CLASSIFICATION OF TERNARY QUASIGROUPS OF ORDER 4 APPLICABLE IN CRYPTOGRAPHY

Vesna Dimitrova
Faculty of Natural Sciences and Mathematics
Institute of Informatics
Skopje, Macedonia

Hristina Mihajloska
Faculty of Natural Sciences and Mathematics
Institute of Informatics
Skopje, Macedonia

ABSTRACT

Quasigroups as algebraic structures are very suitable for construction of cryptographic primitives. There are several classifications of quasigroups. Most of them are made for binary quasigroups.
In this paper we consider ternary quasigroups of order 4. In order to obtain some suitable classification useful for designing cryptographic primitives, we investigate the structure of ternary quasigroups. Using some known classifications of binary quasigroups we give a classification of ternary quasigroups of order 4.

Keywords: quasigroups, ternary quasigroups, classification of quasigroups

I. INTRODUCTION

The finite quasigroups are algebraic structures that are used in many theories like cryptography, coding theory and design theory. Their application in cryptography is rapidly growing. The structures, properties and their large number allow them to be applied in this field. Nevertheless, not all quasigroups are suitable for constriction of cryptographic primitives. There are some quasigroups that usually produce undesirable properties of designs. For cryptographic purposes quasigroups have to be of a good quality. This implies that for successful application of quasigroups it is very important to know which quasigroups have good properties for some designs. The classification of quasigroups is a difficult problem, because the number of quasigroups of order $n \geq 5$ is too big.
In this paper we consider the ternary quasigroups of order 4. We investigate the structure of ternary quasigroups and using the classifications of binary quasigroups given in [2], [3] and [4] we give a classification of ternary quasigroups of order 4. Our goal is to find some good classification that separate ternary quasigroups of order 4 with good cryptographic properties from those with poor cryptographic properties.
A brief introduction to the notions of quasigroup and *n*-quasigroup are given in section 2. In section 3 we describe the method for ordering the finite *n*-quasigroups. The classification of ternary quasigroups of order 4 by their structures is given in section 4.

II. QUASIGROUPS AND n -QUASIGROUPS

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

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

In other words the equations $x*u=v$ and $u*y=v$ for each given $u,v \in Q$ have unique solutions x,y .
Latin square is equivalent combinatorial structure to quasigroup. A Latin square can be associated to any finite quasigroup $(Q,*)$ given by its multiplication table. It consists 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 on the bordering of the matrix of L by the main row and the main column of the multiplication table).
An *n*-groupoid $(n \geq 1)$ is algebra (Q,f) on a nonempty set Q as its universe and with one *n*-ary operation $f: Q^n \to Q$ [1].

An *n*-groupoid (Q,f) is said to be an *n*-quasigroup if any *n* of the elements $a_1,a_2,...,a_{n+1} \in Q$, satisfying the equality

$$f(a_1,a_2,...,a_n)=a_{n+1},$$

uniquely determine the other one.
A unary (Q,f) is in fact a permutation on the set Q .
Equivalent combinatorial structure to *n*-quasigroup is *n*-Latin square. Let $Q=\{1,2,...,r\}$, for $r>0$. An $\underbrace{r\times...\times r}_{n}$-matrix $L=[l_{i_1},...,l_{i_n}]$ such that for each $i_1,i_2,...i_{j-1},i_{j+1},...,i_n$ and for each j the $(i_1,...i_{j-1},i_{j+1},...,i_n)$-th row vector $(l_{i_1,...i_{j-1},1,i_{j+1},...,i_n},l_{i_1,...i_{j-1},2,i_{j+1},...,i_n},...,l_{i_1,...i_{j-1},r,i_{j+1},...,i_n}$ of L is a permutation of Q . The main body of the multiplication table of an *n*-quasigroup (Q,f) is an *n*-Latin square (see [8]). Conversely, from an *n*-Latin square we can obtain an *n*-quasigroup, by its bordering. (Note that a 1-Latin square is a permutation of Q , a 2-Latin square is a Latin square and a 3-Latin square is a Latin cube.)

III. ORDERING OF FINITE n -QUASIGROUPS

The problem of enumerating the set of *n*-quasigroups of given order *r* is well known problem. Up to day, is already known the number of binary quasigroups of order $r \leq 11$, the number of ternary quasigroups of order $r \leq 6$ and the number of *n*-quasigroups of order $r \leq 5$ for $n = 4, 5$ (see [10]).
For computing purposes we present the set of *n*-quasigroups of order *r* linearly and we order them lexicographically as follows. We take that the universe set is

$Q = \{1,2,...,r\}, r > 0$ and that the n-quasigroups are given by their n-Latin squares.

The unary quasigroups are linearly presented and lexicographically ordered in a natural way, since its 1-Latin square consists of only one permutation of Q. The linear presentation of a binary quasigroup of order r is given by string which consists of all its r linearly presented unary quasigroups. In this way the linear presentation of an n-quasigroup (Q, f) of order r is given by string which consists of all its r linearly presented $(n-1)$-quasigroups. Now, the lexicographic ordering of the linear presentations of all n-quasigroups of order r gives the ordering of the n-quasigroups.

For our research we consider the ternary quasigroups (3-quasigroups) of order 4. Their number is 55 296. We take that the set is $Q = \{1,2,3,4\}$ and that the ternary quasigroups are given by their Latin cubes. We use the lexicographical ordering of binary quasigroups given in [2] and using the method describe above we present a ternary quasigroup as a string of 64 characters that is a concatenation of the rows of the corresponding Latin squares. Then we apply the lexicographic ordering of all strings obtained from ternary quasigroups, assuming that the characters are already ordered. Therefore, the linear presentation of the first ternary quasigroup is the following:

1: 1234|2143|3412|4321||2143|1234|4321|3412||3412|4321|1234| 2143||4321|3412|2143|1234

Using the lexicographical numbers of binary quasigroups, we can see that the first ternary quasigroup is built up from the 1-th, 172-th, 405-th and 576-th binary quasigroups, when they are arranged one above the other.

According to the previous for better vision of ternary quasigroups of order 4 we present them graphically. On Figure 1 is given graphical presentation of the ternary quasigroup with lexicographic number 55296 (the last ternary quasigroup).

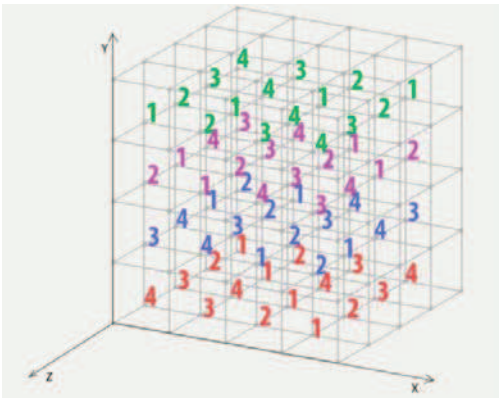

Figure 1: The ternary quasigroup 55296

IV. Classification of Ternary Quasigroups by Their Structures

In this section we use two known classifications of binary quasigroups and give a classification of ternary quasigroups.

First of them is the classification of quasigroups by graphical presentation of sequences obtained by quasigroup transformations given in [2] and [3], where two disjoint classes are presented, 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.

The second is the classification of quasigroups according to their Boolean representation given in [4] and [7], where three classes are presented, the class of so called linear quasigroups, the class of non-linear quasigroups and the class of pure non-linear quasigroups. In this classification the class of linear quasigroup is not recommended to be used in cryptography.

We consider the characterizations of these classifications and we make a classification of ternary quasigroups of order 4.

In order to obtain some suitable classification useful for designing cryptographic primitives, we investigate the structure of ternary quasigroups. This means that in one ternary quasigroup we consider all binary quasigroups and made classification depending on their properties. In a ternary quasigroup we consider all 12 binary quasigroups: 4 arranged one above the other (by y-axis on Figure 1), 4 arranged side by side (by x-axis) and 4 arranged one behind the other (z-axis).

Using the classification of binary quasigroups by graphical presentation of sequences obtained by quasigroup transformations we analyze how many binary quasigroups in given ternary quasigroup are "fractal" or "non-fractal" and we made the first classification of ternary quasigroups of order 4 given in Table 1.

Remark 1. In the tables bellow are given only the numbers of elements in each class. The lexicographical numbers of ternary quasigroups that belong in each class are given at the following link: http://it.winhost.labs.ii.edu.mk/ups/classes.rar

Class	No. of elements in class
C_f	12096
C_{nf}	21312
C_{sf}	21888
Total	55296

Table 1: Classification by fractality

C_f is the class of "fractal ternary quasigroups" - all 12 binary quasigroups in ternary quasigroups are fractal,

C_{nf} is the class of "non-fractal ternary quasigroups" - all 12 binary quasigroups in ternary quasigroups are non-fractal,

C_{sf} is the class of "semi fractal ternary quasigroups" - 6 quasigroups are fractal and 6 are non-fractal, more precisely,

2 of 4 binary quasigroups of each axes in ternary quasigroups are fractal and 2 are non-fractal.
For this classification the following theorem and corollary are true.

Theorem 1: *Let* (Q, f) *be a ternary quasigroup of order 4 build up from four binary quasigroups arranged one above the other. If all four binary quasigroups are fractal, then the four binary quasigroups arranged side by side and the four binary quasigroups arranged one behind the other are also fractal quasigroups.*

Corollary 1: *If in a ternary quasigroup all four binary quasigroups arranged one above the other are non-fractal (semi fractal), then the other eight binary quasigroups are also non-fractal (semi fractal) quasigroups.*

Using the classification of binary quasigroups according to their Boolean representation we analyze how many binary quasigroups in given ternary quasigroup are linear, non-linear or pure non-linear and we made the second classification of ternary quasigroups of order 4 given in Table 2.

Class	No. of elements in class
C_l	8640
C_{nl}	25920
C_{sl}	20736
Total	55296

Table 2: Classification by linearity

C_l is the class of "linear ternary quasigroups" - all 12 binary quasigroups in ternary quasigroups are linear,
C_{nl} is the class of "non-linear ternary quasigroups" - all 12 binary quasigroups in ternary quasigroups are non-linear and
C_{sl} is the class of "semi linear ternary quasigroups" - 6 quasigroups are linear and 6 are non-linear, more precisely, 2 of 4 binary quasigroups of each axes in ternary quasigroups are linear and 2 are non-linear.
The quasigroups that belong to the class C_{nl} of non-linear quasigroups are interesting for cryptographic purposes. The research done for this class showed that there are sub class such that all 12 binary quasigroups in a ternary quasigroup from this sub class are pure non-linear. We noted this sub class as C_{pnl} - the class of "pure non-linear ternary quasigroups". This class contains 6912 ternary quasigroups.

Remark 2. Theorem 1 and Corollary 1 are also true for this classification, if we have linear instead of fractal quasigroups in theorem and non-linear (semi linear) instead of non-fractal (semi fractal) in the corollary.

For application in cryptography or coding theory we are searching for ternary quasigroups with good properties. For this reason we are interesting for the ternary quasigroups that belong to the intersections of some of these classes. We made these intersections and obtained more specific classes.
In Table 3 is given the classification of ternary quasigroups of order 4 made as intersections of some of the classes

Class	No. of elements in class
$C_{f,l}$	8640
$C_{nf,nl}$	21312
$C_{nf,pnl}$	5760

Table 3: Classification by fractality and linearity

$C_{f,l}$ is the class of "fractal and linear ternary quasigroups" - all 12 binary quasigroups in ternary quasigroups are fractal and linear,
$C_{nf,nl}$ is the class of "non-fractal and non-linear ternary quasigroups" - all 12 binary quasigroups in ternary quasigroups are non-fractal and non-linear and
$C_{nf,pnl}$ is the class of "non-fractal and pure non-linear ternary quasigroups" - all 12 binary quasigroups in ternary quasigroups are non-fractal and pure non-linear.
For cryptographic applications is good the class of "non-fractal and pure non-linear ternary quasigroups".
Our additional research with these classifications was focused on finding ternary quasigroups of order 4 which contain only 4 binary quasigroups, not 12. This means that the same 4 quasigroups are obtained by all axes. We obtained only 240 ternary quasigroups with this property. According to the previous classifications the results are given in Table 4 and Table 5.

Sub class	No. of elements
$SubC_f$	96
$SubC_{nf}$	48
$SubC_{sf}$	96
Total	240

Table 4: Specific classification by fractality

Sub class	No. of elements
$SubC_l$	24
$SubC_{nl}$	72
$SubC_{sl}$	144
Total	240

Table 5: Specific classification by linearity

The notations of the sub classes are same as the notations of the classes given in the previous tables.
Our results about the sub class of pure non-linear ternary quasigroups C_{pnl}, showed that only 24 ternary quasigroups that belong to this sub class.

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

Acknowledgement The authors are gratitude to Prof. Smile Markovski for his useful comments and guidelines. That improved the quality of this paper.

REFERENCES

[1] Belousov, V. D: n-arnie Kvazigruppi (n-ary Quasigroups), Stiinca, Kisiniev, (1972).

[2] Dimitrova, V: "*Kvazigrupni transformacii i nivni primeni* (Quasigroup Transformations and Their Applications)", MSc thesis, Skopje, (2005).

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

[4] Gligoroski, D., Dimitrova, V., Markovski, S: "*Quasigroups as Boolean functions, their equation systems and Groebner bases*", Book "*Groebner Bases, Coding, and Cryptography*", Springer (2009), pp. 415–420

[5] Mahesar, Q., Sorge, V: "*Classification of Quasigroup-structures with respect to their Cryptographic Properties*", Proc. of the ARW 2009 Bringing the GAP between Theory and Practice, Liverpool, UK (2009) 23–25.

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

[7] Mileva, A: "*Cryptographic primitives and their applications*", PhD Thesis, Skopje, Macedonia, 2010.

[8] Markovski, S., Dimitrova, V., Mileva, A: "*A new method for computing the number of n-quasygroups*", The Journal "Buletinul Academiei de Stiinte a Republicii Moldova. Matematica", No.3 (52), (2006), pp. 57–64.

[9] Mullen G. L., Weber R. E: Latin cubes of order <= 5, Discrete Math.32 (1980), no. 3, 291–297.

[10] McKey B. D., Wanless I. M: A census of small latin hypercubes, SIAM J Disc. Math. 22 (2008), 719–736.