# New fuzzy subquasigroups

*Muhammad Akram* and *Wieslaw A. Dudek*

**Abstract.** In this paper we introduce new generalized fuzzy subquasigroups and study some of their important properties. We characterize these generalized subquasigroups by their level subsets. Some characterization of the generalized fuzzy subquasigroups are also established.

## 1. Introduction

During the last decade, there have been many applications of quasigroups in different areas, such as cryptography, modern physics [9], coding theory, cryptology and geometry. In 1965, Zadeh [13] introduced the notion of a fuzzy subset of a set as a method for representing uncertainty. Since then it has become a vigorous area of research in different mathematical domains. Rosenfeld inspired the fuzzification of algebraic structures and introduced the notion of fuzzy subgroups. Das [4] characterized fuzzy subgroups by their level subgroups. Murali [8] proposed a definition of a fuzzy point belonging to a fuzzy subset under a natural equivalence on a fuzzy set. The idea of quasi-coincidence of a fuzzy point with a fuzzy set, which is mentioned in [10] played a vital role to generate some different types of fuzzy subgroups. A new type of fuzzy subgroups, $(\in, \in \vee q)$-fuzzy subgroups, was introduced in earlier paper Bhakat and Das [3] by using the combined notions of *belongines* and *quasi-coincidence* of fuzzy point and fuzzy set. In fact, $(\in, \in \vee q)$-fuzzy subgroup is an important and useful generalization of Rosenfeld's fuzzy subgroup. On the other hand, Akram and Dudek applied this concept to subquasigroup in [2] and studied some of its properties. In this paper using general form of the concept of quasi-coincidence of a fuzzy point with a fuzzy subset, the notion of an $(\in, \in \vee\, q_m)-$ fuzzy subquasigroup is introduced and some of its important properties are investigated. We characterize these generalized subquasigroups by their level subsets.

2000 Mathematics Subject Classification: 20N15, 94D05
Keywords: Quasigroup, $(\in, \in \vee q_m)$-fuzzy subquasigroup.

Some characterization of the generalized fuzzy subquasigroups are established. Some recent results obtained by Akram-Dudek [2] are extended and strengthened.

## 2. Preliminaries

A groupoid $(G,\cdot)$ is called a *quasigroup* if for any $a$ , $b \in G$ each of the equations $a\cdot x = b$, $x\cdot a = b$ has a unique solution in $G$. A quasigroup may be also defined as an algebra $(G,\cdot,\backslash,/)$ with three binary operations $\cdot$, $\backslash$, $/$ satisfying the following identities:

$$(x\cdot y)/y = x, \qquad x\backslash(x\cdot y) = y,$$

$$(x/y)\cdot y = x, \qquad x\cdot(x\backslash y) = y.$$

Such defined quasigroup is called an *equasigroup*.

A nonempty subset $S$ of a quasigroup $\mathcal{G} = (G,\cdot,\backslash,/)$ is called a *subquasigroup* if it is closed with respect to these three operations.

In this paper $\mathcal{G}$ always denotes an equasigroup $(G,\cdot,\backslash,/)$; $G$ always denotes a nonempty set.

A mapping $\mu : G \to [0,1]$ is called a *fuzzy set* in $G$. For any fuzzy set $\mu$ in $G$ and any $t\in[0,1]$, we define the set

$$U(\mu;t) = \{x\in G \mid \mu(x)\geqslant t\},$$

which is called the *upper $t$-level* of $\mu$.

**Definition 2.1.** A fuzzy set $\mu$ in a set $G$ of the form

$$\mu(y) = \begin{cases} t\in(0,1] & \text{for } y = x,\\ 0 & \text{for } y\neq x,\end{cases}$$

is said to be a *fuzzy point* with support $x$ and value $t$ and is denoted by $x_t$.

We say that a fuzzy point $x_t$ *belong to* a fuzzy set $\mu$ and write $x_t\in\mu$, if $\mu(x)\geqslant t$. A fuzzy point $x_t$ is *quasicoincident* with a fuzzy set $\mu$, if $\mu(x)+t>1$. In this case we write $x_tq\mu$.

- $x_t\in\vee q\mu$ means that $x_t\in\mu$ or $x_tq\mu$,
- $x_t\in\wedge q\mu$ means that $x_t\in\mu$ and $x_tq\mu$.

**Definition 2.2.** A fuzzy set $\mu$ in $G$ is called an $(\in, \in\vee q)$-*fuzzy subquasigroup* of $\mathcal{G}$, if it satisfies the following condition:

$$x_{t_1}, y_{t_2} \in \mu \Longrightarrow (x * y)_{\min\{t_1,t_2\}} \in \vee q\mu$$

for all $x, y \in G,\ \ t_1, t_2 \in (0, 1]$ and $* \in \{\cdot, \backslash, /\}$.

## 3. New fuzzy subquasigroups

Let $m$ be an element of [0, 1) unless otherwise specified. By $x_t q_m \mu$, we mean $\mu(x) + t + m > 1,\ \ t \in (0, \frac{1-m}{2}]$. The notation $x_t \in \vee q_m\mu$ means that $x_t \in \mu$ or $x_t q_m \mu$.

**Definition 3.1.** A fuzzy set $\mu$ in $G$ is called an $(\in, \in\vee q_m)$-*fuzzy subquasigroup* of $\mathcal{G}$, if

$$x_{t_1}, y_{t_2} \in \mu \Longrightarrow (x * y)_{\min\{t_1,t_2\}} \in \vee q_m\mu$$

for all $x, y \in G$, $t_1, t_2 \in (0, 1]$ and $* \in \{\cdot, \backslash, /\}$.

We note that different types of fuzzy subquasigroups can be constructed for different values of $m \in [0, 1)$. Hence an $(\in, \in\vee q_m)$-fuzzy subquasigroup with $m = 0$ is called an $(\in, \in\vee q)$-fuzzy subquasigroup.

**Example 3.2.** Let $G = \{0, a, b, c\}$ be a quasigroup with the following multiplication table:

| $\cdot$ | 0 | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| 0 | 0 | $a$ | $b$ | $c$ |
| $a$ | $a$ | 0 | $c$ | $b$ |
| $b$ | $b$ | $c$ | 0 | $a$ |
| $c$ | $c$ | $b$ | $a$ | 0 |

$(i)$ Consider a fuzzy set $\mu$ defined by

$$\mu(x) = \begin{cases} 0.7 & \text{if } \ x = 0, \\ 0.8 & \text{if } \ x = a, \\ 0.4 & \text{if } \ x = b, \\ 0.4 & \text{if } \ x = c. \end{cases}$$

If $m = 0.2$, then $U(\mu; t) = G$ for all $t \in (0, 0.4]$. Hence $\mu$ is an $(\in, \in \vee q_{0.2})$–fuzzy subquasigroup of $\mathcal{G}$.

$(ii)$ Now consider a fuzzy set

$$\mu(x)=\begin{cases}0.45 & \text{if } \ x=0,\\ 0.41 & \text{if } \ x=a,\\ 0.41 & \text{if } \ x=c,\\ 0.49 & \text{if } \ x=b.\end{cases}$$

In this case for $m=0.04$ we have

$$U(\mu;t)=\begin{cases}G & \text{if } \ t\in(0,0.4],\\ \{0,b\} & \text{if } \ t\in(0.4,0.45],\\ \{b\} & \text{if } \ t\in(0.45,0.48].\end{cases}$$

Since $\{b\}$ is not a subquasigroup of $\mathcal{G}$, so $U(\mu;t)$ is not a subquasigroup for $t\in(0.45,0.48]$. Hence $\mu$ is not an $(\in,\in\vee q_{0.04})$-fuzzy subquasigroup of a quasigroup $\mathcal{G}$. □

**Proposition 3.3.** *Every $(\in,\in)$-fuzzy subquasigroup is an $(\in,\in\vee q_m)$-fuzzy subquasigroup.*

*Proof.* Straightforward. □

The converse statement may not be true.

**Example 3.4.** Consider the $(\in,\in\vee q_{0.2})$-fuzzy subquasigroup of $\mathcal{G}$ defined in Example 3.2. Then $\mu$ is not an $(\in,\in)$-fuzzy subquasigroup of $\mathcal{G}$ since $a_{0.71}\in\mu$ and $a_{0.75}\in\mu$, but $(a*a)_{\min\{0.71,0.75\}}=0_{0.71}\overline{\in}\mu$. □

**Theorem 3.5.** *A fuzzy set $\mu$ in $\mathcal{G}$ is an $(\in,\in\vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$ if and only if*

$$\mu(x*y)\geqslant\min\Big\{\mu(x),\mu(y),\frac{1-m}{2}\Big\} \tag{1}$$

*holds for all $x$, $y\in G$.*

*Proof.* Let $\mu$ be an $(\in,\in\vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$. Assume that (1) is not valid. Then there exist $x'$, $y'\in G$ such that

$$\mu(x'*y')<\min\Big\{\mu(x'),\mu(y'),\frac{1-m}{2}\Big\}.$$

If $\min(\mu(x'), \mu(y')) < \frac{1-m}{2}$, then $\mu(x' * y') < \min(\mu(x'), \mu(y'))$. Thus

$$\mu(x' * y') < t \leqslant \min\{\mu(x'), \mu(y')\} \qquad \text{for some } t \in (0, 1].$$

It follows that $x'_t \in \mu$ and $y'_t \in \mu$, but $(x' * y')_t \overline{\in} \mu$, a contradiction. Moreover, $\mu(x' * y') + t < 2t < 1 - m$, and so $(x' * y')_t \overline{q_m} \mu$. Hence, consequently $(x' * y')_t \overline{\in \vee q_m} \mu$, a contradiction.

On the other hand, if $\min\{\mu(x'), \mu(y')\} \geqslant \frac{1-m}{2}$, then $\mu(x') \geqslant \frac{1-m}{2}$, $\mu(y') \geqslant \frac{1-m}{2}$ and $\mu(x' * y') < \frac{1-m}{2}$. Thus $x'_{\frac{1-m}{2}} \in \mu$ and $y'_{\frac{1-m}{2}} \in \mu$, but $(x' * y')_{\frac{1-m}{2}} \overline{\in} \mu$. Also

$$\mu(x' * y') + \frac{1-m}{2} < \frac{1-m}{2} + \frac{1-m}{2} = 1 - m,$$

i.e., $(x' * y')_{\frac{1-m}{2}} \overline{q_m} \mu$. Hence $(x' * y')_{\frac{1-m}{2}} \overline{\in \vee q_m} \mu$, a contradiction. So (1) is valid.

Conversely, assume that $\mu$ satisfies (1). Let $x$, $y \in G$ and $t_1$, $t_2 \in (0, 1]$ be such that $x_{t_1}\mu$ and $y_{t_2} \in \mu$. Then

$$\mu(x * y) \geqslant \min\left\{\mu(x), \mu(y), \frac{1-m}{2}\right\} \geqslant \min\left\{t_1, t_2, \frac{1-m}{2}\right\}.$$

Assume that $t_1 \leqslant \frac{1-m}{2}$ or $t_2 \leqslant \frac{1-m}{2}$. Then $\mu(x * y) \geqslant \min\{t_1, t_2\}$, which implies that $(x * y)_{\min\{t_1, t_2\}} \in \mu$. Now suppose that $t_1 > \frac{1-m}{2}$ and $t_2 > \frac{1-m}{2}$. Then $\mu(x * y) \geqslant \frac{1-m}{2}$, and thus

$$\mu(x * y) + \min\{t_1, t_2\} > \frac{1-m}{2} + \frac{1-m}{2} = 1 - m,$$

i.e., $(x * y)_{\min\{t_1, t_2\}} q_m \mu$. Hence $(x * y)_{\min\{t_1, t_2\}} \in \vee q_m \mu$, and consequently, $\mu$ is an $(\in, \in\!\vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$. □

**Theorem 3.6.** *A fuzzy set $\mu$ of $G$ is an $(\in, \in\!\vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$ if and only if each nonempty level set $U(\mu; t)$, $t \in (0, \frac{1-m}{2}]$, is a subquasigroup of $\mathcal{G}$.*

*Proof.* Assume that a fuzzy set $\mu$ is an $(\in, \in \vee q)$-fuzzy subquasigroup of $\mathcal{G}$. Let $t \in (0, \frac{1-m}{2}]$ and $x, y \in U(\mu; t)$. Then $\mu(x) \geqslant t$ and $\mu(y) \geqslant t$. It follows from (1) that

$$\mu(x * y) \geqslant \min\left\{\mu(x), \mu(y), \frac{1-m}{2}\right\} \geqslant \min\left\{t, \frac{1-m}{2}\right\} = t,$$

so that $x * y \in U(\mu;t)$. Hence $U(\mu;t)$ is an $(\in, \in \vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$.

Conversely, suppose that the nonempty set $U(\mu;t)$ is a subquasigroup of $\mathcal{G}$ for all $t \in (0, \frac{1-m}{2}]$. If the condition (1) is not true, then there exists $a$, $b \in G$ such that $\mu(a * b) < \min\{\mu(a), \mu(b), \frac{1-m}{2}\}$. Hence we can take $t \in (0,1]$ such that $\mu(a * b) < t_1 < \min\{\mu(a), \mu(b), \frac{1-m}{2}\}$. Then $t \in (0, \frac{1-m}{2}]$ and $a, b \in U(\mu;t)$. Since $U(\mu;t)$ is a subquasigroup of $\mathcal{G}$, it follows that $a * b \in U(\mu;t)$, so $\mu(a * b) \geqslant t$. This is a contradiction. Therefore the condition (1) is valid, and so $\mu$ is an $(\in, \in \vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$. □

**Theorem 3.7.** *Let $\mu$ be a fuzzy set of a quasigroup $\mathcal{G}$. Then the nonempty level set $U(\mu;t)$ is a subquasigroup of $\mathcal{G}$ for all $t \in (\frac{1-m}{2}, 1]$ if and only if*

$$\max\left\{\mu(x * y), \frac{1-m}{2}\right\} \geqslant \min\{\mu(x), \mu(y)\}$$

*for all $x, y \in G$.*

*Proof.* Suppose that $U(\mu;t) \neq \emptyset$ is a subquasigroup of $\mathcal{G}$. Assume that $\max\{\mu(x * y), \frac{1-m}{2}\} < \min\{\mu(x), \mu(y)\} = t$ for some $x$, $y \in G$, then $t \in (\frac{1-m}{2}, 1]$, $\mu(x * y) < t$, $x \in U(\mu;t)$ and $y \in U(\mu;t)$. Since $x$, $y \in U(\mu;t)$, $U(\mu;t)$ is a subquasigroup of $\mathcal{G}$, so $x * y \in U(\mu;t)$, a contradiction.

The proof of the second part of Theorem is straightforward. □

**Theorem 3.8.** *Let $\mu$ be an $(\in, \in \vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$. If it satisfies $\mu(x) < \frac{1-m}{2}$ for all $x \in G$, then it is a fuzzy subquasigroup of $\mathcal{G}$.*

*Proof.* Let $x, y \in G$ and $t_1, t_2 \in (0,1]$ be such that $x_{t_1} \in \mu$ and $y_{t_2} \in \mu$. Then $\mu(x) \geqslant t_1$ and $\mu(y) \geqslant t_2$. It follows from Theorem 3.5 that

$$\mu(x * y) \geqslant \min\left\{\mu(x), \mu(y), \frac{1-m}{2}\right\} = \min\{\mu(x), \mu(y)\} = \min\{t_1, t_2\},$$

so $(x * y)_{\min\{t_1, t_2\}} \in \mu$. Hence $\mu$ is a fuzzy subquasigroup of $\mathcal{G}$. □

**Theorem 3.9.** *If $0 \leqslant m < n < 1$, then each $(\in, \in\vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$ is an $(\in, \in\vee q_n)$-fuzzy subquasigroup of $\mathcal{G}$.*

*Proof.* Let $\mu$ be an $(\in, \in \vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$ and let $x$,$y \in G$. Then

$$\mu(x * y) \geqslant \min\left\{\mu(x), \mu(y), \frac{1-m}{2}\right\} \geqslant \min\left\{\mu(x), \mu(y), \frac{1-n}{2}\right\}.$$

Thus from Theorem 3.5, it follows that $\mu$ is an $(\in, \in\!\vee q_n)$-fuzzy subquasigroup of $\mathcal{G}$. □

Note that an $(\in, \in\!\vee q_n)$-fuzzy subquasigroup may not be an $(\in, \in\!\vee q_m)$-fuzzy subquasigroup for $0 \leqslant m < n < 1$.

**Example 3.10.** Let $G = \{0, a, b, c\}$ be a quasigroup defined in Example 3.2. Consider a fuzzy set

$$\mu(x) = \begin{cases} 0.42 & \text{if } \ x = 0, \\ 0.4 & \text{if } \ x = a, \\ 0.4 & \text{if } \ x = c, \\ 0.48 & \text{if } \ x = b. \end{cases}$$

If $n = 0.16$, then

$$U(\mu; t) = \begin{cases} G & \text{for } \ t \in (0, 0.4], \\ \{0, b\} & \text{for } \ t \in (0.4, 0.42]. \end{cases}$$

Since $G$ and $\{0, b\}$ are subquasigroups of $\mathcal{G}$, so $U(\mu; t)$ is a subquasigroup for $t \in (0.4, 0.42]$. Hence $\mu$ is an $(\in, \in\!\vee q_{0.16})$-fuzzy subquasigroup of $\mathcal{G}$.

If $m = 0.04$, then

$$U(\mu; t) = \begin{cases} G & \text{for } \ t \in (0, 0.4], \\ \{b\} & \text{for } \ t \in (0.4, 0.48]. \end{cases}$$

Since $\{b\}$ is not a subquasigroup of $\mathcal{G}$, so $U(\mu; t)$ is not a subquasigroup for $t \in (0.4, 0.48]$. Hence $\mu$ is not an $(\in, \in\!\vee q_{0.04})$-fuzzy subquasigroup of $\mathcal{G}$. □

**Theorem 3.11.** *A nonempty subset $M$ of $G$ is a subquasigroup of $\mathcal{G}$ if and only if its characteristic function is an $(\in, \in\!\vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$.*

*Proof.* Let $M$ be a subquasigroup of $\mathcal{G}$. Then $\chi_{_M}(x) = 1$ for $x \in M$ and $\chi_{_M}(x) = 0$ for $x \notin M$. Thus $U(\mu_M; t) = M$ for all $t \in (0, \frac{1-m}{2}]$. Hence, by Theorem 3.6, $\chi_{_M}$ is an $(\in, \in\vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$.

Conversely, suppose that $\mu_M$ is an $(\in, \in\!\vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$. Then

$$\mu(x * y) \geqslant \min\Big\{\chi_{_M}(x), \chi_{_M}(y), \frac{1-m}{2}\Big\} = \min\Big\{1, \frac{1-m}{2}\Big\} = \frac{1-m}{2}$$

for $x, y \in G$. Since $m \in [0, 1)$, it follows that $\chi_{_M}(x * y) = 1$, so $x * y \in M$. Hence $M$ is a subquasigroup of $\mathcal{G}$. □

**Corollary 3.12.** *For every subquasigroup $M$ of $\mathcal{G}$ and every $t \in (0, \frac{1-m}{2}]$ there exists an $(\in, \in\vee q_m)$-fuzzy subquasigroup $\mu$ of $\mathcal{G}$ such that $U(\mu;t) = M$.*

*Proof.* Indeed, $\chi_M$ is this $(\in, \in\vee q_m)$-fuzzy subquasigroup. □

**Theorem 3.13.** *The intersection of any family of $(\in, \in\vee q_m)$-fuzzy subquasigroups of $\mathcal{G}$ is an $(\in, \in\vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$.*

*Proof.* Let $\mu = \bigcap_{i\in\Lambda} \mu_i$ for some $(\in, \in\vee q_m)$-fuzzy subquasigroups $\mu_i$ of $\mathcal{G}$. Then

$$\begin{aligned} \mu(x*y) &= \sup_{i\in\Lambda} \mu_i(x*y) \geqslant \sup_{i\in\Lambda} \min\{\mu_i(x), \mu_i(y), \tfrac{1-m}{2}\} \\ &= \min\{\sup_{i\in\Lambda} \mu_i(x), \sup_{i\in\Lambda} \mu_i(y), \tfrac{1-m}{2}\} \\ &= \min\{\textstyle\bigcap_{i\in\Lambda} \mu_i(x), \bigcap_{i\in\Lambda} \mu_i(y), \tfrac{1-m}{2}\} = \min\{\mu(x), \mu(y), \tfrac{1-m}{2}\}. \end{aligned}$$

Hence, by Theorem 3.5, $\mu$ is an $(\in, \in\vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$. □

The union of two $(\in, \in\vee q_m)$-fuzzy subquasigroups of $\mathcal{G}$ is not an $(\in, \in\vee q_m)$-fuzzy subquasigroup, in general.

**Example 3.14.** Let $\mathcal{G}$ be as in Example 3.2. Consider two fuzzy sets:

$$\mu(x) = \begin{cases} 0.6 & \text{if } x = 0, \\ 0.7 & \text{if } x = a, \\ 0.3 & \text{if } x = b, \\ 0.3 & \text{if } x = c, \end{cases} \quad \text{and} \quad \nu(x) = \begin{cases} 0.4 & \text{if } x = 0, \\ 0.5 & \text{if } x = b, \\ 0.3 & \text{if } x = a, \\ 0.3 & \text{if } x = c. \end{cases}$$

For $m = 0.2$ we have

$$U(\mu;t) = \begin{cases} G & \text{if } t \in (0, 0.3], \\ \{0, a\} & \text{if } t \in (0.4, 0.4], \end{cases} \qquad U(\nu;t) = \begin{cases} G & \text{if t } \in (0,\ 0.3], \\ \{0, b\} & \text{if t } \in (0.3,\ 0.4]. \end{cases}$$

Since $G$, $\{0, a\}$ and $\{0, b\}$ are subquasigroups of $\mathcal{G}$, $\mu$ and $\nu$ are $(\in, \in\vee q_{0.2})$-fuzzy subquasigroups by Theorem 3.6.

The union $\mu \cup \nu$ has the form

$$(\mu \cup \nu)(x) = \begin{cases} 0.6 & \text{if } x = 0, \\ 0.7 & \text{if } x = a, \\ 0.5 & \text{if } x = b, \\ 0.3 & \text{if } x = c. \end{cases}$$

For $m = 0.2$ we have

$$U(\mu \cup \nu; t) = \begin{cases} G & \text{if } t \in (0, 0.3], \\ \{0, a, b\} & \text{if } t \in (0.3, 0.4]. \end{cases}$$

Since $\{0, a, b\}$ is not a subquasigroup, $\mu \cup \nu$ is not an $(\in, \in \vee q_{0.2})$-fuzzy subquasigroup of $\mathcal{G}$. □

**Theorem 3.15.** *The union of ordered family of* $(\in, \in\vee q_m)$*-fuzzy subquasigroups of* $\mathcal{G}$ *is an* $(\in, \in\vee q_m)$*-fuzzy subquasigroup of* $\mathcal{G}$.

*Proof.* Let $\{\mu_i \,|\, i \in \Lambda\}$ be an ordered family of $(\in, \in\vee q_m)$-fuzzy subquasigroups of $\mathcal{G}$, i.e., $\mu_i \subseteq \mu_j$ or $\mu_j \subseteq \mu_i$ for all $i, j \in \Lambda$. Then for $\mu := \bigcup_{i\in\Lambda} \mu_i$ we have

$$\begin{aligned} \mu(x * y) &= \inf_{i\in\Lambda} \mu_i(x * y) \geqslant \inf_{i\in\Lambda} \min\{\mu_i(x)), \mu_i(y), \tfrac{1-m}{2}\} \\ &= \min\{\inf_{i\in\Lambda} \mu_i(x), \inf_{i\in\Lambda} \mu_i(y), \tfrac{1-m}{2}\} \\ &= \min\{\textstyle\bigcup_{i\in\Lambda} \mu_i(x), \bigcup_{i\in\Lambda} \mu_i(y), \tfrac{1-m}{2}\} = \min\{\mu(x), \mu(y), \tfrac{1-m}{2}\}. \end{aligned}$$

It is easy to see that

$$\inf_{i\in\Lambda} \min\Big\{\mu_i(x), \mu_i(y), \frac{1-m}{2}\Big\} \leqslant \bigcup_{i\in\Lambda} \min\Big\{\mu_i(x), \mu_i(y), \frac{1-m}{2}\Big\}.$$

Suppose that

$$\inf_{i\in\Lambda} \min\Big\{\mu_i(x), \mu_i(y), \frac{1-m}{2}\Big\} \neq \bigcup_{i\in\Lambda} \min\Big\{\mu_i(x), \mu_i(y), \frac{1-m}{2}\Big\}.$$

Then there exists $s$ such that

$$\inf_{i\in\Lambda} \min\Big\{\mu_i(x), \mu_i(y), \frac{1-m}{2}\Big\} < s < \bigcup_{i\in\Lambda} \min\Big\{\mu_i(x), \mu_i(y), \frac{1-m}{2}\Big\}.$$

Since $\mu_i \subseteq \mu_j$ or $\mu_j \subseteq \mu_i$ for all $i, j \in \Lambda$, there exists $k \in \Lambda$ such that $s < \min\Big\{\mu_k(x), \mu_k(y), \frac{1-m}{2}\Big\}$. On the other hand, $\min\Big\{\mu_i(x), \mu_i(y), \frac{1-m}{2}\Big\} > s$ for all $i \in \Lambda$, a contradiction. Hence

$$\begin{aligned} \inf_{i\in\Lambda} \min\Big\{\mu_i(x), \mu_i(y), \tfrac{1-m}{2}\Big\} &= \min\Big\{\textstyle\bigcup_{i\in\Lambda} \mu_i(x), \bigcup_{i\in\Lambda} \mu_i(y), \tfrac{1-m}{2}\Big\} \\ &= \min\Big\{\mu(x), \mu(y), \tfrac{1-m}{2}\Big\}. \end{aligned}$$

Theorem 3.5 completes the proof. □

**Theorem 3.16.** *For any finite strictly increasing chain of subquasigroups of $\mathcal{G}$ there exists an $(\in, \in \vee q_m)$-fuzzy subquasigroup $\mu$ of $\mathcal{G}$ whose level subquasigroups are precisely the members of the chain with $\mu_{\frac{1-m}{2}} = G_0 \subset G_1 \subset \ldots \subset G_n = G$.*

*Proof.* Let $\{t_i \,|\, t_i \in (0, \frac{1-m}{2}], i = 1, \ldots, n\}$ be such that $\frac{1-m}{2} > t_1 > t_2 > t_3 > \ldots > t_n$. Consider the fuzzy set $\mu$ defined by

$$\mu(x) = \begin{cases} \frac{1-m}{2} & \text{if } \ x \in G_0, \\ t_k & \text{if } \ x \in G_k \setminus G_{k-1}, \ k = 1, \ldots, n \end{cases}$$

Let $x, y \in G$ be such that $x \in G_i \setminus G_{i-1}$ and $y \in G_j \setminus G_{j-1}$, where $1 \leqslant i, j \leqslant n$. When $i \geqslant j$, then $x \in G_i$, $y \in G_i$, so $x * y \in G_i$. Thus

$$\mu(x * y) \geqslant t_i = \min\{t_i, t_j\} = \min\left\{\mu(x), \mu(y), \frac{1-m}{2}\right\}.$$

When $i < j$, then $x \in G_j$, $y \in G_j$, so $x * y \in G_j$. Thus

$$\mu(x * y) \geqslant t_j = \min\{t_i, t_j\} = \min\left\{\mu(x), \mu(y), \frac{1-m}{2}\right\}.$$

Hence $\mu$ is an $(\in, \in \vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$. □

**Definition 3.17.** For any fuzzy set $\mu$ in $\mathcal{G}$ and $t \in$ (0, 1], we define two sets

$$[\mu]_t = \{x \in G \,|\, x_t \in \vee q_m \, \mu\}$$

and

$$Q(\mu; t) = \{x \in G \,|\, x_t q_m \mu\}.$$

It is clear that $[\mu]_t = U(\mu; t) \cup Q(\mu; t)$.

**Example 3.18.** Let $G = \{0, a, b, c\}$ be a quasigroup which is given in Example 3.2. Consider fuzzy sets

$$\mu(x) = \begin{cases} 0.67 & \text{if } \ x = 0, \\ 0.56 & \text{if } \ x = a, \\ 0.47 & \text{if } \ x = b, \\ 0.41 & \text{if } \ x = c, \end{cases} \qquad \nu(x) = \begin{cases} 0.60 & \text{if } \ x = 0, \\ 0.05 & \text{if } \ x = a, \\ 0.50 & \text{if } \ x = b, \\ 0.06 & \text{if } \ x = c. \end{cases}$$

(1) When $m = 0.6$, then $U(\mu; t) = G$ and $Q(\mu; t) = G$ for all $t \in (0, 0.2]$. Thus $[\mu]_t = G$ for all $t \in (0, 0.2]$. Hence $[\mu]_t$ is an $(\in, \in \vee q_{0.6})$-fuzzy subquasigroup of $\mathcal{G}$.

(2) When $m = 0.8$, then $U(\nu;t) = G$ and $Q(\nu;t) = \{0, b\}$ for all $t \in (0, 0.1]$. Thus $[\nu]_t = G$ for all $t \in (0, 0.1]$. Hence $[\nu]_t$ is an $(\in, \in \vee q_{0.8})$-fuzzy subquasigroup of $\mathcal{G}$. □

**Problem 1.** *Prove or disprove that each nonempty $[\mu]_t$ is an $(\in, \in \vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$.*

**Problem 2.** *Find a simple characterization of $[\mu]_t$.*

An $(\in, \in \vee q_m)$-fuzzy subquasigroup of a quasigroup $\mathcal{G}$ is *proper* if $\mathrm{Im}\mu$ has at least two elements. Two $(\in, \in \vee q_m)$- fuzzy subquasigroups of $\mathcal{G}$ are *equivalent* if they have the same family of level subquasigroups. Otherwise, they are said to be non-equivalent.

**Theorem 3.19.** *Let $\mu$ be a proper $(\in, \in \vee q_m)$-fuzzy subquasigroup $\mu$ of $\mathcal{G}$ having at least two values $t_1, t_2 < \frac{1-m}{2}$. If all $[\mu]_t$, $t \in (0, \frac{1-m}{2}]$, are subquasigroups, then $\mu$ can be decomposed into the union of two proper non-equivalent $(\in, \in \vee q_m)$-fuzzy subquasigroups of $\mathcal{G}$.*

*Proof.* Let $\mu$ be a proper $(\in, \in \vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$ with values $\frac{1-m}{2} > t_1 > t_2 > \ldots > t_n$, where $n \geqslant 2$. Let $G_0 = [\mu]_{\frac{1-m}{2}}$ and $G_k = [\mu]_{t_k}$ for $k = 1, 2, \ldots, n$. Then $\mu_{\frac{1-m}{2}} = G_0 \subset G_1 \subset \ldots \subset G_n = G$ is the chain of $(\in, \in \vee q_m)$-subquasigroups.

Consider two fuzzy sets $\lambda_1$, $\lambda_2 \leqslant \mu$ defined by

$$\lambda_1(x) = \begin{cases} t_1 & \text{if } \ x \in G_1, \\ t_k, & \text{if } \ x \in G_k \setminus G_{k-1},\ k = 2, 3, \ldots, n, \end{cases}$$

$$\lambda_2(x) = \begin{cases} \mu(x) & \text{if } \ x \in G_0, \\ t_2, & \text{if } \ x \in G_2 \setminus G_0, \\ t_k, & \text{if } \ x \in G_k \setminus G_{k-1},\ k = 3, \ldots, n. \end{cases}$$

Then $\lambda_1$ and $\lambda_2$ are $(\in, \in \vee q_m)$-fuzzy subquasigroups of $\mathcal{G}$ with

$$G_1 \subset G_2 \subset \ldots \subset G_n$$

and

$$G_0 \subset G_2 \subset \ldots \subset G_n$$

being respectively chains of $(\in, \in \vee q_m)$-fuzzy subquasigroups. Obviously $\mu = \lambda_1 \cup \lambda_2$. Moreover, $\lambda_1$ and $\lambda_2$ are non-equivalent since $G_0 \neq G_1$. □

# References

[1] **M. Akram**, *Fuzzy subquasigroups with respect to a s-norm*, Bul. Acad. Sci. Republ. Moldova, ser. Mathematica **2** (2008), 3 – 13.

[2] **M. Akram and W. A. Dudek**, *Generalized fuzzy subquasigroups*, Quasigroups and Related Systems **16** (2008), 133 – 146.

[3] **S. K. Bhakat and P. Das**, $(\in, \in \vee q)$-fuzzy subgroup, Fuzzy Sets and Systems **80** (1996), 359 – 368.

[4] **P. Das**, *Fuzzy groups and level subgroups*, J. Math. Anal. Appl. **85** (1981), 264 – 269.

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

[6] **W. A. Dudek**, *On some old and new problems in n-ary groups*, Quasigroups and Related Systems **8** (2001), 15 – 36.

[7] **W. A. Dudek and Y. B. Jun**, *Fuzzy subquasigroups over a t-norm*, Quasigroups and Related Systems **6** (1999), 87 – 98.

[8] **V. Murali**, *Fuzzy points of equivalent fuzzy subsets.* Information Sciences **158** (2004), 277 – 288.

[9] **A. I. Nesterov**, *Some applications of quasigroups and loops in physics*, Inter. Conference Nonassociative Algebra and its Applications, Mexico, 2003.

[10] **P. M. Pu and Y. M. Liu**, *Fuzzy topology,I. Neighborhood structure of a fuzzy point and Moore-Smith convergence*, J. Math. Anal. Appl. **76** (1980), 571 – 599.

[11] **I. G. Rosenberg**, *Two properties of fuzzy subquasigroups of a quasigroup*, Fuzzy Sets and Systems **110** (2000), 447 – 450.

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

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

[14] **H.-J. Zimmermann**, *Fuzzy set theory and applications*, Kluwer-Nijhoff Publishing, 1985.

Received May 19, 2009

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

W.A.Dudek
Institute of Mathematics and Computer Science, Wroclaw University of Technology, Wyb. Wyspianskiego 27, 50-370 Wroclaw, Poland.
E-mail: dudek@im.pwr.wroc.pl

Quasigroups and Related Systems **17** (2009), 119 – 134

# Vague Lie subalgebras over a vague field

*Muhammad Akram* and *Kar-Ping Shum*

**Abstract.** The concept of a vague subfield and some of its fundamental properties are introduced. We then introduce the vague Lie subalgebra over a vague field and present some of its properties. In particular, different methods of constructions of such vague sets are given.

## 1. Introduction

The concept of fuzzy set was first initiated by Zadeh [14] in 1965 and since then, fuzzy set has become an important tool in studying scientific subjects, in particular, it can be applied in a wide variety of disciplines such as Computer Science, Medical Science, Management Science, Social Science, Engineering and so on. In fact, if we let $U$ be a universe of discourse, then a fuzzy set $A$ is a class of objects of $U$ along with a membership function $A$. The grade of membership of $x(x \in U)$ in the universe $U$ is 1, but the grade of membership of $x$ in a fuzzy subset $A$ (of $U$) is a real number in [0, 1] denoted by $\mu_A(x)$ which signifies that $x$ is a member of the fuzzy set $A$ up to certain extent. The degree of membership could be zero or more and at most one. The greater $\mu_A(x)$ means the greater is the truth of the statement that the element $x$ belongs to the set $A$.

Different authors from time to time have made a number of generalizations of Zadeh fuzzy set theory [14]. Recently, the notion of Vague Set (VS) was introduced by Gau and Buehrer in [10]. This is because in most cases of judgments, the evaluation is done by human beings and so the certainty is a limitation of knowledge or intellectual functionaries. Naturally, every decision-maker hesitates more or less on every evaluation activity. For example, in order to judge whether a patient has cancer or not, a medical doctor (the decision-maker) will hesitate because of the fact that a fraction of evaluation he thinks in favor of the truthness, another fraction in favor

2000 Mathematics Subject Classification: 04A72, 17B99
Keywords: Vague field, vague Lie subalgebras, normal vague Lie subalgebra.

of the falseness and the rest part remains undecided to him. This is the breaking philosophy in the notion of vague set theory introduced by Gau and Buehrer in [10]. The notions of fuzzy ideals and fuzzy subalgebras of Lie algebras over a field were considered in [13] by Yehia. In this paper, we first introduce the concept of a vague subfield and study some fundamental properties. Then we introduce the notion of a vague Lie subalgebra over a vague field and present some properties. Finally, we give some important properties of a vague Lie subalgebra over a vague field of different types and describe some methods of constructions for such vague sets. The definitions and terminologies that we used in this paper are standard. For other notations, terminologies and applications, the readers are refereed to [1, 3, 4, 6, 7, 10, 11].

## 2. Preliminaries

Throughout this paper, $L$ is a Lie algebra and $X$ is a field. It is clear that the multiplication of a Lie algebra is not necessary associative, that is, $[[x,y],z]=[x,[y,z]]$ does not hold in general, however it is *anti- commutative*, that is, $[x,y]=-[y,x]$.

Let $\mu$ be a *fuzzy set* on $L$, that is, a map $\mu : L \to [0,1]$.

**Definition 2.1.** [12] A *fuzzy set* $F$ of $X$ is called a *fuzzy field* if

(1) $(\forall\, m,n \in X)(F(m-n) \geqslant \min\{F(m),F(n)\})$,

(2) $(\forall\, m,n \in X, n \neq 0)(F(mn^{-1}) \geqslant \min\{F(m),F(n)\})$.

**Definition 2.2.** [10] A *vague set* (in short, VS) $A$ in the universe $L$ is a pair $(t_A, f_A)$, where $t_A : L \to [0,1]$, $f_A : L \to [0,1]$ are true and false memberships, respectively such that $t_A(x)+f_A(x) \leqslant 1$ for all $x \in L$. The interval $[t_A(x), 1-f_A(x)]$ is called the *vague value* of $x$ in $A$, and is denoted by $V_A(x)$.

**Definition 2.3.** [10] Let $A=(t_A,f_A)$ and $B=(t_B,f_B)$ be two vague sets. Then we define:

(3) $\overline{A}=(f_A, 1-t_A)$,

(4) $A \subset B \Leftrightarrow V_A(x) \leqslant V_B(x)$, i.e., $t_A(x) \leqslant t_B(x)$ and $1-f_A(x) \leqslant 1-f_B(x)$,

(5) $A=B \Leftrightarrow V_A(x)=V_B(x)$,

(6) $C = A \cap B \Leftrightarrow V_C(x) = \min(V_A(x), V_B(x))$,

(7) $C = A \cup B \Leftrightarrow V_C(x) = \max(V_A(x), V_B(x))$

for all $x \in L$.

**Definition 2.4.** [10] A vague set $A = (t_A, f_A)$ of a set $L$ is called

(8) the *zero vague set* if $t_A(x) = 0$ and $f_A(x) = 1$ for all $x \in L$,

(9) the *unit vague set* if $t_A(x) = 1$ and $f_A(x) = 0$ for all $x \in L$,

(10) the *$\alpha$-vague set* if $t_A(x) = \alpha$ and $f_A(x) = 1 - \alpha$ for all $x \in L$, $\alpha \in (0, 1)$.

We also denote the zero vague and the unit vague value by intervals $\mathbf{0} = [0, 0]$ and $\mathbf{1} = [1, 1]$, respectively.

For $\alpha$, $\beta \in [0, 1]$, we define the $(\alpha, \beta)-$cut and the $\alpha$-cut of a vague set.

**Definition 2.5.** [6] Let $A = (t_A, f_A)$ be vague set of a universe $L$. Then the $(\alpha, \beta)-$ cut of a vague set $A$ is a crisp set $A_{(\alpha,\beta)}$ of $L$ given by

$$A_{(\alpha,\beta)} = \{x \in L : V_A(x) \geqslant [\alpha, \beta]\}.$$

Obviously, $A_{(0,0)} = L$. The $(\alpha, \beta)$-cuts are also the vague-cuts of the vague set $A$. The $\alpha$-cut of the vague set $A = (t_A, f_A)$ is a crisp set $A_\alpha$ of $L$ given by $A_\alpha = A_{(\alpha,\alpha)}$. Note that $A_0 = L$. Clearly, $A_\alpha = \{x \in L : t_A(x) \geqslant \alpha\}$.

By an *interval number* $D$, we mean an interval $[a^-, a^+]$ with $0 \leqslant a^- \leqslant a^+ \leqslant 1$. The set of all interval numbers is denoted by $D[0, 1]$. The interval $[a, a]$ is identified with the fuzzy number $a \in [0, 1]$.

For any two interval numbers $D_1 = [a_1^-, b_1^+]$ and $D_2 = [a_2^-, b_2^+]$, we define

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

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

and put

- $D_1 \leqslant D_2 \Longleftrightarrow a_1^- \leqslant a_2^-$ and $b_1^+ \leqslant b_2^+$,
- $D_1 = D_2 \Longleftrightarrow a_1^- = a_2^-$ and $b_1^+ = b_2^+$,
- $D_1 < D_2 \Longleftrightarrow D_1 \leqslant D_2$ and $D_1 \neq D_2$,
- $mD = m[a_1^-, b_1^+] = [ma_1^-, mb_1^+]$, where $0 \leqslant m \leqslant 1$.

It can be easily verified that $(D[0,1], \leqslant, \vee, \wedge)$ forms a complete lattice under the set inclusion with $[0,0]$ as its least element and $[1,1]$ as its greatest element.

## 3. Vague fields

**Definition 3.1.** A *vague set* $F = (t_F, f_F)$ of $X$ is said to be a *vague subfield* of the field $X$ if the following conditions are satisfied:

$$(11) \quad (\forall\, m, n \in X)(V_F(m-n) \geqslant \min\{V_F(m), V_F(n)\}),$$

$$(12) \quad (\forall\, m, n \in X, n \neq 0)(V_F(mn^{-1}) \geqslant \min\{V_F(m), V_F(n)\}),$$

that is,

$$(13) \quad \begin{cases} t_A(m-n) \geqslant \min\{t_A(m), t_A(n)\}, \\ 1 - f_A(m-n) \geqslant \min\{1 - f_A(m), 1 - f_A(n)\}, \end{cases}$$

$$(14) \quad \begin{cases} t_A(mn^{-1}) \geqslant \min\{t_F(m), t_A(n)\}, \\ 1 - f_A(mn^{-1}) \geqslant \min\{1 - f_F(m), 1 - f_A(n)\}, \end{cases}$$

**Example 3.2.** Consider a field $X = \{0, 1, w, w^2\}$, where $w = \frac{-1+\sqrt{-3}}{2}$, with the following Cayley tables:

| + | 0 | 1 | w | $w^2$ |
|---|---|---|---|---|
| 0 | 0 | 1 | w | $w^2$ |
| 1 | 1 | 0 | $w^2$ | w |
| w | w | $w^2$ | 0 | 1 |
| $w^2$ | $w^2$ | w | 1 | 0 |

| . | 0 | 1 | w | $w^2$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | w | $w^2$ |
| w | 0 | w | $w^2$ | 1 |
| $w^2$ | 0 | $w^2$ | 1 | w |

It can be easily seen that the vague set

$$\{(0, [0.3,\ 0.2]), (1, [0.4,\ 0.5]), (w, [0.3,\ 0.6]), (w^2, [0.5,\ 0.4])\}$$

forms a vague subfield of the field $X$. □

The following Lemmas can be easily proved and hence we omit their proofs.

**Lemma 3.3.** *If* $F = (t_F, f_F)$ *is a vague subfield of* $X$, *then*

$$V_F(0) \geqslant V_F(1) \geqslant V_F(m) = V_F(-m) \quad for\ m \in X, \quad and$$

$$V_F(-m) = V_F(m^{-1}) \quad for\ m \in X - \{0\}.$$

**Lemma 3.4.** *A vague set* $A = (t_A, f_A)$ *of* $X$ *is a vague subfield of* $X$ *if and only if* $t_A$ *and* $1 - f_A$ *are fuzzy subfields.*

**Proposition 3.5.** *If $A$ and $B$ are vague subfields of $X$, then $A \cap B$ is a vague subfield of $X$.*

*Proof.* Let $m$, $n \in X$. Then we have

$$\begin{aligned} t_{A\cap B}(m-n) &= \min\{t_A(m-n), t_B(m-n)\} \\ &\geqslant \min\{\min\{t_A(m), t_A(n)\}, \min\{t_B(m), t_B(n)\}\} \\ &= \min\{\min\{t_A(m), t_B(m)\}, \min\{t_A(n), t_B(n)\}\} \\ &= \min\{t_{A\cap B}(m), t_{A\cap B}(n)\}, \end{aligned}$$

and hence, we derive that

$$\begin{aligned} t_{A\cap B}(mn^{-1}) &= \min\{t_A(mn^{-1}), t_B(mn^{-1})\} \\ &\geqslant \min\{\min\{t_A(m), t_A(n)\}, \min\{t_B(m), t_B(n)\}\} \\ &= \min\{\min\{t_A(m), t_B(m)\}, \min\{t_A(n), t_B(n)\}\} \\ &= \min\{t_{A\cap B}(m), t_{A\cap B}(n)\}, \end{aligned}$$

$$\begin{aligned} 1-f_{A\cap B}(m-n) &= \min\{1 - f_A(m-n), 1 - f_B(m-n)\} \\ &\geqslant \min\{\min\{1-f_A(m), 1-f_A(n)\}, \min\{1-f_B(m), 1-f_B(n)\}\} \\ &= \min\{\min\{1-f_A(m), 1-f_B(m)\}, \min\{1-f_A(n), 1-f_B(n)\}\} \\ &= \min\{1 - f_{A\cap B}(m), 1 - f_{A\cap B}(n)\}, \end{aligned}$$

$$\begin{aligned} 1-f_{A\cap B}(mn^{-1}) &= \min\{1 - f_A(mn^{-1}), 1 - f_B(mn^{-1})\} \\ &\geqslant \min\{\min\{1-f_A(m), 1-f_A(n)\}, \min\{1-f_B(m), 1-f_B(n)\}\} \\ &= \min\{\min\{1-f_A(m), 1-f_B(m)\}, \min\{1-f_A(n), 1-f_B(n)\}\} \\ &= \min\{1 - f_{A\cap B}(m), 1 - f_{A\cap B}(n)\}. \end{aligned}$$

Therefore, we have proved that $A \cap B$ is indeed a vague subfield of $X$. □

**Proposition 3.6.** *The zero vague set, unit vague set and $\alpha$- vague set are all vague subfields of $X$.*

*Proof.* Let $A = (t_A,\ f_A)$ be a vague subfield of $X$. For $m, n \in X$, we have

$$t_A(m-n) \geqslant \min\{t_A(m), t_A(n)\} = \min\{\alpha, \alpha\} = \alpha,$$

$$1 - f_A(m-n) \geqslant \min\{1 - f_A(m), 1 - f_A(n)\} = \min\{\alpha, \alpha\} = \alpha,$$

$$t_A(mn^{-1}) \geqslant \min\{t_A(m), t_A(n)\} = \min\{\alpha, \alpha\} = \alpha,$$
$$1 - f_A(mn^{-1}) \geqslant \min\{1 - t_A(m), 1 - t_A(n)\} = \min\{\alpha, \alpha\} = \alpha.$$

This shows that $\alpha$-vague set of $X$ is a vague subfield of $X$. The proofs for the other cases are similar. □

**Proposition 3.7.** *Let $A$ be a vague subfield of $X$. Then for $\alpha \in [0,1]$, the vague-cut $A_\alpha$ is a crisp subfield of $X$.*

*Proof.* Suppose that $A = (t_A, f_A)$ is a vague subfield of $X$. For $m, n \in A_\alpha$ we can deduce that

$$t_A(m) \geqslant \alpha, \quad 1 - f_A(m) \geqslant \alpha, \quad t_A(n) \geqslant \alpha, \quad 1 - f_A(n) \geqslant \alpha,$$

so that

$$t_A(m - n) \geqslant \min\{t_A(m), t_A(n)\} \geqslant \min\{\alpha, \alpha\} = \alpha,$$
$$1 - f_A(m - n) \geqslant \min\{1 - f_A(m), 1 - f_A(n)\} \geqslant \min\{\alpha, \alpha\} = \alpha,$$
$$t_A(mn^{-1}) \geqslant \min\{t_A(m), t_A(n)\} \geqslant \min\{\alpha, \alpha\} = \alpha,$$
$$1 - f_A(mn^{-1}) \geqslant \min\{1 - t_A(m), 1 - t_A(n)\} \geqslant \min\{\alpha, \alpha\} = \alpha.$$

This implies that $m - n$, $mn^{-1} \in A_\alpha$. Hence $A_\alpha$ is a crisp subfield of $X$. □

**Proposition 3.8.** *Any subfield $K$ of $X$ is a vague-cut subfield of some vague subfield of $X$.*

*Proof.* Consider the vague set $A$ of $X$ given by

$$V_A(m) = \begin{cases} [t,\, t] & \text{if } m \in K, \\ [0, 0] & \text{if } m \notin K, \end{cases}$$

where $t \in (0,\, 1)$. Clearly, $A_{(\alpha,\alpha)} = K$. Let $m, n, p \in X$. We now consider the following cases:

Case (i): If $m, n, p \in K$, $p \neq 0$, then $m - n, mp^{-1} \in K$ and

$$V_F(m - n) \geqslant \min\{V_F(m), V_F(n)\} = [t,\, t],$$
$$V_F(mp^{-1}) \geqslant \min\{V_F(m), V_F(p)\} = [t,\, t].$$

Case (ii): If $m, n, p \notin K$, $p \neq 0$, then $V_A(m) = [0, 0] = V_A(n) = V(p)$, and

$$V_F(m - n) \geqslant \min\{V_F(m), V_F(n)\} = [0,\, 0],$$
$$V_F(mp^{-1}) \geqslant \min\{V_F(m), V_F(p)\} = [0,\, 0].$$

Case (iii): If $m \in K$ and $n, p \notin K$, $p \neq 0$, then $V_F(m) = [t,\, t]$, $V_F(n) = [0,\, 0] = V_F(p)$, so

$$V_F(m-n) \geqslant \min\{V_F(m), V_F(n)\} = [0,\, 0],$$
$$V_F(mp^{-1}) \geqslant \min\{V_F(m), V_F(p)\} = [0,\, 0].$$

Case (iv): If $m \notin K$ and $n, p \in K$, $p \neq 0$, then by using the same argument as in Case 3, we conclude the results. Hence, we have proved that $K$ is a vague field of $X$. □

**Proposition 3.9.** *Let $K$ be a vague set of $X$ which is defined by*

$$V_K(m) = \begin{cases} [s, s] & \textit{if} \ \ m \in K \\ [t, t] & \textit{otherwise} \end{cases}$$

*for all $s$, $t \in [0, 1]$ with $s \geqslant t$. Then $K$ is a vague subfield of $X$ if and only if $K$ is a (crisp) subfield of $X$.*

*Proof.* Let $K$ be a vague subfield of $X$. If $m, n, p \in K$, $p \neq 0$, then

$$V_K(m-n) \geqslant \min\{V_K(m), V_K(n)\} = \min\{[s, s], [s, s]\} = [s, s],$$

$$V_K(mp^{-1}) \geqslant \min\{V_K(m), V_K(p)\} = \min\{[s, s], [s, s]\} = [s, s],$$

and so $m - n$, $mp^{-1} \in K$.

Conversely, suppose that $K$ is a (crisp) subfield of $X$. We consider the following situations:

(i) If $m, n, p \in K$, $p \neq 0$, then $m - n, mp^{-1} \in K$. Thus

$$V_K(m-n) \geqslant [s, s] = \min\{V_K(m), V_K(n)\},$$

$$V_K(mp^{-1}) \geqslant [s, s] = \min\{V_K(m), V_K(p)\}.$$

(ii) If $m \notin K$ or $n, p \notin K$, $p \neq 0$, then

$$V_K(m-n) \geqslant [t, t] = \min\{V_K(m), V_K(n)\},$$

$$V_K(mp^{-1}) \geqslant [t, t] = \min\{V_K(m), V_K(p)\}.$$

This shows that $K$ is a vague subfield of $X$. □

## 4. Vague Lie subalgebras over a vague field

**Definition 4.1.** A *vague set* $A = (t_A,\ f_A)$ of $L$ is called a *vague Lie subalgebra over a vague field* $F = (t_F, f_F)$ (briefly, *vague Lie* $\mathbb{F}$*-subalgebra*) of $L$ if the following conditions are satisfied

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

(b) $V_A(mx) \geqslant \min\{V_F(m), V_A(x)\}$,

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

for all $x, y \in L$ and $m \in X$.

In other words,

(d) $\begin{cases} t_A(x+y) \geqslant \min\{t_A(x), t_A(y)\}, \\ 1 - f_A(x+y) \geqslant \min\{1 - f_A(x), 1 - f_A(y)\}, \end{cases}$

(e) $\begin{cases} t_A(mx) \geqslant \min\{t_F(m), t_A(x)\}, \\ 1 - f_A(mx) \geqslant \min\{1 - f_F(m), 1 - f_A(x)\}, \end{cases}$

(f) $\begin{cases} t_A([x,y]) \geqslant \min\{t_A(x), t_A(y)\}, \\ 1 - f_A([x,y]) \geqslant \min\{1 - f_A(x), 1 - f_A(y)\}. \end{cases}$

From (b), it follows that $V_A(0) \geqslant V_F(0)$.

**Example 4.2.** Let $\Re^2 = \{(x,y) : x, y \in R\}$ be the set of all 2-dimensional real vectors. Then $\Re^2$ with $[x,y] = x \times y$ form a real Lie algebra. Define a vague set $A = (t_A, f_A) : \Re^2 \to [0,1]$ by

$$t_A(x,y) = \begin{cases} 0.4 & \text{if } x = y = 0, \\ 0.3 & \text{otherwise}, \end{cases} \qquad f_A(x,y) = \begin{cases} 0.3 & \text{if } x = y = 0, \\ 0.4 & \text{otherwise}, \end{cases}$$

and define $F = (t_F, f_F) : \mathbb{R} \to [0,1]$ for all $m \in \mathbb{R}$ by

$$t_F(m) = \begin{cases} 0.3 & \text{if } m \in \mathbb{Q}, \\ 0.2 & \text{if } 0\ m \in \mathbb{R} - \mathbb{Q}(\sqrt{3}), \end{cases}$$

$$f_F(m) = \begin{cases} 0.2 & \text{if } m \in \mathbb{Q}, \\ 0.4 & \text{if } 0\ m \in \mathbb{R} - \mathbb{Q}(\sqrt{3}). \end{cases}$$

By routine verification, we can easily check that $A$ is a vague Lie $\mathbb{F}$-subalgebra.

The proofs of the following propositions are obvious.

**Proposition 4.3.** *A vague set $A = (t_A, f_A)$ of $L$ is a vague Lie $\mathbb{F}$-subalgebra of $L$ if and only if $t_A$ and $1 - f_A$ are fuzzy Lie $\mathbb{F}$-subalgebras over a fuzzy field.*

**Proposition 4.4.** *Let $\{A_i : i \in \Lambda\}$ be a family of vague Lie $\mathbb{F}$-subalgebras of $L$. Then $\cap_{i\in\Lambda} A_i$ is a vague Lie $\mathbb{F}$-subalgebra of $L$.*

**Proposition 4.5.** *The zero vague set, unit vague set and $\alpha$-vague set are vague Lie $\mathbb{F}$-subalgebras of $L$.*

**Theorem 4.6.** *Let $A$ be a vague Lie $\mathbb{F}$-subalgebra of $L$. Then for any $\alpha$, $\beta$ $\in [0,1]$, the vague-cut $A_{(\alpha,\beta)}$ is a crisp Lie subalgebra of $L$.*

*Proof.* Suppose that $A = (t_A, f_A)$ is a vague Lie subalgebra of $L$ over a vague field $F = (t_F, f_F)$. Let $x, y, m \in A_{(\alpha,\beta)}$, $x, y \in L$, $m \in X$. Then

$$t_A(x) \geqslant \alpha, \quad 1 - f_A(x) \geqslant \beta, \quad t_A(y) \geqslant \alpha, \quad 1 - f_A(y) \geqslant \beta, \quad t_F(m) \geqslant \alpha$$

and $1 - f_F(m) \geqslant \beta$.

From Definition 4.1, it follows that

$$\begin{aligned}
t_A(x+y) &\geqslant \min\{t_A(x), t_A(y)\} \geqslant \min\{\alpha, \alpha\} = \alpha,\\
1 - f_A(x+y) &\geqslant \min\{1 - f_A(x), 1 - f_A(y)\} \geqslant \min\{\beta, \beta\} = \beta,\\
t_A(mx) &\geqslant \min\{t_F(m), t_A(x)\} \geqslant \min\{\alpha, \alpha\} = \alpha,\\
1 - f_A(mx) &\geqslant \min\{1 - t_F(m), 1 - t_A(x)\} \geqslant \min\{\beta, \beta\} = \beta,\\
t_A([x,y]) &\geqslant \min\{t_A(x), t_A(y)\} \geqslant \min\{\alpha, \alpha\} = \alpha,\\
1 - f_A([x,y]) &\geqslant \min\{1 - f_A(x), 1 - f_A(y)\} \geqslant \min\{\beta, \beta\} = \beta.
\end{aligned}$$

This implies that $x + y$, $mx$, $[x,y] \in A_{(\alpha,\beta)}$. Hence $A_{(\alpha,\beta)}$ is a crisp Lie subalgebra of $L$. □

**Corollary 4.7.** *Let $A$ be a vague Lie $\mathbb{F}$-subalgebra of $L$. Then for $\alpha \in [0,1]$, the vague-cut $A_\alpha$ is a crisp Lie subalgebra of $L$.*

The proofs of the following propositions are obvious.

**Proposition 4.8.**

(i) *Let $f : L_1 \to L_2$ be an onto homomorphism of Lie algebras. If $B = (t_B, f_B)$ is a vague Lie $\mathbb{F}$-subalgebra of $L_2$, then the preimage $f^{-1}(B)$ of $B$ under $f$ is a vague Lie $\mathbb{F}$-subalgebra $L_1$.*

(ii) *Let $f : L_1 \to L_2$ be an epimorphism of Lie algebras. If $A = (t_A, f_A)$ is a vague Lie $\mathbb{F}$-subalgebra of $L_2$, then $f^{-1}(A^c) = (f^{-1}(A))^c$.*

(iii) *Let $f : L_1 \to L_2$ be an epimorphism of Lie algebras. If $A = (t_A, f_A)$ is a vague Lie $\mathbb{F}$-subalgebra of $L_2$ and $B = (t_B, f_B)$ is the preimage of $A = (\mu_A, \lambda_A)$ under $f$. Then $B = (t_B, f_B)$ is a vague Lie $\mathbb{F}$-subalgebra of $L_1$.*

**Definition 4.9.** Let $g : L_1 \to L_2$ be a homomorphism of Lie algebras. For any vague fuzzy set $A = (t_A, f_A)$ in a Lie algebra $L_2$, we define a vague fuzzy set $A^g = (t^g_A, f^g_A)$ in $L$ by

$$t^g_A(x) = t_A(g(x)), \quad f^g_A(x) = f_A(g(x))$$

for all $x \in L_1$. Clearly, $A^g(x_1) = A^g(x_2) = A(x)$ for all $x_1, x_2 \in g^{-1}(x)$.

**Lemma 4.10.** *Let $g : L_1 \to L_2$ be a homomorphism of Lie algebras. If $A = (t_A, f_A)$ is a vague Lie $\mathbb{F}$-subalgebra of $L_2$, then $A^g$ is a vague Lie $\mathbb{F}$-subalgebra of $L_1$.*

*Proof.* Let $x, y \in L_1$ and $m \in X$. Then

$$\begin{aligned} t^g_A(x+y) &= t_A(g(x+y)) = t_A(g(x)+g(y)) \\ &\geqslant \min\{t_A(g(x)), t_A(g(y))\} = \min\{t^g_A(x), t^g_A(y)\}, \end{aligned}$$

$$\begin{aligned} 1 - f^g_A(x+y) &= 1 - f_A((g(x+y)) = 1 - f_A(g(x)+g(y)) \\ &\geqslant \min\{1 - f_A(g(x)), 1 - f_A(g(y))\} \\ &= \min\{1 - f^g_A(x), 1 - f^g_A(y)\}. \end{aligned}$$

The verification of the other conditions is similar. Hence, $A^g$ is a vague Lie $\mathbb{F}$-subalgebra of $L_1$. □

**Theorem 4.11.** *Let $g : L_1 \to L_2$ be an epimorphism of Lie algebras. Then $A^g$ is a vague Lie $\mathbb{F}$-subalgebra of $L_1$ if and only if $A$ is a vague Lie $\mathbb{F}$-subalgebra of $L_2$.*

*Proof.* The sufficiency follows from Lemma 4.10. In proving the necessity, we first recall that $g$ is a surjective mapping. Hence for any $x, y \in L_2$, there exist $x_1$, $y_1 \in L_1$ such that $x = g(x_1)$, $y = g(y_1)$. Thus $t_A(x) = t^g_A(x_1)$, $t_A(y) = t^g_A(y_1)$, $1 - f_A(x) = 1 - f^g_A(x_1)$, $1 - f_A(y) = 1 - f^g_A(y_1)$, whence

$$\begin{aligned} t_A(x+y) &= t_A(g(x_1)+g(y_1)) = t_A(g(x_1+y_1)) \\ &= t^g_A(x_1+y_1) \geqslant \min\{t^g_A(x_1), t^g_A(y_1)\} = \min\{t_A(x), t_A(y)\}, \end{aligned}$$

$$\begin{aligned} 1 - f_A(x+y) &= 1 - f_A(g(x_1) + g(y_1)) = 1 - f_A(g(x_1 + y_1)) \\ &= 1 - f_A^g(x_1 + y_1) \geqslant \min\{1 - f_A^g(x_1), 1 - f_A^g(y_1)\} \\ &= \min\{1 - f_A(x), 1 - f_A(y)\}. \end{aligned}$$

The verification of the other conditions is similar. This proves that $A = (t_A, f_A)$ is a vague Lie $\mathbb{F}$-subalgebra of $L_2$. □

## 5. Special types of vague Lie subalgebras

**Definition 5.1.** Let $A = (t_A, f_A)$ be a vague Lie $\mathbb{F}$-subalgebra in $L$. Define inductively a sequence of vague Lie $\mathbb{F}$-subalgebras in $L$ by Lie brackets

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

Then, $A^n$ is said to be the *nth derived vague Lie* $\mathbb{F}$*-subalgebra* of $L$. Moreover, a series

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

is said to be a *derived series* of a vague Lie $\mathbb{F}$-subalgebra $A$ in $L$. A vague Lie $\mathbb{F}$-subalgebra $A$ in $L$ is called a *solvable vague Lie* $\mathbb{F}$*-subalgebra* if there exists a positive integer $n$ such that $A^n = \mathbf{0}$.

**Definition 5.2.** Let $A = (t_A, f_A)$ be a vague Lie $\mathbb{F}$-subalgebra in $L$. We define inductively a sequence of vague Lie $\mathbb{F}$-subalgebras in $L$ by Lie brackets

$$A_0 = A, \quad A_1 = [A, A_0], \quad A_2 = [A, A_1], \ \ldots, \ A_n = [A, A_{n-1}].$$

Then we call the series

$$A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_n \supseteq \cdots$$

the *descending central series* of a vague Lie $\mathbb{F}$-subalgebra $A$ in $L$. An vague vague Lie $\mathbb{F}$-subalgebra $A$ in $L$ is called a *nilpotent vague Lie* $\mathbb{F}$*-subalgebra* if there exists a positive integer $n$ such that $A_n = \mathbf{0}$.

By using similar arguments as in the proof of Theorem 4.7 in [2], we obtain the following theorem.

**Theorem 5.3.**

(I) *The homomorphic image of a solvable vague Lie* $\mathbb{F}$*-subalgebra is a solvable vague Lie* $\mathbb{F}$*-subalgebra.*

(II) *The homomorphic image of a nilpotent vague Lie $\mathbb{F}$-subalgebra is a nilpotent vague Lie $\mathbb{F}$-subalgebra.*

(III) *If $A$ is a nilpotent vague Lie $\mathbb{F}$-subalgebra, then it is solvable.*

**Definition 5.4.** A vague Lie $\mathbb{F}$-subalgebra $A = (t_A, f_A)$ of a Lie algebra $L$ is said to be *normal* if there exists an element $x_0 \in L$ such that $V_A(x_0) = \mathbf{1}$, i.e., $t_A(x_0) = 1$ and $f_A(x_0) = 0$.

The following Lemma is easy to prove and we hence omit the proof.

**Lemma 5.5.** *Let $A = (t_A, f_A)$ be a vague Lie $\mathbb{F}$-subalgebra of $L$ such that $t_A(x) + f_A(x) \leqslant t_A(0) + f_A(0)$ for all $x \in L$. Define $A^+ = (t_A^+, f_A^+)$, where $t_A^+(x) = t_A(x) + 1 - t_A(0)$, $f_A^+(x) = f_A(x) - f_A(0)$ for all $x \in L$. Then $A^+$ is normal vague set.*

By using the above lemma, we deduce the following theorem.

**Theorem 5.6.** *Let $A = (t_A, f_A)$ be a vague Lie $\mathbb{F}$-subalgebra of a Lie algebra $L$. Then the vague set $A^+$ is a normal vague Lie $\mathbb{F}$-subalgebra of $L$ containing $A$.*

*Proof.* Let $x, y \in L$ and $m \in X$. Then

$$\begin{aligned}\min\{V_A^+(x), V_A^+(y)\} &= \min\{V_A(x) + 1 - V_A(0), V_A(y) + 1 - V_A(0)\}\\ &= \min\{V_A(x), V_A(y)\} + 1 - V_A(0)\}\\ &\leqslant V_A(x+y) + 1 - V_A(0) = V_{A^+}(x+y),\end{aligned}$$

$$\begin{aligned}\min\{V_F^+(m), V_A^+(x)\} &= \min\{V_F(m) + 1 - V_F(0), V_A(x) + 1 - V_A(0)\}\\ &= \min\{V_F(m), V_A(x)\} + 1 - (V_F(0) + V_A(0))\}\\ &\leqslant V_A(mx) + 1 - (V_F(0) + V_A(0)) = V_{A^+}(mx),\end{aligned}$$

$$\begin{aligned}\min\{V_A^+(x), V_A^+(y)\} &= \min\{V_A(x) + 1 - V_A(0), V_A(y) + 1 - V_A(0)\}\\ &= \min\{V_A(x), V_A(y)\} + 1 - V_A(0)\}\\ &\leqslant V_A([x,y]) + 1 - V_A(0) = V_{A^+}([x,y]).\end{aligned}$$

Thus, $A^+$ is a normal vague Lie $\mathbb{F}$-subalgebra of $L$. Clearly $A \subseteq A^+$. □

The following theorems are obvious.

**Theorem 5.7.** *A vague Lie $\mathbb{F}$-subalgebra $A$ of a Lie algebra $L$ is normal if and only if $A^+ = A$.*

**Theorem 5.8.** *If $A = (t_A, f_A)$ is a vague Lie $\mathbb{F}$-subalgebra of a Lie algebra $L$, then $(A^+)^+ = A^+$.*

**Corollary 5.9.** *If $A$ is normal vague Lie $\mathbb{F}$-subalgebra of a Lie algebra $L$, then $(A^+)^+ = A$.*

**Theorem 5.10.** *Let $A$ and $B$ be vague Lie $\mathbb{F}$-subalgebras of a Lie algebra $L$. Then $(A \cup B)^+ = A^+ \cup B^+$.*

*Proof.* Let $A = (t_A, f_A)$ and $B = (t_B, f_B)$ be two vague Lie $\mathbb{F}$-subalgebras of a Lie algebra $L$. Then $A \cup B = (t_{A\cup B}, f_{A\cup B})$, where

$$t_{A\cup B}(x) = \max\{t_A(x), t_B(x)\}, \quad f_{A\cup B}(x) = \min\{f_A(x), f_B(x)\}, \quad \forall x \in L.$$

Thus $(A \cup B)^+ = (t_{(A\cup B)^+}(x), f_{(A\cup B)^+}(x))$, where

$$\begin{aligned} t_{(A\cup B)^+}(x) &= t_{(A\cup B)}(x) + 1 - t_{(A\cup B)}(0) \\ &= \max\{t_A(x), t_B(x)\} + 1 - \max\{t_A(0), t_B(0)\} \\ &= \max\{t_A(x) + 1 - t_A(0), t_B(x) + 1 - t_B(0)\} \\ &= \max\{t_{A^+}(x), t_{B^+}(x)\} = t_{A^+\cup B^+}(x). \end{aligned}$$

Similarly, we can prove that $f_{(A\cup B)^+}(x) = f_{A^+\cup B^+}(x)$ for $x \in L$. Hence, $(A \cup B)^+ = A^+ \cup B^+$. □

The proof of the following theorem is obvious.

**Theorem 5.11.** *Let $A$ be a vague Lie $\mathbb{F}$-subalgebra of a Lie algebra $L$. If there exist a vague Lie $\mathbb{F}$-subalgebra $B$ of $L$ satisfying $B \subset A^+$, then $A$ is normal.*

**Corollary 5.12.** *Let $A$ be a vague Lie $\mathbb{F}$-subalgebra of a Lie algebra $L$. If there exists a vague Lie $\mathbb{F}$-subalgebra $B$ of $L$ satisfying $B^+ \subset A$, then $A^+ = A$.*

Denote the family of all vague Lie $\mathbb{F}$-subalgebras of a Lie algebra $L$ by $VLS(L)$, and the set of all normal vague Lie $\mathbb{F}$-subalgebra of $L$ by $\mathcal{N}(L)$. It is clear that $\mathcal{N}(L)$ is a poset under set inclusion.

**Theorem 5.13.** *A non-constant maximal element of $(\mathcal{N}(L), \subseteq)$ takes only the values $\mathbf{0}$ and $\mathbf{1}$.*

*Proof.* Let $A \in \mathcal{N}(L)$ be a non-constant maximal element of $(\mathcal{N}(L), \subseteq)$. Then $t_A(x_0) = 1$ and $f_A(x_0) = 0$ for some $x_0 \in L$. Let $x \in L$ be such that $V_A(x) \neq \mathbf{1}$. We claim that $V_A(x) = \mathbf{0}$. If not, then there exists $a \in L$ such that $\mathbf{0} < V_A(a) < \mathbf{1}$. Let $B$ be a vague set in $L$ over vague field $K$ defined by $V_B(x) := \frac{1}{2}\{V_A(x) + V_A(a)\}$, $V_K(x) := \frac{1}{2}\{V_F(x) + V_F(a)\}$ for all $x \in L$. For $x$, $y \in L$ and $m \in X$, we have

$$\begin{aligned}V_B(x+y) &= \frac{1}{2}\{V_A(x+y) + V_A(a)\} \geqslant \frac{1}{2}\{\min\{V_A(x), V_A(y)\} + V_A(a)\}\\ &= \{\min\{\frac{1}{2}(V_A(x) + V_A(a)), \frac{1}{2}(V_A(y) + V_A(a))\}\\ &= \min\{V_B(x), V_B(y)\},\end{aligned}$$

$$\begin{aligned}V_B(mx) &= \frac{1}{2}\{V_A(mx) + V_A(a)\} \geqslant \frac{1}{2}\{\min\{V_F(m), V_A(x)\} + V_A(a)\}\\ &= \min\{\frac{1}{2}(V_F(m) + V_F(a)), \frac{1}{2}(V_A(x) + V_A(a))\}\\ &= \min\{V_K(m), V_B(x)\},\\ V_B([x,y]) &= \frac{1}{2}\{V_A([x,y]) + V_A(a)\} \geqslant \frac{1}{2}\{\min\{V_A(x), V_A(y)\} + V_A(a)\}\\ &= \min\{\frac{1}{2}(V_A(x) + V_A(a)), \frac{1}{2}(V_A(y) + V_A(a))\}\\ &= \min\{V_B(x), V_B(y)\}.\end{aligned}$$

This proves that $B$ is a vague Lie $\mathbb{F}$-subalgebra of $L$. Now we have

$$\begin{aligned}V_{B^+}(x) &= V_B(x) + 1 - V_B(0)\\ &= \frac{1}{2}\{\min\{V_A(x), V_A(a)\} + 1 - \frac{1}{2}\{\min\{V_A(0), V_A(a)\}\\ &= V_A(x) + 1,\end{aligned}$$

which implies that $V_{B^+}(0) = \frac{1}{2}\{V_A(0) + 1\} = 1$. Thus $B^+$ forms a normal vague Lie $\mathbb{F}$-subalgebra of $L$. But $V_{B^+}(0) = \mathbf{1} > V_{B^+}(a) = \frac{1}{2}\{V_A(a) + 1\} > V_A(a)$, so $B^+$ is a non-constant normal vague Lie $\mathbb{F}$-subalgebra of $L$ and $V_{B^+}(a) > V_A(a)$, which is a contradiction. Hence, a non-constant maximal element of $(\mathcal{N}(L), \subseteq)$ takes only two values: $\mathbf{0}$ and $\mathbf{1}$. □

**Definition 5.14.** A non-constant vague Lie $\mathbb{F}$-subalgebra $A \in VLS(L)$ is called *maximal* if $A^+$ is a maximal element of the poset $(\mathcal{N}(L), \subseteq)$.

**Theorem 5.15.** *A maximal vague Lie $\mathbb{F}$-subalgebra $A \in VLS(L)$ is normal and takes only two values:* $\mathbf{0}$ *and* $\mathbf{1}$.

*Proof.* Let $A \in VLS(L)$ be maximal. Then $A^+$ is a non-constant maximal element of the poset $(\mathcal{N}(L), \subseteq)$ and, by Theorem 5.13, the possible values of $V_A^+(x)$ are $\mathbf{0}$ and $\mathbf{1}$, that is, $t_A^+$ takes only two values 0 and 1. Clearly,

$t_A^+(x) = 1$ if and only if $t_A(x) = t_A(0) = 0$; $t_A^+(x) = 0$ if and only if $t_A(x) = t_A(0) = 1$. But $A \subseteq A^+$ implies $t_A(x) \leqslant t_A^+(x)$ for all $x \in L$. Hence, $t_A^+(x) = 0$ implies $t_A(x) = 0$. Consequently, $V_A(0) = 1$. □

**Theorem 5.16.** *A level subset of a maximal $A \in VLS(L)$ is a maximal Lie subalgebra of $L$.*

*Proof.* Let $S$ be a level subset of a maximal $A \in VLS(L)$, i.e., $S = L = \{x \in L \,|\, V_A(x) = 1\}$. It is not difficult to verify that $S$ is a Lie subalgebra of $L$. Obviously $S \neq L$ because $V_A$ takes only two values. Let $M$ be a Lie subalgebra of $L$ containing $S$. Then $V_S \subseteq V_M$. Since $V_A = V_S$ and $V_A$ takes only two values, $V_M$ also takes only these two values. But, by our assumption, $A \in VLS(L)$ is maximal so that $V_S = V_A = V_M$ or $V_M(x) = 1$, for all $x \in L$. In the last case, we have $S = L$ which is impossible. So, we must have $V_A = V_S = V_M$ which implies that $S = M$. This means that $S$ is a maximal Lie subalgebra of $L$. □

**Definition 5.17.** A normal vague Lie $\mathbb{F}$-subalgebra $A \in VLS(L)$ is called *completely normal* if there exists $x \in L$ such that $A(x) = \mathbf{0}$. The set of all completely normal $A \in VLS(L)$ is denoted by $\mathcal{C}(L)$. Clearly, $\mathcal{C}(L) \subseteq \mathcal{N}(L)$.

**Theorem 5.18.** *A non-constant maximal element of $(\mathcal{N}(L), \subseteq)$ is also a maximal element of $(\mathcal{C}(L), \subseteq)$.*

*Proof.* Let $A$ be a non-constant maximal element of $(\mathcal{N}(L), \subseteq)$. Then, by Theorem 5.13, $A$ takes only the values $\mathbf{0}$ and $\mathbf{1}$ and so $V_A(x_0) = \mathbf{1}$ and $V_A(x_1) = \mathbf{0}$, for some $x_0, x_1 \in L$. Hence $A \in \mathcal{C}(L)$. Assume that there exists $B \in \mathcal{C}(R)$ such that $A \subseteq B$. Then, it follows that $A \subseteq B$ in $\mathcal{N}(L)$. Since $A$ is maximal in $(\mathcal{N}(L), \subseteq)$ and $B$ is non-constant, we have $A = B$. Thus $A$ is maximal element of $(\mathcal{C}(L), \subseteq)$. This completes the proof. □

**Theorem 5.19.** *Every maximal $A \in VLS(L)$ is completely normal.*

*Proof.* Let $A \in VLS(L)$ be maximal. Then by Theorem 5.15, $A$ is normal and $A = A^+$ takes only two values $\mathbf{0}$ and $\mathbf{1}$. Since $A$ is non-constant, it follows that $V_A(x_0) = \mathbf{1}$ and $V_A(x_1) = \mathbf{0}$ for some $x_0, x_1 \in L$. Hence $A$ is completely normal, ending the proof. □

In closing this paper, we state a method of construction for a new normal vague Lie $\mathbb{F}$-subalgebra from an old one.

**Theorem 5.20.** *Let $f : [0, 1] \to [0, 1]$ be an increasing function and $A = (t_A, f_A)$ a vague set on a Lie algebra $L$. Then $A_f = (t_{A_f}, f_{A_f})$ defined by $t_{A_f}(x) = f(t_A(x))$ and $f_{A_f}(x) = f(f_A(x))$ is an vague Lie $\mathbb{F}$-subalgebra if and only if $A = (t_A, f_A)$ is an vague Lie $\mathbb{F}$-subalgebra. Moreover, if $f(t_A(0)) = 1$ and $f(f_A(0)) = 0$, then $A_f$ is normal.*

## References

[1] **A. A. Al-Rababah and R. Biswas**, *Rough vague sets in an approximation space*, Internat. J. Comput. Cognition **6** (2008), 60 – 63.

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

[3] **M. Akram**, *Fuzzy Lie ideals of Lie algebras with interval-valued membership function*, Quasigroups and Related Systems **16** (2008), 1 – 12.

[4] **M. Akram and W. A. Dudek**, *Intuitionistic fuzzy left k-ideals of semirings*, Soft Computing **12** (2008), 881 – 890.

[5] **M. Akram and K. P. Shum**, *Intuitionistic fuzzy Lie algebras*, Southeast Asian Bull. Math. **31** (2007), 843 – 855.

[6] **R. Biswas**, *Vague groups*, Internat. J. Comput. Cognition **4** (2006), 20 – 23.

[7] **R. Crist and J. N. Mordeson**, *Vague rings*, New Math. Neutral Comput. **1** (2005), 215 – 228.

[8] **W. A. Dudek and Y. B. Jun**, *Normalizations of fuzzy BCC-ideals in BCC-algebras*, Math. Moravica **3** (1999), 17 – 24.

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

[10] **W. L. Gau and D. J. Buehrer**, *Vague sets*, IEEE Transactions on Systems, Man and Cybernetics **23** (1993), 610 – 614.

[11] **W. Gu and T. Lu**, *Fuzzy algebras over fuzzy fields redefined*, Fuzzy Sets and Systems **53** (1993), 105 – 107.

[12] **S. Nanda**, *Fuzzy algebra over a fuzzy field*, Fuzzy Sets and Systems **37** (1990), 99 – 103.

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

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

Received August 31, 2009

M.Akram
Punjab University College of Information Technology, University of the Punjab, Old Campus, P. O. Box 54000, Lahore, Pakistan.
E-mail: m.akram@pucit.edu.pk, makrammath@yahoo.com
K.P.Shum
Department of Mathematics, The University of Hong Kong, Pokulam Road, Hong Kong, China (SAR). E-mail: kpshum@math.hku.edu.hk

Quasigroups and Related Systems **17** (2009), 135 – 148

# A probabilistic model of error-detecting codes based on quasigroups

*Verica Bakeva and Nataša Ilievska*

**Abstract.** Error-detecting codes are used to detect errors when messages are transmitted through a noisy communication channel. We propose a new model of error-detecting codes based on quasigroups. In order to detect errors, we extend an input block $a_1a_2\dots a_n$ to a block $a_1a_2\dots a_nb_1b_2\dots b_n$, where $b_i = a_i * a_{r_{i+1}} * a_{r_{i+2}} * a_{r_{i+k-1}}$, $i = 1, 2, \dots, n$ where $*$ is a quasigroup operation and $r_j = \begin{cases} j, & j \leqslant n \\ j \mod n, & j > n \end{cases}$. We calculate an approximate formula which gives the probability that there will be errors which will not be detected in two special cases: for the set $A = \{0, 1\}$ and $k = 4$; and for the set $A = \{0, 1, 2, 3\}$ and $k = 2$. We find the optimal block length such that the probability of undetected errors is smaller than some previous given value $\varepsilon$. Also, we compare two considered codes and conclude that quasigroups of higher order give smaller probability of undetected errors. At the end of this paper we give a classification of quasigroups of order 4 according to goodness for proposed codes.

## 1. Introduction

We propose a new model of error-detecting codes based on quasigroup operations. Recall that a quasigroup $(Q, *)$ is a groupoid (i.e., algebra with one binary operation $*$ on the set $Q$) satisfying the law:

$$(\forall u, v \in Q)(\exists! x, y \in Q) \quad (x * u = v \ \&\ u * y = v) \tag{1}$$

In fact (1) says that the equations $x * u = v$, $u * y = v$ for each given $u, v \in Q$ and $x, y$ unknown, have unique solutions.

In paper [1], using the image pattern authors gave classification of quasigroups of order 4 as fractal and non-fractal. In paper [2], the following definition of linear quasigroup is given. Let $(Q, *)$ be a quasigroup of order $2^n$ and let

2000 Mathematics Subject Classification: 68P30

Keywords: error-detecting codes, quasigroup, noisy channel, probability of undetected errors

$$f(x_1,\dots,x_n) = (f_1(x_1,\dots,x_n),\dots,f_n(x_1,\dots,x_n))$$

be its corresponding representation as vector valued Boolean function. If all $f_i$ for $i = 1,2,\dots,n$ are linear polynomials, then this quasigroup is called linear quasigroup. Otherwise, if there exists function $f_i$ for some $i = 1,2,\dots,n$ which is not linear, this quasigroup is called nonlinear quasigroup.

In papers [4] and [5], there are some design of codes based on quasigroups of order 2. Here, we define the code design based on quasigroups of arbitrary order (Section 2). In Section 3, we find the probability of undetected errors for the codes based on quasigroups of order 2 and $k = 4$ where $k$ is number of symbols used in calculation of each redundancy symbol. On the same way, in Section 4, we give the probability of undetected errors for the codes based on quasigroups of order 4 and $k = 2$. We filter the 576 quasigroups of order 4 such that the probability of undetected errors does not depend of the input message. On that way, we obtain 160 quasigroups. In Section 5, we describe how to choose the block length $n$ such that the probability of undetected errors is smaller than a given value $\varepsilon$. Also, we compare the maximums of the obtained probability functions of undetected errors for two considered codes and make some conclusions. In Section 6, we give a classification of obtained 160 quasigroups according to their goodness for our codes.

## 2. Designing of the codes

Let $A$ be an arbitrary finite set called alphabet and $(A,*)$ be a given quasigroup. Let consider an input message

$$a_1a_2\dots a_na_{n+1}a_{n+2}\dots a_{2n}a_{2n+1}\dots, \qquad (a_i \in A,\ i = 1,2,\dots)$$

which will be transmitted through a noisy channel. Since of the noise, the received message can be different of the sent one. Our goal is designing a code which will detect the errors during transmission such that the probability of undetected errors will be as small as possible. For that reason, we have to add some redundancy to the message, i.e., some control bits.

Let divide the input message to blocks with length $n$:

$$a_1a_2\dots a_n, \quad a_{n+1}a_{n+2}\dots a_{2n},\ \dots$$

We extend each block $a_1a_2\dots a_n$ to a block $a_1a_2\dots a_nb_1b_2\dots b_n$ where

$$\begin{array}{lcl} b_1 & = & a_1 * a_2 * \cdots * a_k \\ b_2 & = & a_2 * a_3 * \cdots * a_{k+1} \\ \ldots & \ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\ b_n & = & a_n * a_1 * \cdots * a_{k-1} \end{array} \tag{2}$$

where $k \leqslant n$.

At first, each letter from the extended block $a_1 a_2 \ldots a_n b_1 b_2 \ldots b_n$ will be presented in 2-base system. After that the obtained binary block will be transmitted through the binary symmetrical channel with probability of bit error $p$ $(0 < p < 0.5)$ (Figure 1)

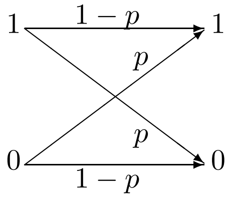

Figure 1: Binary symmetrical channel

The rate of this code is 1/2. Because of the noises in the channel, some of the characters may not be correctly transmitted. Let $a_i$ be transmitted as $a'_i$, $b_i$ as $b'_i$, $i \in \{1, 2, \ldots, n\}$. If the character transmission is correct than $a'_i$ will have the same value as $a_i$. Otherwise, $a'_i$ will not be the same as $a_i$. So, the output message is $a'_1 a'_2 \ldots a'_n b'_1 b'_2 \ldots b'_n$. To check if there are any errors during transmission, the receiver of the message checks if

$$\begin{array}{lcl} b'_1 & = & a'_1 * a'_2 * \cdots * a'_k \\ b'_2 & = & a'_2 * a'_3 * \cdots * a'_{k+1} \\ \ldots & \ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\ b'_n & = & a'_n * a'_1 * \cdots * a'_{k-1} \end{array}$$

If any of these equalities are not satisfied, the receiver concludes that some errors occured during the block transmission and it asks from the sender to send that block once again. But, some equality can be satisfied although some characters in that equality are incorrectly transmitted. In that case, incorrect transmission (error in transmission) will not be detected. We will consider two special cases of the proposed code. For the first one, we choose $A = \{0, 1\}$ and $k = 4$ and for the second one, $A = \{0, 1, 2, 3\}$ and $k = 2$. Our goal is finding approximately the probability of undetected errors and make that probability as small as possible. In the both codes, each redundant symbol $b_i$, defined in (2), includes the same number of bits, i.e., 4 bits from the input message, so it is reasonably to compare the obtained probabilities of undetected errors.

## 3. An error-detecting code based on quasigroup of order 2 and k=4

Let consider the binary set $A = \{0,1\}$. There are only two quasigroup operations on the set A, and here we took $(A,*)$ to be defined by the table

| * | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

Denote that same results will be obtained if another quasigroup is used.

Each block $a_1a_2\dots a_n$ $(a_i \in A)$ is extended to a block

$$a_1a_2\dots a_nb_1b_2\dots b_n,$$

where $b_i = a_i * a_{r_{i+1}} * a_{r_{i+2}} * a_{r_{i+3}}$. Here

$$r_j = \begin{cases} j, & j \leqslant n \\ j(\operatorname{mod} n), & j > n \end{cases}$$

for $j = i+1, i+2, i+3$.

Let introduce the following notation:

$$g(x_1,x_2,\dots,x_n) = x_1 * x_2 * \cdots * x_n,$$

where $x_i \in \{0,1\}$, $i = 1,2,\dots,n$. In order to determine the probability of undetected errors, we need the following proposition which proof is obvious.

**Proposition 1.** *If odd number of $x_1,x_2,\dots,x_n$ $(x_i \in \{0,1\})$ change their values then $g(x_1,x_2,\dots,x_n)$ will change its value, too. If even number of $x_1,x_2,\dots,x_n$ change their values then the value of $g(x_1,x_2,\dots,x_n)$ will be unchanged.* □

Using the previous proposition and some combinatorics the following theorem can be proved.

**Theorem 1.** *Let $f_2(n,p)$ be the probability function of undetected errors in a transmitted block with length $n$ through the binary symmetric channel where $p$ is the probability of incorrect transmission of a bit. Then $f_2(n,p)$ is given by the following formulas:*

$$\begin{aligned}
f_2(4,p) &= 6p^2(1-p)^6 + p^4(1-p)^4 + 4p^5(1-p)^3 + 4p^7(1-p)\\
f_2(5,p) &= 10p^4(1-p)^6 + 16p^5(1-p)^5 + 5p^8(1-p)^2\\
f_2(6,p) &= 2p^3(1-p)^9 + 6p^4(1-p)^8 + 18p^5(1-p)^7\\
&\quad +16p^6(1-p)^6 + 6p^7(1-p)^5 + 9p^8(1-p)^4 + O(p^9)\\
f_2(7,p) &= 7p^4(1-p)^{10} + 21p^5(1-p)^9 + 21p^6(1-p)^8 + 29p^7(1-p)^7\\
&\quad +28p^8(1-p)^6 + O(p^9)\\
f_2(8,p) &= 14p^4(1-p)^{12} + 8p^5(1-p)^{11} + 24p^6(1-p)^{10} + 56p^7(1-p)^9\\
&\quad +49p^8(1-p)^8 + O(p^9)\\
f_2(9,p) &= 9p^4(1-p)^{14} + 9p^5(1-p)^{13} + 36p^6(1-p)^{12} + 81p^7(1-p)^{11}\\
&\quad +63p^8(1-p)^{10} + O(p^9)\\
f_2(10,p) &= 10p^4(1-p)^{16} + 12p^5(1-p)^{15} + 20p^6(1-p)^{14} + 100p^7(1-p)^{13}\\
&\quad +120p^8(1-p)^{12} + O(p^9)\\
f_2(11,p) &= 11p^4(1-p)^{18} + 11p^5(1-p)^{17} + 22p^6(1-p)^{16} + 99p^7(1-p)^{15}\\
&\quad +132p^8(1-p)^{14} + O(p^9)\\
f_2(12,p) &= 12p^4(1-p)^{20} + 12p^5(1-p)^{19} + 30p^6(1-p)^{18} + 72p^7(1-p)^{17}\\
&\quad +162p^8(1-p)^{16} + O(p^9)\\
f_2(13,p) &= 13p^4(1-p)^{22} + 13p^5(1-p)^{21} + 26p^6(1-p)^{20} + 78p^7(1-p)^{19}\\
&\quad +182p^8(1-p)^{18} + O(p^9)\\
f_2(n,p) &= np^4(1-p)^{2n-4} + np^5(1-p)^{2n-5} + 2np^6(1-p)^{2n-6}\\
&\quad +6np^7(1-p)^{2n-7} + Ap^8(1-p)^{2n-8} + Bp^{n/2}(1-p)^{3n/2} + O(p^9),\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \textit{for } n \geqslant 14,
\end{aligned}$$

*where*

$$A = \begin{cases} \dfrac{(n+9)n}{2}, & n = 15, 17, 19, \dots \\ \dfrac{(n+8)n}{2}, & n = 14, 16, 18, \dots \end{cases} \qquad B = \begin{cases} 0, & n \text{ odd} \\ 2, & n \text{ even, but } 4\dagger n \\ 6, & 4|n \end{cases}$$

□

The remainder $O(p^9)$ denotes that the coefficients are exactly determined in terms which contain $p^i$, $i < 9$. To obtain exactly the probability of undetected errors, i.e., to obtain exactly $O(p^9)$, one has to make much complicated combinatorial calculations. In the Figure 2, we can see that for small values of $n$, all functions have maximum in $p = 0,5$. When the block length $n$ increases, the maximum becomes smaller, it goes to the left and the sequence of maximums converges to 0.

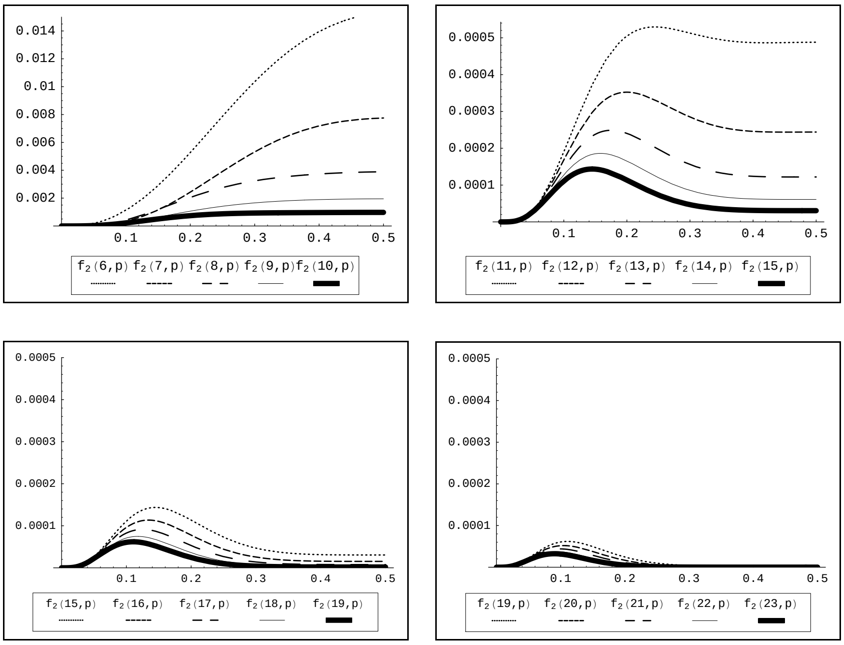

Figure 2: The probability functions of undetected errors

## 4. An error-detecting code based on quasigroup of order 4 and k=2

Let consider the set $A = \{0, 1, 2, 3\}$ and let $*$ be an arbitrary quasigroup operation on $A$. According to (2), we extend each block $a_1a_2 \dots a_n$ $(a_i \in A)$ to a block $a_1a_2 \dots a_nb_1b_2 \dots b_n$, where $b_i = a_i * a_{(i \mod n)+1}$, $i = 1, 2, \dots, n$. The extended message is transmitted through the binary symmetrical channel again. As previous, we want to calculate the probability that there will be errors which will not be detected. There are 576 quasigroups of order 4. We find that for some quasigroups, the probability of undetected errors depends on the distribution of letters in the input message. So, we filtered the quasigroups such that this formula is independent from the distribution of the input message. After filtering, from the 576 quasigroups of order 4, only 160 quasigroups remain. All of them are fractal quasigroups, but not all fractal quasigroups are in these 160 quasigroups ([1]). For the filtered 160 quasigroups, we obtained a formula for calculating the probability function of undetected errors. It is given by the following theorem which proof is done in [3].

**Theorem 2.** *Let $f_4(n,p)$ be the probability of undetected errors in a transmitted block with length $n$ through the binary symmetric channel where $p$ is the probability of incorrect transmission of a bit. If one of the filtered 160 quasigroups is used for designing the code, then the probability of undetected errors is given by the following formulas:*

$$\begin{aligned}
f_4(2,p) &= 2v_0v_1 + r_2\\
f_4(3,p) &= 3v_0^3v_1 + 3v_0v_2 + r_3\\
f_4(4,p) &= 4v_0^5v_1 + 4v_0^3v_2 + 2v_0^2v_1^2 + 4v_0v_3 + r_4\\
f_4(n,p) &= nv_1v_0^{2n-3} + nv_2v_0^{2n-5} + \frac{n(n-3)}{2}v_1^2v_0^{2n-6} + nv_3v_0^{2n-7}\\
&\quad + n(n-4)v_2v_1v_0^{2n-8} + \frac{n(n-4)(n-5)}{6}v_1^3v_0^{2n-9} + nv_4v_0^{2n-9}\\
&\quad + n(n-5)v_3v_1v_0^{2n-10} + \frac{n(n-5)}{2}v_2^2v_0^{2n-10}\\
&\quad + \frac{n(n-5)(n-6)}{2}v_2v_1^2v_0^{2n-11} + \frac{n(n-5)(n-6)(n-7)}{24}v_1^4v_0^{2n-12},
\end{aligned}$$

*for $n \geqslant 5$. In the formulas, we use the following notations:*
*$v_k$ - the probability of undetected errors when exactly $k$ consecutive characters of the initial message $a_1a_2\dots a_n$ are incorrectly transmitted (the characters $a_i, a_{i+1}, \dots, a_{i+k-1}$ are incorrectly transmitted, but $a_{i-1}$ and $a_{i+k}$ are correctly transmitted), $k = 1,2,3,4$;*
*$v_0$ - the probability of correct transmission of a character;*
*$r_k$ - the probability of undetected errors in a block with length $k$ if all $k$ characters are incorrectly transmitted, $k = 2,3,4$.* □

Now, using the Theorem 2 and formulas for the probabilities $v_k$, functions $f_4(n,p)$ can be determined for all 160 fractal quasigroups. These 160 quasigroups do not define 160 different functions for the probability of undetected errors, but only 7. These functions are given in Section 6 (Figure 5) where using these functions, we give a classification of the quasigroups of order 4 according to goodness for our codes.

The quasigroups which give the smallest probability of undetected errors are the best for code design. For these quasigroups, using some combinatorics we calculate the following expressions for $v_i$ and $r_j$.

$$\begin{aligned}
v_0 &= (1-p)^2\\
v_1 &= 3(1-p)^2p^4\\
v_2 &= (1-p)^2p^4(9p^4-16p^3+12p^2-4p+1)\\
v_3 &= (1-p)^2p^6(3p^2-4p+2)(9p^4-20p^3+18p^2-8p+2)\\
v_4 &= (1-p)^2p^8(81p^8-432p^7+1060p^6-1548p^5+1475p^4-944p^3+400p^2\\
&\quad -104p+13)\\
r_2 &= p^4(9p^4-32p^3+48p^2-32p+8)\\
r_3 &= p^4(27p^8-144p^7+348p^6-484p^5+429p^4-252p^3+98p^2-24p+3)\\
r_4 &= p^6(81p^{10}-576p^9+1904p^8-3792p^7+5012p^6-4576p^5+2928p^4-1312p^3\\
&\qquad +404p^2-80p+8)
\end{aligned}$$

Now, the probability of undetected errors is determined by the following formulas:

$$\begin{aligned}
f_{4,1}(2,p) &= p^4(15p^4-56p^3+84p^2-56p+14)\\
f_{4,1}(3,p) &= p^4(63p^8-372p^7+990p^6-1540p^5+1545p^4-1032p^3+452p^2\\
&\quad -120p+15)\\
f_{4,1}(4,p) &= p^4(255p^{12}-2032p^{11}+7560p^{10}-17360p^9+27556p^8-32112p^7\\
&\quad +28440p^6-19440p^5+10206p^4-4000p^3+1104p^2-192p+16)\\
f_{4,1}(n,p) &= np^4(1-p)^{2(2n-8)}\times\\
&\quad \times\Big[4-48p+274p^2-980p^3+(8n+2431)p^4-8(8n+547)p^5\\
&\qquad +2(130n+2853)p^6-4(166n+1259)p^7+(9n^2+1078n+2297)p^8\\
&\qquad -4(9n^2+270n-139)p^9+(81n^2+371n-890)p^{10}\\
&\qquad -2(45n^2-165n+194)p^{11}+(3/8)(9n^3-42n^2+75n-34)p^{12}\Big]\\
&\quad +O(p^7), \qquad \text{for } n\geqslant 5.
\end{aligned}$$

The function $f_{4,1}(n,p)$ without the remainder $O(p^7)$ gives the probability that at most 4 characters of the input message are incorrectly transmitted and the errors are not detected. As previous, to obtain the probability of undetected errors exactly, one has to calculate the probability that more than 4 characters are incorrectly transmitted and the errors are not detected, which is much complicated combinatorial problem. The shape of the probability functions of undetected errors is similar as in the previous case. When the block length $n$ increases the maximum of these functions becomes smaller, it goes to the left and the sequence of maximums converges to 0 (Figure 3).

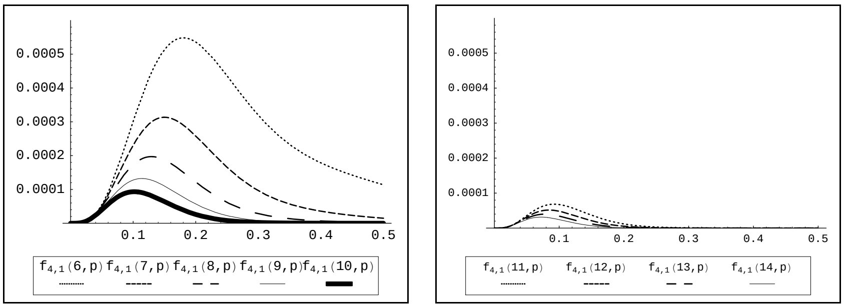

Figure 3: The probability functions of undetected errors

## 5. Controlling of undetected errors and comparing of the previous two codes

We want to control the probability of undetected errors, actually to make that probability smaller than some previous given value $\varepsilon$. So, we can find for which values of $n$ the maximum of the function $f(n,p)$ ($f(n,p)$ can be $f_2(n,p)$ or $f_{4,1}(n,p)$) is smaller then $\varepsilon$. Since the sequence of maximums of the functions $f(n,p)$ is strictly decreasing and converges to 0 when $n \to \infty$, there will be $n_0 \in \mathbb{N}$, such that the maximum of the function $f(n,p)$ will be smaller than $\varepsilon$, for all $n \geqslant n_0$ and the maximum of the function $f(n,p)$ will be greater than $\varepsilon$, for all $n < n_0$. We choose $n = n_0$ (see Figure 4).

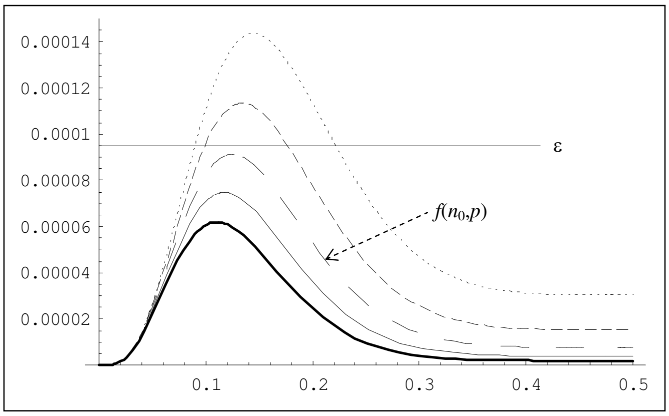

Figure 4: Choosing of $n_0$

Now, we separate the message in blocks with length $n$ and we code every block individually. From all values of $n$ which satisfies the condition $f(n,p) < \varepsilon$, we choose the smallest one since in this case we have fastest transmission. Namely, if the receiver detects errors in the received block, it asks for repeated transmission, so it is better the block length to be as small as possible.

In the Table 1, we give the maximums of the probability functions of undetected errors for the first and the second proposed code. From this table, we can conclude that the maximums of the functions of undetected errors are smaller when the quasigroups of order 4 are used. It suggest that using the quasigroup of order 4 we obtain better and more efficiently codes.

| $n$ | Quasigroups of order 2 | Quasigroups of order 4 |
|---|---|---|
| 10 | $9.75609 \times 10^{-4}$ | $9.35406 \times 10^{-5}$ |
| 11 | $5.29529 \times 10^{-4}$ | $6.82458 \times 10^{-5}$ |
| 12 | $3.52349 \times 10^{-4}$ | $5.14707 \times 10^{-5}$ |
| 13 | $2.48784 \times 10^{-4}$ | $3.97896 \times 10^{-5}$ |
| 14 | $1.86131 \times 10^{-4}$ | $3.14013 \times 10^{-5}$ |
| 15 | $1.43616 \times 10^{-4}$ | $2.52198 \times 10^{-5}$ |
| 16 | $1.13480 \times 10^{-4}$ | $2.05631 \times 10^{-5}$ |
| 17 | $9.13489 \times 10^{-5}$ | $1.69878 \times 10^{-5}$ |
| 18 | $7.47017 \times 10^{-5}$ | $1.41968 \times 10^{-5}$ |
| 19 | $6.19084 \times 10^{-5}$ | $1.19860 \times 10^{-5}$ |
| 20 | $5.19030 \times 10^{-5}$ | $1.02120 \times 10^{-5}$ |
| 21 | $4.39585 \times 10^{-5}$ | $8.77182 \times 10^{-6}$ |
| 22 | $3.75666 \times 10^{-5}$ | $7.59050 \times 10^{-6}$ |
| 23 | $3.23631 \times 10^{-5}$ | $6.61231 \times 10^{-6}$ |
| 24 | $2.80827 \times 10^{-5}$ | $5.79537 \times 10^{-6}$ |
| 25 | $2.45283 \times 10^{-5}$ | $5.10775 \times 10^{-6}$ |
| 26 | $2.15517 \times 10^{-5}$ | $4.52483 \times 10^{-6}$ |

Table 1: The maximums of the probability functions

## 6. Classification of quasigroups of order 4 according to goodness for proposed codes

As we mentioned in Section 4 we filtered 576 quasigroups of order 4 such that the probability of undetected errors does not depend on the distribution of letters in the input messages. After filtering only 160 quasigroups remain and they give 7 different functions of probability of undetected errors. The best of these functions is $f_{4,1}(n,p)$ given in Section 4. Others are given with the following formulas.

$$\begin{array}{rcl}
f_{4,2}(2,p) & = & (1-p)^2p^2(3p^2-4p+2)(5p^2-2p+1)\\
f_{4,2}(3,p) & = & 3(1-p)^4p^4(21p^4-40p^3+44p^2-24p+6)\\
f_{4,2}(4,p) & = & (1-p)^4p^4(255p^8-1012p^7+1982p^6-2468p^5+2145p^4-1320p^3+556p^2\\
 & & -144p+18)\\
f_{4,2}(n,p) & = & np^4(1-p)^{2(2n-8)}\times\\
 & & \times\Big[4-48p+275p^2-990p^3+(8n+2475)p^4-8(8n+561)p^5\\
 & & \quad +2(130n+2943)p^6-4(166n+1305)p^7+(9n^2+1078n+2409)p^8\\
 & & \quad -4(9n^2+270n-131)p^9+(81n^2+371n-890)p^{10}\\
 & & \quad -2(45n^2-165n+194)p^{11}+(3/8)(9n^3-42n^2+75n-34)p^{12}\Big]\\
 & & +O(p^7), \qquad \text{for } n\geqslant 5.
\end{array}$$

$$\begin{array}{rcl}
f_{4,3}(2,p) & = & p^2(-p^6+8p^5-12p^4+8p^3-p^2-2p+1)\\
f_{4,3}(3,p) & = & p^3(-p^9+12p^8-66p^7+220p^6-411p^5+456p^4-312p^3+132p^2-33p+4)\\
f_{4,3}(4,p) & = & p^3(-p^{13}+16p^{12}-120p^{11}+560p^{10}-1628p^9+3216p^8-4568p^7+4800p^6\\
 & & -3765p^5+2188p^4-918p^3+264p^2-47p+4)\\
f_{4,3}(n,p) & = & (1/24)np^3(1-p)^{2(2n-10)}\times\\
 & & \times\Big[24-384p+2952p^2+12(n-1203)p^3-48(3n-1045)p^4+48(18n-2731)p^5\\
 & & +4(n^2-837n+66488)p^6-8(4n^2-1158n+53327)p^7\\
 & & +4(37n^2-4845n+136880)p^8+(n^3-446n^2+31259n-566302)p^9\\
 & & -4(n^3-226n^2+9701n-118268)p^{10}+2(5n^3-658n^2+18469n-159020)p^{11}\\
 & & -4(4n^3-347n^2+6665n-42412)p^{12}+(19n^3-1078n^2+14453n-69890)p^{13}\\
 & & -4(4n^3-149n^2+1433n-5314)p^{14}+2(5n^3-116n^2+817n-2302)p^{15}\\
 & & -4(n^3-14n^2+71n-154)p^{16}+(n^3-10n^2+35n-50)p^{17}\Big]\\
 & & +O(p^7), \qquad \text{for } n\geqslant 5.
\end{array}$$

$$\begin{array}{rcl}
f_{4,4}(2,p) & = & (1-p)^2p^3(-p^3+6p^2-7p+4)\\
f_{4,4}(3,p) & = & (1-p)^3p^3(p^6-9p^5+36p^4-44p^3+30p^2-12p+3)\\
f_{4,4}(4,p) & = & (1-p)^4p^3(-p^9+12p^8-66p^7+220p^6-399p^5+440p^4-300p^3+128p^2-32p+4)\\
f_{4,4}(n,p) & = & (1/24)np^3(1-p)^{2(2n-10)}\times\\
 & & \times\Big[24-384p+2976p^2+12(n-1229)p^3-144(n-361)p^4+24(37n-5729)p^5\\
 & & +4(n^2-891n+70274)p^6-4(8n^2-2535n+113035)p^7\\
 & & +8(20n^2-2709n+72514)p^8+(n^3-530n^2+35747n-601066)p^9\\
 & & -4(n^3-289n^2+11342n-126548)p^{10}+2(5n^3-880n^2+21883n-172004)p^{11}\\
 & & -16(n^3-119n^2+1979n-11494)p^{12}+(19n^3-1474n^2+17129n-74834)p^{13}\\
 & & -4(4n^3-197n^2+1721n-5698)p^{14}+10(n^3-28n^2+197n-518)p^{15}\\
 & & -4(n^3-14n^2+71n-154)p^{16}+(n^3-10n^2+35n-50)p^{17}\Big]\\
 & & +O(p^7), \qquad \text{for } n\geqslant 5.
\end{array}$$

$$\begin{array}{rcl}
f_{4,5}(2,p) & = & (1-p)p^2(p^5+9p^4-19p^3+17p^2-8p+2)\\
f_{4,5}(3,p) & = & (1-p)^3p^3(p^6-9p^5+36p^4-60p^3+54p^2-24p+5)\\
f_{4,5}(4,p) & = & (1-p)^2p^3(-p^{11}+14p^{10}+37p^9-276p^8+567p^7-526p^6+125p^5+216p^4-252p^3\\
 & & +128p^2-34p+4)
\end{array}$$

$$
\begin{array}{rcl}
f_{4,5}(n,p) & = & (1/24)np^3(1-p)^{2(2n-10)}\times \\
& & \times\Big[24 - 330p + 2544p^2 + 12(n-933)p^3 - 24(5n-1424)p^4 + 12(47n-6355)p^5 \\
& & +4(n^2-411n+31844)p^6 - 4(5n^2-849n+39922)p^7 \\
& & +4(7n^2-1431n+37058)p^8 + (n^3+82n^2+8855n-100714)p^9 \\
& & -4(n^3+116n^2+3131n-14012)p^{10} + 2(5n^3+518n^2+7177n-20420)p^{11} \\
& & -4(4n^3+361n^2+2777n-9916)p^{12} + (19n^3+1334n^2+4385n-28466)p^{13} \\
& & -4(4n^3+205n^2-133n-2602)p^{14} + 2(5n^3+148n^2-647n-286)p^{15} \\
& & -4(n^3+10n^2-97n+134)p^{16} + (n^3-10n^2+35n-50)p^{17}\Big] \\
& & +O(p^7), \qquad \text{for } n \geqslant 5.
\end{array}
$$

$$
\begin{array}{rcl}
f_{4,6}(2,p) & = & (1-p)^2p^2(-p^4+6p^3-3p^2+1) \\
f_{4,6}(3,p) & = & (1-p)^3p^3(p^6-9p^5+36p^4-52p^3+42p^2-18p+4) \\
f_{4,6}(4,p) & = & (1-p)^4p^3(-p^9+12p^8-66p^7+220p^6-319p^5+280p^4-180p^3+88p^2 \\
& & -27p+4) \\
f_{4,6}(n,p) & = & (1/24)np^3(1-p)^{2(2n-10)}\times \\
& & \times\Big[24 - 360p + 2592p^2 + 12(n-995)p^3 - 120(n-329)p^4 + 12(51n-8297)p^5 \\
& & +4(n^2-537n+49598)p^6 - 20(n^2-285n+15938)p^7 \\
& & +4(13n^2-2955n+104282)p^8 + (n^3-110n^2+19199n-445066)p^9 \\
& & -4(n^3-52n^2+6047n-96152)p^{10} + 2(5n^3-178n^2+11749n-133004)p^{11} \\
& & -4(4n^3-119n^2+4349n-36172)p^{12} + (19n^3-490n^2+9761n-60338)p^{13} \\
& & -4(4n^3-89n^2+1013n-4594)p^{14} + 2(5n^3-92n^2+649n-2014)p^{15} \\
& & -4(n^3-14n^2+71n-154)p^{16} + (n^3-10n^2+35n-50)p^{17}\Big] \\
& & +O(p^7), \qquad \text{for } n \geqslant 5.
\end{array}
$$

$$
\begin{array}{rcl}
f_{4,7}(2,p) & = & (1-p)^2p^2(1+p)(-p^3+7p^2-6p+2) \\
f_{4,7}(3,p) & = & (1-p)^4p^3(4-p)(p^4-4p^3+12p^2-8p+2) \\
f_{4,7}(4,p) & = & (1-p)^4p^3(-p^3+6p^2-7p+4)(p^6-6p^5+23p^4-36p^3+30p^2-12p+2) \\
f_{4,7}(n,p) & = & (1/24)np^3(1-p)^{2(2n-12)}\times \\
& & \times\Big[48 - 960p + 9168p^2 + 24(2n-2319)p^3 - 48(16n-5021)p^4 \\
& & +48(122n-16489)p^5 + 16(2n^2-1785n+127894)p^6 \\
& & -24(16n^2-4188n+178017)p^7 + 48(42n^2-5635n+152925)p^8 \\
& & +4(4n^3-1492n^2+142127n-2630189)p^9 \\
& & -48(4n^3-224n^2+19395n-263790)p^{10} \\
& & +48(22n^3-263n^2+24382n-265501)p^{11} \\
& & -8(436n^3-1819n^2+139409n-1320164)p^{12} \\
& & +144(53n^3-208n^2+5721n-49048)p^{13} \\
& & -48(240n^3-1285n^2+11191n-79021)p^{14} \\
& & +4(3030n^3-21073n^2+94395n-427394)p^{15} \\
& & -24(366n^3-3035n^2+11013n-29366)p^{16} \\
& & +12(354n^3-3268n^2+11509n-21701)p^{17} \\
& & -8(163n^3-1588n^2+5591n-8906)p^{18} + 12(20n^3-199n^2+699n-1030)p^{19} \\
& & -24(n^3-10n^2+35n-50)p^{20} + (n^3-10n^2+35n-50)p^{21}\Big] \\
& & +O(p^7), \qquad \text{for } n \geqslant 5.
\end{array}
$$

The plots of the previous functions for $n = 7$ are given on the Figure 5. We can see that the function $f_{4,1}(n,p)$ is the best one, it gives the smallest probability of undetected errors. But the function $f_{4,2}(n,p)$ is very closed to the $f_{4,1}(n,p)$. Their plots almost overlap each other. Using functions

$f_{4,i}(n,p)$ for $i = 1, \dots, 7$ we can classify remaining 160 quasigroups in 7 sets.

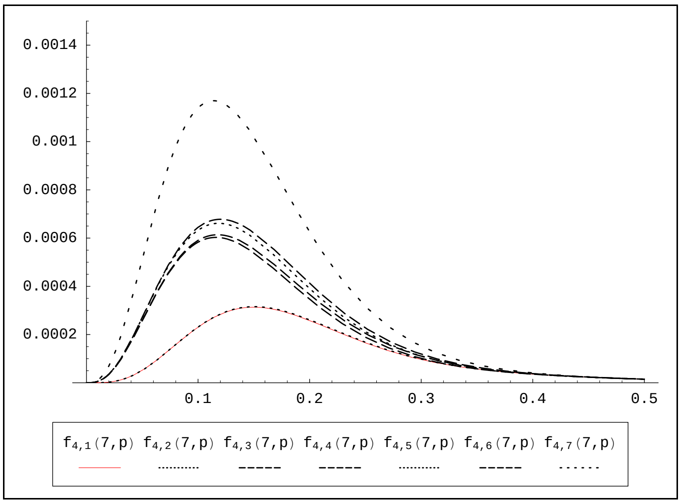

Figure 5: Seven different functions of probability of undetected errors

Each quasigroup is presented by a number according to lexicographic ordering of the set of quasigroups of order 4. Namely, each quasigroup is presented as a string of 16 letters that is a concatenation of the rows of the corresponding Latin square. Then lexicographic ordering of that strings is applied, assuming that the letters are already ordered. The obtained sets of quasigroups are ordered such that the quasigroups from the first set give the smallest, and the quasigroups from the last set give the biggest probability of undetected errors.

**Set 1:** 46, 92, 111, 127, 160, 213, 222, 274, 303, 355, 364, 417, 450, 466, 485, 531
**Set 2:** 43, 93, 101, 133, 157, 196, 235, 275, 302, 342, 381, 420, 444, 476, 484, 534
**Set 3:** 40, 80, 116, 138, 166, 206, 228, 269, 308, 349, 371, 411, 439, 461, 497, 537
**Set 4:** 14, 21, 37, 54, 71, 77, 100, 132, 163, 179, 192, 197, 234, 243, 253, 272, 305, 324, 334, 343, 380, 385, 398, 414, 445, 477, 500, 506, 523, 540, 556, 563
**Set 5:** 27, 83, 113, 139, 146, 203, 229, 285, 292, 348, 374, 431, 438, 464, 494, 550
**Set 6:** 4, 24, 26, 60, 70, 82, 110, 126, 147, 169, 182, 212, 223, 252, 262, 284, 293, 315, 325, 354, 365, 395, 408, 430, 451, 467, 495, 507, 517, 551, 553, 573

Set 7 can be presented as union of two subsets:

**Subset $7'$:** 1, 11, 51, 57, 172, 189, 246, 259, 318, 331, 388, 405, 520, 526, 566, 576
**Subset $7''$:** 7, 9, 49, 63, 174, 185, 242, 263, 314, 335, 392, 403, 514, 528, 568, 570

Repeat that all of these 160 quasigroups are fractal. The sets 1-6 contain only linear fractal quasigroups. The set 7 contains two subsets such that the subset $7'$ contains linear fractal quasigroups too, but the subset $7''$ contains 16 nonlinear fractal quasigroups with nonlinear part $x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4$ (see [2]). Also, one can check that there is not quasigroup in Set 1 which is a group.

## 7. Conclusion

In this paper we compare two special cases of these codes: the first one with the binary set $A = \{0, 1\}$ and $k = 4$ and the second one with the set $A = \{0, 1, 2, 3\}$ and $k = 2$. In the both codes, each control bit includes 4 bits from the input message and the rates of the both codes are the same, so the comparing of two codes are reasonable. From this comparing we can conclude that the obtained results are much better when we use quasigroups of order 4. Also, in this paper we give a classification of quasigroups of order 4 according to goodness for proposed codes. Our next step is to develop some other codes based on quasigroups of order 4 or $2^k$ for $k \geqslant 3$, which give smaller probability of undetected errors.

**Acknowledgment.** We are particularly grateful to Professor Smile Markovski for the valuable ideas and suggestions while working of this paper.

## References

[1] **V. Dimitrova, S. Markovski**, *Classification of quasigroups by image patterns*, Proc. Fifth International Confer. Informatics and Information Technology, Bitola, Republic of Macedonia (2007), 152 – 160.

[2] **D. Gligoroski, V. Dimitrova, S. Markovski**, *Quasigroups as Boolean functons, their equation systems and Gröbner bases*, short-note for RISC Book Series, Springer, "Groebner, Coding, and Cryptography", Ed. T.Mora, L.Perret, S.Sakata, M.Sala, and C.Traverso (2009), 415-420.

[3] **N. Ilievska, V. Bakeva**, *A Model of error-detecting codes based on quasigroups of order 4*, Proc. Sixth International Confer. Informatics and Information Technology, Bitola, Republic of Macedonia (2008), 7 – 11.

[4] **S. Markovski, V. Bakeva**, *On Error-detecting codes based on quasigroup operation*, Proc. Fourth International Confer. Informatics and Information Technology, Bitola, Republic of Macedonia (2003), 400 – 405.

[5] **S. Markovski, V. Bakeva**, *Error-detecting codes with cyclically defined redundancy*, Proc. Third Congress of Math. of Macedonia (2005), 485 – 492.

Received September 2, 2009

Institute of Informatics, Faculty of Natural Sciences and Mathematics, P.O.Box 162,
Skopje, Republic of Macedonia
E-mail: {verica,natasha}@ii.edu.mk

Quasigroups and Related Systems **17** (2009), 149 – 160

# Pure ideals in ternary semigroups

*Shahida Bashir* and *Muhammad Shabir*

**Abstract.** In this paper we introduce the notions of pure ideals, weakly pure ideals in ternary semigroups. We also define purely prime ideals of a ternary semigroup and study some properties of these ideals. The space of purely prime two-sided ideal is topologized.

## 1. Introduction

Cayley and Sylvester along with several other mathematicians, in the 19th century considered ternary algebraic structures and cubic relations. The n-ary structures, which are the generalizations of ternary structures create hopes because of their possible applications in Physics. A few important physical applications have been recorded in [2, 3, 12, 19]. Ternary semigroups exhibit natural examples of ternary algebras.

Banach find some applications in ternary semigroup. He gave an example to show that a ternary semigroup is not necessarily reduce to an ordinary semigroup. Los [13] studied some properties of ternary semigroup and proved that every ternary semigroup can be embedded in a semigroup. Sioson at [18] introduced the ideal theory in ternary semigroups. He also introduced the notion of regular ternary semigroups and characterized them by using the properties of quasi-ideals. In [16], Santiago developed the theory of ternary semigroups and semiheaps. He studied regular and completely regular ternary semigroups. Dixit and Dewan studied quasi-ideals and bi-ideals in ternary semigroups at [5, 6]. Ternary regular semigroups are studied in [8] and [17]. The nice characterization of regularity by ideals is given in [8].

M. Shabir and A. Khan at [14] studied prime ideals and prime one sided ideals in semigroups. Ahsan and Takahashi at [1] have brought forwarded

2000 Mathematics Subject Classification: 20N05,

Keywords: Pure ideal, weakly pure ideal, purely prime ideal, weakly regular ternary semigroup.

the concept of pure and purely prime ideals in semigroups.

M. Shabir and S. Bashir at [15] launched prime ideals in ternary semigroups. At cite8 and [17] ternary and $n$-ary semigroups are given along with an immaculate characterization of regularity by their ideals. At [7] applications of ideals to the divisibility theory in ternary and $n$-ary semigroups is presented.

In this paper we start the study of pure ideals, weakly pure ideals and purely prime ideals in ternary semigroups. We characterize ternary semigroups by the properties of pure and weakly pure ideals.

## 2. Preliminaries

A non-empty set $T$ with a ternary operation ( ) is called a *ternary semigroup* if it satisfies the following associative law:

$$((x_1x_2x_3)x_4x_5) = (x_1(x_2x_3x_4)x_5) = (x_1x_2(x_3x_4x_5))$$

for all $x_i \in T$, $1 \leqslant i \leqslant 5$.

To avoid complexity we denote $(x_1x_2x_3)$ as $x_1x_2x_3$ and take the operation ( ) as multiplication. It is evident that each ordinary semigroup $(T, *)$ induces a ternary semigroup $(T, (\ ))$ by defining $(abc) = (a * b) * c$. Whereas in [13] it has been demonstrated that every ternary semigroup does not enjoy the status of an ordinary semigroup. A ternary semigroup $T$ is said to be a *ternary semigroup with zero* if there exists an element $0 \in T$ such that $0ab = a0b = ab0 = 0$ for all $a, b \in T$. Then 0 is called the *zero element* of $T$. If $A, B, C$ are non-empty subsets of a ternary semigroup $T$ then their product $ABC$ is defined as

$$ABC = \{abc : a \in A, b \in B \ \ and\ c \in C\}.$$

A non-empty subset $S$ of a ternary semigroup $T$ is called a *ternary subsemigroup* of $T$ if $SSS = S^3 \subseteq S$. A non-empty subset $A$ of a ternary semigroup $T$ is called a *left* (*right, lateral*) *ideal* of $T$ if $TTA \subseteq A$ ($ATT \subseteq A$, $TAT \subseteq A$). If $A$ is a left, right and lateral ideal of $T$, then it is called an *ideal* of $T$ and if $A$ is a left and right ideal of $T$, then it is called *two-sided ideal* of $T$. Lateral ideals are also known as *middle ideals*. It is clear that every left, right and lateral ideal is a ternary subsemigroup of $T$. An ideal $A$ of a ternary semigroup $T$ is called *idempotent* if $A^3 = AAA = A$. A ternary semigroup $T$ is called *semisimple* if each ideal of $T$ is idempotent.

An element $x \in T$ is *regular* if there exists an element $a \in T$ such that $x = xax$, that is $x \in xTx$. A ternary semigroup $T$ is *regular* if each element of $T$ is regular.

The intersection of all the left ideals of $T$ containing $X \subseteq T$ is the smallest left ideal of $T$ containing $X$. It is denoted by $\langle X\rangle_l$ and called the *left ideal generated by* $X$. Clearly $\langle X\rangle_l = X \cup XTT$.

Similarly,

$$\begin{aligned}\langle X\rangle_r &= X \cup TTX\\ \langle X\rangle_m &= X \cup TXT \cup TTXTT\\ \langle X\rangle_t &= X \cup TTX \cup XTT \cup TTXTT\\ \langle X\rangle &= X \cup TTX \cup XTT \cup TXT \cup TTXTT\end{aligned}$$

are the right, lateral, two-sided, and ideal of $T$ generated by $X$, respectively.

It is well known that if $A$, $B$ and $C$ are two-sided ideals of $T$, then $(ABC) = \{abc : a \in A, b \in B, c \in C\}$ is a two-sided ideal of $T$. The intersection of any family of (two-sided) ideals of a ternary semigroup $T$ is either empty or a (two-sided) ideal of $T$. Union of any family of (two-sided) ideals of a ternary semigroup $T$ is a (two-sided) ideal of $T$.

## 3. Pure ideals

In [1], Ahsan and Takahashi studied pure ideals in semigroups. In this section we define pure ideals in ternary semigroups.

**Definition 3.1.** A two-sided ideal $I$ of a ternary semigroup $T$ is called *right* (*left*) *pure* if for each $x \in I$ there exist $y, z \in I$ such that $xyz = x$ ($yzx = x$).

An ideal $I$ of a ternary semigroup $T$ is called *right* (*left*) *pure* if for each $x \in I$ there exist $y, z \in I$ such that $xyz = x$ ($yzx = x$).

Similarly we define one-sided right (left) pure ideals.

The following example shows that right pure ideals need not be left pure.

**Example 3.2.** Let $T = \{0, a, b, c, 1\}$. Define the ternary operation ( ) on $T$ as $(abc) = a * (b * c)$ where the binary operation $*$ is defined as

| $*$ | 0 | $a$ | $b$ | $c$ | 1 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| $a$ | 0 | 0 | 0 | $a$ | $a$ |
| $b$ | 0 | 0 | $b$ | $b$ | $b$ |
| $c$ | 0 | 0 | $b$ | $c$ | $c$ |
| 1 | 0 | $a$ | $b$ | $c$ | 1 |

Then $(T, (\ ))$ is a ternary semigroup and the ideal $I_1 = \{0, a\}$ is neither right pure nor left pure; the ideal $I_2 = \{0, b\}$ is both right and left pure; the ideal $I_3 = \{0, a, b, c\}$ is right pure but not left pure.

**Proposition 3.3.** *Each right pure right ideal of a ternary semigroup $T$ is contained in a right pure two-sided ideal of $T$.*

*Proof.* Let $A$ be a right pure right ideal of $T$. Then $A \cup TTA$ is a two-sided ideal of $T$ generated by $A$. Let $x \in A \cup TTA$. Suppose $x \in A$, since $A$ is right pure right ideal of $T$, therefore there exist $y, z \in A$ such that $x = xyz$. If $x \in TTA$, then $x = t_1t_2a$ for some $t_1, t_2 \in T$ and $a \in A$. Again, since $A$ is right pure so there exist $b, c \in A$ such that $a = abc$. Hence $x = t_1t_2a = t_1t_2(abc) = (t_1t_2a)bc = xbc$. This shows that $A \cup TTA$ is a right pure two-sided ideal containing the right pure right ideal $A$. □

**Proposition 3.4.** *A two-sided ideal $I$ of a ternary semigroup $T$ is right pure if and only if $J \cap I = JII$ for all right ideals $J$ of $T$.*

*Proof.* Suppose $I$ is a right pure two-side ideal of $T$. For every right ideal $J$ of $T$, $JII \subseteq J \cap I$ always. Let $x \in J \cap I$. Since $I$ is a right pure two-sided ideal, so there exist $y, z \in I$ such that $xyz = x$. Thus $x = xyz \in JII$. Hence $J \cap I \subseteq JII$. Thus $J \cap I = JII$.

Conversely, assume that $J \cap I = JII$ for every right ideal $J$ of $T$. We show that $I$ is a right pure two-sided ideal. Let $x$ be any element of $I$ and $J = x \cup xTT$ be the right ideal of $T$ generated by $x$. Then by hypothesis

$$(x \cup xTT) \cap I = (x \cup xTT)II = xII \cup (xTT)II \subseteq xII \cup xII = xII.$$

Since $x \in (x \cup xTT) \cap I$, so $x \in xII$. Hence there exist $y, z \in I$ such that $x = xyz$. Thus $I$ is right pure. □

Similarly we can show that, *an ideal $I$ of a ternary semigroup $T$ is right pure if and only if $J \cap I = JII$ for all right ideals $J$ of $T$.*

**Definition 3.5.** A ternary semigroup $T$ is said to be *right weakly regular* if for each $x \in T$, $x \in (xTT)^3$.

Every regular ternary semigroup is right weakly regular but the converse is not true.

**Theorem 3.6.** *For a ternary semigroup $T$, the following assertions are equivalent:*

($a$) *$T$ is right weakly regular.*

($b$) *Every right ideal of $T$ is idempotent, that is $J^3 = J$ for every right ideal $J$ of $T$.*

($c$) *$J \cap I = JII$ for every right ideal $J$ and two-sided ideal $I$ of $T$.*

($d$) *$J \cap I = JII$ for every right ideal $J$ and for every ideal $I$ of $T$.*

*Proof.* ($a$) $\Rightarrow$ ($b$) Let $J$ be a right ideal of $T$, then $J^3 \subseteq JTT \subseteq J$. Let $x \in J$. Then $x \in (xTT)^3 \subseteq J^3$. Thus $J \subseteq J^3$. Hence $J = J^3$.

($b$) $\Rightarrow$ ($a$) Suppose that every right ideal of $T$ is idempotent. Let $x \in T$. Then $J = x \cup xTT$ is the right ideal of $T$, so idempotent, that is

$$\begin{aligned} x \cup xTT &= (x \cup xTT)(x \cup xTT)(x \cup xTT) \\ &= xxx \cup xxxTT \cup xxTTx \cup xxTTxTT \cup xTTxx \cup xTTxxTT \cup \\ &\quad \cup xTTxTTx \cup xTTxTTxTT. \end{aligned}$$

Simple calculations shows that $x \in (xTT)^3$. Hence $T$ is right weakly regular.

($a$) $\Rightarrow$ ($c$) Suppose $T$ is right weakly regular ternary semigroup and $J$ a right ideal and $I$ a two-side ideal of $T$. Then $JII \subseteq J \cap I$ always. Let $x \in J \cap I$. Since $T$ is right weakly regular, so $x \in (xTT)^3$. Thus $x = (xs_1t_1)(xs_2t_2)(xs_3t_3)$ for some $s_1, t_1, s_2, t_2, s_3, t_3 \in T$. Hence $x \in JII$, which shows that $J \cap I \subseteq JII$. Hence $J \cap I = JII$.

($c$) $\Rightarrow$ ($d$) Obvious.

($d$) $\Rightarrow$ ($a$) Let $x \in T$ and $J = x \cup xTT$ be the right ideal of $T$ generated by $x$, $I = x \cup xTT \cup TTx \cup TxT \cup TTxTT$ be the ideal of $T$ generated by $x$. Then, by hypothesis, $(x \cup xTT) \cap (x \cup xTT \cup TTx \cup TxT \cup TTxTT) = (x \cup xTT)(x \cup xTT \cup TTx \cup TxT \cup TTxTT)(x \cup xTT \cup TTx \cup TxT \cup TTxTT) = (xxx \cup xxxTT \cup xxTTx \cup xxTxT \cup xxTTxTT \cup xTTxx \cup xTTxxTT \cup xTTxTTx \cup xTTxTxT \cup xTTxTTxTT \cup xTxTx \cup xTxTxTT \cup xTxTTxT)$.

Simple calculations shows that $x \in (xTT)^3$. Hence $T$ is right weakly regular ternary semigroup. □

**Theorem 3.7.** *For a ternary semigroup $T$, the following assertions are equivalent:*

(1) *$T$ is right weakly regular.*

(2) *Every two-sided ideal $I$ of $T$ is right pure.*

(3) *Every ideal $I$ of $T$ is right pure.*

*Proof.* The proof follows from Theorem 3.6 and Proposition 3.4. □

**Proposition 3.8.** *Let $T$ be a ternary semigroup with* 0. *Then*

(1) $\{0\}$ *is a right pure ideal of $T$.*

(2) *Set theoretic union of any number of right pure two-sided ideals*

*(ideals) of $T$ is a right pure two-sided ideal (ideal) of $T$.*

(3) *Any finite intersection of right pure two-sided ideals (ideals) of $T$ is a right pure two-sided ideal (ideal) of $T$.*

*Proof.* (1) Obvious.

(2) Let $\{I_k\}_{k\in K}$ be a family of right pure two-sided ideals of $T$. Then $\underset{k\in K}{\cup} I_k$ is a two-sided ideal of $T$. Suppose $x \in \underset{k\in K}{U} I_k$. Then there exists some $k \in K$ such that $x \in I_k$. Since $I_k$ is a right pure two-sided ideal of $T$, so there exist $y, z \in I_k$ such that $x = xyz$. It follows that $y, z \in \underset{k\in K}{U} I_k$ such that $x = xyz$. Hence $\underset{k\in K}{U} I_k$ is a right pure two-sided ideal of $T$.

(3) Let $I_1$, $I_2$ be right pure two-sided ideals of $T$ and $x \in I_1 \cap I_2$. Then $x \in I_1$and $x \in I_2$. Since $I_1$and $I_2$ are right pure two-sided ideals of $T$, so there exist $y_1, z_1 \in I_1$ and $y_2, z_2 \in I_2$ such that $x = xy_1z_1$ and $x = xy_2z_2$. Thus we have $x = xy_1z_1 = (xy_2z_2)y_1z_1 = ((xy_1z_1)y_2z_2)y_1z_1 = x(y_1z_1y_2)(z_2y_1z_1)$, where $y_1z_1y_2$ and $z_2y_1z_1 \in I_1 \cap I_2$. Thus $I_1 \cap I_2$ is a right pure ideal of $T$. □

Similarly we can prove the case of ideals.

**Proposition 3.9.** *Let $I$ be any two-sided ideal of a ternary semigroup $T$ with zero $0$. Then $I$ contains a largest right pure two-sided ideal. (We call it the pure part of $I$ and denote by $\mathcal{S}(I)$).*

*Proof.* Let $\mathcal{S}(I)$ be the union of all right pure two-sided ideals contained in $I$. Such ideals exist because $\{0\}$ is a right pure ideal contained in each two-side ideal. By the above Proposition $\mathcal{S}(I)$ is a right pure two-sided ideal. It is indeed the largest right pure two-sided ideal contained in $I$. □

Similarly we can show that if $I$ is an ideal of $T$ then $I$ contains a largest right pure ideal.

**Proposition 3.10.** *Let $I$, $K$ be two-sided ideals of $T$ and $\{I_k\}_{k\in K}$ be the family of two-sided ideals of a ternary semigroup $T$ with zero $0$. Then*

(1) $\mathcal{S}(I \cap K) = \mathcal{S}(I) \cap \mathcal{S}(K)$.

(2) $\underset{k\in K}{\cup} \mathcal{S}(I_k) \subseteq \mathcal{S}(\underset{k\in K}{\cup} I_k)$.

*Proof.* (1) Since $\mathcal{S}(I) \subseteq I$, $\mathcal{S}(K) \subseteq K$, thus $\mathcal{S}(I) \cap \mathcal{S}(K) \subseteq I \cap K$. But $\mathcal{S}(I) \cap \mathcal{S}(K)$ is right pure by Proposition 3.8, so $\mathcal{S}(I) \cap \mathcal{S}(K) \subseteq \mathcal{S}(I \cap K)$. On the other hand $\mathcal{S}(I \cap K) \subseteq I \cap K \subseteq I$ and $\mathcal{S}(I \cap K)$ is pure, so $\mathcal{S}(I\cap K) \subseteq \mathcal{S}(I)$. Similarly, $\mathcal{S}(I\cap K) \subseteq \mathcal{S}(K)$. Thus $\mathcal{S}(I\cap K) \subseteq \mathcal{S}(I)\cap\mathcal{S}(K)$.

Hence, $\mathcal{S}(I \cap K) = \mathcal{S}(I) \cap \mathcal{S}(K)$.

(2) Since $\mathcal{S}(I_k) \subseteq I_k$ so $\underset{k\in K}{\cup}\mathcal{S}(I_k) \subseteq \underset{k\in K}{\cup} I_k$. As $\mathcal{S}(I_k)$ is right pure, so $\underset{k\in K}{\cup}\mathcal{S}(I_k)$ is right pure. Thus we have $\underset{k\in K}{\cup}\mathcal{S}(I_k) \subseteq \mathcal{S}(\underset{k\in K}{\cup} I_k)$. □

**Definition 3.11.** Let $I$ be a right pure two-sided ideal of $T$, then $I$ is called *purely maximal* if $I$ is maximal in the lattice of proper right pure two-sided ideals of $T$.

A proper right pure two-sided ideal $I$ of $T$ is called *purely prime* if $I_1TI_2 \subseteq I$ implies $I_1 \subseteq I$ or $I_2 \subseteq I$ for any right pure two-sided ideals $I_1$ and $I_2$ of $T$. Equivalently $I_1 \cap I_2 \subseteq I$ implies $I_1 \subseteq I$ or $I_2 \subseteq I$ (Because $I_1TI_2 \subseteq I_1 \cap I_2$ and $I_1 \cap I_2 = I_1I_2I_2 \subseteq I_1TI_2$. Thus $I_1TI_2 = I_1 \cap I_2$).

**Proposition 3.12.** *Any purely maximal two-sided ideal is purely prime.*

*Proof.* Suppose $I$ is purely maximal two-sided ideal of $T$ and $I_1, I_2$ are right pure two-sided ideals of $T$ such that $I_1 \cap I_2 \subseteq I$. Suppose $I_1 \nsubseteq I$. Then $I_1 \cup I$ is a right pure ideal such that $I \subsetneq I_1 \cup I$. Since $I$ is purely maximal, so $I_1 \cup I = T$. Thus

$$I_2 = I_2 \cap T = I_2 \cap (I_1 \cup I) = (I_2 \cap I_1) \cup (I_2 \cap I) \subseteq I \cup I = I.$$

Hence $I$ is purely prime. □

**Proposition 3.13.** *The pure part of any maximal two-sided ideal of a ternary semigroup with zero is purely prime.*

*Proof.* Let $M$ be a maximal two-sided ideal of $T$ and $\mathcal{S}(M)$ be its pure part. Suppose $I_1 \cap I_2 \subseteq \mathcal{S}(M)$ where $I_1$, $I_2$ are right pure two-sided ideals of $T$. If $I_1 \subseteq M$ then $I_1 \subseteq \mathcal{S}(M)$. If $I_1 \nsubseteq \mathcal{S}(M)$ then $I_1 \nsubseteq M$. Thus $I_1 \cup M = T$ because $M$ is maximal. Hence we have

$$I_2 = I_2 \cap T = I_2 \cap (I_1 \cup M) = (I_2 \cap I_1) \cup (I_2 \cap M) \subseteq \mathcal{S}(M) \cup M \subseteq M \cup M = M.$$

But $\mathcal{S}(M)$ is the largest right pure two-sided ideal contained in $M$. Thus $I_2 \subseteq \mathcal{S}(M)$. Hence $\mathcal{S}(M)$ is purely prime. □

**Proposition 3.14.** *Let $I$ be a right pure two-sided ideal of $T$ and $a \in T$ such that $a \notin I$, then there exists a purely prime two-sided ideal $J$ of $T$ such that $I \subseteq J$ and $a \notin J$.*

*Proof.* Let

$X = \{J : J$ is a right pure two-sided ideal of $T$, $I \subseteq J$ and $a \notin J\}$,

then $X \neq \emptyset$ since $I \in X$. $X$ is partially ordered by inclusion. Let $\{J_k\}_{k\in K}$ be any totally ordered subset of $X$. By Proposition 3.8, $\underset{k\in K}{\cup} J_k$ is a right pure two-sided ideal. Since $I \subseteq \underset{k\in K}{\cup} J_k$ and $a \notin \underset{k\in K}{\cup} J_k$, so $\underset{k\in K}{\cup} J_k \in X$. Thus by Zorn's Lemma, $X$ has a maximal element, say, $J$ such that $J$ is pure, $I \subseteq J$ and $a \notin J$. We claim that $J$ is purely prime. Suppose $I_1$ and $I_2$ are right pure two-sided ideals of $T$ such that $I_1 \nsubseteq J$ and $I_2 \nsubseteq J$. Since $I_k(k = 1, 2)$ and $J$ are right pure so $I_k \cup J$ is a right pure two-sided ideal such that $J \subsetneq I_k \cup J$. Thus $a \in I_k \cup J$ $(k = 1, 2)$. As $a \notin J$, so $a \in I_k$ $(k = 1, 2)$. Thus $a \in I_1 \cap I_2$. Hence $I_1 \cap I_2 \nsubseteq J$. This shows that $J$ is purely prime. □

**Proposition 3.15.** *Any proper right pure two sided ideal $I$ of $T$ is the intersection of all the purely prime two-sided ideals of $T$ containing $I$.*

*Proof.* By Proposition 3.14, there exists purely prime two-sided ideals containing $I$ . Let $\{J_k\}_{k\in K}$ be the family of all purely prime two-sided ideals of $T$ which contain $I$. Since $I \subseteq J_k$ for all $k \in K$, so $I \subseteq \underset{k\in K}{\cap} J_k$. To show that $\underset{k\in K}{\cap} J_k \subseteq I$. Let $a \notin I$, then by Proposition 3.14, there exists a purely prime two-sided ideal $J$ such that $I \subseteq J$ and $a \notin J$. It follows that $a \notin \underset{k\in K}{\cap} J_k$. Thus $\underset{k\in K}{\cap} J_k \subseteq I$. Hence $I = \underset{k\in K}{\cap} J_k$. □

## 4. Weakly pure ideals

In this section we generalize the concept of pure two sided ideal and define weakly pure two-sided ideal.

**Definition 4.1.** A two-sided ideal $A$ of a ternary semigroup $T$ is called *left* (resp. *right*) *weakly pure* if $A \cap B = AAB$ (resp. $A \cap B = BAA$) for all two-sided ideals $B$ of $T$.

Every left (right) pure two-sided ideal is left (right) weakly pure.

**Proposition 4.2.** *If $A, B$ are two-sided ideals of a ternary semigroup $T$ with zero 0, then*

$$BA^{-1} = \{t \in T : xyt \in B \; for \; all \; x, y \in A\}$$

*and*

$$A_{-1}B = \{t \in T : txy \in B \textit{ for all } x, y \in A\}$$

*are two-sided ideals of $T$.*

*Proof.* $BA^{-1} \neq \emptyset$ because $0 \in BA^{-1}$. Let $s, r \in T$ and $t \in BA^{-1}$. Then for all $x, y \in A$, $(xy(srt)) = (x(ysr)t) = xzt \in B$ because $z = ysr \in A$. Hence $srt \in BA^{-1}$. Also, $(xy(tsr)) = (xyt)sr \in BTT \subseteq B$, because $xyt \in B$. Thus $tsr \in BA^{-1}$. Hence $BA^{-1}$ is a two-sided ideal of $T$.

Now, let $s, r \in T$ and $t \in A_{-1}B$. Then $((srt)xy) = sr(txy) = srb \in TTB \subseteq B$ for all $x, y \in A$, because $b = txy \in B$. Hence $srt \in A_{-1}B$.

Also, $(tsr)xy = t(srx)y = tx_1y \in B$ because $x_1 = srx \in A$. Thus $tsr \in A_{-1}B$. Hence $A_{-1}B$ is a two-sided ideal of $T$. □

**Proposition 4.3.** *For a two-sided ideal $A$ of a ternary semigroup $T$, the following assertions are equivalent.*

(1) *$A$ is left (right) weakly pure.*

(2) *$(BA^{-1}) \cap A = B \cap A$ $(A_{-1}B \cap A = A \cap B)$ for all ideals $B$ of $T$.*

*Proof.* (1) ⇒ (2) Suppose $A$ is left weakly pure. Since $BA^{-1}$ is a two sided ideal, we have $(BA^{-1}) \cap A = AA(BA^{-1})$.

Now we show that $AA(BA^{-1}) \subseteq B$. Let $atx \in AA(BA^{-1})$, where $a, t \in A$, $x \in BA^{-1}$. Then $atx \in B$ (by the definition of $BA^{-1}$). Hence $AA(BA^{-1}) \subseteq B$. Also $AA(BA^{-1}) \subseteq ATT \subseteq A$ and $(BA^{-1}) \cap A = AA(BA^{-1}) \subseteq A \cap B$. Thus $(BA^{-1}) \cap A \subseteq B \cap A$.

Let $b \in B \cap A$, then $xyb \in B$ for all $x, y \in A$. Hence $b \in BA^{-1}$. Thus $B \cap A \subseteq (BA^{-1}) \cap A$. Therefore $(BA^{-1}) \cap A = B \cap A$.

(2) ⇒ (1) Assume that $A, B$ are two-sided ideals of a ternary semigroup $T$ and $(BA^{-1}) \cap A = B \cap A$. We show that $A$ is left weakly pure. First we show that $B \subseteq (AAB)A^{-1}$. Let $b \in B$, then for each $x, y \in A$, we have $xyb \in AAB$. Thus $b \in (AAB)A^{-1}$. Hence $B \in (AAB)A^{-1}$. This shows $B \subseteq (AAB)A^{-1}$. Thus $A \cap B \subseteq (AAB)A^{-1} \cap A = AAB \cap A \subseteq AAB$ by hypothesis. But $AAB \subseteq A \cap B$ always. Hence $A \cap B = AAB$. Thus $A$ is left weakly pure. □

**Proposition 4.4.** *For a ternary semigroup $T$ the following assertions are equivalent.*

(1) *Each two-sided ideal of $T$ is left weakly pure.*

(2) *Each two-sided ideal of $T$ is idempotent.*

(3) *Each two-sided ideal of $T$ is right weakly pure.*

*Proof.* (1) $\Rightarrow$ (2) Suppose each two-sided ideal of $T$ is left weakly pure. Let $X$ be a two-sided ideal of $T$, then for each two-sided ideal $Y$ of $T$ we have $X \cap Y = XXY$. In particular $X = X \cap X = XXX$. Hence each two-sided ideal of $T$ is idempotent.

(2) $\Rightarrow$ (1) Suppose each two-sided ideal of $T$ is idempotent. Let $X$ be a two-sided ideal of $T$, then for any two-sided ideal $Y$ of $T$ we always have $XXY \subseteq X \cap Y$. On the other hand,

$$X \cap Y = (X \cap Y)(X \cap Y)(X \cap Y) \subseteq XXY.$$

Hence we have $X \cap Y = XXY$. Thus $X$ is left weakly pure.

(2) $\Rightarrow$ (3) Similarly as (2) $\Rightarrow$ (1).

(3) $\Rightarrow$ (2) Suppose each two-sided ideal of $T$ is right weakly pure. Let $X$ be any two-sided ideal of $T$. Then $X$ is right weakly pure. Hence for each two-sided ideal $Y$ of $T$, we have $X \cap Y = YXX$. In particular $X \cap X = XXX$. Hence each two-sided ideal of $T$ is idempotent. □

**Example 4.5.** Any set $T$ with the ternary operation $(xyz) = x$ if $x = y = z$, and $(xyz) = 0$ otherwise, where 0 is a fixed element of $T$, is a ternary semigroup in which every subset containing 0 is its two-sided ideal. Every two-sided ideal of this semigroup is its right (left) pure ideal.

If $|T| = 1$ or 2, then every two-sided ideal of $T$ is purely prime. But if $|T| \geq 3$, then the ideal $\{0\}$ is not purely prime. Because if $a, b \in T - \{0\}$, then $I = \{0, a\}$ and $J = \{0, b\}$ are right pure ideals of $T$ such that $I \cap J = \{0\}$ but neither $I \nsubseteq \{0\}$ nor $J \nsubseteq \{0\}$.

## 5. Pure spectrum of a ternary semigroup

In this section $T$ is a ternary semigroup with zero such that $T^3 = T$.

Let $\mathcal{P}(T)$ be the set of all right pure ideals of $T$ and $\mathbf{P}(T)$ be the set of all proper purely prime ideals of $T$. Define for each $I \in \mathcal{P}(T)$,

$$\mathcal{B}_I = \{J \in \mathbf{P}(T) : I \nsubseteq J\}, \qquad \Im(T) = \{\mathcal{B}_I : I \in \mathcal{P}(T)\}.$$

**Theorem 5.1.** $\Im(T)$ *forms a topology on* $\boldsymbol{P}(T)$.

*Proof.* As $\{0\}$ is a right pure ideal of $T$, so $\mathcal{B}_{\{0\}} = \{J \in \mathbf{P}(T) : \{0\} \nsubseteq J\} = \emptyset$, because 0 belongs to every right pure ideal. Since $T$ is a right pure ideal of $T$, $\mathcal{B}_T = \{J \in \mathbf{P}(T) : T \nsubseteq J\} = \mathbf{P}(T)$ because $\mathbf{P}(T)$ is the set of all proper purely prime ideals of $T$.

Let $\{\mathcal{B}_{I_\alpha} : \alpha \in \Lambda\} \subseteq \Im(T)$, then

$$\bigcup_{\alpha\in\Lambda} \mathcal{B}_{I_\alpha} = \{J \in \mathbf{P}(T) : I_\alpha \nsubseteq J \text{ for some } \alpha \in \Lambda\} = \{J \in \mathbf{P}(T) : \cup I_\alpha \nsubseteq J\} = \mathcal{B}_{\cup I_\alpha}.$$

To prove that $\mathcal{B}_{I_1} \cap \mathcal{B}_{I_2} \in \Im(T)$ for any $\mathcal{B}_{I_1}, \mathcal{B}_{I_2} \in \Im(T)$ we consider $J \in \mathcal{B}_{I_1} \cap \mathcal{B}_{I_2}$. Then $J \in \mathbf{P}(T)$, $I_1 \nsubseteq J$ and $I_2 \nsubseteq J$.

Suppose that $I_1 \cap I_2 \subseteq J$. Since $J$ is a purely prime ideal, therefore either $I_1 \subseteq J$ or $I_2 \subseteq J$, which is a contradiction, hence $I_1 \cap I_2 \nsubseteq J$, which implies $J \in \mathcal{B}_{I_1 \cap I_2}$. Thus $\mathcal{B}_{I_1} \cap \mathcal{B}_{I_2} \subseteq \mathcal{B}_{I_1 \cap I_2}$.

On the other hand, if $J \in \mathcal{B}_{I_1 \cap I_2}$, then

$$I_1 \cap I_2 \nsubseteq J \Rightarrow I_1 \nsubseteq J \text{ and } I_2 \nsubseteq J \Rightarrow J \in \mathcal{B}_{I_1} \text{ and } J \in \mathcal{B}_{I_2} \Rightarrow J \in \mathcal{B}_{I_1} \cap \mathcal{B}_{I_2}.$$

Hence $\mathcal{B}_{I_1 \cap I_2} \subseteq \mathcal{B}_{I_1} \cap \mathcal{B}_{I_2}$. Consequently, $\mathcal{B}_{I_1 \cap I_2} = \mathcal{B}_{I_1} \cap \mathcal{B}_{I_2}$, which implies $\mathcal{B}_{I_1} \cap \mathcal{B}_{I_2} \in \Im(T)$.

Thus $\Im(T)$ is a topology on $\mathbf{P}(T)$. □

**Acknowledgement:** The authors would like to thank the referees and Chief Editor for the valuable suggestions and corrections for improvement of this paper.

## References

[1] **J. Ahsan and M. Takahashi**, *Pure spectrum of a monoid with zero*, Kobe J. Math. **6** (1989), 163 – 182.

[2] **M. Amyari and M. S. Moslehian**, *Approximate homomorphisms of ternary semigroups*, Letters Math. Physics **77** (2006), 1 – 9.

[3] **N. Bazunova, A. Borowiec and R. Kerner**, *Universal differential calculus on ternary algebra*, Letters Math. Physics **67** (2004), 195 – 206.

[4] **A. H. Clifford and G. B. Preston**, *Thew algebraic theory of semigroups*, Amer. Math. Soc. 1961/1967.

[5] **V. N. Dixit and S. Dewan**, *A note on quasi and bi-ideals in ternary semigroups*, Int. J. Math. Math. Sci. **18** (1995), 501 – 508.

[6] **V. N. Dixit and S. Dewan**, *Minimal quasi-ideals in ternary semigroups*, Indian J. Pure Appl. Math. **28** (1997), 255 – 632.

[7] **W. A. Dudek**, *On divisibility in $n$-semigroups*, Demonstratio Math. **13** (1980), 355 – 367.

[8] **W. A. Dudek, I. Groździńska**, *On ideals in regular $n$-semigroups*, Mat. Bilten (Skopje) **3/4 (29/30)** (1979-1980), 35 – 44.

[9] **E. Hewitt and H. S. Zuckerman**, *Ternary operations and semigroups*, Semigroups, Proc. Sympos. Wayne State Univ., Detroit, 1968, 55 – 83.

[10] **J. M. Howie**, *Fundamentals of semigroup theory*, Clarendon Press, Oxford 1995.

[11] **R. Kerner**, *The cubic Chess board*, Quantum Grav. **14** (1997), $A203 - A225$.

[12] **R. Kerner**, *Ternary algebraic structures and their applications in Physics*, Univ, P&M, Curie Preprint, Paris (2000), Arxiv math-ph/0011023.

[13] **J. Los**, *On the extending of models I*, Fundamenta Math. **42** (1955), 38 – 54.

[14] **M. Shabir and A. Khan**, *Fully prime semigroups*, Internat. J. Math. and Analysis, **1** (2006), 261 – 268.

[15] **M. Shabir and S. Bashir**, *Prime ideals in ternary semigroups*, Asian-European J. Math. **2** (2009), 139 – 152.

[16] **M. L. Santiago**, *Some contributions to the study of ternary semigroups and semiheaps*, Ph.D. Thesis, 1983, University of Madras.

[17] **F. M. Sioson**, *On regular algebraic systems*, Proc. Japan. Acad. **39** (1963), 283 – 286.

[18] **F. M. Sioson**, *Ideal theory in ternary semigroups*, Math. Japon. **10** (1965), 63 – 84.

[19] **L. Vainerman and R. Kerner**, *On special classes of $n$-algebras*, J. Math. Phys. **37** (1996), 2553 – 2565.

Received November 22, 2008
Revised May 15, 2009

S.Bashir:
Department of Mathematics, University of Gujrat, Gujrat, Pakistan
E-mail: shahidawaraich@yahoo.com

M.Shabir:
Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
E-mail: mshabirbhatti@yahoo.co.uk

Quasigroups and Related Systems **17** (2009), 161 − 176

# Secret-sharing schemes and orthogonal systems of k-ary operations

*Galina B. Belyavskaya*

**Abstract.** We suggest a general method of the construction of secret-sharing schemes based on orthogonal systems of partial (in particular, everywhere determined) $k$-ary operations which generalizes some known methods of the construction of such schemes by a finite fields and point the orthogonal systems of $k$-ary operations respecting to these known schemes. The different transformations of orthogonal systems of $k$-ary operations are reformulated and applied to orthogonal systems of polynomial $k$-ary operations over finite fields, in particular, to orthogonal systems corresponding to some known schemes.

## 1. Introduction

It is known that for receiving the secret information the secret key is used. The problem of construction of secret-sharing schemes is one of tasks of modern cryptography connected with partition of the secret (more exactly, with sharing the secret key). The method of sharing the secret key provides safety of the procedure of acceptance of decision in some critical situation. It consists in definition the group of person which have a right to accept decision. Every member of this group has a part of the secret key, only the full collection of these parts allows to restore the secret key giving access to the secret.

There are many applications for such schemes including communication networks, financial institutions and computing. One of the aspects of a such scheme is a possibility to share responsibility for acceptance of an important decision, concerning application of systems of weapon, signature of bank checks or of access to the bank depository. One example arises in the military where it would be necessary for several high-level officers to

2000 Mathematics Subject Classification: 94A60, 20N05, 20N15, 05B15
Keywords: secret-sharing scheme, $k$-ary operation, $k$-ary quasigroup, orthogonal system of partial $k$-ary operations, transformation of an orthogonal system.

reconstruct the necessary key required to release very important decision.

The problem of construction of a secret-sharing scheme can be generalized when a decision can be accepted not one but any of several distinct groups of users. In this case the secret key is distributed between all members of groups of users and every user obtains his part of the secret.

One of main aims of a such secret-sharing scheme is defence of a key away from loss. It is better to share a key between several users such that the possibility its restoration by a few groups with in advance defined participants, acting in agreement. That eliminates a risk of loss of a key. The possibility of restoration of a secret must appear when all or sufficiently great part of owners of the secret key was joined. But some of keepers of secret key can be absent with respect to different reasons so it need to restoration the secret if an incomplete collection of owners of the secret key but if their number is greater of some threshold value.

Let $1 < k \leqslant n$. A secret-sharing scheme between $n$ users is called $(n, k)$-*threshold* if any group of $k$ from $n$ users can restore a secret but none group of the smaller number of users cannot obtain an information about the secret key [1].

Secret-sharing schemes were introduced in 1979 by A. Shamir [12]. Later his idea was generalized by other authors, which will be mentioned below. In [13] various secret-sharing schemes known at that time were surveyed.

We suggest a general secret-sharing scheme based on orthogonal systems of partial (in particular, everywhere determined) $k$-ary operations which generalizes some of the known schemes and find the orthogonal systems of $k$-ary operations respecting to these known schemes. Some little-known transformations of orthogonal systems of $k$-ary operations are recalled and are applied to orthogonal systems of polynomial $k$-ary operations over finite fields $GF(q)$, in particular, to orthogonal systems corresponding to known secret-sharing schemes.

## 2. Orthogonal systems of partial k-ary operations

At first we recall some necessary definitions and results. By $x_i^j$ we will denote the sequence $x_i, x_{i+1}, \dots, x_j$, $i \leqslant j$. Let $Q$ be a finite or infinite set, $k \geqslant 2$ be a positive integer, and let $Q^k$ denote the $k$-th Cartesian power of the set $Q$.

Let $Q$ be a nonempty set and $D \subseteq Q^k$, $D \neq \emptyset$. If $A$ is a mapping of $D$ into $Q$, then $A$ is said to be *a partial k-ary operation* (and $(Q, A)$ to be a *partial $k$-ary groupoid*). If $D = Q^k$, we have a usual $k$-ary operation (or shortly, $k$-operation) given on the set $Q$ (see, for example, [14]).

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

A *$k$-ary quasigroup* or a *$k$-quasigroup* is a $k$-groupoid $(Q, A)$ such that in the equality $A(x_1^k) = x_{k+1}$ each set of values of $k$ elements from $x_1^{k+1}$ uniquely defines the value of the $(k+1)$-th element. Sometimes a quasigroup $k$-operation $A$ is itself considered as a $k$-quasigroup.

The $k$-operation $E_i$, $1 \leqslant i \leqslant k$, on $Q$ with $E_i(x_1^k) = x_i$ is called the *$i$-th identity operation* (or the *$i$-th selector*) *of arity $k$*.

For $k \geqslant 2$, *an $k$-dimensional hypercube* (briefly, a *$k$-hypercube*) *of order* $n$ is an $\underbrace{n \times n \times \cdots \times n}_{k}$ array with $n^k$ points based upon $n$ distinct symbols.

A *$k$-dimensional permutation cube of order $n$* [6]) is a $k$-dimentional $n \times n \times \cdots \times n$ matrix of $n$ elements with the property that every column (that is, every sequence of $n$ elements parallel to an edge of the cube) contains a permutation of the elements. In particular, a two-dimentional permutation cube is simply a latin square of order $n$ which is an $n \times n$ array in which $n$ distinct symbols are arranged so that each symbol occurs once in each row and column [6].

A $k$-operation (a $k$-quasigroup) defined on a set $Q$ corresponds to every $k$-hypercube (to every permutation $k$-hypercube) with the elements of $Q$ and vice versa (see, for example, [4]).

**Definition 1.** [14] Let $(Q, A_1), (Q, A_2), \ldots, (Q, A_k)$ be partial $k$-groupoids with the same domain $D = D(A_1) = D(A_2) = \ldots = D(A_k) \subseteq Q^k$. The $k$-tuple of $k$-operations $(A_1^k) = (A_1, A_2, ..., A_k)$ is called *orthogonal* if for every $(a_1, a_2, ..., a_k) \in Q^k$ for which the system $\{A_i(x_1^k) = a_i\}_{i=1}^k$ has a unique solution.

The $k$-tuple $(A_1^k)$ of partial $k$-operations with the same domain $D$ is orthogonal if and only if the mapping $(x_1^k) \to (A_1(x_1^k), A_2(x_1^k), \ldots, A_k(x_1^k))$ is a bijection when $(x_1^k) \in D$.

The set of different partial $k$-operations of the same domain $D$ is said to be an *orthogonal system of partial $k$-operations* (a $k$-OSPO) if each $k$-tuple of the $k$-operations of this set is orthogonal [14].

For coding of information it is useful the following

**Theorem 1.** [14] *To every orthogonal system of $k$-ary partial operations* $\sum = \{A_1, A_2, \ldots, A_t\}$, $t \geqslant k$, *in which all partial operations are defined* *on a set of $q$ elements, the set $D$ has $p$ elements and $q < p \leqslant q^k$, there corresponds a code of $p$ $t$-sequences of code distance $t-(k-1)$ over an alphabet of $q$ letters, $q < p \leqslant q^k$, and vise versa.*

An orthogonal system of $k$-ary operations ($k$-OSO) is a partial case of $k$-OSPOs. Such systems were studied in many works (see, for example, [6, 7]).

A $k$-OSPO, in particular, a $k$-OSO can be used for construction of secret-sharing systems in the following way.

Let $\sum = \{A_1, A_2, \dots, A_t\}$ be a $k$-OSPO of partial $k$-operations given on a set $Q$ of order $q$ with $\mid D \mid = p$. Choose $n$, $k < n \leqslant t$, of partial $k$-operations $A_{i_1} = B_1, A_{i_2} = B_2, \dots, A_{i_n} = B_n$ of $\sum$, some $k$-tuple $a = (a_0, a_1, \dots, a_{k-1})$ of $D \subseteq Q^k$ and suppose that the element $a_0$ (or some elements of this $k$-tuple) is the secret. The $k$-tuple $a$ we express in coded form as the $n$-tuple $b = (b_1, b_2, ..., b_n)$, where $b_j = B_j(a_0, a_1, ..., a_{k-1})$. As $\sum$ is a $k$-OSPO and $a = (a_0, a_1, ..., a_{k-1}) \in D \subseteq Q^k$, any $k$ elements $b_{j_1}, b_{j_2}, ..., b_{j_k}$ of $b$ define uniquely a $k$-tuple $a$, as by the definition of a $k$-OSPO the system $\{B_{j_1}(x_1^k) = b_{j_1}, B_{j_2}(x_1^k) = b_{j_2}, \dots, B_{j_k}(x_1^k) = b_{j_k}\}$ has a unique solution $(x_1, x_2, \dots, x_k) = (a_0, a_1, \dots, a_{k-1})$.

Taking that into account, one can suggest the following *construction of an $(n, k)$-threshold secret-sharing scheme between $n$ users, any $k$ of which can unlock the secret.*

1. Choose a $k$-OSPO $\sum = \{A_1, A_2, \dots, A_t\}$ with a great domain $D$ the partial operations of which is given on a set $Q$ of sufficiently great order $q$.

2. Choose a $k$-tuple $a = (a_0, a_1, \dots, a_{k-1})$ of $D$ in which the element $a_0$ (or some elements) is (are) the secret.

3. Choose an $n$-tuple $(i_1, i_2, \dots, i_n)$ of $\{1, 2, \dots, t\}$, $k \leqslant n \leqslant t$.

4. Calculate the $n$-tuple $b = (b_1, b_2, \dots, b_n) =$

$(A_{i_1}(a_0^{k-1}), A_{i_2}(a_0^{k-1}), \dots, A_{i_n}(a_0^{k-1})) = (B_1(a_0^{k-1}), B_2(a_0^{k-1}), \dots, B_n(a_0^{k-1}))$.

5. The pairs $(i_1, b_1), (i_2, b_2), \dots, (i_n, b_n)$, which form the secret key, can be separated between $n$ users which are the keepers of the secret.

Using this system any group of $k$ from $n$ users having $k$ pairs $(i_{j_1}, b_{j_1}), \dots,$ $(i_{j_k}, b_{j_k})$ unlocks the secret deciding the system $\{B_{j_1}(x_1^k) = b_{j_1}, B_{j_2}(x_1^k) = b_{j_2}, \dots, B_{j_k}(x_1^k) = b_{j_k}\}$ and none another group of smaller numbers of users cannot to receive an information about the secret.

This system allows to increase a number of keepers of the secret adding $l$ elements $i_{n+1}, i_{n+2}, \ldots, i_{n+l}$, where $n + l \leqslant t$, in point 3.

If there is only one group of the keepers of the secret, then in item 3 we choose $n = k$.

The pointed algorithm is the same when we use an orthogonal system of $k$-ary operations (a $k$-OSO) given on a set $Q$. In this case $D = Q^k$.

As one variation on theme of secret-sharing schemes, we might want a scheme where some participants' share carry more weight than others. In this case we require that a share from participant $i$ can be replaced by a collection of shares from participant of lower weights. Such a system is often called a multilevel scheme. For example, assume that in a bank, one wants to have a valid signature for transfer of a great sum of money only if the shares of two tellers and one vice-president or two vice-presidents are entered.

In such case we can in the suggested scheme to share secret $(i_1, b_1), (i_2, b_2), \ldots, (i_n, b_n)$ between $l < n$ keepers giving more parts of the secret key to the participants with more weight and less parts to the participants with lower weight.

## 3. Some known secret-sharing schemes

The following connection between $k$-OSOs and codes is well known.

**Theorem 2.** [15] *A code of $q^k$ words of length $t$ with the code distance $t - (k - 1)$ in an alphabet from $q$ letters corresponds to every orthogonal system of $k$-ary operations $\sum = \{A_1, A_2, \ldots, A_t\}$, $t \geqslant k$, defined on a set $Q$ of order $q$ and vice versa.*

It is a partial case of Theorem 1 when $p = q^k$. In this case we have an MDS-code (that is a code with the maximal Hamming distance $n - (k - 1)$ between codewords).

In his book [16] W. W. Wu stated that all the secret-sharing schemes known at the time his book was written are connected with latin squares and provided some constructions of such schemes using orthogonal latin squares. All his examples construct secret-sharing schemes in which only two parts of the secret key are need to unlock the secret. J. Dénes and A. D. Keedwell [7, Chapter 9] made a more general observation that all these schemes can be constructed with the aid of Reed-Solomon codes.

A code of Reed-Solomon over $GF(q)$ is a code with codewords of length $q - 1$. The codes of Reed-Solomon over $GF(q)$ are MDS-codes [7, Ch. 9].

The scheme with the secret $(s_0, s_1, \ldots, s_{k-1})$ due to A. Shamir [12] based on a polynomial $q(x) = s_0+s_1x+\ldots+s_{k-1}x^{k-1}$ modulo $p$, where $p$ is a prime greater than $n$ and where the polynomial is so chosen that it has distinct values modulo $p$ for $n$ different values $x_1, x_2, \ldots, x_n$ of $x$. The secret key is the $n$ different ordered pairs of integers $(x_i, q(x_i))$ for $i = 1, 2, \ldots, n$. The polynomial $q(x)$ is calculated by the Lagrange's interpolation formula

$$q(x) = \sum_{i-1}^{k} \frac{q(x_i)(x-x_1)(x-x_2)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_k)}{(x_i-x_1)(x_i-x_2)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_k)}$$

for polynomials where $x_1, x_2, \ldots, x_k$ are any $k$ of $n$ parts of the secret key.

The second scheme of such kind is due to R. J. McEliece and D. V. Sarwarte [11]. In this scheme a Reed-Solomon code over a finite field $GF(q)$ with words of length $q-1$ is defined by the following matrix $G$:

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_{q-1} \\ a_1^2 & a_2^2 & \cdots & a_{q-1}^2 \\ & \ldots & & \\ a_1^{k-1} & a_2^{k-1} & \cdots & a_{q-1}^{k-1} \end{pmatrix}$$

where $a_0 = 0, a_1 = 1, a_2, \ldots, a_{q-1}$ are the different elements of $GF(q)$ with $q = p^m$ ($p$ is prime) elements. Every $k$-tuple $s = (s_0, s_1, \ldots, s_{k-1})$ in coded form is the $(q-1)$-tuple $b = (b_1, b_2, \ldots, b_{q-1})$, where $b = sG$. In this case $b_i = q(a_i)$, where $q(x) = s_0 + s_1x + \ldots + s_{k-1}x^{k-1}$, so this method is a generalization of that Shamir. The subset of $n \leqslant (q-1)$ pairs of the set $\{(i, b_i) \mid i = 1, 2, \ldots, q-1\}$, any $k$ of which unlock the secret, can be the secret key.

J. W. Greene, M. E. Hellman and E. D. Karnin used the matrix $\overline{G}$ over a finite field to construct an extended Reed-Solomon code [8]:

$$\overline{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & a_1 & a_2 & \cdots & a_{q-1} \\ 0 & 0 & a_1^2 & a_2^2 & \cdots & a_{q-1}^2 \\ & & & \ldots & & \\ 0 & 1 & a_1^{k-1} & a_2^{k-1} & \cdots & a_{q-1}^{k-1} \end{pmatrix}.$$

Thus, the matrix $\overline{G}$ of *an extended Reed-Solomon code* is the matrix $G$ with two first added columns. The first (the second) column contains the element 1 on the first (on the last) place and the element 0 on the rest places.

According to Theorem 5.1 [7] every extended Reed-Solomon code (and that means the corresponding secret-sharing scheme) with a generating matrix of two rows

$$\begin{pmatrix} 1 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 1 & a_1 & a_2 & \cdots & a_{q-1} \end{pmatrix}$$

which is defined over a field $GF(q)$ can be constructed from a complete set of orthogonal latin squares (binary quasigroups) of order $q$.

This result can be generalized to the $k$-ary case. At first we remind that an *$i$-invertible* $k$-operation $A$ defined on $Q$ is a $k$-operation for which the equation $A(a_1^{i-1}, x, a_{i+1}^k) = a_{k+1}$ has a unique solution for each fixed $k$-tuple $(a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{k+1})$ of $Q^k$.

A $k$-ary quasigroup can be defined as a $k$-groupoid $(Q, A)$ such that the $k$-operation $A$ is $i$-invertible for each $i = 1, 2, \ldots, k$.

A $k$-ary operation $A(x_1^k) = a_1x_1 + a_2x_2 + \ldots + a_kx_k$ over a field $GF(q)$ is $i$-invertible, if $a_i \neq 0$ and it is a $k$-quasigroup if and only if all its coefficients are different from 0.

**Theorem 3.** *Every secret-sharing system corresponding to the extended Reed-Solomon code over a field $GF(q)$ with the matrix $\overline{G}$ is equivalent to the orthogonal system $\sum = \{E_1, E_k, A_1, A_2, \ldots, A_{q-1}\}$ of $k$-operations of order $q$, where $E_1(x_0^{k-1}) = x_0$, $E_k(x_0^{k-1}) = x_{k-1}$,*

$$A_i(x_0^{k-1}) = x_0 + a_ix_1 + a_i^2x_2 + \ldots + a_i^{k-1}x_{k-1}.$$

*All $k$-operations $A_i$, $i = 1, 2, \ldots, q-1$, are $k$-quasigroups.*

*Proof.* Let us consider a secret-sharing scheme corresponding to the extended Reed-Solomon code over a field $GF(q)$ with the matrix $\overline{G}$. The determinant formed by any $k$ of the columns of this matrix is nonsingular, so the system of $k$-operations $\sum = \{E_1, E_k, A_1, A_2, \ldots, A_{q-1}\}$ defining by the columns of the matrix $\overline{G}$: $E_1(x_0^{k-1}) = x_0, E_k(x_0^{k-1}) = x_{k-1}$, $A_i(x_0^{k-1}) = x_0 + a_ix_1 + a_i^2x_2 + \ldots + a_i^{k-1}x_{k-1}$, $i = 1, 2, \ldots, q-1$, is orthogonal. All $k$-operations $A_i$ are $k$-quasigroups as $a_i \neq 0$ for any $i = 1, 2, \ldots, q-1$, so a system of permutation $k$-hypercubes corresponds to these $k$-quasigroups.

The $k$-tuple $(s_0, s_1, \ldots, s_{k-1})$, including the secret, is coded as

$$(s_0, s_{k-1}, A_1(s_0^{k-1}), A_2(s_0^{k-1}), \ldots, A_{q-1}(s_0^{k-1})).$$

Converse is evident since the system $\sum = \{E_1, E_k, A_1, A_2, \dots, A_{q-1}\}$ of $k$-operations defines the columns of the matrix $\overline{G}$. So this system defines the secret-sharing scheme, corresponding to the extended Reed-Solomon code. □

Note that $A_i(s_0^{k-1}) = q(a_i)$, $i = 1, 2, \dots, q-1$, where $q(x)$ is the polynomial of Shamir over the field $GF(q)$.

It is easy to see that the system $\sum = \{E_1, E_2, A_1, A_2, \dots, A_{q-1}\}$ of orthogonal binary operations, where $E_1(x, y) = x$, $E_2(x, y) = y$, $A_i(x, y) = x + a_i y$, $i = 1, 2, \dots, q-1$, corresponds to the secret-sharing scheme, which respect to the matrix of two rows of Theorem 5.1 [7]. In this case all operations $A_i(x, y)$, $i = 1, 2, \dots, q-1$, are binary quasigroups.

In the case of the matrix $G$ we have the following

**Corollary 1.** *Every secret-sharing system corresponding to the Reed-Solomon code over a field $GF(q)$ with the matrix $G$ is equivalent to the orthogonal system $\sum = \{A_1, A_2, \dots, A_{q-1}\}$ of $k$-quasigroups of order $q$, where $A_i(x_0^{k-1}) = x_0 + a_i x_1 + a_i^2 x_2 + \dots + a_i^{k-1} x_{k-1}$, $i = 1, 2, \dots, q-1$.*

Note that instead of the matrix $\overline{G}$ one can take the matrix over a field $GF(q)$ with a primitive element (that is a generating element of the multiplicative group) $a$ and with the following $k$-operations (corresponding to the columns of this matrix): $E_1(x_0^{k-1}) = x_0$, $E_k(x_0^{k-1}) = x_{k-1}$, $A_1(x_0^{k-1}) = x_0 + x_1 + \dots + x_{k-1}$, $A_{i+1}(x_0^{k-1}) = x_0 + a^i x_1 + a^{2i} x_2 + \dots + a^{(k-1)i} x_{k-1}$, $i = 1, 2, \dots, q-2$, where $k$-operations $A_1, A_2, \dots, A_{q-1}$ are $k$-quasigroups. We may take the matrix with the $q+1$ rows defined by these $k$-operations.

## 4. Transformations of orthogonal systems

With the point of view of ciphering of an information it is important to obtain many orthogonal systems from one system. In the connect with that we recall some transformations of orthogonal systems of $k$-operations known in the algebraic theory of orthogonal systems of $k$-operations with some additions.

At first we reremind some necessary information from [2] with respect to $k$-OSOs (for the case $k = 2$ see [3]).

Let $(A_1, A_2, \dots, A_k) = (A_1^k)$ be a $k$-tuple of $k$-operations defined on a set $Q$. This $k$-tuple defines the unique mapping $\bar{\theta} : Q^k \to Q^k$ in the following way: $\bar{\theta} : (x_1^k) \to (A_1(x_1^k), A_2(x_1^k), \dots, A_k(x_1^k))$, (or briefly, $\bar{\theta} : (x_1^k) \to (A_1^k)(x_1^k)$).

Conversely, any mapping $Q^k$ into $Q^k$ uniquely defines a $k$-tuple $(A_1^k)$ of $k$-operations on $Q$: if $\bar{\theta}(x_1^k) = (y_1^k)$, then we define $A_i(x_1^k) = y_i$ for all $i = 1, 2, \dots, k$ (or shortly, $i \in \overline{1,k}$). Thus, we obtain $\bar{\theta} = (A_1^k)$, where $\bar{\theta}(x_1^k) = (A_1^k)(x_1^k) = (A_1^k(x_1^k))$. If $C$ is a $k$-operation on $Q$ and $\bar{\theta}$ is a mapping $Q^k$ into $Q^k$, then the operation $C\bar{\theta}$ defined by the equality $C\bar{\theta}(x_1^k) = C(\bar{\theta}(x_1^k))$ is also a $k$-operation. Let $C\bar{\theta} = D$ and $\bar{\theta} = (A_1^k)$, then $D(x_1^k) = C(A_1^k(x_1^k))$ or briefly, $D = C(A_1^k)$. If $\bar{\theta} = (B_1^k)$ and $\bar{\varphi} = (A_1^k)$ are mappings $Q^k$ into $Q^k$, then $\bar{\varphi}\bar{\theta} = (A_1^k)\bar{\theta} = (A_1\bar{\theta}, A_2\bar{\theta}, \dots, A_k\bar{\theta}) = ((A_i\bar{\theta})_{i=1}^k = (A_i(B_1^k))_{i=1}^k$.

If $\bar{\theta} = (B_1^k)$ is a permutation of $Q^k$, then $B_i = E_i\bar{\theta}$ and $B_i\bar{\theta}^{-1} = B_i(B_1^k)^{-1} = E_i$, $i \in \overline{1,k}$.

**Definition 2.** [2] A $k$-tuple $(A_1^k)$ of different $k$-operations on $Q$ is called *orthogonal* if the system $\{A_i(x_1^k) = a_i\}_{i=1}^k$ has a unique solution for all $(a_1^k) \in Q^k$.

The $k$-tuple $(E_1^k)$ of the selectors of arity $k$ is the identity permutation of $Q^k$ and is orthogonal.

There is a close connection between orthogonal $k$-tuples of $k$-operations on $Q$ and permutations of $Q^k$ (such permutations will be called *$k$-permutations*).

**Proposition 1.** [2] *A $k$-tuple $(A_1^k)$ of $k$-operations is orthogonal if and only if the mapping $\bar{\theta} = (A_1^k)$ is a permutation of $Q^k$.*

In [2] it was introduced the notion of a strongly orthogonal system of $k$-operations.

**Definition 3.** [2] A system $\Sigma = \{A_1, A_2, \dots, A_t\} = \{A_1^t\}$, $t \geqslant 1$, of $k$-operations, given on a set $Q$, is called *strongly orthogonal* if the system $\overline{\Sigma} = \{E_1^k, A_1^t\}$ is orthogonal.

In this case all $k$-operations of $\Sigma$ are $k$-quasigroups since an $i$-invertible $k$-operation $A$ defined on $Q$ is $i$-invertible if and only if the mapping $(E_1, E_2, \dots, E_{i-1}, A, E_{i+1}, \dots, E_k)$ is a permutation of $Q^k$.

The system $\overline{\Sigma}$ is called the *orthogonal system of $k$-quasigroups* ($k$-OSQs).

A $k$-operation $A$ is a $k$-quasigroup if and only if the set $\Sigma = \{A\}$ is strongly orthogonal. A set $\Sigma = \{A_1^t\}$ of $k$-quasigroups when $k > 2$, $t \geqslant k$, can be orthogonal but not strongly orthogonal in contrast to the binary case [2].

Note that in the case of a strongly orthogonal set $\Sigma = \{A_1, A_2, \dots, A_t\} = \{A_1^t\}$ of $k$-operations the number $t$ of $k$-operations in $\Sigma$ can be less than arity $k$.

According to [2] if $\sum$ is a $k$-OSO given on a set $Q$, then $\sum' = \sum\overline{\theta} = \{A_1\overline{\theta}, A_2\overline{\theta}, \dots, A_t\overline{\theta}\}$, where $\overline{\theta}$ is a permutation of $Q^k$, is also a $k$-OSO.

Two $k$-OSO $\sum$ and $\sum'$ given on a set $Q$ are *conjugate* if there exists a permutation $\overline{\theta}$ of $Q^k$ such that $\sum' = \sum\overline{\theta}$. They are called *parastrophic* if $\sum' = \sum\overline{\theta}^{-1}$ where $\overline{\theta} = (A_{i_1}, A_{i_2}, \dots, A_{i_k})$, $A_{i_j} \in \sum$ for any $j \in \overline{1,k}$. In this case $\sum' = \sum\overline{\theta}^{-1} = \{E_1, E_2, \dots, E_k, A_i\overline{\theta}^{-1} | i \in \overline{1,t}, i \neq i_j, j \in \overline{1,k}\}$.

By Theorem 1 of [2] every $k$-OSO is conjugate to a $k$-OSQ and by Lemma 3 of [2] two $k$-OSQs are conjugate if and only if they are parastrophic.

In [2] the transformation of isostrophy of $k$-OSOs described below (for $k = 2$ see [3]) which is more general than conjugation was also considered.

Let $\sum = \{A_1^t\}$ be a $k$-OSO given on a set $Q$, $T = (\alpha_1, \alpha_2, \dots, \alpha_t)$ be a system of permutations of $Q$. The transformation $\sum \to \sum'$ where $\sum' = \{\alpha_1 A_1, \alpha_2 A_2, \dots, \alpha_t A_t\}$, $A_i \in \sum$ is called *isotopy* of $k$-OSOs and denoted by $\sum' = \sum^T$.

**Remark 1.** Note that if a $k$-OSO $\sum = \{A_1^t\}$ is strongly orthogonal and $T = (\alpha_1, \alpha_2, \dots, \alpha_{t+k})$, then $\overline{\sum}^T = \{\alpha_1 E_1, \alpha_2 E_2, \dots, \alpha_k E_k, B_1, B_2, \dots, B_t\}$ where $B_j = \alpha_{k+j} A_j$, $j \in \overline{1,t}$, are $k$-quasigroups.

It is true [2] that $(\sum\overline{\theta})^T = (\sum^T)\overline{\theta}$, i.e., if $B_i \in \sum' = (\sum\overline{\theta})^T$, $i \in \overline{1,t}$, then

$$B_i(x_1^k) = (\alpha_i(A_i\overline{\theta}))(x_1^k) = (\alpha_i A_i)\overline{\theta}(x_1^k). \qquad (1)$$

The transformation $\sum \to (\sum\overline{\theta})^T = \sum'$ is called in [2] *isostrophy.*

The system $\sum'$ is also orthogonal. Indeed, any $k$-tuple with different $k$-operations of $\sum'$ defines a permutation of $Q^k$: $(B_{i_1}, B_{i_2}, \dots, B_{i_k}) = ((\alpha_{i_1} A_{i_1})\overline{\theta}, (\alpha_{i_2} A_{i_2})\overline{\theta}, \dots, (\alpha_{i_k} A_{i_k})\overline{\theta}) = (\alpha_{i_1} E_1, \alpha_{i_2} E_2, \dots, \alpha_{i_k} E_k)(A_{i_1}, A_{i_2}, \dots, A_{i_k})\overline{\theta}$. Thus, this $k$-tuple is the product of three permutations of $Q^k$, so it is orthogonal.

In addition, we consider the following case of the transformation of isostrophy of a $k$-OSO, namely, $\sum' = (\sum\overline{\theta}_1)^T$, where $\overline{\theta}_1 = \overline{\theta}\,\overline{\theta}_0$, $\overline{\theta}_0 = (\beta_1 E_1, \beta_2 E_2, \dots, \beta_k E_k)$, $\beta_1, \beta_2, \dots, \beta_k$ are permutations of $Q$, that is $\overline{\theta}_0(x_1^k) = (\beta_1 E_1, \beta_2 E_2, \dots, \beta_k E_k)(x_1^k) = (\beta_1 x_1, \beta_2 x_2, \dots, \beta_k x_k)$.

In this case, if $B_i \in \sum'$, then

$$B_i(x_1^k) = (\alpha_i A_i)\overline{\theta}_1(x_1^k) = (\alpha_i A_i)\overline{\theta}\,\overline{\theta}_0(x_1^k) = ((\alpha_i A_i)\overline{\theta})\overline{\theta}_0(x_1^k). \qquad (2)$$

Let $\overline{\theta} = (C_1, C_2, \dots, C_k)$, then (2) can be written as

$$B_i(x_1^k) = \alpha_i A_i(C_1(\beta_j x_j)_{j=1}^k, C_2(\beta_j x_j)_{j=1}^k, \dots, C_k(\beta_j x_j)_{j=1}^k), \qquad (3)$$

where $(\beta_j x_j)_{j=1}^k = (\beta_1 x_1, \beta_2 x_2, \dots, \beta_k x_k)$.

Transformation (3) of a known $k$-OSO $\sum = \{A_1^t\}$ is realized with the help of a tuple of permutations $\alpha_i$, $i \in \overline{1,t}$, some known orthogonal $k$-tuple of $k$-operations $(C_1, C_2, \ldots, C_k) = \overline{\theta}$ and $k$ permutations $\beta_j$, $j \in \overline{1,k}$, of $Q$.

**Remark 2.** The transformation (3) can be represented by conjugations and isotopy of $k$-operations. Remind that two $k$-operations $(Q,A)$ and $(Q,B)$ are *isotopic* if there exists a $(k+1)$-tuple $T = (\beta_1, \beta_2, \ldots, \beta_k, \alpha)$ of permutations of $Q$ such that $\alpha B(x_1^k) = A(\beta_1 x_1, \beta_2 x_2, \ldots, \beta_k x_k)$ for any $x_1^k \in Q^k$ or, shortly, $B = A^T$. Any $k$-operation isotopic to a $k$-quasigroup is a $k$-quasigroup. Using isotopic $k$-operations transformation (2) can be written as $\sum' = \{B_1, B_2, \ldots, B_t\} = \{(A_1\overline{\theta})^{T_1}, (A_2\overline{\theta})^{T_2}, \ldots, (A_t\overline{\theta})^{T_t}\} = \{\alpha_1(A_1\overline{\theta})^{T_0}, \alpha_2(A_2\overline{\theta})^{T_0}, \ldots, \alpha_t(A_t\overline{\theta})^{T_0}\}$, where $T_i = (\beta_1, \beta_2, \ldots, \beta_k, \alpha_i^{-1})$, $\alpha_i$, $i \in \overline{1,t}$, $\beta_j$, $j \in \overline{1,k}$, are permutations of $Q$, $T_0 = (\beta_1, \beta_2, \ldots, \beta_k, 1)$ (1 is the identity permutation of Q).

If $Q(A)$ is a $k$-quasigroup, then the system $\sum = \{E_1, E_2, \ldots, E_k, A\}$ is orthogonal and $\bar{\theta} = (E_2, \ldots, E_k, A)$ is a $k$-permutation of $Q^k$.

By Proposition 3 of [9] the systems

$$\sum\bar{\theta} = \{E_2, E_3, \ldots, E_k, A, A\bar{\theta}\}, \quad \sum\bar{\theta}^2 = \{E_3, E_4, \ldots, E_k, A, A\bar{\theta}, A\bar{\theta}^2\}, \ldots,$$
$$\sum\bar{\theta}^k = \{A, A\bar{\theta}, A\bar{\theta}^2, \ldots, A\bar{\theta}^k\} \text{ and } \sum\bar{\theta}^s = \{A\bar{\theta}^{s-k}, A\bar{\theta}^{s-k-1}, \ldots, A\bar{\theta}^s\}$$

are orthogonal for every $s \geqslant k+1$. Each of these systems contains $k+1$ operations, any $k$ of which define a $k$-permutation of $Q^k$.

The transformation of isotopy, conjugation or isostrophy of a $k$-OSO $\sum$, described above, corresponds to the transformation of the secret-sharing scheme, based on the $k$-OSO $\sum$, which it is possible to call the transformation of isotopy, conjugation or isostrophy of the secret-sharing scheme respectively.

## 5. Transformations of orthogonal systems

Consider transformations of $k$-OSOs which consist *polynomial $k$-operations*, i.e., $k$-operations of the form

$$A(x_1^k) = a_1x_1 + a_2x_2 + \ldots + a_kx_k$$

over a field $GF(q)$. Any selector $E_i$ of arity $k$ can be considered as a polynomial $k$-operation: $E_i(x_1^k) = a_1x_1 + a_2x_2 + \ldots + a_ix_i + \ldots + a_kx_k$ where $a_i = 1, a_j = 0, i, j \in \overline{1,k}$, $j \neq i$.

Let $\Sigma = \{A_1, A_2, \ldots, A_t\}$, $k \geqslant 2$, $t \geqslant k$, be a set of $k$-operations each of which is a polynomial $k$-operation over a field $GF(q)$, that is

$$\begin{array}{c} A_1(x_1^k) = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1k}x_k, \\ A_2(x_1^k) = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2k}x_k, \\ \ldots \\ A_t(x_1^k) = a_{t1}x_1 + a_{t2}x_2 + \ldots + a_{tk}x_k. \end{array} \tag{4}$$

Let $\overline{A}$ be the matrix $t \times k$ defined by (4). The system $\sum = \{A_1^t\}$, $k \geqslant 2$, $t \geqslant k$, of polynomial $k$-operations from (4) is orthogonal if and only if all $k$-minors of the matrix $\overline{A}$, defined by these $k$-operations, are different from 0 (Proposition 1 of [5]).

Consider the transformations of isotopy, conjugation and isostrophy of $k$-OSOs which consist of polynomial $k$-operations over a finite field $GF(q)$, in particular, when the $k$-OSOs are defined by the columns of the matrix $G$ or $\overline{G}$.

Denote by $\sum_{\overline{A}}$, $\sum_G$ and $\sum_{\overline{G}}$ the $k$-OSOs of polynomial $k$-operations defined by (4), by the columns of the matrix $G$ and by the columns of the matrix $\overline{G}$ respectively. In the following statements the definitions of corresponding transformations of these $k$-OSOs described in the previous item (which give new $k$-OSOs) are applied for the polynomial $k$-operations.

We will consider only these $k$-OSOs over a field $GF(q)$ which contain $t$ $k$-operations $A_1, A_2, \ldots, A_t$.

**Proposition 2.** *Let $B_i \in \sum_{\overline{A}}^T$, where $T = (\alpha_1, \alpha_2, \ldots, \alpha_t)$, $\alpha_i$ is a permutation of a set $Q$ for $i \in \overline{1,t}$, then*

$$B_i(x_1^k) = \alpha_i(a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{ik}x_k), \quad i \in \overline{1,t}.$$

Indeed, $B_i(x_1^k) = \alpha_i A_i(x_1^k) = \alpha_i(a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{ik}x_k)$, $i \in \overline{1,t}$.

For the polynomial $k$-operations defined by the matrix $G$ or $\overline{G}$ we have

**Corollary 2.** *If $B_i \in \sum_G^T$, $T = (\alpha_1, \alpha_2, \ldots, \alpha_{q-1})$, then $B_i(x_0^{k-1}) = \alpha_i(x_0 + a_i x_1 + a_i^2 x_2 + \ldots + a_i^{k-1}x_{k-1})$, $i \in \overline{1, q-1}$, and $B_1 = \alpha_1 E_1$, $B_2 = \alpha_2 E_k$, $B_i(x_0^{k-1}) = \alpha_i(x_0 + a_i x_1 + a_i^2 x_2 + \ldots + a_i^{k-1}x_{k-1})$, $i \in \overline{3, q+1}$, if $B_i \in \sum_{\overline{G}}^T$.*

**Proposition 3.** *Let $B_i \in \sum_{\overline{A}} \overline{\theta}$, where $\overline{\theta} = (C_1, C_2, \ldots, C_k)$, then*

$$B_i(x_1^k) = a_{i1}C_1(x_1^k) + a_{i2}C_2(x_1^k) + \ldots + a_{ik}C_k(x_1^k), \quad i \in \overline{1,t}.$$

Indeed, $B_i(x_1^k) = A_i\overline{\theta}(x_1^k) = a_{i1}C_1(x_1^k) + a_{i2}C_2(x_1^k) + \ldots + a_{ik}C_k(x_1^k)$ for all $i \in \overline{1,t}$.

**Corollary 3.** *If* $B_i \in \sum_G \overline{\theta}$*, where* $\overline{\theta} = (C_1, C_2, \ldots, C_k)$ *, then* $B_i(x_0^{k-1}) = C_1(x_0^{k-1}) + a_i C_2(x_0^{k-1}) + a_i^2 C_3(x_0^{k-1}) + \ldots + a_i^{k-1} C_k(x_0^{k-1})$*,* $i \in \overline{1, q-1}$*. The* $k$*-operations of* $\sum_{\overline{G}} \overline{\theta}$ *have the form:* $B_1 = C_1$*,* $B_2 = C_k$*,* $B_i(x_0^{k-1}) = C_1(x_0^{k-1}) + a_i C_2(x_0^{k-1}) + a_i^2 C_3(x_0^{k-1}) \ldots + a_i^{k-1} C_k(x_0^{k-1})$*,* $i \in \overline{3, q+1}$*.*

Indeed, $B_1 = E_1 \overline{\theta} = C_1$, $B_2 = E_k \overline{\theta} = C_k$ by the definition.

**Corollary 4.** *Let* $A_{i_0}$ *be a* $k$*-operation from* $\sum_G$ *(from* $\sum_{\overline{G}}$*,* $A_{i_0} \neq E_1, E_k$*),* $\overline{\theta} = (E_1, E_2, \ldots, E_{k-1}, A_{i_0})$*. If* $B_i \in \sum_G \overline{\theta}$*,* $i \in \overline{1, q-1}$*,* $i \neq i_0$*, then* $B_i(x_0^{k-1}) = (1 + a_i^{k-1})x_0 + (a_i + a_i^{k-1} a_{i_0})x_1 + \ldots + (a_i^{k-2} + a_i^{k-1} a_{i_0}^{k-2})x_{k-2} + a_i^{k-1} a_{i_0}^{k-1} x_{k-1}$ *and* $B_{i_0}(x_0^{k-1}) = (1 + a_{i_0}^{k-1})x_0 + a_{i_0}(1 + a_{i_0}^{k-1})x_1 + \ldots + a_{i_0}^{k-2}(1 + a_{i_0}^{k-1})x_{k-2} + a_{i_0}^{2k-2} x_{k-1}$*. If* $B_i \in \sum_{\overline{G}} \overline{\theta}$*, then* $B_1 = E_1$*,* $B_2 = A_{i_0}$ *and* $B_i$*,* $i \in \overline{3, q+1}$*, have the same form as above.*

*Proof.* $\overline{\theta} = (E_1, E_2, \ldots, E_{k-1}, A_{i_0})$ is a $k$-permutation, $A_{i_0}$ is a $k$-quasigroup, so by Corollary 3 $B_i(x_0^{k-1}) = E_1(x_0^{k-1}) + a_i E_2(x_0^{k-1}) + a_i^2 E_3(x_0^{k-1}) + \ldots + a_i^{k-2} E_{k-1}(x_0^{k-1}) + a_i^{k-1} A_{i_0}(x_0^{k-1}) = x_0 + a_i x_1 + a_i^2 x_2 + \ldots + a_i^{k-2} x_{k-2} + a_i^{k-1}(x_0 + a_{i_0} x_1 + \ldots + a_{i_0}^{k-1} x_{k-1}) = (1 + a_i^{k-1})x_0 + (a_i + a_i^{k-1} a_{i_0})x_1 + \ldots + (a_i^{k-2} + a_i^{k-1} a_{i_0}^{k-2})x_{k-2} + a_i^{k-1} a_{i_0}^{k-1} x_{k-1}$, $i \in \overline{1, q-1}$, if $B_i \in \sum_G \overline{\theta}$. For $i = i_0$ we obtain $B_{i_0}$.

When $B_i \in \sum_{\overline{G}} \overline{\theta}$, then $B_1 = E_1(E_1, E_2, \ldots, E_{k-1}, A_{i_0}) = E_1$, $B_2 = E_k(E_1, E_2, \ldots, E_{k-1}, A_{i_0}) = A_{i_0}$. The rest $k$-operations has the form as in the first part of the corollary. □

Note that the transformation of Corollary 4 corresponds to the following transformation of the matrix $G$ (or $\overline{G}$): the last row (that is the $k$-th row) multiplied by $a_{i_0}^{j-1}$ is added to the $j$-th row, $j = 1, 2, \ldots, k-1$, the last row is multiplied by $a_{i_0}^{k-1}$ (assume $a_{i_0}^0 = 1$). The $k$-operation $B_i$ is defined by the $i$-th column of the obtained matrix.

Let $\overline{\theta} = (E_1, E_2, \ldots, E_{k-1}, A)$, where the $k$-operation $A$ is $k$-invertible. In this case $\overline{\theta}$ is a $k$-permutation and $\overline{\theta}^{-1} = (E_1, E_2, \ldots, E_{k-1}, {}^{(k)}A)$, where ${}^{(k)}A$ is the $k$-operation such that $A(x_1, x_2, \ldots, x_{k-1}, {}^{(k)}A(x_1^k)) = E_k(x_1^k) = x_k$. If $A$ is a polynomial $k$-operation, that is $A(x_1^k) = a_1x_1 + a_2x_2 + \ldots + a_kx_k$, where $a_k \neq 0$ , then ${}^{(k)}A(x_1^k) = a_k^{-1}(-a_1x_1 - a_2x_2 - \ldots - a_{k-1}x_{k-1} + x_k)$.

**Corollary 5.** *Let* $A_{i_0} \in \sum_G$*,* $B_i \in \sum_G \overline{\theta}^{-1}$*,* $\overline{\theta} = (E_1, E_2, \ldots, E_{k-1}, A_{i_0})$*. Then* $B_i(x_0^{k-1}) = (1 - a_i^{k-1}(a_{i_0}^{k-1})^{-1})x_0 + a_i(1 - a_i^{k-2}(a_{i_0}^{k-2})^{-1})x_1 + \ldots + a_i^{k-2}(1 - a_i(a_{i_0})^{-1})x_{k-2} + a_i^{k-1}(a_{i_0}^{k-1})^{-1}x_{k-1}$*, if* $i \in \overline{1, q-1}$*,* $i \neq i_0$ *and* $B_{i_0} = E_k$*. All* $B_i$ *for* $i \neq i_0$ *are polynomial* $k$*-quasigroups.*

*Proof.* If $A_{i_0} \in \sum_G$, then $A_{i_0}$ is a $k$-quasigroup and ${}^{(k)}A_{i_0}(x_0^{k-1}) = (a_{i_0}^{k-1})^{-1}(-x_0 - a_{i_0}x_1 - \ldots - a_{i_0}^{k-2}x_{k-2} + x_{k-1})$, so $B_i(x_0^{k-1}) = A_i\overline{\theta}^{-1}(x_0^{k-1}) = E_1(x_0^{k-1}) + a_iE_2(x_0^{k-1}) + a_i^2E_3(x_0^{k-1}) + ... + a_i^{k-2}E_{k-1}(x_0^{k-1}) + a_i^{k-1}\,{}^{(k)}A_{i_0}(x_0^{k-1}) = x_0 + a_ix_1 + a_i^2x_2 + \ldots + a_i^{k-2}x_{k-2} + a_i^{k-1}(a_{i_0}^{k-1})^{-1}(-x_0 - a_{i_0}x_1 - \ldots - a_{i_0}^{k-2}x_{k-2} + x_{k-1}) = (1 - a_i^{k-1}(a_{i_0}^{k-1})^{-1})x_0 + (a_i - a_i^{k-1}(a_{i_0}^{k-1})^{-1}a_{i_0})x_1 + \ldots + (a_i^{k-2} - a_i^{k-1}(a_{i_0}^{k-1})^{-1}a_{i_0}^{k-2})x_{k-2} + a_i^{k-1}(a_{i_0}^{k-1})^{-1}x_{k-1} = (1 - a_i^{k-1}(a_{i_0}^{k-1})^{-1})x_0 + (a_i - a_i^{k-1}(a_{i_0}^{k-2})^{-1})x_1 + \ldots + (a_i^{k-2} - a_i^{k-1}(a_{i_0})^{-1})x_{k-2} + a_i^{k-1}(a_{i_0}^{k-1})^{-1}x_{k-1} = (1 - a_i^{k-1}(a_{i_0}^{k-1})^{-1})x_0 + a_i(1 - a_i^{k-2}(a_{i_0}^{k-2})^{-1})x_1 + \ldots + a_i^{k-2}(1 - a_i(a_{i_0})^{-1})x_{k-2} + a_i^{k-1}(a_{i_0}^{k-1})^{-1}x_{k-1}$, $i \in \overline{1, q-1}$, if $B_i \in \sum_G \overline{\theta}^{-1}$. From this expression it follows that $B_{i_0} = E_k$ and all $k$-operations $B_i$, $i \neq i_0$, are polynomial $k$-quasigroups since all coefficients are different from 0. □

**Proposition 4.** *If in Proposition* 3 $\overline{\theta} = (A_{i_1}, A_{i_2}, \ldots, A_{i_k})$, $A_{i_l} \in \sum_{\overline{A}}$, $l \in \overline{1,k}$, $\overline{\theta}^{-1} = (D_1, D_2, \ldots, D_k)$, *then* $\sum_{\overline{A}}\overline{\theta}^{-1}$ *is a k-OSQ and* $B_{i_l} = E_l$, $l \in \overline{1,k}$, $B_i(x_1^k) = a_{i1}D_1(x_1^k) + a_{i2}D_2(x_1^k) + \ldots + a_{ik}D_k(x_1^k)$, $i \in \overline{1,t}$, $i \neq i_l$, $l \in \overline{1,k}$, *if* $B_i \in \sum_{\overline{A}}\overline{\theta}^{-1}$.

*Proof.* If $i \in \overline{1,t}$, $i \neq i_1, i_2, \ldots, i_k$, then $B_i = A_i(D_1, D_2, \ldots, D_k)$. But $A_{i_l} = E_l\overline{\theta}$ and $A_{i_l}\overline{\theta}^{-1} = E_l$, so $B_{i_l} = A_{i_l}\overline{\theta}^{-1} = E_l$ and the system $\sum_{\overline{A}}\overline{\theta}^{-1} = \{E_1, E_2, \ldots, E_k, B_i | i \in \overline{1,t}, i \neq i_1, i_2, \ldots, i_k\}$ is an orthogonal system of $k$-quasigroups ($k$-OSQ). □

Let $\sum \to (\sum\overline{\theta}\,\overline{\theta}_0)^T = (\sum\overline{\theta})^T\overline{\theta}_0$. Then, using (3), we obtain

**Proposition 5.** *Assume that* $B_i \in (\sum_{\overline{A}}\overline{\theta})^T\overline{\theta}_0$, *where* $\overline{\theta} = (C_1, C_2, \ldots, C_k)$, $\overline{\theta}_0 = (\beta_1E_1, \beta_2E_2, \ldots, \beta_kE_k)$ *and* $T = (\alpha_1, \alpha_2, \ldots, \alpha_t)$, *then* $B_i(x_1^k) = \alpha_i(a_{i1}C_1(\beta_jx_j)_{j=1}^k + a_{i2}C_2(\beta_jx_j)_{j=1}^k + \ldots + a_{ik}C_k(\beta_jx_j)_{j=1}^k)$, $i \in \overline{1,t}$.

Indeed, according to (3) $B_i(x_1^k) = \alpha_iA_i(C_1(\beta_jx_j)_{j=1}^k, C_2(\beta_jx_j)_{j=1}^k, \ldots, C_k(\beta_jx_j)_{j=1}^k) = \alpha_i(a_{i1}C_1(\beta_jx_j)_{j=1}^k + a_{i2}C_2(\beta_jx_j)_{j=1}^k + \ldots + a_{ik}C_k(\beta_jx_j)_{j=1}^k)$, $i \in \overline{1,t}$.

**Corollary 6.** *If* $B_i \in (\sum_G\overline{\theta})^T\overline{\theta}_0$, $\overline{\theta} = (C_1, C_2, \ldots, C_k)$, $\overline{\theta}_0 = (\beta_0E_1, \beta_1E_2, \ldots, \beta_{k-1}E_k)$, *then* $B_i(x_0^{k-1}) = \alpha_i(C_1(\beta_jx_j)_{j=0}^{k-1} + a_iC_2(\beta_jx_j)_{j=0}^{k-1} + \ldots + a_i^{k-1}C_k(\beta_jx_j)_{j=0}^{k-1})$, $i \in \overline{1, q-1}$. *If* $B_i \in (\sum_{\overline{G}}\overline{\theta})^T\overline{\theta}_0$, *then* $B_1(x_0^{k-1}) = \alpha_1C_1(\beta_jx_j)_{j=0}^{k-1}$, $B_2(x_0^{k-1}) = \alpha_2C_k(\beta_jx_j)_{j=0}^{k-1}$, $B_i(x_0^{k-1}) = \alpha_i(C_1(\beta_jx_j)_{j=0}^{k-1} + a_iC_2(\beta_jx_j)_{j=0}^{k-1} + \ldots + a_i^{k-1}C_k(\beta_jx_j)_{j=0}^{k-1})$, $i \in \overline{3, q+1}$.

Indeed, if $B_i \in (\sum_{\overline{G}}\overline{\theta})^T\overline{\theta}_0$, then

$$B_1(x_0^{k-1}) = \alpha_1E_1(C_1, C_2, \ldots, C_k)(\beta_jx_j)_{j=0}^{k-1} = \alpha_1C_1(\beta_jx_j)_{j=0}^{k-1},$$

$$B_2(x_0^{k-1}) = \alpha_2 E_k(C_1, C_2, \ldots, C_k)(\beta_j x_j)_{j=0}^{k-1} = \alpha_2 C_k(\beta_j x_j)_{j=0}^{k-1}.$$

Now let $\sum \rightarrow (\sum \overline{\theta}^{-1}\overline{\theta}_0)^T = (\sum \overline{\theta}^{-1})^T\overline{\theta}_0$ (see (1)).

**Proposition 6.** *If* $B_i \in (\sum_{\overline{A}} \overline{\theta}^{-1})^T\overline{\theta}_0$, *where* $\overline{\theta} = (A_{i_1}, A_{i_2}, \ldots, A_{i_k})$,$A_{i_l} \in \sum_{\overline{A}}$, $l \in \overline{1,k}$, $\overline{\theta}^{-1} = (D_1, D_2, \ldots, D_k)$, $\overline{\theta}_0 = (\beta_1 E_1, \beta_2 E_2, \ldots, \beta_k E_k)$, *then* $B_{i_l} = \alpha_{i_l}\beta_l E_l$, $l \in \overline{1,k}$, $B_i(x_1^k) = \alpha_i(a_{i1}D_1(\beta_j x_j)_{j=1}^k + a_{i2}D_2(\beta_j x_j)_{j=1}^k + \ldots + a_{ik}D_k(\beta_j x_j)_{j=1}^k)$, $i \in \overline{1,t}$, $i \neq i_1, i_2, \ldots, i_k$, *where* $B_i$, $i \neq i_1, i_2, \ldots, i_k$, *are* $k$*-quasigroups.*

This proposition is a consequence of Proposition 4, Proposition 5 and Remark 1 since
$B_{i_l}(x_1^k) = (\alpha_{i_l} A_{i_l}\overline{\theta}^{-1})\overline{\theta}_0(x_1^k) = (\alpha_{i_l}E_l)\overline{\theta}_0(x_1^k) = \alpha_{i_l}E_l(\beta_j x_j)_{j=1}^k = \alpha_{i_l}\beta_l E_l(x_1^k)$, $l \in \overline{1,k}$.

**Corollary 7.** *If* $\sum_{\overline{G}} = \{E_1, E_k, A_1, A_2, \ldots, A_{q-1}\} = \{P_1, P_2, \ldots, P_{q+1}\}$, $\overline{\theta} = (P_{i_1}, P_{i_2}, \ldots, P_{i_k})$, $i_1, i_2, \ldots, i_k \in \overline{1, q+1}$, $\overline{\theta}^{-1} = (D_1, D_2, \ldots, D_k)$, $\overline{\theta}_0 = (\beta_0 E_1, \beta_1 E_2, \ldots, \beta_{k-1}E_k)$, $B_i \in (\sum_{\overline{G}} \overline{\theta}^{-1})^T\overline{\theta}_0$, *then* $B_{i_l} = \alpha_{i_l}\beta_{l-1}E_l$, $l \in \overline{1,k}$, $B_i(x_0^{k-1}) = \alpha_i(D_1(\beta_j x_j)_{j=0}^{k-1} + a_i D_2(\beta_j x_j)_{j=0}^{k-1} + \ldots + a_i^{k-1}D_k(\beta_j x_j)_{j=0}^{k-1})$, $i \in \overline{1, q+1}$, $i \neq i_1, i_2, \ldots, i_k$. *All* $B_i$, $i \neq i_1, i_2, \ldots, i_k$, *are* $k$*-quasigroups.*

Indeed, in this case $B_{i_l}(x_0^{k-1}) = (\alpha_{i_l}P_{i_l}\overline{\theta}^{-1})\overline{\theta}_0(x_0^{k-1}) = (\alpha_{i_l}E_l)\overline{\theta}_0(x_0^{k-1}) = \alpha_{i_l}E_l(\beta_j x_j)_{j=0}^{k-1} = \alpha_{i_l}\beta_{l-1}E_l(x_0^{k-1})$, $l \in \overline{1,k}$. The rest $k$-operations are $k$-quasigroups by Remark 1.

If $\overline{\theta}^{-1} = (D_1, D_2, \ldots, D_k)$, then the $k$-operations $B_i$ of $(\sum_G \overline{\theta}^{-1})^T\overline{\theta}_0$, $i \in \overline{1, q-1}$, where $\sum_G = \{A_1, A_2, \ldots, A_t\}$, $\overline{\theta} = (A_{i_1}, A_{i_2}, \ldots, A_{i_k})$, $A_{i_l} \in \sum_G$, $l \in \overline{1,k}$, have the same form as in Corollary 7.

The transformations of $k$-OSOs, given above, allow to construct new secret-sharing schemes or to renew (to renovate secret keys) the known secret-sharing schemes, in particular, based on a Reed-Solomon or an extended Reed-Solomon code in the pointed numerous ways.

**Acknowledgements.** The research in this article was made in part by support of the Russian Fond of Fundamental Research (Grant 08.820.08.08 RFFI).

## References

[1] **A. P. Alferov, A. Yu. Zubov, A. S. Kuz'min, F. V. Cheremushkin**, *Foundations of cryptography*, (Russian), Gelios ARV, 2005.

[2] **A. S. Bektenov and T. Yakubov**, *Systems of orthogonal $n$-ary operations*, (Russian), Izvestiya AN Mold. SSR, Ser. fiz.-mat. nauk **3** (1974), 7 – 14.

[3] **V. D. Belousov**, *Systems of orthogonal operations*, (Russian), Matem. Sbornik **77 (119)** (1968), 38 – 58.

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

[5] **G. Belyavskaya and G. L. Mullen**, *Strongly orthogonal and uniformly orthogonal many-placed operations*, Algebra Discr. Math. **1** (2006), 1 – 17.

[6] **J. Dénes and A. D. Keedwell**, *Latin squares and their applications*, Acadèmiai Kiado, Budapest and Academic Press, New York, 1974.

[7] **J. Dénes and A. D. Keedwell**, *Latin squares. New Developments in the Theory and Applications*, Annals of Discrete Math. 46, North-Holland, 1991.

[8] **J. W. Greene, M. E. Hellman and E. D. Karnin**, *On secret sharing systems*, IEEE Trans. Information Theory IT-29 (1983), 35 – 41.

[9] **V. I. Izbash and P. Syrbu**, *Recursively differentiable quasigroups and complete recursive codes*, Comm. Math. Univ. Carolinae **45** (2004), 257 – 263.

[10] **C. F. Laywine, G. L. Mullen, and G. Whittle**, *D-dimensional hypercubes and the Euler and MacNeish conjectures*, Monatsh. Math. **111** (1995), 223 – 238.

[11] **R. McEliece and D. V. Sarwarte**, *On sharing secrets and Reed Solomon codes*, Comm. ACM **24** (1981), 583 – 584.

[12] **A. Shamir**, *How to share a secret*, Comm. ACM **22** (1979), 612 – 613.

[13] **G. L. Simmons (ed.)**, *Contemporary Cryptology – The Science of Information Integrity*, IEEE Press, New-York, 1992.

[14] **Z. Stojaković and J. Ušan**, *Orthogonal systems of partial operations*, Univ. u Novom Sadu, Zb. Rad. Prirod.-Mat. Fak. **8** (1978), 47 – 51.

[15] **J. Ušan**, *Orthogonal systems of $n$-ary operations and codes*, Mat. Vesnik **2** (1978), 91 – 93.

[16] **W. W. Wu**, *Elements of Digital Satellite Communication*, Computer Science Press, New York, 1985.

Received May 19, 2009

Institute of Mathematics and Computer Science, Academy of Sciences, Academiei str. 5,
MD-2028 Chisinau, Moldova
E-mail: gbel1@rambler.ru

Quasigroups and Related Systems **17** (2009), 177 – 190

# Prolongations of quasigroups by middle translations

*Ivan I. Deriyenko and Andrey I. Deriyenko*

**Abstract.** This article is a continuation of the study of prolongations of quasigroups and Latin squares. Now using complete mappings and middle translations we present various characterizations of prolongations of quasigroups described in [4]. Based on these characterizations we find isotopic prolongations.

## 1. Introduction

Let $Q = \{1, 2, 3, \dots, n\}$ be a finite set, $\varphi$ and $\psi$ permutations of $Q$. The composition of permutations is defined as $\varphi\psi(x) = \varphi(\psi(x))$. Permutations will be written in the form of cycles, and cycles will be separated by points:

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix} = (132.45.6.)$$

$Q(\cdot)$ always denotes a quasigroup.

**Definition 1.1.** A permutation $\varphi_i$ of the set $Q$ such that

$$x \cdot \varphi_i(x) = i, \qquad i \in Q \tag{1}$$

all $x \in Q$ is called the *track* of an element $i$.

It is clear that for a quasigroup $Q(\cdot)$ of order $n$ the set of permutations

$$\{\varphi_1, \varphi_2, \varphi_3, \dots, \varphi_n\},$$

satisfying (1) uniquely determines its Latin square (i.e., its multiplication table). Therefore, we can identify $Q(\cdot)$ with the above set of permutations and write

$$Q(\cdot) = \{\varphi_1, \varphi_2, \varphi_3, \dots, \varphi_n\}.$$

2000 Mathematics Subject Classification: 05B15; 20N05
Keywords: quasigroup, prolongation, isotopism.

In [3] the following very useful result is proved

**Lemma 1.2.** *Let* $Q(\cdot) = \{\varphi_1, \varphi_2, \dots, \varphi_n\}$ *and* $Q(\circ) = \{\psi_1, \psi_2, \dots, \psi_n\}$ *be two quasigroups. Then for any bijections* $\alpha, \beta, \gamma : Q \to Q$ *satisfying the identity* $\gamma(x \circ y) = \alpha(x) \cdot \beta(y)$ *we have* $\psi_{\gamma(i)} = \beta\varphi_i\alpha^{-1}$. □

**Definition 1.3.** Any mapping $\sigma$ of $Q$ defines on a quasigroup $Q(\cdot)$ a new mapping $\bar{\sigma}$ such that

$$\bar{\sigma}(x) = x \cdot \sigma(x), \qquad x \in Q.$$

The number $rg(\sigma) = |\bar{\sigma}(Q)|$, where $\bar{\sigma}(Q) = \{\bar{\sigma}(x) \,|x \in Q\}$, is called the *range of a mapping* $\sigma$ on a quasigroup $Q(\cdot)$.

If $\bar{\sigma}(Q) = Q$, i.e., $rg(\sigma) = n = |Q|$, then we say that $\sigma$ is a *complete mapping.* A quasigroup having at least one complete mapping is called *admissible.* If $rg(\sigma) = n - 1$, the mapping $\sigma$ is called *quasicomplete.* Every track has range 1.

For a quasicomplete mapping $\sigma$ we define its *defect* $def(\sigma)$ putting

$$def(\sigma) = Q - \bar{\sigma}(Q).$$

If $def(\sigma) = d$, then $\bar{\sigma}^{-1}(d) = \emptyset$. In this case $a = \bar{\sigma}(a_1) = \bar{\sigma}(a_2)$ for some $a, a_1, a_2 \in Q$.

It is clear that a permutation $\varphi$ of $Q$ can be extended to $Q' = Q \cup \{q\}$, where $q \notin Q$, by putting $\varphi(q) = q$.

## 2. Classical prolongation

The *classical* method of prolongation of admissible quasigroups proposed by V. D. Belousov [1] is based on the following construction. Let $Q(\cdot)$ be a fixed admissible quasigroup, $\sigma$ its complete mapping. The operation $(\circ)$ on $Q' = Q \cup \{q\}$ is defined by the formula:

$$x \circ y = \begin{cases} x \cdot y & \text{if} \quad x \neq q, \ y \neq q, \ y \neq \sigma(x), \\ \bar{\sigma}\sigma^{-1}(y) & \text{if} \quad x = q, \ y \neq q, \\ \bar{\sigma}(x) & \text{if} \quad x \neq q, \ y = q, \\ q & \text{if} \quad y = \sigma(x), \ x \in Q'. \end{cases} \tag{2}$$

We say that this prolongation is *induced* by a complete mapping $\sigma$.

By $\Delta_\sigma$ we denote the set

$$\Delta_\sigma = \{\sigma_1, \sigma_2, \dots, \sigma_n \mid \sigma_i = \big(q, \bar{\sigma}^{-1}(i)\big)\},$$

where $Q(\cdot)$ is a quasigroup, $q \notin Q$ and $\sigma$ is a complete mapping of $Q(\cdot)$.

Below we present the new description of this prolongation. But first we make some useful observations.

Note first that

$$x_i \cdot \sigma(x_i) = \bar{\sigma}(x_i) = i. \tag{3}$$

Hence

$$x_i = \bar{\sigma}^{-1}(i). \tag{4}$$

Thus the transposition $\sigma_i$ in $\Delta_\sigma$ can be written in the form $\sigma_i = (q, x_i)$. Moreover, from (1) it follows $x_i \cdot \varphi_i(x_i) = i$, which together with (3) gives

$$\sigma(x_i) = \varphi_i(x_i). \tag{5}$$

Now we can give the new characterization of the classical prolongation.

**Theorem 2.1.** *Let $Q(\cdot) = \{\varphi_1, \varphi_2, \varphi_3, \dots, \varphi_n\}$ be a quasigroup with a complete mapping $\sigma$. The quasigroup $Q'(\circ) = \{\psi_1, \psi_2, \psi_3, \dots, \psi_n, \psi_q\}$ coincides with the prolongation of $Q(\cdot)$ defined by (2) if and only if*

$$\begin{cases} \psi_i = \varphi_i \sigma_i & i = 1, 2, \dots, n, \\ \psi_q = \sigma, \end{cases} \tag{6}$$

*where $\sigma_i = \big(q, \bar{\sigma}^{-1}(i)\big)$.*

*Proof.* The first, the second and the third row of (2) is equivalent to the first row of (6). The last row of (2) is equivalent to the second row of (6).

Indeed, the first row of (2) says that

$$x \circ y = x \cdot y \quad \text{for} \quad x \neq q, \; y \neq q, \; y \neq \sigma(x).$$

This for $y = \varphi_i(x)$ gives

$$x \circ \varphi_i(x) = x \cdot \varphi_i(x) = i.$$

Since $x \circ \psi_i(x) = i$, the last implies

$$\varphi_i = \psi_i \quad \text{for} \quad x \neq q, \; y \neq q, \; y \neq \sigma(x). \tag{7}$$

If $x = q$, then from the second row of (2), we obtain

$$q \circ y = \bar{\sigma}\sigma^{-1}(y) \qquad \text{for} \qquad y \neq q,\ y \in Q, \tag{8}$$

whence putting $y = \psi_i(q)$ we get $\bar{\sigma}\sigma^{-1}\psi_i(q) = q \circ \psi_i(q) = i$. Thus $\sigma^{-1}\psi_i(q) = \bar{\sigma}^{-1}(i)$. But $x_i = \bar{\sigma}^{-1}(i)$, so $\psi_i(q) = \sigma(x_i)$, and consequently

$$\psi_i(q) = \varphi_i(x_i). \tag{9}$$

In the case $y = q$, according to the third row of (2), we have $x \circ q = \bar{\sigma}(x)$. If $x \circ q = i$, then $\bar{\sigma}(x) = i$, i.e., $x = \bar{\sigma}^{-1}(i)$, which, by (4), implies $x = x_i$. Hence $x_i \circ q = i$. But on the other hand, by the definition of $\psi_i$, we have $x_i \circ \psi_i(x_i) = i$. So,

$$\psi_i(x_i) = q. \tag{10}$$

Let us consider the first row of (6).

If $x \neq q$ and $x \neq x_i$, then $\sigma_i = (q, x_i)$ can be eliminated from $\psi_i = \varphi_i\sigma_i$. Hence $\psi_i = \varphi_i$. This coincides with (7) and corresponds to the first row of (2).

If $x = q$, then $\psi_i(q) = \varphi_i\sigma_i(q) = \varphi_i(x_i)$. This coincides with (9) and corresponds to the second row of (2).

If $x = x_i$, then $\psi_i(x_i) = \varphi_i\sigma_i(x_i) = \varphi_i(q) = q$. This coincides with (10) and corresponds to the third row of (2).

So, the first, the second and the third rows of (2) correspond to the first row of (6).

Let us consider the fourth row of (2). Then $y = \sigma(x)$ and $x \circ \sigma(x) = q$. But, by the definition, $x \circ \psi_q(x) = q$. Thus $\psi_q(x) = \sigma(x)$. This means that the fourth row of (2) is equivalent to the second row of (6). □

Since quasigroups may have several complete mappings, the natural question is: *when prolongations obtained from the same quasigroup by different complete mappings are isotopic.*

Below we give the partial answer to this question. Our answer is based on the concept of the equivalence of complete mappings.

Remind (see for example [1]) that two permutations $\rho$ and $\sigma$ of a quasigroup $Q(\cdot)$ are *equivalent* if

$$\rho = \beta\sigma\alpha^{-1}$$

for some autotopism $T = (\alpha, \beta, \gamma)$ of $Q(\cdot)$.

**Proposition 2.2.** *Any mapping equivalent to a complete mapping of a quasigroup $Q(\cdot)$ also is a complete mapping of $Q(\cdot)$.*

*Proof.* Let $\rho = \beta\sigma\alpha^{-1}$, where $\sigma$ is a complete mapping of a quasigroup $Q(\cdot)$ and $T = (\alpha, \beta, \gamma)$ its autotopism.

Let $\{\varphi_1, \varphi_2, \varphi_3, \dots, \varphi_n\}$ be tracks of $Q(\cdot)$. We can choose elements $x_1, x_2, \dots, x_n$ of $Q$ for which $\sigma(x_i) = \varphi_i(x_i)$.

Since $\varphi_{\gamma(i)} = \beta\varphi_i\alpha^{-1}$ (see Lemma 1.2), for $y_1, y_2, \dots, y_n$ such that $y_i = \alpha(x_i)$, $i = 1, 2, \dots, n$, we have

$$\rho(y_i) = \beta\sigma\alpha^{-1}(y_i) = \beta\sigma(x_i) = \beta\varphi_i(x_i) = \varphi_{\gamma(i)}\alpha(x_i) = \varphi_{\gamma(i)}(y_i).$$

Thus $\rho(y_i) = \varphi_{\gamma(i)}(y_i)$.

Multiplying this equation by $y_i$ we obtain

$$y_i \cdot \rho(y_i) = y_i \cdot \varphi_{\gamma(i)}(y_i) = \gamma(i),$$

which proves that $\rho$ is a complete mapping. □

**Corollary 2.3.** *If $\alpha$ is an automorphism of a quasigroup $Q(\cdot)$ and $\sigma$ is its complete mapping, then $\rho = \alpha\sigma\alpha^{-1}$ also is a complete mapping of $Q(\cdot)$.* □

**Corollary 2.4.** *If $T = (\alpha, \beta, \gamma)$ is an autotopism of $Q(\cdot)$ and $\sigma_0$ is its complete mapping, then*

$$\sigma_k = \beta^k\sigma_0\alpha^{-k}$$

*is a complete mapping of $Q(\cdot)$.* □

**Corollary 2.5.** *Equivalent permutations have the same range.* □

**Theorem 2.6.** *Classical prolongations induced by equivalent complete mappings are isotopic.*

*Proof.* Let $Q'_\sigma(\circ) = \{\psi_1, \psi_2, \dots, \psi_n, \psi_q\}$ and $Q'_\rho(*) = \{\omega_1, \omega_2, \dots, \omega_n, \omega_q\}$ be prolongations of a quasigroup $Q(\cdot) = \{\varphi_1, \varphi_2, \dots, \varphi_n\}$ induced by complete mappings $\sigma$ and $\rho = \beta\sigma\alpha^{-1}$, respectively. Then, according to Theorem 2.1, we have

$$\begin{cases} \psi_i = \varphi_i\sigma_i & i = 1, 2, \dots, n, \\ \psi_q = \sigma, \end{cases} \qquad \text{and} \qquad \begin{cases} \omega_i = \varphi_i\rho_i & i = 1, 2, \dots, n, \\ \omega_q = \rho, \end{cases}$$

where $\sigma_i = (q, x_i)$, $\rho_i = (q, y_i)$.

Let us consider two sequences $x_1, x_2, \dots, x_n$ and $y_1, y_2, \dots, y_n$ of elements of $Q$ such that

$$\varphi_i(x_i) = \sigma(x_i) \quad \text{and} \quad \varphi_i(y_i) = \rho(y_i) \tag{11}$$

for $i = 1, 2, \dots, n$.

Since $T = (\alpha, \beta, \gamma)$ is an autotopism of $Q(\cdot)$ such that $\rho = \beta\sigma\alpha^{-1}$, by Lemma 1.2, we obtain $\varphi_{\gamma(i)} = \beta\varphi_i\alpha^{-1}$. Thus

$$\varphi_{\gamma(i)}\alpha(x_i) = \beta\varphi_i(x_i) = \beta\sigma(x_i) = \rho\alpha(x_i),$$

i.e., $\varphi_{\gamma(i)}\alpha(x_i) = \rho\alpha(x_i)$, which for $\alpha(x_i) = z$ gives $\varphi_{\gamma(i)}(z) = \rho(z)$. But, by the assumption $\varphi_{\gamma(i)}\left(y_{\gamma(i)}\right) = \rho\left(y_{\gamma(i)}\right)$ (see (11)), hence $z = y_{\gamma(i)}$. Therefore

$$\alpha(x_i) = y_{\gamma(i)} \tag{12}$$

for every $i = 1, 2, \dots, n$.

Now we will prove that

$$\alpha\sigma_i\alpha^{-1} = \rho_{\gamma(i)}. \tag{13}$$

Indeed, according to the definition $\sigma_i = (q, x_i)$ and $\rho_{\gamma(i)} = \left(q, y_{\gamma(i)}\right)$. Thus

$$\begin{aligned}\alpha\sigma_i\alpha^{-1}\left(y_{\gamma(i)}\right) &= \alpha\sigma_i(x_i) = \alpha(q) = q,\\ \alpha\sigma_i\alpha^{-1}(q) &= \alpha\sigma_i(q) = \alpha(x_i) = y_{\gamma(i)}.\end{aligned}$$

This means that $\alpha\sigma_i\alpha^{-1} = \left(q, y_{\gamma(i)}\right) = \rho_{\gamma(i)}$. So, (13) is valid.

Moreover,

$$\begin{aligned}\beta\psi_i\alpha^{-1} &= \beta(\varphi_i\sigma_i)\alpha^{-1} = \beta\varphi_i\left(\alpha^{-1}\alpha\right)\sigma_i\alpha^{-1}\\ &= (\beta\varphi_i\alpha^{-1})(\alpha\sigma_i\alpha^{-1}) = \varphi_{\gamma(i)}\rho_{\gamma(i)} = \omega_{\gamma(i)},\end{aligned}$$

and

$$\beta\psi_q\alpha^{-1} = \beta\sigma\alpha^{-1} = \rho = \omega_q.$$

From the above it follows that $T = (\alpha, \beta, \gamma)$ is an isotopism between $Q'(\circ)$ and $Q'(*)$. This completes the proof. □

**Example 2.7.** Consider the quasigroup $Q(\cdot)$ with the multiplication table:

| $\cdot$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 1 | 4 | 3 | 6 | 5 |
| 3 | 3 | 4 | 5 | 6 | 1 | 2 |
| 4 | 4 | 3 | 6 | 5 | 2 | 1 |
| 5 | 5 | 6 | 2 | 1 | 4 | 3 |
| 6 | 6 | 5 | 1 | 2 | 3 | 4 |

This quasigroup can be written as $Q(\cdot) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}$, where

$$\begin{aligned} &\varphi_1 = (1.2.3546.), \quad &\varphi_2 = (12.3645.), \quad &\varphi_3 = (13.24.56.),\\ &\varphi_4 = (14.23.5.6.), \quad &\varphi_5 = (15.26.3.4.), \quad &\varphi_6 = (16.25.34.). \end{aligned}$$

Choose the following two complete mappings of this quasigroup:

$$\rho_0 = (1.3.6.245.) \quad \text{and} \quad \theta = (1.23456.)\,.$$

Then $\bar{\rho}_0 = (1.23564.)$ and $\bar{\theta} = (1.24.365.)$.

Consider now the autotopism $T = (\alpha, \beta, \gamma)$ of $Q(\cdot)$, where

$$\alpha = (163254.)\,, \quad \beta = (164.253.)\,, \quad \gamma = (146235.)\,.$$

We can construct this autotopism used, for example, the method proposed in [3].

Let $\rho_1 = \beta\rho_0\alpha^{-1} = T\,(\rho_0)$ and $T^k\,(\rho_0) = \rho_k$ for $k \geqslant 1$. Then

$$\begin{aligned} &T\,(\rho_0) = (1345.2.6.) = \rho_1, \qquad &T\,(\rho_1) = (13462.5.) = \rho_2,\\ &T\,(\rho_2) = (143562.) = \rho_3, \qquad &T\,(\rho_3) = (12356.4.) = \rho_4,\\ &T\,(\rho_4) = (1.4.2365.) = \rho_5, \qquad &T\,(\rho_5) = (1.3.6.245.) = \rho_0. \end{aligned}$$

By Corollary 2.4 all mappings $\rho_1, \rho_2, \ldots, \rho_5$ are completeon $Q(\cdot)$. These mappings are equivalent. Hence, by Theorem 2.6, all prolongations $Q'_{\rho_i}\,(\circ)$ of $Q(\cdot)$ are isotopic.

We select two prolongations $Q'_{\rho_0}\,(\circ)$ and $Q'_{\rho_3}(*)$. For simplicity $\rho_0$ will be denoted by $\sigma$, $\rho_3$ – by $\tau$. Since $\beta^3\sigma\alpha^{-3} = \tau$, $\rho$ and $\tau$ are equivalent, and $\bar{\sigma} = (1.23564.)$, $\bar{\tau} = (14653.2.)$.

Let $Q'_\sigma\,(\circ) = \{\psi_1, \psi_2, \ldots, \psi_6, \psi_7\}$, $Q'_\tau\,(*) = \{\omega_1, \omega_2, \ldots, \omega_6, \omega_7\}$. Then $q = 7$ and

$$\Delta_\sigma = \{\sigma_1 = (7,1),\ \sigma_2 = (7,4),\ \sigma_3 = (7,2),\ \sigma_4 = (7,6),\ \sigma_5 = (7,3),\ \sigma_6 = (7,5)\},$$
$$\Delta_\tau = \{\tau_1 = (7,3)\,,\ \tau_2 = (7,2)\,,\ \tau_3 = (7,5)\,,\ \tau_4 = (7,1)\,,\ \tau_5 = (7,6)\,,\ \tau_6 = (7,4)\}.$$

According to (2), the multiplication table of $Q'_\sigma(\circ)$ has the form:

| ∘ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | 7 | 2 | 3 | 4 | 5 | 6 | 1 |
| 2 | 2 | 1 | 4 | 7 | 6 | 5 | 3 |
| 3 | 3 | 4 | 5 | 6 | 7 | 2 | 1 |
| 4 | 4 | 3 | 7 | 5 | 1 | 1 | 6 |
| 5 | 5 | 6 | 2 | 1 | 4 | 7 | 3 |
| 6 | 6 | 7 | 1 | 2 | 3 | 4 | 5 |
| 7 | 2 | 5 | 6 | 4 | 1 | 3 | 7 |

By Theorem 2.1, $Q'_\sigma(\circ)$ has the following tracks:

$$\begin{aligned}
\psi_1 &= \varphi_1\sigma_1 = (1.2.3546.7.)\,(7,1) &&= (17.2.3546.)\,,\\
\psi_2 &= \varphi_2\sigma_2 = (12.3645.7.)\,(7,4) &&= (12.36475.)\,,\\
\psi_3 &= \varphi_3\sigma_3 = (13.24.56.7.)\,(7,2) &&= (13.274.56.)\,,\\
\psi_4 &= \varphi_4\sigma_4 = (14.23.5.6.7.)\,(7,6) &&= (14.23.5.67.)\,,\\
\psi_5 &= \varphi_5\sigma_5 = (15.26.3.4.7.)\,(7,3) &&= (15.26.37.4.)\,,\\
\psi_6 &= \varphi_6\sigma_6 = (16.25.43.7.)\,(7,5) &&= (16.257.43.)\,,\\
\psi_7 &= \quad\sigma \quad\;\; = (1.3.6.245.7.)\,.
\end{aligned}$$

Similarly, $Q'_\tau(*)$ has the multiplication table:

| $*$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 7 | 5 | 6 | 4 |
| 2 | 7 | 1 | 4 | 3 | 6 | 5 | 2 |
| 3 | 3 | 4 | 5 | 6 | 7 | 2 | 1 |
| 4 | 4 | 3 | 7 | 5 | 1 | 1 | 6 |
| 5 | 5 | 6 | 2 | 1 | 4 | 7 | 3 |
| 6 | 6 | 7 | 1 | 2 | 3 | 4 | 5 |
| 7 | 2 | 5 | 6 | 4 | 1 | 3 | 7 |

and tracks:

$$\begin{aligned}
\omega_1 &= \varphi_1\tau_1 = (1.2.3546.7.)\,(7,3) &&= (1.2.37546.)\,,\\
\omega_2 &= \varphi_2\tau_2 = (12.3645.7.)\,(7,2) &&= (127.3645.)\,,\\
\omega_3 &= \varphi_3\tau_3 = (13.24.56.7.)\,(7,5) &&= (13.24.576.)\,,\\
\omega_4 &= \varphi_4\tau_4 = (14.23.5.6.7.)\,(7,1) &&= (174.23.5.6.)\,,\\
\omega_5 &= \varphi_5\tau_5 = (15.26.3.4.7.)\,(7,6) &&= (15.267.3.4.)\,,\\
\omega_6 &= \varphi_6\tau_6 = (16.25.43.7.)\,(7,4) &&= (16.25.473.)\,,\\
\omega_7 &= \quad\tau \quad\;\; = (143562.7.)\,.
\end{aligned}$$

$T^3 = \left(\alpha^3, \beta^3, \gamma^3\right)$ is an isotopism between $Q'_\sigma(\circ)$ and $Q'_\tau(*)$. Hence, by (3) from [3], we have $\beta^3\psi_i\alpha^{-3} = \omega_{\gamma^3(i)}$. This fact can be deduced from the above calculations because $\beta^3 = \varepsilon$, $\alpha^{-3} = (12.34.56.7.)$, $\gamma^3 = (12.24.56.7.)$ and, as it is not difficult to see, $\psi_i\alpha^{-3} = \omega_{\gamma^3(i)}$ for every $i \in Q'$.

Consider now the prolongation $Q'_\theta(\times)$ of $Q(\cdot)$ induced by the complete mapping $\theta = (1.23456.)$. Then $\bar{\theta} = (1.24.365.)$, $\bar{\theta}^{-1} = (1.24.356.)$ and

$$\Delta_\theta = \{\theta_1 = (7,1)\,,\ \theta_2 = (7,4)\,,\ \theta_3 = (7,5)\,,\ \theta_4 = (7,2)\,,\ \theta_5 = (7,6)\,,\ \theta_6 = (7,3)\}.$$

Quasigroups $Q'_\theta(\times)$ and $Q'_\tau(*)$ are not isotopic because complete mappings $\theta$ and $\tau$ are not equivalent. $Q'_\theta(\times)$ has the multiplication table:

| × | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| 1 | 7 | 2 | 3 | 4 | 5 | 6 | 1 |
| 2 | 2 | 1 | 7 | 3 | 6 | 5 | 4 |
| 3 | 3 | 4 | 5 | 7 | 1 | 2 | 6 |
| 4 | 4 | 3 | 6 | 5 | 7 | 1 | 2 |
| 5 | 5 | 6 | 2 | 1 | 4 | 7 | 3 |
| 6 | 6 | 7 | 1 | 2 | 3 | 4 | 5 |
| 7 | 1 | 5 | 4 | 6 | 2 | 3 | 7 |

and tracks:

$$\begin{aligned}
\lambda_1 &= \varphi_1\theta_1 = (1.2.3546.7.)\,(7,1) = (17.2.3546.)\,,\\
\lambda_2 &= \varphi_2\theta_2 = (12.3645.7.)\,(7,4) = (12.36475.)\,,\\
\lambda_3 &= \varphi_3\theta_3 = (13.24.56.7.)\,(7,5) = (13.24.576.)\,,\\
\lambda_4 &= \varphi_4\theta_4 = (14.23.5.6.7.)\,(7,2) = (14.273.5.6.)\,,\\
\lambda_5 &= \varphi_5\theta_5 = (15.26.3.4.7.)\,(7,6) = (15.267.3.4.)\,,\\
\lambda_6 &= \varphi_6\theta_6 = (16.25.43.7.)\,(7,3) = (16.25.437.)\,,\\
\lambda_7 &= \quad \theta \quad = (1.23456.7.)\,.
\end{aligned}$$

The fact that these two quasigroups are non-isotopic can be also deduced from Theorem 2.5 in [3]. □

## 3. Prolongations by fixed element

Consider now the prolongation proposed by G. B. Belyavskaya (see [2] or [4]). This prolongation is a modyfication of a prolongation proposed by V. D. Belousov.

Let $Q\,(\cdot)$ be a quasigroup with a complete mapping $\sigma$. Then for an arbitrary fixed element $a \in Q$ there exists an uniquely determined element $x_a \in Q$ such that

$$x_a \cdot \sigma\,(x_a) = a. \tag{14}$$

Using this fixed element $a \in Q$ and a complete mapping $\sigma$ we can define the prolongation $Q'_{\sigma,a}\,(\circ)$ of $Q\,(\cdot)$ by putting

$$x \circ y = \begin{cases} x \cdot y & y \neq \sigma(x), \ x, y \in Q, \\ q & y = \sigma(x), \ x \neq x_a, \\ a & x = x_a, \ y = \sigma(x_a), \\ \bar{\sigma}(x) & x \neq x_a, \ y = q, \\ \bar{\sigma}\sigma^{-1}(y) & x = q, \ y \neq \sigma(x_a), \\ q & x = q, \ y = \sigma(x_a), \\ q & x = x_a, \ y = q, \\ a & x = y = q. \end{cases} \tag{15}$$

It is clear that for one complete mapping $\sigma$ of $Q(\cdot)$ one can find $n = |Q|$ different elements satisfying (14). So, one complete mapping induces $n$ different prolongations of the form $Q'_{\sigma,a}(\circ)$. Obviously, some of these prolongations can be isotopic.

First observe that the prolongation $Q'_{\sigma,a}(\circ)$ can be characterized by their tracks. Namely, we have

**Theorem 3.1.** *Let $Q(\cdot) = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ be a quasigroup with a complete mapping $\sigma$. The quasigroup $Q'(\circ) = \{\psi_1, \psi_2, \ldots, \psi_n, \psi_q\}$ coincides with the prolongation $Q'_{\sigma,a}(\circ)$ of $Q(\cdot)$ defined by* (15) *if and only if*

$$\begin{cases} \psi_i = \varphi_i \sigma_i, \quad i \neq a, q, \\ \psi_a = \varphi_a, \\ \psi_q = \sigma\sigma_a, \end{cases} \tag{16}$$

*where $\sigma_a = (q, x_a)$ and $\sigma_i = (q, \bar{\sigma}^{-1}(i))$.*

*Proof.* The proof of this theorem is similar to the proof of Theorem 2.1. □

Using this theorem we can prove

**Theorem 3.2.** *Let $T = (\alpha, \beta, \gamma)$ be an autotopism of a quasigroup $Q(\cdot)$ with a complete mapping $\sigma$. If $\beta\sigma\alpha^{-1} = \rho$, then prolongations $Q'_{\sigma,a}(\circ)$ and $Q'_{\rho,b}(*)$, where $b = \gamma(a)$, are isotopic.*

*Proof.* Let $Q'_{\sigma,a}(\circ) = \{\psi_1, \psi_2, \ldots, \psi_n, \psi_q\}$ and $Q'_{\rho,b}(*) = \{\omega_1, \omega_2, \ldots, \omega_n, \omega_q\}$, where $b = \gamma(a)$. In this case

$$\begin{cases} \psi_i = \varphi_i \sigma_i, \quad i \neq a, q, \\ \psi_a = \varphi_a, \\ \psi_q = \sigma\sigma_a, \end{cases} \quad \text{and} \quad \begin{cases} \omega_i = \varphi_i \rho_i, \quad i \neq b, q, \\ \omega_b = \varphi_b, \\ \omega_q = \sigma\rho_b, \end{cases}$$

where $\sigma_a = (q, x_a)$, $\rho_b = (q, y_b)$ and $\sigma_i = (q, x_i)$, $\rho_i = (q, y_i)$.

Since $\varphi_{\gamma(i)} = \beta\varphi_i\alpha^{-1}$ for any autotopism $T = (\alpha, \beta, \gamma)$ of $Q(\cdot)$ (Lemma 1.2), for $i \neq a, q$ we have

$$\beta\psi_i\alpha^{-1} = \beta\varphi_i\sigma_i\alpha^{-1} = \beta\varphi_i\alpha^{-1}\alpha\sigma_i\alpha^{-1} = \varphi_{\gamma(i)}\rho_{\gamma(i)} = \omega_{\gamma(i)},$$

where $\alpha\sigma_i\alpha^{-1} = \rho_{\gamma(i)}$ (as in the proof of Theorem 2.6).

For $i = a$ we obtain $\beta\psi_a\alpha^{-1} = \varphi_{\gamma(a)} = \varphi_b = \omega_b$. Similarly, if $i = q$, then

$$\beta\psi_q\alpha^{-1} = \beta\sigma\sigma_a\alpha^{-1} = \beta\sigma\alpha^{-1}\alpha\sigma_a\alpha^{-1} = \sigma\alpha\sigma_a\alpha^{-1} = \sigma\rho_{\gamma(a)} = \sigma\rho_b = \omega_q.$$

From the above it follows that $T = (\alpha, \beta, \gamma)$ is an isotopism between $Q'_{\sigma,a}(\circ)$ and $Q'_{\rho,b}(*)$. □

**Corollary 3.3.** *Is $\sigma$ is a complete mapping on $Q(\cdot)$ such that $\alpha\sigma\alpha^{-1} = \rho$ for some automorphism $\alpha$ of $Q(\cdot)$, then prolongations $Q'_{\sigma,a}(\circ)$ and $Q'_{\rho,b}(*)$, where $b = \alpha(a)$, are isomorphic.* □

**Example 3.4.** Consider the group $Q(\cdot)$ isomorphic to the group $\mathbb{Z}_5$.

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

This group has the following tracks: $\varphi_1 = (1.25.34.)$, $\varphi_2 = (12.35.4.)$, $\varphi_3 = (13.45.2.)$, $\varphi_4 = (14.23.5.)$, $\varphi_5 = (15.24.3.)$.

The permutation $\sigma = (1.2453.)$ is a complete mapping of this quasigroup, $\alpha = (1.2354.)$ is its automorphism such that $\alpha\sigma\alpha^{-1} = \sigma$. Since $\bar{\sigma} = (1.25.34.) = \bar{\sigma}^{-1}$, for $a = 1$ the formula (15) gives the prolongation $Q'_{\sigma,1}(\circ)$, where:

| $\circ$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 3 | 4 | 6 | 1 | 5 |
| 3 | 3 | 6 | 5 | 1 | 2 | 4 |
| 4 | 4 | 5 | 1 | 2 | 6 | 3 |
| 5 | 5 | 1 | 6 | 3 | 4 | 2 |
| 6 | 6 | 4 | 2 | 5 | 3 | 1 |

$$\psi_1 = \varphi_1 = (1.25.34.6.),$$
$$\psi_2 = \varphi_2\sigma_2 = (12.356.4.),$$
$$\psi_3 = \varphi_3\sigma_3 = (13.465.2.),$$
$$\psi_4 = \varphi_4\sigma_4 = (14.236.5.),$$
$$\psi_5 = \varphi_5\sigma_5 = (15.264.3.),$$
$$\psi_6 = \sigma\sigma_1 = (16.2453.).$$

For $a = 2$ and the same $\sigma$ we obtain the second prolongation $Q'_{\sigma,2}(*)$:

| $*$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 6 | 2 | 3 | 4 | 5 | 1 |
| 2 | 2 | 3 | 4 | 6 | 1 | 5 |
| 3 | 3 | 6 | 5 | 1 | 2 | 4 |
| 4 | 4 | 5 | 1 | 2 | 6 | 3 |
| 5 | 5 | 1 | 2 | 3 | 4 | 6 |
| 6 | 1 | 4 | 6 | 5 | 3 | 2 |

$$\begin{aligned} \omega_1 &= \varphi_1\sigma_1 = (16.25.34.), \\ \omega_2 &= \ \ \sigma_2 \ \ = (12.35.4.6.), \\ \omega_3 &= \varphi_3\sigma_3 = (13.465.2.), \\ \omega_4 &= \varphi_4\sigma_4 = (14.236.5.), \\ \omega_5 &= \varphi_5\sigma_5 = (15.264.3.), \\ \omega_6 &= \sigma\sigma_2 \ = (1.24563.). \end{aligned}$$

From Theorem 2.5 in [3] it follows that these two prolongations are not isotopic, as $\alpha(1) \neq 2$.

Observe by the way, that for the automorphism $\alpha$ we have $\alpha(2) = 3$, $\alpha(3) = 5$, $\alpha(5) = 4$, $\alpha(4) = 2$, which, by Corollary 3.3, means that for this quasigroup $Q'_{\sigma,2} \cong Q'_{\sigma,3} \cong Q'_{\sigma,5} \cong Q'_{\sigma,4}$. The isomorphism $Q'_{\sigma,k} \to Q'_{\sigma,\alpha(k)}$ for $k = 2, 3, 4$, coincides with $\alpha$. □

## 4. Prolongations by quasicomplete mappings

The method of prolongations of quasigroups having at least one quasicomplete mapping was proposed in [4].

Let $Q(\cdot)$ be an arbitrary finite quasigroup with a quasicomplete mapping $\sigma$. Then $def(\sigma) = d$ and for some $a \in Q$ there are two different elements $a_1$, $a_2$ of $Q$ such as $\bar{\sigma}(a_1) = \bar{\sigma}(a_2) = a$. Choosing one of these elements (for example $a_1$) we obtain the prolongation $Q'_{a_1}(\circ)$ of $Q(\cdot)$ defined by:

$$x \circ y = \begin{cases} x \cdot y & x, y \in Q,\ y \neq \sigma(x), \\ q & x \in Q - \{a_1\},\ y = \sigma(x), \\ a & x = a_1,\ y = \sigma(x), \\ \bar{\sigma}(x) & x \in Q - \{a_1, a_2\},\ y = q, \\ \bar{\sigma}\sigma^{-1}(y) & y = q,\ y \neq \sigma(a_1), y \neq \sigma(a_2), \\ q & x = a_1,\ y = q \ \text{ or } \ x = q,\ y = \sigma(a_1), \\ a & x = a_2,\ y = q \ \text{ or } \ x = q,\ y = \sigma(a_2), \\ d & x = y = q. \end{cases} \tag{17}$$

Replacing $a_1$ by $a_2$ we obtain the second prolongation of $Q(\cdot)$ which may not be isotopic to the first.

This construction is a generalization of the previous constructions. Prolongations of $Q(\cdot)$ obtained by these three constructions are not isotopic in general (for details see [4]).

**Theorem 4.1.** *Let $Q(\cdot) = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ be a quasigroup with a quasicomplete mapping $\sigma$. The quasigroup $Q'(\circ) = \{\psi_1, \psi_2, \ldots, \psi_n, \psi_q\}$ coincides with the prolongation of $Q(\cdot)$ obtained by the formula* (17) *if and only if*

$$\begin{cases} \psi_i = \varphi_i \sigma_i & \textit{for} \quad i \neq a, q, d, \\ \psi_d = \varphi_d \varepsilon, & \\ \psi_a = \varphi_a \sigma_{a_1} & \textit{or} \quad \varphi_a \sigma_{a_2}, \\ \psi_q = \sigma \sigma_{a_2} & \textit{or} \quad \sigma \sigma_{a_1}, \end{cases} \tag{18}$$

*where $\sigma_i = \left(q, \bar{\sigma}^{-1}(i)\right)$ for $i \notin \{d, a_1, a_2\}$, $\sigma_d = \varepsilon$, $\sigma_{a_1} = (q, a_1)$ and $\sigma_{a_2} = (q, a_2)$.*

*Proof.* The proof of this theorem is similar to the proof of Theorem 2.1. □

**Theorem 4.2.** *Let $T = (\alpha, \beta, \gamma)$ be an autotopism of a quasigroup $Q(\cdot)$ with a quasicomplete mapping $\sigma$. If $\beta\sigma\alpha^{-1} = \sigma$, $\bar{\sigma}(a_1) = \bar{\sigma}(a_2) = a$ and $\gamma(a) = a$, then prolongations $Q'_{a_1}(\circ)$ and $Q'_{a_2}(*)$ induced by $\sigma$ are isotopic.*

*Proof.* The proof of this theorem is similar to the proof of Theorem 3.2. □

**Example 4.3.** Consider the quasigroup $Q(\cdot)$, where

| $\cdot$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 3 | 1 | 5 | 6 | 4 |
| 3 | 3 | 1 | 2 | 6 | 4 | 5 |
| 4 | 4 | 6 | 5 | 1 | 3 | 2 |
| 5 | 5 | 4 | 6 | 2 | 1 | 3 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

$\varphi_1 = (1.23.4.5.6.)$,
$\varphi_2 = (12.3.465.)$,
$\varphi_3 = (13.2.456.)$,
$\varphi_4 = (14.2635.)$,
$\varphi_5 = (15.2436.)$,
$\varphi_6 = (16.2534.)$.

The permutation $\sigma = (1425.3.6)$ is a quasicomplete mapping of this quasigroup,

$$\bar{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 6 & 5 & 1 \end{pmatrix}, \qquad \bar{\sigma}^{-1} = \begin{pmatrix} 1 & 2 & 4 & 5 & 6 & 6 \\ 6 & 3 & 1 & 5 & 2 & 4 \end{pmatrix},$$

$def(\sigma) = 3$, $a = 6$, $a_1 = 2$, $a_2 = 4$, and $\sigma_1 = (7, 6)$, $\sigma_2 = (7, 3)$, $\sigma_3 = \varepsilon$, $\sigma_4 = (7, 1)$, $\sigma_5 = (7, 5)$, $\sigma_{a_1} = (7, 2)$, $\sigma_{a_2} = (7, 4)$.

Then $Q'_{a_1}(\circ) = \{\psi_1, \psi_2, \ldots, \psi_7\}$ and $Q'_{a_2}(*) = \{\omega_1, \omega_2, \ldots, \omega_7\}$, where

$$\begin{cases} \psi_i = \varphi_i \sigma_i \ \text{ for } i = 1, 2, 4, 5, \\ \psi_3 = \varphi_3 \varepsilon, \\ \psi_6 = \varphi_6 \sigma_{a_1}, \\ \psi_7 = \sigma \sigma_{a_2}, \end{cases} \qquad \begin{cases} \omega_i = \varphi_i \sigma_i \ \text{ for } i = 1, 2, 4, 5, \\ \psi_3 = \varphi_3 \varepsilon, \\ \omega_6 = \varphi_6 \sigma_{a_2}, \\ \omega_7 = \sigma \sigma_{a_1}. \end{cases}$$

It is not difficult to verity that $T = (\alpha, \beta, \gamma)$, where $\alpha = (15.24.36.)$, $\beta = (14.25.36.)$ and $\gamma = (12.45.3.6.)$ is an autotopism of a quasigroup $Q(\cdot)$. For this autotopism we have $\beta\sigma\alpha^{-1} = \sigma$, $\gamma(6) = 6$, which means that prolongations $Q'_{a_1}(\circ)$ and $Q'_{a_2}(*)$ are isotopic. This isotopism has the form $T = (\alpha, \beta, \gamma)$, where $\alpha = (15.24.36.7.)$, $\beta = (14.25.36.7.)$ and $\gamma = (12.45.3.6.7.)$. □

## References

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

[2] **G. B. Belyavskaya**, *A generalized prolongation of quasigroups*, (Russian), Mat. Issled. **5** (1970), No.2, 28 – 48.

[3] **I. I. Deriyenko**, *On middle translations of finite quasigroups*, Quasigroups and Related Systems **16** (2008), 17 – 24.

[4] **I. I. Deriyenko and W. A. Dudek**, *On prolongations of quasigroups*, Quasigroups and Related Systems **16** (2008), 187 – 198.

Received December 10, 2009

I.I.Deriyenko
Department of Higher Mathematics and Informatics, Kremenchuk State University, 20 Pervomayskaya str., 39600 Kremenchuk, Ukraine
E-mail: ivan.deriyenko@gmail.com

A.I.Deriyenko
Department of Fundamental Sciences, Kremenchuk University of Economy, Information Technology and Management, 24/37 Proletarskaya str., 39600 Kremenchuk, Ukraine
E-mail: andrey.deriyenko@gmail.com

# Periodic quasigroup string transformations

*Vesna Dimitrova, Smile Markovski and Aleksandra Mileva*

**Abstract.** Given a finite quasigroup $(Q, *)$, a quasigroup string transformations $e_l$ and $d_l$ over the strings of elements from $Q$ are defined as follows. $e_l(a_1a_2 \dots a_n) = b_1b_2 \dots b_n$ if and only if $b_i = b_{i-1} * a_i$ and $d_l(a_1a_2 \dots a_n) = b_1b_2 \dots b_n$ if and only if $b_i = a_{i-1} * a_i$, for each $i = 1, 2, \dots, n$, where $l = a_0 = b_0$ is a fixed element of $Q$. A quasigroup string $e$- or $d$-transformation $t$ is periodical if for some periodic string we have $t(a_1a_2 \dots a_ka_1a_2 \dots a_k \dots a_1a_2 \dots a_k) = a_1a_2 \dots a_ka_1a_2 \dots a_k \dots a_1a_2 \dots a_k$. The quasigroup string transformations are used in many fields, like: cryptography for designing different cryptographic tools, coding theory for designing error-detecting and error-correcting codes, etc. The properties of the quasigroup string transformations depend on the used quasigroups, and some quasigroups are suitable for cryptographic designs, while some others are suitable for code designs. We give a characterization of the quasigroups producing periodic string transformations, and for that aim quasigroups with period $k$ are defined. One can use this characterization for choosing suitable quasigroups in some applications.

## 1. Introduction

Classification of finite quasigroups is very important for successful application of quasigroups in many fields of applied mathematics or computer science. It is a difficult problem, but it has a practical importance. The classification of quasigroups is difficult, because the number of quasigroups even of small order is very large (there are 161280, $8.1 \times 10^8$, $6.1 \times 10^{13}$ quasigroups of order 5, 6, 7, respectively). In many applications quasigroup string transformations are used, so for application purposes the classification of the class of quasigroups of some fixed order should be given according to the properties of their string transformations. The quasigroup string transformations $e_l$ and $d_l$, for given finite quasigroup $(Q, *)$, are defined by Markovski et al. [6], where some important properties suitable for applications are proved.

2000 Mathematics Subject Classification: 20N05, 05B15

Keywords: quasigroup with period $k$, periodic quasigroup string transformation.

There are several classifications of quasigroups by their algebraic properties. There are also some classification of the quasigroups by the properties of their string transformations, e.g., by random walk on torus [8], by image patterns [2], etc.

In this paper we classify the finite quasigroups according to the property their string transformations to preserve the periodicity of some starting strings. These quasigroups $Q$ have the property some periodical string $a_1a_2\dots a_ka_1a_2\dots a_k\dots a_1a_2\dots a_k$, $a_i\in Q$, with smallest period $k$, to be transformed into a periodical string with period $k$ after arbitrarily many applications of $e$-transformations, i.e.,

$$e_l^n(a_1a_2\dots a_ka_1a_2\dots a_k\dots a_1a_2\dots a_k)=c_1c_2\dots c_kc_1c_2\dots c_k\dots c_1c_2\dots c_k,$$

for each $n=1,2,3,\dots$, where $l$ is some fixed element of the quasigroup and $c_i\in Q$. We define the notion of a quasigroup with period $k$ and we give characterizations of that kind of quasigroups.

In Section 2 we give a brief introduction to the notion of quasigroups and quasigroup string transformations. The method for obtaining graphical presentation of quasigroup string transformations is given in Section 3. In Section 4 are given definitions and characterizations of quasigroups with period $k$ and of periodic quasigroup string transformations. Some experimental results and analysis of experiments made on all quasigroups of order 4 are presented in Section 5.

## 2. Quasigroup string transformations

A *quasigroup* $(Q,*)$ is a groupoid (i.e., algebra with one binary operation $*$ on the set $Q$) satisfying the law:

$$(\forall\ u,v\in Q)\ (\exists!\ x,y\in G)\ (x*u=v\ \wedge\ u*y=v)$$

In other words, the equations $x*u=v$ and $u*y=v$, for each given $u,v\in Q$, have unique solutions $x,y$.

Equivalent combinatorial structure to quasigroups are Latin squares. To any finite quasigroup $(Q,*)$ given by its multiplication table a Latin square can be associated, consisting of the matrix formed by the main body of the table, since each row and column of the matrix is a permutation of $Q$. Conversely, each Latin square $L$ on a set $Q$ gives rise up to $(|Q|!)^2$ different quasigroups (depending of the bordering of the matrix of $L$ by the main row and the main column of the multiplication table).

Let $Q$ be a set of elements ($|Q| \geqslant 2$). We denote by

$$Q^+ = \{a_1 a_2 \dots a_n \,|\, a_i \in Q,\ n \geqslant 2\}$$

the set of all finite strings with elements of $Q$. For a given quasigroup $(Q, *)$ and a fixed element $l \in Q$, called leader, we define the so called quasigroup string transformations (q.s.t.) $e_l, d_l : Q^+ \to Q^+$ as follows:

$$e_l(a_1 a_2 \dots a_n) = (b_1 b_2 \dots b_n) \longleftrightarrow \begin{cases} b_1 = l \ * a_1 \\ b_{i+1} = b_i * a_{i+1}, \quad 1 \leqslant i \leqslant n-1, \end{cases}$$

$$d_l(a_1 a_2 \dots a_n) = (c_1 c_2 \dots c_n) \longleftrightarrow \begin{cases} c_1 = l \ * a_1 \\ c_{i+1} = a_i * a_{i+1}, \quad 1 \leqslant i \leqslant n-1. \end{cases}$$

By using a string of leaders $l_1, l_2, \dots, l_k$, we can apply consecutively $e-$ (or $d-$) transformations on a given string, as a composition of transformations. These compositions of $e-$ or $d-$transformations are called $E-$ or $D-$transformation respectively and they are defined as

$$E = e_{l_1} \circ e_{l_2} \circ \dots \circ e_{l_k}, \quad D = d_{l_1} \circ d_{l_2} \circ \dots \circ d_{l_k}.$$

Further, we will use only one leader $l = l_i$, for $1 \leqslant i \leqslant k$.

**Example 2.1.** Let the quasigroup $(Q, *)$ be given by the table

| $*$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 1 |
| 2 | 1 | 4 | 3 | 2 |
| 3 | 3 | 2 | 1 | 4 |
| 4 | 4 | 1 | 2 | 3 |

If we apply consecutive $e-$transformations with leader $l = 1$ on the string $\alpha = 3\ 4\ 4\ 2\ 2\ 2\ 1\ 2\ 3\ 4\ 1\ 1\ 1\ 1\ 2\ 3\ 3\ 3\ 4$, we obtain the followings strings:

|  | 3 | 4 | 4 | 2 | 2 | 2 | 1 | 2 | 3 | 4 | 1 | 1 | 1 | 1 | 2 | 3 | 3 | 3 | = | $\alpha$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 4 | 3 | 4 | 1 | 3 | 2 | 1 | 3 | 1 | 1 | 2 | 1 | 2 | 1 | 3 | 1 | 4 | 2 | = | $\alpha_1 = e_1(\alpha)$ |
| 1 | 1 | 4 | 3 | 3 | 1 | 3 | 3 | 1 | 2 | 1 | 3 | 3 | 2 | 1 | 4 | 4 | 3 | 2 | = | $\alpha_2 = e_1(\alpha_1)$ |
| 1 | 2 | 2 | 3 | 1 | 2 | 3 | 1 | 2 | 4 | 4 | 2 | 3 | 2 | 1 | 1 | 1 | 4 | 1 | = | $\alpha_3 = e_1(\alpha_2)$ |

## 3. Graphical presentation of strings

We use the lexicographic ordering of the set of quasigroups, defined as follows. For the set of quasigroups of order $n$, we represent the quasigroups by strings of $n^2$ letters that are concatenation of the rows of the corresponding Latin squares. Then we apply the lexicographic ordering of those strings.

**Example 3.1.** There are 576 quasigroups of order 4. For the quasigroups given below by their multiplication tables, the corresponding numbers in the lexicographic ordering are respectively 5, 106 and 275.

| $*$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 3 | 4 | 1 |
| 3 | 3 | 4 | 1 | 2 |
| 4 | 4 | 1 | 2 | 3 |

| $*$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 4 | 2 | 3 |
| 2 | 3 | 1 | 4 | 2 |
| 3 | 4 | 2 | 3 | 1 |
| 4 | 2 | 3 | 1 | 4 |

| $*$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 2 | 4 | 3 | 1 |
| 2 | 3 | 1 | 2 | 4 |
| 3 | 4 | 2 | 1 | 3 |
| 4 | 1 | 3 | 4 | 2 |

We make a graphical presentation of q.s.t. for their better review. The usage of this presentation helps us to investigate their properties. The method for obtaining graphical presentation of $E-$ or $D-$transformation is the following.

Let $Q$ be a quasigroup. We treat each element of $Q$ as a pixel with corresponding color. If we take a string $s \in Q^t$ (of length $t$) then, by consecutive application of $e-$ or $d-$transformations $k$ times, we obtain $k \times t$ matrix with elements from $Q$. By treating the elements as pixels we obtain images that present the corresponding $E-$ or $D-$transformation.

**Example 3.2.** Take the first two quasigroups from Example 3.1, the periodic string $s = 32413241 \dots 3241$ of length $t = 100$, leader $l = 1$ and make $k = 100$ times applications of $e-$transformations ($d-$transformations); the corresponding images are shown on Figure 1 (Figure 2).

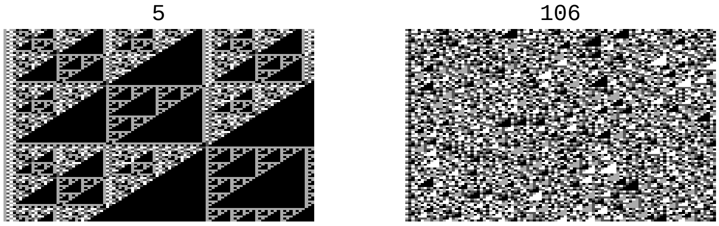

Figure 1. Images of $e-$transformations of quasigroups 5 and 106

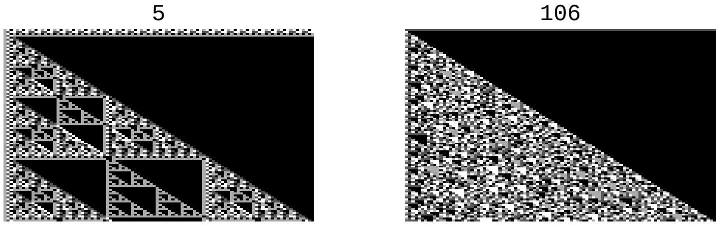

Figure 2. Images of $d-$transformations of quasigroups 5 and 106

The third quasigroup from Example 3.1 gives a pattern shown on Figure 3, that we call a periodical pattern, since $e_1^n(s) = s$ for each $n = 1, 2, 3, \ldots$. (The same pattern appears when the transformation $d_1$ is used as well.)

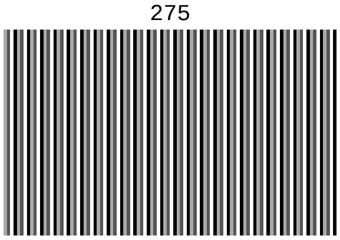

Figure 3. The periodical pattern of $e-$transformations of quasigroup 275

**Example 3.3.** Let the starting periodic string be $s = 32413241\ldots 3241$. We asked for quasigroups on the set $\{1, 2, 3, 4\}$ and q.s.t. $e_l$ that give periodical pattern. Only the quasigroups with lexicographic numbers 275 and 467 for leader $l = 1$ produced periodical patterns.

## 4. Quasigroups with period $k$

We define a quasigroup with period $k$ as follows. Let $(Q, *)$ be a finite quasigroup of order $n$. If there are an element $l \in Q$ and a periodical string $s = a_1a_2\ldots a_ka_1a_2\ldots a_k\ldots a_1a_2\ldots a_k,\ a_i \in Q$, of smallest period $k$ such that for each $n = 1, 2, 3, \ldots$ we have that $e_l^n(s)$ is again a periodical string of smallest period $k$, then we say that $Q$ is a *quasigroup with period* $k$. In that case we say that the transformation $e_l$ is a periodical $e$-transformation of the string $s$.

**Proposition 4.1.** *If the transformation $e_l$ is a periodical $e$-transformation of the string $s$, then $s$ is a fixed element of $e_l$, i.e., $e_l(s) = s$.*

The proof of Proposition 4.1 is almost straightforward and rather technical, so we consider only the case $k = 3$. We have the following situation

| | $a_1$ | $a_2$ | $a_3$ | $a_1$ | $a_2$ | $a_3$ | $a_1$ | $a_2$ | $a_3$ | $\ldots =$ | $s$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $l$ | $b_1$ | $b_2$ | $b_3$ | $b_1$ | $b_2$ | $b_3$ | $b_1$ | $b_2$ | $b_3$ | $\ldots =$ | $e_l(s)$ |
| $l$ | $c_1$ | $c_2$ | $c_3$ | $c_1$ | $c_2$ | $c_3$ | $c_1$ | $c_2$ | $c_3$ | $\ldots =$ | $e_l^2(s)$ |
| $l$ | $d_1$ | $d_2$ | $d_3$ | $d_1$ | $d_2$ | $d_3$ | $d_1$ | $d_2$ | $d_3$ | $\ldots =$ | $e_l^3(s)$ |
| $l$ | $g_1$ | $g_2$ | $g_3$ | $g_1$ | $g_2$ | $g_3$ | $g_1$ | $g_2$ | $g_3$ | $\ldots =$ | $e_l^3(s)$ |
| $l$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | |

meaning that $l * a_1 = b_1, b_1 * a_2 = b_2, b_2 * a_3 = b_3, \ldots, l * b_1 = c_1, c_1 * b_2 = c_2, \ldots$.

The equalities $l * a_1 = b_3 * a_1 = b_1$ imply $b_3 = l$. In the same manner we have $l = b_3 = c_3 = d_3 = g_3 = \ldots$ Then, $c_2 * b_3 = c_3,\ d_2 * c_3 = d_3$ means $c_2 * l = l,\ d_2 * l = l$, implying $c_2 = d_2$ and, in the same way, $c_2 = d_2 = g_2 = \ldots$ Now, by the previous equalities and $d_1 * c_2 = d_2,\ g_1 * c_2 = g_2$ we get $d_1 = g_1 = \ldots$ Then $l * c_1 = d_1,\ l * d_1 = g_1,\ l * b_1 = c_1,\ l * a_1 = b_1$ gives $a_1 = b_1 = c_1 = d_1 = \ldots$. In that way, one can see that $a_1 = b_1 = c_1 = d_1 = \ldots,\ a_2 = b_2 = c_2 = d_2 = \ldots,\ a_3 = b_3 = c_3 = d_3 = \ldots$

Note that $l = a_3 = b_3 = c_3 = d_3 = \ldots$, so in the general case we have the following property too.

**Proposition 4.2.** *If the transformation $e_l$ is a periodical e-transformation of the string $a_1a_2\ldots a_ka_1a_2\ldots a_k\ldots a_1a_2\ldots a_k,\ a_i \in Q$, of smallest period $k$, then $l = a_k$ and*

$$a_i * a_{i+1} = a_{i+1}, \quad i = 1, 2, 3, \ldots, k, \tag{1}$$

*where $a_{k+1} = a_1$.*

**Proposition 4.3.** *If the transformation $e_l$ is a periodical e-transformation of the string $s = a_1a_2\ldots a_ka_1a_2\ldots a_k\ldots a_1a_2\ldots a_k,\ a_i \in Q$, of smallest period $k$, then $a_i \neq a_j$ for $i \neq j$.*

*Proof.* Assume that $a_i = a_j$ for some $1 \leqslant i < j \leqslant k$, and let choose $i$ and $j$ to be the smallest indices with that property. If $i > 1$ then by (1) we have

$$\begin{aligned} a_{i-1} * a_i &= a_i, \\ a_{j-1} * a_i &= a_i, \end{aligned}$$

and that implies $a_{i-1} = a_{j-1}$, a contradiction with the choice of $i$ and $j$.

If $i = 1$ then by (1) we have

$$\begin{aligned} a_{j-1} * a_1 &= a_1, \\ a_k * a_1 &= a_1, \end{aligned}$$

and that implies $a_{j-1} = a_k$. Then we have

$$\begin{aligned} a_{j-2} * a_{j-1} &= a_{j-1}, \\ a_{k-1} * a_{j-1} &= a_{j-1}, \end{aligned}$$

and that implies $a_{j-2} = a_{k-1}$. Continuing that way we have $a_{j-t} = a_{k-t+1}$ for each $t$ such that $j > t$.

If for some $p > 0$ we have $k = p(j-1)$, then we will obtain that the string $a_1a_2 \dots a_k$ reduces to $\underbrace{a_1a_2 \dots a_{j-1} \dots a_1a_2 \dots a_{j-1}}_{p}$, which means that the string $s$ has period $j-1 < k$, a contradiction.

The other possibility is $k = p(j-1) + r$ for some $p > 0$, $0 < r < j-1$. Then the string $a_1a_2 \dots a_k$ reduces to

$$a_1a_2 \dots a_{j-1}a_1a_{j-r+1} \dots a_{j-1} \underbrace{a_1 \dots a_{j-1} \dots a_1 \dots a_{j-1}}_{p-1}.$$

Now, by (1) we have

$$\begin{aligned} a_1 * a_{j-r+1} &= a_{j-r+1}, \\ a_{j-r} * a_{j-r+1} &= a_{j-r+1}, \end{aligned}$$

and that implies $a_1 = a_{j-r}$, a contradiction with the choice of $j$. □

As a consequence of Proposition 4.2 and Proposition 4.3 we get the main result of the paper.

**Theorem 4.1.** *Let $(Q, *)$ be a quasigroup of a finite order $n$. Then $Q$ is with period $k$ if and only if there are different elements $x_1, x_2, \dots, x_k \in Q$ such that*

$$x_i * x_{i+1} = x_{i+1}, \quad i = 1, 2, 3, \dots, k, \tag{2}$$

*where $x_{k+1} = x_1$.*

*Proof.* Let $x_1, x_2, \dots, x_k$ be different elements from $Q$ satisfying (2). Then the string $s = x_1x_2 \dots x_kx_1x_2 \dots x_k \dots x_1x_2 \dots x_k$ satisfies (1), so the transformation $e_{x_k}$ is a periodical $e$-transformation for the string $s$. So, $Q$ is with period $k$.

The opposite statement follows by Propositions 4.2 and 4.3. □

Note that if (2) holds, then for the $d$-transformation $d_{x_k}$ and the string $s = x_1x_2 \dots x_kx_1x_2 \dots x_k \dots x_1x_2 \dots x_k$ we have $d_{x_k}(s) = s$. So, all results for periodical $e$-transformations can be reformulated for periodical $d$-transformations too.

**Corollary 4.1.** *A period $k$ of quasigroup of order $n$ cannot be larger than $n$.*

**Proposition 4.4.** *Let $k$ and $n$, $k \leqslant n$, $n > 2$, be positive integers. Then there is a quasigroup of order $n$ with period $k$.*

*Proof.* The proof follows immediately from the results given by Smetaniuk [3], and Wanless [10]. Smetaniuk proves that any partial $n \times n$ Latin square with $k < n$ entries can be completed to an $n \times n$ Latin square, and Wanless proves that if $n > 2$ then there is an $n \times n$ Latin square that contains a transversal. Now, given a subset $\{a_1, \dots, a_k\}$ of $Q = \{a_1, \dots, a_n\}$, where $k < n$, we define a partial quasigroup $(Q, *)$ by the equalities $a_k * a_1 = a_1$, $a_1 * a_2 = a_2, a_2 * a_3 = a_3, \dots, a_{n-1} * a_k = a_k$. This partial quasigroup can be completed to a quasigroup $(Q, *)$ that satisfies (2).

In the case $n = k > 2$, there is an $n \times n$ Latin square $Q$ with a transversal $\{a_{1,\pi(1)}, a_{2,\pi(2)}, \dots, a_{n,\pi(n)}\}$, where $a_{l,r} \in Q$ denotes the element at the position $(l, r)$ and $\pi$ is a permutation of $\{1, 2, \dots, n\}$. Now, we can obtain a wanted quasigroup $(Q, *)$ by a suitable bordering of the Latin square. The main row of the multiplication table of the quasigroup is bordered by the string $(a_{\pi^{-1}(1),1}, a_{\pi^{-1}(2),2}, \dots, a_{\pi^{-1}(n),n})$, and the main column by the string $(a_{n,\pi(n)}, a_{1,\pi(1)}, a_{2,\pi(2)}, \dots, a_{n-1,\pi(n-1)})$. Then $a_{n,\pi(n)} * a_{1,\pi(1)} = a_{1,\pi(1)}$, $a_{1,\pi(1)} * a_{2,\pi(2)} = a_{2,\pi(2)}, \dots, a_{n-1,\pi(n-1)} * a_{n,\pi(n)} = a_{n,\pi(n)}$. So, by Theorem 4.1, $(Q, *)$ is a quasigroup with period $n$. □

**Example 4.1.** The partial quasigroup given in Table 4.1 can be completed to two different quasigroups. Both are with periods 4; the periodic string $s$ is $32413241\dots$.

| $*$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 |  |  | 3 |  |
| 2 |  |  |  | 4 |
| 3 |  | 2 |  |  |
| 4 | 1 |  |  |  |

| $*$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 2 | 4 | 3 | 1 |
| 2 | 3 | 1 | 2 | 4 |
| 3 | 4 | 2 | 1 | 3 |
| 4 | 1 | 3 | 4 | 2 |

| $*$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 4 | 1 | 3 | 2 |
| 2 | 2 | 3 | 1 | 4 |
| 3 | 3 | 2 | 4 | 1 |
| 4 | 1 | 4 | 2 | 3 |

Table 1. Completions of a partial quasigroup

**Proposition 4.5.** *If a quasigroup of order $n$ is with different periods $n_1, n_2, \dots, n_t$, then $n_1 + n_2 + \cdots + n_t \leqslant n$.*

*Proof.* Let $(Q, *)$ be a quasigroup with different periods $n_1, \dots, n_t$ such that $n_1 + n_2 + \cdots + n_t > k$. Then there are periodic sequences $s_1 = x_1 x_2 \dots$

and $s_2 = y_1y_2\dots$ with smallest periods $x_1x_2\dots x_{n_i}$ and $y_1y_2\dots y_{n_j}$ such that $x_p = y_r$ for some $p \leqslant n_i$, $r \leqslant n_j$ $(n_i \neq n_j)$. We choose $p$ to be the smallest index such that $x_p = y_r$.

If $r \geqslant p > 1$, then we have $x_{p-1} * x_p = x_p$, $y_{r-1} * x_p = y_{r-1} * y_r = y_r = x_p$, implying $x_{p-1} = y_{r-1}$, a contradiction with the choice of $p$. A similar contradiction will be obtained when $p \geqslant r > 1$.

Let $p = 1 \leqslant r$. Then we have $x_{n_i} = y_{r-1}$ since $x_1 = y_r$ implies $x_{n_i} * x_1 = x_1$, $y_{r-1} * x_1 = y_{r-1} * y_r = y_r = x_1$. Continuing that way we have either $x_{n_i} = y_{r-1}$, $x_{n_i-1} = y_{r-2}$, $x_{n_i-2} = y_{r-3}, \dots, x_1 = y_{r-n_i}$ in the case $n_i < r$, or $x_{n_i} = y_{r-1}$, $x_{n_i-1} = y_{r-2}$, $x_{n_i-2} = y_{r-3}, \dots, x_{n_i-r+2} = y_1$ in the case $r \leqslant n_i$.

In the case $n_i < r$ we have that the smallest period $y_1y_2\dots y_{n_j}$ of $s_2$ is $y_1\dots y_{r-n_i-1}x_1\dots x_{n_i}x_1y_{r+1}\dots y_{n_j}$ that contains two times the same element $x_1$, a contradiction with Proposition 4.3.

The case $r \leqslant n_i$ remains yet. Then the smallest period $x_1x_2\dots x_{n_i}$ of $s_1$ is $x_1\dots x_{n_i-r+1}y_1\dots y_{r-1}$. Then we have $x_{n_i-r+1} = y_{n_j}$ since $y_{n_j} * y_1 = y_1$, $x_{n_i-r+1} {*} y_1 = y_1$. Continuing that way we have either $x_{n_i-r+1} = y_{n_j}$, $x_{n_i-r} = y_{n_j-1}$, $x_{n_i-r-1} = y_{n_j-2}, \dots, x_1 = y_{n_j-n_i+r}$ in the subcase $n_i - r < n_j$, or $x_{n_i-r+1} = y_{n_j}$, $x_{n_i-r} = y_{n_j-1}$, $x_{n_i-r-1} = y_{n_j-2}, \dots, x_{n_i-r-n_j+2} = y_1$ in the subcase $n_i - r \geqslant n_j$. Now, the subcase $n_i - r \geqslant n_j$ implies that $y_1$ appears two times in the string $x_1x_2\dots x_{n_i}$, and the subcase $n_i - r < n_j$ implies that $x_1$ appears two times in the string $y_1y_2\dots y_{n_j}$. (Namely, $y_r = x_1$ and $y_{n_j-n_i+r} = x_1$, and $n_i \neq n_j$ implies $n_j - n_i + r \neq r$.) □

## 5. Experimental results

For finding the set of quasigroups of order 4 with period $k$ a module *PeriodicQ*$[q, s]$ in the software package *Mathematica* is given in Appendix 1. Using this module we have made experiments for all 576 quasigroups of order 4 and for all periodical strings with the smallest periods $x_1x_2\dots x_k$, $x_i \in \{1, 2, 3, 4\}$, $k = 1, 2, 3, 4$. The obtained results of these experiments show that: 12 quasigroups are with period 4, 64 are with period 3, 186 with period 2, and 414 with period 1. Also, 16 quasigroups are with period 1 and 3, and 84 quasigroups are with period 1 and 2. The lexicographic numbers of these quasigroups are given in Appendix 2.

The analysis of these classes of quasigroups gives the following.

All of the quasigroups with period 4 are linear [4], non-idempotent, non-commutative, non-associative, non-semisymmetric, without left nor right unit and without proper subquasigroups. (A quasigroup is called *semi-symmetric* if it satisfies the identity $(y * x) * y = x$. It is linear if its representation as vector valued Boolean function contains only linear polynomials.) All of them satisfy the following two identities:

$$x * (x * (x * (x * y))) = y, \quad ((((y * x) * x) * x) * x) * x = y.$$

All of the quasigroups with period 3 are non-idempotent, non-associative, non-semisymmetric, without left unit, without proper subquasigroups. The quasigroups in the subclass $\{149, 151, 201, 207, 226, 257, 282, 288, 291, 295, 317, 347, 351, 370, 373, 426, 437, 460, 463, 489, 493, 516, 519, 545\}$ are non-linear and commutative quasigroups, without right unit. Non-linear and non-commutative quasigroups in the subclass $\{150, 152, 195, 200, 221, 244, 268, 270, 299, 311, 327, 353, 357, 369, 379, 423, 442, 470, 480, 490, 499, 522, 525, 544\}$ satisfy the identity:

$$(((y * x) * x) * x) = y.$$

Other two subclasses have the period 1 also and they are linear. The quasigroups in the subclass $\{77, 100, 197, 272, 305, 380, 477, 500\}$ are non-commutative, with right units and all of them satisfy the following two identities:

$$x * (x * (x * (x * y))) = y, \quad ((y * x) * x) * x = y.$$

The quasigroups in the subclass $\{83, 113, 203, 285, 292, 374, 464, 494\}$ are commutative, without right unit and all of them satisfy the following two identities:

$$x * (x * (x * (x * y))) = y, \quad (((y * x) * x) * x) * x = y.$$

All of the quasigroups with period 1 and 2 are non-idempotent, non-associative, non-semisymmetric, non-commutative, without proper subquasigroups. They can be grouped in tree subclasses. The quasigroups in the subclass $\{38, 45, 56, 66, 74, 81, 90, 98, 105, 115, 124, 129, 153, 162, 202, 205, 216, 225, 240, 255, 258, 279, 281, 283, 300, 310, 312, 316, 328, 337, 350, 362, 363, 366, 412, 424, 440, 441, 469, 473, 479, 483, 486, 487, 512, 518, 533, 543\}$ are without left nor right unit. The quasigroups in the subclass $\{80, 82, 93, 101, 110, 116, 206, 284, 308, 365, 476, 484\}$ are without left nor right unit and all of them satisfy the following two identities:

$$x * (x * (x * (x * y))) = y, \quad ((((y * x) * x) * x) * x) * x = y.$$

The quasigroups in the subclass $\{73, 75, 78, 97, 99, 103, 154, 161, 208, 224, 245, 287, 307, 329, 340, 356, 368, 425, 454, 475, 481, 509, 524, 546\}$ are with right unit and all of them satisfy the following identity:

$$((((y * x) * x) * x) * x) * x = y.$$

The sets of quasigroups with period 2 and period 1 are larger ones, and we do not discuss them.

The experiments show that for any given periodical string $s$ of a period $k$, there is a fixed number $n_k$ of quasigroups with period $k$ for that string $s$. The numbers $n_k$ are given in Table 2.

| $k$ | 4 | 3 | 2 | 1 |
|---|---|---|---|---|
| $n_k$ | 2 | 8 | 32 | 144 |

Table 2. Numbers of quasigroups with period $k$ for a string $s$.

This means that in the set of all quasigroups of order 4, 2 of them are with period 4 for a given starting periodic string of period 4, 8 are with period 3 for a given starting periodic string of period 3, 32 are with period 2 for a given starting periodic string of period 2 and 144 are with period 1 for a given starting periodic string of period 1. We can conclude that the numbers $n_k$ do not depend on the chosen string $s$.

## References

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

[2] **V. Dimitrova and S. Markovski**, *Classification of quasigroups by image patterns*, Proc. Fifth Internat. Confer. Informatics and Information Technology, Bitola, Macedonia 2007, 152 – 160.

[3] **T. Evans**: *Embedding incomplete latin squares*, Amer. Math. Monthly **67** (1960), 959 – 961.

[4] **D. Gligoroski, V. Dimitrova and S. Markovski**, *Quasigroups as Boolean functions, their equation systems and Groebner bases*, in "Groebner, Coding, and Cryptography", Springer, 2009, 415 – 420.

[5] **F. C. Laywine and L. G. Mullen**, *Discrete mathematics using Latin squares*, John Wiley and Sons, Inc., 1998.

[6] **S. Markovski, D. Gligoroski and V. Bakeva**, *Quasigroup string transformations: Part 1*, Contributions, Sec. math. Tech. Sci., MANU, XX, **1-2** (1999), 13 – 28.

[7] **S. Markovski**, *Quasigroup string processing and applications in cryptography*, 1st Confer. Math. and Informatics for Industry, Thessaloniki 2003, 278 – 290.

[8] **S. Markovski, D. Gligoroski and J. Markovski**, *Classification of quasigroups by random walk on torus*, J. Appl. Math. Computing **19** (2005), 57-75.

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

[10] **I. M. Wanless**, *A generalization of transversals for Latin squares*, Electron. J. Comb. **9** (2002), R12.

Received March 27, 2009

V. Dimitrova and S. Markovski:
Institute of Informatics, Faculty of Natural Science, P. O. Box 162, Skopje, Republic of Macedonia
E-mails: vesnap@ii.edu.mk (Dimitrova), smile@ii.edu.mk (Markovski)

A. Mileva:
Faculty of Informatics, University "Goce Delčev","Krste Misirkov" bb, Štip, Republic of Macedonia
E-mail: saskamileva@yahoo.com

# Appendix 1

**Module for finding the set of quasigroups of order 4 with period $k$**

```
PeriodicQ[q, s]
    q - lists of quasigroups
    s - starting periodic string
```

```
(∗ list of quasigroups ∗)
q = Get[”quasigroups.dat”];
(∗ length of the smallest period ∗)
k = Input[ ];
(∗ number of repeating of the smallest period ∗)
n = Input[ ];
(∗ list of elements of the string ∗)
ss = { };
For[i = 1, i <= k, i + +,
x[i] = Input[ ]; ss = Append[ss, x[i]]]
(∗ starting periodic string ∗)
s = Flatten[Table[ss, {i, 1, n}]]
(∗module for e − transformation∗)
etransf[q_ , s_ ] := Module[{}, a[0] = Last[ss];
For[i = 0, i <= Length[s] − 1, i + +, a[i + 1] = q[[a[i], s[[i + 1]]]]];
Table[a[i], {i, 1, Length[s]}]]
(∗module for finding the set of quasigroups of order 4 with period k∗)
PeriodicQ[q_ , s_ ] := Module[{}, P = {};
For[qn = 1, qn <= Length[q]], qn + +, s1 = etransf[First[q[[qn]]], s];
If[s1 == s, P = Append[P, qn]]]; P]
```

# Appendix 2

**List of quasigroups of order 4 with period *k***

Quasigroups with period 4:
196, 212, 269, 275, 293, 302, 371, 381, 461, 467, 495, 497.

Quasigroups with period 3:
77, 83, 100, 113, 149, 150, 151, 152, 195, 197, 200, 201, 203, 207, 221, 226, 244, 257, 268, 270, 272, 282, 285, 288, 291, 292, 295, 299, 305, 311, 317, 327, 347, 351, 353, 357, 369, 370, 373, 374, 379, 380, 423, 426, 437, 442, 460, 463, 464, 470, 477, 480, 489, 490, 493, 494, 499, 500, 516, 519, 522, 525, 544, 545.

Quasigroups with period 2:
38, 45, 56, 66, 73, 74, 75, 78, 80, 81, 82, 90, 93, 97, 98, 99, 101, 103, 105, 110, 115, 116, 124, 129, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 173, 175, 180, 191, 199, 202, 205, 206, 208, 210, 211, 213, 214, 216, 219, 222, 224, 225, 235, 238, 240, 243, 245, 247, 249, 252, 255, 258, 267, 273, 274, 276, 277, 279, 281, 283, 284, 287, 296, 298, 300, 301, 303, 304, 307, 308, 310, 312, 315, 316, 319, 321, 324, 328, 329, 337, 338, 339, 340, 341, 342, 343, 344, 346, 349, 350, 352, 355, 356, 358, 360, 361, 362, 363, 364, 365, 366, 367, 368, 375, 378,391, 393, 394, 396, 412, 417, 418, 419, 420, 424, 425, 436, 439, 440, 441, 445, 448, 454, 459, 465, 466, 468, 469, 471, 473, 475, 476, 479, 481, 482, 483, 484, 485, 486, 487, 488, 492, 501, 505, 506, 507, 508, 509, 510, 511, 512, 513, 515, 517, 518, 521, 523, 524, 527, 533, 537, 538, 539, 540, 543, 546, 560, 561, 562, 565.

Quasigroups with period 1:
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25,26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 153, 154, 161, 162, 169, 170, 171, 172, 174, 176, 177, 178, 179, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 192, 193, 194, 197, 198, 202, 203, 204, 205, 206, 208, 209, 215, 216, 217, 218, 220, 223, 224, 225, 227, 228, 229, 230, 231, 232, 233, 234, 236, 237, 239, 240, 241, 242, 245, 246, 248, 250, 251, 253, 254, 255, 256, 258, 259, 260, 261, 262, 263, 264, 265, 266, 271, 272, 278, 279, 280, 281, 283, 284, 285, 286, 287, 289, 290, 292, 294, 297, 300, 305, 306, 307, 308, 309, 310, 312, 313, 314, 316, 318, 320, 322, 323, 325, 326, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 340, 345, 348, 350, 354, 356, 359, 362, 363, 365, 366, 368, 372, 374, 376, 377, 380, 382, 383, 384, 385, 386, 387, 388, 389, 390, 392, 395, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413,414, 415, 416, 421, 422, 424, 425, 427, 428, 429, 430, 431, 432, 433, 434, 435, 438, 440, 441, 443, 444, 446, 447, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 462, 464, 469, 472, 473, 474, 475, 476, 477, 478, 479, 481, 483, 484, 486, 487, 491, 494, 496, 498, 500, 502, 503, 504, 509, 512, 514, 518, 520, 524, 526, 528, 529, 530, 531, 532, 533, 534, 535, 536, 541, 542, 543, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 563, 564, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576.

Quasigroups with periods 1 and 3:
77, 83, 100, 113, 197, 203, 272, 285, 292, 305, 374, 380, 464, 477, 494, 500.

Quasigroups with periods 1 and 2:
38, 45, 56, 66, 73, 74, 75, 78, 80, 81, 82, 90, 93, 97, 98, 99, 101, 103, 105, 110, 115, 116, 124, 129, 153, 154, 161, 162, 202, 205, 206, 208, 216, 224, 225,240, 245, 255, 258, 279, 281, 283, 284, 287, 300, 307, 308,310, 312, 316, 328, 329, 337, 340, 350, 356, 362, 363, 365, 366, 368, 412, 424, 425, 440, 441, 454, 469, 473, 475, 476,479, 481, 483, 484, 486, 487, 509, 512, 518, 524, 533, 543, 546.

Quasigroups and Related Systems **17** (2009), 205 – 228

# Skew endomorphisms on some n-ary groups

*Wieslaw A. Dudek* and *Nikolay A. Shchuchkin*

**Abstract.** We characterize $n$-ary groups defined on a cyclic group and describe a group of their automorphisms induced by the skew operation. Finally, we consider splitting automorphisms.

## 1. Introduction

The idea of investigations of *$n$-ary groupoids*, i.e., algebras of the form $(G, f)$, where $G$ is a non-empty set and $f : G^n \to G$, $(n > 2)$, seems to be going back to E. Kasner's lecture [21] at the fifty-third annual meeting of the American Association for the Advancement of Science in 1904 where the subsets of groups closed under group multiplication of $n$ elements are considered. But the first paper containing significant results on some $n$-ary groupoids, called now *$n$-ary groups*, was written (under inspiration of Emmy Noether) by W. Dörnte [2]. In this paper Dörnte observed that any $n$-ary groupoid $(G, f)$ with the operation of the form $f(x_1, x_2, \dots, x_n) = x_1 \circ x_2 \circ \dots \circ x_n$, where $(G, \circ)$ is a group, is an $n$-ary group but for every $n > 2$ there are $n$-ary groups which are not of this form.

In recent years, $n$-ary operations find interesting applications in physics. For example, Y. Nambu [23] proposed in 1973 the generalization of classical Hamiltonian mechanics based on the Poisson bracket to the case when the new bracket, called the *Nambu bracket*, is an $n$-ary operation on classical observables. The author of [33] suspects that different $n$-ary structures such as $n$-Lie algebras, Lie ternary systems and linear spaces with additional internal $n$-ary operations, might clarify many important problems of modern mathematical physics (Yang-Baxter equation, Poisson-Lie groups, quantum

2000 Mathematics Subject Classification: 20N15, 08N05
Keywords: $n$-ary group, skew element, endomorphism, automorphism.
The second author wish to express their sincere thanks to Institute of Mathematics and Computer Science, Wroclaw University of Technology. The institute provided comfortable time to our joint research.

groups). For example, ternary $\mathbb{Z}_3$–graded algebras are important (cf. [22]) for their applications in physics of elementary interactions.

## 2. Preliminaries

An $n$-ary groupoid $(G,f)$ is *solvable at the place* $i$ if for all $a_1,...,a_n,b\in G$ there exists $x_i\in G$ such that

$$f(a_1,...,a_{i-1},x_i,a_{i+1},...,a_n)=b\,. \tag{1}$$

If this solution is unique, we say that this groupoid is *uniquely* $i$*-solvable.* An $n$-ary groupoid which is uniquely $i$-solvable for every $i=1,2,\ldots,n$ is called an $n$*-ary quasigroup* or $n$*-quasigroup* (cf. [1]).

An $n$-ary groupoid $(G,f)$ is called $(i,j)$*-associative* if

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

holds for all $x_1,\ldots,x_{2n-1}\in G$. If this identity holds for all $1\leqslant i<j\leqslant n$, then we say that the operation $f$ is *associative* and $(G,f)$ is called an $n$*-ary semigroup.* An associative $n$-ary quasigroup is called an $n$*-ary group.* Note that for $n=2$ it is an arbitrary group.

It is worth to note that in the definition of an $n$-ary group, under the assumption of the associativity of the operation $f$, it suffices to postulate the existence of a solution of (1) at the places $i=1$ 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 $i=1,\ldots,n$ (cf. [25], p.213[17]).

**Proposition 2.1.** (Dudek, Głazek, Gleichgewicht, 1977)
*An $n$-ary groupoid $(G,f)$ is an $n$-ary group if and only if (at least) one of the following conditions is satisfied:*

- $(a)$ *the $(1,2)$-associative law holds and the equation* (1) *is solvable for $i=n$ and uniquely solvable for $i=1$,*
- $(b)$ *the $(n-1,n)$-associative law holds and the equation* (1) *is solvable for $i=1$ and uniquely solvable for $i=n$,*
- $(c)$ *the $(i,i+1)$-associative law holds for some $i\in\{2,...,n-2\}$ and the equation* (1) *is uniquely solvable for $i$ and some $j>i$.* □

In some $n$-ary groups exists an element $e$ (called a *neutral element*) such that

$$f(\underbrace{e,\dots,e}_{i-1},x,\underbrace{e,\dots,e}_{n-i})=x$$

for all $x\in G$ and for all $i=1,\dots,n$. There are $n$-ary groups without neutral elements and $n$-ary groups with two, three and more neutral elements. The set of all neutral elements of a given $n$-ary group (if it is non-empty) forms an $n$-ary subgroup (cf. [9] or [16]).

Directly from the definition of an $n$-ary group $(G,f)$ it follows that for every $x\in G$ there exists only one $z\in G$ satisfying the equation

$$f(x,\dots,x,z)=x.$$

This element is called *skew* to $x$ and is denoted by $\overline{x}$.

One can prove (cf. [2]) that in any $n$-ary group $(G,f)$ the following two identities are satisfied

$$f(y,\underbrace{x,\dots,x}_{n-j-1},\bar{x},\underbrace{x,\dots,x}_{j-1})=y \qquad (1\leqslant j\leqslant n-1) \tag{2}$$

$$f(\underbrace{x,\dots,x}_{i-1},\bar{x},\underbrace{x,\dots,x}_{n-i-1},y)=y \qquad (1\leqslant i\leqslant n-1) \tag{3}$$

Thus, in some sense, the skew element is a generalization of the inverse element in binary groups. In some $n$-ary groups we have $\overline{\overline{x}}=x$, but there are $n$-ary groups in which one fixed element is skew to all elements (see Theorem 2.3 below) and $n$-ary groups in which any element is skew to itself.

A very nice description of $n$-ary groups is given by the following theorem.

**Theorem 2.2.** (Hosszú, 1963)
*An $n$-ary group $(G,f)$, $n>2$, has the form*

$$f(x_1,\dots,x_n)=x_1\circ\varphi(x_2)\circ\varphi^2(x_3)\circ\varphi^3(x_4)\circ\ldots\circ\varphi^{n-1}(x_n)\circ b, \tag{4}$$

*where $(G,\circ)$ is a some group, $b$ – a fixed element of $G$, $\varphi$ – an automorphism of $(G,\circ)$ such that $\varphi(b)=b$ and $\varphi^{n-1}(x)\circ b=b\circ x$ for every $x\in G$.* □

In connection with this fact we say that any $n$-ary group $(G,f)$ is $(\varphi,b)$-*derived* from some group $(G,\circ)$. In the case when $\varphi$ is the identity mapping, we say that an $n$-ary group $(G,f)$ is $b$-*derived* from $(G,\circ)$. If $e$ is the identity of $(G,\circ)$, then an $n$-ary group $e$-derived from $(G,\circ)$ is called *reducible* to $(G,\circ)$ or *derived* from $(G,\circ)$. An $n$-ary group is reducible if and only if it contains at least one neutral element (cf. [2]).

One can prove (cf. for example [14] or [32]) that for a given $n$-ary group $(G,f)$ the group $(G,\circ)$ from the above theorem is determined uniquely up to isomorphism and can be identified with the group $(G,\cdot)=ret_a(G,f)$, where $x\cdot y=f(x,a,\ldots,a,\overline{a},y)$. Fixing in an $n$-ary operation $f$ arbitrary $n-2$ internal elements we obtain a new operation which depends only on two external elements. Choosing different sequences $a_2,\ldots,a_{n-1}$ we obtain different binary groupoids $(G,\diamond)$ of the form $x\diamond y=f(x,a_2,\ldots,a_{n-1},y)$. For a given $n$-ary group $(G,f)$ all these groupoids are groups. Moreover, all these groups are isomorphic to the *retract* $ret_a(G,f)$.

An $n$-ary group having a commutative retract is called *semicommutative.* It satisfies the identity

$$f(x_1,x_2,\ldots,x_{n-1},x_n)=f(x_n,x_2,\ldots,x_{n-1},x_1).$$

An $n$-group $(G,f)$ satisfying the identity

$$f(x_1,x_2,\ldots,x_n)=f(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)}),$$

where $\sigma$ is an arbitrary permutation of the set $\{1,2,\ldots,n\}$, is called *commutative.* In view of Theorem 2.2 any commutative $n$-ary group is $b$-derived from some abelian group.

An *$n$-ary power* of $x$ in an $n$-ary group $(G,f)$ is defined in the following way: $x^{<0>}=x$ and $x^{<k+1>}=f(x,\ldots,x,x^{<k>})$ for all $k>0$. $x^{<-k>}$ is an element $z$ such that $f(x^{<k-1>},x,\ldots,x,z)=x^{<0>}=x$ (cf. [25]). Then $\overline{x}=x^{<-1>}$ and

$$f(x^{<k_1>},\ldots,x^{<k_n>})=x^{<k_1+\ldots+k_n+1>} \tag{5}$$

$$(x^{<k>})^{<t>}=x^{<kt(n-1)+k+t>}. \tag{6}$$

The order of the smallest subgroup of $(G,f)$ containing an element $x$ of $G$ is called the *$n$-ary order of* $x$ and is denoted by $\operatorname{ord}_n(x)$. It is the smallest positive integer $k$ such that $x^{<k>}=x$ (cf. [25]). If $\operatorname{ord}_n(x)=k$, then the smallest subgroup of $(G,f)$ containing $x$ has the form

$$\langle x\rangle=\{x,x^{<1>},x^{<2>},\ldots,x^{<k-1>}\}.$$

It is called *cyclic*. From (5) it follows that a cyclic $n$-ary group is commutative. A cyclic $n$-ary group of order $k$ can be identified with the $n$-ary group $(\mathbb{Z}_k, f_1)$, where

$$f_1(x_1, \ldots, x_n) = (x_1 + x_2 + \ldots + x_n + 1)(\mathrm{mod}\ k).$$

The $n$-ary group $(\mathbb{Z}_k, f_1)$ is generated by 0. In the case when all $n$-ary powers of $x$ are different, we say that $x$ has an infinite $n$-ary order. The smallest $n$-ary subgroup containing all these $n$-ary powers is called the *infinite cyclic n-ary group generated by* $x$. It is isomorphic to $(\mathbb{Z}, g_1)$, where

$$g_1(x_1, \ldots, x_n) = x_1 + x_2 + \ldots + x_n + 1. \tag{7}$$

This isomorphism has the form $h(x^{<s>}) = s$.

Observe also that according to Theorem 2.2 any cyclic $n$-ary group $(G, f)$ generated by $a$ can be considered as an $n$-ary group $a^{<1-n>}$-derived from a cyclic group $(G, *)$, where $x * y = f(x, a, \ldots, a, y)$. Then $\overline{a}$ is the identity of $(G, *)$ and $a^{<k>} = a^{k+1}$ in $(G, *)$, which means that $(G, *)$ and $(G, f)$ are generated by the same element $a$.

Consider the sequence of elements: $x$, $\overline{x}$, $\overline{x}^{(2)}$, $\overline{x}^{(3)}, \ldots$, where $\overline{x}^{(k+1)}$ denotes the element skew to $\overline{x}^{(k)}$ and $\overline{x}^{(0)} = x$. All these elements belong to the same $n$-ary subgroup generated by $x$. Moreover, in view of (6) and $\overline{x} = x^{<-1>}$, we have

$$\begin{aligned}\overline{x}^{(2)} &= (x^{<-1>})^{<-1>} = x^{<n-3>},\\ \overline{x}^{(3)} &= (\,(x^{<-1>})^{<-1>})^{<-1>},\end{aligned}$$

and so on. Generally: $\overline{x}^{(m)} = (\overline{x}^{(m-1)})^{<-1>}$ for all $m \geqslant 1$. This implies that

$$\overline{x}^{(m)} = x^{<S_m>} \quad \text{for} \quad S_m = -\sum_{i=0}^{m-1} (2-n)^i = \frac{(2-n)^m - 1}{n-1} \tag{8}$$

(cf. [6] and [10]). If $\mathrm{ord}_n(x) = k$ is finite, then $\overline{x} = x^{<k-1>}$, $\overline{x}^{(2)} = x^{<n-3>}$, $\overline{x}^{(3)} = x^{<2-n>}$. Since $\overline{x}$ belongs to the $n$-ary subgroup generated by $x$, from Lagrange's theorem for finite $n$-ary groups (cf. [25], p.222), we obtain

$$\mathrm{ord}_n(x) \geqslant \mathrm{ord}_n(\overline{x}) \geqslant \mathrm{ord}_n(\overline{x}^{(2)}) \geqslant \mathrm{ord}_n(\overline{x}^{(3)}) \geqslant \ldots$$

In fact, $\mathrm{ord}_n(\overline{x})$ is a divisor of $\mathrm{ord}_n(x)$ (cf. [3]). Moreover, if $\mathrm{ord}_n(x) < \infty$, then $\mathrm{ord}_n(\overline{x}) = \mathrm{ord}_n(x)$ if and only if $\mathrm{ord}_n(x)$ and $n-2$ are relatively prime.

In this case $\operatorname{ord}_n(\overline{x}^{(s)})=\operatorname{ord}_n(x)$ for every $s$. Thus $\lim\limits_{s\to\infty}\operatorname{ord}_n(\overline{x}^{(s)})=1$ if and only if $\operatorname{ord}_n(x)$ is a divisor of $n-2$ (cf. [3]). Obviously $\overline{x}^{(t)}\neq\overline{y}^{(t)}$ means that also $\overline{x}^{(s)}\neq\overline{y}^{(s)}$ for every $0\leqslant s<t$.

Note by the way, that in some $n$-ary groups (described in [5] and [8]) we have $x^{<s>}=\overline{x}^{(n-s-1)}$. Such $n$-ary groups are the set-theoretic union of disjoint cyclic $n$-ary subgroups of order $k$ isomorphic to the subgroup

$$\{x,\overline{x},\overline{x}^{(2)},\ldots,\overline{x}^{(k-1)}\}.$$

The problem when one fixed element is skew to others was solved by the following theorem proved in [7].

**Theorem 2.3.** (Dudek, 1990)
*$\overline{x}=\overline{y}$ for all elements $x,y$ of an $n$-ary group $(G,f)$ if and only if $(G,f)$ is derived from a binary group of the exponent $t|n-2$.* □

Generally, as it was observed in [28], from Theorem 2.2 it follows that $\overline{x}=\overline{y}$ if and only if the sequences $\underbrace{x,\ldots,x}_{n-2}$ and $\underbrace{y,\ldots,y}_{n-2}$ are equivalent in the sense of Post (cf. [25]).

## 3. Skew endomorphisms of $n$-ary groups

In [17] was proved that in semiabelian $n$-ary groups we have

$$\overline{f(x_1,\ldots,x_n)}=f(\overline{x}_1,\ldots,\overline{x}_n),$$

i.e., the operation $^{-}:x\longrightarrow\overline{x}$ is an endomorphism. In this case also $h(x)=\overline{x}^{(s)}$ is an endomorphism for every $s\geqslant 0$. The converse is not true since, for example, in all ternary ($n=3$) groups $\overline{\overline{x}}=x$ and $\overline{f(x,y,z)}=f(\overline{z},\overline{y},\overline{x})$ (cf. [2]). So, $h(x)=\overline{\overline{x}}$ is an endomorphism, but $^{-}:x\longrightarrow\overline{x}$ is an endomorphism only for ternary groups satisfying the identity $f(x,y,z)=f(z,y,x)$.

This means that $h(x)=\overline{x}^{(s)}$ is an automorphism of semiabelian $n$-ary groups in which $\overline{x}^{(k)}=x$ holds for all $x\in G$ and some fixed $k$.

Any map of the form $h(x)=\overline{x}^{(s)}$, where $s>0$, is called a skew map or a *skew endomorphism* if it is an endomorphism.

The natural question (posed in [6], see also [10]) is:

*When $h(x)=\overline{x}$ is an endomorphism?*

The first partial answer was given in [10]. The full, rather complicated, characterization of $n$-ary groups for which $h(x)=\overline{x}$ is an endomorphism is presented in [31]. It is based on two identities. Later it was proved that such $n$-ary groups can be characterized by one identity containing $n+2$ variables [27].

Below we present new characterizations of such $n$-ary groups .

**Theorem 3.1.** *The map $h(x)=\overline{x}^{(s)}$ is an automorphism of a cyclic $n$-ary group of order $k$ if and only if $k$ and $n-2$ are relatively prime.*

*Proof.* A cyclic $n$-ary group of order $k$ is isomorphic to the $n$-ary group $(\mathbb{Z}_k, f_1)$ in which the skew element has the form $\overline{x}=((2-n)x-1)(\operatorname{mod} k)$. Since $(\mathbb{Z}_k, f_1)$ is commutative, $h(x)=\overline{x}^{(s)}$ is an endomorphism.

Assume that $h(x)=\overline{x}^{(s)}$ is an automorphism and $\gcd(k,n-2)=d$. Then $k=dv$ and $n-2=du$ for some $u,v$. Since

$$f_1(v,\ldots,v,\overline{0})=(n-2)v+v=duv+v=ku+v=v(\operatorname{mod} k),$$

we have $\overline{0}=\overline{v}$. Thus $h(k)=h(0)=\overline{0}^{(s)}=\overline{v}^{(s)}=h(v)$. Hence $k=v$ and $d=1$, i.e., $k$ and $n-2$ are relatively prime.

Conversely, if $k$ and $n-2$ are relatively prime, then $h(u)=h(v)$ implies $(2-n)^s(u-v)=0(\operatorname{mod} k)$. Hence $u=v$. So, $h(x)=\overline{x}^{(s)}$ is an automorphism. □

**Corollary 3.2.** *If each element of an $n$-ary group $(G,f)$ has a finite $n$-ary order, then $h(x)=\overline{x}^{(s)}$ is a bijective map if and only if for every $x\in G$* $\gcd(\operatorname{ord}_n(x),n-2)=1$.

*Proof.* If $h(x)=\overline{x}^{(s)}$ is a bijection, then the restriction of $h$ to an arbitrary cyclic $n$-ary subgroup $\langle a\rangle$ of $(G,f)$ is an automorphism. Hence, by Theorem 3.1, $\operatorname{ord}_n(a)$ and $n-2$ are relatively prime.

Conversely, let $\overline{a}^{(s)}=\overline{c}^{(s)}$ for some $a,c\in G$. If $\operatorname{ord}_n(a)=k<\infty$ and $n-2$ are relatively prime, then $\operatorname{ord}_n(a)=\operatorname{ord}_n(\overline{a})=\operatorname{ord}_n(\overline{a}^{(s)})=\operatorname{ord}_n(\overline{c}^{(s)})=\operatorname{ord}_n(\overline{c})$ and $\langle a\rangle=\langle\overline{a}\rangle=\langle\overline{a}^{(s)}\rangle=\langle\overline{c}^{(s)}\rangle=\langle\overline{c}\rangle=\langle c\rangle$ since $\overline{x}^{(t)}\in\langle x\rangle$ for every $t$. Thus $c=a^{<m>}$ for some $0<m\leqslant k$. Hence, by (8), for some $S$ we have $\overline{c}^{(s)}=c^{<S>}=(a^{<m>})^{<S>}=(a^{<S>})^{<m>}=(\overline{a}^{(s)})^{<m>}=(\overline{c}^{(s)})^{<m>}$, which implies $m=k$. So, $c=a^{<k>}=a$. This proves that $h(x)=\overline{x}^{(s)}$ is a bijection. □

**Corollary 3.3.** *If each element of a semiabelin $n$-ary group $(G,f)$ has finite $n$-ary order, then the skew map $h(x)=\overline{x}^{(s)}$ is an automorphism of $(G,f)$ if and only if* $\gcd(\operatorname{ord}_n(x),n-2)=1$ *for every $x\in G$.* □

**Corollary 3.4.** *The skew map $h(x) = \overline{x}^{(s)}$ is an automorphism of a semiabelian $n$-ary group of finite order $k$ if and only if $k$ and $n-2$ are relatively prime.* □

**Corollary 3.5.** *For $n > 3$ an $n$-ary group $b$-derived from an infinite cyclic group has no non-trivial skew endomorphisms.*

*Proof.* Let $(G, f)$ be an $n$-ary group $b$-derived from a cyclic group generated by $a$. Then $b = a^t$ for some $t$ and $\overline{a^m}^{(s)} = a^{m(2-n)^s+T}$ for every $a^m \in \langle a\rangle$, where $T = -t(2-n)^{s-1} - t(2-n)^{s-2} - \ldots - t$. So, if $h(x) = \overline{x}^{(s)}$ is a non-trivial automorphism, then for every $a^p \in \langle a\rangle$ there exists $a^m \in \langle a\rangle$ such that $a^p = h(a^m)$. In particular, for $a^{1+T}$ there exists $a^k$ such that $a^{1+T} = h(a^k) = a^{k(2-n)^s+T}$, which implies $1 = k(2-n)^s$. Thus $n = 3$. So, for $n > 3$ no non-trivial skew endomorphisms. □

A ternary group $b$-derived from an infinite cyclic group has a non-trivial skew endomorphism. Indeed, in such ternary groups $x \neq \overline{x}$, $x = \overline{\overline{x}}$ and $\overline{f(x,y,z)} = f(\overline{z},\overline{y},\overline{x}) = f(\overline{x},\overline{y},\overline{z})$ (cf. [2]). So, $h(x) = \overline{x}$ is a non-trivial skew automorphism of this group.

All $n$-ary groups $b$-derived from finite cyclic groups have non-trivial skew endomorphisms since, as it is not difficult to see, $h(x) = \overline{x} = x^{2-n}b^{-1}$ is such endomorphism.

## 4. Precyclic $n$-ary groups

In this section we describe $n$-ary groups $(\varphi, b)$-derived from cyclic groups. Such $n$-ary groups are called *semicyclic* or *precyclic*.

An infinite cyclic group has only two automorphisms: $\varphi(x) = x$ and $\varphi(x) = x^{-1}$. Hence, according to Theorem 2.2, on an infinite group $\langle a\rangle$ we can define two types of $n$-ary groups. The operation of an $n$-ary group of the first type is induced by the identity automorphism $\varphi(x) = x$ and has the form

$$f(a^{s_1}, a^{s_2}, a^{s_3}, \ldots, a^{s_{n-1}}, a^{s_n}) = a^{s_1+s_2+s_3+\ldots+s_{n-1}+s_n+l}. \tag{9}$$

The operation of an $n$-ary group of the second type is induced by the automorphism $\varphi(x) = x^{-1}$. Since, by Theorem 2.2, $\varphi^{n-1}(x) = x$ for all $x \in \langle a\rangle$, $n$ must be odd. Moreover, in this case for $b = a^l$ should be $\varphi(a^l) = a^l$, which means that $b$ must be the identity of $\langle a\rangle$. Thus, in this case

$$f(a^{s_1}, a^{s_2}, a^{s_3}, \ldots, a^{s_{n-1}}, a^{s_n}) = a^{s_1-s_2+s_3-s_4+\ldots-s_{n-1}+s_n}, \tag{10}$$

where $n$ is odd.

In the first case we say that this $n$-ary group id $(1,l)$-*derived* from an infinite cyclic group, in the second case that it is $(-1,0)$-*derived*.

Now, consider $n$-ary groups $(\varphi,b)$-derived from finite cyclic groups. Automorphisms of a cyclic group of order $2<k<\infty$ have the form $\varphi(x)=x^m$, where $0<m<k$ and $\gcd(m,k)=1$. So, the operation of an $n$-ary group defined on a cyclic group $\langle a\rangle$ of order $k$ has the form

$$f(a^{s_1},a^{s_2},\ldots,a^{s_{n-1}},a^{s_n})=a^{s_1+ms_2+m^2s_3+m^3s_4+\ldots+m^{n-2}s_{n-1}+s_n+l}, \qquad (11)$$

where $0<m<k$, $\gcd(m,k)=1$, $m^{n-1}=1(\operatorname{mod}k)$, $0\leqslant l<k$ and $lm\equiv l(\operatorname{mod}k)$. We say that such $n$-ary group is $(m,l)$-*derived* from a finite cyclic group of order $k$.

It is clear that $n$-ary groups $(\varphi,b)$-derived from the same group may be isomorphic. The answer to the question when two $n$-ary groups $(\varphi,b)$-derived fom cyclic groups of the same order are isomorphic can be deduced from the existence of some special isomorphisms of their retracts (cf. [15] or [12]) or from the following theorem proved in [14].

**Theorem 4.1.** (Dudek, Michalski, 1982)
*Let an $n$-ary group $(A,f)$ be $(\varphi,a)$-derived from a group $(A,\cdot)$ and an $n$-ary group $(B,g)$ be $(\psi,b)$-derived from a group $(B,\circ)$. Then $(A,f)$ and $(B,g)$ are isomorphic if and only if there exists an isomorphism $\beta:(A,\cdot)\to(B,\circ)$ of groups and an element $c\in B$ such that*

$$\beta(a)=c\circ\psi(c)\circ\ldots\circ\psi^{n-2}(c)\circ b \quad \textit{and} \quad \beta(\varphi(x))\circ c=c\circ\psi(\beta(x))$$

*for all $x\in A$.* □

As a consequence of the above theorem we obtain two important characterizations of $n$-ary groups defined on the same infinite cyclic group.

**Corollary 4.2.** *Two $n$-ary groups $(1,l_1)$ and $(1,l_2)$-derived from the additive group $(\mathbb{Z},+)$ are isomorphic if and only if $l_1\equiv l_2(\operatorname{mod}(n-1))$ or $l_1\equiv -l_2(\operatorname{mod}(n-1))$.* □

**Corollary 4.3.** *On an infinite cyclic group one can defined $[\frac{n-1}{2}]$ non-isomorphic commutative $n$-ary groups. Each such $n$-ary group is isomorphic to one of the $n$-ary groups $(1,l)$-derived $(0\leqslant l\leqslant\frac{n-1}{2})$ from the group $(\mathbb{Z},+)$.* □

Below, for the simplicity of formulations of our results for $n$-ary groups $(m,l)$-derived from finite cyclic groups, by $S(m)$ we will denote the sum $1+m+m^2+\ldots+m^{n-2}$.

We start from one arithmetical lemma. The proof of this lemma is analogous to the proof of Lemma A in [18].

**Lemma 4.4.** *Let* $0<l_1,l_2,m<k$. *Then for* $k,n>2$ *the congruence*

$$xl_1 \equiv (yS(m)+l_2)(\operatorname{mod} k),$$

*where* $\gcd(m,k)=1$, *has a solution in* $x$ *and* $y$ *if and only if*

$$\gcd(l_1,S(m),k)=\gcd(l_2,S(m),k). \qquad \Box$$

Using this lemma and Theorem 4.1 we can prove

**Theorem 4.5.** *Two* $n$*-ary groups* $(m_1,l_1)$ *and* $(m_2,l_2)$*-derived from a cyclic group of a finite order* $k$ *are isomorphic if and only if*

$$gcd(l_1,S(m_1),k)=gcd(l_2,S(m_2),k) \;\text{ and }\; m_1=m_2. \qquad \Box$$

**Corollary 4.6.** *Any* $k$*-element* $n$*-ary group defined on a cyclic group is isomorphic to one of the* $n$*-ary groups* $(m,l)$*-derived from the group* $(\mathbb{Z}_k,+)$, *where* $l$ *is a divisor of* $gcd(S(m),k)$. □

**Proposition 4.7.** *For* $n>3$, *a precyclic* $n$*-ary group has a non-trivial skew endomorphism if and only if it is finite and non-idempotent.*

*Proof.* A precyclic $n$-ary group is semiabelian, hence $h(x)=\overline{x}$ is its skew endomorphism. It is non-trivial only in the case when an $n$-ary group is non-idempotent.

If a precyclic $n$-ary group is infinite, then its operation $f$ is defined by (9) or (10). In the first case it is commutative. Hence, by Corollary 3.5, for $n>3$ it has no non-trivial skew endomorphism. In the second case it is idempotent and has only trivial skew endomorphism. □

Any ternary non-idempotent group has a non-trivial skew endomorphism. Since in ternary groups $\overline{\overline{x}}=x$, a skew endomorphism is an automorphism. An infinite precyclic $n$-ary group has no non-trivial skew automorphisms.

**Corollary 4.8.** *A skew endomorphism of a precyclic* $n$*-ary group of a finite order* $k$ *is its automorphism if and only if* $gcd(n-2,k)=1$.

*Proof.* It follows from Corollary 3.4. □

## 5. Subgroups of $n$-ary precyclic groups

It is not difficult to verify that in an $n$-ary group $(G,f)$ which is $(m,l)$-derived from a finite cyclic group $\langle a\rangle$, each coset $a^r\langle a^v\rangle$ of $\langle a\rangle$, where $rS(m)+l\equiv 0(\operatorname{mod} v)$, is an $n$-ary subgroup of $(G,f)$. But not all $n$-ary subgroups of $(G,f)$ are of this form. For example, in a 5-ary group $(1,0)$-derived from a cyclic group $\langle a\rangle$ of order 4 two 5-ary subgroups $S_0=\{a^0,a^2\}$ and $S_1=\{a^1,a^3\}$ are cosets of $\langle a\rangle$ with respect to $S_0$. Subgroups $\{a^0\}$, $\{a^1\}$, $\{a^2\}$, $\{a^3\}$ are cosets of $\langle a\rangle$ with respect to $\{a^0\}$ but not with respect to $S_0$.

Obviously, each $n$-ary subgroup of an $n$-ary group $(G,f)$ is a subgroup of some retract of $(G,f)$. Indeed, if $H$ is an $n$-ary subgroup of an $n$-ary group $(G,f)$, then $ret_a(H,f)$ is a subgroup of $ret_a(G,f)$ for every $a\in H$. This means that any $n$-ary subgroup of a precyclic $n$-ary group $(\langle a\rangle,f)$ is normal subgroup of some cyclic group isomorphic to $\langle a\rangle$.

In any precyclic $n$-ary group $(G,f)$ the map $h(x)=\overline{x}$ is an endomorphism. So, $h(G)=G^{(1)}=\{\overline{x}\,|\,x\in G\}$ is an $n$-ary subgroup of $(G,f)$. Also $h^2(G)=G^{(2)}=\{\overline{\overline{x}}\,|\,x\in G\}$ is an $n$-ary subgroup of $(G,f)$. In this way we obtain the sequence of $n$-ary subgroups

$$G\supseteq G^{(1)}\supseteq G^{(2)}\supseteq G^{(3)}\supseteq\ldots$$

In finite $n$-ary groups $G^{(k)}=G^{(k+1)}=\ldots$ for some natural $k$, but there are $n$-ary groups for which $G^{(k)}\neq G^{(k+1)}$ for all $k$. Moreover, $G^{(1)}$ is an $n$-ary subgroup also in some $n$-ary groups for which $h(x)=\overline{x}$ is not an endomorphism. For example, in a 4-ary group $(G,f)$ derived from the symmetric group $\mathbb{S}_3$ we have $\overline{x}=x$ for $x^3=e$ and $\overline{x}=e$ for $x^2=e$. Thus $G^{(1)}=\mathbb{A}_3$ is a subgroup of $(G,f)$ but $h(x)=\overline{x}$ is not an endomorphism of $(G,f)$ because $\overline{f(y,z,y,z)}\neq f(\overline{y},\overline{z},\overline{y},\overline{z})$ for $y=(1\,2)$ and $z=(1\,2\,3)$.

The list of unsolved problems connected with $G^{(k)}$ one can find in [6] and [10].

If $h(x)=\overline{x}$ is an endomorphism of $(G,f)$, then the relation

$$x\rho y\Longleftrightarrow\overline{x}=\overline{y}\tag{12}$$

is a congruence on $(G,f)$. We say that this relation is *determined by the skew endomorphism.* Obviously, $\rho$ is a congruence on any precyclic $n$-ary group.

It is not difficult to see that a congruence $\tau$ of an $n$-ary group $(G,f)$ is a congruence of its retract $ret_a(G,f)$. The converse is not true. A congruence $\theta$ of a group $(G,\circ)$ is a congruence of an $n$-ary group $(\varphi,b)$-derived from

$(G,\circ)$ only in the case when for all $x,y\in G$ from $x\theta y$ it follows $\varphi(x)\theta\varphi(y)$, or equivalently, if $\varphi(H)\subseteq H$ for a normal subgroup $H$ of $(G,\circ)$ determining $\theta$. Thus, a relation $\theta$ defined on an $n$-ary group $(G,f)$ $b$-derived from a group $(G,\circ)$ is a congruence if and only if it is a congruence on $(G,\circ)$. The similar result is valid for precyclic $n$-ary group since for any automorphism $\varphi$ and any subgroup $\langle a^m\rangle$ of a cyclic group $\langle a\rangle$ holds $\varphi(\langle a^m\rangle)\subseteq\langle a^m\rangle$.

Thus we have proved

**Proposition 5.1.** *A relation $\theta$ defined on a precyclic group is a congruence if and only if it is a congruence of the corresponding cyclic group.* □

For relation defined by (12) we have stronger result.

**Proposition 5.2.** *On an $n$-ary group $(m,l)$-derived from a cyclic group $\langle a\rangle$ of order $k$ the relation $\rho$ determined by its skew endomorphism is a congruence which coincides with the congruence on $\langle a\rangle$ induced by the subgroup $\langle a^{\frac{k}{d}}\rangle$, where $d=gcd(S(m)-1,k)$. In this case, the class $[a^s]_\rho$ coincides with the coset $a^s\langle a^{\frac{k}{d}}\rangle$.*

*Proof.* At first we consider the case $m=1$. In this case $d=gcd(n-2,k)$, i.e., $n-2=dd_1$ and $k=dk_1$ for some natural $d_1$, $k_1$ such that $gcd(d_1,k_1)=1$. Since an $n$-ary group $(G,f)$ is $(1,l)$-derived from a cyclic group $\langle a\rangle$ of order $k$, we have $\overline{a^s}=a^{s(2-n)-l}$ for every $a^s\in\langle a\rangle$. Thus $a^{s_1}\rho\, a^{s_2}$ if and only if $s_1(n-2)\equiv s_2(n-2)(\operatorname{mod} k)$, i.e., if and only if $s_1dd_1\equiv s_2dd_1(\operatorname{mod} dk_1)$. This is equivalent to $s_1d_1\equiv s_2d_1(\operatorname{mod} k_1)$. In view of $gcd(d_1,k_1)=1$, the last congruence means that $s_1\equiv s_2(\operatorname{mod}\frac{k}{d})$. So, $a^{s_1}\rho\, a^{s_2}$ if and only if $a^{s_1-s_2}\in\langle a^{\frac{k}{d}}\rangle$.

Now let $m\neq 1$, $gcd(m,k)=1$ and $d=gcd(S(m)-1,k)$. Then $a^{s_1}\rho\, a^{s_2}$ if and only if $s_1(S(m)-1)\equiv s_2(S(m)-1)(\operatorname{mod} k)$, i.e., if and only if $s_1\frac{m^{n-2}-1}{m-1}\equiv s_2\frac{m^{n-2}-1}{m-1}$ (mod $k$). Since $S(m)-1=m\frac{m^{n-2}-1}{m-1}=mdm_1$ and $k=dk_1$, where $gcd(m_1,k_1)=1$. The last congruence, similarly as in the first part of this proof, means that $s_1\equiv s_2(\operatorname{mod}\frac{k}{d})$. So, $a^{s_1}\rho\, a^{s_2}$ if and only if $a^{s_1-s_2}\in\langle a^{\frac{k}{d}}\rangle$. □

As is well known in binary groups one equivalence class of any congruence is a subgroup. This class coincides with a normal subgroup determining this congruence. For $n$-ary group it is not true. In a ternary group 1-derived from the additive group $\mathbb{Z}_2$ the congruence $\rho$ defined by (12) has two equivalence classes: $[0]_\rho$ and $[1]_\rho$. These classes are not ternary subgroups. But the same congruence defined on a ternary group 2-derived from the group $\mathbb{Z}_4$ has two classes which are not ternary subgroups and two classes which are ternary subgroups. So, the natural question is: *how many* (*and which*) *the classes are $n$-ary subgroups.* For precyclic $n$-ary groups the answer is given by the following theorem.

**Theorem 5.3.** *Let $(\langle a\rangle, f)$ be an $n$-ary group $(m,l)$-derived from a cyclic group $\langle a\rangle$ of order $k$. If $gcd(S(m),k)$ divides $l$, then the congruence determined by the skew endomorphism of $(\langle a\rangle, f)$ has exactly $gcd(S(m),k)$ equivalence classes which are $n$-ary subgroups. These classes are defined by elements $a^s$, where $sS(m)\equiv 0(\bmod \frac{k}{gcd(S(m)-1,k)})$. In the case $gcd(S(m),k)\nmid l$ no such classes.*

*Proof.* According to Proposition 5.2, in an $n$-ary group $(m,l)$-derived from a cyclic group $\langle a\rangle$ of order $k$ the equivalence class $[a^s]_\rho$ coincides with the coset $a^s\langle a^{\frac{k}{d}}\rangle$, where $d = gcd(S(m)-1,k)$. As it is easy to see, this coset is an $n$-ary subgroup only in the case when

$$sS(m) + l \equiv 0(\bmod \frac{k}{d}). \tag{13}$$

At first we consider the case when $m = 1$. In this case $S(m) = n-1$ and (13) has the form

$$s(n-1) + l \equiv 0(\bmod \frac{k}{d}), \tag{14}$$

where $d = gcd(n-2,k)$.

Since $n-1$ and $n-2$ are relatively prime, $gcd(n-1,k) = gcd(n-1,\frac{k}{d})$. Thus $gcd(n-1,k)$ is a divisor of $n-1$ and $\frac{k}{d}$. This together with (14) proves that $gcd(n-1,k)$ is a divisor of $l$. So, $gcd(l,n-1,k) = gcd(0,n-1,k)$. Hence, by Theorem 4.5, this $n$-ary group is isomorphic to the $n$-ary group $(1,0)$-derived from a cyclic group $\langle a\rangle$ of order $k$. But in the last $n$-ary group the equivalence class $[a^s]_\rho$ is an $n$-ary subgroup only in the case when $s(n-1)\equiv 0(\bmod\frac{k}{d})$.

Since $gcd(n-1,n-2) = 1$, the equation $x(n-1)\equiv 0(\bmod\frac{k}{d})$ has $gcd(n-1,k)$ solutions. So, exactly $gcd(n-1,k)$ classes of the form $[a^s]_\rho$ are $n$-ary subgroups. In the case $gcd(n-1,k)\nmid l$ no $s$ satisfying (14).

This completes the proof for $m = 1$ .

Now let $m \neq 1$. In this case we have $gcd(S(m),k) = gcd(S(m),\frac{k}{d})$, where $d = gcd(S(m)-1,k)$. Indeed, since $k = dk_1$, for any common divisor

$p > 1$ of $S(m) = \frac{m^{n-1}-1}{m-1}$ and $k$, in view of $gcd(m,k) = 1$,

$$S(m) - 1 = m\frac{m^{n-2}-1}{m-1} \quad \text{and} \quad S(m) = \frac{m^{n-2}-1}{m-1} + m^{n-2},$$

from $p|d$ it follows $p|\frac{m^{n-2}-1}{m-1}$. Hence $p|m$ which is a contradiction because $gcd(m,k) = 1$. Thus $p \nmid d$, i.e., $p|k_1 = \frac{k}{q}$. So, $gcd(S(m),k) = gcd(S(m), \frac{k}{q})$.

If $gcd(S(m),k)|l$, then, according to Theorem 4.5, an $n$-ary group $(m,l)$-derived from a cyclic group of order $k$ is isomorphic to some $n$-ary group $(m,0)$-derived from this group. In this $n$-ary group the class $[a^s]_\rho$ is an $n$-ary subgroup only in the case when $sS(m) \equiv 0(\text{mod}\frac{k}{d})$.

Further argumentation is similar to the argumentation used in the first part of this proof. □

**Corollary 5.4.** *If an $n$-ary group $(G,f)$ is $(m,l)$-derived from a cyclic group $\langle a\rangle$ of order $k$, then the image of $G$ under the skew endomorphism $h(x) = \overline{x}$ of $(G,f)$ coincides with the coset $a^{-l}\langle a^d\rangle$ of $\langle a\rangle$, where $d = gcd(S(m)-1,k)$.*

*Proof.* Indeed, $h(G) = \{\overline{a^s} \mid a^s \in \langle a\rangle\} = \{a^{-l-s(S(m)-1)}\} = a^{-l}\langle a^d\rangle$, where $d = gcd(S(m)-1,k)$. □

## 6. Automorphisms of precyclic $n$-ary groups

**Theorem 6.1.** *Any endomorphism $\psi$ of a precyclic $n$-ary group $(\langle a\rangle, f)$ can be presented in the form $\psi(x) = \varphi(x)a^t$, where $\varphi$ is an endomorphism of a group $\langle a\rangle$ and $a^t = \psi(e)$.*

*Proof.* Let $\varphi(x) = \psi(x)a^{-t}$, where $a^t = \psi(e)$. Since $\psi$ is an endomorphism of $n$-ary group $(m,l)$-derived from a cyclic group $\langle a\rangle$, we have $\psi(\overline{x}) = \overline{\psi(x)}$ for every $x \in \langle a\rangle$ and $\overline{e} = \overline{a^0} = a^{-l}$. Thus $\psi(\overline{e}) = \psi(a^{-l}) = a^{-(n-2)t-l}$ for $m = 1$, and $\psi(a^{-l}) = a^{-\frac{m(m^{n-2}-1)}{m-1}t-l}$ for $m \neq 1$. Hence in the case $m = 1$ for all $a^{s_1}$, $a^{s_2} \in \langle a\rangle$ we have

$$\begin{aligned}
\varphi(a^{s_1}a^{s_2}) &= \psi(a^{s_1}a^{s_2})a^{-t} = \psi(f(a^{s_1}, e, \ldots, e, \overline{e}, a^{s_2}))a^{-t} \\
&= f(\psi(a^{s_1}), \psi(e), \ldots, \psi(e), \psi(\overline{e}), \psi(a^{s_2}))a^{-t} \\
&= f(\psi(a^{s_1}), a^t, \ldots, a^t, a^{-(n-2)t-l}, \psi(a^{s_2}))a^{-t} \\
&= \psi(a^{s_1})a^{-t}\psi(a^{s_2})a^{-t} = \varphi(a^{s_1})\varphi(a^{s_2}),
\end{aligned}$$

which proves that $\varphi$ is an endomorphism of $\langle a\rangle$.

For $m\neq 1$ the proof is analogous. Similarly for infinite precyclic $n$-ary groups. □

Since in the above theorem $\psi$ is bijective if and only if $\varphi$ is bijective, we obtain

**Corollary 6.2.** *If $\psi$ is an automorphism of a precyclic $n$-ary group $(\langle a\rangle,f)$, then $\varphi(x)=\psi(x)a^{-t}$ with $a^t=\psi(e)$, is an automorphism of a group $\langle a\rangle$.* □

**Theorem 6.3.** *If $\varphi(x)=x^w$ is an automorphism of a cyclic group $\langle a\rangle$ of order $k$, then $\psi(x)=\varphi(x)a^t$ is an automorphism of an $n$-ary group $(\langle a\rangle,f)$ $(m,l)$-derived from $\langle a\rangle$ if and only if $tS(m)\equiv l(w-1)(\operatorname{mod}k)$.*

*Proof.* The map $\psi$ is a bijection because $\varphi$ is an automorphism of $\langle a\rangle$. We prove that $\psi$ is an endomorphism of an $n$-ary group $(\langle a\rangle,f)$.

Since $(\langle a\rangle,f)$ is $(m,l)$-derived from $\langle a\rangle$, for $\psi(x)=\varphi(x)a^t$ and $m\neq 1$ we obtain

$$\psi(f(a^{s_1},\ldots,a^{s_n}))=\psi(a^{s_1+ms_2+\ldots+m^{n-2}s_{n-1}+s_n+l})=$$
$$=a^{w(s_1+ms_2+\ldots+m^{n-2}s_{n-1}+s_n+l)+t}=a^{ws_1+wms_2+\ldots+wm^{n-2}s_{n-1}+ws_n+t}a^{wl}$$

and

$$f(\psi(a^{s_1}),\ldots,\psi(a^{s_n}))=a^{ws_1+t}a^{m(ws_2+t)}\ldots a^{m^{n-2}(ws_{n-1}+t)}a^{ws_n+t}a^l$$
$$=a^{ws_1+wms_2+\ldots+wm^{n-2}s_{n-1}+ws_n+t}a^{t(1+m+\ldots+m^{n-2})+l}.$$

This means that $\psi$ is an endomorphism of an $n$-ary group $(\langle a\rangle,f)$ if and only if $wl\equiv(t(1+m+\ldots+m^{n-2})+l)(\operatorname{mod}k)$, i.e., if and only if $tS(m)\equiv l(w-1)(\operatorname{mod}k)$.

For $m=1$ the proof is analogous. □

**Corollary 6.4.** *Any automorphism $\psi$ of an $n$-ary group $(m,l)$-derived from a cyclic group $\langle a\rangle$ of order $k$ can be presented in the form $\psi(a^s)=a^{ws+t}$, where $gcd(w,k)=1$ and $tS(m)\equiv l(w-1)(\operatorname{mod}k)$.*

*Proof.* Let $\psi$ be an arbitrary automorphism of an $n$-ary group $(m,l)$-derived from a cyclic group $\langle a\rangle$ of order $k$. Then, according to Theorem 6.1, the map $\varphi:a^s\to\psi(a^s)a^{-t}$, where $\psi(e)=a^t$, is an automorphism of $\langle a\rangle$. Thus $\psi(a^s)=\varphi(a^s)a^t=a^{ws+t}$ for some $w$ relatively prime to $k$ and $tS(m)\equiv l(w-1)(\operatorname{mod}k)$. □

This means that any automorphism of an $n$-ary group $(m,l)$-derived from a finite cyclic group is uniquely determined by two numbers: $w$ and $t$. Hence, it will be denoted by $\psi_{w,t}$.

Corollary 4.6 shows that each precyclic $n$-ary group of order $k$ is isomorphic to some $n$-ary group $(m,l)$-derived from the group $\mathbb{Z}_k$, where $l$ is a divisor of $d=gcd(S(m),k)$. For such defined $l$ and $d$

$$A^*_{d/l}=\{w\in\mathbb{Z}^*_k\,|\,w\equiv 1(\text{mod}\,\frac{d}{l})\}$$

is a subgroup of the multiplicative group $\mathbb{Z}^*_k$ of the ring $(\mathbb{Z}_k,+,\cdot)$.

We use this subgroup to the description of the automorphism group of finite precyclic $n$-ary groups.

**Theorem 6.5.** *The automorphism group of an $n$-ary group $(m,l)$-derived from a cyclic group of order $k$ is isomorphic to the extension of a cyclic group of order $\frac{k}{d}$, where $d=gcd(S(m),k)$, by the multiplicative group $A^*_{d/l}$.*

*Proof.* Let $(\langle a\rangle,f)$ be an $n$-ary group $(m,l)$-derived from a cyclic group $\langle a\rangle$ of order $k$. Then $\langle a^{\frac{k}{d}}\rangle$, where $d=gcd(S(m),k)$, is a group of order $d$ contained in $\langle a\rangle$.

Consider the homomorphism $\zeta: A^*_{d/l}\rightarrow Aut\langle a^{\frac{k}{d}}\rangle$ such that $\zeta(w)=\varphi_r$, where $r$ is the remainder of $w$ after dividing by $d$. In this way, we obtain the extension $A^*_{d/l}\,\langle a^{\frac{k}{d}}\rangle$ of the group $\langle a^{\frac{k}{d}}\rangle$ by the group $A^*_{d/l}$ (see for example [19]) with the group operation

$$w_1a^{v_1\frac{k}{d}}\cdot w_2a^{v_2\frac{k}{d}}=(w_1w_2)a^{(w_2v_1+v_2)\frac{k}{d}}. \tag{15}$$

The map $\tau: Aut(\langle a\rangle,f)\rightarrow A^*_{d/l}\,\langle a^{\frac{k}{d}}\rangle$, where $\tau(\psi_{w,v})=wa^{v\frac{k}{d}}$, is a bijection. Moreover, for $\psi_{w_1,v_1},\psi_{w_2,v_2}\in Aut(\langle a\rangle,f)$ and $a^s\in\langle a\rangle$ we have

$$\begin{aligned}\psi_{w_1,v_1}\circ\psi_{w_2,v_2}(a^s)&=\psi_{w_2,v_2}(\psi_{w_1,v_1}(a^s))=\psi_{w_2,v_2}(a^{sw_1+t_1})\\&=a^{(sw_1+t_1)w_2+t_2}=a^{sw_1w_2+t_1w_2+t_2}\\&=a^{sw_1w_2+(t_1'w_2+t_2')+(w_2v_1+v_2)\frac{k}{d}}\\&=\psi_{w_1w_2,w_2v_1+v_2}(a^s),\end{aligned}$$

for $t_1=t_1'+v_1\frac{k}{d}$, $t_2=t_2'+v_2\frac{k}{d}$ and $(t_1'w_2+t_2')\frac{S(m)}{d}\equiv\frac{l(w_1w_2-1)}{d}(\text{mod}\frac{k}{d})$. Thus

$$\psi_{w_1,v_1}\circ\psi_{w_2,v_2}=\psi_{w_1w_2,w_2v_1+v_2}.$$

This together with (15), implies

$$\tau(\psi_{w_1,v_1}\circ\psi_{w_2,v_2})=(w_1w_2)a^{(w_2v_1+v_2)\frac{k}{d}}=\tau(\psi_{w_1,v_1})\cdot\tau(\psi_{w_2,v_2}).$$

So, $\tau$ is an isomorphism. Therefore $Aut(\langle a\rangle,f)\cong A^*_{d/l}\,\langle a^{\frac{k}{d}}\rangle$. □

**Corollary 6.6.** *The automorphism group of a cyclic $n$-ary group of a finite order $k$ is isomorphic to the direct sum $A_d^*\bigoplus\langle a^{\frac{k}{d}}\rangle$, where $d = gcd(n-1, k)$.*

*Proof.* Any cyclic $n$-ary group of order $k < \infty$ can be identified with $(\mathbb{Z}_k, f_1)$. So, it is $(1,1)$-derived from $\mathbb{Z}_k$. Its automorphism group is isomorphic to $A_d^*\,\langle a^{\frac{k}{d}}\rangle$, where $d = gcd(n-1,k)$ and $A_d^* = \{w \in \mathbb{Z}_k^* \,|\, w \equiv 1(\operatorname{mod} d)\}$.

Since $A_d^*$ and $\langle a^{\frac{k}{d}}\rangle$ are subgroups of $A_d^*\,\langle a^{\frac{k}{d}}\rangle$ which can be identified with $A_d^* \times \langle a^0\rangle$ and $\{1\} \times \langle a^{\frac{k}{d}}\rangle$, respectively, and $1a^{v\frac{k}{d}} \cdot wa^{0\frac{k}{d}} = wa^{0\frac{k}{d}} \cdot 1a^{v\frac{k}{d}}$ for all $w \in A_d^*$, $a^{v\frac{k}{d}} \in \langle a^{\frac{k}{d}}\rangle$ we obtain $A_d^*\,\langle a^{\frac{k}{d}}\rangle \cong A_d^*\bigoplus\langle a^{\frac{k}{d}}\rangle$. □

**Corollary 6.7.** *The automorphism group of a cyclic $n$-ary group of a prime order $p$ is isomorphic to $\mathbb{Z}_p^*$ or to $\mathbb{Z}_p^* \times \mathbb{Z}_p$.*

*Proof.* In this case $d = 1$ or $d = p$. If $d = 1$, then $A_d^* = \mathbb{Z}_p^*$ and $\langle a^{\frac{p}{d}}\rangle = \{a^0\}$. Thus, $A_d^*\,\langle a^{\frac{k}{d}}\rangle \cong \mathbb{Z}_p^*$. For $d = p$ we obtain $A_d^* = \mathbb{Z}_p^*$ and $\langle a^{\frac{p}{d}}\rangle = \langle a\rangle \cong \mathbb{Z}_p$. Hence $A_d^*\,\langle a^{\frac{k}{d}}\rangle \cong \mathbb{Z}_p^* \times \mathbb{Z}_p$. □

**Corollary 6.8.** *If $S(m)$ and $k$ are relatively prime, then the automorphism group of an $n$-ary group $(m,1)$-derived from a cyclic group of order $k$ is isomorphic to the multiplicative group $\mathbb{Z}_k^*$.*

*Proof.* Indeed, in this case $d = gcd(S(m),k) = 1$, $A_{d/l}^* = \mathbb{Z}_k^*$ and $\langle a^{\frac{k}{d}}\rangle = \langle a^k\rangle = \{a^0\}$. Hence $A_{d/l}^*\,\langle a^{\frac{k}{d}}\rangle = A_{d/l}^* = \mathbb{Z}_k^*$. □

**Theorem 6.9.** *A commutative precyclic $n$-ary group of infinite order has at most two automorphisms.*

*Proof.* Any infinite precyclic $n$-ary group is isomorphic to some $n$-ary group $(m,l)$-derived from the additive group $\mathbb{Z}$ of all integers. If it is commutative, then, by Corollary 4.3, there exists $0 \leqslant l \leqslant \left[\frac{n-1}{2}\right]$ for which this $n$-ary group is isomorphic to an $n$-ary group $(1,l)$-derived from the group $\mathbb{Z}$. But, by Theorem 6.1, for any automorphism $\psi$ of an $n$-ary group $(1,l)$- derived from the group $\mathbb{Z}$ the map $\varphi(x) = \psi(x) - t$, where $t = \psi(0)$, is an automorphism of $(\mathbb{Z},+)$. Thus $\psi(x) = x + t$ or $\psi(x) = -x + t$.

Let $\psi(x) = x + t$. Then $\psi(f(0,\ldots,0)) = l + t$ and $f(\psi(0),\ldots,\psi(0)) = nt + l$, which implies $l + t = l + nt$. Thus $t = 0$. Hence $\psi(x) = x$.

In the case $\psi(x) = -x + t$ we obtain $\psi(f(0,\ldots,0)) = -l + t$ and $f(\psi(0),\ldots,\psi(0)) = nt + l$. Thus $\frac{n-1}{2}\,(-t) = l$. If $l = 0$, then also $t = 0$. So, an $n$-ary group $(1,0)$-derived from the group $\mathbb{Z}$ has two automorphisms: $\psi(x) = x$ and $\psi(x) = -x$.

If $l = \frac{n-1}{2}$ (in this case $n$ must be odd), then $t = -1$. This means that an $n$-ary group $(1, \frac{n-1}{2})$-derived from the group $\mathbb{Z}$ has two automorphisms: $\psi(x) = x$ and $\psi(x) = -x - 1$.

For $0 < l < \frac{n-1}{2}$ no $t \in \mathbb{Z}$ such that $\frac{n-1}{2}(-t) = l$. So, in this case is only one automorphism: $\psi(x) = x$. □

**Corollary 6.10.** *For $0 < l < \frac{n-1}{2}$, an $n$-ary group $(1, l)$-derived from an infinite cyclic group has no non-trivial automorphisms.* □

**Corollary 6.11.** *An infinite cyclic $n$-ary group has no non-trivial automorphisms.*

*Proof.* Indeed, an infinite cyclic $n$-ary group is isomorphic to the $n$-ary group $(\mathbb{Z}, g_1)$, where $g_1$ is defined by (7). Hence, it is isomorphic to an $n$-ary group $(1, l)$-derived from the group $\mathbb{Z}$, which , by Corollary 6.10 has no non-trivial automorphisms. □

**Lemma 6.12.** *A non-commutative $n$-ary group $(\langle a\rangle, f)$ of infinite order has infinitely many automorphisms. All these automorphism have the form $a^s \to a^{s+t}$ or $a^s \to a^{-s+t}$, where $t$ is an arbitrary fixed integer.*

*Proof.* A non-commutative $n$-ary group $(\langle a\rangle, f)$ of infinite order exists only for odd $n$. Its operation is defined by (10).

By Theorem 6.1, any automorphism $\psi$ of such $n$-ary group induces on $\langle a\rangle$ an automorphism $\varphi(x) = \psi(x)a^{-t}$, where $a^t = \psi(a^0)$. Thus, $\psi(x) = \varphi(x)a^t$, i.e., $\psi(a^s) = a^{s+t}$ or $\psi(a^s) = a^{-s+t}$. □

**Theorem 6.13.** *The automorphism group of an infinite non-commutative precyclic $n$-ary group is isomorphic to the holomorph of the group $(\mathbb{Z}, +)$.*

*Proof.* Consider the holomorph $\mathbb{Z}^*\mathbb{Z}$ of the group $(\mathbb{Z}, +)$ with the group operation

$$w_1t_1 \cdot w_2t_2 = (w_1w_2)(w_2t_1 + t_2),$$

where $w_1, w_2 \in \mathbb{Z}^* = \{-1, 1\}$ (see for example [19]). Since any automorphism of an $n$-ary group $(-1, 0)$-derived from the infinite cyclic group $\langle a\rangle$ has the form $\psi_{w,t}(a^s) = a^{ws+t}$, where $w = \pm 1$, $t \in \mathbb{Z}$, (Lemma 6.12) the map $\tau : Aut(\langle a\rangle, f) \to \mathbb{Z}^*\mathbb{Z}$ defined by $\tau(\psi_{w,t}) = wt$ is a bijection.

Moreover, for all $\psi_{w_1,t_1}, \psi_{w_2,t_2} \in Aut(\langle a\rangle, f)$ and $a^s \in \langle a\rangle$ we have

$$\begin{aligned}\psi_{w_1,t_1} \circ \psi_{w_2,t_2}(a^s) &= \psi_{w_2,t_2}(\psi_{w_1,t_1}(a^s)) = \psi_{w_2,t_2}(a^{w_1s+t_1}) \\ &= a^{w_2(w_1s+t_1)+t_2} = a^{w_1w_2s+w_2t_1+t_2},\end{aligned}$$

which means that $\psi_{w_1,t_1} \circ \psi_{w_2,t_2} = \psi_{w_1w_2,w_2t_1+t_2}$.

Thus

$$\tau(\psi_{w_1,t_1} \circ \psi_{w_2,t_2}) = (w_1w_2)(w_2t_1 + t_2) = \tau(\psi_{w_1,t_1}) \cdot \tau(\psi_{w_2,t_2}).$$

Hence $Aut(\langle a\rangle, f) \cong \mathbb{Z}^*\mathbb{Z}$. □

## 7. Splitting automorphisms

In some $n$-ary groups $h(x) = \overline{x}$ is an automorphism satisfying for every $i = 1, 2, \ldots, n$ the identity

$$h((f(x_1, \ldots, x_n)) = f(x_1, \ldots, x_{i-1}, h(x_i), x_{i+1}, \ldots, x_n).$$

Such $n$-ary groups are called *distributive* (cf. [8] and [5]). Any distributive $n$-ary group is a set theoretic union of disjoint cyclic $n$-ary subgroups of the same order. But it is not precyclic, in general.

An endomorphism $\psi$ of an $n$-ary groupoid $(G, f)$ is called *splitting* (cf. [24]) if for every $i = 1, \ldots, n$ the identity

$$\psi(f(x_1, \ldots, x_n)) = f(x_1, \ldots, x_{i-1}, \psi(x_i), x_{i+1}, \ldots, x_n) \qquad (16)$$

is satisfied.

It is not difficult to see that the set of all splitting endomorphisms of a given $n$-ary groupoid $(G, f)$ forms a commutative semigroup. Moreover, for every splitting endomorphisms of $(G, f)$ holds $\psi^n = \psi$.

**Proposition 7.1.** *Any splitting endomorphism of an $n$-ary group is its automorphism.*

*Proof.* Let $\psi$ be a splitting endomorphism of an $n$-ary group $(G, f)$. If $\psi(x) = \psi(y)$ for some $x, y \in G$, then

$$f(\psi(x), x_2, x_3, \ldots, x_n) = f(\psi(y), x_2, x_3, \ldots, x_n)$$

for all $x_2, x_3, \ldots, x_n \in G$. This, by (16), gives

$$f(x, \psi(x_2), x_3, \ldots, x_n) = f(y, \psi(x_2), x_3, \ldots, x_n).$$

Hence $x = y$. So, $\psi$ is one-to-one.

Since $(G, f)$ is an $n$-ary group, for all $z, \psi(x_2), x_3, \ldots, x_n \in G$ there exists $y \in G$ such that $z = f(y, \psi(x_2), x_3, \ldots, x_n) = \psi(f(y, x_2, x_3, \ldots, x_n))$. Thus, for every $z \in G$ there exists $x = f(y, x_2, x_3, \ldots, x_n) \in G$ such that $z = \psi(x)$. So, $\psi$ is onto. Consequently it is an automorphism. □

**Corollary 7.2.** *$\psi^{n-1}=\mathrm{id}_G$ for any splitting automorphism $\psi$ of an $n$-ary group $(G,f)$.* □

**Proposition 7.3.** *A non-trivial splitting automorphism of an $n$-ary group has no fixed points.*

*Proof.* Indeed, if $\psi(a)=a$ for some $a\in G$, then, according to (2), for every $x\in G$ we obtain

$$\psi(x)=\psi(f(x,a,\ldots,a,\overline{a}))=f(x,\psi(a),a,\ldots,a,\overline{a})=f(x,a,\ldots,a,\overline{a})=x,$$

which means that $\psi$ is a trivial automorphism. □

**Corollary 7.4.** *An $n$-ary group with only one idempotent has no non-trivial splitting automorphisms.*

*Proof.* Indeed, if $a$ is an idempotent, then $\psi(a)$ also is an idempotent. Hence, in the case when $(G,f)$ has only one idempotent, we obtain $\psi(a)=a$. Thus $\psi$ is the identity mapping. □

**Theorem 7.5.** *The mapping $\psi:G\to G$ is a non-trivial splitting automorphism of an $n$-ary group $(G,f)$ $(\varphi,b)$-derived from a group $(G,\circ)$ with the identity $e$ if and only if $\psi(e)\neq e$ and*
*(i) $\psi(e)$ belongs to the center of $(G,\circ)$,*
*(ii) $\psi(x)=x\circ\psi(e)$ for every $x\in G$,*
*(iii) $\psi(e)=\varphi\psi(e)$,*
*(iv) $\underbrace{\psi(e)\circ\psi(e)\circ\ldots\circ\psi(e)}_{n-1}=e$.*

*Proof.* Let $(G,f)$ be an $n$-ary group $(\varphi,b)$-derived from a group $(G,\circ)$ with the identity $e$. Then, according to Theorem 2.2, $\varphi(b^{-1})=b^{-1}$. Moreover, since $\varphi^{n-1}(x)\circ b=b\circ x$ holds for all $x\in G$, the equation (4) can be written in more useful form

$$f(x_1,\ldots,x_n)=x_1\circ\varphi(x_2)\circ\varphi^2(x_3)\circ\varphi^3(x_4)\circ\ldots\circ\varphi^{n-2}(x_{n-1})\circ b\circ x_n. \quad (17)$$

Thus

$$\psi(x)=\psi(x\circ e)=\psi(f(x,b^{-1};e,\ldots,e))=f(x,b^{-1};e,\ldots,e,\psi(e))=x\circ\psi(e)$$

for every splitting automorphism $\psi$ of $(G,f)$ and every $x\in G$. This proves $(ii)$.

Similarly, using (17), we obtain

$$\psi(x)=\psi(e\circ x)=\psi(f(e,b^{-1},e,\ldots,e,x))=f(\psi(e),b^{-1},e,\ldots,e,x)=\psi(e)\circ x,$$

which together with the previous identity gives $x\circ\psi(e)=\psi(e)\circ x$. So, $\psi(e)$ belongs to the center of $(G,\circ)$.

Further, from $f(\psi(x),e,\ldots,e)=\psi(f(x,e,\ldots,e))=f(x,\psi(e),e,\ldots,e)$ and (17) we conclude (*iii*).

Now, using (17) and (*iii*) we obtain

$$\psi(b)=\psi(f(e,\ldots,e))=f(\psi(e),\ldots,\psi(e))=\psi(e)\circ\ldots\circ\psi(e)\circ b\circ\psi(e),$$

which together with (*ii*) implies (*iv*).

Hence, any splitting automorphism $\psi$ of $(G,f)$ satisfies (*i*), (*ii*), (*iii*) and (*iv*). By (*ii*), it is non-trivial if and only if $\psi(e)\neq e$.

The converse statement is obvious. □

**Corollary 7.6.** *A splitting automorphism of an $n$-ary group $(\varphi,b)$-derived from a group $(G,\circ)$ commutes with $\varphi$.*

*Proof.* By Theorem 7.5, for every $x\in G$ we have

$$\psi\varphi(x)=\varphi(x)\circ\psi(e)=\varphi(x)\circ\varphi\psi(e)=\varphi(x\circ\psi(e))=\varphi\psi(x). \qquad \square$$

**Corollary 7.7.** *An infinite precyclic an $n$-ary group has no non-trivial splitting endomorphisms.*

*Proof.* It follows from Theorem 7.5 (*iv*) and (*ii*) or Corollary 6.11. □

**Corollary 7.8.** *An $n$-ary group $(\varphi,b)$-derived from the centerless group has no non-trivial splitting endomorphisms.*

*Proof.* Indeed, in such $n$-ary group $\psi(e)=e$ for every splitting endomorphism $\psi$. This, by Proposition 7.3, means that $\psi$ is trivial. □

As a simple consequence of the above theorem we obtain the following characterization of skew splitting automorphisms firstly proved in [8].

**Theorem 7.9.** *The mapping $h(x)=\overline{x}$ is a splitting automorphism of an $n$-ary group $(G,f)$ if and only if on $G$ we can define a group $(G,\circ)$ with the identity $e$ and an automorphism $\varphi$ such that*

$$f(x_1,\ldots,x_n)=x_1\circ\varphi(x_2)\circ\varphi^2(x_3)\circ\ldots\circ\varphi^{n-2}(x_{n-1})\circ x_n\circ b,$$

*$\varphi(b)=b$, $b^{n-1}=e$, $x\circ\varphi(x)\circ\varphi^2(x)\circ\ldots\circ\varphi^{n-2}(x)=e$ and $\varphi^{n-1}(x)=x$ for all $x,x_1,\ldots,x_n\in G$ and some $b$ from the center of $(G,\circ)$.*

*Proof.* Directly from the definition of the skew element it follows that in an $n$-ary group $(\varphi, b)$-derived from a group $(G, \circ)$ we have $h(e) = \overline{e} = b^{-1}$. In this case also $\varphi(b) = b$ and $\varphi^{n-1}(x) \circ b = b \circ x$ (see Theorem 2.2).

If $h(x) = \overline{x}$ is a splitting automorphism, then, in view of Theorem 7.5, $b^{-1} = h(e)$ belongs to the center of $(G, \circ)$, $b^{n-1} = (h(e))^{n-1} = e$ and $h(x) = x \circ b^{-1}$. Hence also $b$ belongs to this center. Consequently $\varphi^{n-1}(x) = x$. From $f(x, \ldots, x, \overline{x}) = x$ it follows $x \circ \varphi(x) \circ \varphi^2(x) \circ \ldots \circ \varphi^{n-2}(x) = e$.

Conversely, from (17) it follows that in an $n$-ary group $(G, f)$ we have

$$\overline{x} \circ \varphi(x) \circ \varphi^2(x) \circ \ldots \circ \varphi^{n-2}(x) \circ b = e$$

for every $x \in G$. Hence $\overline{x} = b^{-1} \circ (\varphi(x) \circ \varphi^2(x) \circ \ldots \circ \varphi^{n-2}(x))^{-1}$. Thus in an $n$-ary group satisfying the conditions mentioned in this theorem holds $\overline{x} = b^{-1} \circ x = x \circ b^{-1}$. Therefore $\overline{e} = b^{-1}$ and $\overline{x} = x \circ \overline{e}$. This means that the mapping $h(x) = \overline{x}$ satisfies the conditions $(i)$ and $(ii)$ from Theorem 7.5. The last two conditions also are satisfied. Hence, $h(x) = \overline{x}$ is a splitting automorphism. □

**Corollary 7.10.** *An $n$-ary group containing at least one idempotent has no non-trivial splitting skew endomorphisms.* □

*Proof.* Suppose that an $n$-ary group $(G, f)$ has an idempotent $a$. If it has a splitting skew endomorphism, then, by Theorem 7.9, $a = f(a, \ldots, a) = a \circ b$. Thus $b = e$. Consequently, $f(x, \ldots, x) = e \cdot x \cdot e = x$ for every $x \in G$. Hence $(G, f)$ is an idempotent $n$-ary group. It has no non-trivial skew endomorphisms. □

**Corollary 7.11.** *A non-trivial splitting skew endomorphisms there are only in irreducible $n$-ary groups.* □

**Proposition 7.12.** *The mapping $\psi$ is a non-trivial splitting automorphism of an $n$-ary group $(m, l)$-derived from a cyclic group $\langle a \rangle$ of order $k$ if and only if $\psi(x) = xa^t$ for some $0 < t < k$ such that $t(m-1) \equiv t(n-1) \equiv 0 (\mathrm{mod}\, k)$.*

*Proof.* The proof is based on Theorem 7.5. From $(ii)$ it follows that any splitting automorphism of a precyclic $n$-ary group has the form $\psi(x) = xa^t$, where $a^t = \psi(e)$ and $t \neq 0$. Thus $0 < t < k$. From $(iii)$ we obtain $t(m-1) \equiv 0 (\mathrm{mod}\, k)$. In the same way, $(iv)$ implies $t(n-1) \equiv 0 (\mathrm{mod}\, k)$.

On the other hand, it is not difficult to see that $\psi(x) = xa^t$ with $t$ satisfying the above conditions is a non-trivial splitting automorphism. □

## References

[1] **V. D. Belousov**, *$n$-ary quasigroups*, (Russian), Ştiinţa, Kishinev 1972.

[2] **W. Dörnte**, *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Zeitschr. **29** (1928), 1 – 19.

[3] **I. M. Dudek and W. A. Dudek**, *On skew elements in $n$-groups*, Demonstratio Math. **14** (1981), 827 – 833.

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

[5] **W. A. Dudek**, *Autodistributive $n$-groups*, Commentationes Math. Annales Soc. Math. Polonae, Prace Matematyczne **23** (1983), 1 – 11.

[6] **W. A. Dudek**, *Medial $n$-groups and skew elements*, Proceedings of the V Universal Algebra Symposium "Universal and Applied Algebra", Turawa 1988, World Scientific, Singapore 1989, 55 – 80.

[7] **W. A. Dudek**, *On $n$-ary group with only one skew element*, Radovi Matematički (Sarajevo) **6** (1990), 171 – 175.

[8] **W. A. Dudek**, *On distributive $n$-ary groups*, Quasigroups and Related Systems **2** (1995), 132 – 151.

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

[10] **W. A. Dudek**, *On some old and new problems in $n$-ary groups* Quasigroups and Related Systems **8** (2001), 15 – 36.

[11] **W. A. Dudek**, *Remarks to Glazek's results on $n$-ary groups*, Discussiones Math., General Algebra Appl. **27** (2007), 199 – 233.

[12] **W. A. Dudek and K. Glazek**, *Around the Hosszú-Gluskin Theorem for $n$-ary groups*, Discrete Math. **308** (2008), 4861 – 4876.

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

[14] **W. A. Dudek, J. Michalski**, *On a generalization of Hosszú Theorem*, Demonstratio Math. **15** (1982), 783 – 805.

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

[16] **A. M. Gal'mak**, *An $n$-ary subgroup of identities*, (Russian), Vestsi Nats. Akad. Navuk Belarussi Ser. Fiz.-Mat. Navuk **2** (2003), 25 – 30.

[17] **K. Głazek and B. Gleichgewicht**, *Abelian $n$-groups*, Colloquia Math. Soc. J. Bolyai **29** "Universal Algebra", Esztergom (Hungary) 1977, 321 – 329 (North-Holland, Amsterdam 1982).

[18] **K. Głazek, J. Michalski and I. Sierocki**, *On evaluation of some polyadic groups*, Contributions to General Algebra **3** (1985), 157 – 171.

[19] **M. Hall, Jr.**, *The theory of groups*, Macmillan Co., New York, 1959.

[20] **M. Hosszú**, *On the explicit form of $n$-group operations*, Publ. Math. (Debrecen) **10** (1963), 88 – 92.

[21] **E. Kasner**, *An extension of the group concept*, Bull. Amer. Math. Soc. **10** (1904), 290 – 291.

[22] **R. Kerner**, *Ternary structures and $Z_3$-grading*, Generalized Symmetries in Physics, World Scientific, Singapore 1994, 375 – 394.

[23] **Y. Nambu**, *Generalized Hamiltonian mechanics*, Phys. Rev. D7 (1973), 2405 – 2412.

[24] **J. Plonka**, *On splitting-automorphisms of algebras*, Bull. Soc. Roy. Sci. Liége **42** (1973), 303 – 306.

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

[26] **N. A. Shchuchkin**, *An interconnection between $n$-groups and groups*, (Russian), Chebyshevskii Sb. **4** (2003), 125 – 141.

[27] **N. A. Shchuchkin**, *Skew endomorphisms on $n$-ary groups*, Quasigroups and Related Systems **14** (2006), 217 – 226.

[28] **N. A. Shchuchkin**, *The bijectivity of the skew mapping in $n$-ary groups*, (Russian), Trudy Inst. Mat., Minsk, **16** (2008), no.1, 106 – 112.

[29] **N. A. Shchuchkin**, *Subgroups of semicyclic $n$-ary groups*, (Russian), Fundam. Prikl. Mat. **15** (2009), 211 – 222.

[30] **N. A. Shchuchkin**, *Semicyclic $n$-ary groups*, (Russian), Izv. Gomel State Univ. **3(54)** (2009), 186 – 194.

[31] **F. M. Sokhatsky**, *On Dudek's problems on the skew operation in polyadic groups*, East Math. J. **19** (2003), 63 – 71.

[32] **E. I. Sokolov**, *On the Gluskin-Hosszú theorem for Dörnte $n$-groups*, (Russian), Mat. Issled. **39** (1976), 187 – 189.

[33] **L. Takhtajan**, *On foundation of the generalized Nambu mechanics*, Commun. Math. Phys. **160** (1994), 295 – 315.

Received September 19, 2009

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

N.A.Shchuchkin
Volgograd State Pedagogical University, Lenina prosp., 27, 400131 Volgograd, Russia
E-mail: shchuchkin@fizmat.vspu.ru

Quasigroups and Related Systems **17** (2009), 229 – 236

# Construction for subdirectly irreducible sloops of cardinality $\mathrm{n}2^{\mathrm{m}}$

*Enas M. A. E l-Zayat* and *Magdi H. Armanious*

**Abstract.** Guelzow [8] and similarly Armanious [1] [2] gave generalized doubling constructions to construct nilpotent subdirectly irreducible SQS-skeins and sloops. In [5] the authors have given recursive construction theorems as $n \to 2n$ for subdirectly irreducible sloops and SQS-skeins, these constructions supplies us with a subdirectly irreducible sloop of cardinality $2n$ satisfying that the cardinality of the congruence class of its monolith is equal to 2. In this article, we give a construction for subdirectly irreducible sloops of cardinality $n2^m$ having a monolith with a congruence class of cardinality $2^m$ for each integer $m \geqslant 2$. This construction supplies us with the fact that each sloop is isomorphic to the homomorphic image of the constructed subdirectly irreducible sloop over its monolith.

## 1. Introduction

A *Steiner triple system* is a pair $(L; B)$ where $L$ is a finite set and $B$ is a collection of 3-subsets called blocks of $L$ such that every 2-subset of $L$ is contained in exactly one block of $B$ (cf. [7]). Let $\mathbf{STS}(n)$ denote a Steiner triple system ( briefly a triple system ) of cardinality $n$. It is well known that an $\mathbf{STS}(n)$ exists iff $n \equiv 1$ or $3 \pmod 6$ (cf. [7] and [9]).

There is one to one correspondence between **STSs** and sloops (Steiner loops) (see [7] and [8]). A *sloop* $L = (L; \bullet, 1)$ is a groupoid with a neutral element 1 satisfying the identities:

$$x \bullet y = y \bullet x,$$
$$1 \bullet x = x,$$
$$x \bullet (x \bullet y) = y.$$

A sloop $L$ is called *Boolean sloop* if the binary operation satisfies in

2000 Mathematics Subject Classification: 05B07, 20N05
Keywords: Steiner loop, sloop, subdirectly irreducible sloop, Steiner triple system.

addition the associative law. Each Boolean sloop is a group that is also called a Boolean group.

Let $\mathbf{SL}(n)$ denote a sloop of cardinality $n$. Then $\mathbf{SL}(n)$ exists iff $n \equiv 2$ or $4 \pmod 6$ (cf. [7], [10]). If $\mathbf{SL}(n)$ is Boolean, then $n = 2^m$ for $m \geqslant 1$. Notice that for any $a$ and $b \in L$ the equation $a \bullet x = b$ has the unique solution $x = a \bullet (a \bullet x) = a \bullet b$; i.e., $L$ is a quasigroup [6].

A subsloop $N$ is called a *normal subsloop* of $L$ if and only if :

$$x \bullet (y \bullet N) = (x \bullet y) \bullet N \quad \text{for all} \quad x, y \in L.$$

Equivalently, a subsloop $N$ of $L$ is normal if and only if $N = [1]\theta$ for a congruence $\theta$ on $L$ (cf. [7], [10]).

In fact, there is an isomorphism between the lattice of normal subsloops and the congruence lattice of the sloop [10]. Quackenbush has also proved that the congruences of the sloops are permutable, regular and uniform. Moreover, he has shown that for any finite $\mathbf{SL}(n)$, a subsloop $N$ of cardinality $\frac{1}{2}n$ is normal.

Guelzow [8] and Armanious ([1], [2]) gave generalized doubling constructions for nilpotent subdirectly irreducible **SQS** -skeins and sloops of cardinality $2n$. In [5] the authors gave recursive construction theorems as $n \to 2n$ for subdiredtly irreducible sloops. All these constructions supplies us with subdirectly irreducible sloops having a monolith $\theta$ satisfying $|[x]\theta| = 2$ (the minimal possible order of a proper normal subsloop). Also in these constructions, the authors begin with a subdirectly irreducible $\mathbf{SL}(n)$ to construct a subdirectly irreducible $\mathbf{SL}(2n)$ satisfying that the cardinality of the congruence class of its monolith is equal 2. Armanious [3] has given another construction of a subdirectly irreducible $\mathbf{SL}(2n)$. He begins with a finite simple $\mathbf{SL}(n)$ to costruct a subdirectly irreducible $\mathbf{SL}(2n)$ having a monolith $\theta$ with $|[x]\theta| = n$ (the maximal possible order of a proper normal subsloop).

In this article, we begin with an arbitrary $\mathbf{SL}(n)$ for each possible value $n \geqslant 4$ to construct a subdirectly irreducible $\mathbf{SL}(n2^m)$ for each integer $m \geqslant 2$. This construction enables us to construct a subdirectly irreducible sloop having a monolith $\theta$ satisfying that the congruence class containing the identity is a Boolean $\mathbf{SL}(2^m)$. Moreover, its homomorphic image modulo $\theta$ is isomorphic to $L$.

In view of this result, we may construct several distinct examples of subdirectly irreducible sloops that cannot be able to consrtuct by the well known constructions (cf. [1], [2], [3], [5], [8]).

## 2. Construction of subdirectly irreducible sloops of cardinality $\mathbf{n2^m}$

Let $L = (L; *, 1)$ be an $\mathbf{SL}(n)$ and $B = (B; \bullet, 1)$ be a Boolean $\mathbf{SL}(2^m)$, where $L = \{1, x_1, x_2, \ldots, x_{n-1}\}$ and $B = \{1, a_1, a_2, \ldots, a_{2m-1}\}$. In this section we extend the sloop $L$ to a subdireclty irreducible sloop $L \times_\alpha B$ of cardinality $n2^m$ having $L$ as a homomorphic image.

We divide the set of elements of the direct product $L \times B$ into two subsets $\{1, x_1\} \times B$ and $\{x_2, \ldots, x_{n-1}\} \times B$. Consider the cyclic permutation $\alpha = (a_1 a_2 \ldots a_{2m-1})$ on the set $\{1, a_1, a_2, \ldots, a_{2m-1}\}$ and the characteristic function $\chi$ from the direct product $L \times B$ to $B$ defined as follows

$$\chi((x,a),(y,b)) = \begin{cases} a \bullet \alpha^{-1}(a) & \text{for } \ x = 1, y = x_1, \\ b \bullet \alpha^{-1}(b) & \text{for } \ x = x_1, y = 1, \\ c \bullet \alpha(c) & \text{for } \ x = x_1 = y \text{ and } a \bullet b = c, \\ 1 & \text{otherwise.} \end{cases}$$

The last term means that $\chi((x,a),(y,b)) = 1$ when $x = y = 1$, $(x,a) \notin \{1, x_1\} \times B$ or $(y,b) \notin \{1, x_1\} \times B$.

**Lemma 1.** *The characteristic function $\chi$ has the following properties:*

($i$) $\chi((x,a),(1,1)) = 1$;

($ii$) $\chi((x,a),(x,a)) = 1$;

($iii$) $\chi((x,a),(y,b)) = \chi((y,b),(x,a))$;

($iv$) $\chi((x,a),(x * y, a \bullet b \bullet \chi((x,a),(y,b)))) = \chi((x,a),(y,b))$.

*Proof.* To prove ($i$), let $x = x_1$. Then $\chi((x_1,a),(1,1)) = 1 \bullet \alpha^{-1}(1) = 1$. Otherwise if $x \neq x_1$, then $\chi((x,a),(1,1)) = 1$.

Also in ($ii$), if $x = x_1$, then $\chi((x_1,a),(x_1,a)) = a \bullet a \bullet \alpha(a \bullet a) = 1$. Otherwise, if $x \neq x_1$, then $\chi((x,a),(x,a)) = 1$.

According to the definition of $\chi$, we may deduce that $\chi((x,a),(y,b)) = \chi((y,b),(x,a))$ i.e., ($iii$) is also valid.

To prove the fourth property we consider four cases:

(1) If $x = x_1$ and $y = 1$, then

$$\begin{aligned} \chi((x_1,a),(x_1 * 1, a \bullet b \bullet \chi((x_1,a),(1,b)))) &= \chi((x_1,a),(x_1, a \bullet \alpha^{-1}(b)) \\ &= a \bullet a \bullet \alpha^{-1}(b)) \bullet \alpha(a \bullet a \bullet \alpha^{-1}(b)) \\ &= b \bullet \alpha^{-1}(b) = \chi((x_1,a),(1,b)). \end{aligned}$$

(2) If $x = 1$ and $y = x_1$, then

$$\begin{aligned} \chi((1,a),(1 * x_1, a \bullet b \bullet \chi((1,a),(x_1,b)))) &= \chi((1,a),(x_1, b \bullet \alpha^{-1}(a)) \\ &= a \bullet \alpha^{-1}(a) = \chi((1,a),(x_1,b)). \end{aligned}$$

(3) If $x = y = x_1$, then

$$\begin{aligned}\chi((x_1,a),(x_1*x_1,a\bullet b\bullet\chi((x_1,a),(x_1,b)))) &= \chi((x_1,a),(1,a\bullet b\bullet c\bullet\alpha(c))\\ &= \chi((x_1,a),(1,\alpha(c)) = c\bullet\alpha(c)\\ &= \chi((x_1,a),(x_1,b)) = 1.\end{aligned}$$

(4) Otherwise, when $x = y = 1$ or when $(x,a)$ or $(y,b) \notin \{1,x_1\}\times B$, we have $\chi((x,a),(y,b)) = \chi(x,a),(x*y,a\bullet b\bullet\chi((x,a),(y,b)))) = 1$, because $\{x, x*y\} \nsubseteq \{1,x_1\}$. This completes the proof of the lemma. □

**Lemma 2.** *Let $L = (L;*,1)$ be an arbitrary $\mathbf{SL}(n)$, and $B = (B;\bullet,1)$ be a Boolean $\mathbf{SL}(2^m)$ for $m \geqslant 2$. Also let $\circ$ be a binary operation on the set $L\times B$ defined by:*

$$(x,a)\circ(y,b) := (x*y, a\bullet b\bullet\chi((x,a),(y,b))).$$

*Then $L\times_a B = (L\times B;\circ,(1,1))$ is an $\mathbf{SL}(n2^m)$ for each possible number $n \geqslant 4$.*

*Proof.* Let $L = \{1,x_1,x_2,\dots,x_{n-1}\}$ and $B = \{1,a_1,a_2,\dots,a_{2m-1}\}$. We note that the operation $\circ$ is the same operation of the direct product $L\times B$ for all elements $(x,a),(y,b)$ of the set $\{x_2,x_3,\dots,x_{n-1}\}\times B$. The difference occurs only if $x,y\in\{1,x_1\}$.

For all $(x,a),(y,b)\in L\times B$, we have:

(1) According to Lemma 1 $(i)$

$$(x,a)\circ(1,1) = (x*1, a\bullet 1\bullet\chi((x,a),(1,1))) = (x,a).$$

(2) By using Lemma 1 $(ii)$

$$(x,a)\circ(x,a) = (x*x, a\bullet a\bullet\chi((x,a),(x,a))) = (1,1).$$

(3) Using Lemma 1 $(iii)$ we obtain:

$$\begin{aligned}(x,a)\circ(y,b) &= (x*y, a\bullet b\bullet\chi((x,a),(y,b)))\\ &= (y*x, b\bullet a\bullet\chi((y,b),(x,a)))\\ &= (y,b)\circ(x,a).\end{aligned}$$

(4) Lemma 1 $(iv)$ gives:

$$\begin{aligned}&(x,a)\circ((x,a)\circ(y,b)) = (x,a)\circ(x*y, a\bullet b\bullet\chi((x,a),(y,b)))\\ &= (y, a\bullet a\bullet b\bullet\chi((x,a),(y,b))\bullet\chi((x,a),(x*y,a\bullet b\bullet\chi((x,a),(y,b)))))\\ &= (y,b).\end{aligned}$$

(1), (2), (3) and (4) imply that $L\times_\alpha B = (L\times B;\circ,(1,1))$ is a sloop. □

We note that $((x,a_i))\circ(x_1,a_j)\circ(x_1,a_k)\neq(x,a_i)\circ((x_1,a_j)\circ(x_1,a_k))$, for any $x\notin\{1,x_1\}$ and $a_j\neq a_k$, i.e., the operation $\circ$ is not associative even if the operation $*$ is associative.

In the next theorem we prove that the constructed $L\times_\alpha B$ is a subdirectly irreducible sloop having a monolith $\theta_1$ satisfying that $|[(1,1)]\,\theta_1|=2^m$.

**Theorem 3.** *The constructed sloop* $L\times_\alpha B=(L\times B;\circ,(1,1))$ *is a subdirectly irreducible sloop.*

*Proof.* The projection $\Pi:(x,a)\to x$ from $L\times B$ into $L$ is an onto homomorphism and the congruence Ker $\Pi:=\theta_1$ on $L\times_\alpha B$ is given by

$$\theta_1=\cup_{i=0}^{n-1}\left\{(x_i,1),(x_i,a_1),\ldots,(x_i,a_{2m-1})\right\}^2,$$

where $x_0=1$; so one can directly see that

$$[(1,1)]\theta_1=\left\{(1,1),(1,a_1),\ldots,(1,a_{2m-1})\right\}.$$

Now $\mathbf{Con}(L)\cong\ \mathbf{Con}((L\times_\alpha B)/\theta_1)\cong[\theta_1:1]$. Our proof will now be complete if we show that $\theta_1$ is the unique atom of $\mathbf{Con}(L\times_\alpha B)$.

First, assume that $\theta_1$ is not an atom of $\mathbf{Con}(L\times_\alpha B)$. Then we can find an atom $\gamma$ such that $\gamma\subset\theta_1$ and $|[(1,1)]\,\gamma|=r<|[(1,1)]\,\theta_1|=2^m$. In this case we get a contradiction by proving that $[(1,1)]\,\gamma$ is not a normal subsloop of $L\times_\alpha B$.

Suppose that $[(1,1)]\gamma=\left\{(1,1),(1,a_{s_1}),(1,a_{s_2}),\ldots,(1,a_{s_{r-1}})\right\}$. We will prove that there are two elements $(x,a),(y,b)\in L\times B$ such that:

$$((x,a)\circ(y,b))\circ[(1,1)\gamma]\neq(x,a)\circ((y,b)\circ[(1,1)]\gamma).$$

If $\left\{a_{s_1},a_{s_2},\ldots,a_{s_{r-1}}\right\}$ is an increasing subsequence of $\left\{a_1,a_2,\ldots,a_{2m-1}\right\}$ and if $\alpha(a_{s_i})=a_{s_{i+1}}$ for all $i=1,2,\ldots,r-1$, then $\alpha(a_{s_{r-1}})=a_{s_r}\notin\left\{a_{s_1},a_{s_2},\ldots,a_{s_{r-1}}\right\}$. If $\left\{a_{s_1},a_{s_2},\ldots,a_{s_{r-1}}\right\}$ is increasing and not successive subsequence of $\left\{a_1,a_2,\ldots,a_{2m-1}\right\}$ then there exists an element $a_j\in\left\{a_{s_1},a_{s_2},\ldots,a_{s_{r-1}}\right\}$ such that $\alpha(a_j)=a_{j+1}\notin\left\{a_{s_1},a_{s_2},\ldots,a_{s_{r-1}}\right\}$. For both cases, we can always find an element $(1,a_k)\in[(1,1)]\,\gamma$ such that $(1,\alpha(a_k))\notin[(1,1)]\,\gamma$ ($a_k=a_{s_{r-1}}$ for the first case, and $a_k=a_j$ for the second case).

Consider the two elements $(x_1,a_1)$ and $(x_2,a_2)$ with $x_1\neq x_2\neq 1$, and assume that $((x_2,a_2)\circ(x_1,a_1))\circ[(1,1)]\,\gamma=(x_2,a_2)\circ((x_1,a_1)\circ[(1,1)]\,\gamma)$, then for the element $(1,a_k)$ (determined above) there exists an element $(1,a_{s_1})\in[(1,1)]\,\gamma$ such that

$$((x_2,a_2)\circ(x_1,a_1))\circ(1,a_k)=(x_2,a_2)\circ((x_1,a_1)\circ(1,a_{s_1})).$$

In this case $((x_2,a_2)\circ(x_1,a_1))\circ(1,a_k)=(x_2*x_1,a_2\bullet a_1)\circ(1,a_k)=(x_2*x_1,a_2\bullet a_1\bullet a_k)$ and $(x_2,a_2)\circ((x_1,a_1)\circ(1,a_{s_1}))=(x_2,a_2)\circ(x_1,a_1\bullet\alpha^{-1}(a_{s_1}))=(x_2*x_1,a_2\bullet a_1\bullet\alpha^{-1}(a_{s_1}))$ we obtain $a_k=\alpha^{-1}(a_{s_1})$, which implies $\alpha(a_k)=a_{s_t}$. This contradicts the assumption that $(1,\alpha(a_k))\notin[(1,1)]\gamma$. Hence, we may say that there is no atom $\gamma$ of $\mathbf{Con}(L\times_\alpha B)$ satisfying $\gamma\subset\theta_1$. Therefore, $\theta_1$ is an atom of the lattice $\mathbf{Con}(L\times_\alpha B)$.

Secondly, $\theta_1$ is the unique atom of $\mathbf{Con}(L\times_\alpha B)$. Indeed, if $\delta$ is another atom of $\mathbf{Con}(L\times_\alpha B)$, then $\theta_1\cap\delta=0$. Hence, one can easily see that there is only one element $(x,a_1)\in[(x,a_1)]\delta$ with the first component $x$ (note that $[(x,a_i)]\,\theta_1=\big\{(x,1),(x,a_1),\ldots,(x,a_i),\ldots,(x,a_{2m-1})\big\}$). For this reason we may say that the class $[(1,1)]\delta$ has at most one pair $(x_1,a_i)$ with first component $x_1$. So we have two possibilities: either

($i$) $[(1,1)]\delta$ contains only one pair $(x_1,a_i)$ with first component $x_1$, or

($ii$) $[(1,1)]\delta$ has no pairs with first component $x_1$.

For the first case, we choose two elements $(x,a)\&(x_1,a_s)\in L\times B$ such that $1\neq x\neq x_1$, and $a_s\neq a_i$ then

$$((x,a)\circ(x_1,a_s))\circ(x_1,a_i)=(x*x_1,a\bullet a_s)\circ(x_1,a_i)=(x,a\bullet a_s\bullet a_i).$$

Also,

$$(x,a)\circ((x_1,a_s)\circ(x_1,a_i))=(x,a)\circ(1,\alpha(a_s\bullet a_i))=(x,a\bullet\alpha(a_s\bullet a_i)).$$

Since the class $((x,a)\circ((x_1,a_s))\circ[(1,1)]\delta$ contains at most one element with a first component $x$, it follows that if $((x,a)\circ(x_1,a_s))\circ[(1,1)]\delta=(x,a)\circ((x_1,a_s)\circ[(1,1)]\delta)$, then $\alpha(a_s\bullet a_i)=a_s\bullet a_i$ hence $a_s\bullet a_i=1$, which contradicts the choice that $a_s\neq a_i$. This implies that $[(1,1)]\delta$ is not normal.

For the second case $[(1,1)]\delta$ has no pairs with first component $x_1$. Let $(x,a),(x,b)\in[(1,1)]\delta$ such that $1\neq x\neq x_1$, and $a\neq b$ Then

$$((x_1,c)\circ(x,a))\circ(x,b)=(x_1*x,c\bullet a)\circ(x,b)=(x_1,c\bullet a\bullet b).$$

Also,

$$(x_1,c)\circ((x,a)\circ(x,b))=(x_1,c)\circ(1,a\bullet b)=(x_1,c\bullet\alpha^{-1}(a\bullet b)).$$

By using the fact that the class $((x_1,c)\circ(x,a))\circ[(1,1)]\delta$ contains only one element with the first component $x_1$, we may say that if

$$((x_1,c)\circ(x,a))\circ[(1,1)]\delta=(x_1,c)\circ((x,a)\circ[(1,1)]\delta),$$

then $\alpha^{-1}(a \bullet b) = a \bullet b$, hence $a \bullet b = 1$, which contradicts that $a \neq b$. Thus $[(1,1)]\delta$ is not a normal subsloop of $L \times_\alpha B$. This mean that there is no another atom $\delta$, and $\theta_1$ is the unique atom of $\mathbf{Con}(L \times_\alpha B)$. Therefore, $L \times_\alpha B$ is a subdirectly irreducible sloop. □

Note that in the constructed sloop $L \times_\alpha B$, we may choose $B$ a Boolean $\mathbf{SL}(2^m)$ for each $m \geqslant 2$. Therefore, as a consequence of the proof of Theorem 3, the following holds.

**Corollary 4.** *Let $B$ be a Boolean $\mathbf{SL}(2^m)$ for an integer $m \geqslant 2$. Then the congruence class $[(1,1)]\theta_1$ of the monolith $\theta_1$ of the constucted subdirectly irreducible sloop $L \times_\alpha B$ is a Boolean $\mathbf{SL}(2^m)$.*

Also, Theorem 3 enable us to construct a subdirectly irreducible sloop $L \times_\alpha B$ having a monolith $\theta_1$ satisfying that $(L \times_\alpha B)/\ \theta_1 \cong L$. Then we have the following result.

**Corollary 5**. *Every sloop $L$ is isomorphic to the homomorphic image of the subdirectly irreducible sloop $L \times_\alpha B$ over its monolith, for each Boolean sloop $B$.*

In view of these results, we may construct several distinct examples of subdirectly irreducible sloops.

The smallest non-trivial application of our construction is of cardinality 16. Indeed, if we choose two $\mathbf{SL}(4)$s, $L = (\{1, x_1, x_2, x_3\}; *, 1)$ and $B = (\{1, a, b, c\}; \bullet, 1)$, then the constructed sloop $L \times_\alpha B$ is a subdirectly irreducible $\mathbf{SL}(16)$ having 3 normal sub-$\mathbf{SL}(8)$s:

$$\mathbf{S}_1 = \{(1,1),(1,a),(1,b),(1,c),(x_1,1),(x_1,a),(x_1,b),(x_1,c)\}\,,$$

$$\mathbf{S}_2 = \{(1,1),(1,a),(1,b),(1,c),(x_2,1),(x_2,a),(x_2,b),(x_2,c)\} \text{ and}$$

$$\mathbf{S}_3 = \{(1,1),(1,a),(1,b),(1,c),(x_3,1),(x_3,a),(x_3,b),(x_3,c)\}\,.$$

The constructed $\mathbf{SL}(16)$ corresponds to an $\mathbf{STS}(15)$ having 3 sub-$\mathbf{STS}(7)$s.

In the classification of all subdirectly irreducible $\mathbf{SL}(32)$ given in [5] there are two classes having a monolith $\theta_1$ satisfying $|[(1,1)]\theta_1| = 4$ and 8. The well-known constructions for subdirectly irreducible sloops given in [1], [2], [3], [5], [8] dose not enable us to construct examples for these classes.

In the following example we apply our construction to describe subdirectly irreducible $\mathbf{SL}(32)$ having a monolith $\theta_1$ satisfying $|[(1,1)]\theta_1| = 4$ (or 8).

**Example.** Let $L$ be the Boolean $\mathbf{SL}(8)$ (or $\mathbf{SL}(4)$), $B$ be the Boolean $\mathbf{SL}(4)$ (or $\mathbf{SL}(8)$) and $\alpha$ be the cyclic permutation on the non-unit elements of $B$. By apply our construction $L \times_\alpha B$, we get a subdirectly irreducible $\mathbf{SL}(32)$ having a monolith $\theta_1$ satisfying $(L \times_\alpha B)/\theta_1 \cong L \cong \mathbf{SL}(8)$ (or $\mathbf{SL}(4)$) in which its monolith $\theta_1$ satisfying $|[(1,1)]\theta_1| = 4$ (or 8).

This example of an $\mathbf{SL}(32)$ corresponds to a subdirectly irreducible $\mathbf{SL}(32)$ having exactly 7 normal sub-$\mathbf{SL}(16)$s. (or 3 normal sub-$\mathbf{SL}(16)$s).

Similarly, we can use our construction to give an example for a subdirectly irreducible $\mathbf{SL}(n\mathbf{2}^m)$ having a monolith $\theta_1$ satisfying $|[(1,1)]\theta_1| = 2^m$ for each possible $n \geqslant 4$ and each integer $m \geqslant 2$.

# References

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

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

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

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

[5] **M. H. Armanious and E. M. Elzayat**, *Subdirectly irreducible sloops and SQS-skeins*, Quasigroups and Reelated Systems **15** (2007), 233 – 250.

[6] **O. Chein, H. O. Pflugfelder, and J. D. H. Smith**, *Quasigroups and loops*, Theory and Applications, Sigma Series in Pure Math., Heldermann Verlag, Berlin, 1990.

[7] **B. Ganter and H. Werner**, *Co-ordinatizing Steiner systems*, Ann. Discrete Math. **7** (1980), 3 – 24.

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

[9] **C. C. Lindner and A. Rosa**, *Steiner quadruple system*, Discrete Math. **21** (1978), 147 – 181.

[10] **R. W. Quackenbush**, *Varieties of Steiner loops and Steiner quasigroups*, Canada J. Math. **28** (1976), 11087 – 11098.

Received July 4, 2009

Department of Mathematics, Faculty of Science, Mansoura University, Mansoura, Egypt
E-mail: enaselzyat@yahoo.com

# $\mathcal{N}$-fuzzy quasi-ideals in ordered semigroups

*Asghar Khan, Young Bae Jun and Muhammad Shabir*

**Abstract.** In this paper, we introduce the concept of $\mathcal{N}$-fuzzy quasi-ideals in ordered semigroups and investigate the basic theorem of quasi-ideals of ordered semigroups in terms of $\mathcal{N}$-fuzzy quasi-ideals. We characterize left (resp. right) regular and completely regular ordered semigroups in terms of $\mathcal{N}$-fuzzy quasi-ideals. We define semiprime $\mathcal{N}$-fuzzy quasi-ideals and characterize completely regular ordered semigroups in terms of semiprime $\mathcal{N}$-fuzzy quasi-ideals. We provide characterizations of some semilattices of left and right simple semigroups in terms of $\mathcal{N}$-fuzzy quasi-ideals.

## 1. Introduction

A fuzzy subset $f$ of a given set $S$ is described, as an arbitrary function $f : S \longrightarrow [0,1]$, where $[0,1]$ is the usual closed interval of real numbers. This fundamental concept of a fuzzy set was first introduced by Zadeh in his pioneering paper [26] of 1965, provides a natural frame-work for the generalizations of some basic notions of algebra, e.g. logic, set theory, group theory, ring theory, groupoids, real analysis, topology, and differential equations etc. Rosenfeld (see [21]) was the first who considered the case when $S$ is a groupoid. He gave the definition of a fuzzy subgroupoid and the fuzzy left (right, two-sided) ideals of $S$ and justified these definitions by showing that a subset $A$ of a groupoid $S$ is is a subgroupoid or left (right, or two-sided) ideal of $S$ if and only if the characteristic mapping $f_A : S \longrightarrow \{0,1\}$ of $A$ defined by

$$x \longmapsto f_A(x) := \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A, \end{cases}$$

is respectively, a fuzzy subgroupoid or a fuzzy left (right or two-sided) ideal of $S$. The concept of a fuzzy ideal in semigroups was first developed by

2000 Mathematics Subject Classification: 06F05, 06D72, 08A72

Keywords: $\mathcal{N}$-fuzzy subset; $\mathcal{N}$-fuzzy quasi-ideal; left (right regular), semilattice of left (right) simple semigroups; completely regular ordered semigroup.

Kuroki (see [13-17]). He studied fuzzy ideals, fuzzy bi-ideals, fuzzy quasi-ideals and semiprime fuzzy ideals of semigroups. Fuzzy ideals and Green's relations in semigroups were studied by McLean and Kummer in [18]. Ahsan et. al in [1] characterized semigroups in terms of fuzzy quasi-ideals. A systematic exposition of fuzzy semigroups was given by Mordeson, Malik and Kuroki appeared in [20], where one can find theoretical results on fuzzy semigroups and theoretical results on fuzzy semigroups and their use in fuzzy coding, fuzzy finite state machines and fuzzy languages. The monograph given by Mordeson and Malik [19] deals with the applications of fuzzy approach to the concepts of automata and formal languages. Fuzzy sets in ordered semigroups/ordered groupoids were first introduced by Kehayopulu and Tsingelis in [8]. They also introduced the concepts of fuzzy bi-ideals and fuzzy quasi-ideals in ordered semigroups in (see [9]).

The quasi-ideals in rings and semigroups were studied by Stienfeld in [25] and Kehayopulu extended this concept in ordered semigroups and defined a quasi-ideal of an ordered semigroup $S$ as a non-empty subset $Q$ of $S$ such that

$$(1)\ (QS]\cap(SQ]\subseteq Q \quad\text{and}\quad (2)\ \text{If } a\in Q \text{ and } S\ni b\leqslant a \text{ then } b\in Q.$$

The purpose of this paper, is to initiate and study the new sort of fuzzy quasi-ideals called $\mathcal{N}$-fuzzy quasi-ideals in ordered semigroups. We characterize regular, left and right simple ordered semigroups and completely regular ordered semigroups in terms of $\mathcal{N}$-fuzzy quasi-ideals. In this respect, we prove that: An ordered semigroup $S$ is regular, left and right simple if and only if every $\mathcal{N}$-fuzzy quasi-ideal of $S$ is a constant $\mathcal{N}$-function. We also prove that $S$ is completely regular if and only if for every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$ we have $f(a)=f(a^2)$ for every $a\in S$. We define semiprime $\mathcal{N}$-fuzzy quasi-ideal in ordered semigroups and prove that an ordered semigroup $S$ is completely regular if and only if every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$ is semiprime. Next, we characterize semilattices of left and right simple ordered semigroup in terms of $\mathcal{N}$-fuzzy quasi-ideals. We prove that an ordered semigroup $S$ is a semilattice of left and right simple if and only if for every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$, we have $f(a)=f(a^2)$ and $f(ab)=f(ba)$ for every $a,b\in S$. In the last of this paper, we discuss ordered semigroups having the property $a\leqslant a^2$ for all $a\in S$ and prove that an ordered semigroup $S$ (having the property $a\leqslant a^2$ for all $a\in S$) is a semilattice of left and right simple ordered semigroup if and only if for every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$ we have $f(ab)=f(ba)$ for all $a,b\in S$.

## 2. Some basic definitions and results

By an *ordered semigroup* (or *po-semigroup*) we mean a *structure* $(S,\cdot,\leqslant)$ in which

$(OS1)$ $(S,\cdot)$ is a *semigroup*,

$(OS2)$ $(S,\leqslant)$ is a *poset*,

$(OS3)$ $(\forall a,b,x \in S)(a \leqslant b \Longrightarrow ax \leqslant bx$ and $xa \leqslant xb)$.

Let $(S,\cdot,\leqslant)$ be an ordered semigroup. For $A \subseteq S$, we denote

$$(A] := \{t \in S \,|\, t \leqslant h \text{ for some } h \in A\} \quad\text{and}\quad AB := \{ab \,|\, a \in A, b \in B\}.$$

A non-empty subset $Q$ of $S$ is called a *quasi-ideal* (see [8]) of $S$ if:

(1) $(QS] \cap (SQ] \subseteq Q$ and (2) If $a \in Q$ and $S \ni b \leqslant a$ then $b \in Q$.

Let $A,B \subseteq S$. Then $A \subseteq (A]$, $(A](B] \subseteq (AB]$, $((A]] = (A]$ and $((A](B]] \subseteq (AB]$ (see [8]).

$\emptyset = A \subseteq S$ is called a *subsemigroup* of $S$ if $A^2 \subseteq A$, and a *right* (resp. *left*) *ideal* of $S$ if (1) $AS \subseteq A$ (resp. $SA \subseteq A$) and (2) $a \in A$, $S \ni b \leqslant a$ imply $b \in A$. If $A$ is both a right and a left ideal of $S$, then it is called an *ideal*. A subsemigroup $B$ of $S$ is called a *bi-ideal* of $S$ if: (1) $BSB \subseteq B$ and (2) $a \in B$, $S \ni b \leqslant a$ imply $b \in B$.

By a *negative fuzzy subset* (briefly, an *$\mathcal{N}$-fuzzy subset*) of $S$ we mean a *function* $f : S \longrightarrow [-1,0]$. An $\mathcal{N}$-fuzzy subset $f$ of $S$ is called an *$\mathcal{N}$-fuzzy left* (resp. *right*) *ideal* of $S$ if:

(1) $x \leqslant y \Longrightarrow f(x) \leqslant f(y)$ and (2) $f(xy) \leqslant f(y)$ (resp. $f(xy) \leqslant f(x)$) for all $x,y \in S$.

If $f$ is both an $\mathcal{N}$-fuzzy left and an $\mathcal{N}$-fuzzy right ideal of $S$. Then it is called an *$\mathcal{N}$-fuzzy ideal* of $S$.

For a non-empty *family* of $\mathcal{N}$-fuzzy subsets $\{f_i\}_{i\in I}$, of an ordered semigroup $S$, the $\mathcal{N}$-fuzzy subsets $\bigwedge\limits_{i\in I} f_i$ and $\bigvee\limits_{i\in I} f_i$ of $S$ are defined as follows:

$$\Big(\bigwedge_{i\in I} f_i\Big)(x) := \inf\nolimits_{i\in I}\{f_i(x)\}, \qquad \Big(\bigvee_{i\in I} f_i\Big)(x) := \sup\nolimits_{i\in I}\{f_i(x)\}.$$

The *characterisitic $\mathcal{N}$-function* $\kappa_A$ of $\emptyset \neq A \subseteq S$ is given by:

$$\kappa_A(x) := \begin{cases} -1 \text{ if } x \in A, \\ \ \ 0 \text{ if } x \notin A. \end{cases}$$

For $\mathcal{N}$-fuzzy subsets $f$ and $g$ of $S$ we define the N-composition $fNg$ by

$$fNg(x) := \begin{cases} \bigwedge\limits_{(y,z)\in A_x} \max\{f(y),g(z)\} & \text{if } A_x \neq \emptyset, \\ 0 & \text{if } A_x = \emptyset, \end{cases}$$

where

$$A_x := \{(y,z) \in S \times S \mid x \leqslant yz\}.$$

The set $NF(S)$ of all $\mathcal{N}$-fuzzy subsets of $S$with such defined N-composition and the relation

$$f \preceq g \text{ if and only if } f(x) \leqslant g(x) \text{ for all } x \in S$$

is an ordered semigroup denoted by $(NF(S), N, \preceq)$. The fuzzy subsets $\beta(x) = 0$ and $\alpha(x) = -1$ (for all $x \in S$) the *greatest* and *least element* of $(NF(S), \preceq)$. The fuzzy subset $\beta$ is the *zero element* of $(NF(S), N, \preceq)$ (that is, $fN\beta = \beta Nf = \beta$ and $f \preceq \beta$ for every $f \in NF(S)$). Obviously, $f_S = \alpha$ and $f_\emptyset = \beta$.

**Definition 2.1**. (cf. [11]). Let $S$ be an ordered semigroup. An $\mathcal{N}$-fuzzy subset $f$ of $S$ is called an *$\mathcal{N}$-fuzzy subsemigroup* of $S$ if

$$f(xy) \leqslant \max\{f(x), f(y)\} \text{ for all } x, y \in S.$$

**Definition 2.2.** (cf. [11]). Let $S$ be an ordered semigroup. An $\mathcal{N}$-fuzzy subsemigroup $f$ of $S$ is called an *$\mathcal{N}$-fuzzy bi-ideal* of $S$ if:

(1) $x \leqslant y$ implies $f(x) \leqslant f(y)$.

(2) $f(xay) \leqslant$max$\{f(x), f(y)\}$ for all $x, a, y \in S$.

**Proposition 2.3.** (cf. [11]). *Let $S$ be an ordered semigroup and $A, B \subseteq S$. Then*

$(a)$ *$B \subseteq A$ if and only if $\kappa_B \preceq \kappa_A$.*

$(b)$ *$\kappa_A \vee \kappa_B = \kappa_{A\cap B}$.*

$(c)$ *$\kappa_A N \kappa_B = \kappa_{(AB]}$.*

**Lemma 2.4.** (cf. [22]). *Let $S$ be an ordered semigroup. Then every quasi-ideal of $S$ is subsemigroup of $S$.*

**Lemma 2.5.** (cf. [24]). *An ordered semigroup $(S, \cdot, \leqslant)$ is a semilattice of left and right simple semigroups if and only if for all quasi-ideals $A, B$ of $S$, we have*

$$(A^2] = A \text{ and } (AB] = (BA].$$

An ordered semigroup $S$ is called *regular* (see [5]) if for every $a \in S$ there exists $x \in S$ such that $a \leqslant axa$ or equivalently, (1) $(\forall a \in S)(a \in (aSa])$ and (2) $(\forall A \subseteq S)(A \subseteq (ASA])$.

An ordered semigroup $S$ is called *left* (resp. *right*) *simple* (see [9]) if for every left (resp. right) ideal $A$ of $S$, we have $A = S$.

**Lemma 2.6.** (cf. [9, Lemma 3]). *An ordered semigroup $S$ is left (resp. right) simple if and only if $(Sa] = S$ (resp. $(aS] = S$) for every $a \in S$.*

An ordered semigroup $S$ is called *left* (resp. *right) regular* (see [4]) if for every $a \in S$ there exists $x \in S$ such that $a \leqslant xa^2$ (resp. $a \leqslant a^2x$) or equivalently, (1) $(\forall a \in S)(a \in (Sa^2])$ and (2) $(\forall A \subseteq S)(A \subseteq (SA^2])$. An ordered semigroup $S$ is called *completely regular* if it is regular, left regular and right regular [6].

If $S$ is an ordered semigroup and $\emptyset \neq A \subseteq S$, then the set $(A \cup (AS \cap SA)]$ is the quasi-ideal of $S$ generated by $A$. If $A = \{x\}$ $(x \in S)$, we write $(x \cup (xS \cap Sx)]$ instead of $(\{x\} \cup (\{x\}S \cap S\{x\})]$.

**Lemma 2.7.** (cf. [6]). *An ordered semigroup $S$ is completely regular if and only if $A \subseteq (A^2SA^2]$ for every $A \subseteq S$. Equivalently, if $a \in (a^2Sa^2]$ for every $a \in S$.*

**Lemma 2.8.** (cf. [24]). *An ordered semigroup $(S, \cdot, \leqslant)$ is a semilattice of left and right simple semigroups if and only if for every right ideal $A$ and every left ideal $B$ of $S$, we have $A \cap B = (AB]$.*

**Lemma 2.9**. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup and let $A, B$ be quasi-ideals of $S$. Then $(AB]$ is a bi-ideal of $S$.*

## 3. $\mathcal{N}$-fuzzy quasi-ideals

In this section we prove the basic theorem which characterizes ordered semigroup in terms of $\mathcal{N}$-fuzzy quasi-ideals.

**Definition 3.1**. Let $(S, \cdot, \leqslant)$ be an ordered semigroup. An $\mathcal{N}$-fuzzy subset $f$ of $S$ is called a *$\mathcal{N}$-fuzzy quasi-ideal* of $S$ if

(1) $(fN\alpha) \vee (\alpha N f) \succeq f$.

(2) $x \leqslant y$, then $f(x) \leqslant f(y)$ for all $x, y \in S$.

The set

$$L(f;t) := \{x \in S | f(x) \leqslant t\}$$

is called a *level subset* of $f$.

**Theorem 3.2.** (cf. [11]). *Let $S$ be an ordered semigroup and $f$ an $\mathcal{N}$-fuzzy subset of $S$. Then $\forall t \in [-1, 0)$, $L(f;t)(\neq \emptyset)$ is a bi-ideal if and only if $f$ is an $\mathcal{N}$-fuzzy bi-ideal.*

**Theorem 3.3**. *Let $(S, \cdot, \leqslant)$ be an ordered semigroups and $\emptyset \neq A \subseteq S$. Then $A$ is a quasi-ideal of $S$ if and only if the characteristic $\mathcal{N}$-function $\kappa_A$ of $A$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$.*

*Proof.* Suppose that $A$ is a quasi-ideal of $S$. Then $(\kappa_A N\alpha)\vee(\alpha N\kappa_A)\succeq\kappa_A$. Indeed:

$$(\kappa_A N\alpha)\vee(\alpha N\kappa_A)=(\kappa_A N\kappa_S)\vee(\kappa_S N\kappa_A)=\kappa_{(AS]}\vee\kappa_{(SA]}=\kappa_{(AS]\cap(SA]}$$

by Proposition 2.3.

Since $(AS]\cap(SA]\subseteq A$, then by Proposition 2.3, we have $\kappa_{(AS]\cap(SA]}\succeq\kappa_A$. Thus $(\kappa_A N\alpha)\vee(\alpha N\kappa_A)\succeq\kappa_A$. Let $x,y\in S$ be such that $x\leqslant y$. If $\kappa_A(y)=0$. Then $\kappa_A(x)\leqslant\kappa_A(y)$, because $\kappa_A(x)\leqslant 0\ \forall x\in S$. If $\kappa_A(y)=-1$, then $y\in A$. Since $S\ni x\leqslant y\in A$, we have $x\in A$, then $\kappa_A(x)=-1$ and hence $\kappa_A(x)\leqslant\kappa_A(y)$.

Conversely, assume that $\kappa_A$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$. Then $A$ is a quasi-ideal of $S$ since $(\kappa_A N\alpha)\vee(\alpha N\kappa_A)\succeq\kappa_A$ implies $(\kappa_A N\kappa_S)\vee(\kappa_S N\kappa_A)\succeq\kappa_A$. By Proposition 2.3, $\kappa_S N\kappa_A=\kappa_{(SA]}$ and $\kappa_A N\kappa_S=\kappa_{(AS]}$, then $\kappa_{(AS]}\vee\kappa_{(SA]}=\kappa_{(AS]\cap(SA]}$ and we have $\kappa_{(AS]\cap(SA]}\succeq\kappa_A$. Thus $(AS]\cap(SA]\subseteq A$.

If $x\in A$ and $S\ni y\leqslant x$. Since $y\leqslant x$ and $\kappa_A$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$, we have $\kappa_A(y)\leqslant\kappa_A(x)$. Since $x\in A$ then $\kappa_A(x)=-1$, and hence $\kappa_A(y)=-1$, i.e., $y\in A$. □

**Theorem 3.4.** *Let $S$ be an ordered semigroup and $f$ an $\mathcal{N}$-fuzzy subset of $S$. Then $\forall t\in[-1,0)$, $L(f;t)(\neq\emptyset)$ is a quasi-ideal if and only if $f$ is an $\mathcal{N}$-fuzzy quasi-ideal.*

*Proof.* Assume that $f$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$. Let $x,y\in S$ be such that $x\leqslant y$. If $y\in L(f;t)$, then $f(y)\leqslant t$. Since $x\leqslant y$ and $f(x)\leqslant f(y)\leqslant t$ then $x\in L(f;t)$. Let $a\in S$ be such that $a\in(L(f;t)S]\cap(SL(f;t)]$ then $a\in(L(f;t)S]$ and $a\in(SL(f;t)]$. Then $a\leqslant xy$ and $a\leqslant x'y'$ for some $x,y'\in L(f;t)$ and $x',y\in S$ and so $(x,y)\in A_a$ and $(x',y')\in A_a$. Since $A_a\neq\emptyset$, we have

$$\begin{aligned}f(a)&\leqslant((fN\alpha)\vee(\alpha Nf))(a)=\max\left[(fN\alpha)(a),(\alpha Nf)(a)\right]\\&=\max\Big[\bigwedge_{(p,q)\in A_a}\max\{f(p),\alpha(q)\},\quad\bigwedge_{(p',q')\in A_a}\max\{\alpha(p'),f(q')\}\Big]\\&\leqslant\max\Big[\max\{f(a),\alpha(b)\},\max\{\alpha(a'),f(b')\}\Big]\\&=\max\Big[\max\{f(x),-1\},\max\{-1,f(y')\}\Big]=\max\Big[f(x),f(y')\Big].\end{aligned}$$

Since $x,y'\in L(f;t)$ we have $f(x)\leqslant t$ and $f(y')\leqslant t$. Then

$$f(a)\leqslant\max\Big[f(x),f(y')\Big]\leqslant t,$$

so $a \in L(f;t)$. Thus $(L(f;t)S] \cap (SL(f;t)] \subseteq L(f;t)$.

Conversely. Assume that for all $t \in [-1,0], L(f;t) \neq \emptyset$ is a quasi-ideal of $S$. Let $x, y \in S$ be such that $x \leqslant y$. If $f(x) > f(y)$, then $\exists t \in [-1,0]$ such that $f(x) > t \geqslant f(y)$ then $y \in L(f;t)$ but $x \notin L(f;t)$. This is a contradiction. Thus $f(x) \leqslant f(y)$ for all $x \leqslant y$.

Let $x \in S$ be such that $f(x) > ((fN\alpha) \vee (\alpha Nf))(x)$, then $\exists t \in [-1,0]$ such that $f(x) > t \geqslant ((fN\alpha) \vee (\alpha Nf))(x) = \max[(fN\alpha)(x), (\alpha Nf)(x)]$.

Then $(fN\alpha)(x) \leqslant t$ and $(\alpha Nf)(x) \leqslant t$ and hence $x \in (L(f;t)S]$ and $x \in (SL(f;t)]$, so $x \in (L(f;t)S] \cap (SL(f;t)]$. But $(L(f;t)S] \cap (SL(f;t)] \subseteq L(f;t)$, hence $x \in L(f;t)$, i.e., $f(x) \leqslant t$. This is a contradiction. Thus $f(x) \leqslant ((fN\alpha) \vee (\alpha Nf))(x)$. □

**Example 3.5.** Let $S = \{a, b, c, d, f\}$ be an ordered semigroup with the following multiplication

| $\cdot$ | $a$ | $b$ | $c$ | $d$ | $f$ |
|---|---|---|---|---|---|
| $a$ | $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ | $a$ | $d$ | $a$ |
| $c$ | $a$ | $f$ | $c$ | $c$ | $f$ |
| $d$ | $a$ | $b$ | $d$ | $d$ | $b$ |
| $f$ | $a$ | $f$ | $a$ | $c$ | $a$ |

and let $\leqslant := \{(a,a), (a,b), (a,c), (a,d), (a,f), (b,b), (c,c), (d,d), (f,f)\}$.

The quasi-ideals of $S$ are: $\{a\}$, $\{a,b\}$, $\{a,c\}$, $\{a,d\}$, $\{a,f\}$, $\{a,b,d\}$, $\{a,c,d\}$, $\{a,b,f\}$, $\{a,c,f\}$ and $S$ (see [5]). Define $f : S \longrightarrow [-1,0]$ by $f(a) = -0.8$, $f(b) = -0.6$, $f(d) = -0.5$, $f(c) = f(f) = -0.3$. Then

$$L(f;t) := \begin{cases} S & \text{if} \quad t \in [-0.3, 0], \\ \{a,b,d\} & \text{if} \quad t \in [-0.5, -0.3), \\ \{a,b\} & \text{if} \quad t \in [-0.6, -0.5), \\ \{a\} & \text{if} \quad t \in [-0.8, -0.6), \\ \emptyset & \text{if} \quad t \in [-1, -0.8). \end{cases}$$

is a quasi-ideal and by Theorem 3.4, $f$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$.

**Lemma 3.6**. *Every $\mathcal{N}$-fuzzy quasi-ideal is an $\mathcal{N}$-fuzzy bi-ideal.*

*Proof.* . Let $x, y, z \in S$. Then $xyz = x(yz) = (xy)z$ and $(x, yz) \in A_{xyz}$ and $(xy, z) \in A_{xyz}$. Since $A_{xyz} \neq \emptyset$ then

$$\begin{aligned} f(xyz) &\leqslant [(fN\alpha) \vee (\alpha Nf)]\,(xyz) \\ &= \max\Big[ \bigwedge_{(p,q)\in A_{xyz}} \max\{f(p), \alpha(q)\}, \quad \bigwedge_{(p_1,q_1)\in A_{xyz}} \max\{\alpha(p_1), f(q_1)\}\Big] \end{aligned}$$

$$\begin{aligned}&\leqslant \max[\max\{f(x),\alpha(yz)\},\max\{\alpha(xy),f(z)\}]\\&=\max[\max\{f(x),-1\},\max\{-1,f(z)\}]=\max[f(x),f(z)].\end{aligned}$$

If $x, y \in S$, then $xy = x(y)$ and hence $(x, y) \in A_{xy}$. Since $A_{xy} \neq \emptyset$, we have

$$\begin{aligned}f(xy) &\leqslant [(fN\alpha)\vee(\alpha Nf)](xy)\\&=\max\Big[\bigwedge_{(p,q)\in A_{xy}}\max\{f(p),\alpha(q)\},\quad \bigwedge_{(p,q)\in A_{xy}}\max\{\alpha(p),f(q)\}\Big]\\&\leqslant \max[\max\{f(x),\alpha(y)\},\max\{\alpha(x),f(y)\}]\\&=\max[\max\{f(x),-1\},\max\{-1,f(y)\}]=\max[f(x),f(y)].\end{aligned}$$

Let $x, y \in S$ be such that $x \leqslant y$. Then $f(x) \leqslant f(y)$, because $f$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$. Thus $f$ is an $\mathcal{N}$-fuzzy bi-ideal of $S$. □

The converse of above Lemma is not true, in general.

**Example 3.7.** Consider the semigroup $S = \{a, b, c, d\}$

| $\cdot$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $a$ | $a$ | $a$ |
| $c$ | $a$ | $a$ | $b$ | $a$ |
| $d$ | $a$ | $a$ | $b$ | $b$ |

with the order $\leqslant := \{(a, a), (b, b), (c, c), (d, d), (a, b)\}$.

Then $\{a, d\}$ is a bi-ideal but not a quasi-ideal of $S$. For an $\mathcal{N}$-fuzzy set $f$ defined by $f(a) = f(d) = -0.3$, $f(b) = f(c) = -0.7$ we have

$$L(f;t) := \begin{cases} S & \text{if} \quad t\in[-0.3,0],\\ \{a,d\} & \text{if} \quad t\in[-0.7,-0.3),\\ \emptyset & \text{if} \quad t\in[-0.7,-1).\end{cases}$$

Then $L(f; t)$ is a bi-ideal of $S$ and by Theorem 3.4, $f$ is an $\mathcal{N}$-fuzzy bi-ideal of $S$. Moreover, $L(f; t)$ is a bi-ideal of $S$ but not a quasi-ideal for all $t \in [-0.7, -0.3)$ and by Theorem 3.4, $f$ is not an $\mathcal{N}$-fuzzy quasi-ideal of $S$.

**Proposition 3.8.** *If $(S, \cdot, \leqslant)$ is an ordered semigroup and $f_1, f_2, g_1, g_2$ are $\mathcal{N}$-fuzzy subsets of $S$ such that $g_1 \preceq f_1$ and $g_2 \preceq f_2$, then $g_1Ng_2 \preceq f_1Nf_2$.*

*Proof.* Let $a \in S$. If $A_a = \emptyset$ then $f_1Nf_2(a) = 0 \geqslant g_1Ng_2(a)$. If $A_a \neq \emptyset$ then

$$f_1Nf_2(a)=\bigwedge_{(y,z)\in A_a}\max\{f_1(y),f_2(z)\}\ \geqslant \bigwedge_{(y,z)\in A_a}\max\{g_1(y),g_2(z)\}=g_1Ng_2(a),$$

which completes the proof. □

From the above Proposition we see that the set of all $\mathcal{N}$-fuzzy subsets of an ordered semigroup is a complete lattice.

# 4. Characterizations of regular ordered semigroups

In this section, we prove that an ordered semigroup $S$ is regular, left and right simple if and only if every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$ is a constant $\mathcal{N}$-function. We define semiprime $\mathcal{N}$-fuzzy quasi-ideals of ordered semigroups and prove that an ordered semigroup $(S, \cdot, \leqslant)$ is completely regular if and only if every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$ is a semiprime $\mathcal{N}$-fuzzy quasi-ideal of $S$.

**Theorem 4.1.** *For an ordered semigroup $S$ the following are equivalent:*

(*i*) *$S$ is regular, left and right simple.*

(*ii*) *Every $\mathcal{N}$-fuzzy quasi-ideal of $S$ is a constant $\mathcal{N}$-function.*

*Proof.* (*i*) ⇒ (*ii*). Let $S$ be regular, left and right simple ordered semigroup. Let $f$ be an $\mathcal{N}$-fuzzy quasi-ideal of $S$. We consider the set $E_\Omega := \{e \in S | e^2 \geqslant e\}$. Then $E_\Omega$ is non-empty. In fact, i $a \in S$, since $S$ is regular, then there exists $x \in S$ such that $a \leqslant axa$. We consider the element $ax$ of $S$. Then $(ax)^2 = (axa)x \geqslant ax$, and so $ax \in E_\Omega$.

(A) We first prove that $f$ is a constant $\mathcal{N}$-function on $E_\Omega$. That is, $f(e) = f(t)$ for every $t \in E_\Omega$. In fact: Since $S$ is left and right simple, we have $(St] = S$ and $(tS] = S$. Since $e \in S$ then $e \in (St]$ and $e \in (tS]$. Then $e \leqslant xt$ and $e \leqslant ty$ for some $x, y \in S$. If $e \leqslant xt$ then $e^2 = ee \leqslant (xt)(xt) = (xtx)t$ and $(xtx, t) \in A_{e^2}$. If $e \leqslant ty$ then $e^2 = ee \leqslant (ty)(ty) = t(yty)$ and $(t, yty) \in A_{e^2}$. Since $A_{e^2} \neq \emptyset$, and $f$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$, we have

$$\begin{aligned} f(e^2) &\leqslant ((fN\alpha) \vee (\alpha N f))(e^2) = \max[(fN\alpha)(e^2), (\alpha N f)(e^2)] \\ &= \max\Big[ \bigwedge_{(y_1,z_1)\in A_{e^2}} \max\{f(y_1), \alpha(z_1)\}, \bigwedge_{(y_2,z_2)\in A_{e^2}} \max\{\alpha(z_2), f(y_2)\} \Big] \\ &\leqslant \max[\max\{f(t), \alpha(yty)\}, \max\{f(t), \alpha(xtx)\}] \\ &= \max[\max\{f(t), -1\}, \max\{f(t), -1\}] = \max[f(t), f(t)] = f(t). \end{aligned}$$

Since $e \in E_\Omega$, we have $e^2 \geqslant e$ and $f(e^2) \geqslant f(e)$. Thus $f(e) \leqslant f(t)$. On the other hand since $S$ is left and right simple and $e \in S$, we have $S = (Se]$ and $S = (eS]$. Since $t \in S$ we have $t \in (Se]$ and $t \in (eS]$. Then $t \leqslant ze$ and $t \leqslant es$ for some $z, s \in S$. If $t \leqslant ze$ then $t^2 = tt \leqslant (ze)(ze) = (zez)e$ and $(zez, e) \in A_{t^2}$. If $t \leqslant es$ then $t^2 = tt \leqslant (es)(es) = e(ses)$ and $(e, ses) \in A_{t^2}$. Since $A_{t^2} \neq \emptyset$, we have

$$\begin{aligned} f(t^2) &\leqslant ((fN\alpha) \vee (\alpha N f))(t^2) = \max[(fN\alpha)(t^2), (\alpha N f)(t^2)] \\ &= \max\Big[ \bigwedge_{(p_1,q_1)\in A_{t^2}} \max\{f(p_1), \alpha(q_1)\}, \bigwedge_{(p_2,q_2)\in A_{t^2}} \max\{\alpha(p_2), f(q_2)\} \Big] \\ &\leqslant \max[\max\{f(e), \alpha(xex)\}, \max\{\alpha(yey), f(e)\}] \\ &= \max[\max\{f(e), -1\}, \max\{-1, f(e)\}] = \max[f(e), f(e)] = f(e). \end{aligned}$$

Since $t \in E_\Omega$ then $t^2 \geqslant t$ and $f(t^2) \geqslant f(t)$. Thus $f(t) \leqslant f(e)$. Consequently, $f(t) = f(e)$.

$(B)$. Now, we prove that $f$ is a constant $\mathcal{N}$-function on $S$. That is, $f(t) = f(a)$ for every $a \in S$. Since $S$ is regular and $a \in S$, there exists $x \in S$ such that $a \leqslant axa$. We consider the elements $ax$ and $xa$ of $S$. Then by $(OS3)$, we have

$$(ax)^2 = (axa)x \geqslant ax \text{ and } (xa) = x(axa) \geqslant xa,$$

then $ax$, $xa \in E_\Omega$ and by $(A)$ we have $f(ax) = f(t)$ and $f(xa) = f(t)$. Since

$$(ax)(axa) \geqslant axa \geqslant a,$$

then $(ax, axa) \in A_a$ and $(axa)(xa) \geqslant axa \geqslant a$, then $(axa, xa) \in A_a$ and hence $A_a \neq \emptyset$. Since $f$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$, we have

$$\begin{aligned}
f(a) &\leqslant ((fN\alpha) \vee (\alpha Nf))(a) = \max[(fN\alpha)(a), (\alpha Nf)(a)] \\
&= \max\Big[ \bigwedge_{(y_1,z_1)\in A_a} \max\{f(y_1), \alpha(z_1)\}, \bigwedge_{(y_2,z_2)\in A_a} \max\{\alpha(y_2), f(z_2)\} \Big] \\
&\leqslant \max[\max\{f(ax), \alpha(axa)\}, \max\{\alpha(axa), f(xa)\}] \\
&= \max[\max\{f(ax), -1\}, \max\{-1, f(xa)\}] \\
&= \max[f(ax), f(xa)] = \max[f(t), f(t)] = f(t).
\end{aligned}$$

Since $S$ is left and right simple we have $(Sa] = S$, and $(aS] = S$. Since $t \in S$, we have $t \in (Sa]$ and $t \in (aS]$. Then $t \leqslant pa$ and $t \leqslant aq$ for some $p, q \in S$. Then $(p, a) \in A_t$ and $(a, q) \in A_t$. Since $A_t \neq \emptyset$ and $f$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$, we have

$$\begin{aligned}
f(t) &\leqslant ((fN\alpha) \vee (\alpha Nf))(t) = \max[(fN\alpha)(t), (\alpha Nf)(t)] \\
&= \max\Big[ \bigwedge_{(y_1,z_1)\in A_t} \max\{f(y_1), \alpha(z_1)\}, \bigwedge_{(y_2,z_2)\in A_t} \max\{\alpha(y_2), f(z_2)\}\Big] \\
&\leqslant \max[\max\{f(a), \alpha(p)\}, \max\{\alpha(q), f(a)\}] \\
&= \max[\max\{f(a), -1\}, \max\{-1, f(a)\}] = \max[f(a), f(a)] = f(a).
\end{aligned}$$

Thus $f(t) \leqslant f(a)$ and $f(t) = f(a)$.

$(ii) \Rightarrow (i)$. Let $a \in S$. Then the set $(aS]$ is a quasi-ideal of $S$. Indeed, (a) $(aS] \cap (Sa] \subseteq (aS]$ and (b) If $x \in (aS]$ and $S \ni y \leqslant x \in (aS]$, then $y \in ((aS]] = (aS]$. Since $(aS]$ is quasi-ideal of $S$, by Theorem 3.3, the characteristic $\mathcal{N}$-function $\kappa_{(aS]}$ of $(aS]$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$. By hypothesis, $\kappa_{(aS]}$ is a constant $\mathcal{N}$-function, so $\kappa_{(aS]}(x) = -1$ or $\kappa_{(aS]}(x) = -1$ for every $x \in S$.

Let $(aS] \subset S$ and $a$ be an element of $S$ such that $a \notin (aS]$, then $\kappa_{(aS]}(x) = 0$. On the other hand, since $a^2 \in (aS]$ then $\kappa_{(aS]}(a^2) = -1$. A contradiction to the fact that $\kappa_{(aS]}$ is a constant $\mathcal{N}$-function. Thus $(aS] = S$. By symmetry we can prove that $(Sa] = S$.

Since $a \in S$ and $S = (aS] = (Sa]$, we have $a \in (aS] = (a(Sa]] \subseteq (aSa]$, hence $S$ is regular. □

**Theorem 4.2.** *An ordered semigroup $(S, \cdot, \leqslant)$ is completely regular if and only if for every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$ we have $f(a) = f(a^2)$ for every $a \in S$.*

*Proof.* Let $S$ be a completely regular ordered semigroup and $f$ an $\mathcal{N}$-fuzzy quasi-ideal of $S$. Since $S$ is left and right regular we have $a \in (Sa^2]$ and $a^2 \in (a^2S]$ for every $a \in S$. Then there exists $x, y \in S$ such that $a \leqslant xa^2$ and $a \leqslant a^2y$. Then $(x, a^2)$, $(a^2, y) \in A_a$. Since $A_a \neq \emptyset$, we have

$$\begin{aligned}
f(a) &\leqslant ((fN\alpha) \vee (\alpha N f))(a) = \max[(fN\alpha)(a), (\alpha N f)(a)] \\
&= \max\Big[\bigwedge_{(y,z)\in A_a} \max\{f(y), \alpha(z)\}, \bigwedge_{(y,z)\in A_a} \max\{\alpha(y), f(z)\}\Big] \\
&\leqslant \max[\max\{f(a^2), \alpha(y)\}, \max\{\alpha(x), f(a^2)\}] \\
&= \max[\max\{f(a^2), -1\}, \max\{-1, f(a^2)\}] \\
&= \max[f(a^2), f(a^2)] = f(a^2) = f(aa) \leqslant \max\{f(a), f(a)\} = f(a).
\end{aligned}$$

Thus $f(a) = f(a^2)$.

Conversely, let $a \in S$. We consider the quasi-ideal $Q(a^2)$ generated by $a^2$ $(a \in S)$. That is, the set $Q(a^2) = (a^2 \cup (a^2S \cap Sa^2)]$. By Theorem 3.3, the characteristic $\mathcal{N}$ -function $\kappa_{Q(a^2)}$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$. By hypothesis

$$\kappa_{Q(a^2)}(a) = \kappa_{Q(a^2)}(a^2).$$

Since $a^2 \in Q(a^2)$, we have $\kappa_{Q(a^2)}(a^2) = -1$ then $\kappa_{Q(a^2)}(a) = -1$ and $a \in Q(a^2) = (a^2 \cup (a^2S \cap Sa^2)]$. Then $a \leqslant a^2$ or $a \leqslant a^2x$ and $a \leqslant ya^2$ for some $x, y \in S$. If $a \leqslant a^2$ then $a \leqslant a^2 = aa \leqslant a^2a^2 = aaa^2 \leqslant a^2aa^2 \in a^2Sa^2$ and $a \in (a^2Sa^2]$. If $a \leqslant a^2x$ and $a \leqslant ya^2$ then $a \leqslant (a^2x)(ya^2) = a^2(xy)a^2 \in a^2Sa^2$ and $a \in (a^2Sa^2]$. □

A subset $T$ of an ordered semigroup $S$ is called *semiprime* if for every $a \in S$ from $a^2 \in T$ it follows $a \in T$.

**Definition 4.3.** An $\mathcal{N}$-fuzzy subset $f$ of an ordered semigroup $(S, \cdot, \leqslant)$ is called *semiprime* if $f(a) \leqslant f(a^2)$ for all $a \in S$.

**Theorem 4.4.** *An ordered semigroup $(S, \cdot, \leqslant)$ is completely regular if and only if every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$ is semiprime.*

*Proof.* Let $S$ be a completely regular ordered semigroup and $f$ an $\mathcal{N}$-fuzzy quasi-ideal of $S$. Let $a \in S$. Then $f(a) \leqslant f(a^2)$. Indeed, since $S$ is left and right regular, there exist $x$, $y \in S$ such that $a \leqslant xa^2$ and $a \leqslant a^2y$ then $(x, a^2) \in A_a$ and $(a^2, y) \in A_a$. Since $A_a \neq \emptyset$, then we have

$$\begin{aligned}
f(a) &\leqslant ((fN\alpha) \vee (\alpha N f))(a) = \max[(fN\alpha)(a), (\alpha N f)(a)] \\
&= \max\Big[\bigwedge_{(y,z)\in A_a} \max\{f(y), \alpha(z)\}, \bigwedge_{(y,z)\in A_a} \max\{\alpha(y), f(z)\}\Big]
\end{aligned}$$

$$\leqslant \max\left[\max\{f(a^2), \alpha(y)\}, \max\{\alpha(x), f(a^2)\}\right]$$
$$= \max\left[\max\{f(a^2), -1\}, \max\{-1, f(a^2)\}\right] = \max\left[f(a^2), f(a^2)\right] = f(a^2).$$

To prove the converse, let $f$ be an $\mathcal{N}$-fuzzy quasi-ideal of $S$ such that $f(a) \leqslant f(a^2)$ for all $a \in S$. We consider the quasi-ideal $Q(a^2)$ generated by $a^2 (a \in S)$. That is, the set $Q(a^2) = (a^2 \cup (a^2 S \cap S a^2)]$. Then by Theorem 3.3, $\kappa_{Q(a^2)}$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$. By hypothesis $\kappa_{Q(a^2)}(a) \leqslant \kappa_{Q(a^2)}(a^2)$. Since $a^2 \in Q(a^2)$, we have $\kappa_{Q(a^2)}(a^2) = -1$ and $\kappa_{Q(a^2)}(a) = -1$ we get $a \in Q(a^2)$. Then $a \leqslant a^2$ or $a \leqslant a^2 p$ and $a \leqslant q a^2$ for some $p, q \in S$. If $a \leqslant a^2$ then

$$a \leqslant a^2 = aa \leqslant a^2 a^2 = aaa^2 \leqslant a^2 aa^2 \in a^2 S a^2 \text{ and } a \in (a^2 S a^2].$$

If $a \leqslant a^2 p$ and $a \leqslant q a^2$. Then $a \leqslant (a^2 p)(q a^2) = a^2 (pq) a^2 \in a^2 S a^2$ and $a \in (a^2 S a^2]$. □

## 5. Some semilattices of simple ordered semigroups

A subsemigroup $F$ of an ordered semigroup $S$ is called a *filter* of $S$ if:

$(i)$ $a, b \in S$ and $ab \in F$ implies $a \in F$ and $b \in F$.

$(ii)$ If $a \in F$ and $c \in S$ such that $c \geqslant a$ then $c \in F$ (see [7]).

For $x \in S$, we denote by $N(x)$ the least filter of $S$ generated $x$ $(x \in S)$ and by $\mathcal{N}$ the *equivalence relation*

$$\mathcal{N} := \{(x, y) \in S \times S \mid N(x) = N(y)\}.$$

Let $S$ be an ordered semigroup. An equivalence relation $\sigma$ on $S$ is called *congruence* if $(a, b) \in \sigma$ implies $(ac, bc) \in \sigma$ and $(ca, cb) \in \sigma$ for every $c \in S$. A congruence $\sigma$ on $S$ is called *semilattice congruence* if $(a^2, a) \in \sigma$ and $(ab, ba) \in \sigma$ for each $a, b \in S$ (see [7]). If $\sigma$ is a semilattice congruence on $S$ then the $\sigma$-class $(x)_\sigma$ of $S$ containing $x$ is a subsemigroup of $S$ for every $x \in S$ (see [7]). An ordered semigroup $S$ is called a semilattice of *left and right simple semigroups* if there exists a semilattice congruence $\sigma$ on $S$ such that the *$\sigma$-class* $(x)_\sigma$ of $S$ containing $x$ is a left and right simple subsemigroup of $S$ for every $x \in S$.

Equivalent definition:

There exists a semilattice $Y$ and a family $\{S_\alpha\}_{\alpha \in Y}$ of left and right simple subsemigroups of $S$ such that

$(i)$ $S_\alpha \cap S_\beta = \emptyset \ \forall \alpha, \beta \in Y$, $\alpha \neq \beta$,

$(ii)$ $S = \bigcup\limits_{\alpha \in Y} S_\alpha$,

$(iii)$ $S_\alpha S_\beta \subseteq S_{\alpha\beta} \ \forall \alpha, \beta \in Y$.

**Theorem 5.1.** *An ordered semigroup $(S, \cdot, \leqslant)$ is a semilattice of left and right simple semigroups if and only if for every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$, we have $f(a) = f(a^2)$ and $f(ab) = f(ba)$ for all $a, b \in S$.*

*Proof.* Suppose that $S$ is a semilattice of left and right simple semigroups. Then by hypothesis, there exists a semilattice $Y$ and a family $\{S_\alpha\}_{\alpha\in Y}$ of left and right simple subsemigroups of $S$ satisfying $(i)$, $(ii)$ and $(iii)$.

$(A)$ Let $f$ be an $\mathcal{N}$-fuzzy quasi-ideal of $S$ and $a\in S$. Since $a\in S=\bigcup\limits_{\alpha\in Y} S_\alpha$, then there exists $\alpha\in Y$ such that $a\in S_\alpha$. Since $S_\alpha$ is left simple we have $S_\alpha=(S_\alpha a]$. Since $a\in S_\alpha$, then $a\in(S_\alpha a]$ and so $a\leqslant xa$ for some $x\in S_\alpha$. Since $x\in S_\alpha$, we have $x\in(S_\alpha a]$, then $x\leqslant ya$ for some $y\in S_\alpha$. Thus $a\leqslant xa\leqslant(ya)a=ya^2$ and we have $(y,a^2)\in A_a$. Also $S$ is right simple, we have $S_\alpha=(aS_\alpha]$, since $a\in S_\alpha$ then $a\in(aS_\alpha]$ and we have $a\leqslant az$ for some $z\in S_\alpha$. Since $z\in S_\alpha$ we have $z\in(aS_\alpha]$ then $z\leqslant at$ for some $t\in S$. Thus $a\leqslant az\leqslant a(at)=a^2t$, and we have $(a^2,t)\in A_a$. Since $f$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$ and $A_a\neq\emptyset$, we have

$$\begin{aligned}
f(a)&\leqslant((fN\alpha)\vee(\alpha Nf))(a)=\max[(fN\alpha)(a),(\alpha Nf)(a)]\\
&=\max\Big[\bigwedge_{(y_1,z_1)\in A_a}\max\{f(y_1),\alpha(z_1)\},\quad\bigwedge_{(y_2,z_2)\in A_a}\max\{\alpha(y_2),f(z_2)\}\Big]\\
&\leqslant\max\left[\max\{f(a^2),\alpha(t)\},\max\{\alpha(y),f(a^2)\}\right]\\
&=\max\left[\max\{f(a^2),-1\},\max\{-1,f(a^2)\}\right]=\max\left[f(a^2),f(a^2)\right]=f(a^2).
\end{aligned}$$

On the other hand, since every $\mathcal{N}$-fuzzy quasi-ideal is an $\mathcal{N}$-fuzzy subsemigroup of $S$, we have $f(a^2)=f(aa)\leqslant\max\{f(a),f(a)\}=f(a)$. Thus $f(a)=f(a^2)$.

$(B)$ Let $a,b\in S$. By (A), we have $f(ab)=f((ab)^2)=f((ab)^4)$. Since $(AB]=(BA]=A\cap B$, by Lemmas 2.5 an 2.8, we have

$$\begin{aligned}
(ab)^4&=(aba)(babab)\in Q(aba)Q(babab)\subseteq(Q(aba)Q(babab)]\\
&=(Q(babab)Q(aba)]=((babab\cup(bababS\cap Sbabab](aba\cup(abaS\cap Saba]]\\
&\subseteq((babab\cup(bababS](aba\cup(Saba]]\subseteq((baS\cup(baS](Sba\cup(Sba]]\\
&=((baS](Sba]]=((baSba]]=(baSba]=baS\cap Sba
\end{aligned}$$

Then $(ab)^4\leqslant(ba)x$ and $(ab)^4\leqslant y(ba)$ for some $x,y\in S$. Then $(ba,x)\in A_{(ab)^4}$ and $(y,ba)\in A_{(ab)^4}$. Since $f$ is an $\mathcal{N}$-fuzzy quasi-ideal and $A_{(ab)^4}\neq\emptyset$, we have

$$\begin{aligned}
f((ab)^4)&\leqslant((fN\alpha)\vee(\alpha Nf))((ab)^4)=\max[(fN\alpha)(ab)^4,(\alpha Nf)(ab)^4]\\
&=\max\Big[\bigwedge_{(y_1,z_1)\in A_{(ab)^4}}\max\{f(y_1),\alpha(z_1)\},\quad\bigwedge_{(y_2,z_2)\in A_{(ab)^4}}\max\{\alpha(y_2),f(z_2)\}\Big]\\
&\leqslant\max\left[\max\{f(ba),\alpha(x)\},\max\{\alpha(y),f(ba)\}\right]\\
&=\max\left[\max\{f(ba),-1\},\max\{-1,f(ba)\}\right]=\max\left[f(ba),f(ba)\right]=f(ba).
\end{aligned}$$

By symmetry we can prove that $f(ba)\leqslant f((ab)^4)=f(ab)$.

Conversely, assume that conditions (1) and (2) are true. Then by (1) and Lemma 2.7, $S$ is completely regular. Let $A$ be a quasi-ideal of $S$ and let $a\in A$.

Since $S$ is completely and $a \in S$, there exists $x \in S$ such that $a \leqslant a^2xa^2$. Then

$$\begin{aligned} a \leqslant a^2xa^2 &\in (a^2Sa^2) = a(a(Sa)a) \subseteq a(aSa) \subseteq a(aSa] \\ &= a(aS \cap Sa) \subseteq A(AS \cap SA) \subseteq A(AS) \subseteq AA, \end{aligned}$$

and so $A \subseteq AA \subseteq (A^2]$. On the other hand, by Lemma 2.4, $A$ is a subsemigroup of $S$, we have $A^2 \subseteq A \Longrightarrow (A^2] \subseteq (A] = A$.

Let $A$ and $B$ be any quasi-ideals of $S$ and let $x \in (AB]$, then $x \leqslant ab$ for some $a \in A$ and $b \in B$. We consider the quasi-ideal $Q(ab) = (ab \cup (abS \cap Sab)]$ generated by $ab$. Then by Theorem 3.3, the characteristic $\mathcal{N}$-function $\kappa_{Q(ab)}$ of $Q(ab)$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$. By hypothesis $\kappa_{Q(ab)}(ba) = \kappa_{Q(ab)}(ab)$.

Since $ab \in Q(ab)$, we have $\kappa_{Q(ab)}(ab) = -1$ and $\kappa_{Q(ab)}(ba) = -1$. Therefore $ba \in Q(ab) = (ab \cup (abS \cap Sab)]$ and, by Lemma 2.9,

$$\begin{aligned} ba &\in (ab \cup (abS \cap Sab)] = (ab \cup (abSab]] \subseteq (AB \cup (ABSAB]] \\ &\subseteq (AB \cup ((AB]S(AB]] \subseteq (AB \cup (AB]] = ((AB]] = (AB]. \end{aligned}$$

Hence $(BA] \subseteq (AB]$. By symmetry we can prove that $(AB] \subseteq (BA]$. □

**Lemma 5.2.** *Let $(S, \cdot, \leqslant)$ be an ordered semigroup such that $a \leqslant a^2$ for all $a \in S$. Then for every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$ we have $f(a) = f(a^2)$ for every $a \in S$.*

*Proof.* Let $a \in S$ such that $a \leqslant a^2$. Let $f$ be an $\mathcal{N}$-fuzzy quasi-ideal of $S$. Since $f$ is an $\mathcal{N}$-fuzzy subsemigroup of $S$. Then $f(a) \leqslant f(a^2) \leqslant \max\{f(a), f(a)\} = f(a)$. □

**Theorem 5.3.** *Let $S$ be an ordered semigroup and $a \in S$ such that $a \leqslant a^2$ for all $a \in S$. Then the following are equivalent:*

(*i*) *$ab \in (baS] \cap (Sba]$ for each $a, b \in S$.*

(*ii*) *For every $\mathcal{N}$-fuzzy quasi-ideal $f$ of $S$, we have $f(ab) = f(ba)$ for every $a, b \in S$.*

*Proof.* $(i) \Rightarrow (ii)$. Let $f$ be an $\mathcal{N}$-fuzzy quasi-ideal of $S$. Since $ab \in (baS] \cap (Sba]$, then $ab \in (baS]$ and we have $ab \leqslant (ba)x$ for some $x \in S$. By $(i)$, we have $(ba)x \in (xbaS] \cap (Sxba]$. Then $(ba)x \in (Sxba]$ and we have $(ba)x \leqslant (yx)(ba)$ and so, $ab \leqslant (yx)(ba) \Rightarrow (yx, ba) \in A_{ab}$. Again, since $ab \in (Sba]$, then $ab \leqslant z(ba)$ for some $z \in S$ and by (i) we have $z(ba) \in (bazS]$, then $z(ba) \leqslant (ba)(zt)$ for some $t \in S$. So we have $ab \leqslant (ba)(zt) \Rightarrow (ba, zt) \in A_{ab}$. Since $f$ is an $\mathcal{N}$-fuzzy quasi-ideal of $S$ and $A_{ab} \neq \emptyset$, then

$$\begin{aligned} f(ab) &\leqslant ((fN\alpha) \vee (\alpha Nf))(ab) = \max[(fN\alpha)(ab), (\alpha Nf)(ab)] \\ &= \max\Big[ \bigwedge_{(y_1,z_1)\in A_{ab}} \max\{f(y_1), \alpha(z_1)\}, \bigwedge_{(y_2,z_2)\in A_{ab}} \max\{\alpha(y_2), f(z_2)\} \Big] \\ &\leqslant \max\left[\max\{f(ba), \alpha(zt)\}, \max\{\alpha(yx), f(ba)\}\right] \\ &= \max\left[\max\{f(ba), -1\}, \max\{-1, f(ba)\}\right] = \max[f(ba), f(ba)] = f(ba). \end{aligned}$$

By symmetry we can prove that $f(ba) \leqslant f(ab)$.

$(ii) \Rightarrow (i)$. Let $f$ be an $\mathcal{N}$-fuzzy quasi-ideal of $S$. Since $a \leqslant a^2$ for all $a \in S$, by Lemma 5.2, we have $f(a) = f(a^2)$. By $(ii)$, we obtain $f(ba) = f(ab)$ for each $a, b \in S$. By Theorem 5.1, it follows that $S$, is a semilattice of left and right simple semigroups. Thus by hypothesis, there exists a semilattice $Y$ and a family $\{S_\alpha\}_{\alpha \in Y}$ of left and right simple subsemigroups satisfying $(i)$, $(ii)$ and $(iii)$ from the equivalent definition of a semilattice of simple semigroups.

Let $a, b \in S$, we have to show that $a \in (baS] \cap (Sba]$. Let $\alpha, \beta \in Y$ be such that $a \in S_\alpha$ and $b \in S_\beta$. Then $ab \in S_\alpha S_\beta \subseteq S_{\alpha\beta}$ and $ba \in S_\beta S_\alpha \subseteq S_{\beta\alpha} = S_{\alpha\beta}$. Since $S_{\alpha\beta}$ is left and right simple we have $S_{\alpha\beta} = (S_{\alpha\beta}c]$ and $S_{\alpha\beta} = (cS_{\alpha\beta}]$ for each $c \in S_{\alpha\beta}$. Since $ab, ba \in S_{\alpha\beta}$, we have $ab \in (baS_{\alpha\beta}] \cap (S_{\alpha\beta}ba] \subseteq (baS] \cap (Sba]$. This complete the proof. □

# References

[1] **J. Ahsan, R. M. Latif, and M. Shabir**, *Fuzzy quasi-ideals of semigroups*, J. Fuzzy Math. **2** (2001), 259 – 270.

[2] **A. H. Clifford and G. B. Preston**,*The Algebraic Theory of Semigroups*, Vol. I, Amer. Math. Soc., Math. Survey Providence RI, 1961.

[3] **W. A. Dudek and Y. B. Jun**, *$\mathcal{N}$- quasi-groups*, Quasigroups and Related Systems **17** (2009), 29 – 38.

[4] **N. Kehayopulu**, *On left regular duo ordered semigroups*, Math. Japon. **35** (1990), 1051 – 1056.

[5] **N. Kehayopulu**, *On regular duo ordered semigroups*, Math. Japon. **37** (1992), 535 – 540.

[6] **N. Kehayopulu**, *On completely regular ordered semigroups*, Sci. Math. **1** (1998), 27 – 32.

[7] **N. Kehayopulu and M. Tsingelis**, *On the decomposition of prime ideals in ordered semigroups into their $\mathcal{N}$-classes*, Semigroup Forum **47** (1993), 393 – 395.

[8] **N. Kehayopulu and M. Tsingelis**, *Fuzzy sets in ordered groupoids*, Semigroup Forum **65** (2002), 128 – 132.

[9] **N. Kehayopulu and M. Tsingelis**, *Regular ordered semigroups in terms of fuzzy subsets*, Inform. Sci. **176** (2006), 3675 – 3693.

[10] **N. Kehayopulu and M. Tsingelis**, *Fuzzy ideals in ordered semigroups*, Quasigroups and Related Systems **15** (2007), 185 – 195.

[11] **A. Khan, Y. B. Jun and M. Shabir**, *$\mathcal{N}$-fuzzy bi-ideals in ordered semigroups*, (submitted).

[12] **M. Kondo and W. A. Dudek**, *On the Transfer Principle in fuzzy theory*, Mathware Soft Comput. **12** (2005), 41 – –55.

[13] **N. Kuroki**, *Fuzzy bi-ideals in semigroups*, Comment. Math. Univ. St. Pauli **28** (1979), 17 – 21.

[14] **N. Kuroki**, *On fuzzy ideals and fuzzy bi-ideals in semigroups*, Fuzzy Sets Systems **5** (1982), 71 – 79.

[15] **N. Kuroki**, *On fuzzy semiprime ideals in semigroups*, Inform. Sci. **53** (1991), 203 – 236.

[16] **N. Kuroki**, *Generalized fuzzy bi-ideals in semigroups*, Inform. Sci. **66** (1992), 235 – 243.

[17] **N. Kuroki**, *Fuzzy semiprime quasi-ideals in semigroups*, Inform. Sci. **75** (1993) 201 – 211.

[18] **R. G. McLean and H. Kummer**, *Fuzzy ideals in semigroups*, Fuzzy Sets Systems **48** (1992), 137 – 140.

[19] **J. N. Mordeson and D. S. Malik**, *Fuzzy Automata and language*, Theory and Applications, Computational Math. Series, Chapman and Hall/CRC, Boca Raton, 2002.

[20] **J. N. Mordeson, D. S. Malik and N. Kuroki**, *Fuzzy semigroups*, Studies in Fuzziness and Soft Computing **131**, Springer-Verlag, Berlin, 2003.

[21] **A. Rosenfeld**, *Fuzzy groups*, J. Math. Anal. Appl. **35** (1971), 512-517.

[22] **M. Shabir and A. Khan**, *Characterizations of ordered semigroups by the properties of their fuzzy generalized bi-ideals*, New Math. Natural Comput. **4** (2008), 237 – 250.

[23] **M. Shabir and A. Khan**, *Fuzzy filters in ordered semigroups*, Lobachevskii J. Math. **29** (2008), 82 – 89.

[24] **M. Shabir and A. Khan**, *Fuzzy quasi-ideals in ordered semigroups*, (submitted).

[25] **O. Steinfeld**, *Quasi-ideals in Rings and Semigroups*, Akademiakiado, Budapest, 1978.

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

Received December 27, 2008

A.Khan
Department of Mathematics, COMSATS Institute of Information Technology, Abbottabad, Pakistan
E-mail: azhar4set@yahoo.com

Y.B.Jun
Department of Mathematics Education, Gyeongsang National University, Chinju 660-701, Korea
E-mail: skywine@gmail.com

M.Shabir
Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
E-mail: mshabirbhatti@yahoo.co.uk

Quasigroups and Related Systems **17** (2009), 253 – 270

# Generalized quadratic quasigroup equations with three variables

*Aleksandar Krapež*

**Abstract.** F. M. Sokhats'kyi recently posed the problem of classification of (un)cancellable generalized quadratic quasigroup equations. Refining relevant results of S. Krstić, A. Krapež and D. Živković solved this problem by reducing it to the classification of connected (3–connected) cubic graphs. They also started systematic investigation by solving all equations with two variables. Here we consider equations with exactly three variables. There are 330 of them and they split into five classes of parastrophic equivalence. We give solutions to five representative equations, one from each class.

## 1. Introduction

This paper is a sequel of [7] by A. Krapež and D. Živković. Although we define the most important notions and state essential results of [7], it is assumed that the reader is thoroughly familiar with it.

In [7] authors consider the correspondence between generalized quadratic quasigroup functional equations and connected cubic graphs as established by S. Krstić in his PhD thesis [8]. It is proved that the important notion of parastrophic equivalence of quadratic equations corresponds to the isomorphism of graphs obtained from given equations. The set of nine normal equations with two variables is divided into two classes of parastrophic equivalence corresponding to two nonisomorphic graphs.

Much more is known about the special case of parastrophically uncancellable equations. Various authors obtained instances of number $u_n$ of classes of parastrophically nonequivalent uncancellable equations with small number $n$ of variables. The results are: $u_2 = 1$ (Krapež and Živković [7]),

2010 Mathematics Subject Classification: 20N05, 39B52, 05C25
Keywords: quasigroup, quadratic functional equation, connected cubic graph, parastrophic equivalence.
The author is supported by grants 144013 and 144018 of the Ministry of Science and Technology of Serbia.

$u_3 = 1$ (Sokhats'kyi [10] after Duplák [4]), $u_4 = 2$ (Sokhats'kyi [10]), $u_5 = 4$ (Koval' [5]) and $u_6 = 14$ (Krapež, Simić and Tošić [6]).

In this paper we prove that there are five classes of cancellable and uncancellable equations with three variables, we give their Krstić graphs and solve five parastrophically nonequivalent representative equations.

## 2. Quasigroups and functional equations

Let us recall necessary definitions and results of [7]. For bare essentials on quasigroups see [7]. More can be found in standard references V. D. Belousov [2], O. Chein, H. O. Pflugfelder and J. D. H. Smith [3] and H. O. Pflugfelder [9]. We just state that the language of quasigroups contains six binary operations: multiplication ($\cdot$), left ($\backslash$) and right ($/$) division and their respective dual operations: $*$ (dual of $\cdot$), $\backslash\!\!\backslash$ (dual of $\backslash$) and $/\!\!/$ (dual of $/$). These six operations are known as parastrophes of $\cdot$ (and of each other) and the connection between them is: $xy = z$ iff $x\backslash z = y$ iff $z/y = x$ iff $y * x = z$ iff $z \backslash\!\!\backslash x = y$ iff $y /\!\!/ z = x$.

When we use prefix notation for operations and a quasigroup operation is $A$, we define: $A(x_1, x_2) = x_3$ iff $A^{(1)}(x_1, x_2) = x_3$ iff $A^{(12)}(x_2, x_1) = x_3$ iff $A^{(13)}(x_3, x_2) = x_1$ iff $A^{(23)}(x_1, x_3) = x_2$ iff $A^{(123)}(x_2, x_3) = x_1$ iff $A^{(132)}(x_3, x_1) = x_2$. In general, $A(x_1, x_2) = x_3$ iff $A^{\sigma}(x_{\sigma(1)}, x_{\sigma(2)}) = x_{\sigma(3)}$ for $\sigma \in S_3$.

We assume that all operations are quasigroups. Further:

**Definition 2.1.** Functional equation $s = t$ is *quadratic* if every object variable appears exactly twice in $s = t$.

**Definition 2.2.** Functional equation $s = t$ is *generalized* if every functional variable $F$ (including all parastrophes of $F$) appears only once in $s = t$.

We also need the following:

**Definition 2.3.** Let $Eq[F_1, \ldots, F_n]$ be a generalized quadratic functional equation on quasigroups. We write $F_i \sim F_j$ $(1 \leqslant i, j \leqslant n)$ and say that $F_i$ and $F_j$ are *necessarily isostrophic* if in every solution $Q_1, \ldots, Q_n$ of $Eq$ the operations $Q_i$ and $Q_j$ are isostrophic.

A functional variable $F_i$ is *loop, group, abelian* if $Q_i$ is isostrophic to a loop, group, abelian group respectively.

**Definition 2.4.** A $\sim$–class with one or two elements is called *small*, otherwise it is *big*.

**Definition 2.5.** Two equations $Eq$ and $Eq'$ are *parastrophically equivalent* ($Eq\,\mathrm{PE}\,Eq'$) if one of them can be obtained from the other by applying a finite number of the following steps:

1. Renaming object and/or functional variables.
2. Replacing $s = t$ by $t = s$.
3. Replacing equation $A(t_1, t_2) = t_3$ by one of the following equations: $A^{\sigma}(t_{\sigma(1)}, t_{\sigma(2)}) = t_{\sigma(3)}$ for some $\sigma \in S_3$.
4. Replacing a subterm $A(t_1, t_2)$ of $s$ or $t$ by $A^{(12)}(t_2, t_1)$.
5. Replacing a subterm $A(x, t_2)$ by a new variable $y$ and simultaneously replacing all other occurrences of $x$ by either $A^{(13)}(y, t_2)$ or $A^{(123)}(t_2, y)$.
6. Replacing a subterm $A(t_1, x)$ by a new variable $y$ and simultaneously replacing all other occurrences of $x$ by either $A^{(23)}(t_1, y)$ or $A^{(132)}(y, t_1)$.

If we use notation $Eq[\ldots, A, \ldots]$, we denote by $Eq'[\ldots, A^{\sigma}, \ldots]$ the equation obtained by one of the steps $(3)-(7)$ above, always preserving the order of other functional variables. Using this convention we get:

**Theorem 2.6** (Krstić [8]) **.** *If equations $Eq[F_1, \ldots, F_n]$ and $Eq'[G_1, \ldots, G_n]$ are parastrophically equivalent and $Q_1, \ldots, Q_n$ and $R_1, \ldots, R_n$ are solutions of respectively $Eq, Eq'$ on a set $S$, then the operations $Q_i$ and $R_i$ $(1 \leqslant i \leqslant n)$ are mutually isostrophic.*

## 3. Graphs and functional equations

Following S. Krstić [8] we represent functional equations by graphs. These 'graphs' may have loops and multiple edges between two vertices and are technically known as *multigraphs*.

We define graphs as relation systems $(V, E; I)$ with $I \subseteq V \times E$. It is assumed that the sets $V$ of vertices and $E$ of edges are disjoint and that for every edge $e$ there are at most two vertices incident to $e$. A *loop* is an edge with a unique vertex incident to it. A loop in a graph should not be confused with a loop as a quasigroup with an identity.

A graph is *cubic* if for every vertex $v$ there are exactly three edges to which $v$ is incident, provided that if edge is a loop it is counted twice.

**Definition 3.1.** Two vertices $v_1, v_2$ of a graph $G$ are 3*–connected* (and we write $v_1 \equiv v_2$) if there are three disjoint paths in $G$ from $v_1$ to $v_2$. A graph $G$ is 3*–connected* if all vertices of $G$ are 3–connected.

In graph theory, 3–connectedness, as defined above, is usually called 3–edge–connectedness, but we shortened it to 3–connectedness. A graph is 3–connected iff removal of any two edges does not disconnect it. Obviously, a cubic graph $G$ is 3–connected iff the relation $\equiv$ is a full relation on $V$.

**Definition 3.2.** A $\equiv$–class with one or two elements is called *small*, otherwise it is *big*.

Based on the theory of S. Krstić [8], two constructioins are presented in [7] - the one which produces the graph $\mathrm{K}(Eq)$ for a given generalized quadratic functional equation $Eq$ and the other, which gives an equation $\mathrm{QE}(G)$ for a given finite connected cubic graph $G$.

We have:

**Theorem 3.3** (Krapež and Živković [7] after Krstić [8]). *Generalized quadratic quasigroup functional equations $Eq$ and $Eq^{'}$ are parastrophically equivalent iff their Krstić graphs $\mathrm{K}(Eq)$ and $\mathrm{K}(Eq^{'})$ are isomorphic.*

The following theorem is also important.

**Theorem 3.4** (Krstić [8]). *Let $Eq[F_1, \dots, F_n]$ be a generalized quadratic functional equation. Then $F_i \sim F_j$ in $Eq$ iff $F_i \equiv F_j$ in $\mathrm{K}(Eq)$. Moreover:*

*Every $F_i$ is a loop functional variable.*

*A symbol $F_i$ is a group functional variable iff $F_i/\equiv$ is big iff $K_4$ is homeomorphically embeddable in $\mathrm{K}(Eq)$ within $F_i/\equiv$.*

*A symbol $F_i$ is an abelian functional variable iff the subgraph of $\mathrm{K}(Eq)$ defined by $F_i/\equiv$ is not planar iff $K_{3,3}$ is homeomorphically embeddable in $\mathrm{K}(Eq)$ within $F_i/\equiv$.*

## 4. Equations with three variables

In the paper [7] A. Krapež and D. Živković defined sequences $(E_n)$, $(e_n)$ and $(\pi_n)(n \geq 1)$, where $E_n$ is the number of generalized quadratic quasigroup functional equations with $n$ variables, $e_n$ is the number of normal equations among them and $\pi_n$ is the number of classes of parastrophically equivalent equations with $n$ variables. By the Theorem 5.9 of [7] $\pi_n$ is also the number of nonisomorphic cubic graphs with $2(n-1)$ vertices. We have $E_3 = 3780$ and $e_3 = 330$. It is announced that $\pi_3 = 5$. We give the proof of this fact now but also a new proof that $\pi_2 = 2$.

By the Lemma 5.2 of [7], equations with 2, 3 variables have Krstić graphs which are connected, cubic and have 2, 4 vertices and 3, 6 edges respectively.

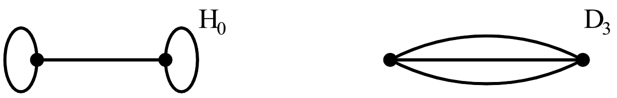

Figure 1. Graphs with two vertices

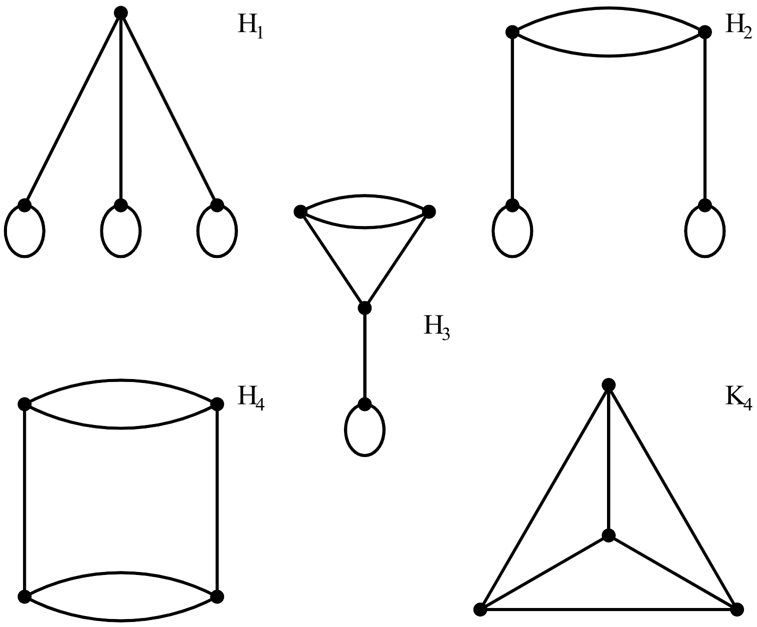

Figure 2. Graphs with four vertices

**Theorem 4.1.** *Every connected cubic graph with two vertices is isomorphic to either the dumbbell graph $H_0$ or to the dipole graph $D_3$ (Figure 1). Every connected cubic graph with four vertices is isomorphic to either one of: $H_1$, $H_2$, $H_3$, $H_4$, $K_4$ (Figure 2). Consequently, $\pi_2 = 2$ and $\pi_3 = 5$.*

*Proof.* Let $G$ be a connected cubic graph with either two or four vertices. There are four possibilities:

(1) $G$ has a loop,

(2) $G$ has no loops but has a triple edge,

(3) $G$ has no loops or triple edges but has a double edge,

(4) $G$ has no loops or multiple edges.

(1) $G$ has a loop. Then there is a vertex, say 1, with the loop. Since $G$ is cubic, there is another edge in 1 connecting it to a new vertex 2. There are three possibilities:

(11) the vertex 2 has a loop,

(12) 2 has no loop but has a double edge,

(13) 2 has no loops or double edges.

(11) The vertex 2 has a loop. Since $G$ is cubic and connected, no further extension is possible. Therefore $G$ is isomorphic to the dumbbell graph $H_0$.

(12) The vertex 2 has no loop but has a double edge. Let the vertex 2 connects to the vertex 3 by the double edge. The single remaining edge at 3 has to connect it to the new vertex 4. All vertices except 4 now have three edges. Therefore 4 has to connect to itself by the loop. The graph $G$ is isomorphic to $H_2$.

(13) The vertex 2 has no loops or double edges. Therefore 2 has to connect to two more vertices 3 and 4 by single edges. There are two possibilities:

(131) there is a loop in 3,

(132) there is no loop in 3.

(131) There is a loop in 3. There must be a loop in 4 as well and $G$ is isomorphic to $H_1$.

(132) There is no loop in 3. Then 3 and 4 must be connected by the double edge. The graph $G$ is isomorphic to $H_3$.

(2) $G$ has no loops but has a triple edge. Then two vertices 1 and 2 are triply connected and no further extension is possible. The graph $G$ is isomorphic to the dipole graph $D_3$.

(3) $G$ has no loops or triple edges but has a double edge. Assume that the vertex 1 has a double edge to the vertex 2 and consequently a single edge to another vrtex 3. There are two possibilities:

(31) there is an edge connecting vertices 2 and 3,

(32) there is no such edge.

(31) There is an edge connecting vertices 2 and 3. The edge must be a single one since 2 is connected to 1 by the double edge. Then 3 must be connected to the only remaining vertex 4 by the single edge. But then the vertex 4 must have a loop which contradicts assumption (3).

(32) There is no edge connecting 2 and 3. Since no loops are alowed, 2 must be singly and 3 doubly connected to 4. The graph $G$ is isomorphic to $H_4$.

(4) $G$ has no loops or multiple edges. Therefore 1 is singly connected to 2, 3 and 4. Since no loops or multiple edges are alowed, 2 must connect to both 3 and 4. Also, the 3 and 4 are connected and the graph $G$ is isomorphic to the graph $K_4$. □

We prove four usefull lemmas. They generalize Lemmas 8.1–8.4 from [7].

**Lemma 4.2.** *Let $a, b$ and $e$ be elements and $\sigma$ a permutation of a set $S$. A general solution to the equation*

$$\sigma F(a,b) = e \tag{1}$$

*on a set $S$ is given by:*

$$F(x,y) = \alpha L(\lambda x, \varrho y)$$

*where:*

- *$L$ is an arbitrary loop on $S$ with the identity $e$,*
- *$\alpha, \lambda$ and $\varrho$ are arbitrary permutations of $S$ such that: $\alpha = \sigma^{-1}$, $\lambda a = e$ and $\varrho b = e$.*

*Proof.* It is trivial to check that the above formulas always give a solution to the equation (1). Next, we prove that every solution to the equation (1) is of the form given in the statement of the Lemma.

Let $F$ be a particular quasigroup on $S$ which satisfies (1). Define $\alpha = \sigma^{-1}, \lambda x = \sigma F(x,b), \varrho x = \sigma F(a,x)$ and $L(x,y) = \sigma F(\lambda^{-1}x, \varrho^{-1}y)$. We see that $\lambda$ and $\varrho$ are permutations of $S$ such that $\lambda a = \varrho b = e$ and $F(x,y) = \alpha L(\lambda x, \varrho y)$. The operation $L$ is a quasigroup as an isotope of the quasigroup $F$. Moreover, it is a loop, as follows from: $L(e,x) = \sigma F(\lambda^{-1}e, \varrho^{-1}x) = \sigma F(a, \varrho^{-1}x) = \varrho\varrho^{-1}x = x$ and $L(x,e) = \sigma F(\lambda^{-1}x, \varrho^{-1}e) = \sigma F(\lambda^{-1}x, b) = \lambda\lambda^{-1}x = x$. □

**Lemma 4.3.** *Let $b$ be an element and $\gamma, \sigma$ and $\tau$ permutations of a set $S$. A general solution to the equation*

$$\sigma F(\gamma x, b) = \tau x \tag{2}$$

*on a set $S$ is given by:*

$$F(x,y) = \alpha L(\lambda x, \varrho y)$$

*where:*

- *$L$ is an arbitrary loop on $S$ with the identity $e$,*
- *$\alpha, \lambda$ and $\varrho$ are arbitrary permutations of $S$ such that: $\alpha = \sigma^{-1}$, $\lambda\gamma = \tau$ and $\varrho b = e$.*

*Proof.* It is easy to check that the above formulas always give a solution to the equation (2).

Assume that a quasigroup $F$ is a solution of (2). We are proving that $F$ must be of the form indicated in the statement of the Theorem.

Take $a \in S$ and define $e = \tau a, \alpha = \sigma^{-1}, \lambda x = \sigma F(x, b), \varrho x = \sigma F(\gamma a, x)$. Operations $\alpha, \lambda$ and $\varrho$ are permutations such that $\lambda\gamma x = \sigma F(\gamma x, b) = \tau x$ and $\varrho b = \sigma F(\gamma a, b) = \tau a = e$.

Define a quasigroup $L$ by $L(u, v) = \alpha^{-1}F(\lambda^{-1}u, \varrho^{-1}v)$. We have $L(e, x) = \alpha^{-1}F(\lambda^{-1}e, \varrho^{-1}x) = \sigma F(\gamma\tau^{-1}e, \varrho^{-1}x) = \sigma F(\gamma a, \varrho^{-1}x) = \varrho\varrho^{-1}x = x$ and $L(x, e) = \alpha^{-1}F(\lambda^{-1}x, \varrho^{-1}e) = \sigma F(\lambda^{-1}x, b) = \lambda\lambda^{-1}x = x$ proving that $L$ is a loop with the identity $e$. □

By duality we have:

**Lemma 4.4.** *Let $a$ be an element and $\delta, \sigma$ and $\tau$ permutations of a set $S$. A general solution to the equation*

$$\sigma F(a, \delta x) = \tau x \tag{3}$$

*on a set $S$ is given by:*

$$F(x, y) = \alpha L(\lambda x, \varrho y)$$

*where:*

- *$L$ is an arbitrary loop on $S$ with the identity $e$,*
- *$\alpha, \lambda$ and $\varrho$ are arbitrary permutations of $S$ such that: $\alpha = \sigma^{-1}$, $\lambda a = e$ and $\varrho\delta = \tau$.*

**Lemma 4.5.** *Let $e$ be an element and $\gamma, \delta$ and $\sigma$ permutations of a set $S$. A general solution to the equation*

$$\sigma F(\gamma x, \delta x) = e \tag{4}$$

*on a set $S$ is given by:*

$$F(x, y) = \alpha L^{(23)}(\lambda x, \varrho y)$$

*where:*

- *$L$ is an arbitrary loop on $S$ with the identity $e$,*
- *$\alpha, \lambda$ and $\varrho$ are arbitrary permutations of $S$ such that: $\sigma\alpha e = e$, $\lambda\gamma = \sigma$ and $\varrho\delta = \sigma$.*

*Proof.* Since $L$ is a loop, we have $L(x, e) = x$ i.e., $L^{-2}(x, x) = e$. Therefore $\sigma F(\gamma x, \delta x) = \sigma\alpha L^{-2}(\lambda\gamma x, \varrho\delta x) = \sigma\alpha L^{-2}(\sigma x, \sigma x) = \sigma\alpha e = e$ so $F$ satisfies (4).

Assume that a quasigroup $F$ is a particular solution of (4). Define $\alpha x = F(\gamma\sigma^{-1}e, \delta\sigma^{-1}x)$. The function $\alpha$ is a permutation and $\sigma\alpha e = \sigma F(\gamma\sigma^{-1}e, \delta\sigma^{-1}e) = e$.

Define also $\lambda = \sigma\gamma^{-1}$ and $\varrho = \sigma\delta^{-1}$. It follows that $\lambda\gamma = \sigma$ and $\varrho\delta = \sigma$.

If a quasigroup $L$ is defined by $L(u, v) = \varrho F^{-2}(\lambda^{-1}u, \alpha v)$ then $F(x, y) = \alpha L^{-2}(\lambda x, \varrho y)$, $L(e, x) = \varrho F^{-2}(\lambda^{-1}e, \alpha x) = \varrho F^{-2}(\lambda^{-1}e, F(\lambda^{-1}e, \varrho^{-1}x)) =$

$\varrho\varrho^{-1}x = x$ and $L(x,e) = \varrho F^{-2}(\lambda^{-1}x, \alpha e) = \varrho F^{-2}(\lambda^{-1}x, F(\lambda^{-1}x, \varrho^{-1}x)) = \varrho\varrho^{-1}x = x$. Therefore $L$ is a loop. □

There are three equations corresponding to the graph $H_1$:

$$A(B(x,x), C(y,y)) = D(z,z),$$
$$A(x, B(C(y,y), D(z,z))) = x, \qquad A(B(C(x,x), D(y,y)), z) = z.$$

To reduce some space we shall not write appropriate generalized equations, as above, but the corresponding equations in the language with the single operation $\cdot$. So the three equations representing generalized equations which correspond to the graph $H_1$ are:

$$\boxed{xx.yy = zz} \qquad x(yy.zz) = x \qquad (xx.yy)z = z$$

One of the equations is also boxed, indicating the equation chosen to represent the whole PE–class. The distinguished equation is then written in full form and its solution is given in the following theorem. In this case the representative equation is:

$$A(B(x,x), C(y,y)) = D(z,z) \tag{5}$$

and the corresponding theorem is:

**Theorem 4.6.** *A general solution of the equation* (5) *on a set $S$ is given by:*

$$\begin{cases} A(x,y) = L(\lambda x, \varrho y) \\ B(x,y) = \lambda^{-1}U_2(x,y) \\ C(x,y) = \varrho^{-1}U_3(x,y) \\ D(x,y) = U_4(x,y) \end{cases}$$

*where:*

- *$L$ is an arbitrary loop on $S$ with an identity $e$,*
- *$U_i$ $(2 \leqslant i \leqslant 4)$ are arbitrary unipotent quasigroups with a common idempotent $e$,*
- *$\lambda$ and $\varrho$ are arbitrary permutations of $S$.*

*Proof.* 1) Let quasigroups $A, B, C, D$ be given by the formulas above. Then $A(B(x,x), C(y,y)) = L(B(x,x), C(y,y)) = L(\lambda\lambda^{-1}U_2(x,x), \varrho\varrho^{-1}U_3(y,y)) = L(e,e) = e = U_4(z,z) = D(z,z)$. Therefore a quadruple of such quasigroups is a solution to (5).

2) Let a quadruple of quasigroups $A, B, C, D$ be a solution to (5). Assume $p, q$ be arbitrary but fixed elements from $S$. Define $b = B(p,p), c = C(q,q)$ and $e = A(b,c)$. Fixing $x$ and $y$ in the equation yields $D(z,z) = e$. We can easily infer $B(x,x) = b$ and $C(y,y) = c$. From $A(b,c) = e$, by the Lemma 4.2, we find $A(x,y) = \alpha L(\lambda x, \varrho y)$ where $L$ is a loop on $S$ with an identity $e$ and $\alpha, \lambda, \varrho$ are permutations of $S$ such that $\alpha = \mathrm{Id}$ and $\lambda b = \varrho c = e$. But then $\lambda B(x,x) = \lambda b = e$ and if we define $U_2(x,y) = \lambda B(x,y)$ we get $B(x,y) = \lambda^{-1} U_2(x,y)$. We can define $U_3$ and $U_4$ similarly. □

The $\sim$–classes of (5) are all singletons.

The question arises as to why we use unipotent quasigroups to express the solutions to functional equations when the Theorem 3.4 stresses the role of loops, groups and/or Abelian groups. The reason is pure convenience since we could use loops instead of unipotent quasigroups. Namely, by the Lemma 4.5, for every unipotent quasigroup $U$ the quasigroup $U^{(23)}$ with the (unique) idempotent $e$ is a loop with the identity $e$, and conversely, if $L$ is a loop with the identity $e$, then the quasigroup $L^{(23)}$ is unipotent and has a unique idempotent $e$. The alternative general solution to (5) is then given in:

**Theorem 4.7.** *A general solution of the equation* (5) *on a set $S$ is given by:*

$$\begin{cases} A(x,y) = L(\lambda x, \varrho y) \\ B(x,y) = \lambda^{-1} L_2^{(23)}(x,y) \\ C(x,y) = \varrho^{-1} L_3^{(23)}(x,y) \\ D(x,y) = L_4^{(23)}(x,y) \end{cases}$$

*where:*

- *$L, L_2, L_3$ and $L_4$ are arbitrary loops on $S$ with an identity $e$,*
- *$\lambda$ and $\varrho$ are arbitrary permutations of $S$.*

Further on, we state only one version of the solution, the one using unipotent quasigroups.

There are 19 equations corresponding to the graph $H_2$:

$\boxed{x.yy = x.zz}$

$x(x.yy) = zz$

$(xx.y)y = zz$

$x.(y.zz)y = x$

$xx.(yy.z) = z$

$x(x.yy).z = z$

$xx.y = y.zz$

$x(yy.x) = zz$

$x.y(y.zz) = x$

$x.(yy.z)z = x$

$(x.yy).zz = x$

$x(yy.x).z = z$

$(xx.y)y.z = z$

$xx.y = zz.y$

$(x.yy)x = zz$

$x.y(zz.y) = x$

$xx.(y.zz) = y$

$(xx.y).zz = y$

$(x.yy)x.z = z$

The $\sim$–classes of operations are again singletons. The representative equation is

$$A(x, B(y, y)) = C(x, D(z, z)) \tag{6}$$

and its solution is given in the following theorem.

**Theorem 4.8.** *A general solution of the equation* (6) *on a set $S$ is given by:*

$$\begin{cases} A(x,y) = L_1(\lambda_1 x, \varrho_1 y) \\ B(x,y) = \varrho_1^{-1} U_2(x,y) \\ C(x,y) = L_3(\lambda_3 x, \varrho_3 y) \\ D(x,y) = \varrho_3^{-1} U_4(x,y) \end{cases}$$

*where:*

- $L_1$ *and* $L_3$ *are arbitrary loops on $S$ with a common identity $e$,*
- $U_2$ *and* $U_4$ *are arbitrary unipotent quasigroups on $S$ with a common idempotent $e$,*
- $\lambda_1, \varrho_1, \lambda_3$ *and* $\varrho_3$ *are arbitrary permutations of $S$ such that $\lambda_1 = \lambda_3$.*

*Proof.* 1) Let quasigroups $A, B, C, D$ be given by the formulas above. Then $A(x, B(y, y)) = L_1(\lambda_1 x, \varrho_1 \varrho_1^{-1} U_2(y, y)) = L_1(\lambda_1 x, e) = \lambda_1 x = \lambda_3 x = L_3(\lambda_3 x, e) = L_3(\lambda_3 x, \varrho_3 \varrho_3^{-1} U_4(z, z)) = C(x, D(z, z))$. Therefore the quadruple of such quasigroups is a solution to (6).

2) Let a quadruple of quasigroups $A, B, C, D$ be a solution to (6). Suppose that $p, q, r$ are arbitrary but fixed elements from $S$ and define $b = B(q, q), e = A(p, b), d = D(r, r)$. Fixing $x$ and $y$ we get $C(p, d) = e$.

Define also $\lambda_1 x = A(x, b), \varrho_1 x = A(p, x), \lambda_3 x = C(x, d)$ and $\varrho_3 x = C(p, x)$. The relation $\lambda_1 = \lambda_3$ immediately follows. The equation (6) reduces to the system: $A(x, b) = \lambda_3 x$, $\varrho_1 B(y, y) = e$, $C(x, d) = \lambda_1 x$, $\varrho_3 D(z, z) = e$.

By the Lemma 4.3 we can choose $A(x, y) = L_1(\lambda_1 x, \varrho_1 y)$ for some $L_1$. It is rather obvious that we have to take $L_1(u, v) = A(\lambda_1^{-1} u, \varrho_1^{-1} v)$. Since $\lambda_1$ and $\varrho_1$ are translations of $A$, the operation $L_1$ must be a loop with the identity $e$. Analogously, $C(x, y) = L_3(\lambda_3 x, \varrho_3 y)$ for a suitable loop $L_3$ with the identity $e$.

If we define $U_2(x, y) = \varrho_1 B(x, y)$ we get $U_2(x, x) = \varrho_1 b = e$ and $B(x, y) = \varrho_1^{-1} U_2(x, y)$. Similarly, $D(x, y) = \varrho_3^{-1} U_4(x, y)$ for a unipotent quasigroup $U_4$ with the idempotent $e$. □

There are 94 equations corresponding to the graph $H_3$.

$\boxed{x.xy = y.zz}$

$x.yy = z.zx$

$xy.x = y.zz$

$xx.y = zy.z$

$x(y.xy) = zz$

$x(y.zz) = yx$

$x(yy.z) = xz$

$xx.yz = zy$

$xy.zz = xy$

$(x.yx)y = zz$

$(xx.y)z = yz$

$(xy.y)x = zz$

$x.y(z.yz) = x$

$x.y(yz.z) = x$

$x(xy.zz) = y$

$x(yy.zx) = z$

$x.(x.yy)z = z$

$x.(y.zz)x = y$

$x.(yz.y)z = x$

$xx.(y.zy) = z$

$xx.(yz.y) = z$

$xy.(zz.y) = x$

$(x.yy).xz = z$

$(xx.y).zy = z$

$x(y.xy).z = z$

$x(y.zz).y = x$

$x(yy.z).x = z$

$(xx.yz)z = y$

$(xy.zz)x = y$

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

$(xx.y)z.y = z$

$x.yx = y.zz$

$xx.y = z.yz$

$xy.y = x.zz$

$xy.x = zz.y$

$x(y.yx) = zz$

$x(xy.y) = zz$

$x(yy.z) = zx$

$xy.xy = zz$

$xy.zz = yx$

$(x.yy)z = xz$

$(xx.y)z = zy$

$x.x(y.zz) = y$

$x.y(z.zy) = x$

$x.y(zy.z) = x$

$x(yx.zz) = y$

$x(yz.yz) = x$

$x.(y.yz)z = x$

$x.(yy.x)z = z$

$x.(yz.z)y = x$

$xy.(x.zz) = y$

$xx.(yz.z) = y$

$(x.xy).zz = y$

$(x.yy).zx = z$

$(xy.x).zz = y$

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

$x(xy.y).z = z$

$x(yy.z).z = x$

$(xy.xy)z = z$

$(xy.zz)y = x$

$(x.yy)z.x = z$

$(xx.y)z.z = y$

$(xy.y)x.z = z$

$x.yy = z.xz$

$xx.y = z.zy$

$xx.y = yz.z$

$xy.y = zz.x$

$x(y.zz) = xy$

$x(yx.y) = zz$

$xx.yz = yz$

$xy.yx = zz$

$(x.xy)y = zz$

$(x.yy)z = zx$

$(xy.x)y = zz$

$x.y(x.zz) = y$

$x.x(yy.z) = z$

$x.y(zz.x) = y$

$x(yy.xz) = z$

$x(yz.zy) = x$

$x.(y.zy)z = x$

$x.(yy.z)x = z$

$xx.(y.yz) = z$

$xy.(y.zz) = x$

$xy.(zz.x) = y$

$(x.yx).zz = y$

$(xx.y).yz = z$

$(xy.y).zz = x$

$x(y.zz).x = y$

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

$(xx.yz)y = z$

$(xy.yx)z = z$

$(x.xy)y.z = z$

$(x.yy)z.z = x$

$(xy.x)y.z = z$

In this case we have two $\sim$–classes which are singletons and one class with two elements. The representative equation is

$$A(x, B(x, y)) = C(y, D(z, z)) \tag{7}$$

and its solution is given in the following theorem.

**Theorem 4.9.** *A general solution of the equation* (7) *on a set $S$ is given by:*

$$\begin{cases} A(x,y) = L_1^{(23)}(\lambda_1 x, \varrho_1 y) \\ B(x,y) = \varrho_1^{-1} L_1(\lambda_2 x, \varrho_2 y) \\ C(x,y) = L_3(\lambda_3 x, \varrho_3 y) \\ D(x,y) = \varrho_3^{-1} U(x,y) \end{cases}$$

*where:*

- *$L_1$ and $L_3$ are arbitrary loops on $S$ with a common identity $e$,*
- *$U$ is an unipotent quasigroup with the idempotent $e$,*
- *$\lambda_1, \varrho_1, \lambda_2, \varrho_2, \lambda_3, \varrho_3$ are arbitrary permutations of $S$ such that $\lambda_1 = \lambda_2$ and $\varrho_2 = \lambda_3$.*

*Proof.* 1) Let quasigroups $A, B, C, D$ be given by the formulas above. Then $A(x, B(x,y)) = L_1^{(23)}(\lambda_1 x, \varrho\varrho^{-1} L_1(\lambda_2 x, \varrho_2 y)) = L_1^{(23)}(\lambda_2 x, L_1(\lambda_2 x, \varrho_2 y)) = \varrho_2 y = \lambda_3 y = L_3(\lambda_3 y, e) = L_3(\lambda_3 y, \varrho_3 \varrho_3^{-1} U(z,z)) = C(y, D(z,z))$. Therefore the quadruple of such quasigroups is a solution to (7).

2) Let a quadruple of particular quasigroups $A, B, C, D$ be a solution to (7). Let $p, q, r$ be arbitrary but fixed elements from $S$. Define $b = B(p,q), d = D(r,r)$ and $e = A(p,b)$. Fixing $x$ and $y$ in the equation yields $C(q,d) = e$. Define $A_2 x = A(p,x), B_1 x = B(x,q), B_2 x = B(p,x), C_1 x = C(x,d)$ and $C_2 x = C(q,x)$ and their various compositions: $\lambda_1 = \lambda_2 = A_2 B_1, \varrho_1 = A_2, \varrho_2 = A_2 B_2, \lambda_3 = C_1, \varrho_3 = C_2$. Equation (7) is equivalent to the system:

$$\begin{cases} A(x, B(x,y)) = \lambda_3 y \\ C(y,d) = \varrho_2 y \\ \varrho_3 D(z,z) = e\ . \end{cases}$$

Moreover, $\varrho_2 = \lambda_3$.

By the Lemma 4.2, there is a unipotent quasigroup $U$ such that $D(x,y) = \varrho_3 U(x,y)$ with a unipotent $e$. Also, by the Lemma , there is a loop $L_3$ with the identity $e$ such that $C(x,y) = L_3(\lambda_3 x, \varrho_3 y)$. If we define a quasigroup $L_1$ by $L_1(u,v) = A^{(23)}(\lambda_1 u, \varrho_1 v)$, then it is a loop with the identity $e$ and $A(x,y) = L_1^{(23)}(\lambda_1 x, \varrho_1 y), B(x,y) = \varrho_1 L_1(\lambda_2 x, \varrho_2 y)$.

The rest of the requirements of the Theorem are satisfied too, which completes the proof. □

There are 114 equations corresponding to the graph $H_4$.

$$\begin{array}{rrr}
x.xy = z.yz & x.xy = z.zy & x.yx = z.yz \\
x.yx = z.zy & \boxed{x.yz = x.yz} & x.yz = x.zy \\
xy.x = z.yz & xy.x = z.zy & xy.y = z.xz \\
xy.y = z.zx & xy.z = z.xy & xy.z = z.yx \\
xy.x = yz.z & xy.x = zy.z & xy.y = xz.z \\
xy.y = zx.z & xy.z = xy.z & xy.z = yx.z \\
x(x.yz) = yz & x(x.yz) = zy & x(y.yz) = xz \\
x(y.yz) = zx & x(y.zy) = xz & x(y.zy) = zx \\
x(yz.x) = yz & x(yz.x) = zy & x(yz.y) = xz \\
x(yz.y) = zx & x(yz.z) = xy & x(yz.z) = yx \\
(x.xy)z = yz & (x.xy)z = zy & (x.yx)z = yz \\
(x.yx)z = zy & (x.yz)x = yz & (x.yz)x = zy \\
(xy.x)z = yz & (xy.x)z = zy & (xy.y)z = xz \\
(xy.y)z = zx & (xy.z)z = xy & (xy.z)z = yx \\
x.x(y.yz) = z & x.x(y.zy) = z & x.y(y.xz) = z \\
x.y(y.zx) = z & x.y(z.xz) = y & x.y(z.zx) = y \\
x.x(yz.y) = z & x.x(yz.z) = y & x.y(xz.y) = z \\
x.y(xz.z) = y & x.y(zx.y) = z & x.y(zx.z) = y \\
x.(y.xy)z = z & x.(y.xz)y = z & x.(y.yx)z = z \\
x.(y.yz)x = z & x.(y.zx)y = z & x.(y.zy)x = z \\
x.(xy.y)z = z & x.(xy.z)z = y & x.(yx.y)z = z \\
x.(yx.z)z = y & x.(yz.y)x = z & x.(yz.z)x = y \\
xy.(z.xy) = z & xy.(z.xz) = y & xy.(z.yx) = z \\
xy.(z.yz) = x & xy.(z.zx) = y & xy.(z.zy) = x \\
xy.(xy.z) = z & xy.(xz.z) = y & xy.(yx.z) = z \\
xy.(yz.z) = x & xy.(zx.z) = y & xy.(zy.z) = x \\
(x.xy).yz = z & (x.xy).zy = z & (x.yx).yz = z \\
(x.yx).zy = z & (x.yz).yz = x & (x.yz).zy = x \\
(xy.x).yz = z & (xy.x).zy = z & (xy.y).xz = z \\
(xy.y).zx = z & (xy.z).xy = z & (xy.z).yx = z \\
x(x.yz).y = z & x(x.yz).z = y & x(y.yz).x = z \\
x(y.yz).z = x & x(y.zy).x = z & x(y.zy).z = x \\
x(yz.x).y = z & x(yz.x).z = y & x(yz.y).x = z \\
x(yz.y).z = x & x(yz.z).x = y & x(yz.z).y = x \\
(x.xy)z.y = z & (x.xy)z.z = y & (x.yx)z.y = z \\
(x.yx)z.z = y & (x.yz)x.y = z & (x.yz)x.z = y \\
(xy.x)z.y = z & (xy.x)z.z = y & (xy.y)z.x = z \\
(xy.y)z.z = x & (xy.z)z.x = y & (xy.z)z.y = x
\end{array}$$

There are two $\sim$–classes with two elements each. The representative equation is

$$A(x, B(y, z)) = C(x, D(y, z)) \tag{8}$$

and its solution is given in the following theorem.

**Theorem 4.10.** *A general solution of the equation* (8) *on a set* $S$ *is given by:*

$$\begin{cases} A(x, y) = L_1(\lambda_1 x, \varrho_1 y) \\ B(x, y) = \varrho_1^{-1} L_2(\lambda_2 x, \varrho_2 y) \\ C(x, y) = L_1(\lambda_3 x, \varrho_3 y) \\ D(x, y) = \varrho_3^{-1} L_2(\lambda_4 x, \varrho_4 y) \end{cases}$$

*where:*

- $L_1$ *and* $L_2$ *are arbitrary loops on* $S$ *with a common unit* $e$,
- $\lambda_1, \varrho_1, \lambda_2, \varrho_2, \lambda_3, \varrho_3, \lambda_4, \varrho_4$ *are arbitrary permutations of* $S$ *such that* $\lambda_1 = \lambda_3$, $\lambda_2 = \lambda_4$, $\varrho_2 = \varrho_4$.

*Proof.* 1) Let quasigroups $A, B, C$ and $D$ be given by the formulas above. Then

$$\begin{aligned} A(x, B(y, z)) &= L_1(\lambda_1 x, \varrho_1 \varrho_1^{-1} L_2(\lambda_2 y, \varrho_2 z)) \\ &= L_1(\lambda_3 x, \varrho_3 \varrho_3^{-1} L_2(\lambda_4 y, \varrho_4 z)) = C(x, D(y, z)) \end{aligned}$$

and the quadruple $A, B, C, D$ is a solution to (8).

2) Let a quadruple $A, B, C, D$ of quasigroups be a solution to (8) and $p, q, r$ arbitrary fixed elements from $S$. Define $b = B(q, r)$, $e = A(p, b)$ and $d = D(q, r)$. It follows that $C(p, d) = e$.

Define also $\lambda_1 x = A(x, b)$, $\varrho_1 x = A(p, x)$, $\lambda_2 x = \varrho_1 B(x, r)$, $\varrho_2 x = \varrho_1 B(q, x)$, $\lambda_3 x = C(x, d)$, $\varrho_3 x = C(p, x)$, $\lambda_4 x = \varrho_3 D(x, r)$, and $\varrho_4 x = \varrho_3 D(q, x)$. It follows that $\lambda_1 x = A(x, b) = A(x, B(q, r)) = C(x, D(q, r)) = C(x, d) = \lambda_3 x$ and $\lambda_2 y = \varrho_1 B(y, r) = A(p, B(y, r)) = C(p, D(y, r)) = \varrho_3 D(y, r) = \lambda_4 y$. Analogously $\varrho_2 z = \varrho_4 z$.

Let us define quasigroups $L_1(u, v) = A(\lambda_1^{-1} u, \varrho_1^{-1} v)$ and $L_2(u, v) = \varrho_1 B(\lambda_2^{-1} u, \varrho_2^{-1} v)$. It is easy to check that $L_1$ and $L_2$ are both loops with a common identity $e$. Trivially $A(x, y) = L_1(\lambda_1 x, \varrho_1 y)$ and $B(x, y) = \varrho_1^{-1} L_2(\lambda_2 x, \varrho_2 y)$. Also $C(x, \varrho_3^{-1} \lambda_4 y) = C(x, \varrho_3^{-1} \varrho_3 D(y, r)) = C(x, D(y, r))$ $= A(x, B(y, r)) = A(x, \varrho_1^{-1} \varrho_1 B(y, r)) = A(x, \varrho_1^{-1} \lambda_2 y) = L_1(\lambda_1 x, \varrho_1 \varrho_1^{-1} \lambda_2 y)$ $= L_1(\lambda_3 x, \varrho_3 \varrho_3^{-1} \lambda_4 y)$. Consequently $C(x, y) = L_1(\lambda_3 x, \varrho_3 y)$.

Finally, $D(y, z) = \varrho_3^{-1} \varrho_3 D(y, z) = \varrho_3^{-1} C(p, D(y, z)) = \varrho_3^{-1} A(p, B(y, z))$ $= \varrho_3^{-1} \varrho_1 B(y, z) = \varrho_3^{-1} L_2(\lambda_2 y, \varrho_2 z) = \varrho_3^{-1} L_2(\lambda_4 y, \varrho_4 z)$. □

There are 100 equations corresponding to the graph $K_4$.

$$\begin{array}{rrr}
x.yz = y.xz & x.yz = y.zx & x.yz = z.xy \\
x.yz = z.yx & \boxed{xy.z = x.yz} & xy.z = x.zy \\
xy.z = y.xz & xy.z = y.zx & xy.z = xz.y \\
xy.z = yz.x & xy.z = zx.y & xy.z = zy.x \\
x(y.xz) = yz & x(y.xz) = zy & x(y.zx) = yz \\
x(y.zx) = zy & x(xy.z) = yz & x(xy.z) = zy \\
x(yx.z) = yz & x(yx.z) = zy & xy.xz = yz \\
xy.xz = zy & xy.yz = xz & xy.yz = zx \\
xy.zx = yz & xy.zx = zy & xy.zy = xz \\
xy.zy = zx & (x.yz)y = xz & (x.yz)y = zx \\
(x.yz)z = xy & (x.yz)z = yx & (xy.z)x = yz \\
(xy.z)x = zy & (xy.z)y = xz & (xy.z)y = zx \\
x.y(x.yz) = z & x.y(x.zy) = z & x.y(z.xy) = z \\
x.y(z.yx) = z & x.y(xy.z) = z & x.y(yx.z) = z \\
x.y(yz.x) = z & x.y(zy.x) = z & x(xy.yz) = z \\
x(xy.zy) = z & x(yx.yz) = z & x(yx.zy) = z \\
x(yz.xy) = z & x(yz.xz) = y & x(yz.yx) = z \\
x(yz.zx) = y & x.(x.yz)y = z & x.(x.yz)z = y \\
x.(y.xz)z = y & x.(y.zx)z = y & x.(xy.z)y = z \\
x.(yx.z)y = z & x.(yz.x)y = z & x.(yz.x)z = y \\
xy.(x.yz) = z & xy.(x.zy) = z & xy.(y.xz) = z \\
xy.(y.zx) = z & xy.(xz.y) = z & xy.(yz.x) = z \\
xy.(zx.y) = z & xy.(zy.x) = z & (x.yz).xy = z \\
(x.yz).xz = y & (x.yz).yx = z & (x.yz).zx = y \\
(xy.z).xz = y & (xy.z).yz = x & (xy.z).zx = y \\
(xy.z).zy = x & x(y.xz).y = z & x(y.xz).z = y \\
x(y.zx).y = z & x(y.zx).z = y & x(xy.z).y = z \\
x(xy.z).z = y & x(yx.z).y = z & x(yx.z).z = y \\
(xy.xz)y = z & (xy.xz)z = y & (xy.yz)x = z \\
(xy.yz)z = x & (xy.zx)y = z & (xy.zx)z = y \\
(xy.zy)x = z & (xy.zy)z = x & (x.yz)y.x = z \\
(x.yz)y.z = x & (x.yz)z.x = y & (x.yz)z.y = x \\
(xy.z)x.y = z & (xy.z)x.z = y & (xy.z)y.x = z \\
 & (xy.z)y.z = x &
\end{array}$$

There is just one $\sim$–class with four elements. The representative equation is

$$A(B(x,y),z) = C(x,D(y,z)) \tag{9}$$

and its solution is given in the following theorem.

**Theorem 4.11** (Aczél, Belousov, Hosszú [1]). *A general solution of the generalized associativity equation* (9) *on a set $S$ is given by:*

$$\begin{cases} A(x,y) = \lambda_1 x \cdot \varrho_1 y \\ B(x,y) = \lambda_1^{-1}(\lambda_2 x \cdot \varrho_2 y) \\ C(x,y) = \lambda_3 x \cdot \varrho_3 y \\ D(x,y) = \varrho_3^{-1}(\lambda_4 x \cdot \varrho_4 y) \end{cases}$$

*where:*

- $\cdot$ *is an arbitrary group on $S$,*
- $\lambda_1, \varrho_1, \lambda_2, \varrho_2, \lambda_3, \varrho_3, \lambda_4, \varrho_4$ *are arbitrary permutations of $S$ such that:* $\lambda_2 = \lambda_3, \quad \varrho_2 = \lambda_4, \quad \varrho_1 = \varrho_4.$

The results are summarized in the Table 1.

| PE–class | Graph | Number of $\sim$–classes | Number of equations | Representative equation |
|---|---|---|---|---|
| 1 | $H_1$ | 4 | 3 | (5) |
| 2 | $H_2$ | 4 | 19 | (6) |
| 3 | $H_3$ | 3 | 94 | (7) |
| 4 | $H_4$ | 2 | 114 | (8) |
| 5 | $K_4$ | 1 | 100 | (9) |

Table 1: Equations with 3 variables – summary

## References

[1] **J. Aczél, V. D. Belousov, M. Hosszú**, *Generalized associativity and bisymmetry on quasigroups*, Acta Math. Acad. Sci. Hungar. **11** (1960), 127 – 136.

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

[3] **O. Chein, H. O. Pflugfelder, J. D. H. Smith**, *Quasigroups and Loops: Theory and Applications*, Sigma Series in Pure Math. 9, Heldermann Verlag, Berlin, 1990.

[4] **J. Duplák**, *Identities and deleting maps on quasigroups*, Czech. Math. J. **38**(113) (1988), 1 – 7.

[5] **R. F. Koval'**, *Classification of quadratic parastrophically uncancellable functional equations for five object variables on quasigroups*, Ukrainian Math. J. **57** (2005), 1249 – 1261 (translation from Ukrain. Mat. Zh. **57** (2005), 1058 – 1068).

[6] **A. Krapež, S. K. Simić, D. V. Tošić**, *Parastrophically uncancellable quasigroup equations*, Aequationes Math. (in print)

[7] **A. Krapež, D. Živković**, *Parastrophically equivalent quasigroup equations*, submitted.

[8] **S. Krstić**, *Quadratic quasigroup identities*, (Serbocroatian), PhD thesis, University of Belgrade, 1985.

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

[10] **F. M. Sokhats'kyi**, *On the classification of functional equations on quasigroups*, Ukrainian Math. J. **56** (2004), 1499 – 1508 (translation from Ukrain. Mat. Zh. **56** (2004), 1259 – 1266).

Received May 14, 2009

Mathematical Institute of the Serbian Academy of Sciences and Arts,
Knez Mihailova 36, 11001 Belgrade, Serbia
E-mail: sasa@mi.sanu.ac.rs

Quasigroups and Related Systems **17** (2009), 271 – 282

# New primitives for digital signature algorithms

*Nikolay A. Moldovyan and Peter A. Moldovyanu*

**Abstract.** Particular types of the multiplication operation over elements of the finite vector space over the field $GF(p^d)$, $d \geqslant 1$, are introduced so that there are formed the finite fields $GF\left((p^d)^m\right)$ with fast multiplication operation that also suites well to parallelized implementation. Finite fields implemented in such form are proposed for accelerating the digital signature algorithms.

## 1. Introduction

The finite fields (FFs) $GF(p)$ and $GF(p^d)$ represented by rings $Z_p$, where $p$ is a prime, and polynomials, correspondingly, are well studied as primitives for the digital signature (DS) algorithms design [8, 11, 13].

Finding discrete logarithm (DL) in a subgroup of the multiplicative group of the FF is used as the hard computational problem put into the base of the DS algorithms (DSAs).

The upper security boundary of such DSAs is limited by the difficulty of the DL problem in the used FF. There are known the general-purpose methods for solving the DL, which work in arbitrary groups [8]. Such methods have exponential complexity $W = O(\sqrt{q})$, where $O(\cdot)$ is the order notation, and $q$ is the largest prime divisor of the group order. If $q \geqslant 2^{160}$, then the general methods are impracticable, i.e., computationally infeasible. However in the case of the mentioned above FFs some particular methods for solving the DL problem can be applied, which have sub-exponential complexity.

Therefore the DSAs based on computations in the ground FFs $GF(p)$ and in the polynomial FFs fields $GF(p^d)$ satisfy the minimum security requirement (difficulty of the best attack should be equal to $\geqslant 2^{80}$ exponentiation operations in the used FF), if the size of the FF order is greater or equal to 1024 bits [4]. This fact restricts significantly the performance of

2000 Mathematics Subject Classification: 11G20, 11T71
Keywords: Cryptography, digital signature, vector space, finite field.

the known DSAs based on computations in the FFs $GF(p)$ and $GF(p^d)$. Higher performance is provided by the DSA using the computations in the finite groups of the elliptic curve (EC) points, while the EC are defined over FFs the size order of which equals 160 to 320 bits [5, 9].

The complexity of the point addition operation is defined by the complexity of the multiplication operation in the underlying FF. However in many cases of the practical use of DSAs there are required the DS schemes providing higher performance in hardware and in software. To meet such requirements there have been proposed different approaches to accelerating the EC-based cryptographic algorithms [9, 7].

These approaches can be categorized into two groups: i) high-level algorithm that manage the ECs selection and ii) low-level algorithm that manage the FF operation. Especially much attention in these researches is paid to the EC-based algorithms implementation using the FFs $GF(2^d)$, $GF\left(\left(2^d\right)^s\right)$, and $GF(p^d)$, because of their efficiency in hardware implementation [1, 2, 3].

However in the both approaches few attention is paid to accelerating the EC-based DSAs with parallelization of the multiplication in the underlying FF. Actually, in these approaches there are used the ground or polynomial FFs in which the multiplication operation involves arithmetic division by a prime or by an irreducible polynomial, respectively.

In present paper it is proposed a particular form of the FFs implementation, called vector FFs, providing possibility of efficient parallelization of the multiplication operation.

Besides, in the proposed particular form of the extension FFs $GF(p^{m'})$ the multiplication complexity is lower than in the ground FFs $GF(p')$ and in polynomial FFs $GF(p^d)$ for the same size of the FF order. The vector FFs are proposed to implement ECs providing faster DSAs.

The rest of the paper is organized as follows. In Section 2, the multiplication operation in the finite vector spaces over the FFs $GF(p^d)$ is defined using so called basis vector multiplication tables (BVMTs). This particular method allows one to define only a particular subclass of all possible variants of the associative multiplication. However this subclass includes the multiplication variants for which the vector space represents a field.

Section 3 provides comparison of the computational efficacy of the multiplication operation in FFs implemented in different forms. Section 4 concludes the paper.

In the paper the following specific term is used:

The *$k$-th power element $a$ of the field* $GF(p^d)$ is an element of the field $GF(p^d)$ for which the equation $x^k = a$ has solutions in the field $GF(p^d)$, $d \geqslant 1$.

## 2. Extension of finite fields in the vector form

The vector form of the extension FFs implementation represents significant interest for the applied cryptography due to lower complexity of the multiplication and possibility to efficient parallelization. This form of the implementation of the extension FFs is introduced using some subclass of possible associative multiplications in finite vector spaces over the FF $GF(p^d)$, where $d \geqslant 1$. The multiplication operation is introduced with BVMT.

This particular method is sufficiently simple and provides possibility to define vector FFs $GF\left((p^d)^m\right)$ for arbitrary value of $m$.

The vector FFs can be defined with BVMT not for all possible triples $m$, $p$, and $d$, though. However the proposed method suites well for defining the vector FFs oriented to application in the applied cryptography.

### 2.1. Addition and multiplication operations in finite vector spaces

Let us consider the set of the $m$-dimension vectors

$$a\mathbf{e} + b\mathbf{i} + \cdots + c\mathbf{j},$$

where $\mathbf{e}$, $\mathbf{i}$, … $\mathbf{j}$ are some formal basis vectors and $a, b, \ldots c \in GF(p^d)$, $d \geqslant 1$, are coordinates. Vector can be also represented as a set of its coordinates $(a, b, \ldots, c)$.

The terms $\epsilon\mathbf{v}$, where $\epsilon \in GF(p^d)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \ldots, \mathbf{j}\}$, are called components of the vector.

The addition of two vectors $(a, b, \ldots, c)$ and $(x, y, \ldots, z)$ is defined in the usual way as follows

$$(a, b, \ldots, c) + (x, y, \ldots, z) = (a + x, b + y, \ldots, c + z),$$

where "+" denotes addition operation in the field $GF(p^d)$. It is easy to see that the first representation of the vectors can be interpreted as sum of the vector components.

The multiplication of the vectors $(a, b, \dots, c)$ and $(x, y, \dots, z)$ is defined analogously to multiplication of polynomials, i.e., it is defined with the formula

$$
\begin{gathered}
(a\mathbf{e} + b\mathbf{i} + \dots + c\mathbf{j}) \cdot (x\mathbf{e} + y\mathbf{i} + \dots + z\mathbf{j}) = \\
= ax\mathbf{e}\cdot\mathbf{e} + bx\mathbf{i}\cdot\mathbf{e} + \dots + cx\mathbf{j}\cdot\mathbf{e} + ay\mathbf{e}\cdot\mathbf{i} + by\mathbf{i}\cdot\mathbf{i} + \dots + cy\mathbf{j}\cdot\mathbf{i} + \dots \\
\dots + az\mathbf{e}\cdot\mathbf{j} + bz\mathbf{i}\cdot\mathbf{j} + \dots + cz\mathbf{j}\cdot\mathbf{j},
\end{gathered}
$$

where $gh$ denotes multiplication of the elements $g \in GF(p^d)$ and $h \in GF(p^d)$. See [12] for more details.

In the final expression each product of two basis vectors is replaced by a vector component $\epsilon\mathbf{v}$ ($\epsilon \in GF(p^d)$) in accordance with some given tables called basis-vector multiplication tables (BVMT).

For example, if the used BVMT defines $\mathbf{i}\cdot\mathbf{j} = \epsilon\mathbf{e}$, then $bz\mathbf{i}\cdot\mathbf{j} = \epsilon bz\mathbf{e}$. The coordinate $\epsilon$ is called the expansion coefficient. The BVMT defines the concrete variant of the multiplication in the finite vector space.

It is easy to see, if the BVMT defines commutative and associative multiplication of the basis vectors, then the multiplication in the finite vector space is also commutative and associative. In this case the finite vector space is a commutative ring. In some particular cases the finite vector rings are FFs $GF\left((p^d)^m\right)$, called vector FFs.

Below there are shown constructions of the vector FFs for diffrent values $m$. For the case $m = 2$ the construction of the vector FF $GF\left((p^d)^2\right)$ is sufficiently close to construction with attaching the root of the irreducible (in $GF(p^d)$) polynomial $x^2 - \epsilon$ to $GF(p^d)$.

Principally for all values $m$ the FFs $GF\left((p^d)^m\right)$ can be constructed with the well known method using irreducible polynomials in $GF(p^d)$, however this method constructs the extension FFs $GF\left((p^d)^m\right)$ as polynomial FFs in which the multiplication operation is more complex and suites less to parallelized implementation than multiplication in the FFs constructed with BVMTs.

Indeed, in the polynomial FFs the multiplication is performed as arithmetic multiplication of two polynomials and arithmetic division of the result by the irreducible polynomial, while the multiplication in the vector FFs is free of such division operation.

Actually, the BVMT-based construction method is less general, however it provides efficient and immediate practical way to construct vector FFs with fast multiplication for arbitrary values $m$.

### 2.2. Vector finite fields $GF\left((p^d)^2\right)$

In the case $m = 2$ the BVMT possessing commutativity and associativity can be described as follows

$$\mathbf{e} \cdot \mathbf{i} = \mathbf{i} \cdot \mathbf{e} = \mathbf{i}, \quad \mathbf{e} \cdot \mathbf{e} = \mathbf{e}, \quad \mathbf{i} \cdot \mathbf{i} = \epsilon \mathbf{e},$$

where different values $\epsilon \in GF(p^d)$ define different variants of the multiplication operation. Each of these variants defines a finite ring of the two-dimension vectors. See, also, [12].

Let us consider a nonzero element of the vector ring $Z = a\mathbf{e} + b\mathbf{i}$. The element $Z^{-1} = x\mathbf{e} + y\mathbf{i}$ is called inverse of $Z$, if $Z^{-1}Z = \mathbf{e} = (1, 0)$, where 1 and 0 are the identity and zero elements in $GF(p^d)$.

In accordance with the multiplication definition we can write

$$Z^{-1}Z = (ax + \epsilon by)\mathbf{e} + (bx + ay)\mathbf{i} = 1\mathbf{e} + 0\mathbf{i}.$$

For given $(a, b)$ there exists a pair $(x, y)$ satisfying the last equation, if

$$a^2 - \epsilon b^2 \neq 0.$$

The last condition holds for all vectors $(a, b)$, except (0,0), if $\epsilon$ is a quadratic non-residue in the field $GF(p^d)$. In this case the vector space is a field $GF\left((p^d)^m\right)$.

If the vector space is defined over a ground field $GF(p)$, then we have the vector finite field $GF(p^2)$ the multiplicative group of which has the order $\Omega = p^2 - 1 = (p - 1)(p + 1)$.

If $\epsilon$ is a quadratic residue in the field $GF(p^d)$, where $d = 1$, then the characteristic equation $a^2 - \epsilon b^2 = 0$ is satisfied for each value $b \in 1, 2, \ldots, p - 1$ at two different values $a$. In this case we have a finite group in the vector space. The group order is equal to

$$\Omega = p^2 - 2(p - 1) - 1 = (p - 1)^2.$$

**Example 1.** For $p = 101$ and $\epsilon = 32$ (quadratic non-residue mod 101) the vector $93\mathbf{e} + 24\mathbf{i}$ has the order $\omega = 10200$ and is a primitive element of the multiplicative group of the field $GF(101^2)$. For $p = 101$ and $\epsilon = 31$ (quadratic residue mod 101) the vector $2\mathbf{e} + 3\mathbf{i}$ has the order $\omega = 100$, the last value being the maximum possible element order in the non-cyclic finite vector group having the order $\Omega = 10000$.

### 2.3. Vector finite fields $GF\left((p^d)^3\right)$

In the case $m = 3$ the general representation of the BVMT possessing commutativity and associativity is shown in Table 1, where $\mu \in GF(p^d)$ and $\epsilon \in GF(p^d)$ are the expansion coefficients. In accordance with the multiplication operation defined by Table 1 for vectors $Z = a\mathbf{e} + b\mathbf{i} + c\mathbf{k}$ and $X = x\mathbf{e} + y\mathbf{i} + z\mathbf{k}$ we can write

$$ZX = (ax+\epsilon\mu cy+\epsilon\mu bz)\mathbf{e}+(bx+ay+\mu cz)\mathbf{i}+(cx+\epsilon by+az)\mathbf{j} = 1\mathbf{e}+0\mathbf{i}+0\mathbf{j}.$$

If the last equation has solution relatively unknown $X$ for all nonzero vectors $Z$, then the vector space will be a vector finite field $GF\left((p^d)^3\right)$. From the last equation the following system of equations can be derived

$$\begin{cases} ax + \epsilon\mu cy + \epsilon\mu bz &= 1 \\ bx + ay + \mu cz &= 0 \\ cx + \epsilon by + az &= 0. \end{cases}$$

From this system the following characteristic equation can be get

$$a^3 - (3\epsilon\mu bc)\,a + \left(\epsilon^2\mu b^3 + \epsilon\mu^2 c^3\right) = 0 \qquad (1)$$

Denoting $B = (\epsilon^2\mu b^3 + \epsilon\mu^2 c^3)/2$ and using the well known formulas [6] for cubic equation roots we get the expression for the equation (1) roots $a$ in the following form

$$a = A' + A'', \quad \text{where,}$$

$$A' = \sqrt[3]{B + \sqrt{B^2 - (\epsilon\mu bc)^3}} = \sqrt[3]{-\epsilon\mu^2 c^3},$$

$$A'' = \sqrt[3]{B - \sqrt{B^2 - (\epsilon\mu bc)^3}} = \sqrt[3]{-\epsilon^2\mu b^3}.$$

Thus, if both of the values $\epsilon\mu^2$ and $\epsilon^2\mu$ are not the 3rd-power elements in the field $GF(p^d)$, then the characteristic equation (1) has no solutions relatively unknown $a$ for all possible pairs $(a, b)$, except $(a, b) = (0, 0)$. In this case the vector space is a field $GF\left((p^d)^3\right)$.

| $\cdot$ | $\overrightarrow{e}$ | $\overrightarrow{\imath}$ | $\overrightarrow{\jmath}$ |
|---|---|---|---|
| $\overrightarrow{e}$ | $\mathbf{e}$ | $\mathbf{i}$ | $\mathbf{j}$ |
| $\overrightarrow{\imath}$ | $\mathbf{i}$ | $\epsilon\mathbf{j}$ | $\mu\epsilon\mathbf{e}$ |
| $\overrightarrow{\jmath}$ | $\mathbf{j}$ | $\mu\epsilon\mathbf{e}$ | $\mu\mathbf{i}$ |

Table 1. The BVMT in the general case for $m = 3$.

In the case of the vector space defined over a ground field $GF(p)$ the analysis of the characteristic equation leads to the following cases.

CASE 1. The value $p$ is such that 3 does not divide $p-1$. Then each nonzero element of the field $GF(p)$ is the 3rd-power element and only for $\Omega = (p-1)^2(p+1)$ different vectors there exist inverses and we have non-cyclic finite vector group having order $\Omega$. Experiment has shown the maximum vector order is $\omega = (p-1)(p+1)$. In this case the finite vector spaces are not fields.

CASE 2. The value $p$ is such that $3|p-1$. This case is divided into the following two cases.

CASE 2A. Each of the products $\epsilon^2\mu$ and $\epsilon\mu^2$ is not a 3rd-power element in the field $GF(p)$. Then for each nonzero vector $Z$ there exists its inverses and the vector space is a field $GF(p^3)$ multiplicative group of which has the order $\Omega = p^3 - 1$. Selecting properly the prime value $p$ one can get prime $q|\Omega$ such that $q = \frac{1}{3}(p^2+p+1)$. Thus, in the case of the field formation in the finite vector spaces it is possible to get vector subgroups of the prime order that has the size significantly larger that the size of the $GF(p)$ field order. Such cases are very interesting for designing fast DSAs.

CASE 2B. Each of the products $\epsilon^2\mu$ and $\epsilon\mu^2$ is a 3rd-power element in $GF(p)$. In this case only for $\Omega = (p-1)^3$ different vectors there exist inverses and we have non-cyclic finite vector group having order $\Omega$. The maximum vector order is $\Omega = (p-1)$ (experimental result).

CASE 3. For $\epsilon = 0$ and $\mu \neq 0$ or for $\epsilon \neq 0$ and $\mu = 0$, or for $\epsilon = 0$ and $\mu = 0$ we have degenerative case, when the characteristic equation has the form $a^3 \equiv 0 \bmod p$ and unique solution $a = 0$ for all pair of the values $(b, c)$. In this case the vector space contains a vector group of the order $\Omega = p^2(p-1)$. This group is non-cyclic and the maximum vector order is $\Omega = p(p-1)$ (experiment).

**Example 2.** Suppose $p = 67$ (i.e., $3|p-1$). Then for $\mu = 1$, and $\epsilon = 0$ there is formed a vector group of the order $\Omega = p^2(p-1) = 296274$, in which the maximum vector order is $\omega = p(p-1) = 4422$. For $\mu = 1$ and $\epsilon = 60$ (this value is not the 3rd-power element) the vector field is formed, in which there exist vectors having order $\omega = p^3 - 1 = 300762$. For $\mu = 1$ and $\epsilon = 1$ (this value is the 3rd-power element) there is formed the vector group of the order $\Omega = (p-1)^3 = 287496$, in which the maximum vector order is $\omega = p - 1 = 66$.

**Example 3.** Suppose $p = 63633348855432197$ (i.e., 3 does not divide $p-1$). Then for $\mu = 1$ and $\epsilon = 3$ there is formed the vector group having the order $\Omega = (p-1)^2(p+1)$. The maximum vector order is $\omega = (p-1)(p+1) = 404920308655713409597535566424680\,8$. For $\mu = 1$ and $\epsilon = 0$ there is formed a vector group having the order $\Omega = p^2(p-1)$, the maximum vector order being $\omega = p(p-1)$.

**Example 4.** Suppose $p = 16406161737685927$ (i.e., $3|p-1$). Then for $\mu = 1$ and $\epsilon = 3$ (this value is the 3rd-power element) there is formed a vector field $GF(p^3)$, containing vectors of the order equal to $\Omega = p^3 - 1 = 4415917651114920002684537723583440985579861692982$. Such vectors are primitive elements of the vector field $GF(p^3)$.

### 2.4. Formation of the vector finite fields in the case $m \geqslant 4$

Analysis of the cases $m = 2$ and $m = 3$ shows that vector fields are formed in the case $m|p^d - 1$, provided some of the expansion coefficients are not the $m$th-power elements in $GF(p^d)$. In this research it has been experimentally established that under such conditions, while using the BVMTs shown as Table 2 the vector fields are formed for $m = 4, 5, \ldots, 55$, if $m|p^d - 1$ and the equation $x^\tau = \epsilon$ has no solutions in $GF(p^d)$ for each divisor $\tau|m$, $\tau > 1$. It appears that for arbitrary $m$ there exists vector FFs defined over the field $GF(p^d)$ such that $m|p^d - 1$.

Our experiments have been stopped since we have estimated that the investigated cases cover the demands of the practical cryptography. To define formation of the $m$-dimension vector FF the BVMT should be properly designed and for given $m$ there exist a variety of different BVMTs, but in this paper the simplest variants of BVMTs have been used.

| $\cdot$ | $\overrightarrow{e}$ | $\overrightarrow{\imath}$ | $\overrightarrow{\jmath}$ | $\overrightarrow{k}$ | $\overrightarrow{u}$ | $\ldots$ | $\overrightarrow{w}$ |
|---|---|---|---|---|---|---|---|
| $\overrightarrow{e}$ | $\mathbf{e}$ | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ | $\mathbf{u}$ | $\ldots$ | $\mathbf{w}$ |
| $\overrightarrow{\imath}$ | $\mathbf{i}$ | $\epsilon\mathbf{j}$ | $\epsilon\mathbf{k}$ | $\epsilon\mathbf{u}$ | $\epsilon\ldots$ | $\epsilon\mathbf{w}$ | $\epsilon\mathbf{e}$ |
| $\overrightarrow{\jmath}$ | $\mathbf{j}$ | $\epsilon\mathbf{k}$ | $\epsilon\mathbf{u}$ | $\epsilon\ldots$ | $\epsilon\mathbf{w}$ | $\epsilon\mathbf{e}$ | $\mathbf{i}$ |
| $\overrightarrow{k}$ | $\mathbf{k}$ | $\epsilon\mathbf{u}$ | $\epsilon\ldots$ | $\epsilon\mathbf{w}$ | $\epsilon\mathbf{e}$ | $\mathbf{i}$ | $\mathbf{j}$ |
| $\overrightarrow{u}$ | $\mathbf{u}$ | $\epsilon\ldots$ | $\epsilon\mathbf{w}$ | $\epsilon\mathbf{e}$ | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ |
| $\ldots$ | $\ldots$ | $\epsilon\mathbf{w}$ | $\epsilon\mathbf{e}$ | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ | $\mathbf{u}$ |
| $\overrightarrow{w}$ | $\mathbf{w}$ | $\epsilon\mathbf{e}$ | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ | $\mathbf{u}$ | $\ldots$ |

Table 2. The used variant of the BVMTs for the cases $m = 4, 5, \ldots, 55$.

Let us consider some examples, where the finite polynomial fields $GF(p^d)$ are defined with the irreducible polynomials $P(x)$ of the degree $d$ and the vector multiplication operation is defined with Table 2 in which the expansion coefficients are polynomials $\epsilon = \epsilon(x)$, where $\epsilon(x)$ is not the $m$th-power element in $GF(p^m)$.

**Example 5.** For prime $p = 268675256028581$ and coefficients $\mu = 1$ and $\epsilon = 3048145277787$ ($\epsilon$ is not the 5th-power element) the vector $G_\Omega = 2\mathbf{e} + 5\mathbf{i} + 7\mathbf{j} + 11\mathbf{k} + 13\mathbf{u}$ is a generator of the multiplicative group of the vector field $GF(p^5)$. The vector $G_\Omega = 88815218764680\mathbf{e} + 238886012231841\mathbf{i} + 157317400153847\mathbf{j} + 21593513218048\mathbf{k} + 204824491909450\mathbf{u}$ is a generator of the $q$-th order cyclic subgroup, where
q=1042175072703434265745203478134729214503105234181740193961
is a prime.

**Example 6.** For $m = 5$, $p = 2$, $P(x) = 101111011 = x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$ $(m|p^s - 1)$, and $\epsilon(x) = x^3 + 1$ there is formed the vector field $GF\left((2^8)^5\right)$. The vector $G = (x^4+1)\mathbf{e} + (x^4+x^2+1)\mathbf{i} + (x^6+x^5+x^2+x+1)\mathbf{j} + (x^5+1)\mathbf{k} + (x^4+1)\mathbf{u}$ having the order $\omega = 1099511627775$ is generator of the multiplicative group of the field.

**Example 7.** For $m = 5$, $p = 2$,

$$P(x) = x^{32} + x^{31} + \cdots + 1 = 111101010100001110001100111010111$$

$(m|p^s - 1,)$ and $\epsilon(x) = x + 1$ there is formed the vector field $GF\left((2^{32})^5\right)$. The vector $G = (x^4+1)\mathbf{e} + (x^4+x^3+x+1)\mathbf{i} + (x^6+x^5+x^2+1)\mathbf{j} + (x^5+1)\mathbf{k} + (x^4+1)\mathbf{u}$ having the order

$$\omega = 1461501637330902918203684832716283019655932542975$$

is a generator of the multiplicative group of the field.

**Example 8.** For $m = 8$, $p = 233$, $P(x) = x^3{+}179x^2{+}13x{+}81 = (m|p^s{-}1)$, and $\epsilon(x) = x + 1$ there is formed the vector field $GF\left((2^{32})^5\right)$. The vector $G = (3x^2{+}7x{+}1, 3x{+}3, x{+}2, x^2{+}2x{+}1, x{+}5, 71x{+}1, 17x{+}1, 11x^2{+}7x{+}1)$ having the order $\omega = 6554538286614627187408670948046098710112280210781 82589120$ is generator of the multiplicative group of the field ($\omega_G = \Omega = p^{ms} - 1$).

## 3. Comparison of the multiplication complexity in FFs implemented in different forms

Performance of the DSAs based on computations on ECs is inversely proportional to the difficulty of the point addition operation that is defined mainly by several field multiplications and one inversion operation in the finite field over which the ECs are defined.

The inversion is the most contributing to the difficulty of the point addition operation. Even though there are some special techniques for computing inverses in the finite field, inversion is still far more expensive than the field multiplication.

The inverse operation needed when adding two points can be eliminated by resorting to projective coordinates [9]. In this way adding two points is performed with about ten field multiplications. Thus, the difficulty of the multiplication in the underlying field defines difficulty of the point addition operation.

The vector finite fields $GF(p^m)$ defined over the ground field $GF(p)$ can be applied to design the EC-based cryptographic algorithms providing significantly higher performance. Indeed, in known EC-based algorithms one can replace the underlying FF in usually used forms by the respective vector FF [10]. For different values $m \in \{2, 3, 4, 5 \dots\}$ it is easy to generate ECs the order of which contains large prime factor $q$ such that $|q| \approx m|p|$, where $|q|$ is the bit size of $q$.

While comparing the computational efficiency of the multiplication operation in different FFs one should consider the case of the approximately equal values of the FF order. Let us compare the difficulty of the multiplication operation in the ground field $GF(p)$ and in the vector extension fields $GF(p_v^m)$ for different values $m$ in the case $|p| = m|p_v|$.

Multiplication in $GF(p)$ is performed with arithmetic multiplication of two $|p|$-bit values and arithmetic division of some $2|p|$-bit value by some $|p|$-bit value. Multiplication in the vector field $GF(p_v^m)$ is performed with $m^2$ arithmetic multiplications of two $|p_v|$-bit values and $m$ arithmetic divisions of some $2|p_v|$-bit values by some $|p_v|$-bit values (because of sufficiently low difficulty we do not take into account the arithmetic additions and $m^2/2$ multiplications with expansion coefficients having usually the size of two bits).

Taking into account that difficulty of the both arithmetic multiplication and arithmetic division is proportional to the squared size of operands one can easily derive the following formula

$$\rho = \frac{W_{GF(p)}}{W_{GF(p_v^m)}} = \frac{m(1+c)}{m+c},$$

where $W_{GF(p)} \quad \left(W_{GF(p_v^m)}\right)$ is the computational difficulty of the multiplication in $GF(p) \quad (GF(p_v^m))$ and $c$ is the ratio of the arithmetic division difficulty to the arithmetic multiplication difficulty.

The value $c$ depends on the hardware used to perform computations. For many types of microcontrollers and microprocessors we have $c > 5$. For example, in this case for $m = 5$ and $c = 6$ ($c = 12$) we have $\rho \approx 3.2$ ($\rho \approx 3.8$).

Analogous consideration of the computational efficacy of the multiplication in polynomial and vector fields gives the ratio $\rho \geqslant 2$. The lower multiplication efficacy in the polynomial fields is connected with the division operation of the $(2s-2)$-power polynomials by the $s$-power irreducible polynomial, which is additionally required to multiplications and additions in the ground field $GF(p)$ over which the polynomial field is defined.

Thus, using elliptic curves over vector FFs one can design the DS algorithms possessing significantly higher performance. Besides, the multiplication in the vector field $GF(p_v^m)$ suites well to cheap parallelization while being implemented in hardware. This is also a significant resource for additional acceleration of the EC-based cryptography.

## 4. Conclusions

A new form of the extension FFs have been proposed to accelerate the EC-based cryptographic algorithms. The proposed vector FFs $GF\left((p^d)^m\right)$, $d \geqslant 1$, are formed in the $m$-dimension vector space over the ground FF $GF(p)$ or over the polynomial FF $GF(p^d)$ , while special types of the vector multiplication operation is defined. It is proposed the BVMT possessing simple structure and providing the associative vector multiplication.

It has been shown that the complexity of the multiplication in vector FFs is lower than in the ground and polynomial FFs, while the size of the field order is the same. This advantage and suitability of the efficient parallelization of the multiplication operation provides possibility to significant acceleration of the EC-based DSAs with application of the vector FFs as underlying fields.

**Acknowledgement.** The work supported by Russian Foundation for Basic Research grant # 08-07-90100-Mol_a.

## References

[1] **G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone**, *An implementation for a fast public key cryptosystem*, J. Cryptology **3** (1991),

63 – 79.

[2] **G. B. Agnew, R. C. Mullin, and S. A. Vanstone**, *An implementation of elliptic curve cryptosystems over* $\mathbf{F}_{2^{155}}$, IEEE Journal on Selected Areas in Communications **11** (1993), 804 – 813.

[3] **G. B. Agnew, T. Beth, R. C. Mullin, and S.A. Vanstone**, *Arithmetic operations in* $GF(2^m)$, J. Cryptology **6** (1993), 3 – 13.

[4] **International Standard ISO/IEC 14888-3:2006(E).**, *Information technology – Security techniques – Digital Signatures with appendix – Part 3: Discrete logarithm based mechanisms.*

[5] **N. Koblitz**, *A course in number theory and cryptography*, Springer-Verlag, Berlin, 2003.

[6] **A.G. Kurosh**, *Course of higher algebra*, (Russian), Moskva, Nauka 1971.

[7] **J. Lee, H. Kim, Y. Lee, S.-M. Hong, H. Yoon**, *Parallelized scalar multiplication on elliptic curves defined over optimal extension field*, Internat. J. Network Security **4** (2007), 99 – 106.

[8] **A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone**, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997.

[9] **A. J. Menezes and S. A. Vanstone**, *Elliptic curve cryptosystems and their implementation*, J. Cryptology **6** (1993), 209 – 224.

[10] **N. A. Moldovyan**, *A method for generating and verifying electronic digital signature certifying an electronic document*, Russian patent application # 2008140403, October 14, 2008.

[11] **J. Pieprzyk, Th. Hardjono, and J. Seberry**, *Fundamentals of computer security*, Springer-Verlag. Berlin, 2003.

[12] **R. Pierce**, *Associative algebras*, (Russian), Moscow, Mir, 1986.

[13] **N. Smart**, *Cryptography: an introduction*, McGraw-Hill Publication, London, 2003.

Received December 18, 2008

St. Petersburg Institute for Informatics and Automation, Russian Academy of Sciences,
St. Petersburg, Russia
E-mail: nmold@cobra.ru

Quasigroups and Related Systems **17** (2009), 283 – 290

# Congruences on an inverse $AG^{**}$-groupoid via the natural partial order

*Petar V. Protić*

In memory of **Nebojša Stevanović (1962–2009)**, my colleague and dear friend.

**Abstract.** In this paper we first describe natural partial order on an inverse $AG^{**}$-groupoid. With it we introduce a notion of pseudo normal congruence pair and normal congruence pair and describe congruences.

## 1. Introduction

A groupoid $S$ on which the following is true

$$(\forall a, b, c \in S) \quad ab \cdot c = cb \cdot a,$$

is called an *Abel-Grassmann's groupoid* (*AG-groupoid*) [8] (or in some papers Left almost semigroups (*LA-semigroups*)) [3]. It is easy to verify that in every $AG$-groupoid *medial law* $ab \cdot cd = ac \cdot bd$ holds. Thus, $AG$-groupoids belong to the wider class of medial groupoids.

We denote the set of all idempotents of S by $E(S)$ .

Abel-Grassmann's groupoid $S$ satisfying

$$(\forall a, b, c \in S) \quad a \cdot bc = b \cdot ac$$

is an $AG^{**}$-*groupoid.* It is obvious that in $AG^{**}$-groupoid for $a, b, c, d \in S$

$$ab \cdot cd = c(ab \cdot d) = c(db \cdot a) = db \cdot ca.$$

2000 Mathematics Subject Classification: 20N02

Keywords: Abel-Grassmann's groupoid, natural partial order, congruence pair

Supported by Grant ON 144013 of Ministry of science through Math. Inst. SANU

If $AG$-groupoid $S$ has the left identity $e$, then

$$a \cdot bc = ea \cdot bc = eb \cdot ac = b \cdot ac,$$

so $S$ is an $AG^{**}$-groupoid.

In [5] an $AG$-groupoid $S$ is called an *inverse AG-groupoid* if for every $a \in S$ there exists $a' \in S$ such that $a = aa' \cdot a$ and $a' = a'a \cdot a'$. Then $a'$ is an inverse element of $a$, and by $V(a)$ we shall mean the set of all inverses of $a$. It is easy to prove that if $a' \in V(a)$, $b' \in V(b)$, then $a'b' \in V(ab)$ and that $aa'$ or $a'a$ are not necessarily idempotents.

**Remark 1.** In [1] it is proved that in an $AG^{**}$-groupoid $S$ the set $E(S)$ is a semilattice (Remark 2). Also, in [1] it is proved that in an inverse $AG^{**}$-groupoid for $a \in S$, by Remark 3, we have $|V(a)| = 1$. If $a^{-1}$ is a unique inverse for $a$, then by Lemma 1 $aa^{-1}, a^{-1}a \in E(S)$ if and only if $aa^{-1} = a^{-1}a$.

The following proposition is is trivially true.

**Proposition 1.** *Let $S$ be an inverse $AG^{**}$-groupoid and $\rho$ congruence relation on $S$. Then $S/_\rho$ is an inverse $AG^{**}$-groupoid. Also, if $a, b \in S$ then $a\rho b$ if and only if $a^{-1}\rho b^{-1}$.* □

## 2. Natural partial order

In this section we define a natural partial relation on inverse $AG^{**}$-groupoid $S$ and prove some of its properties.

**Theorem 1.** *If $S$ is an inverse $AG^{**}$-groupoid, then the relation*

$$a \leqslant b \Longleftrightarrow a = aa^{-1} \cdot b \tag{1}$$

*on $S$ is a natural partial order relation and it is compatible.*

*Proof.* The proof that $\leqslant$ is reflexive is obvious. For antisymmetry let us suppose that $a \leqslant b$ and $b \leqslant a$. Then $a = aa^{-1} \cdot b$ and $b = bb^{-1} \cdot a$, and

$$a = aa^{-1} \cdot b = aa^{-1} \cdot (bb^{-1} \cdot a) = bb^{-1} \cdot (aa^{-1} \cdot a) = bb^{-1} \cdot a = b,$$

imply antisymmetry.

Let us now suppose that $a \leqslant b$ and $b \leqslant c$. Then $a = aa^{-1} \cdot b$, $b = bb^{-1} \cdot c$, and

$$\begin{aligned} a &= aa^{-1} \cdot b = aa^{-1}(bb^{-1} \cdot c) = ((aa^{-1} \cdot a)a^{-1})(bb^{-1} \cdot c) \\ &= (a^{-1}a \cdot aa^{-1})(bb^{-1} \cdot c) = (a^{-1}a \cdot bb^{-1})(aa^{-1} \cdot c) \\ &= b(a^{-1}a \cdot b^{-1}) \cdot (aa^{-1} \cdot c) = b(aa^{-1} \cdot b)^{-1} \cdot (aa^{-1} \cdot c) \\ &= ba^{-1} \cdot (aa^{-1} \cdot c) = ca^{-1} \cdot (aa^{-1} \cdot b) = ca^{-1} \cdot a = aa^{-1} \cdot c, \end{aligned}$$

imply that $a \leqslant c$. Hence transitivity holds and $\leq$ is a partial order on $S$.

Let $a \leqslant b$ and $c \in S$. Then

$$\begin{aligned} ca &= c(aa^{-1} \cdot b) = (cc^{-1} \cdot c)(aa^{-1}) \cdot b = (cc^{-1} \cdot aa^{-1}) \cdot cb \\ &= (ca \cdot c^{-1}a^{-1}) \cdot cb = (ca \cdot (ca)^{-1}) \cdot cb, \end{aligned}$$

and so the relation $\leq$ is left compatible. Also, since

$$\begin{aligned} ac &= (aa^{-1} \cdot b)c = (aa^{-1} \cdot b)(cc^{-1} \cdot c) = (aa^{-1} \cdot cc^{-1}) \cdot bc \\ &= (ac \cdot a^{-1}c^{-1}) \cdot bc = (ac \cdot (ac)^{-1}) \cdot bc, \end{aligned}$$

therefore the relation $\leq$ is right compatible. Hence, $\leq$ is compatible. □

**Corollary 1.** *Let $S$ be an inverse $AG^{**}$-groupoid and $a, b \in S$. Then*

$$a \leqslant b \Longleftrightarrow aa^{-1} = ba^{-1}.$$

*Proof.* If $a \leqslant b$ then by (1) we have

$$aa^{-1} = (aa^{-1} \cdot b)a^{-1} = a^{-1}b \cdot aa^{-1} = a^{-1}a \cdot ba^{-1} = b(a^{-1}a \cdot a^{-1}) = ba^{-1}.$$

Conversely, for $a, b \in S$, $aa^{-1} = ba^{-1}$ implies that

$$a = aa^{-1} \cdot a = ba^{-1} \cdot a = aa^{-1} \cdot b.$$

So, by (1), $a \leqslant b$. □

## 3. Normal congruence pair

In this section by $S$ we mean an inverse $AG^{**}$-groupoid in which for each $a \in S$ we have $aa^{-1} = a^{-1}a$ or equivalently $aa^{-1}, a^{-1}a \in E(S)$.

First, we prove the following consequence of Theorem 1.

**Corollary 2.** *Let $a, b \in S$. Then*

$$a \leqslant b \iff (\exists e \in E(S))\ a = eb.$$

*Proof.* Let $a, b \in S$. Then $a \leqslant b$ if and only if $a = (aa^{-1})b$. Since $aa^{-1} \in E(S)$, therefore if $e = aa^{-1}$ implies that $a = eb$.

Conversely, let $a, b \in S$ be such that $e \in E(S)$ and $a = eb$. Because $aa^{-1} = a^{-1}a \in E(S)$ and $E(S)$ is a semilattice, we have

$$\begin{aligned} aa^{-1} \cdot b &= (eb \cdot eb^{-1})b = (bb^{-1} \cdot e)b = (bb^{-1} \cdot e)(bb^{-1} \cdot b) \\ &= (bb^{-1} \cdot bb^{-1}) \cdot eb = bb^{-1} \cdot eb = e(bb^{-1} \cdot b) = eb = a \end{aligned}$$

and so $a \leqslant b$. □

Let $\rho$ be a congruence on $S$. The restriction $\rho|_{E(S)}$ is the *trace* of $\rho$ and it is denoted by tr$\rho$. Also, kernel $\rho$ is ker$\rho = \{a \in S \mid (\exists e \in E(S))\ a\rho e\}$.

If $\rho$ is a congruence relation on $S$, then ker$\rho$ is a subgroupoid of $S$ and $E(S) \subseteq$ ker$\rho$ it is, ker$\rho$ is a *full* subgroupoid of $S$. Also, tr$\rho$ is a congruence on semillatice $E(S)$.

**Definition 1.** Let $K$ be a full subgroupoid of $S$ and $\tau$ a congruence on $E(S)$ satisfying the following condition:

($i$) For all $a \in S, b \in K$, $b \leqslant a$ and $aa^{-1}\tau bb^{-1}$ imply $a \in K$.

We call $(K, \tau)$ a *pseudo normal congruence pair for S.* If, in addition,

($ii$) For every $a \in K$, there exists $b \in S$ with $b \leqslant a$, $aa^{-1}\tau\, bb^{-1}$ and $b^{-1} \in K$,

then $(K, \tau)$ is called a *normal congruence pair for S.*

For pseudo normal congruence pair $(K, \tau)$, we define a relation

$$a\rho_{(K,\tau)}b \iff ab^{-1}, a^{-1}b, ba^{-1}, b^{-1}a \in K,\ \ aa^{-1} \cdot b^{-1}b\,\tau\, aa^{-1}\tau\, bb^{-1}.$$

**Lemma 1.** *Let $(K, \tau)$ be a pseudo normal congruence pair of $S$, $a, b \in S$. If $a\,\rho_{(K,\tau)}b$ and $b \in K$, then $a \in K$.*

*Proof.* From $a\,\rho_{(K,\tau)}b$ we have $ab^{-1} \in K$ and $aa^{-1} \cdot bb^{-1}\tau\, aa^{-1}\tau\, bb^{-1}$. Since $b \in K$, it follows that $ab^{-1} \cdot b = bb^{-1} \cdot a \in K$.

We prove that $ab^{-1} \cdot b \leqslant a$. Here

$$\begin{aligned} ((ab^{-1} \cdot b)(ab^{-1} \cdot b)^{-1})a &= ((ab^{-1} \cdot b)(a^{-1}b \cdot b^{-1}))a = ((bb^{-1} \cdot a)(b^{-1}b \cdot a^{-1}))a \\ &= ((bb^{-1} \cdot b^{-1}b)aa^{-1})a = (bb^{-1} \cdot aa^{-1})a \\ &= (aa^{-1} \cdot bb^{-1})a = (aa^{-1} \cdot bb^{-1})(aa^{-1} \cdot a) \\ &= (aa^{-1} \cdot aa^{-1})(bb^{-1} \cdot a) = aa^{-1}(bb^{-1} \cdot a) \\ &= bb^{-1}(aa^{-1} \cdot a) = bb^{-1} \cdot a = ab^{-1} \cdot b. \end{aligned}$$

Hence, by (1), it follows that $ab^{-1} \cdot b \leq a$.

Also

$$\begin{aligned}(ab^{-1} \cdot b)(ab^{-1} \cdot b)^{-1} &= (ab^{-1} \cdot b)(a^{-1}b \cdot b^{-1})\\ &= (ab^{-1} \cdot a^{-1}b)bb^{-1} = (aa^{-1} \cdot b^{-1}b)bb^{-1}\\ &= (bb^{-1} \cdot b^{-1}b) \cdot aa^{-1}) = bb^{-1} \cdot aa^{-1}\tau aa^{-1},\end{aligned}$$

whence by Definition 1 $(i)$ it follows that $a \in K$. □

**Theorem 2.** *If $(K,\tau)$ is a pseudo normal congruence pair for $S$, then $\rho_{(K,\tau)}$ is a congruene on $S$ with*

$$\ker \rho_{(K,\tau)} = \{a \in K \mid (\exists b \in S),\ a \geqslant b,\ aa^{-1}\tau\, bb^{-1},\ b^{-1} \in K\} \tag{2}$$

*and the trace is equal to $\tau$. Moreover, if $(K_1,\tau_1)$ and $(K_2,\tau_2)$ are pseudo congruence pairs for $S$ with $K_1 \subseteq K_2$ and $\tau_1 \subseteq \tau_2$, then $\rho_{(K_1,\tau_1)} \subseteq \rho_{(K_2,\tau_2)}$.*

*Proof.* Let $(K,\tau)$ be a pseudo normal congruence pair for $S$ and $\rho = \rho_{(K,\tau)}$. Since $K$ is full it follows that $\rho$ is reflexive. Obviously, $\rho$ is symmetric. We verify that $\rho$ is transitive after we prove that $\rho$ is compatible.

Assume now that $a\rho b$ and let $c \in S$. Then

$$ac \cdot (bc)^{-1} = ac \cdot b^{-1}c^{-1} = ab^{-1} \cdot cc^{-1} \subseteq K \cdot E(S) \subseteq K.$$

Similarly,

$$(ac)^{-1} \cdot bc, bc \cdot (ac)^{-1}, (bc)^{-1} \cdot ac \in K.$$

Next we have

$$\begin{aligned}(ac \cdot (ac)^{-1})((bc)^{-1} \cdot bc)) &= (ac \cdot (bc)^{-1})((ac)^{-1} \cdot bc)\\ &= (ac \cdot b^{-1}c^{-1})(a^{-1}c^{-1} \cdot bc)\\ &= (ab^{-1} \cdot cc^{-1})(a^{-1}b \cdot c^{-1}c)\\ &= (ab^{-1} \cdot a^{-1}b)(cc^{-1} \cdot cc^{-1})\\ &= (aa^{-1} \cdot b^{-1}b)cc^{-1}\tau\, aa^{-1} \cdot cc^{-1}\\ &= ac \cdot a^{-1}c^{-1} = ac \cdot (ac)^{-1}.\end{aligned}$$

By symmetry, it follows that

$$(ac \cdot (ac)^{-1})((bc)^{-1} \cdot bc)\,\tau\, bc \cdot (bc)^{-1},$$

whence $ac\,\rho bc$. Thus $\rho$ is right compatible. Analogously, $\rho$ is left compatible. Hence, $\rho$ is compatible.

Now, suppose that $a\,\rho\,b$ and $b\,\rho\,c$. Then by right compatibility $ac^{-1}\,\rho\,bc^{-1}$ and $bc^{-1}\,\rho\,cc^{-1}$. Since $cc^{-1} \in E(S) \subseteq K$ and $bc^{-1}\rho cc^{-1}$, we have $bc^{-1} \in K$ by Lemma 1, and subsequently $ac^{-1} \in K$. Similarly, $aa^{-1}\rho ba^{-1}, ba^{-1}\rho ca^{-1}$ yield $ca^{-1} \in K$ by Lemma 1.

Similarly, by left compatibility, from $a\rho b$ and $b\rho c$ we have $a^{-1}a\rho a^{-1}b$, $a^{-1}b\rho a^{-1}c$, $c^{-1}a\rho c^{-1}b$ and $c^{-1}b\rho c^{-1}c$. So by Lemma 1 it follows that $a^{-1}c, c^{-1}a \in K$.

Also $a\rho b$, $b\rho c$ yields

$$a^{-1}a \cdot bb^{-1}\tau aa^{-1}\tau bb^{-1}, \quad b^{-1}b \cdot cc^{-1}\tau bb^{-1}\tau cc^{-1}$$

and by transitivity it follows that $aa^{-1}\tau cc^{-1}$. Moreover,

$$(bb^{-1} \cdot cc^{-1})(aa^{-1} \cdot cc^{-1}) = (bb^{-1} \cdot aa^{-1})cc^{-1}\tau\, aa^{-1} \cdot cc^{-1},$$
$$(bb^{-1} \cdot cc^{-1})(aa^{-1} \cdot cc^{-1}) = (bb^{-1} \cdot aa^{-1})cc^{-1}\tau bb^{-1} \cdot cc^{-1}\tau\, cc^{-1},$$

whence $aa^{-1} \cdot cc^{-1}\tau cc^{-1}$.

Now, $ac^{-1}, a^{-1}c, ca^{-1}, c^{-1}a \in K$, $aa^{-1} \cdot cc^{-1}\tau\, aa^{-1}\tau\, cc^{-1}$ is equivalent to $a\rho c$. Hence, $\rho$ is a transitive relation and so is a congruence.

It is apparent that for $e, f \in E(S)$, $e\rho f$ if and only if $e\tau f$ whence $\mathrm{tr}\rho = \tau$.

We let

$$H = \{a \in K \mid (\exists b \in S)\ a \geqslant b, b^{-1} \in K, aa^{-1}\tau bb^{-1}\}$$

and we show that $\ker\rho = H$.

Let $a \in H$, then there exists $b \in K$ such that $b \leqslant a$, $b^{-1} \in H$ and $aa^{-1}\,\tau\, bb^{-1}$. By (1) $b \leqslant a$ it implies that $b = bb^{-1} \cdot a$. We next prove that $a\rho bb^{-1}$ that is

$$bb^{-1} \cdot a^{-1},\ a^{-1} \cdot bb^{-1},\ bb^{-1} \cdot a,\ a \cdot bb^{-1} \in K,\ bb^{-1} \cdot aa^{-1}\tau aa^{-1}\tau\, bb^{-1}.$$

Now $b = bb^{-1} \cdot a \in K$ and $b^{-1} = bb^{-1} \cdot a^{-1} \in K$. Also we have $a \cdot bb^{-1} \in K \cdot E(S) \subseteq K$ and

$$a^{-1} \cdot bb^{-1} = (a^{-1}a \cdot a^{-1})bb^{-1} = (bb^{-1} \cdot a^{-1})a^{-1}a \in K \cdot E(S) \subseteq K.$$

Conversely, let $a \in \ker\rho$. Then $a\rho e$ for some $e \in E(S)$. If $b = ea$, then $b \leqslant a$ by Corollary 2 and $b = ea \in E(S) \cdot K \subseteq K$. From $a\rho e$ it follows that $aa^{-1} = ea^{-1} = b^{-1}$ and since $aa^{-1} \in K$ we have by Lemma 1 that $b^{-1} \in K$. Because $b, b^{-1} \in K$ we have $bb^{-1} = b^{-1}b \in K$ and so $b\rho b^{-1}$. Now

$$\begin{aligned} bb^{-1}\rho b^{-1}b^{-1} &= ea^{-1} \cdot ea^{-1}\rho aa^{-1} \cdot ea^{-1} \\ &= e(a^{-1}a \cdot a^{-1}) = ea^{-1}\rho aa^{-1} \end{aligned}$$

Thus $a \in H$ implies that $\ker\rho \subseteq H$, that is $H = \ker\rho$. □

**Theorem 3.** *If* $(K,\tau)$ *is a normal congruence pair for* $S$*, then* $\rho_{(K,\tau)}$ *is a congruence on* $S$ *with kernel* $K$ *and trace* $\tau$*. Conversely, if* $\rho$ *is a congruence on* $S$*, then* $(\ker\rho, \mathrm{tr}\rho)$ *is a normal congruence pair for* $S$ *and* $\rho = \rho_{(\ker\rho,\mathrm{tr}\rho)}$.

*Proof.* Let $(K,\tau)$ be a normal congruence pair and let $\rho = \rho_{(K,\tau)}$. Then by Theorem 2, $\rho$ is a congruence with trace equal to $\tau$ and $\ker\rho$ as in (2). Thus $\ker\rho \subseteq K$. Now let $a \in K$. Then by Definition 1 $(ii)$ there exist $b \in S$, $b \leqslant a$, $b^{-1} \in K$ and $bb^{-1}\tau aa^{-1}$ such that $a \in \ker\rho$ due to Theorem 2. Thus $K = \ker\rho$.

Conversely, let $\rho$ be a congruence on $S$ and let $K = \ker\rho$, $\tau = \mathrm{tr}\rho$. Then $K$ is a full subgroupoid of $S$ and $\tau$ is a congruence on $E(S)$.

Let $a \in S$, $b \in K$ and $a \geqslant b$. Suppose that $aa^{-1}\rho bb^{-1}$. Then $b = bb^{-1} \cdot a$ (by (1)). From $aa^{-1}\rho\, bb^{-1}$ it follows that $a\rho\,(bb^{-1})a$ and by above argument we have $a\rho b$. Hence $a \in b\rho \subseteq \ker\rho = K$. Thus $(i)$ from the Definition 1 holds for $(K,\tau)$ and that it is a pseudo congruence pair for $S$.

Let $a \in K$. Then there exists $e \in E(S)$ with $a\rho\, e$. If $b = ea$, then $b \leqslant a$ by Corollary 2. From $a\rho\, e$ it follows that $ea\rho\, e$ whence $b\rho\, e$ and so $a\rho\, b$. Now $a^{-1}\rho\, b^{-1}$ by Proposition 1 and so $aa^{-1}\rho\, bb^{-1}$. Moreover, from $a\rho\, e$ follows that $aa^{-1}\rho\, ea^{-1} = (ea)^{-1} = b^{-1}$, that is $b^{-1} \in K$. Hence, $(K,\tau)$ is a congruence pair for $S$.

It remains to prove that $\rho = \rho_{(K,\tau)}$. Let $a\rho\, b$. Then

$$ab^{-1}\rho\, bb^{-1},\ b^{-1}a\rho\, b^{-1}b,\ aa^{-1}\rho\, ba^{-1},\ a^{-1}a\rho\, a^{-1}b$$

and so $ab^1, b^{-1}a, ba^{-1}, a^{-1}b \in \ker\rho = K$. Also

$$\begin{aligned} &aa^{-1} \cdot bb^{-1}\rho\, a^{-1}b \cdot bb^{-1} = (bb^{-1} \cdot b)a^{-1} = ba^{-1}\rho\, aa^{-1},\\ &aa^{-1} \cdot bb^{-1}\rho\, aa^{-1} \cdot ba^{-1} = b(aa^{-1} \cdot a) = ba^{-1}\rho\, b^{-1}b = bb^{-1}, \end{aligned}$$

whence it follows that $a\rho_{(K,\tau)}b$ and so $\rho \subseteq a\rho_{(K,\tau)}$.

Let $a\rho_{(K,\tau)}b$. Then $ab^{-1}, a^{-1}b, ba^{-1}, b^{-1}a \in K$, $aa^{-1} \cdot bb^{-1}\tau\, aa^{-1}\tau\, bb^{-1}$, imply that $ab^{-1}\rho e$, $ba^{-1}\rho f$ for some $e, f \in E(S)$. From $aa^{-1}\rho bb^{-1}$, it follows that

$$a\,\rho\, bb^{-1} \cdot a = ab^{-1} \cdot b\,\rho\, eb \qquad \text{and} \qquad b\rho\, aa^{-1} \cdot b = ba^{-1} \cdot a\rho\, fa.$$

Also

$$\begin{aligned} &a\,\rho\, eb\,\rho\, e \cdot fa\,\rho\, e(f \cdot eb) = e(e \cdot fb) = ee(e \cdot fb)\\ &= (fb \cdot e)ee = (fb \cdot e)e = ee \cdot fb = e \cdot fb = f \cdot eb\,\rho\, fa\,\rho\, b \end{aligned}$$

imply that $a\rho b$, that is $\rho_{(K,\tau)} \subseteq \rho$. Then $\rho_{(K,\tau)} = \rho$. □

## References

[1] **M. Božinović, P. V. Protić and N. Stevanović**, *Kernel normal system of inverse AG$^{**}$-groupoids*, Quasigroups and Related Systems **17** (2008), 1 – 8.

[2] **J. Deneš and A. D. Keedwell**, *Latin squares and their applications*, Akadémia Kiadó, Budapest, 1974.

[3] **M. A. Kazim and M. Naseeruddin**, *On almost semigroups*, The Aligarh Bull. Math. **2** (1972), 1 – 7.

[4] **Q. Mushtaq and Q. Iqbal**, *Decomposition of a locally associative LA-semigroup*, Semigroup Forum **41** (1990), 155 – 164.

[5] **Q. Mushtaq and Q. Iqbal**, *Partial oredering and congruences on LA-semigroups*, Indian J. Pure Appl. **22** (1991), 331 – 336.

[6] **M. Petrich**, *Inverse semigroups*, Pure and Applied Mathematics, John Wiley and Sons, New York, 1984.

[7] **M. Petrich and S. Rankin**, *The kernel – trace approach to right congruences on an inverse semigroup*, Trans. Amer. Math. Soc. **330** (1992), 917 – 932.

[8] **P. V. Protić and N. Stevanović**, *On Abel-Grassmann's groupoids* (*review*), Proc. Math. Conference, Priština, 1994, 31 – 38.

Received September 4, 2009

Faculty of Civil Engineering
University of Niš
Aleksandra Medvedeva 14
18000 Niš
Serbia
e-mail: pvprotic@yahoo.mail.com