Quasigroups and Related Systems **13** (2005), 175 – 184

Fuzzy isomorphism and quotient of fuzzy subpolygroups

Reza Ameri and Hossein Hedayati

Abstract

The aim of this note is the study of fuzzy isomorphism and quotient of fuzzy subpolygroups. In this regards first we introduce the notion of fuzzy isomorphism of fuzzy subpolygroups and then we study the quotient of fuzzy subpolygroups. Finally we obtain some related basic results.

1. Introduction

Hyperstructure theory was born in 1934 when Marty defined hypergroups, began to analyse their properties and applied them to groups, rational algebraic functions. Now they are widely studied from theoretical point of view and for their applications to many subjects of pure and applied properties and applied mathematics. In 1981 Ioulidis introduced the notion of *polygroup* as a hypergroup containing a scalar identity ([14]). Polygroups are studied in [5, 6] were connections with color schemes, relational algebras, finite permutation groups and Pasch geometry.

Following the introduction of fuzzy set by L. A. Zadeh in 1965 ([20]), the fuzzy set theory developed by Zadeh himself and others in mathematics and many applied areas. Rosenfeld in 1971 defined and studied the concept of a fuzzy subgroups [19]. Zahedi and others introduced and study the notion of fuzzy hyper-algebraic structures (for example see [1, 2, 3, 8, 11, 13, 21]). In this note by considering the notion of polygroups, first we introduce the

2000 Mathematics Subject Classification: 20N20, 20N25

Keywords: (fuzzy) subpolygroup, fuzzy normal subpolygroup, fuzzy isomorphism, quotient of fuzzy subpolygroup.

notions of isomorphism, quotient and composition of fuzzy subpolygroups. Finally we study the relation of isomorphism and level subpolygroups.

2. Preliminaries

Let H be a nonempty set by $P_*(H)$ we mean the family of all nonempty subsets of H. A map $\cdot : H \times H \longrightarrow P_*(H)$ is called a *hyperoperation* or *join operation*. A *hypergroup* is a structure $(H, \cdot)$ that satisfies two axioms:

(Associativity) $a(bc) = (ab)c$ for all $a, b, c \in H$,

(Reproduction) $aH = H = Ha$ for all $a \in H$.

Let H be a hypergroup and K a nonempty subset of H. Then K is a *subhypergroup* of H if itself is a hypergroup under hyperoperation restricted to K. Hence it is clear that a subset K of H is a subhypergroup if and only if $aK = Ka = K$, under the hyperoperation on H (See [7]).

A hypergroup is called a *polygroup* if

(1) $\exists e \in H$ such that $e \circ x = x = x \circ e \forall x \in H$,

(2) $\forall x \in H$ there exists an unique element, say $x' \in H$ such that $e \in x \circ x' \cap x' \circ x$ (we denote x' by x^{-1}),

(3) $\forall x, y, z \in H$, $z \in xoy \implies x \circ y \implies x \in z \circ y^{-1} \implies y \in x^{-1} \circ z$.

A *canonical hypergroup* is a commutative polygroup. A nonempty subset A of a polygroup $(H, \cdot)$ is called a *subpolygroup* if $(A, \cdot)$ is itself a polygroup. In this case we write $A <_P H$. A subpolygroup A is called *normal* in H if

$$xNx^{-1} \subseteq N, \quad \forall x \in H.$$

In this case we write $N \lhd_P H$.

Lemma 2.1 [21]. *Let $A <_P H$. Then*

(1) $\forall a \in A \ Aa = aA = A$,

(2) $AA = A$,

(3) $(a^{-1})^{-1} = a$.

Lemma 2.2 [6]. *Let $N \lhd_P H$. Then*

(1) $Na = aN \ \forall a \in H$,

(2) $(Na)(Nb) = Nab$.

Let $A \leq_P H$, $x \in H$. Then Ax is called a *right coset* of A and we denote the set of all right costs of A in H by H/A, that is $H/A = \{Ax \,|\, x \in H\}$.

Define on H/A two hyperoperations:

$$Ax \circ Ay = \{Az \,|\, z \in Ax \cdot Ay\}, \qquad Ax \otimes Ay = \{Az \,|\, z \in xy\}.$$

Lemma 2.3. *Let H be a polygroup and A a normal subpolygroup of H. Then $(H/A, \otimes)$ and $(H/A, \circ)$ are polygroups, which are coincide together.*

Proof. Indeed, for $x, y \in H$, we have $xN \odot yN = \{zN \,|\, z \in xy\} = xyN = \bigcup_{z\in xy} zN = xyN = xN \otimes yN$. □

Definition 2.4 [16]. Let H_1 and H_2 be two polygroups. A function $f : H_1 \longrightarrow H_2$ is called

(1) a *homomorphism* if $f(xy) \subseteq f(x)f(y)$,
(2) a *good homomorphism* if $f(xy) = f(x)f(y)$,
(3) a *homomorphism* of *type* 2, if $f^{-1}(f(x)f(y)) = f^{-1}f(xy)$,
(4) a *homomorphism* of *type* 3, if $f^{-1}(f(x)f(y)) = f^{-1}f(x)f^{-1}f(y)$,
(5) a *homomorphism* of *type* 4, if
$$f^{-1}(f(x)f(y)) = f^{-1}f(xy) = f^{-1}f(x)f^{-1}f(y),$$
(6) a *good isomorphism* if it is an isomorphism and good homomor–phism.

Proposition 2.5 [16]. *Every homomorphism (one-to-one homomorphism) of any of type* 1 *through* 4 *is a homomorphism (isomorphism).*

Definition 2.6. Let $(G, \cdot)$ be a group, $FS(G)$ the set of all fuzzy subset of G. Then $\mu \in FS(G)$ is a *fuzzy subgroup* of G if $\forall a, b \in G$ the following conditions are satisfied:

(i) $\mu(z) \geqslant min(\mu(x), \mu(y))$,
(ii) $\mu(x^{-1}) \geqslant \mu(x)$.

We denote the fuzzy subgroup μ by $\mu <_F G$.

Definition 2.7 [21]. Let $(H, \cdot)$ be a polygroup and $\mu \in FS(H)$. Then μ is a *fuzzy subpolygroup* of H if

(i) $\mu(z) \geqslant min(\mu(x), \mu(y)),\ \forall x, y \in H \ \text{ and } \ \forall z \in xy$,
(ii) $\mu(x^{-1}) \geqslant \mu(x)$.

In this case we write $\mu <_{FP} H$.

Definition 2.8. A fuzzy subpolygroup μ of H is called *fuzzy normal* if for every $x, y \in H$, $z \in xy$, $z' \in yx$ we have $\mu(z) = \mu(z')$. We denote this fact by $\mu \lhd_{FP} H$.

Lemma 2.9 [21]. *Let $\mu <_{FP} H$. Then*

(i) *$\mu(e) \geqslant \mu(x)$ for all $x \in H$,*
(ii) *$\mu(x^{-1}) = \mu(x)$ for all $x \in H$.*

Theorem 2.10 [21]. *Let μ be a fuzzy subset of H. Then $\mu <_{FP} H$ (resp. $\mu \lhd_{FP} H$) if and only if $\mu(e) \geqslant \mu(x)$ for all $x \in H$ and $\mu_t <_{FP} H$ (resp. $\mu_t \lhd_{FP} H$) for all $t \in [0, \mu(e)]$.*

Let $\mu \lhd_{FP} H$. Then we define fuzzy subset $x^{\hat{\mu}}$ by

$$x^{\hat{\mu}}(g) = \sup_{z \in x^{-1}g} \mu(z),$$

which is called a *fuzzy left coset* of μ. Similarly a fuzzy right coset, $\hat{\mu}_x$ of μ is defined.

Suppose that μ is a fuzzy subset of X. Then for $t \in [0,1]$ the *level subset* μ_t is defined by $\mu_t = \{x \in X \mid \mu(x) \geqslant t\}$. The *support* of μ, is defined by

$$Supp(\mu) = \{x \in H \mid \mu(x) > 0\}.$$

If G is a group and μ is a fuzzy subset of G, then we define μ^a as follows:

$$\mu^a = \{x \in G \mid \mu x = \mu a\}.$$

Also we define $a\mu^e$ and $\mu^a \mu^b$ by

$$a\mu^e = \{ax \mid x \in \mu^e\}, \quad \mu^a \mu^b = \{xy \mid x \in \mu^a, y \in \mu^b\}.$$

Theorem 2.11 [1]. *Let G be a group and μ be a fuzzy subset of G. Define $o_\mu : G \times G \longrightarrow P_*(G)$ by $ao_\mu b = \mu^a \mu^b$. Then o_μ is a hyperoperation on G. Moreover, if μ is a fuzzy normal subgroup of G, then (G, o_μ) is a polygroup.*

Extension Principal: Any function $f : X \longrightarrow Y$ induces two functions

$$f : FS(X) \longrightarrow FS(Y) \quad \text{and} \quad f^{-1} : FS(Y) \longrightarrow FS(X),$$

which are defined by

$$f(\mu)(y) = \sup\{\mu(x) \mid y = f(x)\}$$

for all $\mu \in FS(X)$, and

$$f^{-1}(\nu)(x) = \nu(f(x))$$

for all $\nu \in FS(Y)$.

3. Main results

In the sequel by H we mean a polygroup.

Theorem 3.1.

(*i*) *If $\mu <_{FP} H$, then $Supp(\mu) <_P H$.*

(*ii*) *If $\mu \lhd_{FP} H$, then $Supp(\mu) \lhd_P H$.*

Proof. It is easy to verify that $Supp(\mu) = \bigcup_{t \in Im(\mu)\setminus\{0\}} \mu_t$. Then, by Theorem 2.11 and the fact that the sets of level subsets of μ constitute a totally ordered set, $Supp(\mu)$ is a subpolygroup of H. □

Remark 3.2. The converse of Theorem 3.1 is not true. For example the set $H = \{e, a, b\}$ with the hyperoperation

$\cdot$	e	a	b
e	e	a	b
a	a	e	b
b	b	b	$\{e, a\}$

is a polygroup. Define a fuzzy subset μ on H by $\mu(e) = 1$, $\mu(a) = 1/4$, $\mu(b) = 1/3$. Then μ is a fuzzy subpolygroup, but $\mu_{1/3} = \{e, b\}$ is not a subhypergroup of H, since $b \in \mu_{1/3}$, but $b \cdot b = \{e, a\} \nsubseteq \mu_{1/3}$. Thus, by Theorem 2.15, $\mu_{1/3}$ is not a subpolygroup of H. So, $\mu_{1/3}$ is not normal in H, but $supp(\mu) = H$ is a normal subpolygroup of H.

Theorem 3.3. *Let H be a fuzzy polygroup and $\mu <_{FP} H$. Then the set $\mathcal{I}_\mu = \{x^{\hat{\mu}} \,|\, x \in H\}$ with the hyperoperation $x^{\hat{\mu}} \cdot y^{\hat{\mu}} = \{z^{\hat{\mu}} \,|\, z \in xy\}$ is a polygroup.*

Proof. The associativity immediately follows from the associativity. Obviously $e^{\hat{\mu}}$ is the identity element. The inverse of $x^{\hat{\mu}}$ is $(x^{-1})^{\hat{\mu}}$. Now, if $x^{\hat{\mu}}, y^{\hat{\mu}}, z^{\hat{\mu}} \in \mathcal{I}_\mu$, then from $z^{\hat{\mu}} \in x^{\hat{\mu}} \cdot y^{\hat{\mu}}$ it is concluded that $z \in xy$. Thus $x \in zy^{-1}$ and hence $x^{\hat{\mu}} \in (x^{-1})^{\hat{\mu}} \cdot y^{\hat{\mu}}$. Therefore $\mathcal{I}_\mu$ is a polygroup. □

Definition 3.4. Let $\mu <_{FP} H$. Then μ is called *Abelian* if μ_t is Abelian (or a canonical hypergroup) for every $t \in [0, \mu(e)]$.

Theorem 3.5. *Let $\mu <_{FP} H$. Then μ is Abelian if and only if $Supp(\mu)$ is Abelian.*

Proof. Suppose that $Supp(\mu)$ is Abelian. Then for every $t \in (0, \mu(e)]$ we have $\mu_t \subseteq Supp(\mu)$. Thus μ_t is Abelian for every $t \in [0, \mu(e)]$. Therefore μ is Abelian.

Conversely, suppose that for every $t \in (0, \mu(e)]$, μ_t is Abelian. Let $a, b \in Supp(\mu)$. Thus there are μ_{t_1} and μ_{t_2} such that $a \in \mu_{t_1}$ and $b \in \mu_{t_2}$, $t_1, t_2 \in (0, \mu(e)]$. Suppose that $t_1 \leqslant t_2$, then $\mu_{t_2} \leqslant \mu_{t_1}$, and hence $a, b \in \mu_{t_1}$. Thus $ab = ba$. This complete the proof. □

Definition 3.6. Let H_1 and H_2 be polygroups. If $\mu <_{FP} H_1$ and $\nu <_{FP} H_2$, then a good isomorphism $f : Supp(\mu) \longrightarrow Supp(\nu)$ is called a *fuzzy good isomorphism* from μ to ν if there exists a positive real number k such that

$$\mu(x) = k\nu(f(x)), \quad \forall x \in Supp(\mu) \setminus \{e\}.$$

In this case we write $\mu \simeq \nu$ and say that μ and ν are isomorphic. It is clear that $\simeq$ is an equivalence on the set of all fuzzy subpolygroups of H.

Remark 3.7. Note that if two fuzzy polygroups are isomorphic it dose not imply that the underling polygroups are being isomorphic. For instance consider $S_3 = \{e, a, a^2, b, ab, a^2b\}$ and $Z_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Define the fuzzy subsets μ and ν on S_3 and Z_6 respectively as follows:

$$\mu(e) = 1, \mu(a) = 1/2 = \mu(a^2), \mu(b) = 0 = \mu(ab) = \mu(b^2),$$
$$\nu(\overline{0}) = 1, \nu(\overline{2}) = 1/3 = \nu(\overline{4}), \nu(\overline{1}) = \nu(\overline{5}) = \nu(\overline{3}) = 0.$$

Then $(S_3, \circ_\mu)$ and $(Z_6, \circ_\nu)$ are polygroups by Theorem 2.14.

Now we define the mapping $f : Supp(\mu) \longrightarrow Supp(\nu)$ by $f(e) = \overline{0}$, $f(a) = \overline{2}$, $f(a^2) = \overline{4}$. It is easy to verify that $\mu \simeq \nu$, $\mu <_{FP} S_3$ and $\mu <_{FP} Z_6$. Thus $\mu \simeq \nu$, but $(S_3, o_\mu) \not\simeq (Z_6, o_\nu)$.

Theorem 3.8. Let $\mu <_{FP} H_1$ and $\nu <_{FP} H_2$. If $\mu \simeq \nu$, then μ is Abelian if and only if ν is Abelian.

Proof. Let μ be Abelian. We show that also ν is Abelian. By Theorem 3.6 it is enough we show that $Supp(\nu)$ is Abelian. Let $x, y \in Supp(\nu)$. Then there are $a, b \in Supp(\mu)$ such that $x = f(a)$ and $y = f(b)$. On the other hand by hypothesis there exists a positive number k such that

$$\mu(a) = k\nu(f(a)), \quad \mu(b) = k\nu(f(b)).$$

Since $k > 0$, then $\nu(f(a)) > 0$, so $\mu(a) > 0$, $\mu(b) > 0$ and, in the consequence $a, b \in Supp(\mu)$. Thus $ab = ba$ and $f(ab) = f(ba)$. Then $f(a)f(b) = f(b)f(a)$. Thus $xy = yx$. Therefore ν is Abelian.

Conversely, suppose that ν is Abelian. Let $a, b \in Supp(\mu)$. Then $f(a), f(b) \in Supp(\nu)$, henceforth $f(a)f(b) = f(b)f(a)$, that is $ab = ba$. Therefore ν is fuzzy Abelian. □

Theorem 3.9. *Let $\mu <_{FP} H_1$ and $\nu <_{FP} H_2$. If $\mu \simeq \nu$, then for every $t \in (0, \mu(e)]$ there exists an element $s \in (0, \nu(e)]$ such that $\mu_t \simeq \nu_s$.*

Proof. Let $f : Supp(\mu) \longrightarrow Supp(\nu)$ be a fuzzy isomorphism such that $\mu(x) = k\nu(f(x))$ for all $x \in Supp(\mu) \setminus \{e\}$ and for some positive real number k. Let $s = t/k$. Consider $g : \mu_t \longrightarrow \nu_s$, as the restriction of f to μ_t. Let $x \in \mu_t$, then $\mu(x) \geqslant t$, and hence $k\nu(f(x)) \geqslant t$. Thus $f(x) \in \nu_s$ and so g is well-defined. Clearly g is injective and $g(ab) = g(a)g(b)$, $\forall a, b \in \mu_t$. Now suppose that $y \in \nu_s$. Then $\nu(y) \geqslant s$. On the other hand there exists an element $x \in Supp(\mu)$ such that $y = f(x)$, thus $k\nu(f(x)) \geqslant t$, and hence $x \in \nu_t$. Therefore g is surjective and hence $\mu_t \simeq \nu_s$. □

Theorem 3.10. *Let $\mu <_{FP} H_1$, $\nu <_{FP} H_2$, $\mu \simeq \nu$ and $\mu \lhd_{FP} supp(\mu)$. Then $\nu \lhd_{FP} supp(\nu)$.*

Proof. We must prove that for all $x, y \in Supp(\nu)$ we have:

$$\nu(z) = \nu(z') \ \ \forall z \in xy, \ z' \in yx.$$

For $x, y \in Supp(\nu)$ there are $a, b \in Supp(\mu)$ such that $f(a) = x$, $f(b) = y$. Then $xy = f(ab)$ and $yx = f(ba)$. Now let $z \in xy = f(ab)$ and $z' \in yx = f(ba)$, thus there are $t, t' \in Supp(\nu)$ such that $z = f(t)$, $z' = f(t')$, hence $t' \in ba$ and, by hypothesis, $\mu(t) = \mu(t')$. But we have $\mu(t) = k\nu(z)$ and $\mu(t') = k\nu(z')$. Thus $\nu(z) = \nu(z')$. Therefore μ is fuzzy normal. □

Definition 3.11. Let $\mu <_{FP} H_1$, $\nu <_{FP} H_2$ and $Supp(\mu) \subseteq Supp(\nu)$. We define the quotient of μ/ν as follows:

$$\mu/\nu : H/Supp(\nu) \longrightarrow [0,1],$$
$$(\mu/\nu)(xSupp(\nu)) = Sup\{\mu(a) \mid aSupp(\nu) = xSupp(\nu)\}.$$

Remark 3.12. Note that in general $\mu_1/\nu = \mu_2/\nu$ dose not implies that $\mu_1 = \mu_2$. For example, consider the polygroup $H = \{e, a, b\}$ from Remark 3.2 and define the fuzzy subsets μ_1 and μ_2 on H as follows:

$$\mu_1(e) = 1, \ \mu_1(a) = 1/2, \ \mu_1(b) = 1/4,$$

and

$$\mu_2(e) = 1, \ \mu_2(a) = 1/3, \ \mu_2(b) = 1/4,$$

and

$$\nu(e) = 1, \ \nu(a) = 1/4, \ \nu(b) = 0.$$

Clearly $\mu_1, \mu_2 <_{FP} H$, $\nu \unlhd H$ and $\mu_1/\nu = \mu_2/\nu$, but $\mu_1 \neq \mu_2$.

Theorem 3.13. *If $\mu <_{FP} H_1$, then $\mu/\mu_e \simeq \mu$ and $\mu/\mu \simeq \mu_e$, where $\mu_e(t) = \mu(e)$, if $t = e$ and 0, otherwise.*

Proof. Define $f : Supp(\mu/\mu_e) \longrightarrow Supp(\mu)$ putting $f(xSupp(\mu_e)) = x$. Since $Supp(\mu_e) = \{e\}$ and $\mu/\mu_e(xSupp(\mu_e)) = \mu(x)$, then we conclude that f is a fuzzy isomorphism. Now define $g : Supp(\mu_e) \longrightarrow Supp(\mu/\mu)$, by $g(e) = Supp(\mu)$. Clearly $\mu(e) = (\mu/\mu)(g(e))$. Thus $\mu/\mu \simeq \mu_e$. □

Proposition 3.14. *Let H be a polygroup and N its normal subpolygroup. Then the map $\phi_H : H \longrightarrow (H/N, \circ)$ defined by $\phi_H(x) = xN$ is an onto homomorphism of type 3.*

Proof. Clearly ϕ_H is onto. In view of Definition 2.5 we must show that

$$\phi_H^{-1}(\phi_H(x)) \circ \phi_H(y)) = \phi_H^{-1}(\phi_H(x)) \circ \phi_H^{-1}(\phi_H(y)) \ \ \forall x, y \in H.$$

Let $t \in \phi_H^{-1}(\phi_H(x) \circ \phi_H(y))$, then $\phi_H(t) \in \phi_H(x) \circ \phi_H(y)$, yields $t \in xy$ by Lemma 2.4, and hence $t \in \phi_H^{-1}(\phi_H(x)) \circ \phi_H^{-1}(\phi_H(y))$.

Conversely, suppose that $z \in \phi_H^{-1}(\phi_H(x)) \circ \phi_H^{-1}(\phi_H(y)$. Then there exist $u \in \phi_H^{-1}(\phi_H(x))$ and $v \in \phi_H^{-1}(\phi_H(y))$ such that $z \in uv$. Thus $\phi_H(z) \subseteq \phi_H(uv) \subseteq \phi_H(u) \circ \phi_H(v) = \phi_H(x) \circ \phi_H(y)$. Therefore $z \in \phi_H^{-1}(\phi_H(x)) \circ \phi_H^{-1}(\phi_H(y))$. So, ϕ_H is a homomorphism of type 3. □

The map ϕ_H is called a *canonical epimorphism* and for simplicity will be denoted by ϕ.

Let μ be a fuzzy subpolygroup of H and N its normal subpolygroup. Then we can define on H/N the fuzzy set $\overline{\mu}$ putting

$$\overline{\mu}(z) = \sup_{xN=zN} \mu(x).$$

In fact, by the principal extension, we have $\overline{\mu} = \phi(\mu)$. So, from just proved results we conclude

Corollary 3.15. *Let $\mu <_{FP} H_1$, $\nu <_{FP} H_2$ and $Supp(\mu) \subseteq Supp(\nu)$. Then $\phi(\mu) = \mu/\nu$, where $\phi : H \longrightarrow H/Supp(\nu)$ is the canonical epimorphism.* □

The composition of fuzzy subpolygroups μ and ν of H is defined by

$$\mu\nu(x) = \sup_{x \in uv} min(\mu(u), \nu(v)).$$

Lemma 3.16. *If $\mu \leqslant_F PH$, then $\mu^2 = \mu$, and hence $\mu^n = \mu$.*

Proof. For every $x \in H$ we have $\mu^2(x) = \sup\limits_{x \in uv} min(\mu(u), \mu(v)) \leqslant \mu(x)$, since μ is a fuzzy polygroup. On the other hand, $\mu^2(x) \geqslant min(\mu(x), \mu(e)) = \mu(x)$. Thus $\mu^2 = \mu$ and, by induction, $\mu^n = \mu$. □

Theorem 3.17. *Let $\mu \in FS(H)$. Then μ is a fuzzy subpolygroup of H if and only if $\mu^2 = \mu$ and $\mu(x) = \mu(x^{-1})$ for all $x \in H$.*

Proof. If μ is a fuzzy subpolygroup, then by Lemma 3.16 and Definition 2.8 we have $\mu(x) = \mu(x^{-1})$ for all $x \in H$.

Conversely, let $x \in uv$. Then by the hypothesis we have

$$\mu(x) = \mu^2(x) = \sup_{x \in uv} min(\mu(u), \mu(v)) \geqslant min(\mu(u), \mu(v)).$$

Thus μ is a fuzzy subpolygroup of H. □

Corollary 3.18. *If μ and ν are fuzzy subpolygroups of H and $\nu_t \trianglelefteq \mu_t$, for all $t \in Im(\mu)$, then $Supp(\mu) \trianglelefteq Supp(\nu)$.* □

Proposition 3.19. *Let μ and ν are fuzzy subpolygroups of H such that $\mu\nu = \nu\mu$. Then $\mu\nu$ is a fuzzy subpolygroup of H.*

Proof. First we show that $\mu\nu(x) = \mu\nu(x^{-1})$. Indeed,

$$\begin{aligned}\mu\nu(x) &= \sup_{x\in x_1x_2}(\mu(x_1)\mu(x_2)) = \sup_{x^{-1}\in x_2^{-1}x_1^{-1}} min(\mu(x_1),\nu(x_2))\\ &= \sup_{x^{-1}\in x_2^{-1}x_1^{-1}} min(\nu(x_1),\mu(x_2)) = \nu\mu(x^{-1}) = \mu\nu(x^{-1}).\end{aligned}$$

On the other hand $\mu\nu = \mu^2\nu^2 = \mu[(\mu\nu)\nu] = \mu[(\nu\mu)\nu] = (\mu\nu)(\mu\nu) = (\mu\nu)^2$. Then, by Theorem 3.17, $\mu\nu$ is a fuzzy subpolygroup. □

Proposition 3.20. *If $\mu \leqslant_{FP} H$ and $K \trianglelefteq H$. Define $\nu(x) = \mu(x)$, if $x \in K$ and $\nu(x) = 0$ otherwise. Then $\nu_t \trianglelefteq \mu_t$ for all $t \in (0, 1]$.*

Proof. We must show that $x\nu_tx^{-1} \subseteq \nu_t$, $\forall x \in \mu_t$ and $\forall t \in (0, 1]$.

Let $z \in xax^{-1} \subseteq x\nu_tx^{-1}$. If $a \notin K$, then $\nu(a) = 0 \geqslant t > 0$, which is a contradiction. Thus $a \in K$ and hence $\mu(a) = \nu(a) \geqslant t$.

If $a \in K$, then $\mu(a) = \nu(a)$ and $\mu(z) \geqslant min(\mu(x), \mu(a)) \geqslant t$. Hence $\nu(z) \geqslant t$, i.e. $z \in \nu_t$. Therefore $\nu_t \trianglelefteq \mu_t$. □

Acknowledgment. This research supported by the program "studies and researches between universities" project No. 31303386.

References

[1] **R. Ameri, M. M. Zahedi**: *Hypergroup and join spaces induced by a fuzzy subset*, PU.M.A. **8** (1997), 155 – 168.

[2] **R. Ameri**: *Fuzzy transposition hypergrouyps*, Italian J. Pure and Appl. Math. (to appear).

[3] **R. Ameri, M. M. Zahedi**: *Fuzzy subhypermodules over hyperrings*, Proc. Sixth Intern. Congress on Algebraic Hyperstructures and Applications, Prague 1996, 1 – 14.

[4] **P. Bonasinga, P. Corsini**: *Sugil omomorphismi di semi-ipergrupi e di ipergruppi*, Bull. U.M.I. (6)1-B (1982), 717 – 727.

[5] **D. S. Comer**: *Polygroups derived from cogorups*, J. Algebra **89** (1984), 397 – 405.

[6] **D. S. Comer**: *Combinatorial aspect of relations*, Algebra Universalis **18** (1984), 77 – 94.

[7] **P. Corsini**: *Prolegomena of Hypergroup Theory*, second eddition, Aviani 1993.

[8] **P. Corsini**: *Join space, power setes, fuzzy sets*, Proc. Fifth Intern. Congress on Algebraic Hyper-structures and Applications, 1993, Iasi, Romania, Hardonic Press 1994.

[9] **P. Corsini**: *Fuzzy sets, join spaces and factor spaces*, PU.M.A. **11** (2000), 439 – 446.

[10] **P. S. Das**: *Fuzzy groups and level subgroups*, J. Math. Anal. Appl. **84** (1981), 264 – 269.

[11] **B. Davvaz**: *Fuzzy H_v- groups and anti fuzzy H_v-subgroups*, Fuzzy Sets Systems **101** (1999), 191 – 195.

[12] **D. K. Harrison**: *Double coset and orbit spaces*, Pasific J. Math. **80** (1979), 451 – 491.

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

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

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

[16] **J. Jantociak**: *Homomorphisms, equivalences and reductions in hypergroups*, Rivista di Mat. Pure ed Appl. **9** (1991), 23 – 47.

[17] **B. B. Makumba**: *Studies in fuzzy groups*, Ph.D Thesis, Rhodes University, 1992.

[18] **F. Marty**: *Sur une generalization de la notion de group*, $8^i em$ Congr. Math. Scandinaves, Stockholm, 1934. 45 – 49.

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

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

[21] **M. Zahedi, M. Bolurian, A. Hasankhani**: *On polygroups and fuzzy subpolygroups*, J. Fuzzy Math. **1** (1995), 1 – 15.

Department of Mathematics
Faculty of Basic Science
University of Mazandaran
Babolsar
Iran
e-mail: ameri@umz.ac.ir

Received June 4, 2004
Revised April 6, 2005

Quasigroups and Related Systems **13** (2005), 185 – 191

On graded weakly primary ideals

Shahabaddin Ebrahimi Atani

Abstract

Let G be an arbitrary monoid with identity e. Weakly prime ideals in a commutative ring with non-zero identity have been introduced and studied in [1]. Here we study the graded weakly primary ideals of a G-graded commutative ring. Various properties of graded weakly primary ideals are considered. For example, we show that an intersection of a family of graded weakly primary ideals such that their homogeneous components are not primary is graded weakly primary.

1. Introduction

Weakly prime ideals in a commutative ring with non-zero identity have been introduced and studied by D. D. Anderson and E. Smith in [1]. Also, weakly primary ideals in a commutative ring with non-zero identity have been introduced and studied in [2]. Here we study the graded weakly primary ideals of a G-graded commutative ring. In this paper we introduce the concepts of graded weakly primary ideals and the structures of their homogeneous components. A number of results concerning graded weakly primary ideals are given. In section 2, we introduce the concepts primary and weakly primary subgroups (resp. submodules) of homogeneous components of a G-graded commutative ring. Also, we first show that if P is a graded weakly primary ideal of a G-graded commutative ring, then for each $g \in G$, either P_g is a primary subgroup of R_g or $P_g^2 = 0$. Next, we show that if P and Q are graded weakly primary ideals such that P_g and Q_h are not primary for all $g, h \in G$ respectively, then $\mathrm{Grad}(P) = \mathrm{Grad}(Q) = \mathrm{Grad}(0)$ and $P + Q$ is a graded weakly primary ideal of $G(R)$. Moreover, we give two other characterizations of homogeneous components of graded ideals.

2000 Mathematics Subject Classification:Primary: 13A02, 16W50
Keywords:Graded ring, graded weakly primary ideals.

Before we state some results let us introduce some notation and terminology. Let G be an arbitrary monoid with identity e. By a *G-graded commutative ring* we mean a commutative ring R with non-zero identity together with a direct sum decomposition (as an additive group) $R = \underset{g\in G}{\oplus} R_g$ with the property that $R_gR_h \subseteq R_{gh}$ for all $g, h \in G$; here R_gR_h denotes the additive subgroup of R consisting of all finite sums of elements r_gs_h with $r_g \in R_g$ and $s_h \in R_h$. We consider supp$R = \{g \in G : R_g \neq 0\}$. The summands R_g are called *homogeneous components* and elements of these summands are called *homogeneous elements.* If $a \in R$, then a can be written uniquely as $\sum_{g\in G} a_g$ where a_g is the component of a in R_g. Also, we write $h(R) = \cup_{g\in G}R_g$. Moreover, if $R = \underset{g\in G}{\oplus} R_g$ is a graded ring, then R_e is a subring of R, $1_R \in R_e$ and R_g is an R_e-module for all $g \in G$.

Let I be an ideal of R. For $g \in G$, let $I_g = I \cap R_g$. Then I is a graded ideal of R if $I = \underset{g\in G}{\oplus} I_g$. In this case, I_g is called the *g-component* of I for $g \in G$. Moreover, R/I becomes a G-graded ring with g-component $(R/I)_g = (R_g + I)/I \cong R_g/I_g$ for $g \in G$. Clearly, 0 is a graded ideal of R. A graded ideal I of R is said to be *graded prime ideal* if $I \neq R$; and whenever $ab \in I$, we have $a \in I$ or $b \in I$, where $a, b \in h(R)$. The *graded radical* of a graded ideal I of R, denoted by Grad(I), is the set of all $x \in R$ such that for each $g \in G$ there exists $n_g > 0$ with $x_g^{n_g} \in I$. Note that, if r is a homogeneous element of R, then $r \in$ Grad(I) if and only if $r^n \in I$ for some positive integer n. We say that a graded ideal I of R is a *graded primary ideal* of R if $I \neq R$; and whenever $a, b \in h(R)$ with $ab \in I$ then $a \in I$ or $b \in$ Grad(I) (see [4]).

2. Weakly primary subgroups

Let I be a graded ideal of R and $x \in G$. The set

$$\{a \in R_x : a^n \in I \text{ for some positive integer } n\}$$

is a subgroup of R_x and is called the *x-radical* of I, denoted by xrad(I). Clearly, $I_x \subseteq$ xrad(I) and If $r \in R_x$ with $r \in$ Grad(I), then $r \in$ xrad(I). Our starting point is the following definitions:

Definition 2.1. Let P be a graded ideal of R and $g \in G$.

(i) We say that P_g is a *primary subgroup* of R_g if $P_g \neq R_g$; and whenever $a, b \in R_g$ with $ab \in P_g$, then either $a \in P_g$ or $b \in$ grad(P).

(ii) We say that P_g is a *weakly primary subgroup* of R_g if $P_g \neq R_g$; and whenever $a, b \in R_g$ with $0 \neq ab \in P_g$, then either $a \in P_g$ or $b \in \mathrm{grad}(P)$.

(iii) We say that P_g is a *primary submodule* of the R_e-module R_g if $P_g \neq R_g$; and whenever $a \in R_g$, $b \in R_e$ with $ab \in P_g$, then either $a \in P_g$ or $b^n \in (P_g :_{R_e} R_g)$ for some positive integer n (that is, $b \in \mathrm{erad}(P_g :_{R_e} R_g)$).

(iv) We say that P_g is a *weakly primary submodule* of the R_e-module R_g if $P_g \neq R_g$; and whenever $a \in R_g$, $b \in R_e$ with $0 \neq ab \in P_g$, then either $a \in P_g$ or $b^n \in (P_g :_{R_e} R_g)$ for some positive integer n (that is, $b \in \mathrm{erad}(P_g :_{R_e} R_g)$).

(v) We say that P is a *graded weakly primary ideal* of R if $P \neq R$; and whenever $a, b \in h(R)$ with $0 \neq ab \in P$, then either $a \in P$ or $b \in \mathrm{Grad}(P)$.

Clearly, a graded primary ideal of R is a graded weakly primary ideal of R. However, since 0 is always a graded weakly primary (by definition), a graded weakly primary ideal need not be graded primary.

Lemma 2.2. *Let $P = \underset{g\in G}{\oplus} P_g$ be a graded weakly primary ideal of R. Then the following hold:*

(i) *P_g is a weakly primary subgroup of R_g for every $g \in G$.*

(ii) *P_g is a weakly primary submodule of R_g for every $g \in G$.*

Proof. (i) For $g \in G$, assume that $0 \neq ab \in P_g \subseteq P$ where $a, b \in R_g$, so either $a \in P$ or $b^n \in P$ for some positive integer n since P is graded weakly primary. It follows that either $a \in P_g$ or $b \in P_{g^n}$ for some n; hence either $a \in P_g$ or $b \in \mathrm{grad}(P)$.

(ii) Suppose that P is a graded weakly primary ideal of R. For $g \in G$, assume that $0 \neq ab \in P_g \subseteq P$ where $a \in R_g$ and $b \in R_e$, so P graded weakly primary gives either $a \in P$ or $b \in \mathrm{Grad}(P)$. As b is a homogeneous element, either $a \in P$ or $b^m \in P$ for some m. If $a \in P$, then $a \in P_g$. If $b^m \in P$, then $b^m R_g \subseteq P_g$. So P_g is weakly primary. □

Proposition 2.3. *Let P be a graded weakly primary ideal of R and $g \in G$. Then the following hold:*

(i) *For $a \in R_g - \mathrm{grad}(P)$, either $\mathrm{erad}(P_g :_{R_e} a) = \mathrm{erad}(P)$ or $\mathrm{erad}(P_g :_{R_e} a) = (0 :_{R_e} a)$.*

(ii) *For $a \in h(R) - P$, $\mathrm{Grad}(P :_R a) = \mathrm{Grad}P + (0 :_R a)$.*

Proof. (i) It is well-known that if an ideal (resp. a subgroup) is the union of two ideals (resp. two subgroups), then it is equal to one of them, so for $a \in R_g - \mathrm{grad}(P)$, it is enough to show that

$$\mathrm{erad}(P_g :_{R_e} a) = \mathrm{erad}(P) \cup (0 :_{R_e} a) = H.$$

If $b \in \mathrm{erad}(P)$, then $ab^n \in R_g \cap P = P_g$, so $b^n \in (P_g :_{R_e} a)$; hence $b \in \mathrm{erad}(P_g :_{R_e} a)$. Clearly, $(0 :_{R_e} a) \subseteq \mathrm{erad}(P_g :_{R_e} a)$. Thus, $H \subseteq \mathrm{erad}(P_g :_{R_e} a)$. For the reverse inclusion, assume that $c \in \mathrm{erad}(P_g :_{R_e} a)$. Then $ac^m \in P_g$ for some m. If $0 \neq ac^m \in P_g \subseteq P$, then P graded weakly primary gives $c^m \in P$; hence $c \in \mathrm{erad}(P) \subseteq H$. If $ac^m = 0$, then assume that k is the smallest integer with $ac^k = 0$. If $k = 1$, then $c \in (0 :_{R_e} a) \subseteq H$. Otherwise, $c \in \mathrm{erad}(P) \subseteq H$, we have equality.

(ii) Clearly, for $a \in h(R) - P$, $\mathrm{Grad}(P) + (0 :_R a) \subseteq \mathrm{Grad}(P :_R a)$. For the other containment, assume that $b \in \mathrm{Grad}(P :_R a)$ where $a \in h(R) - P$.

Without loss of generality assume $b = \sum_{i=1}^{n} b_{g_i}$ where $b_{g_i} \neq 0$ for all $i = 1, \dots, n$ and $b_g = 0$ for all $g \notin \{g_1, \dots, g_n\}$. As $b \in \mathrm{Grad}(P :_R a)$, for each i, there exists a positive integer m_{g_i} such that $b_{g_i}^{m_{g_i}} a \in P$. If $b_{g_i}^{m_{g_i}} a \neq 0$, then $b_{g_i}^{m_{g_i}} \in \mathrm{Grad}(P)$ since P is graded weakly primary. Therefore, $b_{g_i} \in \mathrm{Grad}(\mathrm{Grad}(P)) = \mathrm{Grad}(P)$ by [4, Proposition 1.2]. So suppose that $b_{g_i}^{m_{g_i}} a = 0$ for some i. Then assume that s_{g_i} is the smallest integer with $b_{g_i}^{s_{g_i}} a = 0$. If $s_{g_i} = 1$, then $b_{g_i} \in (0 :_R a)$. Otherwise, $b_{g_i} \in \mathrm{Grad}(P)$, so $b \in \mathrm{Grad}(P) + (0 :_R a)$, as required. □

Proposition 2.4. *Let* $P = \bigoplus_{g \in G} P_g$ *be a graded weakly primary ideal of* R. *Then for each* $g \in G$, *either* $(P_g :_{R_e} R_g)P_g = 0$ *or* P_g *is a primary submodule of* R_g.

Proof. By Lemma 2.2, P_g is a weakly primary submodule of R_g for every $g \in G$. It is enough to show that if $(P_g :_{R_e} R_g)P_g \neq 0$ for some $g \in G$, then P_g is primary. Let $ab \in P_g$ where $a \in R_g$ and $b \in R_e$. If $ab \neq 0$, then either $a \in P_g$ or $b^n \in (P_g :_{R_e} R_g)$ for some n since P_g is weakly primary. So suppose that $ab = 0$. First suppose that $bP_g \neq 0$, say $bc \neq 0$ where $c \in P_g$. Then $0 \neq bc = b(c + a) \in P_g$, so either $b^m \in (P_g :_{R_e} R_g)$ for some m or $(a + c) \in P_g$. As $c \in P_g$ we have either $b^m \in (P_g :_{R_e} R_g)$ or $a \in P_g$. So we can assume that $bP_g = 0$. Suppose that $a(P_g :_{R_e} R_g) \neq 0$, say $ad \neq 0$ where $d \in (P_g :_{R_e} R_g)$. Then $0 \neq ad = a(d + b) \in P_g$, so either $a \in P_g$ or $(d + b)^s \in (P_g :_{R_e} R_g)$ for some s. It follows that either $a \in P_g$

or $b^s + r \in (P_g :_{R_e} R_g)$ where $r \in (P_g :_{R_e} R_g)$. Thus, either $a \in P_g$ or $b^s \in (P_g :_{R_e} R_g)$. So we can assume that $a(P_g :_{R_e} R_g) = 0$.

Since $(P_g :_{R_e} R_g)P_g \neq 0$, there exist $u \in (P_g :_{R_e} R_g)$ and $v \in P_g$ such that $uv \neq 0$. Then $(b+u)(a+v) = uv \in P_g$, so either $(b+u)^n \in (P_g :_{R_e} R_g)$ for some n or $a+v \in P_g$, and hence either $b^n \in (P_g :_{R_e} R_g)$ or $a \in P_g$. Thus P_g is primary. □

We next give two other characterizations of homogeneous components of graded ideals.

Theorem 2.5. *Let P be a graded ideal of R and $g \in G$. Then the following assertion are equivalent.*

(*i*) *P_g is a weakly primary submodule of R_g.*

(*ii*) *For $a \in R_g - \operatorname{grad}(P)$, $\operatorname{erad}(P_g :_{R_e} a) = \operatorname{erad}(P_g :_{R_e} R_g) \cup (0 :_{R_e} a)$.*

(*iii*) *For $a \in R_g - \operatorname{erad}(P)$, $\operatorname{erad}(P_g :_{R_e} a) = \operatorname{erad}(P_g :_{R_e} R_g)$ or $\operatorname{erad}(P_g :_{R_e} a) = (0 :_{R_e} a)$.*

Proof. (*i*) ⇒ (*ii*) Suppose first that P_g is a weakly primary submodule of R_g. Clearly, if $a \in R_g - \operatorname{grad}(P)$, then $H = \operatorname{erad}(P_g :_{R_e} R_g) \cup (0 :_{R_e} a) \subseteq \operatorname{erad}(P_g :_{R_e} a)$. Let $b \in \operatorname{erad}(P_g :_{R_e} a)$ where $a \in R_g - \operatorname{grad}(P)$. Then $ab \in P_g$. If $ab \neq 0$, then $b^n \in (P_g :_{R_e} R_g)$ for some n since $a \notin \operatorname{grad}(P) \supseteq P_g$ and P_g is weakly primary, so $b \in \operatorname{erad}(P_g :_{R_e} R_g) \subseteq H$. If $ab = 0$, then $b \in (0 :_{R_e} a) \subseteq H$, and hence we have equality.

(*ii*) ⇒ (*iii*) Is obvious.

(*iii*) ⇒ (*i*) Suppose that $0 \neq ab \in P_g$ with $b \in R_e$ and $a \in R_g - P_g$. Then $b \in (P_g :_{R_e} a) \subseteq \operatorname{erad}(P_g :_{R_e} a)$ and $b \notin (0 :_{R_e} a)$. It follows from (ii) that $b \in \operatorname{erad}(P_g :_{R_e} R_g)$, as required. □

Theorem 2.6. *Let $P = \bigoplus_{g\in G} P_g$ be a graded weakly primary ideal of R. Then for each $g \in G$, either P_g is a primary subgroup of R_g or $P_g^2 = 0$.*

Proof. By Lemma 2.2, P_g is a weakly primary subgroup of R_g for every $g \in G$. It is enough to show that if $P_g^2 \neq 0$ for some $g \in G$, then P_g is a primary subgroup of R_g. Let $ab \in P_g$ where $a, b \in R_g$. If $ab \neq 0$, then P_g weakly primary gives either $a \in P_g$ or $b \in \operatorname{grad}(P)$. So suppose that $ab = 0$. If $aP_g \neq 0$, then there is an element c of P_g such that $ac \neq 0$, so $0 \neq ac = a(c + b) \in P$; hence either $a \in P$ or $(c + b) \in \operatorname{Grad}(P)$. As $c \in P \subseteq \operatorname{Grad}(P)$ (by [4, Proposition 1.2]), we have either $a \in P_g$ or

$b \in \text{Grad}(P)$; hence either $p \in P_g$ or $b \in \text{grad}(P)$. So we can assume that $aP_g = 0$. Similarly, we can assume that $bP_g = 0$. Since $P_g^2 \neq 0$, there exist $p, q \in P_g \subseteq P \subseteq \text{Grad}(P)$ such that $pq \neq 0$. Then $(a+p)(b+q) = pq \in P$, so either $a+p \in P$ or $b+q \in \text{Grad}(P)$, and hence either $a \in P_g$ or $b \in \text{grad}(P)$. Thus P_g is primary. □

Proposition 2.7. *Let $P = \bigoplus_{g \in G} P_g$ be a graded weakly primary ideal of R such that P_g is not a primary subgroup of R_g for every $g \in G$. Then* $\text{Grad}(P) = \text{Grad}(0)$.

Proof. Clearly, $\text{Grad}(0) \subseteq \text{Grad}(P)$. For the other containment, assume that $a \in P$. By Theorem 2.6, $a_g^2 = 0 \in (0)$ for every $g \in G$, so $a \in \text{Grad}(0)$; hence $P \subseteq \text{Grad}(0)$. It follows that $\text{Grad}(P) \subseteq \text{Grad}(0)$ by [4, Proposition 1.2], as needed. □

Theorem 2.8. *Let $\{P_i\}_{i \in I}$ be a family of graded weakly primary ideals of R such that for each $i \in I$, $(P_i)_g$ is not a primary subgroup of R_g for every $g \in G$. Then $P = \bigcap_{i \in I} P_i$ is a graded weakly primary ideal of R.*

Proof. First, we show that $\text{Grad}(P) = \bigcap_{i \in I} \text{Grad}(P_i)$. Clearly, $\text{Grad}(P) \subseteq \bigcap_{i \in I} \text{Grad}(P_i)$. For the reverse inclusion, suppose that $a \in \bigcap_{i \in I} \text{Grad}(P_i)$, so for each $g \in G$, $a_g^{m_g} = 0$ for some m_g since $\bigcap_{i \in I} \text{Grad}(P_i) = \text{Grad}(0)$ by Proposition 2.7. It follows that for each $i \in I$, $a_g^{m_g} \in P_i$ for every $g \in G$, and hence $a \in \text{Grad}(P)$.

As $\text{Grad}(P) = \text{Grad}(0) \neq R$, we have P is a proper ideal of R. Suppose that $a, b \in h(R)$ are such that $0 \neq ab \in P$ but $b \notin P$. Then there is an element $j \in I$ such that $b \notin P_j$ and $ab \in P_j$. It follows that $a \in \text{Grad}(P_j) = \text{Grad}(P)$ since P_i is graded weakly primary, as needed. □

Proposition 2.9. *Let $I \subseteq P$ be graded ideals of R with $P \neq R$. Then the following hold:*

(*i*) *If P is graded weakly primary, then P/I is graded weakly primary.*

(*ii*) *If I and P/I are graded weakly primary, then P is graded weakly primary.*

Proof. (*i*) Let $0 \neq (a+I)(b+I) = ab + I \in P/I$ where $a, b \in h(R)$, so $ab \in P$. If $ab = 0 \in I$, then $(a+I)(b+I) = 0$, a contradiction. If $ab \neq 0$,

P graded weakly primary gives either $a \in P$ or $b \in \mathrm{Grad}(P)$; hence either $a + I \in P/I$ or $b^n + I = (b + I)^n \in P/I$ for some integer n. It follows that either $a + I \in P/I$ or $b + I \in \mathrm{Grad}(P/I)$, as needed.

(ii) Let $0 \neq ab \in P$ where $a, b \in h(R)$, so $(a+I)(b+I) \in P/I$. If $ab \in I$, then I graded weakly primary gives either $a \in I \subseteq P$ or $b \in \mathrm{Grad}(I) \subseteq \mathrm{Grad}(P)$. So we may assume that $ab \notin I$. Then either $a + I \in P/I$ or $b^m + I \in P/I$ for some integer m since P/I is graded weakly primary. It follows that either $a \in P$ or $b \in \mathrm{Grad}(P)$, as required. □

Theorem 2.10. *Let P and Q be graded weakly primary ideals of R such that P_g and Q_h are not primary subgroups of R_g and R_h respectively for all $g, h \in G$. Then $P + Q$ is a graded weakly primary ideal of R.*

Proof. By Proposition 2.7, we have

$$\mathrm{Grad}(P) + \mathrm{Grad}(Q) = \mathrm{Grad}(0) \neq R,$$

so $P + Q$ is a proper ideal of R. Since $(P + Q)/Q \cong Q/(P \cap Q)$, we get $(P + Q)/Q$ is graded weakly primary by Propositin 2.9 (i). Now the assertion follows from Proposition 2.9 (ii). □

Acknowledgement. The author thanks the referee for valuable comments.

References

[1] **D. D. Anderson, R. Smith:** *Weakly prime ideals*, Houston J. Math. **29** (2003), 831 – 840.

[2] **S. Ebrahimi Atani, F. Farzalipour:** *On weakly primary ideals*, Georgian Math. J. (to appear).

[3] **C. Nastasescu, F. Van Oystaeyen:** *Graded Ring Theory*, Mathematical Library 28, North Holand, Amsterdam, 1982.

[4] **M. Refai, K. Al-Zoubi:** *On graded primary ideals*, Turkish J. Math. **28** (2004), 217 – 229.

Received February 17, 2005

Department of Mathematics
University of Guilan
P.O. Box 1914
Rasht
Iran
Email: ebrahimi@guilan.ac.ir

Quasigroups and Related Systems **13** (2005), 193 – 202

On decomposable hyper BCK-algebras

Rajab Ali Borzooei and Habib Harizavi

Abstract

In this manuscript, we introduce the concept of decomposable hyper BCK-algebras and we give a condition for a hyper BCK-algebra to be a decomposable hyper BCK-algebra. Moreover, we state and prove some theorems about (weak, implicative) strong hyper BCK-ideal of a decomposable hyper BCK-algebra. Finally, we give a characterization of some decomposable hyper BCK-algebras.

1. Introduction

The study of BCK-algebras was initiated by Y. Imai and K. Iséki [5] in 1966 as a generalization of the concept of set-theoretic difference and propositional calculus. Since then a great deal of literature has been produced on the theory of BCK-algebras. The hyperstructure theory(called also multialgebras) was introduced in 1934 by F. Marty [9] at the 8th congress of Scandinavian Mathematiciens. In [8], Y.B. Jun et al. applied the hyperstructures to BCK-algebras, and introduced the notion of a hyper BCK-algebra which is a generalization of BCK-algebra, and investigated some related properties. Now we follow [7] and [8] and introduce the concept of decomposable hyper BCK-algebra and give a condition for a hyper BCK-algebra to be a decomposable hyper BCK-algebra. Moreover, we state and prove some theorems about (weak, implicative) strong hyper BCK-ideal a of decomposable hyper BCK-algebra.

2. Preliminaries

Definition 2.1. [8] By a *hyper BCK-algebra* we mean a non-empty set H endowed with a hyperoperation "$\circ$" and a constant 0 satisfying the following

2000 Mathematics Subject Classification: 06F35, 03G25
Keywords: Decomposable hyper BCK-algebra, (weak) hyper BCK-ideal.

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.

Theorem 2.2. [8] *In any hyper BCK-algebra H, the following hold:*

(i) $0 \circ 0 = \{0\}$,
(ii) $0 \ll x$,
(iii) $x \ll x$,
(iv) $A \ll A$,
(v) $A \subseteq B$ *implies* $A \ll B$,
(vi) $0 \circ x = \{0\}$,
(vii) $x \circ y \ll x$,
(viii) $x \circ 0 = \{x\}$,
(ix) $y \ll z$ *implies* $x \circ z \ll x \circ y$

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

Definition 2.3. Let I be a subset of a hyper BCK-algebra H and $0 \in I$. Then I is said to be a *week hyper BCK-ideal* of H if $x \circ y \subseteq I$ and $y \in I$ imply $x \in I$ for all $x, y \in H$, *hyper BCK-ideal* of H if $x \circ y \ll I$ and $y \in I$ imply $x \in I$ for all $x, y \in H$, *strong hyper BCK-ideal* if $(x \circ y) \cap I \neq \emptyset$ and $y \in I$ imply $x \in I$ for all $x, y \in H$, *reflexive hyper BCK-ideal* of H if I is a hyper BCK-ideal of H and $x \circ x \subseteq I$ for all $x \in H$.

Theorem 2.4. [6, 7, 8] *Let H be a hyper BCK-algebra. Then,*

(i) *any strong hyper BCK-ideal of H is a hyper BCK-ideal of H,*
(ii) *if I is a hyper BCK-ideal of H and A be a nonempty subset of H, then $A \ll I$ implies $A \subseteq I$,*
(iii) *H is a BCK-algebra if and only if $H = \{x \in H : x \circ x = \{0\}\}$.*

Definition 2.5. [3] Let H be a hyper BCK-algebra, Θ be an equivalence relation on H and $A, B \subseteq H$. Then,

(i) we write $A\Theta B$, if there exist $a \in A$ and $b \in B$ such that $a\Theta b$,
(ii) we write $A\bar{\Theta}B$, if for all $a \in A$ there exists $b \in B$ such that $a\Theta b$ and for all $b \in B$ there exists $a \in A$ such that $a\Theta b$,
(iii) Θ is called a *congruence relation* on H, if $x\Theta y$ and $x^{'}\Theta y^{'}$, then

$x \circ x^{'}\bar{\Theta} y \circ y^{'}$, for all $x, y \in H$,

(iv) Θ is called a *regular relation* on H if $x \circ y\Theta\{0\}$ and $y \circ x\Theta\{0\}$, then $x\Theta y$ for all $x, y \in H$.

Theorem 2.6. [3] *Let Θ and $\Theta^{'}$ are two regular congruence relations on H such that $[0]_\Theta = [0]_{\Theta^{'}}$. Then $\Theta = \Theta^{'}$.*

Theorem 2.7. [3] *Let Θ be a regular congruence relation on H and $H/\Theta = \{I_x : x \in H\}$, where $I_x = [x]_\Theta$, for all $x \in H$. Then $\frac{H}{\Theta}$ with hyperoperation $I_x \circ I_y = \{I_z : z \in x \circ y\}$ and hyper order $I_x < I_y \Longleftrightarrow I \in I_x \circ I_y$ is a hyper BCK-algebra which is called quotient hyper BCK-algebra.*

Theorem 2.8. [3] (Isomorphism Theorem) *Let Θ be a regular congruence relation on hyper BCK-algebra H. If $f : H \longrightarrow H^{'}$ is a homomorphism of hyper BCK-algebras such that $Kerf = [0]_\Theta$, then $H/\Theta \cong f(H)$.*

3. Decomposable hyper BCK-algebras

Definition 3.1. A hyper BCK-algebra H is called *decomposable* if there exists a nontrivial family $\{A_i\}_{i\in\Lambda}$ of hyper BCK-ideals of H such that

(i) $H \neq A_i \neq \{0\}$ for all $i \in \Lambda$,

(ii) $H = \bigcup_{i\in\Lambda} A_i$,

(iii) $A_i \cap A_j = \{0\}$ for all $i \neq j \in \Lambda$.

In this case, we say that $H = \bigcup_{i\in\Lambda} A_i$ is a decomposition of H and we write $H = \bigoplus_{i\in\Lambda} A_i$.

Example 3.2. (i) Let H be a hyper BCK-algebra with the following Cayley table:

$\circ$	0	1	2
0	$\{0\}$	$\{0\}$	$\{0\}$
1	$\{1\}$	$\{0,1\}$	$\{1\}$
2	$\{2\}$	$\{2\}$	$\{0,2\}$

It is easy to check that $A_1 = \{0, 1\}$ and $A_2 = \{0, 2\}$ are hyper BCK-ideals of H such that $H = A_1 \cup A_2$ and $A_1 \cap A_2 = \{0\}$. Therefore, H is decomposable.

(ii) Let $H = N \cup \{0\}$. Consider the hyperoperation

$$x \circ y = \begin{cases} \{0\} & \text{if } x = 0 \text{ or } x = y, \\ \{x\} & \text{otherwise.} \end{cases}$$

It is easily verified that $(H, \circ, 0)$ is a hyper BCK-algebra and $A_n = \{0, n\}$ is a hyper BCK-ideal of H, for all $n \in N$. Now, since $H = \bigcup_{n \in N} A_n$ and $A_n \cap A_m = \{0\}$, for each $n \neq m \in N$. Therefore, H is decomposable.

(iii) Let $N = \{0, 1, 2, 3, ...\}$ and hyper operation "$\circ$" on N is defined as follow:

$$x \circ y = \begin{cases} \{0, x\} & \text{if } x \leqslant y, \\ \{x\} & \text{if } x > y \end{cases}$$

for all $x, y \in H$. Then $(N, \circ, 0)$ is a hyper BCK-algebra but it is not a decomposable hyper BCK-algebra. Since every hyper BCK-ideal of H is equal to H or $\{0, 1, 2, ..., n-1\}$, for some $n \in N$.

Note. From now on, we let H be a hyper BCK-algebra.

Theorem 3.3. *Let H be decomposable with decomposition $H = \bigoplus_{i \in \Lambda} A_i$. Then A_i is a strong hyper BCK-ideal of H for all $i \in \Lambda$.*

Proof. Let $H = \bigoplus_{i \in \Lambda} A_i$ be a decomposition of H and let $(x \circ y) \cap A_i \neq \emptyset$ and $y \in A_i$ for $x \in H$ and $i \in \Lambda$. Then there exists $t \in x \circ y$ such that $t \in A_i$. From $x \in H = \bigcup_{i \in \Lambda} A_i$ we conclude that there exists $j \in \Lambda$ such that $x \in A_j$. Since $x \circ y \ll x \in A_j$, then $x \circ y \ll A_j$ and so by Theorem 2.4, $x \circ y \subseteq A_j$. Therefore, $t \in A_i \cap A_j$. Now, we consider the following two cases. If $j = i$, then $A_j = A_i$ and so $x \in A_i$. If $j \neq i$, then $t \in A_i \cap A_j = \{0\}$ that $t = 0$ and so $0 \in x \circ y$. This implies that $x \ll y$. It follow from $y \in A_i$ and Theorem 2.4 (ii) $x \in A_i$. Therefore, A_i is a strong hyper BCK-ideal of H. □

Theorem 3.4. *Let H be decomposable with decomposition $H = \bigoplus_{i \in \Lambda} A_i$. Then $A_i \cup A_j$ is a strong hyper BCK-ideal of H for all $i, j \in \Lambda$.*

Proof. Let $i, j \in \Lambda$ and $x, y \in H$ be such that $(x \circ y) \cap (A_i \cup A_j) \neq \emptyset$ and $y \in A_i \cup A_j$. Without loss of generality, assume that $y \in A_i$. Since $(x \circ y) \cap (A_i \cup A_j) \neq \emptyset$, then there exists $t \in H$ such that $t \in (x \circ y) \cap (A_i \cup A_j)$ and so $t \in A_i$ or $t \in A_j$. If $t \in A_i$, since A_i is a strong hyper BCK-ideal of H and $y \in A_i$, then $x \in A_i \subseteq A_i \cup A_j$. If $t \in A_j$, then by $x \in H = \bigcup_{i \in \Lambda} A_i$ there exists $k \in \Lambda$ such that $x \in A_k$. It follow from $x \circ y \leqslant x \in A_k$ and Theorem 2.4 (i,ii) that $x \circ y \ll A_k$ and so $x \circ y \subseteq A_k$. Hence we have $t \in A_j \cap A_k$. If $j = k$ then $A_j = A_k$ and so $x \in A_j \subseteq A_i \cup A_j$. If $j \neq k$, then $t \in A_j \cap A_k = \{0\}$ and so $t = 0$. Then $0 \in x \circ y$ and so $x \ll y$. Now, since $y \in A_i$ and A_i is a hyper BCK-ideal of H then $x \in A_i \subseteq A_i \cup A_j$. Therefore, $A_i \cup A_j$ is a strong hyper BCK-ideal of H. □

Theorem 3.5. *Let H be decomposable with decomposition $H = \bigoplus_{i\in\Lambda} A_i$. Then $\bigcup_{i\in\Omega} A_i$ is a strong hyper BCK-ideal of H for all $\emptyset \neq \Omega \subseteq \Lambda$.*

Proof. We proceed by induction on $|\Omega|$. For $\Omega \subseteq \Lambda$ with $|\Omega| = 1$ the result holds by Theorem 3.3. Suppose that for $2 \leqslant m \in N$ and all $\Omega \subseteq \Lambda$ with $|\Omega| \leqslant m$ the result hold and let $\Omega \subseteq \Lambda$ be such that $|\Omega| = m+1$. Let i, j be arbitrary elements of Ω. Taking $A_{ij} = A_i \cup A_j$ and by using Theorems 3.4 and 2.4(i), we conclude that A_0 is a hyper BCK-ideal of H. Taking $\Omega^{'} = (\Omega - \{i,j\}) \cup \{ij\}$ and by using the hypothesis of induction, we conclude that $\bigcup_{i\in\Omega'} A_i$ is a strong hyper BCK-ideal of H. Now, since $\bigcup_{i\in\Omega} A_i = \bigcup_{i\in\Omega'} A_i$ then $\bigcup_{i\in\Omega} A_i$ is a strong hyper BCK-ideal of H. Therefore for all $\emptyset \neq \Omega \subseteq \Lambda$, $\bigcup_{i\in\Omega} A_i$ is a strong hyper BCK-ideal of H. □

Corollary 3.6. *Let H be decomposable. Then there exist nontrivial strong hyper BCK-ideals A, B of H such that $H = A \cup B$ and $A \cap B = \{0\}$, that is $H = A \bigoplus B$.*

Proof. The proof come immediately from Theorem 3.5. □

Theorem 3.7. *Let H be a hyper BCK-algebra. Then H is decomposable if and only if there exists a nontrivial strong hyper BCK-ideal A of H such that $0 \notin (A' \circ B) \circ B$, where $A' = A - \{0\}$ and $B = H - A'$.*

Proof. ($\Longrightarrow$) Let H be decomposable. Then by Corollary 3.6 there exist nontrivial strong hyper BCK-ideals A and B of H such that $H = A \bigoplus B$. Let $0 \in (A' \circ B) \circ B$, by contrary. Since, $(A' \circ B) \circ B = \bigcup_{b\in B,\, t\in A'\circ B} t \circ b$, then there exist $t \in A' \circ B$ and $b \in B$ such that $0 \in t \circ b$. Now, since $b \in B$ and B is a strong hyper BCK-ideal of H, then $t \in B$. But, $t \in A' \circ B$ implies that there exist $a \in A'$ and $b_1 \in B$ such that $t \in a \circ b_1$ and so $a \circ b_1 \cap B \neq \emptyset$ and this implies that $a \in B$. Hence, $0 \neq a \in A \cap B = \{0\}$, which is impossible. Therefore, $0 \notin (A' \circ B) \circ B$.

($\Longleftarrow$) It is enough to prove that B is a hyper BCK-ideal of H. Let for $a, b \in H$, $a \circ b \ll B$ and $b \in B$ but $a \notin B$. Hence, $a \in A'$. Since $a \circ b \ll B$, then there exist $t \in a \circ b$ and $b_1 \in B$ such that $t \ll B_1$ and so $0 \in t \circ B_1$. Hence

$$0 \in t \circ b_1 \subseteq (a \circ b) \circ b' \subseteq (A' \circ B) \circ B$$

which is impossible. □

Theorem 3.8. *Let H be decomposable with decomposition $H = A \bigoplus B$. Then A and B are implicative hyper BCK-ideals of H if and only if for all $x, y \in H$ $x \circ (y \circ x) = \{0\}$ imply $x = 0$.*

Proof. Let A and B be implicative hyper BCK-ideals of H and $x\circ(x\circ y)=\{0\}$ for $x,y\in H$. Then $x\circ(y\circ x)\ll A$ and $x\circ(y\circ x)\ll B$ and so by Theorem 2.4 (iii), $x\in A\cap B=\{0\}$.

Conversely, let for $x,y\in H$, $x\circ(y\circ x)\ll A$ but $x\notin A$, by contrary. Hence, $0\neq x\in B$. By Theorem 2.2 (vii), $x\circ(y\circ x)\ll x\in B$ and so by Theorem 2.4 (ii), $x\circ(y\circ x)\subseteq B$. On the other hand, since $x\circ(y\circ x)\ll A$ then by Theorem 2.4 (ii), $x\circ(y\circ x)\subseteq A$. Hence $x\circ(y\circ x)\subseteq A\cap B=\{0\}$ and so $x\circ(y\circ x)=\{0\}$. Now, by hypothesis $x=0$, which is a contradiction. Therefore, $x\in A$ and so by Theorem 2.4 (iii) A is a implicative hyper BCK-ideal of H. The proof of case B is similar. □

Proposition 3.9. *Let H be decomposable with decomposition $H=A\bigoplus B$. If A and B are reflexive, then H is a BCK-algebra.*

Proof. Let A and B be reflexive. Then we have $x\circ x\subseteq A$ and $x\circ x\subseteq B$ for all $x\in H$. Hence $x\circ x\subseteq A\cap B=\{0\}$ and so $x\circ x=0$. It follows from Theorem 2.4 (iv) that H is a BCK-algebra. □

Definition 3.10. Let $\emptyset\neq A\subset H$. Then subset I of H is called a *weak hyper BCK-ideal of H related to A* if

(r1) $0\in I$,

(r2) $x\circ y\subseteq I$ and $y\in I$ imply $x\in I$ for all $x\in A$.

Note that, for all nonempty subset A of H if I is a weak hyper BCK-ideal of H, then I is a weak hyper BCK-ideal of H related to A. But the converse is not true in general.

Example 3.11. Consider a hyper BCK-algebra H with the following Cayley table:

$\circ$	0	1	2	3
0	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
1	$\{1\}$	$\{0\}$	$\{0\}$	$\{0\}$
2	$\{2\}$	$\{1\}$	$\{0\}$	$\{0\}$
3	$\{3\}$	$\{3\}$	$\{3\}$	$\{0,3\}$

Then $I=\{0,2\}$ is a weak hyper BCK-ideal of H related to $A=\{0,2,3\}$. But, I is not a weak hyper BCK-ideal of H. Since $1\circ 2\subseteq I$ and $2\in I$ but $1\notin I$. □

Theorem 3.12. *Let H be decomposable with decomposition $H=A\bigoplus B$ and $I\subseteq A$. If I is a weak hyper BCK-ideal of H related to A, then I is a weak hyper BCK-ideal of H.*

Proof. Let I be a weak hyper BCK-ideal of H related to A and $x \circ y \subseteq I$ and $y \in I$, for $x, y \in H$. If $x \in A$, then by hypothesis $x \in I$. Now, let $x \in B$. Then by Theorem 2.2 (vii), $x \circ y \ll B$, which implies that $x \circ y \subseteq B$ by Theorem 2.4 (i,ii). Hence $x \circ y \subseteq A \cap B = \{0\}$, which implies that $x \circ y = \{0\}$ and so $x \ll y$. Since $y \in I \subseteq A$, we have $x \ll A$ and so by Theorem 2.4, we get $x \in A$. Thus $x \in A \cap B = \{0\}$. This implies that $x = 0$ and so $x \in I$. Therefore, I is a weak hyper BCK-ideal of H. □

Definition 3.13. Let $\emptyset \neq A \subset H$. Then subset I of H is called a *hyper BCK-ideal of H related to* A if

(r1) $0 \in I$,

(r3) $x \circ y \ll I$ and $y \in I$ imply $x \in I$ for all $x \in A$.

Note that, for all nonempty subset A of H if I is a hyper BCK-ideal of H, then I is a hyper BCK-ideal of H related to A. But the converse is not true in general.

Example 3.14. Let $J = \{0, 1\}$ and $B = \{0, 1, 3\}$ in Example 3.12. It is easy to show that J is a hyper BCK-ideal of H related to B, but J is not hyper BCK-ideal of H. Since $2 \circ 1 \ll J$ and $1 \in J$ but $2 \notin J$. □

Theorem 3.15. *Let H be decomposable with decomposition $H = A \bigoplus B$ and $I \subseteq A$. If I is a hyper BCK-ideal of H related to A, then I is a hyper BCK-ideal of H.*

Proof. The proof is similar to the proof of Theorem 3.12 by some modification. □

4. Quotient structure

Theorem 4.1. *Let H be decomposable with decomposition $H = A \bigoplus B$. Then there exists a regular congruence relation Θ on H and a hyper BCK-algebra X of order 2 such that $H/\Theta \cong X$.*

Proof. Let relation Θ on H is defined as follows:

$$x \Theta y \iff x, y \in A \text{ or } x, y \in B - \{0\}.$$

Since $H = A \bigoplus B$ is a decomposition of H, then it is easily verified that Θ is an equivalence relation on H. Now, let $x, y \in H$ such that $x \Theta y$. Then $x, y \in A$ or $x, y \in B - \{0\}$. Without loss of generality we can suppose that $x, y \in A$. It follow from Theorem 2.2 (vii) and Theorem 2.4 we get that

$x\circ a\subseteq A$ ($y\circ a\subseteq A$), which implies that $x\circ a\bar{\Theta}y\circ a$ for all $a\in H$. On the other hand by using Theorem 2.2 (vii) and Theorem 2.4 (i,ii), we get $a\circ x\subseteq A$ ($a\circ y\subseteq A$) if $a\in A$, and $a\circ x\subseteq B$ ($a\circ y\subseteq B$) if $a\in B$, for all $a\in H$ and so $a\circ x\bar{\Theta}a\circ y$. Hence Θ is a congruence relation on H. Now, let $x,y\in H$ such that $x\circ y\Theta\{0\}$ and $y\circ x\Theta\{0\}$. Then there exist $s\in x\circ y$ and $t\in y\circ x$ such that $s\Theta 0$ and $t\Theta 0$, which imply that $s,t\in A$. Hence, we have $(x\circ y)\cap A\neq\emptyset$ and $(y\circ x)\cap A\neq\emptyset$. Now, if $x\in A$ since $(y\circ x)\cap A\neq\emptyset$ and A is a strong hyper BCK-ideal of H then $y\in A$ and so $x\Theta y$.

Similarly, if $y\in A$, then we get that $x\in A$ and so $x\Theta y$. Now, remind only the case $x,y\in B-\{0\}$. But in this case by definition of Θ, we get that $x\Theta y$. Hence, Θ is a regular relation on H. Therefore, Θ is a regular congruence relation on H and so by Theorem 2.7, H/Θ is a hyper BCK-algebra. Now, it is easy to prove that $H/\Theta=\{[0]_\Theta=A,[b]_\Theta=B\}$, where $b\in B-\{0\}$. Hence $|H/\Theta|=2$. Now, since we have only to hyper BCK-algebra $X=\{0,a\}$ of order 2 which are as follows:

$\circ_1$	0	a
0	$\{0\}$	$\{0\}$
a	$\{a\}$	$\{0\}$

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

Now, if $b\circ b=\{0\}$ then $[b]_\Theta\circ[b]_\Theta=\{[0]_\Theta\}$ and so $H/\Theta\cong(X,\circ_1)$ and if $b\circ b\neq\{0\}$ then $[b]_\Theta\circ[b]_\Theta=\{[0]_\Theta,[b]_\Theta\}$ and so $H/\Theta\cong(X,\circ_2)$. □

Theorem 4.2. *Let H be decomposable with decomposition $H=A\bigoplus B$ and let $b\circ x=b\circ y$ for all $b\in B$ and $x,y\in A$. Then there exists a regular congruence relation Γ on H such that $H/\Gamma\cong B$.*

Proof. Define the relation Γ on H as follows:

$$x\Gamma y \iff x,y\in A \ \text{ or } \ x=y\notin A.$$

It is easy to prove that Γ is an equivalence relation on H. Let $x,y\in H$ be such that $x\Gamma y$. Then $x,y\in A$ or $x=y\notin A$.

Case 1. Let $x,y\in A$. Then by Theorem 2.2 (vii), $x\circ a\ll x$ ($y\circ a\ll y$) and so by Theorem 2.4, we get that $x\circ a\subseteq A$ ($y\circ a\subseteq A$), which implies that $x\circ a\bar{\Gamma}y\circ a$ for all $a\in H$. Now, we prove that $a\circ x\bar{\Gamma}a\circ y$, for all $a\in H$. If $a\in A$, the by the similar way in the above proof, we can show that $a\circ x\bar{\Gamma}a\circ y$. If $a\notin A$, then $a\in B$ and so by the hypothesis we have $a\circ x=a\circ y$, which implies that $a\circ x\bar{\Gamma}a\circ y$.

Case 2. Let $x=y\notin A$. Then $x\circ a=y\circ a$ and $a\circ x=a\circ y$ for all $a\in H$, which implies that $x\circ a\bar{\Gamma}y\circ a$ and $a\circ x\bar{\Gamma}a\circ y$ for all $a\in H$.

Therefore, Γ is a congruence relation on H. Now, let $x, y \in H$ such that $x \circ y\Gamma\{0\}$ and $y \circ x\Gamma\{0\}$. Then, there exist $s \in x \circ y$ and $t \in y \circ x$ such that $s\Gamma 0$ and $t\Gamma 0$ and so $s, t \in A$ and this implies that $(x \circ y) \cap A \neq \emptyset$ and $(y \circ x) \cap A \neq \emptyset$. Now, if $x \in A(y \in A)$, then since A is a strong hyper BCK-ideal of H, then $y \in A(x \in A)$, which implies that $x\Gamma y$. If $x, y \notin A$, then $x, y \in B - \{0\}$. Hence, by Theorem 2.2 (vii), $x \circ y \ll x$ $(y \circ x \ll y)$ and so by Theorem 2.4, $x \circ y \subseteq B$ $(y \circ x \subseteq B)$. So, $t, s \in A \cap B = \{0\}$ and this implies that $s = t = 0$). Thus $x \ll y$ and $y \ll x$ and so $x = y$, which implies that $x\Gamma y$. Therefore, Γ is a regular congruence relation on H. Now, we define the function $f : H \longrightarrow H$ by

$$f(x) = \begin{cases} 0 & \text{if } x \in A, \\ x & \text{if } x \in B. \end{cases}$$

It follows from $A \cap B = \{0\}$, that f is well-defined. Now, let $x, y \in H$. We consider the following four cases:

Case 1. $x, y \in A$.
In this case, by Theorem 2.2 (vii), $x \circ y \ll x$ and so by Theorem 2.4, we get $x \circ y \subseteq A$. Hence,

$$f(x \circ y) = f(\bigcup_{t \in x \circ y} t) = \bigcup_{t \in x \circ y \subseteq A} \{f(t)\} = \{0\} = 0 \circ 0 = f(x) \circ f(y)$$

Case 2. $x, y \in B$.
Similar to the proof of Case 1, we get that $x \circ y \subseteq B$. Hence,

$$f(x \circ y) = f(\bigcup_{t \in x \circ y} t) = \bigcup_{t \in x \circ y \subseteq B} \{f(t)\} = \bigcup_{t \in x \circ y} \{t\} = x \circ y = f(x) \circ f(y)$$

Case 3. $x \in A$ and $y \in B - \{0\}$.
Similar to the proof of Case 1, we get that $x \circ y \subseteq A$ and so $f(x \circ y) = \{0\}$. On the other hand, since $f(x) = 0$, we have $f(x) \circ f(y) = 0 \circ y = \{0\}$. Hence

$$f(x \circ y) = f(x) \circ f(y)$$

Case 4 $x \in B - \{0\}$ and $y \in A$.
By hypothesis, we have $x \circ y = x \circ 0 = \{x\}$ and so

$$f(x \circ y) = \{f(x)\} = f(x) \circ 0 = f(x) \circ f(y)$$

Therefore, $f(x \circ y) = f(x) \circ f(y)$ for all $x, y \in H$ and so f is a homomorphism. It is easy to check that Ker$f = A = [0]_\Gamma$ and $f(H) = B$. Hence by Theorem 2.8, we have $H/\Gamma \cong B$. □

Corollary 4.3. *Let H be decomposable with decomposition $H = A \bigoplus B$ and let $b \circ x = b \circ y$ for all $b \in B$ and $x, y \in A$. Then $|B| = 2$.*

Proof. Let regular congruence relations Θ and Γ on H are as Theorems 4.1 and 4.2, respectively. Since $[0]_\Theta = A = [0]_\Gamma$, then by Theorem 2.6 that $\Theta = \Gamma$ and so $H/\Theta = H/\Gamma$. Now, by Theorem 4.1, $H/\Theta \cong X$, where X is a hyper BCK-algebra of order 2 and by Theorem 4.2, $H/\Gamma \cong B$. Hence,

$$X \cong H/\Theta = H/\Gamma \cong B$$

and so $|B| = |X| = 2$. □

References

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

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

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

[4] **P. Corsini**: *Prolegomena of hypergroups theory*, Aviani Editor, 1993.

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

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

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

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

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

[10] **J. Meng and Y. B. Jun**: *BCK-algebra*, Kyungmoonsa, Seoul, Korea, 1994.

Received November 20, 2005

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

Factorization of simple groups involving the alternating group

Mohammad R. Darafsheh

Abstract

In this paper we will find the structure of the finite simple groups G with two subgroups A and B such that $G = AB$, where A is a non-abelian simple group and B is isomorphic to the alternating group on seven letters.

1. Introduction

Let A and B be subgroups of a group G. If $G = AB$, then G is called a *factorizable group.* We also say G is the product of the two subgroups A and B, or G is a factorizable group. Since we always have the identity $G = AG$, hence in this paper we assume both factors A and B are proper subgroups of G and we say $G = AB$ a non-trivial factorization of G. If $G \cong A \times B$, then we call G a factorizable group as well. In [1] page 13 the question of finding all the factorizable groups is raised. Of course not all groups are factorizable, for example by [14] the Conway's simple group Co_2 of order $2^{18}.3^6.5^3.7.11.23$ is not a factorizable group. Similarly an infinite group whose proper subgroups are finite does not have a proper factorization. Therefore we always search for a special kind of factorization.

A factorization $G = AB$ is called *maximal* if both factors A and B are maximal subgroups of G. In [14] the authors found all the maximal factorization of all the finite simple groups and their automorphism groups. This special kind of factorization is useful because every factorization of a finite group is contained in a maximal factorization. In [2] simple groups G with factorization $G = AB$ and with the additional condition $(|A|, |B|) = 1$

2000 Mathematics Subject Classification: 20D40
Keywords: factorization, symmetric group, simple group.

are determined. In this case we also have $A \cap B = 1$ the trivial group. A factorization $G = AB$ with the condition $A \cap B = 1$ is called an exact factorization. In [19] the authors found all the exact factorizations of the alternating and the symmetric groups. But later in [17] all the factorizations of the alternating and the symmetric groups were found where both factors are simple groups. Recently an interesting application of exact factorization is given in [9]. The authors show that an exact factorization of a finite group leads to the construction of a biperfect Hopf algebra, and then they find such a factorization for the Mathieu group M_{24}. This factorization is of the form $M_{24} = AB$, where $A \cong M_{23}$ and $B \cong 2^4 : \mathbb{A}_7$, both perfect groups.

Here we quote some results concerning the involvement of the alternating or symmetric groups in a factorization. In [13] all finite groups $G = AB$, $A \cong B \cong \mathbb{A}_5$ are classified and in [16] factorizable groups where one factor is a non-abelian simple group and the other factor is isomorphic to the alternating group on 5 letters are classified. In [18] factorizations of finite groups are classified in the case where one factor of a factorizable group is simple and the other factor is almost simple. In [5] all finite groups $G = AB$, where $A \cong \mathbb{A}_6$ and B is isomorphic to the symmetric group on $n \geqslant 5$ letters are determined. Also in [6] we determined the structure of a finite factorizable group with one factor a simple group and the other factor isomorphic to the symmetric group on 6 letters. In [7] we determined the structure of factorizable groups $G = AB$ where $A \cong \mathbb{A}_7$ and $B \cong \mathbb{S}_n$. Motivated by this paper here we will find the structure of the finite simple factorizable groups $G = AB$ such that A is a non-abelian simple group and $B \cong \mathbb{A}_7$, the symmetric group on seven letters. Through the paper all groups are assumed to be finite. Notations for the simple groups is taken from [4].

2. Preliminary results

In the following we quote two Lemmas from [18] which are useful when dealing with factorizable groups.

Lemma 1. *Let A and B be subgroups of a group G. The following statements are equivalent.*

(a) *$G = AB$.*

(b) *A acts transitively on the coset space $\Omega(G : B)$ of right coset of B in G.*

(c) *B acts transitively on the coset space $\Omega(G : A)$ of right coset of A in G.*

(*d*) $(\pi_A, \pi_B) = 1$, *where* π_A *and* π_B *are the permutation characters of* G *on* $\Omega(G : A)$ *and* $\Omega(G : B)$ *respectively.*

Lemma 2. *Let* G *be a permutation group on a set* Ω *of size* n. *Suppose the action of* G *on* Ω *is k-homogeneous,* $1 \leqslant k \leqslant n$. *If a subgroup* H *of* G *acts on* Ω *k-homogeneously, then* $G = G_{(\Delta)}H$, *where* Δ *is a k-subset of* Ω *and* $G_{(\Delta)}$ *denotes its global stabilizer.*

Now it is easy to determine the indices of subgroups of $\mathbb{A}_7$ and $\mathbb{S}_7$. If $H \leqslant \mathbb{A}_7$, then $[\mathbb{A}_7 : H]$ may be one of the following numbers: 1, 7, 15, 21, 35, 42, 70, 105, 120, 126, 140, 210, 252, 280, 315, 360, 420, 504, 630, 840, 1260 or 2520. And if $H \leqslant \mathbb{S}_7$, then $[\mathbb{S}_7 : H]$ is one of the following numbers: 1, 2, 7, 14, 21, 30, 35, 42, 70, 84, 105, 120, 126, 140, 210, 240, 252, 280, 315, 360, 420, 504, 560, 630, 720, 840, 1008, 1260, 1280, 2520 or 5040. Therefore if $\mathbb{A}_7$ (or $\mathbb{S}_7$) acts transitively on a set of size n, then $n = [\mathbb{A}_7 : H]$ (or $n = [\mathbb{S}_7 : H]$) is one of the above numbers. The action is faithful if and only if $n \neq 1$ in the case of $\mathbb{A}_7$ and $n \neq 1, 2$ in the case of $\mathbb{S}_7$. It is well-known that if $\mathbb{S}_7$ has a k-homogeneous (k-transitive) action, $k > 1$, on a set Ω, then $|\Omega| = 7$ and $2 \leqslant k \leqslant 7$, but for $\mathbb{A}_7$ we have the same result in addition with the 2-transitive action of $\mathbb{A}_7$ on 15 points, see [3]. Since we need factorizations of the alternating groups involving $\mathbb{S}_7$ or $\mathbb{A}_7$, hence using [14] we will prove the following results.

Lemma 3. *Let* $\mathbb{A}_m$ *denote the alternating group of degree* m. *If* $\mathbb{A}_m = AB$ *is a non-trivial factorization of* $\mathbb{A}_m$, A *a non-abelian simple subgroup of* $\mathbb{A}_m$ *and* $B \cong \mathbb{A}_7$, *then one of the following cases occurs:*

(*a*) $\mathbb{A}_m = \mathbb{A}_{m-1}\mathbb{A}_7$, *where* $m =$ 15, 21, 35, 42, 70, 105, 120, 126, 140, 210, 252, 280, 315, 360, 420, 504, 630, 840, 1260 *or* 2520.

(*b*) $\mathbb{A}_{15} = \mathbb{A}_{13}\mathbb{A}_7$,

(*c*) $\mathbb{A}_8 = L_2(7)\mathbb{A}_7$, $\mathbb{A}_9 = L_2(8)\mathbb{A}_7$, $\mathbb{A}_{11} = M_{11}\mathbb{A}_7$, $\mathbb{A}_{12} = M_{12}\mathbb{A}_7$.

Proof. It is obvious that m is at least 8. By [14] either $m = 6, 8, 10$ or one of A or B is k-homogeneous on m letters, $1 \leqslant k \leqslant 5$. Factorization of $\mathbb{A}_m$ if $m = 6$, 8 or 10 does not involve $\mathbb{A}_7$. Therefore we will consider the following cases.

Case (*i*). $\mathbb{A}_{m-k} \trianglelefteq A \trianglelefteq \mathbb{S}_{m-k} \times \mathbb{S}_k$ for some k with $1 \leqslant k \leqslant 5$, and B k-homogeneous on m letters.

Since A is assumed to be simple we obtain $\mathbb{A}_{m-k} = 1$ or A. If $\mathbb{A}_{m-k} = 1$, then $m - k = 1$ or 2, hence $k = m - 1$ or $m - 2$. But then from $1 \leqslant k \leqslant 5$ we will obtain $2 \leqslant m \leqslant 6$ or $3 \leqslant m \leqslant 7$, a contradiction because $m \geqslant 8$.

Therefore $A = \mathbb{A}_{m-k}$ and $B \cong \mathbb{A}_7$ is k-homogeneous on m letters, $1 \leqslant k \leqslant 5$. If $k = 1$, then the size of the set Ω on which $\mathbb{A}_7$ can act transitively is as stated in the Lemma and all the factorizations in case (a) occur. If $k \geqslant 2$, then $m = 7$ or 15. If $m = 15$, then $\mathbb{A}_7$ has a transitive action on 15 letters and hence $\mathbb{A}_{15} = \mathbb{A}_{14}\mathbb{A}_7$ and $\mathbb{A}_{15} = \mathbb{A}_{13}\mathbb{A}_7$ which is case (b).

Case (ii). $\mathbb{A}_{m-k} \trianglelefteq B \leqslant \mathbb{S}_{m-k} \times \mathbb{S}_k$, $1 \leqslant k \leqslant 5$, and A is k-homogeneous on m letters.

Since $B \cong \mathbb{S}_7$, we obtain $m - k = 1$ or 7. From $1 \leqslant k \leqslant 5$ we get $2 \leqslant m \leqslant 6$ or $8 \leqslant m \leqslant 12$. Therefore only $m = 8$, 9, 10, 11 or 12 are possible which correspond to $k = 1$, 2, 3, 4, 5 respectively. But now from [3] and [12] for possible (m, k) we obtain:

$(m, k) = (8, 1)$, $\mathbb{A}_8 = L_2(7)\mathbb{A}_{7,}$

$(m, k) = (9, 2)$, $\mathbb{A}_9 = L_2(8)\mathbb{A}_{7,}$

$(m, k) = (11, 4)$, $\mathbb{A}_{11} = M_{11}\mathbb{A}_{7,}$

$(m, k) = (12, 5)$, $\mathbb{A}_{12} = M_{12}\mathbb{A}_{7,}$

and these are all the possibilities in (c) of the Lemma. □

Lemma 4. *Let $\mathbb{A}_m = AB$ be a non-trivial factorization of $\mathbb{A}_m$, where A and B are subgroups of $\mathbb{A}_m$ with A a non-abelian simple group and $B \cong \mathbb{S}_7$. Then*

(a) $\mathbb{A}_m = \mathbb{A}_{m-1}\mathbb{S}_7$ *where* $m = 14$, 21, 30, 35, 42, 70, 84, 105, 120, 126, 140, 210, 240, 252, 280, 315, 360, 420, 504, 560, 630, 720, 840, 1008, 1260, 2520 *or* 5040.

(b) $\mathbb{A}_9 = L_2(8)\mathbb{S}_7$, $\mathbb{A}_{11} = M_{11}\mathbb{S}_7$, $\mathbb{A}_{12} = M_{12}\mathbb{S}_7$.

Proof. In this case we have $m \geqslant 9$. Using [14] again we obtain the groups listed in (a) in case $B \cong \mathbb{S}_7$ is a k-homogeneous group on m letters. If the simple group A is k-homogeneous on $m-$letters again using [3] and [12] together with Lemma 2 we will obtain the groups listed in (b) and the Lemma is proved. □

Remark 1. The factorizations $A_m = AB$ in cases (a), (b) and (c) of Lemma 3 all occur because actually A_m has subgroups isomorphic to A and B. The same is true for case (b) of Lemma 4. But for case (a) of Lemma 4 the equality $A_m = A_{m-1}S_7$ happens only if A_m has a subgroup isomorphic to S_7.

3. Main result

To find the structure of the factorizable simple groups $G = AB$ with A simple and $B \cong \mathbb{A}_7$ we need to know about the primitive groups of certain degrees which are equal to the indices of subgroups of $\mathbb{A}_7$. Simple primitive groups of degree at most 1000 are given in [8] and the index of most of the subgroups of $\mathbb{A}_7$ are less than 1000 except two indices which are 1260 and 2520. Therefore first we deal with these indices.

Lemma 5. *Let G be a non-abelian simple group which is not an alternating group. If G is a primitive group of degree 1260 or 2520, then G does not have a factorization $G = AB$ with A simple and $B \cong \mathbb{A}_7$.*

Proof. By the classification Theorem for the finite simple groups, G is isomorphic either to a sporadic simple group or a simple group of Lie type. By [10] there is no factorization as mentioned in the Lemma for a sporadic group. Therefore we will assume that G is a simple group of Lie type. If the rank of G is 1 or 2, then by [11] no desired factorization occurs. Hence we will assume that the Lie rank of G is at least 3. We will use results on the minimum index of a subgroup of a simple group of Lie type.

Case (a). $G = L_n(q)$, $n \geqslant 4$. In this case the minimum index of a proper subgroup of G is $\frac{(q^n-1)}{(q-1)}$. If $\frac{(q^n-1)}{(q-1)} \leqslant 2520$, then calculations reveal the following possibilities for G: $L_4(2)$, $L_4(3)$, $L_4(4)$, $L_4(5)$, $L_4(7)$, $L_4(8)$, $L_4(9)$, $L_4(11)$, $L_4(13)$, $L_5(2)$, $L_5(3)$, $L_5(4)$, $L_5(5)$, $L_5(7)$, $L_6(2)$, $L_6(3)$, $L_6(4)$, $L_7(2)$, $L_7(3)$, $L_8(2)$, $L_9(2)$, $L_{10}(2)$ or $L_{11}(2)$.

By [15], Proposition 4.8, the groups $L_4(q)$ with $q \not\equiv 1(8)$ are ruled out because they cannot have $\mathbb{A}_7$ in their factorization. Therefore among the possibilities of the form $L_4(q)$ only $L_4(9)$ needs examination. Assume $L_4(9) = A\mathbb{A}_7$ where A is a simple non-abelian group. Therefore $|A| = 2^7.3^{10}.5.13.41\ |A \cap \mathbb{A}_7|$. Since $A \cap \mathbb{A}_7$ is a proper subgroup of $\mathbb{A}_7$, hence $|A \cap \mathbb{A}_7|$ is one of the numbers: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 18, 20, 21, 24, 36, 60, 72, 120, 168 or 360. But by inspecting the simple groups A whose orders do not exceed $|L_4(9)|$ (at the end of [4]) with $13, 41 \mid |A|$, we find only one possibility for A, namely $A = O_8^-(3)$ of order $2^{10}.3^{12}.5.7.13.41$. But then we must have $|A \cap \mathbb{A}_7| = 2^3.3^2.7 = 504$ which is not the case. Therefore all the possibilities $L_4(q)$ are ruled out.

For the groups $L_5(q)$, again by [15], Proposition 4.7, if $q \equiv 3\ (4)$ there is no such factorization as mentioned in the Lemma. Hence the groups $L_5(3)$ and $L_5(7)$ are ruled out. For the groups $L_5(2)$, $L_5(4)$ and $L_5(5)$

similar arguments as used above rule out any factorization of these groups involving $\mathbb{A}_7$ and a simple subgroup. Factorization of the remaining groups in this case involving $\mathbb{A}_7$ are ruled out similarly and we omit the details.

Case (b). $G = U_n(q)$, $n \geqslant 6$. In this case a proper subgroup has index at least $\frac{(q^n-(-1)^n)(q^{n-1}-(-1)^{n-1})}{(q^2-1)}$ and if this number is less than or equal to 2520 we obtain only $G = U_6(2)$. But by [4] the group $U_6(2)$ has no maximal subgroup of index 1260 or 2520.

Case (c). $G = S_{2m}(q)$, $m \geqslant 3$. In this case if $q > 2$, then the index of a proper subgroup of G is at least $\frac{(q^{2m}-1)}{(q-1)}$ and if $q = 2$ then this number is $2^m(2^m-1)$. For these numbers to be less than or equal to 2520 we will obtain the following groups: $S_6(2)$, $S_6(3)$, $S_6(4)$, $S_8(2)$, $S_{10}(2)$ or $S_{12}(2)$. Now using [4] we see that the groups $S_6(2)$, $S_6(3)$ and $S_8(2)$ do not have maximal subgroups of index 1260 or 2520. For the groups $S_6(4)$, $S_{10}(2)$ and $S_{12}(2)$ similar arguments as used in case (a) rule out the possibility of factorizing these groups as product of a simple group and a group isomorphic to $\mathbb{A}_7$.

Case (d). $G = O^{\epsilon}_{2m}(q)$, $m \geqslant 4$, $\epsilon = \pm$. In this case the index of a proper subgroup is at least $\frac{(q^m-1)(q^{m-1}+1)}{(q-1)}$ when $\epsilon = +$, and is at least $\frac{(q^m+1)(q^{m-1}-1)}{(q-1)}$ when $\epsilon = -$ except in the case $(q,\epsilon) = (2,+)$ where this index is at least $2^{m-1}(2^m-1)$. For $G = O_{2m+1}(q)$, $m \geqslant 3$, q odd, $q > 3$, the index of a proper subgroup is at least $\frac{(q^{2m}-1)}{(q-1)}$ and if $q = 3$, this index is at least $\frac{(q^{2m}-q^m)}{(q-1)}$. Again calculations show that if an index is less than or equal to 2520, then $G = O_7(3)$, $O^{\pm}_8(2)$, $O^{\pm}_8(3)$, $O^{\pm}_{10}(2)$ or $O^{\pm}_{12}(2)$. Now again using [4] we ruled out any factorization of these groups involving $\mathbb{A}_7$.

Case (e). Finally we may assume that G is an exceptional simple group of Lie type. In this case by [14] factorizations of G are known and none of them involves $\mathbb{A}_7$. The Lemma is proved now. □

Theorem 1. *Let $G = AB$ be a non-trivial factorization of a simple group G with A a simple non-abelian group and $B \cong \mathbb{A}_7$. Then one of the following occurs:*

(a) $G = \mathbb{A}_m = \mathbb{A}_{m-1}\mathbb{A}_7$, *where* $m = 15$, 21, 35, 42, 70, 105, 120, 126, 140, 210, 252, 280, 315, 360, 420, 504, 630, 840, 1260 *or* 2520.

(b) $G = \mathbb{A}_{15} = \mathbb{A}_{13}\mathbb{A}_7$

(c) $G = \mathbb{A}_8$, $\mathbb{A}_9$, $\mathbb{A}_{11}$ *or* $\mathbb{A}_{12}$ *with appropriate factorizations:*
$\mathbb{A}_8 = L_2(7)\mathbb{A}_7$, $\mathbb{A}_9 = L_2(8)\mathbb{A}_7$, $\mathbb{A}_{11} = M_{11}\mathbb{A}_7$, $\mathbb{A}_{12} = M_{12}\mathbb{A}_7$

(d) $G = O^{+}_8(2) = S_6(2)\mathbb{A}_7$.

Proof. Suppose $G = AB$ is a factorization of a simple group G with A a simple non-abelian group and $B \cong \mathbb{A}_7$. We remind that by a factorization we mean a non-trivial factorization. If M is a maximal subgroup of G containing A, then $G = AB$, hence $[G : M] \mid [B : B \cap M]$. Since $d = [B : B \cap M]$ is equal to the index of a subgroup of $\mathbb{A}_7$, therefore G is a primitive permutation group of degree d. We have $d = 1$, 7, 15, 21, 35, 42, 70, 105, 120, 126, 140, 210, 252, 280, 315, 360, 420, 504, 630, 840, 1260 or 2520. Obviously $d \neq 1$, 7. By Lemma 5 if $d = 1260$ or 2520, then G is isomorphic to an alternating group of these degrees. If G is an alternating group, then by Lemma 3 we obtain the cases (a), (b) and (c) in the Theorem. We will prove if G is not an alternating group, then $G \cong O_8^+(2)$.

Since the remaining degrees d are less than 1000, hence we may use [8]. By Table I in [7] which is obtained from [8] we need only consider primitive simple groups G of degree 21, 105, 120, 126, 280, 315 and 840. Now using [10] and [11] the only cases that we should consider are $S_6(2)$, $S_8(2)$ or $O_8^+(2)$.

If $S_6(2) = A\mathbb{A}_7$, then $|A| = 2^6.3^2\ |A \cap \mathbb{A}_7|$. But $|A|$ must be divisible by at least three distinct primes. Therefore if $A \cap \mathbb{A}_7$ is a proper subgroup of $\mathbb{A}_7$ we must have $|A \cap \mathbb{A}_7| = 5$, 10, 20, 60, 360, 7, 21, 168. Hence $|A| = 2^6.3^2.5$, $2^7.3^2.5$, $2^8.3^2.5$, $2^9.3^3.5$, $2^9.3^4.5$, $2^6.3^2.7$, $2^6.3^3.7$, $2^9.3^3.7$. But by [4] there is no simple group of the above orders.

If $S_8(2) = A\mathbb{A}_7$, then $|A| = 2^{13}.3^3.5.17\ |A \cap \mathbb{A}_7|$. By [4] there is no simple group A such that $2^{13}.3^3.5.17 \mid |A| \mid |S_8(2)|$.

If $O_8^+(2) = A\mathbb{A}_7$, then $|A| = 2^9.3^3.5\ |A \cap \mathbb{A}_7|$. Now $2^9.3^3.5 \mid |A|$ and $|A| \mid 2^{12}.3^5.5^2.7 = \left|O_8^+(2)\right|$. By [4] the only possibility is $A \cong S_6(2)$. Again by [4] and using Lemma 1 we obtain $O_8^+(2) = S_6(2)\mathbb{A}_9$. The intersection of the two factors is a group $H = L_2(8) : 3 = P\Gamma L_2(8)$ and since it acts 2-transitively on 9 points we have $\mathbb{A}_9 = P\Gamma L_2(8).\mathbb{A}_7$, hence $O_8^+(2) = S_6(2)\mathbb{A}_7$ and the Theorem is proved. □

In conclusion we will prove the following Corollary.

Corollary. *Suppose that* $G = AB$ *with* A *a simple group and* B *isomorphic to* $\mathbb{A}_7$. *Then, either* $G = A \supseteq B$, $G \cong A \times B$, *or* G *is as in the Theorem* 1.

Proof. By induction, if G is not simple, G is not isomorphic to $A \times B$, and G is a minimal normal subgroup of G, then $\frac{G}{N}$is simple. By lemma 1 of [17], $|N|$ divides the order of $\mathbb{A}_7$, $|N| = 8$ (which is impossible as $C(N) = N$ and hence, $\mathbb{A}_7$ is isomorphic to a subgroup of $Aut(N)$) or $|N| = p$ where p is a prime dividing $|\mathbb{A}_7|$ for which the Sylow subgroup is non-abelian. It follows that $p = 2$ and $N = Z(G)$. Thus, G is a covering group of the simple group $\frac{G}{N} = (\frac{AN}{N})(\frac{BN}{N})$ which is as in the Theorem 1. But this is impossible as theorem 10 of [17] shows that $\frac{G}{N}$ cannot be isomorphic to an alternating group and a simple order argument shows $\frac{G}{N}$ cannot be isomorphic to $O_8^+(2)$. The result follows. □

Acknowledgement. This work has been supported by the Research Institute for Fundamental Science, Tabriz, Iran. The author would like to thank this support. The author also deeply thanks Dr. Y. Farjami of the mathematics department of the University of Tehran for discussions concerning this paper. Finally, the author would like to express his deep gratitude to the referee for useful remarks concerning Corollary.

References

[1] **B. Amberg, S. Franciosi and F. DeGiovanni**: *Products of groups*, Oxford University Press, 1992.

[2] **Z. Arad and E. Fisman**: *On finite factorizable groups*, J. Algebra **86** (1984), 522 – 548.

[3] **P. J. Cameron**: *Permutation groups*, Cambridge University Press, 1999.

[4] **J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson**, Atlas of Finite Groups, Clarendon Press, Oxford, 1985.

[5] **M. R. Darafsheh and G. R. Rezaeezadeh**: *Factorization of groups involving symmetric and alternating groups*, International J. Math. and Math. Sci. **27** (2001), No.3, 161 – 167.

[6] **M. R. Darafsheh and G. R. Rezaeezadeh and G. L. Walls**: *Groups which are the product of* $\mathbb{S}_6$ *and a simple group*, Alg. Colloq. **10** (2003), No.2, 195 – 204.

[7] **M. R. Darafsheh**: *Product of the symmetric group with the alternating group on seven letters*, Quasigroups and Related Systems **9** (2002), 33 – 44.

[8] **J. D. Dixon and B. Mortimer**: *The primitive permutation groups of degree less than 1000*, Math. Proc. Cam. Phil. Soc. **103** (1998), 213 – 238.

[9] **P. Etingof, S. Gelaki, R. Guralnick and J. Saxl**: *Biperfect Hopf algebras*, J. Algebra **232** (2000), 331 – 335.

[10] **T. R. Gentchev**: *Factorizations of the sporadic simple groups*, Arch. Math. **47** (1986), 97 – 102.

[11] **T. R. Gentchev**: *Factorization of the groups of Lie type of Lie rank* 1 *or* 2, Arch. Math. **47** (1986), 493 – 499.

[12] **W. M. Kantor**: *k-homogeneous groups*, Math. Z. **124** (1972), 261 – 265.

[13] **O. Kegel and H. Luneberg**: *Uber die kleine reidermeister bedingungen*, Arch. Mat. (Basel) **14** (1963), 7 – 10.

[14] **M. W. Liebeck, C. E. Praeger and J. Saxl**: *The maximal factorizations of the finite simple groups and their authomorphism groups*, Mem. AMS **86**, No. 432, 1990.

[15] **U. Preiser**: *Factorization of finite groups*, Math. Z. **185** (1984), 373 – 402.

[16] **W. R. Scott**: *Products of $\mathbb{A}_5$ and a finite simple group*, J. Algebra **37** (1975), 165 – 171.

[17] **G. L. Walls**: *Non-simple groups which are the product of simple groups*, Arch. Math. **53** (1989), 209 – 216.

[18] **G. L. Walls**: *Products of simple groups and symmetric groups*, Arch. Math. **58** (1992), 313 – 321.

[19] **J. Wiegold and A. G. Williamson**: *The factorization of the alternating and symmetric groups*, Math. Z. **175** (1980), 171 – 179.

Received December 20, 2004
Revised March 29, 2005

Department of Mathematics
Statistics and Computer Science
Faculty of Science, University of Tehran
Tehran, Iran

and

Research Institute for Fundamental Science
Tabriz, Iran
e-mail : darafsheh@ut.ac.ir

Quasigroups and Related Systems **13** (2005), 213 – 228

Intuitionistic fuzzy approach to n-ary systems

Wiesław A. Dudek

Abstract

We adopt the fundamental concepts of intuitionistic fuzzy subalgebras to n-ary groupoids, i.e., on algebras containing one n-ary operation. We describe some similarities and differences between the n-ary and binary case. In the case of n-ary quasigroups and groups we suggest the common method of investigations based on some methods used in the universal algebra.

1. Introduction

After the introduction of the concept of fuzzy sets by Zadeh, several researches were conducted on the generalizations of the notion of fuzzy set and application to many algebraic structures such as: groups, quasigroups, rings, semirings, BCK-algebras et cetera. All these applications are connected with binary operations.

But in many branches of mathematics (also in applications) one can find so-called *n-ary groupoids*, i.e., sets with one n-ary operation $f : G^n \to G$, where $n \geqslant 2$ is fixed. Such groupoid are called also *polyadic* or *n-ary systems* and are investigated by many authors, for example by Post [15] and Belousov [2]. Some special types of n-ary groupoids are used by Belousov in the theory of nets [2]. Mullen and Shcherbakov studied codes based on n-ary quasigroups [13]. Grzymała-Busse applied polyadic groupoids to the theory of automata [10]. Applications in modern physics are described by Kerner [11]. In such applications some role plays (intuitionistic) fuzzy subsets.

The main role in the theory of n-ary systems plays n-ary groups and quasigroups, which are a natural generalization of binary ($n = 2$) groups

2000 Mathematics Subject Classification: 20N15, 94D05

Keywords: n-ary system, n-ary quasigroup, intuitionistic fuzzy n-ary quasigroup.

and quasigroups. It is clear that many classical results can be extended to the n-ary case. But for $n > 2$ we obtain the large set of theorems which are not true for $n = 2$. Moreover, the part of obtained results is true only for ternary ($n = 3$) groupoids.

2. Preliminaries

According to the general convention used in the theory of n-ary systems the sequence of elements $x_i, \ldots, x_j$ will be denoted by x_i^j (for $j < i$ it is empty symbol). This means that $f(x_1, x_2, \ldots, x_n)$ will be written as $f(x_1^n)$.

An n-ary groupoid (G, f) is called *unipotent* if it contains an element θ such that $f(x, x, \ldots, x) = \theta$ for all $x \in G$. Such groupoid is obviously an *n-ary semigroup*, i.e., for all $i, j \in \{1, 2, \ldots, n\}$ and $x_1^{2n-1} \in G$ it satisfies the *n-ary associativity*

$$f(x_1^{i-1}, f(x_i^{n+i-1}), x_{n+i}^{2n-1}) = f(x_1^{j-1}, f(x_j^{n+j-1}), x_{n+j}^{2n-1}),$$

which is a natural generalization on the classical associativity.

An *n-ary quasigroup* is defined as an n-ary groupoid (G, f) in which for all $1 \leqslant i \leqslant n$ and all $x_0^n \in G$ there exists a uniquely determined element $z_i \in G$ such that

$$f(x_1^{i-1}, z_i, x_{i+1}^n) = x_0 \,. \tag{1}$$

An n-ary quasigroup (G, f) in which the operation f is associative in the above sense is called an n-ary group. For $n = 2$ we obtain an arbitrary group.

It is worthwhile to note that, under the assumption of the associativity of the operation f, it suffices only to postulate the existence of a solution of (1) at the place $i = 1$ and $i = n$ or at one place i other than 1 and n. Then one can prove uniqueness of the solution of (1) for all $1 \leqslant i \leqslant n$ (cf. [15], p.213^{17}).

For any fixed n, the class of all n-ary groups is a variety. Very useful systems of identities defining this variety one can find in [9] and [7].

3. Intuitionistic fuzzy subgroupoids

Now generalize some classical results obtained for binary algebras such as BCC-algebras [8] and groups [16] to the case of n-ary groupoids.

Definition 3.1. A fuzzy set μ defined on G is called a *fuzzy subgroupoid* of an n-ary groupoid (G,f) if

$$\mu(f(x_1^n)) \geqslant \min\{\mu(x_1),\, \ldots,\, \mu(x_n)\}$$

for all $x_1^n \in G$.

Lemma 3.2. *If μ is a fuzzy subgroupoid of a unipotent groupoid (G,f), then $\mu(\theta) \geqslant \mu(x)$ for all $x \in G$ and $\theta = f(x,x,\ldots,x)$.*

Analogously as in a binary case we can prove

Theorem 3.3. *A fuzzy set μ of an n-ary groupoid (G,f) is a fuzzy subgroupoid if and only if for every $t \in [0,1]$, the level*

$$L(\mu,t) = \{x \in G : \mu(x) \geqslant t\}$$

is either empty or a subgroupoid of (G,f).

This implies that (similarly as in a binary case) any subgroupoid of (G,f) can be realized as a level subgroupoid of some fuzzy subgroupoid μ defined on G.

The *complement* of μ, denoted by $\overline{\mu}$, is the fuzzy set in G given by $\overline{\mu}(x) = 1 - \mu(x)$ for all $x \in G$.

An *intuitionistic fuzzy set* (IFS for short) of a nonempty set X is defined by Atanassov (cf. [1]) in the following way.

Definition 3.4. An *intuitionistic fuzzy set* A of a nonempty set X is an object having the form

$$A = \{(x, \mu_A(x), \gamma_A(x)) : x \in X\},$$

where $\mu_A : X \to [0,1]$ and $\gamma_A : X \to [0,1]$ denote the degree of membership (namely $\mu_A(x)$) and the degree of nonmembership (namely $\gamma_A(x)$) of each element $x \in X$ to the set A, respectively, and $0 \leqslant \mu_A(x) + \gamma_A(x) \leqslant 1$ for all $x \in X$.

For the sake of simplicity, we shall use the symbol $A = (\mu_A, \gamma_A)$ for the intuitionistic fuzzy set $A = \{(x, \mu_A(x), \gamma_A(x)) : x \in X\}$.

Definition 3.5. An IFS $A = (\mu_A, \gamma_A)$ of an n-ary groupoid (G,f) is an *intuitionistic fuzzy subgroupoid* (*IFS subgroupoid* for short) if

$$\mu_A(\,f(x_1^n)\,) \geqslant \min\{\mu_A(x_1),\, \ldots,\, \mu_A(x_n)\}$$
$$\gamma_A(\,f(x_1^n)\,) \leqslant \max\{\gamma_A(x_1),\, \ldots,\, \gamma_A(x_n)\}$$

hold for all $x_1^n \in G$.

It is not difficult to see that the following statements are true.

Proposition 3.6. *If $A = (\mu_A, \gamma_A)$ is an IFS intuitionistic fuzzy subgroupoid of (G, f), then so is $\Box A = (\mu_A, \overline{\mu_A})$ and $\Diamond A = (\overline{\gamma_A}, \gamma_A)$.*

Proposition 3.7. *If $A = (\mu_A, \gamma_A)$ is an IFS subgroupoid of a unipotent n-ary groupoid (G, f), then $\mu_A(\theta) \geqslant \mu_A(x)$ and $\gamma_A(\theta) \leqslant \gamma_A(x)$ for all $x \in G$ and $\theta = f(x, \dots, x)$.*

Proposition 3.8. *If $A = (\mu_A, \gamma_A)$ is an IFS subgroupoid of a unipotent n-ary groupoid (G, f), then*

$$G_\mu = \{x \in G : \mu_A(x) = \mu_A(\theta)\} \quad \text{and} \quad G_\gamma = \{x \in G : \gamma_A(x) = \gamma_A(\theta)\}$$

are subgroupoids of (G, f).

In some n-ary groupoids there exists an element e satisfying the identity

$$f(e, \dots, e, x, e, \dots, e) = x,$$

where x is at the place k. Such element (if it exists) is called a *k-identity*. There are n-ary groupoids containing two or three such elements. Moreover, there are groupoids containing only such elements. For example, in any n-ary group derived from a commutative group $(G, +)$, i.e., in an n-ary groupoid (G, f) with the operation $f(x_1^n) = x_1 + x_2 + \ldots + x_n$, all elements satisfying the identity $nx = x$ are k-identities (for every k). But the set of all k-identities is not an n-ary subgroupoid in general (cf. [6]).

Proposition 3.9. *If $A = (\mu_A, \gamma_A)$ is an IFS subgroupoid of an n-ary groupoid (G, f) with a k-identity e, then $\mu_A(e) \geqslant \mu_A(x)$ and $\gamma_A(e) \leqslant \gamma_A(x)$ for all $x \in G$ and*

$$G_\mu = \{x \in G : \mu_A(x) = \mu_A(e)\}$$
$$G_\gamma = \{x \in G : \gamma_A(x) = \gamma_A(e)\}$$

are subgroupoids of (G, f).

Obviously $\mu_A(e_1) = \mu_A(e_2)$ and $\gamma_A(e_1) = \gamma_A(e_2)$ for any k-identity e_1 and t-identity e_2. This means that in n-ary groupoids containing only k-identities all IFS subgroupoids are constant.

For any $\alpha \in [0,1]$ and fuzzy set μ of G, the set

$$U(\mu;\alpha) = \{x \in G \ : \mu(x) \geqslant \alpha\}$$
$$L(\mu;\alpha) = \{x \in G : \mu(x) \leqslant \alpha\}$$

is called an *upper* (respectively *lower*) *α-level cut* of μ.

Theorem 3.10. *If $A = (\mu_A, \gamma_A)$ is an IFS subgroupoid of an n-ary groupoid (G,f), then the sets $U(\mu_A;\alpha)$ and $L(\gamma_A;\alpha)$ are subgroupoids of (G,f) for every $\alpha \in \mathrm{Im}(\mu_A) \cap \mathrm{Im}(\gamma_A)$.*

Theorem 3.11. *If $A = (\mu_A, \gamma_A)$ is an IFS in an n-ary groupoid (G,f) such that the nonempty sets $U(\mu_A;\alpha)$ and $L(\gamma_A;\alpha)$ are subgroupoids of (G,f) for all $\alpha \in [0,1]$. Then $A = (\mu_A, \gamma_A)$ is an IFS subgroupoid of (G,f).*

The proof of the above two theorems is analogous to the proof of the corresponding theorems for binary groupoids (cf. [12]).

Also it is not difficult to verify that the following two statements are true.

Theorem 3.12. *Let B be a nonempty subset of an n-ary groupoid (G,f) and let $A = (\mu_A, \gamma_A)$ be an intuitionistic fuzzy set on G defined by*

$$\mu_A(x) = \begin{cases} s_0 & \textit{if } x \in B, \\ s_1 & \textit{otherwise}, \end{cases}$$

and

$$\gamma_A(x) = \begin{cases} t_0 & \textit{if } x \in B, \\ t_1 & \textit{otherwise}, \end{cases}$$

for all $x \in G$ and $s_i, t_i \in [0,1]$, where $s_0 > s_1$, $t_0 < t_1$ and $s_i + t_i \leqslant 1$ for $i = 0,1$. Then $A = (\mu_A, \gamma_A)$ is an IFS subgroupoid of (G,f) if and only if B is an n-ary subgroupoid of (G,f). Moreover, $U(\mu_A; s_0) = B = L(\gamma_A; t_0)$.

Corollary 3.13. *Let χ_A be the characteristic function of an n-ary subgroupoid of an n-ary groupoid (G,f). Then the intuitionistic fuzzy set $A_\sim = (\chi_A, \overline{\chi_A})$ is an IFS subgroupoid of (G,f).*

A fuzzy set μ defined on G is said to be *normal* if there exists $x \in G$ such that $\mu(x) = 1$. A simple example of normal fuzzy sets are characteristic functions of subsets of G.

If an n-ary groupoid (G,f) is unipotent, then a fuzzy set μ defined on G is normal if and only if $\mu(\theta) = 1$, where $\theta = f(x,x,\ldots,x)$.

The set $\mathcal{N}(G,f)$ of all normal fuzzy subgroupoids on (G,f) is partially ordered by the relation

$$\mu \sqsubseteq \rho \Longleftrightarrow \mu(x) \leqslant \rho(x)$$

for all $x \in G$.

Moreover, similarly as in the binary case, for any fuzzy subgroupoid μ of (G,f) there exists $\rho \in \mathcal{N}(G,f)$ such that $\mu \sqsubseteq \rho$. If an n-ar groupoid (G,f) is unipotent, then the maximal element of $(\mathcal{N}(G,f),\sqsubseteq)$ is either constant or characteristic function of some subset of G.

4. Fuzzification of quasigroups

A groupoid $(G,\cdot\,)$ is called a *quasigroup* if each of the equations $ax = b$, $xa = b$ has a unique solution for any $a,b \in G$.

A fuzzification of quasigroups (binary and n-ary) is more complicated as a fuzzification of arbitrary groups (cf. for example [16]). The problem lies in the fact that a subset of a quasigroup $(G,\cdot)$ closed with respect to the quasigroup operation in general is not a quasigroup with respect to this operation.

A fuzzification of quasigroups (cf. [4, 12]) is based on the second equivalent definition of a quasigroup. Namely, (cf. [14]) a quasigroup $(G,\cdot)$ may be defined as an algebra $(G,\cdot,\backslash,/)$ with the three binary operations $\cdot$, $\backslash$, $/$ satisfying the identities

$$(xy)/y = x, \quad x\backslash(xy) = y,$$
$$(x/y)y = x, \quad x(x\backslash y) = y.$$

The quasigroup $(G,\cdot,\backslash,/)$ corresponds to quasigroup $(G,\cdot)$, where

$$x\backslash y = z \Longleftrightarrow xz = y \quad \text{and} \quad x/y = z \Longleftrightarrow zy = x.$$

A quasigroup is called *unipotent* if $xx = yy$ for all $x,y \in G$. These quasigroups are connected with Latin squares which have one fixed element in the diagonal. Such quasigroups may be defined as quasigroups $(G,\cdot)$ with the special element θ satisfying the identity $xx = \theta$. In this case also $x\backslash\theta = x$ and $\theta/x = x$ for all $x \in G$.

A nonempty subset S of a quasigroup $(G,\cdot,\backslash,/)$ is called a *subquasigroup* if it is closed under these three operations $\cdot$, $\backslash$, $/$, i.e., if $x * y \in S$ for all $* \in \{\cdot,\backslash,/\}$ and $x,y \in S$.

Thus a fuzzy set μ on a quasigroup $(G,\cdot\,)$ is a *fuzzy subquasigroup* if $\mu(x*y) \geqslant \min\{\mu(x),\mu(y)\}$ for all $* \in \{\cdot,\backslash,/\}$ and $x,y \in S$ (cf. [4]).

In the case of n-ary quasigroups the situation is more complicated. According to [2] in any n-ary quasigroup (G,f) for every $s=1,2,\ldots,n$ one can define the *s-th inverse n-ary operation* $f^{(s)}$ putting

$$f^{(s)}(x_1^n)=y \Longleftrightarrow f(x_1^{s-1},y,x_{s+1}^n)=x_s\,.$$

Obviously, the operation $f^{(s)}$ is the s-inverse operation for the operation f if and only if

$$f^{(s)}(x_1^{s-1},f(x_1^n),x_{s+1}^n)=x_s$$

for all $x_1^n\in G$ (cf. [2]). Therefore the class of all n-ary quasigroups may be treated as the variety of equationally definable algebras with $n+1$ fundamental operations $f,f^{(1)},\ldots,f^{(n)}$.

A nonempty subset S of G is called a *subquasigroup* of (G,f) if it is an n-ary quasigroup with respect to f. This means that a nonempty subset S of an n-ary quasigroup (G,f) is an *n-ary subquasigroup* if and only if it is closed with respect to $n+1$ operations $f,f^{(1)},\ldots,f^{(n)}$, i.e., if and only if $g(x_1^n)\in G$ for all $x_1^n\in G$ and all $g\in\mathcal{F}=\{f,f^{(1)},f^{(2)},\ldots,f^{(n)}\}$.

Basing on the Definition 3.1 we can define a fuzzy subquasigroup of an n-ary quasigroup in the following way.

Definition 4.1. A fuzzy set μ defined on G is called a *fuzzy subquasigroup* of an n-ary quasigroup (G,f) if

$$\mu(g(x_1^n))\geqslant\min\{\mu(x_1),\,\ldots,\,\mu(x_n)\}$$

for all $g\in\mathcal{F}$ and $x_1^n\in G$.

For such defined fuzzy subquasigroups we can prove results analogous to the results from the previous part.

Definition 4.2. An IFS $A=(\mu_A,\gamma_A)$ of an n-ary quasigroup (G,f) is an *intuitionistic fuzzy subquasigroup* (*IFS subquasigroup* for short) if

$$\mu_A(\,g(x_1^n)\,)\geqslant\min\{\mu_A(x_1),\,\ldots,\,\mu_A(x_n)\}$$
$$\gamma_A(\,g(x_1^n)\,)\leqslant\max\{\gamma_A(x_1),\,\ldots,\,\gamma_A(x_n)\}$$

hold for all $g\in\mathcal{F}$ and $x_1^n\in G$.

It is not difficult to see that in an n-ary quasigroup an IFS subquasigroup is an IFS subgroupoid and the results of the previous part will be true for n-ary quasigroup if we replace "IFS subgroupoid" by "IFS subquasigroup".

Moreover, the following characterization of IFS subquasigroups is valid.

Lemma 4.3. *$A=(\mu_A,\gamma_A)$ is an IFS subquasigroup of an n-ary quasigroup (G,f) if and only if μ_A and $\overline{\gamma_A}$ are fuzzy subquasigroups of (G,f).*

Proof. Straightforward. □

Theorem 4.4. *If $A=(\mu_A,\gamma_A)$ is an IFS in an n-ary quasigroup (G,f) such that the nonempty sets $U(\mu_A;\alpha)$ and $L(\gamma_A;\alpha)$ are subquasigroups of (G,f) for all $\alpha\in[0,1]$. Then $A=(\mu_A,\gamma_A)$ is an IFS subquasigroup of (G,f).*

Proof. Let $\alpha\in[0,1]$. Assume that $U(\mu_A;\alpha)\neq\emptyset$ and $L(\gamma_A;\alpha)\neq\emptyset$ are subquasigroups of an n-ary quasigroup (G,f). We must show that $A=(\mu_A,\gamma_A)$ satisfies the Definition 4.2.

Let $g\in\mathcal{F}$. If the first condition of the Definition 4.2 is false, then there exist $x_1^n\in G$ such that

$$\mu_A(g(x_1^n))<\min\{\mu_A(x_1),\ldots,\mu_A(x_n)\}.$$

Taking

$$\alpha_0=\frac{1}{2}\big[\mu_A(g(x_1^n))+\min\{\mu_A(x_1),\ldots,\mu_A(x_n)\}\big],$$

we have

$$\mu_A(g(x_1^n))<\alpha_0<\min\{\mu_A(x_1),\ldots,\mu_A(x_n)\}.$$

It follows that x_1^n are in $U(\mu_A;\alpha_0)$ but $g(x_1^n)$ are not in $U(\mu_A;\alpha_0)$, which is a contradiction.

Assume that the second condition of the Definition 4.2 does not hold. Then

$$\gamma_A(g(x_1^n))>\max\{\gamma_A(x_1),\ldots,\gamma_A(x_n)\}$$

for some $x_1^n\in G$. Let

$$\beta_0=\frac{1}{2}\big[\gamma_A(g(x_1^n))+\max\{\gamma_A(x_1),\ldots,\gamma_A(x_n)\}\big].$$

Then

$$\gamma_A(g(x_1^n))>\beta_0>\max\{\gamma_A(x_1),\ldots,\gamma_A(x_n)\}$$

and so $x_1^n\in L(\gamma_A;\beta_0)$ but $g(x_1^n)\notin L(\gamma_A;\beta_0)$. This contradiction completes the proof. □

Proposition 4.5. *If $A=(\mu_A,\gamma_A)$ is an IFS subquasigroup of an n-ary quasigroup (G,f), then for all $i=1,\ldots,n,\ g\in\mathcal{F}$ we have*

$$\min\{\mu_A(g(x_1^n)),\min\{\bigwedge_{i\neq s}\mu_A(x_i)\}\}=\min\{\mu_A(x_1),...,\mu_A(x_n)\},$$
$$\max\{\gamma_A(g(x_1^n)),\min\{\bigwedge_{i\neq s}\gamma_A(x_i)\}\}=\max\{\gamma_A(x_1),\ldots,\gamma_A(x_n)\}.$$

Proof. Indeed, for $g=f$ we have

$$\begin{aligned}&\min\{\mu_A(f(x_1^n)),\min\{\bigwedge_{i\neq s}\mu_A(x_i)\}\}\geqslant\\&\min\{\min\{\mu_A(x_1),...,\mu_A(x_n)\},\min\{\bigwedge_{i\neq s}\mu_A(x_i)\}\}=\\&\min\{\mu_A(x_1),...,\mu_A(x_n)\}=\\&\min\{\mu_A(f^{(s)}(x_1^{s-1},f(x_1^n),x_{s+1}^n)),\min\{\bigwedge_{i\neq s}\mu_A(x_i)\}\}\geqslant\\&\min\{\min\{\mu_A(f(x_1^n)),\min\{\bigwedge_{i\neq s}\mu_A(x_i)\}\},\min\{\bigwedge_{i\neq s}\mu_A(x_i)\}\}=\\&\min\{\mu_A(f(x_1^n)),\min\{\bigwedge_{i\neq s}\mu_A(x_i)\}\},\end{aligned}$$

which completes the proof in this case. The rest is analogous. □

Theorem 4.6. *If $A=(\mu_A,\gamma_A)$ is an IFS subquasigroup of (G,f), then*

$$\mu_A(x)=\sup\{\alpha\in[0,1]:x\in U(\mu_A;\alpha)\}$$

and

$$\gamma_A(x)=\inf\{\alpha\in[0,1]:x\in L(\gamma_A;\alpha)\}$$

for all $x\in G$.

Proof. Let $\delta=\sup\{\alpha\in[0,1]:x\in U(\mu_A;\alpha)\}$ and let $\varepsilon>0$ be given. Then $\delta-\varepsilon<\alpha$ for some $\alpha\in[0,1]$ such that $x\in U(\mu_A;\alpha)$. This means that $\delta-\varepsilon<\mu_A(x)$ so that $\delta\leqslant\mu_A(x)$ since ε is arbitrary.

We now show that $\mu_A(x)\leqslant\delta$. If $\mu_A(x)=\beta$, then $x\in U(\mu_A;\beta)$ and so

$$\beta\in\{\alpha\in[0,1]:x\in U(\mu_A;\alpha)\}.$$

Hence

$$\mu_A(x)=\beta\leqslant\sup\{\alpha\in[0,1]:x\in U(\mu_A;\alpha)\}=\delta.$$

Therefore

$$\mu_A(x)=\delta=\sup\{\alpha\in[0,1]:x\in U(\mu_A;\alpha)\}.$$

Now let $\eta = \inf\{\alpha \in [0,1] : x \in L(\gamma_A;\alpha)\}$. Then

$$\inf\{\alpha \in [0,1] : x \in L(\gamma_A;\alpha)\} < \eta + \varepsilon$$

for any $\varepsilon > 0$, and so $\alpha < \eta + \varepsilon$ for some $\alpha \in [0,1]$ with $x \in L(\gamma_A;\alpha)$. Since $\gamma_A(x) \leqslant \alpha$ and ε is arbitrary, it follows that $\gamma_A(x) \leqslant \eta$.

To prove $\gamma_A(x) \geqslant \eta$, let $\gamma_A(x) = \zeta$. Then $x \in L(\gamma_A;\zeta)$ and thus $\zeta \in \{\alpha \in [0,1] : x \in L(\gamma_A;\alpha)\}$. Hence

$$\inf\{\alpha \in [0,1] : x \in L(\gamma_A;\alpha)\} \leqslant \zeta,$$

i.e., $\eta \leqslant \zeta = \gamma_A(x)$. Consequently

$$\gamma_A(x) = \eta = \inf\{\alpha \in [0,1] : x \in L(\gamma_A;\alpha)\},$$

which completes the proof. □

Theorem 4.7. *Let $\{\mathcal{H}_\alpha : \alpha \in \Lambda\}$, where Λ is a nonempty subset of $[0,1]$, be a family of subquasigroups of (G,f) such that*

(a) $G = \bigcup\limits_{\alpha\in\Lambda} H_\alpha$,

(b) $\alpha > \beta \Longleftrightarrow H_\alpha \subset H_\beta$ *for all* $\alpha,\beta \in \Lambda$.

Then an IFS $A = (\mu_A,\gamma_A)$ defined by

$$\mu_A(x) = \sup\{\alpha \in \Lambda : x \in H_\alpha\} \quad \textit{and} \quad \gamma_A(x) = \inf\{\alpha \in \Lambda : x \in H_\alpha\}$$

is an IFS subguasigroup of (G,f).

Proof. According to Theorem 4.4, it is sufficient to show that the nonempty sets $U(\mu_A;\alpha)$ and $L(\gamma_A;\beta)$ are subquasigroups of (G,f).

In order to prove that $U(\mu_A;\alpha) \neq \emptyset$ is a subquasigroup of $\mathcal{G}$, we consider the following two cases:

(i) $\alpha = \sup\{\delta \in \Lambda : \delta < \alpha\}$ and (ii) $\alpha \neq \sup\{\delta \in \Lambda : \delta < \alpha\}$.

Case (i) implies that

$$x \in U(\mu_A;\alpha) \Longleftrightarrow \big(x \in H_\delta \;\forall\; \delta < \alpha\big) \Longleftrightarrow x \in \bigcap_{\delta<\alpha} H_\delta,$$

so that $U(\mu_A;\alpha) = \bigcap\limits_{\delta<\alpha} H_\delta$ which is a subquasigroup of (G,f).

For the case (ii), we claim that

$$U(\mu_A;\alpha) = \bigcup_{\delta\geqslant\alpha} H_\delta.$$

If $x \in \bigcup\limits_{\delta \geqslant \alpha} H_\delta$ then $x \in H_\delta$ for some $\delta \geqslant \alpha$. It follows that $\mu_A(x) \geqslant \delta \geqslant \alpha$, so that $x \in U(\mu_A; \alpha)$. This shows that $\bigcup\limits_{\delta \geqslant \alpha} H_\delta \subseteq U(\mu_A; \alpha)$.

Now assume that $x \notin \bigcup\limits_{\delta \geqslant \alpha} H_\delta$. Then $x \notin H_\delta$ for all $\delta \geqslant \alpha$. Since $\alpha \neq \sup\{\delta \in \Lambda : \delta < \alpha\}$, there exists $\varepsilon > 0$ such that $(\alpha - \varepsilon, \alpha) \cap \Lambda = \emptyset$. Hence $x \notin H_\delta$ for all $\delta > \alpha - \varepsilon$, which means that if $x \in H_\delta$ then $\delta \leqslant \alpha - \varepsilon$. Thus $\mu_A(x) \leqslant \alpha - \varepsilon < \alpha$, and so $x \notin U(\mu_A; \alpha)$. Therefore $U(\mu_A; \alpha) \subseteq \bigcup\limits_{\delta \geqslant \alpha} H_\delta$, and thus $U(\mu_A; \alpha) = \bigcup\limits_{\delta \geqslant \alpha} H_\delta$, which is a subquasigroup of $\mathcal{G}$.

Now we prove that $L(\gamma_A; \beta)$ is a subquasigroup of (G, f). We consider the following two cases:

(iii) $\beta = \inf\{\eta \in \Lambda : \beta < \eta\}$ and (iv) $\beta \neq \inf\{\eta \in \Lambda : \beta < \eta\}$.

For the case (iii) we have

$$x \in L(\gamma_A; \beta) \Longleftrightarrow \big(x \in H_\eta \ \forall\, \eta > \beta\big) \Longleftrightarrow x \in \bigcap_{\eta > \beta} H_\eta$$

and hence $L(\gamma_A; \beta) = \bigcap\limits_{\eta > \beta} H_\eta$ which is a subquasigroup of (G, f).

For the case (iv), there exists $\varepsilon > 0$ such that $(\beta, \beta + \varepsilon) \cap \Lambda = \emptyset$. We will show that $L(\gamma_A; \beta) = \bigcup\limits_{\eta \leqslant \beta} H_\eta$. If $x \in \bigcup\limits_{\eta \leqslant \beta} H_\eta$ then $x \in H_\eta$ for some $\eta \leqslant \beta$. It follows that $\gamma_A(x) \leqslant \eta \leqslant \beta$ so that $x \in L(\gamma_A; \beta)$. Hence $\bigcup\limits_{\eta \leqslant \beta} H_\eta \subseteq L(\gamma_A; \beta)$.

Conversely, if $x \notin \bigcup\limits_{\eta \leqslant \beta} H_\eta$ then $x \notin H_\eta$ for all $\eta \leqslant \beta$, which implies that $x \notin H_\eta$ for all $\eta < \beta + \varepsilon$, i.e., if $x \in H_\eta$ then $\eta \geqslant \beta + \varepsilon$. Thus $\gamma_A(x) \geqslant \beta + \varepsilon > \beta$, i.e., $x \notin L(\gamma_A; \beta)$. Therefore $L(\gamma_A; \beta) \subseteq \bigcup\limits_{\eta \leqslant \beta} H_\eta$ and consequently $L(\gamma_A; \beta) = \bigcup\limits_{\eta \leqslant \beta} H_\eta$ which is a subquasigroup of (G, f). This completes the proof. □

Let $IFS(G, f)$ be the family of all IFS subquasigroups of (G, f) and $\alpha \in [0, 1]$ be a fixed real number. For any $A = (\mu_A, \gamma_A)$ and $B = (\mu_B, \gamma_B)$ from $IFS(G, f)$ we define two binary relations $\mathbf{U}^\alpha$ and $\mathbf{L}^\alpha$ on $IFS(G, f)$ as follows:

$$(A, B) \in \mathbf{U}^\alpha \Longleftrightarrow U(\mu_A; \alpha) = U(\mu_B; \alpha)$$

and

$$(A, B) \in \mathbf{L}^\alpha \Longleftrightarrow L(\gamma_A; \alpha) = L(\gamma_B; \alpha)\,.$$

These two relations $\mathbf{U}^\alpha$ and $\mathbf{L}^\alpha$ are equivalence relations, give rise to partitions of $IFS(G,f)$ into the equivalence classes of $\mathbf{U}^\alpha$ and $\mathbf{L}^\alpha$, denoted by $[A]_{\mathbf{U}^\alpha}$ and $[A]_{\mathbf{L}^\alpha}$ for any $A=(\mu_A,\gamma_A)\in IFS(G,f)$, respectively. And we will denote the quotient sets of $IFS(G,f)$ by $\mathbf{U}^\alpha$ and $\mathbf{L}^\alpha$ as $IFS(G,f)/\mathbf{U}^\alpha$ and $IFS(G,f)/\mathbf{L}^\alpha$, respectively.

If $\mathcal{S}(G,f)$ is the family of all subquasigroups of (G,f) and $\alpha\in[0,1]$, then we define two maps U_α and L_α from $IFS(G,f)$ to $\mathcal{S}(G,f)\cup\{\emptyset\}$ as follows:

$$U_\alpha(A)=U(\mu_A;\alpha)\ \text{ and }\ L_\alpha(A)=L(\gamma_A;\alpha),$$

respectively, for each $A=(\mu_A,\gamma_A)\in IFS(G,f)$. Then the maps U_α and L_α are well-defined.

Theorem 4.8. *For any $\alpha\in(0,1)$, the maps U_α and L_α are surjective from $IFS(G,f)$ onto $\mathcal{S}(G,f)\cup\{\emptyset\}$.*

Proof. Let $\alpha\in(0,1)$. Note that $\mathbf{0}_\sim=(\mathbf{0},\mathbf{1})$ is in $IFS(G,f)$, where $\mathbf{0}$ and $\mathbf{1}$ are fuzzy sets in (G,f) defined by $\mathbf{0}(x)=0$ and $\mathbf{1}(x)=1$ for all $x\in G$. Obviously, $U_\alpha(\mathbf{0}_\sim)=L_\alpha(\mathbf{0}_\sim)=\emptyset$. If (H,f) is an n-ary subquasigroup of (G,f), then for the IFS subquasigroup $H=(\chi_H,\overline{\chi_H})$ we have $U_\alpha(H)=U(\chi_H;\alpha)=H$ and $L_\alpha(H)=L(\overline{\chi_H};\alpha)=H$. Hence U_α and L_α are surjective. □

Theorem 4.9. *The quotient sets $IFS(G,f)/\mathbf{U}^\alpha$ and $IFS(G,f)/\mathbf{L}^\alpha$ are equipotent to $\mathcal{S}(G,f)\cup\{\emptyset\}$ for any $\alpha\in(0,1)$.*

Proof. Let $\alpha\in(0,1)$ be fixed and let

$$\overline{U_\alpha}:IFS(G,f)/\mathbf{U}^\alpha\longrightarrow\mathcal{S}(G,f)\cup\{\emptyset\}$$

and

$$\overline{L_\alpha}:IFS(G,f)/\mathbf{L}^\alpha\longrightarrow\mathcal{S}(G,f)\cup\{\emptyset\}$$

be the maps defined by

$$\overline{U_\alpha}([A]_{\mathbf{U}^\alpha})=U_\alpha(A)\ \textit{ and }\ \overline{L_\alpha}([A]_{\mathbf{L}^\alpha})=L_\alpha(A),$$

respectively, for each $A=(\mu_A,\gamma_A)\in IFS(G,f)$.

If $U(\mu_A;\alpha)=U(\mu_B;\alpha)$ and $L(\gamma_A;\alpha)=L(\gamma_B;\alpha)$ for $A=(\mu_A,\gamma_A)$ and $B=(\mu_B,\gamma_B)$ from $IFS(G,f)$, then $(A,B)\in\mathbf{U}^\alpha$ and $(A,B)\in\mathbf{L}^\alpha$, whence $[A]_{\mathbf{U}^\alpha}=[B]_{\mathbf{U}^\alpha}$ and $[A]_{\mathbf{L}^\alpha}=[B]_{\mathbf{L}^\alpha}$. Hence the maps $\overline{U_\alpha}$ and $\overline{L_\alpha}$ are injective.

To show that the maps $\overline{U_\alpha}$ and $\overline{L_\alpha}$ are surjective, let (H,f) be a subquasigroup of (G,f). Then for $H=(\chi_H,\overline{\chi_H})\in IFS(G,f)$ we have $\overline{U_\alpha}([H]_{\mathbf{U}^\alpha})=U(\chi_H;\alpha)=H$ and $\overline{L_\alpha}([H]_{\mathbf{L}^\alpha})=L(\overline{\chi_H};\alpha)=H$. Also $\mathbf{0}_\sim=(\mathbf{0},\mathbf{1})\in IFS(G,f)$. Moreover $\overline{U_\alpha}([\mathbf{0}_\sim]_{\mathbf{U}^\alpha})=U(\mathbf{0};\alpha)=\emptyset$ and $\overline{L_\alpha}([\mathbf{0}_\sim]_{\mathbf{L}^\alpha})=L(\mathbf{1};\alpha)=\emptyset$. Hence $\overline{U_\alpha}$ and $\overline{L_\alpha}$ are surjective. □

For any $\alpha\in[0,1]$, we define another relation $\mathbf{R}^\alpha$ on $IFS(G,f)$ as following:

$$(A,B)\in\mathbf{R}^\alpha \Longleftrightarrow U(\mu_A;\alpha)\cap L(\gamma_A;\alpha)=U(\mu_B;\alpha)\cap L(\gamma_B;\alpha)$$

for any $A=(\mu_A,\gamma_A)$ and $B=(\mu_B,\gamma_B)$ from $IFS(G,f)$. Then the relation $\mathbf{R}^\alpha$ is also an equivalence relation on $IFS(G,f)$.

Theorem 4.10. *For any $\alpha\in(0,1)$ and any IFS subquasigroup $A=(\mu_A,\gamma_A)$ of (G,f) the map $I_\alpha: IFS(G,f)\longrightarrow\mathcal{S}(G,f)\cup\{\emptyset\}$ defined by*

$$I_\alpha(A)=U_\alpha(A)\cap L_\alpha(A)$$

is suriective.

Proof. Indeed, if $\alpha\in(0,1)$ is fixed, then for $\mathbf{0}_\sim=(\mathbf{0},\mathbf{1})\in IFS(G,f)$ we have

$$I_\alpha(\mathbf{0}_\sim)=U_\alpha(\mathbf{0}_\sim)\cap L_\alpha(\mathbf{0}_\sim)=U(\mathbf{0};\alpha)\cap L(\mathbf{1};\alpha)=\emptyset\,,$$

and for any $H\in\mathcal{S}(G,f)$, there exists $H=(\chi_H,\overline{\chi_H})\in IFS(G,f)$ such that $I_\alpha(H)=U(\chi_H;\alpha)\cap L(\overline{\chi_H};\alpha)=H$. □

Theorem 4.11. *For any $\alpha\in(0,1)$, the quotient set $IFS(G,f)/\mathbf{R}^\alpha$ is equipotent to $\mathcal{S}(G,f)\cup\{\emptyset\}$.*

Proof. Let $\alpha\in(0,1)$ be fixed and let

$$\overline{I_\alpha}: IFS(G,f)/\mathbf{R}^\alpha\longrightarrow\mathcal{S}(G,f)\cup\{\emptyset\}$$

be a map defined by $\overline{I_\alpha}([A]_{\mathbf{R}^\alpha})=I_\alpha(A)$ for each $[A]_{\mathbf{R}^\alpha}\in IFS(G,f)/\mathbf{R}^\alpha$.

If $\overline{I_\alpha}([A]_{\mathbf{R}^\alpha})=\overline{I_\alpha}([B]_{\mathbf{R}^\alpha})$ holds for some $[A]_{\mathbf{R}^\alpha}$ and $[B]_{\mathbf{R}^\alpha}$ from $IFS(G,f)/\mathbf{R}^\alpha$, then

$$U(\mu_A;\alpha)\cap L(\gamma_A;\alpha)=U(\mu_B;\alpha)\cap L(\gamma_B;\alpha),$$

hence $(A,B)\in\mathbf{R}^\alpha$ and $[A]_{\mathbf{R}^\alpha}=[B]_{\mathbf{R}^\alpha}$. It follows that $\overline{I_\alpha}$ is injective.

For $\mathbf{0}_\sim=(\mathbf{0},\mathbf{1})\in IFS(G,f)$ we have $\overline{I_\alpha}(\mathbf{0}_\sim)=I_\alpha(\mathbf{0}_\sim)=\emptyset$. If $H\in\mathcal{S}(G,f)$, then for $H=(\chi_H,\overline{\chi_H})\in IFS(G,f)$, $\overline{I_\alpha}(H)=I_\alpha(H)=H$. Hence $\overline{I_\alpha}$ is a bijective map. □

5. Open problems

The above results show that IFS subsets in n-ary quasigroups can be investigated in a similar way as IFS subsets of universal algebras. The problem is with IFS subgroups of n-ary groups.

As it is well known (cf. [2] or [15]), a nonempty subset S of an n-ary group (G, f) is an n-ary subgroup of (G, f) if it is closed with respect to the operation f and $\overline{x} \in S$ for every $x \in S$, where $\overline{x}$ denotes the solution of the equation $f(x, \ldots, x, \overline{x}) = x$. Since (G, f) is an n-ary group for every x there exists only one $\overline{x}$ satisfying this equation. So, the map $\varphi(x) = \overline{x}$ is well-defined but it is not one-to-one in general. Moreover, there exists n-ary groups in which is one fixed element $a = \overline{x}$ such that $f(y, \ldots, y, a) = y$ is valid for all $y \in G$. An element $\overline{x}$ plays a similar (but not identical) role as an inverse element in classical groups.

Thus, by the analogy to the binary case, an *fuzzy n-ary subgroup* can be defined as an fuzzy subgroupoid μ such that $\mu(\overline{x}) \geqslant \mu(x)$ for all $x \in G$, or as an fuzzy subgroupoid μ such that $\mu(\overline{x}) = \mu(x)$ for all $x \in G$. For $n = 3$ these two concepts are equivalent Because in this case $\overline{\overline{x}} = x$ for every x.

Unfortunately, for $n > 3$ these two concepts are not equivalent. Indeed, as it is not difficult to see, in the unipotent 4-ary group derived from the additive group Z_4 the map μ defined by $\mu(0) = 1$ and $\mu(x) = 0.5$ for all $x \neq 0$ is an example of fuzzy subgroupoid in which $\mu(\overline{x}) \geqslant \mu(x)$ for all $x \in Z_4$. Thus μ is a fuzzy subgroup in the first sense, but not in the second because for $x = 2$ we have $\mu(\overline{x}) > \mu(x)$.

These two concepts are equivalent in n-ary groups in which $\varphi^k(x) = x$ for some fixed $k > 0$ and all x.

Problem 1. *Describe the conditions (for n-ary groups) under which these two concepts are equivalent.*

Problem 2. *Describe the similarities and differences between these two concepts of fuzzy n-ary subgroups (and IFS subgroups).*

E. L. Post proved in [15] that any n-ary group can be embedded into some binary group (called the *covering group*). On the other hand (cf. for example [9]), with any n-ary group (G, f) is connected the family of *binary retracts*, i.e., the family of binary groups $(G, \circ)$ with the operation $x \circ y = f(x, a_2, \ldots, a_{n-1}, y)$, where $a_2, \ldots, a_{n-2} \in G$ are fixed. All such retracts are isomorphic to retracts of the form $x \circ y = f(x, a, \ldots, a, y)$ and induce some properties of the corresponding n-ary group.

Problem 3. *Find the connection between fuzzy subgroups of a given n-ary group and fuzzy subgroups of its binary retracts and its covering group.*

Problem 4. *Describe IFS subgroups of n-ary groups and the connection with IFS subgroups of the corresponding binary groups.*

References

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

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

[3] **W. A. Dudek**: *Remarks on n-groups*, Demonstratio Math. **13**(1980), 165 – 181.

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

[5] **W. A. Dudek**: *Fuzzification on n-ary groupoids*, Qusigroups Related Systems, **7** (2000), 45 – 66.

[6] **W. A. Dudek**: *Idempotents in n-ary semigroups*, Southeast Asian Bull. Math. **25** (2001), 97 – 104.

[7] **W. A. Dudek, K. Głazek and B. Gleichgewicht**: *A note on the axioms of n-groups*, in *Colloquia Math. Soc. J. Bolyai* **29** "Universal Algebra", Esztergom (Hungary) 1977, 195 – 202. (North-Holland, Amsterdam 1982.)

[8] **W. A. Dudek and Y. B. Jun**: *Intuitionistic fuzzy approach to BCC-algebras*, Bul. Acad. Sci. Rep. Moldova ser. Mat. **3(37)** (2001), 7 – 12.

[9] **W. A. Dudek and J. Michalski**: *On retracts of polyadic groups*, Demonstratio Math. **17** (1984), 281 – 301.

[10] **J. W. Grzymała-Busse**: *Automorphisms of polyadic automata*, J. Assoc. Computing Machinery **16** (1969), 208 – 219.

[11] **R. Kerner**: *Ternary algebraic structures and their applications in physics*, Preprint of Univ. P. & M. Curie, Paris 2000.

[12] **K. H. Kim, W. A. Dudek and Y. B. Jun**: *On intuitionistic fuzzy subquasigroups of a quasigroups*, Quasigroups Related Systems **7** (2000), 15 – 28.

[13] **G. L. Mullen and V. Shcherbacov**: *Properties of codes with one check symbol from a quasigroup point of view*, Bull. A. S. Rep. Moldova, ser. Math. **40** (2002), 71 – 86.

[14] **H. O. Pflugfelder**: *Quasigroups and loops: introduction*, Sigma Series in Pure Math., vol. **7**, Heldermann Verlag, Berlin 1990.

[15] **E. L. Post**: *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1940), 208 – 350.

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

Received January 15, 2005

Institute of Mathematics and Computer Science
Wroclaw University of Technology
Wyb. Wyspiańskiego 27
50-370 Wrocław
Poland
e-mail: dudek@im.pwr.wroc.pl

Quasigroups and Related Systems **13** (2005), 229 – 236

Affine regular dodecahedron in GS–quasigroups

Zdenka Kolar–Begović and Vladimir Volenec

Abstract

The concept of the affine regular dodecahedron is defined in any GS–quasigroup by means of twelve ARP relation which are valid for five out of twenty points. A number of statements about the connection of the corresponding vertices of the dodecahedron will be proved. Quaternary relations Par, GST, $DGST$ can be found in these statements. The theorem of the unique determination of the affine regular dodecahedron by means of its four vertices which satisfy certain conditions will be proved. The geometrical interpretation of all mentioned concepts and relations will be given in the GS–quasigroup $C(\frac{1}{2}(1+\sqrt{5}))$.

GS–quasigroups are defined in [2]. In [3], [1] and [4] different geometric structures in GS–quasigroups are defined and investigated. In this paper some new "geometric" concepts in the general GS–quasigroup will be defined.

A quasigroup $(Q,\cdot)$ is said to be *GS–quasigroup* if it is idempotent and if it satisfies the (mutually equivalent) identities

$$a(ab\cdot c)\cdot c = b, \qquad\qquad a\cdot(a\cdot bc)c = b.$$

If C is the set of all points in Euclidean plane and if groupoid $(C,\cdot)$ is defined so that $aa = a$ for any $a \in C$ and for any two different points a, $b \in C$ we define $ab = c$ if the point b divides the pair a, c in the ratio of golden section. In [2] it is proved that $(C,\cdot)$ is a GS–quasigroup. We shall denote that quasigroup by $C(\frac{1}{2}(1+\sqrt{5}))$ because we have $c = \frac{1}{2}(1+\sqrt{5})$ if $a = 0$ and $b = 1$. The figures in this quasigroup $C(\frac{1}{2}(1+\sqrt{5}))$ can be used for illustration of "geometrical" relations in any GS–quasigroup.

2000 Mathematics Subject Classification: 20N05
Keywords: GS–quasigroup, affine regular dodecahedron.

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 $\mathrm{Par}(a,b,c,d)$ if the identity $a\cdot b(ca\cdot a)=d$ holds. In [2] numerous properties of the quaternary relation Par on the set Q are proved. Let us mention just the following lemma which we shall use afterwards.

Lemma 1. *From* $Par(a,b,c,d)$ *and* $Par(c,d,e,f)$ *follows* $Par(a,b,f,e)$.

In [3] the concept of the GS–trapezoid is defined and explored. 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. In [3] different characterizations of that relation are investigated, we shall mention the following lemmas.

Lemma 2. $GST(a_1,b_1,b_2,a_2)$,$GST(a_2,b_2,b_3,a_3)$,. . .,$GST(a_{n-1},b_{n-1},b_n,a_n)$ $\Rightarrow GST(a_n,b_n,b_1,a_1)$.

Lemma 3. $GST(a,b,c,d)$, $GST(a,b,c',d')\Rightarrow GST(d,c,c',d')$.

Lemma 4. *Any two of the three statements* $GST(a,b,c,d)$, $GST(a',b,c,d')$, $Par(a,a',d',d)$ *imply the remaining statement.*

Lemma 5. *Any two of the three statements* $GST(a,b,c,d)$, $GST(a,b',c',d)$, $Par(b,b',c',c)$ *imply the remaining statement.*

In [3] it is proved that any two of the five statements

$$GST(a,b,c,d), GST(b,c,d,e), GST(c,d,e,a), GST(d,e,a,b), GST(e,a,b,c) \quad (1)$$

imply the remaining statements.

In [4] the concept of the affine regular pentagon is defined. 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 five statements (1) are valid. In [4] the next properties of the affine regular pentagon are proved.

Lemma 6. *Affine regular pentagon is uniquely determined by any three of its vertices.*

Lemma 7. *If the statement* $GST(a,b,c,d)$ *is valid then there is one and only one point* e *such that the statement* $ARP(a,b,c,d,e)$ *is valid.*

The concept of the DGS–trapezoid is introduced in [1]. Points a, b, c, d are said to be the vertices of the *double golden section trapezoid* or shorter DGS–trapezoid and we write $\mathrm{DGST}(a, b, c, d)$ if the equality $ab = dc$ holds. In [1] it is proved the next connection between GS–trapezoids and DGS–trapezoids in GS–quasigroups.

Lemma 8. *Any two of the three statements $GST(a, e, f, d)$, $GST(e, b, c, f)$ and $DGST(a, b, c, d)$ imply the remaining statement.*

1. Affine regular dodecahedron in GS–quasigroups

Definition 1. We shall say that the points $a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4, b_5, c_1, c_2, c_3, c_4, c_5, d_1, d_2, d_3, d_4, d_5$ are the vertices of an *affine regular dodecahedron* and we shall write

$$ARD(a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4, b_5, c_1, c_2, c_3, c_4, c_5, d_1, d_2, d_3, d_4, d_5)$$

if the following twelve statements are valid (Figure 1)

$$\begin{array}{ll}
ARP(a_1, a_2, a_3, a_4, a_5), & ARP(d_1, d_2, d_3, d_4, d_5) \\
ARP(a_3, b_3, c_1, b_4, a_4), & ARP(d_3, c_3, b_1, c_4, d_4), \\
ARP(a_4, b_4, c_2, b_5, a_5), & ARP(d_4, c_4, b_2, c_5, d_5), \\
ARP(a_5, b_5, c_3, b_1, a_1), & ARP(d_5, c_5, b_3, c_1, d_1), \\
ARP(a_1, b_1, c_4, b_2, a_2), & ARP(d_1, c_1, b_4, c_2, d_2), \\
ARP(a_2, b_2, c_5, b_3, a_3), & ARP(d_2, c_2, b_5, c_3, d_3).
\end{array}$$

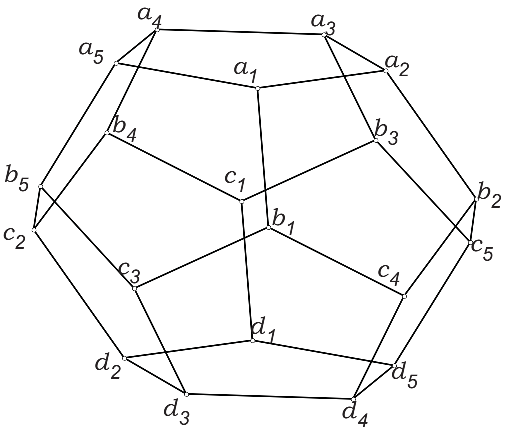

Figure 1.

Let $\mathrm{ARD}(a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4, b_5, c_1, c_2, c_3, c_4, c_5, d_1, d_2, d_3, d_4, d_5)$ be valid further.

For each $i \in \{1, 2, 3, 4, 5\}$ the vertices a_i and d_i, respectively b_i and c_i are called the *opposite vertices.*

Theorem 1. 30 *statements of the form* $Par(a_2, a_5, c_3, c_4)$ *are valid (Figure* 2*).*

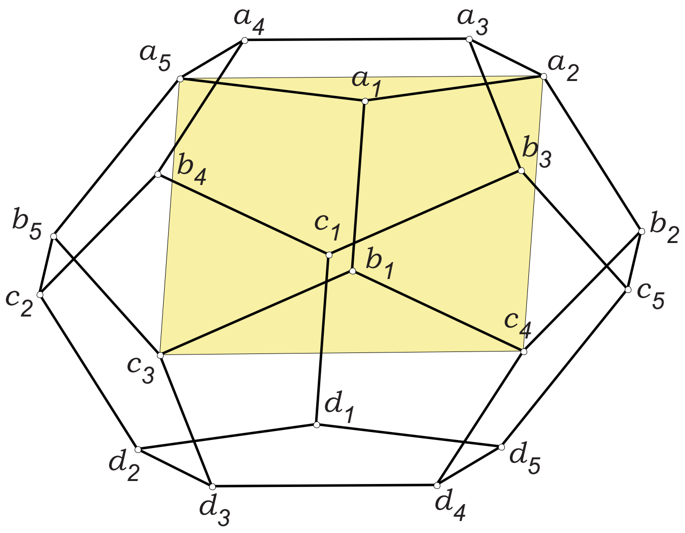

Figure 2.

Proof. The given statement follows from $\mathrm{GST}(a_2, a_1, b_1, c_4)$ and $\mathrm{GST}(a_5, a_1, b_1, c_3)$ according to Lemma 4. □

For opposite vertices of the ARD the following statement is valid.

Theorem 2. *If x and x', respectively y and y' are opposite vertices of the ARD then $Par(x, y, x', y')$ is valid.*

Proof. It is sufficient to prove that, along with the standard symbols, for example the statements $\mathrm{Par}(a_1, b_1, d_1, c_1)$ (Figure 3) and $\mathrm{Par}(a_1, a_3, d_1, d_3)$ are valid (Figure 4). As $\mathrm{GST}(a_2, a_1, b_1, c_4)$ is valid and according to Theorem 1 $\mathrm{Par}(a_2, b_3, d_5, c_4)$ too, so by Lemma 4 $\mathrm{GST}(b_3, a_1, b_1, d_5)$ follows which together with $\mathrm{GST}(b_3, c_1, d_1, d_5)$, based on Lemma 5, implies $\mathrm{Par}(a_1, c_1, d_1, b_1)$.

According to Theorem 1 we have $\mathrm{Par}(a_1, a_3, c_5, c_4)$ and $\mathrm{Par}(c_5, c_4, d_3, d_1)$ from which by Lemma 1 $\mathrm{Par}(a_1, a_3, d_1, d_3)$ follows. □

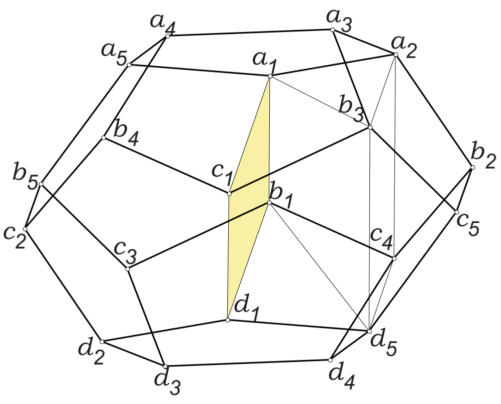

Figure 3.

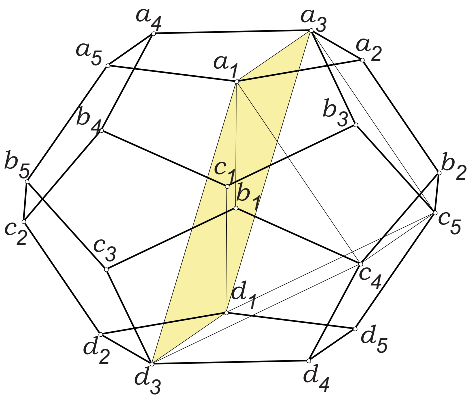

Figure 4.

Theorem 3. 60 *statements of the form* $GST(b_3, a_1, b_1, d_5)$ *are valid* (*see Figure* 5).

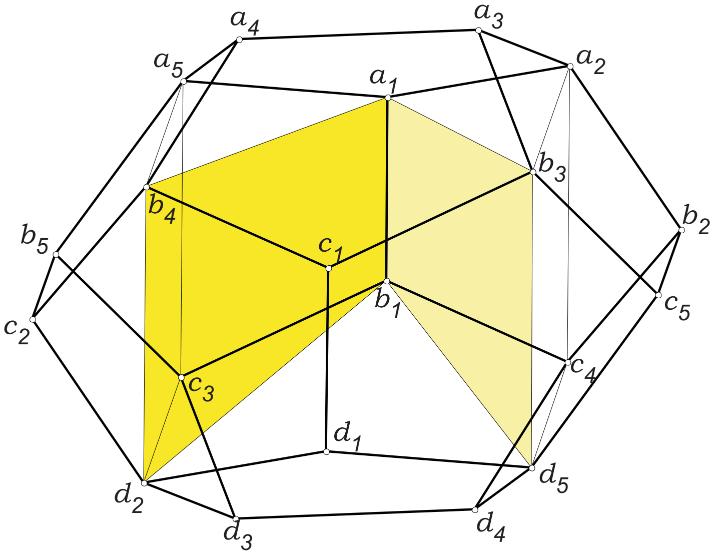

Figure 5.

Proof. The statement is proved in the proof of the previous theorem. □

Theorem 4. 60 *statements of the form* $GST(b_1, a_1, a_3, b_3)$ *are valid* (*see Figure* 6).

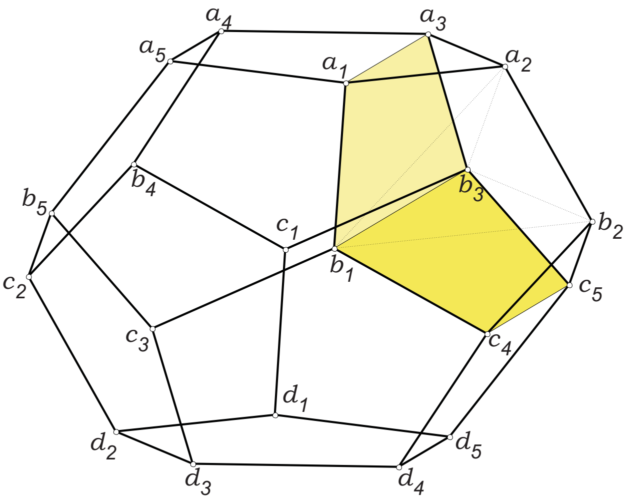

Figure 6.

Proof. The statements follow from GST(b_2, a_2, a_1, b_1) and GST(b_2, a_2, a_3, b_3) according to Lemma 3. □

Theorem 5. 60 *statements of the form DGST*(a_3, a_1, b_1, d_4) *are valid* (*see Figure* 7).

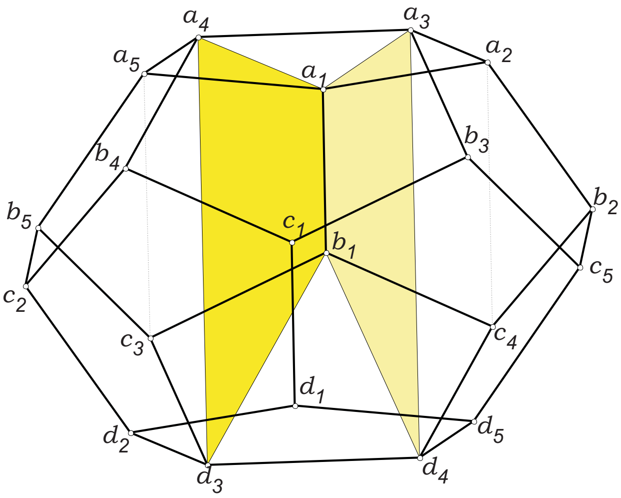

Figure 7.

Proof. According to Theorem 4 $\mathrm{GST}(a_3, a_2, c_4, d_4)$ is valid which together with $\mathrm{GST}(a_2,\ a_1,\ b_1,\ c_4)$ according to Lemma 8 results in $\mathrm{DGST}(a_3, a_1, b_1, d_4)$. □

It is possible to prove that the affine regular dodecahedron is uniquely determined by its four independent vertices i.e. vertices which are not in the relation Par, GST or DGST. We shall prove only the following theorem.

Theorem 6. *For any points a_1, a_2, a_5, b_1 the points $a_3, a_4, b_2, b_3,\ b_4,\ b_5,\ c_1,\ c_2,\ c_3,\ c_4,\ c_5,\ d_1,\ d_2,\ d_3,\ d_4,\ d_5$ are uniquely determined so that $ARD(a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ b_1,\ b_2,\ b_3,\ b_4,\ b_5,\ c_1,\ c_2,\ c_3,\ c_4,\ c_5,\ d_1,\ d_2,\ d_3,\ d_4,\ d_5)$ is valid.*

Proof. Let $a_3, a_4, b_5, c_3, b_2, c_4$ be such points that $\mathrm{ARP}(a_1, a_2, a_3, a_4, a_5)$, $\mathrm{ARP}(a_5,\ b_5, c_3,\ b_1, a_1)$ and $\mathrm{ARP}(a_1, b_1,\ c_4, b_2, a_2)$ and then let the points b_4, c_2, b_3, c_5 be such points that $\mathrm{ARP}(a_4, b_4, c_2, b_5, a_5)$ and $\mathrm{ARP}(a_2, b_2, c_5, b_3, a_3)$ are valid.

From $\mathrm{GST}(b_4, a_4, a_5, b_5)$, $\mathrm{GST}(b_5,\ a_5,\ a_1, b_1)$, $\mathrm{GST}(b_1, a_1, a_2, b_2)$ and $\mathrm{GST}(b_2, a_2, a_3, b_3)$ according to Lemma 2 $\mathrm{GST}(b_3, a_3, a_4, b_4)$ follows. According to Lemma 7 there is the point c_1 such that $\mathrm{ARP}(a_3, b_3, c_1, b_4, a_4)$ is valid, and then according to Lemma 6 there are such points d_3, d_4 that $\mathrm{ARP}(d_3, c_3, b_1, c_4, d_4)$ is valid. From $\mathrm{GST}(c_2, b_5, a_5, a_4)$, $\mathrm{GST}(a_4, a_5, a_1, a_2)$, $\mathrm{GST}(a_2, a_1, b_1, c_4)$ and $\mathrm{GST}(c_4, b_1, c_3, d_3)$ according to Lemma 2 the statement $\mathrm{GST}(d_3, c_3, b_5, c_2)$ follows. In the same way from $\mathrm{GST}(c_5, b_2, a_2, a_3)$, $\mathrm{GST}(a_3, a_2, a_1, a_5)$, $\mathrm{GST}(a_5,\ a_1, b_1, c_3)$ and $\mathrm{GST}(c_3, b_1, c_4,\ d_4)$ the statement $\mathrm{GST}(d_4, c_4, b_2, c_5)$ follows. Therefore according to Lemma 7 there are such points d_2, d_5 that $\mathrm{ARP}(d_2, c_2, b_5, c_3, d_3)$ and $\mathrm{ARP}(d_4,\ c_4, b_2, c_5, d_5)$ are valid. From $\mathrm{GST}(d_5, d_4, c_4, b_2)$, $\mathrm{GST}(b_2, c_4, b_1, a_1)$, $\mathrm{GST}(a_1, b_1,\ c_3, b_5)$ and $\mathrm{GST}(b_5, c_3, d_3, d_2)$ according to Lemma 2 $\mathrm{GST}(d_2,\ d_3, d_4, d_5)$ follows so according to Lemma 7 there is such a point d_1 that $\mathrm{ARP}(d_1, d_2, d_3, d_4, d_5)$ is valid.

With the repeated application of Lemma 2 from $\mathrm{GST}(d_2, c_2, b_5, c_3)$, $\mathrm{GST}(c_3, b_5, a_5, a_1)$, $\mathrm{GST}(a_1, a_5, a_4, a_3)$, $\mathrm{GST}(a_3, a_4, b_4, c_1)$ follows $\mathrm{GST}(c_1,\ b_4, c_2, d_2)$, from $\mathrm{GST}(d_1, d_2, d_3, d_4)$, $\mathrm{GST}(d_4, d_3, c_3, b_1)$, $\mathrm{GST}(b_1, c_3, b_5, a_5)$ and $\mathrm{GST}(a_5, b_5, c_2, b_4)$ follows $\mathrm{GST}(b_4, c_2, d_2, d_1)$, from $\mathrm{GST}(d_5, c_5, b_2, c_4)$, $\mathrm{GST}(c_4, b_2, a_2, a_1)$, $\mathrm{GST}(a_1, a_2, a_3, a_4)$, $\mathrm{GST}(a_4,\ a_3, b_3, c_1)$ follows $\mathrm{GST}(c_1,\ b_3, c_5, d_5)$, and from $\mathrm{GST}(d_1, d_5, d_4, d_3)$, $\mathrm{GST}(d_3, d_4, c_4, b_1)$, $\mathrm{GST}(b_1,\ c_4, b_2,\ a_2)$ and $\mathrm{GST}(a_2, b_2, c_5, b_3)$ follows $\mathrm{GST}(b_3, c_5, d_5, d_1)$ so that we have the final statements $\mathrm{ARP}(d_1,\ c_1, b_4, c_2, d_2)$, $\mathrm{ARP}\ (d_5, c_5, b_3, c_1, d_1)$. □

References

[1] **Z. Kolar–Begović and V. Volenec**: *DGS–trapezoids in GS–quasigroups*, Math. Communications **8** (2003), 215 – 218.

[2] **V. Volenec**: *GS–quasigroups*, Čas. pěst. mat. **115** (1990), 307 – 318.

[3] **V. Volenec and Z. Kolar**: *GS–trapezoids in GS–quasigroups*, Math. Communications **7** (2002), 143 – 158.

[4] **V. Volenec and Kolar–Begović**; *Affine regular pentagons in GS–quasigroups*, Quasigroups Related Systems **12** (2004), 103 – 112.

Received January 6, 2005

Zdenka Kolar–Begović
Department of Mathematics, University of Osijek, Gajev trg 6,
HR-31 000 Osijek, Croatia
e-mail: zkolar@mathos.hr

Vladimir Volenec
Department of Mathematics, University of Zagreb, Bijenička c. 30,
HR-10 000 Zagreb, Croatia,
e-mail: volenec@math.hr

Maple implementation of the ElGamal public key encryption scheme working in SMG($\mathrm{p^m}$)

Czesław Kościelny

Abstract

It has been shown [2, 3, 4] that in ElGamal public key encryption scheme [6, 7, 8] working over $SMG(p^m)$, the need of finding primitive elements of $GF(p^m)$, necessary if the system works traditionally but unfeasible in the case of huge fields, is eliminated. Thus, the discussed system is user-friendly, giving the possibility of very strong encryption with the key of order 10.000 bits and more. The construction of such cryptosystem is of great practical importance, therefore, the paper informs the reader in detail how to resolve this problem using Maple.

1. Introduction

Recall that algorithms describing ElGamal public-key encryption scheme [3, 4, 5] adapted for working in $SMG(p^m)$ are as follows:

Key generation: Each entity creates its public key and the corresponding private key. So each entity $\mathcal{N}$ 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 $\mathbf{M\_}(x, y)$, $x, y \in G$. The function $\mathbf{P\_}(x, k)$, carrying

2000 Mathematics Subject Classification: 94A60, 20N

Keywords: cryptography, public-key ciphers, spurious multiplicative group of Galois field, Maple.

out the operation of rising any element x from G to a k^{th} power, $p^m - 1 \leqslant k \leqslant -p^m + 1$, is also defined.

- Select a random invertible element $\alpha \in SMG(p^m)$, $\alpha \neq 1$.
- Choose a random integer $a \in G$, $2 \leqslant a \leqslant p^m - 2$, and compute the element $\beta = \mathbf{P\_}(\alpha, a)$.
- $\mathcal{N}$'s public key is α and β, together with $f(N)$ and the functions $\mathbf{M\_}$ and $\mathbf{P\_}$, if these last three parameters are not common to all the entities.
- $\mathcal{X}$'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 $\mathbf{M\_}$ and $\mathbf{P\_}$ 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 $c_1 = \mathbf{P\_}(\alpha, k)$ and $c_2 = \mathbf{M\_}(m, \mathbf{P\_}(\beta, k))$.
- 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 $g = \mathbf{P\_}(c_1,\ a)$ and then retrieve the plaintext by computing $m = \mathbf{M\_}(\mathbf{P\_}(g, -1), c_2)$.

2. Maple routines as elements of an application for very secure encrypting of electronic mail using ElGamal algorithm working in $SMG(p^m)$

The application discussed will realize a practical task, so it is assumed that the public, key, secret key, plain text and cryptogram will be files. Therefore, the routines for converting file into number and number into file, denoted as `f2n` and `n2f`, correspondingly, are needed first. Here they are:

```
> f2n := proc(fn::string)
 local l2n, f2l;
     l2n := proc(l::list)
         local t, m;
             t := modp1(ConvertIn(l, x), nn^2);
             subs(x = 256, t)
         end proc;
     f2l := proc(fn::string)
         local l, f, fs;
             f := fopen(fn, READ, BINARY);
             fs := filepos(f, infinity);
             filepos(f, 0);
             l := readbytes(f, fs);
             fclose(f);
             l
         end proc;
     l2n(f2l(fn))
 end proc:
```

```
>   n2f := proc(n::nonnegint, fn::string)
 local l2f, n2l;
     l2f := proc(l::list, fn::string)
         local f;
             f := fopen(fn, WRITE, BINARY);
             writebytes(f, l);
             fclose(f)
         end proc;
     n2l := proc(nn::nonnegint)
             if nn = 0 then [0]
             else convert(nn, base, 256)
             end if
         end proc;
     l2f(n2l(n), fn)
 end proc:
```

The formal parameter `fn` of the procedure `f2n` represents the name of the file, which will be converted into a number, and formal parameters of the routine `n2f` denote the number `n` which will be converted into the file named fn. The variable nn appearing in the routine f2n is global, and it is computed by the routine

```
> INIT_ := proc(pn::posint, fx::polynom)
 global ext, n, nn;
     nn := pn^degree(fx);
     ext := modp1(ConvertIn(modp(fx, pn), x), pn);
     n := pn
 end proc:
```

which initializes calculations in $SMG(p^m)$ and returns, in addition, global variables n and ext, necessary for routines M_, P_ and MI_. These three routines (contained in [5], Appendix C) are also indispensable. They perform multiplication, raising to a power and finding the multiplicative inverse in $SMG(p^m)$, respectively.

The fundamental task in the algorithm of key generations fulfills the routine

```
> frel := proc()
  local alpha, beta, a, l, res, si, i;
    randomize;
    res := "*";
    while res = "*" do
      alpha := rand(rand((nn-1)/2)() .. nn - 1)();
      try res := MI_(alpha) catch: res := "*" end try
    end do;
    a := rand(2 .. nn - 2)();
    beta := P_(alpha, a);
    alpha, beta, a
 end proc:
```

which returns a random invertible element α and an appropriate element β from $SMG(p^m)$ being the components of a public key, and an integer a, playing the role of a secret key. It is evident that there exist many procedures able to do this task.

At last the encryption routine

```
>  ElGEnc := proc(ptfn, c1fn, c2fn::string, alpha, beta)
local c1, c2, k, m;
    m := f2n(ptfn);
    k := rand(2 .. nn - 2)();
    c1 := P_(alpha, k);
    c2 := M_(m, P_(beta, k));
    n2f(c1, c1fn);
    n2f(c2, c2fn)
end proc:
```

and the decryption routine

```
>  ElGDec := proc(c1fn, c2fn, rptfn::string, a::posint)
local c1, c2, g, ig, m;
    c1 := f2n(c1fn);
    c2 := f2n(c2fn);
    g := P_(c1, a);
    m := M_(P_(g, -1), c2);
    n2f(m, rptfn)
end proc:
```

acting according to the description given in Section 1, will be necessary. The `ElGEnc` procedure enciphers the plaintext file having the filename `ptfn` taking into account the public key components `alpha` and `beta` and creates two cryptogram files named as `c1fn` and `c2fn`. The `ElGDec` procedure deciphers cryptogram files `c1fn` and `c2fn` and creates the retrieved plaintext file `rptfn` taking into account the secret key `a`.

From the above 9 blocks a practiced programmer will easily assemble a user-friendly application for encrypting the electronic mail in the Maple environment. As an example, the author, using the above bricks, has built an application consisting of three procedures:

- `KeyGen(plaintextf_file_size, degree_of_fx)`,
- `Encrypting(plaintextf_file, smg_data_file)`,
- `Decrypting(c1_file, c2_file, smg_data_file)`.

The `KeyGen` procedure automatically chooses a Mersenne prime p in such a way that the cryptosystem could process files of the desired size. Doing this it must take into account the degree of the polynomial $f(x)$ over $GF(p)$. Next the routine randomly generates this polynomial, computes the integer $n = p^{deg(f(x))}$ and generates a random cryptographic key. The public and private keys in the files `pkf` and `skf` are stored, correspondingly, while n and $f(x)$ to the file `nfx.smg` are written.

The `Encrypting` procedure takes $f(x)$ and n from the file `nfx.smg` and the public key of the desired correspondent form the file `pkf`. These data are sufficient to encrypt a plaintext file. It is assumed that the name of a plaintext file consists of one character and exactly of three characters of extension. Assuming that the name of a plaintext file is `"n.eee"`, the generated cryptogram is written to the files `c1neee.cry` and `c2neee.cry`. The contents of the plaintext file may be arbitrary (text, voice, picture, etc.), but, evidently, the file could not contain leading 0 bytes.

The `Decrypting` procedure takes $f(x)$ and n from the file `nfx.smg`, an appropriate secret key from the file `skf` and decrypts the crytogram files `c1neee.cry` and `c2neee.cry` (assuming that the file `n.eee` has been enciphered). The retrieved plaintext in the file `nr.eee`, having the proper extension, is stored.

If, for example, we want to process plaintext files of size 1.300 Bytes using $f(x)$ of degree 5, we ought to execute three statements. Under the above assumption a typical use and output of this application is the following:

```
> KeyGen(1300, 5);

KEY GENERATION:
Maximal plaintext file size = 1376 bytes.
Keys computed in 7 s and saved.
Public key file name:  "pkf".
Private key file name:  "skf".
Required for encryption/decryption data,
i.e.  n and f(x) saved in the file "nfx.smg".

> Encrypting("m.txt", "nfx.smg");

ENCRYPTING:
Plaintext file size = 1301 bytes.
Plaintex file name:  "m.txt".
Public key file name:  "pkf".
Cryptogram files named "c1mtxt.cry"
and "c2mtxt.cry" computed in 14 s and saved.

> Decrypting("c1mtxt.cry", "c2mtxt.cry", "nfx.smg");

DECRYPTING:
Secret key taken from the file "skf".
SMG data taken from the file:  "nfx.smg".
```

```
Cryptogram files named:  "c1mtxt.cry" and "c2mtxt.cry".
Recovered plaintext file named "mr.txt"
computed in 7 s and saved.
```

We see that the program informs the user about the stages of processing. In the case considered the computations are performed on integers having 3316 decimal digits. The secret key is an integer belonging to the set of order $0.7004904817 \cdot 10^{3316}$, therefore, the cryptographic key of the system equals exactly to 10.007 bits.

The three discussed procedures are not listed here, because they occupy place without making a contribution to the main problem of the paper. But if the reader wants to see them, the author willingly realizes his wish by email (joczeko@poczta.onet.pl).

3. Conclusions

In the paper it has been proved that ElGamal public key encryption scheme working in $SMG(p^m)$ may be easily implemented in Maple. It is obvious that each elementary routine mentioned in Section 2 and needed for this implementation can be, without difficulty, translated into any compiled language. Such translation allows to considerably accelerate encryption/decryption rate. Thus, the discussed cryptosystem is suitable not only for encrypting keys for symmetric cipher but also for direct encryption of messages.

It is worth noticing that ElGamal public key encryption may also work in the multiplicative system of $gff(n^m)$ [5].

References

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

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

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

[4] **C. Kościelny**: *Spurious multiplicative group of $GF(p^m)$: a new tool for cryptography*, Quasigroups and Related Systems **12** (2004), 61 – 73.

[5] **C. Kościelny**: *Computing in $GF(p^m)$ and in $gff(n^m)$ using Maple*, Quasigroups and Related Systems **13** (2005), 245 – 264.

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

[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 June 6, 2005

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 **13** (2005), 245 − 264

Computing in GF(p^{m}) and in gff(n^{m}) using Maple

Czesław Kościelny

Abstract

It is mentioned in [1] that the author intends to show how to construct strong ciphers using $SMG(p^m)^{\diamondsuit}$. But in order to implement such cryptosystems, an effective tool for computing in $GF(p^m)$ and $SMG(p^m)$, in the form of an appropriate hardware or software, is needed. The operation of this hardware or software ought to be defined by means of the detailed algorithms. Thus, to get ready the execution of his intention, the author describes in the paper these algorithms, which are represented as routines, written in the comprehensive Maple interpreter, intelligible both for mathematicians and programmers as well. The routines may be used either immediately as elements of encrypting/decrypting procedures in the Maple programming environment or can be easily translated into any compiled programming language (in this case encryption/decryption can be performed at least 100 times faster than in the Maple environment). Aside from that on the basis of the mentioned routines any VLSI chip as the encrypting/decrypting hardware for $SMG(p^m)-$ and $GF(p^m)-$based cryptosystems can be produced.

It has also been shown that $SMG(p^m)$ can be considered as a multiplicative system of an algebraic structure with addition and multiplication operations, containing a large class of systems, including $GF(p^m)$. The system is denoted as $gff(n^m)$, and multiplication in it is performed modulo an arbitrary polynomial od degree m over the ring Z_n. That way $gff(n^m)$ is a generalization of Galois field, very well suited for applications in cryptography. This system is named a generalized finite field.

$^{\diamondsuit}$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 $SMG(p^m) = \langle Gx, \bullet \rangle$, consisting of the set Gx of all $p^m - 1$ non-zero polynomials of degree d over $GF(p)$, $0 \leqslant d \leqslant m-1$, 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 is called the spurious multiplicative group of $GF(p^m)$.

2000 Mathematics Subject Classification: 05B15, 20N05, 94B05

Keywords: Galois fields, generalized finite fields, cryptography, Maple.

1. Introduction

It is not possible to do serious application research in the area of cryptology without complete knowledge concerning several algebraic systems. Prominent position on the list of such systems takes the Galois field. Thus, now it will be reminded to the reader about the main properties of this system, which are the most important for cryptographic practice.

Recall that for all prime p, for any positive integer $m \geq 1$ and for any irreducible polynomial

$$f(x) = x^m + \sum_{i=1}^{m} f_{m-i}\, x^{m-i} \tag{1}$$

of degree m over $GF(p)$ there exists an algebraic system called Galois field and denoted as $GF(p^m)$

$$GF(p^m) = \langle \mathcal{F},\ +,\ \cdot \rangle, \tag{2}$$

consisting of the set $\mathcal{F}$ of all p^m polynomials of degree d over $GF(p)$, $0 \leqslant d \leqslant m-1$, and of operations of addition and multiplication of these polynomials. Since $GF(p^m)$ is a field, it must satisfy the following set of axioms, concerning any field:

F1 The system $\langle \mathcal{F},\ + \rangle$, is an abelian group.

F2 The system $\langle \mathcal{F}^*,\ \cdot \rangle$, is an abelian group, $\mathcal{F}^* = \mathcal{F} \setminus \{0\}$, 0 is an additive identity element.

F3 $\forall a,\ b,\ c\ \in \mathcal{F}\ (a \cdot (b+c) = a \cdot b + a \cdot c) \wedge ((a+b) \cdot c = a \cdot c + b \cdot c)$.

In the case of $GF(p^m)$ the above axioms are fulfilled if addition and multiplication are performed according to the way shown beneath.

Let

$$a(x) = \sum_{i=1}^{m} a_{m-i}\, x^{m-i}, \quad b(x) = \sum_{i=1}^{m} b_{m-i}\, x^{m-i} \tag{3}$$

be two elements of $\mathcal{F}$. Then their sum will be

$$a(x) + b(x) = c(x) = \sum_{i=1}^{m} c_{m-i}\, x^{m-i}, \tag{4}$$

where

$$c_i \equiv a_i + b_i \pmod p, \;\; i = 0, \ldots, \; m-1.$$

Similarly

$$a(x) - b(x) = d(x) = \sum_{i=1}^{m} d_{m-i}\, x^{m-i}, \tag{5}$$

where

$$d_i \equiv a_i - b_i \pmod p, \;\; i = 0, \ldots, \; m-1.$$

The multiplication is more complicated. To calculate the product of two elements belonging to $GF(p^m)$ one must first compute

$$g(x) = a(x)\cdot b(x) = g_{2m-2}\, x^{2m-2} + g_{2m-3}\, x^{2m-3} + \cdots + g_2\, x^2 + g_1\, x + g_0$$

where

$$\begin{array}{l}
g_0 \equiv a_0\, b_0 \;\; (\mathrm{mod}\; p),\\
g_1 \equiv a_1\, b_0 + a_0\, b_1 \;\; (\mathrm{mod}\; p),\\
g_2 \equiv a_2\, b_0 + a_0\, b_2 + a_1\, b_1 \;\; (\mathrm{mod}\; p),\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
g_{2m-3} \equiv a_{m-1}\, b_{m-2} + a_{m-2}\, b_{m-1} \;\; (\mathrm{mod}\; p),\\
g_{2m-2} \equiv a_{m-1}\, b_{m-1} \;\; (\mathrm{mod}\; p).
\end{array}$$

Next, to obtain finally the product $h(x)$ of two $GF(p^m)$ elements (3), we must represent $g(x)$ as

$$g(x) = u(x)\cdot f(x) + h(x) \tag{6}$$

using addition and multiplication modulo p, wherefrom

$$a(x)\cdot b(x) = h(x).$$

The operation of multiplication in $GF(p^m)$ may also be shortly written as

$$h(x) \equiv a(x)\cdot b(x) \pmod{f(x)}.$$

The multiplicative inverse $a^{-1}(x)$ of the element $a(x)$ can be determined by means of extended Euclidean algorithm for polynomials, which yields:

$$a(x) \cdot a^{-1}(x) + w(x) \cdot f(x) = 1,$$

that is

$$a(x) \cdot a^{-1}(x) \equiv 1 \pmod{f(x)}.$$

So

$$a(x)/b(x) = a(x) \cdot b^{-1}(x).$$

We see that we can compute in $GF(p^m)$ as in any field, performing addition, subtraction, multiplication, division and the operation of rising to a power (by repeating the multiplication operation). The presented principles of computing in Galois field may be suitably optimized or improved to be well adapted for hardware or software implementation. It's worth mentioning here that elements of $GF(p^m)$ can be represented not only as polynomials or vectors over $GF(p)$, but also as numbers. The latter case is the most interesting for cryptography, therefore, we will continue the problem of computing in Galois field, considering mainly the system

$$GF(p^m) = \langle \mathrm{F},\ +,\ \bullet \rangle, \tag{7}$$

where F$= \{0,\ 1,\ \ldots,\ p^m - 1\}$. The system (7) is obtained from the system (2) using the isomorphic mapping

$$\sigma : \mathcal{F} \rightarrow \mathrm{F}, \tag{8}$$

defined by the function

$$\sigma(a(x)) = a(p) = \mathrm{A}\ \in \mathrm{F}, \tag{9}$$

converting a polynomial $a(x) \in \mathcal{F}$ to a number from the set F.

The mapping σ is an isomorphism, so the inverse mapping σ^{-1} exists and is described by means of the following two-step algorithm:

Step 1:

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

$$\mathrm{A} = a_{m-1}\ \cdots\ a_1\, a_0,\ a_i\ \in \{0,\, 1,\, \ldots,\, p-1\},$$

Step 2:

$$\sigma^{-1}(\mathrm{A}) = a_0 + a_1\, x + \cdots + a_{m-1}\, x^{m-1} \ \in \mathcal{F}.$$

Thus,

$$\begin{aligned} \forall\ \mathrm{A}, \mathrm{B} \in \mathsf{F}\ (\mathrm{A} \bullet \mathrm{B} = \sigma(\sigma^{-1}(\mathrm{A}) \cdot \sigma^{-1}(\mathrm{B}))) \wedge \\ (\mathrm{A} + \mathrm{B} = \sigma(\sigma^{-1}(\mathrm{A})\ +\ \sigma^{-1}(\mathrm{B}))). \end{aligned} \tag{10}$$

It is also said that the field $GF(p^m)$ is the field extension $GF(p)[x]/(f(x))$ where $f(x)$ is an irreducible polynomial of degree m over the integers modulo p.

According to the above description of operations in a Galois field we may note that to efficiently implement arithmetic in $GF(p^m)$ we need fast routines doing addition of polynomials over $GF(p)$ and their multiplication over $GF(p)$ modulo irreducible polynomial with coefficients from $GF(p)$. Besides we also need a function which realizes the mappings σ and σ^{-1}, the function determining the extended Euclidean algorithm for polynomial, etc. The system Maple provides such set of the routines which use a special data representation. Knowledge of this representation is not required by the user who wants to compute in Galois fields only. In this case a user-friendly module **GF** suffices.

It is mentioned in the Maple manual that if the modulus p is sufficiently small, operations in $GF(p^m)$ are performed directly by the hardware. The largest prime for which computations are done in this way is the number 46327 (on a 32 bit machine).

2. Computing in $GF(p^m)$ using Maple GF package

The Maple library package **GF**, having the structure of a module, returns routines and constants performing arithmetic in $GF(p^m)$. To begin computing we must first create an instance `F` of a Galois field $GF(p^m)$ using, for example, the statements

```
#arithmetic in GF(125) has been defined
>  p := 5: m := 3:
   f := 1 + 2*x  + x^3:
   F := GF(p, m, f):
```

The actual parameters p, m and f exactly correspond to the variables p, m, and the polynomial $f(x)$, used in Section 1. The parameter f is optional - if it is absent in the invocation statement of the module GF, then the system Maple selects itself the irreducible polynomial f(T). This case will not be considered here, because we must control the behavior of the field using the polynomial f.

Addition, subtraction, multiplication, raising to the $k-$th power, computation of the multiplicative inverse and division in the Galois field are performed by means of the following routines, respectively:

F:-‘+‘(x1, x2, ..., xn::zppoly)	: $n-$ary addition
F:-‘-‘(x1, x2::zppoly)	: unary or binary subtraction
F:-‘*‘(x1, x2, ..., xn::zppoly)	: $n-$ary multiplication
F:-‘^‘(x::zppoly, k::integer)	: raising x to the $k-$th power
F:-inverse(x::zppoly)	: unary inversion
F:-‘/‘(x1, x2::zppoly)	: unary or binary division

The operands x1, x2, ..., xn and x of the routines performing operations in $GF(p^m)$ must be of a special type, zppoly, relating to the Maple modp1 function. The results returned by these routines are of the same type. But we may need to operate using operands of type polynom, nonnegint and zppoly and obtain these three type of results. To achieve the aim we ought to use the following unary conversion routines:

routine name	type of result
F:-input(x::integer)	zppoly
F:-output(x::zppoly)	integer
F:-ConvertIn(x::symbol, +, * or ^)	zppoly
F:-ConvertOut(x::zppoly)	symbol, +, * or ^

In practice, we usually use operands of type polynom or nonnegint and we want to have the type of results of computations of the same type as that of operands.

Example 1. Suppose that the statements in the beginning of the section and the statements beneath have been executed. We will now compute in $GF(125)$. After defining three elements of $GF(125)$ in the form of polynomials ax, bx and cx, we can observe how to compute the multiplicative inverse of ax, the additive inverse of bx, the sum of ax, bx and cx and the product of these three elements:

```
>  ax := 4*x + 3: bx := 2*x + 1: cx := x^2 + 2:
>  F:-ConvertOut(F:-inverse(
                 F:-ConvertIn(ax)));
```

$$4x^2 + 2x + 4$$

```
>  F:-ConvertOut(F:-‘-‘
                 F:-ConvertIn(bx)));
```

$$3x + 4$$

```
>    F:-ConvertOut(F:-‘+‘(
                   F:-ConvertIn(ax),
                   F:-ConvertIn(bx),
                   F:-ConvertIn(cx)));
```

$$x^2 + x + 1$$

```
>   F:-ConvertOut(F:-‘*‘(
                  F:-ConvertIn(ax),
                  F:-ConvertIn(bx),
                  F:-ConvertIn(cx)));
```

$$3x^2 + 2x + 1$$

Further let us define three numbers A, B and C which will play the role of elements form $GF(125)$ by means of the appropriate statement and let's execute the same operations as previously:

```
>  A := 23: B := 11: C := 27:
>  F:-output(F:-inverse(
             F:-input(A)));
```

$$114$$

```
>  F:-output(F:-‘-‘(
             F:-input(B)));
```

$$19$$

```
>  F:-output(F:-‘+‘(
             F:-input(A),
             F:-input(B),
             F:-input(C)));
```

$$31$$

```
>  F:-output(F:-‘*‘(
             F:-input(A),
             F:-input(B),
             F:-input(C)));
```

$$86$$

It is also possible to calculate more complicated expressions over $GF(125)$ using directly the package **GF**. E.g. the expression

$$w = \frac{A\,B + A\,C + B\,C}{A + B + C}$$

may be calculated as follows:

```
> w := F:-output(F:-‘/‘(
          F:-‘+‘(
          F:-‘*‘(F:-input(A), F:-input(B)),
          F:-‘*‘(F:-input(A), F:-input(C)),
          F:-‘*‘(F:-input(B), F:-input(C))),
          F:-‘+‘(F:-input(A), F:-input(B), F:-input(C))));
```

$$w := 6$$

Programming of similar expressions can be considerably simplified by means of auxiliary procedures having short names. For example, if we use routines named `a_`, `m_` and `d_` for performing addition, multiplication and division in $GF(p^m)$, respectively, then the above expression will have the form

```
> w := d_(a_(m_(A, B), m_(A, C), m_(B, C)), a_(A, B, C));
```

$$w := 6$$

which gives the same result but is much more simple. In Appendices A and B it is shown how to construct such routines.

The module **GF** also exports the following functions:

```
F:-trace(x::zppoly),
F:-norm(x::zppoly),
F:-order(x::zppoly),
F:-random(),
F:-isPrimitiveElement(x::zppoly),
F:-PrimitiveElement(),
F:-zero,
F:-one,
F:-variable,
F:-size,
F:-factors(),
F:-extension,
```

which allow to do an advanced research on applications of Galois fields, but cogitation about them is not within the scope of this paper.

3. A system $gff(n^m)$ - a generalized finite field

It is possible to view Galois field from another angle. Now let n be an arbitrary integer ≥ 2, $m-$ an arbitrary integer ≥ 1, $f(x)-$ an arbitrary polynomial of degree m over the ring Z_n. Next let

$$gff(n^m) = \langle \mathsf{F}[x],\ +,\ \cdot \rangle, \tag{11}$$

be an algebraic system consisting of the set $\mathsf{F}[x]$ of all n^m polynomials of degree d , $0 \leqslant d \leqslant m-1$, 0 included, over the ring Z_{n} and of operations of addition and multiplication of these polynomials. Operations on elements of $gff(n^m)$ are performed nearly in the same manner as in $GF(p^m)$: addition over the ring Z_{n}, multiplication over the same ring modulo polynomial $f(x)$.

It is easy to observe that $gff(n^m)$ fulfills the following set of axioms:

f1 The system $\langle \mathsf{F}[x],\ + \rangle$, is an abelian group.

f2 The system $\langle \mathsf{F}[x]^*,\ \cdot \rangle$ is an abelian quasigroupoid[✠],
$\mathsf{F}[x]^* = \mathsf{F}[x] \setminus \{0\}$, where 0 is an additive identity element.

[✠] 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.

f3 $\forall a,\ b,\ c\ \in \mathsf{F}[x]\ (a \cdot (b+c) = a \cdot b + a \cdot c) \wedge ((a+b) \cdot c = a \cdot c + b \cdot c)$.

The multiplicative system of $gff(n^m)$ is an abelian quasigroupoid $\langle \mathsf{F}[x]^*,\ \cdot \rangle$, which is not closed under multiplication, since if n is not a prime, then for some $a,\ b\ \in \mathsf{F}[x]$ the case $a \cdot b = 0$ may occur. Several properties of this quasigropupoid in [1] are described. For example, the elements of this quasigroupoid belong to two disjoint sets - a set of invertible elements and a set of non invertible elements. Any invertible element is a generator of cyclic group, being a subgroup of the groupoid. Furthermore one should know that if n is not a prime of if $f(x)$ is not irreducible then the system $gff(n^m)$ is not an integral domain. In this case the extended Euclidean algorithm for polynomials fails and cannot be able to determine all invertible elements in $gff(n^m)$.

After applying the mapping (8) to the system (11), taking into account that now $p = n$, we obtain the system

$$gff(n^m) = \langle \mathsf{F},\ \mathsf{+},\ \bullet \rangle, \tag{12}$$

the elements of which are numbers from the set $\{0,\ 1,\ \ldots,\ n^m - 1\}$. Such system is the most useful for cryptography.

Example 2. To familiarize the reader with some properties of $gff(n^m)$ having elements in the form of numbers the tables of operations in $gff(4^2)$ and in $gff(16)$ have been calculated and shown in Table 1 and Table 2. We may notice that multiplication on invertible elements is commutative and associative, so, an appropriate fragment of the multiplication table is a Latin square.

To the family of systems $gff(n^m)$ belongs a big class of algebraic structures. E.g. if n is a prime and $f(x)$ is not irreducible then the multiplicative structure of $gff(p^m)$ forms $SMG(p^m)$, if n is prime and $f(x)$ irreducible, $gff(n^m)$ becomes $GF(p^m)$. Thus, $gff(n^m)$, as a generalization of finite fields, may be called a generalized finite field. Although all properties of $gff(n^m)$ are not yet known, this algebraic structure will certainly be broadly applied, mainly in cryptography and coding.

4. A method of computing in $gff(n^m)$

While defining Galois field using Maple package one invokes the **GF** module with or without the third actual parameter, namely, without the irreducible polynomial. If we use this parameter, the polynomial must be absolutely

Table 1: Addition and multiplication tables in $gff(4^2)$ with $f(x) = x^2+x+3$ over Z[4]. The set of invertible elements: $\{1, 3, 4, 5, 6, 7, 9, 11, 12, 13, 14, 15\}$

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

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

Table 2: Addition and multiplication tables in $gff(16)$ with $f(x) = x$ over Z[16]. The set of invertible elements: $\{1, 3, 5, 7, 9, 11, 13, 15\}$

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

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

irreducible, otherwise the module does not work. This means that the **GF** module is not suitable for computing in $gff(n^m)$, in which multiplication of its elements is taken over Z_n modulo an arbitrary polynomial $f(x)$ with coefficients from Z_n. In order to overcome this obstacle one should resort to the source on the basis of which the **GF** module has been built: the `modp1` function.

It may be said, without going into details, that operations in $gff(n^m)$ are performed by means of the function `modp1` according to the description given in Section 1. Using the function `modp1`, the author worked out the procedures for computing in $gff(n^m)$ and listed them in the Appendix C. These are the routines: `A_`, `S_`, `M_`, `D_`, `AI_`, `MI_` and `P_`, for performing addition, subtraction, multiplication, division, calculation of additive and multiplicative inverses and raising to a power in $gff(n^m)$, respectively. The routine `MI_` determines multiplicative inverses by means of extended Euclidean algorithm for polynomials (and usually cannot find all invertible elements). The routine `MIp_`, for computing multiplicative inverses using the multiplication operation and raising to a power in rather small $gff(n^m)$, is also listed.

To begin calculations one ought to invoke the procedure `INIT_` with determined actual parameters corresponding to formal parameters `nn` and `fx`, representing the modulus n and the polynomial $f(x)$, which defines multiplication. The procedure turns the actual parameter corresponding to the formal parameter `nn` into the global variable `n` and the actual parameter which replaces the formal parameter `fx` into the global variable `ext`. These two global variables are indispensable for assuring the operation of the remaining routines.

Here is an example of usage of these procedures:

Example 3. We will compute the expression

$$t = \frac{AB + AC + BC}{\frac{1}{A} - \frac{1}{B} + \frac{1}{C}}$$

in $gff(16^2)$ with $f(x) = x^2 + 2x + 11$ for $A = 13,\ B = 254,\ C = 50,$. Then we calculate the same expression in $GF(2^8)$ when $f(x) = x^8 + x^4 + x^3 + x + 1$.

```
> INIT_(16, x^2 + 2*x + 11): A := 13: B := 24: C := 1:
>  t := D_(A_(M_(A, B), M_(A, C), M_(B, C)),
          A_(A_(MI_(A), AI_(MI_(B))), MI_(C)));
```

$$t := 60$$

```
> INIT_(2, x^8 + x^4 + x^3 + x + 1):
> t := D_(A_(M_(A, B), M_(A, C), M_(B, C)),
            A_(A_(MI_(A), AI_(MI_(B))), MI_(C)));
```

$$t := 184$$

The result of computations in $gff(16^2)$ has been achieved since there exist there multiplicative inverses for A, B and C. The element $27 \in gff(16^2)$ is not invertible, then if $A = 27$ the expression t will not be determined.

5. Conclusions

Apart from the discussion about using the **GF** Maple library package in application research, in the paper a new algebraic structure denoted as $gff(n^m)$ and named generalized finite field, has been defined. For the defined structure a complete set of routines for performing all possible operations on elements of $gff(n^m)$ has been presented. Since $gff(n^m)$ is a generalization of Galois field, the routines can be also used for doing arithmetic in finite fields and may stand in for the Maple **GF** module in the case of computing in huge fields, when this module is useless (i.e. when it is not able to factorize $p^m - 1$). The time of execution of any operation depends on the number of elements of $gff(n^m)$ and on the size of operands. If, for example, $n^m \approx 10^{30}$, 10^{300}, 10^{3000} and 10^{30000}, $x = \lceil n^m/2 \rceil$, $y = x$, $C(x, y)$ denotes an arbitrary binary or n-ary operation on elements $x,\ y \in gff(n^m)$, then the time of execution of one such operation equals approximately to 0.1 milliseconds, 0.3 milliseconds, 5 milliseconds and 250 milliseconds, respectively (Maple 9.5 on PC with the processor Pentium 4). The **GF** module gives similar results, but it has problems with computing in many fields of order higher than 10^{100}.

The generalized finite field, in comparison with Galois field, seems to be messy and defective. This feature ensures that $gff(n^m)$ will be used mainly for implementing transformations creating diffusion and confusion during the encryption process, and in random number and cryptographic key generators.

Apology and acknowledgment

The author feels obliged to state that not all the errors which were observed in his work [1] by Prof. A. D. Keedwell, have been corrected. It refers to "reversible" instead of a proper term "invertible". This mistake was unintentional and the author apologizes to Prof. A. D. Keedwell and to the readers.

The author also very much appreciates kind advice of Prof. Keedwell, concerning errors in the draft of this paper.

Appendix A

In this Appendix the routines `ax_`, `sx_`, `mx_`, `dx_`, `px_`, `mix_` and `aix_`, for doing addition, subtraction, multiplication, division, rising to a power, computing additive and multiplicative inverses in $GF(p^m)$, respectively, are listed. The procedures will work properly if we create an instance of p^m- element Galois field by means of the statement

```
> F := GF(p, m);
```

or

```
> F := GF(p, m, fx);
```

after previously defining actual parameters `p`, `m`, and, in the second statement, `fx`, which denote a prime, a positive integer and an irreducible polynomial of degree m over $GF(p)$. The routine `ax_` is $n-$ary, the routines `aix_` and `mix_` are unary and the remaining ones binary. The parameters of these routines are elements of $GF(p^m)$ in the form of polynomials and the routines return also the results as polynomials.

```
>  ax_ := proc()
 local i, s, ss;
     s := proc(a, b::polynom)
            F:-ConvertOut(
            F:-`+`(F:-ConvertIn(b), F:-ConvertIn(a)))
         end proc;
     ss := 0;
     for i to nargs do ss := s(ss, args[i]) end do;
     ss
 end proc:

> sx_ := proc(a, b::polynom)
     F:-ConvertOut(F:-‘-‘(F:-ConvertIn(b), F:-ConvertIn(a)))
 end proc:

>  mx_ := proc(a, b::polynom)
     F:-ConvertOut(F:-‘*‘(F:-ConvertIn(b), F:-ConvertIn(a)))
 end proc:

>  dx_ := proc(a, b::polynom)
     F:-ConvertOut(F:-‘/‘(F:-ConvertIn(b), F:-ConvertIn(a)))
 end proc:

> mix_ := proc(a::polynom)
      F:-ConvertOut(F:-inverse(F:-ConvertIn(a)))
 end proc:

> aix_ := proc(a::polynom)
      F:-ConvertOut(F:-‘-‘(F:-ConvertIn(a)))
 end proc:

> px_ := proc(a::polynom, k::integer)
      F:-ConvertOut(F:-‘^‘(F:-ConvertIn(a), k))
 end proc:
```

Appendix B

Similarly as in Appendix A, the routines `a_`, `s_`, `m_`, `p_`, `d_`, `ai_` and `mi_`, for doing addition, subtraction, multiplication, division, rising to a power, computing additive and multiplicative inverses in $GF(p^m)$, respectively, are listed here. The procedures will work properly if we create an instance of p^m- element Galois field by means of the statement

```
> F := GF(p, m);
```

or

```
> F := GF(p, m, fx);
```

after previously defining actual parameters `p`, `m`, and, in the second statement, `fx`, which denote a prime, a positive integer and an irreducible polynomial of degree m over $GF(p)$. The routine `a_` is $n-$ary, the routines `ai_` and `mi_` unary and the remaining ones binary. The parameters of these routines are elements of $GF(p^m)$ in the form of numbers from the set $\{0,\ 1,\ \ldots,\ p^m - 1\}$ and they return also the results as numbers from this set.

```
> a_ := proc()
  local i, s, ss;
     s := proc(a, b::nonnegint)
             F:-output(
             F:-`+`(F:-input(a), F:-input(b)))
         end proc;
     ss := 0;
     for i to nargs do ss := s(ss, args[i]) end do;
     ss
  end proc:

> s_ := proc(a, b::nonnegint)
     F:-output(F:-`-`(F:-input(a), F:-input(b)))
  end proc:

> m_ := proc(a, b::nonnegint)
     F:-output(F:-`*`(F:-input(a), F:-input(b)))
  end proc:

> d_ := proc(a, b::nonnegint)
     F:-output(F:-`/`(F:-input(a), F:-input(b)))
  end proc:

> ai_ := proc(a::nonnegint)
      F:-output(F:-`-`(F:-input(a)))
  end proc:

> mi_ := proc(a::nonnegint)
      F:-output(F:-inverse(F:-input(a)))
  end proc:
```

```
> p_ := proc(a::nonnegint, k::integer)
         F:-output(F:-‘^‘(F:-input(a), k))
  end proc:
```

Appendix C

In this Appendix the routines `INIT_`, `A_`, `S_`, `M_`, `P_`, `D_`, `AI_`, `MI_` and `MIp_`, for initializing computations and for doing addition, subtraction, multiplication, division, rising to a power, computing additive and multiplicative inverses in the generalized finite field $gff(n^m)$, respectively, are listed. The procedures doing computations in $gff(n^m)$ will work properly if we first execute the statement

```
> INIT_(nn, fx);
```

after previously defining actual parameters corresponding to the formal parameters `pn`, and `fx`, which denote an arbitrary positive integer and an arbitrary polynomial of degree m over the ring Z_n, respectively. This routine calculates the global variables $n = nn$ and ext, which represent the modulus n and the polynomial `fx` as the polynomial of type `zppoly`, respectively. These global variables are necessary for all routines doing arithmetic in $gff(n^m)$. The routine `A_` is $n-$ary, the routines `AI_`, `MI_` and `MIp_` are unary and the remaining ones binary. The parameters of these routines are elements of $gff(n^m)$ in the form of numbers from the set $\{0,\ 1,\ \ldots,\ n^m-1\}$ and they also return the results as numbers from this set.

```
> INIT_ := proc(nn::posint, fx::polynom)
 global ext, n;
     ext := modp1(ConvertIn(modp(fx, nn), x), nn);
     n := nn
 end proc:

> A_ := proc()
 local a, i, t;
     a := [args];
     for i to nargs do a[i] :=
         modp1(ConvertIn(convert(a[i], base, n), x), n)
     end do;
     t := modp1(ConvertOut(modp1('Add'(op(a)), n), u), n);
     subs(u = n, t)
 end proc:

> S_ := proc(a, b::nonnegint)
  local t, u;
      t := modp1(ConvertOut(modp1('Subtract'(
          modp1(ConvertIn(convert(a, base, n), x), n),
          modp1(ConvertIn(convert(b, base, n), x), n)), n)
          , u), n);
      subs(u = n, t)
  end proc:

> M_ := proc(a, b::nonnegint)
 local t, u;
     t := modp1(ConvertOut(modp1(Rem('Multiply'(
         modp1(ConvertIn(convert(a, base, n), x), n),
         modp1(ConvertIn(convert(b, base, n), x), n)), ext), n)
         , u), n);
     subs(u = n, t)
 end proc:

> P_ := proc(a::nonnegint, k::integer)
 local t, u;
     t := modp1(ConvertOut(modp1('Powmod'(
         modp1(ConvertIn(convert(a, base, n), x), n), k, ext),
         n), u), n);
     subs(u = n, t)
 end proc:

> D_ := proc(a::nonnegint, b::posint)
      M_(a, MI_(b))
 end proc:

> AI_ := proc(a::nonnegint)
  local t, u;
      t := modp1(ConvertOut(modp1(
          'Subtract'(modp1(ConvertIn(convert(a, base, n), x),
                    n)), n), u), n);
      subs(u = n, t)
  end proc:

> MI_ := proc(a::posint)
 local s, t;
     modp1('Gcdex'(modp1(ConvertIn(convert(a, base, n), x), n),
         ext, 's'), n);
     t := modp1(ConvertOut(s, x), n);
     subs(x = n, t)
 end proc:

> MIp_ := proc(a)
 local mi, k, mk, nn;
     mi := a;
     k := 0;
     nn := n^degree(modp1(ConvertOut(ext, x), n));
     if a = 1 then return 1 end if;
     while mi > 1 do
         k := k + 1;
         mi := M_(mi, a);
         if mi = 0 or k > nn - 1 then
             error "inverse does not exist"
         end if
     end do;
     P_(a, k)
 end proc:
```

References

[1] **C. Kościelny**: *Spurious multiplicative group of $GF(p^m)$: a new tool for cryptography*, Quasigroups and Related Systems **12** (2004), 61 – 73.

[2] **R. Lidl, H. Niederreiter**: *Introduction to finite fields and their applications*, Cambridge University Press (1986).

[3] **A. J. Menezes, Editor**: *Applications of finite fields*, Kluwer Academic Publishers, (1993).

Received June 16, 2005

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 **13** (2005), 265 – 268

AES with the increased confidentiality

Czesław Kościelny

Abstract

It has been shown in the paper how to use well known encrypting algorithms AES -128, AES-192 and AES-256 as algorithms AES-340, AES-404 and AES-468, respectively, having considerably increased key space.

1. Introduction

As it is known, the AES algorithm [1] is a symmetric-key block cipher which uses cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. From the mathematical point of view this algorithm is interesting for any algebraist, as an example of advanced computing in Galois fields. In particular, the algorithm apply one fixed element from $GF(256)$ to compute round constant array, one affine transformation over $GF(2)$ with fixed $8{\times}8$ matrix and c vector, a fixed pair of mutually invertible polynomials of degree $\leqslant 3$ over $GF(256)$ belonging to the polynomial ring modulo x^4-1, a fixed irreducible polynomial of degree 8 over $GF(2)$ defining multiplication in $GF(256)$, and performs many operations of multiplication, addition and inversion in this field. Furthermore, $GF(256)$ can be perceived not only as a field but simultaneously as two groups, two quasigroups or two groupoids as well. That is why this paper deserves, in the author's opinion, to be published in Quasigroups and Related Systems, even though it concerns highly application oriented problem.

2000 Mathematics Subject Classification: 68P25, 11T
Keywords: cryptography, AES algorithm, Galois fields.

2. A method of using the AES algorithm with considerably enlarged key space

Without going into details we may shortly say, that in order to use the algorithm AES [1] as a cryptosystem with the increased confidentiality it simply suffices to replace all fixed constants, appearing in cryptographic transformations and routines of the algorithm, viz.

▷ the value `{02}` in `Rcon[i][1]`,

▷ the elements of affine transformation, i.e. the byte value $c =$ `{63}` and the matrix

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

▷ the non-primitive irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ over $GF(2)$,

▷ the polynomial $a(x) = \texttt{\{03\}}\,x^3 + \texttt{\{01\}}\,x^2 + \texttt{\{01\}}\,x + \texttt{\{02\}}$ over $GF(256)$ and its inverse modulo $x^4 - 1$,

▷ and finally the number of rounds r that should be taken into account during the execution of `KeyExpansion`, `Cipher` and `InvCipher` routines,

▶ by 6 variables, stored in the array

$$K_S = [K_{\texttt{Rcon}}, K_c, K_A, K_m, K_a, K_r], \tag{1}$$

which will form together with 128, 192 or 256 bit key K a cryptographic key for the generalized in this way AES:

$$K_{IC} = K,\, K_S. \tag{2}$$

It should be explained in this place that the sufficient level of diffusion and confusion may be attained already after executing from one to three rounds of encrypting procedure, therefore, the value of actual parameter replacing the formal parameter Nr in the invocation statement of the routines `Cipher` and `InvCipher`, viz. the element K_r of the array K_S may belong to the interval $[3,\, Nr]$.

The presented approach allows the reader either to design a large class of AES ciphers with various cryptographic transformations and rule of multiplication in $GF(256)$, or to use the AES algorithms as a quite strong cipher with 7-element cryptographic key. Considering the second case of this alternative, one should first determine an equivalent increment of the cryptographic key length of the cryptosystem resulting from the presented approach. This increment can be computed by means of the equation

$$\Delta_K = \lfloor \frac{\ln(256^2 \cdot (Nr-2) \cdot Nip \cdot Nnsm_{8\times 8}(2) \cdot Nnscm_{4\times 4}(256))}{\ln(2)} \rfloor, \tag{3}$$

where the formulae

$$Nnsm_{8\times 8}(q) = \prod_{k=0}^{n-1} (q^n - q^k), \quad Nnscm_{4\times 4}(q) = \frac{(q-1)^4\, q^{12}}{4},$$

determine the number of non-singular matrices 8×8 over $GF(q)$ (see [3, p. 3]) and the number of non-singular circulant matrices 4×4 over $GF(q)$ of characteristic 2 (see [3, pp. 7, 80]) (equal also to the number of invertible modulo x^4-1 polynomials of degree $\leqslant 3$ over $GF(256)$), respectively,
Nip – denotes the number of irreducible polynomials of degree 8 over $GF(2)$,
Nr – equals to the number of rounds depending on the key length as is recommended by [1].

Taking into account [1], (3) and the fact that the $Nip = 30$, we get $\Delta_K = 212$, which means that we can use AES-128, AES-192 and AES-256 as AES-128+Δ_K, AES-192+Δ_K and AES-256+Δ_K, that is as AES-340, AES-404 and AES-468, correspondingly. To implement AES-340, AES-404 and AES-468 we may bring into play almost the same software or hardware as for AES-128, AES-192 and AES-256. Assuming that the implementation of described here AES algorithm with the increased level of privacy will explicitly employ the operations in $GF(256)$, namely, addition, multiplication and rising to a positive or negative power, performed by means of the appropriate routines, arrays or hardware, we may summarize the encrypting/decrypting procedures as follows:

Encryption: Entity $\mathcal{B}$ encrypts a plaintext block M for entity $\mathcal{A}$, which $\mathcal{A}$ decrypts. Thus $\mathcal{B}$ should make the following steps:

Step 1: Generate the cryptographic key $K_{IC} = K$, K_S (K_{IC} may be used for encryption the whole message, consisting of many blocks). The elements of the array K_S should be, of course, suitably computed.

Step 2: Send the key K_{IC} to $\mathcal{A}$ using secure channel.

Step 3: Adapt the system for computing in $GF(256)$ defined by the polynomial K_m contained in K_S, compute S-box and inverse S-box tables and the the array `Rcon` taking into account K_A, K_c and $K_{\texttt{Rcon}}$, next modify all these algorithm's transformations and routines given in [1], which depend on data stored in K_S.
Step 4: Generate the key schedule using the the same `KeyExpansion` routine as in [1], but apply the value K_r as the actual parameter of the formal parameter Nr.
Step 5: Compute the ciphertext block C of the plaintext block M using the same routine `Cipher` as given in [1], but apply the value K_r as the actual parameter of the the formal parameter Nr, next send the ciphertext to $\mathcal{A}$ thorough unsecured channel.
Decryption: To find plaintext block M from the ciphertext block C, the entity $\mathcal{A}$ should perform the following operations:
Step 1: Receive the cryptographic key $K_{IC} = K,\ K_S$ by means of a secure channel.
Step 2: Receive the ciphertext block C using the unsecured channel.
Step 3: As Step 3 of Encryption.
Step 4: As Step 4 of Encryption.
Step 5: Retrieve the plaintext block M from the ciphertext block C using the same routine `InvCipher` as presented in [1], but apply the value K_r as the actual parameter of the formal parameter Nr.

3. Conclusion

Although the implementation of the generalized AES algorithm requires some effort, this work is profitable, because it delivers not only a strong symmetric-key block cipher, but also a universal tool for exact examination of properties of algorithms AES-128, AES-192 and AES-256.

References

[1] **NIST**: *Advanced Encryption Standard (AES)*, FIPS PUB 197, 2001.

[2] **C. Kościelny**: *Computing in $GF(p^m)$ and in $gff(n^m)$ using Maple*, Quasigroups and Related Systems **13** (2005), 245 – 264.

[3] **A.J. Menezes, editor**: *Applications of Finite Fields*, Kluwer Academic Publishers, 1993.

Received July 13, 2005

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

Quasigroups and Related Systems **13** (2005), 269 − 280

A class of quasigroups associated with a cubic Pisot number

Vedran Krčadinac and Vladimir Volenec

Abstract

In this paper idempotent medial quasigroups satisfying the identity $(ab \cdot a)a = b$ are studied. An example are the complex numbers with multiplication defined by $a \cdot b = (1-q)a + qb$, where q is a solution of $q^3 - 2q^2 + q - 1 = 0$. The positive root of this cubic equation can be viewed as a generalization of the golden ratio. It turns out that the quasigroups under consideration have many similar properties to the so-called golden section quasigroups.

1. Introduction

Let $q \neq 0, 1$ be a complex number and define a binary operation on $\mathbb{C}$ by $a \cdot b = (1-q)a + qb$. It is known that $(\mathbb{C}, \cdot)$ is an IM-quasigroup, i.e. satisfies the laws of *idempotency* and *mediality*:

$$a \cdot a = a, \tag{1}$$

$$ab \cdot cd = ac \cdot bd. \tag{2}$$

Immediate consequences are the identities known as *elasticity*, *left* and *right distributivity*:

$$ab \cdot a = a \cdot ba, \tag{3}$$

$$a \cdot bc = ab \cdot ac, \tag{4}$$

$$ab \cdot c = ac \cdot bc. \tag{5}$$

This quasigroup will be denoted by $C(q)$. For some special values of q, the quasigroup satisfies additional identities. If $q = \frac{1+\sqrt{5}}{2}$ is the golden ratio,

2000 Mathematics Subject Classification: 20N05.
Keywords: IM-quasigroup, Pisot number.

$C(q)$ is a representative example of the *golden section* or *GS-quasigroups*. GS-quasigroups were defined in [8] as idempotent quasigroups satisfying the (equivalent) identities $a(ab \cdot c) \cdot c = b$, $a \cdot (a \cdot bc)c = b$; see also [2], [3], [4] and [10]. An alternative definition would be as IM-quasigroups with the simpler identity $a(ab \cdot b) = b$. In this paper we study IM-quasigroups satisfying a similar identity:

$$(ab \cdot a)a = b. \tag{6}$$

Representative examples are the quasigroups $C(q)$ with q a root of $q^3 - 2q^2 + q - 1 = 0$. Denote by $r_{1,2} = \sqrt[3]{\frac{25 \pm \sqrt{69}}{2}}$. The roots of this cubic equation are $q_1 = \frac{1}{3}\,(2 + r_1 + r_2) \approx 1.755$ and $q_{2,3} = \frac{1}{6}\,\big(4 - r_1 - r_2 \pm i\sqrt{3}\,(r_1 - r_2)\big) \approx 0.123 \pm 0.745\,i$. The number q_1 is a Pisot number, i.e. an algebraic integer greater than 1 whose algebraic conjugates $q_{2,3}$ have absolute values less than 1. This number was considered in [5] as a generalization of the golden ratio and was called the *second upper golden ratio*. Therefore, we will refer to IM-quasigroups satisfying the identity (6) as *G_2-quasigroups*.

In the context of [5], the *second lower golden ratio* was the positive root of $p^3 - p - 1 = 0$. This is the smallest Pisot number $p_1 \approx 1.325$; note that $q_1 = p_1^2$. For more details about Pisot numbers see [1].

In this paper it is shown that G_2-quasigroups have many properties similar to those of GS-quasigroups. For example, they allow a simple definition of parallelograms using an explicit formula for the fourth vertex. In the last section G_2-quasigroups are characterized in terms of Abelian groups with a certain type of automorphism.

2. Basic properties and further identities

The following lemma will be used quite often.

Lemma 2.1. *In an IM-quasigroup, identity* (6) *is equivalent with either of the identities*

$$(a \cdot ba)a = b, \tag{7}$$

$$a(ba \cdot a) = b. \tag{8}$$

Proof. By using elasticity we get $(ab \cdot a)a \overset{(3)}{=} (a \cdot ba)a \overset{(3)}{=} a(ba \cdot a)$. □

Note that the equivalence holds even in a groupoid satisfying (1) and (2). Elasticity follows directly from idempotency and mediality, without using solvability or cancellativity. Consequently, the definition of G_2-quasigroups can be relaxed to the identities alone.

Proposition 2.2. *Any groupoid satisfying* (1), (2) *and* (6) *is necessarily a quasigroup.*

Proof. Given a and b define $x = ab \cdot a$ and $y = ba \cdot a$. From (6) and (8) we see that $xa = b$ and $ay = b$, i.e. the groupoid is left and right solvable. Now assume $ax_1 = ax_2$ and $y_1 a = y_2 a$. Then, $x_1 \overset{(6)}{=} (ax_1 \cdot a)a = (ax_2 \cdot a)a \overset{(6)}{=} x_2$ and $y_1 \overset{(8)}{=} a(y_1 a \cdot a) = a(y_2 a \cdot a) \overset{(8)}{=} y_2$, so the groupoid is left and right cancellative. □

The next proposition is similar to [8, Theorem 5].

Proposition 2.3. *In a G_2-quasigroup, any two of the equalities $ab = c$, $ca = d$ and $da = b$ imply the third.*

Proof. Denote the equalities by (i), (ii) and (iii), respectively. Then we have:

$$\begin{aligned}
(i), (ii) \Rightarrow (iii):& \quad da \overset{(ii)}{=} ca \cdot a \overset{(i)}{=} (ab \cdot a)a \overset{(6)}{=} b,\\
(i), (iii) \Rightarrow (ii):& \quad ca \overset{(i)}{=} ab \cdot a \overset{(iii)}{=} (a \cdot da)a \overset{(7)}{=} d,\\
(ii), (iii) \Rightarrow (i):& \quad ab \overset{(iii)}{=} a \cdot da \overset{(ii)}{=} a(ca \cdot a) \overset{(8)}{=} c.
\end{aligned}$$

□

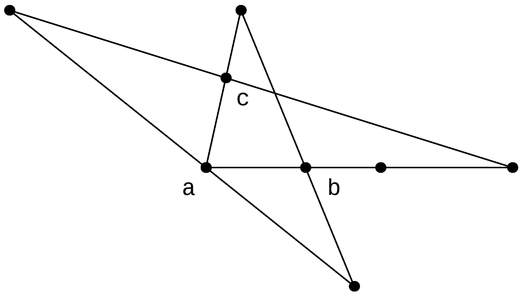

Figure 1: Identity (9) in the complex plane.

We list some more identities valid in G$_2$-quasigroups. They are accompanied by pictures illustrating the example of the complex plane with multiplication defined by $a \cdot b = (1 - q_1)a + q_1 b$.

Proposition 2.4. *The following identity holds in any G_2-quasigroup:*

$$(a \cdot ab)c \cdot a = ac \cdot b. \tag{9}$$

Proof. $(a \cdot ab)c \cdot a \overset{(5)}{=} (a \cdot ab)a \cdot ca \overset{(5)}{=} (a \cdot ab)(ca) \cdot (a \cdot ca) \overset{(3)}{=} (a \cdot ab)(ca) \cdot (ac \cdot a) \overset{(2)}{=} (ac)(ab \cdot a) \cdot (ac \cdot a) \overset{(4)}{=} ac \cdot (ab \cdot a)a \overset{(6)}{=} ac \cdot b.$ □

Proposition 2.5. *The following identity holds in any G_2-quasigroup:*

$$(ab \cdot a)c \cdot b = (ab \cdot c)a. \tag{10}$$

Proof. $(ab{\cdot}a)c{\cdot}b \overset{(5)}{=} (ab{\cdot}b)(ab){\cdot}cb \overset{(3)}{=} (ab)(b{\cdot}ab){\cdot}cb \overset{(2)}{=} (ab{\cdot}c){\cdot}(b{\cdot}ab)b \overset{(7)}{=} (ab{\cdot}c)a.$ □

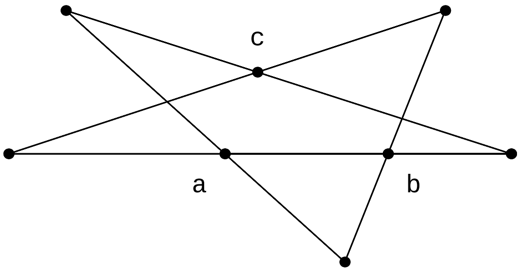

Figure 2: Identity (10) in the complex plane.

Proposition 2.6. *The following identity holds in any G_2-quasigroup:*

$$a \cdot (ba \cdot c)d = b(ac \cdot d). \tag{11}$$

Proof. $a \cdot (ba \cdot c)d \overset{(5)}{=} a \cdot (ba \cdot d)(cd) \overset{(4)}{=} (a \cdot ba)(ad) \cdot (a \cdot cd) \overset{(2)}{=} (a \cdot ba)a \cdot (ad \cdot cd) \overset{(7)}{=} b(ad \cdot cd) \overset{(5)}{=} b(ac \cdot d).$ □

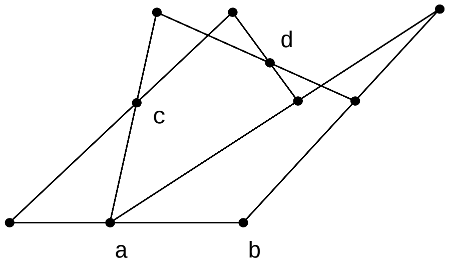

Figure 3: Identity (11) in the complex plane.

3. Parallelograms and other geometric concepts

The points a, b, c, d of a medial quasigroup are said to form a *parallelogram*, denoted by $\mathrm{Par}(a, b, c, d)$, if there are points p, q such that $pa = qb$ and $pd = qc$. In [7] it was proved that this relation satisfies the axioms of *parallelogram space*:

1. For any three points a, b, c there is a unique point d such that $\mathrm{Par}(a, b, c, d)$.

2. $\mathrm{Par}(a, b, c, d)$ implies $\mathrm{Par}(e, f, g, h)$, where (e, f, g, h) is any cyclic permutation of (a, b, c, d) or (d, c, b, a).

3. $\mathrm{Par}(a, b, c, d)$ and $\mathrm{Par}(c, d, e, f)$ imply $\mathrm{Par}(a, b, f, e)$.

In an IM-quasigroup, the unique point d of axiom 1 satisfies the following equation [9, Theorem 12]:

$$ab \cdot dc = ac. \tag{12}$$

This equation can be explicitly solved for d in GS-quasigroups: $d = a{\cdot}b(ca{\cdot}a)$ [8, Theorem 6]. Here we prove a similar result for G$_2$-quasigroups.

Proposition 3.1. *In a G_2-quasigroup, for any a, b, c we have*

$$\mathrm{Par}(a, b, c, (ba \cdot cb)b).$$

Proof. By substituting $d = (ba \cdot cb)b$ into the equation (12) we get

$$ab \cdot [(ba \cdot cb)b \cdot c] = ac.$$

It suffices to show that this is a valid identity in any G_2-quasigroup:

$$ab\cdot[(ba\cdot cb)b\cdot c] \overset{(5)}{=} ab\cdot[(ba\cdot c)(cb\cdot c)\cdot bc] \overset{(2)}{=} ab\cdot[(ba\cdot c)b\cdot(cb\cdot c)c] =$$
$$\overset{(6)}{=} ab\cdot[(ba\cdot c)b\cdot b] \overset{(5)}{=} ab\cdot[(ba\cdot b)\cdot cb]b \overset{(5)}{=} ab\cdot[(ba\cdot b)b\cdot(cb\cdot b)] =$$
$$\overset{(6)}{=} ab\cdot a(cb\cdot b) \overset{(4)}{=} a\cdot b(cb\cdot b) \overset{(8)}{=} ac.$$

□

Now we have a direct definition of parallelograms in G_2-quasigroups, without using auxiliary points:

$$\mathrm{Par}(a,b,c,d) \iff d=(ba\cdot cb)b. \qquad (13)$$

Using the parallelogram relation geometric concepts such as midpoints, vectors and translations can be introduced. Of course, in the special case of the quasigroups $C(q)$ the concepts agree with the usual definitions of plane geometry. Thus, geometric theorems can be proved by formal calculations in a quasigroup. We give an example particular to G_2-quasigroups (Theorem 3.4).

In any medial quasigroup, b is said to be the *midpoint* of the pair of points a, c if $\mathrm{Par}(a,b,c,b)$ holds. This is denoted by $M(a,b,c)$. The following proposition provides a characterization in G_2-quasigroups.

Proposition 3.2. *In a G_2-quasigroup, $M(a,b,c)$ is equivalent with*

$$c=(ab\cdot ba)a. \qquad (14)$$

Proof. By axiom 2 of parallelogram spaces, $M(a,b,c)$ is equivalent with $\mathrm{Par}(b,a,b,c)$, and the claim follows from (13). □

To facilitate notation, we introduce a new binary operation:

$$a*b=(ba\cdot a)b. \qquad (15)$$

Starting from the quasigroup $C(q_1)$, this defines the binary operation in the quasigroup $C(p_1)$, i.e. $a*b=(1-p_1)a+p_1b$. If $ab=c$ (resp. $a*b=c$), we say that b *divides the pair of points a, c in the second upper (resp. lower) golden ratio.* Here are some properties of the new binary operation. It is assumed that the original binary operation has higher priority than '$*$', e.g. $a*bc$ means $a*(bc)$.

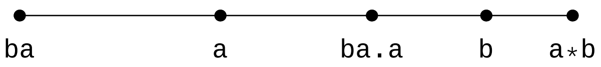

Figure 4: A new binary operation defined by (15).

Lemma 3.3. *The operation defined by* (15) *in a* G_2*-quasigroup satisfies the following identities:*

$$a * a = a, \tag{16}$$

$$ab * cd = (a * c)(b * d), \tag{17}$$

$$(a * (a * b)c)c = b. \tag{18}$$

Proof. Idempotency of the new operation (16) follows directly from (1). Identity (17) follows by repeated application of mediality:

$$\begin{aligned} ab * cd &\overset{(15)}{=} (cd \cdot ab)(ab) \cdot cd \overset{(2)}{=} (ca \cdot db)(ab) \cdot cd \overset{(2)}{=} (ca \cdot a)(db \cdot b) \cdot cd = \\ &\overset{(2)}{=} (ca \cdot a)c \cdot (db \cdot b)d \overset{(15)}{=} (a * c)(b * d). \end{aligned}$$

Here is the proof of identity (18):

$$\begin{aligned} (a * (a * b)c)c &\overset{(15)}{=} \{[(ba \cdot a)b \cdot c]a \cdot a\}[(ba \cdot a)b \cdot c] \cdot c = \\ &\overset{(2)}{=} \{[(ba \cdot a)b \cdot c]a \cdot (ba \cdot a)b\}(ac) \cdot c = \\ &\overset{(2)}{=} \{[(ba \cdot a)b \cdot c](ba \cdot a) \cdot ab\}(ac) \cdot c = \\ &\overset{(2)}{=} \{[(ba \cdot a)b \cdot ba](ca) \cdot ab\}(ac) \cdot c = \\ &\overset{(5)}{=} \{[(ba \cdot b)(ab) \cdot ba](ca) \cdot ab\}(ac) \cdot c = \\ &\overset{(2)}{=} \{[(ba \cdot b)b \cdot (ab \cdot a)](ca) \cdot ab\}(ac) \cdot c = \\ &\overset{(6)}{=} \{[a(ab \cdot a) \cdot ca](ab) \cdot ac\}c \overset{(2)}{=} \{[ac \cdot (ab \cdot a)a](ab) \cdot ac\}c = \\ &\overset{(6)}{=} [(ac \cdot b)(ab) \cdot ac]c \overset{(5)}{=} [(ac \cdot a)b \cdot ac]c \overset{(2)}{=} [(ac \cdot a)a \cdot bc]c = \\ &\overset{(6)}{=} (c \cdot bc)c \overset{(7)}{=} b. \end{aligned}$$

□

Identity (17) could be called *mutual mediality* of the two binary operations. By identifying two factors various kinds of distributivities follow:

$a * bc = (a * b)(a * c)$, $a(b * c) = ab * ac$ and their right counterparts. Identity (18) is an analogue of the defining identity for GS-quasigroups [8]. It is used in the proof of the following theorem.

Theorem 3.4. *In a G_2-quasigroup, suppose that $a * e = c$, $a * f = b$ and $cg = f$. Then, $bg = e$. Furthermore, suppose $M(a, h, g)$ and $h * g = d$. Then, $dh = a$ and $M(b, d, c)$.*

Proof. The first claim follows by substitution:

$$bg = (a * f)g = (a * cg)g = (a * (a * e)g)g \overset{(18)}{=} e.$$

If, in addition, $M(a, h, g)$ and $h * g = d$ hold, we get $g = (ah \cdot ha)a$ by (14), and the remaining claims follow by tedious, but straightforward computations:

$$\begin{aligned} dh &= (h * g)h = [h * (ah \cdot ha)a]h \overset{(15)}{=} \{[(ah \cdot ha)a \cdot h]h \cdot (ah \cdot ha)a\}h = \\ &\overset{(2)}{=} \{[(ah \cdot ha)a \cdot h](ah \cdot ha) \cdot ha\}h \overset{(2)}{=} \{[(ah \cdot ha)a \cdot ah](h \cdot ha) \cdot ha\}h = \\ &\overset{(5)}{=} \{[(ah \cdot a)(ha \cdot a) \cdot ah](h \cdot ha) \cdot ha\}h = \\ &\overset{(2)}{=} \{[(ah \cdot a)a \cdot (ha \cdot a)h](h \cdot ha) \cdot ha\}h = \\ &\overset{(6)}{=} \{[h \cdot (ha \cdot a)h](h \cdot ha) \cdot ha\}h \overset{(4)}{=} \{h[(ha \cdot a)h \cdot ha] \cdot ha\}h = \\ &\overset{(5)}{=} \{h[(ha \cdot h)(ah) \cdot ha] \cdot ha\}h \overset{(2)}{=} \{h[(ha \cdot h)h \cdot (ah \cdot a)] \cdot ha\}h = \\ &\overset{(6)}{=} [h \cdot a(ah \cdot a)](ha) \cdot h \overset{(4)}{=} h[a(ah \cdot a) \cdot a] \cdot h \overset{(3)}{=} h[a \cdot (ah \cdot a)a] \cdot h = \\ &\overset{(6)}{=} (h \cdot ah)h \overset{(7)}{=} a. \end{aligned}$$

To prove $M(b, d, c)$, we utilize (14) once more:

$$\begin{aligned} (bd \cdot db)b &\overset{(4)}{=} (bd \cdot d)(bd \cdot b) \cdot b \overset{(5)}{=} (bd \cdot d)b \cdot (bd \cdot b)b \overset{(6)}{=} (bd \cdot d)b \cdot d = \\ &= (bd \cdot d)b \cdot (h * g) \overset{(15)}{=} (bd \cdot d)b \cdot (gh \cdot h)g = \\ &\overset{(2)}{=} (bd \cdot d)(gh \cdot h) \cdot bg \overset{(2)}{=} (bd \cdot gh)(dh) \cdot bg = \\ &\overset{(2)}{=} (bg \cdot dh)(dh) \cdot bg = (ea \cdot a)e \overset{(15)}{=} a * e = c. \end{aligned}$$

□

In the special case of the quasigroup $C(q_1)$, Theorem 3.4 proves:

Corollary 3.5. *Let ABC be a triangle and suppose the points E and F divide $\overline{AC}$ and $\overline{AB}$ in the second lower golden ratio, respectively. Then the cevians $\overline{BE}$ and $\overline{CF}$ intersect in a point G that divides them in the second upper golden ratio. Furthermore, the midpoint H of $\overline{AG}$ divides the third cevian $\overline{AD}$ in the second upper golden ratio.*

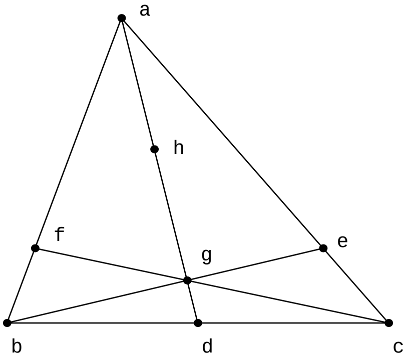

Figure 5: Geometric interpretation of Theorem 3.4.

The statement of Corollary 3.5 remains true if every instance of the second lower/upper golden ratio is replaced by the corresponding n-th golden ratio (for a definition see [5]). For $n = 1$, both the lower and the upper golden ratio are equal to $\frac{1+\sqrt{5}}{2}$ and we get the geometric interpretation of [8, Theorem 15].

4. Representation theorems

Let $(G, +)$ be an Abelian group with an automorphism φ such that the following equality holds for every $x \in G$:

$$\varphi^3(x) - 2\varphi^2(x) + \varphi(x) - x = 0. \tag{19}$$

Define another binary operation on G by the formula

$$a \cdot b = a + \varphi(b - a). \tag{20}$$

It is easy to verify that G is an IM-quasigroup with this new operation. Furthermore, the identity (6) follows from (19):

$$\begin{aligned}
(ab\cdot a)a &= ab\cdot a+\varphi(a)-\varphi(ab\cdot a)\\
&= ab+\varphi(a)-\varphi(ab)+\varphi(a)-\varphi(ab)-\varphi^2(a)+\varphi^2(ab)\\
&= 2\varphi(a)-\varphi^2(a)+ab-2\varphi(ab)+\varphi^2(ab)\\
&= 2\varphi(a)-\varphi^2(a)+(id-2\varphi+\varphi^2)(a+\varphi(b)-\varphi(a))\\
&= \big[a-\varphi(a)+2\varphi^2(a)-\varphi^3(a)\big]+\big[\varphi^3(b)-2\varphi^2(b)+\varphi(b)-b\big]+b\\
&\overset{(19)}{=} b.
\end{aligned}$$

Therefore, $(G,\cdot)$ is a G_2-quasigroup. The purpose of this section is to show that any G_2-quasigroup can be obtained in this way.

Theorem 4.1. *Let $(G,\cdot)$ be a G_2-quasigroup. Choose an arbitrary $o\in G$ and define a new binary operation on G by the formula*

$$a+b=(oa\cdot bo)o. \tag{21}$$

Then, $(G,+)$ is an Abelian group with neutral element o.

Proof. We first prove associativity, commutativity and that o is the neutral element:

$$\begin{aligned}
(a+b)+c &\overset{(21)}{=} [o\cdot(oa\cdot bo)o](co)\cdot o \overset{(5)}{=} [o\cdot(oa\cdot bo)o]o\cdot(co\cdot o)=\\
&\overset{(7)}{=} (oa\cdot bo)(co\cdot o) \overset{(2)}{=} (ob\cdot ao)(co\cdot o) \overset{(2)}{=} (ob\cdot co)(ao\cdot o)=\\
&\overset{(7)}{=} [o\cdot(ob\cdot co)o]o\cdot(ao\cdot o) \overset{(5)}{=} [o\cdot(ob\cdot co)o](ao)\cdot o=\\
&\overset{(2)}{=} (oa)[(ob\cdot co)o\cdot o]\cdot o \overset{(21)}{=} a+(b+c),
\end{aligned}$$

$$a+b \overset{(21)}{=} (oa\cdot bo)o \overset{(2)}{=} (ob\cdot ao)o \overset{(21)}{=} b+a,$$

$$a+o \overset{(21)}{=} (oa\cdot oo)o \overset{(1)}{=} (oa\cdot o)o \overset{(6)}{=} a.$$

For any $a\in G$ define $-a=o\cdot(o\cdot oa)a$. This is the inverse of a:

$$\begin{aligned}
a+(-a) &\overset{(21)}{=} \{oa\cdot[o\cdot(o\cdot oa)a]o\}o \overset{(5)}{=} (oa\cdot o)\{[o\cdot(o\cdot oa)a]o\cdot o\}=\\
&\overset{(6)}{=} (oa\cdot o)\cdot(o\cdot oa)a \overset{(2)}{=} (oa)(o\cdot oa)\cdot oa \overset{(7)}{=} o.
\end{aligned}$$

□

Theorem 4.2. *The mappings $\varphi : x \mapsto ox$ and $\psi : x \mapsto xo$ are automorphisms of the group $(G, +)$ of Theorem* 4.1 *and satisfy the identity*

$$\psi(a) + \varphi(b) = ab. \tag{22}$$

Proof. The following shows that φ is an automorphism:

$$\begin{aligned} \varphi(a) + \varphi(b) &= oa + ob \overset{(21)}{=} (o \cdot oa)(ob \cdot o) \cdot o \overset{(3)}{=} (o \cdot oa)(o \cdot bo) \cdot o = \\ &\overset{(4)}{=} o(oa \cdot bo) \cdot o \overset{(3)}{=} o \cdot (oa \cdot bo)o \overset{(21)}{=} o(a+b) = \varphi(a+b). \end{aligned}$$

The proof that ψ is an automorphism is similar. Finally,

$$\begin{aligned} \psi(a) + \varphi(b) &= ao + ob \overset{(21)}{=} (o \cdot ao)(ob \cdot o) \cdot o \overset{(3)}{=} (o \cdot ao)(o \cdot bo) \cdot o = \\ &\overset{(4)}{=} o(ao \cdot bo) \cdot o \overset{(5)}{=} o(ab \cdot o) \cdot o \overset{(7)}{=} ab. \end{aligned}$$

□

Theorem 4.3. *Equations* (19) *and* (20) *are satisfied in the setting of the previous two theorems.*

Proof. As a special case of (22), we see that $\psi(x) + \varphi(x) = xx \overset{(1)}{=} x$, i.e. $\psi(x) = x - \varphi(x)$. Now equation (20) follows directly from (22):

$$ab = \psi(a) + \varphi(b) = a - \varphi(a) + \varphi(b) = a + \varphi(b - a).$$

To prove equation (19), note that

$$\psi^2(x) = \psi(x - \varphi(x)) = x - \varphi(x) - \varphi(x - \varphi(x)) = \varphi^2(x) - 2\varphi(x) + x.$$

Therefore, $\varphi^3(x) - 2\varphi^2(x) + \varphi(x) = \varphi(\psi^2(x)) = o(xo \cdot o) \overset{(8)}{=} x$. □

This is a direct proof of a G$_2$-version of Toyoda's representation theorem for medial quasigroups [6].

References

[1] **M.-J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse and J.-P. Schreiber**: *Pisot and Salem numbers*, Birkhäuser Verlag, Basel, 1992.

[2] **V. Havel and M. Sedlářová**: *Golden section quasigroups as special idempotent medial quasigroups*, Acta Univ. Palack. Olomuc. Fac. Rerum Natur. Math. **33** (1994), 43 – 50.

[3] **Z. Kolar-Begović and V. Volenec**: *GS-trapezoids in GS-quasigroups*, Math. Commun. **7** (2002), no. 2, 143 – 158.

[4] **Z. Kolar-Begović and V. Volenec**: *DGS-trapezoids in GS-quasigroups*, Math. Commun. **8** (2003), no. 2, 215 – 218.

[5] **V. Krčadinac**: *A new generalization of the golden ratio*, The Fibonacci Quarterly (to appear).

[6] **K. Toyoda**: *On axioms of linear functions*, Proc. Imp. Acad. Tokyo **17** (1941), 221 – 227.

[7] **V. Volenec**: *Geometry of medial quasigroups*, Rad Jugoslav. Akad. Znan. Umjet. **421** (1986), 79 – 91.

[8] **V. Volenec**: *GS-quasigroups*, Časopis Pěst. Mat. **115** (1990), no. 3, 307–318.

[9] **V. Volenec**: *Geometry of IM-quasigroups*, Rad Jugoslav. Akad. Znan. Umjet. **456** (1991), 139 – 146.

[10] **V. Volenec and Z. Kolar-Begović**: *Affine regular pentagons in GS-quasigroups*, Quasigroups Related Systems **12** (2004), 103 – 112.

Received October 5, 2005

Department of Mathematics
University of Zagreb
Bijenička 30
HR-10000 Zagreb
Croatia
e-mail: krcko@math.hr, volenec@math.hr

Quasigroups and Related Systems **13** (2005), 281 – 288

On medial-like identities

Mirko Polonijo

Abstract

The description of the quasigroups that satisfy the identities of the form $(a \cdot b) \cdot (c \cdot d) = (\pi(a) \cdot \pi(b)) \cdot (\pi(c) \cdot \pi(d))$, where π is a certain permutation on $\{a, b, c, d\}$, is given. Those quasigroups include internally medial ($ab \cdot cd = ac \cdot bd$), externally medial ($ab \cdot cd = db \cdot ca$) and palindromic ($ab \cdot cd = dc \cdot ba$) quasigroups. There are six identities that are the equivalents of commutativity, and fourteen identities are the equivalents of commutative mediality.

It is well-known that a groupoid $(Q, \cdot)$ is medial ([1]; entropic in [5]) if it satisfies

$$(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d) \tag{M}$$

i.e.

$$ab \cdot cd = ac \cdot bd \tag{M}$$

for all $a, b, c, d \in Q$. In the identity (M) we interchange the internal pair of the variables and now we could look for the identity in which the external pair is interchanged

$$ab \cdot cd = db \cdot ca \tag{M_e}$$

or the identity in which the both pairs are interchanged

$$ab \cdot cd = dc \cdot ba\,. \tag{P}$$

Therefore, we could call (M) *internal mediality* and (M_e) *external mediality* (paramediality in [2], [3]). The identity (P) we shall call *palindromity.*

Proposition 1. *For any groupoid $(Q, \cdot)$, any two of the three identities (M), (M_e) and (P) imply the third one.*

2000 Mathematics Subject Classification: 20N05
Keywords: Quasigroup, medial quasigroup, paramedial quasigroup.

Proof. $((M)\&(M_e) \Rightarrow (P))$ $\quad ab \cdot cd = ac \cdot bd = dc \cdot ba.$
$((P)\&(M_e) \Rightarrow (M))$ $\quad ab \cdot cd = dc \cdot ba = ac \cdot bd.$

$((P)\&(M) \Rightarrow (M_e))$ $\quad ab \cdot cd = dc \cdot ba = db \cdot ca.$ □

Proposition 2. *Let $(Q,\cdot)$ be a commutative groupoid. Then $(Q,\cdot)$ is palindromic. Further, the constraints (M) and (M_e) are equivalent, i.e. a commutative groupoid $(Q,\cdot)$ is internally medial if and only if it is externally medial.*

Proof. The first statement is obvious, and the second one follows from the previous proposition. □

Proposition 3. *Let $(Q,\cdot)$ be an idempotent groupoid. If it is externally medial or palindromic, then it is commutative.*

Proof. Any externally medial groupoid satisfies $xx \cdot yy = yx \cdot yx$, and for palindromic quasigroup $xx \cdot yy = yy \cdot xx$ is valid. Therefore, if the groupoid is idempotent, i.e. $xx = x$ holds for all $x \in Q$, it is commutative. □

Remark 1. There are idempotent internally medial groupoids (moreover quasigroups) which are not commutative. For instance, take Z_3 and define multiplication by $x \cdot y = x + 2y$.

Proposition 4. *Let $(Q,\cdot)$ be an internally medial or externally medial or palindromic quasigroup. Its center is empty or Q.*

Proof. The center is the set of all $c \in Q$ which commutes with all elements of Q. Therefore, if the center is not empty and c is in the center, then any $a, b \in Q$ can be written in the form $a = cx = xc$, $b = cy = yc$ for some $x, y \in Q$. Then (M) implies $ab = cx \cdot yc = cy \cdot xc = ba$, (M_e) implies $ab = xc \cdot cy = yc \cdot cx = ba$, (P) implies $ab = cx \cdot yc = cy \cdot xc = ba$, i.e. in any case $(Q,\cdot)$ is commutative. □

Proposition 5. *A loop is internally medial or externally medial if and only if it is an abelian group.*

Proof. $(\Rightarrow)$ If $(Q,\cdot)$ is internally medial or externally medial loop it is commutative, since a loop has nonempty center. Now, put the unit element for b and associativity follows. Sufficiency $(\Leftarrow)$ is obvious. □

Proposition 6. *A loop is palindromic if and only if it is commutative.*

Proof. Notice that a loop has nonempty center. □

Corollary 1. *A group is internally medial or externally medial or palindromic if and only if it is an abelian group.*

Remark 2. As we know, every commutative quasigroup (groupoid) is palindromic, but the converse is not true. If we take an abelian group $(Q,+)$, then quasigroup $(Q,-)$ satisfies (P), but is not commutative. Notice that $(Q,-)$ is internally medial and externally medial.

Proposition 7. *A quasigroup $(Q,\cdot)$ is palindromic if and only if exists its automorphism α such that*

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

holds for all $x,y\in Q$.

Proof. $(\Rightarrow)$ For arbitrary $a,b\in Q$ put $ab=u, ba=v$ and take permutation $\alpha=L_v^{-1}R_u$ (where L_v is left translation for v and R_u is right translation for u i.e. $L_v(x)=v\cdot x$ and $R_u(x)=x\cdot u$, for any $x\in Q$).

Then we have $L_v\alpha(xy)=R_u(xy)=xy\cdot ab=ba\cdot yx=L_v(yx)$ and therefore $\alpha(xy)=yx$. Further, for any $x,y\in Q$ taking $x=x_1x_2, y=y_1y_2$ we have $\alpha(xy)=yx=y_1y_2\cdot x_1x_2=x_2x_1\cdot y_2y_1=\alpha(x_1x_2)\cdot\alpha(y_1y_2)=\alpha(x)\cdot\alpha(y)$ i.e. α is an automorphism.

$(\Leftarrow)$ If α is an automorphism such that $\alpha(x\cdot y)=y\cdot x$ then follows $ab\cdot cd=\alpha(cd\cdot ab)=\alpha(cd)\cdot\alpha(ab)=dc\cdot ba$ i.e. quasigroup is palindromic. □

Proposition 8. *If $(Q,\cdot)$ is internally or externally medial quasigroup, then it satisfies Thomsen's closure condition, i.e.*

$$x_1y_2=x_2y_1 \ \text{ and } \ x_1y_3=x_3y_1 \ \text{ imply } \ x_2y_3=x_3y_2$$

for all $x_1,x_2,x_3,y_1,y_2,y_3\in Q$. Therefore, any internally and any externally medial quasigroup is an abelian group isotope.

Proof. Let us suppose $x_1y_2=x_2y_1$ and $x_1y_3=x_3y_1$ hold and take $z\in Q$. Now, for internally medial quasigroup we get

$$x_2y_3\cdot y_1z=x_2y_1\cdot y_3z=x_1y_2\cdot y_3z=x_1y_3\cdot y_2z=x_3y_1\cdot y_2z=x_3y_2\cdot y_1z$$

and for externally medial quasigroup we have

$$x_2y_3 \cdot zx_1 = x_1y_3 \cdot zx_2 = x_3y_1 \cdot zx_2 = x_2y_1 \cdot zx_3 = x_1y_2 \cdot zx_3 = x_3y_2 \cdot zx_1.$$

Hence, in both cases, $x_2y_3 = x_3y_2$.

Since Thomsen's closure condition is valid in $(Q, \cdot)$ it follows that $(Q, \cdot)$ is isotopic to an abelian group (cf. [1], [5]). □

Proposition 9. *For a quasigroup $(Q, \cdot)$ and $e, f \in Q$ let us define binary operation $+$ on Q by*

$$xe \ + \ fy = xy$$

for all $x, y \in Q$. If $(Q, \cdot)$ is internally or externally medial quasigroup, then $(Q, +)$ is an abelian group.

Proof. It is well-known (and easy to check) that $(Q, +)$ is a loop (with the unity $0 = fe$). If $(Q, \cdot)$ is internally or externally medial quasigroup then it is isotopic to an abelian group and therefore loop $(Q, +)$ is an abelian group isotope too. Because of Albert's theorem (cf. [1]), $(Q, +)$ is an abelian group. □

Proposition 10. ([6], [4]) *Let $(Q, \cdot)$ be internally or externally medial quasigroup. Then there is an abelian group $(Q, +)$, an element $q \in Q$ and group automorphisms α, β such that*

$$x \cdot y = \alpha(x) + \beta(y) + q$$

for all $x, y \in Q$. For internally medial quasigroup $\alpha\beta = \beta\alpha$ is fulfilled, and for externally medial quasigroup $\alpha\alpha = \beta\beta$.

Proof. Let $(Q, +)$ be the abelian group defined in the previous proposition and $\varphi(x) = R_e(x) = xe$, $\psi(x) = L_f(x) = fx$ for all $x \in Q$. For internally medial quasigroup and externally medial quasigroup we get respectively

$$\varphi(\varphi(a) + \psi(b)) + \psi(\varphi(c) + \psi(d)) = \varphi(\varphi(a) + \psi(c)) + \psi(\varphi(b) + \psi(d)),$$

$$\varphi(\varphi(a) + \psi(b)) + \psi(\varphi(c) + \psi(d)) = \varphi(\varphi(d) + \psi(b)) + \psi(\varphi(c) + \psi(a)).$$

The first equality implies

$$\varphi(a + b) + \psi(\varphi(0) + \psi(0)) = \varphi(a + \psi(0)) + \psi(\varphi\psi^{-1}(b) + \psi(0)),$$

$$\varphi(\varphi(0) + \psi(0)) + \psi(c + d) = \varphi(\varphi(0) + \psi\varphi^{-1}(c)) + \psi(\varphi(0) + d),$$

and the second one gives

$$\varphi(a+b)+\psi(\varphi(0)+\psi(0))=\varphi(\varphi(0)+b)+\psi(\varphi(0)+\psi\varphi^{-1}(a)),$$

$$\varphi(\varphi(0)+\psi(0))+\psi(c+d)=\varphi(\varphi\psi^{-1}(d)+\psi(0))+\psi(c+\psi(0)).$$

In both cases it follows that there are such permutations $\varphi_1,\varphi_2,\psi_1,\psi_2$ on Q for which

$$\varphi(a+b)=\varphi_1(a)+\varphi_2(b),\quad \psi(c+d)=\psi_1(c)+\psi_2(d).$$

Hence, φ and ψ are quasi-automorphisms of the abelian group $(Q,+)$. It implies that there are automorphisms α,β of $(Q,+)$ and $q_1,q_2\in Q$ such that

$$\varphi(x)=\alpha(x)+q_1,\quad \psi(x)=\beta(x)+q_2\,.$$

Therefore, putting $q=q_1+q_2$ we have

$$x\cdot y=\alpha(x)+\beta(y)+q\,.$$

Now, for internally medial quasigroup we get

$$\alpha(\alpha(a)+\beta(b))+\beta(\alpha(c)+\beta(d))=\alpha(\alpha(a)+\beta(c))+\beta(\alpha(b)+\beta(d))$$

and putting $a=c=d=0$ we obtain $\alpha\beta=\beta\alpha$.

For externally medial quasigroup we have

$$\alpha(\alpha(a)+\beta(c))+\beta(\alpha(b)+\beta(d))=\alpha(\alpha(d)+\beta(c))+\beta(\alpha(b)+\beta(a))$$

and putting $b=c=d=0$ it follows $\alpha\alpha=\beta\beta$. □

Remark 3. It is widely known that K. Toyoda (cf. [6]) proved the previously mentioned proposition for internally medial quasigroups, which is commonly named Toyoda's theorem (see also [1], [5]). The proposition was proved in [4] for externally medial quasigroups (see also [2], [3]). We gave the above proof to stress that it is the same for both types of quasigroups, as is expected.

Any of the identities (M), (M_e), (P) is of the form

$$ab\cdot cd=(\pi(a)\cdot\pi(b))\cdot(\pi(c)\cdot\pi(d))$$

where π is a certain permutation on $\{a,b,c,d\}$. Therefore we would like to look on such identities on the quasigroups for any permutation π. Beside the identities $(M), (M_e), (P)$ and trivial identity $ab \cdot cd = ab \cdot cd$ which is fulfilled in any groupoid, we have the following twenty "medial-like" identities more:

$$ab \cdot cd = ab \cdot dc \quad (C_1), \qquad ab \cdot cd = ba \cdot cd \quad (C_2),$$

$$ab \cdot cd = ba \cdot dc \quad (C_3), \qquad ab \cdot cd = cd \cdot ab \quad (C_4),$$

$$ab \cdot cd = cd \cdot ba \quad (C_5), \qquad ab \cdot cd = dc \cdot ab \quad (C_6),$$

$$ab \cdot cd = ac \cdot db \quad (CM_1), \qquad ab \cdot cd = ad \cdot bc \quad (CM_2),$$

$$ab \cdot cd = ad \cdot cb \quad (CM_3), \qquad ab \cdot cd = bc \cdot ad \quad (CM_4),$$

$$ab \cdot cd = bc \cdot da \quad (CM_5), \qquad ab \cdot cd = bd \cdot ac \quad (CM_6),$$

$$ab \cdot cd = bd \cdot ca \quad (CM_7), \qquad ab \cdot cd = ca \cdot bd \quad (CM_8),$$

$$ab \cdot cd = ca \cdot db \quad (CM_9), \qquad ab \cdot cd = cb \cdot ad \quad (CM_{10}),$$

$$ab \cdot cd = cb \cdot da \quad (CM_{11}), \qquad ab \cdot cd = da \cdot bc \quad (CM_{12}),$$

$$ab \cdot cd = da \cdot cb \quad (CM_{13}), \qquad ab \cdot cd = db \cdot ac \quad (CM_{14}).$$

Proposition 11. *For a quasigroup $(Q, \cdot)$ and $i \in \{1, 2, \ldots, 6\}$, (C_i) is valid if and only if the quasigroup is commutative.*

Proof. $(\Leftarrow)$ is obvious. $(\Rightarrow)$ is evident for $(C_1), (C_2), (C_4)$. For (C_3) put $c = d$; for (C_5) put $c = b,\ d = a$; for (C_6) put $c = a,\ d = b$. □

Proposition 12. *For a quasigroup $(Q, \cdot)$ and $i \in \{1, 2, \ldots, 14\}$, (CM_i) holds if and only if the quasigroup is both commutative and internally medial.*

Proof. $((CM_1), \Leftarrow)$ is obvious.

$((CM_1), \Rightarrow)$ Put $c = b$ and commutativity follows; hence (M).

$((CM_2), \Leftarrow)$ $ab \cdot cd = ba \cdot cd = bc \cdot ad = ad \cdot bc.$

$((CM_2), \Rightarrow)$ Put $d = b$ and commutativity follows; therefore $ab \cdot cd = ba \cdot cd = bd \cdot ac = ac \cdot bd.$

$((CM_3), \Leftarrow)$ Commutative internally medial quasigroup satisfies (CM_2), hence (CM_3) follows.

$((CM_3), \Rightarrow)$ Put $c = a$ and commutativity follows; hence (CM_2) and therefore (M).

$((CM_4), \Leftarrow)$ Commutative internally medial quasigroup satisfies (CM_2), hence (CM_4) follows.

$((CM_4), \Rightarrow)$ Put $c = a$ and commutativity follows; hence (CM_2) and therefore (M).

$((CM_5), \Leftarrow)$ Commutative internally medial quasigroup satisfies (CM_2), hence (CM_5) follows.

$((CM_5), \Rightarrow)$ Because of $ab \cdot cd = bc \cdot da = cd \cdot ab$ commutativity follows; hence (CM_2) and therefore (M).

$((CM_6), \Leftarrow)$ is obvious.

$((CM_6), \Rightarrow)$ Put $c = b$ and commutativity follows; hence (M).

$((CM_7), \Leftarrow)$ is obvious.

$((CM_7), \Rightarrow)$ Put $d = a$ and commutativity follows; hence (M).

$((CM_8), \Leftarrow)$ is obvious.

$((CM_8), \Rightarrow)$ Put $c = b$ and commutativity follows; hence (M).

$((CM_9), \Leftarrow)$ is obvious.

$((CM_9), \Rightarrow)$ Put $d = a$ and commutativity follows; hence (M).

$((CM_{10}), \Leftarrow)$ Commutative internally medial quasigroup satisfies (CM_2), hence (CM_{10}) follows.

$((CM_{10}), \Rightarrow)$ Put $d = b$ and commutativity follows; hence (CM_2) and therefore (M).

$((CM_{11}), \Leftarrow)$ Commutative internally medial quasigroup satisfies (CM_2), hence (CM_{11}) follows.

$((CM_{11}), \Rightarrow)$ Put $c = a$ and commutativity follows; hence (CM_2) and therefore (M).

$((CM_{12}), \Leftarrow)$ Commutative internally medial quasigroup satisfies (CM_2), hence (CM_{12}) follows.

$((CM_{12}), \Rightarrow)$ Because of $ab \cdot cd = da \cdot bc = cd \cdot ab$ commutativity follows; hence (CM_2) and therefore (M).

$((CM_{13}), \Leftarrow)$ Commutative internally medial quasigroup satisfies (CM_2), hence (CM_{13}) follows.

$((CM_{13}), \Rightarrow)$ Put $d = b$ and commutativity follows; hence (CM_2) and therefore (M).

$((CM_{14}), \Leftarrow)$ is obvious.

$((CM_{14}), \Rightarrow)$ Put $d = a$ and commutativity follows; hence (M). □

Corollary 2. *For a quasigroup* $(Q, \cdot)$ *and* $i \in \{1, 2, \ldots, 14\}$, (CM_i) *is valid if and only if the quasigroup is both commutative and externally medial.*

Corollary 3. ([3]) *If* (CM_i) *is fulfilled in a quasigroup* $(Q, \cdot)$ *for some* $i \in \{1, 2, \ldots, 14\}$, *i.e. if* $(Q, \cdot)$ *is internally or externally medial quasigroup which is commutative, then there is an abelian group* $(Q, +)$, *an element* $q \in Q$ *and group automorphisms* α *such that*

$$x \cdot y = \alpha(x + y) + q$$

is valid for all $x, y \in Q$. □

References

[1] **V. D. Belousov**: *Osnovy teorii kvazigrupp i lup*, (Russian), Nauka, Moskva, 1967.

[2] **J. R. Cho, J. Ježek, T. Kepka**: *Paramedial groupoids*, Czechoslovak. Math. J. **49** (1999), 277 – 290.

[3] **W. Förg, A. Krapež**: *Equations which preserve the height of variables*, Aequationes Math, to appear.

[4] **P. Nemec, T. Kepka**: *T-quasigroups, Part I*, Acta Univ. Carol. Math. Phys. **12** (1971), 39 – 49.

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

[6] **K. Toyoda**: *On axioms of linear functions*, Proc. Imp. Acad. Jap. **17** (1941), 221 – 227.

Received March 13, 2005

University of Zagreb
Department of Mathematics
Bijenička c. 30
10000 Zagreb
Croatia