A NEW CRYPTOGRAPHIC PROPERTY BASED ON THE ORTHOGONALITY OF QUASIGROUPS

Hristina Mihajloska
UKIM, Faculty of Computer Science and Engineering
hristina.mihajloska@finki.ukim.mk

Abstract

In order to achieve better cryptographic properties of quasigroups of order 4, we make a new classification. In our research we use an approach with generalized quasigroup orthogonality, which leads us to this interesting classification, on reducible and irreducible quasigroups. Existence of the classes of reducible and irreducible quasigroups depends on the property of orthogonality of quasigroups which can be studied in the light of right quasigroups. Two right quasigroups r, s of order 4 are orthogonal if and only if there exists a quasigroup q of the same order and $r \cdot q = s$ is satisfied. Furthermore, for every quasigroup out of 576 of order 4 we find all pairs of orthogonal right quasigroups that satisfy previously mentioned property.

Experimentally we show that all quasigroups which belong to the class of linear by their Boolean presentation can be presented as product of two other linear quasigroups. All this quasigroups formed the class of product reducible quasigroups and remaining belong to the class of product irreducible quasigroups.

Key words: cryptography, orthogonality, quasigroup, right quasigroup

I. Introduction

The earliest interest for quasigroups and their application in cryptography, according to the eminent specialists Denes and Keedwell [5] in the area of quasigroups, dates from 1948. In that year the German mathematician R. Shauffler in his PhD dissertation reduced the problem of breaking the known Vigenere cipher to determining a particular Latin square. From then on the theory of quasigroups further developed for in order significant results to be achieved in the 80's of the 20th century.

Almost all known error detecting and correcting codes, cryptographic algorithms and encrypting systems use associative algebraic structures like groups and fields. On the other hand, it is possible to use non-associative structures like quasigroups and neo-fields in almost all areas of coding theory and cryptography. The efficiency of quasigroups in cryptography is based on the fact that the quasigroups are in a way generalized permutations and the number of quasigroups of order n is greater than $n! * (n-1)! * \cdots * 2! * 1!$. Researches in the area of cryptography have shown that cryptographic primitives based on non-associative algebraic structures have much better properties than the one based on associative structures. The development in this direction is going upward.

Our research interest is focus on a lightweight cryptography. This type of cryptography is not a definition for a weak crypto or a cryptography that intended to replace the traditional cryptography. However lightweight cryptography should influence new algorithms that are small and fast, which implementation require as lightweight hardware and software area as possible. Therefore we have interest in developing secure and small lightweight devices that are easy to use. In order to achieve this, the idea is to find out how we can use quasigroups of small order (order 4) to obtain a secure communication that fulfills the base principles of lightweight cryptography.

In this paper we present a new classification of quasigroups of order 4. Also we make a connection between the newly obtained classes and the classes of already known linear quasigroups by their Boolean presentation.

II. Preliminaries - Quasigroups and Orthogonality

In this section we give a brief mathematical introduction in the area of quasigroups and their properties suitable for cryptography. Definitions and properties are already known, so a more detailed explanation can be found in [1], [3], [4], [12], [13].

Let $(Q, *)$ be a finite binary groupoid, i.e., an algebra with one binary operation $*$ on the non-empty set Q and $a, b \in Q$.

Definition 1: A finite binary groupoid $(Q, *)$ is called a quasigroup if for all ordered pairs $(a, b) \in Q^2$ there exist unique solutions $x, y \in Q$ to the equations $x * a = b$ and $a * y = b$.

This implies the cancellation laws for quasigroup i.e., $x * a = x' * a \Longrightarrow x = x'$ and $a * y = a * y' \Longrightarrow y = y'$.

Given groupoid $(Q, *)$ and fixed element $a \in Q$, mappings $R_a, L_a : Q \to Q$, called right translation R_a and left translation L_a are defined by:

$$\begin{array}{rcl} R_a(x) & = & x * a, \\ L_a(x) & = & a * x \end{array} \qquad (1)$$

for every $x \in Q$.

Definition 2: Finite groupoid $(Q, *)$ is right (left) quasigroup if right (left) cancellation low holds:

$$x * a = x' * a \Longrightarrow x = x', \quad \forall a, x, x' \in Q, \qquad (2)$$

$$(a * x = a * x' \Longrightarrow x = x', \quad \forall a, x, x' \in Q). \qquad (3)$$

Any quasigroup is possible to be presented as a multiplication table known as Cayley table. The order of a quasigroup $(Q,*)$ is the cardinality $|Q|$ of the non-empty set Q. The set of all quasigroups of order n is denoted by $\mathbb{Q}_n$. The set of all right quasigroups of order n is denoted by $\mathbb{R}_n$. $\mathbb{Q}_n \subset \mathbb{R}_n$.

In what follows we will work with finite quasigroups of order 4.

Example 1: Let $Q = \{0,1,2,3\}$. A quasigroup $(Q,*)$ of order 4 has the following Cayley table:

$*$	0	1	2	3
0	0	1	2	3
1	3	2	1	0
2	2	3	0	1
3	1	0	3	2

(4)

Example 2: Let $R = \{0,1,2,3\}$. A right quasigroup $(R,*)$ of order 4 is given by its Cayley table shown in (5)

$*$	0	1	2	3
0	1	3	1	0
1	0	0	2	1
2	2	1	0	3
3	3	2	3	2

(5)

Quasigroups are closely related to Latin squares. Removing the topmost row and the leftmost column of the Cayley table of a quasigroup, results in a Latin square. A Latin square is an arrangement of n symbols in a $n \times n$ matrix such that no row and no column contains any of the symbols twice. Also in terms of Latin squares the right (left) quasigroups correspond to the column (row) latin square.

A. Orthogonality

The notion of orthogonality plays an important role in the theory of quasigroups, because it has good perspective in the area of cryptology. There are many research papers in this field. We reference some of them [8], [9], [10].

Two quasigroups are said to be orthogonal when we superimpose their Cayley tables, and every ordered pair of elements $(x,y) \in Q \times Q$ will be mentioned exactly once.

The concept of orthogonality can be described easily in algebraic language:

Definition 3: Two quasigroups $(Q,*)$, $(Q,\cdot)$ i.e. quasigroups with operations $*$ and $\cdot$ defined on the same set Q, are orthogonal if the system of equations

$$\begin{aligned} x * y &= a, \\ x \cdot y &= b \end{aligned} \tag{6}$$

has a unique solution for every pair of elements $(a,b) \in Q^2$.

We use the notation $(Q,*) \perp (Q,\cdot)$ to express orthogonality. It is clear that $(Q,*) \perp (Q,\cdot) \Longrightarrow (Q,\cdot) \perp (Q,*)$.

Example 3: This is an example of two orthogonal quasigroups of order 4.

$*_{q_1}$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	3	2	1	0
3	2	3	0	1

$*_{q_2}$	0	1	2	3
0	0	1	3	2
1	2	3	1	0
2	3	2	0	1
3	1	0	2	3

III. A new classification of quasigroups of order 4

It is well known that the set of all right quasigroups of order n, $\mathbb{R}_n$ together with an operation $\cdot$ builts a group $(\mathbb{R}_n,\cdot)$.

Let $r,s \in \mathbb{R}_n$, so we have

$$x *_{r\cdot s} y = (x *_r y) *_s y.$$

In 1942 Mann in his article [8] stated that two Latin squares L_1 and L_2 are orthogonal if and only if there exists a Latin square L_{12} such that $L_1 \cdot L_{12} = L_2$. Later in 1952 using the orthogonal property of row-Latin squares, Northon published a paper [11] in which he presented some useful lemmas and theorems about orthogonality.

Lemma 1: [11] A row-Latin square is orthogonal to the square I if and only if it is a Latin square.

Lemma 2: [11] If $A, B, \ldots, L$ are a set of mutually orthogonal row-Latin squares and X is any row-Latin square, then $XA, XB, \ldots, XL$ are a set of mutually orthogonal row-Latin squares.

From these two lemmas, implies the theorem below:

Theorem 1: [11] Two row-Latin squares A and B are orthogonal if and only if there is a Latin square L such that $A \cdot L = B$.

All these facts are generalized for the right quasigroups in the paper of Michael H. Damm [2], so we will use the following result.

Lemma 3: [2] Right quasigroups $r,s \in \mathbb{R}_n$ are orthogonal if and only if a quasigroup $q \in \mathbb{Q}_n$ exists with $r \cdot q = s$.

Example 4: Let $r \in \mathbb{R}_n$ and $q \in \mathbb{Q}_n$ are known, we find $s \in \mathbb{R}_n$ like $r \cdot q = s$

$*_r$	0	1	2	3
0	0	0	3	3
1	1	1	2	1
2	2	2	1	0
3	3	3	0	2

$\cdot$

$*_q$	0	1	2	3
0	3	2	1	0
1	2	1	0	3
2	1	0	3	2
3	0	3	2	1

$=$

$*_s$	0	1	2	3
0	3	2	3	2
1	2	3	2	1
2	0	1	0	0
3	1	0	1	3

and we can see in (7) that $r \perp s$

$*_r$	0	1	2	3
0	0	0	3	3
1	1	1	2	1
2	2	2	1	0
3	3	3	0	2

$\times$

$*_s$	0	1	2	3
0	3	2	3	2
1	2	3	2	1
2	0	1	0	0
3	1	0	1	3

$\rightarrow$

$(*_r, *_s)$	$(0,0)$	$(1,1)$	$(2,2)$	$(3,3)$
$(0,0)$	$(0,3)$	$(0,2)$	$(3,3)$	$(3,2)$
$(1,1)$	$(1,2)$	$(1,3)$	$(2,2)$	$(1,1)$
$(2,2)$	$(2,0)$	$(2,1)$	$(1,0)$	$(0,0)$
$(3,3)$	$(3,1)$	$(3,0)$	$(0,1)$	$(2,3)$

(7)

According to the previous Lemma 3 we make a program that produce all of the ordered pairs of right orthogonal quasigroups of order 4. Because the number of different right quasigroups from one quasigroup of order 4 is $(4!)^4$ we get $576 * (4!)^4$ different ordered pairs of orthogonal right quasigoups of order 4.

When we generate all pairs of orthogonal right quasigroups of order 4, we are interested whether among these pairs of right quasigroups there exist such that, which are in the same time quasigroups, or $r, s \in \mathbb{Q}_4$. There are only 144 quasigroups out of 576 of order 4 for which $r, s \in \mathbb{Q}_4$ is satisfied. The other interesting experimental result is that for every quasigroup the number of pairs (r, s) that are in the same time quasigroups is 48. So the total number of pairs (r, s) for which $r \cdot q = s$ and $r, q, s \in \mathbb{Q}_4$ is 6.912.

A. Reducible and irreducible quasigroups

In mathematical language irreducibility means that an object cannot be expressed as the product of two or more non-trivial factors in a given set, and the reducibility means that the object can be expressed as a product of two or more non-trivial factors in a given set. Also the property of irreducibility depends on the field. According to this, and having the set $\mathbb{Q}_4$ of all quasigroups of order 4, over the ring $\mathbb{Z}$ of integ
new classes of quasigroups of ord
quasigroups and class of irreducible quasigroups, given with the following definitions:

Definition 4: A quasigroup $q \in \mathbb{Q}_4$ is a product reducible if there exist two quasigroups $q_1, q_2 \in \mathbb{Q}_4$ such that $q = q_1 \cdot q_2$. A quasigroup is product irreducible if it is not reducible.

From our experimental results we find that the number of product reducible quasigroups of order 4 is 144. The set of product reducible quasigroups of order 4 is given in Table 1. They are presented with their lexicographic indexes [6].

Table 1: Class of product reducible quasigroups of order 4

{0, 3, 10, 13, 20, 23, 25, 26, 36, 39, 42, 45, 50, 53, 56, 59, 69, 70, 76, 79, 81, 82, 91, 92, 99, 100, 109, 110, 112, 115, 125, 126, 131, 132, 137, 138, 145, 146, 156, 159, 162, 165, 168, 171, 178, 181, 188, 191, 195, 196, 202, 205, 211, 212, 221, 222, 227, 228, 233, 234, 242, 245, 251, 252, 258, 261, 268, 271, 273, 274, 283, 284, 291, 292, 301, 302, 304, 307, 314, 317, 323, 324, 330, 333, 341, 342, 347, 348, 353, 354, 363, 364, 370, 373, 379, 380, 384, 387, 394, 397, 404, 407, 410, 413, 416, 419, 429, 430, 437, 438, 443, 444, 449, 450, 460, 463, 465, 466, 475, 476, 483, 484, 493, 494, 496, 499, 505, 506, 516, 519, 522, 525, 530, 533, 536, 539, 549, 550, 552, 555, 562, 565, 572, 575}

Let as look at the following example.

Example 5: Let $q \in \mathbb{Q}_4$ be with lexicographic index 92. The number of ordered pairs (r, s) such that $r \cdot q = s$ are 48 and all of the elements of that pairs belong to the class of product reducible quasigroups of order 4.

This leads to a more general propositions.

Proposition 1: Every product reducible quasigroup of order 4 can be presented only as a product of two other product reducible quasigroups of order 4.

Proposition 2: If q_1, q_2 and q_3 are product reducible quasigroups of order 4, and connected by the identity $q_1 \cdot q_2 = q_3$, then $q_1 \perp q_3$.

When we compare these classes of product reducible and irreducible quasigroups, with the classes of linear and non-linear quasigroups of order 4 [6], [7], we will note that the class of product reducible and the class of linear quasigroups is actually the same class of quasigroups of order 4. The same applies for the class of product irreducible and class of non-linear quasigroups. This implies the following:

Proposition 3: Every linear quasigroup of order 4 can be presented only as a product of two other linear quasigroups, thus

$$q_1 \cdot q_2 = q_3, \quad \text{iff} \quad q_1 \perp q_3, \quad \text{where} \quad q_1, q_2, q_3 \in \mathbb{Q}_4. \quad (8)$$

lers $n \neq 2, 6$ the maximum cardinality of a set of mutually orthogonal quasigroups of order n is less or equal to $n-1$, we find it interesting to see which quasigroups of order 4 form 3-tuples of mutually orthogonal quasigroups. According to Proposition 1, these 3-tuples of mutually orthogonal quasigroups of order 4 are actually 3-tuples of mutually orthogonal product reducible quasigroups of order 4.

A set of mutually orthogonal quasigroups is a set of pairwise orthogonal quasigroups. If $\{q_1, q_2, q_3\}$ is a set of mutually orthogonal quasigroups, than $q_1 \perp q_2$, $q_2 \perp q_3$ and $q_1 \perp q_3$ is satisfied.

Table 2: 3-tuples of mutually orthogonal product reducible quasigroups of order 4

{0, 76, 99},	{0, 196, 271},	{0, 304, 379},	{0, 476, 499},
{25, 50, 125},	{25, 222, 245},	{25, 330, 353},	{25, 450, 525},
{50, 146, 222},	{50, 353, 429},	{50, 450, 550},	{76, 171, 196},
{76, 379, 404},	{76,476, 575},	{99, 171, 271},	{99, 304, 404},
{99, 499, 575},	{125, 146, 245},	{125, 330, 429},	{125, 525, 550},
{146, 330, 450},	{146, 353, 525},	{171, 304, 476},	{171, 379, 499},
{196, 304, 575},	{196, 404, 499},	{222, 330, 550},	{222, 429, 525},
{245, 353, 550},	{245, 429, 450},	{271, 379, 575},	{271, 404, 476}

From Table 2 we can perceive that every quasigroup member can be met exactly four times in the given 3-tuples. Thus, we can say that every product reducible quasigroup from this set can be presented in exactly four

different ways as a product of two reducible quasigroups. The number of product reducible quasigroups of order 4 which can form 3-tuples of mutually orthogonal product reducible quasigroups is $4 * 3! = 24$. These quasigroups given with their lexicographic indexes, presented in Table 3 form the subclass of a class of product reducible quasigroups.

Table 3: Subclass of product reducible quasigroups of order 4

{0, 76, 99, 196, 271, 304, 379, 476, 499, 25, 50, 125, 222, 245, 330, 353, 450, 525, 146, 429, 550, 171, 404, 575}

IV. Conclusion

In this paper we define a new classification of the quasigroups of order 4. By connecting quasigroups of order 4 and their properties based on the orthogonality and linearity we find out new properties that are not known previously and many new open questions whose solutions are challenge for research in the field of higher order quasigroups. As a future work, all our experimental findings remain to be proven theoretically and generalized for the quasigroups of order n.

V. Acknowledgment

The author would like to thank Danilo Gligoroski, professor at the Norwegian University of Science and Technology, for his insightful ideas, valuable comments and clever question during this research.

References

[1] V. D. Belousov *Osnovi teorii kvazigrupp i lupp*, Nauka, Moskva, 1967
[2] H. Michael Damm, *Half quasigroups and generalized quasigroup orthogonality*, Elsevier, Discret Mathematics, pages 145-153, 2011
[3] J. Denes, and A. D. Keedwell, *Latin squares and their applications*, Academic Press Inc, Dec 1974
[4] J. Denes, and A. D. Keedwell, *Latin squares: New developments in the theory and applications*, Elsevier science publisher, 1991
[5] J. Denes, and A. D. Keedwell, *Some applications of non-associative algebraic systems in cryptology*, Pure Mathematics and Applications 12 (2), 2001
[6] V. Dimitrova *Quasigroup Processing String, their Boolean Representations and Application in Cryptography and Coding Theory*, PhD thesis, Ss. Cyril and Methodius University, Skopje, S. Markovski (promotor), 2010
[7] D. Gligoroski, V. Dimitrova, and S. Markovski *Quasigroups as Boolean functions, their equation system and Groebner bases*, Groebner Bases, Coding and Cryptography, Springer Berlin Heilderberg, 2009, pages 415-420
[8] H. B. Mann, *The Construction of Orthogonal Latin Squares*, The Annals of Mathematical Statistics, vol. 13, pages 418-423, 1942
[9] H. B. Mann, *On orthogonal Latin squares*, Bull. Amer. Math. Soc, pages 249-257, 1944
[10] G. L. Mullen and V. A. Shcherbacov, *On orthogonality of binary operations and squares*, Bul. Acad. Stiinte Repub. Mold. Mat 2, pages 3-42, 2005
[11] D. A. Northon, *Groups of orthogonal row-latin squares*, Pacific Journals of Mathematics, vol 2, pages 335-341, 1952
[12] V. A. Shcherbacov *Quasigroups in cryptology*, Computer Science Journal of Moldova, vol 17, pages 193-228, 2009
[13] J. D. H. Smith *An Introduction to Quasigroups and Their Representations*, Chapman and Hall/CRC, 2007