Testing Quasigroup Identities using Product of Sequence*

Eliška Ochodková[1], Jiří Dvorský[1], Václav Snášel[1] and Ajith Abraham[2]

[1] Department of Computer Science
FEECS, VŠB – Technical University of Ostrava
17. listopadu 15, 708 33 Ostrava – Poruba, Czech Republic
{eliska.ochodkova, jiri.dvorsky, vaclav.snasel,}@vsb.cz

[2] Center of Excellence for Quantifiable,
Quality of Service,
Norwegian University of Science and Technology
O.S. Bragstads plass 2E,
N-7491 Trondheim, Norway
ajith.abraham@ieee.org

Abstract. Non-associative quasigroups are well known combinatorial designs with many different applications. Many cryptographic algorithms based on quasigroups primitives have been published. There are several classifications of quasigroups based on their algebraic properties. In this paper we propose a new classification of quasigroups based upon strings (product elements) obtained by a product of a sequence. It is shown in this paper that the more various results of the product elements, the less associative quasigroup.

1 Introduction

Almost all known constructions of cryptographic algorithms have made use of associative algebraic structures such as groups and fields. There is a possibility to use non-associative quasigroups [7] , well known combinatorial designs with a lot of theoretical results concerning them, too. Many cryptographic algorithms based on quasigroups primitives have been published. Proposed cryptographic algorithms are used for ciphering [15], for constructing pseudorandom generators [9], hash functions [12], for zero knowledge protocols [2], etc. Majority of published algorithms can be seen as rather simple experimental algorithms. As a representative of the ambitious proposals include the stream cipher Edon80 [5] published as an eSTREAM[3] candidate, and the NIST's SHA-3[4] competition candidate, hash function Edon$\mathcal{R}$ [4].

If a quasigroup is a base of some cryptographic primitive, it is necessary to examine whether its algebraic properties, structure or other features possess a

[3] http://www.ecrypt.eu.org/stream/
[4] http://csrc.nist.gov/groups/ST/hash/sha-3/

* This paper was partially supported by GACR 205/09/1079 grant.

security risk to the whole cryptographic algorithm. From all existing quasigroups of a given order we have to select those, which do not have various identities (as associativity is) and in which various identities appears rarely, or rather not at all. Properties of small quasigroups (e.g. of order 4), represented as a look-up table only, may be examined by the exhaustive search. But examination of identities of the quasigroups of a large order, e.g. 2^{16}, may not be easy.

Testing of all possible identities at once may be expensive, both in terms of time and in terms of space. Therefore we have focused on associativity only. If associativity holds, then for each element $a, b, c \in Q : a \circ (b \circ c) = (a \circ b) \circ c$. The situation differs when we work with non-group (i.e. non-associative) structure: $a \circ (b \circ c) \neq (a \circ b) \circ c$. We have made experiments with powers a^k of all elements $a \in Q$, where $k = 2, 3, \ldots, n, n = |Q|$, obtained by a product of a sequence. Obtained results were evaluated and compared to the number of associative triples identified for each quasigroup used in experiments. Tested set of quasigroups was the subset of all distinct quasigroups of order 8. For better representation of the results, we have used their visualization.

The paper is organized as follows. Motivation of our work is introduced in Section 2, some necessary concepts are given here too. Concept of a product of sequence, experiments and their results are described in Section 3. Finally, Section 4 comprise conclusion and some ideas of future works.

2 Preliminaries

2.1 Basic Concepts

Definition 1. *Let $A = \{a_1, a_2, \ldots, a_n\}$ be a finite alphabet, $n \times n$* Latin square *L of order n is a matrix with entries $l_{ij} \in A$, $i, j = 1, 2, \ldots, n$, such that each row and each column consists of different elements of A.*

The numbers of all LSs of order ≤ 11 are known [14]. Number of distinct Latin squares[5] of a given order grows exceedingly quickly with the order. Latin squares are equivalent to quasigroups. The multiplication table of a quasigroup of order n is a Latin square of order n, and conversely every Latin square of order n is the multiplication table of a quasigroup of order n [3].

Definition 2. *A* quasigroup *is a pair $(Q, \circ)$, where $\circ$ is a binary operation on (finite) set Q such that for all not necessarily distinct $a, b \in Q$, the equations $a \circ x = b$ and $y \circ a = b$. have unique solutions. We say that quasigroup $(Q, \circ)$ is of order n if $|Q| = n$.*

In general, the operation $\circ$ is neither a commutative nor an associative operation. Every quasigroup satisfying the associative law has an identity element and is, hence, a group. There is, for example, 576 distinct quasigroups of order 4, but only 16 are associative. So non-associative quasigroups dominate heavily.

[5] We abbreviate 'Latin square' to LS.

Isotopism. Various methods of generating a practically unlimited number of quasigroups of a (theoretically) arbitrary order are known and shown in various publications. One common way of creating quasigroups is through isotopism [3].

Definition 3. *Let* $(Q_1, \cdot)$ *and* $(Q_2, \circ)$ *be two quasigroups with* $|Q_1| = |Q_2|$. *An ordered triple* (α, β, γ) *of one-to-one mappings* α, β, γ *of the set* Q_1 *onto the set* Q_2 *is called an* isotopism *of* Q_1 *upon* Q_2 *if* $\alpha(x) \circ \beta(y) = \gamma(x \cdot y)$ *for all* $x, y \in Q_1$.

One can prove that the set of all isotopisms of a quasigroup of order n forms a group of order $(n!)^3$. It should be noted that the mapping γ permutes the elements in the table of operations in a quasigroup Q_1, while α and β operate on the elements of the row and column borders of this table, respectively.

2.2 Motivation

Design of many of the existing algorithms is based on *quasigroup string transformations* [7, 11]. The following concepts are taken from [7].

Consider an alphabet (i.e. a finite set) Q, and denote by Q^+ the set of all nonempty words (i.e. finite strings) formed by the elements of Q. Let $(Q, \circ)$ is a quasigroup. Let $q = q_1 q_2 \dots q_n \in Q^+, q_i \in Q$ and $l \in Q$ is a fixed element called leader. For each $l \in Q$ we define two functions $e_{l_\circ}$ and $d_{l_\circ} \colon Q^+ \to Q^+$ as follows:

$$e_{l_\circ}(q) = b_1 b_2 \dots b_n \iff b_1 = l \circ q_1,\ b_2 = b_1 \circ q_2,\ \dots,\ b_n = b_{n-1} \circ q_n \quad (1)$$

i.e. $b_{i+1} = b_i \circ q_{i+1}$ for each $i = 0, 1, \dots, n-1$, where $b_0 = l$, and

$$d_{l_\circ}(q) = c_1 c_2 \dots c_n \iff c_1 = l \circ q_1,\ c_2 = q_1 \circ q_2,\ \dots,\ c_n = q_{n-1} \circ q_n \quad (2)$$

i.e. $c_{i+1} = q_i \circ q_{i+1}$ for each $i = 0, 1, \dots, n-1$, where $q_0 = l$.

The functions $e_{l_\circ}$ and $d_{l_\circ}$ are called $e-$ and $d-$*transformation* of Q^+ based on the operation $\circ$ with leader l. In general, several quasigroup operations on the set Q can be used for defining quasigroup transformations. Let, $\circ_1, \circ_2, \dots, \circ_k$ be such a sequence of (not necessarily distinct) quasigroup transformations. We may also choose leaders $l_1, l_2, \dots l_k \in Q$ (not necessarily distinct), and then the compositions $\bullet$ of mappings

$$E_k = E_{l_1 l_2 \dots l_k} = e_{l_1} \bullet e_{l_2} \bullet \dots \bullet e_{l_k} \quad (3)$$

and

$$D_k = D_{l_1 l_2 \dots l_k} = d_{l_1} \bullet d_{l_2} \bullet \dots \bullet d_{l_k} \quad (4)$$

are said to be $E-$ and $D-$transformations of Q^+ respectively. In the last notation, we use e_{l_1} for the clarity, but formally we should use $e_{l_{1_{\circ_1}}}$.

The experiments with the length of a period of a string generated by e-transformations are mentioned in [6] and in [10]. Quasigroups are divided into two groups, to *linear* and *exponential* quasigroups. What algebraic properties must quasigroups of order 4 have to be linear resp. exponential? The quasigroups are of a small order (order 4), it is therefore impossible to say whether (besides identities) it is their structure, which affects the resulting period of the transformed string. Quasigroups of larger order are more convenient for analogical tests described in Sec. 3.

3 Experiment with Product of Sequence

Let $\circ$ be the binary operation. Consider the finite sequence A of elements $a_1, \ldots, a_n$, $a_i \in A, i = 1, 2, \ldots, n, n \geq 2$. What does mean a product of this sequence? Clearly, for $n = 2$ we have $a_1 \circ a_2$, by juxtaposition $a_1 a_2$. For $n = 3$ a product of the sequence a_1, a_2, a_3 is defined as a set consisting of product elements $a_1(a_2 a_3)$ and $(a_1 a_2)a_3$. The product is denoted as $\{a_1 a_2 a_3\}$ and symbol $a_1 a_2 a_3$ means any product element. Generally, we can define a product of a sequence of n elements of the set A as follows [1].

Definition 4. *The product of a sequence $a_1, a_2, \ldots, a_n$ of elements $a_i \in A, i = 1, 2, \ldots, n$ is the set $\{a_1 a_2 \ldots a_n\}$ defined by:*

- *for $n = 2$ the set $\{a_1 a_2\}$ consist of only one element $a_1 a_2$,*
- *for $n \geq 2$ the set $\{a_1 a_2 \ldots a_n\}$ is defined as*

$$\{a_1 a_2 \ldots a_n\} = \{a_1\}\{a_2 \ldots a_n\} \cup \{a_1 a_2\}\{a_3 \ldots a_n\} \cup \ldots \cup \{a_1 \ldots a_{n-1}\} \cup \{a_n\}.$$

The n elements can be joined, without changing their order, in $\frac{(2n-2)!}{n!(n-1)!}$ ways. For e.g. $n = 1, 2 \ldots, 10$ we obtain $1, 1, 2, 5, 14, 42,\ 132, 429,\ 1430, 4862$ ways of joining n elements. These numbers are called *Catalan numbers* [8]. The mth Catalan number, for $m \geq 0$ is given by:

$$C_m = \frac{1}{m+1}\binom{2m}{m} = \frac{(2m-2)!}{m!(m-1)!}.$$

If the operation $\circ$ on the set A does not hold an associativity law, we can generally obtain distinct values $a_1 a_2 \ldots a_n$ (not one common value) for all C_m ($m = n - 1$, because Catalan numbers are numbered from 0) possible product elements of the product set $\{a_1 a_2 \ldots a_n\}$ of the sequence $a_1, a_2, \ldots, a_n$.

3.1 Experiment

We have tested product $\{q_1 q_2 \ldots q_k\}$ of the sequence $q_1, q_2, \ldots, q_k$, where all $q_i \in Q, i = 1, 2, \ldots, k$ are equal. So, if all elements are equal, each element is denoted as a and we will compute a product $\{\underbrace{aa \ldots a}_{k}\}$ of the sequence $\underbrace{a, a, \ldots, a}_{k}$. This product consists of all C_{k-1} product elements. Questions is, how many distinct values $q_1 q_2 \ldots q_k = \underbrace{aa \ldots a}_{k} = a^k$ for all $a \in Q$ we obtain. In the ideal case we can obtain all possible values as a result; the set of possible values has only max. n values from Q (of order n) for all powers a^k.

Better information about the identities in the given quasigroup gain from the evaluation of particular product elements by the e-transformation defined in Eq. (2). Therefore all strings $b_1 \ldots b_8$, see Fig. 1, obtained during evaluation of product elements of a^k (for $k = 8, a^8 = b_8$, Fig. 1) were stored. The experiment:

- Generate a quasigroups Q of order n.

- For each element $a \in Q$ and for each $k, 2 \leq k \leq n$ create the product $\{aa \dots a\}$ of the sequence $a, a, \dots, a$, evaluate all C_{k-1} product elements a^k.
- Store strings $b_1 \dots b_k$ and compute the number of their occurrence during evaluation of all product elements a^k.

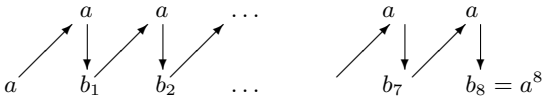


Fig. 1. e-transformation used for valuing the product elements $a^k, k = 8$

3.2 Quasigroups used in tests

Quasigroups were represented by corresponding Latin squares. We decided to use a subset of quasigroups of order 8. We have tested:

- all $n! = 40320$ distinct quasigroups isotopic to additive group $(\mathbb{Z}_8, +)$ when only permutation α was not an identity permutation,
- a set of one million randomly generated quasigroups,
- a set of special quasigroups that consist of e.g. additive group $(\mathbb{Z}_8, +)$, of six well described quasigroups published in [13], etc.

3.3 Ideal results

Results are shown on the highest (8th) power of element a. There are $C_7 = 429$ distinct ways how to obtain it.

- Ideally, for each $a \in Q$, i.e. for each $a = 0, 1, \dots, 7$, we obtain all 8 possible values of $a^8 \in Q$.
- For each $a \in Q$ we obtain all 429 distinct strings $b_1 \dots b_8$.
- Finally, for each quasigroup $(Q, \circ)$ we ideally obtain all together $429 \times 8 = 3432$ distinct strings $b_1 \dots b_8$ for all $a \in Q$.

3.4 Experimental results

Results of experiments are shown on the set of five chosen quasigroups represented by their corresponding LSs. The first quasigroup is randomly generated quasigroup No. 24 represented by L_{24}. The second quasigroup, obtained by non-affine isotopy [13], is represented by corresponding LS L_{103}. The third quasigroup is quasigroup 104 obtained by complete mapping [13] and represented

by LS L_{104}. The fourth quasigroup is quasigroup No. 106, from [13], is represented by LS L_{106}. The last quasigroup $(Q_1, \circ)$ with No. 107 is represented by corresponding LS L_{107} (this quasigroup is the additive group $(\mathbb{Z}_8, +)$).

Numbers of distinct values a^8 for each $a \in Q$ for five chosen quasigroups are shown in Table 1. Only quasigroups No. 24 and 104 have ideal results. Conversely, quasigroup's No. 107 results are always the same; a^8 is always 0.

Results of the process evaluating the strings $b_1 \dots b_8$: the best results have quasigroups No. 24 and 104. Number of all distinct strings is higher comparing the remaining three quasigroups. This fact is evident from Table 2 (sums of distinct strings for each quasigroup and all $a \in Q$ are shown). The higher number of associative triples, the lower the sum of all strings. Results were also visualized, Sec. 3.5. The greater number of subsquares of different brightness in the image corresponds with the greater number of distinct strings $b_1 \dots b_8$ for each a^8, see Figs. 2 and 3.

Table 1. Number of obtained distinct values of a^8 for each $a \in Q$

	L_{24}	L_{103}	L_{104}	L_{106}	L_{107}
0^8	8	8	8	8	$1(0^8 = 0)$
1^8	8	8	8	1	$1(1^8 = 0)$
2^8	8	8	8	2	$1(2^8 = 0)$
3^8	8	$1(3^8 = 3)$	8	3	$1(3^8 = 0)$
4^8	8	8	8	4	$1(4^8 = 0)$
5^8	8	8	8	2	$1(5^8 = 0)$
6^8	8	8	8	2	$1(6^8 = 0)$
7^8	8	8	8	2	$1(7^8 = 0)$

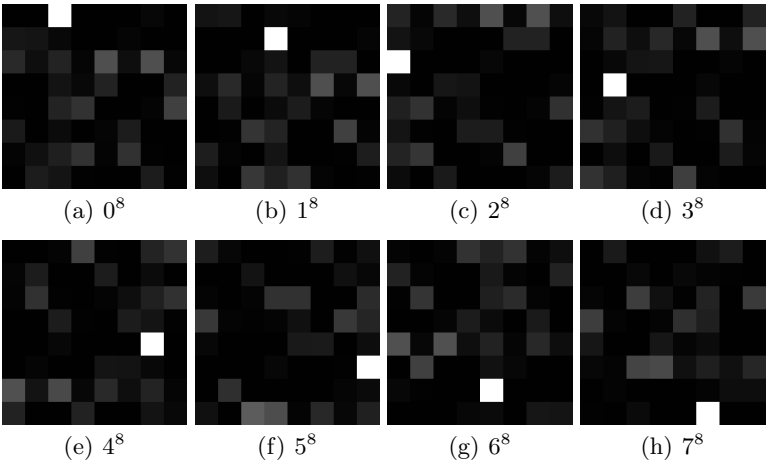
Table 2. Number of obtained strings $b_1, \dots, b_8$ for all $a \in Q$

	L_{24}	L_{103}	L_{104}	L_{106}	L_{107}
number of strings	2426	2019	2666	664	307
number of AT	72	70	60	304	512

3.5 Visualization of strings $b_1, ..., b_n$ valuation

We have focused only on the 8th power of quasigroups elements. For each quasigroup $(Q, \circ)$ and for each $a^8, a \in Q$, we have generated 512×512 pixels images where each subsquare (64×64 pixels) represents one element l_{ij} of tested quasigroup represented by corresponding Latin square $L, l_{ij} \in L$. The more visits of particular element, the brighter subsquare. The brightness of the subsquares is calculated relatively to the number $C_7 \times ir = 429 \times 6 = 2574$, where $ir = 6$

is number of strings from a^2 to a^8 when computing a^8. The greater the sum of distinct strings $b_1 \dots b_n$, the greater the number of subsquares of different brightness in the image.



(a) 0^8 (b) 1^8 (c) 2^8 (d) 3^8

(e) 4^8 (f) 5^8 (g) 6^8 (h) 7^8

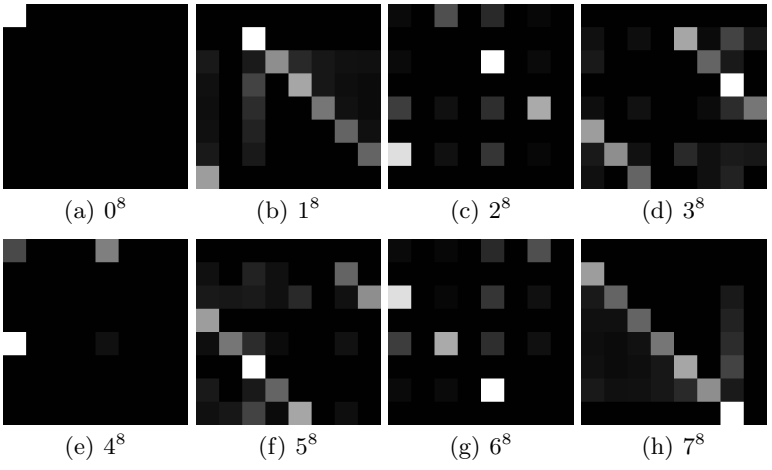
Fig. 2. Quasigroup No. 104

4 Conclusion

Our goal is to find a new way of testing the properties of large quasigroups and to explore the interpretation of experimental results. We have reported a new classification of quasigroups based upon strings (product elements) obtained by a product of a sequence. As is shown, the more various results of the product elements, the less associative quasigroup. More precisely, values of all possible product elements from the product set of a sequence of elements from a given quasigroup were examined and relationships between experiment results and associativity of tested quasigroup have been tested. Testing of quasigroup's identities through the product of a sequence is an appropriate method with good results. Experiments will be repeated with quasigroups of larger order. Several consecutive applications of a quasigroup transformations on the sequences will be tested, too.

References

1. O. Borůvka. *Foundations of the theory of groupoids and groups.* Wiley, 1976.
2. J. Dénes, and T. Dénes. Non-associative algebraic system in cryptology. Protection against "meet in the middle" attack. *Q. and Related Systems* 8 (2001): 7–14.



(a) 0^8 (b) 1^8 (c) 2^8 (d) 3^8

(e) 4^8 (f) 5^8 (g) 6^8 (h) 7^8

Fig. 3. Quasigroup No. 107

3. J. Dénes, and A. Keedwell. *Latin Squares and their Applications.* New York: Akadémiai Kiadó, Budapest, Academic Press, 1974.
4. D. Gligoroski, et al. EdonR cryptographic hash function. NIST's SHA-3 hash function competition, 2008, http://csrc.nist.gov/groups/ST/hash/sha-3/index.html
5. D. Gligoroski, S. Markovski, L. Kocarev, and J. Svein. The Stream Cipher Edon80. The eSTREAM Finalists, *LNCS* 4986 (2008): 152–169.
6. D. Gligoroski. One-Way Functions and One-Way Permutations Based on Quasigroup String Transformations. *Cryptology ePrint Archive.* Report 2005/352.
7. D. Gligoroski, and S. Markovski. Cryptographic potentials of quasigroup transformations. Talk at EIDMA Cryptography Working Group, Utrecht, 2003.
8. P. Hilton, and J. Pedersen. Catalan Numbers, Their Generalization, and Their Uses. *Journal The Mathematical Intelligencer,* 13, no. 2 (1991): 64–75.
9. C. Kościelny. NLPN Sequences over GF(q). *Quasigroups an Related Systems* 4 (1997): 89–102.
10. S. Markovski, D. Gligoroski, and J. Markovski. Classification of quasigroups by random walk on torus. *J. of Appl. Math. and Comp.* 19, no. 1-2 (2005): 57–75.
11. S. Markovski, D. Gligoroski, and L. Kocarev. Unbiased Random Sequences from Quasigroup String Transformations. in *12th International Workshop FSE,* Paris, LNCS 3557 (2005): 163.
12. S. Markovski, D. Gligoroski, and V. Bakeva. Quasigroup and Hash Functions. *Disc. Math. and Appl.*, In Proceedings of the 6th ICDMA, Bansko, 2001.
13. K. A. Meyer. A new message authentication code based on the non-associativity of quasigroups. Ph.D Thesis, 2006, http://orion.math.iastate.edu/dept/thesisarchive/PHD/KMeyerPhDSp06.pdf
14. B. D. McKay, and I. M. Wanless. On the Number of Latin Squares. *Journal Annals of Combinatorics* 9, no. 3 (2005): 335–344.
15. E. Ochodková, and V. Snášel. Cryptographic Algorithms with Uniform Statistics. In *NATO Regional Conference on Military Communications and Informations Systems* Zegrze, Poland: 165–172, 2001.
16. K. Toyoda. On axioms of linear functions. *P*roc. Imp. Acad. Tokyo, 17 (1941): 221–227.