Прилози, *Одд. май. йех. науки*, МАНУ, **XXX**, 1–2 (2009), стр. 75–93
Contributions, *Sec. Math. Tech. Sci.*, MANU, **XXX**, 1–2 (2009), pp. 75–90
ISSN 0351–3246
UDC: 512.541.5: 512.548.7

Original scientific paper

QUASIGROUPS CONSTRUCTED FROM COMPLETE MAPPINGS OF A GROUP $\left(Z_2^n,\oplus\right)$

Aleksandra Mileva, Vesna Dimitrova

Abstract: The quasigroups constructed from complete mappings of a group $\left(Z_{2,}^n \oplus\right)$ in a term of their properties like: satisfying the associative, commutative and idempotent law, having proper subquasigroups, having left or right unit, their representation with ANF, their prop ratio tables and correlation matrices and satisfying some other identities are examined in this paper. This is important for their applicability in cryptography, coding theory and other fields. As an example, we give quasigroups constructed from 384 complete mappings of a group $\left(Z_2^3,\oplus\right)$.

Key words: quasigroup; complete mapping; TA-quasigroup

1. INTRODUCTION

There are many different ways of constructing quasigroups. One can construct a quasigroup by isotopies and/or their combination with Feistel network [12], with T-functions (special type of functions defined by Klimov and Shamir [9]), with diagonal method by complete mappings [15], with direct or quasi-direct product of smaller quasigroups [3, 17], (generalized) singular direct product [10, 16] etc.

In this paper are examined the quasigroups constructed by Sade's diagonal method from complete mappings of the group$\left(Z_2^n,\oplus\right)$, and specially, of the group $\left(Z_2^3,\oplus\right)$. There are 384 such quasigroups. In Section 2 are given some basic mathematical definition for quasigroups and complete mappings. Definition of prop ratio tables and correlation matrices are given in Section 3. Some propositions about constructed quasigroups are presented in Section 4. In Section 5 are shown a special case of quasigroups constructed from complete mappings of a group $\left(Z_2^3,\oplus\right)$. List of all complete mappings of group $\left(Z_2^3,\oplus\right)$ are given in Appendix A and corresponding quasigroups (in ANF) constructed from complete mappings of a group $\left(Z_2^3,\oplus\right)$ in Appendix B.

2. QUASIGROUPS AND COMPLETE MAPPINGS

Definition 2.1. Let * be a binary operation on *Q*. The groupoid (*Q*,*) is a **quasigroup** if the following law is satisfied:

$$\forall \mathrm{a, b} \in \mathrm{Q}) (\exists! \mathrm{~x, y} \in \mathrm{Q}) (\mathrm{a} * \mathrm{x} = \mathrm{y}*\mathrm{a} = \mathrm{b})$$

Related combinatorial structures to finite quasigroups are the Latin squares, since the main body of the multiplication table of a quasigroup is a Latin square [1].

Quasigroup (*Q*,*) have a proper subquasigroup *H*, if $H \subset Q$, and (*H*, *) is a quasigroup.

Definition 2.2 A **complete mapping** of a group (G, +) is a bijection θ*: G→G* such that the mapping ϕ*: G→G* defined by $\phi(x) = -x + \theta(x)$ ($\phi = -I + \theta$, where *I* is the identity mapping) is also a bijection of *G*. The mapping ϕ is said to be the **orthomorphism** associated to complete mapping θ.

A group *G* is **admissible** if there is a complete mapping θ*: G→G*. Some properties about admissible groups are given in [8, 13, 14].

Proposition 2.1 Let (*G*, +) be a group and let θ*: G→G* be a bijection. If $\theta(x) = x$ and $\theta(y) = y$ for some $x \neq y \in G$, then θ is not a complete mapping of (*G*, +).

Proof. Let $\theta(x) = x$ and $\theta(y) = y$ for some $x \neq y \in G$ and let ϕ: *G→G* be defined as $\phi(x) = -x + \theta(x)$. Then ϕ is not a bijection, because $\phi(x) = 0$ and $\phi(y) = 0$. This implies that θ is not a complete mapping of (*G*, +).

The method for creating a quasigroup from an admissible group is proposed by Sade [15]:

Proposition 2.2 Let $(Q,+)$ be an admissible group with complete mapping θ. If * is an operation on Q defined by

$$x * \mathrm{y} = \theta(x - y) + y, \tag{1}$$

where $x, y \in Q$, then $(Q,*)$ is a quasigroup.

In this paper are considered only complete mappings of the Abelian group $\left(Z_2^n, \oplus_n\right)$, where $\oplus_\mathrm{n}$ is bitwise XOR operation on words with n bits. For this group the operation * is defined as:

$$x * y = \theta(x \oplus_n y) \oplus_n y \tag{2}$$

Definition 2.3 Let $(G,+)$ be a group. The mapping $f\colon G \to G$ is an **affine mapping** if $f(x + y) = f(x) + f(y) - f(0)$ for each $x, y \in G$, where $0 \in G$ is the identity element. A **linear mapping** is an affine mapping f with $f(0) = 0$.

In the following, we give some definitions for special kind of quasigroups.

Definition 2.4 A quasigroup $(Q, *)$ is called **Shroeder quasigroup** if it satisfy the identity

$$(x * y) * (y * x) = x$$

for all $x, y \in Q$.

Definition 2.5 A quasigroup $(Q,*)$ is called **totally anti-symmetric** (**TA-quasigroup**) if it satisfy the following implications

$$(1)\ (c * x) * y = (c * y) * x \Rightarrow x = y\,,$$

$$(2)\ x * y = y * x \Rightarrow x = y,$$

for all $c, x, y \in Q$.

The quasigroup that satisfies only the first implication is called **weak totally anti-symmetric** (**WTA-quasigroup**).

TA-quasigroups are used in check digit systems for recognizing early typing errors [6]. Let $(Q,*)$ be a quasigroup and let $d_m d_{m-1}...d_1$ be a given number. The check digit is defined to be the unique solution d_0 of the equation

$$((...((d_m * d_{m-1}) * d_{m-2}) * ...) * d_1) * d_0 = 0$$

The cancellation laws and the TA property guarantee the detection of the two most frequent errors: the single errors (*...a...* → *...b...*) and the transposition errors (*...ab...* → *...ba...*).

3. CORRELATION MATRICES AND PROP RATIO TABLES

A *Boolean function f* is a function $f: \mathrm{Z}_2^n \to \mathrm{Z}_2$. A *vector-valued Boolean function h* is a mapping $h: \mathrm{Z}_2^n \to \mathrm{Z}_2^m$ and it can be decomposed into m component Boolean functions (h_0, h_1, ..., $h_{m\text{-}1}$). Quasigroups can be examined as vector valued Boolean function. For example, if $(Q, *)$ is a quasigroup of order 8 then it can be represented as vector-valued Boolean function $h: \mathrm{Z}_2^6 \to \mathrm{Z}_2^3$ where (x_0, x_1, x_2), (x_3, x_4, x_5), $(y_0, y_1, y_2) \in Q = \mathrm{Z}_2^3$ and

$$h(x_0, x_1, x_2, x_3, x_4, x_5) = (x_0, x_1, x_2) * (x_3, x_4, x_5) = (y_0, y_1, y_2)$$

The correlation matrix of a vector-valued Boolean function is a useful concept [5] for proving some properties of Boolean functions and mappings. The elements of the correlation matrices are the correlation coefficients associated with linear combinations of input bits and linear combinations of output bits. Linear cryptanalysis [11] can be seen as the exploitation of correlations between linear combinations of bits of different intermediate encryption values in a block cipher calculation. So, correlation matrices can be used for understanding the mechanisms of linear cryptanalysis.

Definition 3.1 The **correlation coefficient** associated with a pair of Boolean functions $f(a)$ and $g(a)$ is denoted by $C(f, g)$ and it is given by

$$C\,(f, g) = 2P[f\,(a) = g\,(a)] - 1$$

where P is probability of *f*(*a*) = *g*(*a*). The correlation coefficient range is between −1 and 1. If it is different from 0, the functions are said to be **correlated**.

A **selection vector** *w* is a binary vector that selects all components *i* of a vector *a* where $w_i = 1$. For example, the selection vector (1, 0, 1) selects the bits a_0 and a_2 from vector $a = (a_0, a_1, a_2)$. $w^T a$ represents the linear combination of the components of a vector *a* selected by *w*. All correlation coefficients between linear combinations of input bits and output bits of the mapping *h* can be arranged in a correlation $2^m \times 2^n$ – matrix C^h. C_{uw} is the element in the *u*-row and the *w*-column and it is equal to $C\left(u^T h(a), w^T a\right)$. The rows in this matrix can be interpreted as

$$(-1)^{u^T h(a)} = \sum_w C_{uw}^h (-1)^{w^T a}.$$

This means that the real-valued function corresponding to a linear combination of output bits can be written as a linear combination of the real-valued functions corresponding to a linear combination of input bits.

Other useful concept of the Boolean functions and mappings are prop ratio tables [4]. This concept is important for differential cryptanalysis [2]. Let *a* and *a** be *n*-bit vectors with bitwise difference *a* + *a** = *a'*. Let *b* = *h*(*a*), *b** = *h*(*a**) and *b'*= *b* + *b**. Hence, the difference *a'* propagates the difference *b'* through mapping *h* and this can be represented by $(a' \dashv h \vdash b')$.

Definition 3.2 The **prop ratio** R_p of a difference propagation $(a' \dashv h \vdash b')$ is given by

$$Rp\,(a' \dashv h \vdash b') = 2^{-n} \sum_a \delta\left(b' + h(a + a') + h(a)\right)$$

where $\delta(w)$ is the real-valued function equal to 1 if *w* is the zero vector and 0 otherwise.

The prop ratio range is between 0 and 1. If a pair is chosen uniformly from the set of all pairs (*a*, *a**) with *a* + *a** = *a'*, the equality *h*(*a*) + *h*(*a**) = *b'* is true with some probability. It is clear that $\sum_b R_p\,(a' \dashv h \vdash b') = 1$.

4. ANALYSIS OF QUASIGROUPS CONSTRUCTED FROM COMPLETE MAPPINGS OF THE GROUP $\left(\mathrm{Z}_2^n, \oplus_n\right)$

Some properties like associability, commutability, the idempotent law, having left or right unit and satisfying some identities for quasigroups constructed from complete mappings of the group $\left(\mathrm{Z}_2^n, \oplus_n\right)$ are examined. Specially, for quasigroups constructed from complete mappings of the group $\left(\mathrm{Z}_2^3, \oplus_3\right)$, are examined their prop ratio tables, correlation matrices, their representation with ANF (Algebric Normal Form) and do they have proper subquasigoup.

Proposition 4.1 The quasigroup $(Q,*)$, constructed by a complete mapping θ of the group $\left(\mathrm{Z}_2^n, \oplus_n\right)$ with operation * defined by equation (2) is a Shroeder quasigroup.

Proof. If $x, y \in Q$, then

$$\begin{aligned}(x * y) * (y * x) = {} & (\theta(x \oplus_n y) \oplus_n y) * (\theta(y \oplus_n x) \oplus_n x) = \\ & \theta(\theta(x \oplus_n y) \oplus_n y \oplus_n \theta(y \oplus_n x) \oplus_n x) \oplus_n \theta(y \oplus_n x) \oplus_n x = \\ & \theta(y \oplus_n x) \oplus_n \theta(y \oplus_n x) \oplus_n x = x.\end{aligned}$$

Proposition 4.2 The quasigroup $(Q,*)$, constructed by a complete mapping θ of the group $\left(\mathrm{Z}_2^n, \oplus_n\right)$ is anti-commutative quasigroup.

Proof. Let $x, y \in Q$ and $x * y = y * x$. Then $x = (x * y) * (y * x) = (y * x) * (x * y) = y$.

Proposition 4.3 The quasigroup $(Q,*)$, constructed by an affine complete mapping θ of the group $\left(\mathrm{Z}_2^n, \oplus_n\right)$ is a TA-quasigroup.

Proof. Let $\phi = I \oplus_{\mathrm{n}} \theta$ be (is) orthomorphism of θ, so ϕ is affine bijection too.

If $x, y, c \in Q$ and $(c * x) * y = (c * y) * x$, then

$$\theta(\theta(c \oplus_{\mathrm{n}} x) \oplus_{\mathrm{n}} x \oplus_{\mathrm{n}} y) \oplus_{\mathrm{n}} y = \theta(\theta(c \oplus_{\mathrm{n}} y) \oplus_{\mathrm{n}} y \oplus_{\mathrm{n}} x) \oplus_{\mathrm{n}} x \Rightarrow (\theta \text{ is affine})$$

$\theta(\theta(c \oplus_n x)) \oplus_n y = \theta(\theta(c \oplus n\, y)) \oplus n\, x \Rightarrow$

$\theta(\theta(c) \oplus_n \theta(x) \oplus_n \theta(0)) \oplus_n y = \theta(\theta(c) \oplus n\, \theta(y) \oplus_n \theta(0)) \oplus_n x \Rightarrow$

$\theta(\theta(x)) \oplus_n y = \theta(\theta(y)) \oplus_n x \Rightarrow$

$\theta(\theta(x)) \oplus_n \theta(x) \oplus_n \theta(x) \;\oplus_n\; x = \theta(\theta(y)) \oplus_n \theta(y) \oplus_n \theta(y) \oplus_n y \Rightarrow$

$\phi(\theta(x)) \oplus_n \phi(x) \oplus_{\mathrm{n}} \phi(0) = \phi(\theta(y)) \oplus_n \phi(y) \oplus_n \phi(0) \;\Rightarrow (\phi$ is affine)

$\phi(\theta(x) \oplus_n x) = \phi(\theta(y) \oplus_n y) \Rightarrow (\phi$ is bijection)

$\theta(x) \oplus_n x = \theta(y) \oplus_n y \Rightarrow$

$\phi(x) = \phi(y) \Rightarrow (\phi$ is bijection) $x = y$.

Proposition 4.2. implies that Q is TA-quasigroup.

Proposition 4.4 The quasigroup $(Q,*)$, constructed by a complete mapping θ of the group $(Z_2^n, \oplus_n)$ is idempotent quasigroup iff $\theta(0) = 0$.

Proof. If $x \in Q$, then $x * x = x \Leftrightarrow \theta(x \oplus_n x) \oplus_{\mathrm{n}} x = x \Leftrightarrow \theta(0) \oplus_n x = x \Leftrightarrow \theta(0) = 0$.

Proposition 4.5 The quasigroup $(Q,*)$ constructed by a complete mapping θ of the group $(Z_2^n, \oplus_n)$ is without left or right unit.

Proof. Let e be the right unit of $(Q,*)$. Then

$$x * e = x \Rightarrow \theta(x \oplus_n e) \oplus_n e = x \Rightarrow \theta(x \oplus_n e) = x \oplus_n e$$

for all $x \in Q$. This means that $\theta = I$ is the identity mapping. This is contradiction with θ is a complete mapping of a $(Z_2^n, \oplus_n)$ (identity mapping isn't complete mapping of a $(Z_2^n, \oplus_n)$, from Proposition 2.1). So, Q is without right unit.

Let e be the left unit of $(Q,*)$. Then

$$e * x = x \Rightarrow \theta(e \oplus_n x) \oplus_n x = x \Rightarrow \theta(e \oplus_n x) = 0$$

for all $x \in Q$. This means that θ is a zero mapping. This is contradiction with θ is a bijection. So, Q is without left unit.

Proposition 4.6 The quasigroup (Q, *), constructed by a complete mapping θ of the group $\left(Z_2^n, \oplus_n\right)$ is non-associative

Proof. Every associative quasigroup is a group, and every group possesses a unit element, so because of Proposition 4.5, the quasigroup (Q, *) is non-associative.

Some "pairing" properties for quasigroup (Q, *) constructed by affine complete mapping of a group $\left(Z_2^n, \oplus_n\right)$ are defined and proved [12]. First "pairing" property tells us that every row in the multiplication table of (Q, *) is the reversal of another row and every column of (Q, *) is the reversal of another column. This can be defined as follows.

Definition 4.1 Let (Q, *) be a quasigroup and $k, x, y \in Q$. Rows x and y **are paired over *k*** if for any $a, z \in Q$, whenever a appears in row x, column z, a also appears in row y, column $z + k$.

Definition 4.2 Let (Q, *) be a quasigroup and let $k, x, y \in Q$. Columns x and y **are paired over *k*** if for any $a, z \in Q$, if a appears in row z and column x, then a also appears in row $z + k$ and column y.

Proposition 4.7 [12] Let (Q, *) be a quasigroup constructed from the group $\left(Z_2^n, \oplus_n\right)$ by

$$x * y = \theta(x \oplus_n y) \oplus_n y$$

where $\theta : Q \to Q$ is an affine complete mapping and $k, x, y \in Q$. Then rows x and y are paired over k if and only if $x * k = \theta(y)$, i.e., for any $z \in Q$,

$$x * z = y * (z \oplus_n k) \Leftrightarrow x * k = \theta(y).$$

Notice that for any k, $x \in Q$, there exists y, because the quasigroup equations have unique solutions.

Similarly, columns x and y are paired over k if and only if $k * x = \phi(y)$, where ϕ: $Q \to Q$ is the orthomorphism of θ, i.e., for any $z \in Q$,

$$z * x = (z \oplus_n k) * y \Leftrightarrow k * x = \phi(y).$$

Another "pairing" property tells us that every element has its "pair" element that appear next to it in every row and every column in multiplication table of $(Q, *)$.

5. SPECIAL CASE – QUASIGROUPS CONSTRUCTED FROM COMPLETE MAPPINGS OF THE GROUP $\left(Z_2^3, \oplus_3\right)$

There are 384 complete mappings of the group $\left(Z_2^3, \oplus\right)$, given in Appendix A. All these mapping are affine mappings, and 48 of them are linear mappings.

With exhaustive search and examination in software package Matlab and with properties from Section 4, we have found that all 384 constructed quasigroups are non-associative, non-commutative, without left or right unit and without proper subquasigroup. All of them are Shoreder's quasigroups and TA-quasigroups. 48 of them are idempotent quasigroups. Also, all of them have prop ratio table with one element 1 in every column and others elements 0, and correlation matrix with one element 1 or –1 in every row and others elements 0.

From their prop ratio tables and correlation matrices we can conclude that all 384 quasigroups are linear quasigroups [7]. If they are represented as vector valued Boolean functions, then every bit of the output is represented as affine function of input bits. The representation of all 384 quasigroups with ANF is given in Appendix B.

Example 1. Let θ: $Q \to Q$ be a complete mapping given by the table below.

x	0	1	2	3	4	5	6	7
$\theta(x)$	2	5	1	6	4	3	7	0
$\phi(x)$	2	4	3	5	0	6	1	7

The corresponding quasigroup is given by the table

*	0	1	2	3	4	5	6	7
0	2	4	3	5	0	6	1	7
1	5	3	4	2	7	1	6	0
2	1	7	0	6	3	5	2	4
3	6	0	7	1	4	2	5	3
4	4	2	5	3	6	0	7	1
5	3	5	2	4	1	7	0	6
6	7	1	6	0	5	3	4	2
7	0	6	1	7	2	4	3	5

The prop ratio table of this quasigroup is:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1
2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
3	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
4	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0
6	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0
7	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0

	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0
	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0
	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0
	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1

One can see that all difference propagations are with prop ratio 1. For example, the input differences 000010 (= 2), 001001 (= 9), 010100 (= 20), 011111 (= 31), 100011 (= 35), 101000 (= 40), 110101 (= 53), 111110 (= 62), always propagate to output difference 001 (=1). The correlation matrix is:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0
3	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Every nonzero output selection vector is correlated only to one input selection vector with correlation 1 or –1. For example, the output selection vector (001) = 1 is correlated with input selection vector (011010) = 26 with correlation 1, which means that the output bit y_2 is $y_2 = x_1 \oplus x_2 \oplus x_4$. The output selection vector (010) = 2 is correlated with input selection vector (111101) = 61 with correlation –1, which means that the output bit y_1 is $y_1 = 1 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_5$. This means that the every output bit can be represented by an affine function from the input bits. So, the representation of this quasigroup with ANF is

$$h(x_0, x_1, x_2, x_3, x_4, x_5) = (\ x_0 \oplus x_2 \oplus x_5,\ 1 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_5,\ x_1 \oplus x_2 \oplus x_4).$$

6. CONCLUSIONS

The quasigroups constructed from complete mappings of the groups $\left(Z_2^n, \oplus_n\right)$ are examined in this paper. The analyze show that all of them are Shroeder's quasigroups, anti-commutative, non-associative and without left nor right unit. If a complete mapping is affine, the corresponding quasigroup is TA-quasigroup. If $\theta(0) = 0$, the quasigroup is idempotent.

There are 384 complete mappings for group $\left(Z_2^3, \oplus\right)$. Only 48 of constructed quasigroups are idempotent. From their prop ratio tables and correlation matrices we can conclude that all of them are linear quasigroups. If they are represented as vector valued Boolean functions, every bit of the output is represented as affine function of input bits. They can not be used as nonlinear building blocks in cryptography, but they can be used in places where linear building blocks are needed.

REFERENCES

[1] Belousov V. D. (1967), *Osnovi teorii kvazigrup i lup*, “Nauka”, Moskva.

[2] Biham E., Shamir A. (1990), Differential Cryptanalysis of DES-like Cryptosystems, Advances in Cryptology, EUROCRYPT 1990, p. 2–21.

[3] Bruck R. H. (1944), Simple quasigroups, *Bull. Amer. Math. Soc*. **50**, p. 769–781.

[4] Daemen J. (1995), *Cipher and Hash Function Design. Strategies based on Linear and Differential Cryptanalysis*, PhD thesis, Katholieke Universiteit Leuven.

[5] Daemen J., Govaerts R., Vandewalle J. (1995), *Correlation matrices*, Fast Software Encryption 1994, LNCS 1008, Springer-Verlag, p. 275–285.

[6] Damm H. M. (2007), *Totally anti-symmetric quasigroups for all orders n* $\neq 2,6$, Discrete Mathematics 307–6, p. 715–729.

[7] Gligoroski D., Dimitrova V., Markovski S. (2009), *Quasigroups as Boolean functions*, *their equation systems and Groebner bases*, short-note for RISC Book Series, Springer, "Groebner, Coding, and Cryptography", Ed. T. Mora, L. Perret, S. Sakata, M. Sala, and C. Traverso.

[8] Hall M., Paige L. J. (1955), Complete mappings of finite groups, *Pacific Journal of Mathematics* **5**, p. 541–549.

[9] Klimov A., Shamir A. (2002), *A new class of invertible mappings*, Lecture Notes in Computer Science 2523, p. 470–483.

[10] Lindner C. C. (1971), The generalized singular direct product for quasigroups, *Can. Math. Bull.* **14**, p. 61–63.

[11] Matsui M. (1993), *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology, EUROCRYPT 1993, p. 386–397.

[12] Meyer K. A. (2006): *A new message authentication code based on the non-associativity of quasigroups*, Ph.D. dissertation, Iowa State University.

[13] Paige L. J. (1947), A note on finite abelian groups, *Bull. Amer. Math. Soc*. **53**, p. 590–593.

[14] Paige L. J. (1951), Complete mappings of finite groups, *Pacific Journal of Mathematics* **1**, p. 111–116.

[15] Sade A. (1957), Quasigroups automorphes par le groupe cyclique, *Canadian Journal of Mathematics* **9**, p. 321–335.

[16] Sade A. (1960), Produit direct singulier de quasigroups orthogonaux et anti-ab´eliens, *Ann. Soc. Sci. Bruxelles Ser.* I, **74**, p. 91–99.

[17] Wilson R. L. (1975), Quasidirect products of quasigroups, *Commun. Algebra* **3**, p. 835–850.

APPENDIX A

Here is a list of all complete mappings of the group $\left(Z_2^3,\oplus\right)$. 1 0 2 4 6 3 1 7 5 means complete mapping with number 1 that maps 0→0, 1→2, 2→4, 3→6, 4→3, 5→1, 6→7 and 7→5

1 0 2 4 6 3 1 7 5
2 0 2 4 6 5 7 1 3
3 0 2 5 7 1 3 4 6
4 0 2 5 7 6 4 3 1
5 0 2 6 4 1 3 7 5
6 0 2 6 4 5 7 3 1
7 0 2 7 5 3 1 4 6
8 0 2 7 5 6 4 1 3
9 0 3 4 7 1 2 5 6
10 0 3 4 7 5 6 1 2
11 0 3 5 6 2 1 7 4
12 0 3 5 6 7 4 2 1
13 0 3 6 5 1 2 7 4
14 0 3 6 5 7 4 1 2
15 0 3 7 4 2 1 5 6
16 0 3 7 4 5 6 2 1
17 0 4 1 5 3 7 2 6
18 0 4 1 5 6 2 7 3
19 0 4 3 7 2 6 1 5
20 0 4 3 7 6 2 5 1
21 0 4 5 1 2 6 7 3
22 0 4 5 1 7 3 2 6
23 0 4 6 2 3 7 5 1
24 0 4 6 2 7 3 1 5
25 0 5 1 4 2 7 3 6
26 0 5 1 4 6 3 7 2
27 0 5 3 6 2 7 1 4
28 0 5 3 6 7 2 4 1
29 0 5 4 1 3 6 7 2
30 0 5 4 1 7 2 3 6
31 0 5 7 2 3 6 4 1
32 0 5 7 2 6 3 1 4
33 0 6 1 7 2 4 3 5
34 0 6 1 7 5 3 4 2
35 0 6 3 5 1 7 2 4
36 0 6 3 5 7 1 4 2
37 0 6 4 2 1 7 5 3
38 0 6 4 2 7 1 3 5
39 0 6 7 1 2 4 5 3
40 0 6 7 1 5 3 2 4
41 0 7 1 6 3 4 2 5
42 0 7 1 6 5 2 4 3
43 0 7 3 4 1 6 2 5
44 0 7 3 4 6 1 5 2
45 0 7 5 2 1 6 4 3
46 0 7 5 2 6 1 3 4
47 0 7 6 1 3 4 5 2
48 0 7 6 1 5 2 3 4
49 1 2 4 7 3 0 6 5
50 1 2 4 7 6 5 3 0
51 1 2 5 6 0 3 4 7
52 1 2 5 6 4 7 0 3
53 1 2 6 5 3 0 4 7
54 1 2 6 5 4 7 3 0
55 1 2 7 4 0 3 6 5
56 1 2 7 4 6 5 0 3
57 1 3 4 6 0 2 5 7
58 1 3 4 6 7 5 2 0
59 1 3 5 7 2 0 6 4
60 1 3 5 7 4 6 0 2
61 1 3 6 4 2 0 5 7
62 1 3 6 4 7 5 0 2
63 1 3 7 5 0 2 6 4
64 1 3 7 5 4 6 2 0

65 1 4 0 5 3 6 2 7
66 1 4 0 5 7 2 6 3
67 1 4 2 7 3 6 0 5
68 1 4 2 7 6 3 5 0
69 1 4 5 0 2 7 6 3
70 1 4 5 0 6 3 2 7
71 1 4 6 3 2 7 5 0
72 1 4 6 3 7 2 0 5
73 1 5 0 4 2 6 3 7
74 1 5 0 4 7 3 6 2
75 1 5 2 6 3 7 0 4
76 1 5 2 6 7 3 4 0
77 1 5 4 0 3 7 6 2
78 1 5 4 0 6 2 3 7
79 1 5 7 3 2 6 4 0
80 1 5 7 3 6 2 0 4
81 1 6 0 7 2 5 3 4
82 1 6 0 7 4 3 5 2
83 1 6 2 5 0 7 3 4
84 1 6 2 5 7 0 4 3
85 1 6 4 3 0 7 5 2
86 1 6 4 3 7 0 2 5
87 1 6 7 0 2 5 4 3
88 1 6 7 0 4 3 2 5
89 1 7 0 6 3 5 2 4
90 1 7 0 6 4 2 5 3
91 1 7 2 4 0 6 3 5
92 1 7 2 4 6 0 5 3
93 1 7 5 3 0 6 4 2
94 1 7 5 3 6 0 2 4
95 1 7 6 0 3 5 4 2
96 1 7 6 0 4 2 3 5
97 2 0 4 6 3 1 5 7
98 2 0 4 6 7 5 1 3
99 2 0 5 7 1 3 6 4
100 2 0 5 7 4 6 3 1
101 2 0 6 4 1 3 5 7
102 2 0 6 4 7 5 3 1
103 2 0 7 5 3 1 6 4
104 2 0 7 5 4 6 1 3
105 2 1 4 7 3 0 5 6
106 2 1 4 7 5 6 3 0
107 2 1 5 6 0 3 7 4
108 2 1 5 6 7 4 0 3
109 2 1 6 5 3 0 7 4
110 2 1 6 5 7 4 3 0
111 2 1 7 4 0 3 5 6
112 2 1 7 4 5 6 0 3
113 2 4 1 7 3 5 0 6
114 2 4 1 7 5 3 6 0
115 2 4 3 5 0 6 1 7
116 2 4 3 5 7 1 6 0
117 2 4 5 3 0 6 7 1
118 2 4 5 3 7 1 0 6
119 2 4 6 0 3 5 7 1
120 2 4 6 0 5 3 1 7
121 2 5 1 6 3 4 0 7
122 2 5 1 6 4 3 7 0
123 2 5 3 4 1 6 0 7
124 2 5 3 4 7 0 6 1
125 2 5 4 3 1 6 7 0
126 2 5 4 3 7 0 1 6
127 2 5 7 0 3 4 6 1
128 2 5 7 0 4 3 1 6
129 2 6 1 5 0 4 3 7
130 2 6 1 5 4 0 7 3
131 2 6 3 7 1 5 0 4
132 2 6 3 7 4 0 5 1
133 2 6 4 0 1 5 7 3
134 2 6 4 0 5 1 3 7
135 2 6 7 3 0 4 5 1
136 2 6 7 3 5 1 0 4
137 2 7 1 4 0 5 3 6
138 2 7 1 4 5 0 6 3
139 2 7 3 6 0 5 1 4
140 2 7 3 6 4 1 5 0
141 2 7 5 0 1 4 6 3
142 2 7 5 0 4 1 3 6
143 2 7 6 3 1 4 5 0
144 2 7 6 3 5 0 1 4
145 3 0 4 7 1 2 6 5
146 3 0 4 7 6 5 1 2
147 3 0 5 6 2 1 4 7
148 3 0 5 6 4 7 2 1
149 3 0 6 5 1 2 4 7
150 3 0 6 5 4 7 1 2
151 3 0 7 4 2 1 6 5
152 3 0 7 4 6 5 2 1
153 3 1 4 6 0 2 7 5
154 3 1 4 6 5 7 2 0
155 3 1 5 7 2 0 4 6
156 3 1 5 7 6 4 0 2
157 3 1 6 4 2 0 7 5
158 3 1 6 4 5 7 0 2
159 3 1 7 5 0 2 4 6
160 3 1 7 5 6 4 2 0
161 3 4 0 7 2 5 1 6
162 3 4 0 7 5 2 6 1
163 3 4 2 5 0 7 1 6
164 3 4 2 5 6 1 7 0
165 3 4 5 2 0 7 6 1
166 3 4 5 2 6 1 0 7
167 3 4 6 1 2 5 7 0
168 3 4 6 1 5 2 0 7
169 3 5 0 6 2 4 1 7
170 3 5 0 6 4 2 7 1
171 3 5 2 4 1 7 0 6
172 3 5 2 4 6 0 7 1
173 3 5 4 2 1 7 6 0
174 3 5 4 2 6 0 1 7
175 3 5 7 1 2 4 6 0
176 3 5 7 1 4 2 0 6
177 3 6 0 5 1 4 2 7
178 3 6 0 5 4 1 7 2
179 3 6 2 7 1 4 0 5
180 3 6 2 7 5 0 4 1
181 3 6 4 1 0 5 7 2
182 3 6 4 1 5 0 2 7
183 3 6 7 2 0 5 4 1
184 3 6 7 2 4 1 0 5
185 3 7 0 4 1 5 2 6
186 3 7 0 4 5 1 6 2
187 3 7 2 6 0 4 1 5
188 3 7 2 6 5 1 4 0
189 3 7 5 1 0 4 6 2
190 3 7 5 1 4 0 2 6
191 3 7 6 2 1 5 4 0
192 3 7 6 2 4 0 1 5
193 4 0 1 5 3 7 6 2
194 4 0 1 5 6 2 3 7
195 4 0 2 6 3 7 5 1
196 4 0 2 6 7 3 1 5
197 4 0 5 1 2 6 3 7
198 4 0 5 1 7 3 6 2
199 4 0 7 3 2 6 1 5
200 4 0 7 3 6 2 5 1
201 4 1 0 5 3 6 7 2
202 4 1 0 5 7 2 3 6
203 4 1 3 6 2 7 5 0
204 4 1 3 6 7 2 0 5
205 4 1 5 0 2 7 3 6
206 4 1 5 0 6 3 7 2
207 4 1 7 2 3 6 0 5
208 4 1 7 2 6 3 5 0
209 4 2 0 6 3 5 7 1
210 4 2 0 6 5 3 1 7
211 4 2 3 5 1 7 6 0
212 4 2 3 5 6 0 1 7
213 4 2 5 3 1 7 0 6
214 4 2 5 3 6 0 7 1
215 4 2 7 1 3 5 0 6
216 4 2 7 1 5 3 6 0
217 4 3 1 6 2 5 7 0
218 4 3 1 6 5 2 0 7
219 4 3 2 5 1 6 7 0
220 4 3 2 5 7 0 1 6
221 4 3 5 2 1 6 0 7
222 4 3 5 2 7 0 6 1
223 4 3 7 0 2 5 1 6
224 4 3 7 0 5 2 6 1

225 4 6 0 2 1 3 5 7
226 4 6 0 2 7 5 3 1
227 4 6 1 3 2 0 7 5
228 4 6 1 3 5 7 0 2
229 4 6 2 0 1 3 7 5
230 4 6 2 0 5 7 3 1
231 4 6 3 1 2 0 5 7
232 4 6 3 1 7 5 0 2
233 4 7 0 3 1 2 5 6
234 4 7 0 3 5 6 1 2
235 4 7 1 2 3 0 6 5
236 4 7 1 2 6 5 3 0
237 4 7 2 1 3 0 5 6
238 4 7 2 1 5 6 3 0
239 4 7 3 0 1 2 6 5
240 4 7 3 0 6 5 1 2
241 5 0 1 4 2 7 6 3
242 5 0 1 4 6 3 2 7
243 5 0 2 7 3 6 4 1
244 5 0 2 7 6 3 1 4
245 5 0 4 1 3 6 2 7
246 5 0 4 1 7 2 6 3
247 5 0 6 3 2 7 1 4
248 5 0 6 3 7 2 4 1
249 5 1 0 4 2 6 7 3
250 5 1 0 4 7 3 2 6
251 5 1 3 7 2 6 4 0
252 5 1 3 7 6 2 0 4
253 5 1 4 0 3 7 2 6
254 5 1 4 0 6 2 7 3
255 5 1 6 2 3 7 0 4
256 5 1 6 2 7 3 4 0
257 5 2 0 7 3 4 6 1
258 5 2 0 7 4 3 1 6
259 5 2 3 4 0 7 6 1
260 5 2 3 4 6 1 0 7
261 5 2 4 3 0 7 1 6
262 5 2 4 3 6 1 7 0
263 5 2 6 1 3 4 0 7
264 5 2 6 1 4 3 7 0
265 5 3 1 7 2 4 6 0
266 5 3 1 7 4 2 0 6
267 5 3 2 4 0 6 7 1
268 5 3 2 4 7 1 0 6
269 5 3 4 2 0 6 1 7
270 5 3 4 2 7 1 6 0
271 5 3 6 0 2 4 1 7
272 5 3 6 0 4 2 7 1
273 5 6 0 3 2 1 7 4
274 5 6 0 3 7 4 2 1
275 5 6 1 2 0 3 4 7
276 5 6 1 2 4 7 0 3
277 5 6 2 1 0 3 7 4
278 5 6 2 1 7 4 0 3
279 5 6 3 0 2 1 4 7
280 5 6 3 0 4 7 2 1
281 5 7 0 2 3 1 6 4
282 5 7 0 2 4 6 1 3
283 5 7 1 3 0 2 4 6
284 5 7 1 3 6 4 2 0
285 5 7 2 0 3 1 4 6
286 5 7 2 0 6 4 1 3
287 5 7 3 1 0 2 6 4
288 5 7 3 1 4 6 2 0
289 6 0 1 7 3 5 4 2
290 6 0 1 7 4 2 3 5
291 6 0 2 4 1 7 5 3
292 6 0 2 4 7 1 3 5
293 6 0 5 3 1 7 2 4
294 6 0 5 3 7 1 4 2
295 6 0 7 1 3 5 2 4
296 6 0 7 1 4 2 5 3
297 6 1 0 7 3 4 5 2
298 6 1 0 7 5 2 3 4
299 6 1 3 4 0 7 5 2
300 6 1 3 4 7 0 2 5
301 6 1 5 2 0 7 3 4
302 6 1 5 2 7 0 4 3
303 6 1 7 0 3 4 2 5
304 6 1 7 0 5 2 4 3
305 6 2 0 4 1 5 7 3
306 6 2 0 4 5 1 3 7
307 6 2 3 7 1 5 4 0
308 6 2 3 7 4 0 1 5
309 6 2 5 1 0 4 3 7
310 6 2 5 1 4 0 7 3
311 6 2 7 3 0 4 1 5
312 6 2 7 3 5 1 4 0
313 6 3 1 4 0 5 7 2
314 6 3 1 4 5 0 2 7
315 6 3 2 7 1 4 5 0
316 6 3 2 7 5 0 1 4
317 6 3 5 0 1 4 2 7
318 6 3 5 0 4 1 7 2
319 6 3 7 2 0 5 1 4
320 6 3 7 2 4 1 5 0
321 6 4 0 2 3 1 5 7
322 6 4 0 2 7 5 1 3
323 6 4 1 3 0 2 7 5
324 6 4 1 3 5 7 2 0
325 6 4 2 0 3 1 7 5
326 6 4 2 0 5 7 1 3
327 6 4 3 1 0 2 5 7
328 6 4 3 1 7 5 2 0
329 6 5 0 3 1 2 7 4
330 6 5 0 3 7 4 1 2
331 6 5 1 2 3 0 4 7
332 6 5 1 2 4 7 3 0
333 6 5 2 1 3 0 7 4
334 6 5 2 1 7 4 3 0
335 6 5 3 0 1 2 4 7
336 6 5 3 0 4 7 1 2
337 7 0 1 6 2 5 4 3
338 7 0 1 6 4 3 2 5
339 7 0 2 5 1 6 4 3
340 7 0 2 5 6 1 3 4
341 7 0 4 3 1 6 2 5
342 7 0 4 3 6 1 5 2
343 7 0 6 1 2 5 3 4
344 7 0 6 1 4 3 5 2
345 7 1 0 6 2 4 5 3
346 7 1 0 6 5 3 2 4
347 7 1 3 5 0 6 4 2
348 7 1 3 5 6 0 2 4
349 7 1 4 2 0 6 3 5
350 7 1 4 2 6 0 5 3
351 7 1 6 0 2 4 3 5
352 7 1 6 0 5 3 4 2
353 7 2 0 5 1 4 6 3
354 7 2 0 5 4 1 3 6
355 7 2 3 6 0 5 4 1
356 7 2 3 6 4 1 0 5
357 7 2 4 1 0 5 3 6
358 7 2 4 1 5 0 6 3
359 7 2 6 3 1 4 0 5
360 7 2 6 3 5 0 4 1
361 7 3 1 5 0 4 6 2
362 7 3 1 5 4 0 2 6
363 7 3 2 6 0 4 5 1
364 7 3 2 6 5 1 0 4
365 7 3 4 0 1 5 2 6
366 7 3 4 0 5 1 6 2
367 7 3 6 2 1 5 0 4
368 7 3 6 2 4 0 5 1
369 7 4 0 3 2 1 5 6
370 7 4 0 3 5 6 2 1
371 7 4 1 2 0 3 6 5
372 7 4 1 2 6 5 0 3
373 7 4 2 1 0 3 5 6
374 7 4 2 1 5 6 0 3
375 7 4 3 0 2 1 6 5
376 7 4 3 0 6 5 2 1
377 7 5 0 2 1 3 6 4
378 7 5 0 2 4 6 3 1
379 7 5 1 3 2 0 4 6
380 7 5 1 3 6 4 0 2
381 7 5 2 0 1 3 4 6
382 7 5 2 0 6 4 3 1
383 7 5 3 1 2 0 6 4
384 7 5 3 1 4 6 0 2

APPENDIX B

Quasigroups are represented in a form

No. C(100, z_0) z_0 C(010, z_1) z_1 C(001, z_2) z_2

where C(100, z_0) is the correlation coefficient between input selection vector 100 and output selection vector z_0. z_0 is output selection vector in integer representation and it is used for representing output bit y_0 as an affine function of input bits. C(010, z_1) is correlation coefficient between input selection vector 010 and output selection vector z_1. z_1 is output selection vector in integer representation and it is used for representing output bit y_1 as an affine function of input bits. C(001, z_2) is correlation coefficient between input selection vector 001 and output selection vector z_2. z_2 is output selection vector in integer representation and it is used for representing output bit y_2 as an affine function of input bits. If correlation coefficient is 1, the function is linear, and if is –1, the function is affine.

So, 1 1 22 1 47 1 37 means quasigroup constructed from the complete mapping with number 1 (0 2 4 6 3 1 7 5) as $h(x_0, x_1, x_2, x_3, x_4, x_5) = (x_1 \oplus x_3 \oplus x_4,\ x_0 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5,\ x_0 \oplus x_3 \oplus x_5)$ because 22 = 010110, 47 = 101111 and 37 = 100101.

178 1 41 –1 52 –1 62 means quasigroup constructed from the complete mapping with number 178 (3 6 0 5 4 1 7 2) as $h(x_0, x_1, x_2, x_3, x_4, x_5) = (x_0 \oplus x_2 \oplus x_5, 1 \oplus x_0 \oplus x_1 \oplus x_3, 1 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4)$ because 41 = 101001, 52 = 110100 and 62 = 111110.

1	1	22	1	47	1	37
2	1	50	1	11	1	37
3	1	22	1	11	1	55
4	1	50	1	47	1	19
5	1	22	1	25	1	37
6	1	50	1	25	1	37
7	1	22	1	61	1	55
8	1	50	1	61	1	19
9	1	22	1	11	1	44
10	1	50	1	11	1	44
11	1	22	1	47	1	26
12	1	50	1	47	1	62
13	1	22	1	25	1	44
14	1	50	1	61	1	44
15	1	22	1	61	1	26
16	1	50	1	25	1	62
17	1	13	1	38	1	55
18	1	41	1	38	1	19
19	1	13	1	52	1	19
20	1	41	1	52	1	19
21	1	31	1	38	1	19
22	1	59	1	38	1	55
23	1	31	1	52	1	37
24	1	59	1	52	1	37
25	1	13	1	38	1	26
26	1	41	1	38	1	26
27	1	13	1	52	1	26
28	1	41	1	52	1	62
29	1	31	1	38	1	44
30	1	59	1	38	1	44
31	1	31	1	52	1	62
32	1	59	1	52	1	26
33	1	13	1	47	1	19
34	1	41	1	11	1	55
35	1	13	1	25	1	55
36	1	41	1	61	1	55
37	1	31	1	11	1	37
38	1	59	1	47	1	37
39	1	31	1	61	1	19
40	1	59	1	25	1	55

41	1	13	1	47	1	62
42	1	41	1	11	1	62
43	1	13	1	25	1	62
44	1	41	1	61	1	26
45	1	31	1	11	1	62
46	1	59	1	47	1	26
47	1	31	1	61	1	44
48	1	59	1	25	1	44
49	1	22	1	47	-1	26
50	1	50	1	47	-1	62
51	1	22	1	11	-1	44
52	1	50	1	11	-1	44
53	1	22	1	61	-1	26
54	1	50	1	25	-1	62
55	1	22	1	25	-1	44
56	1	50	1	61	-1	44
57	1	22	1	11	-1	55
58	1	50	1	47	-1	19
59	1	22	1	47	-1	37
60	1	50	1	11	-1	37
61	1	22	1	61	-1	55
62	1	50	1	61	-1	19
63	1	22	1	25	-1	37
64	1	50	1	25	-1	37
65	1	13	1	38	-1	26
66	1	41	1	38	-1	26
67	1	13	1	52	-1	26
68	1	41	1	52	-1	62
69	1	31	1	38	-1	44
70	1	59	1	38	-1	44
71	1	31	1	52	-1	62
72	1	59	1	52	-1	26
73	1	13	1	38	-1	55
74	1	41	1	38	-1	19
75	1	13	1	52	-1	19
76	1	41	1	52	-1	19
77	1	31	1	38	-1	19
78	1	59	1	38	-1	55
79	1	31	1	52	-1	37
80	1	59	1	52	-1	37
81	1	13	1	47	-1	62
82	1	41	1	11	-1	62
83	1	13	1	25	-1	62
84	1	41	1	61	-1	26
85	1	31	1	11	-1	62
86	1	59	1	47	-1	26
87	1	31	1	61	-1	44
88	1	59	1	25	-1	44
89	1	13	1	47	-1	19
90	1	41	1	11	-1	55
91	1	13	1	25	-1	55
92	1	41	1	61	-1	55
93	1	31	1	11	-1	37
94	1	59	1	47	-1	37
95	1	31	1	61	-1	19
96	1	59	1	25	-1	55
97	1	22	-1	25	1	37
98	1	50	-1	25	1	37
99	1	22	-1	61	1	55
100	1	50	-1	61	1	19
101	1	22	-1	47	1	37
102	1	50	-1	11	1	37
103	1	22	-1	11	1	55
104	1	50	-1	47	1	19
105	1	22	-1	25	1	44
106	1	50	-1	61	1	44
107	1	22	-1	61	1	26
108	1	50	-1	25	1	62
109	1	22	-1	11	1	44
110	1	50	-1	11	1	44
111	1	22	-1	47	1	26
112	1	50	-1	47	1	62
113	1	13	-1	25	1	55
114	1	41	-1	61	1	55
115	1	13	-1	47	1	19
116	1	41	-1	11	1	55
117	1	31	-1	61	1	19
118	1	59	-1	25	1	55
119	1	31	-1	11	1	37
120	1	59	-1	47	1	37
121	1	13	-1	25	1	62
122	1	41	-1	61	1	26
123	1	13	-1	47	1	62
124	1	41	-1	11	1	62
125	1	31	-1	61	1	44
126	1	59	-1	25	1	44
127	1	31	-1	11	1	62
128	1	59	-1	47	1	26
129	1	13	-1	52	1	19
130	1	41	-1	52	1	19
131	1	13	-1	38	1	55
132	1	41	-1	38	1	19
133	1	31	-1	52	1	37
134	1	59	-1	52	1	37
135	1	31	-1	38	1	19
136	1	59	-1	38	1	55
137	1	13	-1	52	1	26
138	1	41	-1	52	1	62
139	1	13	-1	38	1	26
140	1	41	-1	38	1	26
141	1	31	-1	52	1	62
142	1	59	-1	52	1	26
143	1	31	-1	38	1	44
144	1	59	-1	38	1	44
145	1	22	-1	61	-1	26
146	1	50	-1	25	-1	62
147	1	22	-1	25	-1	44
148	1	50	-1	61	-1	44
149	1	22	-1	47	-1	26
150	1	50	-1	47	-1	62
151	1	22	-1	11	-1	44
152	1	50	-1	11	-1	44
153	1	22	-1	61	-1	55
154	1	50	-1	61	-1	19
155	1	22	-1	25	-1	37
156	1	50	-1	25	-1	37
157	1	22	-1	11	-1	55
158	1	50	-1	47	-1	19
159	1	22	-1	47	-1	37
160	1	50	-1	11	-1	37
161	1	13	-1	25	-1	62
162	1	41	-1	61	-1	26
163	1	13	-1	47	-1	62
164	1	41	-1	11	-1	62
165	1	31	-1	61	-1	44
166	1	59	-1	25	-1	44
167	1	31	-1	11	-1	62
168	1	59	-1	47	-1	26
169	1	13	-1	25	-1	55
170	1	41	-1	61	-1	55
171	1	13	-1	47	-1	19
172	1	41	-1	11	-1	55
173	1	31	-1	61	-1	19
174	1	59	-1	25	-1	55
175	1	31	-1	11	-1	37
176	1	59	-1	47	-1	37
177	1	13	-1	52	-1	26
178	1	41	-1	52	-1	62
179	1	13	-1	38	-1	26
180	1	41	-1	38	-1	26
181	1	31	-1	52	-1	62
182	1	59	-1	52	-1	26
183	1	31	-1	38	-1	44
184	1	59	-1	38	-1	44
185	1	13	-1	52	-1	19
186	1	41	-1	52	-1	19
187	1	13	-1	38	-1	55
188	1	41	-1	38	-1	19
189	1	31	-1	52	-1	37
190	1	59	-1	52	-1	37
191	1	31	-1	38	-1	19
192	1	59	-1	38	-1	55
193	-1	59	1	38	1	55
194	-1	31	1	38	1	19
195	-1	59	1	52	1	37
196	-1	31	1	52	1	37
197	-1	41	1	38	1	19
198	-1	13	1	38	1	55
199	-1	41	1	52	1	19
200	-1	13	1	52	1	19
201	-1	59	1	38	1	44
202	-1	31	1	38	1	44
203	-1	59	1	52	1	26
204	-1	31	1	52	1	62
205	-1	41	1	38	1	26
206	-1	13	1	38	1	26
207	-1	41	1	52	1	62
208	-1	13	1	52	1	26
209	-1	59	1	47	1	37
210	-1	31	1	11	1	37
211	-1	59	1	25	1	55
212	-1	31	1	61	1	19
213	-1	41	1	11	1	55
214	-1	13	1	47	1	19
215	-1	41	1	61	1	55
216	-1	13	1	25	1	55
217	-1	59	1	47	1	26
218	-1	31	1	11	1	62
219	-1	59	1	25	1	44
220	-1	31	1	61	1	44

```
221 -1 41 1 11 1 62
222 -1 13 1 47 1 62
223 -1 41 1 61 1 26
224 -1 13 1 25 1 62
225 -1 50 1 11 1 37
226 -1 22 1 47 1 37
227 -1 50 1 47 1 19
228 -1 22 1 11 1 55
229 -1 50 1 25 1 37
230 -1 22 1 25 1 37
231 -1 50 1 61 1 19
232 -1 22 1 61 1 55
233 -1 50 1 11 1 44
234 -1 22 1 11 1 44
235 -1 50 1 47 1 62
236 -1 22 1 47 1 26
237 -1 50 1 61 1 44
238 -1 22 1 25 1 44
239 -1 50 1 25 1 62
240 -1 22 1 61 1 26
241 -1 59 1 38 -1 44
242 -1 31 1 38 -1 44
243 -1 59 1 52 -1 26
244 -1 31 1 52 -1 62
245 -1 41 1 38 -1 26
246 -1 13 1 38 -1 26
247 -1 41 1 52 -1 62
248 -1 13 1 52 -1 26
249 -1 59 1 38 -1 55
250 -1 31 1 38 -1 19
251 -1 59 1 52 -1 37
252 -1 31 1 52 -1 37
253 -1 41 1 38 -1 19
254 -1 13 1 38 -1 55
255 -1 41 1 52 -1 19
256 -1 13 1 52 -1 19
257 -1 59 1 47 -1 26
258 -1 31 1 11 -1 62
259 -1 59 1 25 -1 44
260 -1 31 1 61 -1 44
261 -1 41 1 11 -1 62
262 -1 13 1 47 -1 62
263 -1 41 1 61 -1 26
264 -1 13 1 25 -1 62
265 -1 59 1 47 -1 37
266 -1 31 1 11 -1 37
267 -1 59 1 25 -1 55
268 -1 31 1 61 -1 19
269 -1 41 1 11 -1 55
270 -1 13 1 47 -1 19
271 -1 41 1 61 -1 55
272 -1 13 1 25 -1 55
273 -1 50 1 47 -1 62
274 -1 22 1 47 -1 26
275 -1 50 1 11 -1 44
276 -1 22 1 11 -1 44
277 -1 50 1 25 -1 62
278 -1 22 1 61 -1 26
279 -1 50 1 61 -1 44
280 -1 22 1 25 -1 44
281 -1 50 1 47 -1 19
282 -1 22 1 11 -1 55
283 -1 50 1 11 -1 37
284 -1 22 1 47 -1 37
285 -1 50 1 61 -1 19
286 -1 22 1 61 -1 55
287 -1 50 1 25 -1 37
288 -1 22 1 25 -1 37
289 -1 59 -1 25 1 55
290 -1 31 -1 61 1 19
291 -1 59 -1 47 1 37
292 -1 31 -1 11 1 37
293 -1 41 -1 61 1 55
294 -1 13 -1 25 1 55
295 -1 41 -1 11 1 55
296 -1 13 -1 47 1 19
297 -1 59 -1 25 1 44
298 -1 31 -1 61 1 44
299 -1 59 -1 47 1 26
300 -1 31 -1 11 1 62
301 -1 41 -1 61 1 26
302 -1 13 -1 25 1 62
303 -1 41 -1 11 1 62
304 -1 13 -1 47 1 62
305 -1 59 -1 52 1 37
306 -1 31 -1 52 1 37
307 -1 59 -1 38 1 55
308 -1 31 -1 38 1 19
309 -1 41 -1 52 1 19
310 -1 13 -1 52 1 19
311 -1 41 -1 38 1 19
312 -1 13 -1 38 1 55
313 -1 59 -1 52 1 26
314 -1 31 -1 52 1 62
315 -1 59 -1 38 1 44
316 -1 31 -1 38 1 44
317 -1 41 -1 52 1 62
318 -1 13 -1 52 1 26
319 -1 41 -1 38 1 26
320 -1 13 -1 38 1 26
321 -1 50 -1 25 1 37
322 -1 22 -1 25 1 37
323 -1 50 -1 61 1 19
324 -1 22 -1 61 1 55
325 -1 50 -1 11 1 37
326 -1 22 -1 47 1 37
327 -1 50 -1 47 1 19
328 -1 22 -1 11 1 55
329 -1 50 -1 61 1 44
330 -1 22 -1 25 1 44
331 -1 50 -1 25 1 62
332 -1 22 -1 61 1 26
333 -1 50 -1 11 1 44
334 -1 22 -1 11 1 44
335 -1 50 -1 47 1 62
336 -1 22 -1 47 1 26
337 -1 59 -1 25 -1 44
338 -1 31 -1 61 -1 44
339 -1 59 -1 47 -1 26
340 -1 31 -1 11 -1 62
341 -1 41 -1 61 -1 26
342 -1 13 -1 25 -1 62
343 -1 41 -1 11 -1 62
344 -1 13 -1 47 -1 62
345 -1 59 -1 25 -1 55
346 -1 31 -1 61 -1 19
347 -1 59 -1 47 -1 37
348 -1 31 -1 11 -1 37
349 -1 41 -1 61 -1 55
350 -1 13 -1 25 -1 55
351 -1 41 -1 11 -1 55
352 -1 13 -1 47 -1 19
353 -1 59 -1 52 -1 26
354 -1 31 -1 52 -1 62
355 -1 59 -1 38 -1 44
356 -1 31 -1 38 -1 44
357 -1 41 -1 52 -1 62
358 -1 13 -1 52 -1 26
359 -1 41 -1 38 -1 26
360 -1 13 -1 38 -1 26
361 -1 59 -1 52 -1 37
362 -1 31 -1 52 -1 37
363 -1 59 -1 38 -1 55
364 -1 31 -1 38 -1 19
365 -1 41 -1 52 -1 19
366 -1 13 -1 52 -1 19
367 -1 41 -1 38 -1 19
368 -1 13 -1 38 -1 55
369 -1 50 -1 25 -1 62
370 -1 22 -1 61 -1 26
371 -1 50 -1 61 -1 44
372 -1 22 -1 25 -1 44
373 -1 50 -1 47 -1 62
374 -1 22 -1 47 -1 26
375 -1 50 -1 11 -1 44
376 -1 22 -1 11 -1 44
377 -1 50 -1 61 -1 19
378 -1 22 -1 61 -1 55
379 -1 50 -1 25 -1 37
380 -1 22 -1 25 -1 37
381 -1 50 -1 47 -1 19
382 -1 22 -1 11 -1 55
383 -1 50 -1 11 -1 37
384 -1 22 -1 47 -1 37
```

Резиме

КВАЗИГРУПИ КОНСТРУИРАНИ ОД КОМПЛЕТНИТЕ ПРЕСЛИКУВАЊА НА ГРУПАТА $\left(Z_2^n,\oplus\right)$

Во овој труд испитувани се квазигрупите конструирани од комплетните пресликувања на групата $\left(Z_{2,}^n\ \oplus\right)$ и нивните својства како: асоцијативен закон, комутативен закон, идемпотентен закон, дали содржат потквазигрупи, дали имаат лева и десна единица, нивно претставување во алгебарска нормална форма, проп ратио табели и корелациони матрици и дали исполнуваат други идентитети. Ова е важно за нивната примена во криптографијата, теоријата на кодирање и други полиња. Како пример, ги даваме квазигрупите конструирани од 384-те комплетни пресликувања на групата $\left(Z_2^3,\oplus\right)$.

Клучни зборови: квазигрупа; комплетно пресликување; ТА-квазигрупа

Address:

Aleksandra Mileva
Faculty of Informatics, *"Goce Delcev" University*,
Štip, *Republic of Macedonia*
e-mail: Aleksandra.mileva@ugd.edu.mk

Vesna Dimitrova
Faculty of Natural Sciences and Mathematics,
"Ss. Cyril and Methodius" University in Skopje,
Republic of Macedonia
e-mail:vesnap@ii.edu.mk

Received: 26. III 2009
Accepted: 1. XII 2009