УДК 512.643 DOI 10.17223/20710410/56/2

THE CONSTRUCTION OF CIRCULANT MATRICES RELATED TO MDS MATRICES

S. S. Malakhov, M. I. Rozhkov

HSE University, Moscow, Russia

E-mail: ssmalakhov@edu.hse.ru, mirozhkov@hse.ru

The objective of this paper is to suggest a method of the construction of circulant matrices, which are appropriate for being MDS (Maximum Distance Separable) matrices utilising in cryptography. Thus, we focus on designing so-called bi-regular circulant matrices, and furthermore, impose additional restraints on matrices in order that they have the maximal number of some element occurrences and the minimal number of distinct elements. The reason to construct bi-regular matrices is that any MDS matrix is necessarily the bi-regular one, and two additional restraints on matrix elements grant that matrix-vector multiplication for the samples constructed may be performed efficiently. The results obtained include an upper bound on the number of some element occurrences for which the circulant matrix is bi-regular. Furthermore, necessary and sufficient conditions for the circulant matrix bi-regularity are derived. On the basis of these conditions, we developed an efficient bi-regularity verification procedure. Additionally, several bi-regular circulant matrix layouts of order up to 31 with the maximal number of some element occurrences are listed. In particular, it appeared that there are no layouts of order 32 with more than 5 occurrences of any element which yield a bi-regular matrix (and hence an MDS matrix).

Keywords: *circulant matrix, MDS code, MDS matrix.*

О ПОСТРОЕНИИ ЦИРКУЛЯНТНЫХ МАТРИЦ, СВЯЗАННЫХ С MDS-МАТРИЦАМИ

С. С. Малахов, М. И. Рожков

Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия

Цель данной работы — предложить метод построения таких циркулянтных матриц, которые могут быть MDS-матрицами, используемыми в криптографии. Мы рассматриваем так называемые би-регулярные циркулянтные матрицы и, кроме того, налагаем на них дополнительные ограничения с тем, чтобы они имели максимальное число вхождений некоторого элемента и минимальное количество различных элементов. Интерес к би-регулярным матрицам обусловлен тем, что любая MDS-матрица обязательно является би-регулярной, а дополнительные ограничения на элементы матриц позволяют эффективнее реализовывать матрично-векторные операции с использованием таких матриц. Полученные результаты включают верхнюю границу числа вхождений некоторого элемента, при котором циркулянтная матрица остаётся би-регулярной, а также необходимые и достаточные условия би-регулярности циркулянтной матрицы. Кроме того, описан эффективный алгоритм проверки би-регулярности циркулянтной матрицы.

С его помощью построены шаблоны би-регулярных циркулянтных матриц порядка до 31 с максимальным числом вхождений некоторого элемента и установлено отсутствие би-регулярных циркулянтных матриц (и следовательно, MDS-матриц) порядка 32 с более чем пятью вхождениями одного элемента.

Ключевые слова: *циркулянтная матрица, МДР-код, MDS-код, MDS-матрица.*

1. Introduction

Suppose that $\boldsymbol{M}$ is a $k \times m$ matrix over a finite field $\mathbb{F}_q$. Then a set

$$\left\{(\boldsymbol{x}, \boldsymbol{x} \cdot \boldsymbol{M}) : \boldsymbol{x} \in (\mathbb{F}_q)^k\right\}$$

is a linear $[n, k, d]$ code of the length $n = k + m$ and the dimension k with the minimum Hamming distance d between any two code words. For a linear $[n, k, d]$ code the Singleton bound holds [1]:

$$d \leqslant n - k + 1 = m + 1.$$

A code with $d = m + 1$ is called the MDS code (Maximum Distance Separable code), and the corresponding matrix $\boldsymbol{M}$ is referred to as the MDS matrix.

The problem of MDS code existence relates to Segre's MDS conjecture proposed in [2]. It suggests that a set S of vectors of the vector space $(\mathbb{F}_q)^k$ such that every subset of S of size $k \leqslant q$ is a basis, comprises at most $q + 1$ elements, unless q is even and $k = 3$ or $k = q - 1$, in which case it comprises at most $q + 2$ elements. S. Ball has shown in [3] that S generates an MDS code and proved that a linear MDS code with the dimension $k \leqslant q$ has the length at most $q + k + 1 - \min\{k, \operatorname{char} \mathbb{F}_q\}$.

Furthermore, it is shown in [1, p. 321] that a linear code is MDS if and only if every square submatrix of $\boldsymbol{M}$ is non-singular. Therefore, we will define the MDS matrix as follows.

Definition 1. A matrix $\boldsymbol{M}$ is the MDS matrix if every square submatrix of $\boldsymbol{M}$ is non-singular.

MDS matrices are demanded for block cryptographic algorithms, where they are responsible for the input diffusion. An MDS matrix performs a linear transformation of an input block $\boldsymbol{x}$ of the following property: if $i, 1 \leqslant i \leqslant k$, elements of $\boldsymbol{x}$ are altered, then at least $m - i + 1$ elements of the output block $\boldsymbol{x} \cdot \boldsymbol{M}$ alter, where both the input and the output blocks can be interpreted as vectors of a k-dimensional vector space over a finite field $\mathbb{F}_q$. In this sense, MDS matrices provide perfect diffusion [4]. Several algorithms utilize MDS matrices including block ciphers Rijndael, GOST R 34.12-2015, IDEA NXT and hash functions GOST R 34.11-2012 and Whirlpool.

Although construction of MDS matrices is a computationally hard problem in general case, there are plenty of different particular techniques. One approach presumes that a specific matrix layout comprising variables is set. Then, variables are initialized with concrete values, and the resulting matrix is tested for being the MDS matrix. The approach described was proposed in [4] and performed in [5]. Not every matrix layout may produce MDS matrices, and therefore, it is of an interest to filter those layouts which never produce any. A method to filter matrix layouts is to verify their bi-regularity. The definition of the bi-regularity is given below.

Definition 2. Let $\mathscr{K}$ be a subset of a multiplicative group. The 2×2 matrix over $\mathscr{K}$ is bi-regular if at least in one row and one column there are two distinct entries. An arbitrary $k \times m$ matrix over $\mathscr{K}$ is bi-regular if every its 2×2 submatrix is bi-regular.

Remark 1. One may distinguish two particular cases, when $\mathscr{K}$ is exactly a multiplicative subgroup of a finite field, and when $\mathscr{K}$ represents a set of variables that cannot take nought values.

It is obvious that an MDS matrix is necessarily bi-regular, and so is a matrix layout that produces MDS matrices.

This paper focuses on the construction of bi-regular circulant matrix layouts which yield bi-regular matrices and hence may produce MDS matrices.

Definition 3. A circulant matrix denoted by its zeroth row $(a_0, \ldots, a_{m-1})$ is a matrix of the form

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{m-2} & a_{m-1} \\ a_1 & a_2 & \cdots & a_{m-1} & a_0 \\ \cdots & & & & \\ a_{m-2} & a_{m-1} & a_0 & \cdots & a_{m-3} \\ a_{m-1} & a_0 & \cdots & a_{m-3} & a_{m-2} \end{pmatrix}.$$

Remark 2. Speaking more generally, as rows of a matrix may be circularly shifted to the left or to the right, there exist two types of circulant matrices. Although this paper takes a left shift case as a basis for description, all the techniques presented are essentially applicable to both circulant matrix types.

Previously, circulant matrices were studied in several papers, for instance, in [6 – 9]. It was proved in [6] that circulant MDS matrices over a finite field of characteristic 2 are neither involutary nor orthogonal. However, [7] reveals that involutory circulant MDS matrices over the ring of matrices whose entries lie in characteristic 2 field do exist. The authors of [9] managed to construct circulant MDS matrices over the general linear group over the two-element field, and in [8] the authors studied circulant-like MDS matrices.

The objective of this paper is to suggest a method for the construction of bi-regular circulant matrices with the maximal number of some element occurrences and the minimal number of distinct elements. These two additional restraints on matrix elements allow performing matrix-vector multiplication more efficiently. The results obtained include the upper bound of the number of some element occurrences for which the circulant matrix bi-regularity preserves. Furthermore, necessary and sufficient conditions for the circulant matrix bi-regularity are derived. On the basis of these conditions, we developed an efficient bi-regularity verification procedure. Additionally, several bi-regular circulant matrix layouts of order up to 31 with the maximal number of some element occurrences are listed. In particular, it appeared that there are no layouts of order 32 with more than 5 occurrences of any element which yield a bi-regular matrix (and hence an MDS matrix).

This paper follows the report *On the construction of bi-regular circulant matrices, relating to MDS matrices* [10] made at the conference *Engineering Technologies and Informatics: Innovations and Applications* (En&T-2021).

The paper consists of two parts, not taking the introduction and the conclusion into account. The first part carries proofs for the upper bound of the number of arbitrary element occurrences together with the proof of necessary and sufficient conditions for the circulant matrix be-regularity. The second part contains instances of bi-regular circulant matrix layouts of an order up to 31 with maximum number of a given element occurrences.

2. Necessary and sufficient conditions for the circulant matrix bi-regularity

The following Lemma 1 provides one of the necessary conditions for the circulant matrix bi-regularity.

Lemma 1. Let $\boldsymbol{M}$ be a bi-regular circulant matrix over a subset $\mathscr{K}$ of some multiplicative group, denoted by its zeroth row $(a_0, \ldots, a_{m-1})$. Suppose that an element α is in the positions with indices $i_0, \ldots, i_{t-1}$, $t > 1$. Then the set of differences between two distinct indices

$$D_\alpha = \{(i - i') \bmod m : i \in \{i_0, \ldots, i_{t-1}\} \ni i', i \neq i'\}$$

comprises $t\,(t-1)$ elements.

Proof. Suppose that there exist indices $i_r < i_s$ and $i_u < i_v$ of the positions occupied by an element α such that $i_s - i_r = i_v - i_u$ or $i_s - i_r = m - i_v + i_u$. The following three cases are possible.

I. If $i_s - i_r = i_v - i_u$, while $i_r < i_s \leqslant i_u < i_v$, then in the zeroth row and in the row obtained from it by the $(i_u - i_r)$-position left circular shift there is an element α in the columns i_r and i_s. Hence, $\boldsymbol{M}$ is not bi-regular:

$$\begin{array}{c} \\ 0 \\ \\ i_u - i_r \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & i_r & & i_s & & i_u & & i_v & \\ \end{array} \\ \begin{pmatrix} \cdots & \alpha & \cdots & \alpha & \cdots & \alpha & \cdots & \alpha & \cdots \\ & \vdots & & & & & & & \\ \cdots & \alpha & \cdots & \alpha & \cdots & & & & \end{pmatrix} \end{array}.$$

II. If $i_s - i_r = i_v - i_u$, while $i_r < i_u < i_s < i_v$, then in the zeroth row and in the row obtained from it by the $(i_u - i_r)$-position left circular shift there is an element α in the columns i_r and i_s. Hence, $\boldsymbol{M}$ is not bi-regular:

$$\begin{array}{c} \\ 0 \\ \\ i_u - i_r \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & i_r & & i_u & & i_s & & i_v & \\ \end{array} \\ \begin{pmatrix} \cdots & \alpha & \cdots & \alpha & \cdots & \alpha & \cdots & \alpha & \cdots \\ & \vdots & & & & & & & \\ \cdots & \alpha & \cdots & & & \alpha & \cdots & & \end{pmatrix} \end{array}.$$

III. If $i_s - i_r = (i_u - i_v) \bmod m$, while $i_r \leqslant i_u < i_v \leqslant i_s$, then in the zeroth row and in the row obtained from it by the $(i_v - i_r)$-positions left circular shift there is an element α in the columns i_r and i_s. Hence, $\boldsymbol{M}$ is not bi-regular:

$$\begin{array}{c} \\ 0 \\ \\ i_v - i_r \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & i_r & & i_u & & i_v & & i_s & \\ \end{array} \\ \begin{pmatrix} \cdots & \alpha & \cdots & \alpha & \cdots & \alpha & \cdots & \alpha & \cdots \\ & \vdots & & & & & & & \\ \cdots & \alpha & \cdots & & & & & \alpha & \cdots \end{pmatrix} \end{array}.$$

Thus, all the cases possible contradict to the matrix $\boldsymbol{M}$ bi-regularity. ■

Now we derive the upper bound of the number of arbitrary element occurrences in the bi-regular circulant matrix. Note that K. Zarankiewicz in [11] addressed the problem equivalent to finding the largest positive integer $z(k, m, p, q)$ such that a binary $k \times m$ matrix containing $z(k, m, p, q)$ ones may not have a $p \times q$ submatrix consisting entirely of ones. If we now take $p = q = 2$, then Zarankiewicz's problem is to find the largest number of arbitrary element occurrences at which the matrix bi-regularity preserves. I. Reiman proved in [12] that

$$z(k, m, 2, 2) \leqslant 1/2 \left(k + \left(k^2 + 4km(m-1)\right)^{1/2}\right),$$

$$z(t^2 - t + 1, t^2 - t + 1, 2, 2) = t^3 - t^2 + t.$$

It is an immediate corollary to Lemma 1 that for a circulant matrix of order $m = t(t-1)+1$ the maximal number of element occurrences, at which the matrix still can be bi-regular, meets the upper bound proved by Reiman, i.e., $z(m, m, 2, 2) = t^3 - t^2 + t$. Besides, the next corollary shows that Reiman's inequality remains strong enough for circulant matrices.

Corollary 1. Under conditions of the Lemma 1, the following inequality holds:

$$m \leqslant mt \leqslant 1/2 \left(m + \left(m^2 + 4m^2(m-1)\right)^{1/2}\right).$$

Proof. On the one hand, Lemma 1 asserts that the set D_α of differences of two distinct indices comprises $t\,(t-1)$ elements. On the other hand, the aggregate number of differences between two distinct indices does not exceed $m-1$. Therefore,

$$t\,(t-1) \leqslant m-1,$$

and hence,

$$1 \leqslant t \leqslant 1/2 + (m - 3/4)^{1/2} \Leftrightarrow m \leqslant mt \leqslant 1/2 \left(m + \left(m^2 + 4m^2(m-1)\right)^{1/2}\right).$$

The Corollary 1 is proved. ■

Remark 3. It is noteworthy that D_α is a difference set in case $t\,(t-1) = m-1$.

The next Lemma introduces an interrelationship between numbers of different element occurrences in a bi-regular matrix.

Lemma 2. Let $\boldsymbol{M}$ be a bi-regular circulant matrix over a subset $\mathscr{K}$ of some multiplicative group denoted by its zeroth row $(a_0, \ldots, a_{m-1})$. Suppose that an element α is in the positions with the indices $i_0, \ldots, i_{t_\alpha - 1}$, $t_\alpha > 1$, and an element β is in the positions with the indices $j_0, \ldots, j_{t_\beta - 1}$, $t_\beta > 1$. Then the sets of differences between two distinct indices of α and β

$$D_\alpha = \left\{(i - i')_{\bmod m} : i \in \{i_0, \ldots, i_{t_\alpha - 1}\} \ni i', i \neq i'\right\}$$
$$D_\beta = \left\{(j - j')_{\bmod m} : j \in \{j_0, \ldots, j_{t_\beta - 1}\} \ni j', j \neq j'\right\}$$

are disjoint.

Proof. Suppose that there exist indices $i_r < i_s$ and $j_u < j_v$ of positions occupied by an element α and an element β respectively. The following three cases are possible.

I. If $i_s - i_r = j_v - j_u$, while $i_r < i_s < j_u < j_v$, then in the columns i_r and i_s there are the element α in the zeroth row and the element β in the row obtained from the zeroth one by the $(j_u - i_r)$-position left circular shift. Hence, $\boldsymbol{M}$ is not bi-regular:

$$\begin{array}{c} \\ 0 \\ \\ j_u - i_r \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & i_r & & i_s & & j_u & & j_v & \\ \end{array} \\ \begin{pmatrix} \cdots & \alpha & \cdots & \alpha & \cdots & \beta & \cdots & \beta & \cdots \\ & \vdots & & & & & & & \\ \cdots & \beta & \cdots & \beta & \cdots & & & & \end{pmatrix} \end{array}.$$

II. If $i_s - i_r = j_v - j_u$, while $i_r < j_u < i_s < j_v$, then in the columns i_r and i_s there are the element α in the zeroth row and the element β in the row obtained from the zeroth one by the $(j_u - i_r)$-positions left circular shift. Hence, $\boldsymbol{M}$ is not bi-regular:

$$\begin{array}{c} \\ 0 \\ \\ j_u - i_r \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & i_r & & j_u & & i_s & & j_v & \\ \end{array} \\ \begin{pmatrix} \cdots & \alpha & \cdots & \beta & \cdots & \alpha & \cdots & \beta & \cdots \\ & \vdots & & & & & & & \\ \cdots & \beta & \cdots & & & \beta & \cdots & & \end{pmatrix} \end{array}.$$

III. If $i_s - i_r = m - (j_v - j_u)$, while $i_r < j_u < j_v < i_s$, then in the columns i_r and i_s there are the element α in the zeroth row and the element β in the row obtained from the zeroth one by the $(j_v - i_r)$-positions left circular shift. Hence, $\boldsymbol{M}$ is not bi-regular:

$$\begin{array}{c} \\ 0 \\ \\ j_v - i_r \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & i_r & & j_u & & j_v & & i_s & \\ \end{array} \\ \begin{pmatrix} \cdots & \alpha & \cdots & \beta & \cdots & \beta & \cdots & \alpha & \cdots \\ & \vdots & & & & & & & \\ \cdots & \beta & \cdots & & & & & \beta & \cdots \end{pmatrix} \end{array}.$$

Thus, all the cases possible contradict to the matrix $\boldsymbol{M}$ bi-regularity. ■

The following Theorem provides the necessary and sufficient conditions for the circulant matrix bi-regularity.

Theorem 1. Let $\boldsymbol{M}$ be an $m \times m$ circulant matrix over a subset $\mathscr{K}$ of some multiplicative group, denoted by its zeroth row $(a_0, \ldots, a_{m-1})$. Suppose that an element α is in the positions with the indices $i_0, \ldots, i_{t_\alpha - 1}$, $t_\alpha > 1$, and an element β is in the positions with the indices $j_0, \ldots, j_{t_\beta - 1}$, $t_\beta > 1$. Let

$$D_\alpha = \left\{ (i - i') \bmod m : i \in \{i_0, \ldots, i_{t_\alpha - 1}\} \ni i', i \neq i' \right\}$$
$$D_\beta = \left\{ (j - j') \bmod m : j \in \{j_0, \ldots, j_{t_\beta - 1}\} \ni j', j \neq j' \right\}$$

be the sets of differences between two distinct indices of the positions occupied by α and β respectively. Then the matrix $\boldsymbol{M}$ is bi-regular if and only if for each such α and β:

1) the set D_α comprises $t_\alpha (t_\alpha - 1)$ elements, while D_β comprises $t_\beta (t_\beta - 1)$ elements;
2) the sets D_α and D_β are disjoint.

Proof. The necessity immediately follows from Lemmas 1 and 2.

To prove sufficiency, suppose the matrix $\boldsymbol{M}$ is not bi-regular. The following three cases are possible.

I. Consider a design where i_r and i_s, $i_r < i_s$, are the indices of the positions occupied by the element α in the zeroth row and in the row $(i_u - i_r) \bmod m$, while $i_u \neq i_r$:

$$\begin{array}{c} \\ 0 \\ \\ (i_u - i_r) \bmod m \end{array} \begin{array}{c} \begin{array}{ccccc} & i_r & & i_s & \\ \end{array} \\ \begin{pmatrix} \cdots & \alpha & \cdots & \alpha & \cdots \\ & \vdots & & & \\ \cdots & \alpha & \cdots & \alpha & \cdots \end{pmatrix} \end{array}.$$

Then in the zeroth row there is an element α in the positions i_r, i_s, i_u and $(i_u + i_s - i_r) \bmod m$. Note that

$$((i_u + i_s - i_r) \bmod m - i_u) \bmod m = i_s - i_r,$$

and hence the set D_α consists of less than $t_\alpha (t_\alpha - 1)$ elements.

Similarly, one may verify that if the matrix $\boldsymbol{M}$ is not bi-regular against the element β then the set D_β consists of less than $t_\beta (t_\beta - 1)$ elements.

II. Consider a design where i_r and i_s, $i_r < i_s$, are the indices of the positions occupied by the element α in the zeroth row and by the element β in the row $(j_u - i_r) \bmod m$,

while $j_u \neq i_r$:

$$\begin{array}{c} \\ 0 \\ (j_u - i_r)_{\bmod m} \end{array} \begin{array}{c} \begin{array}{cccc} & i_r & & i_s & \end{array} \\ \begin{pmatrix} \cdots & \alpha & \cdots & \alpha & \cdots \\ & \vdots & & & \\ \cdots & \beta & \cdots & \beta & \cdots \end{pmatrix} \end{array}.$$

Then in the zeroth row there is the element β in the positions j_u and $(j_u + i_s - i_r)_{\bmod m}$. Note that

$$((j_u + i_s - i_r)_{\bmod m} - j_u)_{\bmod m} = i_s - i_r,$$

and hence the sets D_α and D_β have a common element $i_s - i_r$.

III. Consider a design where in the zeroth row and in the row $(i_s - i_r)_{\bmod m}$ in the columns i_r and j_u, $i_r < j_u$, there are the element α and the element β respectively, while $i_s \neq i_r$:

$$\begin{array}{c} \\ 0 \\ (i_s - i_r)_{\bmod m} \end{array} \begin{array}{c} \begin{array}{cccc} & i_r & & j_u & \end{array} \\ \begin{pmatrix} \cdots & \alpha & \cdots & \beta & \cdots \\ & \vdots & & & \\ \cdots & \alpha & \cdots & \beta & \cdots \end{pmatrix} \end{array}.$$

Then in the zeroth row there is the element α in the positions i_r and i_s and the element β in the positions j_u and $((i_s - i_r)_{\bmod m} + j_u)_{\bmod m}$. Note that

$$\left(((i_s - i_r)_{\bmod m} + j_u)_{\bmod m} - j_u\right)_{\bmod m} = (i_s - i_r)_{\bmod m},$$

and hence the sets D_α and D_β have a common element $(i_s - i_r)_{\bmod m}$.

The Theorem 1 is proved. ■

Corollary 2. Note the following particular case. An $m \times m$ circulant matrix with $t_\alpha > 1$ occurrences of an element α and $m - t_\alpha$ unique entries per row is bi-regular if and only if the set D_α comprises $t_\alpha (t_\alpha - 1)$ elements.

The next Lemma states that reducing the number of some element occurrences may result in a non-linear increase in the number of another element occurrences.

Lemma 3. Let $\boldsymbol{M}$ be a bi-regular circulant matrix over a subset $\mathscr{K}$ of some multiplicative group denoted by its zeroth row $(a_0, \ldots, a_{m-1})$. Suppose that there are $t_\alpha > 1$ and $t_\beta \geqslant 1$ positions occupied by an element α and an element β respectively. Then the decrease in the number t_α of element α occurrences by $k \in \{1, \ldots, t_\alpha - 1\}$ allows increase in the number t_β of element β occurrences by at most Δ_{t_β},

$$\Delta_{t_\beta} = \left\lfloor \frac{1}{2} + \left(\frac{1}{4} + t_\alpha (t_\alpha - 1) - (t_\alpha - k)(t_\alpha - k - 1) + t_\beta (t_\beta - 1) \right)^{1/2} \right\rfloor - t_\beta.$$

Proof. Given $t_\alpha > 1$, there exist $\binom{t_\alpha}{2}$ ways to select a pair of distinct indices of the positions occupied by the element α. A decrease in the number t_α by $k \in \{1, \ldots, t_\alpha - 1\}$ releases $\binom{t_\alpha}{2} - \binom{t_\alpha - k}{2}$ differences between two distinct indices that might be distributed to elements other than α. We now estimate Δ_{t_β} by which the number t_β of element β

occurrences might be increased while preserving the matrix $\boldsymbol{M}$ bi-regularity property. To achieve this objective, the following equation should be solved in integers for Δ_{t_β}:

$$\binom{t_\beta + \Delta_{t_\beta}}{2} - \binom{t_\beta}{2} = \binom{t_\alpha}{2} - \binom{t_\alpha - k}{2}.$$

Hence,

$$\Delta_{t_\beta} = \left\lfloor \frac{1}{2} + \left(\frac{1}{4} + t_\alpha \left(t_\alpha - 1\right) - \left(t_\alpha - k\right)\left(t_\alpha - k - 1\right) + t_\beta \left(t_\beta - 1\right) \right)^{1/2} \right\rfloor - t_\beta.$$

The Lemma 3 is proved. ■

Example 1. For $t = 4$ and $m = t(t-1) + 1 = 13$ consider a vector

$$(\alpha, \alpha, \beta, \gamma, \alpha, \delta, \alpha, \epsilon, \zeta, \eta, \theta, \iota, \kappa)$$

over a subset $\mathscr{K}$ of some multiplicative group. Note that distinct characters denote different group elements, and there are 10 distinct entries. One may verify that according to Theorem 1, this vector represents a bi-regular circulant matrix. If one element α is replaced by β, then there is a space for one more occurrence of β due to the fact that $\Delta_{t_\beta} = 2$. As an instance, we can take a vector

$$(\alpha, \alpha, \beta, \gamma, \alpha, \delta, \epsilon, \beta, \zeta, \beta, \eta, \theta, \iota)\,.$$

It can be verified that the new vector also represents a bi-regular circulant matrix.

3. Bi-regular circulant matrix layouts

Theorem 1 provides an efficient method of validation whether a circulant matrix is a bi-regular one. This method may be reduced to Algorithm 1.

Algorithm 1. Matrix bi-regularity validation algorithm

Require: circulant matrix $\boldsymbol{M} = \boldsymbol{M}_{m\times m}$.
Ensure: matrix $\boldsymbol{M}$ bi-regularity validation result.
$D := \varnothing$.
Reconstruct the set $\mathscr{K}$ of the elements of $\boldsymbol{M}$.
For all $e \in \mathscr{K}$:
    Find the indices $i_0, \ldots, i_{t_e - 1}$ of the positions occupied by an element e in one row, and count the number t_e.
    If $t_e > 1$, **then** construct the set D_e:

$$D_e = \left\{ (i - i') \bmod m : i, i' \in \{i_0, \ldots, i_{t_e-1}\}, i \neq i' \right\}.$$

        If $|D_e| < t_e\,(t_e - 1)$, **then return** «$\boldsymbol{M}$ is not bi-regular»,
            else if $D \cap D_e \neq \varnothing$, **then return** «$\boldsymbol{M}$ is not bi-regular»,
                else $D := D \cup D_e$.
Return «$\boldsymbol{M}$ is bi-regular».

The computational complexity of the algorithm 1 depends on the number $|\mathscr{K}|$ of different matrix elements and the number t_e of every distinct element e occurrences.

In essence, to positively validate the circulant matrix bi-regularity, algorithm 1 observes all the ordered pairs (i, i') for each element e, and the overall number of those pairs equals

$$2 \sum_{e \in \mathcal{K}} \binom{t_e}{2} = \sum_{e \in \mathcal{K}} (t_e^2 - t_e).$$

Note that, in contrast, negative validation result is obtained immediately after processing the first inappropriate matrix element. Thus, obtaining the negative validation result does not require observation of every ordered pair (i, i') for each element e, in general case.

Example 2. Consider a circulant $m \times m$ matrix with t_α occurrences of some element α per row, where $t_\alpha(t_\alpha - 1) = m - 1$. Other elements in each row occur only once. Then to positively validate such a matrix's bi-regularity, algorithm 1 must observe $m - 1$ ordered pairs of the distinct indices of the positions occupied by α.

As far as a general algorithm of the matrix bi-regularity validation is concerned, it takes to process all

$$\binom{m}{2}^2 = \frac{m^4 - 2m^3 + m^2}{4}$$

2×2 submatrices to ensure that a circulant matrix is bi-regular.

Now, an efficient method of the bi-regularity validation makes feasible the exhaustive search of arrays of variables that define bi-regular matrix layouts. Further, those layouts may be initialized by non-zero finite field elements. Following Table 1 gives a list of all non-equivalent arrays of the length $m = t_a\,(t_a - 1) + 1$ with $t_a \in \{2, 3, 4, 5, 6\}$ entries of some variable a which define bi-regular circulant matrix layouts. Here, two arrays are said to be non-equivalent if one is not a cyclic shifted representation of the other. These arrays are denoted by vectors $(i_0, \ldots, i_{t_a - 1})$ of indices of the variable a entries with $i_0 = 0$.

Table 1

t_a	m	Arrays of variables
2	3	$(0, 1)$
3	7	$(0, 1, 3)$ $(0, 2, 3)$
4	13	$(0, 1, 3, 9)$ $(0, 1, 4, 6)$ $(0, 1, 5, 11)$ $(0, 1, 8, 10)$
5	21	$(0, 1, 4, 14, 16)$ $(0, 1, 6, 8, 18)$
6	31	$(0, 1, 3, 8, 12, 18)$ $(0, 1, 3, 10, 14, 26)$ $(0, 1, 4, 6, 13, 21)$ $(0, 1, 4, 10, 12, 17)$ $(0, 1, 6, 18, 22, 29)$ $(0, 1, 8, 11, 13, 17)$ $(0, 1, 11, 19, 26, 28)$ $(0, 1, 14, 20, 24, 29)$ $(0, 1, 15, 19, 21, 24)$ $(0, 1, 15, 20, 22, 28)$

Remark 4. There are no arrays for $t_a = 7$ and $m = 43$ that denote bi-regular matrices.

Remark 5. Since for each array from Table 1 there are t_a occurrences of variable a and $m = t_a\,(t_a - 1) + 1$, all the variables different from a must occur only once conforming to Lemmas 1 and 2.

For software or hardware implementation arrays of the length $m \in \{8, 16, 32\}$ are preferable. Table 2 comprises a list of all non-equivalent arrays of the length $m \in \{8, 16\}$ with the maximal number t_a of the entries of some variable a for which the bi-regularity preserves. As in Table 1, these arrays are denoted by vectors $(i_0, \ldots, i_{t_a-1})$ of indices of the variable a entries with $i_0 = 0$.

Table 2

t_a	m	Arrays of variables
3	8	$(0, 1, 3)$ $(0, 1, 6)$
4	16	$(0, 1, 3, 7)$ $(0, 1, 3, 12)$ $(0, 1, 4, 6)$ $(0, 1, 4, 11)$ $(0, 1, 5, 7)$ $(0, 1, 5, 14)$ $(0, 1, 6, 13)$ $(0, 1, 10, 14)$ $(0, 1, 11, 13)$ $(0, 2, 5, 12)$ $(0, 2, 6, 13)$

Remark 6. There are no arrays for $t_a = 6$ and $m = 32$ producing bi-regular matrices.

4. Conclusion

The conducted survey of the circulant matrices comprises the following results. The upper bound of the number of some element occurrences for which the bi-regularity of a circulant matrix preserves was derived. Furthermore, necessary and sufficient conditions for the circulant matrix bi-regularity were proved, which made it possible to develop the efficient procedure of bi-regularity verification. We then managed to construct several bi-regular circulant matrix layouts of order up to 31 with the maximal number of some element occurrences. Besides, it was revealed that there are no layouts of order 32 with more than 5 occurrences of any element which yield a bi-regular matrix (and hence an MDS matrix).

Acknowledgement

The authors are grateful to the anonymous reviewer for the interest in the paper and the help in its improvement.

REFERENCES

1. *MacWilliams F. J. and Sloane N. J.* The Theory of Error-Correcting Codes, vol. 16. Elsevier, 1977.
2. *Segre B.* Curve razionali normali ek-archi negli spazi finiti. Ann. Matem. Pura Appl., 1955, vol. 39, no. 1, pp. 357–379.
3. *Ball S.* On sets of vectors of a finite vector space in which every subset of basis size is a basis. J. Europ. Math. Soc., 2012, vol. 14, no. 3, pp. 733–748.
4. *Junod P. and Vaudenay S.* Perfect diffusion primitives for block ciphers. LNCS, 2004, vol. 3357, pp. 84–99.
5. *Rozhkov M. I. and Malakhov S. S.* Experimental methods for constructing MDS matrices of a special form. J. Appl. Industr. Math., 2019, vol. 13, no. 2, pp. 302–309.
6. *Gupta K. C. and Ray I. G.* On constructions of circulant MDS matrices for lightweight cryptography. LNCS, 2014, vol. 8434, pp. 564–576.

7. *Li Y. and Wang M.* On the construction of lightweight circulant involutory MDS matrices. Intern. Conf. FSE, LNCS, 2016, vol. 9783, pp. 121–139.
8. *Cauchois V. and Loidreau P.* On circulant involutory MDS matrices. Designs, Codes and Cryptography, 2019, vol. 87, pp. 249–260.
9. *Kesarwani A., Sarkar S., and Venkateswarlu A.* Exhaustive search for various types of MDS matrices. IACR Trans. Symmetric Cryptology, 2019, pp. 231–256.
10. *Malakhov S. S. and Rozhkov M. I.* On construction of bi-regular circulant matrices, relating to MDS matrices. 2021 Intern. Conf. Engineering Technologies and Computer Science (EnT), IEEE, 2021, pp. 56–58.
11. *Zarankiewicz K.* Problem P 101. Colloq. Math., 1951, vol. 2, p. 131.
12. *Reiman I.* Über ein problem von K. Zarankiewicz. Acta Mathematica Academiae Scientiarum Hungarica, 1958, vol. 9, no. 3–4, pp. 269–273.