Quasigroups and Related Systems **18** (2010), 149 – 163

Identity sieves for quasigroups

Smile Markovski, Vesna Dimitrova and Simona Samardjiska

Abstract. In this paper we consider the set $\mathcal{Q}_n$ of all finite quasigroups of a given order n, where n is a positive integer. Using left and right translations, as well as suitably chosen quasigroup terms t, we define sets of identities that are satisfied in the class $\mathcal{Q}_n$. The set $\mathcal{Q}_n$ can be represented as a union of isomorphism classes $\mathbb{C}_i$, $\mathcal{Q}_n = \cup_{i=1}^{h} \mathbb{C}_i$, and we use sets of identities as sieves for classifying the isomorphism classes. In such a way we make a presentation of the set of all isomorphism classes of $\mathcal{Q}_n$ in the form of a disjoint union $\{\mathbb{C}_1, \ldots, \mathbb{C}_p\} = \cup_{i=1}^{s} \mathcal{Q}^{(i)}$, where $\mathcal{Q}^{(i)}$ are unions of isomorphism classes. We show that these classifications can be used for obtaining quasigroups with special qualities, that can be applied for designing several kinds of cryptographic primitives (PRNG, hash functions, stream and block ciphers,...), or for defining error detecting and error correcting codes.

Also, by using suitably chosen identities, we show the fractal structure of some quasigroups in $\mathcal{Q}_4$.

1. Introduction

A groupoid $(G, \cdot)$ is a pair of a nonempty set G and a binary operation $\cdot : G^2 \to G$. Given a groupoid $(G, \cdot)$ and an element $a \in G$, the translations L_a and R_a, called left translation and right translation, are defined by $L_a(x) = ax$ and $R_a(x) = xa$, for each $x \in G$. A groupoid $(G, \cdot)$ is said to be a quasigroup if and only if L_a and R_a are permutations on G for each $a \in G$.

Note that each set of translations

$$S = \{L_{a_1}, \ldots, L_{a_m}, R_{b_1}, \ldots, R_{b_k}\},\ m \geqslant 0,\ k \geqslant 0,$$

on a groupoid $(G, \cdot)$ generates a semigroup $<S>$.

We have the following result.

Theorem 1.1. *Let $(G, \cdot)$ be a finite quasigroup, and let $S = \{L_{a_1}, \ldots, L_{a_n}, R_{a_1}, \ldots, R_{a_n}\}$, where $G = \{a_1, \ldots, a_n\}$. Then for each $T \in <S>$ there is a smallest integer $r = r(T)$ such that $T^r = 1_G$.*

2010 Mathematics Subject Classification: 20N05

Keywords: quasigroup, identity, isomorphism class, identity sieve, fractal quasigroup.

Proof. Since L_a and R_a are permutations on G, $< S >$ is a group of permutations on G, so $r(T)$ is the order of the permutation T. □

If T is a permutation of a set $G = \{a_1, \ldots, a_n\}$, then for each element $b \in G$ there is a number $r_b \leqslant n$ such that $T^{r_b}(b) = b$. (Namely, the set $\{b, T(b), T^2(b), \ldots\}$ is a subset of G.) Then, for the number

$$r_T = LCM(r_{a_1}, r_{a_2}, \ldots, r_{a_n}) \leqslant LCM(1, 2, \ldots, n)$$

we have $T^{r_T}(x) = x$ for each $x \in G$. Hence, $T^{r_T} = 1_G$, and $r(T)$ is a factor of r_T. So, we have the next theorem:

Theorem 1.2. *The order $r(T)$ of each $T \in <S>$, where S is a set of left and right translations of a finite quasigroup G, is a factor of the number $LCM(1, 2, \ldots, |G|)$.*

We need as well to introduce the notion of a term.

A groupoid term, where f denotes a binary functional symbol and X denotes a nonempty set of variables, is defined inductively as follows:

1) x is a term for each $x \in X$;

2) if $t_1, \ldots, t_n$ are terms, then the expression $f(t_1, \ldots, t_n)$ is a term.

Given a term t and different variables $x_1, \ldots, x_k \in X$, by $t(x_1, \ldots, x_k)$ we denote that only the variables $x_1, \ldots, x_k$ may appear in the term t; hence, some variable x_j may not appear in t. In the sequel we consider special types of terms $t(x_1, \ldots, x_k)$, where a variable x_i appears exactly once, and we denote it by $t(\bar{x}_i, x_i)$, where $\bar{x}_i$ denotes a fixed tuple of all other variables occurring in t. For example, the term $t(x, y, z, u, v, w) = (y(x((yz)u)))(zy)$ can be denoted as $t = t(\bar{x}, x)$ or $t = t(\bar{u}, u)$. There are several choices for $\bar{x}$ ($\bar{x} = (y, z, u)$, or $\bar{x} = (u, z, y)$, or $\bar{x} = (y, u, z)$, ...) as well as for $\bar{u}$, and for our purposes it does not matter which one is chosen.

Let $(G, \cdot)$ be a given groupoid. Each term $t = t(x_1, \ldots, x_k)$ defines an s-ary function t^G on the set G, where s is the number of all different variables that occur in t. Denote by $y_1, \ldots, y_s \in X$ all different variables in t, in some ordering. (Depending on the ordering, different functions t^G can be defined.) The definition of t^G follows the inductive definition of a term. For each variable x we have that x^G is the identity mapping. If $t = t_1 t_2$, where t_1 contains the different variables $y_{i_1}, \ldots, y_{i_p}$ and t_2 contains the different variables $y_{j_1}, \ldots, y_{j_q}$, then for all $a_i \in G$ we define $t^G(a_1, \ldots, a_s) = t_1^G(a_{i_1}, \ldots, a_{i_p}) \cdot t_2^G(a_{j_1}, \ldots, a_{j_q})$.

Given a term $t(y_1, \ldots, y_s)$, where y_i are different variables that occur in t, and given an l-tuple $(a_{i_1}, \ldots, a_{i_l}) \in G^l$, we can define an $(s-l)$-ary function $t^G_{a_{i_1}, \ldots, a_{i_l}}$ on G by $t^G_{a_{i_1}, \ldots, a_{i_l}}(a_1, \ldots, a_{i_1-1}, a_{i_1+1}, \ldots, a_{i_l-1}, a_{i_l+1}, \ldots, a_s) =$

$t^G(a_1,\dots,a_s)$. We say that $t^G_{a_{i_1},\dots,a_{i_l}}$ is the l-th projection of t defined by the l-tuple $(a_{i_1},\dots,a_{i_l}) \in G^l$.

By using the notation $t(\bar{x},x)$ of a term t with s different variables, where x occurs exactly once in t, we denote by $t^G_{\bar{a}}$ the $(s-1)$-th projection of t, obtained by the $(s-1)$-tuple $\bar{a} \in G^{s-1}$. So, $t^G_{\bar{a}}$ is the mapping on G defined by $t^G_{\bar{a}}(x) = t^G(\bar{a},x)$.

In the case of quasigroups, we have that $t^G_{\bar{a}} \in < S >$, where $G = \{a_1,\dots,a_n\}$ and $S = \{L_{a_1},\dots,L_{a_n},\ R_{a_1},\dots,R_{a_n}\}$. For example, when $t = (y(x((yz)u)))(zy) = t(\bar{x},x)$, $\bar{x} = (u,y,z)$ and $\bar{a} = (b,c,d)$, we have $t^G_{\bar{a}} = R_{dc}L_cR_{(cd)b}$. Therefore, Theorem 1.1 and Theorem 1.2 hold for these mappings too.

Given two terms t_1 and t_2, the expression $t_1 \approx t_2$ is called an identity. An identity $t_1(x_1,\dots,x_k) \approx t_2(x_1,\dots,x_k)$ is said to be satisfied in a groupoid G if for every $a_i \in G$ we have $t^G_1(a_1,\dots,a_k) = t^G_2(a_1,\dots,a_k)$. An identity is satisfied in a class of groupoids $\mathcal{C}$ if it is satisfied in every groupoid of $\mathcal{C}$. (Note that t^G_1 and t^G_2 are not considered as k-ary functions on G, since some of the variables $x_1,\dots,x_k$ may not appear neither in t_1 nor in t_2.)

Further on, if there is no confusion, instead of t^G we will write simply t.

2. Sieve construction

In this Section we consider finite quasigroups only.

Lately, quasigroups have been intensively studied for use in cryptography and coding theory. The notion of a shapeless quasigroup was defined in [5] as a kind of quasigroup suitable for building cryptographic primitives. According to this definition, a shapeless quasigroup Q should not satisfy any identity of the form $x(x(\dots(xy)\dots)) = y$ or $(\dots((yx)x)\dots)x = y$, where x occurs $n < 2|Q|$ times. In general, quasigroups may satisfy different types of laws in the form of identities. Here, we make a wider characterization regarding a special form of identities that refines the notion of a shapeless quasigroup.

Let t be a term of the form $t = t(\bar{y},y)$ such that $\bar{y} = (x_1,\dots,x_k)$, $k \geqslant 1$ (and $y \neq x_i$ for each $i = 1,\dots,k$). A t-sieve is said to be the set $Sieve(t)$ of identities defined recursively as follows:

$$Sieve(t) = \{t^{(1)} = t(\bar{y},y),\ t^{(2)} = t(\bar{y},t^{(1)}),\ t^{(3)} = t(\bar{y},t^{(2)}),\dots\}.$$

Note that $t^{(2)} = t(\bar{y},t(\bar{y},y)),\ t^{(3)} = t(\bar{y},t(\bar{y},t(\bar{y},y))),\dots$.

Theorem 2.1. *For each term $t = t(\bar{y}, y)$ and for each finite quasigroup Q, there is a smallest number $r(t, Q)$ such that $t^{(r(t,Q))} \approx y$ is an identity in Q.*

Proof. Let $t = t(\bar{y}, y)$, $\bar{y} = (x_1, \ldots, x_k)$ and $\bar{a} = (a_1, \ldots, a_k) \in Q^k$. Then, by Theorem 1.1, there is a smallest number $r(t_{\bar{a}})$ such that $t_{\bar{a}}^{r(t_{\bar{a}})}(y) = y$ for each $y \in Q$. Note that $t_{\bar{a}}^{r(t_{\bar{a}})} = t_{\bar{a}}^{(r(t_{\bar{a}}))}$, since $t_{\bar{a}}^{(p)}(y) = t(\bar{a}, t(\bar{a}, \ldots, t(\bar{a}, y))) = t_{\bar{a}}^{p}(y)$. It follows that for the number $r(t, Q) = LCM\{r(t_{\bar{a}}) |\ \bar{a} \in Q^k\}$ we have $t_{\bar{a}}^{(r(t,Q))}(y) = y$ for every $\bar{a} \in Q^k$ and for each $y \in Q$. This means that $t^{(r(t,Q))} \approx y$ is an identity in Q. □

The number $r(t, Q)$ is called a rang of t in Q.

Let $\mathcal{Q}_n$ denote the set of all quasigroups of order n. We have the following.

Theorem 2.2. *For each term $t = t(\bar{y}, y)$ there is a number $r(t, n)$, such that $t^{(r(t,n))} \approx y$ is an identity in the set $\mathcal{Q}_n$.*

Proof. By Theorem 2.1 we have that for each $Q \in \mathcal{Q}_n$ there is a number $r(t, Q)$ such that $t^{(r(t,Q))} \approx y$ is an identity in Q. Let $r(t, n) = LCM\{r(t, Q) |\ Q \in \mathcal{Q}_n\}$. Then $t^{(r(t,n))} \approx y$ is an identity in Q for each $Q \in \mathcal{Q}_n$, i.e., it is an identity in $\mathcal{Q}_n$ as well. □

The number $r(t, n)$ is called a rang of t in $\mathcal{Q}_n$. It follows, by the definition of $r(t, n)$, that it is the smallest number such that $t^{(r(t,n))}(\bar{y}, y) \approx y$ is an identity in $\mathcal{Q}_n$. The upper bound of $r(t, n)$ is $LCM(2, 3, \ldots, n)$. When considering $Sieve(t)$ on $\mathcal{Q}_n$ in order to produce identities of the type $t^{(r(t,n))} \approx y$, it is enough to take its restriction, i.e., its finite subset

$$Sieve(t, n) = \{t^{(i)} |\ \ i | LCM(2, 3, \ldots, n)\}.$$

Using $Sieve(t, n)$, where $t = t(\bar{y}, y)$, we sieve the quasigroups from $\mathcal{Q}_n$ via the isomorphism classes of $\mathcal{Q}_n$. The sieving algorithm $SA(t, n)$ is the following.

1. Input: the set $\mathcal{Q}_n$.
2. Represent the set $\mathcal{Q}_n$ as (disjoint) union of its isomorphism classes, $\mathcal{Q}_n = \mathbb{C}_1 \cup \mathbb{C}_2 \cup \cdots \cup \mathbb{C}_h$.
3. For $j = 1, 2, \ldots, h$, take a representative quasigroup $Q_j \in \mathbb{C}_j$.

4. For each $i|LCM(2,3,\ldots,n)$ form families of isomorphism classes $\mathcal{Q}^{(i)}$ as follows. $\mathbb{C}_j \in \mathcal{Q}^{(i)}$ if i is the smallest integer such that the identity $t^{(i)} \approx y$ is satisfied in Q_j.

5. Output: representation of the isomorphism classes of $\mathcal{Q}_n$ as a disjoint union of families of isomorphism classes,

$$\{\mathbb{C}_1,\ldots,\mathbb{C}_h\} = \bigcup\{\mathcal{Q}^{(i)}|\ \ i|LCM(2,3,\ldots,n)\}.$$

The definition of $\mathcal{Q}^{(i)}$ does not depend on Q_j, since if an identity is satisfied in Q_j, then it is satisfied in each quasigroup $Q \in \mathbb{C}_j$ too.

Note that the families $\mathcal{Q}^{(i)} = \mathcal{Q}^{(i)}(t)$ depend on the chosen term t. For different terms $t_1, t_2, t_3, \ldots$, we can obtain different families $\mathcal{Q}^{(i)}(t_j), j = 1,2,3,\ldots$. Then by using the intersection $\bigcap\{\mathcal{Q}^{(i)}(t_j)|\ j = 1,2,\ldots\}$, we can classify the isomorphism classes in several different ways. By this classification we can separate isomorphism classes of quasigroups of given order n suitable for different purposes. The Section 3 contains such classifications for the set $\mathcal{Q}_4$ of quasigroups of order 4.

3. Classifications of quasigroups of order 4

In this section we consider the set $\mathcal{Q}_4$ of all binary quasigroups of order 4, consisting of 576 quasigroups. We order the set $\mathcal{Q}_4$ by lexicographic ordering, using the presentation of the multiplicative table of a quasigroup as a concatenation of the strings of its rows. The set $\mathcal{Q}_4$ can be represented as a union of 35 isomorphism classes $\mathbb{C}_j$, and we take the quasigroups with lexicographic numbers 1, 2, 3, 4, 6, 10, 14, 25, 26, 27, 28, 29, 30, 33, 34, 35, 37, 38, 39, 40, 73, 74, 77, 80, 83, 92, 149, 150, 155, 157, 158, 159, 160, 196, 213 as representatives for the classes $\mathbb{C}_1, \mathbb{C}_2, \ldots, \mathbb{C}_{35}$, respectively.

We have $LCM(2,3,4) = 12$, and there are 6 factors of 12: 1, 2, 3, 4, 6 and 12. Thus, $Sieve(t,4) = \{t^{(i)}|\ \ i = 1,2,3,4,6,12\}$. Using the algorithm $SA(t,4)$, for different choices of the terms t, we can obtain different classifications of the isomorphism classes. Table 1 and Table 2 present special type of sieves constructed from all terms $t = t(\bar{y}, y)$ such that $\bar{y} = (x)$, and with $m \leq 3$ appearances of the variable x in t. So, for $m = 1$ we have two terms xy, yx, for $m = 2$ we have 6 terms $x(xy), (yx)x, (xy)x, x(yx), (xx)y, y(xx)$, and so on. Altogether, there are 24 terms of this type. Instead of $\mathbb{C}_j$, the isomorphism classes in Table 1 (and in all other tables in this section) are denoted simply by j.

How can we read Tables 1 and 2? For $m = 3$, let us consider the term $t = x(x(xy))$ in Table 2. In column 1 we have 6 isomorphism classes: $\mathbb{C}_{23}, \mathbb{C}_{24}, \mathbb{C}_{25}$, $\mathbb{C}_{26}, \mathbb{C}_{34}, \mathbb{C}_{35}$. This means that the identity $t^{(1)} \approx y$, i.e., $x(x(xy)) \approx y$, is satisfied in all of these classes. We note that these classes also satisfy the identities $t^{(i)} \approx y$ for all other values of i, but $i = 1$ is the smallest value of i such that $t^{(i)} \approx y$ is an identity in these classes. Next, the identity $t^{(2)} \approx y$, i.e., $x(x(x(x(x(xy))))) \approx y$, is satisfied in the classes $\mathbb{C}_1, \mathbb{C}_4, \mathbb{C}_7, \mathbb{C}_8, \mathbb{C}_{11}, \mathbb{C}_{16}, \mathbb{C}_{29}$, and $i = 2$ is the smallest value of i such that $t^{(i)} \approx y$ is an identity in these classes. In all of the other classes the identity $t^{(i)} \approx y$ is satisfied for $i = 4$ (and also for $i = 12$), so they are given in column 4. Note that the rang of the term $t = x(x(xy))$ in $\mathcal{Q}_4$ is $r(t, 4) = 4$, the same rang has the term $((yx)x)x$, and the rang of the other terms in Tables 1 and 2 is 12, except of the terms $x(xy)$ and $(yx)x$, that have rang 6.

m	$t \setminus i$	1	2	3	4	6	12
6*1	xy		1,4,7,8, 11,16,29	23,24,25,26, 34,35	2,3,5,6,9, 10,17,20,30, 33		12,13,14,15, 18,19,21,22, 27,28,31,32
	yx		1,3,9,11, 14,23,28	7,20,25,26, 30,35	2,4,8,10,12, 17,21,24,33, 34		5,6,13,15, 16,18,19,22, 27,29,31,32
10*2	$x(xy)$	1,4,7,8, 11,16,29	2,3,5,6,9, 10,17,20,30, 33	23,24,25,26, 34,35		12,13,14,15, 18,19,21,22, 27,28,31,32	
	$(xy)x$	1,11,26	2,3,4,8,9, 10,35	7,17,23,25, 33	15,20,22,24, 30,34	13,14,16,19, 27,28,29	5,6,12,18, 21,31,32
	$x(yx)$	1,11,26	2,3,4,8,9, 10,35	7,17,23,25, 33	15,20,22,24, 30,34	13,14,16,19, 27,28,29	5,6,12,18, 21,31,32
	$(yx)x$	1,3,9,11, 14,23,28	2,4,8,10,12, 17,21,24,33, 34	7,20,25,26, 30,35		5,6,13,15, 16,18,19,22, 27,29,31,32	
	$(xx)y$	1,3	2,4,7,8,9, 10,11,15,16, 20,29	22,23,24,25, 26,34,35	5,6,17,30, 33	13,14,19,28	12,18,21,27, 31,32
	$y(xx)$	1,8	2,3,4,9,10, 11,14,22,23, 24,28	7,15,20,25, 26,30,35	12,17,21,33, 34	13,16,19,29	5,6,18,27, 31,32

Table 1: Application of $SA(t, 4)$ on $\mathcal{Q}_4$ by using terms $t = t(\bar{y}, y)$ with $\bar{y} = (x)$, for $m = 1$ and $m = 2$.

We analyze the obtained results in Tables 1 and 2. For that aim, we look at the frequency of appearance of an isomorphism class in different

m	$t \setminus i$	1	2	3	4	6	12
31*3	$x(x(xy))$	23,24,25,26, 34,35	1,4,7,8, 11,16,29		2,3,5,6,9,10, 12,13,14,15, 17,18,19,20, 21,22,27,28, 30,31,32,33		
	$(x(xy))x$	25	1,3,9,11, 17,24,34	7,20,23,26, 30,35	2,4,8,10, 13,27,33	5,12,14,15, 18,19,22	6,16,21,28, 29,31,32
	$x((xy)x)$	25	1,3,9,11, 17,24,34	7,20,23,26, 30,35	2,4,8,10, 13,27,33	5,12,14,15, 18,19,22	6,16,21,28, 29,31,32
	$((xy)x)x$	25	1,4,8,11, 17,20,30	7,23,24,26, 34,35	2,3,9,10, 13,27,33	5,12,15,16, 18,19,22	6,14,21,28, 29,31,32
	$x(x(yx))$	25	1,3,9,11, 17,24,34	7,20,23,26, 30,35	2,4,8,10, 13,27,33	5,12,14,15, 18,19,22	6,16,21,28, 29,31,32
	$(x(yx))x$	25	1,4,8,11, 17,20,30	7,23,24,26, 34,35	2,3,9,10, 13,27,33	5,12,15,16, 18,19,22	6,14,21,28, 29,31,32
	$x((yx)x)$	25	1,4,8,11, 17,20,30	7,23,24,26, 34,35	2,3,9,10, 13,27,33	5,12,15,16, 18,19,22	6,14,21,28, 29,31,32
	$((yx)x)x$	7,20,25,26, 30,35	1,3,9,11, 14,23,28		2,4,5,6,8,10, 12,13,15,16, 17,18,19,21, 22,24,27,29, 31,32,33,34		
	$x((xx)y)$	17	1,4,7,9,10, 20,30,33	23,24,25,26, 34,35	2,3,5,6,8, 11,15,16,18, 27,29,32	12,13,19,31	14,21,22,28
	$((xx)y)x$	26,35	1,3,8,10, 15,20,30	7,17,23,25, 33	2,4,9,11,19, 24,27,31,34	5,6,12,13, 14,18,32	16,21,22,28, 29
	$x(y(xx))$	26,35	1,3,8,10, 22,24,34	7,17,23,25, 33	2,4,9,11,19, 20,27,30,32	5,12,13,16, 18,21,31	6,14,15,28, 29
	$(y(xx))x$	17	1,4,9,10, 23,24,33,34	7,20,25,26, 30,35	2,3,8,11,12, 14,18,21,22, 27,28,31	5,13,19,32	6,15,16,29
	$(x(xx))y$		1,4,5,6,7,8, 11,16,17,20, 29,30,33	23,24,25,26, 34,35	2,3,9,10,18, 31	12,13,14,19, 21,27,32	15,22,28
	$y(x(xx))$	23	1,3,9,11,12, 14,17,24,28,34	7,20,25,26, 30,35	2,4,8,10,21, 33	5,13,18,19, 27,31	6,15,16,22, 29,32
	$((xx)x)y$	7	1,4,5,8,11, 16,17,20,29,30	23,24,25,26, 34,35	2,3,6,9,10, 33	12,13,18,19, 27,32	14,15,21,22, 28,31
	$y((xx)x)$		1,3,9,11,12, 14,17,21,23, 24,28,33,34	7,20,25,26, 30,35	2,4,8,10, 18,32	5,6,13,16, 19,27,31	15,22,29

Table 2: Application of $SA(t,4)$ on $\mathcal{Q}_4$ by using terms $t = t(\bar{y}, y)$ with $\bar{y} = (x)$, for $m = 3$.

columns. For example, the class $\mathbb{C}_1$ appears only in columns 1 and 2. It means that the identity $t^{(2)} \approx y$ is satisfied for each term t from Tables 1 and 2. Consequently, the quasigroups of the class $\mathbb{C}_1$ should not be used for cryptographic purposes, since they allow to be attacked by applying very simple identities. Nevertheless, they are suitable for defining some error detecting codes ([1]). On the other hand, the classes $\mathbb{C}_{31}$ and $\mathbb{C}_{32}$ appear 13 times in column 12, 6 times in column 6 and 5 times in column 4. We conclude that the quasigroups of the classes $\mathbb{C}_{31}$ and $\mathbb{C}_{32}$ are suitable for cryptographic purposes. They have better cryptographic properties regarding t, because it would be more unlikely and more difficult to reach an expression that can be replaced by a simpler one. They belong also to the class of shapeless quasigroups. Even more, for any term of the form $t = t(\bar{y}, y)$ from Tables 1 and 2, they satisfy the identity $t^{(i)} \approx y$ only when $mi \geqslant 12$. One can find some identities of type $t = t(\bar{y}, y)$, where x appears at least 5 times in t, such that the inequality $mi \geqslant 12$ is not satisfied. Nevertheless, the inequality $mi \geqslant 8$ was satisfied in all terms $t = t(\bar{y}, y)$, where $\bar{y} = (x)$, we have checked.

The discussion above can help improve the definition of a shapeless quasigroup. Now, we define that a shapeless quasigroup should not satisfy any identity of the form $t^{(i)} \approx y$, for any term $t = t(\bar{y}, y)$, where $\bar{y} = (x)$, for $mi < 2n$. By this new definition, we have that only the quasigroups of the classes $\mathbb{C}_{13}, \mathbb{C}_{18}, \mathbb{C}_{19}, \mathbb{C}_{27}, \mathbb{C}_{31}$ and $\mathbb{C}_{32}$ can be considered as shapeless.

In Tables 1 and 2 we considered only special types of terms, in order to get more complete picture of the distribution of the isomorphism classes in the families $\mathcal{Q}^{(i)}$. Still, sieves of general type $Sieve(t)$, where $t = t(\bar{y}, y)$ such that $\bar{y} = (x_1, \ldots, x_s)$, $s \geqslant 1$, can be considered as well. For that aim we investigate the left and the right translations, which define the quasigroups. From the properties of these translations, we can derive general conclusions about the structure of the quasigroups, and how they can be sieved. This gives a different classification of the classes of isomorphism.

As we said earlier, in a quasigroup Q, for an arbitrary term $t = t(\bar{y}, y)$, and each $\bar{a} \in Q^{s-1}$, the mapping $t^Q_{\bar{a}} \in < S >$, where $Q = \{a_1, \ldots, a_n\}$ and $S = \{L_{a_1}, \ldots, L_{a_n}, R_{a_1}, \ldots, R_{a_n}\}$. Even more, each translation (being a permutation) can be represented as a composition of disjoint cycles. Hence, the permutation $t^Q_{\bar{a}}$ can be given by cycles and the order of $t^Q_{\bar{a}}$ depends on the lengths of these cycles. On the other hand, by Theorem 2.1, $r(t, Q) = LCM\{r(t^Q_{\bar{a}}) |\ \bar{a} \in Q^{s-1}\}$, so $r(t, Q)$ depends on $L_{a_1}, \ldots, L_{a_n}, R_{a_1}, \ldots, R_{a_n}$, i.e., on the properties of their cycles.

Example 3.1. Consider the quasigroup $(Q, \cdot)$ that is a representative of the isomorphism class $\mathbb{C}_2$, given by its multiplicative table

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	2	1
4	4	3	1	2

Let $t = (xy)z = t(\bar{y}, y)$, where $\bar{y} = (x, z)$. Then, for $\bar{a} = (a, b) \in Q^2$, we have $t^Q_{\bar{a}} = L_a R_b$. Q is commutative with unit 1, so $L_1 = R_1 = (1)(2)(3)(4)$, $L_2 = R_2 = (12)(34)$, $L_3 = R_3 = (1324)$ and $L_4 = R_4 = (1423)$.

Now, $L_1R_1 = (1)(2)(3)(4)$, $L_1R_2 = L_2R_1 = (12)(34)$, $L_1R_3 = L_3R_1 = (1324)$, $L_1R_4 = L_4R_1 = (1423)$, $L_2R_2 = (1)(2)(3)(4)$, $L_2R_3 = L_3R_2 = (1423)$, $L_2R_4 = L_4R_2 = (1324)$, $L_2R_4 = L_4R_2 = (1324)$, $L_3R_3 = (12)(34)$, $L_3R_4 = L_4R_3 = (1)(2)(3)(4)$, $L_4R_4 = (12)(34)$.

Since we have cycles of lengths 1, 2 and 4, $r(t, Q) = LCM(1, 2, 4) = 4$.

This example shows how we can calculate $r(t, Q)$ for given t and Q. But, of course, there are an infinite number of terms, so such approach is not always suitable. Especially, if we are considering the properties of quasigroups used in some kind of quasigroup transformations in a cryptographic primitive. Still, the nature of the left and the right quasigroup translations can show how the mapping $t^Q_{\bar{a}}$ behaves for any t or Q. For cryptographic purposes, a quasigroup Q needs bigger $r(t, Q)$ for any t.

Denote by $r_{max} = max\{r(t, Q) |\ t \text{ is a term}\}$, which in fact is the maximal i for any $Sieve(t, 4)$ that sieves the quasigroup Q. Analyzing the cycles of the translations $L_1, R_1, \ldots, L_4, R_4$ from Example 3.1 we can conclude that any composition of these translations, produces only permutations with cycles of lengths 1, 2 and 4. Hence, we have that $r_{max} = 4$ for all quasigroups in the class $\mathbb{C}_2$.

r_{max}	Isomorphism class
2	1
3	7,23,25,26,35
4	2,3,4,8,9,10,11,17,20,24,30,33,34
12	5,6,12,13,14,15,16,18,19,21,22,27,28,29,31,32

Table 3: Classification of $\mathcal{Q}_4$ by $Sieve(t, 4)$, for any term t.

Table 3 gives the values r_{max} for all isomorphism classes in $\mathcal{Q}_4$. The analysis that led to this classification is rather cumbersome and not especially neat. That is why, here we give only a few examples that prove the correctness of Table 3.

Example 3.2. Consider the quasigroup with lexicographic order 1, that is a representative of the isomorphism class $\mathbb{C}_1$, and is given by its multiplication table

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

This quasigroup is commutative with unit 1, so $L_1 = R_1 = (1)(2)(3)(4)$, $L_2 = R_2 = (12)(34)$, $L_3 = R_3 = (13)(24)$ and $L_4 = R_4 = (14)(23)$.

Let t be an arbitrary term. Then the mapping $t^Q_{\bar{a}}$, $\bar{a} \in Q^{s-1}$ is some finite composition of the translations $L_1 = R_1, \ldots, L_4 = R_4$. When composing any two of these translations, we have only the following three possibilities: $(ij)(kl) \cdot (ij)(kl) = (i)(j)(k)(l)$, $(ij)(kl) \cdot (ik)(jl) = (il)(kj)$ and $(ij)(kl) \cdot (i)(j)(k)(l) = (ij)(kl)$ (or $(i)(j)(k)(l) \cdot (ij)(kl) = (ij)(kl)$), i.e., again we get permutations of the same type. Hence, an arbitrary composition produces only permutations with cycles of lengths 1 and 2, which implies that $r_{max} = 2$ for all quasigroups in the class $\mathbb{C}_1$.

Example 3.3. Consider the quasigroups with lexicographic orders 92 and 213, that are representatives of the isomorphism classes $\mathbb{C}_{26}$ and $\mathbb{C}_{35}$ respectively. The quasigroups from these two different isomorphic classes have identical properties regarding the translations that define them. Namely, the left translations of the quasigroup 92 (given in Subsection 4.2) are $(1)(234), (2)(143), (3)(124), (4)(132)$, which on the other hand are the right translations of the quasigroup 213. Again, the right translations of the quasigroup 92, $(1)(243), (2)(134), (3)(142), (4)(123)$, are the left translations of the quasigroup 213.

Similarly, as in the previous example, it is crucial to discover all of the different cases of composing an arbitrary number of the translations that define these quasigroups. We make several observations.

When composing any two left, or any two right translations, we have these two possibilities: $(i)(jkl) \cdot (i)(jkl) = (i)(jlk)$ or $(i)(jkl) \cdot (j)(ilk) = (l)(ijk)$, i.e., again we have permutations of the same type and of order 3.

When composing a left and a right translation (in any order) we have $(i)(jkl) \cdot (i)(jlk) = (i)(j)(l)(k)$ or $(i)(jkl) \cdot (j)(ikl) = (il)(jk)$, i.e., we get a new permutation of order at most 2. Now, this new type of permutation can be composed with any of the quasigroup translations yielding $(i)(jkl) \cdot (il)(jk) = (ijl)(k)$, $(i)(jlk) \cdot (il)(jk) = (ikl)(j)$, and $(il)(jk) \cdot (i)(jkl) = (ilk)(j)$, $(il)(jk) \cdot (i)(jlk) = (ilj)(k)$, or two such permutations can be composed to give $(il)(jk) \cdot (il)(jk) = (i)(l)(j)(k)$ or $(ij)(lk) \cdot (il)(jk) = (ik)(lj)$.

Hence, an arbitrary composition produces only permutations with cycles of lengths 1 and 2, or only permutations with cycles of lengths 1 and 3. This means that $r_{max} = 3$ for the quasigroups in the classes $\mathbb{C}_{26}$ and $\mathbb{C}_{35}$.

Example 3.4. The quasigroup with lexicographic order 158, that is a representative of the isomorphism class $\mathbb{C}_{31}$, has the following multiplication table

$\cdot$	1	2	3	4
1	2	1	3	4
2	3	4	2	1
3	1	3	4	2
4	4	2	1	3

The left translations of this quasigroup are $(12)(34), (1324), (1)(234), (143)(2)$, while the right ones are $(123)(4), (1)(3)(24), (134)(2), (1432)$. Since these permutations have cycles of length 12, this immediately implies that $r_{max} = 12$.

We combine Tables 1, 2 and 3 to obtain Table 4, where the values r'_{max} come only from terms t from Tables 1 and 2, i.e., $r'_{max} = max\{r(t, Q) |\ t$ is a term from Tables 1 and 2$\}$. The families of isomorphism classes in Table 4 are separated by semi-columns. So, '1;' denotes the family $\{\mathbb{C}_1\}$, '7,23,35;' denotes the family $\{\mathbb{C}_7, \mathbb{C}_{23}, \mathbb{C}_{35}\}$, and so on. The family '3,4,8,9,11;' appears in the columns $i = 1$, $i = 2$ and $i = 4$. It means that for any term t from Tables 1 and 2, only identities of the form $t^{(i)} \approx y$ are satisfied (for the corresponding value of i). Note that $r'_{max} = r_{max} = 4$.

Tables 4 gives another information about the applications of quasigroups. Generally, the quasigroups from the classes in the row $r'_{max} = 12$ and columns $i = 4$, $i = 6$ and $i = 12$ should be used for building cryptographic primitives, while those in the rows $r'_{max} = 2, 3$ and columns $i = 1, 2, 3$ should be used for designing codes. As we have noted before, the family '13,18,19,27,31,32;' contains the best quasigroups for cryptographic purposes. Nevertheless, some other classes can be used quite as well. They

are denoted by italic letters in the table (6, 21, 28 and 29). Namely, the "italic" classes have the properties that in at least half of the terms t from Tables 1 and 2, the identity $t^{(i)} \approx y$ is satisfied only for $i = 12$.

$r'_{max} \setminus i$	1	2	3	4	6	12
2	1;	1;				
3	7,23,35; 25,26;	7,23,35;	7,23,35; 25,26;			
4	 3,4,8,9,11; 17,20,24,30,34;	2,10; 3,4,8,9,11; 33; 17,20,24,30,34;	 33; 17,20,24,30,34;	2,10; 3,4,8,9,11; 33; 17,20,24,30,34;	 	
12	 14,16, *28,29*; 	15,22; 14,16, *28,29*; 5,12, *6,21*;	15,22;	15,22; 14,16, *28,29*; 5,12, *6,21*; 13,18,19,27, *31,32*;	15,22; 14,16, *28,29*; 5,12, *6,21*; 13,18,19,27, *31,32*;	15,22; 14,16, *28,29*; 5,12, *6,21*; 13,18,19,27, *31,32*;

Table 4: Classification of isomorphism classes by r'_{max}.

4. Proving the fractal structure of quasigroup transformations

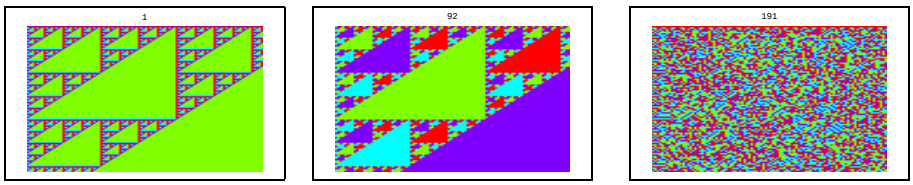
There are several papers [6, 7], where quasigroup e- and d-transformations are considered. In [4] a method for graphical presentation of sequences obtained by quasigroup transformations is proposed. Using this method (without mathematical proof) the quasigroups are classified in two disjoint classes: the class of fractal quasigroups and the class of non-fractal quasigroups. Initiated by the identities sieves, here we give a proof that the quasigroups of order 4 with lexicographic numbers 1 and 92 are fractal (see Figure 1, where the patterns obtained from quasigroups with lexicographic numbers 1, 92 and 191 are given; 1 and 92 are fractal, 191 is non-fractal). In the same way it can be shown that all fractal quasigroups as classified in [4] have really a fractal structure too. The proofs given here use suitably chosen identities, satisfied in the quasigroup in question.

We consider here only e-transformations, defined on a quasigroup $(Q, *)$ as follows. Let $Q^+ = \{a_1 a_2 \dots a_n | a_i \in Q,\ n \geqslant 2\}$ denote the set of all finite sequences with elements of Q and let us take a fixed element $l \in Q$, called

a leader. The e-transformation $e_l : Q^+ \to Q^+$ is defined by:

$$e_l(a_1a_2\dots a_n) = (b_1b_2\dots b_n) \Longleftrightarrow \begin{cases} b_1 & = l * a_1, \\ b_{i+1} & = b_i * a_{i+1}, \ 1 \leqslant i \leqslant n-1 \end{cases}$$

The method of producing images of quasigroup processed sequences is defined as follows. Take a sequence $aaa\dots a,\ a \in Q$, and put one under the other the sequences $e_l(aaa\dots a), e_l^2(aaa\dots a), \dots, e_l^k(aaa\dots a)$. For graphical presentation, like the one in Figure 1, we take different colors for different elements of Q.



a) b) c)

Figure 1: Images of e-transformations of the quasigroups 1, 92 and 191

4.1 The case of the quasigroup with lexicographic number 1

The quasigroup with lexicographic number 1 is given in Example 3.2. It can be checked that the following identities are satisfied by this quasigroup:

$$I_1: \quad xy \approx yx,\ (yx)x \approx y,\ y(yx) \approx x,\ (yx)^2y \approx y,\ x^2x^2 \approx x^2.$$

Let the starting sequence be $xxxxxxxxx\dots$ and let the leader be $l = y$, where x, y are variables. If we apply the e-transformation e_y consecutively on each produced sequence, then, using the identities I_1, we obtain the sequences shown on the table below,where the fractal structure appears clearly.

	x	x	x	x	x	x	x	x	x	x	$\dots$
y	yx	y	yx	y	yx	y	yx	y	yx	y	$\dots$
y	x	yx	$(yx)^2$	y	x	yx	$(yx)^2$	y	x	yx	$\dots$
y	yx	$(yx)^2$	$(yx)^2$	y	yx	$(yx)^2$	$(yx)^2$	y	yx	$(yx)^2$	$\dots$
y	x	x	x	yx	$(yx)^2$	$(yx)^2$	$(yx)^2$	y	x	x	$\dots$
y	yx	y	yx	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	y	yx	y	$\dots$
y	x	yx	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	y	x	yx	$\dots$
y	yx	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	y	yx	$(yx)^2$	$\dots$
y	x	x	x	x	x	x	x	yx	$(yx)^2$	$(yx)^2$	$\dots$
y	yx	y	yx	y	yx	y	yx	$(yx)^2$	$(yx)^2$	$(yx)^2$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

4.2 The case of the quasigroup with lexicographic number 92

The quasigroup with lexicographic number 92 is given by its multiplicative table:

$\cdot$	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

In this quasigroup the following identities are satisfied:

$$I_{92}: \begin{array}{l} xx \approx x,\ ((yx)x)x \approx y,\ y(yx) \approx (yx)x,\ ((yx)x)y \approx yx, \\ (yx)((yx)x) \approx y,\ y(y(yx)) \approx x,\ x((yx)x) \approx yx,\ (yx)y \approx x, \\ (yx)x \approx xy,\ ((yx)x)(yx) \approx x,\ x(yx) \approx y. \end{array}$$

We use the same starting sequence and leader as in the case of the quasigroup 1, and the resulting e-transformations are presented in the table below,where again a fractal structure appears.

	x	x	x	x	x	x	x	x	x	x	...
y	yx	$(yx)x$	y	yx	$(yx)x$	y	yx	$(yx)x$	y	yx	...
y	$(yx)x$	$(yx)x$	yx	yx	y	y	$(yx)x$	$(yx)x$	yx	yx	...
y	x	yx	yx	yx	x	$(yx)x$	$(yx)x$	$(yx)x$	x	y	...
y	yx	yx	yx	yx	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	y	y	...
y	$(yx)x$	x	y	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	yx	x	...
y	x	x	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	x	x	...
y	yx	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	y	yx	...
y	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	yx	yx	...
y	x	yx	y	x	yx	y	x	yx	yx	yx	...
...	...	...	...	...	...	...	...	...	...	...	...

The proofs for other fractal quasigroups are similar, and they may be quite complicated. But, if we try to write the sequences obtained by e-transformation for non-fractal quasigroups, we get very complicated terms, and it is almost impossible to obtain suitable identities.

Since if an identity is satisfied in a quasigroup Q, it is satisfied in all quasigroups isomorphic to Q, we conclude that all of the quasigroups of the isomorphism classes $\mathcal{C}_1$ and $\mathcal{C}_{26}$ are fractal.

References

[1] **V. Bakeva, N. Ilievska**, *A probabilistic model of error-detecting codes based on quaisgroups*, Quasigroups and Related Systems **17** (2009, 151 – 164.

[2] **V. D. Belousov**, *Osnovi teorii kvazigrupp i lupp*, (Russian), Nauka, Moskva, 1967.

[3] **J. Dénes, A. D. Keedwell**, *Latin squares and their applications*, Akademiai Kiado, Budapest, 1974.

[4] **V. Dimitrova, S. Markovski**, *Classification of quasigroups by image patterns*, Proc. of the Fifth International Conference for Informatics and Information Technology, 2007, Bitola, Macedonia, 152 – 160.

[5] **D. Gligoroski, S. Markovski, Lj. Kocarev**, *Edon-$\mathcal{R}$, an Infinite Family of Cryptographic Hash Functions*, The Second NIST Cryptographic Hash Workshop, UCSB, Santa Barbara, CA, 2006, 275 – 285.

[6] **S. Markovski**, *Quasigroup string processing and applications in cryptography*, Proc. of the 1st MII 2003 Conference, Thessaloniki, 2003, 278 – 290.

[7] **S. Markovski, D. Gligoroski, V. Bakeva**, *Quasigroup string processing: Part 1*, Contributions, Sec. Math. Tech. Sci., MANU, **XXI** (1999), 13 – 28.

[8] **V. Shcherbacov**, *Quasigroups in cryptology*, Computer Sci. J. Moldova **17** (2009), 193 – 228.

[9] **J. D. H. Smith**, *An introduction to quasigroups and their representations*, Academic Press, Inc., 1974.

Received August 30, 2010

S.Markovski and V.Dimitrova
Ss Cyril and Methodius University, Faculty of Sciences, Institute of Informatics, P.O. Box 162, 1000 Skopje, Republic of Macedonia,
E-mail: {smile,vesnap}@ii.edu.mk

S.Samardjiska
Department of Telematics, Faculty of Information Technology, Mathematics and Electrical Engineering, Norwegian University of Science and Technology, O.S.Brag-stads plass 2B, N-7491 Trondheim, Norway,
E-mail: simona.samardziska@gmail.com