Classifications of Quasigroups of Order 4 by Parastrophic Quasigroup Transformation

Vesna Dimitrova [1]

joint research with
V. Bakeva[1], *A. Popovska-Mitrovikj*[1] *and*
A. Krapež[2]

[1]Faculty of Computer Science and Engineering,UKIM, Skopje, Macedonia
[2]Serbian Academy of Sciences and Arts, Beograd, Serbia

Loops ′11Třešť, Czech Republic, 25-27 July 2011

Outline

- Introduction
- Quasigroups and transformations
- Parastrophes and transformations
- Classifications of quasigroups
- Conclusion

Introduction

- Application of quasigroups
  - *cryptography*
  - *coding theory*
  - *design theory,...*
- Properties of quasigroups
  - *algebraic structures*
  - *quasigoup identities*
  - *number of quasigroups, ...*

Quasigroups

Not all quasigroups are suitable for cryptographic purposes!

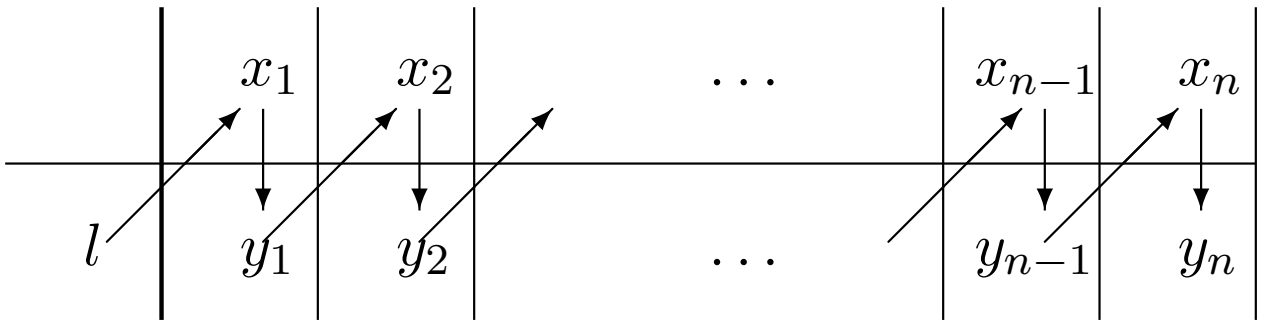
- Classifications of quasigroups
  - *algebraic properties*
  - *images of sequences obtained by quasigroup transformations:*
    - **fractal**
    - **non-fractal**

Quasigroup E-transformation

Assuming that $(A, *)$ is a given quasigroup, for a fixed letter $l \in A$ we define transformation $E = E_{*,l} : A^+ \to A^+$

Definition

$$E_{*,l}(x_1 \dots x_k) = y_1 \dots y_k \Leftrightarrow \begin{cases} y_1 = l * x_1, \\ y_j = y_{j-1} * x_j, \quad j = 2, \dots, k \end{cases}$$



Example of E-transformation

Quasigroup

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

E-transformation

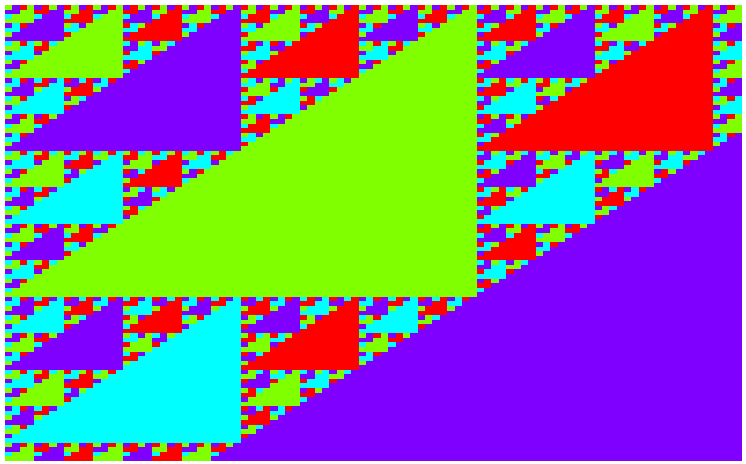
e_1	3 4 4 2 2 2 1 2 3 4 1 1 1 1 2 3 3 3 4 1	$=$	α		
1	4 3 4 1 3 2 1 3 1 1 2 1 2 1 3 1 4 2 2 1	$=$	α_1	$=$	$e_1(\alpha)$
1	1 4 3 3 1 3 3 1 2 1 3 3 2 1 4 4 3 2 4 4	$=$	α_2	$=$	$e_1(\alpha_1)$
1	2 2 3 1 2 3 1 2 3 3 1 4 1 2 2 2 3 2 2 2	$=$	α_3	$=$	$e_1(\alpha_2)$

Fractal Structures

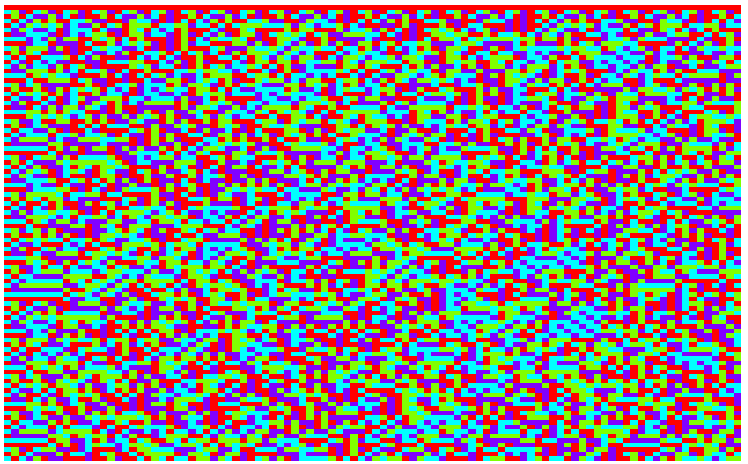
Paper

Dimitrova V., Markovski S.: ***Classification of quasigroups by image patterns*****, Proc. of CIIT 2007, Macedonia, pp. 152 - 160.**

92



191



Proof of the fractal structure of quasigroups

Paper

Markovski S., Dimitrova V., Samardziska S.: *Identities Sieves for Quasigroups*, Quasigroups and Related Systems, vol.18 No. 2, 2010, pp. 149-164

- In this paper using the quasigroup identities the authors give a proof of the fractal structure of quasigroup transformations for the some quasigroups of order 4.

Motivation

Paper

Krapež, A.: *An Application Of Quasigroups in Cryptology*, Proceeding of the Mathematical Conference 2010 - Dedicated to Professor Gorgi Cupona (2010)

- In this paper using quasigroup parastrophes, the author gives an idea for quasigroup string transformation based on parastrophes which can be applicable in cryptography.
- Here, we propose an improvement of this quasigroup transformation.

Parastrophes

Every quasigroup $(Q, *)$ has a set of five quasigroups, called parastrophes denoted with $/, \backslash, \cdot, //, \backslash\backslash$ are defined in the following table.

Parastrophic operation					Name
$x\backslash y = z$	$\Longleftrightarrow$	$x * z = y$			left division
$x/y = z$	$\Longleftrightarrow$	$z * y = x$			right division
$x \cdot y = z$	$\Longleftrightarrow$	$y * x = z$			opposite multiplication
$x//y = z$	$\Longleftrightarrow$	$y/x = z$	$\Longleftrightarrow$	$z * x = y$	opposite right division
$x\backslash\backslash y = z$	$\Longleftrightarrow$	$y\backslash x = z$	$\Longleftrightarrow$	$y * z = x$	opposite left division

Notations for parastrophic operations:

$$f_1(x, y) = x * y, \quad f_2(x, y) = x\backslash y, \quad f_3(x, y) = x/y,$$
$$f_4(x, y) = x \cdot y, \quad f_5(x, y) = x//y, \quad f_6(x, y) = x\backslash\backslash y.$$

PE - Parastrophic E-transformation

- Let p be a positive integer and $x_1x_2\dots x_n$ be an input message.
- Using E-transformation we define a parastrophic transformation $PE = PE_{l,p} : A^+ \to A^+$ as follows.
- At first, let $d_1 = p$, $q_1 = d_1$, $s_1 = (d_1 \bmod 6) + 1$ and $A_1 = x_1x_2\dots x_{q_1}$.
- Applying the transformation $E_{f_{s_1},l}$ on the block A_1, we obtain the encrypted block

$$B_1 = y_1y_2\dots y_{q_1-2}y_{q_1-1}y_{q_1} = E_{f_{s_1},l}(x_1x_2\dots x_{q_1}).$$

PE - Parastrophic E-transformation

- Further on, using last two symbols in B_1 we calculate the number $d_2 = 4y_{q_1-1} + y_{q_1}$ which determines the length of the next block.
- Let $q_2 = q_1 + d_2$, $s_2 = (d_2 \bmod 6) + 1$ and $A_2 = x_{q_1+1} \dots x_{q_2-1} x_{q_2}$.
- After applying $E_{f_{s_2}, y_{q_1}}$, the encrypted block B_2 is

$$B_2 = y_{q_1+1} \dots y_{q_2-2} y_{q_2-1} y_{q_2} = E_{f_{s_2}, y_{q_1}}(x_{q_1+1} \dots x_{q_2-2} x_{q_2-1} x_{q_2}).$$

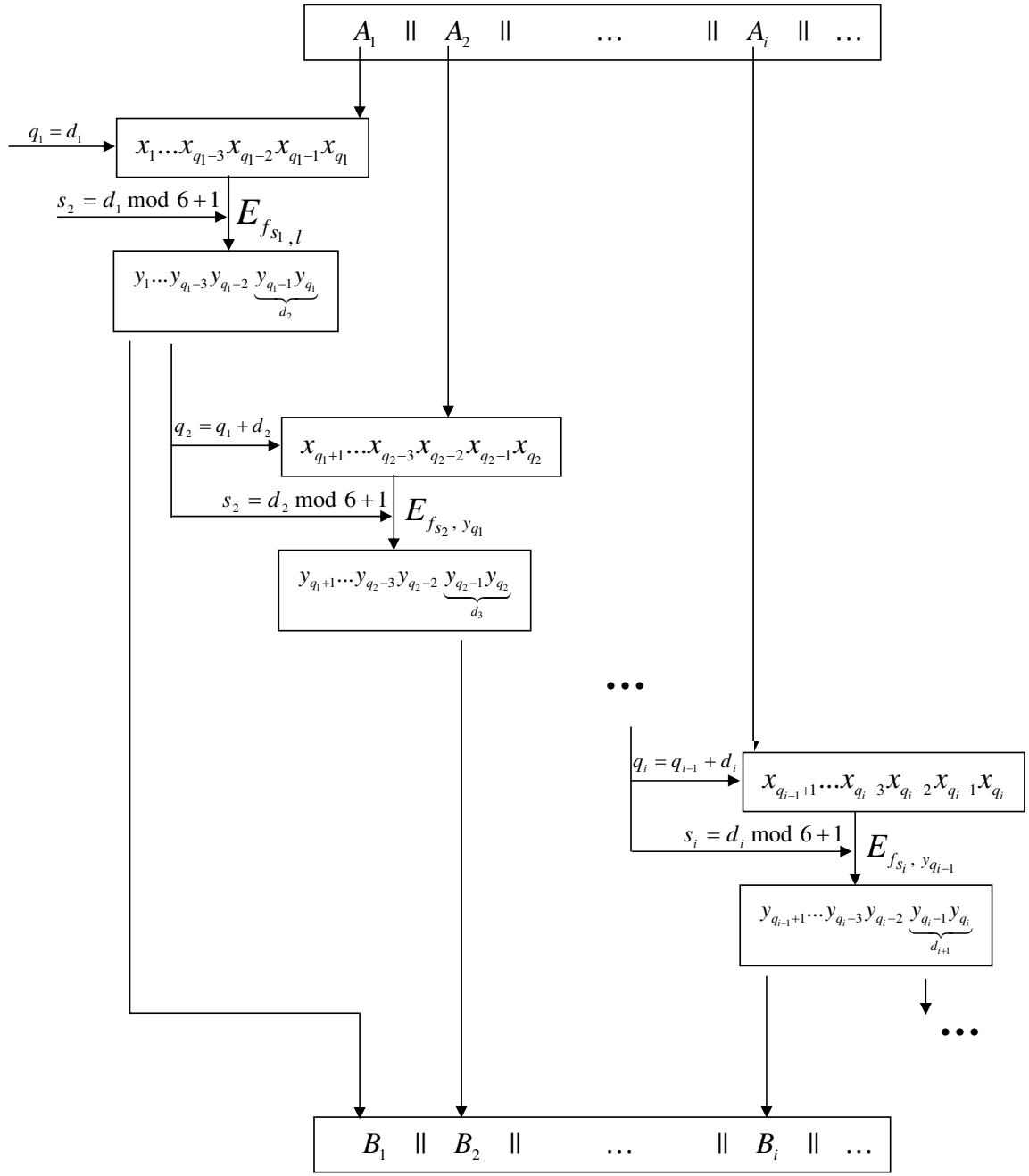
PE - Parastrophic E-transformation

- In general case, for given i, let the encrypted blocks B_1,..., B_{i-1} be obtained and d_i be calculated using the last two symbols in B_{i-1} as previous.
- Let $q_i = q_{i-1} + d_i$, $s_i = (d_i \mod 6) + 1$ and $A_i = x_{q_{i-1}+1} \dots x_{q_i-1} x_{q_i}$.
- We apply the transformation $E_{f_{s_i}, y_{q_{i-1}}}$ on the block A_i and obtain the encrypted block

$$B_i = E_{f_{s_i}, y_{q_{i-1}}}(x_{q_{i-1}+1} \dots x_{q_i}).$$

- Now, the parastrophic transformation is defined as

$$PE_{l,p}(x_1 x_2 \dots x_n) = B_1 || B_2 || \dots || B_r.$$



Parastrophic transformation PE

PE - Parastrophic E-transformation

- For given $l_1, \ldots, l_n$ and $p_1, \ldots, p_n$, we define mappings PE_1, PE_2, $\ldots$, PE_n as previous, such that PE_i is corresponding to p_i and l_i.
- Let

$$PE^{(n)} = PE^{(n)}_{(l_n,p_n),\ldots,(l_1,p_1)} = PE_n \circ PE_{n-1} \circ \cdots \circ PE_1,$$

where $\circ$ is the usual composition of mappings.

PE - Parastrophic E-transformation

Experimentally, we proved the following results:

Let $\alpha \in A^+$ be an arbitrary string and $\beta = PE^{(n)}(\alpha)$. Then m-tuples in β are uniformly distributed for $m \leq n$.

Classifications of quasigroups of order 4

Proposition

The set of all quasigroups (depending on the number of different parastrophes) is divided in 4 classes. The number of elements of each class of quasigroups of order 4 is:

No. parastrophes	No. quasigroups
1	16
2	2
3	240
6	318
Total	576

Classifications of fractal quasigroups of order 4

Proposition

The class of fractal quasigroups of order 4 is divided in 4 subclasses. The number of elements of each class is:

No. parastrophes	No. quasigroups
1	16
2	2
3	96
6	78
Total	192

Proposition

All fractal quasigroups of order 4 have fractal parastrophes.

Classifications of non-fractal quasigroups of order 4

Proposition

The class of non- fractal quasigroups of order 4 is divided in just 2 subclasses. The number of elements of each class is:

No. parastrophes	No. quasigroups
3	144
6	240
Total	384

Parastrophic fractal quasigroups

- Let apply the new transformation $PE^{(n)}$ to the sequence 123412341234... and consider the fractal structure of the obtained image.

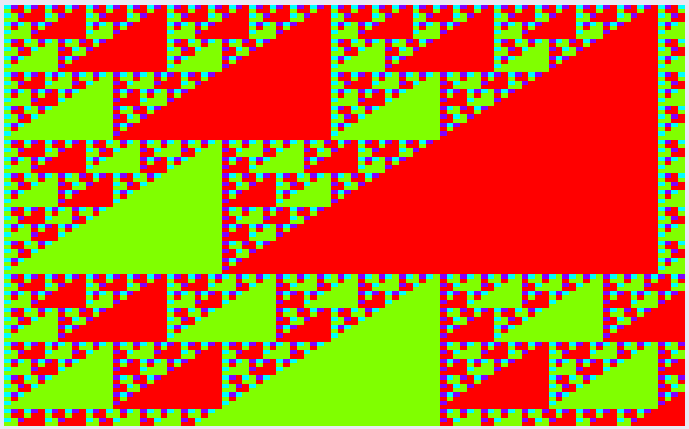
Definition

Quasigroups with fractal structure obtained after applying of PE-transformation are called *parastrophic fractal quasigroups*.

Fractal, but Parastrophic Non-fractal Quasigroup

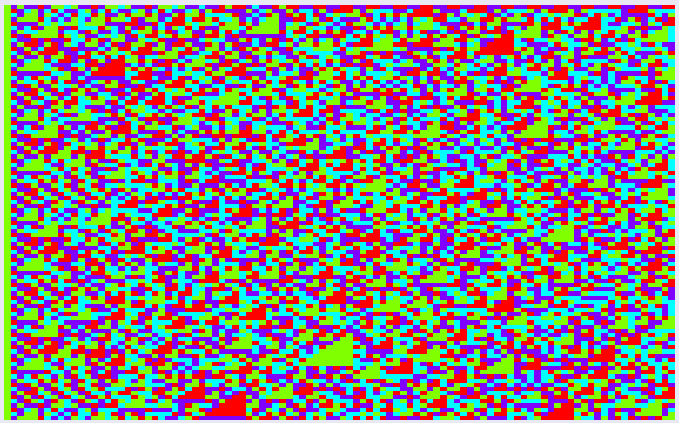
Fractal Quasigroup

40 Kvazigrupa



Parastrophic Non-Fractal Q.

40 Kvazigrupa



Proposition

Some of fractal quasigroups are parastrophic fractal, and some of them are not.

PE - transformation and classifications

Proposition

The set of all 192 *fractal quasigroups is divided in* 2 *subclasses:*

No. par.	No. parastroph. fractal
1	16
2	0
3	72
6	0
Total	88

No. par.	No. parastroph. non-fractal
1	0
2	2
3	24
6	78
Total	104

Properties of Parastrophic Fractal Quasigroups

Each parastrophic fractal quasigroup satisfies the identity $(I): \ x(x(x(xy))) = y$ and belongs to one of the following class:

- Loops (L)
- Totally symmetric quasigroups (TS)
- Left Loops (LL), Right symmetric quasigroups (RS)
- Right Loops (RL), Left symmetric quasigroups (LS)
- Left Loops, Skew symmetric quasigroups (SS)
- Right Loops, Skew symmetric quasigroups
- Commutative quasigroups (C), Skew symmetric quasigroups

Properties of Parastrophic Fractal Quasigroups

Parastrophic Fractal Quasigroups

Using the previous notations, the set of all parastrophic quasigroups can be presented as:

$$I \cap [L + TS + (LL \cap RS) + (RL \cap LS) + (LL \cap SS) + (RL \cap SS) + (C \cap SS)]$$

Conclusion

The analyses of the obtained results show that:

- Parastrophic fractal quasigroups should not be used for cryptographic primitives, since they have fractal structure, properties of symmetry and shape.
- These parastrophes tranformations are more suitable for designing of cryptographic primitives.

Thank you for your attention!