Quasigroups and Related Systems **17** (2009), 191 – 204

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, 8.1×10^8, 6.1×10^{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 $a_1a_2\ldots a_ka_1a_2\ldots a_k\ldots a_1a_2\ldots a_k$, $a_i \in Q$, with smallest period k, to be transformed into a periodical string with period k after arbitrarily many applications of e-transformations, i.e.,

$$e_l^n(a_1a_2\ldots a_ka_1a_2\ldots a_k\ldots a_1a_2\ldots a_k) = c_1c_2\ldots c_kc_1c_2\ldots c_k\ldots c_1c_2\ldots c_k,$$

for each $n = 1, 2, 3, \ldots$, 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	=	α
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 $s = 32413241\ldots3241$ 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).

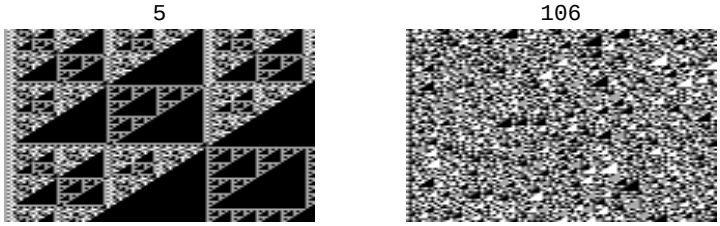

Figure 1. Images of $e-$transformations of quasigroups 5 and 106

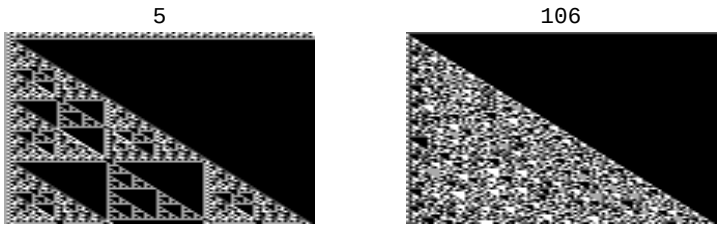

Figure 2. Images of $d-$transformations of quasigroups 5 and 106

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.)

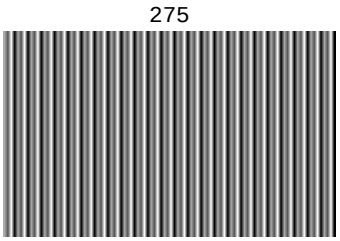

Figure 3. The periodical pattern of $e-$transformations of quasigroup 275

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 $s = a_1 a_2 \ldots a_k a_1 a_2 \ldots a_k \ldots a_1 a_2 \ldots a_k$, $a_i \in Q$, 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

$$a_{i-1} * a_i = a_i,$$
$$a_{j-1} * a_i = a_i,$$

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

$$a_{j-1} * a_1 = a_1,$$
$$a_k * a_1 = a_1,$$

and that implies $a_{j-1} = a_k$. Then we have

$$a_{j-2} * a_{j-1} = a_{j-1},$$
$$a_{k-1} * a_{j-1} = a_{j-1},$$

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

$$a_1 * a_{j-r+1} = a_{j-r+1},$$
$$a_{j-r} * a_{j-r+1} = a_{j-r+1},$$

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 $\{a_1, \ldots, a_k\}$ of $Q = \{a_1, \ldots, a_n\}$, where $k < n$, we define a partial quasigroup $(Q, *)$ by the equalities $a_k * a_1 = a_1$, $a_1 * a_2 = a_2, a_2 * a_3 = a_3, \ldots, a_{n-1} * a_k = a_k$. 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 $\{a_{1,\pi(1)}, a_{2,\pi(2)}, \ldots, a_{n,\pi(n)}\}$, where $a_{l,r} \in Q$ denotes the element at the position (l, r) and π is a permutation of $\{1, 2, \ldots, n\}$. 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 $(a_{\pi^{-1}(1),1}, a_{\pi^{-1}(2),2}, \ldots, a_{\pi^{-1}(n),n})$, and the main column by the string $(a_{n,\pi(n)}, a_{1,\pi(1)}, a_{2,\pi(2)}, \ldots, a_{n-1,\pi(n-1)})$. Then $a_{n,\pi(n)} * a_{1,\pi(1)} = a_{1,\pi(1)}$, $a_{1,\pi(1)} * a_{2,\pi(2)} = a_{2,\pi(2)}, \ldots, a_{n-1,\pi(n-1)} * a_{n,\pi(n)} = a_{n,\pi(n)}$. 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 $32413241\ldots$.

$*$	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 $n_1, n_2, \ldots, n_t$, then $n_1 + n_2 + \cdots + n_t \leqslant n$.*

Proof. Let $(Q, *)$ be a quasigroup with different periods $n_1, \ldots, n_t$ such that $n_1 + n_2 + \cdots + n_t > k$. Then there are periodic sequences $s_1 = x_1 x_2 \ldots$

and $s_2 = y_1 y_2 \ldots$ with smallest periods $x_1 x_2 \ldots x_{n_i}$ and $y_1 y_2 \ldots y_{n_j}$ 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 $x_{n_i} = y_{r-1},\ x_{n_i-1} = y_{r-2},\ x_{n_i-2} = y_{r-3}, \ldots, x_1 = y_{r-n_i}$ in the case $n_i < r$, or $x_{n_i} = y_{r-1},\ x_{n_i-1} = y_{r-2},\ x_{n_i-2} = y_{r-3}, \ldots, x_{n_i-r+2} = y_1$ in the case $r \leqslant n_i$.

In the case $n_i < r$ we have that the smallest period $y_1 y_2 \ldots y_{n_j}$ of s_2 is $y_1 \ldots y_{r-n_i-1} x_1 \ldots x_{n_i} x_1 y_{r+1} \ldots y_{n_j}$ 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 $x_1 x_2 \ldots x_{n_i}$ of s_1 is $x_1 \ldots x_{n_i-r+1} y_1 \ldots y_{r-1}$. 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 $x_{n_i-r+1} = y_{n_j},\ x_{n_i-r} = y_{n_j-1},\ x_{n_i-r-1} = y_{n_j-2}, \ldots, x_1 = y_{n_j-n_i+r}$ in the subcase $n_i - r < n_j$, or $x_{n_i-r+1} = y_{n_j},\ x_{n_i-r} = y_{n_j-1},\ x_{n_i-r-1} = y_{n_j-2}, \ldots, x_{n_i-r-n_j+2} = y_1$ 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 $x_1 x_2 \ldots x_{n_i}$, and the subcase $n_i - r < n_j$ implies that x_1 appears two times in the string $y_1 y_2 \ldots y_{n_j}$. (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 $x_1 x_2 \ldots x_k,\ x_i \in \{1, 2, 3, 4\},\ k = 1, 2, 3, 4$. 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.