Matrix Presentation of Quasigroups of Order 4

Conference Paper · April 2013

CITATIONS
0

READS
297

3 authors:

Maja Siljanoska
Ss. Cyril and Methodius University in Skopje
7 PUBLICATIONS **6** CITATIONS
SEE PROFILE

Marija Mihova
Ss. Cyril and Methodius University in Skopje
66 PUBLICATIONS **164** CITATIONS
SEE PROFILE

Smile Markovski
Ss. Cyril and Methodius University in Skopje
95 PUBLICATIONS **735** CITATIONS
SEE PROFILE

MATRIX PRESENTATION OF QUASIGROUPS OF ORDER 4

Maja Siljanoska
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University
Skopje, Macedonia

Marija Mihova
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University
Skopje, Macedonia

Smile Markovski
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University
Skopje, Macedonia

ABSTRACT

In this paper we give a matrix presentation of quasigroups of order 4 and their parastrophes. For that purpose we use the presentation of quasigroups as vector valued Boolean functions. According to matrix presentations, the classes of linear, semi-linear and quadratic quasigroups of order 4 are defined. The results obtained will open possibilities for future constructons of new cryptographic primitives.

I. INTRODUCTION

Quasigroups are simple algebraic structures whose properties and especially their large number enable them to be applicable in many areas, including cryptography, coding theory, telecommunications etc. In applications, the quaisgroups of order 2^n and their parastrophe operations are of special interest. The quasigroups of order 2^n can be represented as vector valued Boolean functions $f : \{0,1\}^{2n} \to \{0,1\}^n$ [1]. According to the degree of the polynomials in the Boolean presentations, the quasigroups of order 4 can be classified as linear, semi-linear and quadratic quasigroups. In this paper we use some algebraic properties of matrices and matrix operations to derive and characterize the matrix form of the quasigroups of order 4 and their left parastrophes.

The paper is organized as follows. Section II outlines the notion of Boolean presentation of quasigroups of order 2^n. Then, using this notion, in Section III we introduce a matrix presentation of the classes of linear, semi-linear and quadratic quasigroups of order 4. Thereby, we generalize the matrix presentation of the quasigroups of order 4 and use it to derive a matrix presentation of their left parastrophes. We give some conclusions and directions for future work in Section IV.

II. BOOLEAN PRESENTATION OF QUASIGROUPS

Below we give a brief overview of quasigroups; a more detailed explanation can be found in [3].

A quasigroup $(Q, *)$ is a groupoid satysfying the law

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

i.e., the equations $x * u = v$ and $u * y = v$ have unique solutions x, y for each $u, v \in Q$. If $(Q, *)$ is a quasigroup, then $*$ is called a quasigroup operation.

Given a quasigroup $(Q, *)$, new operations on the set Q, called parastrophes (or conjugate operations), can be adjoint to the quasigroup operation $*$. The parastrophe operation left division $\backslash$ (known as left parastrophe) of a quasigroup $(Q, *)$ is defined by

$$x \setminus z = y \Longleftrightarrow x * y = z\,.$$

Then $(Q, \backslash)$ is a quasigroup too, and the identities

$$x \setminus (x * y) = y, x * (x \setminus z) = z$$

hold true as well. (These identities are used in defining encryption and decryption functions for cryptographic purposes.)

Let $(Q, *)$ be a quasigroup of order 2^n. Then the elements of Q can be represented in a one-to-one way by n-tuples of bits $(x_1, x_2, \ldots, x_n),\ x_i \in \{0,1\}$. If for $\mathbf{a}, \mathbf{b}, \mathbf{c} \in Q$ we have $\mathbf{a} * \mathbf{b} = \mathbf{c}$, then for the corresponding bit representations of $\mathbf{a}, \mathbf{b}, \mathbf{c}$ we have that

$$(a_1, a_2, \ldots, a_n) * (b_1, b_2, \ldots, b_n) = (c_1, c_2, \ldots, c_n),$$

where $c_i = c_i(a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n) : \{0,1\}^{2n} \to \{0,1\}$ are Boolean functions on $2n$ variables. Since the quasigroup operation $*$ is uniquely determined by the Boolean functions c_i, we say that the n-tuple $< c_1, c_2, \ldots, c_n >$ of Boolean functions is a Boolean presentation of the quasigroup $(Q, *)$.

Note that every Boolean function $f(x_1, \ldots, x_k)$ can be uniquely given in its algebraic normal form (ANF), i.e., as a polynomial in the Galois field $GF(2)$ as follows:

$$f(x_1, \ldots, x_k) = \sum_{I \in \{0,1\}^k} \alpha_I x^I,$$

where $\alpha_I \in \{0,1\}$ and $x^I = x_i x_j \ldots x_t$ when $I \in \{0,1\}^k$ has 1 in the positions $i, j, \ldots, t$. A Boolean function is said to be of degree d if its ANF is of degree d.

Given a Boolean presentation $< c_1, c_2, \ldots, c_n >$ of a quasigroup $(Q, *)$, for any fixed bits $\alpha_1, \alpha_2, \ldots, \alpha_n$ we have that $< c_1+\alpha_1, c_2+\alpha_2, \ldots, c_n+\alpha_n >$ is a Boolean presentation of a quasigroup, too. Let $(Q, \widetilde{*})$ denote a quasigroup of order 2^n with Boolean presentation $< c_1, c_2, \ldots, c_n >$ such that the free coefficient of each c_i is equal to 0. Then we say that $(Q, \widetilde{*})$ is in a standard form.

Theorem 1: To each quasigroup $< c_1, c_2, \ldots, c_n >$ of order 2^n in standard form, $2^n - 1$ different quasigroups $< c_1 + \alpha_1, c_2 + \alpha_2, \ldots, c_n + \alpha_n >$ of order 2^n can be associated.

The next Theorem was proven in [2].

Theorem 2: Each quasigroup of order 4 has a Boolean presentation $< f, g >$ with Boolean functions f, g of degree 2:

$$\begin{aligned} f(a,b,c,d) &= \alpha_0 + \alpha_a a + \alpha_b b + \alpha_c c + \alpha_d d \\ &\quad + \alpha_{ac} ac + \alpha_{ad} ad + \alpha_{bc} bc + \alpha_{bd} bd, \\ g(a,b,c,d) &= \beta_0 + \beta_a a + \beta_b b + \beta_c c + \beta_d d \\ &\quad + \beta_{ac} ac + \beta_{ad} ad + \beta_{bc} bc + \beta_{bd} bd \,, \end{aligned} \tag{1}$$

where $\alpha_i, \beta_i \in \{0,1\}$ for each index i.

In what follows we consider only quasigroups of order 4 with Boolean presentations $< f, g >$ and we represent the elements of those quasigroups by pairs (x, y) of bits. According to the degree of the polynomials f, g, the quasigroups of order 4 are divided into three classes as follows:

1) *Linear quasigroups.* Both f and g are linear polynomials.
2) *Semi-linear quasigroups.* One of the functions f or g is linear and the other is quadratic.
3) *Quadratic quasigroups.* Both f and g are quadratic polynomials.

III. Matrix Presentation of the Quasigroups of Order 4

Using the standard form of the Boolean presentation of quasigroups of order 4, given by (1), we derive the matrix form of the different classes of standard quasigroups of order 4. That suffices because, by Theorem 1, 3 other different quasigroups of order 4 can be associated to each standard one, characterizing the full range of quasigroups of order 4.

Theorem 3: Each standard linear quasigroup of order 4 is of the form

$$\begin{aligned} (a,b) \,\widetilde{*}\, (c,d) = (&\alpha_a a + \alpha_b b + \alpha_c c + \alpha_d d, \\ &\beta_a a + \beta_b b + \beta_c c + \beta_d d) \end{aligned} \tag{2}$$

for any $\mathbf{x} = (a,b), \mathbf{y} = (c,d) \in \{0,1\}^2$, and has a matrix presentation

$$\mathbf{x} \,\widetilde{*}\, \mathbf{y} \;\equiv \mathbf{A} \cdot \mathbf{x}^T + \mathbf{B} \cdot \mathbf{y}^T, \tag{3}$$

where $\mathbf{A} = \begin{bmatrix} \alpha_a & \alpha_b \\ \beta_a & \beta_b \end{bmatrix}$ and $\mathbf{B} = \begin{bmatrix} \alpha_c & \alpha_d \\ \beta_c & \beta_d \end{bmatrix}$ are nonsingular 2-dimensional Boolean matrices.

Proof: $\Rightarrow$: Let $(Q, \widetilde{*})$ be a standard linear quasigroup of order 4 whose quasigroup operation $\widetilde{*} : Q^2 \to Q$ is defined by (2) over the elements of $Q = \{0,1\}^2$. Suppose $\mathbf{x} \,\widetilde{*}\, \mathbf{y} = \mathbf{z}$. This can be written in an equivalent matrix form as

$$\mathbf{A}\mathbf{x}^T + \mathbf{B}\mathbf{y}^T = \mathbf{z}^T \,.$$

Given $\mathbf{y}, \mathbf{z} \in Q$, we get

$$\mathbf{A}\mathbf{x}^T = \mathbf{z}^T - \mathbf{B}\mathbf{y}^T \,,$$

which represents the matrix form of a linear system with unknown vector $\mathbf{x}$. This system has a unique solution $\mathbf{x}$, given $\mathbf{y}, \mathbf{z}$, which follows from the unique solution $\mathbf{x}$ of the quasigroup equation $\mathbf{x} \,\widetilde{*}\, \mathbf{y} = \mathbf{z}$. Consequently, the Boolean matrix $\mathbf{A}$ is nonsingular. It can be shown in an analog way that the Bolean matrix $\mathbf{B}$ must be nonsingular as well.

$\Leftarrow$: Conversely, assume that $(Q, \widetilde{*})$ is a groupoid whose operation $\widetilde{*} : Q^2 \to Q$ is defined by (3) where the Boolean matrices $\mathbf{A}$ and $\mathbf{B}$ are nonsingular, and $\mathbf{x}, \mathbf{y} \in Q$. Then, for given arbitrary $\mathbf{x}, \mathbf{z} \in Q$ we have the linear system

$$\mathbf{B}\mathbf{y}^T = \mathbf{z}^T - \mathbf{A}\mathbf{x}^T$$

with unknown vector $\mathbf{y}$. Since $\mathbf{B}$ is nonsingular, the system has a unique solution $\mathbf{y}$. Hence, there is a unique solution $\mathbf{y}$ of the equation $\mathbf{x} \,\widetilde{*}\, \mathbf{y} = \mathbf{z}$, given $\mathbf{x}$ and $\mathbf{z}$. In the same way, given $\mathbf{y}$ and $\mathbf{z}$, the equation $\mathbf{x} \,\widetilde{*}\, \mathbf{y} = \mathbf{z}$ has a unique solution $\mathbf{x}$. So, $\widetilde{*}$ is a quasigroup operation on Q. ■

Corolary 1: The number of all linear quasigroups of order 4 is 144.

Proof: There are 6 nonsingular Boolean 2×2-matrices, hence the matrix presentation (3) yields $6 \cdot 6$ standard linear quasigroups of order 4. By Theorem 1, 3 other linear quasigroups can be associated to each standard one, so the number of all linear quasigroups of order 4 is $6 \cdot 6 \cdot 4 = 144$. ■

The class of semi-linear quasigroups of order 4 has Boolean presentation $< f, g >$, where one of the functions f or g is linear, and the other one is quadratic. It is characterized by the following theorem.

Theorem 4: Assume that f is a quadratic polynomial and g is a linear polynomial. Then each standard semi-linear quasigroup of order 4 with Boolean presentation $< f, g >$ is of the form

$$\begin{aligned} (a,b) \,\widetilde{*}\, (c,d) = (&\alpha_a a + \alpha_b b + \alpha_c c + \alpha_d d \\ &+ (\beta_a a + \beta_b b)(\beta_c c + \beta_d d), \\ &\beta_a a + \beta_b b + \beta_c c + \beta_d d) \end{aligned} \tag{4}$$

for any $\mathbf{x} = (a,b), \mathbf{y} = (c,d) \in \{0,1\}^2$, and has a matrix presentation

$$\mathbf{x} \,\widetilde{*}\, \mathbf{y} \equiv \mathbf{A} \cdot \mathbf{x}^T + \mathbf{B} \cdot \mathbf{y}^T + \left(\mathbf{C}\mathbf{A} \cdot \mathbf{x}^T\right) \circ \left(\mathbf{C}\mathbf{B} \cdot \mathbf{y}^T\right), \tag{5}$$

where $\mathbf{A} = \begin{bmatrix} \alpha_a & \alpha_b \\ \beta_a & \beta_b \end{bmatrix}$ and $\mathbf{B} = \begin{bmatrix} \alpha_c & \alpha_d \\ \beta_c & \beta_d \end{bmatrix}$ are nonsingular 2-dimensional Boolean matrices, $\mathbf{C} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, and $\circ$ denotes the component-wise multiplication of vectors.

For the case when g is a quadratic polynomial and f is a linear polynomial, the choice for the matrix $\mathbf{C}$ is $\mathbf{C} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$.

Proof: $\Rightarrow$: Let $(Q, \widetilde{*})$ be a standard semi-linear quasigroup of order 4 whose quasigroup operation $\widetilde{*}$ is defined by (4) over the elements of $Q = \{0,1\}^2$. Assume $(a,b) \,\widetilde{*}\, (c,d) = (u,v)$. This can be written equivalently as

$$\begin{bmatrix} \alpha_a + (\beta_c c + \beta_d d)\,\beta_a & \alpha_b + (\beta_c c + \beta_d d)\,\beta_b \\ \beta_a & \beta_b \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} + \begin{bmatrix} \alpha_c & \alpha_d \\ \beta_c & \beta_d \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix}.$$

Given $(c,d),(u,v) \in Q$, we get the following system

$$\begin{bmatrix} \alpha_a + (\beta_c c + \beta_d d)\beta_a & \alpha_b + (\beta_c c + \beta_d d)\beta_b \\ \beta_a & \beta_b \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} u - \alpha_c c - \alpha_d d \\ v - \beta_c c - \beta_d d \end{bmatrix}.$$

This system has a unique solution (a,b) for any c,d,u,v, which follows from the unique solution (a,b) of the quasigroup equation $(a,b) \widetilde{*} (c,d) = (u,v)$, given $(c,d),(u,v)$. Hence, $\mathbf{A}' = \begin{bmatrix} \alpha_a + (\beta_c c + \beta_d d)\beta_a & \alpha_b + (\beta_c c + \beta_d d)\beta_b \\ \beta_a & \beta_b \end{bmatrix}$ is nonsingular, i.e. $\det(\mathbf{A}') = 1$. Since

$$\begin{aligned} \det(\mathbf{A}') &= \begin{vmatrix} \alpha_a + (\beta_c c + \beta_d d)\beta_a & \alpha_b + (\beta_c c + \beta_d d)\beta_b \\ \beta_a & \beta_b \end{vmatrix} \\ &= \begin{vmatrix} \alpha_a & \alpha_b \\ \beta_a & \beta_b \end{vmatrix} + \begin{vmatrix} (\beta_c c + \beta_d d)\beta_a & (\beta_c c + \beta_d d)\beta_b \\ \beta_a & \beta_b \end{vmatrix} \\ &= \det(\mathbf{A}) + 0 = \det(\mathbf{A}), \end{aligned}$$

it follows that $\det(\mathbf{A}) = 1$. Therefore, the Boolean matrix $\mathbf{A}$ is nonsingular. Analogly, $\mathbf{B}$ must be nonsingular as well.

$\Leftarrow$: Conversely, assume that $(Q, \widetilde{*})$ is a groupoid whose function $\widetilde{*} : Q^2 \to Q$ is defined by (4), and the Boolean matrices $\mathbf{A} = \begin{bmatrix} \alpha_a & \alpha_b \\ \beta_a & \beta_b \end{bmatrix}$ and $\mathbf{B} = \begin{bmatrix} \alpha_c & \alpha_d \\ \beta_c & \beta_d \end{bmatrix}$ are nonsingular. The nonsingularity of the Boolean matrix $\mathbf{B}$ implies that $\mathbf{B}$ cannot have a zero row, that is, $(\beta_c, \beta_d) \neq (0,0)$. This means that $\beta_c c + \beta_d d$ cannot be always 0. Hence, there are 2 possible cases to consider regarding the value of $\beta_c c + \beta_d d$:

Case 1. $\beta_c c + \beta_d d = 1$ for some $(c,d) \in Q$. This yields

$$\begin{aligned} &(\alpha_a a + \alpha_b b + \alpha_c c + \alpha_d d + \beta_a a + \beta_b b, \\ &\beta_a a + \beta_b b + \beta_c c + \beta_d d) = (u,v) \ , \end{aligned}$$

or, in matrix form

$$\begin{bmatrix} \alpha_a + \beta_a & \alpha_b + \beta_b \\ \beta_a & \beta_b \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} + \begin{bmatrix} \alpha_c & \alpha_d \\ \beta_c & \beta_c \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix}.$$

Then for a given $(u,v) \in Q$,

$$\begin{bmatrix} \alpha_a + \beta_a & \alpha_b + \beta_b \\ \beta_a & \beta_b \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} u - \alpha_c c - \alpha_d d \\ v - \beta_c c - \beta_d d \end{bmatrix} \qquad (6)$$

represents the matrix form of a system of 2 linear equations with 2 variables a,b and parameters c,d,u,v. Its coefficient matrix $\mathbf{A}' = \begin{bmatrix} \alpha_a + \beta_a & \alpha_b + \beta_b \\ \beta_a & \beta_b \end{bmatrix}$ has a determinant

$$\begin{aligned} \det(\mathbf{A}') &= \begin{vmatrix} \alpha_a + \beta_a & \alpha_b + \beta_b \\ \beta_a & \beta_b \end{vmatrix} = \begin{vmatrix} \alpha_a & \alpha_b \\ \beta_a & \beta_b \end{vmatrix} + \begin{vmatrix} \beta_a & \beta_b \\ \beta_a & \beta_b \end{vmatrix} \\ &= \det(\mathbf{A}) + 0 = \det(\mathbf{A}). \end{aligned}$$

Since $\mathbf{A}'$ is nonsingular, $\det(\mathbf{A}) = 1$, and therefore $\det(\mathbf{A}') = 1$, i.e. $\mathbf{A}'$ is nonsingular as well. This means that the system (6) has a unique solution (a,b) for any given c,d,u,v. Hence, there is a unique solution (a,b) of the equation $(a,b) \widetilde{*} (c,d) = (u,v)$, given $(c,d),(u,v)$. Similarly, given $(a,b),(u,v)$, there is a unique solution (c,d) of the equation $(a,b) \widetilde{*} (c,d) = (u,v)$. So, $\widetilde{*}$ is a quasigroup operation on Q.

Case 2. $\beta_c c + \beta_d d = 0$ for some $(c,d) \in Q$. Then we have

$$(\alpha_a a + \alpha_b b + \alpha_c c + \alpha_d d, \beta_a a + \beta_b b + \beta_c c + \beta_d d) = (u,v).$$

Given $(u,v) \in Q$, we get the following system

$$\begin{bmatrix} \alpha_a & \alpha_b \\ \beta_a & \beta_b \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} u - \alpha_c c - \alpha_d d \\ v - \beta_c c - \beta_d d \end{bmatrix},$$

whose coefficient matrix $\mathbf{A} = \begin{bmatrix} \alpha_a & \alpha_b \\ \beta_a & \beta_b \end{bmatrix}$ is nonsingular. Therefore, the system has a unique solution (a,b), given c,d,u,v. This means that, for given $(c,d),(u,v)$, the equation $(a,b) \widetilde{*} (c,d) = (u,v)$ has a unique solution (a,b). In the same way, $(a,b) \widetilde{*} (c,d) = (u,v)$ has a unique solution (c,d), given $(a,b),(u,v)$. Hence, $(Q, \widetilde{*})$ represents a quasigroup. ■

Corolary 2: The number of all semi-linear quasigroups of order 4 is 288.

Proof: Using the matrix presentation (5), there are 6 nonsingular Boolean 2×2-matrices and two choices for the matrix $\mathbf{C}$ depending on which of the Boolean functions f,g is a quadratic and which one is a linear polynomial, yielding $6 \cdot 6 \cdot 2$ standard semi-linear quasigroups of order 4. By Theorem 1, 3 other semi-linear quasigroups of order 4 can be associated to each standard one, leading to $6 \cdot 6 \cdot 2 \cdot 4 = 288$ as the number of all semi-linear quasigroups of order 4. ■

The class of quadratic quasigroups of order 4 is characterized by the following theorem.

Theorem 5: Each standard quadratic quasigroup of order 4 given by its Boolean presentation $< f,g >$ is of the form

$$\begin{aligned} &(a,b) \widetilde{*} (c,d) = \\ &\quad (\alpha_a a + \alpha_b b + \alpha_c c + \alpha_d d + ((\alpha_a + \beta_a)a \\ &\quad + (\alpha_b + \beta_b)b)((\alpha_c + \beta_c)c + (\alpha_d + \beta_d)d), \\ &\quad \beta_a a + \beta_b b + \beta_c c + \beta_d d + ((\alpha_a + \beta_a)a \\ &\quad + (\alpha_b + \beta_b)b)((\alpha_c + \beta_c)c + (\alpha_d + \beta_d)d)) \end{aligned} \qquad (7)$$

for any $\mathbf{x} = (a,b), \mathbf{y} = (c,d) \in \{0,1\}^2$, and has a matrix presentation

$$\mathbf{x} \widetilde{*} \mathbf{y} \equiv \mathbf{A} \cdot \mathbf{x}^T + \mathbf{B} \cdot \mathbf{y}^T + \left(\mathbf{C}\mathbf{A} \cdot \mathbf{x}^T\right) \circ \left(\mathbf{C}\mathbf{B} \cdot \mathbf{y}^T\right), \quad (8)$$

where $\mathbf{A} = \begin{bmatrix} \alpha_a & \alpha_b \\ \beta_a & \beta_b \end{bmatrix}$ and $\mathbf{B} = \begin{bmatrix} \alpha_c & \alpha_d \\ \beta_c & \beta_d \end{bmatrix}$ are nonsingular 2-dimensional Boolean matrices, $\mathbf{C} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, and $\circ$ denotes the component-wise multiplication of vectors.

Proof: $\Rightarrow$: Let $(Q, \widetilde{*})$ be a standard quadratic quasigroup of order 4 and its quasigroup operation $\widetilde{*}$ is defined by (7). Assume $(a,b) \widetilde{*} (c,d) = (u,v)$. Then, both polynomials f and g in its Boolean presentation must be quadratic. This implies that $\alpha_c \neq \beta_c$ and $\alpha_d \neq \beta_d$, because otherwise $(\alpha_c + \beta_c)c + (\alpha_d + \beta_d)d$ would be always 0 and f and g would be linear polynomials, yielding a contradiction. Hence, there are 2 possible cases to consider:

Case 1. $(\alpha_c+\beta_c)\,c+(\alpha_d+\beta_d)\,d=1$ for some $(c,d)\in Q$. This yields

$$(\alpha_a a+\alpha_b b+\alpha_c c+\alpha_d d+(\alpha_a+\beta_a)\,a+(\alpha_b+\beta_b)\,b,$$
$$\beta_a a+\beta_b b+\beta_c c+\beta_d d+(\alpha_a+\beta_a)\,a+(\alpha_b+\beta_b)\,b)$$
$$=(u,v)\,,$$

or, in a matrix form,

$$\begin{bmatrix}\alpha_a+(\alpha_a+\beta_a) & \alpha_b+(\alpha_b+\beta_b)\\ \beta_a+(\alpha_a+\beta_a) & \beta_b+(\alpha_b+\beta_b)\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix}$$
$$+\begin{bmatrix}\alpha_c & \alpha_d\\ \beta_c & \beta_d\end{bmatrix}\begin{bmatrix}c\\d\end{bmatrix}=\begin{bmatrix}u\\v\end{bmatrix},$$

which is equivalent to

$$\begin{bmatrix}\beta_a & \beta_b\\ \alpha_a & \alpha_b\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix}+\begin{bmatrix}\alpha_c & \alpha_d\\ \beta_c & \beta_d\end{bmatrix}\begin{bmatrix}c\\d\end{bmatrix}=\begin{bmatrix}u\\v\end{bmatrix}.$$

Given $(u,v)\in Q$ we get the following system

$$\begin{bmatrix}\beta_a & \beta_b\\ \alpha_a & \alpha_b\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix}=\begin{bmatrix}u-\alpha_c c-\alpha_d d\\ v-\beta_c c-\beta_d d\end{bmatrix}. \tag{9}$$

This system has a unique solution (a,b) for any given c,d,u,v, which follows from the uniqueness of the solution (a,b) of the quasigroup equation $(a,b)\,\widetilde{*}\,(c,d)=(u,v)$, for given $(c,d)\,,(u,v)$. So, the cooeficient matrix $\mathbf{A}'=\begin{bmatrix}\beta_a & \beta_b\\ \alpha_a & \alpha_b\end{bmatrix}$ of the system (9) is nonsingular and $\det(\mathbf{A}')=1$. Since

$$\det(\mathbf{A}')=\begin{vmatrix}\beta_a & \beta_b\\ \alpha_a & \alpha_b\end{vmatrix}=-\begin{vmatrix}\alpha_a & \alpha_b\\ \beta_a & \beta_b\end{vmatrix}=-\det(\mathbf{A})\,,$$

it follows that $\det(\mathbf{A})=1$, i.e. the Boolean matrix $\mathbf{A}$ is nonsingular. Similarly, $\mathbf{B}$ must be nonsingular as well.

Case 2. $(\alpha_c+\beta_c)\,c+(\alpha_d+\beta_d)\,d=0$ for some $(c,d)\in Q$. Then, for a given $(u,v)\in Q$, we get the following system

$$\begin{bmatrix}\alpha_a & \alpha_b\\ \beta_a & \beta_b\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix}=\begin{bmatrix}u-\alpha_c c-\alpha_d d\\ v-\beta_d d-\beta_d d\end{bmatrix},$$

which has a unique solution (a,b) implied by the unique solution (a,b) of the quasigroup equation $(a,b)\,\widetilde{*}\,(c,d)=(u,v)$ for given $(c,d),(u,v)$. Consequently, the Boolean matrix $\mathbf{A}=\begin{bmatrix}\alpha_a & \alpha_b\\ \beta_a & \beta_b\end{bmatrix}$ is nonsingular. The nonsingularity of the matrix $\mathbf{B}$ can be shown in an analog way.

$\Leftarrow$: Conversely, let $(Q,\widetilde{*})$ be a groupoid whose function $\widetilde{*}:Q^2\to Q$ is defined over the elements of $Q=\{0,1\}^2$ by (7) and the Boolean matrices $\mathbf{A}=\begin{bmatrix}\alpha_a & \alpha_b\\ \beta_a & \beta_b\end{bmatrix}$ and $\mathbf{B}=\begin{bmatrix}\alpha_c & \alpha_d\\ \beta_c & \beta_d\end{bmatrix}$ are nonsingular. The nonsingularity of $\mathbf{B}$ implies $\alpha_c\neq\beta_c$ or $\beta_c\neq\beta_d$. Otherwise, if $\alpha_c=\beta_c$ and $\alpha_d=\beta_d$, then $\det(\mathbf{B})$ would be 0, leading to a contradiction. This means that $\alpha_c+\beta_c$ and $\alpha_d+\beta_d$ cannot both equal 0, so $(\alpha_c+\beta_c)\,c+(\alpha_d+\beta_d)\,d$ cannot be always 0. Hence, we can again consider 2 cases:

Case 1. $(\alpha_c+\beta_c)\,c+(\alpha_d+\beta_d)\,d=1$ for some $(c,d)\in Q$. Similarly as before, for a given $(u,v)\in Q$, this is equivalent to the following system with unknown vector (a,b):

$$\begin{bmatrix}\beta_a & \beta_b\\ \alpha_a & \alpha_b\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix}=\begin{bmatrix}u-\alpha_c c-\alpha_d d\\ v-\beta_c c-\beta_d d\end{bmatrix}.$$

Its coefficient matrix $\mathbf{A}'=\begin{bmatrix}\beta_a & \beta_b\\ \alpha_a & \alpha_b\end{bmatrix}$ has a determinant $\det(\mathbf{A}')=-\det(\mathbf{A})$. Hence, since $\mathbf{A}$ is a nonsingular Boolean matrix and $\det(\mathbf{A})=1$, it follows that $\det(\mathbf{A}')=1$ and $\mathbf{A}'$ is nonsingular, too. This means that the above system has a unique solution a,b for given c,d,u,v. Then, the quasigroup equation $(a,b)\,\widetilde{*}\,(c,d)=(u,v)$ has a unique solution (a,b) for given $(c,d)\,,(u,v)$. In the same way, $(a,b)\,\widetilde{*}\,(c,d)=(u,v)$ has a unique solution (c,d) for given $(a,b)\,,(u,v)$. So, $\widetilde{*}$ defines a quasigroup operation on Q.

Case 2. $(\alpha_c+\beta_c)\,c+(\alpha_d+\beta_d)\,d=0$ for some $(c,d)\in Q$. Then, for a given $(u,v)\in Q$, we get the system

$$\begin{bmatrix}\alpha_a & \alpha_b\\ \beta_a & \beta_b\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix}=\begin{bmatrix}u-\alpha_c c-\alpha_d d\\ v-\beta_c c-\beta_d d\end{bmatrix}$$

whose coefficient matrix $\mathbf{A}=\begin{bmatrix}\alpha_a & \alpha_b\\ \beta_a & \beta_b\end{bmatrix}$ is nonsingular. Hence, this system has a unique solution (a,b), given c,d,u,v. Consequently, the quasigroup equation $(a,b)\,\widetilde{*}\,(c,d)=(u,v)$ has a unique solution (a,b) for given $(c,d)\,,(u,v)\in Q$, and similarly, a unique solution (c,d) for given $(a,b)\,,(u,v)\in Q$. Therefore, $\widetilde{*}$ defines a quasigroup operation on Q. ■

Corolary 3: The number of all quadratic quasigroups of order 4 is 144.

Proof: There are 6 nonsingular Boolean 2×2-matrices, and therefore, using the matrix presentation (8), the number of standard quadratic quasigroups of order 4 is $6\cdot 6$. By Theorem 1, 3 other different quadratic quasigroups of order 4 can be associated to each standard one, yielding in total $6\cdot 6\cdot 4=144$ quadratic quasigroups of order 4. ■

Theorems 3-5 characterize the matrix form of the classes of linear, semi-linear and quadratic quasigroups of order 4. These characterizations can be embedded together into the following theorem which represents a generalization of the matrix presentation of quasigroups of order 4.

Theorem 6: Each quasigroup $(Q,*)$ of order 4 has a matrix presentation of form

$$\mathbf{x}*\mathbf{y}\equiv\mathbf{m}^T+\mathbf{A}\cdot\mathbf{x}^T+\mathbf{B}\cdot\mathbf{y}^T+(\mathbf{C}\mathbf{A}\cdot\mathbf{x}^T)\circ(\mathbf{C}\mathbf{B}\cdot\mathbf{y}^T), \tag{10}$$

where $\mathbf{x},\mathbf{y}\in Q$, $\mathbf{m}$ is some constant from Q, $\mathbf{A}$ and $\mathbf{B}$ are nonsingular 2-dimensional matrices of bits, $\mathbf{C}$ is one of the matrices $\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&0\end{bmatrix},\begin{bmatrix}0&0\\1&0\end{bmatrix},\begin{bmatrix}1&1\\1&1\end{bmatrix}$, and $\circ$ denotes the component-wise multiplication of vectors.

Theorem 6 implies that by taking 2 arbitrary nonsingular 2-dimensional Boolean matrices $\mathbf{A},\mathbf{B}$ and an appropriate choice for the matrix $\mathbf{C}$, an appropriate quasigroup of order 4 can be generated. Hereby, if $\mathbf{C}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$, then a linear quasigroup of order 4 is obtained. Whereas, if the choice for the matrix $\mathbf{C}$ is $\mathbf{C}=\begin{bmatrix}0&1\\0&0\end{bmatrix}$ or $\mathbf{C}=\begin{bmatrix}0&0\\1&0\end{bmatrix}$, the obtained quasigroup of order 4 is semi-linear. Finally, if $\mathbf{C}=\begin{bmatrix}1&1\\1&1\end{bmatrix}$, then a quadratic quasigroup of order 4 is obtained.

Using the matrix presentation (10) of a quasigroup $(Q, *)$ of order 4, we can derive the matrix form of the left parastrophe $\backslash$ of the quasigroup $(Q, *)$. For that purpose, we will first show the following lemma.

Lemma 1: Let $(Q, *)$ be a standard quasigroup of order 4, given by its matrix presentation (10). If $\mathbf{A} = \mathbf{B} = \mathbf{I}$, then the parastrophe $\backslash_*$ of $*$ is defined by

$$\mathbf{x} \backslash_* \mathbf{z} \equiv (\mathbf{I} + \mathbf{C})\mathbf{x}^T + \mathbf{z}^T + \mathbf{C}\mathbf{x}^T \circ \mathbf{C}\mathbf{z}^T, \qquad (11)$$

where $\mathbf{I}$ denotes the identity matrix.

Proof: Since $(Q, *)$ is a standard quasigroup, $\mathbf{m} = \mathbf{0}$. Furthermore, $\mathbf{A} = \mathbf{B} = \mathbf{I}$, so the quasigroup operation $*$ is given by the matrix presentation

$$\mathbf{x} * \mathbf{y} \equiv \mathbf{x}^T + \mathbf{y}^T + \mathbf{C}\mathbf{x}^T \circ \mathbf{C}\mathbf{y}^T.$$

Note that for any $\mathbf{x} \in Q$, $\mathbf{x} + \mathbf{x} = \mathbf{0}$, $\mathbf{C}\mathbf{C} = \mathbf{O}$, and $\mathbf{C}\mathbf{x}^T \circ C\mathbf{x}^T = \mathbf{C}\mathbf{x}^T$, where $\mathbf{O}$ is the zero matrix. Also, for any $\mathbf{x}, \mathbf{y} \in Q$ there is an $\mathbf{a}$ such that $\mathbf{C}\mathbf{x}^T \circ C\mathbf{y}^T = C\mathbf{a}^T$.

Now, let $\mathbf{x} * \mathbf{y} = \mathbf{z}$. Then we have

$$\begin{aligned}
\mathbf{x} \backslash_* \mathbf{z} &\equiv (\mathbf{I} + \mathbf{C})\mathbf{x}^T + \mathbf{z}^T + \mathbf{C}\mathbf{x}^T \circ C\mathbf{z}^T \\
&= (\mathbf{I} + \mathbf{C})\mathbf{x}^T + (\mathbf{x}^T + \mathbf{y}^T + \mathbf{C}\mathbf{x}^T \circ \mathbf{C}\mathbf{y}^T) \\
&\quad + \mathbf{C}\mathbf{x}^T \circ \mathbf{C}(\mathbf{x}^T + \mathbf{y}^T + \mathbf{C}\mathbf{x}^T \circ \mathbf{C}\mathbf{y}^T) \\
&= \mathbf{I}\mathbf{x}^T + \mathbf{C}\mathbf{x}^T + \mathbf{x}^T + \mathbf{y}^T + \mathbf{C}\mathbf{x}^T \circ \mathbf{C}\mathbf{y}^T \\
&\quad + \mathbf{C}\mathbf{x}^T \circ \mathbf{C}\mathbf{x}^T + \mathbf{C}\mathbf{x}^T \circ \mathbf{C}\mathbf{y}^T + \mathbf{C}\mathbf{x}^T \circ \mathbf{C}(\mathbf{C}\mathbf{a}^T) \\
&= (\mathbf{x}^T + \mathbf{x}^T) + (\mathbf{C}\mathbf{x}^T \circ \mathbf{C}\mathbf{x}^T) + \mathbf{y}^T \\
&\quad + (\mathbf{C}\mathbf{x}^T \circ \mathbf{C}\mathbf{y}^T) + \mathbf{C}\mathbf{x}^T \circ \mathbf{0} \\
&= \mathbf{y}^T,
\end{aligned}$$

i.e. $\mathbf{x} \backslash_* \mathbf{z} = \mathbf{y}$. ■

The following theorem gives the matrix presentation of the left parastrophes of quasigroups of order 4.

Theorem 7: The parastrophe operation $\backslash$ of the quasigroup operation $*$ given by (10) has a matrix presentation of form

$$\begin{aligned}
\mathbf{x} \backslash \mathbf{z} = \mathbf{B}^{-1}\mathbf{m}^T &+ \mathbf{B}^{-1}(\mathbf{I} + \mathbf{C})\mathbf{A}\mathbf{x}^T \\
&+ \mathbf{B}^{-1}(\mathbf{C}\mathbf{m}^T \circ \mathbf{C}\mathbf{A}\mathbf{x}^T) \\
&+ \mathbf{B}^{-1}\mathbf{z}^T + \mathbf{B}^{-1}(\mathbf{C}\mathbf{A}\mathbf{x}^T \circ \mathbf{C}\mathbf{z}^T),
\end{aligned} \qquad (12)$$

where $\mathbf{I}$ denotes the identity matrix.

Proof: Let $(Q, *)$ be a quasigroup of order 4, defined by (10), and let us define a new quasigroup operation $\bullet$ on Q, given by

$$\mathbf{x} \bullet \mathbf{y} \equiv \mathbf{x}^T + \mathbf{y}^T + \mathbf{C}\mathbf{x}^T \circ C\mathbf{y}^T.$$

Then, by Lemma 1, the parastrophe $\backslash_\bullet$ of $\bullet$ is defined by (11). Assume $\mathbf{x} * \mathbf{y} = \mathbf{z}$. Then, we have that

$$\begin{aligned}
\mathbf{z} = \mathbf{x} * \mathbf{y} &\equiv \mathbf{m}^T + \mathbf{A}\mathbf{x}^T + \mathbf{B}\mathbf{y}^T + \mathbf{C}\mathbf{A}\mathbf{x}^T \circ \mathbf{C}\mathbf{B}\mathbf{y}^T \\
&= \mathbf{m}^T + \mathbf{A}\mathbf{x}^T \bullet \mathbf{B}\mathbf{y}^T,
\end{aligned}$$

i.e. $\mathbf{m}^T + \mathbf{A}\mathbf{x}^T \bullet \mathbf{B}\mathbf{y}^T = \mathbf{z}^T$, and therefore, we get

$$\begin{aligned}
\mathbf{B}\mathbf{y}^T &= \mathbf{A}\mathbf{x}^T \backslash_\bullet (\mathbf{m}^T + \mathbf{z}^T) \\
&= (\mathbf{I} + \mathbf{C})\mathbf{A}\mathbf{x}^T + (\mathbf{m}^T + \mathbf{z}^T) + \mathbf{C}\mathbf{A}\mathbf{x}^T \circ \mathbf{C}(\mathbf{z}^T + \mathbf{m}^T).
\end{aligned}$$

This implies

$$\begin{aligned}
\mathbf{x} \backslash \mathbf{z} &\equiv \mathbf{y}^T \\
&= \mathbf{B}^{-1}(\mathbf{I} + \mathbf{C})\mathbf{A}\mathbf{x}^T + \mathbf{B}^{-1}(\mathbf{m}^T + \mathbf{z}^T) \\
&\quad + \mathbf{B}^{-1}(\mathbf{C}\mathbf{A}\mathbf{x}^T \circ \mathbf{C}(\mathbf{m}^T + \mathbf{z}^T)) \\
&= \mathbf{B}^{-1}(\mathbf{I} + \mathbf{C})\mathbf{A}\mathbf{x}^T + \mathbf{B}^{-1}\mathbf{m}^T + \mathbf{B}^{-1}\mathbf{z}^T \\
&\quad + \mathbf{B}^{-1}(\mathbf{C}\mathbf{A}\mathbf{x}^T \circ \mathbf{C}\mathbf{m}^T) + \mathbf{B}^{-1}(\mathbf{C}\mathbf{A}\mathbf{x}^T \circ \mathbf{C}\mathbf{z}^T) \\
&= \mathbf{B}^{-1}\mathbf{m}^T + \mathbf{B}^{-1}(\mathbf{I} + \mathbf{C})\mathbf{A}\mathbf{x}^T + \mathbf{B}^{-1}(\mathbf{C}\mathbf{m}^T \circ \mathbf{C}\mathbf{A}\mathbf{x}^T) \\
&\quad + \mathbf{B}^{-1}\mathbf{z}^T + \mathbf{B}^{-1}(\mathbf{C}\mathbf{A}\mathbf{x}^T \circ C\mathbf{z}^T),
\end{aligned}$$

which concludes the proof of the theorem. ■

IV. Conclusions and Future Work

In this paper, by using the presentations of quasigroups of order 4 as vector valued Boolean functions, we could present them in matrix form as well. Matrix presentations of the classes of linear, semi-linear and quadratic quasigroups of order 4 were derived. The generalization of the matrix presentation of quasigroups of order 4 was explored to derive also a matrix presentation for the corresponding quasigroup parastrophes. The results obtained are the needed prerequisites for continuing our efforts to give matrix presentations of quasigroups of order 2^n, as well as the matrix presentations of their parastrophes. In such a way their applications for building cryptographic primitives will be opened.

References

[1] D. Gligoroski, V. Dimitrova, S. Markovski, *Quasigroups as Boolean Functions, Their Equation Systems and Gröbner Bases*. In: Sala, M., Mora, T., Perret, L., Sakata, S., Traverso, C. (eds.), Gröbner Bases, Coding, and Cryptography, pp. 415-420. Springer, Heidelberg (2009)

[2] M. Mihova, M. Siljanoska, S. Markovski, *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)

[3] J.D.H. Smith, *An Introduction to Quasigroups and Their Representations*. Chapman & Hall/CRC (2007)