J. Math. Cryptol. **7** (2013), 111–141
DOI 10.1515/jmc-2012-0006

On a special class of multivariate quadratic quasigroups (MQQs)

Yanling Chen, Danilo Gligoroski and Svein J. Knapskog

Communicated by Otokar Grosek

Abstract. In this paper, we study a special class of recently introduced quasigroups called multivariate quadratic quasigroups (MQQs) and solve several open research problems about them. Our main contributions are threefold. The first is to provide a standard form of the MQQ generating function. Secondly, we show how to explicitly construct MQQs of higher orders and give lower bounds on the number of MQQs, which so far were open problems. Last, but not least, we refine the definition of MQQs of different types by introducing the notion of "MQQs of strict type". The new concept has the advantage of being invariant under invertible affine transformations over the set of the rows, columns and symbols of the multiplication table of an MQQ. It is therefore better suited to characterize the complexity of the underneath multivariate quadratic system.

Keywords. Quasigroup, multivariate quadratic system, Boolean function, matrix algebra.

2010 Mathematics Subject Classification. 20N05, 06E30, 15B34.

1 Introduction

The existence and importance of quasigroups (or equivalently Latin squares) in contemporary cryptology have been known for more than half a century since the work of Shannon [17]. The potential of quasigroups in the design of different types of cryptographic primitives and codes has been addressed in numerous works. For instance, Cooper et al. [3] used Latin squares to design secret sharing schemes; Carter et al. [2] proposed a version of the block cipher DES that uses Latin squares; in [16] Schnorr and Vaudenay discussed the need to use quasigroups in the design of cryptographic hash functions; the fast software stream cipher CryptMT by Matsumoto et al. [11] actually uses polynomially defined quasigroups that belong to the class of quasigroups Rivest analyzed in [14]; and a hardware stream cipher, Edon80 using four different quasigroups of order 4, was proposed in [7]. Recently, Grošek and Horák [9] addressed the problem of finding quasigroups with few associative triplets, emphasizing recent interest in quasigroups for design of cryptographic hash functions. Besides, applications of Latin squares to code con-

structions can be found in [13, 18] for designing new classes of structured low-density parity-check (LDPC) codes.

In this paper, we are interested in a new class of quasigroups, called *multivariate quadratic quasigroups* (MQQs), which was introduced in [6]. The characteristic of this class of quasigroups is that when represented as Boolean functions in their algebraic normal form, the quasigroups are multivariate quadratic. The authors of [6] constructed only MQQs of lower orders (up to 2^5) and left the following problems open:

(1) How to construct MQQs of higher orders?

(2) What is the number of MQQs or what is the lower bound of that number?

(3) What are the numbers for different sub-types or what are the lower bounds of those numbers?

Problem (1) was considered in [1], where the authors proposed a randomized algorithm to generate MQQs of higher orders. However, due to the random nature of the algorithm, their results are limited by the computational power of the computer. As a consequence, they can only generate MQQs of order 2^d, where d is up to 14. Besides, problems (2) and (3) are not under their investigation.

In [15], an approach is taken to construct quasigroups based on T-functions defined by Klimov and Shamir [10]. The new type of quasigroups is called T-multivariate quasigroups, which can be (but are not exclusively limited to be) quadratic. The quadratic quasigroups under their investigation are called T-MQQs, which are different from the ones defined in [6].

In this paper, we focus on the special class of MQQs introduced in [6] and provide answers to the open research problems (1), (2) and (3). Furthermore, we refine their classification of MQQs into different sub-types by a more strictly defined concept. The new classification has the advantage of being invariant under linear transformations and thus it better characterizes the complexity of the underneath multivariate quadratic system.

In this paper, the main mathematical tool we use is matrix algebra. So, unlike the randomized methods employed in [6] and [1] for the generation of MQQs, the nature of our analytical method leads us to general results regarding the construction, size and complexity of MQQs, which apply to the MQQs of order 2^d, for any positive integer d. Our fundamental results have already been applied in the new MQQ-SIG digital signature scheme [8] making the whole scheme several orders of magnitude faster than the corresponding RSA or ECC schemes.

2 Preliminaries

Unless otherwise defined in this paper, additions and multiplications are operations that are induced by the binary field GF(2).

Definition 2.1. A quasigroup $(Q, *)$ is a set Q with a binary operation $*$ such that for any $a, b \in Q$, there exist unique l, r such that

$$l * a = b; \quad a * r = b.$$

A quasigroup $(Q, *)$ is said to be of order n if the set Q has n elements.

Definition 2.2. Let $*$ and $\circ$ be two operations defined on Q. The operation $*$ is said to be isotopic to $\circ$, if there exist three permutations α, β, γ such that

$$l * r = \gamma^{-1}(\alpha(l) \circ \beta(r)) \tag{2.1}$$

for all $l, r \in Q$. We also say that $(Q, *)$ and $(Q, \circ)$ are isotopic, or that $(Q, *)$ is an isotope of $(Q, \circ)$ of the form (2.1). We denote the isotopy by (α, β, γ). In case that γ is the identical permutation, $(Q, *)$ is said to be a principal isotope of $(Q, \circ)$.

Consider a quasigroup $(Q, *)$ of order 2^d. One can choose a bijection $\rho : Q \mapsto \mathbb{Z}_2^d$ and represent $a \in Q$ by a unique d-bit binary string, i.e., $\rho(a) = (x_1, \ldots, x_d)$. The binary operation $*$ on Q can be seen as a vector valued operation

$$*_{\text{vv}} : \mathbb{Z}_2^d \times \mathbb{Z}_2^d \mapsto \mathbb{Z}_2^d$$

defined by

$$a * b = c \Leftrightarrow (x_1, \ldots, x_d) *_{\text{vv}} (y_1, \ldots, y_d) = (z_1, \ldots, z_d),$$

where $(x_1, \ldots, x_d), (y_1, \ldots, y_d)$ and $(z_1, \ldots, z_d)$ are the binary representations of a, b and c under bijection ρ, respectively. Each z_i, which depends on the $2d$ bits $x_1, \ldots, x_d, y_1, \ldots, y_d$, can be regarded as a $2d$-ary Boolean function $z_i = f_i(x_1, \ldots, x_d, y_1, \ldots, y_d)$, where $f_i : \mathbb{Z}_2^{2d} \mapsto \mathbb{Z}_2$ is determined by $*$.

Recall that each Boolean function can be represented in a unique way by its algebraic normal form (ANF) as a multivariate polynomial over GF(2). One can accordingly classify the quasigroups via the degrees of $(f_i)_{1 \le i \le d}$ (in their ANFs). Without loss of generality, we restrict our attention to those quasigroups defined upon the standard vector space $\mathbb{Z}_2^d$. In particular, we are interested in those quasigroups in which the degrees of $(f_i)_{1 \le i \le d}$ are at most 2, i.e., either linear or quadratic.

Definition 2.3 ([6, Definition 3]). Let $(\mathbb{Z}_2^d, *)$ be a quasigroup of order 2^d, and let $f_1, \ldots, f_d$ be the uniquely determined Boolean functions in their ANFs. The quasigroup $(\mathbb{Z}_2^d, *)$ is called multivariate quadratic quasigroup (MQQ) of *type* $\mathrm{Quad}_{d-k}\mathrm{Lin}_k$ if exactly $d-k$ of the polynomials $(f_i)_{1\le i\le d}$ are quadratic and k of them are linear, where $0 \le k < d$.

Suppose that f_i is quadratic. Then it can be written as a linear combination of $1, x_j, y_j, x_j x_k, y_j y_k$ and $x_j y_k$, where $1 \le i, j, k \le d$. Let $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$. Setting different terms apart, we can express f_i as follows:

$$f_i(x, y) = a_i(x, y) + b_{1i}(x) + b_{2i}(y) + c_i, \tag{2.2}$$

where $a_i(x, y)$ is a linear combination of $x_j y_k$, $b_{1i}(x)$ and $b_{2i}(y)$ are quadratic or linear polynomials with respect to $x_1, \ldots, x_d$ and $y_1, \ldots, y_d$, respectively, and $c_i \in \{0, 1\}$.

We denote by $\mathcal{B}[x]$ the ring of Boolean polynomials in $x = (x_1, \ldots, x_d)$. In this paper, we are mostly working with matrices whose elements are over $\mathcal{B}[x]$. In general, the determinant of a matrix over $\mathcal{B}[x]$ is also an element of $\mathcal{B}[x]$. However, we are interested in a special kind for our purpose of generating MQQs. Note that polynomial functions are used only for defining the quasigroup operation in this paper.

We recall [6, Theorem 2], in which sufficient conditions are proposed for a quasigroup to be an MQQ.

Theorem 2.4 ([6, Theorem 2]). *Let $A_1(x)$ and $A_2(y)$ be two $d \times d$ matrices over $\mathcal{B}[x]$ and $\mathcal{B}[y]$, respectively, with elements of linear Boolean polynomials. Let $b_1(x)$ and $b_2(y)$ be two $d \times 1$ vectors over $\mathcal{B}[x]$ and $\mathcal{B}[y]$, respectively, with elements of linear or quadratic Boolean polynomials. Suppose that*

$$\det(A_1(x)) = \det(A_2(y)) = 1, \tag{2.3}$$

and that

$$A_1(x) \cdot y^{\mathrm{T}} + b_1(x) = A_2(y) \cdot x^{\mathrm{T}} + b_2(y). \tag{2.4}$$

Define $(f_1(x, y), \ldots, f_d(x, y)) = z$ by

$$z^{\mathrm{T}} = A_1(x) \cdot y^{\mathrm{T}} + b_1(x). \tag{2.5}$$

Then the operation $a * b = (f_1(a, b), \ldots, f_d(a, b))$, $a, b \in Z_2^d$, defines an MQQ.

In [6], the authors run a heuristic algorithm to search for MQQs of order 2^5. Once $A_1(x), A_2(y), b_1(x), b_2(y)$ are found satisfying the sufficient conditions (2.3) and (2.4), then an MQQ can be produced by the generating function (2.5).

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

Table 1. An MQQ quasigroup $(\mathbb{Z}_2^3, *)$ of order 8.

Example 2.5. Recall [6, Example 1]. Let the quasigroup $(\mathbb{Z}_2^3, *)$ of order $2^3 = 8$ be given by the multiplication table in Table 1. This quasigroup can be generated by $A_1(x), A_2(y), b_1(x), b_2(y)$ defined as follows:

$$A_1(x) = \begin{bmatrix} x_1 + x_2 + x_3 & 1 + x_1 + x_2 + x_3 & x_1 + x_2 + x_3 \\ 1 + x_1 + x_2 + x_3 & x_1 + x_2 + x_3 & x_1 + x_2 + x_3 \\ x_3 & 1 + x_3 & 1 + x_1 + x_2 + x_3 \end{bmatrix},$$

$$A_2(y) = \begin{bmatrix} 1 + y_1 + y_2 + y_3 & y_1 + y_2 + y_3 & 1 + y_1 + y_2 + y_3 \\ y_1 + y_2 + y_3 & 1 + y_1 + y_2 + y_3 & 1 + y_1 + y_2 + y_3 \\ y_3 & 1 + y_3 & y_1 + y_2 + y_3 \end{bmatrix};$$

and

$$b_1(x) = \begin{bmatrix} x_1 + x_3 \\ 1 + x_2 + x_3 \\ 1 + x_2 \end{bmatrix}, \quad b_2(y) = \begin{bmatrix} y_2 \\ 1 + y_1 \\ 1 + y_2 + y_3 \end{bmatrix}.$$

It is easy to verify that in $\mathcal{B}[x]$, indeed $\det(A_1(x)) = \det(A_2(y)) = 1$ and (2.4) is fulfilled as well. By (2.5) we have $z = (f_1, f_2, f_3)$, where

$$\begin{aligned} f_1 &= x_1y_1 + x_1y_2 + x_1y_3 + x_2y_1 + x_2y_2 + x_2y_3 + x_3y_1 + x_3y_2 + x_3y_3 \\ &\quad + x_1 + x_3 + y_2, \\ f_2 &= x_1y_1 + x_1y_2 + x_1y_3 + x_2y_1 + x_2y_2 + x_2y_3 + x_3y_1 + x_3y_2 + x_3y_3 \\ &\quad + x_2 + x_3 + y_1 + y_2 + 1, \\ f_3 &= x_1y_3 + x_2y_3 + x_3y_1 + x_3y_2 + x_3y_3 + x_2 + y_2 + y_3 + 1. \end{aligned}$$

3 Observations and insights

In this section we review Theorem 2.4. We shall simplify the sufficient conditions for generating an MQQ and define a standard form for the matrices involved.

First, we note that in (2.4), $A_1(x)\cdot y^{\mathrm{T}}$ and $A_2(y)\cdot x^{\mathrm{T}}$ contain linear or quadratic Boolean expressions but no constant term 1. So the constant part (the part of the Boolean expressions of degree 0) of the MQQ generating function (2.5), as a binary vector c^{T}, must be from $b_1(x)$ or $b_2(y)$. Easily we have the following lemma.

Lemma 3.1. *$b_1(x)$ and $b_2(y)$ contain the same constant part, a binary vector c^{T}.*

Both $A_1(x)\cdot y^{\mathrm{T}}$ and $A_2(y)\cdot x^{\mathrm{T}}$ have quadratic terms in the form $x_i y_j$, $1 \le i, j \le d$. Thus we easily prove the following.

Lemma 3.2. *$b_1(x)$ and $b_2(y)$ contain no quadratic terms.*

Proof. Assume that $b_1(x)$ has a quadratic term $x_i x_j$, where $1 \le i \ne j \le d$. Then $A_1(x)\cdot y^{\mathrm{T}} + b_1(x)$ still contains the term $x_i x_j$, since $A_1(x)\cdot y^{\mathrm{T}}$ has quadratic terms only of the form $x_{i'} y_{j'}$, $1 \le i', j' \le d$, which cannot cancel $x_i x_j$. Thus $x_i x_j$ must also appear in $A_2(y)\cdot x^{\mathrm{T}} + b_2(y)$, due to (2.4). However, it is impossible since $A_2(y)\cdot x^{\mathrm{T}}$ has quadratic terms only of the form $y_{i'} x_{j'}$, $1 \le i', j' \le d$, and $b_2(y)$ does not depend on $x_1, \ldots, x_d$ at all. This implies that $b_1(x)$ has no quadratic terms. A similar proof can be applied to $b_2(y)$ to conclude the lemma. □

So far, we have narrowed down the choices of $b_1(x), b_2(y)$ to those with elements of linear Boolean polynomials. Recall that $A_1(x)\cdot y^{\mathrm{T}}$ and $A_2(y)\cdot x^{\mathrm{T}}$ have quadratic terms only of the form $x_i y_j$, $1 \le i, j \le d$. If we write the generating function of the MQQs defined in Theorem 2.4 in the form of (2.2),

$$f_i = a_i(x, y) + b_{1i}(x) + b_{2i}(y) + c_i,$$

it is easy to see that Theorem 2.4 defines a special class of MQQs with restrictive choices of $a_i(x, y)$ for being bilinear, $b_{1i}(x)$ and $b_{2i}(y)$ for being linear.

3.1 Linear transformation

By Lemma 3.2, $b_1(x)$ and $b_2(y)$ are vectors of linear Boolean polynomials. So there exist square matrices B_1 and B_2 such that

$$b_1(x) = \mathrm{B}_1 x^{\mathrm{T}} + c^{\mathrm{T}} \quad \text{and} \quad b_2(y) = \mathrm{B}_2 y^{\mathrm{T}} + c^{\mathrm{T}}.$$

Setting $x = 0$, we have $x * y = \mathrm{B}_2 y^{\mathrm{T}} + c^{\mathrm{T}}$ by (2.4) and (2.5). According to the definition of the quasigroup, B_2 must be non-singular. So is B_1 as well.

Let β_1, β_2 be the linear transformations determined by $\mathrm{B}_1, \mathrm{B}_2$, respectively, i.e.,

$$\beta_1(x) = x{\mathrm{B}_1}^{\mathrm{T}} \quad \text{and} \quad \beta_2(y) = y{\mathrm{B}_2}^{\mathrm{T}}. \tag{3.1}$$

We apply them to express the sufficient conditions in Theorem 2.4. First we obtain the followings on $A_1(x) \cdot y^{\mathrm{T}}$ and $A_2(y) \cdot x^{\mathrm{T}}$:

$$A_1(x) \cdot y^{\mathrm{T}} = A_1^*(\beta_1(x)) \cdot \beta_2(y)^{\mathrm{T}},$$
$$A_2(y) \cdot x^{\mathrm{T}} = A_2^*(\beta_2(y)) \cdot \beta_1(x)^{\mathrm{T}},$$

where

$$A_1^*(x) = A_1(\beta_1^{-1}(x)) \cdot {\mathrm{B}_2}^{-1},$$
$$A_2^*(y) = A_2(\beta_2^{-1}(y)) \cdot {\mathrm{B}_1}^{-1}.$$

Since $\det(A_1(x)) = \det(A_2(y)) = 1$ is irrelevant to the values of x and y, and $\mathrm{B}_1, \mathrm{B}_2$ are both binary non-singular matrices, i.e., $\det(\mathrm{B}_1) = \det(\mathrm{B}_2) = 1$, straightforwardly we have

$$\det(A_1^*(x)) = \det(A_2^*(y)) = 1, \tag{3.2}$$

and (3.2) is equivalent to condition (2.3) in Theorem 2.4. Moreover, condition (2.4) in Theorem 2.4 can be rewritten to be

$$A_1^*(\beta_1(x)) \cdot \beta_2(y)^{\mathrm{T}} + \beta_1(x)^{\mathrm{T}} = A_2^*(\beta_2(y)) \cdot \beta_1(x)^{\mathrm{T}} + \beta_2(y)^{\mathrm{T}},$$

and further simplified to be

$$A_1^*(x) \cdot y^{\mathrm{T}} + x^{\mathrm{T}} = A_2^*(y) \cdot x^{\mathrm{T}} + y^{\mathrm{T}}. \tag{3.3}$$

3.2 $A_1^*(x), A_2^*(y)$ instead of $A_1(x), A_2(y)$

By $A_1^*(x), A_2^*(y)$, which are matrices over $\mathcal{B}[x]$ and $\mathcal{B}[y]$, respectively, with elements of linear Boolean polynomials, we denote the following:

$$A_1^*(x) = \left[f_0^{ij} + \sum_{k=1}^{d} f_k^{ij} x_k \right]_{d \times d}, \quad A_2^*(y) = \left[g_0^{ij} + \sum_{k=1}^{d} g_k^{ij} y_k \right]_{d \times d},$$

where $f_k^{ij}, g_k^{ij} \in \{0, 1\}$, for $1 \le i, j, k \le d$. In order to fulfill (3.3), we have that for $1 \le i \le d$, the following equation holds:

$$\sum_{j=1}^{d} y_j \cdot \left(f_0^{ij} + \sum_{k=1}^{d} f_k^{ij} x_k \right) + x_i = \sum_{j=1}^{d} x_j \cdot \left(g_0^{ij} + \sum_{k=1}^{d} g_k^{ij} y_k \right) + y_i.$$

Easy comparisons show that for $1 \le i, j, k \le d$,

$$\begin{cases} f_0^{ii} = g_0^{ii} = 1; \\ f_0^{ij} = g_0^{ij} = 0, \quad i \neq j; \\ f_k^{ij} = g_j^{ik}. \end{cases} \tag{3.4}$$

From (3.4), we see that $A_1^*(x)$ and $A_2^*(x)$ are kind of symmetric. To better illustrate this property, we define F_i, for $1 \le i \le d$, by

$$\mathrm{F}_i = \begin{bmatrix} f_1^{i1} & f_2^{i1} & \cdots & f_d^{i1} \\ f_1^{i2} & f_2^{i2} & \cdots & f_d^{i2} \\ \vdots & \vdots & \vdots & \vdots \\ f_1^{id} & f_2^{id} & \cdots & f_d^{id} \end{bmatrix}.$$

It is easy to see that $A_1^*(x)$ and $A_2^*(x)$ which fulfill (3.3) are in the form of

$$A_1^*(x) = \mathrm{I}_d + \begin{bmatrix} x \cdot \mathrm{F}_1^{\mathrm{T}} \\ x \cdot \mathrm{F}_2^{\mathrm{T}} \\ \vdots \\ x \cdot \mathrm{F}_d^{\mathrm{T}} \end{bmatrix}, \tag{3.5}$$

$$A_2^*(y) = \mathrm{I}_d + \begin{bmatrix} y \cdot \mathrm{F}_1 \\ y \cdot \mathrm{F}_2 \\ \vdots \\ y \cdot \mathrm{F}_d \end{bmatrix}, \tag{3.6}$$

where I_d is the identity matrix of order d.

3.3 A instead of $A_1^*(x)$ and $A_2^*(x)$

Definition 3.3. Let vec$(\cdot)$ be an operator that turns a matrix into a long vector by collecting the elements column-wise, i.e., for an $m \times n$ matrix $\mathrm{C} = [c_{ij}]_{m \times n}$,

$$\mathrm{vec}(\mathrm{C}) = (c_{11}, \ldots, c_{m1}, c_{12}, \ldots, c_{m2}, \ldots, c_{n1}, \ldots, c_{nm})^{\mathrm{T}}.$$

Let A be a $d \times d^2$ matrix with $\mathrm{vec}(\mathrm{F}_i)^{\mathrm{T}}$ being its i-th row, i.e.,

$$\mathrm{A} = (\mathrm{vec}(\mathrm{F}_1), \mathrm{vec}(\mathrm{F}_2), \ldots, \mathrm{vec}(\mathrm{F}_d))^{\mathrm{T}}. \tag{3.7}$$

Clearly A is uniquely determined by $\mathrm{F}_1, \mathrm{F}_2, \ldots, \mathrm{F}_d$ and vice versa. In particular,

$$\mathrm{A} \cdot (x \otimes y)^{\mathrm{T}} \overset{(a)}{=} \begin{bmatrix} y \cdot \mathrm{F}_1 \cdot x^{\mathrm{T}} \\ y \cdot \mathrm{F}_2 \cdot x^{\mathrm{T}} \\ \vdots \\ y \cdot \mathrm{F}_d \cdot x^{\mathrm{T}} \end{bmatrix} = \begin{bmatrix} x \cdot \mathrm{F}_1^{\mathrm{T}} \cdot y^{\mathrm{T}} \\ x \cdot \mathrm{F}_2^{\mathrm{T}} \cdot y^{\mathrm{T}} \\ \vdots \\ x \cdot \mathrm{F}_d^{\mathrm{T}} \cdot y^{\mathrm{T}} \end{bmatrix}, \tag{3.8}$$

where $\otimes$ is the Kronecker product; and (a) is due to the property of the $\mathrm{vec}(\cdot)$ operator and the Kronecker product: $(\mathrm{X} \otimes \mathrm{Y})\,\mathrm{vec}(\mathrm{F}) = \mathrm{vec}(\mathrm{YFX}^{\mathrm{T}})$.

Definition 3.4. For any A as defined in (3.7), let $\Gamma_{\mathrm{A}}(x)$ and $\Delta_{\mathrm{A}}(y)$ be $A_1^*(x)$ and $A_2^*(y)$ in the associate symmetric form of (3.5) and (3.6), respectively.

For any A, we can further simplify the sufficient conditions (3.2) and (3.3) for an MQQ into the following one:

$$\det(\Gamma_{\mathrm{A}}(x)) = \det(\Delta_{\mathrm{A}}(y)) = 1.$$

3.4 A standard MQQ generating function

As a conclusion of the above discussion, we rewrite the generating function (2.5) of the MQQs in Theorem 2.4 as follows:

$$\begin{aligned} z^{\mathrm{T}} &= A_1(x) \cdot y^{\mathrm{T}} + b_1(x) \\ &\overset{(a)}{=} A_1^*(\beta_1(x)) \cdot \beta_2(y)^{\mathrm{T}} + \beta_1(x)^{\mathrm{T}} + c^{\mathrm{T}} \\ &\overset{(b)}{=} \begin{bmatrix} \beta_1(x) \cdot \mathrm{F}_1^{\mathrm{T}} \cdot \beta_2(y)^{\mathrm{T}} \\ \beta_1(x) \cdot \mathrm{F}_2^{\mathrm{T}} \cdot \beta_2(y)^{\mathrm{T}} \\ \vdots \\ \beta_1(x) \cdot \mathrm{F}_d^{\mathrm{T}} \cdot \beta_2(y)^{\mathrm{T}} \end{bmatrix} + \beta_1(x)^{\mathrm{T}} + \beta_2(y)^{\mathrm{T}} + c^{\mathrm{T}} \\ &\overset{(c)}{=} \mathrm{A} \cdot (\beta_1(x) \otimes \beta_2(y))^{\mathrm{T}} + \beta_1(x)^{\mathrm{T}} + \beta_2(y)^{\mathrm{T}} + c^{\mathrm{T}} \\ &\overset{(a)}{=} \mathrm{A} \cdot (\mathrm{B}_1 x^{\mathrm{T}} \otimes \mathrm{B}_2 y^{\mathrm{T}}) + \mathrm{B}_1 x^{\mathrm{T}} + \mathrm{B}_2 y^{\mathrm{T}} + c^{\mathrm{T}} \\ &\overset{(d)}{=} \mathrm{A} \cdot (\mathrm{B}_1 \otimes \mathrm{B}_2) \cdot (x \otimes y)^{\mathrm{T}} + \mathrm{B}_1 x^{\mathrm{T}} + \mathrm{B}_2 y^{\mathrm{T}} + c^{\mathrm{T}}. \end{aligned}$$

where (a) is obtained by applying linear transformations as defined in (3.1); (b) is by (3.5); (c) is by (3.8); (d) is by the Kronecker rules: $\mathrm{CD} \otimes \mathrm{EF} = (\mathrm{C} \otimes \mathrm{E}) \cdot (\mathrm{D} \otimes \mathrm{F})$ and $(\mathrm{C} \otimes \mathrm{D})^{\mathrm{T}} = \mathrm{C}^{\mathrm{T}} \otimes \mathrm{D}^{\mathrm{T}}$.

As a direct result, we provide in Theorem 3.5 a standard form of Theorem 2.4.

Theorem 3.5. *Let* A *be a* $d \times d^2$ *matrix as defined in* (3.7)*. Correspondingly one obtains matrices* $\Gamma_{\mathrm{A}}(x)$ *and* $\Delta_{\mathrm{A}}(y)$*, both of which are* $d \times d$ *matrices as defined in Definition* 3.4*. Suppose that for each possible value of* x, y *in* $\mathbb{Z}_2^d$*,*

$$\det(\Gamma_{\mathrm{A}}(x)) = \det(\Delta_{\mathrm{A}}(y)) = 1. \tag{3.9}$$

Then for any non-singular $d \times d$ *binary matrices* $\mathrm{B}_1, \mathrm{B}_2$*, and any binary vector* c *of* d *elements, we have a generating function* $z = (f_1(x, y), \ldots, f_d(x, y))$ *by*

$$z^{\mathrm{T}} = \mathrm{A} \cdot (\mathrm{B}_1 \otimes \mathrm{B}_2) \cdot (x \otimes y)^{\mathrm{T}} + \mathrm{B}_1 x^{\mathrm{T}} + \mathrm{B}_2 y^{\mathrm{T}} + c^{\mathrm{T}}. \tag{3.10}$$

The operation $a * b = (f_1(a, b), \ldots, f_d(a, b))$*,* $a, b \in \mathbb{Z}_2^d$*, defines an MQQ* $(\mathbb{Z}_2^d, *)$*.*

Theorem 3.5 is a standard form of Theorem 2.4, since the MQQ's generating function (3.10) is presented in the same way as a normal quadratic equation, in the order of the quadratic term, linear term and constant term. Notably, it is of the form (2.2) as well.

Implied by the above theorem, to generate MQQs, one only needs to find the appropriate A such that condition (3.9) is satisfied. This significantly simplifies the method deployed in [6], which needs to search for $A_1(x), A_2(y), b_1(x), b_2(y)$ which fulfill constraints (2.3) and (2.4).

Example 3.6. Consider the MQQ defined in Example 2.5. We write down its generating function in a standard form. Easily we identify the quadratic parameter A, linear parameters $\mathrm{B}_1, \mathrm{B}_1$ and constant term c to be the following:

$$\mathrm{A} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}; \tag{3.11}$$

$$\mathrm{B}_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \mathrm{B}_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}; \quad c^{\mathrm{T}} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}.$$

Easy calculation gives us

$$\mathrm{A}(\mathrm{B}_1 \otimes \mathrm{B}_2) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Note that the i-th row elements of $\mathrm{A}(\mathrm{B}_1 \otimes \mathrm{B}_2)$ are a collection of the coefficients of the quadratic terms of f_i, with respect to $x_1y_1, x_1y_2, \ldots, x_3y_3$; whilst the i-th row elements of B_1 and B_2 correspond to the coefficients of the linear terms, in the order of x_1, x_2, x_3 and y_1, y_2, y_3. For f_i, $1 \leq i \leq 3$, one can refer to Example 2.5.

3.5 Isotopic MQQs

Definition 3.7. Let A fulfill Theorem 3.5. Define $(f_1(x, y), \ldots, f_d(x, y)) = z$ by

$$z^{\mathrm{T}} = \mathrm{A} \cdot (x \otimes y)^{\mathrm{T}} + x^{\mathrm{T}} + y^{\mathrm{T}} + c^{\mathrm{T}}.$$

Then the operation $a *_e b = (f_1(a, b), \ldots, f_d(a, b))$, $a, b \in \mathbb{Z}_2^d$, defines an MQQ $(\mathbb{Z}_2^d, *_e)$, which is isotopic to $(\mathbb{Z}_2^d, *)$ in the manner that $a * b = (a\mathrm{B}_1{}^{\mathrm{T}}) *_e (b\mathrm{B}_2{}^{\mathrm{T}})$.

By Definition 2.2, the isotopy between $(\mathbb{Z}_2^d, *)$ and $(\mathbb{Z}_2^d, *_e)$ is defined by the triplet of permutations $(\mathrm{B}_1, \mathrm{B}_2, \mathrm{I}_d)$, where I_d corresponds to the identity permutation. Therefore, we have the following result.

Theorem 3.8. *$(\mathbb{Z}_2^d, *)$ and $(\mathbb{Z}_2^d, *_e)$ are isotopic.*

Definition 3.9. Let A fulfill Theorem 3.5 and $\mathrm{A}, \mathrm{B}_1, \mathrm{B}_2, c$ define $(\mathbb{Z}_2^d, *)$. For a non-singular binary matrix B, define $(f_1(x, y), \ldots, f_d(x, y)) = z$ by

$$z^{\mathrm{T}} = \mathrm{B} \cdot \left\{ \mathrm{A} \cdot (\mathrm{B}_1 \otimes \mathrm{B}_2) \cdot (x \otimes y)^{\mathrm{T}} + \mathrm{B}_1 x^{\mathrm{T}} + \mathrm{B}_2 y^{\mathrm{T}} + c^{\mathrm{T}} \right\}. \tag{3.12}$$

Then the operation $a *_i b = (f_1(a, b), \ldots, f_d(a, b))$, $a, b \in \mathbb{Z}_2^d$, defines an MQQ $(\mathbb{Z}_2^d, *_i)$, which is isotopic to $(\mathbb{Z}_2^d, *)$ in the manner that $a *_i b = (a * b) \cdot \mathrm{B}^{\mathrm{T}}$.

By Definition 2.2, it is easy to see that $(\mathbb{Z}_2^d, *_i)$ is also isotopic to $(\mathbb{Z}_2^d, *_e)$. The isotopy is defined by the triplet of permutations $(\mathrm{B}_1, \mathrm{B}_2, \mathrm{B}^{-1})$.

Theorem 3.10. *$(\mathbb{Z}_2^d, *_i)$ is an isotope of $(\mathbb{Z}_2^d, *_e)$.*

In the following, we show that every MQQ of kind $(\mathbb{Z}_2^d, *_i)$ has its generating function also in a standard form as described in Theorem 3.5. Consider its generating function (3.12). We take Bc as the constant term, BB_1 and BB_2 as the linear parameters and further proceed to the quadratic term:

$$\begin{aligned}
\mathrm{BA}(\mathrm{B}_1 \otimes \mathrm{B}_2) &= \mathrm{BA}(\mathrm{B}^{-1}\mathrm{BB}_1 \otimes \mathrm{B}^{-1}\mathrm{BB}_2) \\
&\overset{(a)}{=} \mathrm{BA}(\mathrm{B}^{-1} \otimes \mathrm{B}^{-1})(\mathrm{BB}_1 \otimes \mathrm{BB}_2) \\
&\overset{(b)}{=} \mathrm{BA}(\mathrm{B} \otimes \mathrm{B})^{-1}(\mathrm{BB}_1 \otimes \mathrm{BB}_2),
\end{aligned}$$

where (a), (b) follow by the Kronecker rules

$$\mathrm{CD} \otimes \mathrm{EF} = (\mathrm{C} \otimes \mathrm{E})(\mathrm{D} \otimes \mathrm{F}) \quad \text{and} \quad (\mathrm{C} \otimes \mathrm{D})^{-1} = \mathrm{C}^{-1} \otimes \mathrm{D}^{-1}.$$

We obtain the quadratic parameter $\mathrm{Q} = \mathrm{BA}(\mathrm{B} \otimes \mathrm{B})^{-1}$. Moreover, we can prove that Q satisfies the sufficient condition (3.9), i.e., $\det(\Gamma_{\mathrm{Q}}(x)) = \det(\Delta_{\mathrm{Q}}(y)) = 1$ for each possible value of x, y in $\mathbb{Z}_2^d$. This can be done by equivalently showing that $\mathrm{B}^{-1}\Gamma_{\mathrm{Q}}(x\mathrm{B}^{\mathrm{T}})\mathrm{B} = \Gamma_{\mathrm{A}}(x)$ and $\mathrm{B}^{-1}\Delta_{\mathrm{Q}}(y\mathrm{B}^{\mathrm{T}})\mathrm{B} = \Delta_{\mathrm{A}}(y)$ which follow directly by the definition of $\Gamma_{\mathrm{Q}}(x)$ and $\Delta_{\mathrm{Q}}(y)$.

So far, we have shown that one can derive isotopic MQQs of $(\mathbb{Z}_2^d, *_e)$ by employing permutations on the rows x, columns y and output symbols z. The permutations under our consideration are invertible linear transformations that can be represented by nonsingular matrices $\mathrm{B}_1, \mathrm{B}_2$ and B, respectively.

Not surprisingly, one can extend the scope of the permutations used to derive isotopic MQQs, by considering the invertible affine transformations that can be represented by a nonsingular matrix and a constant vector. The reason why we restrict our attention to this kind of permutations is to ensure that the derived isotopic quasigroups are quadratic in their ANFs, i.e., MQQs.

Theorem 3.11. *One can derive isotopic MQQs from* $(\mathbb{Z}_2^d, *)$ *according to Definition* 2.2 *by assigning the triplet* (α, β, γ) *of permutations to be invertible affine transformations. Notably the derived MQQs have their generating functions maintain a standard form as described in Theorem* 3.5.

Proof. First, we recall the fact that employing permutations as linear transformations provides us with isotopic MQQs with their generating functions still in a standard form, as one derives $(\mathbb{Z}_2^d, *_i)$ from $(\mathbb{Z}_2^d, *_e)$ by a triplet of permutations determined by $(\mathrm{B}_1, \mathrm{B}_2, \mathrm{B}^{-1})$.

Now let us consider the permutations determined by affine transformations. For simplicity's sake, we apply to $(\mathbb{Z}_2^d, *_e)$ the triplet permutation (α, β, γ) defined by

$$\alpha(x) = x + l; \quad \beta(y) = y + r; \quad \gamma(z) = z + t. \tag{3.13}$$

We obtain an isotopic quasigroup $(\mathbb{Z}_2^d, \circ)$ defined by the operation

$$a \circ b = \gamma^{-1}(\alpha(a) *_e \beta(b)) \quad \text{for } a, b \in \mathbb{Z}_2^d.$$

Note that $(\mathbb{Z}_2^d, \circ)$ has the generating function $(f_1(x, y), \ldots, f_d(x, y)) = z$, where

$$z^{\mathrm{T}} = \mathrm{A} \cdot [(x + l) \otimes (y + r)]^{\mathrm{T}} + (x + l)^{\mathrm{T}} + (y + r)^{\mathrm{T}} + (c - t)^{\mathrm{T}},$$

which is equal to

$$\mathrm{A} \cdot (x \otimes y)^{\mathrm{T}} + \Delta_{\mathrm{A}}(r) \cdot x^{\mathrm{T}} + \Gamma_{\mathrm{A}}(l) \cdot y^{\mathrm{T}} + \mathrm{A} \cdot (l \otimes r)^{\mathrm{T}} + (c + l + r - t)^{\mathrm{T}}. \tag{3.14}$$

Note that we have $\det(\Gamma_{\mathrm{A}}(l)) = \det(\Delta_{\mathrm{A}}(r)) = 1$ by (3.9). So $\Gamma_{\mathrm{A}}(l)$ and $\Delta_{\mathrm{A}}(r)$ are binary non-singular matrices. Taking $\Gamma_{\mathrm{A}}(l)$ and $\Delta_{\mathrm{A}}(r)$ as linear parameters of the generating function of $(\mathbb{Z}_2^d, \circ)$, we obtain the quadratic parameter $\mathrm{Q} = \mathrm{A}[\Delta_{\mathrm{A}}(r) \otimes \Gamma_{\mathrm{A}}(l)]^{-1}$ due to the fact that

$$\mathrm{A} \cdot (x \otimes y)^{\mathrm{T}} \overset{\text{(a)}}{=} \mathrm{A} \cdot (x^{\mathrm{T}} \otimes y^{\mathrm{T}}) \overset{\text{(b)}}{=} \mathrm{Q} \cdot \big(\Delta_{\mathrm{A}}(r)x^{\mathrm{T}} \otimes \Gamma_{\mathrm{A}}(l)y^{\mathrm{T}}\big),$$

where (a), (b) follow by the Kronecker rules

$$(\mathrm{C} \otimes \mathrm{D})^{\mathrm{T}} = \mathrm{C}^{\mathrm{T}} \otimes \mathrm{D}^{\mathrm{T}} \quad \text{and} \quad \mathrm{CD} \otimes \mathrm{EF} = (\mathrm{C} \otimes \mathrm{E}) \cdot (\mathrm{D} \otimes \mathrm{F}).$$

Similarly to the fact that A is uniquely determined by $\mathrm{F}_1, \mathrm{F}_2, \ldots, \mathrm{F}_d$ as in (3.7), it is easy to see that Q is uniquely determined by $\mathrm{G}_1, \mathrm{G}_2, \ldots, \mathrm{G}_d$, where $\mathrm{G}_i = (\Gamma_{\mathrm{A}}(l)^{-1})^{\mathrm{T}} \cdot \mathrm{F}_i \cdot \Delta_{\mathrm{A}}(r)^{-1}$ for $1 \le i \le d$. Moreover, we can prove that Q satisfies the sufficient condition (3.9), i.e., $\det(\Gamma_{\mathrm{Q}}(x)) = \det(\Delta_{\mathrm{Q}}(y)) = 1$ for each possible value of x, y in $\mathbb{Z}_2^d$. This can be done by equivalently showing that

$$\Gamma_{\mathrm{Q}}(x\Delta_{\mathrm{A}}(r)^{\mathrm{T}}) \cdot \Gamma_{\mathrm{A}}(l) = \Gamma_{\mathrm{A}}(x + l),$$
$$\Delta_{\mathrm{Q}}(y\Gamma_{\mathrm{A}}(l)^{\mathrm{T}}) \cdot \Delta_{\mathrm{A}}(r) = \Delta_{\mathrm{A}}(y + r).$$

Thus we conclude that the generating function (3.14), which can be represented in a standard form, defines the MQQ $(\mathbb{Z}_2^d, \circ)$. □

As a conclusion, Theorem 3.5 generates MQQs of kind $(\mathbb{Z}_2^d, *)$, which include isotopic MQQs of kinds

- $(\mathbb{Z}_2^d, *_e)$ by permutations as linear transformations on the rows x, columns y;
- $(\mathbb{Z}_2^d, *_i)$ by permutations as linear transformations on output symbols z;
- $(\mathbb{Z}_2^d, \circ)$ by permutations determined by invertible affine transformations.

For detailed parameter settings of MQQs of kinds $(\mathbb{Z}_2^d, *_e)$, $(\mathbb{Z}_2^d, *)$ and $(\mathbb{Z}_2^d, *_i)$ and their relations, one can refer to Table 2. Besides, we have the following theorem as a byproduct of the above discussions.

Theorem 3.12. *If a* $d \times d^2$ *binary matrix* A *fulfills Theorem* 3.5*, then*

- $\mathrm{A}[\Delta_{\mathrm{A}}(r) \otimes \Gamma_{\mathrm{A}}(l)]^{-1}$ *for any* $r, l \in \mathbb{Z}_2^d$,
- $\mathrm{BA}(\mathrm{B} \otimes \mathrm{B})^{-1}$ *for any binary non-singular* $d \times d$ *matrix* B

fulfill Theorem 3.5 *as well.*

	quadratic parameter	linear parameters	constant parameter
$(\mathbb{Z}_2^d, *_e)$	A	$\mathrm{I}_d, \mathrm{I}_d$	c
$(\mathbb{Z}_2^d, *)$	A	$\mathrm{B}_1, \mathrm{B}_2$	c
$(\mathbb{Z}_2^d, *_i)$	$\mathrm{BA}(\mathrm{B} \otimes \mathrm{B})^{-1}$	$\mathrm{BB}_1, \mathrm{BB}_2$	$\mathrm{B}c$
$a *_i b = \gamma^{-1}(a * b) = \gamma^{-1}(\alpha(a) *_e \beta(b))$ for all $a, b \in \mathbb{Z}_2^d$, where α, β and γ are permutations determined by $\mathrm{B}_1, \mathrm{B}_2$ and B^{-1}, respectively.			

Table 2. Relation between MQQs $(\mathbb{Z}_2^d, *_e)$, $(\mathbb{Z}_2^d, *)$ and $(\mathbb{Z}_2^d, *_i)$.

Note that once an appropriate A is found, according to the generating function of $(\mathbb{Z}_2^d, *)$, i.e. (3.10) in Theorem 3.5, different MQQs can be derived by choosing two non-singular binary matrices $\mathrm{B}_1, \mathrm{B}_2$ and a binary vector c differently. It is known that for a fixed d, there are $\prod_{t=0}^{d-1}(2^d - 2^t)$ non-singular binary matrices in total. Consequently, we have the following lemma.

Lemma 3.13. *Corresponding to one appropriate* A, $\prod_{t=0}^{d-1}(2^d - 2^t)^2 \cdot 2^d$ *MQQs can be derived according to Theorem* 3.5 *by choosing* $\mathrm{B}_1, \mathrm{B}_2$ *and* c *differently.*

According to the heuristic algorithm in [6], the average number of attempts for finding an MQQ of order 2^5 is around 2^{15}. However, by Theorem 3.5, once one appropriate A is found, about 2^{51} MQQs can be straightforwardly derived.

4 MQQs of strictly defined types

Consider the MQQ $(\mathbb{Z}_2^d, *)$ defined in Theorem 3.5. We let $f_1, \ldots, f_d$ be the polynomials uniquely determined by the generating function (3.10). It is easy to see that they are $2d$-ary linear or quadratic Boolean functions. Recall that the underlying MQ problem is NP-complete [5, p. 251] over GF(2). That is, it is generally hard to solve a randomly selected multivariate system of m equations in n variables $x_1, x_2, \ldots, x_n$ over GF(2), for given $f_1, \ldots, f_m \in \mathrm{GF}(2)$,

$$\begin{cases} f_1 = p_1(x_1, \ldots, x_n), \\ f_2 = p_2(x_1, \ldots, x_n), \\ \quad \vdots \\ f_m = p_m(x_1, \ldots, x_n), \end{cases}$$

where the polynomials $p_i(x_1, \ldots, x_n)$ have the form

$$p_i(x_1, \ldots, x_n) = \sum_{1 \le j \le k \le n} \gamma_{i,j,k} x_j x_k + \sum_{j=1}^{n} \beta_{i,j} x_j + \alpha_i$$

for $1 \le i \le m$ and $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in \mathrm{GF}(2)$. However, not all instances of MQ problems are difficult. For example, if one polynomial p_i (or a linear combination of $p_1, \ldots, p_m$) is linear, then replacing p_i by f_i in other polynomials will result in an MQ problem involving at most $m-1$ equations in at most $n-1$ unknowns. If the resulting system still consists of linear equations, the problem clearly can be even further simplified. And we know that a linear multivariate system or a multivariate system involving only one polynomial of degree ≥ 2 can be easily solved in polynomial time. In fact, as being demonstrated in [4], such linear relations can be employed to simplify the system of multivariate quadratic equations and eventually solve some underdefined MQ problems.

In [6], the authors emphasize the set of MQQs of type $\mathrm{Quad}_{d-k}\mathrm{Lin}_k$, $0 \le k < d$, as an important complexity character. They also point out that the quadratic polynomials could cancel each other and thus result in a linear form. Actually, this phenomenon can be more common than previously expected. For instance, given an MQQ of type $\mathrm{Quad}_{d-k}\mathrm{Lin}_k$, $1 \le k < d$, one can simply replace the original linear polynomials by their combination with some of the quadratic polynomials and the result will be an isotopic MQQ of type $\mathrm{Quad}_{d-k'}\mathrm{Lin}_{k'}$ with $k' < k$, i.e., with more quadratic polynomials and less linear ones. (This is an instance of deriving isotopic $(\mathbb{Z}_2^d, *_i)$ from $(\mathbb{Z}_2^d, *)$ through a permutation on the output symbols, which is determined by a non-singular binary matrix B.) Thus the type $\mathrm{Quad}_{d-k}\mathrm{Lin}_k$ of an MQQ does not reveal its true complexity. Therefore, a new criteria is needed in order to better characterize the complexity of an MQQ. To fulfill such a need, we refine the definition of MQQs of type $\mathrm{Quad}_{d-k}\mathrm{Lin}_k$ into a strictly defined type.

Definition 4.1. Let $(\mathbb{Z}_2^d, *)$ be a quasigroup of order 2^d, and let $f_1, \ldots, f_d$ be the uniquely determined Boolean functions in their ANFs. The quasigroup $(\mathbb{Z}_2^d, *)$ is called an MQQ of *strict type* and denoted by $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_k$, where $0 \le k < d$, if there are at most $d-k$ quadratic polynomials in $(f_i)_{1 \le i \le d}$ whose linear combinations do not result in a linear form.

4.1 Invariance under invertible affine transformations

In general, applying permutations determined by affine transformations to an MQQ on its rows and columns of their multiplication tables does not effect the number of the quadratic polynomials in the output of their generating functions.

Therefore, the type of the MQQs is invariant under such row and column permutations. However, this property does not hold for the permutations on the output symbols, as we have discussed previously. One can also refer to Example 4.4 for a concrete example. So we have the following theorem.

Theorem 4.2. *The type of the MQQs as defined in Definition* 2.3 *is invariant under the row and column permutations which are determined by invertible affine transformations, but not to the output symbol permutations.*

Speaking of the strictly defined type of MQQs, we first consider the MQQ $(\mathbb{Z}_2^d, *)$ as defined in Theorem 3.5. Taking a look at its generating function (3.10), we note that the i-th row of $\mathrm{A}(\mathrm{B}_1 \otimes \mathrm{B}_2)$ is a collection of the quadratic coefficients of the output polynomial f_i with respect to $x_1y_1, x_1y_2, \ldots, x_dy_d$, for $1 \leq i \leq d$. Whenever the output polynomials cancel each other resulting in a linear form, correspondingly there is a linear combination of the rows of $\mathrm{A}(\mathrm{B}_1 \otimes \mathrm{B}_2)$ resulting in a zero vector, and vice versa. If we suppose that $(\mathbb{Z}_2^d, *)$ is of strict type $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_k$, $0 \leq k < d$, we have by Definition 4.1

$$d - k = \mathrm{rk}(\mathrm{A}(\mathrm{B}_1 \otimes \mathrm{B}_2)) = \mathrm{rk}(\mathrm{A}),$$

where $\mathrm{rk}(\mathrm{A})$ is the rank of the matrix A. The last equation is obtained since $\mathrm{B}_1, \mathrm{B}_2$ are both non-singular and so is $\mathrm{B}_1 \otimes \mathrm{B}_2$. That is, the strict type of MQQ $(\mathbb{Z}_2^d, *)$ is characterized by A, the quadratic parameter of its generating function.

In the following, we show that this new concept is invariant under invertible affine transformations, in the manner that the isotopic MQQs derived by employing the row, column and symbol permutations determined by invertible affine transformations are still of the same strict type.

Row and column permutation as linear transformations. Let us consider MQQ $(\mathbb{Z}_2^d, *_e)$ as defined in Definition 3.7. Note that $(\mathbb{Z}_2^d, *_e)$ has the same quadratic parameter A as $(\mathbb{Z}_2^d, *)$ does. So it is of the same strict type. Recall the fact that MQQ $(\mathbb{Z}_2^d, *)$ is isotopic to $(\mathbb{Z}_2^d, *_e)$ and the isotope is defined by the triplet of permutation $(\mathrm{B}_1, \mathrm{B}_2, \mathrm{I}_d)$, respectively. This implies that the strict type is invariant to the row and column permutations as invertible linear transformations.

Output symbol permutation as linear transformation. Let us consider MQQ $(\mathbb{Z}_2^d, *_i)$, which is defined in Definition 3.9 and derived by applying a symbol permutation determined by B to $(\mathbb{Z}_2^d, *)$. Its generating function has $\mathrm{BA}(\mathrm{B} \otimes \mathrm{B})^{-1}$ as its quadratic parameter. Thus $(\mathbb{Z}_2^d, *_i)$ is of the same strict type as $(\mathbb{Z}_2^d, *)$ since

$$\mathrm{rk}(\mathrm{BA}(\mathrm{B} \otimes \mathrm{B})^{-1}) = \mathrm{rk}(\mathrm{A}),$$

which holds due to the fact that B is non-singular and so is $\mathrm{B} \otimes \mathrm{B}$.

Permutations as affine transformations. Without loss of generality, let us consider MQQ $(\mathbb{Z}_2^d, \circ)$, which is defined by (3.14) and derived by applying a permutation determined by an affine transformation as defined in (3.13) to $(\mathbb{Z}_2^d, *_e)$. Its generating function has $\mathrm{A}[\Delta_\mathrm{A}(r) \otimes \Gamma_\mathrm{A}(l)]^{-1}$ as its quadratic parameter. Therefore, $(\mathbb{Z}_2^d, \circ)$ is of the same strict type as $(\mathbb{Z}_2^d, *)$ due to the fact that

$$\mathrm{rk}\big(\mathrm{A}[\Delta_\mathrm{A}(r) \otimes \Gamma_\mathrm{A}(l)]^{-1}\big) = \mathrm{rk}(\mathrm{A}),$$

which holds since both $\Gamma_\mathrm{A}(l)$ and $\Delta_\mathrm{A}(r)$ are non-singular and so is $\Delta_\mathrm{A}(r) \otimes \Gamma_\mathrm{A}(l)$.

As a conclusion of the above discussions, we make the following observation.

Theorem 4.3. *The strict type of the MQQs as defined in Definition* 4.1 *is invariant to the row, column and symbol permutations which are determined by invertible affine transformations.*

In particular, if an MQQ $(\mathbb{Z}_2^d, *)$ *is generated by Theorem* 3.5*, then it is of strict type* $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_k$ *with* $k = d - \mathrm{rk}(\mathrm{A})$*, where* A *is the quadratic parameter in the generating function* (3.10)*.*

Example 4.4. Recall the MQQ $(\mathbb{Z}_2^3, *)$ given in Example 2.5. We obtain its isotope $(\mathbb{Z}_2^3, *_i)$, by applying the symbol permutation determined by the following matrix:

$$\mathrm{B} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Its output polynomials g_1, g_2, g_3 can be obtained by

$$(g_1, g_2, g_3)^{\mathrm{T}} = \mathrm{B} \cdot (f_1, f_2, f_3)^{\mathrm{T}}$$

as

$$\begin{aligned} g_1 = f_1 + f_2 &= x_1 + x_2 + y_1 + 1, \\ g_2 = f_2 &= x_1y_1 + x_1y_2 + x_1y_3 + x_2y_1 + x_2y_2 + x_2y_3 + x_3y_1 \\ &\quad + x_3y_2 + x_3y_3 + x_2 + x_3 + y_1 + y_2 + 1, \\ g_3 = f_3 &= x_1y_3 + x_2y_3 + x_3y_1 + x_3y_2 + x_3y_3 + x_2 + y_2 + y_3 + 1. \end{aligned}$$

By Definition 2.3, $(\mathbb{Z}_2^3, *)$ is of type $\mathrm{Quad}_3\mathrm{Lin}_0$, since f_1, f_2, f_3 are all quadratic; and $(\mathbb{Z}_2^3, *_i)$ is of type $\mathrm{Quad}_2\mathrm{Lin}_1$, since g_1 is linear while g_2, g_3 are quadratic. However, by Definition 4.1, we see that both are of strict type $\mathrm{Quad}^{\mathrm{s}}_2\mathrm{Lin}^{\mathrm{s}}_1$. In particular, the number of the linearly independent quadratic polynomials is equal to the rank of the quadratic parameter A as given in (3.11) in Example 3.6.

5 Construction of MQQs

By Theorem 3.5, those A which satisfy the sufficient condition (3.9) are desired in order to generate MQQs accordingly. Moreover, for MQQs of a specified type, those A also need to fulfill the constraint defined in Theorem 4.3.

5.1 Deterministic construction

One can construct A by the following theorem, and subsequently generate MQQs in accordance with Theorem 3.5.

Theorem 5.1. *Let* A *be as defined in* (3.7) *and correspondingly* $\Gamma_{\mathrm{A}}(x)$ *and* $\Delta_{\mathrm{A}}(y)$ *be as defined in Definition* 3.4. *For* $1 \leq i, j, k \leq d$,

(a) *both* $\Gamma_{\mathrm{A}}(x)$ *and* $\Delta_{\mathrm{A}}(y)$ *are upper triangular, if* A *has*

$$f_k^{ij} = 0 \quad \textit{for } j \leq i \textit{ or } k \leq i;$$

(a) *both* $\Gamma_{\mathrm{A}}(x)$ *and* $\Delta_{\mathrm{A}}(y)$ *are lower triangular, if* A *has*

$$f_k^{ij} = 0 \quad \textit{for } j \geq i \textit{ or } k \geq i;$$

(a) $\Gamma_{\mathrm{A}}(x)$ *is upper triangular and* $\Delta_{\mathrm{A}}(y)$ *is lower triangular, if* A *has*

$$f_k^{ij} = 0 \quad \textit{for } j \leq i \textit{ or } k \geq i;$$

(a) $\Gamma_{\mathrm{A}}(x)$ *is lower triangular and* $\Delta_{\mathrm{A}}(y)$ *is upper triangular, if* A *has*

$$f_k^{ij} = 0 \quad \textit{for } j \geq i \textit{ or } k \leq i.$$

In all these cases, $\det(\Gamma_{\mathrm{A}}(x)) = \det(\Delta_{\mathrm{A}}(y)) = 1$.

Proof. We only prove the case (a). It is easy to verify that $\Gamma_{\mathrm{A}}(x)$ is upper triangular, since $f_k^{ij} = 0$ for $j \leq i$; $\Delta_{\mathrm{A}}(y)$ is also upper triangular, since $g_k^{ij} = f_j^{ik} = 0$ for $k \leq i$. Since the diagonal elements of both matrices are all ones, clearly we have $\det(\Gamma_{\mathrm{A}}(x)) = \det(\Delta_{\mathrm{A}}(y)) = 1$. □

Theorem 5.2. *The number of* A *by the construction in Theorem* 5.1 (a) *or* (b) *is* $2^{d(d-1)(2d-1)/6}$.

Proof. Consider the construction as described in Theorem 5.1 (a). We look at the i-th row of A. For $j \leq i$ or $k \leq i$, it is required that $f_k^{ij} = 0$. However, for $j > i$ and $k > i$, one can freely set the value of f_k^{ij} to be 0 or 1. It is easy to count that there are $2^{(d-i)^2}$ possibilities. So the number of choices of A in this case is

$$\prod_{i=1}^{d} 2^{(d-i)^2} = \prod_{t=1}^{d-1} 2^{t^2} = 2^{\sum_{t=1}^{d-1} t^2} = 2^{d(d-1)(2d-1)/6}.$$

We can prove the same for the construction described in Theorem 5.1 (b). □

Theorem 5.3. *The number of* A *by the construction described in Theorem* 5.1 (c) *or* (d) *is* $2^{d(d-1)(d-2)/6}$.

Proof. Consider the construction as described in Theorem 5.1 (c). We look at the i-th row of A. Theorem 5.1 (c) requires that $f_k^{ij} = 0$, for $j \leq i$ or $k \geq i$. For $j > i$ and $k < i$, one can set the value of f_k^{ij} to be 0 or 1 freely. It is easy to count that there are $2^{(d-i)(i-1)}$ possibilities. So the number of choices of A in this case is

$$\prod_{i=1}^{d} 2^{(d-i)(i-1)} = 2^{\sum_{i=1}^{d} (d-i)(i-1)} = 2^{d(d-1)(d-2)/6}.$$

We can prove the same for the construction stated in Theorem 5.1 (d). □

Remark 5.4. A brute forth search shows that for $d = 2$, there are 2^2 appropriate A; whilst for $d = 3$, the number of appropriate A is $2192 > 2^{11}$. Both include the degraded case where the corresponding $\Gamma_{\mathrm{A}}(x), \Delta_{\mathrm{A}}(y)$ are equal to I_d. On the other hand, it is easy to verify that the number of appropriate A constructed according to Theorem 5.1 is 3 for $d = 2$ and 65 for $d = 3$ (both include the one degraded case). We could say to some extent that those A constructed according to Theorem 5.1 are just a very small fraction of all appropriate A especially as d increases.

According to Theorem 4.3, the strict type of an MQQ depends on the quadratic parameter A of its generating function. So in order to construct MQQs of type $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_{k}$, one shall further concretize A such that $\mathrm{rk}(\mathrm{A}) = d - k$ holds.

Theorem 5.5. *Let* A *be as defined in* (3.7)*; and* $\Gamma_{\mathrm{A}}(x)$ *and* $\Delta_{\mathrm{A}}(y)$ *be correspondingly defined as in Definition* 3.4. *Let* $S_k = \{t_1, \ldots, t_{d-k}\}$*, where* $t_1 < t_2 < \cdots < t_{d-k}$*, be a set of indices of* $d - k$ *different rows of* A. *We let* $t_0 = 1$ *and* $t_{d-k+1} = d$. *One can generate the MQQs of type* $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_{k}$ *in accordance with Theorem* 3.5*, by* A *with the following specifications.*

(a) *Both* $\Gamma_{\mathrm{A}}(x)$ *and* $\Delta_{\mathrm{A}}(y)$ *are upper triangular: for the* i*-th row of* A, $1 \leq i \leq d$, *if* $i \notin S_k$, *let* $f_k^{ij} = 0$ *for* $1 \leq j,k \leq d$*; and if* $i = t_r \in S_k$, *let*

$$f_k^{ij} = 0 \quad \text{for } j \leq i \text{ or } k \leq i;$$
$$f_k^{ij} = 1 \quad \text{for at least one pair } (j,k), \text{ where } i < j < d, i < k \leq t_{r+1}.$$

(a) *Both* $\Gamma_{\mathrm{A}}(x)$ *and* $\Delta_{\mathrm{A}}(y)$ *are lower triangular: for the* i*-th row of* A, $1 \leq i \leq d$, *if* $i \notin S_k$, *let* $f_k^{ij} = 0$ *for* $1 \leq j,k \leq d$*; and if* $i = t_r \in S_k$, *let*

$$f_k^{ij} = 0 \quad \text{for } j \geq i \text{ or } k \geq i;$$
$$f_k^{ij} = 1 \quad \text{for at least one pair } (j,k), \text{ where } 1 \leq j < i, t_{r-1} \leq k < i.$$

(a) $\Gamma_{\mathrm{A}}(x)$ *is upper triangular and* $\Delta_{\mathrm{A}}(y)$ *is lower triangular: for the* i*-th row of* A, $1 \leq i \leq d$, *if* $i \notin S_k$, *let* $f_k^{ij} = 0$ *for* $1 \leq j,k \leq d$*; and if* $i = t_r \in S_k$, *let*

$$f_k^{ij} = 0 \quad \text{for } j \leq i \text{ or } k \geq i;$$
$$f_k^{ij} = 1 \quad \text{for at least one pair } (j,k), \text{ where } i < j \leq d, t_{r-1} \leq k < i.$$

(a) $\Gamma_{\mathrm{A}}(x)$ *is lower triangular and* $\Delta_{\mathrm{A}}(y)$ *is upper triangular: for the* i*-th row of* A, $1 \leq i \leq d$, *if* $i \notin S_k$, *let* $f_k^{ij} = 0$ *for* $1 \leq j,k \leq d$ *and if* $i = t_r \in S_k$, *let*

$$f_k^{ij} = 0 \quad \text{for } j \geq i \text{ or } k \leq i;$$
$$f_k^{ij} = 1 \quad \text{for at least one pair } (j,k), \text{ where } 1 \leq j < i, i < k \leq t_{r+1}.$$

Proof. We only prove the case (a). It is easy to verify that for an A as specified in (a), the correspondingly derived $\Gamma_{\mathrm{A}}(x)$ and $\Delta_{\mathrm{A}}(y)$ are upper triangular matrices and $\det(\Gamma_{\mathrm{A}}(x)) = \det(\Delta_{\mathrm{A}}(y)) = 1$. So one can generate the MQQs by A according to (3.10) in Theorem 3.5, with random choices of non-singular binary matrices $\mathrm{B}_1, \mathrm{B}_2$ and a binary vector c. Furthermore, we note that A has exactly k rows which are zero vectors and $d-k$ rows are non-zero vectors. In order to prove that the generated MQQ is of type $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_{k}$, according to Theorem 4.3, we only need to show that $\mathrm{rk}(\mathrm{A}) = d-k$. This holds due to the fact that the t_r-th row of A contains an element 1 at its $(kd - d + j)$-th position, for a (j,k) pair such that $t_r < j < d$ and $t_r < k \leq t_{r+1}$; while it is not present at the rows of indices larger than t_r. □

Remark 5.6. Note that the constructions described in Theorem 5.1 and Theorem 5.5 do not provide us with MQQs of type $\mathrm{Quad}^{\mathrm{s}}_{d}\mathrm{Lin}^{\mathrm{s}}_{0}$. MQQs of this special type

have the property that they have d quadratic polynomials which could not cancel each other and thus may serve as good candidates for MQQ based cryptosystems. However, as we show in the following subsection, MQQs of this special type can be constructed recursively.

5.2 Recursive construction

Let A_d stand for a $d \times d^2$ binary matrix, which satisfies Theorem 3.5. We have run an exhaustive search for A_d in order to generate MQQs of order 2^d, where $d = 2, 3$. For $d = 2$, A_2 must be one of the following:

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}; \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

It is easy to see that $\mathrm{rk}(\mathrm{A}_2) = 1$ always holds. So for $d = 2$, no MQQs of type $\mathrm{Quad}_2^{\mathrm{s}}\mathrm{Lin}_0^{\mathrm{s}}$ have been found. For $d = 3$, we have found 2191 appropriate A_3 for MQQs of order 2^3. In particular, 105 of them can be used to derive MQQs of type $\mathrm{Quad}_1^{\mathrm{s}}\mathrm{Lin}_2^{\mathrm{s}}$; 930 of them for MQQs of type $\mathrm{Quad}_2^{\mathrm{s}}\mathrm{Lin}_1^{\mathrm{s}}$; and 1156 of them for MQQs of type $\mathrm{Quad}_3^{\mathrm{s}}\mathrm{Lin}_0^{\mathrm{s}}$. Note that the complexity of an exhaustive search for A, is about 2^{d^3} in order to go through all the possibilities. For instance, it is about 2^{64} for $d = 4$; and 2^{125} for $d = 5$. Clearly a brute forth search soon becomes infeasible as d increases.

However, one can generate MQQs of order 2^d, especially those of type $\mathrm{Quad}_d^{\mathrm{s}}\mathrm{Lin}_0^{\mathrm{s}}$, where $d \geq 4$, from MQQs of smaller orders. Some instances are given in the following theorems. Their proofs follow directly from the calculation of the desirable determinants [12].

Theorem 5.7. *Let* $\mathrm{A}_d = (\mathrm{vec}(\mathrm{F}_1), \mathrm{vec}(\mathrm{F}_2), \ldots, \mathrm{vec}(\mathrm{F}_d))^{\mathrm{T}}$ *be a* $d \times d^2$ *matrix as defined in* (3.7)*, which satisfies Theorem* 3.5 *for an MQQ of order* 2^d*. From* A_d*, one can construct* A_{d+1} *which satisfies Theorem* 3.5 *for an MQQ of order* 2^{d+1}*, to be the following* $(d+1) \times (d+1)^2$ *matrix*

$$\mathrm{A}_{d+1} = (\mathrm{vec}(\mathrm{P}_1), \mathrm{vec}(\mathrm{P}_2), \ldots, \mathrm{vec}(\mathrm{P}_d), \mathrm{vec}(\mathrm{P}_{d+1}))^{\mathrm{T}},$$

where for $1 \leq i \leq d+1$, P_i *is defined to be*

$$\mathrm{P}_i = \begin{bmatrix} \mathrm{F}_i & \mathrm{O}_{d\times 1} \\ \mathrm{O}_{1\times d} & 0 \end{bmatrix},$$

where F_{d+1} *is an arbitrary* $d \times d$ *binary matrix; and* O *is a zero-matrix of the indicated order. In particular, if* F_{d+1} *is linearly independent from* $\mathrm{F}_1, \ldots, \mathrm{F}_d$*, we have* $\mathrm{rk}(\mathrm{A}_{d+1}) = \mathrm{rk}(\mathrm{A}_d) + 1$.

Proof. Corresponding to A_i, we let $\Gamma_i(x), \Delta_i(y)$ stand for $\Gamma_{A_i}(x), \Delta_{A_i}(y)$. Given that A_d satisfies Theorem 3.5, we have $\det(\Gamma_d(x)) = \det(\Delta_d(y)) = 1$.

Now let us consider $\Gamma_{d+1}(x)$ and $\Delta_{d+1}(y)$ corresponding to A_{d+1}. We have

$$\Gamma_{d+1}(x) = I_{d+1} + \begin{bmatrix} (x_1, \ldots, x_{d+1}) \cdot P_1^T \\ (x_1, \ldots, x_{d+1}) \cdot P_2^T \\ \vdots \\ (x_1, \ldots, x_{d+1}) \cdot P_{d+1}^T \end{bmatrix}.$$

It can be represented to be

$$\begin{bmatrix} I_d + \begin{bmatrix} (x_1, \ldots, x_d) \cdot F_1^T \\ (x_1, \ldots, x_d) \cdot F_2^T \\ \vdots \\ (x_1, \ldots, x_d) \cdot F_d^T \end{bmatrix} & O_{d\times 1} \\ (x_1, \ldots, x_d) \cdot F_{d+1}^T & 1 \end{bmatrix} = \begin{bmatrix} \Gamma_d(x) & O_{d\times 1} \\ (x_1, \ldots, x_d) \cdot F_{d+1}^T & 1 \end{bmatrix}.$$

Since $\det(\Gamma_d(x)) = 1$, we easily obtain $\det(\Gamma_{d+1}(x)) = 1$. Applying a similar proof to $\Delta_{d+1}(y)$, we get $\det(\Delta_{d+1}(y)) = 1$. So A_{d+1} satisfies Theorem 3.5. □

Theorem 5.8. *From one* A_d *for an MQQ of order* 2^d*, the number of appropriate* A_{d+1} *for MQQs of order* 2^{d+1} *one can obtain by Theorem* 5.7 *is* 2^{d^2}.

In particular, if $\mathrm{rk}(A_d) = d$*, i.e.,* A_d *satisfies Theorem* 3.5 *for an MQQ of strict type* $\mathrm{Quad}_d^s \mathrm{Lin}_0^s$*, then the number of appropriate* A_{d+1} *for MQQs of strict type* $\mathrm{Quad}_{d+1}^s \mathrm{Lin}_0^s$ *one can obtain by Theorem* 5.7 *is* $2^{d^2} - 2^d$.

Proof. It follows from the fact that the elements of F_{d+1} can be 0 or 1, which are in total 2^{d^2} possibilities. In addition, if $\mathrm{rk}(A_d) = d$, then $\mathrm{vec}(F_1), \ldots, \mathrm{vec}(F_d)$ are linearly independent. Thus the number of possibilities that $\mathrm{vec}(F_{d+1})$ is a linear combination of $\mathrm{vec}(F_1), \ldots, \mathrm{vec}(F_d)$ is in total 2^d. Thus the number of A_{d+1} such that $\mathrm{rk}(A_{d+1}) = d + 1$ is $2^{d^2} - 2^d$. □

Theorem 5.9. *Let* $A_{d_1} = (\mathrm{vec}(F_1), \mathrm{vec}(F_2), \ldots, \mathrm{vec}(F_{d_1}))^T$ *be a* $d_1 \times d_1^2$ *matrix, which satisfies Theorem* 3.5 *for an MQQ of order* 2^{d_1}*; and* A_{d_2} *be a* $d_2 \times d_2^2$ *matrix with* $A_{d_2} = (\mathrm{vec}(G_1), \mathrm{vec}(G_2), \ldots, \mathrm{vec}(G_{d_2}))^T$*, which satisfies Theorem* 3.5 *for an MQQ of order* 2^{d_2}.

From A_{d_1} *and* A_{d_2}*, one can construct* $\mathrm{A}_{d_1+d_2}$ *satisfying Theorem* 3.5 *for an MQQ of order* $2^{d_1+d_2}$ *to be the following* $(d_1+d_2)\times(d_1+d_2)^2$ *matrix:*

$$\mathrm{A}_{d+1} = \big(\mathrm{vec}(\mathrm{P}_1), \mathrm{vec}(\mathrm{P}_2), \ldots, \mathrm{vec}(\mathrm{P}_{d_1}), \mathrm{vec}(\mathrm{Q}_1), \mathrm{vec}(\mathrm{Q}_2), \ldots, \mathrm{vec}(\mathrm{Q}_{d_2})\big)^{\mathrm{T}},$$

where the $(d_1+d_2)\times(d_1+d_2)$ *matrices* $\mathrm{P}_i, \mathrm{Q}_j$, $1 \le i \le d_1, 1 \le j \le d_2$*, can be*

$$\mathrm{P}_i = \begin{bmatrix} \mathrm{F}_i & \mathrm{O}_{d_1\times d_2} \\ \mathrm{O}_{d_2\times d_1} & \mathrm{O}_{d_2\times d_2} \end{bmatrix} \quad \textit{and} \quad \mathrm{Q}_j = \begin{bmatrix} \mathrm{L}_j & \mathrm{O}_{d_1\times d_2} \\ \mathrm{O}_{d_2\times d_1} & \mathrm{G}_j \end{bmatrix}; \tag{5.1}$$

or

$$\mathrm{P}_i = \begin{bmatrix} \mathrm{F}_i & \mathrm{O}_{d_1\times d_2} \\ \mathrm{O}_{d_2\times d_1} & \mathrm{R}_i \end{bmatrix} \quad \textit{and} \quad \mathrm{Q}_j = \begin{bmatrix} \mathrm{O}_{d_1\times d_1} & \mathrm{O}_{d_1\times d_2} \\ \mathrm{O}_{d_2\times d_1} & \mathrm{G}_j \end{bmatrix}, \tag{5.2}$$

where L_j *is an arbitrary* $d_1\times d_1$ *binary matrix;* R_i *is an arbitrary* $d_2\times d_2$ *binary matrices; and* O *is a zero-matrix of the indicated order.*

In particular, we have

$$\mathrm{rk}(\mathrm{A}_{d_1+d_2}) \ge \mathrm{rk}(\mathrm{A}_{d_1}) + \mathrm{rk}(\mathrm{A}_{d_2}).$$

Specifically, if $\mathrm{rk}(\mathrm{A}_{d_1}) = d_1$ *and* $\mathrm{rk}(\mathrm{A}_{d_2}) = d_2$*, then* $\mathrm{rk}(\mathrm{A}_{d_1+d_2}) = d_1+d_2$.

Proof. Corresponding to A_i, we let $\Gamma_i(x), \Delta_i(y)$ stand for $\Gamma_{\mathrm{A}_i}(x), \Delta_{\mathrm{A}_i}(y)$. Given that both A_{d_1} and A_{d_2} satisfy Theorem 3.5, we have

$$\det(\Gamma_{d_1}(x)) = \det(\Delta_{d_1}(y)) = 1, \quad \det(\Gamma_{d_2}(x)) = \det(\Delta_{d_2}(y)) = 1. \tag{5.3}$$

Now let us consider $\Gamma_{d_1+d_2}(x)$ and $\Delta_{d_1+d_2}(y)$ corresponding to $\mathrm{A}_{d_1+d_2}$ with $\mathrm{P}_i, \mathrm{Q}_j$ as specified in (5.1). We have

$$\Gamma_{d_1+d_2}(x) = \mathrm{I}_{d_1+d_2} + \begin{bmatrix} (x_1,\ldots,x_{d_1+d_2})\cdot \mathrm{P}_1^{\mathrm{T}} \\ \vdots \\ (x_1,\ldots,x_{d_1+d_2})\cdot \mathrm{P}_{d_1}^{\mathrm{T}} \\ (x_1,\ldots,x_{d_1+d_2})\cdot \mathrm{Q}_1^{\mathrm{T}} \\ \vdots \\ (x_1,\ldots,x_{d_1+d_2})\cdot \mathrm{Q}_{d_2}^{\mathrm{T}} \end{bmatrix}.$$

It can be represented to be

$$\begin{bmatrix} \mathrm{I}_{d_1} + \begin{bmatrix} (x_1,\ldots,x_{d_1})\cdot \mathrm{F}_1^{\mathrm{T}} \\ (x_1,\ldots,x_{d_1})\cdot \mathrm{F}_2^{\mathrm{T}} \\ \vdots \\ (x_1,\ldots,x_{d_1})\cdot \mathrm{F}_d^{\mathrm{T}} \end{bmatrix} & \mathrm{O}_{d_1\times d_2} \\ \begin{bmatrix} (x_1,\ldots,x_{d_1})\cdot \mathrm{L}_1^{\mathrm{T}} \\ (x_1,\ldots,x_{d_1})\cdot \mathrm{L}_2^{\mathrm{T}} \\ \vdots \\ (x_1,\ldots,x_{d_1})\cdot \mathrm{L}_{d_2}^{\mathrm{T}} \end{bmatrix} & \mathrm{I}_{d_2} + \begin{bmatrix} (x_{d_1+1},\ldots,x_{d_1+d_2})\cdot \mathrm{G}_1^{\mathrm{T}} \\ (x_{d_1+1},\ldots,x_{d_1+d_2})\cdot \mathrm{G}_2^{\mathrm{T}} \\ \vdots \\ (x_{d_1+1},\ldots,x_{d_1+d_2})\cdot \mathrm{G}_{d_2}^{\mathrm{T}} \end{bmatrix} \end{bmatrix},$$

whose diagonal elements are in fact $\Gamma_{d_1}(x)$ and $\Gamma_{d_2}(x)$. We recall from (5.3) that $\det(\Gamma_{d_1}(x)) = \det(\Gamma_{d_2}(x)) = 1$ and thereby obtain $\det(\Gamma_{d_1+d_2}(x)) = 1$. Applying a similar proof to $\Delta_{d_1+d_2}(y)$, we get $\det(\Delta_{d_1+d_2}(y)) = 1$ as well. So $\mathrm{A}_{d_1+d_2}$ with $\mathrm{P}_i, \mathrm{Q}_j$ as specified in (5.1) satisfies Theorem 3.5 for an MQQ of order $2^{d_1+d_2}$. The same proof applies to $\mathrm{A}_{d_1+d_2}$ with $\mathrm{P}_i, \mathrm{Q}_j$ as specified in (5.2). □

Theorem 5.10. *From a pair of* A_{d_1} *and* A_{d_2} *for MQQs of order* 2^{d_1} *and* 2^{d_2}*, respectively, the number of appropriate* $\mathrm{A}_{d_1+d_2}$ *for MQQs of order* $2^{d_1+d_2}$ *one can obtain by Theorem* 5.9 *is* $2^{d_1^2\cdot d_2} + 2^{d_1\cdot d_2^2} - 1$.

Proof. First we count the choices of L_j, $1 \le j \le d_2$, as $d_1 \times d_1$ binary matrices, with elements being 0 or 1. It is in total $2^{d_1^2\cdot d_2}$. In addition, we count the choices of R_i, $1 \le i \le d_1$, as $d_2 \times d_2$ binary matrices, with elements being 0 or 1. It is in total $2^{d_1\cdot d_2^2}$. Besides, we note that there is one $\mathrm{A}_{d_1+d_2}$ in common when both L_j and R_i are zero matrices. □

6 Bounds on the number of MQQs

In this section, we give some lower bounds on the number of MQQs of order 2^d, and on the number of MQQs of different sub-types as well.

6.1 Bounds on the number of MQQs of order 2^d

To provide a lower bound on the number of MQQs of order 2^d, we first count the number of appropriate A, which fulfill Theorem 3.5 and serve as the quadratic

d	2	3	4	5	6	7	8
MQQs	2^8	2^{28}	2^{52}	2^{87}	2^{135}	2^{198}	2^{278}
d	9	10	11	12	13	14	15
MQQs	2^{377}	2^{497}	2^{640}	2^{808}	2^{1003}	2^{1227}	2^{1482}

Table 3. A lower bound on the number of MQQs of order 2^d.

parameter in the generating function; then we take into account the choices of the linear parameters B_1, B_2 and constant term c by applying Lemma 3.13.

For instance, applying Theorem 5.2 gives us the number of those A constructed by Theorem 5.1 (a) and (b). (It is much greater than the one by construction described in Theorem 5.1 (c) and (d), which is given in Theorem 5.3.) We easily derive the following bound.

Theorem 6.1. *The number of the MQQs of order 2^d is greater than*

$$2 \cdot \left[2^{d(d-1)(2d-1)/6} - 1\right] \cdot \prod_{t=0}^{d-1} (2^d - 2^t)^2 \cdot 2^d > 2^{d(d+5)(2d-1)/6}.$$

Another lower bound can be given by considering A constructed recursively according to Theorem 5.7. Based on the initial result of an exhaustive search, where 2191 A have been found for MQQs of order 2^3, we derive the following lower bound on the number of MQQs of order 2^d, for $d \geq 3$.

Theorem 6.2. *The number of the MQQs of order 2^d is greater than*

$$2191 \cdot \prod_{i=3}^{d-1} 2^{i^2} \cdot \prod_{t=0}^{d-1} (2^d - 2^t)^2 \cdot 2^d.$$

One can refer to Table 3 for $d \leq 15$. It is easy to verify that this bound is slightly better than the one in Theorem 6.1. The difference is caused by the different constructions of A for the calculations, where in Theorem 6.2, A is constructed recursively; whilst in Theorem 6.1 only those A resulting in triangular $\Gamma_A(x)$ and $\Delta_A(y)$ are considered in the calculation.

6.2 Bound on the number of MQQs of the strictly defined types

We give a lower bound on the number of MQQs of type $\mathrm{Quad}^s_{d-k}\mathrm{Lin}^s_k$, $1 \leq k < d$, in the following theorem.

Theorem 6.3. *The number of MQQs of type* $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_{k}$ *is greater than*

$$2 \cdot N_k \cdot \prod_{t=0}^{d-1} (2^d - 2^t)^2 \cdot 2^d,$$

where

$$N_k = \sum_{S_k} \prod_{r=1}^{d-k} \left[2^{(d-t_r)^2} - 2^{(d-t_r)(d-t_r-1)}\right],$$

$S_k = \{t_1, \ldots, t_{d-k}\}$ *is a subset of* $\{1, 2, \ldots, d\}$ *consisting of* $d-k$ *different elements.*

Proof. Consider the MQQs of strict type $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_{k}$, where $1 \le k < d$, generated by appropriate A satisfying Theorem 3.5. It is easy to verify that the MQQs generated by A under the following specification are of strict type $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_{k}$, i.e., $\mathrm{rk}(\mathrm{A}) = d-k$. The following construction is an instance of Theorem 5.5 (a), where the correspondingly derived $\Gamma_{\mathrm{A}}(x)$ and $\Delta_{\mathrm{A}}(y)$ are both upper triangular.

Let A be as described in (3.7), and $S_k = \{t_1, \ldots, t_{d-k}\}$, where t_r, $1 \le r \le d-k$, are indices of $d-k$ rows of A. For $1 \le i \le d$, if $i \notin S_k$, we set the elements of the i-th row of A to be zeros; otherwise, if $i = t_r$, we set $f_h^{ij} = 0$ for either $j \le i$ or $h \le i$; and $f_{i+1}^{ij} = 1$ for at least one choice of j, where $t_r < j \le d$. It is easy to count that, for row $i = t_r$, there are $(2^{(d-t_r)} - 1) \cdot 2^{(d-t_r)(d-t_r-1)}$ possibilities. Therefore, for chosen S_k, at least $\prod_{r=1}^{d-k}(2^{(d-t_r)^2} - 2^{(d-t_r)(d-t_r-1)})$ suitable A can be constructed. By going through all possible choices of S_k, we obtain N_k suitable A, where

$$N_k = \sum_{S_k} \prod_{r=1}^{d-k} \left(2^{(d-t_r)^2} - 2^{(d-t_r)(d-t_r-1)}\right).$$

By a similar construction, we can prove that there are at least the same number of appropriate A such that the corresponding $\Gamma_{\mathrm{A}}(x)$ and $\Delta_{\mathrm{A}}(y)$ are both lower triangular and the derived MQQs are of strict type $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_{k}$. Therefore, there are at least $2 \cdot N_k$ suitable A from which the derived MQQs are of type $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_{k}$.

In addition, by Lemma 3.13, for each appropriate A, there are $\prod_{t=0}^{d-1}(2^d - 2^t)^2 \cdot 2^d$ choices of $\mathrm{B}_1, \mathrm{B}_2$ and c. As a result, at least $2 \cdot N_k \cdot \prod_{t=0}^{d-1}(2^d - 2^t)^2 \cdot 2^d$ MQQs of type $\mathrm{Quad}^{\mathrm{s}}_{d-k}\mathrm{Lin}^{\mathrm{s}}_{k}$ can be generated accordingly by Theorem 3.5. □

As a straightforward consequence, we have the following lower bound on the number of MQQs of type $\mathrm{Quad}^{\mathrm{s}}_{d-1}\mathrm{Lin}^{\mathrm{s}}_{1}$.

Corollary 6.4. *By choosing appropriate* A*, non-singular binary matrices* B_1, B_2 *and a binary vector* c*, one can construct more than*

$$2 \cdot \prod_{i=1}^{d-1} [2^{(d-i)^2} - 2^{(d-i)(d-i-1)}] \cdot \prod_{t=0}^{d-1} (2^d - 2^t)^2 \cdot 2^d$$

MQQs of type $\mathrm{Quad}^{\mathrm{s}}_{d-1}\mathrm{Lin}^{\mathrm{s}}_1$.

6.3 Bound on the number of MQQs of type $\mathbf{Quad}^{\mathbf{s}}_{\boldsymbol{d}}\mathbf{Lin}^{\mathbf{s}}_{\mathbf{0}}$

Based on the initial result on the number of A for $d = 3$ by an exhaustive search, where 1156 A have been found for MQQs of type $\mathrm{Quad}^{\mathrm{s}}_3\mathrm{Lin}^{\mathrm{s}}_0$, we apply Theorem 5.7 to construct appropriate A for a greater d with $\mathrm{rk}(\mathrm{A}) = d$. Counting the number of appropriate A obtained for a specified d, and applying Lemma 3.13, we derive a lower bound on the number of MQQs of type $\mathrm{Quad}^{\mathrm{s}}_d\mathrm{Lin}^{\mathrm{s}}_0$ as follows.

Theorem 6.5. *By choosing appropriate* A*, non-singular binary matrices* B_1, B_2 *and a binary vector* c*, one can construct at least*

$$1156 \cdot \prod_{i=3}^{d-1} (2^{i^2} - 2^i) \cdot \prod_{t=0}^{d-1} (2^d - 2^t)^2 \cdot 2^d$$

MQQs of type $\mathrm{Quad}^{\mathrm{s}}_d\mathrm{Lin}^{\mathrm{s}}_0$*, where* $d \geq 3$.

One can refer to Table 4 for the lower bound on the number of MQQs of type $\mathrm{Quad}^{\mathrm{s}}_d\mathrm{Lin}^{\mathrm{s}}_0$, for $d \leq 15$. Comparing to Table 3 for the lower bound on the number of MQQs of order 2^d, we see that except for $d = 2$, the MQQs of type $\mathrm{Quad}^{\mathrm{s}}_d\mathrm{Lin}^{\mathrm{s}}_0$ seem to cover half of the MQQs of the same order. This is because the A used in the calculation of both tables are based on the recursive construction by Theorem 5.7. At the initial state $d = 3$, about 52.76% (by $1156/2191$) of appropriate A_3 are for MQQs of type $\mathrm{Quad}^{\mathrm{s}}_3\mathrm{Lin}^{\mathrm{s}}_0$; at each subsequent state $d+1$, $(2^{d^2} - 2^d)/2^{d^2}$ of the candidates A_{d+1} constructed from those A_d (appropriate for MQQs of type $\mathrm{Quad}^{\mathrm{s}}_d\mathrm{Lin}^{\mathrm{s}}_0$) are appropriate for MQQs of type $\mathrm{Quad}^{\mathrm{s}}_{d+1}\mathrm{Lin}^{\mathrm{s}}_0$. So under this construction, about $52.76 \cdot \prod_{i=3}^{d-1}(1 - 1/2^{d^2-d})$ percent of the correspondingly derived MQQs are of type $\mathrm{Quad}^{\mathrm{s}}_d\mathrm{Lin}^{\mathrm{s}}_0$ at $d \geq 4$. However, it is not clear whether this applies to the general case. In fact, the probability distribution of an MQQ being of different sub-types still remains an open problem.

d	2	3	4	5	6	7	8
MQQs	0	2^{27}	2^{51}	2^{86}	2^{134}	2^{197}	2^{277}
d	9	10	11	12	13	14	15
MQQs	2^{376}	2^{496}	2^{639}	2^{807}	2^{1002}	2^{1226}	2^{1481}

Table 4. A lower bound on the number of MQQs of type $\mathrm{Quad}_d^s\mathrm{Lin}_0^s$.

7 Discussion

In algebra, it is well known that a real matrix has determinant 0 if and only if the rows (also the columns) of the matrix are linearly dependent. However, this does not apply to the matrices of Boolean polynomials. As an example, we consider $\Gamma_A(x)$ and $\Delta_A(y)$, as defined in Definition 3.4 such that $\det(\Gamma_A(x)) = \det(\Delta_A(y)) = 1$. Although we prove in Theorem 7.1 that $\det(I_d + \Gamma_A(x)) = \det(I_d + \Delta_A(y)) = 0$ always holds, the rows (and the columns) of $I_d + \Gamma_A(x)$, $I_d + \Delta_A(y)$ still can be linearly independent in the manner that no linear combinations of them over GF(2) will result in a zero vector, as shown in Example 7.2.

Theorem 7.1. *Both* $\Gamma_A(x)$ *and* $\Delta_A(y)$*, as defined in Definition* 3.4 *such that* $\det(\Gamma_A(x)) = \det(\Delta_A(y)) = 1$*, have eigenvalue* $\lambda = 1$.

Proof. Let $\Gamma_A(x)$, $\Delta_A(y)$ be as defined in Definition 3.4 such that $\det(\Gamma_A(x)) = \det(\Delta_A(y)) = 1$, where A is in the form of (3.7). Assume that $\lambda = 1$ is not one of the eigenvalues of $\Gamma_A(x)$. That is, $\det(I_d + \Gamma_A(x))$ is not always 0 for different realizations of $\Gamma_A(x)$. Suppose there exists $u = (u_1, u_2, \ldots, u_d)$ such that $\det(I_d + \Gamma_A(u)) = 1$. Define

$$H_i = \begin{bmatrix} f_i^{11} & f_i^{12} & \cdots & f_i^{1d} \\ f_i^{21} & f_i^{22} & \cdots & f_i^{2d} \\ \vdots & \vdots & \vdots & \vdots \\ f_i^{d1} & f_i^{d2} & \cdots & f_i^{dd} \end{bmatrix} \overset{(a)}{=} \begin{bmatrix} g_1^{1i} & g_2^{1i} & \cdots & g_d^{1i} \\ g_1^{2i} & g_2^{2i} & \cdots & g_d^{2i} \\ \vdots & \vdots & \vdots & \vdots \\ g_1^{di} & g_2^{di} & \cdots & g_d^{di} \end{bmatrix},$$

where (a) is due to (3.4). Easy calculation gives us

$$I_d + \Gamma_A(u) = \sum_{i=1}^{d} u_i \cdot H_i.$$

Since $\det(I_d + \Gamma_A(u)) = 1$, we have $\det(\sum_{i=1}^{d} u_i H_i) = 1$. Clearly u is not an

all-zero vector and the binary matrix $\sum_{i=1}^{d} u_i \mathrm{H}_i$ is non-singular. Let e_i be the unit vector, which has 1 at its i-th position and 0 at others. Then the following matrix equation with respect to $y = (y_1, y_2, \ldots, y_d)$ always has a solution:

$$\sum_{i=1}^{d} u_i \cdot \mathrm{H}_i \cdot y^{\mathrm{T}} = \sum_{i=1}^{d} u_i \cdot \mathrm{e}_i^{\mathrm{T}}, \quad \text{i.e.,} \quad \sum_{i=1}^{d} u_i \cdot (\mathrm{e}_i^{\mathrm{T}} + \mathrm{H}_i \cdot y^{\mathrm{T}}) = 0.$$

Let $v = (v_1, v_2, \ldots, v_d)$ be the solution to the above matrix equation. We denote by $\Delta_{\mathrm{A}}(v)$ the realization of $\Delta_{\mathrm{A}}(y)$ at v. We notice that $\mathrm{e}_i^{\mathrm{T}} + \mathrm{H}_i \cdot y^{\mathrm{T}}$ is in fact the i-th column of matrix $\Delta_{\mathrm{A}}(y)$. Recall that u is not an all-zero vector. The above equation implies that the column vectors of the binary matrix $\Delta_{\mathrm{A}}(v)$ are linearly dependent, which leads to $\det(\Delta_{\mathrm{A}}(v)) = 0$. This contradicts the fact that $\det(\Delta_{\mathrm{A}}(y)) = 1$ for any value of y. We apply a similar proof to $\Gamma_{\mathrm{A}}(x)$ and so complete the proof. □

Example 7.2. Let A be the 3×9 matrix

$$\mathrm{A} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Correspondingly, we have $\Gamma_{\mathrm{A}}(x)$ and $\Delta_{\mathrm{A}}(y)$ as follows:

$$\Gamma_{\mathrm{A}}(x) = \mathrm{I}_3 + \begin{bmatrix} x_3 & x_3 & x_2 + x_3 \\ x_3 & x_1 & x_1 + x_2 \\ x_1 + x_2 & x_1 + x_3 & x_2 + x_3 \end{bmatrix},$$

$$\Delta_{\mathrm{A}}(y) = \mathrm{I}_3 + \begin{bmatrix} 0 & y_3 & y_1 + y_2 + y_3 \\ y_2 + y_3 & 0 & y_1 \\ y_1 + y_2 & y_1 + y_3 & y_2 + y_3 \end{bmatrix},$$

where I_3 is the identity matrix of order 3.

It is easy to verify that indeed $\det(\Gamma_{\mathrm{A}}(x)) = \det(\Delta_{\mathrm{A}}(y)) = 1$ and $\det(\mathrm{I}_3 + \Gamma_{\mathrm{A}}(x)) = \det(\mathrm{I}_3 + \Delta_{\mathrm{A}}(y)) = 0$. However, the rows and the columns of either $\mathrm{I}_3 + \Gamma_{\mathrm{A}}(x)$ or $\mathrm{I}_3 + \Delta_{\mathrm{A}}(y)$ are linear independent in the manner that no linear combinations of them over GF(2) will result in a zero vector.

8 Conclusions

In this paper we studied a special class of MQQs which was recently introduced in [6, Theorem 2]. Based on a few observations, we obtained a standard form of the

MQQ generating function, which gives us insights into how to construct MQQs of higher orders, yield lower bounds on the number of MQQs, and eventually solve several open research problems about them.

Besides, we reviewed the concept of MQQs of type $\mathrm{Quad}_{d-k}\mathrm{Lin}_k$, $0 \leq k < d$. We noticed that it does not reveal the true complexity of the MQQs. So we refined it into MQQs of a strict type, by which a new classification of the MQQs is defined. The new concept has the advantage of being invariant under invertible affine transformations over the set of the rows, columns and symbols of the multiplication table of an MQQ. It therefore better characterizes the complexity of the underneath multivariate quadratic system.

Last, but not least, although in this paper our analysis are conducted mainly over the binary field GF(2), the newly introduced definitions and results can be easily extended to the field GF(p), where p is a prime number or a prime power.

Bibliography

[1] R. Ahlawat, K. Gupta and S. K. Pal, Fast generation of multivariate quadratic quasigroups for cryptographic applications, in: *Proceeding of Mathematics in Defence* (2009).

[2] G. Carter, E. Dawson, and L. Nielsen, DESV: A Latin square variation of DES, in: *Proc. Workshop of Selected Areas in Cryptography*, Ottawa (1995).

[3] J. Cooper, D. Donovan and J. Seberry, Secret sharing schemes arising from Latin squares, *Bull. Inst. Combin. Appl.* **4** (1994), 33–43.

[4] N. Courtois, L. Goubin, W. Meier and J.-D. Tacier, Solving underdefined dystems of multivariate quadratic equations, in: *Proceedings of Public Key Cryptography*, Lecture Notes in Comput. Sci. 2274, Springer (2002), 211–227.

[5] M. R. Garey and D. S. Johnson, *Computers and Intractability. A Guide to the Theory of NP-Completeness*, W. H. Freeman and Company, New York, 1979.

[6] D. Gligoroski, S. Markovski and S. J. Knapskog, Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups, in: *Proceedings of the American Conference on Applied Mathematics* (MATH'08), WSEAS Press (2008), 44–49; extended version: Public key block cipher based on multivariate quadratic quasigroups, preprint (2008), `http://eprint.iacr.org/2008/320`.

[7] D. Gligoroski, S. Markovski and S. J. Knapskog, The stream cipher Edon80, in: *New Stream Cipher Designs*, Lecture Notes in Comput. Sci. 4986, Springer, Berlin (2008), 152–169.

[8] D. Gligoroski, R. S. Ødegård, R. E. Jensen, L. Perret, J.-C. Faugère, S. J. Knapskog and S. Markovski, MQQ-SIG, in: *Trusted Systems*, Lecture Notes in Comput. Sci. 7222, Springer, Berlin (2012), 184–203.

[9] O. Grošek and P. Horák, On quasigroups with few associative triples, *Des. Codes Cryptogr.* **64** (2012), 221–227.

[10] A. Klimov and A. Shamir, A new class of invertible mappings, in: *4th Workshop on Cryptographic Hardware and Embedded Systems* (CHES), Springer (2002), 471–484.

[11] M. Matsumoto, M. Saito, T. Nishimura and M. Hagita, CryptMT stream cipher version 3, in: *Workshop Record of SASC 2007: The State of the Art of Stream Ciphers*, eSTREAM report 2007/028 (2007), `www.ecrypt.eu.org/stream/papers.html`.

[12] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*, Society for Industrial and Applied Mathematics (SIAM), 2001.

[13] D. V. Nguyen, S. K. Chilappagari, M. W. Marcellin and B. Vasić, LDPC codes from Latin squares free of small trapping sets, preprint (2010), `http://arxiv.org/abs/1008.4177`.

[14] R. L. Rivest, Permutation polynomials modulo 2^w, *Finite Fields Appl.* **7** (2001), 287–292.

[15] S. Samardjiska, S. Markovski and D. Gligoroski, Multivariate quasigroups defined by T-functions, in: *2nd International Conference on Symbolic Computation and Cryptography* (2010), 117–127.

[16] C. P. Schnorr and S. Vaudenay, Black box cryptanalysis of hash networks based on multipermutations, in: *Advances of Cryptology* (EUROCRYPT'94), Springer, Berlin (1995), 47–57.

[17] C. E. Shannon, Communication theory of secrecy systems, *Bell Sys. Tech. J.* **28** (1949), 657–715.

[18] L. Zhang, Q. Huang, S. Lin, K. Abdel-Ghaffar and I. F. Blake, Quasicyclic LDPC codes on Latin squares and the ranks of their parity-check matrices, in: *Inf. Theory and Appl. Workshop*, IEEE (2010), 16–22.

Received October 7, 2011; revised May 3, 2013; accepted July 21, 2013.

Author information

Yanling Chen, Department of Telematics,
Norwegian University of Science and Technology, Norway.
E-mail: `yanling@item.ntnu.no`

Danilo Gligoroski, Department of Telematics,
Norwegian University of Science and Technology, Norway.
E-mail: `danilog@item.ntnu.no`

Svein J. Knapskog, Q2S, Centre of Excellence,
Norwegian University of Science and Technology, Norway.
E-mail: `knapskog@q2s.ntnu.no`