PARASTROPHIC QUASIGROUP STRING PROCESSING

Verica Bakeva Vesna Dimitrova Aleksandra Popovska-Mitrovikj
UKIM, Faculty of the Natural Sciences and Mathematics, Institute of Informatics
{verica,vesnap,aleksandrap}@ii.edu.mk

Abstract

In this paper, we propose a new quasigroup string transformation based on quasigroup parastrophes. Using the proposed quasigroup string transformation, a new classification of quasigroups of order 4 is given.

Key words: quasigroup, string transformation, parastrophe, parastrophic fractal and parastrophic non-fractal quasigroup.

I. Introduction

The quasigroup string transformations E and their properties were considered in several papers ([1], [2], [3], [4], [6] and [7]).

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

$$(\forall u,v\in Q)(\exists! x,y\in Q)\ \ (x*u=v\ \&\ u*y=v) \qquad (1)$$

In fact, (1) says that a groupoid $(Q,*)$ is a quasigroup if and only if the equations $x*u=v$ and $u*y=v$ have unique solutions x and y for each given $u,v\in Q$. It has been noted that every quasigroup $(Q,*)$ has a set of five quasigroups, called parastrophes denoted with $/,\backslash,\cdot$, $//,\backslash\backslash$ which are defined on Table 1.

Table 1: Parastrophes of quasigroup operations $*$

Parastrophes operation				
$x\backslash y=z$	$\Longleftrightarrow$	$x*z=y$		
$x/y=z$	$\Longleftrightarrow$	$z*y=x$		
$x\cdot y=z$	$\Longleftrightarrow$	$y*x=z$		
$x//y=z$	$\Longleftrightarrow$	$y/x=z$	$\Longleftrightarrow$	$z*x=y$
$x\backslash\backslash y=z$	$\Longleftrightarrow$	$y\backslash x=z$	$\Longleftrightarrow$	$y*z=x$

Further on, we introduce the following notations for parastrophe operations:

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

Let $A=\{1,\dots,s\}$ be an alphabet ($s\geq 2$) and denote by $A^+=\{x_1\dots x_k|\ \ x_i\in A,\ k\geq 1\}$ the set of all finite strings over A.

Note that $A^+=\bigcup_{k\geq 1}A^k$, where $A^k=\{x_1\dots x_k|\ x_i\in A\}$. Assuming that (A,f_i) is a given quasigroup, for a fixed letter $l\in A$ (called leader) we define transformation $E=E_{f_i,l}:A^+\to A^+$ by

$$E_{f_i,l}(x_1\dots x_k)=y_1\dots y_k\Leftrightarrow\left\{\begin{array}{lcll} y_1 & = & f_i(l,x_1), & \\ y_j & = & f_i(y_{j-1},x_j), & j=2,\dots,k\end{array}\right. \qquad (2)$$

where $x_i,y_i\in A$.

II. Parastrophic transformation

In [8], using quasigroup parastrophes, Krapež gives an idea for quasigroup string transformation which can be applicable in cryptography. Further on, we propose an improvement of this quasigroup transformation.

Let p be a positive integer and $x_1x_2\dots x_n$ be an input message. Using previous transformation E, 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

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

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

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

In general case, for given i, let the encrypted blocks $B_1,\dots,B_{i-1}$ be obtained and d_i be calculated using the last two symbols in B_{i-1} as previous. Let $q_i=q_{i-1}+d_i$, $s_i=(d_i \bmod 6)+1$ 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

$$PE_{l,p}(x_1x_2\dots x_n)=B_1||B_2||\dots||B_r. \qquad (3)$$

Note that the length of the last block A_r may be shorter than d_r (depends on the number of letters in input message). The transformation PE is schematically presented in Figure 1.

For arbitrary quasigroup operations $f_1,f_2,\dots,f_n$ on the set A, Markovski et al. [1] defined mappings $E_1,E_2,\dots,E_n$, as in (2) by choosing fixed elements

$l_1, l_2, \ldots, l_n \in A$ (such that E_i is corresponding to f_i and l_i) and

$$E^{(n)} = E^{(n)}_{l_n,\ldots,l_1} = E_n \circ E_{n-1} \circ \ldots \circ E_1$$

where $\circ$ is the usual composition of mappings. They proved the following theorem.

Theorem 1: Let $\alpha \in A^+$ be an arbitrary string and $\beta = E^{(n)}(\alpha)$. Then m-tuples in β are uniformly distributed for $m \leq n$.

Similarly, for given $l_1, \ldots l_n$ and $p_1, \ldots, p_n$, we define mappings PE_1, PE_2, ..., PE_n, as in (3) such that PE_i is corresponding to p_i and l_i. Using them, we define the transformation $PE^{(n)}$ as follows:

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

With the transformation $PE^{(n)}$, we make a new classification of quasigroups of order 4.

III. Classification of quasigroups of order 4

In [5], using image pattern, Dimitrova and Markovski give a classification of quasigroups of order 4 as fractal and non-fractal. This classification is made on the following way. Let start with a periodical sequence 123412341... with length 100 and apply 100 times the E-transformation given in (2) with given leaders. The authors present the transformed sequences visually using different color for each symbol 1,2,3,4. On this way, they obtain an image pattern for each quasigroup and they analyze the structure of this patterns. If the pattern has a fractal structure, the suitable quasigroup is called fractal. In opposite case, the quasigroup is called non-fractal. The number of fractal quasigroups of order 4 is 192 and the number of non-fractal quasigroups is 384. Fractal quasigroups are not good for designing of cryptographic primitives since they give a regular structures.

In this paper, we make a similar classification using new PE-transformation. If a quasigroup gives fractal structure with PE-transformation we named it as *parastrophic fractal* quasigroup. In the opposite case, the quasigroup is called *parastrophic non-fractal*.

We conclude that all parastrophic fractal quasigroups are fractal, but not all fractal quasigroups are parastrophic fractal. In the Figure 2, we give the quasigroup with lexicographic number 40 which is fractal (a), but it is not parastrophic fractal (b). We find that from 192 fractal quasigroups, 88 are parastrophic fractal and the rest of them (104 quasigroups) are parastrophic non-fractal.

IV. Conclusion

In this paper, we give a generalization PE of transformation defined in [8] and using this transformation we make a classification of quasigroups of order 4 as parastrophic fractal and parastrophic non-fractal. On this way, we increase the number of quasigroups of order 4 which are suitable for designing of cryptographic primitives.

References

[1] Markovski,S., Gligoroski,D., Bakeva,V.: *Quasigrouop string processing: Part 1*, Contributions, Sec. Math. Tech. Sci., MANU, **XX 1-2** (1999) 13–28.

[2] Markovski, S., Kusakatov, V.: *Quasigroup String Processing: Part 2*, Contributions, Sec. Math. Tech.Sci., MANU, XXI, 1-2 (2000) 15–32.

[3] Markovski, S., Kusakatov, V.: *Quasigroup String Processing: Part 3*, Contributions, Sec. Math. Tech.Sci., MANU, XXIII-XXIV, 1-2 (2002-2003), 7–27.

[4] Markovski, S. and Bakeva, V.: *Quasigrouop string processing: Part 4*, Contributions, Sec.Math.Tech.Sci., MANU, **XXVII-XXVIII**, 1-2 (2006-2007), p.41–53.

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

[6] Markovski, S.: *Quasigroup string processing and applications in cryptography*, First Intern. Conf. Mathematics and Informatics for Industry, Thessaloniki, Greece (2003), 278–289.

[7] Bakeva, V., Dimitrova, V.: *Some Probabilistic Properties of Quasigroup Processed Strings useful in Cryptanalysis*, M.Gusev, P.Mitrevski (Eds.): ICT-Innovations 2010, Springer (2010), pp. 61-70.

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

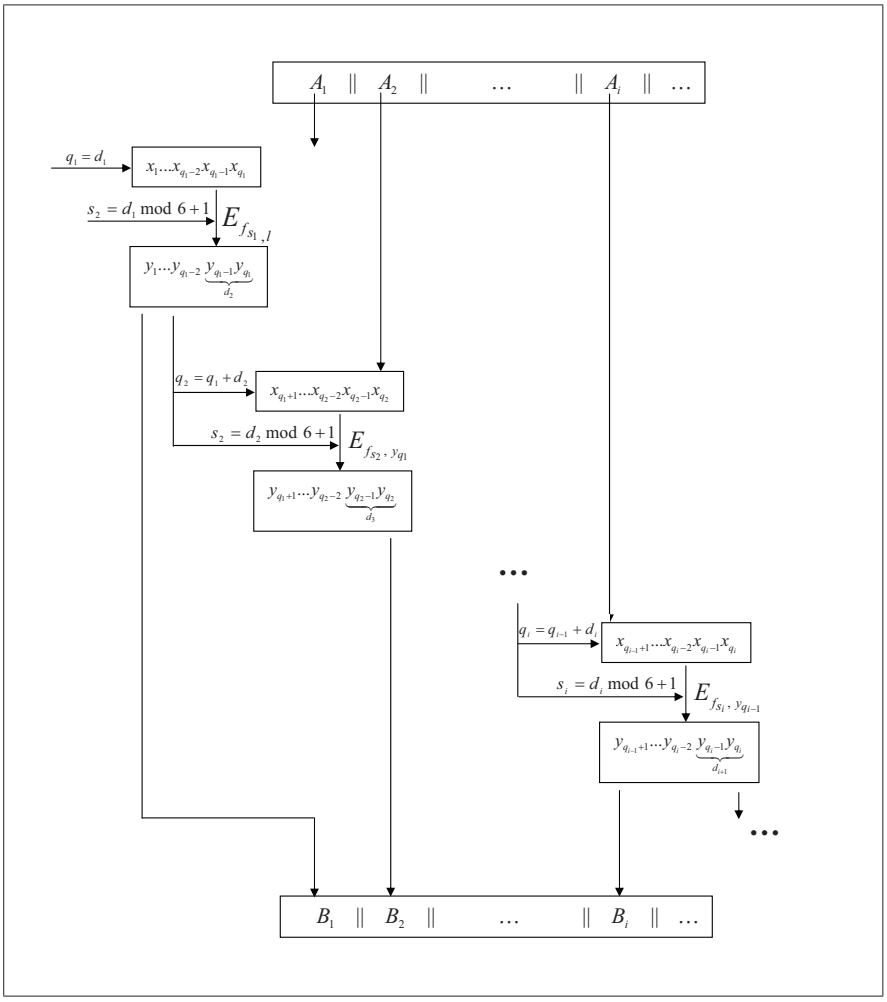
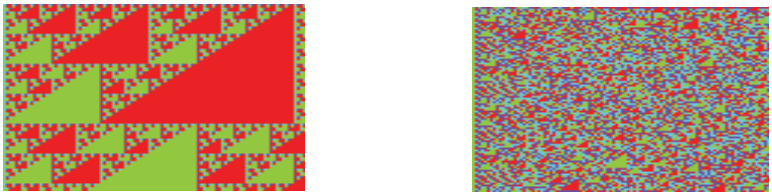


Figure 1: Parastrophic transformation PE



(a) (b)

Figure 2: Quasigroup 40 is fractal, but parastrophic non-fractal