On Bilinear Quasigroups of Order 2^n

Marija Mihova[1] and Aleksandra Stojanova[2]

[1] Ss. Cyril and Methodius University, Faculty of Computer Science and Engineering, Skopje, Macedonia
marija.mihova@finki.ukim.mk
[2] Goce Delcev University, Faculty of Computer Science, Stip, Macedonia
aleksandra.stojanova@ugd.edu.mk

Abstract. The standard representation of a quasigroup of order m uses m^2 bits. In this paper, it is introduced a new way for representation of a class of quasigroups of order 2^n, that reduces the number of bits required for the representation. The focus is placed on a class of quasigroups that can be represented as a linear combination of the operands, which requires $\ln(m)$ bits for storage a quasigroup of order m. Moreover, some characteristics about the parameters, i.e. matrices, that are used for defining such quasigroups are given. This model for presentation of quasigroups can be easily used for further testing of their coding and cryptographic features.

Keywords: Quasigroups of order 2^n · Boolean matrix · Boolean vectors · Linear combination.

1 Introduction

Like many other mathematical theories, the theory of quasigroups is introduced with no useful purpose and without taking care about its applicability. But, because of the interesting properties of these structures, the theory of quasigroups has been developed into a very respectable branch of mathematics with various applications. Quasigroups, in theory of designs known as Latin squares, found statistical applications as experimental designs. Many row-column designs are constructed by concatenating Latin squares [1]. Nowadays, they have practical applications in cryptology and coding theory. A class of codes, Random codes, based on quasigroups, is proposed in [2] and their properties are analyzed in [3]. There are also many cryptographic algorithms formed based on quasigroups. J. Denes and A. D. Keedwell are the first cryptologists that apply quasigroups [4-6]. Quasigroups with some specific properties are used for construction of block ciphers [7-9] and hash functions [10-12]. Since the quality of a crypto product depends of its resistance on different types of attacks, the differential and statistical crypto analysis are integral part in designing such product [7, 9]. Studying the quasigroup properties, is of crucial importance [10].

The interesting nature, as well as their applicability, contributes researching quasigroups to not lose its popularity. Many researchers are involved in studying some

specific quasigroups like quadratic and rectangular quasigroups, [13, 14], right product quasigroups, [15], inverse quasigroups, [16] and some other. Those researches are mostly concentrating in finding conditions when some properties or identities are satisfied. Other approach is counting the number of Latin squares as well as enumerating them up to isomorphism or equivalences [17-20].
Because the number of bit strings of length n is 2n, quasigroups of order 2n and their parastrophe operations have special importance in coding theory and cryptography [7]. Therefore, our interest here is based on these types of quasigroups. The representation of such quasigroups as vector valued Boolean functions is initially introduced by Gligoroski et al [21, 22], and the benefit of this representation in cryptography and coding theory is given in [7] and [23]. According to the degree of the polynomials in the Boolean presentations, the quasigroups of order 4 are classified as linear, semi-linear and quadratic. Further analyze of this type of representation is done in [24], while in [25] it is shown that all quasigroups of order 4 can be presented using binary matrices of order 2. Using this approach, the quasigroups can be classified depending on the type of matrices that characterizes it. This classification is the same with that given in [22]. Moreover, it can be concluded that greater number of linearly independent vectors that characterizes given quasigroups indicates better cryptographic properties. From the other hand, such matrix representation is very simple and clear, needs fewer bits for presentation than the standard way, and can be easily used for further investigations of its cryptographic and coding properties [24]. All this have contributed to the idea of considering a generalization of matrix presentation of quasigroups of order 2n. Therefore, in this paper is considered a special type of quasigroups having Boolean presentation that can be represented as a sum of linear combinations of the multipliers. The benefit of such quasigroups is in the fact that it is needed small number (O(n2)) of bits for their representation. That makes them usable in applications that requires limited memory. They are defined in the next section, while some properties about the form of matrices that are used for representations are given in the sections 3 and 4.

2 Boolean Bilinear Quasigroups

Definition 1. Given groupoid $(G, *)$ is a quasigroup iff for all $a, b, c \in G$ the following statements holds:
$a * b = a * c \Leftrightarrow b = c$
$b * a = c * a \Leftrightarrow b = c$.

Definition 2. Given a set $G = \{0, 1, \ldots, m-1\}$, the $m \times m$ quadrate structure is called *Latin square* iff all elements in each column and each row are distinct.

Each Latin square defines finite quasigroup on G and vice versa.

Let $G = \{0, 1, 2, ..., m-1\}$. Then, a *normalized*, or reduced, Latin square, is a Latin square with the first row and column given by $\{0, 1, 2, ..., m-1\}$. Similarly, can be defined a normalized quasigroup as a quasigroup that satisfies $a * 0 = 0 * a = a$. The total number of Latin squares $N(m,m)$ of order m, can be computed from the number of normalized Latin squares, $L(m,m)$, using the formula $N(m, m) = m!(m-1)!L(m,m)$. The

exact number of Latin squares is known only for $m \leq 11$, while the asymptotic value of $L(m,m)$ is not known [19].

Our interest is concentrated only on quasigroups with $|G|=2^n$. One can choose a bijection $G \rightarrow \{0,1\}^n$ and represent each element from G as a n-bit sequence. Now, each quasigroup can be considered as a binary function f: $\{0,1\}^n$ x $\{0,1\}^n \rightarrow \{0,1\}^n$. And as it is stated in [7] it can be represented as a vector valued Boolean polynomials.

Lemma 1. For every quasigroup $(\{0,1\}^n, *)$ and for each bijection $\{0,1\}^{2n} \rightarrow \{0,1\}^n$ there are uniquely determined vector valued Boolean functions $f_1, \dots, f_n$ such that, for each $x, y \in \{0,1\}^n$

$\vec{x} * \vec{y} = f(\vec{x}, \vec{y}) = \left(f_1(\vec{x}, \vec{y}), \dots, f_n(\vec{x}, \vec{y})\right)$

Moreover, as it is proven in [22], each quasigroup of order 2^n can be represented as vector value Boolean polynomials (this is not true for different order).

The quasigroups of order 2^n with degrees of the polynomial Boolean functions greater than 2 are not suitable for construction of multivariate quadratic public-key cryptosystem. Those with degree at most two are named in [21] as Multivariate Quadratic Quasigroups (MQQ). Special types of MQQ, having a property that all quadratic terms are of the form $x_i y_j$, are introduced in [23] as bilinear MQQ, and we will refer them here as a Bilinear Quasigroups (BQ). Formally BQs are defined as follows:

Definition 3. The quasigroup $(\{0,1\}^n, *)$ is a *Bilinear Quasigroup* if the quasigroup operation can be represented by a vector valued Boolean function $f(\vec{x}, \vec{y}) = \vec{z} = \vec{x} * \vec{y}$ where for some constants $c_k, a_{ki}, b_{ki} \in \{0,1\}, k, i = \overline{1,n}$

$$z_k = c_k + \sum_{i=1}^{n} a_{ki} x_i + \sum_{i=1}^{n} b_{ki} y_i + \sum_{i,j=1}^{n} d_{kij} x_i y_j, \tag{1}$$

Using following notation: $A = [a_{ki}]$, $B = [b_{ki}]$, $\vec{c} = [c_k]$, $D'_i = \left[d'^{i}_{kj}\right]$, where $d'^{i}_{kj} = d_{kij}$, and $D''_j = \left[d''^{j}_{ki}\right]$ where $d''^{j}_{ki} = d_{ki}$, $\vec{x} * \vec{y}$ can be represented as

$$\vec{x} * \vec{y} = \vec{z} = \vec{c} + A\vec{x} + B\vec{y} + \sum_{i=1}^{n} x_i D'_i \vec{y} = \vec{c} + A\vec{x} + B\vec{y} + \sum_{j=1}^{n} y_j D''_j \vec{x}. \tag{2}$$

Note 1. Note that the j-th column of the matrix D'_i is the same with the i-th column of the matrix D''_j. According to Note 1, for a given matrix D'_i we may construct matrix D''_j and vice versa.

Next Example gives features of matrices A and B.

Example 1 Given quasigroup of order 2^3 defined by

$\vec{x} * \vec{y} = (x_1 + x_3 + y_2 + x_3 y_3, x_2 + y_1 + y_3 + x_3 y_3 + 1, x_3 + y_3 + (x_1 + x_2 + x_3) y_2)$.

we have $\vec{c} = (0,1,0)$, $A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$, $D'_1 = D'_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

and

$D'_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$. Also $D''_1 = \mathbf{0}, D''_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$ and $D''_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$.

3 Normalized Bilinear Quasigroups and Connection between BQ and Normalized BQ

It is easy to check that the matrices *A* and *B* in the Example 1 are nonsingular. Next Theorem proves that this assumption must be always true.

Theorem 1. Let a BQ $(\{0,1\}^n, *)$ is defined by (2). Then the matrices *A* and *B* are nonsingular.

Proof. Clearly for different $\vec{x}$, $\vec{x} * \vec{0} = \vec{c} + A\vec{x}$ are all different. This is possible iff *A* is a nonsingular. The non-singularity of *B* can be shown similarly. □

Theorem 2. Let $(\{0,1\}^n, *)$ be a groupoid where $*$ is defined as $\vec{x} * \vec{y} = \vec{x} + \vec{y} + \sum_{i=1}^{n} x_i D'_i \vec{y}$ and $(\{0,1\}^n, *')$ be a groupoid with *' is defined as $\vec{x} *' \vec{y} = (A\vec{x}) * (B\vec{y}) + \vec{c}$, where *A* and *B* are nonsingular $n \times n$ binary matrices and $\vec{c}$ is a binary *n*-vector. Then, $(\{0,1\}^n, *)$ is a quasigroup iff $(\{0,1\}^n, *')$ is a quasigroup.

Proof. Let assume that $(\{0,1\}^n, *)$ is a quasigroup, and let $\vec{x} *' \vec{y} = \vec{x} *' \vec{z}$, then it is obtained

$\vec{x} *' \vec{y} = \vec{x} *' \vec{z} \Leftrightarrow (A\vec{x}) * (B\vec{y}) + \vec{c} = (A\vec{x}) * (B\vec{z}) + \vec{c} \Leftrightarrow (A\vec{x}) * (B\vec{y}) = (A\vec{x}) * (B\vec{z})$.

Since $*$ is a quasigroup operation

$(A\vec{x}) * (B\vec{y}) = (A\vec{x}) * (B\vec{z}) \Leftrightarrow B\vec{y} = B\vec{z}$, and because *B* is nonsingular we obtain that $\vec{y} = \vec{z}$.

Similarly, it can be proven that $\vec{x} *' \vec{y} = \vec{t} *' \vec{y} \Leftrightarrow \vec{x} = \vec{t}$, which completes the proof that $(\{0,1\}^n, *')$ is a quasigroup.

In opposite, let us assume that $(\{0,1\}^n, *')$ is a quasigroup, and let $\vec{x} * \vec{y} = \vec{x} * \vec{z}$. Because *A* and *B* are nonsingular A^{-1} and B^{-1} exist, therefore, it is obtained:

$\vec{x} * \vec{y} = \vec{x} * \vec{z} \Leftrightarrow A(A^{-1}\vec{x}) * B(B^{-1}\vec{y}) + \vec{c} = A(A^{-1}\vec{x}) * B(B^{-1}\vec{z}) + \vec{c} \Leftrightarrow$

$\Leftrightarrow (A^{-1}\vec{x}) *' (B^{-1}\vec{y}) = (A^{-1}\vec{x}) *' (B^{-1}\vec{z})$

Since $*$ is a quasigroup operation $B^{-1}\vec{y} = B^{-1}\vec{z} \Leftrightarrow \vec{y} = \vec{z}$. The proof that $\vec{x} * \vec{y} = \vec{t} * \vec{y} \Leftrightarrow \vec{x} = \vec{t}$, is similar. This completes the proof that $(\{0,1\}^n, *)$ is a quasigroup.

□

It is easy to check that a BQ is normalized if and only if $A = B = E$ and $c = 0$, so we will refer to them as *normalized BQs*, (NBQ). Note that not all normalized quasigroups are of this form.

Below we will prove that each BQ can be represented using NBQ, two nonsingular $n \times n$ binary matrices and a binary *n*-vector.

Theorem 3. Let a BQ $(\{0,1\}^n, *)$ is defined with (2). Then there is a NBQ $(\{0,1\}^n, *')$ such that

$$\vec{x} *' \vec{y} = (A\vec{x}) * (B\vec{y}) + \vec{c}, \tag{3}$$

where A and B are nonsingular $n \times n$ Boolean matrices and $\vec{c}$ is a Boolean n-vector.

Proof. Since, A and B are nonsingular, A^{-1} and B^{-1} exist and (2) can be represented as

$$\vec{x} * \vec{y} = \vec{c} + A\vec{x} + B\vec{y} + \sum_{i=1}^{n} \vec{e}_i^T \vec{x}(D_i' B^{-1})B\vec{y} = \vec{c} + A\vec{x} + B\vec{y} + \sum_{i=1}^{n} (\vec{e}_i^T A^{-1})\left(A\vec{x}\right)(D_i' B^{-1})B\vec{y}$$

If we denote the m-th coordinate of the vector $\vec{e}_i^{\,T} A^{-1}$ with $\hat{a}_{im}$ and the m-th coordinate of the vector $A\vec{x}$ with $(A\vec{x})_m$, the above equation can be represented as:

$$\vec{x} * \vec{y} = \vec{c} + A\vec{x} + B\vec{y} + \sum_{i=1}^{n} \vec{e}_i^T \vec{x}(D_i' B^{-1})B\vec{y} = \vec{c} + A\vec{x} + B\vec{y} + \sum_{i=1}^{n}\sum_{m=1}^{n} \hat{a}_{im} \left(A\vec{x}\right)_m (D_i' B^{-1})B\vec{y} =$$

$$= \vec{c} + A\vec{x} + B\vec{y} + \left(A\vec{x}\right)_m \sum_{m=1}^{n} \left(\sum_{i=1}^{n} \hat{a}_{im} (D_i' B^{-1}) \right) B\vec{y}$$

Taking $D_m' = \sum_{i=1}^{n} \hat{a}_{im} (D_i' B^{-1})$, the quasigroup operation defined by $\vec{x} *' \vec{y} = \vec{x} + \vec{y} + \sum_{m=1}^{n} x_m \hat{D}'_m \vec{y}$ is a NBQ, for which (3) exists. □

Example 2. The quasigroup of order 2^3 defined in Example 1 can be represented by $(A\vec{x}) * (B\vec{y}) + \vec{c}$, where A, B and $\vec{c}$ are given in Example 1 and its corresponding NBQ $(\{0,1\}^3, *)$ is defined by:

$$(x_1, x_2, x_3) * (y_1, y_2, y_3) = (x_1 + y_1 + x_3 y_1 + x_3 y_2, x_2 + y_2 + x_3 y_1 + x_3 y_2, x_3 + y_3 + x_1 y_1 + x_2 y_1)$$

For this NBQ $D'_1 = D'_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ and $D'_3 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$.

The last Theorem shows that, for a given NBQ operation we may construct others BQ by choosing two $n \times n$ nonsingular binary matrices and one n-binary vector.

This result shows that using this type of representation, BQ can be defined with log complexity, while standard definition has quadratic complexity. In fact, to represent quasigroup (G, *) of order $m=2^n$ in standard way, n bits representation is needed for each element of G and 4^n places for representation of the quasigroup operation. There are total $n4^n = m^2 \log_2 m = \Theta(m^2 \ln m)$ bits. Using the results obtained here, it is shown that each normalized BQ can be represented using n nonsingular binary matrices of order n, which requires n^3 bits. For matrices A and B, $2n^2$ bits are required, while to represent the n-vector $\vec{c}$, n bits are needed. There are total $n^3 + 2n^2 + n = \Theta(\ln m)$ bits, which is significantly better compared to the standard way.

Note that for a given normalized quasigroup of order m, there are $m!(m-1)!$ other quasigroups that are obtained by permutation of column and rows of the corresponding Latin square. And not all of them are obtained on this way. The number of BQ is given by the next Theorem.

Theorem 4. Given NBQ $(\{0,1\}^n, *)$, there are exactly $2^n \prod_{k=0}^{n-1}(2^n - 2^k)^2$ BQ $(\{0,1\}^n, *')$ such that $\vec{x} *' \vec{y} = (A\vec{x}) * (B\vec{y}) + \vec{c}$.

Proof. The number of such BQs of order 2^n depends of the number of choices for A, B and $\vec{c}$, i.e. if N_A, N_B and $N_{\vec{c}}$ are numbers of choices for A, B and $\vec{c}$ respectivly, then the number of BQs $(\{0,1\}^n, *')$ such that $\vec{x} *' \vec{y} = (A\vec{x}) * (B\vec{y}) + \vec{c}$ is equal to $N_A N_B N_{\vec{c}}$. Clearly, $N_{\vec{c}} = 2^n$. Moreover, $N_A = N_B$ is equal to the number of nonsingular binary matrices of order *n*. It can be proven that this number is equal to $\prod_{k=0}^{n-1}(2^n - 2^k)$. Given first *k* row vectors of *A*, there are exactly $2^n - 2^k$ possibilities to choose *k*+1-th row vector. The last statement is true for $k = 1$, since the first-row vector of A can be any other *n*-vector except $\vec{0}$ and that can be chosen in $2^n - 1 = 2^n - 2^0$ different ways. The k + 1-th row vector is independent of the previously chosen k vectors, $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_k$, therefore, it can be represented as $\sum_{i=1}^{k} \alpha_i \vec{a}_i$. Since there are 2^k possibilities for choosing such vector, this one can be chosen in $2^n - 2^k$ ways. Those are the number of $n \times n$ nonsingular binary matrices that are equal to $\prod_{k=0}^{n-1}(2^n - 2^k)$, which completes the proof. □

Directly from the last Theorem we obtain the following:

Corollary 1. The number of BQ$(\{0,1\}^n, *')$ is equal to $2^n \left(\prod_{k=0}^{n-1}(2^n - 2^k)^2 \right) \eta$, where η is the number of NBQ of order 2^n.

4 Properties of NBQs

Since any BQ of order 2^n can be represented trough some NBQ of order 2^n, the problem of constructing some BQ is reduced to a problem of constructing NBQ. But, not all matrices D define quasigroup. Therefore, in this section we make a deeper analysis of the properties of that matrices. That can be helpful for determining and generating a BQ. Let us refer to the form of the NBQ:

$$\vec{x} * \vec{y} = \vec{x} + \vec{y} + \sum_{i=1}^{n} x_i D'_i \vec{y} = \vec{x} + \vec{y} + \sum_{j=1}^{n} y_j D''_j \vec{x} \tag{4}$$

It is clear that, each NBQ is completely defined by one of the vectors of binary $n \times n$ matrices $(D'_1, \ldots, D'_n)$ and $(D''_1, \ldots, D''_n)$. The first vector, $(D'_1, \ldots, D'_n)$, corresponding to the first operand is called *NBQ matrix vector for the first operand* (*NBQV*$_1$), and the second one, the vector $(D''_1, \ldots, D''_n)$ corresponding to the second operand, is called *NBQ matrix vector for the second operand* (*NBQV*$_2$). According to Note 1, the *j*-th column of the matrix D'_i is the same with the *i*-th column of the matrix

D''_j. Thus, if $NBQV_1$ $(D'_1, \dots, D'_n)$ is given, $NBQV_2$ is uniquely determined. Therefore, we will refer *$NBQV_2$ corresponding to $NBQV_1$* $(D'_1, \dots, D'_n)$, to the vector of binary $n \times n$ matrices $(D''_1, \dots, D''_n)$ obtained such that *i*-th column of the matrix $D''j$ is equal to the *j*-th column of the matrix $D'i$. Similarly, for a given $NBQV_2$, $(D''_1, \dots, D''_n)$ the vector of binary $n \times n$ matrices $(D'_1, \dots, D'_n)$ obtained such that *j*-th column of the matrix $D'i$ is equal to the *i*-th column of the matrix $D''j$ will be called *$NBQV_1$ corresponding to $NBQV_2$* $(D''_1, \dots, D''_n)$.

Next, we analyze a property $NBQV_k$, k=1,2, that matrices have.

Theorem 5. A vector of binary $n \times n$ matrices $(\hat{D}_1, \dots, \hat{D}_n)$ is a $NBQV_1$ ($NBQV_2$) for some BQ $(\{0,1\}^n, *)$ if and only if $\forall \alpha_1, \dots, \alpha_n \in \{0,1\}, \left| E + \sum_{i=1}^{n} \alpha_i \hat{D}_i \right| = 1$

Proof. We will give the proof for $NBQV_1$ only, since the proof for $NBQV_2$ is similar. Let $\vec{x} = (\alpha_1, \dots, \alpha_n)$. Since the operation * is quasigroup operation, from (4) follows that $\vec{y}_1 \neq \vec{y}_2$ and implies

$\left(E + \sum_{i=1}^{n} \alpha_i \hat{D}_i \right) \vec{y}_1 \neq \left(E + \sum_{i=1}^{n} \alpha_i \hat{D}_i \right) \vec{y}_2$ so,

$\left| E + \sum_{i=1}^{n} \alpha_i \hat{D}_i \right| = 1$.

On the other hand, let $(\hat{D}_1, \dots, \hat{D}_n)$ $\forall \alpha_1, \dots, \alpha_n \in \{0,1\}$, $\left| E + \sum_{i=1}^{n} \alpha_i \hat{D}_i \right| = 1$ and let $\vec{x}$, $\vec{y}_1$ and $\vec{y}_2$ are vectors such that $\vec{x} * \vec{y}_1 = \vec{x} * \vec{y}_2$. Choosing $\vec{x}$ such that $x_i = \alpha_i$, can be obtained:

$$\vec{y}_1 + \sum_{i=1}^{n} \alpha_i \hat{D}_i \vec{y}_1 = \vec{y}_2 + \sum_{i=1}^{n} \alpha_i \hat{D}_i \vec{y}_2 \Leftrightarrow \left(E + \sum_{i=1}^{n} \alpha_i \hat{D}_i \right) \vec{y}_1 = \left(E + \sum_{i=1}^{n} \alpha_i \hat{D}_i \right) \vec{y}_2.$$

From $\left| E + \sum_{i=1}^{n} \alpha_i \hat{D}_i \right| = 1$ follows that $\left(E + \sum_{i=1}^{n} \alpha_i \hat{D}_i \right)^{-1}$ exists, so $\vec{y}_1 = \vec{y}_2$. □

Example 3. For the normalized BQ given in Example 2 follows:

$$|E + D'_1| = |E + D'_2| = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{vmatrix},$$

$$|E + D'_3| = |E + D'_1 + D'_2 + D'_3| = \begin{vmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{vmatrix},$$

$$|E + D'_1 + D'_2| = |E| \text{ and } |E + D'_1 + D'_3| = |E + D'_2 + D'_3| = \begin{vmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{vmatrix}.$$

All those determinants are equal to 1.

The next Lemma gives characteristic about row and column vectors of the $n \times n$ matrix H which satisfies $H + E = 1$.

Lemma 2. Given $n \times n$ matrix H, we denote i-th row vector by $\vec{h}_i$ and i-th column vector by $\vec{h}'_i$. Then, $|H + E| = 1$ iff $\forall \alpha_1, \ldots, \alpha_n \in \{0,1\}$ such that at least one of them is different than 0, $\sum_{i=1}^{n} \alpha_i \vec{h}_i \neq \sum_{i=1}^{n} \alpha_i \vec{e}_i$ and $\sum_{i=1}^{n} \alpha_i \vec{h}'_i \neq \sum_{i=1}^{n} \alpha_i \vec{e}_i$.

Proof. Assume that $\exists \alpha_1, \ldots, \alpha_n \in \{0,1\}$ such that at least one of them is different than 0 and $\sum_{i=1}^{n} \alpha_i \vec{h}_i \neq \sum_{i=1}^{n} \alpha_i \vec{e}_i$, ($\sum_{i=1}^{n} \alpha_i \vec{h}'_i \neq \sum_{i=1}^{n} \alpha_i \vec{e}_i$). This is equivalent to $\sum_{i=1}^{n} \alpha_i \left(\vec{h}_i + \vec{e}_i \right) = 0$, ($\sum_{i=1}^{n} \alpha_i \left(\vec{h}'_i + \vec{e}_i \right) = 0$). This is true if and only if there is a nontrivial linear combination of the row vectors (column vectors) in $H + E$, equals to 0. That is in contradiction with $|H + E| = 1$. □

Using this Lemma, the following will be proven:

Theorem 6. The vector of binary $n \times n$ matrices $(\hat{D}_1, \ldots, \hat{D}_n)$ is a *NBQV*$_1$ and *NBQV*$_2$ for some quasigroup $(\{0,1\}^n, *)$ if and only if $\forall \alpha_1, \ldots, \alpha_n \in \{0,1\}$ such that $\prod_{k=0}^{n-1} (1 + \alpha_i) \neq 0$, the vector space generated by the column vectors of the matrix $\sum_{i=1}^{n} \alpha_i \hat{D}_i$ is independent of the vector $\sum_{i=1}^{n} \alpha_i \vec{e}_i$. And the vector space generated by the row vectors of the matrix $\sum_{i=1}^{n} \alpha_i \hat{D}_i$ is independent of the vector $\sum_{i=1}^{n} \alpha_i \vec{e}_i$.

Proof. The proof only for *NBQV*$_1$ and the vector space generated by column vectors of the matrix $\sum_{i=1}^{n} \alpha_i \hat{D}_i$ will be given, since the proof for *NBQV*$_2$ and the proof for row vectors are similar. Let $\left(\hat{D}_1, \ldots, \hat{D}_n\right) = (D'_1, \ldots, D'_n)$. In order to prove that the vector space generated by column vectors of the matrix $M = \sum_{i=1}^{n} \alpha_i \hat{D}_i$ is independent of the vector $\sum_{i=1}^{n} \alpha_i \vec{e}_i$, we need to prove that $\forall x_1, \ldots, x_n \in \{0,1\}$, $\sum_{i=1}^{n} \alpha_i \vec{e}_i \neq \sum_{j=1}^{n} x_j \vec{m}_j$. Let $(D''_1, \ldots, D''_n)$ be the *NBQV*$_2$ corresponding to $(D'_1, \ldots, D'_n)$ and set $H = \sum_{j=1}^{n} x_j D''_j$, for arbitrary $x_1, \ldots, x_n \in \{0,1\}$. From Theorem 5 $|H + E| = 1$ and from Lemma 2 this is equivalent to $\sum_{i=1}^{n} \alpha_i \vec{h}_i \neq \sum_{i=1}^{n} \alpha_i \vec{e}_i$. Now,

$$\sum_{i=1}^{n} \alpha_i \vec{e}_i \neq \sum_{i=1}^{n} \alpha_i \vec{h}_i = \sum_{i=1}^{n} \alpha_i \left(\sum_{j=1}^{n} x_j D''_j \right)_i = \sum_{i=1}^{n} \alpha_i \sum_{j=1}^{n} x_j \overrightarrow{\left(D''_j\right)_i},$$

where $\overrightarrow{\left(\sum_{j=1}^{n} x_\iota D''_j\right)_\iota}$ is the i-th column vector of the matrix $\sum_{j=1}^{n} x_i D''_j$, and $\overrightarrow{\left(D''_j\right)_i}$ is the i-th column vector of the matrix D''_j. Since j-th column vector of the matrix D'_i is equal to the i-th column vector of the matrix D'_j , it follows

$$\sum_{i=1}^{n} \alpha_i \vec{e}_i \neq \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i x_j \overrightarrow{\left(D'_i\right)_j} = \sum_{j=1}^{n} x_j \sum_{i=1}^{n} \alpha_i \overrightarrow{\left(\hat{D}_i\right)_j} = \sum_{j=1}^{n} x_j \vec{m}_j . \quad \square$$

Using $NBQV_1$ vector of binary $n \times n$ matrices $(D'_1, \dots, D'_n)$ or $NBQV_2$ vector of binary $n \times n$ matrices $(D''_1, \dots, D''_n)$, we will construct new matrices F_i from the i-th rows of the matrices $D'_j, j = 1, .. n$, accordingly. According to Note 1, the columns of F_i are in fact the i-th rows of the matrices D''_i. More formally, next definition is given.

Definition 5. Given $NBQV_1$, $(D'_1, \dots, D'_n)$ and its corresponding $NBQV_2$ $(D''_1, \dots, D''_n)$, we define vector of matrices $(F_1, \dots, F_n)$, where the j-th row of the matrix F_i is equal to the i-th row of the matrix D'_j and the j-th column of the matrix F_i is equal to the i-th row of the matrix D''_j . This vector will be called *normalized BQ matrix vector* (*NBQMV*).

Note that besides $NBQV_1$, and $NBQV_2$, each NBQ is completely defined by *NBQMV* , too. Moreover, given a *NBQMV* $(F_1, \dots, F_n)$, its corresponding $NBQV_1$, $(D'_1, \dots, D'_n)$ and $NBQV_2$ $(D''_1, \dots, D''_n)$, can be constructed, by setting the i-th row of the matrix $D_{'j}$ to be the j-th row of the matrix F_i, and i-th row of the matrix D''_j to be the j-th column of the matrix F_i .

From the last Theorem and the construction of row vectors of $(F_1, \dots, F_n)$ the following is obtained:

Theorem 7. The vector of binary $n \times n$ matrices $(F_1, \dots, F_n)$ is *NBQMV* if and only if $\forall \alpha_1, \dots, \alpha_n \in \{0,1\}$, the vector $\sum_{i=1}^{n} \alpha_i \vec{e}_i$ is independent of the vector spaces generated by the row-vectors and the column-vectors of the matrix $\sum_{i=1}^{n} \alpha_i F_i$.

Next Theorem gives a form of the matrices $(F_1, \dots, F_n)$.

Theorem 8. If the vector of binary $n \times n$ matrices $(F_1, \dots, F_n)$ is *NBQMV* then the i-th row vector of the matrix F_i is a linear combination of the other row vectors of F_i and the i-th column vector of the matrix F_i is a linear combination of the other column vectors of F_i .

Proof. Assume that $(F_1, \dots, F_n)$ is *NBQMV* and that the i-th column vector of F_i is not a linear combination of the other column vectors of F_i. It can be constructed the $n \times (n-1)$ matrix F'_i by deleting the i-th column of F_i. Clearly, the rang of F'_i, k', is less than the rank of F_i, k, i.e. $k' < k < n$. By row Gauss transformation, F'_i can be transformed in upper triangular matrix $\widehat{F'}_i$, and there is a matrix N such that $NF'_i = \widehat{F'}_i$. By the same transformation on F_i , matrix $NF_i = \hat{F}_i$ can be obtained. And since the rank of $\hat{F}_i$ is lower than the rank of $\widehat{F'}_i$, the k+1-th row vector of that matrix $\hat{F}_i$ must be $\vec{e}_i$. Now, it is obtained that the k + 1-th row vector of the matrix N defines linear transformation of the row vectors of F_i equal to $\vec{e}_i$. That is in contradiction with

Theorem 7, which says that the vector $\vec{e}_i$ is independent to the vector spaces generated by the row vectors of the matrix F_i. Similarly, it can be proven that, when the *i*-th row vector of F_i is not a linear combination of the other row vectors of F_i, then there is a linear combination of the column vectors of F_i equal to $\vec{e}_i$. □

According to the last Theorem, instead with n^2 parameters, each $n \times n$ matrix F_i can be represented by $(n-1)^2 + 2(n-1)$ parameters. $(n-1)^2$ of those parameters are for the coordinates that are not on the *i*-th row and *i*-th column, and the rest $2(n-1)$ parameters define the linear combinations of the the *i*-th row and *i*-th column.

Example 4. Refer to the NBQ from Example 2 where
$F_1 = F_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$ and $F_3 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$.

Because, the first-row vector of F_1, the second-row vector of F_2 and the third row and column vector of F_3 are zero vectors. Therefore, they can be represented as a (trivial) linear combination of other row vectors of appropriate matrices. On the other hand, the column vectors of F_1 and F_2 are (0,0,1), (0,0,1) and (0,0,0). Since (0,0,1) = 1· (0,0,1) +1· (0,0,0), the first column vector of F_1 is a linear combination of the other column vectors of F_1 and the second column vector of F_2 is a linear combination of the other column vectors of F_2.

Let us consider the vector spaces generated by the row vectors of the linear combinations of those matrices. First, the row vectors of F_1 and F_2 generate the vector space: {(0,0,0), (0,1,1)} and it is obvious that (1,0,0) and (0,1,0) are not in that vector space. Also, (0,0,1) and (1,1,1) are not in the vector space generated by the row vectors of $F_3 = F_1 + F_2 + F_3$: {(0,0,0), (1,0,0)}. $F_1 + F_2 = 0$, therfore, this matrix generates the vector spaces {(0,0,0)}. Clearly, (1,1,0) is not in this space. With $F_1 + F_3 = F_2 + F_3 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$ the vector space {(0,0,0), (1,0,0), (0,1,1), (1,1,1)} is generated. The vectors (1,0,1) and (0,1,1) are not in this space.

5 Conclusion and Future Work

Starting from the representation of the quasigroups of order 2^n as a vector valued Boolean polynomials, we consider all quasigroups having a property that by fixing one of the operands, the Boolean function becomes a linear, named BLCO-quasigroups. It is shown that each BQ operation on $\{0,1\}^n$ can be represent as $\vec{x} * \vec{y} = (A\vec{x}) *' (B\vec{y}) + \vec{c}$, where $(\{0,1\}^n, *')$ is a NBQ and *A* and *B* are nonsingular $n \times n$ Boolean matrices. This type of representation allows us to define BQ using $\Theta(n)$ bits, instead $\Theta(2^n)$ bits required for standard definition. This is usable for application where a small memory for memorizing quasigroups is essential. In the rest of the paper, some properties about the matrices that are used for defining a normalized BLCO-quasigroup, are given.

By using the obtained results, future work can be focused on few directions: determining additional regularities of matrices that define BLCO-quasigroups; classification of B and finding formulas that define all normalized quasigroups for small orders, especially for order 2^3 and 2^4; as well as analyzing properties in order to determine whether such quasigroups are suitable to be used in coding theory and cryptography. Initial observations show that these quasigroups do not have good cryptographic properties although there are some attempts to be used in cryptography. But simplicity of these quasigroups can be helpful in designing algorithms for error detection in codding theory.

References

1. Hinkelmann, K., Kempthorne, O.: Design and Analysis of Experiments. I and II (Second ed.). Wiley (2008.)
2. Gligoroski, D., Markovski, S., Kocarev, Lj.: Error-correcting codes based on quasigroups, In: Proc. 16th Intern. Confer. Computer Communications and Networks, 165 – 172, (2007)
3. Popovska-Mitrovikj, A., Bakeva, V., Markovski S.:On random error correcting codes based on quasigroups, In: Quasigroups And Related Systems, vol 19, No.2 pp. 301-316, (2011).
4. Denes, J. and Keedwell, A. D.: Latin Squares and their Applications. Academiai Kiado, Budapest, (1974).
5. Denes, J.: Latin squares and non-binary encoding. In: Proc. conf. information theory, CNRS, pages 215-221, Paris, (1979).
6. Denes, J.: On latin squares and a digital encrypting communication system. In: P.U.M.A., Pure Math. Appl., 11(4):559-563, (2000).
7. Gligoroski, D., Markovski, S., and Knapskog, S. J.: A public key block cipher based on multivariate quadratic quasigroups, (2008).
8. Hassinen, M. and Markovski, S.: Secure SMS messaging using Quasigroup encryption and Java SMS API. In SPLST'03, Kuo-pio, Finland, (2003)
9. Hassinen, M. and Markovski, S.: Differential cryptanalysis of the quasigroup cipher. Definition of the encryption method. In Differential cryptanalysis, Petrozavodsk, (2004).
10. Gligoroski, D., Ødegård, R.S., Mihova, M., Knapskog, S.J., Drapal, A., Klima, V., Amundse, J., El-Hadedy, M., Cryptographic hash function Edon-R, Proceedings on the 1st International Workshop on Security and Communication Networks (IWSCN), 2009, IEEE, (2011)
11. Gligoroski, D., Markovski, S., and Kocarev, L.: Edon-R, An infinite family of cryptographic hash functions (2006).
12. Markovski, S., Mileva, A.: NaSHA - The ECRYPT Hash Function, Submission to NIST, (2008).
13. Dudek, W. A.: Quadratical quasigroups, Quasigroups and Related Systems, 4, 913, (1997).
14. Kinyon, M. K. and Phillips, J. D.: Rectangular quasigroups and loops, Comput. Math. Appl. 49, 1679 – 1685, (2005).
15. Kinyon, M. K., Krape, A. and Phillips, J. D.: Right product quasigroups and loops, Quasigroups and Related Systems 19, 239 – 264, (2011)
16. Keedwell, D. and Shcherbacov, V. A.: Quasigroups with an inverse property and generalized parastrophic identities, Quasigroups and Related Systems 13, 109 – 124 (2005).

17. Hulpke, P., Kaski, P. R. J. OSTERGARD: The Number of Latin Squares of Order 11, Mathematic of Computation, Volume 80, Number 274, Pages 1197–1219 (2011).
18. McKay, B.D., Meynert, A., and Myrvold, W.: Small Latin squares, quasigroups, and loops, J. Combin. Des. 15, 98–119, (2007).
19. McKay, B.D. and Wanless, I.M.: On the number of Latin squares, Ann. Comb. 9 335–344, (2005).
20. Wells, M. B.: The Number of Latin Squares of Order Eight. J. Combin. Th. 3, 98-99, (1967).
21. Gligoroski, D., Dimitrova, V., Markovski, S.: Quasigroups as Boolean Functions, Their Equation Systems and Grobner Bases. In: Sala, M.,Mora, T., Perret, L., Sakata, S., Traverso, C. (eds.), Gr¨ obner Bases, Coding, and Cryptography, pp. 415-420. Springer, Heidelberg (2008).
22. Gligoroski, D. and Dimitrova, V. and Markovski, S.: Classification of Quasigroups as Boolean Functions, their Algebraic Complexity and Application of Gröbner Bases in Solving Systems of Quasigroup Equations, Invited short-note for RISC Book Series, Springer, "Groebner, Coding, and Cryptography", Ed. M. Sala, (2007).
23. Ilievska, N, Gligorovski, D.: Simulation of a quasigroup error-detecting linear code, MIPRO, 436- 441 (2015)
24. Mihova, M., Siljanoska, M., Markovski, S.: Tracing Bit Differences in Strings Transformed by Linear Quasigroups of Order 4. In: Proceedings of the 9th Conference for Informatics and Information Technology (CIIT 2012), Bitola, Macedonia, pp. 229-233 (2012).
25. Siljanoska, M., Mihova, M., Markovski, S.: Matrix Presentation of Quasigroups of Order 4, proceeding of: 10th Conference for Informatics and Information Technologies (CIIT 2013), 192- 196, (2014).