Classification of quasigroups by image patterns

Vesna Dimitrova and Smile Markovski

Institute of Informatics, Faculty of Natural Sciences and Mathematics
Skopje, MACEDONIA
{vesnap,smile}@ii.edu.mk
http://www.ii.edu.mk/

Abstract. Given a finite quasigroup $(Q, *)$, we define a quasigroup string transformation e over the strings of elements from Q by $e(a_1a_2 \dots a_n) = b_1b_2 \dots b_n$ if and only if $b_i = b_{i-1} * a_i$ for each $i = 1, 2, \dots, n$, where b_0 is a fixed element of Q, and a_i are elements from Q. These kind of quasigroup string transformations are used for designing several cryptographic primitives and error-correcting codes. Not all quasigroups are suitable for that kind of designs. The set of quasigroups of given order can be separated in two disjoint classes, the class of so called fractal quasigroups and the class of non-fractal quasigroups. The classification is obtained by presenting several consecutive sequences generated by $e-$transformations and their presentation in matrix form, used to produce suitable image pattern. We note that the fractal quasigroups are usually not suitable for designing cryptographic primitives.

Key words: quasigroup string transformation, classification of quasigroups

1 Introduction

Finite quasigroups theory is used in many applications: cryptography, coding theory, design theory and many more. It was noticed that some quasigroups are suitable for cryptographic purposes, and some other are not. For this reason the classification of finite quasigroups is very important for successful application of quasigroups in many fields of applied mathematics or computer science. The classification of quasigroups is a difficult problem, because the number of quasigroups of order 2^n, $n \geq 3$, is too big. Thus, for $n = 3$, it is $10877603245908295680 0 \sim 2^{66.56}$.

There are several classifications of quasigroups. By using isotopism and isomorphism of the quasigroups two main classifications of the classes of isotopic and the classes of isomorphic quasigroups are obtained (known only for quasigroups of order $n \leq 11$ [2], [16]). Also, there are some other classifications: by algebraic properties [20], by random walk on torus [13], by graphical presentation of sequences obtained by quasigroup transformations [3], etc.

In this paper we present a new type of classification of quasigroups. In section 2 we give a brief introduction to the notion of quasigroup and quasigroup transformations. In section 3 we present new method for obtaining graphical presentation of quasigroup transformations and we give a classification of quasigroups by this presentation.

2 Quasigroup and Quasigroup Transformations

2.1 Definition of Quasigroup

A quasigroup $(Q, *)$ is a groupoid (i.e. algebra with one binary operation $*$ on the set Q) satisfying the law:

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

In other words the equations $x * u = v,\quad u * y = v$ 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) [9].

2.2 Quasigroup Transformations

Let Q be a set of elements ($|Q| \geq 2$). We denote by $Q^+ = \{a_1 a_2 \dots a_n | a_i \in Q,\ n \geq 2\}$ the set of all finite sequences with elements of Q. Assuming that $(Q, *)$ is a given quasigroup, for a fixed element $l \in Q$, called the leader, we define transformations $e_l, d_l : Q^+ \to Q^+$ on the quasigroup as follows:

$$e_l(a_1 a_2 \dots a_n) = (b_1 b_2 \dots b_n) \Leftrightarrow \begin{cases} b_1 & = l * a_1 \\ b_{i+1} & = b_i * a_{i+1}\ , 1 \leq i \leq n-1 \end{cases} \tag{2}$$

$$d_l(a_1 a_2 \dots a_n) = (c_1 c_2 \dots c_n) \Leftrightarrow \begin{cases} c_1 & = l * a_1 \\ c_{i+1} & = a_i * a_{i+1}\ , 1 \leq i \leq n-1 \end{cases} \tag{3}$$

If we have a string of leaders $l_1 l_2 \dots l_k$, we can apply consecutive $e-$ or $d-$ transformation on a given string, as a composition of $e-$ or $d-$ transformations. This composition of $e-$ or $d-$transformations we called $E-$ or $D-$transformation respectively and they are defined as

$$E_k = e_{l_1} \circ e_{l_2} \circ \dots \circ e_{l_k}, \quad D_k = d_{l_1} \circ d_{l_2} \circ \dots \circ d_{l_k}.$$

Further, we will use only one leader $l = l_i$, for $1 \leq i \leq k$.

Example 1. Let the quasigroup $(Q, *)$ is given as below, $l = 1$ is a leader and $\alpha = 3\ 4\ 4\ 2\ 2\ 2\ 1\ 2\ 3\ 4\ 1\ 1\ 1\ 1\ 2\ 3\ 3\ 3\ 4\ 1$ is the finite sequence of elements of Q.

$$\begin{array}{c|cccc} * & 1 & 2 & 3 & 4 \\ \hline 1 & 2 & 3 & 4 & 1 \\ 2 & 1 & 4 & 3 & 2 \\ 3 & 3 & 2 & 1 & 4 \\ 4 & 4 & 1 & 2 & 3 \end{array} \tag{4}$$

If we apply consecutive $e-$transformation on a given sequence we obtain the follows sequences:

$$\begin{array}{c|l} e_l & 3\ 4\ 4\ 2\ 2\ 2\ 1\ 2\ 3\ 4\ 1\ 1\ 1\ 1\ 2\ 3\ 3\ 3\ 4\ 1 = \alpha \\ \hline 1 & 4\ 3\ 4\ 1\ 3\ 2\ 1\ 3\ 1\ 1\ 2\ 1\ 2\ 1\ 3\ 1\ 4\ 2\ 2\ 1 = \alpha_1 = e_1(\alpha) \\ 1 & 1\ 4\ 3\ 3\ 1\ 3\ 3\ 1\ 2\ 1\ 3\ 3\ 2\ 1\ 4\ 4\ 3\ 2\ 4\ 4 = \alpha_2 = e_1(\alpha_1) \\ 1 & 2\ 2\ 3\ 1\ 2\ 3\ 1\ 2\ 3\ 3\ 1\ 4\ 1\ 2\ 2\ 2\ 3\ 2\ 2\ 2 = \alpha_3 = e_1(\alpha_2) \end{array} \tag{5}$$

2.3 Properties of Quasigroup Transformations

The quasigroup transformations have many interesting properties. The following theorems are true for these transformations [9], [11], [13], [14], [15]:

Theorem 1. *The transformations E_k and D_k are permutations of Q^+.*

Theorem 2. *Consider an arbitrary string $\alpha = a_1 a_2 \dots a_n \in Q^+$, where $a_i \in Q$ and let $\beta = E_k(\alpha)$, $\gamma = D_k(\alpha)$.*
(a) If n is a large enough then, for each $l : 1 \leq l \leq k$, where k is the number of applied transformations, the distribution of substrings of β of length l is uniform.
(b) If n and k are large enough, then the distribution of substrings of γ of a fixed length l $(l \geq 1)$ is uniform.

We say that a string $\alpha = a_1 a_2 \dots a_n \in Q^+$, where $a_i \in Q$, has a period p if p is the smallest positive integer such that

$a_{i+1} a_{i+2} \dots a_{i+p} = a_{i+p+1} a_{i+p+2} \dots a_{i+2p}$ for each $i \geq 0$.

Let α and β be as in Theorem 1.

Theorem 3. *The periods of the string β are increasing at least linearly by k, where k is the number of applied transformations.*

The increasing of the periods depends of the quasigroup operations. So, for some of them it is exponential (if α has a period p, then β may has periods greater than $p \cdot 2^k$).

3 Classification of Quasigroups by Graphical Presentation of Sequences Obtained by Quasigroup Transformations

The previously defined quasigroup string transformations are used for designing several cryptographic primitives and error-correcting codes. It was notice that not all quasigroups are suitable for that kind of designs. There are some quasigroups that usually produce undesirable properties of the designs, and the classification of quasigroups into suitable classes is helpful for producing better designs. Here we classify the set of all quasigroups of given finite order n into 2 disjoint classes, the class of so called fractal quasigroups, and the class of non-fractal quasigroups. The class of fractal quasigroup is not recommended to be used for producing cryptographic primitives.

3.1 Ordering of Finite Quasigroups

We use the lexicographic ordering of the set of quasigroups of order n. We present a quasigroup as a string of n^2 letters that is a concatenation of the rows of the corresponding Latin square (the main body of the quasigroup). Then we apply the lexicographic ordering of that strings, assuming that the letters are already ordered.

Example 2. There are 576 quasigroups of order 4. For quasigroups shown below, the corresponding indexes in the lexicographic ordering are: 5, 106, 381.

$*$	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	3	2	4	1
2	4	1	3	2
3	3	3	1	4
4	1	4	2	3

3.2 Graphical Presentation of Sequences Obtained by Quasigroup Transformations

We give a graphical presentation of quasigroup transformations in order to obtain a suitable tool for their classification. We can use this presentation to discover and investigate some of their properties. The method for obtaining graphical presentation of E_k- or D_k-transformations is the following.

Let Q be a quasigroup of given order. If we take a periodical sequence s of length t, then by consecutive application of $e-$transformation (or $d-$transformation) k times, we obtain a $k \times t$–matrix with elements from Q. If we treat the elements

of Q as a pixels with the corresponding color, then we have images that present E_k-transformation (or D_k- transformation) for given quasigroup.

In Appendix 1 are given the source codes of two modules, $ETransforma-tion[k,s,l,n]$ and $DTransformation[k,s,l,n]$, made in software package *Mathematica*. Using this modules a lot of experiments with quasigroups of order $n \leq 4$ are made.

Example 3. For the first two quasigroups from Example 2 and the periodical sequence $s = 12341234\ldots1234$ with length $t = 100$, leader $l = 4$, and $k = 100$ times of $e-$transformation, the corresponding images obtained by the module $ETransformation$ are shown on Figure 1. The corresponding images of the $d-$transformation by the module $DTransformation$ are shown on Figure 2.

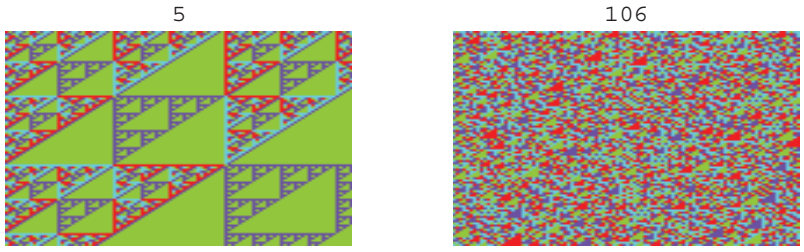

Fig. 1. Images of e-transformations of quasigroups 5 and 106.

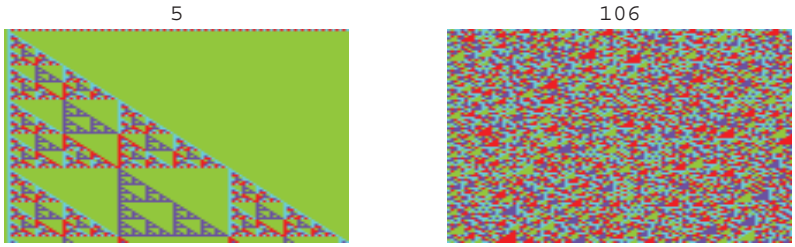

Fig. 2. Images of d-transformations of quasigroups 5 and 106.

3.3 Classification of Quasigroups by Graphical Presentation

By using the modules describe previously we made experiments for all quasigroups of order 3 and 4. The results showed interesting "graphical" property of the quasigroups. The quasigroups that have images like left-hand side images in Figures 1 and 2, we named "fractal" quasigroups, and the others "non-fractal". By using this terms we can conclude that all 12 quasigroups of order 3, as well as the quasigroups of order 2, are "fractal".

For all 576 quasigroups of order 4 we obtained that some of them are "fractal" and the others are "non-fractal". We made a lot of experiments by the modules and we conclude that the appearing of fractalness property depends on the starting periodical sequence and the leader.

We took $Q = \{1, 2, 3, 4\}$ and we considered periodical sequences with the smallest periods $x_1x_2x_3x_4$, $x_i \in Q$, where $x_1x_2x_3x_4$ is a permutation of 1234, and for different leaders $l \in Q$. The obtained results showed the following.

Case 1: If $l = x_1$, then the number of "fractal" quasigroups of order 4 is 200 and the number of "non-fractal" quasigroups is 376.

Case 2: If $l \in \{x_2, x_3\}$, then the number of "fractal" quasigroups of order 4 is 197 and the number of "non-fractal" quasigroups is 379.

Case 3: If $l = x_4$, then the number of "fractal" quasigroups of order 4 is 209 and the number of "non-fractal" quasigroups is 367.

Also, we made experiments for periodical sequences with smallest period $x_1 \dots x_k$, $x_i \in Q$ and $k \leq 3$.

Our investigation show that the number of "fractal" quasigroups differs in different experiments. The intersection of all sets of "fractal" quasigroups appearing in different experiments consists of 192 quasigroups. By this method we conclude that the set of all quasigroups of order 4 can be grouped in two classes: "the class of fractal quasigroups" and "the class of non-fractal quasigroups". The class of 192 fractal quasigroups of order 4 is the following:
{1, 2, 3, 4, 5, 7, 9, 11, 14, 18, 21, 24, 25, 26, 27, 28, 37, 40, 43, 46, 49, 51, 54, 57, 60, 63, 70, 71, 77, 80, 82, 83, 92, 93, 100, 101, 110, 111, 113, 116, 121, 126, 127, 132, 133, 138, 139, 144, 145, 146, 147, 148, 157, 160, 163, 166, 169, 170, 171, 172, 174, 176, 178, 179, 182, 185, 189, 192, 196, 197, 203, 206, 212, 213, 218, 222, 223, 228, 229, 232, 234, 235, 242, 243, 246, 252, 253, 259, 262, 263, 269, 272, 274, 275, 284, 285, 292, 293, 302, 303, 305, 308, 314, 315, 318, 324, 325, 331, 334, 335, 342, 343, 345, 348, 349, 354, 355, 359, 364, 365, 371, 374, 380, 381, 385, 388, 392, 395, 398, 399, 401, 403, 405, 406, 407, 408, 411, 414, 417, 420, 429, 430, 431, 432, 433, 438, 439, 444, 445, 450, 451, 456, 461, 464, 466, 467, 476, 477, 484, 485, 494, 495, 497, 500, 506, 507, 514, 517, 520, 523, 526, 528, 531, 534, 537, 540, 549, 550, 551, 552, 553, 556, 559, 563, 566, 568, 570, 572, 573, 574, 575, 576}.

Also, we conclude that if a quasigroup is "fractal" by E_k-transformation, it is "fractal" also by D_k-transformation.

The same kind of classification can be made for the quasigroups of order $k > 4$, but the process of their classification is tedious and time consuming, having in mind the numbers of quasigroups of order 5, 6, ...

References

1. Bedford, D., Johnson, M., Ollis, M.A.,: Defining sets for lating squares given that they are based on groups
2. Denes, J., Keedwell, D.: Latin Squares and their Applications, English Univer. Press. Ltd. (1974)
3. Dimitrova, V: Quasigroup Transformations and Their Applications, MSc thesis, Skopje, (in Macedonian) (2005)
4. Dimitrova, V., Markovski, J.: On Quasigroup Pseudo Random Sequence Generators, First Balkan Conference in Informatics, BCI1, Thessaloniki, 393 - 401 (2003)
5. Dimitrova, V., Markovski, J.: Implementation of Pseudo Random Sequence Generator using Quasigroup Processing, ETAI 2003, Ohrid,I-86-I-90 (2003)
6. Gligoroski, D.: Candidate One-Way Functions and One-Way Permutations Based on Quasigroup String Transformations,Cryptology ePrint Archive Report 2005/352, (2005) `http://eprint.iacr.org`
7. Laywine, F. C., Mullen, L.G.: Discrete Mathematics using Latin Squares, John Wiley and Sons, Inc. (1998)
8. Markovski, J.,Dimitrova, V.: Improving existing PRSG using QSP, CIIT 2003, Bitola, 380-386 (2003)
9. Markovski, S.: Quasigroup String Processing and Applications in Cryptography, 1st Conference of Mathematics and Informatics for Industry, Thessaloniki, 278-290 (2003)
10. Markovski, S., Bakeva, V.: On a streem error correcting codes, Proc. of the 2nd Confer. CIIT, Bitola (2001)
11. Markovski, S., Gligoroski, D., Bakeva, V.: Quasigroup String Processing - Part 1, Contributions, Sec. Math. Tech. Sci.,MANU, XXI, 1-2, Skopje, 15-28 (1999)
12. Markovski, S., Gligoroski, D., Bakeva, V.: Random walk tests for pseudo-random number generators, Mathematical Communications Vol.6, No.2, Osijek, 135-143 (2001)
13. Markovski, S., Gligoroski, D., Markovski, J.: Classification of Quasigroups by Random Walk on Torus, Journal of Applied Mathematics and Computing, Vol. 19, No. 1-2 (2005)
14. Markovski, S., Kusakatov, V.: Quasigroup String Processing - Part 2, Contributions, Sec. math. Tech. Sci., MANU, XXI, 1-2, Skopje, 15-32 (2000)
15. Markovski, S., Kusakatov, V.: Quasigroup String Processing - Part 3, Contributions, Sec. Math. Tech. Sci., MANU, XXI, 1, Skopje (2001)
16. McKay, B., Meynert, A., Myrvold, W.: Small Latin Squares, Quasigroups and Loops
17. Shcherbacov, V.: Elements of quasigroup theory and some its applications in code theory and cryptology
18. Wanless, I. M.: A Generalization of Transversals for Latin Squares
19. The On-Line Encyclopedia of Integer Sequances: A Web Resourse. `http://www.research.att.com/~njas/sequences/`
20. McCasland, R.,Sorge, V.: Automating Algebra's Tedious Tasks: Computerised Classification, Proc. First Worshop on Challenges and Novel Applications for Automated Reasoning, Miami, 37-40 (2003) `http://www.uclic.ucl.ac.uk/usr/jgov/cnaar.pdf`

Appendix: Program Codes

Mathematica modules for graphical presentation of quasigroups of order 4

1. $ETransformation[k, s, l, n]$
k - lists of quasigroups
s - starting periodic sequence
l - leader
n - number of transformations

```
kk=Get["m01.dat"];
    (lists of quasigroups)
s=Flatten[Table[{1,2,3,4},{i,1,25}]];
    (starting sequence)
cryptone[q_,s_,l_]:=Module[{},
    b[0]=l;
    For[i=0,i<=Length[s]-1,i++,
        b[i + 1]=q[[b[i],s[[i+1]]]]
    ];
    niza[t]=Table[b[i],{i,1,Length[s]}]
]
cryptntimes[q_,s_,l_,n_]:=Module[{s1=s,l1=l},
    Transf={};
    For[ik=1,ik<=n,ik++,
        k=cryptone[q,s1,l1];
        Transf=Join[Transf,{k}];
        s1=k
    ];
    Transf
]
ETransformation[q_,s_,l_,n_]:=Module[{},
    For[qt=1,qt<=576,qt++,
        t=cryptntimes[First[q[[qt]]],s,l,n];
        p[qt]=Graphics[RasterArray[Reverse
        [Table[Hue[t[[i,j]]/4],{i,1,n},{j,1,n}]]],
        PlotLabel -> qt];
        If[Mod[qt,4]==0,Show[GraphicsArray
        [Table[p[qq],{qq,qt-3,qt}]]]
        ]
    ]
```

```
]
```

2. $DTransformation[k, s, l, n]$
   k - lists of quasigroups
   s - starting periodic sequence
   l - leader
   n - number of transformations

```
kk=Get["m01.dat"];
    (lists of quasigroups)
s=Flatten[Table[{1,2,3,4},{i,1,25}]];
    (starting sequence)
decryptone[q_,s_,l_]:=Module[{},
    s1=s;
    s1=Prepend[s1,l];
    For[i=1,i<=Length[s1]-1,i++,
        b[i]=q[[s1[[i]],s1[[i+1]]]]
    ];
    niza[t]=Table[b[i],{i,1,Length[s1]-1}]
]
decryptntimes[q_,s_,l_,n_]:=Module[{s1=s,l1=l},
    Transf={};
    For[ik=1,ik<=n,ik++,
        k=decryptone[q,s1,l1];
        Transf=Join[Transf,{k}];
        s1=k
    ];
    Transf
]
DTransformation[q_,s_,l_,n_]:=Module[{},
    For[qt=1,qt<=576,qt++,
        t=decryptntimes[First[q[[qt]]],s,l,n];
        p[qt]=Graphics[RasterArray[Reverse
        [Table[Hue[t[[i,j]]/4],{i,1,n},{j,1,n}]]],
        PlotLabel -> qt];
        If[Mod[qt,4]==0,Show[GraphicsArray
        [Table[p[qq],{qq,qt-3,qt}]]]
        ]
    ]
]
```