Quasigroups and Related Systems **12** (2004), 1 − 12

Extending sloops of cardinality 16 to SQS-skeins with all possible congruence lattices

Magdi H. Armanious and Enas M. A. Elzayat

Abstract

It is well known that each STS(15) with a sub-$STS(7)$ is derived [11]. In this article, we will improve this result by showing that each non-simple sloop L of cardinality 16 with any possible congruence lattice $C(L)$ can be extended to a non-simple SQS-skein S of cardinality 16 with all possible congruence lattices for $C(S)$. Accordingly, we may say that any triple system $STS(15)$ with m sub-$STS(7)$s is a derived triple system from an $SQS(16)$ having n sub-$SQS(8)$s for all possible non-zero numbers of m and n.

1. Introduction

A *Steiner quadruple* (*triple*) *system* is a pair $(L;B)$, where L is a finite set and B is a collection of 4-subsets (3-subsets) called blocks of L such that every 3-subset (2-subset) of L is contained in exactly one block of B [9], [10]. Let $SQS(m)$ denote a Steiner quadruple system (briefly: quadruple system) of cardinality m and $STS(n)$ denote Steiner triple system (briefly: triple system) of 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. [9], [10]).

Let $\mathbf{L} = (L;B)$ be a quadruple system. If one considers $L_x = L - \{x\}$ for any point $x \in L$ and deletes that point from all blocks which contain it then the resulting system $(L_x; B(x))$ is a triple system, where $B(x) = \{b^{‘} = b - \{x\} : b \in B$ and $x \in b\}$. Now, $(L_x; B(x))$ is called a derived triple system (or briefly DTS) of $(L;B)$ (cf. [9], [10]).

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

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

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

Notice that for any a and $b \in L$ the equation $a \cdot x = b$ has the unique solution $x = a \cdot (a \cdot x) = a \cdot b$, i. e., $\mathbf{L}$ is a quasigroup.

A sloop $\mathbf{L}$ is called *Boolean* if it satisfies in addition the associative law.

Also, there is one to one correspondence between SQSs and SQS-skeins (cf. [9], [10]). An SQS-skein $(S;q)$ is an algebra with a unique ternary operation q satisfying:

$$\begin{aligned} q(x,y,z) &= q(x,z,y) = q(z,x,y), \\ q(x,x,y) &= y, \\ q(x,y,q(x,y,z)) &= z. \end{aligned}$$

Since the equation $q(a,b,x) = c$ has the unique solution $q(a,b,c) = x$ for $a,b,c \in S$, it follows that an SQS-skein $(S;q)$ is a ternary quasigroup (3-quasigroup).

An SQS-skein $(S;q)$ is called *Boolean* if it satisfies in addition the identity: $q(a,x,q(a,y,z)) = q(x,y,z)$.

The sloop associated with a derived triple system is also called derived.

A subsloop $\mathbf{N}$ of $\mathbf{L}$ (sub-SQS-skein of $\mathbf{S}$) is called *normal* if and only if $\mathbf{N} = [1]\theta$ ($\mathbf{N} = [x]\theta$) for a congruence θ on $\mathbf{L}$(*respectively*, $\mathbf{S}$) (cf. [1], [12]).

A subsloop $\mathbf{N}$ is called normal if and only if

$$x \cdot (y \cdot N) = (x \cdot y) \cdot N$$

for all $x, y \in L$ [12].

There is an isomorphism between the lattice of normal subsloops (sub-SQS-skeins containing a fixed element) and the congruence lattice of the sloop (SQS-skein) (cf. [1], [12]). Quackenbush in [12] and similarly the author in [1] have proven that the congruences of sloops (of SQS-skeins) are permutable, regular and uniform. Moreover, they proved the following property well known from groups.

Theorem 1. *Every subsloop (sub-SQS-skein) of a finite sloop $\mathbf{L} = (L; \cdot, 1)$ (SQS-skein $\mathbf{S} = (S;q)$) with cardinality $\frac{1}{2}|L|$ (respectively, $\frac{1}{2}|S|$) is normal.*

The variety of all sloops (SQS-skeins) is a Mal‘cev variety. Any Boolean group is a sloop that is called a *Boolean sloop.* If $(G;+)$ is a Boolean group, then $(G; q(x,y,z) = x + y + z)$ is a Boolean SQS-skein [1]. The class of all Boolean sloops (Boolean SQS-skeins) is the smallest non-trivial subvariety of the variety of all sloops (SQS-skeins).

In section 2, we will do an algebraic classification of the class of all sloops of cardinality 16 according to the shape of its congruence lattice and the concepts of solvability and nilpotence. We will show that this classification coincides with the combinatorial classification based on the number of subsystems of cardinality 7 (cf. [5], [7]) and the classification of the class of all SQS-skeins of cardinality 16 (cf. [1]).

Let $\mathbf{L}$ be a derived sloop from an SQS-skein $\mathbf{S}$, then the congruence lattice $C(\mathbf{S})$ of $\mathbf{S}$ is a sublattice of the congruence lattice $C(\mathbf{L})$ of $\mathbf{L}$. We are faced with the question: is any sloop $\mathbf{L}$ of cardinality 16 derived from an SQS-skein $\mathbf{S}$ for all possible sublattice $C(\mathbf{S})$ of the lattice $C(\mathbf{L})$?

Among the $DTS(15)$s determined in [11], there are 23 systems having a subsystem of order 7. In this article, it will be shown that any $STS(15)$ with n sub-$STS(7)$s can be extended to an $SQS(16)$ with $2n$ sub-$SQS(8)$s in particular and to an $SQS(16)$ with all possible number of sub-$SQS(8)$s in general.

Clearly any Boolean sloop is derived from a Boolean SQS-skein and both have the same congruence lattice. In subsection 3.1, we will show that any non-simple sloop $\mathbf{L}$ of cardinality 16 can be derived from an SQS-skein $\mathbf{S}$ in which both $\mathbf{L}$ and $\mathbf{S}$ have the same congruence lattice.

In [8] Guelzow constructed a semi-Boolean SQS-skein of cardinality 16 all of whose derived sloops are Boolean. Then, we may say that if the congruence lattices of all derived sloops of an SQS-skein are isomorphic, it is not necessary that the congruence lattice of this SQS-skein is isomorphic to them.

Subsection 3.2 is devoted to the proof that any non-simple sloop $\mathbf{L}$ of cardinality 16 can be extended to an SQS-skein $\mathbf{S}$ with any proper sub-lattice $C(\mathbf{S})$ of the lattice $C(\mathbf{L})$.

2. Algebraic classification of sloops of cardinality 16

We define the solvability of sloops similarly as the definition of solvability of SQS-skeins given in [1]. A congruence θ of a sloop $\mathbf{L}$ (an SQS-skein $\mathbf{S}$) will be called *Boolean* if $\mathbf{L}/\theta$ ($\mathbf{S}/\theta$) is Boolean. Clearly, the largest congruence of any sloop (SQS-skein) is Boolean and the intersection of any two Boolean congruences is Boolean.

A *Boolean series* of congruences on a sloop $\mathbf{L}$ (an SQS-skein $\mathbf{S}$) is a series of congruences

$$1 := \theta_0 \supseteq \theta_1 \supseteq \theta_2 \supseteq ... \supseteq \theta_n := 0$$

such that the factor algebra $[1]\theta_i/\theta_{i+1}$ (respectively, $[x]\theta_i/\theta_{i+1}$) is a Boolean sloop (respectively, SQS-skein) for all $i = 0, 1, ..., n-1$. If n is the smallest length of a Boolean series, then $\mathbf{L}$ (respectively, $\mathbf{S}$) is *solvable of length n*.

Centrality in Mal'cev varieties is defined in [13]. We apply this definition on sloops similarly as in SQS-skeins [1]. A congruence of a sloop $\mathbf{L}$ (an SQS-skein $\mathbf{S}$) is called *central*, if it contains the diagonal relation

$$\Delta_L = \{(a,a) : a \in L\} \quad (\Delta_S = \{(a,a) : a \in S\})$$

as a normal subsloop of $\mathbf{L}$ (respectively, sub-SQS-skein of $\mathbf{S}$). A central congruence of the sloop $\mathbf{L}$ (SQS-skein $\mathbf{S}$) is denoted by $\xi(\mathbf{L})$ (respectively, by $\xi(\mathbf{S})$). If there is a series of congruences on $\mathbf{L}$ (of $\mathbf{S}$)

$$1 := \theta_0 \supseteq \theta_1 \supseteq \theta_2 \supseteq \ldots \supseteq \theta_n := 0$$

such that $\theta_i/\theta_{i+1} \subseteq \xi(\mathbf{L}/\theta_{i+1})$ (respectively, $\theta_i/\theta_{i+1} \subseteq \xi(\mathbf{S}/\theta_{i+1})$) for all $i = 0, 1, ..., n-1$, then this series is called central series of $\mathbf{L}$ (of $\mathbf{S}$). Also, $\mathbf{L}$ (respectively, $\mathbf{S}$) is called nilpotent of class n, if n is the smallest length of central series in $\mathbf{L}$ (in $\mathbf{S}$). A construction of nilpotent sloops (SQS-skeins) of class n for each positive integer n is given in [3] and [4].

It is routine matter to see that the class of all solvable sloops (SQS-skeins) and the class of all nilpotent sloops (SQS-skeins) are varieties. It is easy to show that each central series of $\mathbf{L}$ (of $\mathbf{S}$) is a Boolean series (cf.[1]). Then we may say that the variety of nilpotent sloops (SQS-skeins) is a subvariety of the variety of solvable sloops (SQS-skeins) [1]. Notice that not every solvable sloop (SQS-skein) is nilpotent (examples of a solvable sloop $\mathbf{L}$ (SQS-skein $\mathbf{S}$), which is not nilpotent, will be given in Lemma 2 for $n = 1$ and 2).

By the definition of solvability, we may say that the cardinality $|L|$ ($|S|$) of a solvable sloop $\mathbf{L}$ (SQS-skeins $\mathbf{S}$) is equal to 2^n for a positive integer n. The class of solvable sloops (SQS-skeins) of order 1 and the nilpotent sloops (SQS-skeins) of class 1 are exactly the Boolean sloops (SQS-skeins). Notice that all sloops (SQS-skeins) of cardinality 2, 2^2 and 2^3 are Boolean and for any positive integer n, there is exactly one Boolean sloop (SQS-skein) (up to isomorphism) with cardinality 2^n that is the direct power of the 2-element group.

To determine the different classes of sloops of cardinality 16, let $\mathbf{L}$ (respectively, $\mathbf{S}$) be a non-simple sloop (SQS-skein) with $|L|= 16$ ($|S|= 16$) and $C(\mathbf{L})$ ($C(\mathbf{S})$) be its congruence lattice. If $C(\mathbf{L})$ ($C(\mathbf{S})$) has more than one atom, then $\mathbf{L}$ (respectively, $\mathbf{S}$) is Boolean. If $C(\mathbf{L})$ ($C(\mathbf{S})$) has exactly one atom θ, then $C(\mathbf{L}/\theta)$ (respectivelt, $C(\mathbf{S}/\theta)$) is isomorphic to the lattice of subgroups $Sub(\mathbb{Z}_2^n)$ for $n = 1, 2$ or 3, where $\mathbb{Z}_2$ is the 2-element group. This leads directly to a similar classification of the class of SQS-skeins of cardinality 16 (cf. [1], [2]).

Lemma 2. *Let $\mathbf{L}(\mathbf{S})$ be a sloop (an SQS-skein) of cardinality 16 and θ be an atom of the congruence lattice $C(\mathbf{L})$ ($C(\mathbf{S})$). Then $\mathbf{L}(\mathbf{S})$ is simple or $C(\mathbf{L}/\theta) \cong C(\mathbf{S}/\theta) \cong Sub(\mathbb{Z}_2^n)$ for $n = 1, 2, 3$ or $C(\mathbf{L}) \cong C(\mathbf{S}) \cong Sub(\mathbb{Z}_2^4)$. Moreover, $\mathbf{L}(\mathbf{S})$ is solvable of length 2 for $n = 1$ or 2, nilpotent of length 2 for $n = 3$ and Boolean for the last case.*

Proof. The proof for SQS-skeins is given in [1]. Similarly, one can easily prove the lemma for sloops. □

Any subsloop (sub-SQS-skein) of cardinality $\frac{1}{2}|L|$ ($\frac{1}{2}|S|$) corresponds to a maximal congruence in $C(\mathbf{L})$ ($C(\mathbf{S})$). The converse is true specially for sloops (SQS-skeins) of cardinality 16, which means that a maximum congruence in $C(\mathbf{L})$ ($C(\mathbf{S})$) corresponds to a subsloop (2 sub-SQS-skeins) of cardinality 8. This leads us to reformulate the classification given in Lemma 2 into classification depending on the number of subsloops (sub-SQS-skeins) of cardinality 8, as in the following lemma.

Lemma 3. *Let $\mathbf{L}(\mathbf{S})$ be a sloop of cardinality 16, then $\mathbf{L}(\mathbf{S})$ has n subsloops ($2n$ sub-SQS-skeins) of cardinality 8 for $n = 0, 1, 3, 7$ or 15.*

In fact, these classes associate with the same well-known classes of triple systems of cardinality 15. In [5], [6] and [7] all possible triple systems of order 15 were given. This means that structures of sloops of cardinality 16 with any possible congruence lattice (equivalently with any possible number of subsloops of cardinality 8) are well known. Also, examples of SQS-skeins of cardinality 16 with each possible congruence lattice (equivalently with any possible number of sub-SQS-skeins of cardinality 8) are well known (cf. [1] and [2]).

3. Extending a sloop L(16) to an SQS-skein S(16)

Cole, White and Cummtings [7] first determined that there are exactly 80 non-isomorphic triple systems of order 15. A listing of all 80 triple systems can be found in Bussemark and Seidel [5]. A triple system is called derived, if it can be extended to a quadruple system. There are 23 triple systems of order 15 having subsystems of order 7. All are derived [11].

Let $\mathbf{L} = (L; \cdot, 1)$ be a derived sloop of an SQS-skein $\mathbf{S} = (S; q)$, so the fundamental operations of $\mathbf{L}$ are polynomial functions of the operation q, which means in general that the congruence lattice $C(\mathbf{S})$ is a sublattice of $C(\mathbf{L})$. Namely, if $C(\mathbf{L}/\theta) \cong Sub(\mathbb{Z}_2^m)$ and $C(\mathbf{S}/\theta) \cong Sub(\mathbb{Z}_2^n)$ for an atom θ, then $n \leqslant m$. As a special case, if $\mathbf{L}$ is simple derived sloop from the SQS-skein $\mathbf{S}$, then $\mathbf{S}$ must be simple. Notice that each triple system having no subsystems of order 7 associates with a simple sloop.

This paper is a generalization of the result of Phelps in [11] that every non-simple sloop of order 16 can be extended to a SQS-skein of order 16. The question that the following two sections nearly answers is therefore: Given a non-simple sloop $\mathbf{L}$ (Steiner loop) with any congruence lattice $C(\mathbf{L})$, does there exist an SQS-skein $\mathbf{S}$ of order 16 such that $\mathbf{L}$ is derived from $\mathbf{S}$ for all possible $C(\mathbf{S})$? The only situation not answered in this paper is: $\mathbf{L}$ any sloop and $\mathbf{S}$ simple. Otherwise, the answer is yes.

3.1. Extending a sloop L(16) to an SQS-skein S(16) with $C(\mathbf{S})$=$C(\mathbf{L})$

In this section, we will show that: A non-simple sloop $\mathbf{L}$ with a certain congruence lattice $C(\mathbf{L})$ can be extended to a non-simple SQS-skein $\mathbf{S}$ having the same congruence lattice $C(\mathbf{S})$; i. e., $C(\mathbf{L}) = C(\mathbf{S})$. In other words, an $STS(15)$ with a non-zero number n of sub-$STS(7)$s can be extended to an $SQS(16)$ having $2n$ sub-$SQS(8)$, for each possible number n; i.e., $n = 1, 3, 7$ or 15.

Now, let $\mathbf{L}_1 = (L_1; \cdot, 1)$ be the Boolean sloop of cardinality 8 and $(L_1 - \{1\}; B_1)$ be the corresponding triple system of $\mathbf{L}_1$. It is known that $(L_1 - \{1\}; B_1)$ and the projective plane $PG(2, 2)$ are isomorphic, so we can index the element of $L_1 - \{1\}$ as follows:

$\{a_0, a_1, ..., a_6\}$ where $\{0, 1, ..., 6\}$ is the set of points of $PG(2, 2)$ such that $\{i, j, k\}$ is a line in $PG(2, 2)$ if and only if $\{a_i, a_j, a_k\}$ is a block in B_1. Moreover, we denote the set of lines of $PG(2, 2)$ by the set $\{i, i + 1, i + 3\}$ (mod 7).

Let $\mathbf{F} = \{F_0, F_1, ..., F_6\}$ be a 1-factorization of the complete graph with the vertices L_1, where $F_i = \{a_j a_k : a_j \cdot a_k = a_i \text{ in } \mathbf{L}_1\}$. We observe that $1a_i$ is an edge in F_i for each i. Also, we consider the sets $L_2 = \{b, b_0, b_1, ..., b_6\}$ and $L = L_1 \cup L_2$ such that $L_1 \cap L_2 = \emptyset$. We define the 1-factorization $\mathbf{G}$ of the complete graph K_8 with the set of vertices L_2 similarly as $\mathbf{F}$ by writing b instead of 1 and b_i instead of a_i in each factor of $\mathbf{F}$. Now we are ready to formulate the following well-known constructions for sloops and SQS-skeins of cardinality 16 [10].

Construction 1. *Let α be a permutation on the set $\{0, 1, ..., 6\}$. By taking $B := B_1 \cup \{\{a_i, b_j, b_k\} : b_j b_k \in G_{\alpha(i)}\}$, then $(L - \{1\}; B)$ is a triple system containing $(L_1 - \{1\}; B_1)$ as a subsystem* [10].

Let $\mathbf{L} = (L; \cdot, 1)$ be the given associated sloop with the triple system $(L - \{1\}; B)$ and $\mathbf{L}_1 = (L_1; \cdot, 1)$ be the associated subsloop, where the binary operation "." is defined by:

$$x \cdot y := \begin{cases} z & if \quad \{x, y, z\} \in B \\ 1 & if \quad x = y \end{cases}$$

By Theorem 1, we may say that $\mathbf{L}$ has at least one maximal congruence θ_0 determined by the normal subsloop $\mathbf{L}_1$.

Theorem 4. *Construction* 1 *yields precisely all non-simple sloops of cardinality* 16.

Proof. Without loss of generality, we may call the elements of L, L_1 and $L_2 = L - L_1$, the sloop $\mathbf{L} = (L; \cdot, 1)$, the subsloop $\mathbf{L}_1 = (L_1; \cdot, 1)$ and the 1-factorization $\mathbf{F}$ on L_1 exactly as the preceding definitions. Since $b \cdot a_i \in L_2$ for each $a_i \in L_1$, we may define the permutation α on the set $\{0, 1, 2, ..., 6\}$ by $b_{\alpha(i)} = b \cdot a_i$.

Moreover, we define a 1-factor $G_{\alpha(i)}$ on L_2 by the rule: $xy \in G_{\alpha(i)}$ if and only if $x \cdot y = a_i$ in $\mathbf{L}$. This supplies us with a 1-factorization $\mathbf{G} = \{G_0, G_1, ..., G_6\}$ on the set of points L_2.

Let $(L - \{1\}; B)$ be the triple system constructed by construction 1. If $\{a_i, a_j, a_k\}$ is a block in B_1, then $a_i \cdot a_j = a_k$ in $\mathbf{L}_1$ and if $\{a_i, b_j, b_k\}$ is a block in B, then $a_i = b_j \cdot b_k$ in $\mathbf{L}$. This means that the triple system $(L - \{1\}; B)$ coincides with the associated triple system with the sloop $\mathbf{L}$. This completes the proof of the theorem. $\square$

Construction 2. *Let*

$Q_1 = \{\{x_1, x_2, y_1, y_2\} : 0 \leqslant i \leqslant 6, x_1x_2 \in F_i \& y_1y_2 \in F_i\}$,

$Q_2 = \{\{x_1, x_2, y_1, y_2\} : 0 \leqslant i \leqslant 6, x_1x_2 \in G_i \& y_1y_2 \in G_i\}$,

$Q = Q_1 \cup Q_2 \cup \{\{x_1, x_2, y_1, y_2\} : 0 \leqslant i \leq 6, x_1x_2 \in F_i \; \& y_1y_2 \in G_{\alpha(i)}\}$.

Since $\mathbf{L}_1$ is a Boolean sloop, so for all $x, y, z, w \in L_1$ if $x \cdot y = z \cdot w$, then $x \cdot z = y \cdot w$ and $y \cdot z = x \cdot w$. Then if $xy, zw \in F_i$, hence $xz, yw \in F_j$ and $xw, zy \in F_k$ for some j and k. This means that $\{x, y, z, w\}$ is the unique block *in* $\mathbf{Q}_1$ *containing any* 3*-element subset of it. Accordingly,* $\mathbf{Q}_1 = (L_1; Q_1)$ *and* $\mathbf{Q}_2 = (L_2; Q_2)$ *are* $SQS(8)$*s. Hence* $\mathbf{Q} = (L; Q)$ *is a quadruple system in which* $\mathbf{Q}_1$ *and* $\mathbf{Q}_2$ *are subsystems.*

The associated SQS-skein $\mathbf{S} = (L; q)$ with the quadruple system $\mathbf{Q} = (L; Q)$ has at least one maximum congruence θ_0 determined by the two classes L_1 and L_2 (cf. [1], [9], where the operation q is defined by:

$$q(x,y,z) = \begin{cases} w & if \quad \{x,y,z,w\} \in Q \\ z & if \quad x = y \end{cases}$$

By the definition of F_i, if $\{a_i, a_j, a_k, 1\} \in Q_1$, then $1a_i, a_ja_k \in F_i$, which means that $\mathbf{L}_1$ is a derived sloop of $\mathbf{Q}_1$. Moreover, if $\{x,y,z\} \in B$, then $\{x,y,z\} \in B_1$ or $\{x,y,z\} \in \{\{a_i, b_j, b_k\} : b_jb_k \in G_{\alpha(i)}\}$.

Hence $\{x,y,z\} = \{a_i, a_j, a_k\}$ or $\{x,y,z\} = \{a_i, b_j, b_k\}$ for $b_jb_k \in G_{\alpha(i)}$, which means that $1a_i, a_ja_k \in F_i$ or $1a_i \in F_i$ and $b_jb_k \in G_{\alpha(i)}$. This implies that $\{1,x,y,z\} \in Q$. Therefore, $(L - \{1\}; B)$ is a derived triple system of the quadruple system $\mathbf{Q} = (L; Q)$.

Now, consider two sets:

$$S`_1 = \{1, a_i, a_{i+1}, a_{i+3}, b, b_{\alpha(i)}, b_{\alpha(i+1)}, b_{\alpha(i+3)}\}$$

and

$$S`_2 = \{1, a_i, a_{i+1}, a_{i+3}, b_{\alpha(i+2)}, b_{\alpha(i+4)}, b_{\alpha(i+5)}, b_{\alpha(i+6)}\}.$$

By choosing a suitable permutation α, we will show in the following that there is a derived sloop $\mathbf{L}$ from an SQS-skein $\mathbf{S}$ of cardinality 16 in which both $\mathbf{L}$ and $\mathbf{S}$ have the same congruence lattice.

Lemma 5. $\mathbf{S}`_1$ *is a subsloop of* $\mathbf{L}$ *a sub-*SQS*-skein of* $\mathbf{S}$ *if and only if* $\{\alpha(i), \alpha(i+1), \alpha(i+3)\}$ *is a line in* $PG(2,2)$.

Proof. Let $\mathbf{S}`_1$ be a subsloop of $\mathbf{L}$, then we have:

$$b \cdot b_{\alpha(i)} = a_i = b_{\alpha(i+1)} \cdot b_{\alpha(i+3)} \iff b\, b_{\alpha(i)}, b_{\alpha(i+1)} b_{\alpha(i+3)} \in G_{\alpha(i)}$$
$$\iff \{\alpha(i), \alpha(i+1), \alpha(i+3)\} \text{ is a line in } PG(2,2).$$

Also,

$$b \cdot b_{\alpha(i+1)} = a_{i+1} = b_{\alpha(i)} \cdot b_{\alpha(i+3)} \iff \{\alpha(i), \alpha(i+1), \alpha(i+3)\}$$
$$\text{is a line in } PG(2,2) \iff b \cdot b_{\alpha(i+3)} = a_{i+3} = b_{\alpha(i)} \cdot b_{\alpha(i+1)}.$$

Similarly, one can prove the other direction. The proof of this lemma for the SQS-skeins is given in [1]. □

Lemma 6. *If* $\mathbf{S}`_1$ *is a subsloop of* $\mathbf{L}$ *(a sub-*$SQS$*-skein of* $\mathbf{S}$*), then* $\mathbf{S}`_2$ *is also a subsloop of* $\mathbf{L}$ *(a sub-*SQS*-skein of* $\mathbf{S}$*).*

Proof. The 1-factorization of the complete graph K_4 with the set of vertices $\{b_{\alpha(i+2)}, b_{\alpha(i+4)}, b_{\alpha(i+5)}, b_{\alpha(i+6)}\}$ is included in the factors $G_{\alpha(i)}$, $G_{\alpha(i+1)}$, $G_{\alpha(i+3)}$. This shows directly that $\mathbf{S}`_2$ is a subsloop of $\mathbf{L}$ (an sub-SQS-skein of $\mathbf{S}$). □

Lemma 7. *For each line transformed into a line by the permutation α in $PG(2,2)$, two maximum congruences are formed in the lattice $C(\mathbf{L})$ ($C(\mathbf{S})$) in addition to θ_0.*

Proof. We have $|S`_1| = |S`_2| = \frac{1}{2}\,|L|$, so $\mathbf{S}`_1$ and $\mathbf{S}`_2$ are two distinct normal subsloops of $\mathbf{L}$ (sub-SQS-skeins of $\mathbf{S}$). Let θ_1 and θ_2 be the associated congruences with $\mathbf{S}`_1$ and $\mathbf{S}`_2$, respectively. Then $\theta_1 \cap \theta_2$ is a congruence with 4 congruence classes, which implies that there are exactly three covers of $\theta_1 \cap \theta_2$, namely θ_0, θ_1, θ_2. This completes the proof. □

In fact, this similarity between properties of sloops and SQS-skeins leads directly to the following result.

Theorem 8. *Let $\mathbf{L}$ ($\mathbf{S}$) be a sloop (an SQS-skein) of cardinality 16 and assume that its congruence lattice $C(\mathbf{L})$ ($C(\mathbf{S})$) has an atom θ. If the permutation α transforms $2^{n-2}-1$ lines into lines in $PG(2,2)$ for $n = 2,3,4$, or 5, then $C(\mathbf{L}/\theta) \cong C(\mathbf{S}/\theta) \cong Sub(\mathbb{Z}_2^{n-1})$ for $n = 2,3,4$ and $C(\mathbf{L}) \cong C(\mathbf{S}) \cong Sub(\mathbb{Z}_2^4)$ for $n = 5$.*

Proof. According to the Lemmas 4, 5 and 6, we get directly the required. □

Consequently, we may say that any sloop of cardinality 16 with n subsloops of cardinality 8 is a derived sloop from an SQS-skein of cardinality 16 having $2n$ sub-SQS-skeins for each possible non-zero number n; i.e. for $n = 1,3,7$ and 15.

3.2. Extending a sloop L(16) to an SQS-skein S(16) with arbitrary $C(\mathbf{S}) \leqslant C(\mathbf{L})$

In this section, we will show that: A non-simple sloop $\mathbf{L}$ with any possible congruence lattice $C(\mathbf{L})$ can be extended to a non-simple SQS-skein $\mathbf{S}$ with all possible congruence lattice $C(\mathbf{S})$; i.e., for all possible sublattice $C(\mathbf{S})$ of $C(\mathbf{L})$.

Without loss of generality and according to the definition of the 1-factorization $\mathbf{F}$ given in constructions 1 and 2, we may choose the sub-1-factors:

1− $f_0 = \{a_1a_3, a_4a_5\} \subseteq F_0$ and $f_2 = \{a_1a_4, a_3a_5\} \subseteq F_2$ on the set $\{a_1, a_3, a_4, a_5\}$.

2− $f_1 = \{a_2a_4, a_5a_6\} \subseteq F_1$ and $f_3 = \{a_2a_5, a_4a_6\} \subseteq F_3$ on the set $\{a_2, a_4, a_5, a_6\}$.

3− $f_4 = \{a_1a_2, a_0a_5\} \subseteq F_4$ and $f_6 = \{a_0a_2, a_1a_5\} \subseteq F_6$ on the set $\{a_0, a_1, a_2, a_5\}$.

By interchanging the sub-1-factors f_0 and f_2 in the 1-factors F_0 and F_2 we get new 1-factors $F_0^`$ and $F_2^`$, where $F_0^` = \{1a_0, a_1a_4, a_3a_5, a_2a_6\}$ and $F_2^` = \{1a_2, a_1a_3, a_4a_5, a_0a_6\}$. Similarly, we interchange the sub-1-factors f_1 and f_3 in the 1-factors F_1 and F_3 to get new 1-factors $F_1^`$ *and* $F_3^`$ and the sub-1-factors f_4 and f_6 in the 1-factors F_4 and F_6 to get new 1-factors $F_4^`$ and $F_6^`$.

Now, we consider three new 1-factorizations on the set L_1 :

$$
\begin{aligned}
{}_1\mathbf{F}^{‘} &= \{F_0^{‘}, F_1, F_2^{‘}, F_3, F_4, F_5, F_6\},\\
{}_2\mathbf{F}^{‘} &= \{F_0^{‘}, F_1^{‘}, F_2^{‘}, F_3^{‘}, F_4, F_5, F_6\},\\
{}_3\mathbf{F}^{‘} &= \{F_0^{‘}, F_1^{‘}, F_2^{‘}, F_3^{‘}, F_4^{‘}, F_5, F_6^{‘}\}.
\end{aligned}
$$

Let Q_1 and Q_2 be the same as in construction 2, and let

$$
{}_jQ^{‘} = Q_1 \cup Q_2 \cup \overline{Q},
$$

where

$$
\overline{Q} = \{\{x_1, x_2, y_1, y_2\} : x_1x_2 \in F_i^{‘} \in_j \mathbf{F}^{‘} \text{ and } y_1y_2 \in G_{\alpha(i)} \text{ for some } 0 \leqslant i \leqslant 6\}.
$$

Indeed, the changes occurs only in the quadruple systems, so we will denote the new quadruple systems by $(L; {}_jQ^{‘})$ for $j = 1, 2, 3$. Notice that the triple system $(L - \{1\}; B)$ is still as a derived triple system of $(L; {}_jQ^{‘})$ for each $j = 1, 2, 3$.

The 1-factorization ${}_1\mathbf{F}^{‘}$ contains exactly the three sub-1-factorizations $\{F_0^{‘}, F_2^{‘}, F_6\}$, $\{F_1, F_5, F_6\}$, $\{F_3, F_4, F_6\}$ in which each of them contains two disjoint sub-1-factorizations of the complete graph K_4. Similarly, the 1-factorization ${}_2\mathbf{F}^{‘}$ contains exactly one sub-1-factorization$\{F_0^{‘}, F_2^{‘}, F_6\}$ containing two disjoint sub-1-factorizations of the complete graph K_4 and the 1-factorization ${}_3\mathbf{F}^{‘}$ does not contain any sub-1-factorization of the complete graph K_4.

We observe that α may transform $2^{n-2} - 1$ lines into lines in $PG(2, 2)$ for $n = 2, 3, 4, 5$. Thus:

If $n = 2$, then α does not transform any line into a line.

If $n = 3$, then α transforms at most one line into a line among the lines of the subset $R = \{\{0, 2, 6\}, \{1, 5, 6\}, \{3, 4, 6\}\}$.

If $n \geqslant 4$, then α transforms 1 or 3 lines into lines among the lines of R.

Now, let $(L; {}_jq^{‘})$ be the associated SQS-skein with $(L; {}_jQ^{‘})$ for $j = 1, 2, 3$. Analogously, we may deduce the following result.

Theorem 9. *The constructed sloop $\mathbf{L} = (L; \cdot, 1)$ is a derived sloop from the constructed SQS-skein ${}_j\mathbf{S} = (L; {}_jq^{‘})$ for each $j = 1, 2$ and 3 and for any permutation α. Moreover, each non-simple sloop L can be extended to a non-simple SQS-skein ${}_j\mathbf{S}$ with all possible congruence lattices for $C(\mathbf{L})$ and $C({}_j\mathbf{S})$.*

Proof. Any permutation α transforms $2^{n-2} - 1$ lines into lines in $PG(2, 2)$ for $n = 2, 3, 4, 5$. Notice in all cases that θ_0 is a congruence of each of $\mathbf{L}$ and ${}_j\mathbf{S}$ for $j = 1, 2$ and 3, where θ_0 is determined by the two classes L_1 and L_2.

In the following, we consider θ to be the unique atom of the lattices $C(\mathbf{L})$ and $C({}_j\mathbf{S})$ for $j = 1, 2$ and 3, except in the case for $n = 5$, when θ is considered to be any atom of $C(\mathbf{L})$. Now, we have the following result:

When $n = 2$, then α does not transform any line to a line, hence $C(\mathbf{L}/\theta) \cong C({}_j\mathbf{S}/\theta) \cong Sub(\mathbb{Z}_2)$ for $j = 1$, 2 and 3, where the atom θ is equal to θ_0.

When $n = 3$, then α transforms one line into line in $PG(2,2)$, by Lemma 3 hence $C(\mathbf{L}/\theta \cong Sub(\mathbb{Z}_2^2)$. Also, α transforms nothing or one line into a line in $PG(2,2)$ among the lines of the subset R, so $C({}_3\mathbf{S}/\theta) \cong C({}_2\mathbf{S}/\theta) \cong C({}_1\mathbf{S}/\theta) \cong Sub(\mathbb{Z}_2)$, where the atom θ is equal to θ_0 , or $C({}_2\mathbf{S}/\theta) \cong C({}_1\mathbf{S}/\theta) \cong Sub(\mathbb{Z}_2^2)$.

When $n = 4$, then α transforms 3 lines into 3 lines in $PG(2,2)$, by Lemma 3 hence $C(\mathbf{L}/\theta) \cong Sub(\mathbb{Z}_2^3)$. Also, α transforms 1 or 3 lines into lines in $PG(2,2)$ among the lines of the subset $R = \{\{0,2,6\},\{1,5,6\},\{3,4,6\}\}$, so $C({}_3\mathbf{S}/\theta) = C({}_3\mathbf{S}/\theta_0) \cong Sub(\mathbb{Z}_2)$ and $C({}_2\mathbf{S}/\theta) \cong C({}_1\mathbf{S}/\ \theta) \cong Sub(\mathbb{Z}_2^2)$ or $C({}_1\mathbf{S}/\theta) \cong Sub(\mathbb{Z}_2^3)$.

When $n\ = 5$, then α transforms 7 lines into 7 lines in $PG(2,2)$, by Lemma 3 and since $C(\mathbf{L})$ contains in this case more than one atom, hence $C(\mathbf{L}/\theta) \cong Sub(\mathbb{Z}_2^3)$ for each atom θ of $C(\mathbf{L})$ or $C(\mathbf{L}) \cong Sub(\mathbb{Z}_2^4)$. This means that α transforms the three lines of R into 3 lines in $PG(2,2)$, so $C({}_3\mathbf{S}/\theta) = C({}_3\mathbf{S}/\theta_0\ ) \cong Sub(\mathbb{Z}_2)$, $C({}_2\mathbf{S}/\theta) \cong Sub(\mathbb{Z}_2^2)$ and $C({}_1\mathbf{S}/\theta) \cong Sub(\mathbb{Z}_2^3)$, where θ is still the unique atom of $C({}_j\mathbf{S})$ for $j = 1,2$ and 3.

For the case $C(\mathbf{L}) \cong C(\mathbf{S}) \cong Sub(\mathbb{Z}_2^4)$, we may choose the Boolean SQS-skein $\mathbf{S}$ of cardinality 16 and $\mathbf{L}$ any of its derived sloops. This completes the proof. $\square$

Consequently, we may say that any sloop with a non-zero number n of subsloops of cardinality 8 can be extended to an SQS-skein having $2m$ sub-SQS-skeins of cardinality 8 for each possible positive numbers n and m; i.e., for each n and $m = 1,3,7$ or 15 with $m \leqslant n$.

Examples. Example for each case can be determined by choosing the permutation α as follows:

• For $n = 2$ take $\alpha = (12)(345)$, hence α does not transform any line into a line in $PG(2,2)$, which means that the congruence lattices $C(\mathbf{L})$ and $C({}_j\mathbf{S})$ for $j = 1,2$ and 3 have exactly one co-atom θ_0.

• For $n = 3$ take $\alpha = (012)(345)$ or $\alpha = (345)$. In both cases α transforms one line into a line in $PG(2,2)$. This implies that $\mathbf{L}$ has three maximum congruences, so $C(\mathbf{L}/\theta) \cong Sub(\mathbb{Z}_2^2)$. The permutation $\alpha = (012)(345)$ transforms the line $\{0,1,3\}$ into the line $\{1,2,4\}$, this means that $C({}_j\mathbf{S})$ for $j = 1,2$ and 3 have only one co-atom θ_0.

But the permutation $\alpha = (345)$ transforms the line $\{0,2,6\}$ into itself, hence $C({}_j\mathbf{S})$ has exactly three co-atoms for $j = 1$ and 2 and $C({}_3\mathbf{S})$ has only one co-atom θ_0.

• For $n = 4$ take $\alpha = (012345)$ or $\alpha = (4321)(650)$, both cases α transforms three lines into three lines in $PG(2,2)$, then $\mathbf{L}$ has exactly 7 maximum congruences. $\alpha = (012345)$ transforms the three lines of the set $R = \{\{0,2,6\},\{1,5,6\},\{3,4,6\}\}$ into three lines in $PG(2,2)$, which implies that $C({}_1\mathbf{S})$ has exactly 7 co-atoms, $C({}_2\mathbf{S})$ has exactly three co-atoms and $C({}_3\mathbf{S})$ has only one co-atom θ_0.

$\alpha = (4321)(650)$ transforms only the line $\{0,2,6\}$ of R into a line of R, which means that the congruence lattices $C({}_j\mathbf{S})$ has exactly three co-atoms for $j = 1$ and 2 and $C({}_3\mathbf{S})$ has only the co-atom θ_0.

• For $n = 5$ take $\alpha = identity$ on $\{0, 1, ..., 6\}$, so α transforms all lines into lines in $PG(2, 2)$, which means that $C(\mathbf{L})$ has 15 co-atoms, $C({}_1\mathbf{S})$ has 7 co-atoms, $C({}_2\mathbf{S})$ has 3 co-atoms and $C({}_3\mathbf{S})$ has only the co-atom θ_0. $\square$

Consequently, we may say that any $STS(15)$ with a non-zero number n of sub-$STS(7)$s can be extended to an $SQS(16)$ having $2m$ sub-$SQS(8)$s for all possible non-zero positive numbers n and m; i.e., for any n and $m \in \{1, 3, 7, 15\}$ with $m \leqslant n$.

Among the $DTS(15)$s determined in [11], there are 57 systems having no subsystems of order 7. The sloops associated with these 57 systems are simple. We therefore see that the sloops associated with these 57 systems must be derived from simple SQS-skeins. But it is not necessary for a sloop derived from a simple SQS-skein to be simple.

We finish this work with a natural question:

Question. *Is whether or not a sloop of cardinality* 16 *with each possible congruence lattice can be extended to a simple SQS-skein ?*

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**: *Construction of nilpotent sloops of class n*, Discrete Math. **171** (1997), 17 – 25.

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

[5] **F. C. Bussemark and J. J. Seidel**: *Symmetric Hadamard matrices of order* 36, T. H. Report 70-WSK-02, Dept. of Mathematics Tech. University Eindhoven, Netherlands 1970.

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

[7] **F.N. Cole, L. D. Cummings and H. S. White**: *The complete enumeration of triad systems in* 15 *elements*, Nat. Acad. Proc. **3** (1916), 197 – 199.

[8] **A. J. Guelzow**: *Semiboolean SQS-skeins,* J. Alg. Comb. **2** (1993), 147 – 153.

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

[10] **C. C. Lindner and A. Rosa**: *Steiner quadruple systems. A survey*, Discrete Math. **21** (1978), 147 – 181.

[11] **K. T. Phelps**: *A survey of derived triple systems*, Annals Discrete Math. **7** (1980), 105 – 114.

[12] **R. W. Quackenbush**: *Varieties of Steiner loops and Steiner quasigroups*, Canad. J. Math. **28** (1978), 1187 – 1198.

[13] **J. D.H. Smith**: *Mal'cev varieties*, Lecture Notes in Mathematics, Berlin, Heidelberg, New York, Springer-Verlag (1976).

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

Received June 24, 2003
Revised May 17, 2004

Quasigroups and Related Systems **12** (2004), 13 – 28

(Weak) Implicative hyper BCK-ideals

Radjab A. Borzooei and M. Bakhshi

Abstract

In this manuscript first we define the notion of weak implicative hyper BCK-ideal of a hyper BCK-algebra. Then we state and prove some theorems which determine the relationship among this notion and (weak, commutative, (strong) implicative) hyper BCK-ideals, positive implicative hyper BCK-ideals of type $1, 3, \ldots, 8$ and (strong) positive implicative hyper BCK-ideals. Specially, we prove that if $H = \{0, a, b, c\}$ is a hyper BCK-algebra of order 4, such that $a \circ x = \{0\}$, for all $0 \neq x \in H$ and I is a hyper BCK-ideal and weak implicative hyper BCK-ideal of H, then I is a positive implicative hyper BCK-ideal of type 3.

1. Introduction

The study of BCK-algebras was initiated by Y. Imai and K. Iséki [7] in 1966 as a generalization of the concept of set-theoretic difference and propositional calculi. Since then a great deal of literature has been produced on the theory of BCK-algebras. In particular, emphasis seems to have been put on the ideal theory of BCK-algebras. The hyperstructure theory (called also multialgebras) was introduced in 1934 by F. Marty [13] at the 8th congress of Scandinavian Mathematiciens. Around the 40's, several authors worked on hypergroups, especially in France and in the United States, but also in Italy, Russia and Japan. Over the following decades, many important results appeared, but above all since the 70's onwards the most luxuriant flourishing of hyperstructures has been seen. Hyperstructures have many applications to several sectors of both pure and applied sciences. In [12], Y. B. Jun et al. applied the hyperstructures to BCK-algebras, and introduced the notion of a hyper BCK-algebra which is a

2000 Mathematics Subject Classification: 06F35, 03G25
Keywords: hyper BCK-algebra, (weak) implicative hyper BCK-ideal, positive implicative hyper BCK-ideals of types 1,3,...,8

generalization of BCK-algebra, and investigated some related properties. They also introduced the notion of a hyper BCK-ideal and a weak hyper BCK-ideal and gave relations between hyper BCK-ideals and weak hyper BCK-ideals. Y. B. Jun et al. [12] gave a condition for a hyper BCK-algebra to be a BCK-algebra. In [2], R. A. Borzooei and M. Bakhshi introduced the notions of positive implicative hyper BCK-ideals of types $1, 2, \ldots, 8$ and gave relations between these notions and (weak, strong) hyper BCK-ideals. They also in [1], introduced the concept of commutative hyper BCK-ideals of types $1, 2, 3$ and 4 and give some relations among these notions and positive implicative hyper BCK-ideals of types $1, 2, \ldots, 8$ and (weak) hyper BCK-ideals and state its characterizations. In [8], Y. B. Jun et al. introduced the notion of implicative hyper BCK-ideals and gave some relations between this notion and hyper BCK-ideals. Now, in this paper we introduce the concept of weak implicative hyper BCK-ideal and we study some related properties. Moreover, we give some relations among (weak) hyper BCK-ideal, (weak) implicative hyper BCK-ideal, positive implicative hyper BCK-ideals of types $1, 2, \ldots, 8$ and commutative hyper BCK-ideals of types $1, 2, 3$ and 4, under suitable conditions.

2. Preliminaries

Definition 2.1. By a *hyper BCK-algebra* we mean a non-empty set H endowed with a hyperoperation "$\circ$" and a constant 0 satisfying 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 $x \ll y$ is defined by $0 \in x \circ y$ and for every $A, B \subseteq H$, $A \ll B$ is defined by $\forall a \in A$, $\exists b \in B$ such that $a \ll b$. In such case, we call "$\ll$" the *hyperorder* in H.

Example 2.2. (i) Define a hyperoperation "$\circ$" on $H = [0, \infty)$ by

$$x \circ y = \begin{cases} [0, x] & \text{if} \quad x \leq y \\ (0, y] & \text{if} \quad x > y \neq 0 \\ \{x\} & \text{if} \quad y = 0 \end{cases}$$

for all $x, y \in H$. Then H is a hyper BCK-algebra.

(ii) Let $H = \{0, a, b, c\}$. Consider the following table:

$\circ$	0	a	b	c
0	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
a	$\{a\}$	$\{0\}$	$\{0\}$	$\{0\}$
b	$\{b\}$	$\{b\}$	$\{0\}$	$\{0\}$
c	$\{c\}$	$\{c\}$	$\{c\}$	$\{0, c\}$

Then H is a hyper BCK-algebra.

Proposition 2.3. [12] *In any hyper BCK-algebra H, the following hold:*

(i) $x \circ 0 = \{x\}$, (iv) $A \ll A$,

(ii) $x \circ y \ll x$, (v) $A \subseteq B$ *implies* $A \ll B$,

(iii) $0 \circ A = \{0\}$, (vi) $A \circ \{0\} = \{0\}$ *implies* $A = \{0\}$,

for all $x, y, z \in H$ and for all non-empty subsets A and B of H.

Let I be a non-empty subset of a hyper BCK-algebra H and $0 \in I$. Then I is said to be a *strong hyper BCK-ideal* of H if $(x \circ y) \cap I \neq \emptyset$ and $y \in I$ implies that $x \in I$, *hyper BCK-ideal* of H if $x \circ y \ll I$ and $y \in I$ imply $x \in I$, *weak hyper BCK-ideal* of H if $x \circ y \subseteq I$ and $y \in I$ imply $x \in I$, *hyper BCK-subalgebra* of H if $x \circ y \subseteq I$ for all $x, y \in I$, *reflexive* if $x \circ x \subseteq I$, for all $x \in H$, *positive implicative hyper BCK-ideal* of *type 1* if $(x \circ y) \circ z \subseteq I$ and $y \circ z \subseteq I$ imply $x \circ z \subseteq I$, *positive implicative hyper BCK-ideal* of *type* 3 if $(x \circ y) \circ z \ll I$ and $y \circ z \ll I$ imply $x \circ z \subseteq I$, *commutative hyper BCK-ideal* of *type 1* if $(x \circ y) \circ z \subseteq I$ and $z \in I$ imply $x \circ (y \circ (y \circ x)) \subseteq I$, *commutative hyper BCK-ideal* of *type* 3 if $(x \circ y) \circ z \ll I$ and $z \in I$ imply $x \circ (y \circ (y \circ x)) \subseteq I$, for all $x, y, z \in H$. It is easy to see that any positive implicative hyper BCK-ideal of type 3 and commutative hyper BCK-ideal of type 3 (positive implicative hyper BCK-ideal of type 1 and commutative hyper BCK-ideal of type 1) is a (weak) hyper BCK-ideal, any (strong) hyper BCK-ideal is a (hyper BCK-ideal) weak hyper BCK-ideal and a hyper BCK-subalgebra of H. Moreover, any reflexive hyper BCK-ideal of H is a strong hyper BCK-ideal of H.

Theorem 2.4. [1, 2] *Let I be a non-empty subset of hyper BCK-algebra H. Then,*

(i) *if I is a positive implicative hyper BCK-ideal of type* 3 (*type* 1)*, then I and I_a are* (*weak*) *hyper BCK-ideals of H, where for all $a \in H$,*

$$I_a = \{x \in H : x \circ a \subseteq I\}$$

(ii) *if H is a positive implicative hyper BCK-algebra (that is, for all $x, y, z \in H, (x \circ y) \circ z = (x \circ z) \circ (y \circ z)$) and I is a (weak) hyper BCK-ideal of H, then I is a positive implicative hyper BCK-ideal of type 3 (type 1),*

(iii) *if I is a commutative hyper BCK-ideal of type 3 (type 1), then I is a (weak) hyper BCK-ideal of H.*

Lemma 2.5. [1, 9] *Let A, B and I are non-empty subsets of hyper BCK-algebra H. Then,*

(i) *if I is a hyper BCK-ideal of H, then $A \ll I$ implies $A \subseteq I$,*

(ii) *if I is a hyper BCK-ideal of H, then $A \circ B \ll I$ and $B \subseteq I$ imply $A \subseteq I$,*

(iii) *if I is a weak hyper BCK-ideal of H, then $A \circ B \subseteq I$ and $B \subseteq I$ imply $A \subseteq I$,*

(iv) *if I is a reflexive hyper BCK-ideal of H and for $x, y \in H$, $(x \circ y) \cap I \neq \emptyset$, then $x \circ y \ll I$.*

3. Weak implicative hyper BCK-ideals

From now on in this paper, we let H denote a hyper BCK-algebra.

Definition 3.1. Let I be a non-empty subset of H and $0 \in I$. Then I is called a *weak implicative hyper BCK-ideal* of H if, $(x \circ z) \circ (y \circ x) \subseteq I$ and $z \in I$ imply $x \in I$, for all $x, y, z \in H$.

Example 3.2. Let H be hyper BCK-algebra which is defined in Example 2.2 (ii). Then, $I_1 = \{0, a, b\}$ is a weak implicative hyper BCK-ideal of H, but $I_2 = \{0, a\}$ is not a weak implicative hyper BCK-ideal . Since we have $(b \circ 0) \circ (c \circ b) = b \circ c = \{0\} \subseteq I$ and $0 \in I$ but $b \notin I$.

Theorem 3.3. *Let I be a non-empty subset of H. Then, I is a weak implicative hyper BCK-ideal of H if and only if I is a weak hyper BCK-ideal of H and $x \circ (y \circ x) \subseteq I$ implies $x \in I$, for all $x, y \in H$.*

Proof. Let I be a weak implicative hyper BCK-ideal of H, $x \circ y \subseteq I$ and $y \in I$, for $x, y \in H$. Since $(x \circ y) \circ (0 \circ x) = x \circ y \subseteq I$ and $y \in I$ then $x \in I$ and so I is a weak hyper BCK-ideal of H. Now, let $x \circ (y \circ x) \subseteq I$, for $x, y \in H$. Then by Proposition 2.3(i), $(x \circ 0) \circ (y \circ x) = x \circ (y \circ x) \subseteq I$. Since $0 \in I$ and I is a weak implicative hyper BCK-ideal of H, then $x \in I$. Conversely, let I be a weak hyper BCK-ideal of H and for all $x, y \in H, x \circ$

$(y \circ x) \subseteq I$ implies that $x \in I$. Now, let $(x \circ z) \circ (y \circ x) \subseteq I$ and $z \in I$, for $x, y, z \in H$. Then by (HK2), $(x \circ (y \circ x)) \circ z = (x \circ z) \circ (y \circ x) \subseteq I$. Since I is a weak hyper BCK-ideal of H and $z \in I$, then by Lemma 2.5(iii) we get that $x \circ (y \circ x) \subseteq I$ and so by hypothesis $x \in I$. Therefore, I is a weak implicative hyper BCK-ideal of H. $\square$

Example 3.4. Let H be hyper BCK-algebra which is defined in Example 2.2(ii). Then, $I = \{0, a\}$ is a weak hyper BCK-ideal of H, but it is not a weak implicative hyper BCK-ideal of H. Since $b \circ (c \circ b) = b \circ c = \{0\} \subseteq I$ but $b \notin I$.

Theorem 3.5. *Let $H = \{0, a, b\}$ be a hyper BCK-algebra of order 3. Then, proper subset I of H is a weak hyper BCK-ideal of H if and only if I is a weak implicative hyper BCK-ideal of H.*

Proof. ($\Leftarrow$) The proof follows by Theorem 3.3.

($\Rightarrow$) The only proper weak hyper BCK-ideals of H are $I = \{0, a\}$ or $I = \{0, b\}$. Let $I = \{0, a\}$ be a weak hyper BCK-ideal of H. By Theorem 3.3, it is enough to show that for all $x, y \in H$, if $x \circ (y \circ x) \subseteq I$ then $x \in I$. Let $x \circ (y \circ x) \subseteq I$ but $x \notin I$, for $x, y \in H$. Hence, $x = b$. Thus, $b \circ (y \circ b) \subseteq I$ and $b \notin I$. Now we consider the following cases for y.

If $y = 0$, then $\{b\} = b \circ 0 = b \circ (0 \circ b) \subseteq I$, which is a contradiction. If $y = a$ and $a \ll b$, since $0 \in a \circ b$ then we get that $\{b\} = b \circ 0 \subseteq b \circ (a \circ b) \subseteq I$ which is impossible. If $y = a$ and $b \ll a$, then H satisfies the normal condition and so by Lemma 2.6(iv) of [1], $a \circ b = \{0\}$ or $\{0, a\}$. Hence $0 \in a \circ b$ and so $a \ll b$ which is a contradiction. If $y = a$, $a \not\ll b$ and $b \not\ll a$, then H satisfies the simple condition and so by Lemma 2.6(i) of [1], $a \circ b = \{a\}$ and $b \circ a = \{b\}$. Therefore, $\{b\} = b \circ a \subseteq b \circ (a \circ b) \subseteq I$, which is impossible. If $y = b$, since $0 \in b \circ b$ then $\{b\} = b \circ 0 \subseteq b \circ (b \circ b) \subseteq I$, which is impossible. Therefore, $x \in I$ and so I is a weak implicative hyper BCK-ideal of H.

Now, let $I = \{0, b\}$ be a weak hyper BCK-ideal of H and $x \circ (y \circ x) \subseteq I$ but $x \notin I$. Hence $x = a$. Therefore, $a \circ (y \circ a) \subseteq I$ and $a \notin I$. If $y = 0$ or a, then by similar way in the proof of case $I = \{0, a\}$, we get a contradiction. Now let $y = b$. If $b \ll a$, then $0 \in b \circ a$ and so $\{a\} = a \circ 0 \subseteq a \circ (b \circ a) = a \circ (y \circ a) \subseteq I$, which is impossible. If $a \ll b$, then H satisfies the normal condition. Hence by Lemma 2.6(b) of [1], $a \circ b = \{0\}$ or $\{0, a\}$ and $b \circ a = \{a\}$ or $\{b\}$ or $\{a, b\}$. If $b \circ a = \{b\}$ or $\{a, b\}$, then $a \circ b \subseteq a \circ (b \circ a) \subseteq I$. Since $b \in I$ and I is a weak hyper BCK-ideal of H, then $a \in I$ which is a contradiction. Thus $b \circ a = \{a\}$. If $a \circ b = \{0\}$, then $a \circ b \subseteq I$ and $b \in I$. Since I is a weak hyper BCK-ideal, then $a \in I$, which is impossible. Hence, $a \circ b = \{0, a\}$. By

Lemma 2.6(iii) of [1], $a \circ a = \{0\}$ or $\{0, a\}$. If $a \circ a = \{0, a\}$, since $b \circ a = \{a\}$, then $a \in a \circ a = a \circ (b \circ a) = a \circ (y \circ a) \subseteq I$ which is a contradiction. Hence $a \circ a = \{0\}$. But in this case by (HK1), $\{0, a\} = (a \circ b) \circ (a \circ b) \ll a \circ a = \{0\}$ and so $a \ll 0$, which is impossible.

If $b \not\ll a$ and $a \not\ll b$, then H satisfies the simple condition and so by Lemma 2.6(a) of [1], $a \circ b = \{a\}$ and $b \circ a = \{b\}$. Hence $\{a\} = a \circ b = a \circ (b \circ a) = a \circ (y \circ a) \subseteq I$, which is impossible. Therefore, $x \in I$ and so I is a weak implicative hyper BCK-ideal of H. □

Corollary 3.6. *Let $H = \{0, a, b\}$ be a hyper BCK-algebra of order 3 and I be a non-empty subset of H. Then,*

(i) *I is a weak implicative hyper BCK-ideal of H if and only if I is a positive implicative hyper BCK-ideal of type 1,*

(ii) *I is a weak implicative hyper BCK-ideal of H if and only if I is a commutative hyper BCK-ideal of type 1.*

Proof. (i) The proof follows by Theorem 3.5 and Theorem 3.10(ii) of [1].

(ii) The proof follows from Theorems 3.5 and Theorem 4.6 of [1]. □

Theorem 3.7. *Let $H = \{0, a, b, c\}$ be a hyper BCK-algebra of order 4 such that $a \circ x = \{0\}$, for all $0 \neq x \in H$ and I be a proper subset of H. If I is a hyper BCK-ideal and a weak implicative hyper BCK-ideal of H, then I is a positive implicative hyper BCK-ideal of type 3.*

Proof. Let I be a proper hyper BCK-ideal and weak implicative hyper BCK-ideal of H. Then, there is the following cases for I;

$$\{0, a\}, \{0, b\}, \{0, c\}, \{0, a, b\}, \{0, a, c\}, \{0, b, c\}$$

If I is equal to $\{0, b\}$ or $\{0, b, c\}$ (or $\{0, c\}$), since by hypothesis $a \circ b = (a \circ c =)\{0\} \ll I$, $b \in I (c \in I)$ and I is a hyper BCK-ideal of H, then $a \in I$ which is impossible. Now, we consider the following cases for I;

(i) $I = \{0, a, b\}$.

Let I not be a positive implicative hyper BCK-ideal of type 3, that is $(x \circ y) \circ z \ll I$ and $y \circ z \ll I$ but $x \circ z \not\subseteq I$. Then, $c \in x \circ z$ and so by hypothesis and Proposition 2.3(iii), $x \neq 0, a$. Since I is a hyper BCK-ideal, then by Lemma 2.5(i), $(x \circ y) \circ z \subseteq I$ and $y \circ z \subseteq I$. Hence, by (HK2) we have $c \circ y \subseteq (x \circ z) \circ y = (x \circ y) \circ z \subseteq I$. Now, if $y = 0$ or a or b, since $c \circ y \subseteq I$ and $y \in I$ then $c \in I$ which is impossible. If $y = c$, then $c \circ c \subseteq I$ and $c \circ z = y \circ z \subseteq I$. Now, if $z \in \{0, a, b\}$ then $c \in I$ and so we get a contradiction. Hence $z = c$. By above, $x \neq 0, a$. If $x = c$, then $c \in x \circ z = c \circ c \subseteq I$, which is impossible. Thus $x = b$. By (HK3), $c \in b \circ c \ll b$ and so $0 \in c \circ b$. Hence, by (HK4) $0 \notin b \circ c$. Moreover, if $b \in b \circ c$ then $c \in b \circ c \subseteq (b \circ c) \circ c = (x \circ y) \circ z \subseteq I$ which is a contradiction. Hence $b \circ c = \{c\}$ or $\{a, c\}$. Since $c \ll b$, then $b \circ c \ll \{0, a, b\} = I$. Moreover, since I is a hyper BCK-ideal of H then by Lemma 2.5(i), $c \in b \circ c \subseteq I$ which is a contradiction. Therefore, I is a positive implicative hyper BCK-ideal of type 3.

(ii) $I = \{0, a, c\}$.

The proof of this case is nearly similar to the proof of case (i).

(iii) $I = \{0, a\}$.

Let I not be a positive implicative hyper BCK-ideal of type 3, that is $(x \circ y) \circ z \ll I$ and $y \circ z \ll I$ but $x \circ z \not\subseteq I$. Then, $(x \circ z) \cap \{b, c\} \neq \emptyset$. Now we consider the following cases.

Case 1. $c \in x \circ z$.

By Lemma 2.5(i), $(x \circ y) \circ z \subseteq I$ and $y \circ z \subseteq I$. By (HK2), $c \circ y \subseteq (x \circ z) \circ y = (x \circ y) \circ z \subseteq I$.

Case 1-1. If $y = 0$ or a, since $c \circ y \subseteq I$ and $y \in I$ and I is a weak hyper BCK-ideal of H, then $c \in I$ which is impossible.

Case 1-2. If $y = b$, then we consider the following cases for z:

Case 1-2-1. If $z = 0$ or a, since $b \circ z = y \circ z \subseteq I$ and $z \in I$ and I is a weak hyper BCK-ideal of H, then $b \in I$ which is impossible.

Case 1-2-2. If $z = b$, then $c \in x \circ z = x \circ b$, $b \circ b = y \circ z \subseteq I$ and $c \circ b = c \circ y \subseteq I$. By hypothesis and Proposition 2.3(iii), $x \neq 0$ and a. If $x = b$, then $c \in x \circ b = b \circ b \subseteq I$ which is impossible. If $x = c$, then $c \in x \circ b = c \circ b \subseteq I$ which is impossible.

Case 1-2-3. If $z = c$, then $c \in x \circ c$, $c \circ b = c \circ y \subseteq I$ and $b \circ c = y \circ z \subseteq I$. It is clear that $x \neq 0$ and a. If $x = b$, then $c \in x \circ c = b \circ c \subseteq I$ which is impossible. If $x = c$, then $c \in x \circ c = c \circ c$. By (HK1), $(c \circ c) \circ (b \circ c) \ll c \circ b \subseteq I$ and so $(c \circ c) \circ (b \circ c) \ll I$. Hence, by Lemma 2.5(i), $(c \circ c) \circ (b \circ c) \subseteq I$. Since $b \circ c \subseteq I$ and I is a weak hyper BCK-ideal of H, then $c \in c \circ c \subseteq I$, which is impossible.

Case 1-3. If $y = c$, then $c \circ c \subseteq I$ and $c \circ z \subseteq I$. Now, we consider the following cases for z;

Case 1-3-1. If $z = 0$ or a, since $c \circ z = y \circ z \subseteq I$ and $z \in I$ and I is a weak hyper BCK-ideal of H, then $c \in I$ which is impossible.

Case 1-3-2. If $z = b$, then $c \in x \circ z = x \circ b$, $c \circ c = c \circ y \subseteq I$ and $c \circ b = y \circ z \subseteq I$. It is clear that $x \neq 0$ and a. If $x = c$, then $c \in x \circ b = c \circ b \subseteq I$ which is impossible. Now, we let $x = b$. Then

$$c \circ c \subseteq I, \quad c \circ b \subseteq I, \quad (b \circ c) \circ b \subseteq I, \quad c \in b \circ b$$

By (HK3), $c \in b \circ b \ll b$. Then $0 \in c \circ b$ and so $0 \notin b \circ c$. Moreover, $b \notin b \circ c$. Since if $b \in b \circ c$, then $c \in b \circ b \subseteq (b \circ c) \circ b \subseteq I$, which is impossible. Hence, $b \circ c = \{a\}$ or $\{c\}$ or $\{a, c\}$.

Case 1-3-2-1. If $b \circ c = \{a\}$, by (HK1), $(b \circ b) \circ (c \circ b) \ll b \circ c = \{a\} \subseteq I$ and so by Lemma 2.5(i), $(b \circ b) \circ (c \circ b) \subseteq I$. Since $c \circ b \subseteq I$ and I is a weak hyper BCK-ideal of H, then $c \in b \circ b \subseteq I$, which is impossible.

Case 1-3-2-2. If $b \circ c = \{c\}$, then $c \circ (b \circ c) = c \circ c \subseteq (b \circ b) \circ c = (b \circ c) \circ b \subseteq I$. Since I is a weak implicative hyper BCK-ideal of H, then by Theorem 3.3, $c \in I$, which is impossible.

Case 1-3-2-3. If $b \circ c = \{a, c\}$, since I is a hyper BCK-ideal of H, then it is a hyper BCK-subalgebra of H and so by (HK2), we get that $(c \circ a) \circ b = (c \circ b) \circ a \subseteq I \circ a \subseteq I$. If $b \in c \circ a$, then $c \in b \circ b \subseteq (c \circ a) \circ b \subseteq I$, which is impossible. Moreover, if $c \circ a \subseteq I$, since $a \in I$ and I is a weak hyper BCK-ideal of H, then $c \in I$ which is impossible. Hence, $c \circ a = \{c\}$ or $\{a, c\}$. If $c \circ a = \{a, c\}$, since $c \circ c \subseteq I$ then

$$\begin{aligned} (c \circ a) \circ (c \circ a) &= \{a, c\} \circ \{a, c\} = (a \circ a) \cup (a \circ c) \cup (c \circ a) \cup (c \circ c) \\ &= \{0\} \cup \{0\} \cup \{a, c\} \cup (c \circ c) = \{0, a, c\} \end{aligned}$$

Hence, by (HK1), $\{0, a, c\} = (c \circ a) \circ (c \circ a) \ll c \circ c \subseteq I$, and so by Lemma 2.5(i), $\{0, a, c\} \subseteq I$ which is impossible. Therefore, $c \circ a = \{c\}$. Now, by (HK2), $(b \circ a) \circ c = (b \circ c) \circ a = \{a, c\} \circ a = (a \circ a) \cup (c \circ a) = \{0\} \cup \{c\} = \{0, c\}$. If $b \in b \circ a$, then $\{a, c\} = b \circ c \subseteq (b \circ a) \circ c = \{0, c\}$ which is impossible. Moreover, since $0 \in \{0\} = a \circ b$, then $0 \notin b \circ a$. Thus, $b \circ a = \{a\}$ or $\{c\}$ or $\{a, c\}$. If $b \circ a = \{a\}$, since $b \circ a \subseteq I$ and $a \in I$, then $b \in I$ which is impossible. If $b \circ a = \{c\}$ or $\{a, c\}$, then $c \circ a \subseteq (b \circ b) \circ a = (b \circ a) \circ b \subseteq \{a, c\} \circ b = (a \circ b) \cup (c \circ b) = \{0\} \cup (c \circ b) \subseteq I$. Since $a \in I$ and I is a weak hyper BCK-ideal of H, then $c \in I$, which is impossible.

Case 1-3-3. If $z = c$, then $c \in x \circ z = x \circ c$, $c \circ c \subseteq I$. It is clear that $x \neq 0$ and a. If $x = c$, then $c \in x \circ c = c \circ c \subseteq I$ which is impossible.
Now, let $x = b$. Hence

$$c \in b \circ c, \quad (b \circ c) \circ c \subseteq I, \quad c \circ c \subseteq I$$

Since I is a hyper BCK-subalgebra of H, then by (HK2), $(c \circ a) \circ c = (c \circ c) \circ a \subseteq I \circ a \subseteq I$. Now, by similar way to the proof of Case 1-3-2-3, we can prove that $c \circ a = \{c\}$. Also, since $c \in b \circ c \ll b$, then $0 \notin b \circ c$. Moreover, if $b \in b \circ c$, then $c \in b \circ c \subseteq (b \circ c) \circ c \subseteq I$ which is impossible. Thus, $b \circ c = \{c\}$ or $\{a, c\}$. If $b \circ c = \{c\}$, then $c \circ (b \circ c) = c \circ c \subseteq I$. Since I is a weak implicative hyper BCK-ideal of H, then by Theorem 3.3, $c \in I$ which is impossible. If $b \circ c = \{a, c\}$, then $(b \circ a) \circ c = (b \circ c) \circ a = \{0, c\}$.

Now, $(b \circ a) \cap \{0, b\} = \emptyset$. Since $0 \in \{0\} = a \circ b$ then $0 \notin b \circ a$. Moreover, if $b \in b \circ a$, then $a \in b \circ c \subseteq (b \circ a) \circ c = \{0, c\}$ which is impossible. Hence $b \circ a = \{a\}$ or $\{c\}$ or $\{a, c\}$. If $b \circ a = \{a\}$, then $\{0\} = (b \circ a) \circ c = \{0, c\}$ which is a impossible. If $b \circ a = \{c\}$ or $\{a, c\}$, then $\{0, c\} = \{0\} \cup \{c\} = (a \circ a) \cup (c \circ a) = \{a, c\} \circ a = (b \circ c) \circ a = (b \circ a) \circ c = c \circ c \subseteq I$, which is impossible. Thus, I is a positive implicative hyper BCK-ideal of type 3.

Case 2. $b \in x \circ z$

The proof is similar to the proof of Case 1, by the some modification. □

Example 3.8. Let $H = \{0, a, b, c\}$. Consider the following tables:

$\circ_1$	0	a	b	c
0	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
a	$\{a\}$	$\{0\}$	$\{0\}$	$\{0\}$
b	$\{b\}$	$\{a\}$	$\{0\}$	$\{a\}$
c	$\{c\}$	$\{c\}$	$\{0, c\}$	$\{0, c\}$

$\circ_2$	0	a	b	c
0	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
a	$\{a\}$	$\{0\}$	$\{0\}$	$\{0\}$
b	$\{b\}$	$\{b\}$	$\{0\}$	$\{0\}$
c	$\{c\}$	$\{c\}$	$\{c\}$	$\{0, c\}$

Thus $(H, \circ_1)$ and $(H, \circ_2)$ are hyper BCK-algebras such that $a \circ x = \{0\}$ for all $0 \neq x \in H$. It is easy to check that $I_1 = \{0, a, b\}$ is a weak implicative hyper BCK-ideal of $(H, \circ_1)$ but it is not a hyper BCK-ideal of $(H, \circ_1)$ (since $c \circ b = \{0, c\} \ll \{0, a, b\} = I_1$ and $b \in I_1$ but $c \notin I_1$) and so it is not a positive implicative hyper BCK-ideal of type 3 in $(H, \circ_1)$. Therefore, the hyper BCK-ideal condition is necessary in Theorem 3.7. Moreover, $I_2 = \{0, a\}$ is a positive implicative hyper BCK-ideal of type 3 in $(H, \circ_2)$ but it is not a weak implicative hyper BCK-ideal. Since, $(b \circ a) \circ (c \circ b) = \{0\} \subseteq I_2$ and $a \in I_2$ but $b \notin I_2$. Therefore, the converse of the Theorem 3.7 is not correct in general.

Definition 3.9. Let I be a non-empty subset of H. Then,

(i) I is said to be an *implicative hyper BCK-ideal* of H if $0 \in I$ and for all $x, y, z \in H$, $(x \circ z) \circ (y \circ x) \ll I$ and $z \in I$ imply $x \in I$,

(ii) H is called an *implicative hyper BCK-algebra* if $x \ll x \circ (y \circ x)$, for all $x, y \in H$.

It is easy to check that H is an implicative hyper BCK-algebra if and only if $x \in x \circ (y \circ x)$, for all $x, y \in H$.

Theorem 3.10. *Every implicative hyper BCK-ideal of H is a weak implicative hyper BCK-ideal of H.*

Proof. The proof is straightforward. □

Example 3.11. Consider the following table on $H = \{0, a, b\}$:

$\circ$	0	a	b
0	$\{0\}$	$\{0\}$	$\{0\}$
a	$\{a\}$	$\{0, a\}$	$\{0, a\}$
b	$\{b\}$	$\{a\}$	$\{0, a\}$

Then $(H, \circ)$ is hyper BCK-algebra. We can see that $I = \{0, b\}$ is a weak implicative hyper BCK-ideal of H, but it is not an implicative hyper BCK-ideal of H. Because, $(a \circ 0) \circ (a \circ a) = a \circ \{0, a\} = \{0, a\} \ll \{0, b\} = I$ and $0 \in I$, but $a \notin I$.

Theorem 3.12. [8] *Let I be a non-empty subset of H. Then,*

(i) *if I is an implicative hyper BCK-ideal of H, then it is a hyper BCK-ideal of H,*

(ii) *if I is a hyper BCK-ideal of H, then I is an implicative hyper BCK-ideal of H if and only if $x \circ (y \circ x) \ll I$ implies that $x \in I$, for all $x, y \in H$.*

Corollary 3.13. *Let $H = \{0, a, b, c\}$ be a hyper BCK-algebra such that $a \circ x = \{0\}$, for all $0 \neq x \in H$ and I be a proper subset of H. If I is an implicative hyper BCK-ideal of H, then I is a positive implicative hyper BCK-ideal of type* 3.

Proof. Since every implicative hyper BCK-ideal of H is a weak implicative and a hyper BCK-ideal, then the proof follows by Theorem 3.7. □

Theorem 3.14. *Let H be a positive implicative and an implicative hyper BCK-algebra and I be a non-empty subset of H. Then the following statements are equivalent:*

(i) *I is a (weak) hyper BCK-ideal of H,*

(ii) *I is a positive implicative hyper BCK-ideal of type* 3 *(type* 1*) of H,*

(iii) *I_a is a (weak) implicative hyper BCK-ideal of H, for all $a \in H$,*

(iv) *I is a (weak) implicative hyper BCK-ideal of H.*

Proof. (i) $\Rightarrow$ (ii) The proof follows from Theorem 3.6 of [1] and Theorem 2.4(ii).

(ii) $\Rightarrow$ (iii) Since I is a positive implicative hyper BCK-ideal of type 3 (type 1), then by Theorem 2.4, I_a is a (weak) hyper BCK-ideal of H. Now, let $a \in H$ and $(x \circ (y \circ x) \subseteq I_a)$ $x \circ (y \circ x) \ll I_a$, for $x, y \in H$. Since H is an implicative hyper BCK-algebra, then $x \in I_a$ and so I_a is an (weak) implicative hyper BCK-ideal of H.

(iii) $\Rightarrow$ (iv) Since $I_0 = I$, it is enough set $a = 0$.

(iv) $\Rightarrow$ (i) The proof follows from Theorem 3.3. □

Example 3.15. (i) Let $H = \{0, a, b, c\}$. Consider the following table:

$\circ$	0	a	b	c
0	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
a	$\{a\}$	$\{0\}$	$\{0\}$	$\{0\}$
b	$\{b\}$	$\{b\}$	$\{0\}$	$\{0\}$
c	$\{c\}$	$\{c\}$	$\{b\}$	$\{0, b\}$

Then $(H, \circ)$ is a hyper BCK-algebra which it is not a positive implicative hyper BCK-algebra. Since $(c \circ b) \circ b \neq (c \circ b) \circ (b \circ b)$. Now, $I = \{0, a\}$ is a (weak) hyper BCK-ideal of H but it is not a positive implicative hyper BCK-ideal of type 1(and so it is not of type 3). Because $(c \circ b) \circ c = \{0\} \subseteq \{0, a\}$ and $b \circ c = \{0\} \subseteq \{0, a\}$ but $c \circ c = \{0, b\} \nsubseteq \{0, a\}$. Therefore, the positive implicative hyper BCK-algebra condition is necessary in Theorem 3.14.

(ii) The hyper BCK-algebra in Example 2.2(ii) is not an implicative hyper BCK-algebra. Because, $b \notin \{0\} = b \circ (0 \circ b)$. Now, $I = \{0, a\}$ is a (weak) hyper BCK-ideal of H but it is not a weak implicative hyper BCK-ideal and so is not an implicative hyper BCK-ideal of H. Thus, the implicative hyper BCK-algebra condition is necessary in Theorem 3.14.

Definition 3.16. Let I be a non-empty subset of H. Then I is called a

(i) *strong implicative hyper BCK-ideal* of H if $0 \in I$ and
$$((x \circ z) \circ (y \circ x)) \cap I \neq \emptyset \text{ and } z \in I \text{ imply } x \in I$$

(ii) *strong positive implicative hyper BCK-ideal* of H if $0 \in I$ and
$$((x \circ y) \circ z) \cap I \neq \emptyset \text{ and } y \circ z \subseteq I \text{ imply } x \circ z \subseteq I$$

for all $x, y, z \in H$.

Theorem 3.17. [14]

(i) *Every strong implicative hyper BCK-ideal of H is a (strong, implicative) hyper BCK-ideal,*

(ii) *Every reflexive strong implicative hyper BCK-ideal of H is a strong positive implicative hyper BCK-ideal .*

(iii) *Every strong positive implicative hyper BCK-ideal of H is a (strong hyper BCK-ideal) positive implicative hyper BCK-ideal of type 3.*

Theorem 3.18.

(i) *Every reflexive implicative hyper BCK-ideal of H is a strong implicative hyper BCK-ideal,*

(ii) *Every reflexive positive implicative hyper BCK-ideal of type 3 is a strong positive implicative hyper BCK-ideal .*

(iii) *Every reflexive implicative hyper BCK-ideal of H is a positive implicative hyper BCK-ideal of type* 3.

Proof. (i) Let I be a reflexive implicative hyper BCK-ideal of H, $((x \circ (y \circ x) \circ z) \cap I = ((x \circ z) \circ (y \circ x)) \cap I \neq \emptyset$ and $z \in I$, for $x, y, z \in H$. Then, there is $u \in x \circ (y \circ x)$ such that $(u \circ z) \cap I \neq \emptyset$ and $z \in I$. Since I is a reflexive hyper BCK-ideal of H and so is a strong hyper BCK-ideal of H, then $u \in I$. This implies that $(x \circ (y \circ x)) \cap I \neq \emptyset$ and so by Lemma 2.5, $x \circ (y \circ x) \ll I$ and since I is an implicative hyper BCK-ideal, then $x \in I$. Therefore, I is a strong implicative hyper BCK-ideal of H.

(ii) Let I be a reflexive positive implicative hyper BCK-ideal of type 3, $((x \circ y) \circ z) \cap I \neq \emptyset$ and $y \circ z \subseteq I$, for $x, y, z \in H$. Then by Lemma 2.5(iv), $(x \circ y) \circ z \ll I$ and $y \circ z \subseteq I$. Since I is a positive implicative hyper BCK-ideal of type 3, then $x \circ z \subseteq I$, which implies that I is a strong positive implicative hyper BCK-ideal of H.

(iii) The proof follows from (i), Theorem 3.17(ii) and (iii) □

Theorem 3.19. *Let H be an implicative hyper BCK-algebra and I be a non-empty subset of H. Then I is a* (*weak*) *hyper BCK-ideal of H if and only if it is a* (*weak*) *implicative hyper BCK-ideal of H.*

Proof. By Theorems 3.3 and 3.12, any (weak) implicative hyper BCK-ideal of H is a (weak) hyper BCK-ideal of H. Conversely, let I be a (weak) hyper BCK-ideal of H and $(x \circ (y \circ x) \subseteq I)$ $x \circ (y \circ x) \ll I$. Since H is an implicative hyper BCK-algebra, then $(x \in x \circ (y \circ x) \subseteq I)$ $x \in x \circ (y \circ x) \ll I$. Hence, by Lemma 2.5(i), Theorems 3.3 and 3.12(iii) I is a (weak) implicative hyper BCK-ideal of H. □

Corollary 3.20. *Let H be an implicative hyper BCK-algebra. Then,*

(i) *every commutative hyper BCK-ideal of type* 3 (*type* 1) *is an implicative* (*weak implicative*) *hyper BCK-ideal of H,*

(ii) *every reflexive commutative hyper BCK-ideal of type* 3 *is a positive implicative hyper BCK-ideal of type* 3.

Proof. (i) Since every commutative hyper BCK-ideal of type 3 (type 1) is a (weak) hyper BCK-ideal of H, then the proof follows from Theorem 3.19.

(ii) The proof follows from (i), Theorems 3.18(i), 3.17(ii) and (iii). □

Example 3.21. Let $(H, \circ_1)$ be hyper BCK-algebra which is defined in Example 3.8. Then, $I = \{0, a, b\}$ is a commutative hyper BCK-ideal of type 3 but it is not an implicative hyper BCK-ideal of H. Because, $c \notin I$

but for all $z \in I$ and $y \in H$, $(c \circ z) \circ (y \circ c) \subseteq \{0, c\} \ll I$. Moreover, H is not an implicative hyper BCK-algebra because, $a \notin \{0\} = a \circ (c \circ a)$. Thus the implicative hyper BCK-algebra condition is necessary in Corollary 3.20.

Corollary 3.22. *Let $H = \{0, a, b\}$ be a hyper BCK-algebra of order 3 and I be a non-empty subset of H. Then,*

(i) *I is an implicative hyper BCK-ideal of H if and only if I is a hyper BCK-ideal of H,*

(ii) *I is an implicative hyper BCK-ideal of H if and only if I is a positive implicative hyper BCK-ideal of type 3 of H,*

(iii) *I is an implicative hyper BCK-ideal of H if and only if it is a commutative hyper BCK-ideal of type 3,*

(iv) *there are only 16 non-isomorphic hyper BCK-algebra of order 3 such that each of them has at least one proper (commutative hyper BCK-ideal of type 3) implicative hyper BCK-ideal.*

Proof. (i) ($\Rightarrow$) The proof follows by Theorem 3.12(i).

($\Leftarrow$) By Theorem 3.12(ii) it is enough to show that $x \circ (y \circ x) \ll I$ implies $x \in I$, for all $x, y \in H$. Now, by considering Lemmas 2.5(i) and Lemma 2.6 of [1], the proof is similar to the proof of Theorem 3.5.

(ii) The proof follows by (i) and Theorem 3.10 of [1].

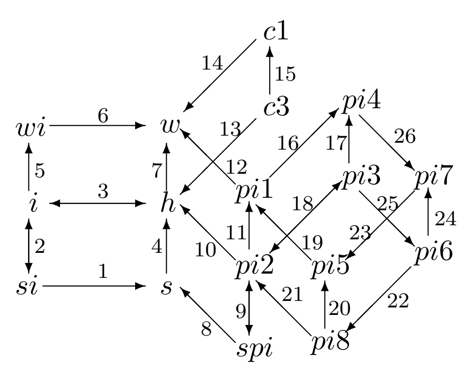
(iii) The proof follows from (i) and Theorem 4.6(i) of [1].

(iv) The proof follows by (i), (iii) and Theorem 3.14 of [2]. □

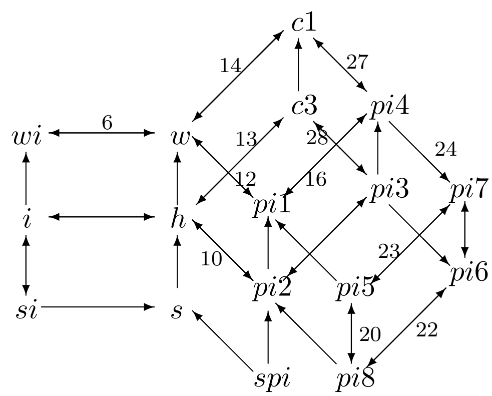
4. Conclusion

Theorem 3.23.

(i) *The following diagram hold for any hyper BCK-algebras:*



(ii) *the following diagram hold for any hyper BCK-algebras of order* 3*:*



where,

c1	*commutative hyper BCK-ideal of type* 1
c3	*commutative hyper BCK-ideal of type* 3
pij	*positive implicative hyper BCK-ideal of type* j $(j = 1, ..., 8)$
spi	*strong positive implicative hyper BCK-ideal*
h	*hyper BCK-ideal*
s	*strong hyper BCK-ideal*
w	*weak hyper BCK-ideal*
i	*implicative hyper BCK-ideal*
si	*strong implicative hyper BCK-ideal*
wi	*weak implicative hyper BCK-ideal*

Proof. (i)

Arrow(s)	**Reason(s)**
1	By Theorem 3.17(i)
2	By Theorems 3.17(i) and 3.18(i)
3	By Theorems 3.12(i) and 3.19
$4, 7, 10, 12, 13, 14$	Remark befor Theorem 2.4
5	By Theorem 3.10
6	By Theorem 3.3
$8, 9$	By Theorems 3.17(iii) and 3.18(ii)
$11, 16, 17, ..., 26$	See Ref. [2]
15	See Ref. [1]

(ii)

Arrow(s)	**Reason(s)**
6	By Theorem 3.5
$10, 12, 16, 20, 22, 23, 24$	See Ref. [2]
$13, 14, 27, 28$	See Ref. [1]

□

Open problems

(i) *Under what condition(s), a weak implicative hyper BCK-ideal is an implicative hyper BCK-ideal ?*

(ii) *By Theorem* 3.5*, the notions of weak hyper BCK-ideal and weak implicative hyper BCK-ideal are equivalent in any hyper BCK-algebras of order* 3*. Is it correct this theorem in any hyper BCK-algebras of order greater than* 3 *?*

References

[1] **R. A. Borzooei, M. Bakhshi**: *Some results on hyper BCK-algebras*, Quasigroups and Related Systems **11** (2004), 9 – 24.

[2] **R. A. Borzooei, M. Bakhshi**: *On positive implicative hyper BCK-ideals*, Sci. Math. Japonicae (2004), to appear.

[3] **R. A. Borzooei, P. Corsini, M. M. Zahedi**: *Some kinds of positive implicative hyper K-ideals*, Discrete Math. Sci. Cryptography, **6** (2003), 97 – 108.

[4] **R. A. Borzooei, M. M. Zahedi, H. Rezaei**: *Classification of hyper BCK-algebras of order* 3, Italian J. Pure Appl. Math. **12** (2002), 175 – 184.

[5] **R. A. Borzooei, M. M. Zahedi**: *Positive implicative hyper K-ideals*, Sci. Math. Japonicae **53** (2001), 525 – 533.

[6] **P. Corsini, V. Leoreanu**: *Applications of hyperstructures theory*, Advanced in Mathematics, Kluwer Academic Publishers, 2003.

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

[8] **Y. B. Jun, X. L. Xin**: *Implicative hyper BCK-ideals of hyper BCK-algebras*, Math. Japonicae **52** (2000), 435 – 443.

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

[10] **Y. B. Jun, X. L. Xin**: *Positive implicative hyper BCK-algebras*, Sci. Math. Japonicae **55** (2002), 97 – 106.

[11] **Y. B. Jun, X. L. Xin, E. H. Roh, M. M. Zahedi**: *Strong hyper BCK-ideals of hyper BCK-algebras*, Math. Japonicae **51** (2000), 493 – 498.

[12] **Y. B. Jun, M. M. Zahedi, X. L. Xin, R. A. Borzooei**: *On hyper BCK-algebras*, Italian J. Pure Applied Math. **8** (2000), 127 – 136.

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

[14] **E. H. Roh, Q. Zhang, Y. B. Jun**: *Some results in hyper BCK-algebras*, Sci. Math. Japonicae **55** (2002), 297 − 304.

Department of Mathematics
Sistan and Baluchestan University
Zahedan
Iran
e-mail: borzooei@hamoon.usb.ac.ir,
mbakhshi@hamoon.usb.ac.ir

Received November 14, 2003
Revised January 16, 2004

Quasigroups and Related Systems **12** (2004), 29 − 38

Necessary and sufficient conditions for the continuity of a pre-Haar system at a unit with singleton orbit

Mădălina R. Buneci

Abstract

For developing an algebraic theory of functions on a locally compact groupoid, one needs an analogue of Haar measure on locally compact groups. This analogue is a system of measures, called Haar system, subject to suitable invariance and smoothness conditions called respectively "left invariance" and "continuity". Unlike the case of locally compact group, Haar system on groupoid need not exists. In this paper we shall consider a locally compact groupoid G, and we shall denote by $G_s^{(0)}$ the set of units with singleton orbit and by G_s the reduction $G|_{G_s^{(0)}}$ of G to $G_s^{(0)}$. We shall prove that if G admits Haar systems, then the restriction of the range map at G_s is an open map from G_s to $G_s^{(0)}$. Conversely, we shall prove that if this map is open at every $x \in G_s$, then the continuity condition of a Haar system holds at every unit with singleton orbit.

1. Introduction

In order to establish notation for this paper we shall include some definitions that can be found in several places (e.g. [4], [5], [6], [7]).

Definition 1. A *groupoid* is a set G endowed with a product map

$$(x, y) \to xy \ \left[: G^{(2)} \to G\right]$$

where $G^{(2)}$ is a subset of $G \times G$ called the *set of composable pairs*, and an *inverse map*

$$x \to x^{-1} \ [: G \to G]$$

2000 Mathematics Subject Classification: 22A22, 28C99, 43A05
Keywords: locally compact groupoid, Haar system, orbit.

such that the following conditions hold:

(1) If $(x,y) \in G^{(2)}$ and $(y,z) \in G^{(2)}$, then $(xy,z) \in G^{(2)}$, $(x,yz) \in G^{(2)}$ and $(xy)\,z = x\,(yz)$,
(2) $\left(x^{-1}\right)^{-1} = x$ for all $x \in G$,
(3) $\left(x, x^{-1}\right) \in G^{(2)}$, and if $(z,x) \in G^{(2)}$, then $(zx)\,x^{-1} = z$, for each $x \in G$,
(4) $\left(x^{-1}, x\right) \in G^{(2)}$, and if $(x,y) \in G^{(2)}$, then $x^{-1}(xy) = y$, for each $x \in G$.

The maps r and d on G, defined by the formulae $r(x) = xx^{-1}$ and $d(x) = x^{-1}x$, are called the *range* and the *source maps*. It follows easily from the definition that they have a common image called the *unit space* of G, which is denoted $G^{(0)}$. Its elements are units in the sense that $xd(x) = r(x)\,x = x$. Units will usually be denoted by letters as u, v, w while arbitrary elements will be denoted by x, y, z. It is useful to note that a pair (x,y) lies in $G^{(2)}$ precisely when $d(x) = r(y)$, and that the cancellation laws hold (e.g. $xy = xz$ iff $y = z$). The fibres of the range and the source maps are denoted $G^u = r^{-1}(\{u\})$ and $G_v = d^{-1}(\{v\})$, respectively. More generally, given the subsets A, $B \subset G^{(0)}$, we define $G^A = r^{-1}(A)$, $G_B = d^{-1}(B)$ and $G_B^A = r^{-1}(A) \cap d^{-1}(B)$. The reduction of G to $A \subset G^{(0)}$ is $G|A = G_A^A$. The relation $u \sim v$ iff $G_v^u \neq \emptyset$ is an equivalence relation on $G^{(0)}$. Its equivalence classes are called *orbits* and the orbit of a unit u is denoted $[u]$. The quotient space for this equivalence relation is called the *orbit space* of G and denoted $G^{(0)}/G$. A groupoid is called *transitive* iff it has a single orbit, or equivalently if the map $(r,d) : G \to G^{(0)} \times G^{(0)}, (r,d)(x) = (r(x), d(x))$ is surjective. A groupoid is said *principal* if the map $(r,d) : G \to G^{(0)} \times G^{(0)}, (r,d)(x) = (r(x), d(x))$ is injective.

Examples structures which fit naturally into the study of groupoids:

1. *Groups*: A group G is a groupoid with $G^{(2)} = G \times G$ and $G^{(0)} = \{e\}$ (the unit element).

2. *Spaces*. A space X is a groupoid letting $X^{(2)} = \{(x,x) \in G \times G\} = diag(X)$, $xx = x$, and $x^{-1} = x$.

3. *Equivalence relations*. Let $R \subset X \times X$ be an equivalence relation on the set X. Let $R^{(2)} = \{((x_1,y_1),(x_2,y_2)) \in R \times R : y_1 = x_2\}$. With product $(x,y)(y,z) = (x,z)$ and $(x,y)^{-1} = (y,x)$, R is a principal groupoid. $R^{(0)}$ may be identified with X. Two extreme cases deserve to be single out. If $R = X \times X$, then R is called the *trivial groupoid* on X, while if $R = diag(X)$, then R is called the *co-trivial groupoid* on X (and may be identified with the groupoid in Example 2).

4. *Transformation groups.* Let Γ be a group acting on a set X such that for $x \in X$ and $g \in \Gamma$, xg denotes the transform of x by g. Let $G = X \times \Gamma$, $G^{(2)} = \{((x,g),(y,h)) : y = xg\}$. With the product $(x,g)(xg,h) = (x,gh)$ and the inverse $(x,g)^{-1} = \left(xg, g^{-1}\right)$ G becomes a groupoid. The unit space of G may be identified with X.

Definition 2. A *topological groupoid* consists of a groupoid G and a topology compatible with the groupoid structure:

(1) $x \to x^{-1}$ $[: G \to G]$ is continuous.

(2) (x,y) $\left[: G^{(2)} \to G\right]$ is continuous where $G^{(2)}$ has the induced topology from $G \times G$.

If G is a topological groupoid, then r and d are identification maps, and $x \to x^{-1}$ is a homeomorphism. If G is Hausdorff, $G^{(0)}$ is closed, and if $G^{(0)}$ is Hausdorff, $G^{(2)}$ is closed in $G \times G$.

We are exclusively concerned with topological groupoids which are locally compact and Hausdorff. It was shown in [6] that measured groupoids (in the sense of Definition 2.3. from [4]) may be assume to have locally compact topologies, with no loss in generality.

There are several generalizations of the classical Haar measure associated with a locally compact topological group to the setting of a locally compact topological groupoid (see [14], [9], [10], [11], [4], [7]). Now in general use is the definition adopted by Jean Renault in [7]:

Definition 3. A *Haar system* on a locally compact groupoid G is a family of positive Radon measures on G, $\left\{\nu^u,\, u \in G^{(0)}\right\}$, having the following properties:

1) For all $u \in G^{(0)}$, $supp(\nu^u) = G^u$.

2) For all $f \in C_c(G)$

$$u \to \int f(x)\, d\nu^u(x) \quad \left[: G^{(0)} \to \mathbf{C}\right]$$

is continuous.

3) For all $f \in C_c(G)$ and all $x \in G$,

$$\int f(y)\, d\nu^{r(x)}(y) = \int f(xy)\, d\nu^{d(x)}(y)$$

The system of measures $\left\{\nu^u,\, u \in G^{(0)}\right\}$ will be called *Borel Haar system* if it has the properties 1), 3) and

2′) For all $f \geqslant 0$ Borel on G,

$$u \to \int f(x)\, d\nu^u(x) \quad \left[: G^{(0)} \to \bar{\mathbf{R}}\right]$$

is a real-extended Borel map, where the Borel sets of a topological spaces G and $G^{(0)}$ are taken to be the σ-algebra generated by the open sets.

Unlike the case of locally compact group, Haar system on groupoid need not exists. The continuity assumption 2) has topological consequences for G. It entails that the range map $r : G \to G^{(0)}$, and hence the domain map $d : G \to G^{(0)}$ is an open (Proposition I.4 [13]). So "the range map is an open map" is a necessary condition for the existence of Haar systems. A. K. Seda has established sufficient conditions for the existence of Haar systems. He has proved that if for all $u \in G^{(0)}$, the map $r_u : G_u \to G^{(0)},\ r_u(x) = r(x)$ is open, then the continuity assumption 2) follows from the left invariance assumption 3) (Theorem 2, p.430 [10]). Thus he has proved that locally transitive groupoids admit Haar system. At the opposite case of totally intransitive groupoids, Renault has established necessary and sufficient conditions. More precisely, Renault has proved that a locally compact group bundle (a groupoid with the property that $r(x) = d(x)$ for all x) admits a Haar system if and only if r is open (Lemma 1.3, p.6 [8]).

In this paper we shall study the continuity of a pre-Haar system at the units u with singleton orbits (this means $[u] = \{u\}$). We shall establish necessary and sufficient conditions. When all units of the groupoid are with singleton orbits we shall re-obtain the result of Renault Lemma 1.3, p.6 [8].

2. The existence of a pre-Haar system

Definition 4. A (*left*) *pre-Haar system* on G is a family of (positive) Radon measures on G, $\{\nu^u,\ u \in G^{(0)}\}$,with the following properties:

1) ν^u concentrated on G^u for all $u \in G^{(0)}$;
2) $\int f(y)\, d\nu^{r(x)}(y) = \int f(xy)\, d\nu^{d(x)}(y)$ for all $x \in G$ and $f \in C_c(G)$
3) $\sup\{\nu^u(K),\ u \in G^{(0)}\} < \infty$ for each compact set $K \subset G$.

Definition 5. The pre-Haar system $\{\nu^u,\ u \in G^{(0)}\}$ is said *continuous at* u_0 if for all $f \in C_c(G)$, the map

$$u \to \int f(x)\, d\nu^u(x) \quad \left[: G^{(0)} \to \mathbf{C}\right]$$

is continuous is continuous at u_0.

The pre-Haar system is said *continuous* if it is continuous at every unit (or equivalently if it is a Haar system).

In [2] we have shown that the continuity of a pre-Haar system is equivalent with the continuity of a family of homomorphisms associated to the pre-Haar system.

Notation 6. Let $\{\nu^u,\ u \in G^{(0)}\}$ be a pre-Haar system on the locally compact groupoid G. For each $f \in C_c(G)$ let us denote by $F_f : G \to \mathbf{C}$ the map defined by

$$F_f(x) = \int f(y)\, d\nu^{d(x)}(y) - \int f(y)\, d\nu^{r(x)}(y) \quad (\forall)\ x \in G$$

For each f, F_f is a homomorphism of groupoids:

$$F_f(xy) = F_f(x) - F_f(y) \text{ for all } (x, y) \in G^{(2)}.$$

$\{F_f\}_{f \in C_c(G)}$ will be called the *family of homomorphisms associated with the pre-Haar system.*

We state Lemma 4.2 p.40 [2]:

Lemma 7. *Let G be a locally compact groupoid whose unit space $G^{(0)}$ is paracompact, let $\{\nu^u,\ u \in G^{(0)}\}$ be a pre-Haar system on G and let $\{F_f\}_f$ the family of associated homomorphisms. Then for each $f \in C_c(G)$ and each $\varepsilon > 0$ there is W_ε, a conditionally compact neighborhood of $G^{(0)}$, such that:*

$$|F_f(x)| < \varepsilon \text{ for all } x \in W_\varepsilon$$

We shall show how to construct a pre-Haar system. Let G be a locally compact second countable groupoid. In Section 1 of [8] Jean Renault constructs a Borel Haar system for G'. One way to do this is to choose a function F_0 continuous with conditionally support which is nonnegative and equal to 1 at each $u \in G^{(0)}$. Then for each $u \in G^{(0)}$ choose a left Haar measure β_u^u on G_u^u so the integral of F_0 with respect to β_u^u is 1.

Renault defines $\beta_v^u = x\beta_v^v$ if $x \in G_v^u$ (where $x\beta_v^v(f) = \int f(xy)\, d\beta_v^v(y)$ as usual). If z is another element in G_v^u, then $x^{-1}z \in G_v^v$, and since β_v^v is a left Haar measure on G_v^v, it follows that β_v^u is independent of the choice of x. If K is a compact subset of G, then $\sup\limits_{u,v} \beta_v^u(K) < \infty$.

For constructing a pre-Haar system it is enough to choose a family of probability measure on $G^{(0)}$ indexed on the orbit space $\left\{\mu^{\dot{u}},\ \dot{u} \in G^{(0)}/G\right\}$ such that $supp\left(\mu^{\dot{u}}\right) = [u]$. We define

$$\int f(y)\, d\nu^{u}(y) = \int f(y)\, d\beta_{v}^{u}(y)\, d\mu^{\dot{u}}(y)$$

for all continuous function f on G with compact support.

It is not hard to see that $\{\nu^{u},\ u \in G^{(0)}\}$ is a pre-Haar system. Applying a result of Federer and Morse [3], it follows that the map

$$(r, d) : G \to (r, d)(G)$$

has Borel section σ. If we define $h(x) = F_0\left(\sigma(r(x), d(x))^{-1} x\right)$, then we obtain a Borel function with the property that

$$\int h(x)\, \nu^{u}(y) = 1 \text{ for all } u.$$

Another construction of pre-Haar system can be found in [1].

3. The continuity of a pre-Haar system

Lemma 8. *Let G be a locally compact groupoid with the range map r open. Then the set of units with singleton orbit is a closed subset of the unit space.*

Proof. Let $(u_i)_i$ be net of units with singleton orbits. Let us assume that $(u_i)_i$ converges to u and let x in G with $r(x) = u$. We shall prove that $r(x) = d(x)$, and it will follows that $[u] = \{u\}$. Since r is an open map, eventually passing to a subnet, we may assume that there is a net $(x_i)_i$ in G that converges to x, such that $r(x_i) = u_i$. Since each u_i is with singleton orbit, $d(x_i) = r(x_i) = u_i$. Hence

$$d(x) = \lim d(x_i) = \lim u_i = u.$$

Thus the set of units with singleton orbit is a closed subset of the unit space. ☐

Notation 9. Let G be a locally compact groupoid with the range map r open. Let us denote by $G_s^{(0)}$ the set of units with singleton orbit. According to the preceding lemma $G_s^{(0)}$ is a closed subset of the unit space. Let us denote by G_s the reduction $G|_{G_s^{(0)}}$ of G to $G_s^{(0)}$. Then G_s is a closed subgroupoid of G'.

Lemma 10. *Let G be a locally compact groupoid that admits a Haar system. Then*

$$r_s : G_s \to G_s^{(0)}, \quad r_s(x) = r(x)$$

is an open map.

Proof. Let $\{\nu^u,\ u \in G^{(0)}\}$ be a Haar system on G. Let $x_0 \in G_s$ and let U be a nonempty compact neighborhood of x_0 in G_s. Choose a nonnegative continuous function, f on G_s , with $f(x_0) > 0$ and $supp\,(f) \subset U$. Let V be an open neighborhood of G_s. Let $\tilde{f}$ be a continuous function extending f to G with $supp\left(\tilde{f}\right) \subset V$. Let W the set of units u with the property that $\nu^u(f) > 0$. Then W is an open neighborhood of $u_0 = r(x_0)$ contained in $r(U) \cup r(V - G_s)$. Since $W \cap G_s^{(0)} \subset r(U) \cap G_s^{(0)}$, it follows that $r(U)$ is a neighborhood of u_0 in $G_s^{(0)}$. □

Definition 11. Let u be a unit with singleton orbit. We shall say that the *restriction of r to G_s is open at $x \in G_u^u$*, if it sends every open neighborhood of x to a open neighborhood of u in $G^{(0)}$.

Lemma 12. *Let u be a unit with singleton orbit. If the restriction of r to G_s is open at $x \in G_u^u$, then G_sW is a neighborhood of x in G, for each neighborhood W of $G^{(0)}$.*

Proof. Let x be an element of G_u^u. Let V be an open neighborhood of $G^{(0)}$ contained in W. Let us prove that G_sW contains x in its interior. Let $(x_i)_i$ be a net converging to x . Since r sends every open neighborhood of x, to an open neighborhood of u, eventually passing to a subnet we may assume that there is a net $(z_i)_i$ in G_s that converges to x, such that $r(x_i) = r(z_i)$. The net $\left(z_i^{-1}x_i\right)_i$ converges to $d(x)$, so for i large enough $z_i^{-1}x_i$ belongs to W. Consequently, $x_i = z_i t_i$ with $z_i \in G'$ and $t_i = z_i^{-1}x_i$ in W. Hence G_sW is a neighborhood of x. □

Theorem 13. *Let G be a locally compact groupoid whose unit space $G^{(0)}$ is paracompact and whose range map r is open. Let $\{\nu^u,\ u \in G^{(0)}\}$ be pre-Haar system. Let u be a unit with singleton orbit $[u]$. Assume that if W is an open neighborhood of $G^{(0)}$, then each $x \in G_s$ is in the interior of G_sW.*

If there exists a function $h : G \to [0,1]$, universally measurable on each transitivity component $G|_{[w]}$, with $\nu^w(h) = 1$ for all $w \in G^{(0)}$, then the pre-Haar system is continuous at u.

Proof. To prove the continuity of the pre-Haar system at u we shall use the same argument as in Lemma 1.3 p.6 [8]. Let $\mathcal{B}$ be the linear space of the bounded sequences of real numbers. Let $s \mapsto Lim\,(s)\,[: \mathcal{B} \to \mathbf{R}]$ be a linear map with the following properties:

1) If $s = (s_i)_i$ and $s_i \geqslant 0$, then $Lim\,(s) \geqslant 0$;

2) $Lim\,(1, 1, ..., 1...) = 1$;

3) $Lim\,(s_1, s_2, s_3, ...) = Lim\,(s_1, s_1, s_2, s_2, s_3, s_3...)$;

4) If $s, t \in \mathcal{B}$ and $\lim_n (s_n - t_n) = 0$, then $Lim\,(s) = Lim\,(t)$;

It is not hard to show that $\lim_n s_n = a$ implies that $Lim\,(s_1, s_2, ...) = a$. Also if $Lim\,(s') = a$ for every subsequence s' of s, then $\lim_n s_n = a$.

Let $\{F_f\}_{f \in C_c(G)}$ be the family of homomorphisms associated with the pre-Haar system.

Let $(u_i)_i$ a sequence converging to u. For each continuous function with compact support, $f : G \to \mathbf{R}$, we set

$$\mu\,(f) = Lim\left(i \mapsto \int f\,(y)\,d\nu^{u_i}\,(y)\right)$$

μ is a positive linear functional on the space of continuous functions with compact support. We claim that $\mu\,(f)$ depends only on the restriction on f on G_u^u. Suppose that f and g coincide on G_u^u. We denote by K the compact set

$$(supp\,(f) \cup supp\,(g)) \cap r^{-1}\,(\{u_i, i = 1, 2, ...\} \cup \{u\})$$

Then we have

$$\left|\int f\,(y)\,d\nu^{u_i}\,(y) - \int g\,(y)\,d\nu^{u_i}\,(y)\right| \leqslant \int |f\,(y) - g\,(y)|\,d\nu^{u_i}\,(y) \leqslant$$

$$\leqslant \sup_{y \in G^{u_i}} |f\,(y) - g\,(y)|\,\nu^{u_i}\,(K)$$

One observes that $\sup_{y \in G^{u_i}} |f\,(y) - g\,(y)|\,\nu^{u_i}\,(K)$ converges to 0. Therefore $\mu\,(f) = \mu\,(g)$. Next we show that μ is left invariant on G_u^u, and consequently, a Haar measure on G_u^u.Let $x \in G_u^u$. Because $r : G \to G^{(0)}$ is an open map there exists a sequence $(x_i)_i$ converging to x such that $r\,(x_i) = u_i$.

Let $f, g : G \to \mathbf{R}$ two continuous function with compact support such that $g\,(y) = f\left(x^{-1}y\right)$ for all $y \in G^u$.

Then we have

$$\left|\int f\,(y)\,d\nu^{u_i}\,(y) - \int g\,(y)\,d\nu^{u_i}\,(y)\right| =$$

$$\leqslant \left|\int f d\nu^{r(x_i)} - \int f d\nu^{d(x_i)}\right| + \left|\int f(y)\, d\nu^{d(x_i)}(y) - \int g(x_i y)\, d\nu^{d(x_i)}(y)\right|$$
$$\leqslant |F_f(x_i)| + \sup_{y\in G^{d(x_i)}} |f(y) - g(x_i y)|\, \nu^{d(x_i)}(K_1),$$

where K_1 is the compact set

$$(supp\,(f) \cup \{x, x_i, i = 1, 2, ..\}\, supp\,(g)) \cap r^{-1}(\{d(x_i), i = 1, 2, ...\} \cup \{u\}).$$

The sequence $i \mapsto \sup_{y\in G^{d(x_i)}} |f(y) - g(x_i y)|\, \nu^{d(x_i)}(K_1)$ converges to 0.

Let $\varepsilon > 0$ and let W be a neighborhood of $G^{(0)}$ such that

$$|F_f(y)| < \frac{\varepsilon}{2} \quad \text{for all } y \in W.$$

Since $G_s W$ is a neighborhood of x, and $(x_i)_i$ converges to x, we may assume that x_i belongs to $G_s W$ for large i. Thus there is $z_i \in G_s$ and $y_i \in W$ such that $x_i = z_i y_i$ Consequently, we have

$$|F_f(x_i)| = |F_f(z_i y_i)| = |F_f(z_i) + F_f(y_i)| = |F_f(y_i)| < \frac{\varepsilon}{2}.$$

and this imply

$$\left|\int f(y)\, d\nu^{u_i}(y) - \int g(y)\, d\nu^{u_i}(y)\right| \leqslant \varepsilon \quad \text{for large } i$$

Therefore $\mu(f) = \mu(g)$ and hence μ and ν^u are Haar measures on G_u^u and $\mu(h) = 1 = \nu^u(h)$. From uniqueness of Haar measure on G_u^u it follows that $\mu = \nu^u$. This means that $i \mapsto \int f(y)\, d\nu^{u_i}(y)$ converges to $\int f(y)\, d\nu^u(y)$ for every continuous function with compact support f. □

Theorem 14. *Let G be a locally compact groupoid with paracompact unit space and open range map. If G admits a Haar system then*

$$r_s : G_s \to G_s^{(0)}, \quad r_s(x) = r(x)$$

is an open map. And conversely, if the restriction of r to G_s is open at any $x \in G_s$, then there is a pre-Haar system on G that is continuous at any unit in $G_s^{(0)}$.

Proof. It follows from Theorem 13 and Lemma 10. □

Remark 15. If G is a locally compact group bundle, then from the preceding theorem we obtain the result of J. Renault about the existence of Haar systems Lemma 1.3 p.6 [8].

References

[1] **M. Buneci**: *Consequences of Hahn structure theorem for the Haar measure*, Math. Reports **4**(54), 4 (2002), 321 – 334.

[2] **M. Buneci**: *Haar systems and homomorphisms on groupoids*, Operator Algebras and Mathematical Physics: Conference Proceedings Constanţa (Romania), July 2-7, 2001, Theta Foundation (2003), 35 – 50.

[3] **H. Federer and A. Morse**: *Some properties of measurable functions*, Bull. Amer. Math. Soc. **49** (1943), 270 – 277.

[4] **P. Hahn**: *Haar measure for measure groupoids*, Trans. Amer. Math. Soc. **242** (1978), 1 – 33.

[5] **P. Muhly**: *Coordinates in operator algebra*, (Book in preparation).

[6] **A. Ramsay**: *Topologies on measured groupoids*, J. Funct. Anal. **47** (1982), 314 – 343.

[7] **J. Renault**: *A groupoid approach to C^* - algebras*, Lecture Notes in Math. Springer-Verlag, **793**, 1980.

[8] **J. Renault**: *The ideal structure of groupoid crossed product algebras*, J. Operator Theory **25** (1991), 3 – 36.

[9] **A. K. Seda**: *An extension theorem for transformation groupoids*, Proc. Royal Irish Acad. **75**, Sec. A, no. 18, (1975), 255 – 262.

[10] **A. K. Seda**: *A continuity property of Haar systems of measures*, Ann. Soc. Sci. Bruxelles **89** IV (1975), 429 – 433.

[11] **A. K. Seda**: *Haar measures for groupoids*, Proc. Royal Irish Acad. **76**, Sec. A, no. 5, (1976), 25 – 36.

[12] **A. K. Seda**: *On the continuity of Haar measure on topological groupoids*, Proc. Amer. Math. Soc. **96** (1986), 115 – 120.

[13] **J. Westman**: *Nontransitive groupoid algebras*, Univ. of California at Irvine, 1967.

[14] **J. Westman**: *Harmonic analysis on groupoids*, Pacific J. Math. **27** (1968), 621 – 632.

Received September 15, 2003

University Constantin Brâncuşi of Târgu-Jiu
Bulevardul Republicii Nr. 1
210152 Târgu-Jiu , Gorj
Romania
e-mail: ada@utgjiu.ro

Quasigroups and Related Systems **12** (2004), 39 − 60

The structure of extra loops

Michael K. Kinyon and Kenneth Kunen

Abstract

The Sylow theorems hold for finite extra loops, as does P. Hall's theorem for finite solvable extra loops. Every finite nonassociative extra loop Q has a nontrivial center, $Z(Q)$. Furthermore, $Q/Z(Q)$ is a group whenever $|Q| < 512$. Loop extensions are used to construct an infinite nonassociative extra loop with a trivial center and a nonassociative extra loop Q of order 512 such that $Q/Z(Q)$ is nonassociative. There are exactly 16 nonassociative extra loops of order $16p$ for each odd prime p.

1. Introduction

Definition 1.1. A loop Q is an *extra loop* iff Q is both conjugacy closed (a CC-loop) and a Moufang loop.

Lemma 1.2. A loop Q is an extra loop iff Q satisfies one (equivalently all) of the following equations:

1. $(x \cdot yz) \cdot y = xy \cdot zy$.
2. $yz \cdot yx = y \cdot (zy \cdot x)$.
3. $(xy \cdot z) \cdot x = x \cdot (y \cdot zx)$.

Extra loops were first introduced via these equations by Fenyves [11, 12], who proved the equivalence of (1)(2)(3). Goodaire and Robinson [18] showed that Definition 1.1 is equivalent, and this definition is often more useful in practice, since one may combine results in the literature on CC-loops and on Moufang loops to prove theorems about extra loops.

Moufang loops are discussed in standard texts [3, 4, 24] on loop theory. In particular, these loops are diassociative by Moufang's Theorem.

2000 Mathematics Subject Classification:20N05
Keywords:extra loop, Moufang loop, conjugacy closed loop
The second author was partially supported by NSF Grant DMS-0097881

CC-loops were introduced by Goodaire and Robinson [17, 18], and independently (with different terminology) by Сойкис [26]. Further discussion can be found in [9, 10, 20, 21].

If Q is an extra loop and $N = N(Q)$ is the nucleus of Q, then N is a normal subloop of Q and Q/N is a boolean group (see Fenyves [12]). Besides leading to the result of Chein and Robinson that extra loops are exactly those Moufang loops with squares in the nucleus [8], Fenyves's result suggests that one might provide a detailed structure theory for finite extra loops. A start on such a theory was made in [20], where it was shown that if Q is a finite nonassociative extra loop, then $|N|$ is even and $|Q : N| \geqslant 8$, so that $16 \mid |Q|$. The five nonassociative Moufang loops of order 16 are all extra loops (see Chein [5], p. 49). Among these five is the Cayley loop (1845), which is the oldest known example of a nonassociative loop.

The Cayley loop is usually described by starting with the octonion ring ($\mathbb{R}^8$), and restricting the multiplication to $\{\pm e_i : 0 \leqslant i \leqslant 7\}$, where the e_i are the standard basis vectors. Restricting to $\mathbb{R}^8\backslash\{0\}$ or to S^7 does not yield an extra loop (it is Moufang, but not CC). In fact, by Nagy and Strambach ([23], Corollary 2.5, p. 1043), there are no nonassociative connected smooth extra loops. There are also no nonassociative connected compact extra loops, since Q/N is boolean, and hence totally disconnected.

The main results of this paper are listed in the abstract. After we review basic facts about extra loops in §, we characterize the nuclei of nonassociative extra loops in §. The Sylow theorems are proved in §, and P. Hall's theorem is proved in §. The center is discussed in §. In §, we consider loop extensions and describe the two examples mentioned in the abstract. In § we analyze the nonassociative extra loops of order $16p$, for p an odd prime, and show that the number of such loops is independent of p; it follows that this number is 16, since by [16], there are 16 such loops of order 48.

2. Basic facts

We collect some facts from the literature. In particular, we point out that an extra loop yields four boolean groups which help elucidate the loop structure. One is the quotient by the nucleus:

Lemma 2.1. Let Q be an extra loop with nucleus $N = N(Q)$.

1. For each $x \in Q$, $x^2 \in N$.
2. Q/N is a boolean group.

3. Every finite subloop of Q of odd order is contained in N.

4. Every element of Q of finite odd order is contained in N.

The lemma, particularly (1), is due to Fenyves [12]. Considered as a Moufang or CC-loop, an extra loop has a normal nucleus, so (2) follows from (1) and the fact that a Moufang or CC-loop of exponent 2 is a boolean group. (3) follows from (2) (since $Q \to Q/N$ maps the subloop to $\{1\}$), and (4) follows from (3).

Corollary 2.2. Every finite extra loop has the Lagrange property; that is, the order of every subloop divides the order of the loop.

This follows from the fact that Q/N is a group, so that both Q/N and N have the Lagrange property; see Bruck [4], §V.2, Lemma 2.1. This corollary holds for all CC-loops Q, because Basarab [2] has shown that Q/N is an abelian group; see also [20] for an exposition of Basarab's proof, and see [9] for related results.

Another boolean group is generated by the associators:

Definition 2.3. For x, y, z in a loop Q, define the *associator* $(x, y, z) \in Q$ by $(x \cdot yz)(x, y, z) = xy \cdot z$. Let $A(Q)$ be the subloop of Q generated by all the associators.

In an extra loop Q, $A(Q) \leqslant N(Q)$, since $Q/N(Q)$ is a group. Furthermore, by §5 of [20], we have:

Lemma 2.4. In any extra loop Q:

1. (x, y, z) is invariant under all permutations of the set $\{x, y, z\}$.

2. $(x, y, z) = (ux, vy, wz)$ for all $x, y, z \in Q$ and $u, v, w \in N(Q)$.

3. $(x, y, z) = (x^{-1}, y, z)$.

4. (x, y, z) commutes with each of x, y, z.

5. $A(Q) \leqslant Z(N(Q))$ and $A(Q)$ is a boolean group.

Note that Lemma 2.4 shows that the associator (x, y, z) determines a totally symmetric mapping from $(Q/N)^3$ into $A(Q)$.

If $|Q| < 512$, then Theorem 6.6 will show that $A(Q) \leqslant Z(Q)$ (equivalently, $Q/Z(Q)$ is a group); this fails for some Q of order 512; see Example . For any finite nonassociative extra loop, $|Z(Q) \cap A(Q)| \geqslant 2$ (see Theorem 6.1).

The properties we have listed for associators actually characterize extra loops:

Lemma 2.5. Suppose that Q is a loop with the following properties:

1. Q is flexible, that is, $(x, y, x) = 1$ for all $x, y \in Q$.
2. Every associator is in the nucleus.
3. The square of every associator is 1.
4. (x, y, z) is invariant under all permutations of {x,y,z}.
5. (x, y, z) commutes with each of x, y, z.

Then Q is an extra loop.

Proof. $x \cdot [y \cdot zx] = x \cdot yz \cdot x \cdot (y, z, x) = [xy \cdot z](x, y, z)x(y, z, x) = [xy \cdot z] \cdot x$. □

The third boolean group is the right inner mapping group, which turns out in this case to coincide with the left inner mapping group (see 2.7(5) below). We use the following notation.

Definition 2.6. For any loop Q, the *left translations* L_x and *right translations* R_y are defined by: $xy = xR_y = yL_x$. The *right* and *left multiplication groups* are, respectively

$$\mathrm{RMlt} = \mathrm{RMlt}(Q) = \langle R_y : y \in Q \rangle \quad \text{and} \quad \mathrm{LMlt} = \mathrm{LMlt}(Q) = \langle L_x : x \in Q \rangle.$$

For $S \subset Q$, set $R(S) := \{R_x : x \in S\}$. The *right* and *left inner mapping groups* are, respectively,

$$\mathrm{RMlt}_1 = \mathrm{RMlt}_1(Q) = \{g \in \mathrm{RMlt} : 1g = 1\} \text{ and}$$
$$\mathrm{LMlt}_1 = \mathrm{LMlt}_1(Q) = \{g \in \mathrm{LMlt} : 1g = 1\}.$$

Also for $x, y \in Q$, define

$$R(x, y) := R_x R_y R_{xy}^{-1} \qquad \text{and} \qquad L(x, y) := L_x L_y L_{yx}^{-1}.$$

It is easily seen that $R(x, y) \in \mathrm{RMlt}_1$ and that RMlt_1 is the group generated by $\{R(x, y) : x, y \in Q\}$; likewise for the $L(x, y)$ and LMlt_1.

Lemma 2.7. For any extra loop Q:

1. All permutations in RMlt_1 and LMlt_1 are automorphisms of Q.
2. $R(x, y)R(u, v) = R(u, v)R(x, y)$.

3. $L(x, y) = R(x, y) = L(y, x) = R(y, x)$
4. $R(x, y)^2 = I$.
5. $\mathrm{RMlt}_1 = \mathrm{LMlt}_1$ is a boolean group.
6. $zR(x, y) = z(x, y, z)$.

(1) is due to Goodaire and Robinson [17], and (2),(3) are from [20]; these are true for all CC-loops. (4) is also from [20], and (5) is immediate from (2),(3),(4). Also, [20] shows that $zL(y, x) = z(x, y, z)^{-1}$ holds in all CC-loops, so (6) follows, using (3) and Lemma 2.4.

Besides the left and right inner mappings, we have the middle inner mappings $T_x = R_x L_x^{-1}$. In any CC-loop, the group generated by the middle inner mappings coincides with the group generated by all inner mappings [9].

Lemma 2.8. In any extra loop Q with $N = N(Q)$ and $A = A(Q)$:

1. $T_a \in \mathrm{Aut}(Q)$ iff $a \in N(Q)$.
2. For each $x \in Q$, $\mathcal{T}(x) := T_x{\restriction}N \in \mathrm{Aut}(N)$.
3. $\mathcal{T} : Q \to \mathrm{Aut}(N)$ is a homomorphism.
4. Each T_x maps A onto A, so that $A \trianglelefteq Q$ and Q/A is a group.
5. Each $(T_x)^2$ is the identity on A.

(1) is from [9], and holds for all CC-loops. (2) is due to Goodaire and Robinson [17], and (3) is from [21]. Both are true for all CC-loops. $(A)T_x = A$ is due to Fook [13], and is true for all Moufang loops; see also Lemma 6.2 below. Note that by the remark preceding the lemma, to prove that A is normal, it is sufficient to show that $(A)T_x = A$. (5) follows from (3) and (4), since $x^2 \in N$, so T_{x^2} is the identity on A by Lemma 2.4.

Our last boolean group is related to two of the others. In an extra loop Q with $A = A(Q)$, set

$$A^* := \{g \in \mathrm{RMlt} : xg \in Ax,\ \forall x \in Q\}$$

Note that this subgroup of RMlt is the kernel of the natural homomorphism $\mathrm{RMlt}(Q) \to \mathrm{RMlt}(Q/A); g \mapsto (Ax \mapsto Axg)$, and so $A^* \trianglelefteq \mathrm{RMlt}(Q)$.

Lemma 2.9. Let Q be an extra loop. Then $A^* = \mathrm{RMlt}_1(Q) \cdot R(A)$, a direct product. Hence A^* is a boolean group.

Proof. Obviously $R(A) \leqslant A^*$, and conversely, if $R_a \in A^*$, then $a \in A$. By Lemma 2.7(6), $\mathrm{RMlt}_1 \leqslant A^*$. If $g \in A^*$, write $g = hR_a$ for $h \in \mathrm{RMlt}_1$, $a = 1g$. Since $h \in A^*$, $R_a \in A^*$, and so $A^* = \mathrm{RMlt}_1 \cdot R(A)$. Since $A \leqslant N(Q)$ and $\mathrm{RMlt}_1 \leqslant \mathrm{Aut}(Q)$, the product $\mathrm{RMlt}_1 \cdot R(A)$ is direct. Since $A \leqslant N(Q)$, $R(A)$ is a boolean group (an isomorphic copy of A), and so A^* is a boolean group by Lemma 2.7(5). □

3. The nucleus

We describe which groups can be nuclei of nonassociative extra loops.

Proposition 3.1. For a group G, the following are equivalent:

1. $Z(G)$ contains an element of order 2.
2. There is a nonassociative extra loop Q with $G = N(Q)$.
3. There is an extra loop Q with $G = N(Q)$, $|Q : G| = 8$, and $Z(Q) = Z(G)$.

Proof. (2) → (1) is by Lemma 2.4. Now, assume (1) and we shall prove (3). Fix $-1 \in Z(G)$ of order 2, and let $C = \{\pm 1, \pm e_1 \cdots \pm e_7\}$ be the 16-element Cayley loop. In the extra loop $G \times C$, let $M = \{(1,1), (-1,-1)\}$. Note that M is a normal subloop. Let $Q = (G \times C)/M$. □

4. Sylow Theorems

We begin by remarking that for extra loops, two possible definitions of "p-loop" are equivalent. For Moufang loops, the following result is due to Glauberman and Wright [14, 15]. It also holds for power-associative CC-loops, as follows easily from ([20], Coro. 3.2, 3.4).

Lemma 4.1. If Q is a finite extra loop and p is a prime, then the following are equivalent:

1. $|Q|$ is a power of p.
2. The order of every element of Q is a power of p.

Definition 4.2. Let π be a set of primes. A finite loop Q is a *π-loop* if the set of prime factors of $|Q|$ is a subset of π. If $|Q|$ has prime factorization $|Q| = \Pi_p p^{i_p}$, then a *Hall π-subloop* of Q is a subloop of order $\Pi_{p\in\pi} p^{i_p}$. If

$\pi = \{p\}$, than a Hall π-subloop is called a *Sylow p-subloop*. Let $\mathrm{Syl}_p(Q)$ denote the set of all Sylow p-subloops of Q, and let $\mathrm{Hall}_\pi(Q)$ denote the set of all Hall π-subloops of Q.

Of course, in general, Sylow p-subloops and Hall π-subloops need not exist. But for extra loops, Sylow p-subloops do exist and satisfy the familiar Sylow Theorems for groups (Theorem 4.5 below). In §, we will show that Hall π-subloops exist for solvable extra loops and satisfy P. Hall's Theorem for groups (Theorem 5.3). As a preliminary to both theorems:

Lemma 4.3. Let π be a set of primes with $2 \in \pi$, and let Q be a finite extra loop with $A = A(Q)$.

1. If P is a Hall π-subloop of Q, then $A \leqslant P$.
2. If G is a Hall π-subgroup of $\mathrm{RMlt}(Q)$, then $A^* \leqslant G$.

Proof. Since $A \trianglelefteq Q$ and is a boolean group, AP is a subloop of Q of order $|A||P|/|A \cap P|$, and so AP is a π-subloop of Q. By the Lagrange property (Corollary 2.2), Hall π-subloops are maximal π-subloops, and so $AP = P$, establishing (1). The proof for (2) is similar. □

Next we need a minor refinement of the Sylow Theorems for groups. For a finite group G, let $O^p(G)$ denote the subgroup generated by all elements of order prime to p ([1], p. 5). Note that $O^p(G) \trianglelefteq G$.

Lemma 4.4. Assume that G is a finite group, p is prime, and $P, Q \in \mathrm{Syl}_p(G)$. Then $Q = x^{-1}Px$ for some $x \in O^p(G)$.

Proof. If $|G| = p^m j$, where $p \nmid j$, then $|O^p(G)| = p^\ell j$, where $0 \leqslant \ell \leqslant m$. Also $|P \cap O^p(G)| = p^\ell$, since $P \cap O^p(G) \in \mathrm{Syl}_p(O^p(G))$ ([1], (6.4)). Thus $|P \cdot O^p(G)| = |P||O^p(G)|/|P \cap O^p(G)| = p^m j = |G|$, and so $G = P \cdot O^p(G)$. Finally, by the usual Sylow Theorem, let $Q = y^{-1}Py$, where $y = ux$, with $u \in P$ and $x \in O^p(G)$. But then $Q = x^{-1}Px$. □

Theorem 4.5. Suppose that Q is a finite extra loop and $|N(Q)| = p^m r$, where p is prime and $p \nmid r$. Then

1. $|\mathrm{Syl}_p(Q)| = 1 + kp$, where $1 + kp \mid r$.
2. If S is a p-subloop of Q, then there exists $P \in \mathrm{Syl}_p(Q)$ containing S.
3. If $P_1, P_2 \in \mathrm{Syl}_p(Q)$, then there exists $x \in N(Q)$ such that $P_1 T_x = P_2$, so that P_1 and P_2 are isomorphic.

Proof. For $p > 2$: By Lemma 2.1(3), every p-subloop is contained in N, so the Sylow Theorems for groups can be applied to N.

For $p = 2$: The natural homomorphism $[\cdot] : Q \to Q/A; x \mapsto [x]$ yields a map $[\cdot] : P \mapsto P/A$ from the set of 2-subloops P of Q with $A \leqslant P$ to the set of 2-subgroups of Q/A. If $P/A \in \mathrm{Syl}_2(Q/A)$, then $P \in \mathrm{Syl}_2(Q)$, and so by Lemma 4.3, $[\cdot]$ yields a $1-1$ correspondence between $\mathrm{Syl}_2(Q)$ and $\mathrm{Syl}_2(Q/A)$. One can now apply the Sylow Theorems to the group Q/A. To get $x \in N(Q)$ in (3), we apply Lemma 4.4 to Q/A to get $P_1 T_x = P_2$, where $[x] \in O^2(Q/A)$. Now $x = x_1 \cdots x_n$ where the order of each $[x_i]$, say t_i, is odd. Then $x_i = a_i z_i$, where $a_i = x_i^{t_i} \in A$ and $z_i = x_i^{1-t_i} \in N$ since $1 - t_i$ is even. Thus each $x_i \in N$, and so $x \in N$. Finally, that P_1 and P_2 are isomorphic follows from Lemma 2.8(1). □

Next we relate the Sylow p-subloops of an extra loop Q to the Sylow p-subgroups of the right multiplication group $\mathrm{RMlt}(Q)$.

Theorem 4.6. Let Q be an extra loop with $\mathrm{RMlt} = \mathrm{RMlt}(Q)$.

1. If $g \in \mathrm{RMlt}$ has odd order, then $g = R_a$ for some $a \in N(Q)$.
2. $O^2(\mathrm{RMlt}) \leqslant R(N(Q))$.
3. Each subgroup of RMlt of odd order is isomorphic to a subgroup of $N(Q)$.
4. $S \mapsto R(S)$ is a $1-1$ correspondence between the subloops of Q of odd order and the subgroups of RMlt of odd order.

Proof. For $g \in \mathrm{RMlt}$, write (uniquely) $g = hR_a$, where $a = 1g$ and $h \in \mathrm{RMlt}_1$. Note that $hR_a h = R_{ah}$ because $h \in \mathrm{Aut}(Q)$ and $h^2 = I$ (Lemma 2.7(1)(5)). From this plus induction, $g^{2k} = (R_{ah}R_a)^k$ and $g^{2k+1} = hR_a(R_{ah}R_a)^k$ for $k \geqslant 0$. Now, the Moufang identity $R_xR_yR_x = R_{xyx}$ plus induction yields $R_x(R_yR_x)^k = R_{x(yx)^k}$. Thus, $g^{2k+1} = hR_u$, where $u = a \cdot (ah \cdot a)^k$. If $g^{2k+1} = I$ then $h = I$ and $1 = u = a^{2k+1}$, so $a \in N(Q)$ by Lemma 2.1(4). This establishes (1), and the rest follows from (1) and Lemma 2.1(3). □

Theorem 4.7. Let Q be an extra loop. Then $P \mapsto \mathrm{RMlt}_1 \cdot R(P)$ is a $1 - 1$ correspondence between the 2-subloops of Q containing A and the 2-subgroups of $\mathrm{RMlt}(Q)$ containing A^*.

Note that in the theorem, $\mathrm{RMlt}_1 \cdot R(P)$ is not a direct product of subgroups, but is rather a factorization of a group into a subgroup and a subset. The multiplication in this group is given by $hR_a \cdot kR_b = hkR(ak, b)R_{ak \cdot b}$.

Proof. If $A \leqslant P \leqslant Q$, then certainly $A^* \leqslant \mathrm{RMlt}_1 \cdot R(P)$ by Lemma 2.9. Conversely, suppose G is a 2-subgroup of RMlt with $A^* \leqslant G$, and set $P = 1G$, the orbit of G through $1 \in Q$. Each $g \in G$ can be uniquely written as $g = hR_a$ for some $h \in \mathrm{RMlt}_1$, $a = 1g \in P$, and since $\mathrm{RMlt}_1 \leqslant G$, we have $G = \mathrm{RMlt}_1 \cdot R(P)$. $|P|$ is a power of 2, so what remains is to show that P is a subloop. For $a, b \in P$, $R_a R_b = R(a,b)R_{ab}$, and so $ab \in P$ as $R(a,b) \leqslant G$. Similarly, $a \in P$ implies $a^{-1} \in P$, which completes the proof. □

Corollary 4.8. Let Q be a finite extra loop, and let p be a prime. Then $\mathrm{Syl}_p(Q)$ is in a $1-1$ correspondence with $\mathrm{Syl}_p(\mathrm{RMlt}(Q))$.

Proof. If $p > 2$, then Theorem 4.6 yields that $P \mapsto R(P)$ is a $1-1$ correspondence between $\mathrm{Syl}_p(Q)$ and $\mathrm{Syl}_p(\mathrm{RMlt})$.

If $p = 2$, then Theorem 4.7 and Lemma 4.3(2) yield that $P \mapsto \mathrm{RMlt}_1 \cdot R(P)$ is a $1-1$ correspondence between $\mathrm{Syl}_p(Q)$ and $\mathrm{Syl}_p(\mathrm{RMlt})$. □

5. Solvability and Hall π-subloops

Recall that a loop Q is *solvable* if there exists a normal series

$$1 = Q_0 \trianglelefteq Q_1 \trianglelefteq \cdots \trianglelefteq Q_m = Q$$

of subloops Q_i such that each factor Q_{i+1}/Q_i is an abelian group.

Theorem 5.1. An extra loop Q is solvable if and only if $N = N(Q)$ is solvable.

Proof. Since solvability is inherited by subloops, the solvability of Q implies the solvability of N. Conversely, if $1 = N_0 \trianglelefteq \cdots \trianglelefteq N_m = N$ is a normal series for N, then $1 = N_0 \trianglelefteq \cdots \trianglelefteq N_m \trianglelefteq Q$ is a normal series for Q, since Q/N is an abelian group. □

By Proposition 3.1 and the fact that the nucleus of a nonassociative extra loop has index at least 8, the smallest nonsolvable nonassociative extra loop has order 960.

Corollary 5.2. Let Q be an extra loop of order $p^a q^b$, where p, q are primes. Then Q is solvable.

Proof. Since $|N(Q)| = p^c q^d$, the result follows from Burnside's $p^a q^b$-Theorem for groups ([1], (35.13)) and Theorem 5.1. □

This theorem and its corollary actually hold for CC-loops Q because Q/N is an abelian group by Basarab [2] (or see [9, 20]). However, the Sylow theorems and P. Hall's Theorem (cf. [1], (18.5)) can fail in CC-loops, since the 6-element nonassociative CC-loop does not have a subloop of order 2. P. Hall's Theorem for extra loops is:

Theorem 5.3. Let Q be a finite solvable extra loop and π a set of primes. Then

1. Q has a Hall π-subloop.
2. If $P_1, P_2 \in \mathrm{Hall}_\pi(Q)$, then there exists $x \in Q$ such that $P_1 T_x = P_2$.
3. Any π-subloop of Q is contained in some Hall π-subloop of Q.

The proof is similar to that of the Sylow Theorem 4.5.

Proof. For $2 \notin \pi$: If S is any π-subloop of Q, then the natural homomorphism $Q \to Q/N$ takes S onto a π-subloop of a boolean group, so that $S \leqslant N$.

The result then follows from P. Hall's Theorem applied to the solvable group N (Theorem 5.1).

For $2 \in \pi$: The natural homomorphism $[\cdot] : Q \to Q/A$ yields a map $[\cdot] : P \mapsto P/A$ from the set of π-subloops P of Q with $A \leqslant P$ to the set of π-subgroups of Q/A. If $P/A \in \mathrm{Hall}_\pi(Q/A)$, then $P \in \mathrm{Hall}_\pi(Q)$, and so by Lemma 4.3, $[\cdot]$ restricts to a $1-1$ correspondence between $\mathrm{Hall}_\pi(Q)$ and $\mathrm{Hall}_\pi(Q/A)$. Now apply P. Hall's Theorem to the solvable group Q/A. □

6. The center

Theorem 6.1. If Q is a nonassociative extra loop and $A(Q)$ is finite, then $|Z(Q) \cap A(Q)| > 1$.

Proof. Applying Lemma 2.8, define $\mathcal{T}' : Q \to \mathrm{Aut}(A)$ by $\mathcal{T}'(x) = T_x \restriction A$. By Lemma 2.4, $\mathcal{T}'(x) = I$ for $x \in N$. Thus, via $\mathcal{T}'$, the boolean group Q/N acts on the boolean group A. Since $|A|$ is even and the size of each orbit is a power of 2, there must be some $a \in A \backslash \{1\}$ which is fixed by this action. Then $a \in Z(Q)$. □

This can fail when $A(Q)$ is infinite; see Example .

Lemma 6.2. In an extra loop,

$$(x, y, zt) = (x, y, tz) = (x, y, z) \cdot (x, y, t)T_z = (x, y, z)T_t \cdot (x, y, t).$$

Proof. Applying Lemma 2.7, we have $zR(x,y) = z(x,y,z)$, $tR(x,y) = t(x,y,t)$, and $zR(x,y) \cdot tR(x,y) = (zt)R(x,y) = zt \cdot (x,y,zt)$, so

$$z(x,y,z) \cdot t(x,y,t) = zt \cdot (x,y,zt) \quad .$$

Since associators are in the nucleus, we get $(x,y,z)T_t \cdot (x,y,t) = (x,y,zt)$. Also, $(x,y,tz) = (x,y,zt)$ by Lemma 2.4, since Q/N is abelian> Therefore $tz \in Nzt$. $\square$

Since $(x,y,t)T_z = (x,y,z) \cdot (x,y,zt)$, we have, in the case of extra loops, another proof of Fook's result (Lemma 2.8.3) that $(A)T_z = A$. Lemma 6.2 yields:

Lemma 6.3. In an extra loop, z commutes with (x,y,t) iff t commutes with (x,y,z) iff $(x,y,z)(x,y,t) = (x,y,zt)$.

Lemma 6.4. If Q is an extra loop, with $a = (x,y,z)$, then

$$a \in Z(\langle\{x,y,z\} \cup N\rangle), \text{ and } A(\langle\{x,y,z\} \cup N\rangle) = \{1,a\}.$$

Proof. $a \in N$ implies that T_a is an automorphism of Q (Lemma 2.8), so that $\{s \in Q : sa = as\}$ is a subloop of Q, and this subloop contains all elements of $\{x,y,z\} \cup N$ by Lemma 2.4, which also implies that $(u,v,w) \in \{1,a\}$ for all $u,v,w \in \{x,y,z\} \cup N$. Then $A(\langle\{x,y,z\} \cup N\rangle) \subseteq \{1,a\}$ follows by using Lemma 6.2. $\square$

Lemma 6.5. If Q is an extra loop, then $|A(Q) : A(Q) \cap Z(Q)| \notin \{2,4,8\}$.

Proof. Set $Z = A(Q) \cap Z(Q)$, and define $\mathcal{T}' : Q \to \mathrm{Aut}(A)$, as in the proof of Theorem 6.1. Assume that $|A : Z| > 1$. Fix $e_1, e_2, e_3 \in Q$ with $(e_1,e_2,e_3) \notin Z$, and then fix $e_4 \in Q$ such that $(e_1,e_2,e_3)\mathcal{T}'(e_4) \neq (e_1,e_2,e_3)$. Define

$$q_1 := (e_2,e_3,e_4) \quad q_2 := (e_1,e_3,e_4) \quad q_3 := (e_1,e_2,e_4) \quad q_4 := (e_1,e_2,e_3).$$

By Lemmas 6.3 and 2.4, $q_i\mathcal{T}'(e_j) = q_i$ iff $j \neq i$. Now, let $q_S = \prod_{i\in S} q_i$ for $S \subseteq \{1,2,3,4\}$, and observe that $q_S\mathcal{T}'(e_j) = q_S$ iff $j \notin S$, so that the q_S are all in distinct cosets of Z. Thus, $|A : Z| \geqslant 16$. $\square$

Theorem 6.6. If Q is a finite extra loop with some associator not contained in $Z(Q)$, then $|A(Q)| \geqslant 32$ and $|Q : N(Q)| \geqslant 16$, so that $512 \mid |Q|$.

Proof. $|Q : N| \geqslant 16$ follows from Lemma 6.4. $|A(Q) \cap Z(Q)| \geqslant 2$ follows from Theorem 6.1, so $|A(Q)| \geqslant 32$ follows from Lemma 6.5, so $512 \mid |Q|$. $\square$

The "512" is best possible; see Example . The construction there is suggested by the proof of Lemma 6.5. We shall get $A(Q) = N(Q) = \langle q_0, q_1, q_2, q_3, q_4\rangle$, of order 32, $Q/N = \langle [e_1], [e_2], [e_3], [e_4]\rangle$, of order 16, and $Z(Q) = \{1, q_0\}$.

7. Extension

Say we are given an abelian group $(G, +)$ and a boolean group $(B, +)$, and we wish to construct all extra loops Q such that $G \trianglelefteq Q$, $G \leqslant N(Q)$, and $Q/G \cong B$. We may view this as an extension problem; see [7] §II.3, p. 35.

Assuming that we already have Q, let $\pi : Q \to B$ be the natural quotient map. By the Axiom of Choice, we can assume that B is a section; that is, B is a subset of Q and $\pi \restriction B$ is the identity function. Then for $a, b \in B$, we have the loop product $a \cdot b$ from Q and the abelian group sum $a + b \in B$. Since $a \cdot b$ and $a + b$ are in the same left coset of G, there is a function $\psi : B \times B \to G$ with $a \cdot b = (a + b)\psi(a, b)$. We may assume that the identity element of B is the 1 of Q, so that $\psi(1, a) = \psi(a, 1) = 1$. Each $T_a \restriction G \in \mathrm{Aut}(G)$. Also, the map $x \mapsto T_x \restriction G$ is a homomorphism from Q to $\mathrm{Aut}(G)$, and is the identity map on G (since G is abelian), so it defines a homomorphism: $B \to \mathrm{Aut}(G)$. Every element of Q is in some left coset of G, so it can be expressed uniquely in the form au, with $a \in B$ and $u \in G$. Since $G \leqslant N(Q)$, we can compute the product of two elements of this form as $au \cdot bv = ab \cdot uT_b v = (a + b) \cdot \psi(a, b)(uT_b)v$. In particular, for $b \in B$, $b^2 = b \cdot b = (b + b) \cdot \psi(b, b) = \psi(b, b)$.

Turning this around, and converting to additive notation,

Definition 7.1. Suppose we are given:

1. An abelian group $(G, +)$ and a boolean group $(B, +)$.
2. A map $\psi : B \times B \to G$ with $\psi(0, a) = \psi(a, 0) = 0$.
3. A homomorphism, $a \mapsto \tau_a$, from B to $\mathrm{Aut}(G)$.

Then $B \ltimes_\tau^\psi G$ denotes the set $B \times G$ given the product operation:

$$(a, u) \cdot (b, v) = (a + b,\ \psi(a, b) + u\tau_b + v).$$

$B \ltimes_\tau G$ denotes $B \ltimes_\tau^\psi G$ in the case that $\psi(a, b) = 0$ for all a, b.

Then $B \ltimes_\tau G$ is a group, and is the usual semidirect product.

Lemma 7.2. $B \ltimes_\tau^\psi G$ is always a loop with identity element $(0, 0)$. The map $u \mapsto (0, u)$ is an isomorphism from G onto $\{0\} \times G \trianglelefteq B \ltimes_\tau^\psi G$.

Proof. We can solve the equations $(a, u) \cdot (b, v) = (c, w)$ for (b, v) or (a, u):

$$(a, u)\backslash(c, w) = (a + c,\ w - \psi(a, a + c) - u\tau_a\tau_c)$$
$$(c, w)/(b, v) = (b + c,\ w\tau_b - \psi(b + c, b)\tau_b - v\tau_b).$$

Here, we have simplified the expression using the facts that B is boolean and the map $b \mapsto \tau_b$ is a homomorphism. This proves that $B \ltimes_\tau^\psi G$ is a loop. $\{0\} \times G$ is a normal subloop because the map $(a,u) \mapsto a$ is a homomorphism. $\square$

It is fairly easy to calculate, in terms of ψ and τ, what is required for $B \ltimes_\tau^\psi G$ to satisfy various properties, such as the inverse property, the Moufang law, etc. In the case of extra loops, we shall use the conditions of Lemma 2.5 on the associators; some of these conditions can be verified immediately:

Lemma 7.3. Let $Q = B \ltimes_\tau^\psi G$. Then $A(Q) \leqslant \{0\} \times G \leqslant N(Q)$.

Proof. To compute the associators, we solve:

$$[(a,u) \cdot (b,v)(c,w)] \;\cdot\; \big((a,u),(b,v),(c,w)\big) \;=\; (a,u)(b,v) \cdot (c,w).$$

First, we compute both associations:

$$\begin{aligned}
(a,u) \cdot (b,v)(c,w) &= (a,u)(b+c,\ \psi(b,c) + v\tau_c + w) \\
&= (a+b+c,\ \psi(a,b+c) + u\tau_b\tau_c + \psi(b,c) + v\tau_c + w) \\
(a,u)(b,v) \cdot (c,w) &= (a+b,\ \psi(a,b) + u\tau_b + v) \cdot (c,w) \\
&= (a+b+c,\ \psi(a+b,c) + \psi(a,b)\tau_c + u\tau_b\tau_c + v\tau_c + w).
\end{aligned}$$

So,

$$\big((a,u),(b,v),(c,w)\big) \;=\; \big(0,\ \psi(a+b,c) + \psi(a,b)\tau_c - \psi(a,b+c) - \psi(b,c)\big).$$

Observe that this depends only on a,b,c, and has value 0 if any of a,b,c are 0, so that $\{0\} \times G \leqslant N(Q)$, and all $(x,y,z) \in \{0\} \times G$. $\square$

We now consider in more detail the case when both B and G are boolean. We shall in fact start with τ and the desired associator map $\alpha : B^3 \to G$, where $\big(0, \alpha(a,b,c)\big)$ denotes the intended value of $\big((a,u),(b,v),(c,w)\big)$ for some (any) $u,v,w \in G$. We plan to construct ψ from α and τ. This is useful because α is determined by its values on a basis for B. We need to assume some conditions on α suggested by Lemmas 6.2 and 2.4:

Lemma 7.4. Suppose that G and B are boolean groups and E is a basis for B. Let $\tau \in \mathrm{Hom}(B, \mathrm{Aut}(G))$, and assume that $\alpha : E^3 \to G$ satisfies the equations:

H1. $(\alpha(a_1, b, c))\tau_{a_2} + \alpha(a_2, b, c) = \alpha(a_1, b, c) + (\alpha(a_2, b, c))\tau_{a_1}$,

H2. $(\alpha(a, b_1, c))\tau_{b_2} + \alpha(a, b_2, c) = \alpha(a, b_1, c) + (\alpha(a, b_2, c))\tau_{b_1}$,

H3. $(\alpha(a, b, c_1))\tau_{c_2} + \alpha(a, b, c_2) = \alpha(a, b, c_1) + (\alpha(a, b, c_2))\tau_{c_1}$,

F1. $(\alpha(a, b, c))\tau_a = \alpha(a, b, c)$,

F2. $(\alpha(a, b, c))\tau_b = \alpha(a, b, c)$,

F3. $(\alpha(a, b, c))\tau_c = \alpha(a, b, c)$.

Then α extends uniquely to a map $\overline{\alpha} : B^3 \to G$ satisfying these same equations for all elements of B, together with

P1. $\overline{\alpha}(a_1 + a_2, b, c) = (\overline{\alpha}(a_1, b, c))\tau_{a_2} + \overline{\alpha}(a_2, b, c)$,

P2. $\overline{\alpha}(a, b_1 + b_2, c) = (\overline{\alpha}(a, b_1, c))\tau_{b_2} + \overline{\alpha}(a, b_2, c)$,

P3. $\overline{\alpha}(a, b, c_1 + c_2) = (\overline{\alpha}(a, b, c_1))\tau_{c_2} + \overline{\alpha}(a, b, c_2)$.

If α is symmetric, then the same holds for $\overline{\alpha}$. If in addition, α satisfies $\alpha(a, a, b) = 0$ for all $a, b \in E$, then $\overline{\alpha}(a, a, b) = 0$ for all $a, b \in B$.

Proof. First, fix $a, b \in E$, and consider the map $\varphi : E \to B \ltimes_\tau G$ defined by $\varphi(c) = (c, \alpha(a, b, c))$. H3 says that $\varphi(c_1)\varphi(c_2) = \varphi(c_2)\varphi(c_1)$, and F3 says that each $(\varphi(c))^2 = 1$. It follows that φ extends uniquely to a homomorphism $\varphi' : B \to B \ltimes_\tau G$; then $\varphi'(c) = (c, \alpha'(a, b, c))$.

Doing this for every $a, b \in E$, we get $\alpha' : E \times E \times B \to G$, which is the unique extension of α satisfying H3,F3,P3. But then it is easily seen that α' satisfies H1,H2,F1,F2 also. α' is computed inductively using P3; the purpose of φ was just to prove that this computation yields a well-defined function.

Repeating this on the second coordinate yields $\alpha'' : E \times B \times B \to G$, which is the unique extension of α satisfying H2,H3,F2,F3,P2,P3. Doing it again yields $\overline{\alpha}$.

If α is symmetric, then the symmetry of $\overline{\alpha}$ follows from the uniqueness of $\overline{\alpha}$. Finally, assume in addition that $\alpha(a, a, b) = 0$ holds on E. First, for each $e \in E$, note that $\{b \in B : \overline{\alpha}(e, e, b) = 0\}$ is a subgroup of B, so that $\overline{\alpha}(e, e, b) = 0$ for all $b \in B$. Then, for each fixed $b \in B$, $\{a \in B : \overline{\alpha}(a, a, b) = 0\}$ is a also a subgroup, so that $\overline{\alpha}(a, a, b)$ for all $a, b \in B$. $\square$

We now analyze the special case that in $Q = B \ltimes_\tau^\psi G$, the elements of $E \times \{0\}$ all have order 2 and all commute with each other. We can then use α to compute the correct ψ. Observe first:

Lemma 7.5. In an extra loop Q, suppose that the elements $x_1, x_2, \ldots, x_n$ all pairwise commute. Let π be a permutation of the set $\{1, 2, \ldots, n\}$. Then $x_1 \cdot x_2 \cdot \cdots \cdot x_n = x_{\pi(1)} \cdot x_{\pi(2)} \cdot \cdots \cdot x_{\pi(n)}$, where both products are right-associated.

Proof. It is sufficient to prove $x \cdot yz = y \cdot xz$ when $xy = yx$, and this follows by $x \cdot yz = xy \cdot z \cdot (x, y, z) = yx \cdot z \cdot (x, y, z) = y \cdot xz$. □

Thus, if the elements of $E \times \{0\}$ all commute, then the value of a right-associated product from $E \times \{0\}$ must be independent of the order in which that product is taken. This will simplify the form of ψ. If the elements of $E \times \{0\}$ also have order 2 in Q, then it is easy to say what properties α must satisfy:

Theorem 7.6. Suppose that we are given boolean groups G and B, with $E \subset B$ a basis for B. Suppose that we also have $\tau \in \mathrm{Hom}(B, \mathrm{Aut}(G))$ and a map $\alpha : E^3 \to G$ satisfying:

1. α is invariant under permutations of its arguments,
2. $\alpha(e_1, e_1, e_2) = 0$,
3. $(\alpha(e_1, e_2, e_3))\tau_{e_4} + \alpha(e_1, e_2, e_4) = \alpha(e_1, e_2, e_3) + (\alpha(e_1, e_2, e_4))\tau_{e_3}$.

Then there is a unique $\psi : B \times B \to G$ satisfying:

a. $\psi(0, a) = \psi(a, 0) = 0$ for all $a \in B$,

b. $Q := B \ltimes_\tau^\psi G$ is an extra loop,

c. In Q, whenever $e_1, e_2, e_3 \in E$, we have
$$(e_1, 0) \cdot (e_1, 0) = 0, \quad (e_1, 0) \cdot (e_2, 0) = (e_2, 0) \cdot (e_1, 0),$$
and the associator $\big((e_1, 0), (e_2, 0), (e_3, 0)\big) = \big(0, \alpha(e_1, e_2, e_3)\big)$,

d. $\psi(e, b) = 0$ whenever $e \in E$.

Condition (d) expresses the intent that the elements of the section be right-associated products from E.

Proof. Note that (1 – 3) implies that $(\alpha(e_1, e_2, e_3))\tau_{e_1} = \alpha(e_1, e_2, e_3)$.

By Lemma 7.4, α extends uniquely to a symmetric map $\overline{\alpha} : B^3 \to G$ satisfying the conditions Hi, Fi, Pi there. For the uniqueness part of the theorem, we note that assuming that $B \ltimes_\tau^\psi G$ is an extra loop, this $\overline{\alpha}$ must indeed yield the associator; that is, by condition (c) and Lemma 6.2, we have:

$$\big((a,u),(b,v),(c,w)\big) = \big(0, \overline{\alpha}(a,b,c)\big).$$

Then, by the computation in the proof of Lemma 7.3, we get:

$$\overline{\alpha}(a,b,c) = \psi(a+b,c) + \psi(a,b)\tau_c + \psi(a,b+c) + \psi(b,c).$$

Consider the case where $a = e \in E$. Then condition (d) implies that $\psi(e,b) = \psi(e,b+c) = 0$, so we get $\psi(e+b,c) = \psi(b,c)+\overline{\alpha}(e,b,c)$. Repeating this, we see that for $e_1,\ldots,e_n \in E$,

$$\psi(e_1+\cdots+e_n,c) \;=\; \sum_{j=1}^{n} \overline{\alpha}\big(e_j,\ \sum_{k<j} e_k,\ c\big). \tag{$*$}$$

For example,

$$\begin{aligned}
\psi(e_1+e_2,c) &= \overline{\alpha}(e_2,e_1,c)\\
\psi(e_1+e_2+e_3,c) &= \overline{\alpha}(e_2,e_1,c) + \overline{\alpha}(e_3,e_1+e_2,c) =\\
&\qquad \overline{\alpha}(e_2,e_1,c) + (\overline{\alpha}(e_3,e_1,c))\tau_{e_2} + \overline{\alpha}(e_3,e_2,c)
\end{aligned}$$

This proves the uniqueness of ψ. To prove existence, one can take $(*)$ as a definition of ψ (after proving that it is well-defined), and then prove that it yields an extra loop with the correct associators.

To prove that it is well-defined, fix c and define, $\Psi_n = \Psi_n^{(c)} : E^n \to B$ for $n \geqslant 1$ so that

$$\begin{aligned}
\Psi_1(e) &= 0.\\
\Psi_{n+1}(e_0,e_1,\ldots,e_n) &= \Psi_n(e_1,\ldots,e_n) + \overline{\alpha}(e_0,e_1+\cdots+e_n,c).
\end{aligned}$$

It is easy to see that $\Psi_2(e,e) = 0$ and $\Psi_{n+2}(e,e,e_1,\ldots,e_n) = \Psi_n(e_1,\ldots,e_n)$. We need to prove that each Ψ_n is invariant under permutations of its arguments. Then, it will be unambiguous to define $\psi(e_1+\cdots+e_n,c) = \Psi_n^{(c)}(e_1,\ldots,e_n)$. To prove invariance under permutations, we induct on n; for the induction step, it is sufficient to prove that $\Psi_{n+2}(e,e',e_1,\ldots,e_n) = \Psi_{n+2}(e',e,e_1,\ldots,e_n)$, and this follows from the fact that

$$\begin{aligned}
\overline{\alpha}(e,e'+b,c) + \overline{\alpha}(e',b,c) &= (\overline{\alpha}(e,e',c))\tau_b + \overline{\alpha}(e,b,c) + \overline{\alpha}(e',b,c)\\
&= \overline{\alpha}(e',e+b,c) + \overline{\alpha}(e,b,c).
\end{aligned}$$

Now that we have ψ defined, we need to check that our given $\overline{\alpha}(a,b,c)$ is really the true associator. Use $\big(0,(a,b,c)\big)$ to denote $\big((a,u),(b,v),(c,w)\big)$ for some (any) $u,v,w \in G$; then, as in the proof of Lemma 7.3,

$$(a,b,c) = \psi(a+b,c) + \psi(a,b)\tau_c + \psi(a,b+c) + \psi(b,c).$$

We prove $\overline{\alpha}(a,b,c) = (a,b,c)$ by induction on the number of basis elements needed to add up to a. If $a = 0$, then $\overline{\alpha}(a,b,c) = (a,b,c) = 0$. For the induction step, note that $\overline{\alpha}(e+a,b,c) - \overline{\alpha}(a,b,c) = \overline{\alpha}(e,b,c)\tau_a$, which is the same as $(e+a,b,c) - (a,b,c)$, since using $\psi(e+b,c) = \psi(b,c) + \overline{\alpha}(e,b,c)$, we get:

$$(e+a,b,c) - (a,b,c) = \overline{\alpha}(e,a+b,c) + \overline{\alpha}(e,a,b)\tau_c + \overline{\alpha}(e,a,b+c) =$$

$$\overline{\alpha}(e,b,c)\tau_a + \overline{\alpha}(e,a,c) + \overline{\alpha}(e,a,b)\tau_c + \overline{\alpha}(e,a,b)\tau_c + \overline{\alpha}(e,a,c) = \overline{\alpha}(e,b,c)\tau_a\,.$$

Now that we have identified $\overline{\alpha}(a,b,c)$ as the associator, it is easy to prove that Q is an extra loop by verifying the conditions in Lemma 2.5. (2) and (3) are clear from Lemma 7.3. (1) (Q is flexible) holds because $\overline{\alpha}(a,b,a) = 0$, and (4) holds because $\overline{\alpha}$ is symmetric. For (5), we must check that $\big(0,\overline{\alpha}(a,b,c)\big)$ commutes with (a,u), and this follows from the fact that $(\overline{\alpha}(a,b,c))\tau_a = \overline{\alpha}(a,b,c)$. ☐

We now describe three examples.

If $|G| = 2$ and $|B| = 8$ (so $E = \{e_1,e_2,e_3\}$), there is only one non-associative option. $\alpha(e_1,e_2,e_3)$ must be the non-identity element of G, and each τ_x must be I. This extra loop of order 16 is the opposite extreme from the Cayley loop (where the elements outside the nucleus have order 4 and anticommute).

Example 7.7. There is an extra loop Q of order 512 such that $Q/Z(Q)$ is nonassociative.

Proof. Let $E = \{e_1,e_2,e_3,e_4\}$ and $G = \langle q_0,q_1,q_2,q_3,q_4\rangle$, so that $|Q| = 512$. Define τ so that $q_0\tau_{e_k} = q_0$ and $q_j\tau_{e_k} = q_j + \delta_{j,k}q_0$ for $j,k \in \{1,2,3,4\}$; then $Z(Q)$ will be $\{(0,0),(q_0,0)\}$. Define α so that $\alpha(e_i,e_j,e_k) = q_\ell$ whenever $i,j,k,\ell \in \{1,2,3,4\}$ are distinct. ☐

The ψ of this example was first found using McCune's program Mace4 [22], and the abstract discussion of this section was then obtained by reverse engineering.

Example 7.8. There is an infinite nonassociative extra loop Q with $Z(Q) = \{1\}$.

Proof. Let B be any infinite boolean group, and we use a wreath product construction. B acts on $(\mathbb{Z}_2)^B$ by permuting the indices; that is, for $u : B \to \mathbb{Z}_2$, let $((u)\tau_a)(b) = u(a+b)$. Let $G = \{u \in (\mathbb{Z}_2)^B : |u^{-1}\{1\}| < \aleph_0\}$; so G is a direct sum of $|B|$ copies of $\mathbb{Z}_2$ (and is hence isomorphic to B, since $\dim(B) = |B|$). Since B is infinite, $B \ltimes_\tau G$ (and hence also $B \ltimes_\tau^\psi G$) will have trivial center.

Let E be a basis for B. For $e_1, e_2, e_3 \in E$, let $\alpha(e_1, e_2, e_3) = 0$ unless e_1, e_2, e_3 are distinct, in which case $\alpha(e_1, e_2, e_3)$ is the element of $G \leqslant (\mathbb{Z}_2)^B$ which is 1 on the 8 members of $\langle e_1, e_2, e_3\rangle$ and 0 elsewhere. To verify condition (3), we let $u = (\alpha(e_1, e_2, e_3))\tau_{e_4} + \alpha(e_1, e_2, e_4)$ and let $v = \alpha(e_1, e_2, e_3) + (\alpha(e_1, e_2, e_4))\tau_{e_3}$, and consider cases: If $e_1 = e_2$, then $u = v = 0$, so assume that $e_1 \neq e_2$. If $e_3 \in \{e_1, e_2\}$, then $u = v = \alpha(e_1, e_2, e_4)$, and if $e_4 \in \{e_1, e_2\}$, then $u = v = \alpha(e_1, e_2, e_3)$, so assume also that $\{e_3, e_4\} \cap \{e_1, e_2\} = \emptyset$. If $e_3 = e_4$ then $u = v = 0$. In the remaining case, e_1, e_2, e_3, e_4 are all distinct; then both u, v are 1 on the 16 members of $\langle e_1, e_2, e_3, e_4\rangle$ and 0 elsewhere. $\square$

8. Semidirect Products

The loop $B \ltimes_\tau^\psi G$ from Definition 7.1 is not really a semidirect product, since it need not contain an isomorphic copy of B. If we delete the ψ, we get a true semidirect product. Following Robinson [25]:

Definition 8.1. Let B, G be loops, and assume that $\tau \in \mathrm{Hom}(B, \mathrm{Aut}(G))$. Then $B \ltimes_\tau G$ denotes the set $B \times G$ given the product operation:

$$(a, u) \cdot (b, v) = (ab,\ (u)\tau_b \cdot v).$$

We write $B \ltimes G$ when τ is clear from context.

It is easily verified that $B \ltimes G$ is a loop, with identity element $(1, 1)$, but $B \ltimes G$ need not inherit all the properties satisfied by B and G. The general situation for extra loops was discussed in [25]. Here, we consider only an easy special case:

Lemma 8.2. Assume that $\tau \in \mathrm{Hom}(B, \mathrm{Aut}(G))$, B is an extra loop, and G is a group. Then $B \ltimes_\tau G$ is an extra loop, and the inverse is given by $(a, u)^{-1} = (a^{-1}, (u^{-1})\tau_{a^{-1}})$.

Proof. Note that $(a, u) \cdot (a^{-1}, (u^{-1})\tau_{a^{-1}}) = (1, 1)$. We verify the extra loop equation $(xy \cdot z) \cdot x = x \cdot (y \cdot zx)$, setting $x = (a, u)$, $y = (b, v)$, $z = (c, w)$:

$$((a,u)(b,v) \cdot (c,w)) \cdot (a,u) = \big((ab \cdot c) \cdot a,\ (u)\tau_{bca} \cdot (v)\tau_{ca} \cdot (w)\tau_a \cdot u\big)$$
$$(a,u) \cdot ((b,v) \cdot (c,w)(a,u)) = \big(a \cdot (b \cdot ca),\ (u)\tau_{bca} \cdot (v)\tau_{ca} \cdot (w)\tau_a \cdot u\big)$$

These are clearly equal, since B is an extra loop. In writing these equations, we used the facts that G is associative, and that $\mathrm{Aut}(G)$ is associative and τ is a homomorphism, so that the notation τ_{bca} is unambiguous, even though $b \cdot ca$ need not equal $bc \cdot a$. □

Of course, the same reasoning will work for other equations which are weakenings of the associative law; for example, if B is Moufang and G is a group, then $B \ltimes G$ is Moufang.

In some cases, we can prove that every extra loop of a given order is a semidirect product:

Lemma 8.3. Suppose that Q is a finite extra loop and $N = N(Q)$ is abelian. Then Q is isomorphic to $B \ltimes_\tau G$, where $B \in \mathrm{Syl}_2(Q)$, $G = O^2(N)$, $\tau_a = T_a{\restriction}G$, and each $(\tau_a)^2 = I$.

Proof. Say $|Q| = 2^n r$, where r is odd, so $|B| = 2^n$. Then $|N| = 2^m r$ for some $m \leqslant n$, and $|B \cap N| = 2^m$. Since N is abelian, it is an internal direct sum of $B \cap N$ and $G = O^2(N)$, which must have order r. Then $Q = BG$, since $B \cap G = \{1\}$. Furthermore, each T_a maps G to G because $T_a \in \mathrm{Aut}(N)$ and G is a characteristic subgroup of N. Then $Q \cong B \ltimes_\tau G$ follows. Also, $(\tau_a)^2 = \tau_{a^2} = I$ because $a^2 \in N$, which is abelian. □

Lemma 8.4. Suppose that Q is a nonassociative extra loop of order $16p$, where p is an odd prime. Then $N(Q) \cong \mathbb{Z}_2 \times \mathbb{Z}_p$.

Proof. $|Q : N| \geqslant 8$ because any $\langle \{x, y\} \cup N \rangle$ is associative, and $Z(N)$ contains an element of order 2 by Lemma 2.4, so $|N| = 2p$ and N cannot be the dihedral group, so N must be $\mathbb{Z}_2 \times \mathbb{Z}_p$. □

Combining Lemmas 8.3 and 8.4, we see that such Q must be of the form $B \ltimes_\tau \mathbb{Z}_p$, where B is one of the five extra loops of order 16 and each $\tau_a \in \{1, -1\} \leqslant \mathrm{Aut}(\mathbb{Z}_p)$; this is because $(\tau_a)^2 = I$, and the only element of $\mathrm{Aut}(\mathbb{Z}_p)$ of order 2 is the map $u \mapsto -u$. We shall now show that the number of such loops is independent of p. Obviously, $\mathrm{Hom}(B, \{1, -1\})$ does not depend on p, but different homomorphisms can result in isomorphic loops, so we must show that for $\tau, \sigma \in \mathrm{Hom}(B, \{1, -1\})$, the question of whether $B \ltimes_\tau \mathbb{Z}_p \cong B \ltimes_\sigma \mathbb{Z}_p$ does not depend on p:

Lemma 8.5. If B is a finite extra 2-loop and $\tau, \sigma \in \mathrm{Hom}(B, \{1, -1\})$, say $\tau \sim \sigma$ iff there is an $\alpha \in \mathrm{Aut}(B)$ with $\tau = \alpha\sigma$. Let p be an odd prime. Then, identifying $\{1, -1\} \leqslant \mathrm{Aut}(\mathbb{Z}_p)$, $B \ltimes_\tau \mathbb{Z}_p \cong B \ltimes_\sigma \mathbb{Z}_p$ iff $\tau \sim \sigma$.

Proof. If $\tau = \alpha\sigma$, then define $\Phi : B \ltimes_\tau \mathbb{Z}_p \to B \ltimes_\sigma \mathbb{Z}_p$ by $(a, u)\Phi = ((a)\alpha, u)$. To verify that Φ is an isomorphism, use

$$\begin{aligned} ((a,u) \cdot_\tau (b,v))\Phi &= (ab,\ (u)\tau_b + v)\Phi \ = \ ((ab)\alpha,\ (u)\tau_b + v) \\ (a,u)\Phi \cdot_\sigma (b,v)\Phi &= ((a)\alpha, u) \cdot_\sigma ((b)\alpha, v) \ = \ ((a)\alpha \cdot (b)\alpha,\ (u)\sigma_{(b)\alpha} + v), \end{aligned}$$

and these are equal because τ_b (i.e., $(b)\tau$) is the same as $\sigma_{(b)\alpha}$ (i.e., $(b)\alpha\sigma$).

Conversely, suppose we are given an isomorphism $\Phi : B \ltimes_\tau \mathbb{Z}_p \to B \ltimes_\sigma \mathbb{Z}_p$. Then $\Phi(B \times \{0\}) \in \mathrm{Syl}_2(B \ltimes_\sigma \mathbb{Z}_p)$. But also $(B \times \{0\}) \in \mathrm{Syl}_2(B \ltimes_\sigma \mathbb{Z}_p)$, and $\mathrm{Aut}(B \ltimes_\sigma \mathbb{Z}_p)$ acts transitively on the set of Sylow 2-subloops by Theorem 4.5. Thus, composing Φ with an automorphism, we may assume WLOG that $\Phi(B \times \{0\}) = B \times \{0\}$. Also, $\Phi(\{1\} \times \mathbb{Z}_p) = \{1\} \times \mathbb{Z}_p$ because $\{1\} \times \mathbb{Z}_p$ is the only subloop of $B \ltimes_\sigma \mathbb{Z}_p$ isomorphic to $\mathbb{Z}_p$. So, we have $(a, 0)\Phi = ((a)\alpha, 0)$ and $(1, u)\Phi = (1, (u)\beta)$ for some $\alpha \in \mathrm{Aut}(B)$ and $\beta \in \mathrm{Aut}(\mathbb{Z}_p)$. Since $(a, u) = (a, 0) \cdot (1, u)$, we also have $(a, u)\Phi = ((a)\alpha, (u)\beta)$. Furthermore, the map $(c, w) \mapsto (c, (w)\beta^{-1})$ is an automorphism of $B \ltimes_\sigma \mathbb{Z}_p$, since $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ is abelian. Composing Φ with this automorphism, we may assume WLOG that $\beta = I$, so that $(a, u)\Phi = ((a)\alpha, u)$. Then, since Φ is an isomorphism, we have:

$$((ab)\alpha, (u)\tau_b + v) = ((a,u) \cdot_\tau (b,v))\Phi = (a,u)\Phi \cdot_\sigma (b,v)\Phi = ((ab)\alpha, (u)\sigma_{(b)\alpha} + v),$$

so $\tau = \alpha\sigma$. ☐

It follows now that the number of nonassociative extra loops of order $16p$ is independent of p. In the case $p = 3$, that number is already known to be 16, since Goodaire, May, and Raman [16], following the classification of Chein [6], have listed all nonassociative Moufang loops of order less than 64. From Appendix E of [16], we find that 16 of the Moufang loops of order 48 are extra loops.

Theorem 8.6. For each odd prime p, there are exactly 16 nonassociative extra loops of order $16p$.

9. Conclusion

Although this paper has focused on extra loops, many of the lemmas hold more generally for CC-loops. For example, if Q is a CC-loop, then by

Басараб [2], Q/N is an abelian group. Of course, Q/N need not be boolean, but if Q is power-associative, then Q/N has exponent 12. Also, if Q is power-associative, nonassociative, and finite, then $|Q|$ is divisible by either 16 or 27. These results on power-associative CC-loops will appear elsewhere [19].

Acknowledgement. We would like to thank M. Aschbacher for suggesting the proof of Lemma 4.4, which is somewhat shorter than our original proof.

References

[1] **M. Aschbacher**; *Finite Group Theory*, Second edition, Cambridge University Press.

[2] **A. S. Basarab**: *A class of LK-loops*, (Russian), Mat. Issled. **120** (1991),3–7.

[3] **V. D. Belousov**: *Foundations of the theory of quasigroups and loops*, (Russian), Izdat. "Nauka", Moscow, 1967.

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

[5] **O. Chein**: *Moufang loops of small order, I*, Trans. Amer. Math. Soc. **188** (1974), 31 – 51.

[6] **O. Chein**: *Moufang loops of small order*, Mem. Amer. Math. Soc. **13** (1978), no. 197.

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

[8] **O. Chein and D. A. Robinson**: *An "extra" law for characterizing Moufang loops*, Proc. Amer. Math. Soc. **33** (1972), 29 – 32.

[9] **A. Drápal**: *Conjugacy closed loops and their multiplication groups*, J. Algebra **272** (2004), 838 – 850.

[10] **A. Drápal**: *Structural interactions of conjugacy closed loops*, preprint

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

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

[13] **L. Fook**: *The devil and the angel of loops*, Proc. Amer. Math. Soc. **54** (1976), 32 – 34.

[14] **G. Glauberman**: *On loops of odd order. II*, J. Algebra **8** (1968), 393 – 414.

[15] **G. Glauberman and C. R. B. Wright**: *Nilpotence of finite Moufang 2-loops*, J. Algebra **8** (1968), 415 – 417.

[16] **E. G. Goodaire, S. May and M. Raman**: *The Moufang Loops of Order Less Than 64*, Nova Science Publishers, NY, 1999.

[17] **E. G. Goodaire and D. A. Robinson**: *A class of loops which are isomorphic to all loop isotopes*, *Canadian J. Math.* **34** (1982), 662 – 672.

[18] **E. G. Goodaire and D. A. Robinson**: *Some special conjugacy closed loops*, Canadian Math. Bull. **33** (1990), 73 – 78.

[19] **M. K. Kinyon and K. Kunen**: *Power-Associative, Conjugacy Closed Loops*, (*in preparation*).

[20] **M. K. Kinyon, K. Kunen and J. D. Phillips**: *Diassociativity in conjugacy closed loops*, Comm. Algebra **32** (2004), 767 – 786.

[21] **K. Kunen**: *The structure of conjugacy closed loops*, Trans. Amer. Math. Soc. **352** (2000), 2889 – 2911.

[22] **W. W. McCune**: *Mace 4.0 Reference Manual and Guide*, Argonne National Laboratory Technical Memorandum ANL/MCS-TM-264,2003, available at: `http://www.mcs.anl.gov/AR/mace4/`

[23] **P. T. Nagy and K. Strambach**: *Loops as invariant sections in groups, and their geometry*, Canad. J. Math. **46** (1994), 1027 – 1056.

[24] **H. O. Pflugfelder**: *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990.

[25] **D. A. Robinson**: *Holomorphy theory of extra loops*, Publ. Math. Debrecen **18** (1971), 59 – 64 (1972).

[26] **L. R. Soĭkis**: *The special loops*, (Rusian), Questions of the Theory of Quasigroups and Loops, Izdat. Otdel Akad. Nauk Moldav. SSR, Kishinev, 1970, 122 – 131.

Received April 22, 2004

Michael K. Kinyon
Department of Mathematical Sciences
Indiana University South Bend
South Bend, IN 46634 USA
e-mail: mkinyon@iusb.edu
http://mypage.iusb.edu/~mkinyon

Kenneth Kunen
Department of Mathematics
University of Wisconsin
Madison, WI 57306 USA
e-mail: kunen@math.wisc.edu
http://www.math.wisc.edu/~kunen

Quasigroups and Related Systems **12** (2004), 61 – 73

Spurious multiplicative group of GF($\mathrm{p^m}$): a new tool for cryptography

Czesław Kościelny

Abstract

An unconventional approach to cryptography, consisting in application of an algebraic structure, called spurious multiplication group of $GF(p^m)$ and denoted as $SMG(p^m)$, the operation table of which is not, in general, a Latin square, has been presented. This algebraic system is a natural generalization of the multiplicative group of $GF(p^m)$, so, one can operate on elements of these two structures using the same routine or the same hardware. On the basis of $SMG(p^m)$ many strong symmetric-key ciphers, and at least, as it is shown in the paper, one public-key cipher, can be built.

1. Introduction

At the beginning of the silicon era technological applications of semiconductors in the form of pure crystalline germanium or silicon were very limited. The meaningful development of semiconductor electronics has begun only when the trace amounts of dopants, causing defects of the crystal's structure, to the silicon or germanium crystals have been added. It is possible to perceive some analogy between contemporary cryptography and the pre-semiconductor era in electronics: generally in all currently proposed and used cryptographic systems encrypting/decrypting procedures compute cryptograms corresponding to given plaintexts, and vice versa, using pure algebraic structures such as groups, rings and fields. Doubtlessly, applying in cryptographic operations algebraic structures with small "defects" can

2000 Mathematics Subject Classification: 05B15, 20N05, 94B05
Keywords: cryptography, symmetric-key and public-key ciphers, non-associative algebraic structure.

have positive influence on the properties of ciphers, because it makes crypt-analysis more difficult and may not change the complexity of cryptographic algorithms. As it turned out, this guess was correct, thus, one of many possible "defected" algebraic systems, a spurious multiplicative group of $GF(p^m)$ is described in the paper. This system can deliver many strong and useful ciphers.

The present work is mainly addressed to application researches. Then it is assumed that the books [2, 5, 7, 8] are known to the reader, who also ought to have an adequate mathematical knowledge. There would be no harm if the reader is well-informed about the new trends in modern conventional cryptology [1, 6].

2. Definition of $\mathbf{SMG(p^m)}$

For all prime p, for any positive integer $m \geq 2$ and for any polynomial $f(x)$ of degree m over $GF(p)$ there exists an algebraic system denoted as $SMG(p^m)$

$$SMG(p^m) = \langle Gx, \bullet \rangle, \tag{1}$$

consisting of the set Gx of all $p^m - 1$ non-zero polynomials of degree dg over $GF(p)$, $0 \leq dg \leq m-1$, and of an operation of multiplication of these polynomials modulo polynomial $f(x)$. Such an algebraic system is a generalization of the multiplicative group of $GF(p^m)$, therefore, it will be called the spurious multiplicative group of $GF(p^m)$.

The spurious multiplicative group of $GF(p^m)$, more convenient for applications

$$SMG(p^m) = \langle G, \circ \rangle, \tag{2}$$

is obtained using the isomorphic mapping

$$\sigma : Gx \to G, \tag{3}$$

defined by function $\sigma(v(x)) = v(p)$, converting a polynomial $v(x) \in Gx$ to a number from the set $G = \{1, \ldots, p^m - 1\}$. Therefore

$$\forall\, a, b \in G \;\; a \circ b \;\; = \;\; \sigma(\sigma^{-1}(a) \bullet \sigma^{-1}(b) \pmod{f(x)}). \tag{4}$$

Evidently, the inverse mapping σ^{-1} is described by means of the following two-step algorithm:

Step 1:

convert a base 10 number $a \in G$ to base p, namely,

$$a = a_{m-1} \cdots a_1 \, a_0, \; a_i \in \{0, \, 1, \, \dots, \, p-1\},$$

Step 2:

$$\sigma^{-1}(a) = a_0 + a_1 \, x + \cdots + a_{m-1} \, x^{m-1} \in Gx.$$

In principle, $SMG(p^m)$ is a commutative quasigroupoid* in which the operation may not neither be closed, nor be fully associative. The operation in G may be implemented in any programming language or by means of an appropriate hardware. However, it is not a trivial task to construct such software or hardware. It requires, for serious applications, very efficient arithmetic operations in the domain of univariate polynomials over the integers modulo p. Since $SMG(p^m)$ is a natural generalization of the multiplicative group of $GF(p^m)$, the multiplication, rising to a power and inversion in $SMG(p^m)$ can be performed by the same routines or by the same hardware as in the multiplicative group of $GF(p^m)$.

3. Known properties of SMG($\mathbf{p^m}$)

Spurious multiplicative group of p^m-element Galois field is rather a simple algebraic structure, but it has many very interesting properties. From the cryptographic point of view, the most important attribute of $SMG(p^m)$ is the relationship between the number of its reversible elements and a polynomial of degree m over $GF(p)$, defining multiplication of its elements.

The following properties of $SMG(p^m)$ are already known:

P01: The number of $SMG(p^m)$ equals to p^m.

P02: The $p^m - 1$ elements of $SMG(p^m)$ belong to two disjoint sets - a set of reversible elements $SR = \{r_1, \, r_2, \, \dots, \, r_{N_r}\}$ and a set of irreversible elements $SI = \{i_1, \, i_2, \, \dots, \, i_{N_i}\}$, where

$$N_r = |SR|, \; N_i = |SI| \text{ and } N_r + N_i = p^m - 1.$$

* The groupoid is an algebraic structure on a set with a binary operator. The only restriction on the operator is closure. It is assumed here that for the quasigroupoid a closure is not required.

P03: Any reversible element of $SMG(p^m)$ is a generator of cyclic group, being a subgroup of $SMG(p^m)$.

P04: If $f(x)$ is irreducible, $SMG(p^m)$ becomes a multiplicative group of $GF(p^m)$.

P05: In a "truly spurious" $SMG(p^m)$ (when $f(x)$ is not irreducible) the maximum order of reversible elements is, in most cases, less than N_r.

P06: In a "truly spurious" $SMG(p^m)$ the system $\langle SR, \circ \rangle$ in most cases forms non-cyclic abelian group.

P07: In a "truly spurious" $SMG(p^m)$ the operation $\circ$ is not closed, since for some $a,\ b\ \in SMG(p^m)$ the case $a \circ b = 0$ occurs.

P08: The multiplication table of a "truly spurious" $SMG(p^m)$ has the form shown in Table 1,

Table 1: Multiplication table in a "truly spurious" $SMG(p^m)$

$\circ$	$r_1 \quad r_2 \quad \cdots \quad r_{N_r}$	$i_1 \quad i_2 \quad \cdots \quad i_{N_i}$
r_1, r_2, $\vdots$, r_{N_r}	A	B^T
i_1, i_2, $\vdots$, i_{N_i}	B	C

where $A = SR \times SR$, $B = SI \times SR$, $C = SI \times SI$, and only A is a Latin square.

P09: Conjecture: The polynomial $f(x) = x^m$ generates an $SMG(2^m)$ with $N_r = 2^{m-1}$.

P10: Conjecture: If $p > 2$ then the polynomial $f(x) = a\,x^2$, where $a \in \{1, 2, \ldots, p-1\}$, generates $SMG(p^m)$ in which all reversible elements form a cyclic group of order $p^2 - p$.

P11: CONJECTURE: In $SMG(p^m)$ with $p > 2$:

if $m = 2$ then there are only three values of N_r such that

N_r	$N_{f(x)}$
$(p-1)^2$	$p\,(p-1)/2$
$p\,(p-1)$	p
p^2-1	$p\,(p-1)/2$

if $m = 3$ then there are only five values of N_r such that

N_r	$N_{f(x)}$
$(p-1)^3$	$p\,(p-1)(p-2)/6$
$p\,(p-1)^2$	$p\,(p-1)$
$(p+1)\,(p-1)^2$	$p^2\,(p-1)/2$
$p^2\,(p-1)$	p
p^3-1	$p\,(p^2-1)/3$

where $N_{f(x)}$ denotes the number of polynomials generating $SMG(p^m)$ with the number of reversible elements equal to N_r.

All reversible elements of $SMG(p^m)$ behave as usual: any such element $a_r \in SMG(p^m)$ has its proper multiplicative order t_r (t_r is the least positive integer such that $a_r^{t_r} = 1$). As regards irreversible elements $a_i \in SMG(p^m)$, each a_i may be characterized by means of so-called multiplicative quasi order t_i, e. g. the least positive integer such that the set $\{a_i^k,\ k = 1, 2, \ldots, t_i\}$ contains all distinct powers of an element a_i.

Although all properties of $SMG(p^m)$ are not yet known, the existence of such quasigroupoids seems to be important for application in cryptography, therefore, some Maple routines aiding the reader in examining the properties of $SMG(p^m)$ in [4] are presented.

4. Examples of $\mathbf{SMG(p^m)}$

First example concerns $SMG(3^2) = \langle Gx, \bullet \rangle$, generated by means of a polynomial $f(x) = x^2$, where

$$Gx = \{1,\, 2,\, 1+x,\, 2+x,\, 1+2\,x,\, 2+2\,x,\, x,\, 2\,x\}.$$

In the above set of elements of the spurious multiplicative group of order 8 first six elements have their multiplicative inverses, while the last two ones are irreversible.

It is easy to verify that the multiplication table for considered $SMG(3^2)$ in Table 2 is presented.

Table 2: Multiplication table of $SMG(3^2) = \langle Gx, \bullet\rangle$ generated using $f(x) = x^2$

$\bullet$	1	2	$1+x$	$2+x$	$1+2x$	$2+2x$	x	$2x$
1	1	2	$1+x$	$2+x$	$1+2x$	$2+2x$	x	$2x$
2	2	1	$2+2x$	$1+2x$	$2+x$	$1+x$	$2x$	x
$1+x$	$1+x$	$2+2x$	$1+2x$	2	1	$2+x$	x	$2x$
$2+x$	$2+x$	$1+2x$	2	$1+x$	$2+2x$	1	$2x$	x
$1+2x$	$1+2x$	$2+x$	1	$2+2x$	$1+x$	2	x	$2x$
$2+2x$	$2+2x$	$1+x$	$2+x$	1	2	$1+2x$	$2x$	x
x	x	$2x$	x	$2x$	x	$2x$	0	0
$2x$	$2x$	x	$2x$	x	$2x$	x	0	0

Using the mapping (1.3) we obtain $SMG(3^2) = \langle G, \circ\rangle$, where

$$G = \{1,\ 2,\ 4,\ 5,\ 7,\ 8,\ 3,\ 6,\ 7,\ 8\},$$

with the following operation table:

Table 3: Multiplication table in $SMG(3^2) = \langle G, \circ\rangle$ generated using $f(x) = x^2$

$\circ$	1	2	4	5	7	8	3	6
1	1	2	4	5	7	8	3	6
2	2	1	8	7	5	4	6	3
4	4	8	7	2	1	5	3	6
5	5	7	2	4	8	1	6	3
7	7	5	1	8	4	2	3	6
8	8	4	5	1	2	7	6	3
3	3	6	3	6	3	6	0	0
6	6	3	6	3	6	3	0	0

We may notice that operation tables have the form defined by the property **P09**.

In the second example the polynomial $f(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2$ over $GF(2)$ is used to construct $SMG(2^4) = \langle G, \circ \rangle$, where

$$G = \{1, 2, 3, 4, 5, 6, 8, 10, 11, 12, 13, 15, 7, 9, 14\}.$$

Similarly, as in the previous example, we take reversible elements as the first 12 elements of the set G, this way the last 3 elements are irreversible.

Table 4: Multiplication table in $SMG(2^4) = \langle G, \circ \rangle$ generated using $f(x) = x^4 + x^2 + 1$

$\circ$	1	2	3	4	5	6	8	10	11	12	13	15	7	9	14
1	1	2	3	4	5	6	8	10	11	12	13	15	7	9	14
2	2	4	6	8	10	12	5	1	3	13	15	11	14	7	9
3	3	6	5	12	15	10	13	11	8	1	2	4	9	14	7
4	4	8	12	5	1	13	10	2	6	15	11	3	9	14	7
5	5	10	15	1	4	11	2	8	13	3	6	12	14	7	9
6	6	12	10	13	11	1	15	3	5	2	4	8	7	9	14
8	8	5	13	10	2	15	1	4	12	11	3	6	7	9	14
10	10	1	11	2	8	3	4	5	15	6	12	13	9	14	7
11	11	3	8	6	13	5	12	15	4	10	1	2	14	7	9
12	12	13	1	15	3	2	11	6	10	4	8	5	14	7	9
13	13	15	2	11	6	4	3	12	1	8	5	10	9	14	7
15	15	11	4	3	12	8	6	13	2	5	10	1	7	9	14
7	7	14	9	9	14	7	7	9	14	14	9	7	0	0	0
9	9	7	14	14	7	9	9	14	7	7	14	9	0	0	0
14	14	9	7	7	9	14	14	7	9	9	7	14	0	0	0

The multiplication table of the considered $SMG(2^4)$ is presented in Table 4. Using this table we can examine multiplicative orders of all reversible elements and multiplicative quasi-order of any irreversible elements as well. This task is a little laborious, but to make it easier the multiplicative orders of all 12 reversible elements as well as multiplicative quasi-orders of 3 irreversible elements of the examined $SMG(2^4)$, together with the sets of distinct successive powers of any element, have been computed and presented below.

reversible element	multiplicative order	set of distinct successive powers of the element
1	1	{1}
2	6	{1, 2, 4, 5, 8, 10}
3	6	{1, 3, 4, 5, 12, 15}
4	3	{1, 4, 5}
5	3	{1, 4, 5}
6	2	{1, 6}
8	2	{1, 8}
10	6	{1, 2, 4, 5, 8, 10}
11	6	{1, 4, 5, 6, 11, 13}
12	6	{1, 3, 4, 5, 12, 15}
13	6	{1, 4, 5, 6, 11, 13}
15	2	{1, 15}
irreversible element	multiplicative quasi-order	set of distinct successive powers of the element
7	2	{0, 7}
9	2	{0, 9}
14	2	{0, 14}

The next example concerns $SMG(5^2)$ with 16 reversible elements. According to the property **P11** in this case $N_{f(x)} = 10$ and the polynomials $x^2+1,\ x^2+4,\ x^2+x,\ x^2+x+3,\ x^2+2\,x,\ x^2+2\,x+2,\ x^2+3\,x,\ x^2+3\,x+2,\ x^2+4\,x,\ x^2+4\,x+3$ for constructing such spurious multiplicative group of $GF(5^2)$ may be used. Using the polynomial $f(x) = x^2+1$ we obtain the following elements of the interior of the multiplication table:

$$A = \begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 9 & 10 & 12 & 13 & 15 & 17 & 18 & 20 & 21 & 24 \\
2 & 4 & 1 & 3 & 10 & 12 & 13 & 20 & 24 & 21 & 5 & 9 & 6 & 15 & 17 & 18 \\
3 & 1 & 4 & 2 & 15 & 18 & 17 & 5 & 6 & 9 & 20 & 21 & 24 & 10 & 13 & 12 \\
4 & 3 & 2 & 1 & 20 & 24 & 21 & 15 & 18 & 17 & 10 & 13 & 12 & 5 & 9 & 6 \\
5 & 10 & 15 & 20 & 4 & 9 & 24 & 3 & 13 & 18 & 2 & 12 & 17 & 1 & 6 & 21 \\
6 & 12 & 18 & 24 & 9 & 10 & 3 & 13 & 20 & 1 & 17 & 4 & 5 & 21 & 2 & 15 \\
9 & 13 & 17 & 21 & 24 & 3 & 15 & 18 & 1 & 5 & 12 & 20 & 4 & 6 & 10 & 2 \\
10 & 20 & 5 & 15 & 3 & 13 & 18 & 1 & 21 & 6 & 4 & 24 & 9 & 2 & 12 & 17 \\
12 & 24 & 6 & 18 & 13 & 20 & 1 & 21 & 15 & 2 & 9 & 3 & 10 & 17 & 4 & 5 \\
13 & 21 & 9 & 17 & 18 & 1 & 5 & 6 & 2 & 10 & 24 & 15 & 3 & 12 & 20 & 4 \\
15 & 5 & 20 & 10 & 2 & 17 & 12 & 4 & 9 & 24 & 1 & 6 & 21 & 3 & 18 & 13 \\
17 & 9 & 21 & 13 & 12 & 4 & 20 & 24 & 3 & 15 & 6 & 10 & 2 & 18 & 5 & 1 \\
18 & 6 & 24 & 12 & 17 & 5 & 4 & 9 & 10 & 3 & 21 & 2 & 15 & 13 & 1 & 20 \\
20 & 15 & 10 & 5 & 1 & 21 & 6 & 2 & 17 & 12 & 3 & 18 & 13 & 4 & 24 & 9 \\
21 & 17 & 13 & 9 & 6 & 2 & 10 & 12 & 4 & 20 & 18 & 5 & 1 & 24 & 15 & 3 \\
24 & 18 & 12 & 6 & 21 & 15 & 2 & 17 & 5 & 4 & 13 & 1 & 20 & 9 & 3 & 10
\end{bmatrix}$$

$$B = \begin{bmatrix} 7 & 14 & 16 & 23 & 14 & 16 & 7 & 23 & 7 & 14 & 7 & 16 & 23 & 16 & 23 & 14 \\ 8 & 11 & 19 & 22 & 19 & 22 & 11 & 8 & 19 & 22 & 22 & 8 & 11 & 11 & 19 & 8 \\ 11 & 22 & 8 & 19 & 8 & 19 & 22 & 11 & 8 & 19 & 19 & 11 & 22 & 22 & 8 & 11 \\ 14 & 23 & 7 & 16 & 23 & 7 & 14 & 16 & 14 & 23 & 14 & 7 & 16 & 7 & 16 & 23 \\ 16 & 7 & 23 & 14 & 7 & 23 & 16 & 14 & 16 & 7 & 16 & 23 & 14 & 23 & 14 & 7 \\ 19 & 8 & 22 & 11 & 22 & 11 & 8 & 19 & 22 & 11 & 11 & 19 & 8 & 8 & 22 & 19 \\ 22 & 19 & 11 & 8 & 11 & 8 & 19 & 22 & 11 & 8 & 8 & 22 & 19 & 19 & 11 & 22 \\ 23 & 16 & 14 & 7 & 16 & 14 & 23 & 7 & 23 & 16 & 23 & 14 & 7 & 14 & 7 & 16 \end{bmatrix}$$

$$C = \begin{bmatrix} 23 & 0 & 0 & 16 & 14 & 0 & 0 & 7 \\ 0 & 8 & 11 & 0 & 0 & 19 & 22 & 0 \\ 0 & 11 & 22 & 0 & 0 & 8 & 19 & 0 \\ 16 & 0 & 0 & 7 & 23 & 0 & 0 & 14 \\ 14 & 0 & 0 & 23 & 7 & 0 & 0 & 16 \\ 0 & 19 & 8 & 0 & 0 & 22 & 11 & 0 \\ 0 & 22 & 19 & 0 & 0 & 11 & 8 & 0 \\ 7 & 0 & 0 & 14 & 16 & 0 & 0 & 23 \end{bmatrix}$$

If we use the polynomial $f(x) = x^2 + 4\,x + 3$ we get correspondingly:

$$A' = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 7 & 9 & 10 & 13 & 14 & 15 & 16 & 17 & 20 & 21 & 23 \\ 2 & 4 & 1 & 3 & 10 & 14 & 13 & 20 & 21 & 23 & 5 & 7 & 9 & 15 & 17 & 16 \\ 3 & 1 & 4 & 2 & 15 & 16 & 17 & 5 & 9 & 7 & 20 & 23 & 21 & 10 & 13 & 14 \\ 4 & 3 & 2 & 1 & 20 & 23 & 21 & 15 & 17 & 16 & 10 & 14 & 13 & 5 & 9 & 7 \\ 5 & 10 & 15 & 20 & 7 & 17 & 2 & 14 & 4 & 9 & 16 & 21 & 1 & 23 & 3 & 13 \\ 7 & 14 & 16 & 23 & 17 & 1 & 10 & 9 & 20 & 2 & 21 & 3 & 5 & 13 & 15 & 4 \\ 9 & 13 & 17 & 21 & 2 & 10 & 23 & 4 & 16 & 20 & 1 & 5 & 14 & 3 & 7 & 15 \\ 10 & 20 & 5 & 15 & 14 & 9 & 4 & 23 & 3 & 13 & 7 & 17 & 2 & 16 & 1 & 21 \\ 13 & 21 & 9 & 17 & 4 & 20 & 16 & 3 & 7 & 15 & 2 & 10 & 23 & 1 & 14 & 5 \\ 14 & 23 & 7 & 16 & 9 & 2 & 20 & 13 & 15 & 4 & 17 & 1 & 10 & 21 & 5 & 3 \\ 15 & 5 & 20 & 10 & 16 & 21 & 1 & 7 & 2 & 17 & 23 & 13 & 3 & 14 & 4 & 9 \\ 16 & 7 & 23 & 14 & 21 & 3 & 5 & 17 & 10 & 1 & 13 & 4 & 15 & 9 & 20 & 2 \\ 17 & 9 & 21 & 13 & 1 & 5 & 14 & 2 & 23 & 10 & 3 & 15 & 7 & 4 & 16 & 20 \\ 20 & 15 & 10 & 5 & 23 & 13 & 3 & 16 & 1 & 21 & 14 & 9 & 4 & 7 & 2 & 17 \\ 21 & 17 & 13 & 9 & 3 & 15 & 7 & 1 & 14 & 5 & 4 & 20 & 16 & 2 & 23 & 10 \\ 23 & 16 & 14 & 7 & 13 & 4 & 15 & 21 & 5 & 3 & 9 & 2 & 20 & 17 & 10 & 1 \end{bmatrix}$$

$$B' = \begin{bmatrix} 6 & 12 & 18 & 24 & 12 & 24 & 6 & 24 & 12 & 18 & 6 & 12 & 18 & 18 & 24 & 6 \\ 8 & 11 & 19 & 22 & 22 & 8 & 19 & 19 & 8 & 11 & 11 & 19 & 22 & 8 & 11 & 22 \\ 11 & 22 & 8 & 19 & 19 & 11 & 8 & 8 & 11 & 22 & 22 & 8 & 19 & 11 & 22 & 19 \\ 12 & 24 & 6 & 18 & 24 & 18 & 12 & 18 & 24 & 6 & 12 & 24 & 6 & 6 & 18 & 12 \\ 18 & 6 & 24 & 12 & 6 & 12 & 18 & 12 & 6 & 24 & 18 & 6 & 24 & 24 & 12 & 18 \\ 19 & 8 & 22 & 11 & 11 & 19 & 22 & 22 & 19 & 8 & 8 & 22 & 11 & 19 & 8 & 11 \\ 22 & 19 & 11 & 8 & 8 & 22 & 11 & 11 & 22 & 19 & 19 & 11 & 8 & 22 & 19 & 8 \\ 24 & 18 & 12 & 6 & 18 & 6 & 24 & 6 & 18 & 12 & 24 & 18 & 12 & 12 & 6 & 24 \end{bmatrix}$$

$$C' = \begin{bmatrix} 18 & 0 & 0 & 6 & 24 & 0 & 0 & 12 \\ 0 & 11 & 22 & 0 & 0 & 8 & 19 & 0 \\ 0 & 22 & 19 & 0 & 0 & 11 & 8 & 0 \\ 6 & 0 & 0 & 12 & 18 & 0 & 0 & 24 \\ 24 & 0 & 0 & 18 & 12 & 0 & 0 & 6 \\ 0 & 8 & 11 & 0 & 0 & 19 & 22 & 0 \\ 0 & 19 & 8 & 0 & 0 & 22 & 11 & 0 \\ 12 & 0 & 0 & 24 & 6 & 0 & 0 & 18 \end{bmatrix}$$

Finally, Table 5 contains the multiplication table in the multiplicative group of $GF(2^4)$. Comparing it with Table 4 we may notice that $SMG(2^4)$ clumsily imitates the multiplicative group of $GF(2^4)$, since these tables are coincident only in 48 places (about 21,3 %).

Table 5: Multiplication table in $SMG(2^4)$, being the multiplicative group of $GF(2^4)$, generated using $f(x) = x^4 + x^3 + x^2 + x + 1$ (irreducible polynomial)

$\circ$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	4	6	8	10	12	14	15	13	11	9	7	5	3	1
3	3	6	5	12	15	10	9	7	4	1	2	11	8	13	14
4	4	8	12	15	11	7	3	1	5	9	13	14	10	6	2
5	5	10	15	11	14	1	4	9	12	3	6	2	7	8	13
6	6	12	10	7	1	11	13	14	8	2	4	9	15	5	3
7	7	14	9	3	4	13	10	6	1	8	15	5	2	11	12
8	8	15	7	1	9	14	6	2	10	13	5	3	11	12	4
9	9	13	4	5	12	8	1	10	3	7	14	15	6	2	11
10	10	11	1	9	3	2	8	13	7	6	12	4	14	15	5
11	11	9	2	13	6	4	15	5	14	12	7	8	3	1	10
12	12	7	11	14	2	9	5	3	15	4	8	13	1	10	6
13	13	5	8	10	7	15	2	11	6	14	3	1	12	4	9
14	14	3	13	6	8	5	11	12	2	15	1	10	4	9	7
15	15	1	14	2	13	3	12	4	11	5	10	6	9	7	8

The examples presented concern very small $SMG(p^m)$, whereas, in practice, strong cryptographic system are built using $SMG(p^m)$ having, say, 10^{3000} and more elements.

5. SMG($\mathbf{p^m}$)-based public key cryptosystem

On the basis of $SMG(p^m)$ one can construct many strong symmetric-key block ciphers with a really huge key space. The author intend to publish this problem in the next article, presenting now more difficult task of constructing $SMG(p^m)$-based public-key cryptosystem.

Public-key cryptographic algorithms are designed to resist chosen plain text attacks and their security is based both on the difficulty of finding the secret key from the public key and the difficulty of determining the plaintext from the cryptogram. At present, the most common public-key cryptosystem is the RSA algorithm. It is guessed that the security of RSA depends on the problem of factoring large numbers. It has never been mathematically proven that one needs to factor the modulus n to calculate a plaintext knowing a cryptogram and a public key. It is conceivable that an entirely different way to break RSA can be discovered (perhaps this way is already known to some cryptanalysts). Therefore, cryptographers attempt to activate alternative public-key encryption algorithms, e.g. the basic ElGamal encryption scheme. It is well known that the progress in the discrete logarithm problem forces the users of the basic ElGamal public-key cryptosystem, working in a multiplicative group of $GF(p)$, to permanently increase a prime modulus p in order to ensure the desired security. For long-term security, at least 2000-bit moduli should be used at present. Common system-wide parameters need even larger key sizes, since computing the database of discrete logarithms for one particular p will discredit the secrecy of all private keys computed using this value of p. But the task of finding a generator of a multiplicative group of $GF(p)$ is infeasible for an ordinary user if $p > 2^{2000} \approx 0.11510^{603}$. As shown in the sequel, it is possible to overcome this inconvenience by forming an ElGamal public-key cryptosystem which works in a spurious multiplicative group of $GF(p^m)$. In this case an infeasible task of determining a generator of the multiplicative group of $GF(p)$ is eliminated and the use of 10000-bit modulus, and even more, is possible.

A concise description of slightly modified algorithms for ElGamal public-key encryption scheme [3, 4, 5], working in $SMG(p^m)$, is given below.

Key generation: Each entity creates its public key and the corresponding private key. So each entity $\mathcal{A}$ ought to do the following:

- Choose an arbitrary polynomial $f(x)$ of the degree m over $GF(p)$ and construct a spurious multiplicative group of $GF(p^m)$ that is $SMG(p^m)$, consisting of the set $G = \{1, \ldots, p^m - 1\}$ and of the operation of multiplication of elements from this set, which is performed by means of a function **mult**(x, y), $x, y \in G$. The function **pow**(x, k), carrying out the operation of rising any element x from G to a k^{th} power, $p^m - 1 \leq k \leq -p^m + 1$, is also defined.

- Select a random reversible element $\alpha \in SMG(p^m)$, $\alpha \neq 1$.
- Choose a random integer $a \in G$, $2 \leq a \leq p^m - 2$, and compute the element $\beta =$ **pow**(α, a).
- $\mathcal{A}$'s public key is α and β, together with $f(x)$ and the functions **mult** and **pow**, if these last three parameters are not common to all the entities.
- $\mathcal{A}$'s private key is a.

Encryption: Entity $\mathcal{B}$ encrypts a message m for $\mathcal{A}$, which $\mathcal{A}$ decrypts. Thus $\mathcal{B}$ should make the following steps:

- Obtain $\mathcal{A}$'s authentic public key α, β, and $f(x)$ together with the functions **mult** and **pow** if these parameters are not common.
- Represent the message m as a number from the set G.
- Choose a random integer $k \in G$.
- Determine numbers $c_1 =$**pow**(α, k) and $c_2 =$**mult**$(m,$ **pow**$(\beta, k))$.
- send the ciphertext $c = (c_1,\ c_2)$ to $\mathcal{A}$.

Decryption: To find plaintext m from the ciphertext $c = (c_1,\ c_2)$, $\mathcal{A}$ should perform the following operations:

- Use the private key a to compute $g =$ **pow**$(c_1,\ a)$ and then compute $g^{-1} =$ **pow**$(g,\ -1)$.
- Retrieve the plaintext by computing $m =$ **mult**$(g^{-1},\ c_2)$.

If $f(x)$ is irreducible, then ElGamal cryptosystem works in a subgroup of the multiplicative group of $GF(p^m)$. In this case $SMG(p^m)$ becomes a multiplicative group of $GF(p^m)$ and all its elements are reversible. If, in addition, $f(x)$ is primitive, then we can easily compute a set of cryptographic keys for public-key cryptosystem, working in a multiplicative group of $GF(p^m)$ choosing $\alpha = p$ in the second step of a key generation algorithm.

5. Conclusions

A new simple algebraic structure very useful in cryptography, which was named $SMG(p^m)$, being the generalization of the multiplicative group of $GF(p^m)$, has been presented. The structure described, apart from immediate application in cryptography, may be interesting to mathematicians, because all its properties are not known yet. Furthermore, all reversible elements of any $SMG(p^m)$ form an interesting group, which was earlier not noticed.

Acknowledgment

The author wishes to thank A. D. Keedwell for very valuable suggestions.

References

[1] **A. Biryukov**: *Block Ciphers and Stream Ciphers: the State of the Art*, `http://www.esat.kuleuven.ac.be/abiryukov/lecturenotes.pdf`, 2003.

[2] **N. Ferguson, B. Schneier**: *Practical Cryptography*, John Wiley & Sons, 2003.

[3] **C. Kościelny**: *A New Approach to the ElGamal Encryption Scheme*, Int. J. Appl. Math. Comput. Sci. **14** (2004), 101 – 103.

[4] **C. Kościelny**: *User-Friendly ElGamal Public-Key Encryption Scheme*, `http://www.mapleapps.com`, 2003.

[5] **A. J. Menezes, P. C. van Oorschot, S. A. Vanstone**: *Handbook of Applied Cryptography*, CRC Press, 1998.

[6] **B. Preneel et. al.**: *New Trends in Cryptology*, `http://www.stork.eu.org/documents/ENS-D4-1-4.pdf`, 2003.

[7] **B. Schneier**: *Applied Cryptography*, (Second Edition): Protocols, Algorithms, and Cource Code in C, John Wiley & Sons, 1996.

[8] **D. R. Stinson**: *Cryptography – Theory and Practice*, CRC Press, 1995.

Received August 31, 2004

Academy of Management in Legnica
Faculty of Computer Science
ul. Reymonta 21
59-220 Legnica
Poland
e-mail: c.koscielny@wsm.edu.pl

Quasigroups and Related Systems **12** (2004), 79 − 92

Permutation representations of triangle group $\Delta(2,4,5)$

Qaiser Mushtaq and Muhammad S. Saeed

Abstract

Let $G(2,4,Z)$ be a linear-fractional group generated by the transformations $x : z \longmapsto \frac{-1}{2z}$ and $y : z \longmapsto \frac{-1}{2(z+1)}$, satisfying the relations $x^2 = y^4 = 1$. In this paper, corresponding to each θ in F_p we shall determine the coset diagrams $D(\theta,p)$ depicting the actions of $G(2,4,Z)$ on $PL(F_p)$ and find also the values of p for which there exist vertices on the vertical line of symmetry in $D(\theta,p)$. Also, we find conditions for the existence of certain useful fragments of coset diagrams in $D(\theta,p)$.

1. Introduction

The group $G(2,4,Z)$ is defined as a linear-fractional group generated by the transformations $x : z \longmapsto \frac{-1}{2z}$ and $y : z \longmapsto \frac{-1}{2(z+1)}$, satisfying the relations $x^2 = y^4 = 1$. The group $G(2,4,Z)$ can be extended by adjoining an involution $t : z \longmapsto \frac{1}{2z}$ such that $(xt)^2 = (yt)^2 = 1$. We denote the extended group by $G^*(2,4,Z)$.

Let $PL(F_p)$ denote the projective line over the Galois field F_p, where p is a prime. The points of $PL(F_p)$ are the elements of F_p together with the additional point ∞.

The group $G^*(2,4,p)$ has its customary meanings, as the group of all transformations $z \rightarrow \frac{az+b}{cz+d}$ where a,b,c,d are in F_p and $ad - bc \neq 0$.

The homomorphism $\alpha : G^*(2,4,Z) \longrightarrow G^*(2,4,p)$ give rise to an action of $G^*(2,4,Z)$ on $PL(F_p)$. We denote the generators $x\alpha$ and $y\alpha$ of $G^*(2,4,p)$ by $\overline{x}$ and $\overline{y}$ respectively. A homomorphism $\alpha : G^*(2,4,Z) \longrightarrow G^*(2,4,p)$ is called a *non-degenerate homomorphism* if neither x nor y lies in the kernel

2000 Mathematics Subject Classification: 20G40, 20F05, 05C25
Keywords: permutation representation, linear fractional group, triangle group, coset diagram.

of α, so that $\overline{x} = x\alpha$ and $\overline{y} = y\alpha$ are of orders 2 and 4 respectively. As always, two non-degenerate homomorphisms α and β are called *conjugate* if there exists an inner automorphism ρ of $G^*(2,4,p)$ such that $\beta = \alpha\rho$. These conjugacy classes will contain homomorphisms from $G^*(2,4,Z)$ to $G^*(2,4,p)$.

The *triangle groups* $\Delta(l,m,k) =< x,y : x^l = y^m = (xy)^k = 1 >$, where $l,m,k > 1$, are described explicitly in [1, 2, 3, 4]. The triangle groups $\Delta(2,4,k) =< x,y : x^2 = y^4 = (xy)^k = 1 >$ can be obtained as subgroups of S_{q+1} through actions of the group $G(2,4,Z)$ on $PL(F_q)$ where q is a power of a prime p. According to [2], the triangle groups $\Delta(2,4,k)$ are known as infinite groups if and only if $k \geqslant 4$. The group $\Delta(2,4,k)$ is C_2, D_8, and S_4, for $k = 1$, 2, 3, respectively. When $k = 4$, the triangle group $\Delta(2,4,4)$ is Abelian-by-cyclic [6].

2. Coset diagrams

The coset diagrams depict an action of

$$G^*(2,4,Z) =< x,y,t : x^2 = y^4 = t^2 = (xt)^2 = (yt)^2 = 1 >$$

on a finite set (or space).

These coset diagrams may be used to provide diagrammatic interpretations of several aspects of combinatorial group theory, such as the proof of the Ree-Singerman theorem (on the cycle structures of generating-permutations for a transitive group). They can be used also as an equivalent to the Abelianized form of the Reidemeister-Schreier process. The same sort of method is also useful for the construction of infinite families of finite quotients of a given finitely-presented group. Use of coset diagrams to find torsion-free subgroups of certain finitely-presented groups has been instrumental in the construction of small volume hyperbolic 3-orbifolds and other hyperbolic 3-manifolds with interesting properties. They are also applied to the construction of arc-transitive graphs and maximal automorphism groups of Riemann surfaces. Coset diagrams can often be used to prove certain groups are infinite, by joining diagrams together to construct permutation representations (of a given group) of arbitrarily large degree.

The coset diagrams for the action of $G^*(2,4,Z)$ on a finite set (or space) are defined as follows.

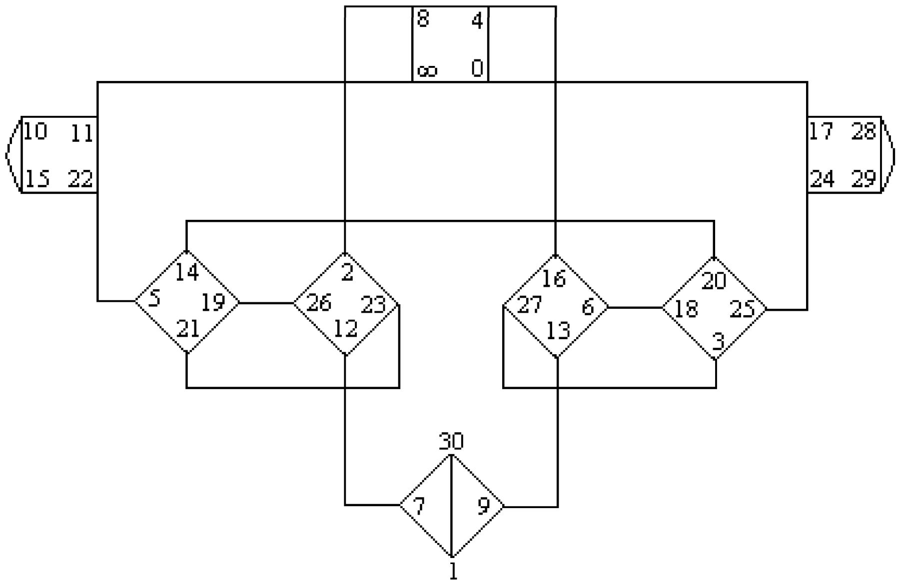
The four cycles of y are represented by small squares whose vertices are permuted counter-clockwise by y. Any two vertices which are interchanged by the involution x, is represented by an edge. The action of t is represented by reflection about a vertical axis of symmetry. The fixed points of x and y, if they exist, are denoted by heavy dots.

For instance, the action of $G^*(2,4,Z)$ on $PL\,(F_{31})$ yields the following permutation representations

$$\overline{x}\ :\ (\infty,11)\,(0,17)\,(1,30)\,(2,8)\,(3,27)\,(4,16)\,(5,22)\,(6,18)\,(7,12)\,(9,13)$$
$$(10,15)(14,20)(19,26)(21,23)(24,25)(28,29)$$

$$\overline{y}\ :\ (0,4,8,\infty)\,(1,9,30,7)\,(2,26,12,23)\,(3,25,20,18)\,(5,21,19,14)$$
$$(6,16,27,13)(10,15,22,11)(17,24,29,28)$$

and the coset diagram depicting this action is:



We shall determine coset diagrams, denoted by $D(\theta,p)$, depicting the actions of $G(2,4,Z)$ on $PL(F_p)$ and find also the values of p for which there exist vertices on the vertical line of symmetry in $D(\theta,p)$. Also, we find conditions for the existence of certain fragments of coset diagrams in $D(\theta,p)$.

The conjugacy classes of non-degenerate homomorphisms α of $G^*(2,4,Z)$ into $G^*(2,4,p)$ correspond in a one-to-one fashion with the conjugacy classes of non-trivial elements of $G^*(2,4,p)$, under a correspondence which assigns to the non-degenerate homomorphism α the class containing the element $(xy)\alpha$. This, of course, means that we can actually parametrize the conjugacy classes of non-degenerate homomorphisms except for a few uninteresting ones, by the elements of F_p. That is, we can in fact parametrize the actions of $G^*(2,4,Z)$ on $PL(F_p)$.

Let X, Y and T denote matrices corresponding to the elements $\overline{x}, \overline{y}$ and $\overline{t}$ in $G^*(2,4,p)$, where as described earlier, $\overline{x} = x\alpha$, $\overline{y} = y\alpha$ and $\overline{t} = t\alpha$, for some non-degenerate homomorphism α from the group $G^*(2,4,Z)$ into $G^*(2,4,p)$. Then X, Y and T will satisfy the relations

$$X^2 = Y^4 = T^2 = (XT)^2 = (YT)^2 = \lambda I$$

for some scalar λ. Since X, Y and T are of orders 2,4, and 2 respectively therefore we can choose

$$X = \begin{bmatrix} a & kc \\ c & -a \end{bmatrix}, \quad Y = \begin{bmatrix} d & kf \\ f & m-d \end{bmatrix} \text{ and } T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix},$$

where $m = trace(Y)$ and $a, c, d, f, k \in F_p$ with $k \neq 0$. Also $m \equiv \theta (mod\, p)$ for some θ in F_p.

To find m, the trace of Y, we adopt the following method. Since $y^4 = 1$, we have $Y^4 = \lambda I$. As in Theorem 3.3.1 in [5], some scalar multiple of Y is conjugate to the matrix $\begin{bmatrix} \rho & 0 \\ 0 & \rho^{-1} \end{bmatrix}$, where ρ is $8th$ root of unity, so that $\rho^8 = 1$ or $(\rho^4 - 1)(\rho^4 + 1) = 0$. But $\rho^4 \neq 1$, therefore $(\rho^4 + 1) = 0$. This implies that $(\rho^2 + \sqrt{2}\rho + 1)(\rho^2 - \sqrt{2}\rho + 1) = 0$. That is,

$$\begin{aligned} (\rho^2 + \sqrt{2}\rho + 1) &= 0 \qquad (2.1) \\ \text{or} \quad (\rho^2 - \sqrt{2}\rho + 1) &= 0 \end{aligned}$$

But $m = \rho + \rho^{-1}$ implies that $m\rho = \rho^2 + 1$, that is, $\rho^2 - m\rho + 1 = 0$. Thus comparing this equation with the characteristic equation of Y, we obtain $m = \pm\sqrt{2}$. Let $m = \sqrt{2}$, so that $trace(Y) = \sqrt{2}$ where Y satisfy the relation $Y^4 = \lambda I$ for some scalar λ.

So $X = \begin{bmatrix} a & kc \\ c & -a \end{bmatrix}$, and $Y = \begin{bmatrix} e & kf \\ f & \sqrt{2}-e \end{bmatrix}$, and the characteristic equations of X, Y and XY are:

$$X^2 + \Delta I = 0, \qquad (2.2)$$

$$Y^2 - \sqrt{2}Y + I = 0, \qquad (2.3)$$

and

$$(XY)^2 - rXY + \Delta I = 0. \qquad (2.4)$$

In the following we see that any element g (not of order 1, 2 or 5) of $G^*(2,4,p)$ is the image of xy under some non-degenerate homomorphism of $G^*(2,4,Z)$ into $G^*(2,4,p)$.

By Lemma 3.2 [5], it is sufficient to show that every element of $G^*(2,4,p)$ is a product of an element of order 2 and an element of order 4. So we shall look for elements $\overline{x},\overline{y},\overline{t}$ of $G^*(2,4,p)$ satisfying the relations

$$\overline{x}^2=\overline{y}^4=\overline{t}^2=(\overline{x}\overline{t})^2=(\overline{y}\overline{t})^2=1 \tag{2.5}$$

with $\overline{x}\,\overline{y}$ in a given conjugacy class.

We shall take $\overline{x}$, $\overline{y}$ and $\overline{t}$ to be represented by

$$X=\begin{bmatrix} a & kc \\ c & -a \end{bmatrix},\quad Y=\begin{bmatrix} d & kf \\ f & m-d \end{bmatrix} \text{ and } T=\begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix},$$

where $a,c,d,f,k \in F_p$.

Since X is non-singular, we shall write

$$a^2+kc^2=-\Delta \tag{2.6}$$

and require that $\det Y=1$ so that

$$d^2-\sqrt{2}d+kf^2+1=0 \tag{2.7}$$

This certainly yields the elements satisfying the relations (2.5). So we only have to check on the conjugacy class of $\overline{x}\,\overline{y}$.

Now the matrix XY is

$$\begin{bmatrix} ad+kfc & akf+\sqrt{2}kc-kcd \\ cd-af & kfc-\sqrt{2}a+ad \end{bmatrix}$$

and therefore the matrix representing $\overline{x}\,\overline{y}$ has the trace

$$r=a(2d-\sqrt{2})+2kfc \tag{2.8}$$

and the determinant $\Delta=-(a^2+kc^2)$, because $\det Y=1$.

The matrix XYT is given by

$$\begin{bmatrix} akf+\sqrt{2}kc-kcd & -akd-k^2fc \\ kfc-\sqrt{2}a+ad & akf-kcd \end{bmatrix}$$

and if $sk=trace(XYT)$ then

$$s=2af+c(\sqrt{2}-2d), \tag{2.9}$$

and so

$$r^2 + ks^2 = 2\Delta\,. \tag{2.10}$$

Thus, corresponding to each θ in F_p, by using equations (2.6) to (2.10), we can find a triplet $(\overline{x}, \overline{y}, \overline{t})$ such that $\overline{x}^2 = \overline{y}^4 = \overline{t}^2 = (\overline{x}\overline{t})^2 = (\overline{y}\overline{t})^2 = 1$. Therefore, we can draw the coset diagram depicting an action of $G^*(2, 4, Z)$ on $PL(F_p)$.

Example 1. If $p = 89$ and $\theta = 11$, then by using equations (2.6) to (2.10), we obtain $\Delta = 1$, $k = -1$, $r = 10$, $s = 3$, $f = 20$, $d = 2$, $a = -13$, $c = -9$ and so

$$x(z) = \frac{-13z + 9}{-9z + 13}\,, \qquad y(z) = \frac{2z - 20}{20z + 23}\,, \qquad t(z) = \frac{1}{z}\,.$$

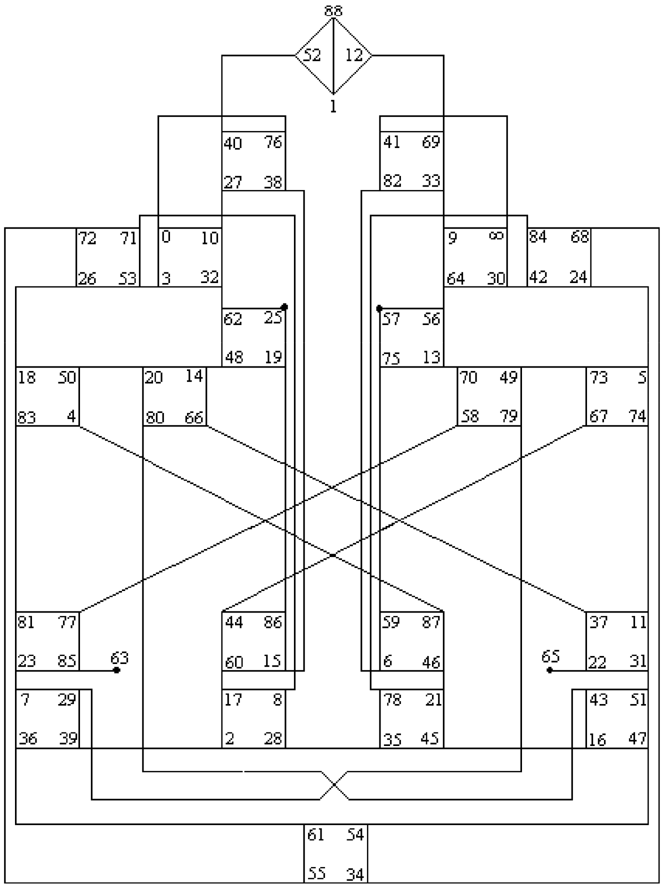
Thus our $\overline{x}, \overline{y}, \overline{t}$ act as

$\overline{x}$: $(\infty, 41)(0, 76)(1, 88)(2, 39)(3, 53)(4, 87)(5, 24)(6, 82)(7, 23)(8, 71)(9, 33)$
$(10, 27)(11, 74)(12, 69)(13, 70)(14, 48)(15, 38)(16, 45)(17, 60)(18, 26)$
$(19, 86)(20, 50)(21, 46)(22, 65)(25)(28, 35)(29, 79)(30, 42)(31, 51)(32, 62)$
$(34, 68)(36, 61)(37, 66)(40, 52)(43, 80)(44, 67)(47, 54)(49, 73)(55, 72)$
$(56, 64)(57)(58, 77)(63, 85)(59, 75)(78, 84)(81, 83)$

$\overline{y}$: $(0, 3, 32, 10)(1, 12, 88, 52)(2, 28, 8, 17)(4, 50, 18, 83)(5, 73, 67, 74)$
$(6, 46, 87, 59)(7, 36, 39, 29)(9, 64, 30, \infty)(11, 37, 22, 31)(13, 56, 57, 75)$
$(14, 20, 80, 66)(15, 86, 44, 60)(16, 47, 51, 43)(19, 25, 62, 48)(21, 78, 35, 45)$
$(23, 85, 77, 81)(24, 68, 84, 42)(26, 53, 71, 72)(27, 38, 76, 40)(33, 69, 41, 82)$
$(34, 54, 61, 55)(49, 70, 58, 79)(63)(65)$

$\overline{t}$: $(0, \infty)(1)(2, 45)(3, 30)(4, 67)(5, 18)(6, 15)(7, 51)(8, 78)(9, 10)(11, 81)$
$(12, 52)(13, 48)(14, 70)(16, 39)(17, 21)(19, 75)(20, 49)(22, 85)(23, 31)$
$(24, 26)(25, 75)(27, 33)(28, 35)(29, 43)(32, 64)(34, 55)(36, 47)(37, 77)$
$(38, 82)(40, 69)(41, 76)(42, 53)(44, 87)(46, 60)(50, 73)(54, 61)(56, 62)$
$(58, 66)(59, 86)(63, 65)(68, 72)(71, 84)(74, 83)(79, 80)(88)$

and yield the coset diagram $D(11, 89)$



D(11,89)

The coset diagrams for the actions of $G^{*}(2,4,Z)$ on $PL\,(F_p)$ contain fixed points of t, which lie on the vertical line of symmetry. Here we have determined the condition under which these fixed vertices exist in $D(\theta,p)$.

Theorem 1. *The transformation $\bar{t}$ has fixed vertices in $D\,(\theta,p)$ if and only if $\theta\,(\theta-2)$ is a square in F_p.*

Proof. First we show that the fixed points of $\overline{x}$ exist in $D\,(\theta,p)$ if $p \equiv 1\,(mod\,4)$ and there do not exist fixed points of $\overline{x}$ if $p \equiv 3\,(mod\,4)$.

Since $\overline{y}$ and $\overline{x}\ \overline{y}$ have even orders, they lie in $G^{*}(2,4,p)$ and hence so does $\overline{x}$. This implies that the permutation $\overline{x}$ is even. Since $r^2 = \Delta\theta$, Δ is a square if and only if θ is. This means that $\overline{x}$ is in $G^{*}(2,4,p)$ if and only if -2 is not a square in F_p and $p \equiv 1\,(mod\,4)$. Thus $\overline{x}$ has fixed vertices in $D\,(\theta,p)$ if and only if -1 and θ are either both squares or both non-squares in F_p. That is, $\overline{x}$ has fixed vertices in $D\,(\theta,p)$ if $p \equiv 1\,(mod\,4)$

and it does not have fixed vertices if $p \equiv 3\,(mod\,4)$. This means that for the non-degenerate homomorphism with parameters θ, $\overline{x}$ is an element of $G^*(2,4,p)$ if and only if $-\theta$ is a square in F_p.

Let δ be the automorphism of $G^*(2,4,p)$ defined by $x\delta = \overline{x}\overline{t}$, $y\delta = \overline{y}$ and $t\delta = \overline{t}$. Then if $\alpha : G^*(2,4,Z) \longrightarrow G^*(2,4,p)$ maps x, y, t to $\overline{x}, \overline{y}, \overline{t}$, the homomorphism $\alpha^{'} = \delta\alpha$ maps x, y, t to $\overline{x}, \overline{y}, \overline{t}$. If we let X, Y and T denote elements of $GL(2,p)$ which yield the elements $\overline{x}$, $\overline{y}$ and $\overline{t}$ in $G^*(2,4,p)$, then obviously X, Y and T can be taken as follows

$$X = \begin{bmatrix} a & kc \\ c & -a \end{bmatrix}, \quad Y = \begin{bmatrix} d & kf \\ f & \sqrt{2} - d \end{bmatrix} \quad \text{and} \quad T = \begin{bmatrix} 0 & -k \\ 1 & 0 \end{bmatrix}$$

where $k \neq 0$ and $a, c, d, k, f \in F_p$ such that they satisfy the equations (2.6) to (2.10). We recall that, $\overline{x}\,\overline{y}$ will be of order 2 if and only if $tr\,(XY) = r = 0$ and similarly $\overline{x}\ \overline{y}\overline{t}$ will be of order 2 if and only if $tr\,(XYT) = ks = 0$. Since the determinant of XY is Δ, therefore the parameter of $\overline{x}\,\overline{y}$ is r^2/Δ, which we have denoted by θ. Also ks is the trace of XYT and $k\Delta$ is its determinant. If we let $\varphi = \frac{ks^2}{\Delta}$ we get $\theta + \varphi = r^2 + ks^2/\Delta$. Substituting the values of r and s from the equations (2.8) and (2.9), in $\theta + \varphi = r^2 + ks^2/\,\Delta$ and then making the substitution of the equation (2.7) and $\Delta = -(a^2 + kc^2)$ we obtain $\theta + \varphi = 2$. That is if θ is the parameter of α then $2 - \theta$ is the parameter of α'.

Since change from α to α' interchanges both $\overline{x}$ and $\overline{x}\overline{t}$ and θ and $2 - \theta$, it follows that $\overline{x}\overline{t}$ maps to an element of $G^*(2,4,p)$ if and only if $\theta\,(2 - \theta)$ is a square in F_p. Since $\overline{t}$ is in $G^*(2,4,p)$ if both of $\overline{x}$ and $\overline{x}\overline{t}$ is, but not if just one of them is, $\overline{t}$ is in $G^*(2,4,p)$ if and only if $\theta\,(2-\theta)$ is a square in F_p. Now $\overline{t}$ has fixed points in $PL\,(F_p)$ if either $\overline{t}$ belongs to $G^*(2,4,p)$ and $p \equiv -1\,(mod\,4)$ or $\overline{t}$ dose not belong to $G^*(2,4,p)$ and $p = 1\,(mod\,4)$ is equivalent to saying that -1 is a square in F_p, we conclude that $\overline{t}$ has fixed vertices in $D\,(\theta, p)$ if and only if $-\theta\,(2-\theta) = \theta\,(\theta - 2)$ is a square in F_p. Hence the result. □

We can see in Example 1 that the coset diagram depicting actions of $G(2,4,Z)$ on $PL\,(F_{89})$ contain fixed points of $\overline{t}$ on the line of symmetry.

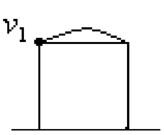
The fact that $\overline{t}$ has fixed vertices on the line of symmetry in $D(\theta, p)$ or not helps us to determine the structure of the group $< \overline{x}, \overline{y}, \overline{t} >$. It also enables us to show that for infinitely many values of p, the group $G^*(2,4,p)$ has minimal genus.

Corollary 1. *If* $p \equiv \pm 1\,(mod\,5)$ *then the transformation* $\overline{t}$ *has fixed vertices in* $D\,(\theta, p)$ *if and only if* $\theta - 2$ *is a square in* F_p *and* $(\overline{x}\ \overline{y})^5 = 1$.

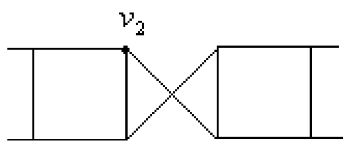
3. Fragments of coset diagrams

By joining graphs representing groups of smaller degree we can obtain a bigger graph representing a group of larger degree. Then it is easy to study the properties of the new group just by studying its graph. We have different methods of joining graphs together, to give representations of the group of larger degree. We need not have to study the entire group of a smaller degree, we can achieve this just by studying its fragment and find a condition for the existence of the fragment in the coset diagram, so that if the fragment exists in a coset diagram of larger degree, we can study the properties of the diagram for the related group of larger degree.

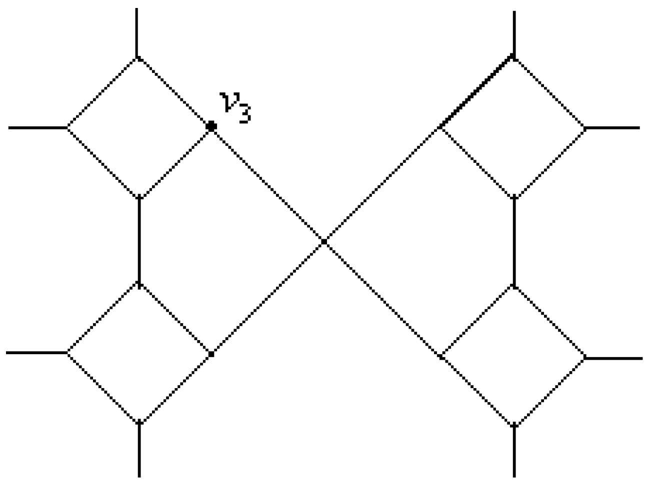
The coset diagrams, depicting actions of $G^*(2,4,p)$ on $PL(F_p)$, frequently contain some special fragments, namely γ_1, γ_2 and γ_3 respectively



γ_1



γ_2



γ_3

We determine conditions on θ and p for the existence of these fragments in the coset diagrams $D(\theta,p)$.

Theorem 2.

(i) *The fragment* γ_1 *will occur in* $D(\theta, p)$ *if* 5 *is a square in* F_p.

(ii) *The fragment* γ_2 *will occur in* $D(\theta, p)$ *if* -11 *is a square in* F_p.

(iii) *The fragment* γ_3 *will occur in* $D(\theta, p)$ *if* -19 *is a square in* F_p.

Proof. The vertices v_1, v_2 and v_3 are fixed by the elements $\overline{x}\;\overline{y}$, $\overline{x}\;\overline{y}^3$ and $\overline{x}\;\overline{y}^3\overline{xy}^3\overline{xyxy}$ respectively. Recall that $\det X = \Delta$, $trace(Y) = \sqrt{2}$, $\det(XY) = \Delta$, and $trace(XY) = r$. After suitable manipulations, the equations

$$Y^3 = Y - \sqrt{2}I \tag{3.1}$$

$$Y^4 = -I \tag{3.2}$$

$$XYX = rX + \Delta Y - \sqrt{2}\Delta I \tag{3.3}$$

can be obtained from the equations (2.2), (2.3) and (2.4).

In fragment γ_1 the vertex v_1 is fixed by $\overline{x}\;\overline{y}$. The matrix corresponding to $\overline{x}\;\overline{y}$ will be $M_1 = XY$. The determinant of M_1 will be $\det(XY) = \det(X)\det(Y) = \Delta$, and the trace of M_1 will be equal to $trace(XY) = r$. So the discriminant of the characteristic equation of M_1 will be $r^2 - 4\Delta$. But $r^2 = \theta\Delta$. This means that the discriminant is, in fact, $r^2 - 4\Delta = \theta\Delta - 4\Delta = (\theta - 4)\Delta$. Since Δ is a square if and only if θ is, we can eliminate Δ, as we are in field F_p. So the discriminant of the characteristic equation of the matrix corresponding to the element $\overline{x}\;\overline{y}$ of $G^*(2, 4, p)$ will be $d_1(\theta) = \theta - 4$.

In fragment γ_2 the vertex v_2 is fixed by $\overline{x}\;\overline{y}^3\overline{x}\;\overline{y}$. The matrix corresponding to $\overline{x}\;\overline{y}^3\overline{x}\;\overline{y}$ will be $M_2 = XY^3XY$. Now $\det M_2 = \Delta^2$. If we substitute the value of Y^3 from equation (3.1) in equation $M_2 = XY^3XY$, we get $M_2 = X(Y - \sqrt{2}I)XY = (XY)^2 - \sqrt{2}X^2\dot{Y}$. If we now substitute values of $(XY)^2$ and X^2 (from equations (2.4) and (2.2)) in equation $M_2 = (XY)^2 - \sqrt{2}X^2Y$ the result will be an equation $M_2 = rXY - \Delta I + \sqrt{2}\Delta M$. So the trace of M_2 will be $trace(rXY) - trace(\Delta I) + \sqrt{2}\,trace(\Delta Y)$. That is, $trace(M_2) = r^2 - 2\Delta + 2\Delta = r^2$. This implies that the discriminant of the characteristic equation of M_2 will be $r^4 - 4\Delta^2$. But $r^2 = \theta\Delta$. This means that the discriminant is, in fact, $\theta^2\Delta^2 - 4\Delta^2 = (\theta^2 - 4)\Delta^2$. Since Δ is a square if and only if θ is, we can eliminate Δ so the discriminant of the characteristic equation of the matrix corresponding to the element $\overline{x}\;\overline{y}^3\overline{x}\;\overline{y}$ of $G^*(2, 4, p)$ will be $d_2(\theta) = \theta^2 - 4 = (\theta - 2)(\theta + 2)$.

In fragment γ_3 the vertex v_3 is fixed by $\overline{x}\;\overline{y}^3\overline{x}\;\overline{y}^3\overline{x}\;\overline{y}\;\overline{x}\;\overline{y}$. The matrix corresponding to $\overline{x}\;\overline{y}^3\overline{x}\;\overline{y}^3\overline{x}\;\overline{y}\;\overline{x}\;\overline{y}$ will be $M_3 = XY^3XY^3XYXY$. So $\det M_3 = \Delta^4$. If we substitute the value of Y^3 from equation (3.1) in equation $M_3 = XY^3XY^3XYXY$, we get

$$\begin{aligned} M_3 &= X(Y-\sqrt{2}I)X(Y-\sqrt{2}I)(XY)^2 \\ &= (XY-\sqrt{2}X)(XY-\sqrt{2}X)(XY)^2 \\ &= [(XY)^2+2X^2-\sqrt{2}XYX-\sqrt{2}X^2Y](XY)^2. \end{aligned} \tag{3.4}$$

If we now substitute values of $(XY)^2$, X^2 and XYX (from equations (2.4), (2.2) and (3.3)) in equation (3.4) the result will be an equation

$$M_3 = r^3XY - r^2\Delta I - 2r\Delta XY + \Delta^2 I + \sqrt{2}r^2\Delta Y + \sqrt{2}rX. \tag{3.5}$$

So the trace of M_3 will be $r^4 - 2r^2\Delta - 2r^2\Delta + 2\Delta^2 + 2r^2\Delta$. That is, $trace(M_3) = r^4 - 2r^2\Delta + 2\Delta^2$. This implies that the discriminant of the characteristic equation of M_3 will be

$$(r^4 - 2r^2\Delta + 2\Delta^2)^2 - 4\Delta^4 = r^8 + 8r^4\Delta^2 - 4r^6\Delta - 8r^2\Delta^3.$$

This means that the discriminant is, in fact,

$$\theta^4\Delta^4 + 8\theta^2\Delta^4 - 4\theta^3\Delta^4 - 8\theta\Delta^4 = (\theta^4 + 8\theta^2 - 4\theta^3 - 8\theta)\Delta^4.$$

Since Δ is a square if and only if θ is, we can eliminate Δ, so the discriminant of the characteristic equation of the matrix corresponding to $\overline{x}\ \overline{y}^3\overline{x}\ \overline{y}^3\overline{x}\ \overline{y}\ \overline{x}\ \overline{y}$ of $G^*(2,4,p)$ will be

$$d_3(\theta) = \theta^4 - 4\theta^3 + 8\theta^2 - 8\theta = \theta(\theta-2)[\theta-(1+\sqrt{-3})][(\theta-(1-\sqrt{-3})]$$

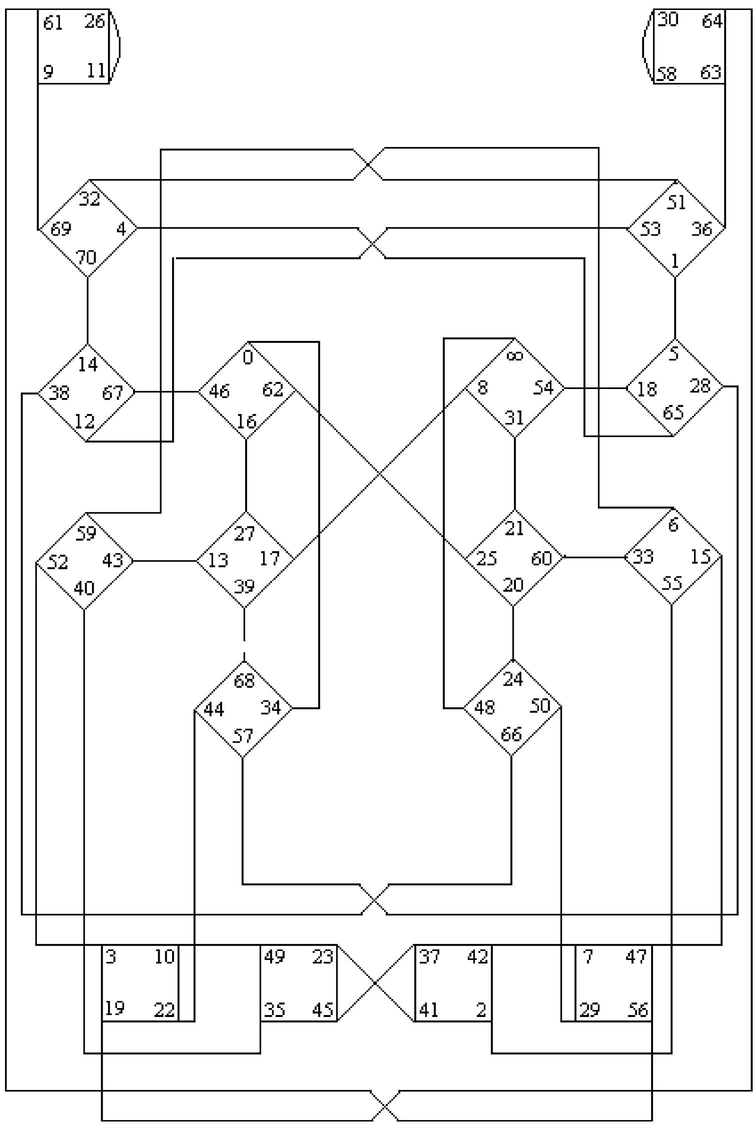
Thus,

(i) the fragment γ_1 will occur in $D(\theta,p)$ if and only if $d_1(\theta) = \theta - 4$ is a square in F_p. If θ_1 and θ_2 are the roots of $f(z) = z^2 - 3z + 1$ then $\prod_{i=1}^{2} d_1(\theta_i) = f(4) = 5$. Thus γ_1 will exist in some $D(\theta_i,p)$ if 5 is a square in F_p.

(ii) the fragment γ_2 will occur in $D(\theta,p)$ if and only if $d_2(\theta) = (\theta-2)(\theta+2)$ is a square in F_p. If θ_1 and θ_2 are the roots of $f(z) = z^2-3z+1$ then $\prod_{i=1}^{2} d_2(\theta_i) = f(2)f(-2) = -11$. Thus γ_2 will exist in some $D(\theta_i,p)$ if -11 is a square in F_p.

(iii) the fragment γ_3 will occur in $D(\theta,p)$ if and only if $d_3(\theta) = \theta(\theta-2)(\theta-(1+\sqrt{-3}))((\theta-(1-\sqrt{-3}))$ is a square in F_p. If θ_1 and θ_2 are the roots of $f(z) = z^2 - 3z + 1$ then $\prod_{i=1}^{2} d_3(\theta_i) = f(0)f(2)f(1+\sqrt{-3})$ $f(1-\sqrt{-3}) = -19$. Thus γ_3 will occur in some $D(\theta_i,p)$ if -19 is a square in F_p. Hence the result. $\square$

Example 2. In the coset diagram given below, we can see that all the three fragments are present.



D(64,71)

In the following we give a hand-calculated list summarizing the situation for all primes $p \leqslant 241$. We let p denote the primes congruent to ± 1 or $\pm 9(mod\, 40)$ and θ is a root of the polynomial $\theta^2 - 3\theta + 1$.

p	θ	$\overline{x}$	$\overline{y}$	$\bar{t}$
31	14	$z \longrightarrow \dfrac{z+2}{z-1}$	$z \longrightarrow \dfrac{-z+6}{3z+5}$	$z \longrightarrow \dfrac{-2}{z}$
	20	$z \longrightarrow \dfrac{2z-3}{3z-2}$	$z \longrightarrow \dfrac{1}{-z+8}$	$z \longrightarrow \dfrac{1}{z}$
41	8	$z \longrightarrow \dfrac{3z-7}{16z-3}$	$z \longrightarrow \dfrac{-z-18}{6z+25}$	$z \longrightarrow \dfrac{3}{z}$
	36	$z \longrightarrow \dfrac{4z+21}{7z-4}$	$z \longrightarrow \dfrac{z-5}{12z+13}$	$z \longrightarrow \dfrac{-3}{z}$
71	10	$z \longrightarrow \dfrac{7z-10}{5z-7}$	$z \longrightarrow \dfrac{-2}{z+2}$	$z \longrightarrow \dfrac{2}{z}$
	64	$z \longrightarrow \dfrac{13z-16}{-16z-13}$	$z \longrightarrow \dfrac{z+9}{9z+11}$	$z \longrightarrow \dfrac{-1}{z}$
79	51	$z \longrightarrow \dfrac{-1}{z}$	$z \longrightarrow \dfrac{z-25}{25z+8}$	$z \longrightarrow \dfrac{1}{z}$
	31	$z \longrightarrow \dfrac{23z-21}{29z-23}$	$z \longrightarrow \dfrac{2z+42}{21z+7}$	$z \longrightarrow \dfrac{-2}{z}$
89	11	$z \longrightarrow \dfrac{-13z+9}{-9z+13}$	$z \longrightarrow \dfrac{2z-20}{20z+23}$	$z \longrightarrow \dfrac{1}{z}$
	81	$z \longrightarrow \dfrac{20z-34}{-17z-20}$	$z \longrightarrow \dfrac{8}{4z+5}$	$z \longrightarrow \dfrac{-2}{z}$
151	29	$z \longrightarrow \dfrac{-29z+67}{28z+29}$	$z \longrightarrow \dfrac{z+64}{29z+45}$	$z \longrightarrow \dfrac{3}{z}$
	125	$z \longrightarrow \dfrac{4z-35}{35z-4}$	$z \longrightarrow \dfrac{z-4}{4z+22}$	$z \longrightarrow \dfrac{1}{z}$
191	90	$z \longrightarrow \dfrac{-60z+4}{65z+60}$	$z \longrightarrow \dfrac{3z+30}{10z+54}$	$z \longrightarrow \dfrac{-3}{z}$
	104	$z \longrightarrow \dfrac{-31z-46}{46z+31}$	$z \longrightarrow \dfrac{-z-21}{21z+58}$	$z \longrightarrow \dfrac{1}{z}$
199	63	$z \longrightarrow \dfrac{41z-45}{-45z-41}$	$z \longrightarrow \dfrac{z+60}{60z+19}$	$z \longrightarrow \dfrac{-1}{z}$
	139	$z \longrightarrow \dfrac{-41z+63}{-63z+41}$	$z \longrightarrow \dfrac{-2z-29}{29z+22}$	$z \longrightarrow \dfrac{1}{z}$
239	17	$z \longrightarrow \dfrac{-21z+43}{-43z+21}$	$z \longrightarrow \dfrac{z-57}{57z+98}$	$z \longrightarrow \dfrac{1}{z}$
	225	$z \longrightarrow \dfrac{-38z+25}{25z+38}$	$z \longrightarrow \dfrac{z-57}{57z+98}$	$z \longrightarrow \dfrac{-1}{z}$
241	53	$z \longrightarrow \dfrac{33z+119}{119z-33}$	$z \longrightarrow \dfrac{32}{32z+11}$	$z \longrightarrow \dfrac{-1}{z}$
	191	$z \longrightarrow \dfrac{97z-101}{101z-97}$	$z \longrightarrow \dfrac{32}{32z+11}$	$z \longrightarrow \dfrac{-1}{z}$

References

[1] **G. Baumslag, J. W. Morgan, and P. B. Shalen**: *Generalized triangle groups*, Math. Proc. Camb. Phil. Soc. **102** (1987), 25 – 31.

[2] **H. S. M. Coxeter and W. O. J Moser**: *Generators and relations for discrete groups*, Springer-verlag, Berlin 1980.

[3] **J. Howie, V. Metaftsis and R. M. Thomas**: *Finite generalized triangle groups*, Trans. Amer. Math. Soc. **347** (1995), 3613 – 3623.

[4] **L. Levai, G. Rosenberger and B. Souvignier**: *All finite generalized triangle groups*, Trans. Amer. Math. Soc. **347** (1995), 3625 – 3627.

[5] **Q. Mushtaq**: *Parametrization of all homomorphisms from* $PGL(2, Z)$ *into* $PSL(2, q)$, Comm. Algebra **20** (1992), 1023 – 1040.

[6] **Q. Mushtaq and F. Shaheen**: *Finite presentation of alternating groups*, Acta Math. Sinica, New Ser. **11** (1995), 221 – 224.

Department of Mathematics
Quaid-i-Azam University
Islamabad
Pakistan
e-mail: qmushtaq@apollo.net.pk

Received March 29, 2003

Quasigroups and Related Systems **12** (2004), 93 – 102

Quotient hyper BCK-algebras

Arsham Borumand Saeid and Mohammad M. Zahedi

Abstract

In this note first we use the equivalence relation $\sim_I$ which has been introduced in [1] and construct a quotient hyper BCK-algebra H/I from a hyper BCK-algebra H via a reflexive hyper BCK-ideal I of H. Then we study the properties of this algebra, in particular we give some examples of this algebra. Finally we obtain some relationships between H/I and H.

1. Introduction

The hyperalgebraic structure theory was introduced by F. Marty [7] in 1934. Imai and Iséki [4] in 1966 introduced the notion of a BCK-algebra. Recently [6] Jun, Borzooei and Zahedi et.al. applied the hyperstructure to BCK-algebras and introduced the concept of hyper BCK-algebra which is a generalization of BCK-algebra. Now, in this note we use the equivalence relation given in [1] and construct a quotient hyper BCK-algebra H/I via a hyper BCK-ideal I, then we obtain some related results which have been mentioned in the abstract.

2. Preliminaries

Definition 2.1. Let H be a nonempty set and "$\circ$" be a *hyperoperation* on H, that is "$\circ$" is a function from $H \times H$ to $\mathcal{P}^*(H) = \mathcal{P}(H)\backslash\{\emptyset\}$. Then H is called a *hyper BCK-algebra* if it contains a constant 0 and satisfies the following axioms:

2000 Mathematics Subject Classification: 06F35, 03G25
Keywords: hyper BCK-algebra, quotient hyper BCK-algebra, hyper BCK-ideal

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

Proposition 2.2. [6] *In any hyper BCK-algebra H, for all $x, y, z \in H$, the following statements hold*:

(i)	$0 \circ 0 = \{0\}$,	(iv)	$0 \circ x = \{0\}$,
(ii)	$0 \ll x$,	(v)	$x \circ y \ll x$,
(iii)	$x \ll x$,	(vi)	$x \circ 0 = \{x\}$.

Definition 2.3. Let I be a nonempty subset of a hyper BCK-algebra $(H, \circ, 0)$ and $0 \in I$. Then, I is called a *hyper BCK-ideal* of H if $x \circ y \ll I$ and $y \in I$ imply that $x \in I$, for all $x, y \in H$. If additionally $x \circ x \subseteq I$ for all $x \in H$, then I is called a *reflexive hyper BCK-ideal.*

Lemma 2.4. [5] *Let A, B and I be subsets of H.*

(i) *If $A \subseteq B \ll C$, then $A \ll C$.*

(ii) *If $A \circ x \ll I$ for $x \in H$, then $a \circ x \ll I$ for all $a \in A$.*

(iii) *If I is a hyper BCK-ideal of H and if $A \circ x \ll I$ for $x \in I$, then $A \ll I$.*

(iv) *If I be a reflexive hyper BCK-ideal of H and let A be a subset of H. If $A \ll I$, then $A \subseteq I$.*

Definition 2.5. [3] A hyper BCK-algebra H is said to be

– *weak positive implicative* if $(x \circ z) \circ (y \circ z) \ll (x \circ y) \circ z)$,

– *positive implicative* if $(x \circ z) \circ (y \circ z) = (x \circ y) \circ z$,

– *implicative* if $x \ll x \circ (y \circ x)$

holds for all $x, y, z \in H$.

Definition 2.6. [3] A nonempty subset I of a hyper BCK-algebra H containing 0 is called

– a *weak implicative hyper BCK-ideal* if for all $x, y, z \in H$

$$(x \circ z) \circ (y \circ x) \subseteq I \text{ and } z \in I \text{ imply } x \in I,$$

– an *implicative hyper BCK-ideal* if for all $x, y, z \in H$

$$(x \circ z) \circ (y \circ x) \ll I \text{ and } z \in I \text{ imply } x \in I.$$

Definition 2.7. [6] Let H be a hyper BCK-algebra. Define the set $\nabla(a, b) := \{x \in H \mid 0 \in (x \circ a) \circ b\}$. If for any $a, b \in H$, the set $\nabla(a, b)$ has the greatest element, then we say that H satisfies the hyper condition.

Proposition 2.8. [1] *Let I be a reflexive hyper BCK-ideal of H and let*

$$x \sim_I y \quad \textit{if and only if} \quad x \circ y \subseteq I \quad \textit{and} \quad y \circ x \subseteq I.$$

Then $\sim_I$ is an equivalence relation on H.

Proposition 2.9. [1] *Let A, B are subsets of H, and I a reflexive hyper BCK-ideal of H. Then we define $A \sim_I B$ if and only if $\forall a \in A$, $\exists b \in B$ in which $a \sim_I b$, and $\forall b \in B$, $\exists a \in A$ in which $a \sim_I b$. Then relation $\sim_I$ is an equivalence relation on $\mathcal{P}^*(H)$.*

3. Quotient hyper BCK-algebras

From now on H is a hyper BCK-algebra and I is a reflexive hyper BCK-ideal of H, unless otherwise is stated.

Lemma 3.1. *Let $A, B \in \mathcal{P}^*(H)$, and I be a hyper BCK-ideal of H. Then $A \circ B \ll I$ and $B \circ A \ll I$ imply that $A \sim_I B$.*

Proof. For all $a \in A$ and $b \in B$ we have $b \circ a \subseteq B \circ A$ and $a \circ b \subseteq A \circ B$. Since $A \circ B \ll I$, and $B \circ A \ll I$, then we have $b \circ a \ll I$, and $a \circ b \ll I$. Since I is reflexive then $a \sim_I b$, which implies that $A \sim_I B$. □

Theorem 3.2. *The relation $\sim_I$ is a congruence relation on H.*

Proof. By considering Proposition 2.8, it is enough to show that If $x \sim_I y$ and $u \sim_I v$, then $x \circ u \sim_I y \circ v$. Since $x \sim_I y$, we have $x \circ y \ll I$ and $y \circ x \ll I$. So $(x \circ v) \circ (y \circ v) \ll x \circ y$ and $x \circ y \ll I$ imply that $(x \circ v) \circ (y \circ v) \ll I$. Similarly $(y \circ v) \circ (x \circ v) \ll I$. Therefore by Lemma 3.1 $x \circ v \sim_I y \circ v$.

Also we have $(x \circ u) \circ (v \circ u) \ll x \circ v$. Then for all $t \in x \circ u$ and $r \in v \circ u$ we have $t \circ r \subseteq (x \circ u) \circ (v \circ u)$. Therefore for all $s \in t \circ r$ there exists $a \in x \circ v$ such that $s \ll a$, hence $(s \circ a) \cap I \neq \emptyset$. Since $s \circ a \subseteq (t \circ r) \circ a$, then $((t \circ r) \circ a) \cap I \neq \emptyset$. By Lemma 2.4 we have $(t \circ r) \circ a \ll I$. Thus $(t \circ a) \circ r \ll I$ and $r \in I$, which implies that $t \circ a \ll I$. Since $t \in x \circ u$ and $r \in v \circ u$ we can get that $(x \circ u) \circ (x \circ v) \ll I$. Similarly $(x \circ v) \circ (x \circ u) \ll I$. Then by Lemma 3.1 we can see that $x \circ v \sim_I x \circ u$.

Since $\sim_I$ is an equivalence relation on $\mathcal{P}^*(H)$, then $x \circ v \sim_I y \circ v$ and $x \circ v \sim_I x \circ u$ imply that $x \circ u \sim_I y \circ v$. □

Suppose I is a reflexive hyper BCK-ideal of $(H, \circ, 0)$. Denote the equivalence classes of x by C_x.

Lemma 3.3. *In any hyper BCK-algebra H we have $I = C_0$.*

Proof. Let $x \in I$. Since $x \in x \circ 0$, we have $(x \circ 0) \cap I \neq \emptyset$. Then $x \circ 0 \subseteq I$ and since $0 \circ x = 0$ hence $0 \circ x \subseteq I$. Then $0 \sim_I x$ therefore $x \in C_0$. Conversely let $x \in C_0$ hence $x \sim_I 0$ which means that $x \circ 0 \subseteq I$. Since $x \in x \circ 0$ then we have $x \in I$. □

Denote $H/I = \{C_x : x \in H\}$ and define $C_x * C_y = \{C_t \mid t \in x \circ y\}$. If $C_x = C_{x'}$ and $C_y = C_{y'}$, then $C_x * C_y = C_{x'} * C_{y'}$. Indeed, if $C_x = C_{x'}$ and $C_y = C_{y'}$ then $x \sim_I x'$ and $y \sim_I y'$, we can conclude that $x \circ y \sim_I x' \circ y'$ since $\sim_I$ is a congruence relation. Now let $C_t \in C_x * C_y$ then $t \in x \circ y$. Then there exist $r \in x' \circ y'$ such that $t \sim_I r$ hence $C_t = C_r$. Therefore $C_x * C_y \subseteq C_{x'} * C_{y'}$, and similarly $C_{x'} * C_{y'} \subseteq C_x * C_y$. Hence $*$ is well-defined.

On H/I we define $\ll$ putting: $C_x \ll C_y$ if and only if $C_0 \in C_x * C_y$. Observe that: $x \ll y \Longrightarrow 0 \in x \circ y \Longrightarrow C_0 \in C_x * C_y \Longrightarrow C_x \ll C_y$.

Theorem 3.4. *Let $(H, \circ, 0)$ be a hyper BCK-algebra and let I be a reflexive hyper BCK-ideal of H. Then $(H/I, *, C_0)$ is a hyper BCK-algebra.*

Proof. (HK1): Since H is a hyper BCK-algebra, we have $(x \circ z) \circ (y \circ z) \ll (x \circ y)$. So for all $t \in a \circ b \subseteq (x \circ z) \circ (y \circ z)$ there exists $s \in (x \circ y)$ such that $t \ll s$. Therefore $C_t \ll C_s$, where $C_t \in C_a * C_b \subseteq (C_x * C_z) * (C_y * C_z)$ and $C_s \in C_x * C_y$, hence $(C_x * C_z) * (C_y * C_z) \ll C_x * C_y$.

(HK2): We must show that $(C_x * C_y) * C_z = (C_x * C_z) * C_y$. Let $C_t \in (C_x * C_y) * C_z$. Then $t \in a \circ z \subseteq (x \circ y) \circ z = (x \circ z) \circ y$, which means that $C_t \in (C_x * C_z) * C_y$. Hence $(C_x * C_y) * C_z \subseteq (C_x * C_z) * C_y$. Similarly $(C_x * C_z) * C_y \subseteq (C_x * C_y) * C_z$.

(HK3): $C_x * \{C_t \mid t \in H\} = \{C_x * C_t \mid t \in H\} = \bigcup_{t \in H} \{C_y \mid y \in x \circ t\}$.
By Proposition 2.2 for all $y \in x \circ t$ we have $y \ll x$. So $C_y \ll C_x$, therefore $\{C_y \mid y \in x \circ t\} \ll C_x$. Thus $\bigcup_{t \in H} \{C_y \mid y \in x \circ t\} \ll C_x$. Therefore $C_x * H/I \ll C_x$.

(HK4): Let $C_x \ll C_y$ and $C_y \ll C_x$. We must show that $C_x = C_y$. Since $C_x \ll C_y$ then $C_0 \in C_x * C_y$. So there exists a $t \in x \circ y$ such that $t \sim_I 0$. Therefore $t \circ 0 \ll I$, thus $t \in I$. Hence $(x \circ y) \cap I \neq \emptyset$. Now, since I is a reflexive hyper BCK-ideal we conclude that $x \circ y \subseteq I$. Similarly $y \circ x \subseteq I$. Thus $x \sim_I y$ which means that $C_x = C_y$. □

Theorem 3.5. *If H is a bounded hyper BCK-algebra with the greatest element 1, then $(H/I, *, C_0)$ is also a bounded hyper BCK-algebra with the greatest element C_1.*

Proof. It is enough to prove that C_1 is the greatest element of H/I. For any $x \in H$, since $0 \in x \circ 1$ then $C_0 \in C_x * C_1$. This means that C_1 is the greatest element of H/I. □

The inverse of the above theorem does not hold.

Example 3.6. Let $H = \{0, 1, 2\}$. Then the following table shows a hyper BCK-algebra structure on H, which is not bounded.

$\circ$	0	1	2
0	$\{0\}$	$\{0\}$	$\{0\}$
1	$\{1\}$	$\{0\}$	$\{1\}$
2	$\{2\}$	$\{2\}$	$\{0, 2\}$

Then $I = \{0, 2\}$ is a reflexive hyper BCK-ideal of H. Now construct the quotient hyper BCK-algebra H/I via I. Because

$$C_0 = I = \{0, 2\} = C_2 = \{y \mid y \sim_I 2\}, \qquad C_1 = \{y \mid y \sim_I 1\} = \{1\},$$

then $H/I = \{C_0,\ C_1\}$ and

$*$	C_0	C_1
C_0	C_0	C_0
C_1	C_1	C_0

We can check that $(H/I, *, C_0)$ is a bounded hyper BCK-algebra. □

Theorem 3.7. *If J is a reflexive hyper BCK-ideal of H and $I \subseteq J$, then:*

(a) *I is a hyper BCK-ideal of the hyper BCK-subalgebra J of H,*

(b) *the quotient hyper BCK-algebra J/I is a hyper BCK-ideal of H/I.*

Proof. (a) At first we show that J is a hyper BCK-subalgebra of H. To show this let $x, y \in J$ we must show that $x \circ y \subseteq J$. Since $x \circ y \ll x$, then for all $a \in x \circ y$ we have $a \ll x$. Hence $0 \in a \circ x$. Thus $(a \circ x) \cap I \neq \emptyset$, since I is reflexive then $a \circ x \subseteq I$ and therefore $a \circ x \subseteq J$. Now $x \in J$ implies that $a \in J$, thus $x \circ y \subseteq J$. Hence J is a hyper BCK-subalgebra of H. It is clear that I is hyper BCK-ideal of the hyper BCK-subalgebra of J.

(b) We can check that $J/I \subseteq H/I$. If $C_x * C_y \ll J/I$ and $C_y \in J/I$, then for any $t \in x \circ y$, there exists $s \in J$ such that $C_t \ll C_s$. Thus $C_0 \in C_t * C_s$. So $C_0 = C_r$ for some $r \in t \circ s$. Therefore $0 \sim_I r$ and this implies that $0 \circ r \subseteq I$ and $r \circ 0 \subseteq I$. Hence $r \in I$, which means that $(t \circ s) \cap I \neq \emptyset$. Since I is reflexive, then $t \circ s \subseteq I$. Now $t \circ s \subseteq J$, and $s \in J$ implies that $t \in J$. Thus $x \circ y \ll J$. Since $y \in J$, so $x \in J$, thus $C_x \in J/I$. Hence J/I is a hyper BCK-ideal of H/I. □

Theorem 3.8. *If L is a hyper BCK-ideal of H/I, then $J = \{x \mid C_x \in L\}$ is a hyper BCK-ideal of H and moreover $I \subseteq J$. Furthermore $L = J/I$.*

Proof. Since $I = C_0 \in L$, then $0 \in J$. Let $x \circ y \ll J$ and $y \in J$. Then for any $t \in x \circ y$ there exists $s \in J$ such that $t \ll s$. Hence $C_t \ll C_s$, which implies that $C_x * C_y \ll L$. Since $y \in J$, we get that $C_y \in L$, thus $C_x \in L$. Therefore $x \in J$, hence J is a hyper BCK-ideal of H. Let $x \in I = C_0$. Then $x \sim_I 0$, thus $C_x = C_0$ and hence $C_x \in L$. Therefore $x \in J$, that is $I \subseteq J$. Clearly $L = J/I$. □

Theorem 3.9. *If I is a hyper BCK-ideal of H, then there is a bijection from the set $\mathcal{I}(H, I)$ of all hyper BCK-ideals of H containing I to the set $\mathcal{I}(H/I)$ of all hyper BCK-ideals of H/I.*

Proof. Define $f : \mathcal{I}(H, I) \to \mathcal{I}(H/I)$ by $f(J) = J/I$. By Theorem 3.7(b) f is well-defined, also Theorems 3.8 implies that f is onto. Let $A, B \in \mathcal{I}(H, I)$ and $A \neq B$. Without loss of generality, we may assume that there is an $x \in (B \backslash A)$. If $f(A) = f(B)$, then $C_x \in f(B) = B/I$ and $C_x \in f(A) = A/I$. Thus there exists $y \in A$ such that $C_x = C_y$ so $x \sim_I y$, that is $x \circ y \ll I$ and $y \circ x \ll I$. Since $I \subseteq A$ we have $x \circ y \ll A$. Thus $y \in A$ implies that $x \in A$, which is a contradiction. So f is one-to-one. □

Theorem 3.10. *Let I be a hyper BCK-ideal of H. Then there exists a canonical surjective homomorphism $\varphi : H \longrightarrow H/I$ by $\varphi(x) = C_x$, and $ker\varphi = I$, where $ker\varphi = \varphi^{-1}(C_0)$.*

Proof. It is clear that φ is well-defined. Let $x, y \in H$. Then $\varphi(x \circ y) = \{\varphi(t) \mid t \in x \circ y\} = \{C_t \mid t \in x \circ y\} = C_x * C_y = \varphi(x) * \varphi(y)$. Hence φ is homomorphism. Clearly φ is onto. We have $ker\varphi = \{x \in H \mid \varphi(x) = C_0\} = \{x \in H \mid C_x = C_0 = I\} = \{x \in H \mid x \in I\} = I$. □

Theorem 3.11. *Let $f : H_1 \longrightarrow H_2$ be a homomorphism of hyper BCK-algebras, and let I be a hyper BCK-ideal of H_1 such that $I \subseteq kerf$. Then there exists a unique homomorphism $\bar{f} : H_1/I \longrightarrow H_2$ such that $\bar{f}(C_x) = f(x)$ for all $x \in H_1$, $Im(\bar{f}) = Im(f)$ and $ker\bar{f} = kerf/I$. Moreover $\bar{f}$ is an isomorphism if and only if f is surjective and $I = kerf$.*

Proof. Let $C_x = C_{x'}$. Then $x \sim_I x'$, which implies that $x \circ x' \subseteq I$ and $x' \circ x \subseteq I$. Thus there exists $t \in (x \circ x') \bigcap I$. Then $0 = f(t) \in f(x \circ x') = f(x) \circ f(x')$, hence $f(x) \ll f(x')$. Similarly $f(x') \ll f(x)$, therefore $\bar{f}$ is well-defined.

We have $\bar{f}(C_x * C_y) = \bar{f}(\{C_t \mid t \in x \circ y\}) = \{\bar{f}(C_t) \mid t \in x \circ y\} = \{f(t) \mid t \in x \circ y\} = f(x \circ y) = f(x) \circ f(y) = \bar{f}(C_x) * \bar{f}(C_y)$. Then $\bar{f}$ is a homomorphism. On the other hand

$$C_x \in ker\bar{f} \Longleftrightarrow \bar{f}(C_x) = 0 \Longleftrightarrow f(x) = 0 \Longleftrightarrow x \in kerf.$$

Note that $\bar{f}$ is unique, since it is completely determined by f. Finally it is clear that $\bar{f}$ is surjective if and only if f is surjective. □

Theorem 3.12. *Let $f : H_1 \longrightarrow H_2$ be a homomorphism of hyper BCK-algebras. Then $H_1/kerf \cong Im(f)$.* □

Theorem 3.13. *Let I, J be hyper BCK-ideals of H. Then there is a (natural) homomorphism of hyper BCK-algebras between $I/(I \cap J)$ and $< I \cup J > /J$, where $< I \cup J >$ is the hyper BCK-ideal generated by $I \cup J$.*

Proof. Define $\varphi : I \rightarrow < I \cup J > /J$ by $\varphi(x) = C_x^J$, where C_x^J is the equivalence classes C_x via the hyper BCK-ideal J. If $x_1 = x_2$, then it is clear that $C_{x_1}^J = C_{x_2}^J$, which means that φ is well-defined. Also we have

$$\varphi(x \circ y) = \{\varphi(t) \mid t \in x \circ y\} = \{C_t^J \mid t \in x \circ y\} = C_x^J * C_y^J = \varphi(x) * \varphi(y).$$

So that φ is a homomorphism. Moreover

$$\begin{aligned} ker\varphi &= \{x \in I \mid \varphi(x) = C_0^J\} = \{x \in I \mid C_x^J = C_0^J = J\} \\ &= \{x \in I \mid x \in J\} = I \cap J. \end{aligned}$$

Thus by Theorem 3.12 the proof is completed. □

Open Problem 1. *Under what condition(s) is the defined homomorphism in Theorem* 3.11 *an isomorphism* ?

Theorem 3.14. *Let I, J be hyper BCK-ideals of H such that $I \subseteq J$. Then $(H/I)/(J/I) \cong H/J$.*

Proof. It is clear that $J/I \subseteq H/I$. Define $f : H/I \longrightarrow H/J$ by $C_x^I \mapsto C_x^J$, where $C_x^I \in H/I$ and $C_x^J \in H/J$.

If $C_x^I = C_y^I$, then $x \sim_I y$ which implies that $x \circ y \subseteq I$ and $y \circ x \subseteq I$. Since $I \subseteq J$ hence $x \circ y \subseteq J$ and $y \circ x \subseteq J$. Thus $x \sim_J y$ then $C_x^J = C_y^J$ which means that f is well-defined.

$$f(C_x^I * C_y^I) = f(\{C_t^I \mid t \in x \circ y\}) = \{C_t^J \mid t \in x \circ y\} = C_x^J * C_y^J = f(C_x^I) * f(C_y^I).$$

Clearly f is onto and

$$\begin{aligned} kerf &= \{C_x^I \in H/I \mid f(C_x^I) = C_0^J\} = \{C_x^I \in H/I \mid C_x^J = C_0^J\} \\ &= \{C_x^I \in H/I \mid x \in J\} = J/I. \end{aligned}$$

Now by Theorem 3.12 the proof is completed. □

4. Some result in quotient hyper BCK-algebras

Let $C_a, C_b \in H/I$. Then according to Definition 2.7 we have

$$\nabla(C_a, C_b) := \{C_x \in H/I \mid C_0 \in (C_x * C_a) * C_b\}.$$

Obviously $C_0, C_a, C_b \in \nabla(C_a, C_b)$, $\nabla(C_0, C_0) = \{C_0\}$ and $\nabla(C_a, C_b) = \nabla(C_b, C_a)$ for all $C_a, C_b \in H/I$.

Theorem 4.1. *If H satisfies the hyper condition, then H/I so is.*

Proof. If $x \in \nabla(a, b)$, then we have $x \circ a \ll b$. Thus for all $t \in x \circ a$, $t \ll b$. Therefore $C_t \ll C_b$, thus $C_x * C_a \ll C_b$. Hence $C_x \in \nabla(C_a, C_b)$. Since $\nabla(a, b)$ has the greatest element, then by Theorem 3.5, $\nabla(C_a, C_b)$ has the greatest element too. $\square$

Remark 4.2. The converse of the above theorem is not correct in general. Let $H = \{0, 1, 2\}$ and

$\circ$	0	1	2
0	$\{0\}$	$\{0\}$	$\{0\}$
1	$\{1\}$	$\{0, 1\}$	$\{1\}$
2	$\{2\}$	$\{2\}$	$\{0\}$

Then $I = \{0, 1\}$ is a reflexive hyper BCK-ideal of a hyper BCK-algebra $(H, \circ, 0)$ and the elements of the quotient hyper BCK-algebra H/I are as follows: $C_0 = I = \{0, 1\} = C_1 = \{y \mid y \sim_I 1\}$, $C_2 = \{y \mid y \sim_I 2\} = \{2\}$. Hence $H/I = \{C_0, C_2\}$ and

$*$	C_0	C_2
C_0	C_0	C_0
C_2	C_2	C_0

It can be checked that the quotient hyper BCK-algebra H/I satisfies the hyper condition, but H does not satisfy the hyper condition, since $\nabla(1, 2) = \{0, 1, 2\}$, $1 \not\ll 2$ and $2 \not\ll 1$. $\square$

Theorem 4.3. *If H is an implicative hyper BCK-algebra, then so is H/I.*

Proof. The proof is easy. $\square$

Note that the converse of the above theorem is not correct in general.

Example 4.4. The set $H = \{0, 1, 2\}$ with the operation

$\circ$	0	1	2
0	$\{0\}$	$\{0\}$	$\{0\}$
1	$\{1\}$	$\{0\}$	$\{0\}$
2	$\{2\}$	$\{1\}$	$\{0, 1\}$

is a hyper BCK-algebra. $I = \{0, 1\}$ is a reflexive hyper BCK-ideal such that $C_0 = I = \{0, 1\} = C_1 = \{y \mid y \sim_I 1\}$, $C_2 = \{y \mid y \sim_I 2\} = \{2\}$ and

$*$	C_0	C_2
C_0	C_0	C_0
C_2	C_2	C_0

We can check that $H/I = \{C_0, C_2\}$ is an implicative hyper BCK-algebra, while the hyper BCK-algebra H is not, since $1 \not\ll 1 \circ (2 \circ 1)$. $\square$

Theorem 4.5. *If H is a (weak) positive implicative hyper BCK algebra, then so is H/I.*

Proof. Let H be a positive implicative hyper BCK-algebra. Then we have

$$\begin{aligned} C_t \in (C_x * C_z) * (C_y * C_z) &\Longleftrightarrow C_t = C_s \text{ for some } s \in (x \circ z) \circ (y \circ x), \quad t \sim_I s \\ &\Longleftrightarrow C_t = C_s \text{ for some } s \in (x \circ y) \circ z, \quad s \sim_I t \\ &\Longleftrightarrow C_t \in (C_x * C_y) * C_z. \end{aligned}$$

The other case is similar. $\square$

Note that Example 4.4 shows that the converse of the above theorem is not correct in general. Since H/I is positive implicative while H is not, since $(2 \circ 2) \circ (2 \circ 2) = \{0, 1\} \neq \{0\} = (2 \circ 2) \circ 2$.

Theorem 4.6. *Let I and J be reflexive hyper BCK-ideals of H and $I \subseteq J$. If J is a weak implicative hyper BCK-ideal of H, then J/I is a weak implicative hyper BCK-ideal of H/I.*

Proof. Let J be a weak implicative hyper BCK-ideal of H and $(C_x * C_z) * (C_y * C_x) \subseteq J/I$ and $C_z \in J/I$. Then for all $C_s \in (C_x * C_z) * (C_y * C_x)$ where $s \in (x \circ z) \circ (y \circ x)$, we have $C_s \in J/I$. Thus $s \sim_I r$, for some $r \in J$. So $s \circ r \subseteq I$, hence $s \circ r \subseteq J$. Consequently $r \in J$ implies that $s \in J$. Thus $(x \circ z) \circ (y \circ x) \subseteq J$, and from $C_z \in J/I$ we can conclude that $z \in J$. Since J is a weak implicative hyper BCK-ideal, then we get that $x \in J$. Hence $C_x \in J/I$, which means that J/I is a weak implicative hyper BCK-ideal of H/I. $\square$

Open Problem 2. *Does the converse of the above theorem true ?*

Theorem 4.7. *Let $I \subseteq J$ be reflexive hyper BCK-ideals of H. Then J/I is an implicative hyper BCK-ideal of H/I if and only if J is an implicative hyper BCK-ideal of H.*

Proof. Let J be an implicative hyper BCK-ideal and $C_x * (C_y * C_x) \ll J/I$. Then for all $C_t \in C_x * (C_y * C_x)$ there exists $C_r \in J/I$ such that $C_t \ll C_r$, where $t \sim_I s$, $s \in x \circ (y \circ x)$ and $r \in J$. Since $C_t \ll C_r$ then $C_0 \in C_t * C_r$, hence there exists $u \in t \circ r$ such that $0 \sim_I u$. Thus $u \circ 0 \subseteq I$, therefore $u \in I$. Then $(t \circ r) \cap I \neq \emptyset$ which means that $t \circ r \cap J \neq \emptyset$. Therefore $r \in J$ implies that $t \in J$. Since $t \sim_I s$ thus $s \circ t \subseteq I$ and hence $s \circ t \subseteq J$. Thus $t \in J$

implies that $s \in J$, hence $x \circ (y \circ x) \ll J$. Since J is an implicative hyper BCK-ideal by Theorem 3.6 of [3] we can get that $x \in J$. Hence $C_x \in J/I$. Now Theorem 3.6 [3] implies that J/I is an implicative hyper BCK-ideal of H/I.

Conversely, let J/I be an implicative hyper BCK-ideal of H/I and $x \circ (y \circ x) \ll J$. Then for all $t \in x \circ (y \circ x)$ there exists $r \in J$ such that $t \ll r$. Thus $C_t \ll C_r$, and we can conclude that $C_x * (C_y * C_x) \ll J/I$. Since J/I is an implicative hyper BCK-ideal of H, then $C_x \in J/I$, we can get that $x \in J$. Therefore J is an implicative hyper BCK-ideal of H, by Theorem 3.6 of [3]. $\square$

References

[1] **A. B. Saeid and M. M. Zahedi**: *Uniform structure on hyper BCK-algebras*, Italian J. Pure and Appl. Math. (to appear).

[2] **R. A. Borzooei and M. Bakhshi**: *Some kinds of positive implicative hyper BCK-ideals*, (to appear).

[3] **Y. B. Jun and X. L. Xin**: *Implicative hyper BCK-ideals of hyper BCK-algebras*, Math. Japonica, **52** (2000), 435 − 443.

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

[5] **Y. B. Jun, X. L. Xin, E. H. Roh and M. M. Zahedi**: *Strong hyper BCK-ideals of hyper BCK-algebras*, Math. Japon. **51** (2000), 493 − 498.

[6] **Y. B. Jun, M. M. Zahedi, X. L. Xin and R. A. Borzooei**: *On hyper BCK-algebras,* Italian J. Pure and Appl. Math. **8** (2000), 127 − 136.

[7] **F. Marty**: *Sur une generalization de la notion de groups*, 8th Congress Math. Scandinaves, Stockholm 1934, 45 − 49.

A. B. Saeid
Department of Mathematics
Islamic Azad University of Kerman
Kerman
Iran
e-mail: arsham@iauk.ac.ir

Received July 14, 2003

M. M. Zahedi
Department of Mathematics
Shahid Bahonar University of Kerman
Kerman
Iran
e-mail: zahedi_mm@mail.uk.ac.ir

Quasigroups and Related Systems **12** (2004), 103 – 112

Affine regular pentagons in GS–quasigroups

Vladimir Volenec and Zdenka Kolar–Begović

Abstract

The "geometric" concept of affine regular pentagon and affine regular star–shaped pentagon in general GS–quasigroup will be introduced. Some characteristics of the introduced concepts will be proved and the geometric interpretation in the GS–quasigroup $C(\frac{1}{2}(1+\sqrt{5}))$ will be given.

1. Introduction

A quasigroup $(Q,\cdot)$ is said to be *GS–quasigroup* if it satisfies (mutually equivalent) identities

$$a(ab\cdot c)\cdot c=b, \qquad a\cdot(a\cdot bc)c=b \tag{1}$$

and moreover the identity of *idempotency*

$$aa=a. \tag{2}$$

The considered GS–quasigroup $(Q,\cdot)$ satisfies the identities of *mediality, elasticity, left* and *right distributivity* i.e. we have the identities

$$ab\cdot cd=ac\cdot bd, \tag{3}$$

$$a\cdot ba=ab\cdot a, \tag{4}$$

$$a\cdot bc=ab\cdot ac, \qquad ab\cdot c=ac\cdot bc. \tag{5}$$

Further, the identities

$$a(ab\cdot b)=b, \qquad (b\cdot ba)a=b, \tag{6}$$

2000 Mathematics Subject Classification: 20N05

Keywords: GS–quasigroup, affine regular pentagon

$$a(ab \cdot c) = b \cdot bc, \qquad (c \cdot ba)a = cb \cdot b, \tag{7}$$

$$a(a \cdot bc) = b(b \cdot ac), \qquad (cb \cdot a)a = (ca \cdot b)b \tag{8}$$

and equivalencies

$$ab = c \Leftrightarrow a = c \cdot cb, \qquad ab = c \Leftrightarrow b = ac \cdot c \tag{9}$$

also hold. GS–quasigroups are studied in [1].

Example 1. Let C be the set of points of the Euclidean plane. For any two different points a, b we define $ab = c$ if the point b or a divides the pair a, c or the pair b, c, respectively, in the ratio of the golden section.

In [1] it is proved that $(Q, \cdot)$ is a GS–quasigroup in both cases. We shall denote these two quasigroups by $C(\frac{1}{2}(1+\sqrt{5}))$ and $C(\frac{1}{2}(1-\sqrt{5}))$ because we have $c = \frac{1}{2}(1+\sqrt{5})$ or $c = \frac{1}{2}(1-\sqrt{5})$ if $a = 0$ and $b = 1$. These quasigroups can give a motivation for the definition of "geometric" notions and proving of "geometric" properties of a general GS–quasigroup. In the quasigroup $C(\frac{1}{2}(1+\sqrt{5}))$ we shall illustrate (by figures) the properties of general GS–quasigroup.

The considered two quasigroups are equivalent because it can be shown that if the operations $\cdot$ and $\bullet$ on the set Q are connected with the identity $a \bullet b = b \cdot a$, then $(Q, \bullet)$ is a GS–quasigroup if and only if $(Q, \cdot)$ is a GS–quasigroup.

From now on, let $(Q, \cdot)$ be any GS–quasigroup. The elements of the set Q are said to be *points*. The points a, b, c, d are said to be the vertices of a *parallelogram* and we write $Par(a, b, c, d)$ if the identity $d = a \cdot b(ca \cdot a)$ holds. The points a, b, c, d successively are said to be the vertices of the *golden section trapezoid* and it is denoted by $\mathrm{GST}(a, b, c, d)$ if the identity $a \cdot ab = d \cdot dc$ holds.

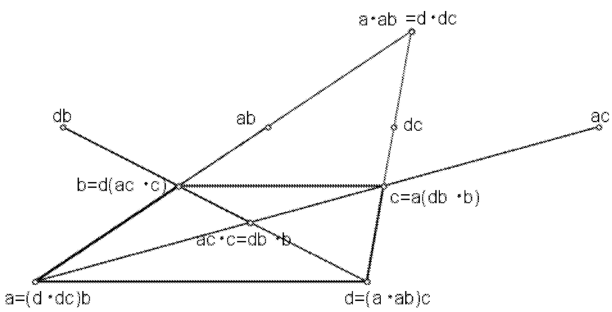


Figure 1.

In [2] the different properties of the quaternary relation GST on the set Q are proved. We shall mention just a few of them which will be used afterwards.

Theorem 1. *$GST(a, b, c, d)$ implies $GST(d, c, b, a)$.* □

If the relation $\mathrm{GST}(a, b, c, d)$ holds we shall say that the points c, a, d, b form a *GS–trapezoid of the second* kind and we shall write $\overline{GST}(c, a, d, b)$.

Remark 1. In [2] it is proved that a GS–trapezoid in one of the two quasigroups mentioned in Example 1 will be a GS–trapezoid of the second kind in the other quasigroup and vice versa. It means that it is a matter of convention which of the two quadrangles (a, b, c, d) or (c, a, d, b) will be called GS–trapezoid and which one a GS–trapezoid of the second kind, since we cannot differ them in the general GS–quasigroup.

Theorem 2. *The statement $GST(a, b, c, d)$ is equivalent to the equality $ac \cdot c = db \cdot b$ (Figure 1).* □

Theorem 3. *The statement $GST(a, b, c, d)$ is equivalent to any of the four equalities $a = (d \cdot dc)b$, $b = d(ac \cdot c)$, $c = a(db \cdot b)$, $d = (a \cdot ab)c$ (Figure 1).* □

Corollary 1. *GS–trapezoid is uniquely determined by any 3 of its vertices.*

Theorem 4.

(*i*) *Any two of the three statements $GST(a, b, c, d)$, $GST(b, c, d, e)$, $GST(c, d, e, a)$ imply the remaining statement (Figure 2).*

(*ii*) *Any two of the three statements $GST(a, b, c, d)$, $GST(b, c, d, e)$, $GST(d, e, a, b)$ imply the remaining statement (Figure 2).* □

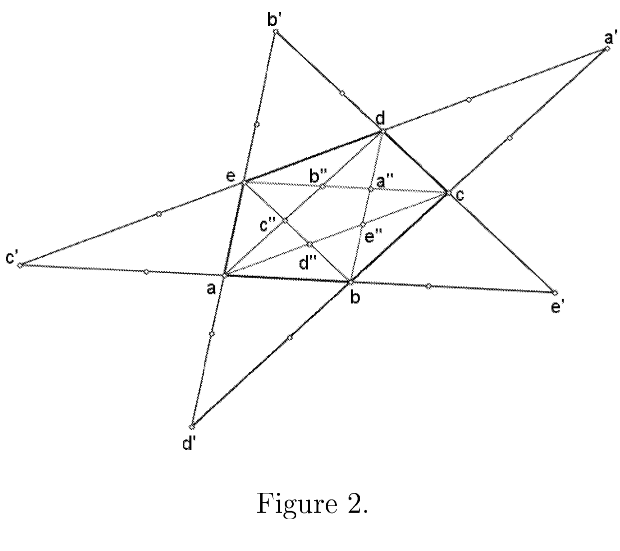


Figure 2.

If we apply Theorem 4 it immediately follows that any two of the five statements imply the remaining statement

$$GST(a,b,c,d), GST(b,c,d,e), GST(c,d,e,a), GST(d,e,a,b), GST(e,a,b,c).$$

Definition 1. The points a,b,c,d,e successively are said to be the vertices of the *affine regular pentagon* and it is denoted by $ARP(a,b,c,d,e)$ if any two (and then all five) of the above five statements are valid (Figure 2).

Based on Theorem 1 and Corollary 1 following three statements immediately follow.

Theorem 5. *If* (f,g,h,i,j) *is any cyclic permutation of* (a,b,c,d,e) *or of* (e,d,c,b,a)*, then* $ARP(a,b,c,d,e)$ *implies* $ARP(f,g,h,i,j)$*.* □

Theorem 6. *Affine regular pentagon is uniquely determined by any three of its vertices.* □

Theorem 7. *If the statement* $GST(a,b,c,d)$ *holds then there is one and only one point* e *such that the statement* $ARP(a,b,c,d,e)$ *holds.* □

Definition 2. If the relation $ARP(a,b,c,d,e)$ holds we shall say that the points a,c,e,b,d successively are the vertices of *affine regular star–shaped pentagon* and write $\overline{ARP}(a,c,e,b,d)$.

It is obvious, because of Theorem 5, that the equivalency of the statements $\overline{ARP}(a,b,c,d,e)$ and $ARP(a, c,e,b,d)$ is valid, it means that the relations ARP and $\overline{ARP}$ are mutually symmetric. From the Theorem about duality for GS–trapezoids (cf. [2]) now an analogous theorem follows.

Theorem 8 (about duality for affine regular pentagons).
From every theorem about affine regular pentagons we get an analogous theorem about affine regular star–shaped pentagons (and vice versa) if the roles of both factors are interchanged in all products which appear in the theorem. □

Corollary 2. *From every theorem about affine regular pentagons again we get a theorem about affine regular pentagons, if every statement of the form* $ARP(a,b,c,d,e)$ *is interchanged by the corresponding statement* $ARP(a,c,e,b,d)$*, and the roles of both factors are interchanged in all products.* □

In the interchanges mentioned in Theorem 8 and Corollary 2 it is not necessary to make an interchange in possible statements about the relation Par.

It follows from Remark 1 that in the general GS–quasigroup, whose model is the Euclidean plane, mentioned in Example 1 on one of the two ways, we cannot make out the difference between the affine regular pentagon and the affine regular star–shaped pentagon because what is an affine regular pentagon in one model that is an affine regular star–shaped pentagon in the other model (and vice versa); so it is just the matter of convention which of two pentagons we shall call affine regular and which affine regular star–shaped pentagon.

Theorem 6 can be expressed by the following theorem more precisely.

Theorem 9. *For any points* a, b, c *we have* $ARP((c\cdot cb)a,\ a,\ b,\ c,\ (a\cdot ab)c)$ *and* $ARP(a,\ c(ba\cdot a),\ b,\ a(bc\cdot c),\ c)$.

Proof. The second statement follows from the first applying the Corollary 2 and Theorem 5, and the first statement follows from the fact that $GST(a, b, c, d)$ is equivalent to $d = (a \cdot ab)c$, and $GST(e, a,\ b,\ c)$ to $e = (c \cdot cb)a$ (Theorem 3). □

From now on, let the statement $\mathrm{ARP}(a, b, c, d, e)$ be valid.

From $\mathrm{GST}(b, c, d, e)$ according to the definition of the relation GST and because of Theorem 2 follow the equations

$$b \cdot bc = e \cdot ed, \qquad bd \cdot d = ec \cdot c.$$

Set

$$a' = b \cdot bc = e \cdot ed, \qquad a'' = bd \cdot d = ec \cdot c,$$

and similarly the points b', b'', c', c'', d', d'', e', e'' (Figure 2) can be defined.

Let us prove several statements about these points.

Theorem 10. *The statements* $ARP(a', b', c', d', e')$ *and* $ARP(a'', b'', c'', d'', e'')$ *hold.*

Proof. According to Theorem 9 from [2] we have the statements

$$\mathrm{GST}(e \cdot ed,\ a \cdot ae,\ d \cdot de,\ e \cdot ea), \quad \mathrm{GST}(ec \cdot c,\ ce \cdot e,\ be \cdot e,\ eb \cdot b).$$

However,

$$e \cdot ed = a', \quad a \cdot ae = b', \quad d \cdot de = c', \quad e \cdot ea = d',$$
$$ec \cdot c = a'', \quad ce \cdot e = b'', \quad be \cdot e = c'', \quad eb \cdot b = d'',$$

so we get

$$\mathrm{GST}(a', b', c', d'), \qquad \mathrm{GST}(a'', b'', c'', d''),$$

and the remaining statements follow by the cyclical exchange of letters. □

Theorem 11. *The statements $Par(a, c, a', d)$, $Par(a, b', a', e')$, $Par(a, b, a'', e)$, $Par(a, c'', a'', d'')$ etc. hold.*

Proof. First, the equalities

$$\begin{aligned} a'c &= (b \cdot bc)c \overset{(6)}{=} b, \\ b'a &= (a \cdot ae)a \overset{(4)}{=} a(ae \cdot a) \overset{(7)}{=} e \cdot ea = d', \\ ba'' &= b(bd \cdot d) \overset{(6)}{=} d, \\ ac'' &= a(da \cdot a) \overset{(4)}{=} (a \cdot da)a \overset{(7)}{=} ad \cdot d = b'' \end{aligned}$$

are valid, and then, according to Lemma 2 from [2] we get these implications

$$\begin{aligned} \mathrm{GST}(d, c, b, a), &\quad a'c = b \Rightarrow \mathrm{Par}(a', d, a, c), \\ \mathrm{GST}\ (b', a', e', d'), &\quad b'a = d' \Rightarrow \mathrm{Par}(b', a', e', a), \\ \mathrm{GST}(b, a, e, d), &\quad ba'' = d \Rightarrow \mathrm{Par}(b, a, e, a''), \\ \mathrm{GST}(d'', c'', b'', a''), &\quad ac'' = b'' \Rightarrow \mathrm{Par}(a, d'', a'', c''), \end{aligned}$$

where, in the assumptions, the results of Theorem 10 are used. □

In the Theorem 11 we have come to some statements about the relation Par from the statements about the relation ARP. It can be also done in the opposite way, because the following theorem holds.

Theorem 12. *From $Par(a, b, c, d)$ follow $ARP(b, ab, c, ad, d)$ and $ARP(ba, d, c, b, da)$ (Figure 3).*

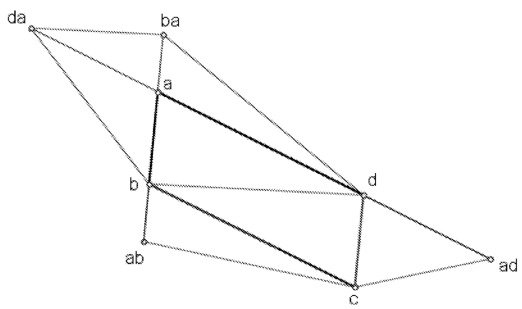


Figure 3.

Proof. According to Theorem 7 from [2] $GST(ad, d, b, ab)$ is valid, and from $\mathrm{Par}(a, d, c, b)$ by Lemma 2 from [2] it follows $GST(d, b, ab, c)$ so the first statement holds, and the second statement follows from the first one according to Corollary 2. □

Let us further prove

Theorem 13. *The statements $ARP(a, b, c, d, e)$, $ARP(c, ac, f, ad, d)$ hold where we have $f = b \cdot bc = e \cdot ed$ (Figure 4).*

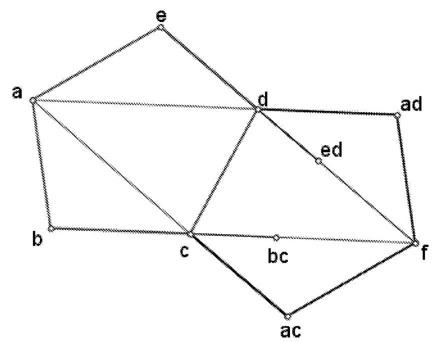


Figure 4.

Proof. According to Theorem 10 from [2], from the statement $\mathrm{GST}(a, b, c, d)$ it follows $\mathrm{GST}(c, d, ad, b \cdot bc)$, and from $\mathrm{GST}(a, e, d, c)$ it follows $\mathrm{GST}(d, c, ac, e{\cdot}ed)$. However, because of $\mathrm{GST}(b, c, d, e)$ we have the equality $b \cdot bc = e \cdot ed$. □

The following theorem about affine regular pentagons also holds.

Theorem 14. *Any two of the three statements $ARP(a, b, c, d, e)$, $ARP(f, g, h, i, j)$, $ARP(af, bg, ch, di, ej)$ imply the remaining statement (Figure 5).*

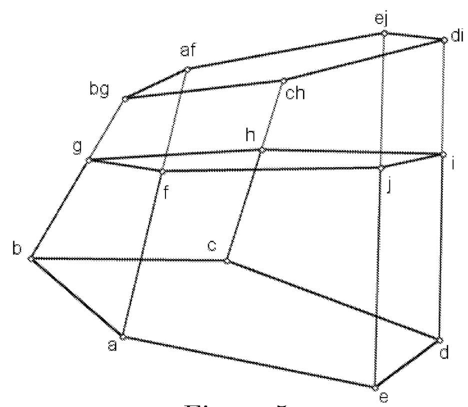


Figure 5.

Proof. It is sufficient to prove that any two of three statements $GST(a,b,c,d)$, $GST(f,g,h,i)$ and $GST(af,bg,ch,di)$ imply the remaining statement. However, according to (3) we have successively

$$\begin{aligned}[(af)\cdot(af)(bg)](ch) &= [(af)\cdot(ab\cdot fg)](ch) = [(a\cdot ab)\cdot(f\cdot fg)](ch)\\ &= (a\cdot ab)c\cdot(f\cdot fg)h\end{aligned}$$

and then it is obvious that any two of the three equalities $(a\cdot ab)c = d$, $(f\cdot fg)h = i$ and $[ae\cdot(af)(bg)](ch) = di$ imply the remaining equality. □

Corollary 3. *$ARP(a,b,c,d,e)$ always implies $ARP(ab,bc,cd,de,ea)$, $ARP(ac,bd,ce,da,eb)$, $ARP(ad,be,ca,db,ec)$, $ARP(ae,ba,cb,dc,ed)$.* □

For any point p we have obviously $\mathrm{ARP}(p,p,p,p,p)$ and from Theorem 14 it follows further:

Corollary 4. *The statements $ARP(a,b,c,d,e)$, $ARP(ap,bp,cp,dp,ep)$, $ARP(pa,pb,pc,pd,pe)$ are mutually equivalent (for any point p).* □

Theorem 15. *From $c = (ob\cdot a)o$ it follows $a = (ob\cdot c)o$, and from $c = (ob\cdot a)o$ and $d = (oc\cdot b)o$ it follows $GST(a,b,c,d)$ (Figure 6).*

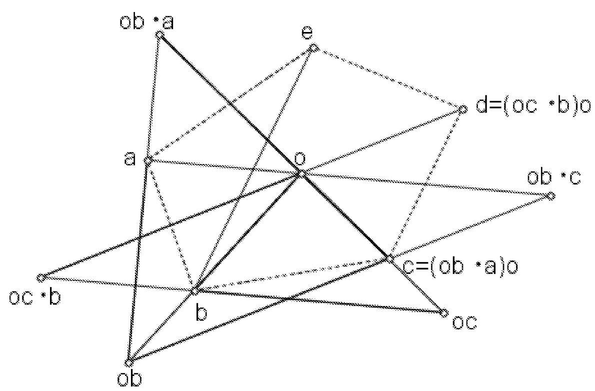


Figure 6.

Proof. We have successively

$$(ob\cdot c)o = [ob\cdot(ob\cdot a)o]o \overset{(1)}{=} a$$

$$\begin{aligned}(a\cdot ab)c &= (a\cdot ab)\cdot(ob\cdot a)o \overset{(3)}{=} a(ob\cdot a)\cdot(ab\cdot o) \overset{(4)}{=} (a\cdot ob)a\cdot(ab\cdot o)\\ &\overset{(3)}{=} (a\cdot ob)(ab)\cdot ao \overset{(5)}{=} a\cdot(ob\cdot b)o = (ob\cdot c)o\cdot(ob\cdot b)o\\ &\overset{(5)}{=} (ob\cdot c)(ob\cdot b)\cdot o \overset{(5)}{=} (ob\cdot cb)o \overset{(5)}{=} (oc\cdot b)o = d.\end{aligned}$$

□

Based on Theorem 15 this definition makes sense.

Definition 3. We say that the point o is the *centre of affine regular pentagon* with vertices a_o, a_1, a_2, a_3, a_4 if for each $i \in \{0,1,2,3,4\}$ is valid (modulo 5) the following equality

$$(oa_{i+1} \cdot a_i)o = a_{i+2} \qquad \text{respectively} \qquad (oa_{i-1} \cdot a_i)o = a_{i-2}.$$

On the Figure 6 the point o is the centre of affine regular pentagon with the vertices a, b, c, d, e.

Theorem 16. *Under the hypothesis of Theorem* 15 *equalities* $d = a\cdot(ob\cdot b)o$, $d = o(c \cdot ao)$, $b = o(c \cdot co) \cdot a$ *are valid.*

Proof. The first equality is proved in the proof of Theorem 15. Then we have successively

$$\begin{aligned} o(c\cdot ao) &\overset{(5)}{=} oc\cdot(o\cdot ao) \overset{(5)}{=} (oc\cdot o)(oc\cdot ao) = (oc\cdot o)\cdot[o\cdot(ob\cdot a)o](ao) \\ &\overset{(4)}{=} (oc\cdot o)\cdot[o(ob\cdot a)\cdot o](ao) \overset{(7)}{=} (oc\cdot o)[(b\cdot ba)o\cdot ao] \\ &\overset{(5)}{=} [oc\cdot(b\cdot ba)a]o \overset{(6)}{=} (oc\cdot b)o = d, \end{aligned}$$

and then from $(ob\cdot a)o = c$ because of (9) first follows $ob\cdot a = c\cdot co$, and then $ob = (c\cdot co)\cdot(c\cdot co)a$, and finally out of that according to (9) we get

$$\begin{aligned} b &= o[(c\cdot co)\cdot(c\cdot co)a]\cdot[(c\cdot co)\cdot(c\cdot co)a] \\ &\overset{(3)}{=} o(c\cdot co)\cdot[(c\cdot co)\cdot(c\cdot co)a][(c\cdot co)a] \\ &\overset{(5)}{=} o(c\cdot co)\cdot(c\cdot co)[(c\cdot co)a\cdot a] \overset{(6)}{=} o(c\cdot co)\cdot a., \end{aligned}$$

which completes the proof. □

If the point o is the centre of affine regular pentagon a_o, a_1, a_2, a_3, a_4 then the equalities from the Theorem 16 can be written in the form

$$\begin{aligned} a_i\cdot(oa_{i+1}\cdot a_{i+1})o &= a_{i+3}, \\ o(a_{i+2}\cdot a_io) &= a_{i+3}, \\ o(a_{i+2}\cdot a_{i+2}o)\cdot a_i &= a_{i+1}, \end{aligned}$$

and similarly because of symmetry the equalities

$$\begin{aligned} a_i\cdot(oa_{i-1}\cdot a_{i-1})o &= a_{i-3}, \\ o(a_{i-2}\cdot a_io) &= a_{i-3}, \\ o(a_{i-2}\cdot a_{i-2}o)\cdot a_i &= a_{i-1} \end{aligned}$$

are valid.

Under the hypothesis of the Theorem 15 and 16 and labels from Figure 2 the equalities

$$ab'' = d = a \cdot (ob \cdot b)o,$$
$$c'a = b = o(c \cdot co) \cdot a$$

are valid, and then immediately follows

$$b'' = (ob \cdot b)o,$$
$$c' = o(c \cdot co).$$

In general case, using analogous labels, we get the equalities

$$a_i' = o(a_i \cdot a_i o),$$
$$a_i'' = (oa_i \cdot a_i)o.$$

From previous considerations also follows

Theorem 17. *Affine regular pentagon is uniquely determined by its centre and with any two of its vertices.* □

References

[1] **V. Volenec**: *GS–quasigroups*, Čas. pěst. mat. **115** (1990), 307 – 318.

[2] **V. Volenec and Z. Kolar**, *GS–trapezoids in GS–quasigroups*, Math. Communications **7** (2002), 143 – 158.

Received November 2, 2003

V. Volenec
Department of Mathematics
University of Zagreb
Bijenička 30
HR-10 000 Zagreb
Croatia
e-mail: volenec@math.hr

Z. Kolar–Begović
Department of Mathematics
University of Osijek
Gajev trg 6
HR-31 000 Osijek
Croatia
e-mail: zkolar@mathos.hr