpha$. Since, R satisfies the sup property, then there exist $v_0 \in a \circ y$ and $u_0 \in a \circ x$ such that $R(u, v_0) = \bigvee_{v \in a \circ y} R(u,v) \geqslant \alpha$ for all $u \in a \circ x$ and $R(u_0, v) = \bigvee_{u \in a \circ x} R(u,v) \geqslant \alpha$ for all $v \in a \circ y$. Hence, $(u, v_0) \in R^{\alpha}$ and $(u_0, v) \in R^{\alpha}$, for all $u \in a \circ x$ and $v \in a \circ y$. This implies that R^{α} is left compatible.

$(ii) \Longrightarrow (iii)$ Let $R^{\alpha^>} \neq \emptyset$, for $\alpha \in [0,1]$ and $x, y, a \in H$ be such that $xR^{\alpha^>}y$ and $u \in a \circ x$. Thus by Lemma 1, there exists $\beta \in (\alpha, 1]$ such that $xR^{\beta}y$. Since R^{β} is left compatible, then $a \circ x \bar{R}^{\beta} a \circ y$, and so there exists $v \in a \circ y$ such that $uR^{\beta}v$. Thus, $R(u,v) \geqslant \beta > \alpha$. This shows that $uR^{\alpha^>}v$. Similarly, if $v \in a \circ y$, then there exists $u \in a \circ x$ such that $R(u,v) > \alpha$ and so $uR^{\alpha^>}v$. Therefore, $R^{\alpha^>}$ is left compatible.

$(iii) \Longrightarrow (i)$ Suppose that $x, y, a \in H$ are such that $R(x,y) = \alpha$. Then by Lemma 1, for all $\beta \in [0, \alpha)$ we have $xR^{\beta^>}y$. So, by (iii) we have $a \circ x \bar{R}^{\beta^>} a \circ y$, and so for all $u \in a \circ x$ there exists $v \in a \circ y$ such that $uR^{\beta^>}v$ i.e., $R(u,v) > \beta$. This implies that $\bigwedge_{u \in a \circ x} \bigvee_{v \in a \circ y} R(u,v) > \beta$, for all $\beta \in [0, \alpha)$. Similarly, for all $v \in a \circ y$ there exists $u \in a \circ x$ such that $uR^{\beta^>}v$ and so $\bigwedge_{v \in a \circ y} \bigvee_{u \in a \circ x} R(u,v) > \beta$, for all $\beta \in [0, \alpha)$. Hence, $\bigwedge_{u \in a \circ x} \bigvee_{v \in a \circ y} R(u,v) \geqslant \alpha =$

$R(x,y)$ and $\bigwedge\limits_{v\in a\circ y}\bigvee\limits_{u\in a\circ x} R(u,v) \geqslant \alpha = R(x,y)$, which implies

$$\Big(\bigwedge_{u\in a\circ x}\bigvee_{v\in a\circ y} R(u,v)\Big)\wedge\Big(\bigwedge_{v\in a\circ y}\bigvee_{u\in a\circ x} R(u,v)\Big)\geqslant R(x,y).$$

Thus, R is fuzzy left compatible. □

Theorem 3. *For a fuzzy relation R on a hypergroupoid H satisfying the sup property the following properties are equivalent:*

(*i*) *R is fuzzy strong left (resp. right) compatible,*

(*ii*) *$R^\alpha \neq \emptyset$ is strong left (resp. right) compatible, for all $\alpha \in [0,1]$,*

(*iii*) *$R^{\alpha^>} \neq \emptyset$ is strong left (resp. right) compatible, for all $\alpha \in [0,1]$.*

Proof. (*i*) $\Longrightarrow$ (*ii*) Let R be a fuzzy strong left compatible relation on H, $a \in H$ and $x, y \in H$ be such that $xR^\alpha y$, for some $\alpha \in [0,1]$. Then for all $u \in a\circ x$ and $v \in a\circ y$,

$$R(u,v) \geqslant \bigwedge_{w\in a\circ x,\, w'\in a\circ y} R(w,w') \geqslant R(x,y) \geqslant \alpha$$

that is $uR^\alpha v$. This shows that R^α is a strong left compatible relation on H.

(*ii*) $\Longrightarrow$ (*iii*) Let $R^\alpha \neq \emptyset$ be a strong left compatible relation on H, for $\alpha \in L$, $x, y \in H$ be such that $xR^{\alpha^>}y$ and $a \in H$. Then, there exists $\beta \in (\alpha, 1]$ such that $xR^\beta y$ and so by (*ii*), $a\circ x \overset{=}{R}{}^\beta a\circ y$. This implies that for all $u \in a\circ x$ and for all $v \in a\circ y$, $R(u,v) \geqslant \beta > \alpha$ and so $uR^{\alpha^>}v$. Hence, $a\circ x \overset{=}{R}{}^{\alpha^>} a\circ y$, which implies that $R^{\alpha^>}$ is a strong left compatible relation on H.

(*iii*) $\Longrightarrow$ (*i*) Let $a \in H$ and $x, y \in H$ be such that $R(x,y) = \alpha$, for $\alpha \in [0,1]$. Then, by Lemma 1, for all $\beta \in [0,\alpha)$ we have $xR^{\beta^>}y$ and so by (*iii*), $a\circ x \overset{=}{R}{}^{\beta^>} a\circ y$; i.e., for all $u \in a\circ x$ and for all $v \in a\circ y$, $uR^{\beta^>}v$ i.e., $R(u,v) > \beta$, for all $\beta \in [0,\alpha)$. Thus $R(u,v) \geqslant \alpha$, and hence

$$\bigwedge_{u\in a\circ x, v\in a\circ y} R(u,v) \geqslant \alpha = R(x,y).$$

Therefore, R is a fuzzy strong left compatible relation on H. □

Definition 5. Let R be a fuzzy relation on a hypergroupoid H. Then, R is said to be

(i) *fuzzy compatible* if

$$\Big(\bigwedge_{u\in a\circ c}\bigvee_{v\in b\circ d} R(u,v)\Big)\wedge\Big(\bigwedge_{v\in b\circ d}\bigvee_{u\in a\circ c} R(u,v)\Big) \geqslant R(a,b)\wedge R(c,d),\ \ \forall a,b,c,d\in H,$$

(ii) *fuzzy strong compatible* if

$$\bigwedge_{u\in a\circ c, v\in b\circ d} R(u,v) \geqslant R(a,b)\wedge R(c,d),\quad \forall a,b,c,d\in H.$$

Definition 6. By a *fuzzy* (resp. *strong*) *congruence relation* we mean a fuzzy (resp. strong) compatible equivalence relation.

Theorem 4. *A fuzzy relation R is a (resp. strong) fuzzy congruence relation if and only if it is both a (resp. strong) left and right fuzzy compatible equivalence relation.*

Proof. Let R be a fuzzy congruence relation on H and $a,x,y\in H$. Then

$$\Big(\bigwedge_{u\in a\circ x}\bigvee_{v\in a\circ y} R(u,v)\Big)\wedge\Big(\bigwedge_{v\in a\circ y}\bigvee_{u\in a\circ x} R(u,v)\Big) \geqslant R(x,y)\wedge R(a,a)=R(x,y)$$

which shows that R is a fuzzy left compatible relation on H. Similarly, it can be shown that R is a fuzzy right compatible relation on H.

Conversely, suppose that R is both a fuzzy left and right compatible equivalence relation on H and $a,b,c,d\in H$. Now, for every $u\in a\circ c$ and every $v\in b\circ d$, by transitivity of R, we have

$$R(u,v)\geqslant\bigvee_{y\in H}(R(u,y)\wedge R(y,v))\geqslant R(u,w)\wedge R(w,v),\quad \forall w\in b\circ c$$

and so

$$R(u,v)\geqslant\Big(\bigvee_{w\in b\circ c} R(u,w)\Big)\wedge\Big(\bigvee_{w\in b\circ c} R(w,v)\Big).$$

Thus

$$\bigvee_{v\in b\circ d} R(u,v)\geqslant\bigwedge_{v\in b\circ d} R(u,v)\geqslant\Big(\bigvee_{w\in b\circ c} R(u,w)\Big)\wedge\Big(\bigwedge_{v\in b\circ d}\bigvee_{w\in b\circ c} R(w,v)\Big)$$

and hence

$$\begin{aligned}\bigwedge_{u\in a\circ c}\bigvee_{v\in b\circ d} R(u,v) &\geqslant \Big(\bigwedge_{u\in a\circ c}\bigvee_{w\in b\circ c} R(u,w)\Big)\wedge\Big(\bigwedge_{v\in b\circ d}\bigvee_{w\in b\circ c} R(w,v)\Big)\\ &\geqslant R(a,b)\wedge R(c,d).\end{aligned}$$

Therefore, R is a fuzzy congruence relation on H.

Now, let R be a fuzzy strong congruence relation on H and $x, y, a \in H$. Then,

$$\bigwedge_{u\in a\circ x,\ v\in a\circ y} R(u,v) \geqslant R(a,a)\wedge R(x,y) = R(x,y).$$

Hence, R is fuzzy strong left compatible. The proof for "fuzzy strong right" is similar.

Conversely, let R be a fuzzy strong left and right compatible, $a, b, c, d \in H$. Then,

$$R(a,b) \leqslant \bigwedge_{u\in a\circ c,\ v\in b\circ c} R(u,v) \quad \text{and} \quad R(c,d) \leqslant \bigwedge_{u\in b\circ c,\ v\in b\circ d} R(u,v)$$

and so

$$R(a,b)\wedge R(c,d) \leqslant \Big(\bigwedge_{u\in a\circ c,\ v\in b\circ c} R(u,v)\Big)\wedge\Big(\bigwedge_{u\in b\circ c,\ v\in b\circ d} R(u,v)\Big).$$

For every $u \in a\circ c$ and $v \in b\circ d$, by transitivity of R, we have

$$\begin{aligned}R(u,v) &\geqslant \bigvee_{y\in H}(R(u,y)\wedge R(y,v)) \geqslant R(u,w)\wedge R(w,v), \quad \forall w \in b\circ c\\ &\geqslant \Big(\bigwedge_{u\in a\circ c,\, v\in b\circ c} R(u,v)\Big)\wedge\Big(\bigwedge_{w\in b\circ c,\, z\in b\circ d} R(u,v)\Big) \geqslant R(a,b)\wedge R(c,d).\end{aligned}$$

Thus R is a fuzzy strong congruence relation on H. □

By Theorems 1, 2, 3 and 4 we have the following corollary.

Corollary 1. *Let R be a fuzzy relation on a hypergroupoid H that satisfies the sup property. Then,*

(*i*) *R is a fuzzy congruence relation on H if and only if every nonempty α-level set R^α of R is both left and right compatible equivalence relation,*

(*ii*) *R is a fuzzy strong congruence relation on H if and only if every nonempty α-level set R^α of R is both strong left and right compatible equivalence relation on H.* □

Let R be a fuzzy relation on H. For all $x \in H$, define a fuzzy subset μ on H by $\mu_x(y) = R(y, x)$, for all $y \in H$.

Lemma 2. *Let R be a fuzzy equivalence relation on a hypergroupoid H. Then, $\mu_x = \mu_y$ if and only if $R(x, y) = \bigvee_{u,v \in H} R(u, v)$.*

Proof. (i) Let $\mu_x = \mu_y$, for $x, y \in H$. Since, R is fuzzy reflexive, then

$$R(x, y) = \mu_y(x) = \mu_x(x) = R(x, x) = \bigvee_{u,v \in H} R(u, v).$$

Conversely, suppose that $R(x, y) = \bigvee_{u,v \in H} R(u, v)$, for $x, y \in H$ and $w \in H$. Since R is fuzzy symmetric and fuzzy transitive, we obtain

$$\begin{aligned} \mu_x(w) &= R(w, x) = R(x, w) \geqslant R(x, y) \wedge R(y, w) \\ &= \left(\textstyle\bigvee_{u,v \in H} R(u, v) \right) \wedge R(y, w) = R(y, w) = \mu_y(w). \end{aligned}$$

Similarly, we can show that $\mu_y(w) \geqslant \mu_x(w)$. Thus, $\mu_x(w) = \mu_y(w)$ and so $\mu_x = \mu_y$. □

Theorem 5. *Let R be a fuzzy congruence relation on H with the sup property and $H/R = \{\mu_x : x \in H\}$. Then $(H/R, \diamond)$ is a hypergroupoid, where binary hyperoperation "$\diamond$" is defined by*

$$\mu_x \diamond \mu_y = \{\mu_z : z \in x \circ y\} = \mu_{x \circ y}.$$

Proof. First, we show that "$\diamond$" is well-defined. Let $\mu_x = \mu_{x'}$ and $\mu_y = \mu_{y'}$, for $\mu_x, \mu_{x'}, \mu_y, \mu_{y'} \in H/R$. Then, by Lemma 2, $R(x, x') = \bigvee_{u,v \in H} R(u, v) = R(y, y')$. Let $\alpha = \bigvee_{u,v \in H} R(u, v)$. Then $xR^\alpha x'$ and $yR^\alpha y'$ and by Corollary 1, R^α is a congruence relation on H, then $x \circ y \bar{R}^\alpha x' \circ y'$. Now, let $\mu_z \in \mu_x \diamond \mu_y = \mu_{x \circ y}$. Then there exists $z' \in x \circ y$ such that $\mu_z = \mu_{z'}$. On the other hand, since $x \circ y \bar{R}^\alpha x' \circ y'$, then there exists $u \in x' \circ y'$ such that $z' R^\alpha u$ and so $R(z', u) \geqslant \alpha = \bigvee_{u,v \in H} R(u, v) \geqslant R(z', u)$. Hence, $R(z', u) = \alpha$. Now, for $w \in H$ we have

$$\begin{aligned} \mu_z(w) = \mu_{z'}(w) = R(w, z') = R(z', w) &\geqslant R(z', u) \wedge R(u, w) = \alpha \wedge R(u, w) \\ = R(u, w) = R(w, u) &= \mu_u(w) \end{aligned}$$

and so $\mu_z \geqslant \mu_u$. Similarly $\mu_u \geqslant \mu_z$. Hence, $\mu_z = \mu_u$ and so $\mu_z = \mu_u \in \mu_{x' \circ y'} = \mu_{x'} \diamond \mu_{y'}$, since $u \in x' \circ y'$. Thus $\mu_x \diamond \mu_y \subseteq \mu_{x'} \diamond \mu_{y'}$. Analogously, $\mu_{x'} \diamond \mu_{y'} \subseteq \mu_x \diamond \mu_y$. Thus $\mu_x \diamond \mu_y = \mu_{x'} \diamond \mu_{y'}$. This completes the proof. □

In the following, we briefly give some preliminaries about hypergroups.

Definition 7. (cf. [5]) Let $(H, \circ)$ be a hypergroupoid. Then H is called a *semihypergroup* if "$\circ$" is associative i.e., $(x \circ y) \circ z = x \circ (y \circ z)$, for all $x, y, z \in H$. Moreover, if H is a semihypegroup that satisfies the *reproduction axioms* that is, $x \circ H = H \circ x = H$, for all $x \in H$, then we say that H is a *hypergroup*. Now, let H be a hypergroup. An, element $e \in H$ is called an *identity* if for all $x \in H$, $x \in (x \circ e) \cap (e \circ x)$, an element $a \in H$ is said to be a *scalar identity* if for all $x \in H$, $|a \circ x| = |x \circ a| = 1$. Let H has an identity e, an element $a' \in H$ is said to be an *inverse* of $a \in H$ if $e \in (a \circ a') \cap (a' \circ a)$. H is called *regular* if it has at least one identity and each element has at least one inverse. H is said to be *reversible* if for all $x, y, z \in H$, $y \in a \circ x$ implies that there exists an inverse a' of a such that $x \in a' \circ y$ and $y \in x \circ a$ implies that there exists an inverse a" of a such that $x \in y \circ a$", a hypergroup $(H, \circ)$ is called *canonical* if it is commutative, with a scalar identity, such that every element has an unique inverse and it is reversible.

Theorem 6. *If $(H, \circ)$ is a semihypergroup and R is a fuzzy congruence relation on H, then H/R is a semihypergroup. In particular, if $(H, \circ)$ is a hypergroup then H/R is a hypergroup.*

Proof. Let $\mu_x, \mu_y, \mu_z \in H/R$ and $\mu_u \in (\mu_x \diamond \mu_y) \diamond \mu_z$. Then there exists $\mu_w \in \mu_x \diamond \mu_y$ such that $\mu_u \in \mu_w \diamond \mu_z = \mu_{w \circ z}$ and so there exists $v \in w \circ z$ such that $\mu_u = \mu_v$. But, $v \in w \circ z \subseteq (x \circ y) \circ z = x \circ (y \circ z)$ and so there exists $u' \in y \circ z$ such that $v \in x \circ u'$. Hence, $\mu_u = \mu_v \in \mu_{x \circ u'} = \mu_x \diamond \mu_{u'} \subseteq \mu_x \diamond (\mu_y \diamond \mu_z)$, which shows that $(\mu_x \diamond \mu_y) \diamond \mu_z \subseteq \mu_x \diamond (\mu_y \diamond \mu_z)$. By a similar way, we can show that $\mu_x \diamond (\mu_y \diamond \mu_z) \subseteq (\mu_x \diamond \mu_y) \diamond \mu_z$. Hence, $(\mu_x \diamond \mu_y) \diamond \mu_z = \mu_x \diamond (\mu_y \diamond \mu_z)$, which shows that "$\diamond$" is associative. Therefore, H/R is a semihypergroup.

Now, suppose that $(H, \circ)$ is a hypergroup and $\mu_x \in H/R$. Obviously $\mu_x \diamond H/R \subseteq H/R$. Now, let $\mu_u \in H/R$. Since, $u \in H = x \circ H$, then there exists $y \in H$ such that $u \in x \circ y$ and so $\mu_u \in \mu_{x \circ y} = \mu_x \diamond \mu_y \subseteq \mu_x \diamond H/R$. Hence, $H/R \subseteq \mu_x \diamond H/R$ and so $\mu_x \diamond H/R = H/R$. Similarly, $H/R \diamond \mu_x = H/R$ and hence H/R satisfies the reproduction axioms. Therefore, H/R is a hypergroup. □

Theorem 7. *Let $(H, \circ)$ be a semihypergroup and R be a fuzzy strong congruence relation on H. Then:*

(*i*) *H/R is a semigroup,*

(*ii*) *if H is a hypergroup, then H/R is a group.*

Proof. (*i*) By Theorem 6, H/R is a semihypergroup. It is enough to show that $|\mu_x \diamond \mu_y| = 1$, for all $\mu_x, \mu_y \in H/R$. Let $\mu_x, \mu_y \in H/R$. Since, R is a fuzzy strong congruence relation, then

$$\bigwedge_{a\in x\circ y,\ b\in x\circ y} R(a,b) \geqslant R(x,x) \wedge R(y,y) = \bigvee_{u,v\in H} R(u,v).$$

Thus for all $a, b \in x\circ y$, $R(a,b) \geqslant \bigvee_{u,v\in H} R(u,v)$ and so $R(a,b) = \bigvee_{u,v\in H} R(u,v)$. Hence, by Lemma 1, $\mu_a = \mu_b$, for all $a, b \in x \circ y$, which implies that $|\mu_x \diamond \mu_y| = 1$.

(*ii*) Similar to the proof of (i), it is enough to show that for all $\mu_x, \mu_y \in H/R$, $|\mu_x \diamond \mu_y| = 1$. But, this immediately follows from (*i*). □

Theorem 8. *If $(H, \circ)$ is a canonical hypergroup, then H/R is a canonical hypergroup.*

Proof. Let H be a canonical hypergroup and $\mu_x, \mu_y \in H/R$. Then,

$$\mu_x \diamond \mu_y = \{\mu_z : z \in x \circ y\} = \{\mu_z : z \in y \circ x\} = \mu_y \diamond \mu_x$$

which shows that H/R is commutative. Since, H has a scalar identity, then there exists $e \in H$, such that $e \circ x = x \circ e = \{x\}$. Hence, for all $\mu_x \in H/R$,

$$\mu_x \diamond \mu_e = \mu_{x\circ e} = \mu_x = \mu_{e\circ x} = \mu_e \diamond \mu_x.$$

This shows that μ_e is a scalar identity. Let $\mu_x \in H/R$ and x' be the unique inverse of x. Since, $e \in (x\circ x')\cap(x'\circ x)$, then $\mu_e \in (\mu_x\diamond\mu_{x'})\cap(\mu_{x'}\diamond\mu_x)$, which shows that $\mu_{x'}$ is an inverse of μ_x. Now, let μ_y be another inverse of μ_x. Then $\mu_e \in (\mu_x\diamond\mu_y)\cap(\mu_y\diamond\mu_x)$ and so there exists $b \in y\circ x$ such that $\mu_e = \mu_b$. Hence, by Lemma 1, $R(e,b) = \bigvee_{u,v\in H} R(u,v)$. Let $\alpha = \bigvee_{u,v\in H} R(u,v)$. Then, $eR^\alpha b$ i.e., $\{e\}R^\alpha y \circ x$. Since, R^α is compatible, then $e \circ x'\bar{R}^\alpha(y \circ x) \circ x'$ and so $x'\bar{R}^\alpha y \circ (x \circ x')$. Since, $y \in y \circ e \subseteq y \circ (x \circ x')$, then $x'R^\alpha y$ and so $R(x', y) \geqslant \alpha = \bigvee_{u,v\in H} R(u,v)$. Hence, $R(x', y) = \bigvee_{u,v\in H} R(u,v)$ and so by Lemma 1, $\mu_y = \mu_{x'}$, says that the inverse of μ_x is unique. Now, we show that H/R is reversible. For this, let $\mu_x, \mu_y, \mu_a \in H/R$ and $\mu_y \in \mu_a \diamond \mu_x = \mu_{a\circ x}$.

Then, there exists $u \in a \circ x$ such that $\mu_y = \mu_u$. Since, $u \in a \circ x$, then there exists an inverse a' of a such that $x \in a' \circ y$ and so $\mu_x \in \mu_{a'} \diamond \mu_y$, and $\mu_{a'}$ is an inverse of μ_a. Similarly, if $\mu_y \in \mu_x \diamond \mu_a$, then there exists an inverse a" of a such that $\mu_x \in \mu_y \diamond \mu_a$". Hence, H/R is reversible. Therefore, H/R is a canonical hypergroup. □

3. Fuzzy congruence relations on hyper BCK-algebras

Definition 8. (cf. [10, 11]) By a *hyper BCK-algebra* we mean a hypergroupoid $(H, \circ)$ equipped a constant element "0" that satisfies the following axioms:

(HK1) $(x \circ z) \circ (y \circ z) \ll x \circ y$,
(HK2) $(x \circ y) \circ z = (x \circ z) \circ y$,
(HK3) $x \circ H \ll \{x\}$,
(HK4) $x \ll y$ and $y \ll x$ imply $x = y$,

for all $x, y, z \in H$, where by $x \ll y$ we mean $0 \in x \circ y$ and for every $A, B \subseteq H$, $A \ll B$ is defined by $\forall a \in A$, $\exists b \in B$ such that $a \ll b$.

Definition 9. Let R be a fuzzy relation on a hyper BCK-algebra H. Then, R is said to be *fuzzy regular* if

$$R(x, y) \geqslant \Big(\bigvee_{a \in x \circ y} R(a, 0) \Big) \wedge \Big(\bigvee_{b \in y \circ x} R(b, 0) \Big).$$

Lemma 3. *Let R be a fuzzy relation on a hyper BCK-algebra H with the sup property. Then, R is fuzzy regular if and only if for all $\alpha \in [0, 1]$, each nonempty α-level subset R^α is regular.*

Proof. Let R be a fuzzy regular relation on H. Then $x \circ yR^\alpha\{0\}$ and $y \circ xR^\alpha\{0\}$, for $x, y \in H$ and $\alpha \in [0, 1]$. Then, there exist $a \in x \circ y$ and $b \in y \circ x$ such that $aR^\alpha 0$ and $bR^\alpha 0$. This implies that $R(a, 0), R(b, 0) > \alpha$ and so $\bigvee_{a \in x \circ y} R(a, 0) > \alpha$ and $\bigvee_{b \in y \circ x} R(b, 0) > \alpha$. Thus,

$$R(x, y) \geqslant \Big(\bigvee_{a \in x \circ y} R(a, 0) \Big) \wedge \Big(\bigvee_{b \in y \circ x} R(b, 0) \Big) > \alpha$$

and so $xR^\alpha y$, which shows that R^α is regular.

Conversely, suppose that

$$\Big(\bigvee_{a \in x \circ y} R(a, 0) \Big) \wedge \Big(\bigvee_{b \in y \circ x} R(b, 0) \Big) = \alpha$$

for $x, y \in H$. Then $\bigvee_{a \in x \circ y} R(a,0) \geqslant \alpha$ and $\bigvee_{b \in y \circ x} R(b,0) \geqslant \alpha$ and since R has the sup property, then there exist $a_0 \in x \circ y$ and $b_0 \in y \circ x$ such that $R(a_0,0) = \bigvee_{a \in x \circ y} R(a,0) \geqslant \alpha$ and similarly $R(b_0,0) = \bigvee_{b \in y \circ x} R(b,0) \geqslant \alpha$. Hence, $a_0 R^\alpha 0$ and $b_0 R^\alpha 0$ and so $x \circ y R^\alpha \{0\}$ and $y \circ x R^\alpha \{0\}$. Since R^α is regular, then $x R^\alpha y$ and so

$$R(x,y) \geqslant \alpha = \Big(\bigvee_{a \in x \circ y} R(a,0) \Big) \wedge \Big(\bigvee_{b \in y \circ x} R(b,0) \Big)$$

Therefore, R is a fuzzy regular relation. □

Theorem 9. *Let $(H, \circ)$ be a hyper BCK-algebra and R be a fuzzy regular congruence relation on H. Then, H/R is a hyper BCK-algeba.*

Proof. It is enough to establish the axioms of a hyper BCK-algebra.

(HK1) Let $\mu_x, \mu_y, \mu_z, \mu_v \in H/R$ be such that $\mu_v \in (\mu_x \diamond \mu_z) \diamond (\mu_y \diamond \mu_z)$. Then there exist $\mu_u \in \mu_x \diamond \mu_z$ and $\mu_w \in \mu_y \diamond \mu_z$ such that $\mu_v \in \mu_u \diamond \mu_w$ and so there exists $a \in u \circ w$ such that $\mu_v = \mu_a$. Since $a \in u \circ w \subseteq (x \circ z) \circ (y \circ z) \ll x \circ y$, then there exists $b \in x \circ y$ such that $a \ll b$ and so $0 \in a \circ b$. This implies that $\mu_0 \in \mu_a \diamond \mu_b = \mu_v \diamond \mu_b \subseteq (\mu_u \diamond \mu_w) \diamond (\mu_x \diamond \mu_y) \subseteq ((\mu_x \circ \mu_z) \diamond (\mu_y \diamond \mu_z)) \diamond (\mu_x \diamond \mu_y)$. Thus $(\mu_x \diamond \mu_z) \diamond (\mu_y \diamond \mu_z) \ll \mu_x \diamond \mu_y$.

(HK2) Let $\mu_u \in (\mu_x \diamond \mu_y) \diamond \mu_z$. Then there exists $v \in (x \circ y) \circ z$ such that $\mu_u = \mu_v$. Since by (HK2) of H, $(x \circ y) \circ z = (x \circ z) \circ y$, then $v \in (x \circ z) \circ y$ and so $\mu_u = \mu_v \in (\mu_x \diamond \mu_z) \diamond \mu_y$. This implies that $(\mu_x \diamond \mu_y) \diamond \mu_z \subseteq (\mu_x \diamond \mu_z) \diamond \mu_y$. Similarly, we can show that $(\mu_x \diamond \mu_z) \diamond \mu_y \subseteq (\mu_x \diamond \mu_y) \diamond \mu_z$. Thus $(\mu_x \circ \mu_y) \diamond \mu_z = (\mu_x \diamond \mu_z) \diamond \mu_y$.

(HK3) Let $\mu_z \in \mu_x \diamond H/R$, for $\mu_x \in H/R$. Then there exists $\mu_y \in H/R$ such that $\mu_z \in \mu_x \diamond \mu_y$ and so there exists $w \in x \circ y$ such that $\mu_z = \mu_w$. Since by (HK3) of H, $x \circ y \ll x$, then $w \ll x$ and so $0 \in w \circ x$. Thus $\mu_0 \in \mu_w \diamond \mu_x = \mu_z \diamond \mu_x$. This implies that $\mu_z \ll \mu_x$ and so $\mu_x \diamond H/R \ll \mu_x$.

(HK4) Let $\mu_x \ll \mu_y$ and $\mu_y \ll \mu_x$, for $\mu_x, \mu_y \in H/R$. Then $\mu_0 \in \mu_x \diamond \mu_y$ and $\mu \in \mu_x \diamond \mu_y$. Hence there exist $z \in x \circ y$ and $w \in y \circ x$ such that $\mu_z = \mu_0 = \mu_w$. Since, $\mu_z = \mu$, then by Lemma 1, $R(z,w) = \bigvee_{u,v \in H} R(u,v)$. Since $\mu_z = \mu$ (and also $\mu_w = \mu$), then $R(z,0) = \bigvee_{u,v \in H} R(u,v) = R(w,0)$. Let $\alpha = \bigvee_{u,v \in H} R(u,v)$. Then $z R^\alpha 0$ and $w R^\alpha 0$, means that $x \circ y R^\alpha \{0\}$ and

$y \circ xR^{\alpha}\{0\}$ and since R^{α} is regular, then $xR^{\alpha}y$. Hence, $R(x,y) \geqslant \alpha = \bigvee_{u,v \in H} R(u,v)$ and so $R(x,y) = \bigvee_{u,v \in H} R(u,v)$, which implies that $\mu_x = \mu_y$, by Lemma 1. Therefore, H/R is a hyper BCK-algebra. □

References

[1] **R. Ameri**: *Fuzzy binary relations on (semi)hypergroups*, J. Basic Science **2** (2003), 11 – 16.

[2] **R. Ameri and M. M. Zahedi**: *Hypergoup and join spaces induced by a fuzzy subset*, Pure Math. Appl. **8** (1997), 155 – 168.

[3] **R. A. Borzooei, M. Bakhshi and Y. B. Jun**: *Fuzzy congruence relations on hyper BCK-algebras*, J. Fuzzy Math. **13** (2005), 627 – 636.

[4] **R.A. Borzooei and H. Harizavi**: *Regular congruence relations on hyper BCK-algebras*, Sci. Math. Jpn. **61** (2005), 83 – 97.

[5] **P. Corsini**: *Prolegomena of Hypergroup Theory*, Aviani Editore, 1993.

[6] **H. Hedayati and R. Ameri**: *Some equivalent conditions on fuzzy hypergroups*, 32nd Iranian Math. Confer. 2002, Babolsar, Iran (to appear).

[7] **Y. Imai and K. Iséki**: *On axiom systems of propositional calculi XIV*, Proc. Japan Academy **42** (1966), 19 – 22.

[8] **S. Ioudilis**: *Polygroups et certaines de leurs properetes*, Bull. Greek Math. Soc. **22** (1981), 95 – 104.

[9] **J. Jantosciak**: *Transposition hypergroups: Noncommutative join spaces*, J. Algebra **187** (1997), 97 – 119.

[10] **Y. B. Jun and X. L. Xin**: *Scalar elements and hyperatoms of hyper BCK-algebras*, Sci. Math. **2** (1999), 303 – 309.

[11] **Y. B. Jun, M. M. Zahedi, X. L. Xin and R. A. Borzooei**: *On Hyper BCK-algebras*, Ital. J. Pure Appl. Math. **10** (2000), 127 – 136.

[12] **J. P. Kim and D. R. Bae**: *Fuzzy congruences in groups*, Fuzzy Sets and Systems, **85** (1997), 115 – 120.

[13] **F. Marty**: *Sur une generalization de la notion de groups*, 8th congress Math. Scandinaves, Stockholm (1934), 45 – 49.

[14] **H. T. Nguyen and E. A. Walker**: *A First Course in Fuzzy Logic*, 3rd Edition, Chapman and Hall/ CRC, 2006.

[15] **R. Rosenfeld**: *Fuzzy groups*, J. Math. Anal. Appl. **35** (1971), 512 – 517.

[16] **L. A. Zadeh**: *Fuzzy sets*, Information and Control **8** (1965), 338 – 353.

Received March 10, 2007

R. Ameri: Department of Mathematics, Mazandaran University, Babolsar, Iran
E-mail: rez_ameri@yahoo.com

M. Bakhshi: Department of Mathematics, Bojnord University, Bojnord, Iran
E-mail:bakhshimahmood@yahoo.com

S. A. Nematollah Zadeh Department of Mathematics, Payam Nour University, Bam, Iran

R. A. Borzooei: Department of Mathematics, Shahid Beheshti University, Tehran, Iran
E-mail:borzooei@sbu.ac.ir

Quasigroups and Related Systems **15** (2007), 233 – 250

Subdirectly irreducible sloops and SQS-skeins

Magdi. H. Armanious and Enas. M. A. Elzayat

Abstract

It was shown in [2] that there is 8 classes of nonsimple subdirectly irreducible SQS-skeins of cardinality 32 (SK(32)s). Now, we present the same classification for sloops of cardinality 32 (SL(32)s) and unify this classification for both SL(32)s and SK(32)s in one table. Next, some recursive construction theorems for subdirectly irreducible SL($2n$)s and SK($2n$)s which are not necessary to be nilpotent are given. Further, we construct an SK($2n$) with a derived SL($2n$) such that SK($2n$) and SL($2n$) are subdirectly irreducible and have the same congruence lattice. We also construct an SK($2n$) with a derived SL($2n$) such that the congruence lattice of SK($2n$) is a proper sublattice of the congruence lattice of SL($2n$).

1. Introduction

A *Steiner quadruple* (*triple*) *system* is a pair $(S;B)$ where S is a finite set and B is a collection of 4-subsets (3-subsets) called *blocks* of S such that every 3-subset (2-subset) of S is contained in exactly one block of B (cf. [13] and [17]). Let SQS(m) denotes a Steiner quadruple system (briefly quadruple system) of cardinality m and STS(n) be a Steiner triple system (briefly: triple system) of the cardinality n. It is well known that SQS(m) exists iff $m \equiv 2$ or 4 (mod 6), and STS(n) exists iff $n \equiv 1$ or 3 (mod 6) (cf. [13] and [17]). Let $(S;B)$ be an SQS. If $S_a = S - \{a\}$ for some point $a \in S$, then deleting a from all blocks which contain it we obtain the triple system $(S_a; B(a))$, where

$$B(a) = \{b' = b - \{a\} : b \in B \text{ and } a \in b\}.$$

The system $(S_a; B(a))$ is called a *derived triple system* (or briefly DTS) of $(S;B)$ (cf. [13] and [17]).

2000 Mathematics Subject Classification: 05B30, 08A99, 05B07, 20N05
Keywords: Steiner triple system, Steiner loops, Steiner quadruple system, SQS-skein.

There is one-to-one correspondence between STSs and sloops. A *sloop* (briefly SL) $L = (L; \cdot, 1)$ is a groupoid with a neutral element 1 satisfying the identities:

$$x \cdot y = y \cdot x, \quad 1 \cdot x = x, \quad x \cdot (x \cdot y) = y.$$

A sloop L is called *Boolean* if it satisfies the associative law.

Also, there is one-to-one correspondence between SQSs and SQS-skeins (cf. [13] and [17]). An SQS-*skein* (briefly: SK) $(Q; q)$ is an algebra with a ternary operation q such that

$$q(x, y, z) = q(x, z, y) = q(z, x, y), \quad q(x, x, y) = y, \quad q(x, y, q(x, y, z)) = z$$

is valid for all $x, y, z \in Q$. An SQS-skein $(Q; q)$ satisfying the identity:

$$q(a, x, q(a, y, z)) = q(x, y, z)$$

is called *Boolean*. Any sloop associated with a given derived triple system is also called *derived*. A sloop $(Q_a; \cdot, a)$ with the binary operation "$\cdot$" defined by $x \cdot y = q(a, y, z)$, where $a \in Q$, is called *derived sloop* of an SQS-skein $(Q; q)$ *with respect to* $a \in Q$.

A subsloop N of L is called *normal* if and only if $N = [1]\theta$ for a congruence θ on L. Similarly, a sub-SQS-skein of Q is called *normal* if and only if $N = [a]\theta$ for a congruence θ of Q (cf. [13] and [18]). The congruence θ associated with the normal subsloop (sub-SQS-skein) N is given by:

$$\theta = \{(x, y) : x \cdot y \in N\}.$$

All congruences of sloops (SQS-skeins) are permutable, regular and uniform (cf. [1] and [18]). Congruence lattices of sloops and SQS-skeins are modular.

Theorem 1. *Every subsloop (sub-SQS-skein) M of a finite sloop $(L; \cdot, 1)$ (SQS-skein $(Q; q)$) such that $|L| = 2\,|M|$ (resp. $|Q| = 2\,|M|$) is normal.* □

If $(G; +)$ is a Boolean sloop or, equivalently, a Boolean group, then $(G; q)$ with $q(x, y, z) = x + y + z$ is a Boolean SQS-skein [1]. The class $\mathbf{A}_0$ of all Boolean sloops (SQS-skeins) is the smallest non-trivial subvariety of the variety of all sloops (SQS-skeins).

A congruence θ on a sloop L or on an SQS-skein Q is called *central*, if the diagonal relation Δ_L (resp. Δ_Q) is a normal subsloop (sub-SQS-skein) of L (resp. Q). The largest central congruence is called the *center* of L (resp. Q) and is denoted by $\zeta(L)$ (resp. $\zeta(Q)$) (cf. [1] and [11]). A series of

congruences $1 = \theta_0 \supseteq \theta_1 \supseteq \theta_2 \supseteq \ldots \supseteq \theta_n = 0$ (or Δ) is called *central series* if $\theta_i/\theta_{i+1} \subseteq \zeta(L/\theta_{i+1})$ (resp. $\theta_i/\theta_{i+1} \subseteq \zeta(Q/\theta_{i+1})$). If L (resp. Q) contains a central series, then L (resp. Q) is called *nilpotent*. If in nilpotent L (resp. Q) the smallest length of a central series is n, then it is called *nilpotent of class* n (cf. [4] and [5]).

Lemma 2. (cf. [4] and [15]) *If θ is a congruence on a sloop L or on an SQS-skein Q and $|[x]\theta| = 2$, then θ is a central congruence. Moreover, if L (resp. Q) is subdirecly irreducible, then $\theta = \zeta(L)$ (resp. $\theta = \zeta(Q)$).* □

2. Subdirectly irreducible SL(32)s and SK(32)s

For any congruence θ on a sloop L or on an SQS-skein Q we may define the dimension $d(\theta)$ as the length of the maximal chain between the smallest congruence 0 (the diagonal relation) and θ in $\mathrm{C}(L)$ or $\mathrm{C}(Q)$. All maximal chains in a finite modular lattice have the same length [16].

All SL(16)s (also SK(16)s) can be divided into 5 classes according to the shape of its congruence lattice or, equivalently, to the number of sub-SL(8)s (sub-SK(8)s) (cf. [8] and [9]). Let L_* (resp. Q_*) be an SL(16) (resp. SK(16)) and let θ_* be an atom in $\mathrm{C}(L_*)$ (resp. $\mathrm{C}(Q_*)$), then $\mathrm{C}(L_*/\theta_* \cong S(\mathbb{Z}_2^r))$ (resp. $\mathrm{C}(Q_1/\theta_*)) \cong S(\mathbb{Z}_2^r)$ (the lattice of all subgroups of the Boolean group $\mathbb{Z}_2^r$). Consequently, for the length of the maximal chain in $\mathrm{C}(L)$ or $\mathrm{C}(Q)$) we have $d(1) = r + 1$ with $r = 0, 1, 2, 3, 4$. So, there are 5 classes for each of SL(16)s and SK(16)s which are presented in Table 1. Examples for each class of SL(16)s and SK(16)s and for an SK(16)s with a derived SL(16) for all possible congruence lattices of SK(16) and its derived SL(16), can be found in [8] and [9].

Armanious gave in [2] all 8 classes of nonsimple subdirectly irreducible SK(32)s. The same classification holds for nonsimple subdirectly irreducible SL(32)s.

If in modular lattice two elements θ and φ cover $\theta \wedge \varphi$, then $\theta \vee \varphi$ covers θ and φ [16]. Moreover, $\theta \vee \varphi = \theta \circ \varphi$ in permutable varieties. This implies that if θ and φ are atoms in the congruence lattice $\mathrm{C}(L)$ (resp. $\mathrm{C}(Q)$) of a finite sloop (SQS-skein), then the congruence $\theta \vee \varphi = \theta \circ \varphi$ covers θ and φ. Also, the dimensions d(1) of the largest congruence 1 of both L/θ and L/φ (resp. Q/θ and Q/φ) are the same.

d(1)	C(L_*) and C(Q_*) are isomorphic to	Algebraic properties of SL(16) = L_* and SQ(16) = Q_*	Properties of the STS(15) and SQS(16)
1	$\theta_* = 1$ $\mid [x] \mid \theta_* = 16$	L_* and Q_* are simple.	STS(15) has no sub-STS(7)s and SQS(16) has no sub-SQS(8)s.
2	$\mid [x] \mid \theta_* = 8$	$\mathbf{C}(L_*)$ and $\mathbf{C}(Q_*)$ have one proper congruence. L_* and Q_* are sub-directly irreducible, but not nilpotent.	STS(15) has one sub-STS(7) and SQS(16) has two disjoint sub-SQS(8)s.
3	$\mid [x]\theta_* \mid = 4$	$\mathbf{C}(L_*)$ and $\mathbf{C}(Q_*)$ have 3 co-atoms. L_* and Q_* are subdirectly irreducible, but not nilpotent.	STS(15) has 3 sub-STS(7)s and SQS(16) has 6 sub-SQS(8)s.
4	$\mid [x]\theta_* \mid = 2$	$\mathbf{C}(L_*)$ and $\mathbf{C}(Q_*)$ have 7 co-atoms. The atom θ_* is the center of L_* (resp. Q_*). L_* and Q_* are subdirectly of nilpotence calss 2.	STS(15) has exactly 7 sub-STS(7)s and SQS(16) has exactly 14 sub-SQS(8)s.
5	It has more than one atom.	Both L_* and Q_* are Boolean. So $L_* \cong \mathrm{SL}(2)^4$ and $Q_* \cong \mathrm{SK}(2)^4$. It has $2^4 - 1$ atoms and $2^4 - 1$ co-atoms.	STS(15) has exactly 15 sub-STS(7)s and SQS(16) has exactly 30 sub-SQS(8)s.

Table 1. All classes of subdirectly irreducible sloops and SQS-skeins of cardinality 16.

So, $d(1) = 1$ iff L (resp. Q) is simple and $d(1) = n$ if L (resp. Q) is Boolean of the cardinality 2^n. In general, $1 \leqslant d(1) \leqslant n$ for each of $\mathrm{SL}(2^n)$ and $\mathrm{SK}(2^n)$.

Consider a sloop $L = \mathrm{SL}(32)$ and an SQS-skein $Q = SK(32)$, in which both L and Q are subdirectly irreducible with a monolith θ_0. It is well-known that there are simple $\mathrm{SK}(n)$s and simple $\mathrm{SL}(n)$s for each $n \equiv 2$ or $4 \pmod 6$ (see [1], [7], [10] and [18]). Except the case $d(1) = 1$, when $\mathrm{SK}(n)$s and $\mathrm{SL}(n)$s are simple, we have four other cases $d(1) = 2, 3, 4, 5$. For each $d(1) = r$, we have two different classes of L/θ_0 (resp. Q/θ_0). In the first class L/θ_0 (resp. Q/θ_0) is Boolean and has 2^{r-1} elements. In the second L/θ_0 (resp. $Q\theta_0$) is an $\mathrm{SL}(16)$ (resp. $\mathrm{SK}(16)$) and belongs to the class $r-1$ of Table 1. This means that the congruence lattice $C(L)$ (resp. $C(Q)$) is isomorphic to one of the following two lattices:

In the following table, we review the algebraic and combinatoric properties of each class of nonsimple subdirectly irreducible SL(32)s and SK(32)s.

d(1)	The lattices $\mathrm{C}(L_*)$ and $\mathrm{C}(Q_*)$	Properties of $\mathrm{SL}(32) = L$ and $\mathrm{SQ}(32) = Q$	Properties of the associated STS(31) and SQS(32)
2 (a)	$\mid [x]\theta_0 \mid = 2$	Normal subalgebras of L and Q have 2 elements. Has no subalgebras of cardinality > 8. Only homomorphic images of L/θ_0 and Q/θ_0 are simple of cardinality 16.	STS(31) has $(15 \cdot 14)/6$ sub-STS(7)s. SQS(32) has $(16 \cdot 15 \cdot 14)/24$ sub-SQS(8)s.
2 (b)	$\mid [x]\theta_0 \mid = 16$	L has one sub-SL(16) and Q has two disjoint sub-SK(16)s. Only proper homomorphic images of L/θ_0 and Q/θ_0 are of cardinality 2.	STS(31) has only one sub-STS(15). SQS(32) has two disjoint sub-SQS(16)s. These 3 subsystems belongs to the classes from Table 1.

3 (a)	$\mid [x]\theta_1 \mid = 16$ $\mid [x]\theta_0 \mid = 2$	$\mid L/\theta_0 \mid = \mid Q/\theta_0 \mid = 16$, $\mid L/\theta_1 \mid = \mid Q/\theta_1 \mid = 2$. L/θ_0 and Q/θ_0 belong to the class 2 from Table 1. $L(Q)$ has only one normal sub-SL(16) (two disjoint normal sub-SK(16)s). These subsystems belong to the class $4(a)$ or $4(b)$ of Table 1.	STS(31) has only one sub-STS(15) and at least $(15 \cdot 14)/6$ sub-STS(7)s. The SQS(32) has two disjoint sub-SQS(16)s and at least $(16 \cdot 15 \cdot 14)/24$ sub-SQS(8)s.
3 (b)	$\mid [x]\theta_0 \mid = 8$	$\mid L/\theta_0 \mid = \mid Q/\theta_0 \mid = 4$. $L(Q)$ has 3 normal sub-SL(16)s (6 normal sub-SK(16)s) and only one normal sub-SL(8) (4 disjoint normal sub-SK(8)s). Sub-SL(16)s and sub-SK(16)s are not simple and belong to some nonsimple class from Table 1.	The STS(31) has exactly three sub-STS(15)s and the SQS(32) has six sub-SQS(16)s.
4 (a)	$\mid [x]\theta_1 \mid = 8$ $\mid [x]\theta_0 \mid = 2$	$\mid L/\theta_1 \mid = \mid Q/\theta_1 \mid = 4$, $\mid L/\theta_0 \mid = \mid Q/\theta_0 \mid = 16$. L/θ_0 and Q/θ_0 belong to the class 3 of Table 1. $L(Q)$ has three normal sub-SL(16)s (6 normal sub-SK(16)s) and only one normal sub-SL(8) (4 disjoint normal sub-SK(8)s). Sub-SL(16)s and sub-SK(16)s belong to the class $4(a)$ or $4(b)$ of Table 1.	STS(31) has only 3 sub-STS(15)s. The associated SQS(32) has 6 sub-SQS(16)s.

4 (b)	$\mid [x]\theta_0 \mid = 4$	$\mid L/\theta_0 \mid = \mid Q/\theta_0 \mid = 8$. $L(Q)$ has 7 normal sub-SL(16)s (14 normal sub-SK(16)s) and only one normal sub-SL(4) (8 disjoint normal sub-SK(4)s). Sub-SL(16)s and sub-SK(16)s belong to the class 3 or 4 of Table 1.	The STS(31) has exactly 7 sub-STS(15)s. The associated SQS(32) has 14 sub-SQS(16)s.
5 (a)	$\mid [x]\theta_1 \mid = 4$ $\mid [x]\theta_0 \mid = 2$	$\mid L/\theta_1 \mid = \mid Q/\theta_1 \mid = 8$, $\mid L/\theta_0 \mid = \mid Q/\theta_0 \mid = 16$. L/θ_0 and Q/θ_0 belong to the class 4(a) of Table 1. θ_0 is the center of $L(Q)$ and θ_1/θ_0 is the center of $L/\theta_0(Q/\theta_0)$. $L(Q)$ is of nilpotence class 3 and has 7 normal sub-SL(16)s (14 normal sub-SK(16)s) and exactly one normal sub-SL(4) (8 disjoint normal sub-SK(4)s) and one normal sub-SL(2) (16 disjoint normal sub-SK(2)s).	The STS(31) has exactly 7 sub-STS(15)s and the associated SQS(32) has exactly 14 sub-SQS(16)s. All sub-STS(16)s and sub-SQS(16)s belong to the class 4(a) or 4(b) of Table 1.
5 (b)	$\mid [x]\theta_0 \mid = 2$	$\mid L/\theta_0 \mid = \mid Q/\theta_0 \mid = 16$. $L(Q)$ is nilpotent of the class 2 and θ_0 is its center. $L(Q)$ has 15 normal sub-SL(16)s (30 normal sub-SK(16)s) and exactly one normal sub-SL(2) (16 disjoint normal sub-SK(2)s). Sub-SL(16)s and sub-SK(16)s belong to the class 4(a) or 4(b) of Table 1.	STS(31) has exactly 15 sub-STS(15)s and the associated SQS(32) has exactly 30 sub-SQS(16)s.

3. Subdirectly irreducible SL(2n)s and SK(2n)s

In this section, we find recursive constructions for subdirectly irreducible sloops and SQS-skeins, i.e., for subdirectly irreducible $\mathrm{SK}(n) = Q_*$ and $\mathrm{SL}(n) = L_*$ with a monolith θ_*, we construct subdirectly irreducible $Q = SK(2n)$ (resp. $L = SL(2n)$) having a homomorphic image which congruent to Q_* (resp. to L_*).

For a given subdirectly irreducible $\mathrm{SK}(n)$ and $\mathrm{SL}(n)$ of nilpotence class $k > 1$ Guelzow (cf. [14], [15]) and Armanious (cf. [3], [4], [5]) constructed a subdirectly irreducible $\mathrm{SK}(2n)$ (resp. $\mathrm{SL}(2n)$) of nilpotence class $k + 1$. Below, basing on results of [15] and [4], we present three recursive constructions for subdirectly irreducible SQS-skeins and sloops. Namely, for a given subdirectly irreducible $\mathrm{SK}(n)$ and $\mathrm{SL}(n)$ (not necessary nilpotent or simple) with a monolith, we construct a subdirectly irreducible $\mathrm{SK}(2n)$ (resp. $\mathrm{SL}(2n)$).

Construction. Let $Q_* = (Q_*; q_*)$ be an $\mathrm{SK}(n)$ and $L_* = (L_*; *, 1)$ be an $\mathrm{SL}(n)$. Let $L_* = Q_* = \{x_0, x_1, \ldots, x_{n-1}\}$ and R be a set of sub-SK(4)s of Q_* (sub-SL(4)s of L_*), where x_0 denotes the unit 1 of sloops. Consider the binary operation $\bullet$ on $L = L_* \times GF(2)$ and the ternary operation q on $Q = Q_* \times GF(2)$ defined as follows:

$$q((x, i_x), (y, i_y), (z, i_z)) = (q_*(x, y, z), i_x + i_y + i_z + \chi_R\langle x, y, z\rangle_{Q_*}),$$
$$(x, i_x) \bullet (y, i_y) = (x * y, i_x + i_y + \chi_R\langle x, y\rangle_{L_*}),$$

where χ_R is the characteristic function such that $\chi_R\langle x, y, z\rangle_{Q_*} = 1$ if $\langle x, y, z\rangle_{Q_*}$ generates a sub-SK(4) $\in R$, and 0 otherwise; $\chi_R\langle x, y\rangle_{L_*} = 1$ if $\langle x, y\rangle_{L_*}$ generates a sub-SL(4) $\in R$, and 0 otherwise.

It easy to prove that $Q = (Q; q)$ is an $\mathrm{SK}(2n)$ and $L = (L; \bullet)$ is an $\mathrm{SL}(2n)$ (for details see [15] and [4]). In the sequel, the SQS-skein Q and the sloop L will be denoted by $2 \times_R Q_*$ and $2 \times_R L_*$, respectively.

If R is empty, then $\chi_R\langle x, y, z\rangle_{Q_*} = 0$ for $x, y, z \in Q_*$ and $\chi_R\langle x, y\rangle_{L_*} = 0$ for $x, y \in L_*$. Thus $(Q; q) = Q_* \times SK(2)$ and $(L; \bullet, (1, 0)) = L_* \times SL(2)$. If R is the set of all sub-SK(4)s of Q_* (resp. sub-SL(4)s of L_*), then $Q(L)$ is Boolean or of nilpotence class $k + 1$ if and only if Q_*L_*) is Boolean or of nilpotence class $k > 1$, respectively. Moreover, Q is semi-boolean if and only if Q_* is semi-boolean (see [15]).

Lemma 3. *Let Q_* (resp. L_*) be a subdirectly irreducible SQS-skein (sloop) with monolith θ_* and let R be the set of sub-*SK(4)*s (sub-*SL(4)*s). The con-*

structed SKS-*skein* $2\times_R Q_*$ (*resp. sloop* $2\times_R L_*$) *has a congruence* θ_1 *which covers all its minimal congruences.*

Proof. The projection π from $Q(L)$ into the first component is onto homomorphism and the congruence $\ker\pi = \theta_0$ on $Q(L)$ is determined by the relation $\{((x,i),(x,j)) : \forall x \in Q_*(L_*), \forall i,j \in \{0,1\}\}$. Now $Q/\theta_0 \cong Q_*$ and $L/\theta_0 \cong L_*$. Since θ_* is the monolith of Q_* and L_*, Q/θ_0 (resp. L/θ_0) has a monolith θ_1/θ_0 for a congruence θ_1 on Q (resp. on L). Thus θ_1 is the unique congruence in $\mathrm{C}(Q)$ (resp. $C(L)$) which covers θ_0. If δ is another atom of $\mathrm{C}(Q)$ (resp. $C(L)$), then $\delta \circ \theta_0 = \theta_1$ covers δ and θ_0. Therefore, θ_1 covers all atoms of $\mathrm{C}(Q)$ (resp. $C(L)$). □

Moreover, since $|\ [(x_0,0)]\theta_0 \mid = 2$, it follows that if $|\ [(x_0)]\theta_* \mid = m$, then $|\ [(x_0,0)]\theta_1 \mid = 2m$.

Guelzow [15] and Armanious [4] for a given subdirectly irreducible $\mathrm{SK}(n) = Q_*$ ($\mathrm{SL}(n) = L_*$) of nilpotence class k with a minimal congruence θ_* such that $|\ [x]\theta_* \mid = 2$ constructed subdirectly irreducible $\mathrm{SK}(2n) = Q$ and $\mathrm{SL}(2n) = L$ of nilpotence class $k+1$.

Below we prove that for a subdirectly irreducible $\mathrm{SK}\ (n) = Q_*$ (resp. $\mathrm{SL}(n) = L_*$) with a monolith θ_* for each possible cardinality of $|[x]\theta_*\ |$ the constructed $Q = 2 \times_R Q_*$ (resp. $L = 2 \times_R L_*$) is subdirectly irreducible. Note that Q_* and L_* are not nilpotent, in general.

In the following three theorems, let x_0 be the unit 1 of sloops, $*$ the binary operation on L_* and $\bullet$ the operation on L, i.e., $x * y = q_*(x_0, x, y)$ on the set Q_* and $(x,i) \bullet (y,j) = q((x_0,\ 0),\ (x,\ i),\ (y,\ j))$ on the set Q.

The proof of the theorem presented below is analogous to the proof of the corresponding theorems for nilpotent SQS-skeins and sloops from [3] and [4].

Theorem 4. *Let* $n > 8$. *If* $\mathrm{SK}(n) = Q_*$ (*resp.* $\mathrm{SL}(n) = L_*$) *is subdirectly irreducible with a monolith* $\theta_* = \cup\{\{x_i, x_{i+1}\}^2 : i = 0, 2, \ldots, n-2\}$ *and* $R = \{x_0, x_1, x_2, x_3\}$, *then the constructed SQS-skein* $Q = 2 \times_R Q_*$ (*resp. sloop* $L = 2 \times_R L_*$) *is also subdirectly irreducible.*

Proof. As in Lemma 3, $\theta_0 = \{((x,i),(x,j)) : x \in Q_*,\ i,j \in \{0,1\}\}$ (resp. $x \in L_*$) is an atom of $\mathrm{C}(Q)$(*resp.*$\mathrm{C}(L)$) and $\theta_1 \in \mathrm{C}(Q)$ (resp. $\mathrm{C}(L)$) is the unique congruence covering all atoms of $\mathrm{C}(Q)$ (resp. $\mathrm{C}(L)$). The theorem will be proved if we show that the congruence θ_0 is the unique atom in the congruence lattice $\mathrm{C}(Q)$ (resp. $\mathrm{C}(L)$). If there is another atom $\delta \neq \theta_0$ in the congruence lattice $\mathrm{C}(Q)$ (resp. $\mathrm{C}(L)$), then $\delta \circ \theta_0 = \theta_1$ covers both

δ and θ_0. Since $[x_0]\theta_* = \{x_0,\ x_1\}$ and $|\ [(x_0,0)]\theta_0\ | = 2$, it follows that $|\ [(x_0,0)]\theta_1\ | = 4$. Then $[(x_0,0)]\theta_1 = \{(x_0,0),\ (x_0,1),\ (x_1,0),\ (x_1,1)\}$. This means that if there is another atom δ in $C(Q)$ (resp. $C(L)$), then

$$[(x_0,0)]\delta = \{(x_0,0),(x_1,0)\} \quad \text{or} \quad [(x_0,0)]\delta = \{(x_0,0),(x_1,1)\},$$

which is impossible.Indeed, each 2-element subset $\{x,y\}$ of an SK is a sub-SK(2) and for each element x of an SL the set $\{1,x\}$ is a sub-SL(2). Also, if θ is a congruence on an SK (resp. SL), then $[x]\theta \cup [y]\theta([1]\theta \cup [x]\theta)$ is a sub-SK (sub-SL). In addition, $x\theta y$ if and only if $q(a,y,z)\theta a$ (resp. $x \cdot y\theta 1$). Moreover, for 3 distinct elements x, y, z, we have $q(x,y,z) \notin \{x,y,z\}$ because, for example, $q(x,y,z) = z$ implies $y = q(x,z,q(x,z,y)) = q(x,z,z) = x$.

In the case of SQS-skeins, according to the definition of θ_*, we see that $\{x_0,x_1\} \cup \{x_2,x_3\}$ and $\{x_0,x_1\} \cup \{x_4,x_5\}$ are sub-SK(4). Thus $q_*(x_0,x_1,x_2) = x_3$ and $q_*(x_0,x_1,x_4) = x_5$. So, $q_*(x_0,x_2,x_4) = x_k$ and $[x_k]\theta_* = \{x_k,x_{k+1}\}$. Therefore, $q_*(x_0,x_k,x_{k+1}) = x_1$.

For $[(x_0,0)]\delta = \{(x_0,0),(x_1,0)\}$, we have $q((x_0,0),(x_2,0),(x_3,1)) = (x_1,0)$ and $q((x_0,0),(x_4,0),(x_5,0)) = (x_1,0)$. Thus $(x_2,0)\delta(x_3,1)$ and $(x_4,0)\delta(x_5,0)$. But $(x_0,0)\delta(x_0,0)$, so, $(q_*(x_0,x_2,x_4),0)\delta(q_*(x_0,x_3,x_5),1)$, i.e., $(x_k,0)\delta(q_*(x_0,x_3,x_5),1)$. This means that $(q_*(x_0,x_3,x_5),1) \in [(x_k,0)]\delta$, which is a contradiction because $[(x_k,0)]\delta = q((x_0,0),(x_k,0),[(x_0,\ 0)]\delta) = \{(x_k,0),(x_{k+1},0)\}$, where $q_*(x_0,x_k,x_{k+1}) = x_1$.

For $[(x_0,0)]\delta = \{(x_0,0),(x_1,1)\}$, we have $q((x_0,0),(x_2,0),(x_3,0)) = (x_1,1)$ and $q((x_0,0),(x_4,0),(x_5,1)) = (x_1,1)$. Whence $(x_2,0)\delta(x_3,0)$ and $(x_4,0)\delta(x_5,1)$. This implies that $(q_*(x_0,x_2,x_4),0)\delta(q_*(x_0,x_3,x_5),1)$. Thus $(x_k,0)\delta(q_*(x_0,x_3,x_5),1)$. From this, as a simple consequence, we obtain $q((x_0,0),(x_5,1),(x_k,0))\delta q((x_0,0),(x_5,1),(q_*(x_0,x_3,x_5),1))$. This means that $(q_*(x_0,x_5,x_k),1)\delta(x_3,0)$, i.e., $(q_*(x_0,x_5,x_k),1) = (x_2,0)$ or $(x_3,0)$, which is impossible.

Therefore, the congruence θ_0 is the unique atom of C(Q). □

Note that for each positive integers n and k there exists a subdirectly irreducible SK(2^n) (resp. SL(2^n)) of nilpotence class k with a monolith θ_* such that $|\ [x]\theta_*\ | = 2$ (cf. [15] and [4]).

The above results we can summarize in the following table:

If Q_* (resp. L_*) is a subdirectly irreducible SK(n) (resp. SL(n)) for $n \geq 16$ with a monolith θ_* such that $\mid [x]\theta_* \mid = 2$, then the constructed SQS-skein Q (sloop L) is a subdirectly irreducible with a congruence lattice C(Q) (resp. C(L)) isomorphic to the lattice Γ and C(Q_*) (resp. C(L_*)) is equal to $[\theta_0 : 1]$. Note that in general Q_* and L_* are not nilpotent.	
In particular, Q_* (resp. L_*) may be of nilpotence class $t \geqslant 1$ of cardinality $n = 2^{r+t}$, $r \geqslant 3$, with C(Q_*) (resp. C(L_*)) isomorphic to Γ_1. Then $Q(L)$ is of nilpotence class $t+1$ having a congruence lattice C(Q) (resp. C(L)) isomorphic to Γ_2 with $\mid [x]\theta_i \mid = 2^{i+1}$ $(i = 0, 1, \ldots, t-1)$ and $Q/\theta_0 \cong Q_*$ (resp. $L/\theta_0 \cong L_*$). Also, θ_{i+1}/θ_i is the center and in the same time is the monolith of Q/θ_i (resp. L/θ_i). For example, let $r = 3$ and $t = 1$, then Q_* =SK(16) (resp. L_* =SL(16)) belongs to the class 4(a) of Table 1 and Q =SK(32) (resp. L =SL(32)) belongs to the class 5(a) of Table 2.	

Theorem 5. *Let* $(Q_*; q_*)$ *(resp.* $L_*; *, 1)$*) be a subdirectly irreducible SQS-skein (resp. sloop) of cardinality* $n > 8$ *with a minimum congruence* θ_* *such that* $\mid [x]\theta_* \mid = 4$*. If* $R = [x_0]\theta_*$ *is a sub-SK*(4) *(resp. sub-SL*(4)*), then the constructed SQS-skein* $Q = 2 \times_R Q_*$ *(sloop* $L = 2 \times_R L_*$*) is also subdirectly irreducible.*

Proof. As in Lemma 3, θ_0 is an atom and θ_1 is the unique congruence covering θ_0 in C(Q) (resp. in C(L)). Similar to the above theorem, it is suffices to show that θ_0 is the unique atom in the congruence lattice C(Q) (resp. C(L)).

If there is another atom δ in C(Q)(**C**(L)), then θ_1 covers δ and θ_0, and also $\delta \circ \theta_0 = \theta_1$. If $[x_0]\theta_* = \{x_0, x_1, x_2, x_3\}$, then

$$[(x_0, 0)]\theta_1 = \{(x_0, 0), (x_1, 0), (x_2, 0), (x_3, 0), (x_0, 1), (x_1, 1), (x_2, 1), (x_3, 1)\}.$$

This means that the class $[(x_0, 0)]\theta_1$ is divided in to two subclasses $[(x_0, 0)]\delta$ and $[(x_0, 1)]\delta$ such that both $(x, 0)$ and $(x, 1)$ can not be in the same sub-

class. Indeedd, if $(x,0)\delta(x,1)$, then

$$q((x_0,0),(x,0),(x,1)) = (q_*(x_0,x,x),1) = (x_0,1) \in [(x_0,0)]\delta,$$

which implies $[(x_0,0)]\delta \supseteq [(x_0,0)]\theta_0$. But this is impossible.

If $(x_1,0)$ and $(x_2,0) \in [(x_0,0)]\delta$, then

$$q((x_1,0),(x_2,0),(x_0,0)) = (q_*(x_1,x_2,x_0),1) = (x_3,1).$$

Thus, $(x_3,1) \in [(x_0,0)]\delta$. If $(x_1,1),(x_2,1) \in [(x_0,0)]\delta$, then

$$q((x_1,1),(x_2,1),(x_0,0)) = (q_*(x_1,x_2,x_0),1) = (x_3,1),$$

which gives $(x_3,1) \in [(x_0,0)]\delta$. This means that $[(x_0,0)]\delta$ contains exactly 3-element subset of the set $\{x_0,x_1,x_2,x_3\} \times \{0,1\}$ with the same second component.

We have $|[(x_0,0)]\delta| = 4$ and $|[(x_0,0)]\theta_1| = 8$. Without loss of generality, we can assume that

(i) $[(x_0,0)]\delta = \{(x_0,0),(x_1,0),(x_2,0),(x_3,1)\}$ or

(ii) $[(x_0,0)]\delta = \{(x_0,0),(x_1,1),(x_2,1),(x_3,1)\}$.

Case (i) for SQS-skeins: Assume that $(x,0) \in Q$ such that $x \notin \{x_0,x_1,x_2,x_3\}$, then:

$$\begin{aligned}
[(x,0)]\delta &= q((x,0),(x_0,0),[(x_0,0)]\delta) \\
&= \{q((x,0),(x_0,0),(x_0,0)), q((x,0),(x_0,0),(x_1,0)), \\
&\qquad q((x,0),(x_0,0),(x_2,0)), q((x,0),(x_0,0),(x_3,1))\} \\
&= \{(x,0),(q_*(x,x_0,x_1),0),(q_*(x,x_0,x_2),0),(q_*(x,x_0,x_3),1)\}
\end{aligned}$$

and

$$\begin{aligned}
[(q_*(x,x_0,x_3),1)]\delta &= q((q_*(x,x_0,x_3),1),(x_0,0),[(x_0,0)]\delta) \\
&= \{q((q_*(x,x_0,x_3),1),(x_0,0),(x_0,0)), \\
&\quad q((q_*(x,x_0,x_3),1),(x_0,0),(x_1,0)), \\
&\quad q((q_*(x,x_0,x_3),1),(x_0,0),(x_2,0)), \\
&\quad q((q_*(x,x_0,x_3),1),(x_0,0),(x_3,1))\} \\
&= \{(q_*(x,x_0,x_3),1),(q_*(q_*(x,x_0,x_3),x_0,x_1),1), \\
&\quad (q_*(q_*(x,x_0,x_3),x_0,x_2),1),(x,0)\}.
\end{aligned}$$

This means that $[(x,0)]\delta \cap [(q_*(x,\ x_0,\ x_3),\ 1)]\delta \neq \emptyset$ and $[(x,0)]\delta$ is not identical with $[(q_*(x,x_0,x_3),1)]\delta$, which contradicts the fact that δ is a congruence. So, this case is impossible.

In a similar way we can prove that also the second case is impossible. □

Theorem 6. *Let $(Q_*; q_*)$ (resp. $(L_*; *, 1)$) be a subdirectly irreducible SQS-skein (resp. sloop) of cardinality $n > 8$ with a minimum congruence θ_* such that $|[x]\theta_*| > 4$. If $R = \{x_0, x_1, x_2, x_3\}$ is a sub-SK(4) of Q_* (resp. sub-SL(4) of L_*) contained in $[x_0]\theta_*$, then the constructed SQS-skein $Q = 2 \times_R Q_*$ (sloop $L = 2 \times_R L_*$) is also subdirectly irreducible with a monolith θ_0 and $Q/\theta_0 \cong Q_*$ (resp. $L/\theta_0 \cong L_*$).*

Proof. As in Lemma 3, θ_1 is the unique congruence covering the atom θ_0 and all other atoms in $\mathrm{C}(Q)$ (resp. $\mathrm{C}(L)$). We need only prove that θ_0 is the unique atom in the congruence lattice $\mathrm{C}(Q)$ (resp. $\mathrm{C}(L)$). Assume that there is another atom δ of $\mathrm{C}(Q)$ (resp. $\mathrm{C}(L)$). Then $\theta_1 = \delta \circ \theta_0$ covers both δ and θ_0. Since $|\ [(x, i_x)]\theta_0\ | = 2$ and θ_1 covers δ, it follows that if $|\ [(x, i_x)]\theta_1\ | = 2m$, then $|\ [(x, i_x)]\delta\ | = m$.

Let $[x_0]\theta_* = \{x_0, x_1, x_2, x_3, \ldots, x_{m-1}\}$, then

$$[(x_0, 0)]\theta_1 = \{(x_0, 0), (x_1, 0), (x_2, 0), \ldots, (x_0, 1), (x_1, 1), (x_2, 1), \ldots\}.$$

This means that the class $[(x_0, 0)]\theta_1$ is divided in to two disjoint subclasses $[(x_0, 0)]\delta$ and $[(x_0, 1)]\delta$. In the same manner as in the previous proof, we can prove that $[(x_0, 0)]\delta$ contains exactly 3-element subset of the set $\{x_0, x_1, x_2, x_3\} \times \{0, 1\}$ with the same second component.

Now, $|[(x_0, 0)]\delta| > 4$, i.e., $|[(x_0, 0)]\theta_1| > 8$ and $R = \{x_0, x_1, x_2, x_3\}$. So,

$$[(x_0, 0)]\delta = \{(x_0, 0), (x_1, 0), (x_2, 0), (x_3, 1), (a_1, 0), \ldots, (a_i, 0), (b_1, 1), \ldots, (b_j, 1)\}$$

or

$$[(x_0, 0)]\delta = \{(x_0, 0), (x_1, 1), (x_2, 1), (x_3, 1), (a_1, 0), \ldots, (a_i, 0), (b_1, 1), \ldots, (b_j, 1)\},$$

where $x_0, x_1, x_2, x_3, a_1, a_2, \ldots, a_i, b_1, b_2, \ldots, b_j$ are m distinct elements.

In the first case for SQS-skeins for all $(a_h, 0) \in [(x_0, 0)]\delta$ with $a_h \notin \{x_0, x_1, x_2, x_3\}$, we have $q((x_3, 1), (a_h, 0), (x_0, 0)) = (b_k, 1) \in [(x_0, 0)]\delta$ and $(b_k, 1) \neq (x_3, 1)$. Moreover, if $(a_{h_1}, 0) \neq (a_{h2}, 0)$, then $(b_{k_1}, 1) \neq (b_{k_2}, 1)$. Also, for all $(b_h, 1) \in [(x_0, 0)]\delta$ with $b_h \notin \{x_0, x_1, x_2, x_3\}$, we can see that $q((x_3, 1), (b_h, 1), (x_0, 0)) = (a_l, 0) \in [(x_0, 0)]\delta$ for $(a_l, 0) \neq (x_0, 0), (x_1, 0)$ or $(x_2, 0)$. Also, if $(b_{h_1}, 1) \neq (b_{h_2}, 1)$, then $(a_{k_1}, 0) \neq (a_{k_2}, 0)$. This implies that the sets $\{a_1, a_2, \ldots, a_i\}$ and $\{b_1, b_2, \ldots, b_j\}$ have the same cardinality. Then $i = j \geqslant 1$. Let $i = j = r$, then

$$[(x_0, 0)]\delta = \{(x_0, 0), (x_1, 0), (x_2, 0), (x_3, 1), (a_1, 0), ..., (a_r, 0), (b_1, 1), ..., (b_r, 1)\}.$$

Hence the class $[(x_0, 0)]\delta$ is a sub-SQS-skein having $r + 3$ elements with the second component 0 and $r+1$ elements with the second component 1.

But $q((b_1,1),(x_0,0),\{(x_0,0),(x_1,0),(x_2,0),(a_1,0),\ldots,(a_r,0)\}$ gives $r+3$ distinct elements with second component 1, which is impossible.

In the second case we obtain a similar contradiction. This proves that θ_0 is the unique minimal congruence on Q (resp. L). □

In view of Theorems 5 and 6 we get the following constructions:

If Q_* (resp. L_*) is a subdirectly irreducible SK(n) (resp. SL(n)) for $n \geq 16$ with a monolith θ_* satisfying $\mid [x]\theta_* \mid > 2$, then Q_* (resp. L_*) is not nilpotent. The constructed SQS-skein Q (sloop L) is a subdirectly irreducible having a congruence lattice C(Q) (resp. C(L)) isomorphic to $\mathbf{\Gamma}_2$ and C(Q_*) = $[\theta_0 : 1]$ (resp. C(L_*) = $[\theta_0 : 1]$) isomorphic to $\mathbf{\Gamma}_1$. The sublattice $[\theta_* : 1]$ of Γ_1 is not necessary to be isomorphic to S($\mathbb{Z}_2^r$).	
In particular, if Q_* (resp. L_*) is a subdirectly irreducible SK(2^n) (resp. SL(2^n)) for $n \geqslant 4$ with a monolith θ_* such that $\mid [x]\theta_* \mid = 2^r$, then then the constructed SQS-skein Q (resp. sloop L) is a subdirectly irreducible and has a congruence lattice C(Q) (resp. C(L) isomorphic to $\mathbf{\Gamma}_2$ and C(Q_*) = $[\theta_0 : 1]$ (resp. C(L_*) = $[\theta_0 : 1]$) isomorphic to $\mathbf{\Gamma}_1$. Indeed, $\mid [x]\theta_1 \mid = 2^{r+1}$ and $\mid [x]\theta_0 \mid = 2$, for each $n \geqslant 4$ and $r = n, n-1, \ldots, 1$. Note that Q_* (resp. L_*) is not nilpotent for $r > 1$ and Q_* (resp. L_*) is simple for $r = n$.	

Examples. 1. For $n = 4$ and $r = 3, 2$ or 1, we may choose an SK(2^4) = Q_* (resp. SL(2^4) = L_*) belonging to the classes 2, 3 or 4(a) of Table 1, respectively. Applying Theorems 6, 5 and 4 to Q_* (resp. L_*), we get three examples of a subdirectly irreducible SK(2^5) = Q (resp. SL(2^5) = L) belonging to classes 3(a), 4(a) and 5(a) of Table 2.

2. For $n > 3$ and $r = n$, we observe that Q_* (resp. L_*) is simple of cardinality 2^n and the congruence lattice of C(Q) (resp. C(L)) is a chain of length 2, i.e., θ_1 is the largest congruence in C(Q) (resp. C(L)) and θ_0 is the monolith. For instance, take $r = n = 4$ and choose a simple SK(2^4) = Q_* (resp. SL(2^4) = L_*) as in the class 1 of Table 1. In view of Theoerem 6, we

get a subdirectly irreducible $\mathrm{SK}(2^5) = Q$ (resp. $\mathrm{SL}(2^5) = L$) belonging to the class $2(a)$ of Table 2.

3. In [6] and [7] Armanious has shown that if we have a simple $\mathrm{SK}(n) = Q_*$ (resp. SL $(n) = L_*$), then there is a subdirectly irreducible $\mathrm{SK}(2n)$ (resp. $\mathrm{SL}(2n)$) having only one proper congruence. In particular, for $n = 16$, choose a simple $\mathrm{SK}(16) = Q_*$ (resp. $\mathrm{SL}(16) = L_*$) the construction $\mathrm{SK}(32) = 2 \otimes_\alpha Q_*$ [7] (resp. $\mathrm{SL}(32) = 2 \otimes_\alpha L_*$ [6]) is an example of a subdirectly irreducible SK(32) (resp. SL(32)) belonging to the class $2(b)$ of Table 2.

4. For $n \geqslant 3$ and $r = 0$, Q_* (resp. L_*) is Boolean of cardinality 2^n. According to the constructions given in [15] and [5], we may say that there is a subdirectly irreducible $\mathrm{SK}(2^{n+1}) = Q$ (resp. $\mathrm{SL}(2^{n+1}) = L$) with a monolith θ_0 such that Q/θ_0 (resp. (L/θ_0) is a Boolean $\mathrm{SK}(2^n)$ (resp. $\mathrm{SL}(2^n)$). For instance, let $n = 4$ and $r = 0$, then the constructed $\mathrm{SK}(2^5) = Q$ (resp. $\mathrm{SL}(2^5) = L$) is an example of $5(b)$ of Table 2. □

In fact, these theorems permit us to construct examples for 6 classes of Table 2, but it is not enough to construct examples for classes $3(b)$ and $4(b)$.

3.1. The SQS-skein $2 \times_R Q_*$ having $2 \times_R L_*$ as a derived sloop

In [4] Armaniuous has constructed a nilpotent SQS-skein of whose all derived sloops are nilpotent of the same class and both have the same congruence lattice. Also, he has constructed [7] a subdirectly irreducible $\mathrm{SK}(2n)$ having a derived subdirectly irreducible $\mathrm{SL}(2n)$ for $n > 8$, in which the congruence lattice of each of $\mathrm{SL}(2n)$ and $\mathrm{SK}(2n)$ are isomorphic to a chain of length 2.

Let L_* be a derived sloop of the SQS-skein Q_* with respect to the element x_0, in which L_* and Q_* are subdirectly irreducible with the same monolith θ_* (Theorems 4, 5 and 6). Let R be the same 4-element subalgebra $\{x_0, x_1, x_2, x_3\}$ in both Q_* and L_* such that $R = [x_0]\theta_* \cup [x_2]\theta_*$ (as in Theorem 4), $R = [x_0]\theta_*$ as in Theorem 5 and $R \subseteq [x_0]\theta_*$ as in Theorem 6. Therefore, $x * y = q_*(x_0, x, y)$, and consequently $\chi_R\langle x, y\rangle_{L_*} = \chi_R\langle x_0, x, y\rangle_{Q_*}$ for all $x, y \in L_* = Q_*$. Hence $(x, i_x) \bullet (y, i_y) = q((x_0, 0), (x, i_x), (y, i_y))$ for all $(x, i_x), (y, i_y) \in L = Q$, this means directly that the constructed sloop $L = 2 \times_R L_*$ is derived sloop of the constructed SQS-skein $Q = 2 \times_R Q_*$. Therefore, we have the following result.

Corollary 7. *Let L_* be a derived sloop of the SQS-skein Q_* with respect to the element x_0 and let both Q_* and L_* be subdirectly irreducible having a*

monolith θ_*. If θ_* and $R = \{x_0, x_1, x_2, x_3\}$ are defined as stated in Theorem 4, 5 and 6, then the sloop $L = 2 \times_R L_*$ is always a derived sloop of the SQS-skein $Q = 2 \times_R Q_*$ with respect to $(x_0, 0)$ for each case of θ_*. $|Box$

We may choose an SQS-skein Q_* with a derived sloop L_* and both Q_* and L_* are subdirectly irreducible of cardinality n (or in particular of cardinality 2^n). In view of Theorems 4, 5, 6 and Corollary 7, we may say that:

There is an SQS-skein $Q = 2 \times_R Q_*$ with a derived sloop $L = 2 \times_R L_*$ of cardinality n (or 2^n), in which both Q and L are subdirectly irreducible of cardinality $2n$ (or 2^{n+1}) having the same congruence lattice for each possible number n. In particular, there is always an $SK(32)$ with a derived $SL(32)$, both are subdirectly irreducible and have the same congruence lattices.

Note that the construction of a semi-Boolean SQS-skein Q (each derived sloop L of Q is Boolean) given in [14] guarantees that $\mathrm{C}(Q)$ is a proper sublattice of the congruence lattice $\mathrm{C}(L)$ of its derived sloop L. Also each nonsimple $\mathrm{SL}(16) = L$ can be extended to a nonsimple $\mathrm{SK}(16) = Q$ with all possible congruence lattice $\mathrm{C}(Q)$ as a sublattice of $\mathrm{C}(L)$ (for details see [8]).

We know that if L_* is a derived sloop from Q_*, then each congruence on Q_* is a congruence on L_*. If both Q_* and L_* are subdirectly irreducible, then the monolith φ_* of Q_* is a congruence on L_* containing the monolith θ_* of L_* (examples for $L_* = SL(16)$ and $Q_* = SK(16)$ one can find in [8]). This means that we can choose the sub-$\mathrm{SL}(4) = R = [x_0]\theta_* \cup [x_0]\theta_*$, $R = [x_0]\theta_*$ or $R \subseteq [x_0]\theta_*$, if $|[x_0]\theta_*| = 2, 4$ or > 4, respectively. Note that x_0 represents the unit of L_*. Since $\varphi_* \supseteq \theta_*$, R is a sub-$\mathrm{SK}(4)$ such that

$$
\begin{aligned}
&R = [x_0]\varphi_* \cup [x_0]\varphi_* \ \text{ if } \ |\,[x_0]\varphi_*\,| = |\,[x_0]\theta_*\,| = 2,\\
&R = [x_0]\varphi_* \ \text{ if } \ |\,[x_0]\varphi_*\,| = 4 \ \text{ and } \ |\,[x_0]\theta_*\,| = 2 \text{ or } 4,\\
&R \subseteq [x_0]\varphi_* \ \text{ if } \ |\,[x_0]\varphi_*\,| > 4 \ \text{ and } \ |\,[x_0]\theta_*\,| = 2, 4 \text{ or } > 4.
\end{aligned}
$$

In view of Theorems 4, 5 and 6, $Q = 2 \times_R Q_*$ and $L = 2 \times_R L_*$ are subdirectly irreducible with a monolith θ_0 such that $L/\theta_0 \cong L_*$ and $Q/\theta_0 \cong Q_*$. And as a result of Corollary 7, L is a derived sloop of Q, which means that $\mathrm{C}(Q)$ is a proper sublattice of $\mathrm{C}(L)$, if φ_* properly contains θ_*. In particular, we may construct the following examples:

Examples. Let $L_* = SL(16)$ be a derived sloop of $Q_* = SK(16)$. The result obtained in [8] enables us to choose L_* belonging to class $4(a)$ and Q_* belonging to class $4(a)$, 3 or 2 of Table 1. Now, we may construct an

SQS-skein SK(32) $= 2 \times_R Q_*$ with a derived sloop SL(32) $= 2 \times_R L_*$, in which the SL(32) belongs to the class $5(a)$ of Table 2. The SK(32) will belong to the class $5(a)$ of Table 2, if Q_* belongs to the class $4(a)$ of Table 1. Also, the SK (32) will belong to $4(a)$ or $3(a)$ of Table 2, if Q_* belongs to the class 3 or 2 of Table 1, respectivly. For the last two cases the congruence lattice C(SK(32)) is a proper sublattice of C(SL(32)). □

A natural open problem for future investigations is a construction of an SQS-skein Q with a derived sloop L for which a congruence lattice C(Q) is a sublattice of C(L).

References

[1] **M. H. Armanious**: *Algebraische Theorie der Quadrupelsysteme*, Ph. D.Thesis, Technischen Hochschule Darmstadt 1981.

[2] **M. H. Armanious**: *Classification of the Steiner Quadruple systems of cardinality* 32, Beitrage zur Algebra und Geometrie, **28** (1989), 39 – 50.

[3] **M. H. Armanious**: *Existence of nilpotent SQS-skeins of class n*, Ars Combinoria **29** (1990), 97 – 105.

[4] **M. H. Armanious**: *Construction of nilpotent sloops of class n*, Discrete Math. **171** (1997), 17 – 25.

[5] **M. H. Armanious**: Nilpotent SQS-skeins with nilpotent derived sloops, Ars Combinoria **56** (2000), 193 – 200.

[6] **M. H. Armanious**: *On subdirectly irreducible Steiner loops of cardinality* $2n$, Beitrage zur Algebra und Geometrie **43** (2002), 325 – 331.

[7] **M. H. Armanious**: *On subdirectly irreducible SQS-skeins*, J. Combin. Math. Combin. Comput. **52** (2005), 117 – 130.

[8] **M.H. Armanious and E. M. A. Elzayat**: *Extending sloops of cardinality 16 to SQS-skeins with all possible congruence lattices*, Quasigroups and Related Systems **12** (2004), 1 – 12.

[9] **C. Colbourn and J. Dinitz (eds):** *The CRC The CRC Handbook of Combinatorial Designs,* CRC Press, New York 1996.

[10] **J. Doyen:** *Sur la structure de certains systemes triples de Steiner*, Math. Z. **111** (1969), 289 – 300.

[11] **R. Freese and R. McKenzie:** *Commutator Theory for Congruence Modular Varieties*, LMS Lecture Note Series v.125, Cambridge Uni. Press, 1987.

[12] **B. Ganter and H. Werner:** *Co-ordinatizing Steiner Systems,* Ann. Discrete Math. **7** (1980), 83 – 24.

[13] **B. Ganter and H. Werner:**

[14] **A. J. Guelzow:** *Semi-boolean SQS-skeins*, J. Alg. Comb. **2** (1993), 147−153.

[15] **A. J. Guelzow:** *The structure of nilpotent Steiner quadruple systems*, J. Comb. Designs **1** (1993), 301 – 321.

[16] **H. Hermes:** *Einfuhrung in die Verbandstheorie*, Springer Verlag, Berlin – Heidelberg – New York, 1967.

[17] **C. C. Lindner and A. Rosa:** *Steiner Quadruple Systems: A Survey* Discrete Math. **21** (1978), 147 – 181.

[18] **R. W. Quackenbush:** *Varieties of Steiner Loops and Steiner Quasigroups,* Canada J. Math. **28** (1978), 1187 – 1198.

Department of Mathematics,
Faculty of Science,
Mansoura University,
Mansoura,
Egypt
E-mail: m.armanious@excite.com

Received June 16, 2006
Revised March 26, 2007

Quasigroups and Related Systems **15** (2007), 251 – 260

S-systems of n-ary quasigroups

Galina Belyavskaya

Abstract

In the theory of binary quasigroups the notions of a right (left) S-system and an S-system [1] are known. An S-system is simultaneously a left and right S-system. We introduce (k)-S-systems and S-systems (otherwise than in [10]) of n-ary quasigroups for $n \geqslant 2$ and $1 \leqslant k \leqslant n$, give examples of such systems and prove that any (k)-S-system, given on a finite set, is a pairwise orthogonal set ([3]) of n-ary operations.

1. Introduction

In the theory of binary quasigroups the notion of a right (left) Stein system (shortly, a right S-system or a left S-system) is known. Such system is defined in the following way [1].

A system $Q(\Sigma)$, $\Sigma = \{E, A_1^s\}$ ($\Sigma = \{F, A_1^s\}$, where A_1^s denotes the sequence $A_1, A_2, ..., A_s$), which consists of binary quasigroups and the right (left) identity operation E (F): $E(x, y) = y$ ($F(x, y) = x$) given on a set Q is called a right (left) S-system if Σ is a group with respect to the Stein's right (left) multiplication $\cdot$ ($\circ$) of binary operations:

$$(A \cdot B)(x, y) = A(x, B(x, y)) \ ((A \circ B)(x, y) = A(B(x, y), y)).$$

A system $Q(\Sigma)$, $\Sigma = \{E, F, A_1^s\}$, is called an *S-system* if $\Sigma' = \{E, A_1^s\}$ ($\Sigma'' = \{F, A_1^s\}$) is a right (left) S-system.

Finite binary S-systems are completely described in the works [1], [5], [6] by V.Belousov, G. Belyavskaya and A. Cheban.

2000 Mathematics Subject Classification: 20N05, 20N15
Keywords: binary quasigroup, k-invertible n-ary operation, n-ary quasigroup, latin square, n-dimensional hypercube, pairwise orthogonal set of n-ary operations.

Any two operations A and B on a set Q from a right (left) S-system $Q(\Sigma)$ of binary quasigroups are orthogonal, that is the pair of equations $A(x,y) = a, B(x,y) = b$ has a unique solution for any $a, b \in Q$ and any $A, B \in \Sigma$, $A \neq B$.

In this article we introduce (k)-S-systems of n-ary quasigroups for $n \geqslant 2$, $1 \leqslant k \leqslant n$, give some examples of such systems and prove that any finite (k)-S-system is a pairwise orthogonal set. We also consider S-systems of n-ary quasigroups in the more natural sense, than the S-systems of T. Yakubov [10], and prove that such a finite S-system contains only one n-quasigroup, whereas S-systems of [10] do not at all exist.

2. Necessary notions and results

We recall some notations, concepts and results which are used in the article. At first remember the following notations from [2]. By x_i^j we will denote the sequence $x_i, x_{i+1}, \ldots, x_j$, $i \leqslant j$. If $j < i$, then x_i^j is the empty sequence, $\overline{1,n} = \{1, 2, \ldots, n\}$. Let Q be a finite or an infinite set, $n \geqslant 2$ be a positive integer and let Q^n denote the Cartesian power of the set Q.

An *n-ary operation* A (briefly, an *n-operation*) on a set Q is a mapping $A : Q^n \to Q$ defined by $A(x_1^n) \to x_{n+1}$, and in this case we write $A(x_1^n) = x_{n+1}$.

A *finite n-groupoid (Q, A) of order m* is a set Q with one n-ary operation A defined on Q, where $|Q| = m \geqslant 2$.

An *n-ary quasigroup (n-quasigroup)* is an n-groupoid such that in the equality

$$A(x_1^n) = x_{n+1}$$

every n elements from x_1^{n+1} uniquely define the $(n+1)$-th element. Usually a quasigroup n-operation A is itself considered as an n-quasigroup.

The n-operation E_k, $1 \leqslant k \leqslant n$, on a set Q with $E_k(x_1^n) = x_k$ is called the *k-th identity operation* (or the *k-th selector) of arity n*.

An n-operation A on Q is called *k-invertible* for some $k \in \overline{1,n}$ if the equation

$$A(a_1^{k-1}, x_k, a_{k+1}^n) = a_{n+1}$$

has a unique solution for each fixed n-tuple $(a_1^{k-1}, a_{k+1}^n, a_{n+1}) \in Q^n$.

For a k-invertible n-operation there exists the *k-inverse n-operation* ${}^{(k)}A$ defined in the following way:

$${}^{(k)}A(x_1^{k-1}, x_{n+1}, x_{k+1}^n) = x_k \Leftrightarrow A(x_1^n) = x_{n+1}$$

for all $x_1^{n+1} \in Q^{n+1}$.

It is evident that

$$A(x_1^{k-1}, {}^{(k)}A(x_1^n), x_{k+1}^n) = {}^{(k)}A(x_1^{k-1}, A(x_1^n), x_{k+1}^n) = x_k$$

and ${}^{(k)}[{}^{(k)}A] = A$ for $k \in \overline{1,n}$.

Let Ω_n be the set of all n-ary operations on a finite or an infinite set Q. On Ω_n define a binary operation $\underset{k}{\oplus}$ (the k-multiplication) in the following way:

$$(A \underset{k}{\oplus} B)(x_1^n) = A(x_1^{k-1}, B(x_1^n), x_{k+1}^n),$$

$A, B \in \Omega_n$, $x_1^n \in Q^n$. Shortly this equality can be written as

$$A \underset{k}{\oplus} B = A(E_1^{k-1}, B, E_{k+1}^n)$$

where E_k is the k-th selector.

In [11] it was proved that $(\Omega_n, \underset{k}{\oplus})$ is a semigroup with the identity E_k. If Λ_k is the set of all k-invertible n-operations from Ω_n for some $k \in \overline{1,n}$, then $(\Lambda_k, \underset{k}{\oplus})$ is a group. In this group E_k is the identity, the inverse element of A is the operation ${}^{(k)}A \in \Lambda_k$, since $A \underset{k}{\oplus} E_k = E_k \underset{k}{\oplus} A$, $A \underset{k}{\oplus} {}^{(k)}A = {}^{(k)}A \underset{k}{\oplus} A = E_k$.

An n-ary quasigroup (Q, A) (or simply A), is an n-groupoid with an k-invertible n-operation for each $k \in \overline{1,n}$ [2].

Let $(x_1^n)_k$ denote the $(n-1)$-tuple $(x_1^{k-1}, x_{k+1}^n) \in Q^{n-1}$ and let A be an n-operation, then the $(n-1)$-operation A_a:

$$A_a(x_1^n)_k = A(x_1^{k-1}, a, x_{k+1}^n)$$

is called the $(n-1)$-*retract* of A, defined by position k, $k \in \overline{1,n}$, with the element a in this position (with $x_k = a$).

If in an n-operation A we fix all positions except two positions k and l we obtain a binary operation $\overline{A}(x_k, x_l) = A(a_1^{k-1}, x_k, a_{k+1}^{l-1}, x_l, a_{l+1}^n)$ which is called a *binary retract* of A [2].

An n-ary operation A on Q is called *complete* if there exists a permutation $\overline{\varphi}$ of Q^n such that $A = E_1\overline{\varphi}$ (that is $A(x_1^n) = E_1\overline{\varphi}(x_1^n)$). If a complete n-operation A is finite and has order m, then the equation $A(x_1^n) = a$ has exactly m^{n-1} solutions for any $a \in Q$ [11].

Any k-invertible n-operation A, $k \in \overline{1,n}$, is complete, but there exist complete n-operations, which are not k-invertible for each $k \in \overline{1,n}$ [11].

Definition 1. (cf. [3]) Two n-ary operations ($n \geqslant 2$) A and B given on a set Q of order m are called *orthogonal* (shortly, $A \perp B$) if the system $\{A(x_1^n) = a, B(x_1^n) = b\}$ has exactly m^{n-2} solutions for any $a, b \in Q$.

A set $\Sigma = \{A_1^s\}$, $s \geqslant 2$, of n-operations is called *pairwise orthogonal* if each pair of distinct n-operations from Σ is orthogonal.

It is an algebraic analog of orthogonality of n-dimensional hypercubes which (just as n-operations and n-quasigroups) are used in various areas including affine and projective geometries, designs of experiments, error-correcting and error-detecting coding theory and cryptology.

In the article [7] a connection between n-dimensional hypercubes and n-ary operations and different types of their orthogonality were considered. The pairwise orthogonality is the weakest from these types.

In [3] the algebraic approach was first used for study of orthogonality of two n-dimensional hypercubes and the following criterion of orthogonality of two finite k-invertible n-operations was established.

Theorem 1. (cf. [3]) *Let k be a fixed number from $\overline{1,n}$. Two finite k-invertible n-operations A and B on a set Q are orthogonal if and only if the $(n-1)$-retract C_a of the n-operation $C = B \underset{k}{\oplus}^{(k)} A$, defined by $x_k = a$, is complete for every $a \in Q$.*

3. (k)-S-systems of n-quasigroups

For the n-ary case, $n \geqslant 2$, we introduce (k)-S-systems of n-quasigroups in the following way.

Definition 2. A system $Q(\Sigma_k)$, $\Sigma_k = \{E_k, A_1^s\}$, $s \geqslant 1$, where all A_i are n-quasigroups, given on a set Q, is called a (k)-*S-system of n-quasigroups* if $(\Sigma_k, \underset{k}{\oplus})$ is a group.

If $n = 2$ and $\Sigma_2 = \{E, A_1^s\}$ ($\Sigma_1 = \{F, A_1^s\}$) we obtain a right (left) S-system of binary quasigroups, since $\underset{2}{\oplus} = \cdot$ ($\underset{1}{\oplus} = \circ$) (the right and the left multiplications of binary operations respectively).

Examples of (k)-S-systems. Let $(Q, +)$ be an elementary abelian group (that is a group which is a direct power of a group of a prime order p [9]) of order $m = p^t$, $p \geqslant 3$, and an n-quasigroup (Q, A) has the form:

$$A(x_1^n) = \alpha_1 x_1 + \ldots + \alpha_{k-1} x_{k-1} + x_k + \alpha_{k+1} x_{k+1} + \ldots + \alpha_n x_n \qquad (1)$$

where all α_i are permutations of Q. Consider the (k)-powers $A, A^2, \ldots, A^{p-1}$, that is the powers of A with respect to the k-multiplication of n-operations: $A^l = A \underset{k}{\oplus} A \underset{k}{\oplus} \ldots \underset{k}{\oplus} A$ (l times) [4]. By Corollary 6 of [4] all these powers are n-quasigroups, $A^p = E_k$ and $(\Sigma'_k, \underset{k}{\oplus})$ where $\Sigma'_k = \{E_k, A, A^2, \ldots, A^{p-1}\}$ is a (cyclic) group. Hence, $Q(\Sigma'_k)$ is a (k)-S-systems of n-quasigroups.

Moreover, if $m = p \geqslant 3$ and in (1) α_i is the identity permutation for each $i \in \overline{1,n}$, that is

$$A(x_1^n) = x_1 + x_2 + \ldots + x_n, \tag{2}$$

then $Q(\Sigma'_k)$ is a (k)-S-system for any $k \in \overline{1,n}$.

Note, that n-quasigroups of Σ'_k can be different from n-quasigroups of Σ'_l, if $k \neq l$. So, it is easy to check that if an n-quasigroup A of order p has the form (2), then the sets Σ'_k and Σ'_l are intersected only by the n-quasigroup A.

Indeed, let $1 \leqslant k \leqslant l \leqslant n$ and the (k)-power A^r coincide with the (l)-power A^t for $1 \leqslant r < t \leqslant p-1$. Then

$$r(x_1+...+x_{k-1})+x_k+r(x_{k+1}+...+x_n) = t(x_1+...+x_{l-1})+x_l+t(x_{l+1}+...+x_n),$$

whence it follows that

$$(t-r)(x_1+\ldots+x_{k-1})+t(x_k+\ldots+x_{l-1})+x_l-x_k-r(x_{k+1}+\ldots+x_l)+$$

$$+(t-r)(x_{l+1}+\ldots+x_n)=0.$$

Setting $x_1 = \ldots = x_{k-1} = x_{k+1} = \ldots = x_{l-1} = x_{l+1} = \ldots = x_n = 0$, we obtain $tx_k - x_k = rx_l - x_l$ for all x_k, x_l of Q and so $t = r = 1$. □

Proposition 1. *Let $Q(\Sigma_k)$, $\Sigma_k = \{E_k, A_1^s\}$, be a (k)-S-system of n-quasigroups, $n \geqslant 3$, $1 \leqslant l < k \leqslant n$ and $u = a_1^{l-1}$, $v = a_{l+1}^{k-1}$, $w = a_{k+1}^n$ be fixed (ordered) tuples of elements from Q. Then the system $Q(\Sigma_{u,v,w})$ of binary retracts where $\Sigma_{u,v,w} = \{E, \overline{A}_1^s\}$ with $\overline{A}_i(x_l, x_k) = A_i(u, x_l, v, x_k, w)$, is a right S-system of binary quasigroups for any $u \in Q^{l-1}$, $v \in Q^{k-l-1}$, $w \in Q^{n-k}$.*

Proof. We must prove that $\Sigma_{u,v,w}$ is a group with respect to the right multiplication of binary operations. At first we note that $E_k(u, x_l, v, x_k, w) = \overline{E}_k(x_l, x_k) = x_k$, that is $\overline{E}_k = E$.

Let $A_i \in \Sigma_k$, then ${}^{(k)}A_i \in \Sigma_k$, $\overline{A}_i \in \Sigma_{u,v,w}$ and ${}^{(k)}\overline{A}_i \in \Sigma_{u,v,w}$. Prove that ${}^{(2)}\overline{A}_i \in \Sigma_{u,v,w}$. Indeed, from $(A_i \underset{k}{\oplus}^{(k)} A_i)(x_1^n) = x_k$ it follows

$$\begin{aligned}(A_i \underset{k}{\oplus}^{(k)} A_i)(u, x_l, v, x_k, w) &= A_i(u, x_l, v, {}^{(k)}A_i(u, x_l, v, x_k, w), w)\\ &= \overline{A}_i(x_l, {}^{(k)}\overline{A}_i(x_l, x_k)) = x_k.\end{aligned}$$

But $\overline{A}_i(x_l, {}^{(2)}\overline{A}_i(x_l, x_k)) = x_k$. Hence, ${}^{(k)}\overline{A}_i = {}^{(2)}\overline{A}_i$ and ${}^{(2)}\overline{A}_i \in \Sigma_{u,v,w}$.

Further, if $A_i \underset{k}{\oplus} A_j = A_r \in \Sigma_k$, then

$$\begin{aligned}(A_i \underset{k}{\oplus} A_j)(u, x_l, v, x_k, w) &= A_i(u, x_l, v, A_j(u, x_l, v, x_k, w), w)\\ &= \overline{A}_i(x_l, \overline{A}_j(x_l, x_k)) = (\overline{A}_i \cdot \overline{A}_j)(x_l, x_k)\\ &= A_r(u, x_l, v, x_k, w) = \overline{A}_r(x_l, x_k),\end{aligned}$$

that is $\overline{A}_i \cdot \overline{A}_j = \overline{A}_r \in \Sigma_{u,v,w}$.

It still remains to prove that $\overline{A}_i \neq \overline{A}_j$ if $i \neq j$. Let $\overline{A}_i = \overline{A}_j$, then $A_i(u, x_l, v, x_k, w) = A_j(u, x_l, v, x_k, w)$, ${}^{(k)}A_i(u, x_l, v, A_j(u, x_l, v, x_k, w), w) = x_k$. But $B = {}^{(k)} A_i \underset{k}{\oplus} A_j \in \Sigma_k$, so $B(u, x_l, v, x_k, w) = x_k$ for any $x_l \in Q$ implies that B is not an n-quasigroup, so $B = E_k$ and $i = j$.

Therefore, we proved that the set $\Sigma_{u,v,w}$ is a group with respect to the right multiplication of binary operations. □

Remark. If in Proposition 1 $k < l$, $u = a_1^{k-1}$, $v = a_{k+1}^{l-1}$, $w = a_{l+1}^n$, $\overline{A}_i(x_k, x_l) = A_i(u, x_k, v, x_l, w)$, then analogously one can prove that $\Sigma_{u,v,w} = = \{F, \overline{A}_1^s\}$ is a left S-system of binary quasigroups.

Theorem 2. *Let $n \geqslant 3$, k $(1 \leqslant k \leqslant n)$ be a fixed number, Q be a set of order m, $Q(\Sigma_k)$, $\Sigma_k = \{E_k, A_1^s\}$, be a (k)-S-system of n-quasigroups. Then Σ_k is a pairwise orthogonal set of n-operations and $s \leqslant m-1$.*

Proof. Let $A_i, A_j \in \Sigma_k$, $i \neq j$, then ${}^{(k)}A_j \in \Sigma_k$ and $A_i \underset{k}{\oplus} ({}^{(k)}A_j)$ is an n-quasigroup of Σ_k, so any $(n-1)$-retract of this n-quasigroup is an $(n-1)$-quasigroup which is always complete. By Theorem 1 $A_i \perp A_j$. Now it is evident that $A_i \perp E_k$, since $A_i \underset{k}{\oplus} E_k = A_i$ and ${}^{(k)}E_k = E_k$. Thus, Σ_k is a pairwise orthogonal set of n-operations.

But by Proposition 1 $Q(\Sigma_{u,v,w})$, where $\Sigma_{u,v,w} = \{E, \overline{A}_1^s\}$, is a right S-system of binary quasigroups which is an orthogonal set and can not contain more than $m-1$ binary quasigroups (latin squares) of order m [8], so $s \leqslant m-1$. □

Definition 3. A (k)-S-system $Q(\Sigma_k)$ with $\mid Q \mid = m$ is called *complete* if it contains $m-1$ n-quasigroups, that is if $\mid \Sigma_k \mid = m$.

Proposition 2. *For any $n \geqslant 3$ and any $k \in \overline{1,n}$ there exist complete (k)-S-systems of n-quasigroups of each prime order $p \geqslant 3$.*

Proof. Examples of such (k)-S-systems are the (cyclic) systems obtained with the help of n-quasigroups of the form (2) where $(Q,+)$ is a group of a prime order $p \geqslant 3$. □

Note that (cyclic) (k)-S-systems which are obtained from an n-quasigroup A of the form (1) are not complete if $m = p^t$, $t > 1$.

4. S-systems of n-quasigroups

In [10] n-ary S-systems were considered in the following sense.

Definition 4. (cf. [11]) A system $Q(\Sigma)$, $\Sigma = \{E_1^n, A_1^s\}$, $s \geqslant 1$, where A_i is an n-quasigroup for each $i \in \overline{1,s}$, $n \geqslant 2$, is called an *S-system of n-quasigroups* if Σ is closed with respect to the (Menger's) superposition: $C(B_1^n) = C(B_1, B_2, \ldots, B_n) \in \Sigma$ $(C(B_1^n)(x_1^n) = C(B_1(x_1^n), \ldots, B_n(x_1^n))$ for any $C, B_1, \ldots, B_n \in \Sigma$.

T. Yakubov in [10] proved that if $Q(\Sigma)$ is a finite (that is the set Q is finite) n-ary S-system in this sense, then $\Sigma_k = \{E_k, A_1^s\}$ is a group with respect to the k-multiplication of n-operations for each $k \in \overline{1,n}$. Using this fact and the definition of (k)-S-systems it is natural to define an S-system of n-ary quasigroups in the following way.

Definition 5. A system $Q(\Sigma)$, $\Sigma = \{E_1^n, A_1^s\}$, $s \geqslant 1$, $n \geqslant 2$, where all A_i are n-quasigroups is called an *S-system of n-quasigroups* if $\Sigma_k = \{E_k, A_1^s\}$ is a (k)-S-system for any $k \in \overline{1,n}$.

Proposition 3. *Let $Q(\Sigma)$, $\Sigma = \{E_1^n, A_1^s\}$, be an S-system of n-quasigroups, $n \geqslant 3$, $1 \leqslant p < q \leqslant n$ and $u = a_1^{p-1}$, $v = a_{p+1}^{q-1}$, $w = a_{q+1}^n$ be fixed (ordered) tuples of elements from Q. Then the system $Q(\Sigma_{u,v,w})$ of binary retracts where $\Sigma_{u,v,w} = \{E, F, \overline{A}_1^s\}$ with $\overline{A}_i(x_p, x_q) = A_i(u, x_p, v, x_q, w)$, is an S-system of binary quasigroups for any $u \in Q^{p-1}$, $v \in Q^{q-p-1}$, $w \in Q^{n-q}$.*

Proof. In this case $E_p(u, x_p, v, x_q, w) = x_p = F(x_p, x_q)$, $E_q(u, x_p, v, x_q, w) = x_q = E(x_p, x_q)$. From Definition 5 it follows that $\Sigma_k = \{E_k, A_1^s\}$ is a (k)-S-system for any $k \in \overline{1,n}$. If $k = q$, then by Proposition 1 $\Sigma_{u,v,w} = \{E, \overline{A}_1^s\}$

of binary retracts is a right S-system of binary quasigroups. On the other hand, if $k = p$, then $\Sigma'_{u,v,w} = \{F, \overline{A}_1^s\}$ for the same u, v, w is a left S-system of binary quasigroups (see Remark). Thus, $Q(\Sigma_{u,v,w})$ is an S-system of binary quasigroups. □

For the binary case Definition 4 and Definition 5 are equivalent (see Theorem 4.1 of [1]). We shall prove that when $n > 2$ it is not true. At first remind that an n-quasigroup (Q, A) is called an *n-TS- quasigroup* if its k-inverse n-quasigroups coincide with A for each $k \in \overline{1,n}$ (see [2]).

Theorem 3. *A finite system $Q(\Sigma)$, $\Sigma = \{E_1^n, A_1^s\}$, $n \geqslant 3$, is an S-system of n-quasigroups if and only if $s = 1$ and the n-quasigroup A_1 is an n-TS-quasigroup.*

Proof. By Proposition 3 the system $Q(\Sigma_{u,v,w})$ of binary retracts, where $\Sigma_{u,v,w} = \{F, E, \overline{A}_1^s\}$, $\overline{A}_i(x_p, x_q) = A_i(u, x_p, v, x_q, w)$, is an S-system of binary quasigroups. By Theorem 4.2 of [1] all operations of a finite S-system of binary quasigroups are idempotent if $s \geqslant 2$ (note that in [1] $s \geqslant 4$ since s designates the number of all operations in an S-system), that is $A_i(u, x, v, x, w) = \overline{A}_i(x, x) = x$ for every $x \in Q$. Now we use the idea of the proof from [10].

If $n = 3$, then $\overline{A}_i(a, a) = a$ and $A_i(a, a, w) = a$ (if, for example, $p = 1$, $q = 2$) for any w of Q. But it is impossible as A_i is a 3-quasigroup.

Let $n \geqslant 4$, $a \neq b$, the element a be in A_i in positions p, q $(p < q)$ and the element b is in positions r, t $(q < r < t)$, i.e., $A_i(\ldots, a, \ldots, a, \ldots, b, \ldots, b, \ldots)$. Fix tuples $u \in Q^{p-1}$, $v \in Q^{q-p-1}$, $w \in Q^{n-q}$ where in the tuple w the element b is in the positions r, t. Then for a binary quasigroup $\overline{A}_i$ of the system $\Sigma_{u,v,w}$ we have

$$\overline{A}_i(x_p, x_q) = A_i(u, x_p, v, x_q, w) = A_i(u, x_p, v, x_q, w_1, b, w_2, b, w_3),$$

if $w = (w_1, b, w_2, b, w_3)$, and

$$\overline{A}_i(a, a) = A_i(u, a, v, a, w) = A_i(u, a, v, a, w_1, b, w_2, b, w_3) = a. \qquad (3)$$

Now consider the system Σ_{u_1,w_2,w_3} with $u_1 = (u, a, v, a, w_1)$, then

$$\overline{\overline{A}}_i(x_r, x_t) = A_i(u_1, x_r, w_2, x_t, w_3),$$
$$\overline{\overline{A}}_i(b, b) = A_i(u, a, v, a, w_1, b, w_2, b, w_3) = b.$$

Taking into account the equality (3), we conclude that $a = b$. Thus, the case $s \geqslant 2$ for $n > 2$ is impossible.

It remains only the case $s = 1$. In this case the n-quasigroup A_1 coincides with all its inverse n-quasigroups, that is it is an n-TS-quasigroup. On the other hand, if an n-quasigroup A is an n-TS-quasigroup, then $A =^{(k)} A$ for any $k \in \overline{1,n}$, $A \underset{k}{\oplus} A = E_k$ and $\Sigma = \{E_1^n, A\}$ is an S-system. □

Unfortunately, such S-systems of n-quasigroups are trivial.

As an example of an n-TS-quasigroup can be the n-quasigroup of the form (2) where $(Q, +)$ is an (abelian) group of exponent two ($2x = 0$ for all $x \in Q$). Such group has order 2^t for some natural $t \geqslant 1$.

In [10] it was proved that finite S-systems of n-quasigroups in the sense of Definition 4 do not exist even for $s = 1$. Taking into account Theorem 3 we conclude that Definition 4 and Definition 5 are not equivalent for $n > 2$.

References

[1] **V. D. Belousov**: *Systems of quasigroups with generalized identities*, (Russian), Uspehi Matem. Nauk, vol. XX, I(121), (1965), 75 – 146.

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

[3] **G. B. Belyavskaya**: *Pairwise orthogonality of n-ary operations*, Bul. Acad. Sţi. Republ. Moldova, ser. Matematica **3(49)**, (2005), 5 – 18.

[4] **G. B. Belyavskaya**: *Power sets of n-ary quasigroups*, Bul. Acad. Sţi. Republ. Moldova, ser. Matematica (2007) (to appear).

[5] **G. B. Belyavskaya and A. M. Cheban**: *S-systems of an arbitrary index, I*, (Russian), Mat. Issled. **7** no. 1(23), (1972), 27 – 43.

[6] **G .B. Belyavskaya and A. M. Cheban**: *S-systems of an arbitrary index, II*, (Russian), Mat. Issled. **7** no. 2(24), (1972), 3 – 13.

[7] **G. B. Belyavskaya and G. L. Mullen**: *Orthogonal hypercubes and n-ary operations*, Quasigroups and Related Systems **13** (2005), 73 – 86.

[8] **J. Denés and A. D. Keedwell**: *Latin squares and their applications*, Budapest, Academiai Kiado, 1974.

[9] **A. I. Kostrikin**: *Introduction in algebra*, (Russian), Nauka, Moscow, 1977.

[10] **T. Yakubov**: *Research of n-ary operations*, (Russian), Ph. D. Thesis, Tashkent, 1974.

[11] **T. Yakubov**, *On $(2,n)$-semigroup of n-ary operations*, (Russian), Izv. AN MSSR., Ser. fiz.-teh. i mat. nauk **1** (1974), 29 – 46.

Received December 28, 2006

Institute of Mathematics and Computer Science
Academy of Sciences
Academiei str. 5
MD-2028 Chisinau
Moldova
E-mail: gbel@math.md

Quasigroups and Related Systems **15** (2007), 261 – 262

Double Ward quasigroups

Nick C. Fiala

Abstract

In this short note, we prove a one-to-one correspondence between groups and a variety of quasigroups that we call double Ward quasigroups analogous to the correspondence between groups and Ward quasigroups.

1. Introduction

A quasigroup consists of a non-empty set Q equipped with a binary operation $*$ such that for all $a, b \in Q$, there exist unique $x, y \in Q$ such that $a * x = b$ and $y * a = b$. Alternatively, a quasigroup is an algebra $(Q; *, \backslash, /)$ of type $(2, 2, 2)$ such that $x\backslash(x * y) = y$, $(x * y)/y = x$, $x * (x\backslash y) = y$, and $(x/y) * y = x$.

Given a group $(G; \circ, ^{-1}, e)$, we can construct a quasigroup by defining $x * y = x \circ y^{-1}$. The operation $*$ on G is sometimes referred to as *right division* in G. Clearly, this quasigroup satisfies the identity $(x*z)*(y*z) = x * y$. Quasigroups satisfying the above identity are referred to as *Ward quasigroups*. Conversely, given a Ward quasigroup Q, it can be shown that Q is *unipotent* $(x * x = y * y)$, so we may write $x * x = e$, and defining $x^{-1} = e * x$ and $x \circ y = x * y^{-1}$ makes $(Q; \circ, ^{-1}, e)$ a group. Writing $W(G)$ for the Ward quasigroup constructed from the group G and $Gr(Q)$ for the group constructed from the Ward quasigroup Q, it can also be shown that $Gr(W(G)) = G$ and $W(Gr(Q)) = Q$. Therefore, there is a one-to-one correspondence between groups and Ward quasigroups. This seems to have first been noticed in [1] and [3].

Similarly, given a group $(G; \circ, ^{-1}, e)$, we can construct a quasigroup by defining $x * y = x^{-1} \circ y^{-1}$. The operation $*$ on G is sometimes referred to as *double division* in G. Clearly, this quasigroup satisfies the Ward-like identity

2000 Mathematics Subject Classification: 20N05
Keywords: group, right division, double division, Ward quasigroup, double Ward quasigroup, automated reasoning

$((e*e)*(x*z))*((e*y)*z) = x*y$. For lack of a better term, we will refer to quasigroups with an element e that satisfy the above identity as *double Ward quasigroups* (not to be confused with the Ward double quasigroups of [4]). In this short note, we prove an analogous one-to-one correspondence between groups and double Ward quasigroups.

Remark 1.1. The author gratefully acknowledges the assistance of the automated theorem-prover Prover9 [2]. Theorem 2.2 was found and proved with the aid of Prover9. As such, the proof has been suppressed. However, the proof is available from the author or can quickly be regenerated with Prover9.

2. Results

Theorem 2.2. *Let Q be a double Ward quasigroup. Define $x^{-1} = e*x$ and $x \circ y = x^{-1} * y^{-1}$. Then $(Q; \circ, ^{-1}, e)$ is a group.*

Theorem 2.3. *Let G be a group and let Q be a double Ward quasigroup. Denote by $DW(G)$ the double Ward quasigroup constructed from G and denote by $Gr(Q)$ the group constructed from Q. Then $Gr(DW(G)) = G$ and $DW(Gr(Q)) = Q$.*

Problem 2.4. Characterize double Ward quasigroups by a shorter more appealing identity such as is the case for Ward quasigroups.

Problem 2.5. Prove similar results for other well-known varieties of loops with two-sided inverses, such as (left, right) inverse property loops, anti-automorphic inverse property loops, extra loops, Moufang loops, left (right) Bol loops, C-loops, LC-loops, RC-loops, and flexible loops.

References

[1] **S. K. Chatterjea**: *On Ward quasigroups*, Pure Math. Manuscript **6** (1987), 31 – 34.

[2] **W. McCune**: *Prover9* (`http://www.cs.unm.edu/~mccune/prover9/`).

[3] **M. Polonijo**: *A note on Ward quasigroups*, An. Ştiinţ. Univ. Al. I. Cuza Iaşi Secţ. I a Mat. **32** (1986), 5 – 10.

[4] **M. Polonijo**: *Ward double quasigroups*, in: Proc. Confer. "Algebra and Logic", Cetinje 1986, 153 – 156, Univ. Novi Sad, Novi Sad, 1987.

Received November 30, 2006

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

Quasigroups and Related Systems **15** (2007), 263 – 271

Short identities implying a quasigroup is a loop or group

Nick C. Fiala

Abstract

In this note, we find all identities in product only with at most six variable occurrences that imply that a quasigroup satisfying the identity is a not necessarily trivial loop (group). These investigations were aided by the automated theorem-prover Prover9 and the model-finder Mace4.

1. Introduction

A *quasigroup* consists of a non-empty set Q equipped with a binary operation, which we simply denote by juxtaposition, such that for all $a, b \in Q$, there exist unique $x, y \in Q$ such that $ax = b$ and $ya = b$. Quasigroups are of interest not only in algebra but in combinatorics as well. Alternatively, we may define quasigroups equationally as algebras $(Q; \cdot, \backslash, /)$ of type $(2, 2, 2)$ such that $x\backslash(x \cdot y) = y$, $(x \cdot y)/y = x$, $x \cdot (x\backslash y) = y$, and $(x/y) \cdot y = x$.

A quasigroup is *trivial* if it consists of a single element. A quasigroup Q is a *left* (*right*) *loop* if there exists a *left* (*right*) *neutral element* $e \in Q$ such that $ex = x$ ($xe = x$) for all $x \in Q$. A *loop* is a quasigroup that is both a left loop and a right loop.

Henceforth, e will always denote the (left, right) neutral element of a (left, right) loop and the variables x, y, and z will always be universally quantified over the elements of a quasigroup.

Definition 1.1. We say that an identity *implies that a quasigroup is a* (*left, right*) *loop* (*group*) if and only if all quasigroups satisfying the identity are (left, right) loops (groups). Furthermore, if there exists a non-trivial (left, right) loop (group) satisfying the identity, then we say that the identity *implies that a quasigroup is a not necessarily trivial* (*left, right*) *loop* (*group*).

2000 Mathematics Subject Classification: 20N05
Keywords: quasigroup, loop, group, automated reasoning

In [1], Belousov raised the problem of determining which identities imply that a quasigroup is a loop. It is well-known that an associative quasigroup is a loop, and therefore a group. In [5], it is shown that each of the four *Moufang identities*

$$(x(yz))x = (xy)(zx) \quad (xz)(yx) = x((zy)x)$$
$$((xy)z)y = x(y(zy)) \quad ((yz)y)x = y(z(yx))$$

imply that a quasigroup is a loop, but not necessarily a group. More generally, in [6], Kunen considers *weak associative laws* (identities, other than associativity, for which the left-hand side and right-hand side are different associations of the same word) that imply that a quasigroup is a loop. In particular, he completely settles the problem for the identities of *Bol-Moufang type* (weak associative laws with three distinct variables and eight variable occurrences). Similarly, one may ask which identities imply that a quasigroup is a group. This question was settled for the identities of Bol-Moufang type in [11].

In this note, we endeavor to find all identities in product only with at most six variable occurrences that imply that a quasigroup is a not necessarily trivial loop (group). Perhaps some interesting identities will arise. The author hopes that this note will be of some use as a sort of beginner's tutorial on the use of automated reasoning in equational logic in general and on the powerful software Prover9 and Mace4 in particular. As such, a great deal of detail is shown and many examples and references are given.

2. Prover9 and Mace4

In this section, we briefly describe the software Prover9 and Mace4.

Prover9 [10] is a resolution-style [2], [13] automated theorem-prover for first-order logic with equality that was developed by McCune. Prover9 is the successor to the well-known OTTER [8] theorem-prover and, like OTTER, utilizes the *set of support strategy* [2], [14].

The language of Prover9 is the language of *clauses*, a clause being a disjunction of (possible one or zero) literals in which all variables whose names begin with u, v, w, x, y, or z are implicitly universally quantified and all other symbols represent constants, functions, or predicates (relations). An axiom may also be given to Prover9 as an explicitly quantified first-order formula which is immediately transformed by Prover9 into a set of

clauses by a *Skolemization* [2], [3] procedure. The conjunction of these clauses is not necessarily logically equivalent to the formula, but they will be *equisatisfiable* (one is satisfiable if and only if the other is as well) [2], [3]. Therefore, the set of clauses can be used by Prover9 in place of the formula in proofs by contradiction.

Prover9 can be asked to prove a potential theorem by giving it clauses or formulas expressing the hypotheses and a clause or formula expressing the negation of the conclusion. Prover9 finds a proof when it derives the *empty clause*, a contradiction. Prover9 can also be used for *question answering* through the use of *answer literals* [2], [4], [7].

Prover9 has an *autonomous mode* [10] in which all inference rules, settings, and parameters are automatically set based upon a syntactic analysis of the input clauses. The mechanisms of inference for purely equational problems are *paramodulation* and *demodulation*, a restricted from of paramodulation [2], [12]. Paramodulation *from* an equation i *into* an equation j is accomplished as follows: *unify* the left-hand side l of i with a subterm s of j by finding a substitution into the variables of l and s that make them identical (a *most general unifier*), instantiate j with the corresponding substitution, and infer the equation obtained by replacing s in j with the corresponding instance of the right-hand side of i.

One very important parameter used by Prover9 is the *maximum weight* [10] of a clause. By default, the weight of a literal is the number of occurrences of constants, variables, functions, and predicates in the literal and the weight of a clause is the sum of the weights of its literals. Prover9 discards derived clauses whose weight exceeds the maximum weight specified. By specifying a maximum weight, we sacrifice *refutation-completeness* (the guarantee of the existence of a derivation of the empty clause from a non-satisfiable set of clauses) [2], [13], although in practice it is frequently necessary in order to control the size of the clause space while searching for a proof. We will use the autonomous mode throughout this paper, sometimes overriding Prover9's assignment to the maximum weight parameter.

A useful companion to Prover9 is Mace4 [9], also developed by McCune. Mace4 is a finite first-order model-finder. With possibly some minor modifications, the same input can be given to Mace4 as to Prover9, Prover9 searching for a proof by contradiction and Mace4 searching for counterexamples of specified sizes (a structure of size n with a single binary operation found by Mace4 would be returned as an $n \times n$ Cayley table with the elements of the structure assumed to be $0, 1, \ldots, n-1$ and the element in

the ith row and jth column being ij).

Remark 2.1. The reader should note that Mace4 interprets non-negative integers as *distinct* constants and other constants as not necessarily distinct unless otherwise stated. This is in contrast to Prover9 which interprets all constants as not necessarily distinct unless otherwise stated. The use of non-negative integers for constants in Mace4 can have the advantage of speeding up the search for a model.

The scripting language Perl was also used to further automate the process.

3. The Search

In this section, we describe our search for identities in product only with at most six variable occurrences that imply that a quasigroup is a not necessarily trivial loop. Clearly, we need not consider identities with more than three distinct variables.

First, all identities in product only with at most three distinct variables and at most six variable occurrences with different left-hand side and right-hand side were generated up to renaming, canceling, mirroring, and symmetry. This resulted in 1353 identities.

Next, we sent each identity (stored in the Perl variable `$identity`) to Prover9 and ran

```
set(auto).                  % autonomous mode
assign(max_seconds, 1).     % one second time limit
                            % per identity
op(500, infix, [/, *, \]).  % quasigroup operations
clauses(sos).               % set of support clauses
x \ (x * y) = y.
(x * y) / y = x.
x * (x \ y) = y.
(x / y) * y = x.            % quasigroup
e * x = x.
x * e = x.                  % loop
$identity.                  % candidate identity
a != e.                     % non-trivial
end_of_list.                % end of set of support clauses
```

to search for a proof that a loop satisfying the identity must be trivial. Any identity for which a proof was found was eliminated. This resulted in 332 identities.

Remark 3.1. We determine whether or not Prover9 has found a proof by observing its exit status. Prover9 outputs an exit code of 0 if and only if it finds a proof.

We then sent each remaining identity to Mace4 and ran

```
assign(max_seconds, 60).                    % one minute time limit
                                            % per identity
op(500, infix, [/, *, \]).                  % quasigroup operations
clauses(theory).                            % theory clauses
x \ (x * y) = y.
(x * y) / y = x.
x * (x \ y) = y.
(x / y) * y = x.                            % quasigroup
$identity.                                  % candidate identity
end_of_list.                                % end of theory clauses
formulas(theory).                           % theory formulas
-(exists e all x (e * x = x & x * e = x)).  % not a loop
end_of_list.                                % end of
                                            % theory formulas
```

to search for a non-loop quasigroup of size at most 200 (this is simply Mace4's upper limit and is specified on the command line with `-n2 -N200` or just `-N200`) that satisfies the identity. Any identity for which an example was found was eliminated. This resulted in 35 identities. For example, the identity

$$x(((yx)z)y) = z$$

was eliminated since it is valid in the non-loop quasigroup below.

```
* :
     | 0 1 2 3 4 5 6 7
   --+----------------
   0 | 1 6 4 3 5 0 7 2
   1 | 3 2 5 1 4 7 0 6
   2 | 0 4 6 7 2 1 3 5
   3 | 5 7 3 4 1 2 6 0
   4 | 2 3 7 6 0 5 4 1
   5 | 7 5 2 0 6 3 1 4
   6 | 6 1 0 2 7 4 5 3
   7 | 4 0 1 5 3 6 2 7
```

Remark 3.2. We determine whether or not Mace4 has found a model by observing its exit status. Mace4 outputs an exit code of 0 if and only if it finds a model.

Next, we sent each remaining identity to Prover9 and ran

```
set(auto).                          % autonomous mode
assign(max_seconds, 60).            % one minute time limit
                                    % per weight per identity
assign(max_weight, $max_weight).    % maximum clause weight
op(500, infix, [/, *, \]).          % quasigroup operations
clauses(sos).                       % set of support clauses
x \ (x * y) = y.
(x * y) / y = x.
x * (x \ y) = y.
(x / y) * y = x.                    % quasigroup
$identity.                          % candidate identity
x * f(x) != f(x) # answer(x).       % not a left loop
end_of_list.                        % end of
                                    % set of support clauses
```

to search for a proof that the identity implies that a quasigroup is a left loop. We have *Skolemized* [2], [3] the negation of $(\exists e)(\forall x)(ex = x)$ to obtain the clause `x * f(x) != f(x)`, where `f` is a *Skolem function* [2], [3]. We use the answer literal `answer(x)` to obtain an expression for the left neutral element for the identities for which we find a proof (this information could also be extracted from the proof itself, although this is not always so easy to do and does not lend itself to automating). We always make a run for every value of the Perl variable `$max_weight` from 20 to 100 in steps of 10. A proof was found for all 35 identities. For example, Prover9 found the following proof that the identity

$$(xy)(x(zy)) = z$$

implies that a quasigroup is a left loop.

```
-------- PROOF --------
Length of proof is 31.
Level of proof is 13.
Maximum clause weight is 11.
7 x \ (x * y) = y.  [input]
8 (x * y) / y = x.  [input]
9 x * (x \ y) = y.  [input]
10 (x / y) * y = x.  [input]
11 (x * y) * (x * (z * y)) = z.  [input]
12 x * f(x) != f(x) # answer(x).  [input]
13 x / (y \ x) = y.  [para (9 (a 1) 8 (a 1 1))]
14 (x / y) \ x = y.  [para (10 (a 1) 7 (a 1 2))]
15 (x * y) \ z = x * (z * y).  [para (11 (a 1) 7 (a 1 2))]
16 x / (y * (x * z)) = y * z.  [para (11 (a 1) 8 (a 1 1))]
17 x * (y * (z * (y \ x))) = z.  [para (9 (a 1) 11 (a 1 1))]
19 x * ((x / y) * (z * y)) = z.  [para (10 (a 1) 11 (a 1 1))]
```

```
26 x \ y = z * (y * (z \ x)).  [para (9 (a 1) 15 (a 1 1))]
29 x / (y * z) = y * (x \ z).  [para (9 (a 1) 16 (a 1 2 2))]
34 x / (x * y) = y.  [back_demod 9 demod (29 (R))]
35 x / (y \ z) = z * (y * x).  [para (10 (a 1) 17 (a 1 2 2)) flip a]
41 x * (y * x) = y.  [back_demod 13 demod (35)]
43 (x * y) / z = x * (z * y).  [para (11 (a 1) 34 (a 1 2))]
44 x \ y = y * x.  [para (34 (a 1) 14 (a 1 1))]
45 x / y = z * (y * (x * z)).  [para (17 (a 1) 34 (a 1 2)) demod (44)]
47 x * (y * y) = x.  [back_demod 8 demod (43)]
52 x / (y * z) = y * (z * x).  [back_demod 35 demod (44)]
55 x * (y * (z * x)) = y * z.  [back_demod 26 demod (44 44) flip a]
62 x / y = y * x.  [back_demod 45 demod (55)]
68 (x * y) * z = x * (y * z).  [back_demod 52 demod (62)]
71 x * (x * y) = y.  [back_demod 19 demod (62 68 55)]
75 x * x = y * y.  [para (47 (a 1) 71 (a 1 2))]
76 x * x = c0.  [new_symbol 75]
77 x * c0 = x.  [back_demod 47 demod (76)]
80 c0 * x = x.  [para (77 (a 1) 41 (a 1 2))]
81 $F # answer(c0).  [resolve (80 a 12 a)]
-------- end of proof  -------
```

Furthermore, lines 76 and 81 show that $xx = e$. The interested reader should consult [10] for information on how to read such computer-generated proofs.

We then sent each of these 35 identities, along with the corresponding expression for the left neutral element (stored in the Perl variable `$left_neutral`), to Prover9 and ran

```
set(auto).                          % autonomous mode
assign(max_seconds, 60).            % one minute time limit
                                    % per weight per identity
assign(max_weight, $max_weight).    % maximum clause weight
op(500, infix, [/, *, \]).          % quasigroup operations
clauses(sos).                       % set of support clauses
x \ (x * y) = y.
(x * y) / y = x.
x * (x \ y) = y.
(x / y) * y = x.                    % quasigroup
e * x = x.                          % left loop
$left_neutral = e.                  % might help Prover9
$identity.                          % candidate identity
a * e != a.                         % not a right loop
end_of_list.                        % end of set of support clauses
```

to search for a proof that the identity implies that a quasigroup is a right loop (if `$left_neutral` contains the Skolem function `f`, then we omit the line `$left_neutral = e.`). A proof was found for all 35 identities.

Finally, we sent each of these 35 identities to Mace4 and ran

```
assign(max_seconds, 60).    % one minute time limit per identity
op(500, infix, [/, *, \]).  % quasigroup operations
clauses(theory).            % theory clauses
x \ (x * y) = y.
(x * y) / y = x.
x * (x \ y) = y.
(x / y) * y = x.            % quasigroup
0 * x = x.
x * 0 = x.                  % loop
$identity.                  % candidate identity
end_of_list.                % end of theory clauses
```

to search for a non-trivial loop that satisfies the identity. An example was found for all 35 identities.

4. Conclusion

In this final section, we state our main results.

Theorem 4.1. *There are exactly* 35 *identities in product only with at most six variable occurrences that imply that a quasigroup is a not necessarily trivial loop* (*up to renaming, canceling, mirroring, and symmetry*). *These* 35 *identities are shown below.*

$(xx)y = x(yx)$	$x(x((yy)z)) = z$	$(xx)(y(yz)) = z$	$(x(x(yy)))z = z$
$((x(xy))y)z = z$	$(xx)y = z(yz)$	$x(((xy)z)y) = z$	$(xx)(y(zy)) = z$
$((xx)(yz))y = z$	$x(xy) = (zz)y$	$((xx)y)z = zy$	$x(y(xy)) = zz$
$x((yx)y) = zz$	$x(y((xy)z)) = z$	$x((yx)(yz)) = z$	$(xy)(x(yz)) = z$
$(x(y(xy)))z = z$	$((x(yx))y)z = z$	$x((yx)z) = yz$	$(xy)(x(zy)) = z$
$((xy)(xz))y = z$	$x(y(xz)) = zy$	$x((yy)(xz)) = z$	$(x(y(yx)))z = z$
$((x(yy))x)z = z$	$(xy)(yz) = xz$	$x(((yy)z)x) = z$	$x((yy)z) = zx$
$x(yz) = (xy)z$	$x(y(zx)) = yz$	$(xy)(zx) = yz$	$x(yz) = (xz)y$
$(xy)(zx) = zy$	$x(yz) = y(zx)$	$(xy)z = y(zx)$	

Similarly, one can prove the following.

Theorem 4.2. *There are exactly* 16 *identities in product only with at most six variable occurrences that imply that a quasigroup is a not necessarily trivial group* (*up to renaming, canceling, mirroring, and symmetry*). *These* 16 *identities are shown below.*

$x(((xy)z)y) = z$	$x(y((xy)z)) = z$	$x((yx)(yz)) = z$	$(xy)(x(yz)) = z$
$x((yx)z) = yz$	$(xy)(x(zy)) = z$	$((xy)(xz))y = z$	$x(y(xz)) = zy$
$(xy)(yz) = xz$	$x(yz) = (xy)z$	$x(y(zx)) = yz$	$(xy)(zx) = yz$
$x(yz) = (xz)y$	$(xy)(zx) = zy$	$x(yz) = y(zx)$	$(xy)z = y(zx)$

References

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

[2] **C. Chang and R. Lee**: *Symbolic Logic and Mechanical Theorem Proving*, Academic Press, San Diego, CA, 1973.

[3] **M. Davis and H. Putnam**: *A computing procedure for quantification theory*, J. Assoc. Comput. Mach. **7** (1960), 201–215.

[4] **C. Green**: *Proving by resolution as a basis for question-answering systems*, in: Machine Intelligence Vol. 4, Elsevier, New York, 1969, 183–205.

[5] **K. Kunen**: *Moufang quasigroups*, J. Algebra **183** (1996), 231–234.

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

[7] **K. Kunen**: *The semantics of answer literals*, J. Automat. Reason. **17** (1996), 83–95.

[8] **W. McCune**: *OTTER* (`http://www.cs.unm.edu/~mccune/otter/`).

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

[10] **W. McCune**: *Prover9* (`http://www.cs.unm.edu/~mccune/prover9/`).

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

[12] **G. A. Robinson and L. Wos**: *Paramodulation and theorem-proving in first-order theories with equality*, in: Machine Intelligence Vol. 4, Elsevier, New York, 1969, 135–150.

[13] **J. A. Robinson**: *A machine-oriented logic based on the resolution principle*, J. Assoc. Comput. Mach. **12** (1965), 23–41.

[14] **L. Wos, G. A. Robinson and D. F. Carson**: *Efficiency and completeness of the set of support strategy in theorem proving*, J. Assoc. Comput. Mach. **12** (1965), 536–541.

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

Received November 30, 2006
Revised February 7, 2007

Quasigroups and Related Systems **15** (2007), 273 – 278

Biembeddings of Latin squares of side 8

Mike J. Grannell, Terry S. Griggs and Martin Knor

Abstract

Face 2-colourable triangular embeddings of complete tripartite graphs $K_{n,n,n}$ correspond to biembeddings of Latin squares of side n. We consider biembeddings that contain any of the five Latin squares derived from the Cayley tables of finite groups of order 8. Up to isomorphism, we determine all such biembeddings.

1. Background

In our paper [1] we discuss, in some detail, face 2-colourable topological embeddings of complete regular tripartite graphs $K_{n,n,n}$ in which all faces are triangular. Such embeddings are equivalent to biembeddings of Latin squares of side n and, as proved in [1], the supporting surfaces are necessarily orientable. Up to isomorphism, this earlier paper gives all such biembeddings for $n = 3, 4, 5$ and 6, and it summarizes the results for $n = 7$. For $n = 4, 5$ and 6, there are Latin squares which do not appear in any biembedding. Another interesting feature is the partitioning of the 147 main classes of Latin squares of side 7 into sub-classes of sizes 1, 1, 1, 2, 3, 3, 3, 6, 6, 8, 8, 9, 18, 19, 26 and 33, such that within each sub-class most of the squares biembed with one another, but there are no biembeddings of two squares taken from different sub-classes. We refer the reader to [1] for details of this and for items of terminology.

In the current paper we turn our attention to Latin squares of side 8, where there are 283 657 main classes [3]. It is computationally infeasible to determine all possible biembeddings of these squares and here we restrict

2000 Mathematics Subject Classifications: 05B15, 05C10.
Keywords: Topological embedding, Latin square, complete tripartite graph.
M.Knor acknowledges partial support by Slovak research grants VEGA 1/2004/05, APVT-20-000704 and APVV-0040-06.

ourselves to seeking biembeddings that contain at least one of those squares that arise from the Cayley tables of groups of order 8. Another reason for considering these particular squares is that, whilst squares which arise from the Cayley tables of cyclic groups always appear in biembeddings, those from the groups $C_2 \times C_2$ and D_3 do not. It is therefore appropriate to consider the Cayley tables of the groups of order 8. There are five such groups, usually denoted by $C_2^3 = C_2 \times C_2 \times C_2$, $C_4 \times C_2$, C_8, D_4 and Q. Here C_n denotes the cyclic group of order n, D_n is the dihedral group of order $2n$, and Q is the quaternion group. We take the corresponding Latin squares as shown in Table 1.

0	1	2	3	4	5	6	7
1	0	4	5	2	3	7	6
2	4	0	6	1	7	3	5
3	5	6	0	7	1	2	4
4	2	1	7	0	6	5	3
5	3	7	1	6	0	4	2
6	7	3	2	5	4	0	1
7	6	5	4	3	2	1	0

C_2^3

0	1	2	3	4	5	6	7
1	2	3	0	5	6	7	4
2	3	0	1	6	7	4	5
3	0	1	2	7	4	5	6
4	5	6	7	0	1	2	3
5	6	7	4	1	2	3	0
6	7	4	5	2	3	0	1
7	4	5	6	3	0	1	2

$C_4 \times C_2$

0	1	2	3	4	5	6	7
1	2	3	4	5	6	7	0
2	3	4	5	6	7	0	1
3	4	5	6	7	0	1	2
4	5	6	7	0	1	2	3
5	6	7	0	1	2	3	4
6	7	0	1	2	3	4	5
7	0	1	2	3	4	5	6

C_8

0	1	2	3	4	5	6	7
1	2	3	0	5	6	7	4
2	3	0	1	6	7	4	5
3	0	1	2	7	4	5	6
4	7	6	5	0	3	2	1
5	4	7	6	1	0	3	2
6	5	4	7	2	1	0	3
7	6	5	4	3	2	1	0

D_4

0	1	2	3	4	5	6	7
1	0	3	2	5	4	7	6
2	3	1	0	6	7	5	4
3	2	0	1	7	6	4	5
4	5	7	6	1	0	2	3
5	4	6	7	0	1	3	2
6	7	4	5	3	2	1	0
7	6	5	4	2	3	0	1

Q

Table 1. Group-based squares of side 8.

2. Results

There are 3 167 nonisomorphic biembeddings that contain at least one of the five group-based squares of side 8. Table 2 gives a breakdown of these by the individual squares and the size of the automorphism group Γ of the biembedding. The column sums given in the last line of the table exclude

duplications arising from biembeddings that contain a pair of group-based squares.

$\lvert\Gamma\rvert$	1	2	3	4	6	8	12	16	> 16	$\sum$
C_2^3	23	6	4	6	–	2	2	5	1	49
$C_4 \times C_2$	1 750	126	19	55	–	7	5	2	–	1 964
C_8	568	54	60	–	6	–	1	1	11	701
D_4	159	37	18	5	–	3	–	5	–	227
Q	183	16	20	12	–	2	2	1	–	236
$\sum$	2 683	235	120	75	6	14	10	12	12	3 167

Table 2. Biembeddings containing a group-based square.

As regards the biembeddings whose groups of automorphisms have orders greater than 16, there is one of C_2^3 with 48 automorphisms, while C_8 has one with 24 automorphisms (forming S_4), four with 32 automorphisms, one with 64 automorphisms, two with 128 automorphisms, one with 192 automorphisms, one with 256 automorphisms and one with 768 automorphisms. This last biembedding, which is of C_8 with a copy of itself, is the unique regular triangular embedding of $K_{8,8,8}$ in an orientable surface (see [1] and [2] for details). The biembedding of C_2^3 with an automorphism group of order 48 is with a non group-based Latin square, but all 11 biembeddings of C_8 are with copies of itself.

The method for obtaining these biembeddings was to select one of the five group-based squares and to regard its triples of row, column and entry symbols as triangles with the common clockwise orientation (row, column, entry). In any biembedding containing this Latin square, the rotation about each point contains 8 known ordered pairs; what remains unknown is the ordering of these pairs. By considering all possible orderings and rejecting those which give rise to pseudosurfaces, all biembeddings containing the given square may be determined. Working through the five squares, each new biembedding was checked for isomorphism with those found previously. The large number of biembeddings to be checked required the use of an effective invariant in order to establish the isomorphism classes. The invariant used was as follows.

Consider a fixed biembedding of Latin squares of side 8. Denote by ρ_z the rotation around a vertex z. Since ρ_z is a cyclic permutation of order 16,

for each two neighbours x and y of z there are integers m_1 and m_2 such that $y = \rho_z^{m_1}(x)$ and $y = \rho_z^{-m_2}(x)$, where $1 \leqslant m_1, m_2 \leqslant 15$ and $m_1 + m_2 = 16$. Put

$$d(z; x, y) = \min\{m_1, m_2\}.$$

Now if $d(z; x, v) = d(z; v, y) = 1$, and $x \neq y$, then $d(v; x, y) = 2$. However if $d(z; x, v) = d(z; v, y) = 3$, and $x \neq y$, then $d(v; x, y)$ can be any even number from 2 to 8. (Note we cannot use $d(z; x, v) = d(z; v, y) = 2$ because then v is not adjacent to either x or y, being in the same vertex partition set.) Let I_v be the sum of the 16 numbers given by the formula

$$I_v = \sum_{vz \in E(G)} (d(v; x, y) : \text{where } d(z; x, v) = d(z; v, y) = 3 \text{ and } x \neq y).$$

Now the multiset of 24 elements I_v, together with the number of automorphisms, forms a satisfactory invariant for our biembeddings. There is just one pair of biembeddings for $C_4 \times C_2$ and two pairs for C_8, which represent nonisomorphic biembeddings, although their invariants coincide.

Up to isomorphism, there are 23 biembeddings where *both* the Latin squares are group-based. In Table 3, in each of these cases, we specify a representative biembedding from the isomorphism class by means of a vector (A, B, p_1, p_2, p_3) where A, B identify the two squares as in Table 1, and p_1, p_2, p_3 specify permutations applied respectively to the rows, columns and entries of the second square. From these, the biembedding may be constructed by taking the two squares exactly as in Table 1 and then applying the permutations to the second square, finally sewing the resulting triangular faces together along their common edges. A permutation entry such as $p_1 = 31267405$ is to be read as the permutation $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 6 & 7 & 4 & 0 & 5 \end{pmatrix}$, indicating that row 0 of the square from Table 1 is placed in row 3, row 3 is placed in row 6, and so on. We use I to denote the identity permutation. In no case do we need to permute rows, columns and entries with each other. We also give information about the automorphism group Γ of each biembedding with a second vector $(M; m_1, m_2, m_3, m_4)$ denoting that $|\Gamma| = M$ and that there are m_1 mappings which preserve orientation and colour classes, m_2 mappings which preserve orientation and reverse the colour classes, m_3 mappings which reverse orientation and preserve the colour classes, and m_4 mappings which reverse orientation and reverse the colour classes.

1. $(C_2^3, D_4, 31267405, 45203617, 35061427)$, $(3; 3, 0, 0, 0)$,
2. $(C_4 \times C_2, D_4, 64752103, 32104567, 21034567)$, $(16; 8, 0, 8, 0)$,
3. $(C_4 \times C_2, D_4, 53261407, 61204357, 41263057)$, $(4; 2, 0, 2, 0)$,
4. $(C_4 \times C_2, D_4, 51302647, 61250347, 40351267)$, $(2; 2, 0, 0, 0)$,
5. $(C_4 \times C_2, D_4, 24673105, 12306547, 23561047)$, $(2; 2, 0, 0, 0)$,
6. $(C_4 \times C_2, Q, 54670213, 13024657, 20134657)$, $(16; 8, 0, 8, 0)$,
7. $(C_4 \times C_2, Q, 53601472, 64310257, 03152647)$, $(4; 2, 0, 2, 0)$,
8. $(C_4 \times C_2, Q, 24601573, 64210357, 13254607)$, $(4; 2, 0, 2, 0)$,
9. $(C_4 \times C_2, Q, 21706354, 53420617, 20134657)$, $(2; 2, 0, 0, 0)$,
10. $(C_4 \times C_2, Q, 54601273, 64310257, 14253607)$, $(2; 2, 0, 0, 0)$,
11. $(C_8, C_8, 12345670, I, I)$, $(768; 192, 192, 192, 192)$, regular,
12. $(C_8, C_8, 52741630, I, I)$, $(256; 64, 64, 64, 64)$,
13. $(C_8, C_8, 56341270, 05634127, 45230167)$, $(192; 48, 48, 48, 48)$,
14. $(C_8, C_8, 16745230, I, I)$, $(128; 32, 32, 32, 32)$,
15. $(C_8, C_8, 52741630, I, 45230167)$, $(128; 32, 32, 32, 32)$,
16. $(C_8, C_8, 52741630, 05634127, 45230167)$, $(64; 16, 16, 16, 16)$,
17. $(C_8, C_8, 12367450, I, I)$, $(32; 8, 8, 8, 8)$,
18. $(C_8, C_8, 14763250, I, I)$, $(32; 8, 8, 8, 8)$,
19. $(C_8, C_8, 12547630, I, I)$, $(32; 8, 8, 8, 8)$,
20. $(C_8, C_8, 16347250, I, I)$, $(32; 8, 8, 8, 8)$,
21. $(C_8, C_8, 16345270, 01634527, 05234167)$, $(24; 12, 0, 12, 0)$,
22. $(C_8, C_8, 34561270, 05634127, 45230167)$, $(16; 4, 4, 4, 4)$,
23. $(C_8, C_8, 34561270, 03456127, 23450167)$, $(12; 3, 3, 3, 3)$.

Table 3. Biembeddings containing two group-based squares.

Table 4 summarizes these biembeddings where both squares are group-based. The entries give the number of biembeddings of square A with square B.

	C_2^3	$C_4 \times C_2$	C_8	D_4	Q
C_2^3	–	–	–	1	–
$C_4 \times C_2$	–	–	–	4	5
C_8	–	–	13	–	–
D_4	1	4	–	–	–
Q	–	5	–	–	–

Table 4. Numbers of mutual biembeddings of group-based squares.

It can be seen that there are, for example, no biembeddings of two squares both derived from C_2^3. A very recent result gives a partial explanation for the partitioning of the squares of side 7 described in our earlier paper and establishes the non-biembeddability of two copies of C_2^n for $n \geqslant 2$, as well as other non-biembeddability results. A paper describing these results is in preparation.

Finally we give the exceptional biembedding of C_2^3 with a non group-based square and having an automorphism group of order 48. The square C_2^3 is taken as in Table 1, and the other square is as follows.

7	0	1	4	2	3	5	6
6	4	5	2	3	7	1	0
1	2	7	5	0	6	4	3
4	6	0	7	1	2	3	5
5	3	6	1	4	0	2	7
2	5	3	6	7	1	0	4
0	1	4	3	6	5	7	2
3	7	2	0	5	4	6	1

The two squares generate triangular faces that are sewn together along common edges to form the embedding. The automorphism type is given by the vector $(48; 24, 0, 24, 0)$.

References

[1] **M. J. Grannell, T. S. Griggs and M. Knor**: *Biembeddings of Latin squares and Hamiltonian decompositions*, Glasgow Math. J. **46** (2004), 443 – 457.

[2] **M. J. Grannell, T. S. Griggs, M. Knor and J. Širáň**: *Triangulations of orientable surfaces by complete tripartite graphs*, Discrete Math. **306** (2006), 600 – 606.

[3] **G. Kolesova, C. W. H. Lam and L. Thiel**: *On the number of* 8×8 *Latin squares*, J. Combin. Theory Ser. A **54** (1990), 143 – 148.

Received August 1, 2007

M.J.Grannell and T.S.Griggs
Department of Mathematics and Statistics, The Open University, Walton Hall, Milton Keynes MK7 6AA, United Kingdom
E-mails: m.j.grannell@open.ac.uk, t.s.griggs@open.ac.uk

M.Knor
Department of Mathematics, Faculty of Civil Engineering, Slovak University of Technology, Radlinského 11, 813 68 Bratislava, Slovakia
E-mail: knor@math.sk

Quasigroups and Related Systems **15** (2007), 279 – 289

Fuzzy ideals in ordered semigroups

Niovi Kehayopulu and Michael Tsingelis

Abstract

The right (left) ideals, quasi- and bi-ideals play an essential role in studying the structure of some ordered semigroups. In an attempt to show how similar is the theory of ordered semigroups based on ideals or ideal elements with the theory of ordered semigroups based on fuzzy ideals, keeping the usual definitions of fuzzy right ideal, fuzzy left ideal, fuzzy quasi-ideal and fuzzy bi-ideal, we show here that in ordered groupoids, the fuzzy right (resp. left) ideals are fuzzy quasi-ideals and in ordered semigroups, the fuzzy quasi-ideals are fuzzy bi-ideals. Moreover, we prove that in regular ordered semigroups, the fuzzy quasi-ideals and the fuzzy bi-ideals coincide. We finally show that in an ordered semigroup the fuzzy quasi-ideals are just intersections of fuzzy right and fuzzy left ideals.

1. Introduction and prerequisites

The notion of ideals created by Dedekind for the theory of algebraic numbers, was generalized by Emmy Noether for associative rings. The one- and two-sided ideals introduced by her, are still central concepts in ring theory. A further generalization of ideals, the concept of quasi-ideals, was introduced by Ottó Steinfeld. Steinfeld remarked first that the concept of quasi-ideals could be defined not only for rings, but for semigroups as well, and that a quasi-ideal of a semigroup was just the intersection of a right and a left ideal –generalizing a correspondence result given by L. Kovács for rings. Since then many papers on ideals for rings and semigroups appeared showing the importance of the concept [A.H. Clifford, L.M. Gluskin, M.–P. Schützenberger, S. Lajos, K. Iséki and many others]. Further generalization

2000 Mathematics Subject Classification: 06F05, 06D72, 08A72
Keywords: Fuzzy right ideal, fuzzy left ideal, fuzzy quasi-ideal, fuzzy bi-ideal, ordered semigroup, regular ordered semigroup.

of ideals by lattice-theoretical methods was given by G. Birkhoff, O. Steinfeld, and N. Kehayopulu. The concepts of fuzzy one- and two-sided ideals in groupoids have been introduced by A. Rosenfeld in [11], the concepts of fuzzy bi-ideals and fuzzy quasi-ideals in semigroups have been introduced by N. Kuroki in [8] and [9], respectively. Fuzzy ideals in semigroups have been first studied by N. Kuroki, later by other authors as well (for a detailed exposition see the introduction in [7]). Fuzzy ideals in ordered groupoids-semigroups have been introduced by Kehayopulu and Tsingelis in [5]. For a recent work on fuzzy ideals see also [3, 4].

In semigroups the right (resp. left) ideals are quasi-ideals, and the quasi-ideals are bi-ideals. In regular (in the sense of J.v. Neumann) semigroups the bi-ideals and the quasi-ideals coincide [10]. Analogous results are true for ordered semigroups as well. In ordered semigroups the right (resp. left) ideals are quasi-ideals and the quasi-ideals are bi-ideals, and in regular ordered semigroups the bi-ideals and the quasi-ideals coincide. Moreover, in lattice ordered semigroups having a greatest element, the right (resp. left) ideal elements are quasi-ideal elements, the quasi-ideal elements are bi-ideal elements, and in regular lattice ordered semigroups which have a greatest element the bi-ideal elements and the quasi-ideal elements are the same. It might be noted that the concept of right and left ideal elements in an ordered groupoid has been introduced by G. Birkhoff (see, for example [1] p. 328). Ideals play an important role in studying the structure of some ordered semigroups. In an attempt to show how similar is the theory of fuzzy ordered semigroups based on ideals (right, quasi- etc.) with the theory of ordered semigroups based on ideals or the theory of lattice ordered semigroups based on ideal elements, keeping the usual definitions of fuzzy right ideal, fuzzy left ideal, fuzzy quasi-ideal and fuzzy bi-ideal, we show here that in ordered groupoids the fuzzy right (resp. fuzzy left) ideals are fuzzy quasi-ideals, in ordered semigroups the fuzzy quasi-ideals are fuzzy bi-ideals, and in regular ordered semigroups the fuzzy quasi-ideals and the fuzzy bi-ideals coincide. Moreover, we show that if S is an ordered semigroup, then a fuzzy subset f is a fuzzy quasi-ideal of S if and only if there exist a fuzzy right ideal g and a fuzzy left ideal h of S such that $f = g \cap h$.

Following the terminology given by L.A. Zadeh, if $(S, \cdot, \leqslant)$ is an ordered groupoid, we say that f is a fuzzy subset of S (or a fuzzy set in S) if S is a mapping of S into the real closed interval [0,1] (cf. [5]). For $a \in S$, we define $A_a = \{(y, z) \in S \times S \mid a \leqslant yz\}$. For two fuzzy subsets f and g of S,

we define the multiplication of f and g as the fuzzy subset of S defined by:

$$(f \circ g)(a) = \begin{cases} \sup\limits_{(y,z)\in A_a} \{\min\{f(y), g(z)\}\} & \text{if} \quad A_a \neq \emptyset, \\ 0 & \text{if} \quad A_a = \emptyset \end{cases}$$

and in the set of all fuzzy subsets of S we define the order relation as follows: $f \subseteq g$ if and only if $f(x) \leqslant g(x)$ for all $x \in S$. Finally for two fuzzy subsets f and g of S we define the operations $f \cap g$ and $f \cup g$ as the fuzzy subsets of S defined by:

$$(f \cap g)(x) = \min\{f(x), g(x)\} \text{ and } (f \cup g)(x) = \max\{f(x), g(x)\}.$$

For an ordered groupoid S, the fuzzy subset 1 of S is defined by $1(x) = 1$ for all $x \in S$. If $F(S)$ is the set of fuzzy subsets of S, it is clear that the fuzzy subset 1 of S is the greatest element of the ordered set $(F(S), \subseteq)$. Moreover, as we have already seen in [6], if S is an ordered groupoid (resp. ordered semigroup), then the set $F(S)$ of all fuzzy subsets of S with the multiplication $\circ$ and the order $\subseteq$ on S defined above is an ordered groupoid (resp. ordered semigroup) as well.

2. Main results

Definition 1. (cf. [5]) Let $(S, \cdot, \leqslant)$ be an ordered groupoid. A fuzzy subset f of S is called a *fuzzy right ideal* (resp. *fuzzy left ideal*) of S if

(1) $f(xy) \geqslant f(x)$ (resp. $f(xy) \geqslant f(y)$) for every $x, y \in S$ and

(2) $x \leqslant y$ implies $f(x) \geqslant f(y)$.

Definition 2. (cf. [5]) Let $(S, \cdot, \leqslant)$ be an ordered groupoid. A fuzzy subset f of S is called a *fuzzy quasi-ideal* of S if

(1) $(f \circ 1) \cap (1 \circ f) \subseteq f$ and

(2) $x \leqslant y$ implies $f(x) \geqslant f(y)$.

Definition 3. Let $(S, \cdot, \leqslant)$ be an ordered semigroup. A fuzzy subset f of S is called a *fuzzy bi-ideal* of S if the following assertions are satisfied:

(1) $f(xyz) \geqslant \min\{f(x), f(z)\}$ for all $x, y, z \in S$ and

(2) $x \leqslant y$ implies $f(x) \geqslant f(y)$.

Proposition 1. *If $(S, \cdot, \leqslant)$ is an ordered groupoid, then the fuzzy right (resp. left) ideals of S are fuzzy quasi-ideals of S.*

Proof. Let f be a fuzzy right ideal of S and $x \in S$. First of all,

$$((f \circ 1) \cap (1 \circ f))(x) = \min\{(f \circ 1)(x), (1 \circ f)(x)\}.$$

If $A_x = \emptyset$ then we have $(f \circ 1)(x) = 0 = (1 \circ f)(x)$ and, since f is a fuzzy right ideal of S, we have $\min\{(f \circ 1)(x), (1 \circ f)(x)\} = 0 \leqslant f(x)$.

Let $A_x \neq \emptyset$. Then

$$(f \circ 1)(x) = \sup_{(u,v) \in A_x} \{\min\{f(u), 1(v)\}\}.$$

On the other hand,

$$f(x) \geqslant \min\{f(u), 1(v)\} \ \ \forall\ (u, v) \in A_x.$$

Indeed, if $(u, v) \in A_x$, then $x \leqslant uv$, $f(x) \geqslant f(uv) \geqslant f(u) = \min\{f(u), 1(v)\}$. Hence we have

$$\begin{aligned} f(x) &\geqslant \sup_{(u,v) \in A_x} \{\min\{f(u), 1(v)\}\} = (f \circ 1)(x) \\ &\geqslant \min\{(f \circ 1)(x), (1 \circ f)(x)\} \\ &= ((f \circ 1) \cap (1 \circ f))(x). \end{aligned}$$

Therefore f is a fuzzy quasi-ideal of S. □

Proposition 2. *If $(S, \cdot, \leqslant)$ is an ordered semigroup, then the fuzzy quasi-ideals are fuzzy bi-ideals of S.*

Proof. Let f be a fuzzy quasi-ideal of S and $x, y, z \in S$. Then we have

$$f(xyz) \geqslant ((f \circ 1) \cap (1 \circ f))(xyz) = \min\{(f \circ 1)(xyz), (1 \circ f)(xyz)\}.$$

Since $(x, yz) \in A_{xyz}$, we have

$$(f \circ 1)(xyz) = \sup_{(u,v) \in A_{xyz}} \{\min\{f(u), 1(v)\}\} \geqslant \min\{f(x), 1(yz)\} = f(x).$$

Since $(xy, z) \in A_{xyz}$, we have

$$(1 \circ f)(xyz) = \sup_{(u,v) \in A_{xyz}} \{\min\{1(u), f(v)\}\} \geqslant \min\{1(xy), f(z)\} = f(z).$$

Thus we have

$$f(xyz) \geqslant \min\{(f \circ 1)(xyz), (1 \circ f)(xyz)\} \geqslant \min\{f(x), f(z)\}.$$

So f is a fuzzy bi-ideal of S. □

Proposition 3. *In a regular ordered semigroup S, the fuzzy quasi-ideals and the fuzzy bi-ideals coincide.*

Proof. Let f be a fuzzy bi-ideal of S and $x \in S$. We will prove that

$$((f \circ 1) \cap (1 \circ f))(x) \leqslant f(x). \tag{1}$$

First of all, we have

$$((f \circ 1) \cap (1 \circ f))(x) = \min\{(f \circ 1)(x), (1 \circ f)(x)\}.$$

If $A_x = \emptyset$ then, as we have already seen in Proposition 1, condition (1) is satisfied.

Let $A_x \neq \emptyset$. Then

$$(f \circ 1)(x) = \sup_{(z,w)\in A_x} \{\min\{f(z), 1(w)\}\} \tag{2}$$

$$(1 \circ f)(x) = \sup_{(u,v)\in A_x} \{\min\{1(u), f(v)\}\} \tag{3}$$

Let $(f \circ 1)(x) \leqslant f(x)$. Then we have

$$\begin{aligned} f(x) &\geqslant (f \circ 1)(x) \geqslant \min\{(f \circ 1)(x), (1 \circ f)(x)\} \\ &= ((f \circ 1) \cap (1 \circ f))(x), \end{aligned}$$

and condition (1) is satisfied.

Let $(f \circ 1)(x) > f(x)$. Then, by (2), there exists $(z, w) \in A_x$ such that

$$\min\{f(z), 1(w)\} > f(x) \tag{4}$$

(otherwise $f(x) \leqslant (f \circ 1)(x)$, which is impossible).

Since $(z, w) \in A_x$, we have $z, w \in S$ and $x \leqslant zw$. Similarly, from $\min\{f(z), 1(w)\} = f(z)$, by (4), we obtain

$$f(z) > f(x). \tag{5}$$

We will prove that $(1 \circ f)(x) \leqslant f(x)$, Then

$$\min\{(f \circ 1)(x), (1 \circ f)(x)\} \leqslant (1 \circ f)(x) \leqslant f(x),$$

so $((f \circ 1) \cap (1 \circ f))(x) \leqslant f(x)$, and condition (1) is satisfied.

By (3), it is enough to prove that

$$\min\{1(u), f(v)\} \leqslant f(x) \quad \forall \ (u,v) \in A_x.$$

Let $(u,v) \in A_x$. Then $x \leqslant uv$ for some $u, v \in S$. Since S is regular, there exists $s \in S$ such that $x \leqslant xsx$. Then $x \leqslant zwsuv$. Then, since f is a fuzzy bi-ideal of S, we have

$$f(x) \geqslant f(zwsuv) \geqslant \min\{f(z), f(v)\}.$$

If $\min\{f(z), f(v)\} = f(z)$, then $f(z) \leqslant f(x)$ which is impossible by (5). Thus we have $\min\{f(z), f(v)\} = f(v)$, then $f(x) \geqslant f(v) = \min\{1(u), f(v)\}$. □

In the following, using the usual definitions of ideals mentioned above, we show that the fuzzy quasi-ideals of an ordered semigroup are just intersections of fuzzy right and fuzzy left ideals.

Lemma 1. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and f a fuzzy subset of S. Then we have the following:*

(i) $(1 \circ f)(xy) \geqslant f(y)$ *for all* $x, y \in S$,

(ii) $(1 \circ f)(xy) \geqslant (1 \circ f)(y)$ *for all* $x, y \in S$.

Proof. *(i)* Let $x, y \in S$. Since $(x,y) \in A_{xy}$, we have

$$(1 \circ f)(xy) = \sup_{(w,z) \in A_{xy}} \{\min\{1(w), f(z)\}\} \geqslant \min\{1(x), f(y)\} = f(y).$$

(ii) Let $x, y \in S$. If $A_y = \emptyset$, then $(1 \circ f)(y) = 0$. Since $1 \circ f$ is a fuzzy subset of S, we have $(1 \circ f)(xy) \geqslant 0 = (1 \circ f)(y)$.

Let now $A_y \neq 0$. Then

$$(1 \circ f)(y) = \sup_{(w,z) \in A_y} \{\min\{1(w), f(z)\}\}.$$

On the other hand,

$$(1 \circ f)(xy) \geqslant \min\{1(w), f(z)\} \quad \forall \ (w,z) \in A_y. \tag{6}$$

Indeed, let $(w,z) \in A_y$. Since $(x,y) \in A_{xy}$, we have

$$(1 \circ f)(xy) = \sup_{(s,t) \in A_{xy}} \{\min\{1(s), f(t)\}\}.$$

Since $(w,z) \in A_y$, we have $y \leqslant wz$, then $xy \leqslant xwz$, and $(xw,z) \in A_{xy}$. Hence we have

$$(1 \circ f)(xy) \geqslant \min\{1(xw), f(z)\} = f(z) = \min\{1(w), f(z)\}.$$

By (6), we have

$$(1 \circ f)(xy) \geqslant \sup_{(w,z)\in A_y} \{\min\{1(w), f(z)\}\} = (1 \circ f)(y). \qquad \square$$

In a similar way we prove the following:

Lemma 2. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and f a fuzzy subset of S. Then we have the following:*

(i) $(f \circ 1)(xy) \geqslant f(x)$ *for all* $x, y \in S$,

(ii) $(f \circ 1)(xy) \geqslant (f \circ 1)(x)$ *for all* $x, y \in S$.

Lemma 3. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup, f a fuzzy subset of S and $x \leqslant y$. Then we have*

$$(1 \circ f)(x) \geqslant (1 \circ f)(y).$$

Proof. If $A_y = \emptyset$, then $(1 \circ f)(y) = 0$. Since $1 \circ f$ is a fuzzy subset of S, we have $(1 \circ f)(x) \geqslant 0$, then $(1 \circ f)(x) \geqslant (1 \circ f)(y)$.

Let $A_y \neq \emptyset$. Then

$$(1 \circ f)(y) = \sup_{(w,z)\in A_y} \{\min\{1(w), f(z)\}\} = \sup_{(w,z)\in A_y} \{f(z)\}.$$

On the other hand,

$$(1 \circ f)(x) \geqslant f(z) \quad \forall\ (w,z) \in A_y. \tag{7}$$

Indeed, let $(w,z) \in A_y$. Since $x \leqslant y \leqslant wz$, we have $(w,z) \in A_x$. Then

$$(1 \circ f)(xy) = \sup_{(s,t)\in A_{xy}} \{\min\{1(s), f(t)\}\} \geqslant \min\{1(w), f(z)\} = f(z).$$

Thus, by (7), we have

$$(1 \circ f)(x) \geqslant \sup_{(w,z)\in A_y} \{f(z)\} = (1 \circ f)(y). \qquad \square$$

In a similar way we prove the following:

Lemma 4. *Let $(S,\cdot,\leqslant)$ be an ordered semigroup, f a fuzzy subset of S and $x \leqslant y$. Then*

$$(f \circ 1)(x) \geqslant (f \circ 1)(y).$$

Lemma 5. *Let $(S,\cdot,\leqslant)$ be an ordered semigroup and f a fuzzy subset of S. Then*

$$(f \cup (1 \circ f))(xy) \geqslant (f \cup (1 \circ f))(y) \quad \forall\ x,y \in S.$$

Proof. Let $x,y \in S$. Since $1 \circ f \subseteq f \cup (1 \circ f)$, we have

$$(f \cup (1 \circ f))(xy) \geqslant (1 \circ f)(xy).$$

By Lemma 1, $(1 \circ f)(xy) \geqslant f(y)$ and $(1 \circ f)(xy) \geqslant (1 \circ f)(y)$, so we have

$$(1 \circ f)(xy) \geqslant \max\{f(y),(1 \circ f)(y)\} = (f \cup (1 \circ f))(y).$$

Therefore $(f \cup (1 \circ f))(xy) \geqslant (f \cup (1 \circ f))(y)$. □

In a similar way we prove the following:

Lemma 6. *Let $(S,\cdot,\leqslant)$ be an ordered semigroup and f a fuzzy subset of S. Then*

$$(f \cup (f \circ 1))(xy) \geqslant (f \cup (f \circ 1))(x) \quad \forall\ x,y \in S.$$

Lemma 7. *Let $(S,\cdot,\leqslant)$ be an ordered semigroup and f a fuzzy subset of S such that for all $x,y \in S$ such that $x \leqslant y$, we have $f(x) \geqslant f(y)$. Then the fuzzy subset $f \cup (1 \circ f)$ is a fuzzy left ideal of S.*

Proof. Let $x,y \in S$. By Lemma 5, we have $(f \cup (1 \circ f))(xy) \geqslant (f \cup (1 \circ f))(y)$. Let now $x \leqslant y$. Then $(f \cup (1 \circ f))(x) \geqslant (f \cup (1 \circ f))(y)$. Indeed: Since f is a fuzzy subset of S and $x \leqslant y$, by Lemma 3, we get $(1 \circ f)(x) \geqslant (1 \circ f)(y)$ and, by hypothesis, $f(x) \geqslant f(y)$. Then

$$\begin{aligned}(f \cup (1 \circ f))(x) &= \max\{f(x),(1 \circ f)(x)\} \geqslant \max\{f(y),(1 \circ f)(y)\} \\ &= (f \cup (1 \circ f))(y).\end{aligned}$$

□

In a similar way we prove the following:

Lemma 8. *Let $(S,\cdot,\leqslant)$ be an ordered semigroup and f a fuzzy subset of S such that for all $x,y \in S$ such that $x \leqslant y$, we have $f(x) \geqslant f(y)$. Then the fuzzy subset $f \cup (f \circ 1)$ is a fuzzy right ideal of S.*

Lemma 9. *If a, b, c are real numbers, then*

(i) $\min\{a, \max\{b, c\}\} = \max\{\min\{a, b\}, \min\{a, c\}\}$ *and*

(ii) $\max\{a, \min\{b, c\}\} = \min\{\max\{a, b\}, \max\{a, c\}\}$.

Proof. (i) Let $a \leqslant \max\{b, c\}$. Then $\min\{a, \max\{b, c\}\} = a$. If $b \leqslant c$, then $\max\{b, c\} = c$, $a \leqslant c$, $\min\{a, b\} \leqslant a = \min\{a, c\}$, and

$$\max\{\min\{a, b\}, \min\{a, c\}\} = a,$$

so condition (i) is satisfied. If $c < b$ then, in a similar way we prove that condition (i) is satisfied.

Let now $a > \max\{b, c\}$. Then $\min\{a, \max\{b, c\}\} = \max\{b, c\} \geqslant b$, $a > b$, and $\min\{a, b\} = b$. Similarly $\min\{a, c\} = c$. Then

$$\max\{\min\{a, b\}, \min\{a, c\}\} = \max\{b, c\},$$

and condition (i) is satisfied.

The proof of (ii) is similar. □

Lemma 10. *Let S be an ordered semigroup and f, g, h fuzzy subsets of S. Then*

$$f \cap (g \cup h) = (f \cap g) \cup (f \cap h).$$

Proof. Indeed,

$$\begin{aligned}
(f \cap (g \cup h))(x) &= \min\{f(x), (g \cup h)(x)\} \\
&= \min\{f(x), \max\{g(x), h(x)\}\} \\
&= \max\{\min\{f(x), g(x)\}, \min\{f(x), h(x)\}\} \text{ (by Lemma 9)} \\
&= \max\{f \cap g)(x),\ (f \cap h)(x)\} \\
&= ((f \cap g) \cup (f \cap h))(x).
\end{aligned}$$

□

By Lemma 10, we have the following:

Corollary 1. *If S is an ordered semigroup, then the set of all fuzzy subsets of S is a distributive lattice.*

Proposition 4. *Let $(S, \cdot, \leqslant)$ be and ordered semigroup. A fuzzy subset f of S is a fuzzy quasi-ideal of S if and only if there exist a fuzzy right ideal g and a fuzzy left ideal h of S such that $f = g \cap h$.*

Proof. $\Longrightarrow$. By Lemmas 7 and 8, $f\cup(1\circ f)$ is a fuzzy left ideal and $f\cup(f\circ 1)$ is a fuzzy right ideal of S. Moreover, we have

$$f = (f \cup (1 \circ f)) \cap (f \cup (f \circ 1)).$$

In fact, by Corollary 1, we have

$$\begin{aligned}(f \cup (1 \circ f)) \cap (f \cup (f \circ 1)) &= ((f \cup (1 \circ f)) \cap f) \cup ((f \cup (1 \circ f)) \cap (f \circ 1)) \\ &= (f \cap f) \cup ((1 \circ f) \cap f) \cup (f \cap (f \circ 1)) \cup ((1 \circ f) \cap (f \circ 1)) \\ &= f \cup ((1 \circ f) \cap f) \cup (f \cap (f \circ 1)) \cup ((1 \circ f) \cap (f \circ 1)).\end{aligned}$$

Since f is a fuzzy quasi-ideal of S, we have $(f\circ 1)\cap(1\circ f)\subseteq f$. Besides, $(1\circ f)\cap f\subseteq f$ and $f\cap(f\circ 1)\subseteq f$. Hence

$$(f \cup (1 \circ f)) \cap (f \cup (f \circ 1)) = f.$$

$\Longleftarrow$. Let $x\in S$. Then

$$((f \circ 1) \cap (1 \circ f))(x) \leqslant f(x) \tag{8}$$

In fact, $((f\circ 1)\cap(1\circ f))(x) = \min\{(f\circ 1)(x), (1\circ f)(x)\}$. If $A_x=\emptyset$, then $(f\circ 1)(x) = 0 = (1\circ f)(x)$. So, in this case condition (8) is satisfied.

If $A_x\neq\emptyset$, then

$$(f \circ 1)(x) = \sup_{(y,z)\in A_x} \{\min\{f(y), 1(z)\}\} = \sup_{(y,z)\in A_x} \{f(y)\}. \tag{9}$$

We have

$$f(y) \leqslant h(x) \quad \forall\ (y,z)\in A_x. \tag{10}$$

Indeed, for $(y,z)\in A_x$ we have $x\leqslant yz$ and $h(x)\geqslant h(yz)\geqslant h(y)$ because h is a fuzzy left ideal of S.

Thus, applying (10) to (9), we obtain

$$(f \circ 1)(x) = \sup_{(y,z)\in A_x} \{f(y)\} \leqslant h(x).$$

In a similar way, we get $(1\circ f)(x)\leqslant g(x)$. Hence

$$\begin{aligned}((f \circ 1) \cap (1 \circ f))(x) &= \min\{(f \circ 1)(x), (1 \circ f)(x)\} \\ &\leq \min\{h(x), g(x)\} \\ &= (h \cap g)(x) \\ &= f(x),\end{aligned}$$

which completes the proof of (8). □

We thank the managing editor of the journal Professor Wieslaw A. Dudek for editing, communicating the paper and the useful discussions concerning this paper we had, and we also thank the referee for his time to read the paper carefully and his (her) prompt reply.

References

[1] **G. Birkhoff:** *Lattice Theory*, Amer. Math. Soc., Coll. Publ., Vol. **XXV**, Providence, Rhode Island, 1967.

[2] **A. H. Clifford and G. B. Preston:** *The Algebraic Theory of Semigroups*, Vol **I**, Amer. Math. Soc., Math. Surveys 7, Providence, Rhode Island, 1977.

[3] **Y. B. Jun:** *Intuitionistic fuzzy bi-ideals of ordered semigroups*, Kyungpook Math. J. **45** (2005), 527 – 537.

[4] **Y. B. Jun, S. Z. Song:** *Generalized fuzzy interior ideals in semigroups*, Inform. Sci. **176** (2006), 3079 – 3093.

[5] **N. Kehayopulu, M. Tsingelis:** *Fuzzy sets in ordered groupoids*, Semigroup Forum **65** (2002), 128 – 132.

[6] **N. Kehayopulu, M. Tsingelis:** *The embedding of an ordered groupoid into a poe-groupoid in terms of fuzzy sets*, Inform. Sci. **152** (2003), 231 – 236.

[7] **N. Kehayopulu, M. Tsingelis:** *Regular ordered semigroups in terms of fuzzy subsets*, Inform. Sci. **176** (2006), 3675 – 3693.

[8] **N. Kuroki:** *Fuzzy bi-ideals in semigroups*, Comment. Math. Univ. St. Paul. **28** (1980), 17 – 21.

[9] **N. Kuroki:** *Fuzzy semiprime quasi-ideals in semigroups*, Inform. Sci. **75** (1993), 201 – 211.

[10] **S. Lajos:** *Generalized ideals in semigroups*, Acta Sci. Math. Szeged **22** (1961), 217 – 222.

[11] **A. Rosenfeld:** *Fuzzy groups*, J. Math. Anal. Appl. **35** (1971), 338 – 353.

University of Athens
Department of Mathematics
157 84 Panepistimiopolis
Athens, Greece
E-mail: nkehayop@math.uoa.gr

Received November 16, 2006
Revised January 12, 2007

Quasigroups and Related Systems **15** (2007), 291 – 294

A note on Belousov quasigroups

Aleksandar Krapež

Abstract

A Belousov identity is a balanced identity which is a consequence of commutativity. It is proved that a quasigroup is Belousov iff it has a permutation π satisfying $\pi(xy) = yx$ and a weak (anti)automorphism–like property depending on Belousov identities the quasigroup satisfies.

A *balanced* (also called *linear*) *identity* is one in which each variable appears precisely twice, once on each side of the equality symbol. Instead of identity the word *equation* is sometimes used. We note that, although quasigroups might be defined equationally, using multiplication ($\cdot$) and both division operations ($\backslash$ and $/$), the identities which we consider contain the multiplication symbol only. The dual operation $*$ of $\cdot$ is defined by $x * y = y \cdot x$. The symbol $*$ is considered not to belong to the language of quasigroups. When unambiguous, the term $x \cdot y$ is usually shortened to xy.

The product symbol ($\prod$) is used *but only for products of* 2^n *factors*. Formally: $\prod_{i=m}^{m} x_i = x_m$ and $\prod_{i=m}^{m+2^n-1} x_i = (\prod_{i=m}^{m+2^{n-1}-1} x_i)(\prod_{i=m+2^{n-1}}^{m+2^n-1} x_i)$.

V. D. Belousov defined in [1] an important class of balanced identities which were named *Belousov equations* by A. Krapež and M. A. Taylor in [3]. A balanced identity $s = t$ is *Belousov* if for every subterm p of s (t) there is a subterm q of t (s) such that p and q have exactly the same variables.

2000 Mathematics Subject Classification: 20N05
Keywords: Balanced identities, Belousov identities, Belousov quasigroup, almost commutative quasigroup, swap.
Supported by the Ministry of Science and Environmental Protection of Serbia, grants 144013 and 144018

Examples of Belousov identities are:

$$x = x \tag{B_0}$$
$$xy = xy$$
$$xy = yx \tag{B_1}$$
$$x \cdot yz = zy \cdot x$$
$$xy \cdot uv = vu \cdot yx \tag{B_{11}}$$
$$xy \cdot (zu \cdot vw) = (uz \cdot wv) \cdot yx$$

The identity (B_0) and all identities $t = t$ are *trivial*. Belousov identities not equivalent to (B_0) are *nontrivial*. A quasigroup satisfying a set of Belousov identities, not all of them trivial, is a *Belousov quasigroup*.

The characteristic property of Belousov identities is:

Theorem 1. (partially in Krapež [2]) *A balanced quasigroup identity $s = t$ is Belousov:*

- *iff $s = t$ is a consequence of the theory of commutative quasigroups,*
- *iff there is an identity $Eq(\cdot, *)$ which is true in all quasigroups and $s = t$ is $Eq(\cdot, \cdot)$,*
- *iff the trees of terms s, t are isomorphic.*

Their importance stems from:

Theorem 2. (Krapež [2], Belousov [1]) *A quasigroup satisfying a balanced but not Belousov identity is isotopic to a group.*

Belousov identities are described in [4] using polynomials from $\mathbb{Z}_2[x]$.

Theorem 3. (Krapež, Taylor [4]) *Every set of Belousov identities is equivalent to a single normal Belousov identity.*

For the reduction algorithm and the proof consult [4]. Below we just give the definition of a normal Belousov identity.

Definition 1. A quasigroup for which there is a permutation π such that $\pi(xy) = yx$ is called *almost commutative*. The permutation π is called a *swap*.

The next theorem was proved by Belousov, except that he forgot to exclude the trivial identities (i.e., $t = t$).

Theorem 4. (Belousov [1]) *Every Belousov quasigroup is almost commutative.*

A sequence $\alpha_1 \dots \alpha_n$ of zeros and ones is a *pattern*. It is a *normal pattern* if $\alpha_1 = \alpha_n = 1$.

Let π be a swap, $p = \alpha_1 \dots \alpha_n$ a pattern and st a term. We define :

$$\pi^{\alpha_1 \dots \alpha_n}(st) = \pi^{\alpha_1}(\pi^{\alpha_2 \dots \alpha_n}(s) \cdot \pi^{\alpha_2 \dots \alpha_n}(t)).$$

The relations $\pi^0 = Id$ $(Id(x) = x)$ and $\pi^1 = \pi$ are assumed.

Definition 2. Let π be a swap and p a pattern of length $n > 0$. The Belousov identity (B_p) is:

$$\prod_{i=1}^{2^n} x_i = \pi^p(\prod_{i=1}^{2^n} x_i). \qquad (B_p)$$

This is a *normal Belousov identity* if p is a normal pattern.

We assume that (B_0) is also a normal Belousov identity.

Note that the identity (B_p) does not contain a single occurrence of π. It is used up while transforming various subterms st of $\prod_{i=1}^{2^n} x_i$ into ts.

Theorem 5. *Let p be a nontrivial normal pattern $\alpha_1 \dots \alpha_n$. A quasigroup satisfies the normal Belousov identity (B_p) iff it has a swap π satisfying:*

$$\pi(\prod_{i=1}^{2^{n-1}} y_i) = \pi^{0\alpha_2 \dots \alpha_{n-1}}(\prod_{i=1}^{2^{n-1}} \pi(y_i)). \qquad (1)$$

Proof. Apply π to both sides of (B_p); then use $\pi^2(x) = x$; next push π inside the product on the right hand side of the equation; then pull out π back, preserving expressions $\pi(x_{2i-1}x_{2i})$; and finally substitute y_i for $x_{2i-1}x_{2i}$. We get (1).

All transformations are equivalent, so the theorem follows. □

Example 1. For $p = 1$ we get that a quasigroup is commutative if Id is a swap.

Example 2. For $p = 11$ we get the result of M. Polonijo [5] that a quasigroup satisfies (B_{11}) (or palindromic identity in the terminology of [5]) iff it has a swap π satisfying $\pi(xy) = \pi^{01}(x \cdot y) = \pi(x) \cdot \pi(y)$.

Example 3. For $p = 101$ we get that a quasigroup satisfies $\prod_{i=1}^{8} x_i = \pi^{101}(\prod_{i=1}^{8} x_i) = (x_6x_5 \cdot x_8x_7)(x_2x_1 \cdot x_4x_3)$ iff it has a swap π satisfying $\pi(xy \cdot uv) = \pi^{001}(xy \cdot uv) = \pi(x)\pi(y) \cdot \pi(u)\pi(v)$.

The last two examples suggest:

Corollary 1. A quasigroup satisfies $(B_{10\ldots01})$ (with $n \geqslant 0$ zeros) iff it has a swap π satisfying $\pi(\prod_{i=1}^{2^{n+1}} y_i) = \prod_{i=1}^{2^{n+1}} \pi(y_i)$.

Example 4. For $p = 111$ we get that a quasigroup satisfies $\prod_{i=1}^{8} x_i = \pi^{111}(\prod_{i=1}^{8} x_i) = (x_8x_7 \cdot x_6x_5)(x_4x_3 \cdot x_2x_1)$ iff it has a swap π satisfying $\pi(xy \cdot uv) = \pi^{011}(xy \cdot uv) = \pi(\pi(x)\pi(y)) \cdot \pi(\pi(u)\pi(v)) = \pi(y)\pi(x) \cdot \pi(v)\pi(u)$.

Another way of looking at Theorem 5 is:

Theorem 6. *The equational theory of B_p–quasigroups $(p = \alpha_1 \ldots \alpha_n, n > 0)$ is equivalent to the equational theory of algebras $(S; \cdot, \backslash, /, \pi)$ with the quasigroup axioms: $x\backslash xy = y$, $x(x\backslash y) = y$, $xy/y = x$, $(x/y)y = x$, the swap axiom $\pi(xy) = yx$ and (1).*

The last axiom has a half as many variables as the identity (B_p).

In case of an equational theory with arbitrary nontrivial Belousov identities we can combine the Theorem 6 with the Theorem 3 to get the appropriate axiom (1).

References

[1] **V. D. Belousov**: *Quasigroups with completely reducible balanced identities*, (Russian), Mat. Issled. **83** (1985), 11 – 25.

[2] **A. Krapež**: *On solving a system of balanced functional equations on quasigroups III*, Publ. Inst. Math. (Belgrade) **26(40)** (1979), 145 – 156.

[3] **A. Krapež and M. A. Taylor**: *Belousov equations on quasigroups*, Aequationes Math. **34** (1987), 174 – 185.

[4] **A. Krapež and M. A. Taylor**: *Irreducible Belousov equations on quasigroups*, Czechoslovak Math. J. **43(118)** (1993), 157 – 175.

[5] **M. Polonijo**: *On medial-like identities*, Quasigroups and Related Systems **13** (2005), 281 – 288.

Received October 18, 2007

Mathematical Institute of the Serbian Academy of Sciences and Arts, Kneza Mihaila 35, 11001 Beograd, Serbia, E-mail: sasa@mi.sanu.ac.yu

Quasigroups and Related Systems **15** (2007), 295 – 301

A note on an Abel-Grassmann's 3-band

Qaiser Mushtaq and Madad Khan

Abstract

An Abel-Grassmann's groupoid is discussed in several papers. In this paper we have investigated AG-3-band and ideal theory on it. An AG-3-band S has associative powers and is fully idempotent. A subset of an AG-3-band is a left ideal if and only it is right and every ideal of S is prime if and only if the set of all ideals of S is totally ordered under inclusion. An ideal of S is prime if and only if it is strongly irreducible. The set of ideals of S is a semilattice.

1. Introduction

An *left almost semigroup* [3], abbreviated as an *LA-semigroup*, is a groupoid S whose elements satisfy for all $a, b, c \in S$ the *invertive law*:

$$(ab)c = (cb)a. \tag{1}$$

In [[1], the same structure is called a *left invertive groupoid* and in [7] it is called an *AG-groupoid*. It is a useful non-associative algebraic structure, midway between a groupoid and a commutative semigroup, with wide applications in the theory of flocks and has a character similar to commutative semigroup.

An AG-groupoid S is *medial* [3], that is,

$$(ab)(cd) = (ac)(bd) \tag{2}$$

holds for all $a, b, c, d, \in S$.

If an AG-groupoid S satisfies for all $a, b, c, d, \in S$ one of the following properties

$$(ab)c = b(ca), \tag{3}$$

2000 Mathematics Subject Classification: 20M10, 20N99
Keywords: LA-semigroup, AG-3-band, invertive law, medial law, paramedial and prime ideals.

$$(ab)c = b(ac), \tag{4}$$

then it is called an AG*-*groupoid* [9]. It is easy to see that the conditions (3) and (4) are equivalent.

In AG*-groupoid S holds all permutation identities of a next type [9],

$$(x_1x_2)(x_3x_4) = (x_{p(1)}x_{p(2)})(x_{p(3)}x_{p(4)}) \tag{5}$$

where $\{p(1), p(2), p(3), p(4)\}$ means any permutation of the set $\{1, 2, 3, 4\}$.

An AG-groupoid satisfying the identity

$$a(bc) = b(ac) \tag{6}$$

is called an AG**-*groupoid* [6]. An AG-groupoid in which $(aa)a = a(aa) = a$ holds for all a is called an AG-3-*band* [9]. In an AG-3-band S we have $S^2 = S$, $(Sa)S = S(aS)$ and $(SS)S = S(SS)$.

It has been shown in [9], that $(aa)a = a(aa) = a$ and $(bb)b = b(bb) = b$ imply

$$ab = (ab)((ab)(ab)) = ((ab)(ab))(ab).$$

2. AG-3-bands

By an AG**-3-*band* we mean an AG-3-band satisfying identity (6). An AG**-3-band S is a commutative semigroup because using (2), (6) and (1), we get

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

for all $x, y \in S$. The commutativity and (1) leads us to the associativity.

By an AG*-3-*band* we mean an AG-3-band satisfying (3). If S is an AG-3-band, then $S = S^2$ and by virtue of identity (5), a non-associative AG*-3-band does not exist.

An AG-groupoid S is *paramedial* [2], that is,

$$(ab)(cd) = (db)(ca)$$

holds for all $a, b, c, d, \in S$.

A paramedial AG-3-band becomes a commutative semigroup because

$$ab = (ab)((ab)(ab)) = (ab)((ba)(ba)) = ((ba)(ba))(ba) = ba.$$

Lemma 1. *Every left identity in an AG-3-band is a right identity.*

Proof. Let e be a left identity and a be any element in an AG-3-band S. Then using (1), we get

$$ae = (a(aa))e = (e(aa))a = (aa)a = a.$$

Hence e is right identity. □

As a consequence of Lemma 1, one can see that an AG-3-band with a left identity becomes a commutative monoid, because it has been shown in [5] that every right identity is the unique identity in an AG-groupoid and the identity implies commutativity which further implies associativity.

Lemma 2. *An AG-3-band S is a commutative semigroup if and only if $(xy)^2 = (yx)^2$ holds for all $x, y \in S$.*

Proof. Indeed, using (1), (2), we get

$$\begin{aligned} sa &= ((ss)s)a = (as)(ss) = ((a(aa))s)(ss) = (as)((aa)s)s) \\ &= (as)((ss)(aa)) = (as)((aa)(ss)) = (a(aa))(s(ss)) = as. \end{aligned}$$

The converse is easy. □

Lemma 3. *If S is an AG-3-band, then $aS \subseteq Sa$ for all a in S.*

Proof. Using (1) and (2), we get

$$\begin{aligned} as &= (a(aa))(xy) = (ax)((aa)y) = (ax)(ya)a) \\ &= (a(ya))(xa) = ((xa)(ya))a, \end{aligned}$$

which completes the proof. □

It is easy fact that $(aS)S = Sa$, $S(aS) = (Sa)S$, $(Sa)S \subseteq S(Sa)$ and $Sa \subseteq (Sa)S$.

Lemma 4. *If S is an AG-3-band, then $a^n = a$ and $a^{n+1} = a^2$, where n is a positive odd integer.*

Proof. Obviously $a^3 = (aa)a = a(aa)$. Let the result be true for an odd integer k, that is $a^k = a$. Then using (1), we obtain $a^{k+2} = a^{k+1+1} = a^{k+1}a^1 = (a^k a)a = a^2a^k = a^2a = a^3 = a$. Hence $a^n = a$ for all odd integers n. This proves the first identity. To prove the second, observe that $a^4 = a^3a = aa = a^2$ and assume that $a^s = a^2$ is true for an even integer s. Then using (1), we get $a^{s+2} = a^2a^s = a^2a^2 = a^4 = a^2$, which proves that $a^{n+1} = a^2$ is true for a positive odd integer n. □

Lemma 5. *An AG-3-band has associative powers.*

Proof. The proof is easy. □

As a consequence of Lemmas 4 and 5, one can easily see that the sequence of the powers of a has an element a at odd position and a^2 at even position that is, $a, a^2, a, a^2....$

The following proposition can be proved easily.

Proposition 1. *In an AG-3-band S for all $a, b \in S$ and all positive integers m, n we have*

$$a^m a^n = a^{m+n}, \quad (ab)^n = a^n b^n, \quad (a^m)^n = a^{mn}.$$

Let $\{S_\alpha : \alpha \in I\}$ be a family of AG-3-bands containing a zero element. We may denote all the zeros elements by common symbol 0. The disjoint union of $\{0\}$ and all $S_\alpha \backslash \{0\}$ becomes an AG-3-band if we define the product of x and y as their product in S_α, if they are in the same S_α, and zero otherwise.

An AG-groupoid S is called *locally associative* if $a(aa) = (aa)a$ holds for all $a \in S$ [4].

Lemma 6. *Every AG-3-band is locally associative AG-groupoid, but the converse is not true.*

Example 1. Let the binary operation on $S = \{a, b, c, d\}$ be defined as follows [4]:

$\cdot$	a	b	c	d
a	d	d	b	d
b	d	d	a	d
c	a	b	c	d
d	d	d	d	d

Then $(S, \cdot)$ is locally associative but it is not AG-3-band because $a(aa) = (aa)a = d \neq a$.

A subset I of an AG-groupoid S is said to be *right* (*left*) *ideal* if $IS \subseteq I$ ($SI \subseteq I$). As usual I is said to be an *ideal* if it is both right and left ideal. An ideal I of an AG-groupoid is called 3-*potent* if $I(II) = (II)I = I$.

An AG-groupoid S without zero is called *simple* (*left simple, right simple*) if it does not properly contain any two sided (left, right) ideal.

An AG-groupoid S with zero is called *zero-simple* if it has no proper ideals and $S^2 \neq \{0\}$.

The existence of non-associative simple and zero-simple AG-3-bands is guaranteed by the following example.

Example 2. The set $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$ with the binary operation defined as follows [9]:

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

is an AG-3-band which has no proper ideals, so it is simple. If we add the element 0 to the set S and extend the binary operation putting $0 \cdot 0 = 0 \cdot s = s \cdot 0 = 0$ for all s in S, then $(S \cup \{0\}, \cdot)$ will be a zero-simple AG-3-band.

Proposition 2. *A subset of an AG-3-band is a right ideal if and only if it is left.*

Proof. Let A be a right ideal of S. Then using (1) we get $sa = ((ss)s)a = (as)(ss)$, which implies that A is a left ideal of S.

The converse follows from Lemma 3. □

A subset M of an AG-groupoid S is called an *m-system* if for $a, b \in M$ there exists $x \in S$ such that $(ax)b \in M$.

A subset B of an AG-groupoid S is called a *p-system* if for every $b \in B$ there exists $x \in S$ such that $(bx)b \in B$.

Proposition 3. *In an AG-groupoid each m-system is a p-system.* □

Lemma 7. *In an AG-3-band every (left, right) ideal is p-system, but the converse is not true.*

Proof. If a, b belongs to an ideal I of an AG-3-band S, then $(as)a \in (IS)I$.

The converse statement follows from Example 2. In this example $B = \{1, 2\}$ is a p-system but not an ideal. □

Two subsets A, B of an AG-groupoid S are called *right* (*left*) *connected* if $AS \subseteq B$ and $BS \subseteq A$ (resp. $SA \subseteq B$ and $SB \subseteq A$) [8]. A and B are *connected* if they are both left and right connected.

Lemma 8. *If A and B are ideal of an AG-3-band S, then AB band BA are right and left connect.*

Proof. Using (1), we get $(AB)S = (SB)A \subseteq BA$. Similarly $(BA)S \subseteq AB$. So, AB and BA are right connected. Also $S(BA) = (SS)(BA) = ((BA)S)S = ((SA)B)S \subseteq AB$, and $S(AB) \subseteq BA$. □

Proposition 4. *If A and B are ideals of an AG-3-band, then AB is an ideal.*

Proof. Using (2), one can easily show that AB is an ideal. □

It is interesting to note that if S is an AG-3-band and I_1, I_2, I_3 are proper ideals of S, then $(I_1I_2)I_3$ is an ideal of S. It can be generalized, that is, if $I_1, I_2, \ldots, I_n$ are ideals, then $(...((I_1I_2)I_3)...)I_n$ is also an ideal and $(...((I_1I_2)I_3)...)I_n \subseteq I_1 \cap I_2 \cap \ldots \cap I_n$.

An AG-groupoid S is said to be *fully idempotent* if every ideal of S is idempotent, i.e., for ecery ideal I of S we have $I^2 = I$.

An AG-groupoid S is said to be *fully semiprime* if every ideal of S is *semiprime*, i.e., for every ideal P of S from $A^2 \subseteq P$, where A is an ideal of S, it follows $A \subseteq P$.

Every AG-3-band is fully idempotent and fully semiprime. Consequently, $A^n = A$ for an ideal A and any positive integer n.

Lemma 9. *$IJ = JI = I \cap J$ for all ideals of an AG-3-band.*

Proof. If $x \in I \cap J$, then $x = x(xx) \in IJ$, whence $IJ = I \cap J$. So, $IJ = JI$. □

An ideal I of an AG-groupoid S is said to be *strongly irreducible* if and only if for ideals H and K of S, $H \cap K \subseteq I$ implies either $H \subseteq I$ or $K \subseteq I$.

An AG-groupoid S is called *totally ordered* if for all ideals A, B of S either $A \subseteq B$ or $B \subseteq A$.

An ideal P of an AG-groupoid S is called *prime* if and only if $AB \subseteq P$ implies that either $A \subseteq P$ or $B \subseteq P$ for all ideals A and B in S.

Using Lemma 9, one can prove the following Theorems.

Theorem 1. *In an AG-3-band an ideal is strongly irreducible if and only if it is prime.*

Theorem 2. *An ideal of an AG-3-band S is prime if and only if the set of all ideals of S is totally ordered under inclusion.*

Theorem 3. *The set of ideals of an AG-3-band S form a semilattice, $(L_S, \wedge)$, where $A \wedge B = AB$, A and B are ideals of S.*

References

[1] **P. Holgate**: *Groupoids satisfying a simple invertive law*, The Math. Stud. **61** (1992), 101 – 106.

[2] **J. Ježek and T. Kepka**: *Equational theory of paramedial groupoids*, Czechoslovak Math. J. **50(125)** (2000), 25 – 34.

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

[4] **Q. Mushtaq and Q. Iqbal**: *Decomposition of a locally associative LA-semigroup*, Semigroup Forum **41** (1990), 154 – 164.

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

[6] **P. V. Protić and M. Bozinović**: *Some congruences on an AG^{**}-groupoid*, Algebra Logic and Discrete Math., **14-16** (1995), 879 – 886.

[7] **P. V. Protić and N. Stevanović**: *On Abel-Grassmann's groupoids*, Proc. Math. Conf. Pristina, 1994, 31 – 38.

[8] **P. V. Protić and N. Stevanović**: *AG-test and some general properties of Abel-Grassmann's groupoids*, PU. M. A. **6** (1995), 371 – 383.

[9] **N. Stevanović and P. V. Protić**: *Some decomposition on Abel-Grassmann's groupoids*, PU. M. A. **8** (1997), 355 – 366.

[10] **N. Stevanović and P. V. Protić**: *Composition of Abel-Grassmann's 3-bands*, Novi Sad. J. Math. **34.2** (2004), 175 – 182.

Department of Mathematics
Quaid-i-Azam University
Islamabad
Pakistan
E-mail: qmushtaq@apollo.net.pk

Received April 26, 2006

Quasigroups and Related Systems **15** (2007), 303 – 308

Decomposition of AG*-groupoids

Qaiser Mushtaq and Madad Khan

Abstract

We have shown that an AG*-groupoid S has associative powers, and S/ρ, where $a\rho b$ if and only if $ab^n = b^{n+1}$, $ba^n = a^{n+1}$ $\forall$ $a, b \in S$, is a maximal separative commutative image of S.

An *Abel-Grassmann's groupoid* [9], abbreviated as an *AG-groupoid*, is a groupoid S whose elements satisfy the invertive law:

$$(ab)c = (cb)a. \tag{1}$$

It is also called a *left almost semigroup* [3, 4, 5, 7]. In [1], the same structure is called a *left invertive groupoid*. In this note we call it an AG-groupoid. It is a useful non-associative algebraic structure, midway between a groupoid and a commutative semigroup, with wide applications in the theory of flocks.

An AG-groupoid S is *medial* [2], i.e., it satisfies the identity

$$(ab)(cd) = (ac)(bd). \tag{2}$$

It is known [3] that if an AG-groupoid contains a left identity then it is unique. It has been shown in [3] that an AG-groupoid contains a left identity then it is unique. It has been proved also that an AG-groupoid with right identity is a commutative monoid, that is, a semigroup with identity element.

If an AG-groupoid satisfy one of the following equivalent identities:

$$(ab)c = b(ca) \tag{3}$$

$$(ab)c = b(ac) \tag{4}$$

2000 Mathematics Subject Classification: 20M10, 20N99
Keywords: LA-semigroup, AG^*-groupoid, invertive law, medial law, congruence.

then it is called an *AG*-groupoid* [10].

Let S be an AG*-groupoid and a relation ρ be defined in S as follows. For a positive integer n, $a\rho b$ if and only if $ab^n = b^{n+1}$ and $ba^n = a^{n+1}$, for all a and b in S.

In this paper, we have shown that ρ is a *separative congruence* in S, that is, $a^2\rho ab$ and $ab\rho b^2$ implies that $a\rho b$ when $a, b \in S$.

The following four propositions have been proved in [10].

Proposition 1. *Every AG*-groupoid has associative powers, i.e.,* $aa^n = a^n a$ *for all* a.

Proposition 2. *In an AG*-groupoid* S, $a^m a^n = a^{m+n}$ *for all* $a \in S$ *and positive integers* m, n.

Proposition 3. *In an AG*-groupoid* S, $(a^m)^n = a^{mn}$ *for all* $a \in S$ *and positive integers* m, n.

Proposition 4. *If* S *is an AG*-groupoid, then for all* $a, b \in S$, $(ab)^n = a^n b^n$ *and positive integer* $n \geqslant 1$ *and* $(ab)^n = b^n a^n$ *for* $n > 1$.

Theorem 1. *Let* S *be an AG*-groupoid. If* $ab^m = b^{m+1}$ *and* $ba^n = a^{n+1}$ *for* $a, b \in S$ *and positive integers* m, n *then* $a\rho b$.

Proof. For the sake of definiteness assume that $m < n$ and $m > 1$. Then by multiplying, $ab^m = b^{m+1}$ by b^{n-m} and successively applying Proposition 1, identities (1) and (2), we obtain

$$\begin{aligned} b^{m+1}b^{n-m} &= (ab^m)b^{n-m} = a(b^{m-1}b)b^{n-m} = (b^{m-1}a)bb^{n-m} \\ &= (b^{n-m}b)(b^{m-1}a) = (bb^{n-m})(b^{m-1}a) = b^{n-m}(b(b^{m-1}a)) \\ &= b^{n-m}((ab)b^{m-1}) = ((ab)b^{n-m})b^{m-1} = (b^{n-m+1}a)b^{m-1} \\ &= a(b^{n-m+1}b^{m-1}) = ab^n. \end{aligned}$$

Thus $ab^n = b^{n+1}$, $ba^n = a^{n+1}$ and so $a\rho b$. □

Theorem 2. *The relation* ρ *on an AG*-groupoid is a congruence relation.*

Proof. Evidently ρ is reflexive and symmetric. For transitivity we may proceed as follows.

Let $a\rho b$ and $b\rho c$ so that there exist positive integers n, m such that,

$$ab^n = b^{n+1}, \quad ba^n = a^{n+1} \quad \text{and} \quad bc^m = c^{m+1}, \quad cb^m = b^{m+1}.$$

Let $k = (n+1)(m+1) - 1$, that is, $k = n(m+1) + m$. Using identities (1), (2) and Propositions 2 and 3, we get

$$\begin{aligned}
ac^k &= ac^{n(m+1)+m} = a(c^{n(m+1)}c^m) = a((c^{m+1})^n c^m) = a((bc^m)^n c^m) \\
&= a((b^n c^{mn})c^m) = a(c^{m(n+1)}b^n) = (b^n a)c^{m(n+1)} = (b^n a)(c^{m(n+1)-1}c) \\
&= (b^n c^{m(n+1)-1})(ac) = ((ac)c^{m(n+1)-1})b^n = (c(ac^{m(n+1)-1}))b^n \\
&= (b^n(ac^{m(n+1)-1}))c = ((ab^n)c^{m(n+1)-1})c = (b^{n+1}c^{m(n+1)-1})c \\
&= ((bb^n)c^{m(n+1)-1})c = (b^n(bc^{m(n+1)-1}))c = (c(bc^{m(n+1)-1}))b^n \\
&= ((bc)c^{m(n+1)-1})b^n = (b^n c^{m(n+1)-1})(bc) = (b^n b)(c^{m(n+1)-1}c) \\
&= b^{n+1}c^{m(n+1)} = (bc^m)^{n+1} = c^{(m+1)(n+1)} = c^{k+1}.
\end{aligned}$$

Similarly, $ca^k = a^{k+1}$. Thus ρ is an equivalence relation. To show that ρ is compatible, assume that $a\rho b$ such that for some positive integer n,

$$ab^n = b^{n+1} \quad \text{and} \quad ba^n = a^{n+1}.$$

Let $c \in S$. Then by identity (2) and Propositions 4 and 1, we get

$$(ac)(bc)^n = (ac)(b^n c^n) = (ab^n)(cc^n) = b^{n+1}c^{n+1}.$$

Similarly, $(bc)(ac)^n = (ac)^{n+1}$. Hence ρ is a congruence relation on S. □

Theorem 3. *The relation ρ is separative.*

Proof. Let $a, b \in S$, $ab\rho a^2$ and $ab\rho b^2$. Then by definition of ρ there exist positive integers m and n such that,

$$\begin{aligned}
(ab)(a^2)^m &= (a^2)^{m+1}, \qquad a^2(ab)^m = (ab)^{m+1}, \\
(ab)(b^2)^n &= (b^2)^{n+1}, \qquad b^2(ab)^n = (ab)^{n+1}.
\end{aligned}$$

Now using identities (3), (2), (1) and Proposition 1, we get

$$\begin{aligned}
ba^{2m+1} &= b(a^{2m}a) = (ab)a^{2m} = (ab)(a^m a^m) = (aa^m)(ba^m) \\
&= a^{m+1}(ba^m) = (ba^{m+1})a^m = (b(a^m a))a^m = ((a^m b)a)a^m \\
&= (a^m a)(a^m b) = (aa^m)(a^m b) = a^m(a(a^m b)) \\
&= a^m((ba)a^m) = ((ba)a^m)a^m = ((a^m a)b)a^m \\
&= (a^{m+1}b)a^m = b(a^{m+1}a^m) = ba^{2m+1} = b(a^{2m}a) \\
&= (ab)a^{2m} = (ab)(a^2)^m = (a^2)^{m+1} = a^{2m+2}.
\end{aligned}$$

Using identities (3), (2) and (1) and Theorem 2, 3, we get

$$\begin{aligned} ab^{2n+1} &= a(b^{2n}b) = (ba)b^{2n} = (ba)(b^nb^n) = (bb^n)(ab^n) \\ &= (b^n(bb^n))a = ((b^nb^n)b)a = (ab)(b^nb^n) \\ &= (ab)(b^{2n}) = (ab)(b^2)^n = (b^2)^{n+1} = b^{2n+2}. \end{aligned}$$

Now by Theorem 1, $a\rho b$. Hence ρ is separative. □

The following Lemma has been proved in [10]. We re-state it without proof for use in our later results.

Lemma 1. *Let σ be a separative congruence on an AG^*-groupoid S, then for all $a, b \in S$ it follows that $ab\sigma ba$.*

Theorem 4. *Let S be an AG^*-groupoid. Then S/ρ is a maximal separative commutative image of S.*

Proof. By Theorem 3, ρ is separative, and hence S/ρ is separative. We now show that ρ is contained in every separative congruence relation σ on S. Let $a\rho b$ so that there exists a positive integer n such that,

$$ab^n = b^{n+1} \quad \text{and} \quad ba^n = a^{n+1}.$$

We need to show that $a\sigma b$, where σ is a separative congruence on S. Let k be any positive integer such that,

$$ab^k\sigma b^{k+1} \quad \text{and} \quad ba^k\sigma a^{k+1}.$$

Suppose $k \geqslant 2$. Putting $ab^0 = a$ in the next term (if $k = 2$)

$$\begin{aligned} (ab^{k-1})^2 &= (ab^{k-1})(ab^{k-1}) = a^2b^{2k-2} = (aa)(b^{k-2}b^k) \\ &= (ab^{k-2})(ab^k) = (ab^{k-2})b^{k+1}, \end{aligned}$$

i.e., $ab^{k-2})(ab^k)\sigma(ab^{k-2})b^{k+1}$.

Using identity (1) and Proposition 2 we get

$$\begin{aligned} (ab^{k-2})b^{k+1} &= (b^{k+1}b^{k-2})a = b^{2k-1}a = (b^kb^{k-1})a = (ab^{k-1})b^k, \\ (ab^{k-1})b^k &= (b^kb^{k-1})a = b^{2k-1}a = (b^{k-1}b^k)a = (ab^k)b^{k-1}. \end{aligned}$$

Thus $(ab^{k-1})^2\sigma(ab^k)b^{k-1}$.

Since $ab^k\sigma b^{k+1}$ and $(ab^k)b^{k-1}\sigma b^{k+1}b^{k-1}$, hence $(ab^{k-1})^2\sigma(b^k)^2$. It further implies that, $(ab^{k-1})^2\sigma(ab^{k-1})b^k\sigma(b^k)^2$. Thus $ab^{k-1}\sigma b^k$. Similarly, $ba^{k-1}\sigma a^k$.

Thus if (1) holds for k, it holds for $k+1$. By induction down from k, it follows that (1) holds for $k=1$, $ab\sigma b^2$ and $ba\sigma a^2$. Hence by Lemma 1 and separativity of σ it follows that $a\sigma b$. □

Lemma 2. *If $xa = x$ for some x and for some a in an AG^*-groupoid, then $x^n a = x^n$ for some positive integer n.*

Proof. Let $n = 2$, then identity (3) implies that

$$x^2a = (xx)a = x(xa) = xx = x^2.$$

Let the result be true for k, that is $x^k a = x^k$. Then by identity (3) and Proposition 1, we get

$$x^{k+1}a = (xx^k)a = x^k(xa) = x^k x = x^{k+1}.$$

Hence $x^n a = x^n$ for all positive integers n. □

Theorem 5. *Let a be a fixed element of an AG^*-groupoid S, then*

$$Q = \{x \in S \mid xa = x \text{ and } a = a^2\}$$

is a commutative subsemigroup.

Proof. As $aa = a$, we have $a \in Q$. Now if $x, y \in Q$ then by identity (2),

$$xy = (xa)(ya) = (xy)(aa) = (xy)a.$$

To prove that Q is commutative and associative, assume that x and y belong to Q. Then by using identity (1), we get $xy = (xa)y = (ya)x = yx$, and commutativity gives associativity. Hence Q is a commutative subsemigroup of S. □

Theorem 6. *Let η and ξ be separative congruences on an AG^*-groupoid S and $x^2a = x^2$, for all $x \in S$. If $\eta \cap (Q \times Q) \subseteq \xi \cap (Q \times Q)$, then $\eta \subseteq \xi$.*

Proof. If $x\eta y$ then,

$$(x^2(xy))^2 \eta (x^2(xy)(x^2y^2)\eta (x^2y^2)^2.$$

It follows that $(x^2(xy))^2, (x^2y^2)^2 \in Q$. Now by identities (2), (1), (3), respectively and Lemma 2, it means that,

$$\begin{aligned}(x^2(xy))(x^2y^2) &= (x^2x^2)((xy)y^2) = (x^2x^2)(y^3x)\\ &= x^4(y^3x) = (xx^4)y^3 = x^5y^3,\\ (x^5y^3)a &= (x^5y^3)(aa) = (x^5a)(y^3a) = x^5y^3.\end{aligned}$$

So, $x^2(xy)(x^2y^2) \in Q$. Hence $(x^2(xy))^2\xi(x^2(xy)(x^2y^2)\xi(x^2y^2)^2$ implies that $x^2(xy)\xi x^2y^2$.

Since $x^2y^2\eta x^4$ and $x^2a = x^2$ for all $x \in S$, so $(x^2y^2), x^4 \in Q$. Thus $x^2y^2\xi x^4$ and it follows from Proposition 4 that $x^2y^2 = (xy)^2$. So $(x^2)^2\xi x^2(xy)\xi(xy)^2$ which means that $x^2\xi xy$. Finally, $x^2\eta y^2$ and $x^2, y^2 \in Q$, means that $x^2\xi y^2, x^2\xi xy\xi y^2$. As ξ is separative so $x\xi y$. Hence $\eta \subseteq \xi$ and by Lemma 1, S/η is the maximal separative commutative image of S. □

References

[1] **P. Holgate**: *Groupoids satisfying a simple invertive law*, The Math. Stud. **61** (1992), 101 – 106.

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

[3] **Q. Mushtaq**: *Abelian groups defined by LA-semigroups*, Studia Sci. Math. Hungar. **18** (1983), 427 – 428.

[4] **Q. Mushtaq and Q. Iqbal**: *Decomposition of a locally associative LA-semigroup*, Semigroup Forum **41** (1990), 154 – 164.

[5] **Q. Mushtaq and Q. Iqbal**: *On representation theorem for inverse LA-semigroups*, Proc. Pakistan Acad. Sci. **30** (1993), no. 4.

[6] **Q. Mushtaq and M. Khan**: *Ideals in AG-band and AG*-groupoid*, Quasigroups and Related Systems **14** (2006), 207 – 216.

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

[8] **P. V. Protić and N. Stevanović**: *On Abel-Grassmann's groupoids*, Proc. Math. Conf. Pristina, 1994, 31 – 38.

[9] **P. V. Protić and N. Stevanović**: *AG-test and some general properties of Abel-Grassmann's groupoids*, PU. M. A. **6** (1995), 371 – 383.

[10] **N. Stevanović and P. V. Protić**: *Some decomposition on Abel-Grassmann's groupoids*, PU. M. A. **8** (1997), 355 – 366.

Received October 9, 2006
Revised December 18, 2006

Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
E-mail: qmushtaq@isb.apollo.net.pk

Quasigroups and Related Systems **15** (2007), 309 – 316

On finite quasigroups whose subquasigroup lattices are distributive

Konrad Pióro

Abstract

We prove that if the subquasigroup lattice of a finite quasigroup Q is distributive, then Q is cyclic (i.e., Q is generated by one element) and also, each of its subquasigroups is also cyclic. Finally, we give examples which show that the inverse implication does not hold.

It is a classical result of Group Theory, showed by Ore in [5] (see also [7]), that the subgroup lattice of a group $\mathcal{G}$ is distributive if and only if $\mathcal{G}$ is locally cyclic (i.e., each finitely generated subgroup of $\mathcal{G}$ is cyclic). In particular, a finite group $\mathcal{G}$ has a distributive subgroup lattice if and only if $\mathcal{G}$ is cyclic.

In the present paper we prove the following result for quasigroups (for definitions and simple facts of quasigroups and lattices see e.g. [1], [2], [3])

Theorem 1. *Let $\mathcal{Q} = (Q, \circ, \backslash, /)$ be a finite quasigroup such that its subquasigroup lattice $\mathcal{S}(\mathcal{Q})$ is distributive. Then $\mathcal{Q}$ and each subquasigroup of $\mathcal{Q}$ are cyclic.*

Before the proof observe that, in the contrary to groups, a subquasigroup of a cyclic quasigroup need not be cyclic. Let $\mathcal{Q}$ be a six-element quasigroup given by the following table (recall, see e.g. [1], that a finite groupoid $(Q, \circ)$ is a quasigroup if and only if the multiplication table of $\circ$ is a Latin square, i.e., each element of Q occurs exactly once in each row and each column)

2000 Mathematics Subject Classification: 05B15, 06D05, 06B15, 20N05, 08A30.
Keywords: quasigroup, cyclic quasigroup, subquasigroup, subquasigroup lattice, distributive lattice.

∘	a	b	c	d	e	f
a	a	c	b	f	e	d
b	c	b	a	d	f	e
c	b	a	c	e	d	f
d	f	d	e	c	a	b
e	e	f	d	a	b	c
f	d	e	f	b	c	a

Then $\mathcal{Q} = \langle f \rangle = \langle e \rangle = \langle d \rangle$, so $\mathcal{Q}$ is cyclic. On the other hand, $\{a, b, c\}$ is a subquasigroup of $\mathcal{Q}$ which is non-cyclic, because $a \circ a = a$, $b \circ b = b$ and $c \circ c = c$. Note that the constructed quasigroup $\mathcal{Q}$ is even commutative.

Observe also that such example cannot be found among quasigroups having less than 6 elements. More precisely, it is easy to see that any two-element quasigroup is cyclic. So if a quasigroup $\mathcal{Q}$ contains a non-cyclic subquasigroup $\mathcal{G}$, then $\mathcal{G}$ must have at least three elements, say a, b, c. Next, there is $q \in Q$ which generate $\mathcal{Q}$, in particular $q \in Q \setminus G$. The elements $q \circ a$, $q \circ b$ and $q \circ c$ are pairwise different. They are also different from a, b, c (more precisely, $\{q \circ a, q \circ b, q \circ c\} \cap G = \emptyset$, because $a, b, c \in G$ and $\mathcal{G}$ is a quasigroup). At most one of them may be equal q. Thus we have obtained at least six different elements of $\mathcal{Q}$.

Theorem 1 is straightforward implied by the following more general lemma (where $\wedge$ and $\vee$ are lattice operations of infimum and supremum respectively)

Lemma 1. *Let $\mathcal{Q} = (Q, \circ, \backslash, /)$ be a finite quasigroup such that for any two different elements $p, q \in Q$*

$$(*)\ \ \langle p \circ q \rangle = (\langle p \circ q \rangle \wedge \langle p \rangle) \vee (\langle p \circ q \rangle \wedge \langle q \rangle).$$

Then all subquasigroups of $\mathcal{Q}$ are cyclic.

Obviously if the subquasigroup lattice $\mathcal{S}(\mathcal{Q})$ is distributive, then $(*)$ holds. Because $\langle p \circ q \rangle = \langle p \circ q \rangle \wedge \langle p, q \rangle = \langle p \circ q \rangle \wedge (\langle p \rangle \vee \langle q \rangle) = (\langle p \circ q \rangle \wedge \langle p \rangle) \vee (\langle p \circ q \rangle \wedge \langle q \rangle)$.

Proof. Assume that $\mathcal{Q}$ contains subquasigroups which are non-cyclic. Take a family $\mathcal{A}$ of all such subquasigroups. Since $\mathcal{Q}$ is a finite quasigroup, $\mathcal{A}$ is a finite set which is partially ordered by set-inclusion. Thus $(\mathcal{A}, \subseteq)$ contains at least one minimal element, say $\mathcal{G}$. Then $\mathcal{G}$ is a subquasigroup of $\mathcal{Q}$ such that

(*i*) $\mathcal{G}$ is non-cyclic,

(*ii*) each proper (i.e., non-empty and non-equal $\mathcal{G}$) subquasigroup of $\mathcal{G}$ is cyclic.

Further,

(*iii*) $\mathcal{G}$ is generated by two elements.

More precisely, $\mathcal{G}$ is finite, so $\mathcal{G}$ is generated by some elements $g_1, g_2, \ldots, g_k$, i.e.,

$$\mathcal{G} = \langle g_1, g_2, \ldots, g_k \rangle.$$

Take the new subquasigroup $\langle g_1, g_2 \rangle \leq \mathcal{G}$. If $\mathcal{G} \neq \langle g_1, g_2 \rangle$, then $\langle g_1, g_2 \rangle$ is a cyclic subquasigroup. Let $\langle g_1, g_2 \rangle = \langle g' \rangle$ for some $g' \in G$. Then

$$\mathcal{G} = \langle g', g_3, \ldots, g_k \rangle.$$

Thus by simple induction on k we obtain that $\mathcal{G}$ is generated by two elements.

Let $\mathcal{B}$ be a set of all pairs (g_1, g_2) of elements of $\mathcal{G}$ which generate $\mathcal{G}$ (i.e., $\langle g_1, g_2 \rangle = \mathcal{G}$). Note that $\mathcal{B}$ is finite and non-empty.

Now from the set

$$\{g_1 \in G \colon (g_1, g_2) \in \mathcal{B} \text{ for some } g_2 \in \mathcal{G}\}$$

we choose an element g such that

$$|\langle g \rangle| = \min\{|\langle g_1 \rangle| \colon (g_1, g_2) \in \mathcal{B} \text{ for some } g_2 \in G\} \tag{1}$$

Next, from the set

$$\{g_2 \in G \colon (g, g_2) \in \mathcal{B}\}$$

we choose an element h such that

$$|\langle h \rangle| = \min\{|\langle g_2 \rangle| \colon (g, g_2) \in \mathcal{B}\} \tag{2}$$

Observe that

$$g \circ h \notin \langle g \rangle \quad \text{and} \quad g \circ h \notin \langle h \rangle \tag{3}$$

Assume for example that $g \circ h \in \langle g \rangle$. Then $h = g \backslash (g \circ h) \in \langle g \rangle$, so $\langle h \rangle \subseteq \langle g \rangle$, and consequently $\mathcal{G} = \langle g, h \rangle = \langle g \rangle$. But it is a contradiction with the assumption that $\mathcal{G}$ is not cyclic.

Thus $\langle g\rangle$, $\langle h\rangle$ and $\langle g\circ h\rangle$ are three different subquasigroups of $\mathcal{G}$. Of course $\langle g\rangle$ and $\langle h\rangle$ are not comparable (otherwise $\mathcal{G}$ would be cyclic).

By the condition $(*)$ we have

$$\langle g\circ h\rangle = (\langle g\circ h\rangle \wedge \langle g\rangle) \vee (\langle g\circ h\rangle \wedge \langle h\rangle).$$

Let

$$\mathcal{G}_1 = \langle g\circ h\rangle \wedge \langle g\rangle = \langle g\circ h\rangle \cap \langle g\rangle$$

and

$$\mathcal{G}_2 = \langle g\circ h\rangle \wedge \langle h\rangle = \langle g\circ h\rangle \cap \langle h\rangle$$

Then $\mathcal{G}_1 \subseteq \langle g\rangle$ and $\mathcal{G}_2 \subseteq \langle h\rangle$. Moreover,

$$\mathcal{G}_1 \neq \langle g\rangle \quad \text{or} \quad \mathcal{G}_2 \neq \langle h\rangle \tag{4}$$

Assume that both equalities hold. Then g and h both belong to $\langle g\circ h\rangle$, because $\mathcal{G}_1$ and $\mathcal{G}_2$ are contained in $\langle g\circ h\rangle$. Hence $\langle g,h\rangle$ is contained in $\langle g\circ h\rangle$, and consequently $\mathcal{G} = \langle g,h\rangle = \langle g\circ h\rangle$, which is impossible.

Since $\mathcal{G}_1 \subseteq \langle g\rangle \subsetneqq \mathcal{G}$, we have by the minimality of $\mathcal{G}$, that $\mathcal{G}_1$ is cyclic, i.e.,

$$\mathcal{G}_1 = \langle g_1\rangle \ \text{ for some } g_1.$$

Analogously, $\mathcal{G}_2$ is also cyclic, i.e.,

$$\mathcal{G}_2 = \langle h_1\rangle \ \text{ for some } h_1.$$

Assume first that

$$\langle g_1\rangle \subsetneqq \langle g\rangle \tag{a.1}$$

Then $|\langle g_1\rangle| \lneqq |\langle g\rangle|$. So by the choice of g we obtain that for each element $\overline{h}$ of $\mathcal{G}$, g_1 and $\overline{h}$ don't generate $\mathcal{G}$. In particular,

$$\langle g_1,h\rangle \subsetneqq \mathcal{G}.$$

Hence $\langle g_1,h\rangle$ has less elements than $\mathcal{G}$, so (by the minimality of $\mathcal{G}$) $\langle g_1,h\rangle$ is cyclic. Let $\overline{g_1}$ be an element of $\mathcal{G}$ such that

$$\langle g_1,h\rangle = \langle \overline{g_1}\rangle.$$

On the other hand,

$$\mathcal{G}_1 \subseteq \langle g_1,h\rangle, \quad \mathcal{G}_2 \subseteq \langle h\rangle \subseteq \langle g_1,h\rangle$$

and

$$\langle g \circ h \rangle = \mathcal{G}_1 \vee \mathcal{G}_2.$$

Thus

$$g \circ h \in \langle g \circ h \rangle \subseteq \langle g_1, h \rangle = \langle \overline{g_1} \rangle.$$

Since $\langle \overline{g_1} \rangle$ contains $g \circ h$ and h, we obtain that $\langle \overline{g_1} \rangle$ contains also g, because $g = (g \circ h)/h$. Hence, the cyclic quasigroup $\langle \overline{g_1} \rangle$ contains g and h, which implies

$$\mathcal{G} = \langle g, h \rangle = \langle \overline{g_1} \rangle.$$

But it is impossible, because we have assumed that $\mathcal{G}$ is not cyclic.

Now assume that

$$\mathcal{G}_2 = \langle h_1 \rangle \subsetneqq \langle h \rangle \tag{a.2}$$

Then

$$|\langle h_1 \rangle| \lneqq |\langle h \rangle|,$$

so by the choice of h we obtain that g and h_1 don't generate $\mathcal{G}$, i.e.,

$$\langle g, h_1 \rangle \subsetneqq \mathcal{G}.$$

Hence, $\langle g, h_1 \rangle$ has less elements than $\mathcal{G}$, so $\langle g, h_1 \rangle$ is cyclic (by the minimality of $\mathcal{G}$). Let $\overline{h_1}$ be an element of $\mathcal{G}$ such that

$$\langle g, h_1 \rangle = \langle \overline{h_1} \rangle.$$

Similarly as in the first case we have

$$g \circ h \in \langle g \circ h \rangle = \mathcal{G}_1 \vee \mathcal{G}_2 = \langle g_1, h_1 \rangle \subseteq \langle g, h_1 \rangle.$$

Since $\langle \overline{h_1} \rangle = \langle g, h_1 \rangle$ contains $g \circ h$ and g, we have that $\langle \overline{h_1} \rangle$ contains also h, because $h = g \backslash (g \circ h)$. This fact implies that

$$\mathcal{G} = \langle g, h \rangle = \langle \overline{h_1} \rangle.$$

Thus we again obtain a contradiction.

Summarizing we have shown that $\mathcal{G}_1 = \langle g \rangle$ and $\mathcal{G}_2 = \langle h \rangle$. But it contradicts (4), which completes the proof. □

Obviously any groupoid (in particular, each quasigroup) with at most three elements in which each subgroupoid is cyclic, has at most four subgroupoids (together with the empty subgroupoid). In particular, its subgroupoid lattice is distributive.

Unfortunately, there is a four-element quasigroup with a non-distributive subquasigroup lattice, although each of its subquasigroups is cyclic. For example, let $\mathcal{Q} = \{a, b, c, d\}$ be a quasigroup defined by the following multiplication table

∘	a	b	c	d
a	c	a	d	b
b	d	b	a	c
c	b	d	c	a
d	a	c	b	d

Then $\langle a\rangle = \langle b, c\rangle = \langle b, d\rangle = \langle c, d\rangle = \mathcal{Q}$, and $\langle b\rangle = \{b\}, \langle c\rangle = \{c\}, \langle d\rangle = \{d\}$. Thus $\mathcal{Q}$ has exactly five subquasigroups $\emptyset, \langle b\rangle, \langle c\rangle, \langle d\rangle$ and $\mathcal{Q}$. These subquasigroups form the non-distributive lattice $\mathcal{M}_5$, so $\mathcal{S}(\mathcal{Q})$ is not distributive. Observe also that, for example, elements b and d (together with $b \circ d = c$) do not satisfy $(*)$ of Lemma 1.

Now we show that even commutativity is not enough as an additional assumption. Let $\mathcal{Q}$ be a commutative five-element quasigroup such that

∘	a	b	c	d	e
a	a	c	d	b	e
b	c	b	e	d	a
c	d	e	c	a	b
d	b	d	a	e	c
e	e	a	b	c	d

Then $\langle a\rangle = \{a\}, \langle b\rangle = \{b\}, \langle c\rangle = \{c\}$ and $\langle e\rangle = \langle d\rangle = \langle a, b\rangle = \langle a, c\rangle = \langle b, c\rangle = \mathcal{Q}$. Thus $\emptyset, \langle a\rangle, \langle b\rangle, \langle c\rangle$ and $\mathcal{Q}$ are all pairwise different subquasigroups of $\mathcal{Q}$. Moreover, the lattice $\mathcal{S}(\mathcal{Q})$ is isomorphic with $\mathcal{M}_5$, so it is not distributive. Note also that elements a and b do not satisfy $(*)$ of Lemma 1.

Remark 1. For any commutative quasigroup $\mathcal{Q}$ with at most four elements, if each subquasigroup of $\mathcal{Q}$ is cyclic, then the subquasigroup lattice $\mathcal{S}(\mathcal{Q})$ is distributive.

It is true for an arbitrary groupoid with at most three elements, so we take a four-element commutative quasigroup $\mathcal{Q}$. Note that if each subquasigroup of $\mathcal{Q}$ is cyclic, then $\mathcal{Q}$ has at most $|Q| + 1 = 5$ subquasigroups (because the empty set is also a subquasigroup). But if a quasigroup has at most four subquasigroups, then of course it has distributive subquasigroup lattice. Thus we can take $\mathcal{Q}$ with exactly five subquasigroups (three proper subquasigroups).

Assume that $\mathcal{S}(\mathcal{Q})$ is not distributive. Then $\mathcal{S}(\mathcal{Q})$ is isomorphic with the non-modular lattice $\mathcal{N}_5$ or with the non-distributive lattice $\mathcal{M}_5$.

First we consider the case when $\mathcal{S}(\mathcal{Q})$ is isomorphic with $\mathcal{N}_5$. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be proper subquasigroups of $\mathcal{Q}$ such that $\mathcal{G}_1 \subsetneqq \mathcal{G}_2$. Let $\emptyset \neq \mathcal{G}_3 \subsetneqq \mathcal{Q}$ be the subquasigroup which is not comparable with $\mathcal{G}_1$ and $\mathcal{G}_2$ (i.e., $\mathcal{G}_3 \cap \mathcal{G}_2 = \emptyset$ and $\mathcal{G}_3 \vee \mathcal{G}_1 = \mathcal{Q}$). Let q generates $\mathcal{Q}$; and g_1, g_2, g_3 generate $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$ respectively. Of course q, g_1, g_2, g_3 are pairwise different elements, i.e., $Q = \{q, g_1, g_2, g_3\}$. Moreover, it is easy to see that $G_1 = \{g_1\}$, $G_2 = \{g_1, g_2\}$ and $G_3 = \{g_3\}$. In other words we have

$$g_1 \circ g_1 = g_1, \;\; g_3 \circ g_3 = g_3, \;\; g_2 \circ g_2 = g_1.$$

By the first equality and the definition of quasigroup we have also

$$g_2 \circ g_1 = g_2 \;\; \text{and} \;\; g_1 \circ g_2 = g_2,$$

because each of equations $x \circ g_1 = g_1$ and $g_1 \circ x = g_1$ has exactly one solution.

These all equalities imply that $g_3 \circ g_1$ and $g_3 \circ g_2$ cannot be equal g_3, g_1 and g_2. Thus $g_3 \circ g_1 = q$ and $g_3 \circ g_2 = q$. But it is impossible, because the equation $g_3 \circ x = q$ has two different solutions. This contradiction shows that $\mathcal{S}(\mathcal{Q})$ cannot be isomorphic with $\mathcal{N}_5$.

Now assume that $\mathcal{S}(\mathcal{Q})$ is isomorphic with $\mathcal{M}_5$. Then there are pairwise different proper and non-comparable subquasigroups $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$ of $\mathcal{Q}$. Let g_1, g_2, g_3 generate these three subquasigroups, respectively. Let q be a generator of $\mathcal{Q}$. Of course q, g_1, g_2, g_3 are pairwise different, so $Q = \{q, g_1, g_2, g_3\}$. Hence we obtain $G_1 = \{g_1\}, G_2 = \{g_2\}, G_3 = \{g_3\}$. So

$$g_1 \circ g_1 = g_1, \quad g_2 \circ g_2 = g_2, \quad g_3 \circ g_3 = g_3.$$

Moreover, since q generate $\mathcal{Q}$ we have that $q \circ q \neq q$. Of course we can assume that $q \circ q = g_1$. Then $q \circ g_1 = g_1 \circ q$ is different from g_1 (because the equation $q \circ x = g_1$ has exactly one solution) and $q \circ g_1$ is not equal q (because q generates $\mathcal{Q}$). Of course we can assume that $g_1 \circ q = q \circ g_1 = g_2$ (replacing g_3 by g_2 if necessary).

Now observe that equalities $q \circ q = g_1$, $g_1 \circ q = g_2$ and $g_3 \circ g_3 = g_3$ imply that $g_3 \circ q$ cannot equals g_1, g_2 and g_3. So $g_3 \circ q = q$. Analogously $q \circ g_1 = g_2$, $g_1 \circ g_1 = g_1$ and $g_3 \circ g_3 = g_3$ imply $g_3 \circ g_1 = q$. But these equalities cannot hold in a quasigroup, because $g_1 \neq q$. This contradiction completes the proof.

At the end of the paper observe that if $\mathcal{G}$ is a finite group satisfying the condition $(*)$ from Lemma 1, then $\mathcal{G}$ is cyclic, and consequently its subgroup lattice $\mathcal{S}(\mathcal{G})$ is distributive. But the following example shows that for finite (and even commutative) quasigroups the condition $(*)$ is indeed weaker.

Let $\mathcal{Q} = (Q, \circ)$ be a commutative six-element quasigroup such that

$\circ$	a	b	c	d	e	f
a	a	c	f	e	b	d
b	c	b	a	f	d	e
c	f	a	d	b	e	c
d	e	f	b	d	c	a
e	b	d	e	c	a	f
f	d	e	c	a	f	b

Then $\langle a\rangle = \{a\}$, $\langle b\rangle = \{b\}$, $\langle d\rangle = \{d\}$ and $\langle c\rangle = \langle e\rangle = \langle f\rangle = \langle a, b\rangle = \langle a, d\rangle = \langle b, d\rangle = \mathcal{Q}$. So $\mathcal{Q}$ has exactly five subquasigroups (together with the empty subquasigroup) which form the non-distributive lattice $\mathcal{M}_5$.

On the other hand, we obtain by a straightforward verification that $\mathcal{Q}$ satisfies $(*)$. More precisely, if $g \in \{c, e, f\}$, then $\langle g \circ h\rangle \wedge \langle g\rangle = \langle g \circ h\rangle \wedge \mathcal{Q} = \langle g \circ h\rangle$; so $(*)$ holds. The analogous situation we have for $h \in \{c, e, f\}$. If $g, h \in \{a, b, d\}$, then $g \circ h \in \{c, e, f\}$; so $\langle g \circ h\rangle = \mathcal{Q}$ which implies $(*)$ (because then $\langle g \circ h\rangle \wedge \langle g\rangle = \langle g\rangle$ and $\langle g \circ h\rangle \wedge \langle h\rangle = \langle h\rangle$, thus the right hand side of $(*)$ equals $\langle g\rangle \vee \langle h\rangle = \mathcal{Q}$).

References

[1] **S. Burris and H. P. Sankappanawar**: *A Course in Universal Algebra*, Springer-Verlag, New York-Berlin, 1981.

[2] **G. Grätzer**: *Universal Algebra*, second edition, Springer-Verlag, New York-Heidelberg 1979.

[3] **G. Grätzer**: *General Lattice Theory*, second edition, Birkhäuser Verlag, Basel 1998.

[4] **O. Ore**: *Structures and group theory I*, Duke Math. J. **3** (1937), 149 – 173.

[5] **O. Ore**: *Structures and group theory II*, Duke Math. J. **4** (1938), 247 – 269.

[6] **K. Pióro**: *On some finite groupoids with distributive subgroupoid lattices*, Discuss. Math. Gen. Algebra Appl. **22** (2002), 25 – 31.

[7] **R. Schmidt**: *Subgroup Lattices of Groups*, Walter de Gruyter, New York 1994.

Received February 26, 2007

Institute of Mathematics, Warsaw University, ul. Banacha 2, PL-02-097 Warsaw, Poland
E-mail: kpioro@mimuw.edu.pl