Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 24, 2018, No. 4, 133–143
DOI: 10.7546/nntdm.2018.24.4.133-143

Canonical matrices with entries integers modulo p

Krasimir Yordzhev

Faculty of Mathematics and Natural Sciences
South-West University "Neofit Rilski"
Blagoevgrad, Bulgaria
e-mail: yordzhev@swu.bg

Received: 27 June 2018 **Accepted:** 27 October 2018

Abstract: The work considers an equivalence relation in the set of all $n \times m$ matrices with entries in the set $[p] = \{0, 1, \ldots, p-1\}$. In each element of the factor-set generated by this relation, we define the concept of canonical matrix, namely the minimal element with respect to the lexicographic order. We have found a necessary and sufficient condition for an arbitrary matrix with entries in the set $[p]$ to be canonical. For this purpose, the matrices are uniquely represented by ordered n-tuples of integers.
Keywords: Permutation matrix, Weighing matrix, Hadamard matrix, Semi-canonical matrix, Canonical matrix, Ordered n-tuples of integers.
2010 Mathematics Subject Classification: 05B20, 15B36.

1 Introduction and notation

This paper presents a generalization and an improvement of the results obtained in [7].

Let k and p be integers, $k \leq p$. By $[k, p]$ we denote the set

$$[k, p] = \{k, k+1, \ldots, p\}$$

and by $[p]$ the set

$$[p] = [0, p-1] = \{0, 1, 2, \ldots, p-1\}\,.$$

With $\mathcal{M}^p_{n\times m}$ we will denote the set of all $n \times m$ matrices with entries in the set $[p]$.

When $p = 2$, a matrix whose entries belong to the set $[2] = \{0, 1\}$ is called *binary* (or *boolean*, or *(0,1)-matrix*).

When $p = 3$, a $n \times n$ matrix H whose entries belong to the set $\{1, -1\} \equiv \{1, 2\}$ $(mod\, 3)$ is *Hadamard* if $HH^T = n\, I_n$, where H^T is the transposed matrix of H and I_n is the $n \times n$ identity matrix. It is well known that n is necessarily 1, 2, or a multiple of four [2,3].

When $p = 3$, a $n \times n$ matrix W whose entries belong to the set $\{0, 1, -1\} \equiv \{0, 1, 2\}$ $(mod\, 3)$ is *weighing matrix* of order n with weight k, if $W\, W^T = k\, I_n$. For more information on applications of weighing matrices, we refer the reader to [4]. A $n \times n$ weighing matrix W with weight k is Hadamard if $k = n$ (see [1]).

A square binary matrix is called a *permutation matrix*, if there is exactly one 1 in every row and every column. Let us denote the group of all $n \times n$ permutation matrices by $\mathcal{P}_n$. It is well known (see [5, 6]) that the multiplication of an arbitrary real or complex matrix A from the left with a permutation matrix (if the multiplication is possible) leads to permutation of the rows of the matrix A, while the multiplication of A from the right with a permutation matrix leads to permutation of the columns of A.

A *transposition* is a matrix obtained from the $n \times n$ identity matrix I_n by interchanging two rows or two columns. With $\mathcal{T}_n \subset \mathcal{P}_n$ we denote the set of all transpositions in $\mathcal{P}_n$, i.e., the set of all $n \times n$ permutation matrices, which multiplying from the left an arbitrary $n \times m$ matrix swaps the places of exactly two rows, while multiplying from the right an arbitrary $k \times n$ matrix swaps the places of exactly two columns.

Definition 1.1. *Let $A, B \in \mathcal{M}^p_{n\times m}$. We will say that the matrices A and B are* equivalent *and we will write*

$$A{\sim}B,$$

if there exist permutation matrices $X \in \mathcal{P}_n$ and $Y \in \mathcal{P}_m$, such that

$$A = XBY.$$

In other words, $A \sim B$, if A is received from B after a permutation of some of the rows and some of the columns of B. Obviously, the introduced relation is an equivalence relation.

In each element of the factor-set generated by the relation "$\sim$" described in Definition 1.1, we define the concept of canonical matrix, namely the minimal element with respect to the lexicographic order. For this purpose, the matrices are uniquely represented by ordered n-tuples of integers. The purpose of this work is to get a necessary and sufficient condition for an arbitrary matrix with entries in the set $[p]$ to be canonical. This task is solved in the particular case where $p = 2$ in [7]. The case where $p = 3$ will be useful in classification of Hadamard matrices and weighing matrices.

2 Representation of matrices from $\mathcal{M}^p_{n\times m}$ via ordered n-tuples of integers

Let $A = (a_{ij})_{n\times m} \in \mathcal{M}^p_{n\times m}$, $1 \le i \le n$, $1 \le j \le m$ and let

$$x_i = \sum_{j=1}^{m} a_{ij} p^{m-j},\ i = 1, 2, \ldots n. \tag{1}$$

Obviously

$$0 \leq x_i \leq p^m - 1 \quad \text{for every} \quad i = 1, 2, \dots n \tag{2}$$

and x_i is a natural number written in notation in the number system with the base p whose digits are consistently the entries of the i-th row of A.

With $r(A)$ we will denote the ordered n-tuple

$$r(A) = \langle x_1, x_2, \dots, x_n \rangle. \tag{3}$$

Similarly, with $c(A)$ we will denote the ordered m-tuple

$$c(A) = \langle y_1, y_2, \dots, y_m \rangle, \tag{4}$$

where

$$y_j = \sum_{i=1}^{n} a_{ij} p^{n-i}, \quad 0 \leq y_j \leq p^n - 1, \quad j = 1, 2, \dots m \tag{5}$$

and y_j is a natural number written in notation in the number system with the base p whose digits are consistently the entries of the i-th column of A.

It is easy to see that for every $A \in \mathcal{M}^p_{n\times m}$, $c(A) = r(A^T)$ and $r(A) = c(A^T)$, where A^T is the transposed matrix of A.

We consider the sets:

$$\begin{array}{rcl} \mathcal{R}^p_{n\times m} & = & [0, p^m - 1]^n \\ & = & \{\langle x_1, x_2, \dots, x_n \rangle \mid 0 \leq x_i \leq p^m - 1, \ i = 1, 2, \dots n\} \\ & = & \{r(A) \mid A \in \mathcal{M}^p_{n\times m}\} \end{array}$$

and

$$\begin{array}{rcl} \mathcal{C}^p_{n\times m} & = & [0, p^n - 1]^m \\ & = & \{\langle y_1, y_2, \dots, y_m \rangle \mid 0 \leq y_j \leq p^n - 1, \ j = 1, 2, \dots m\} \\ & = & \{c(A) \mid A \in \mathcal{M}^p_{n\times m}\} \end{array}$$

Thus, we define the following two mappings:

$$r : \mathcal{M}^p_{n\times m} \to \mathcal{R}^p_{n\times m}$$

and

$$c : \mathcal{M}^p_{n\times m} \to \mathcal{C}^p_{n\times m},$$

which are bijective and therefore

$$\mathcal{R}^p_{n\times m} \cong \mathcal{M}^p_{n\times m} \cong \mathcal{C}^p_{n\times m}.$$

We will denote the lexicographic orders in $\mathcal{R}^p_{n\times m}$ and in $\mathcal{C}^p_{n\times m}$ with "$<$".

Example 2.1. Let

$$A = \begin{pmatrix} 1 & 0 & 3 & 2 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 1 & 3 \end{pmatrix} \in \mathcal{M}^4_{3\times 4}.$$

Then

$$x_1 = 1 \cdot 4^3 + 0 \cdot 4^2 + 3 \cdot 4^1 + 2 \cdot 4^0 = 1 \cdot 64 + 0 \cdot 16 + 3 \cdot 4 + 2 \cdot 1 = 78,$$
$$x_2 = 0 \cdot 4^3 + 2 \cdot 4^2 + 1 \cdot 4^1 + 0 \cdot 4^0 = 0 \cdot 64 + 2 \cdot 16 + 1 \cdot 4 + 0 \cdot 1 = 36,$$
$$x_3 = 0 \cdot 4^3 + 1 \cdot 4^2 + 1 \cdot 4^1 + 3 \cdot 4^0 = 0 \cdot 64 + 1 \cdot 16 + 1 \cdot 4 + 3 \cdot 1 = 23,$$
$$y_1 = 1 \cdot 4^2 + 0 \cdot 4^1 + 0 \cdot 4^0 = 1 \cdot 16 + 0 \cdot 4 + 0 \cdot 1 = 16,$$
$$y_2 = 0 \cdot 4^2 + 2 \cdot 4^1 + 1 \cdot 4^0 = 0 \cdot 16 + 2 \cdot 4 + 1 \cdot 1 = 9,$$
$$y_3 = 3 \cdot 4^2 + 1 \cdot 4^1 + 1 \cdot 4^0 = 3 \cdot 16 + 1 \cdot 4 + 1 \cdot 1 = 53,$$
$$y_4 = 2 \cdot 4^2 + 0 \cdot 4^1 + 3 \cdot 4^0 = 2 \cdot 16 + 0 \cdot 4 + 3 \cdot 1 = 35,$$
$$r(A) = \langle 78, 36, 23 \rangle,$$
$$c(A) = \langle 16, 9, 53, 35 \rangle.$$

Theorem 2.1. *Let A be an arbitrary matrix from $\mathcal{M}^p_{n\times m}$. Then:*

a) If $X_1, X_2, \cdots, X_s \in \mathcal{T}_n$ are such that

$$r(X_1X_2\dots X_sA) < r(X_2X_3\dots X_sA) < \cdots < r(X_{s-1}X_sA) < r(X_sA) < r(A),$$

then

$$c(X_1X_2\dots X_sA) < c(A).$$

b) If $Y_1, Y_2, \cdots, Y_t \in \mathcal{T}_m$ are such that

$$c(AY_1Y_2\dots Y_t) < c(AY_1Y_2\dots Y_{t-1}) < \cdots < c(AY_1Y_2) < c(AY_1) < c(A),$$

then

$$r(AY_1Y_2\dots Y_t) < r(A).$$

Proof. a) Induction by s.

Let $s = 1$ and let $X \in \mathcal{T}_n$ be a transposition which multiplying an arbitrary matrix $A = (a_{ij}) \in \mathcal{M}^p_{n\times m}$ from the left swaps the places of the rows of A with numbers u and v $(1 \le u < v \le n)$, while the remaining rows stay in their places. In other words, if

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2r} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{u1} & a_{u2} & \cdots & a_{ur} & \cdots & a_{um} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{v1} & a_{v2} & \cdots & a_{vr} & \cdots & a_{vm} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nr} & \cdots & a_{nm} \end{pmatrix},$$

then

$$XA = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2r} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{v1} & a_{v2} & \cdots & a_{vr} & \cdots & a_{vm} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{u1} & a_{u2} & \cdots & a_{ur} & \cdots & a_{um} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nr} & \cdots & a_{nm} \end{pmatrix},$$

where $a_{ij} \in [p] = \{0, 1, \ldots, p-1\}$, $1 \leq i \leq n$, $1 \leq j \leq m$.

Let

$$r(A) = \langle x_1, x_2, \ldots x_{u-1}, x_u, \ldots x_{v-1}, x_v, \ldots, x_n \rangle.$$

Then,

$$r(XA) = \langle x_1, x_2, \ldots x_{u-1}, x_v, \ldots x_{v-1}, x_u, \ldots, x_n \rangle.$$

Since $r(XA) < r(A)$, then according to the properties of the lexicographic order $x_v < x_u$. Let the representation of x_u and x_v in notation in the number system with the base p (with an eventual addition of unessential zeros in the beginning if necessary) be respectively as follows:

$$x_u = a_{u1} a_{u2} \cdots a_{ur} \cdots a_{um},$$

$$x_v = a_{v1} a_{v2} \cdots a_{vr} \cdots a_{vm}.$$

Since $x_v < x_u$, then there exists an integer $r \in \{1, 2, \ldots, m\}$, such that $a_{uj} = a_{vj}$ when $j < r$, and $a_{vr} < a_{ur}$. Hence, if $c(A) = \langle y_1, y_2, \ldots, y_m \rangle$, $c(XA) = \langle z_1, z_2, \ldots, z_m \rangle$, then $y_j = z_j$ when $j < r$, while the representation of y_r and z_r in notation in the number system with the base p (with an eventual addition of unessential zeros in the beginning if necessary) is respectively as follows:

$$y_r = a_{1r} a_{2r} \cdots a_{u-1\,r} a_{ur} \cdots a_{vr} \cdots a_{nr},$$

$$z_r = a_{1r} a_{2r} \cdots a_{u-1\,r} a_{vr} \cdots a_{ur} \cdots a_{nr}.$$

Since $a_{vr} < a_{ur}$, then $z_r < y_r$, whence it follows that $c(XA) < c(A)$.

We assume that for every s-tuple of transpositions $X_1, X_2, \ldots, X_s \in \mathcal{T}_n$ and for every matrix $A \in \mathcal{M}_{n \times m}^p$ from

$$r(X_1 X_2 \ldots X_s A) < r(X_2 \cdots X_s A) < \cdots < r(X_s A) < r(A)$$

it follows that

$$c(X_1 X_2 \ldots X_s A) < c(A)$$

and let $X_{s+1} \in \mathcal{T}_n$ be such that

$$r(X_1 X_2 \ldots X_s X_{s+1} A) < r(X_2 \cdots X_{s+1} A) < \cdots < r(X_{s+1} A) < r(A).$$

According to the above proved $c(X_{s+1} A) < c(A)$.

We put

$$A_1 = X_{s+1}A.$$

According to the induction assumption from

$$r(X_1X_2 \dots X_sA_1) < r(X_2 \cdots X_sA_1) < \cdots < r(X_sA_1) < r(A_1),$$

it follows that

$$c(X_1X_2 \cdots X_sX_{s+1}A) = c(X_1X_2 \cdots X_sA_1) < c(A_1) = c(X_{s+1}A) < c(A),$$

with which we have proven a).

b) is proven similarly to a). □

In effect is also the dual to Theorem 2.1 statement, in which instead of the sign "$<$" everywhere we put the sign "$>$".

Theorem 2.2. (**Dual theorem**) *Let A be an arbitrary matrix from $\mathcal{M}^p_{n\times m}$. Then:*

a) If $X_1, X_2, \dots, X_s \in \mathcal{T}_n$ are such that

$$r(X_1X_2 \dots X_sA) > r(X_2X_3 \dots X_sA) > \dots > r(X_{s-1}X_sA) > r(X_sA) > r(A),$$

then

$$c(X_1X_2 \dots X_sA) > c(A).$$

b) If $Y_1, Y_2, \cdots, Y_t \in \mathcal{T}_m$ are such that

$$c(AY_1Y_2 \dots Y_t) > c(AY_1Y_2 \dots Y_{t-1}) > \dots > c(AY_1Y_2) > c(AY_1) > c(A),$$

then

$$r(AY_1Y_2 \dots Y_t) > r(A).$$

3 Semi-canonical and canonical $\mathcal{M}^p_{n\times m}$-matrices

Definition 3.1. Let $A \in \mathcal{M}^p_{n\times m}$, $r(A) = \langle x_1, x_2, \dots, x_n\rangle$ and $c(A) = \langle y_1, y_2, \dots, y_m\rangle$. We will call the matrix A *semi-canonical*, if

$$x_1 \le x_2 \le \cdots \le x_n$$

and

$$y_1 \le y_2 \le \cdots \le y_m.$$

Lemma 3.1. *Let $A = (a_{st})_{n\times m} \in \mathcal{M}^p_{n\times m}$ be a semi-canonical matrix. Then, there exist integers s, t, such that $1 \le s \le n$, $1 \le t \le m$ and*

$$a_{11} = a_{12} = \cdots = a_{1s} = 0, \quad 1 \le a_{1,s+1} \le a_{1,s+2} \le \cdots \le a_{1m} \le p-1, \tag{6}$$

$$a_{11} = a_{21} = \cdots = a_{t1} = 0, \quad 1 \le a_{t+1,1} \le a_{t+2,1} \le \cdots \le a_{n1} \le p-1. \tag{7}$$

Proof. Let $r(A) = \langle x_1, x_2, \ldots x_n \rangle$ and $c(A) = \langle y_1, y_2, \ldots y_m \rangle$. We assume that there exist integers p and q, such that $1 \leq p < q \leq m$, $a_{1p} \geq a_{1q}$. In this case $y_p > y_q$, which contradicts the condition for semi-canonicity of the matrix A. We have proven (6). Similarly, we prove (7) as well. □

Definition 3.2. We will call the matrix $A \in \mathcal{M}^p_{n\times m}$ *canonical matrix*, if $r(A)$ is the minimal element with respect to the lexicographic order in the set $\{r(B) \mid B \sim A\}$.

Problem 3.1. *For given m, n and p, find all canonical $\mathcal{M}^p_{n\times m}$-matrices satisfying certain conditions.*

Particular cases of Problem 3.1 are as follows:

Problem 3.2. *For given n and k, find all $n \times n$ canonical weighing matrix with weight k.*

Problem 3.3. *For given n, find all $n \times n$ canonical Hadamard matrices.*

If the matrix $A \in \mathcal{M}^p_{n\times m}$ is canonical and $r(A) = \langle x_1, x_2, \ldots, x_n \rangle$, then obviously

$$x_1 \leq x_2 \leq \ldots \leq x_n. \tag{8}$$

From Definition 3.2 it immediately follows that there exists only one canonical binary matrix in every class on the equivalence relation "$\sim$" (see Definition 1.1).

Lemma 3.2. *If the matrix $A \in \mathcal{M}^p_{n\times m}$ is a canonical matrix, then A is a semi-canonical matrix.*

Proof. Let $A \in \mathcal{M}^p_{n\times m}$ be a canonical matrix and $r(A) = \langle x_1, x_2, \ldots, x_n \rangle$. Then, from (8) it follows that $x_1 \leq x_2 \leq \cdots \leq x_n$. Let $c(A) = \langle y_1, y_2, \ldots, y_m \rangle$. We assume that there are s and t such that $s \leq t$ and $y_s > y_t$. Then, we swap the columns of numbers s and t. Thus, we obtain the matrix $A' \in \mathcal{M}^p_{n\times m}$, $A' \neq A$. Obviously $c(A') < c(A)$. From Theorem 2.1 and Theorem 2.2 it follows that $r(A') < r(A)$, which contradicts the minimality of $r(A)$. □

In the next example, we will see that the opposite statement of Lemma 3.2 is not always true.

Example 3.1. We consider the matrices:

$$A = \begin{pmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}^3_{4\times 4}$$

and

$$B = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}^3_{4\times 4}.$$

After immediate verification, we find that $A \sim B$. Furthermore, $r(A) = \langle 5, 8, 18, 27 \rangle$, $c(A) = \langle 1, 6, 45, 72 \rangle$, $r(B) = \langle 2, 15, 24, 27 \rangle$, $c(B) = \langle 1, 15, 24, 54 \rangle$. So A and B are two equivalent semi-canonical matrices, but they are not canonical. The canonical matrix in this equivalence class is the matrix

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 1 & 2 & 0 & 0 \\ 2 & 2 & 0 & 0 \end{pmatrix} \in \mathcal{M}^3_{4\times 4},$$

where $r(C) = \langle 1, 6, 45, 72 \rangle$ and $c(C) = \langle 5, 8, 18, 27 \rangle$.

From Example 3.1 it immediately follows that there may be more than one semi-canonical element in a given equivalence class.

4 Necessary and sufficient conditions for a $\mathcal{M}^p_{n\times m}$-matrix to be canonical

Let $A = (a_{ij}) \in \mathcal{M}^p_{n\times m}$, $r(A) = \langle x_1, x_2, \ldots, x_n \rangle$. We introduce the following notations:

- $\nu_i(A) = \nu(x_i) =$ the number of nonzero entries in the i-th row of A, $i = 1, 2, \ldots n$.
- $Z_i(A) = Z(x_i) = \{x_k \in r(A) |\ x_k = x_i\}$ – the set of all rows $x_k \in r(A)$, such that $x_k = x_i$. By definition $x_i \in Z(x_i)$, $i = 1, 2, \ldots n$.
- $\zeta_i(A) = \zeta(x_i) = |Z_i(A)|$, $i = 1, 2, \ldots n$.

Lemma 4.1. *Let $A = (a_{ij}) \in \mathcal{M}^p_{n\times m}$, $r(A) = \langle x_1, x_2, \ldots, x_n \rangle$ and let $x_1 \le x_2 \le \cdots \le x_n$. Then, for each $i = 2, 3, \ldots, n$, for which $x_{i-1} < x_i$, or $i = 1$ the condition*

$$Z(x_i) = \{x_i, x_{i+1}, \ldots, x_{i+\zeta(x_i)-1}\}$$

is fulfilled.

Proof. Trivial. □

The formulation of the following theorem will help us to construct a recursive algorithm for obtaining all canonical $\mathcal{M}^p_{n\times m}$-matrices.

Theorem 4.2. *Let $A = (a_{ij}) \in \mathcal{M}^p_{n\times m}$, $r(A) = \langle x_1, x_2, \ldots, x_n \rangle$, $c(A) = \langle y_1, y_2, \ldots, y_m \rangle$, $s = \nu_1(A)$, $t = \zeta_1(A)$. Then, A is canonical if and only if the following conditions are satisfied:*

1. $x_1 \le x_2 \le \cdots \le x_n \le p^m - 1$;
2. $\dfrac{p^s - 1}{p - 1} \le x_1 \le p^s - 1$;
3. *If $s > 1$, then $y_{m-s+1} \le y_{m-s+2} \le y_m$;*

4. *For each* $i = 2, 3, \ldots, n$, $\nu_1(A) \le \nu_i(A)$*;*

5. *Let* $t < n$*. Let an integer* i *exist such that* $t < i \le n$ *and* $\nu_i(A) = \nu_1(A) = s$*. Then, we successively get the matrices* A', A'' *and* A''' *in the following way:*

   (a) We get the matrix A' *by moving the rows from the set* $Z_i(A)$ *so they become first;*

   (b) If $s = m$*, then* $A'' = A'$*. Let* $s < m$, $A' = (a'_{ij})$ *and let* $\Upsilon = \{j \mid a'_{1\,j} \neq 0\} = \{u_1, u_2, \ldots u_s\}$*. Then, we get the matrix* A'' *by moving successively the* u_k*-th column* $(k = 1, 2, \ldots, s)$ *from* A' *so it becomes last in* A''*;*

   (c) We get the matrix A''' *by sorting the last* s *columns of* A'' *in ascending order.*

   Then, $r(A) \le r(A''')$*.*

6. *Let* $1 \le t < n$ *and* $0 \le s < m$*. Let the matrix* $B \in \mathcal{M}^p_{(n-t)\times(m-s)}$ *be obtained from* A *by removing the first* t *rows and the last* s *columns. Then,* B *is canonical.*

Proof. **Necessity**. Let $A = (a_{ij}) \in \mathcal{M}^p_{n\times m}$ be a canonical matrix and let $r(A) = \langle x_1, x_2, \ldots, x_n\rangle$, $c(A) = \langle y_1, y_2, \ldots, y_m\rangle$.

Condition 1 follows from the fact that every canonical matrix is semi-canonical (Lemma 3.2), so $x_1 \le x_2 \le \cdots \le x_n$ and from inequality (2).

From equation (1) and Lemma 3.1 it follows that

$$x_1 = \sum_{j=1}^{m} a_{1j} p^{m-j} = \sum_{j=m-s+1}^{m} a_{1j} p^{m-j} \ge \sum_{j=m-s+1}^{m} 1 \cdot p^{m-j} = \frac{p^s - 1}{p - 1}$$

and

$$x_1 = \sum_{j=m-s+1}^{m} a_{1j} p^{m-j} \le \sum_{j=m-s+1}^{m} (p-1) p^{m-j} = (p-1)\frac{p^s - 1}{p-1} = p^s - 1.$$

Therefore, Condition 2 is true.

Condition 3 follows from the fact that every canonical matrix is semi-canonical (Lemma 3.2).

We assume that an integer i, $2 \le i \le n$ exists, such that $\nu_i(A) < \nu_1(A) = s$ and let $\nu_i(A) = u < s$. Then, a matrix $A' = (a'_{i\,j}) \sim A$ exists such that $a'_{i\,1} = a'_{i\,2} = \cdots = a'_{i\,m-u} = 0$ and $1 \le a'_{i\,m-u+1} \le a'_{i\,m-u+2} \le \cdots \le a'_{i\,m} \le p - 1$. We move the i-th row of A' at first place and we obtain a matrix A''. Obviously $A'' \sim A$. Let $r(A'') = \langle x''_1, x''_2, \ldots, x''_n\rangle$. From the above proven Condition 2, it follows that $x_1 \ge \dfrac{p^s - 1}{p - 1} = p^{s-1} + p^{s-2} + \cdot + p^u + p^{u-1} + \cdots + p + 1 > p^u > p^u - 1 \ge x''_1$. Therefore, $x_1 > x''_1$, i.e., $r(A) > r(A'')$, which is impossible, due to the fact that A is canonical. Thus, Condition 4 is true.

Condition 5 comes directly from the fact that A is canonical and $r(A) \le r(U)$ for each matrix $U \sim A$.

Let $t = \zeta_1(A) < n$ and let $s = \nu_1(A) < m$. From the already proved Conditions 1, 2, 4 and 5 and Lemma 4.1, it follows that A is presented in the form:

$$A = \begin{pmatrix} O & N \\ B & C \end{pmatrix}, \tag{9}$$

where O is a $t \times (m-s)$ matrix, all elements of which are equal to 0, N is a $t \times s$ matrix, all elements of which are equal to each other and which are not equal to 0 and all rows of the matrix $(O\ N)_{t\times m}$ coincide with the elements of the set $Z_1(A)$, $B \in \mathcal{M}^p_{(n-t)\times(m-s)}$, $C \in \mathcal{M}^p_{(n-t)\times s}$.

Let $B' \sim B$ and let B' be a canonical $\mathcal{M}^p_{(n-t)\times(m-s)}$-matrix. Then, the following matrices $A' \in \mathcal{M}^p_{n\times m}$ and $C' \in \mathcal{M}^p_{(n-t)\times s}$ exist, such that $A' \sim A$, $C' \sim C$, $A' = \begin{pmatrix} O & N \\ B' & C' \end{pmatrix}$, and C' is obtained from C after an eventual permutation of the rows. Let $r(A') = \langle x'_1, x'_2, \dots, x'_n\rangle$. Obviously $x'_i = x_i$ for all $i = 1, 2, \dots t$. Let us assume that $B' \neq B$, i.e., $r(B') < r(B)$. Let $r(B) = \langle b_{t+1}, b_{t+2}, \dots, b_n\rangle$, $r(B') = \langle b'_{t+1}, b'_{t+2}, \dots, b'_n\rangle$, $r(C) = \langle c_{t+1}, c_{t+2}, \dots, c_n\rangle$, $r(C') = \langle c'_{t+1}, c'_{t+2}, \dots, c'_n\rangle$. From assumption it follows that there exist $i \in [t+1, n]$ such that $b'_{t+1} = b_{t+1}$, $b'_{t+2} = b_{t+2}, \dots, b'_{i-1} = b_{i-1}$ and $b'_i < b_i$, i.e., $b'_i + 1 \leq b_i$. Then, $x'_1 = x_1, x'_2 = x_2, \dots, x'_{i-1} = x_{i-1}$. Since $0 \leq c_k < p^s$ and $0 \leq c'_i < p^s$, for each $i \in [t+1, n]$, then $x'_i = b'_i p^s + c'_i \leq (b'_i + 1)p^s + c'_i = b_i p^s + p^s + c'_i + c_i - c_i \leq b_i p^s + p^s + p^s + c_i - 0 < b_i p^s + c_i$. Consequently $r(A') < r(A)$. But A is canonical, i.e., $r(A) \leq r(A')$, which is a contradiction. Therefore, $B' = B$ and B is canonical. Thus, we have proved Condition 6.

Sufficiency. Let $A \in \mathcal{M}^p_{n\times m}$ satisfy Conditions $1 \div 6$ and hence the conditions of Lemma 4.1 are fulfilled. Let $r(A) = \langle x_1, x_2, \dots, x_n\rangle$ and $c(A) = \langle y_1, y_2, \dots, y_m\rangle$.

If $t = n$, then $x_1 = x_2 = \dots = x_n$ and according to Condition 3 it is easy to see that A is a canonical $\mathcal{M}^p_{n\times m}$-matrix.

If $t < n$ and $s = m$, then according to Condition 1, Lemma 4.1 and Conditions 4 and 5 it is easy to see that A is a canonical $\mathcal{M}^p_{n\times m}$-matrix.

Let $1 \leq t < n$ and $0 \leq s < m$. Let $U \sim A$ and let U be a canonical $\mathcal{M}^p_{n\times m}$-matrix. Since the Conditions $1 \div 6$ are necessary for the canonicity of a matrix, consequently U also satisfies these conditions. According to Condition 4,

$$\nu_1(U) = \nu_1(A) = s. \tag{10}$$

Thus, the matrix U is represented in the form (9) and let

$$A = \begin{pmatrix} O & N \\ B & C \end{pmatrix} \quad \text{and} \quad U = \begin{pmatrix} O' & N' \\ B' & C' \end{pmatrix}, \tag{11}$$

Let us assume that U is obtained from A only by permutation of the columns. In this case obviously $\zeta_1(U) = \zeta_1(A) = t$, $\nu_1(U) = \nu_1(A) = s$, $O' = O$, $N' \sim N$, $B' \sim B$ and $C' \sim C$.

Permutation of columns which are different each other and which belong only to the set $Y_1 = \{y_1, y_2, \dots, y_{m-s}\}$ without permutation of different each other rows is impossible in accordance with Condition 6.

Permutation of columns, which are different from each other and which belong only to the set $Y_2 = \{y_{m-s+1}, y_{m-s+2}, \dots, y_m\}$ without permutation of mutually different rows, is impossible in accordance with Condition 3.

Therefore, there are k, l such that $1 \leq k \leq m - s < l \leq m$ and the k-th column has become the l-th, or the l-th column has become the k-th. Then, according to Condition 3 and equation (9) easily see that it is impossible if we did not change the places of some rows.

Therefore, U is obtained from A by swapping some of the rows. Without loss of generality, we can assume that U is obtained from A in the beginning by swapping some rows, then (if it is necessary) swapping some columns.

Permutation of rows that belong only to the set $X_1 = \{x_1, x_2, \ldots, x_t\} = Z_1(A)$ does not change the matrix A because $x_1 = x_2 = \ldots = x_t$.

Permutation of rows that belong only to the set $X_2 = \{x_{t+1}, x_{t+2}, \ldots, x_n\}$ is impossible in accordance with Condition 6.

Therefore, taking into account the Conditions 1 and 4 and Lemma 4.1, we conclude that we have changed the first $t = \zeta_1(A)$ rows with another equal to each rows of the set $Z_j(A)$, $t + 1 \leq j \leq n$. After that, in order to obtain a matrix of kind (9), if it is necessary, we have to change the places of some columns of the matrix A. According to Conditions 3 and 5 it follows that $r(A) \leq r(U)$. But U is canonical, i.e., $r(U) \leq l(A)$. Therefore, $U = A$, i.e., A is canonical. □

References

[1] Best, D., & Kharaghani, H. (2010) Unbiased complex hadamard matrices and bases. *Cryptography and Communications*, 2 (2), 199–209.

[2] Hedayat, A., & Wallis, W. D. (1978) Hadamard matrices and their applications. *The Annals of Statistic*, 6 (6), 1184–1238.

[3] Horadam, K. J. (2007) *Hadamard Matrices and Their Applications*. Princeton University Press, Princeton, New Jersey.

[4] Koukouvinos, C., & Seberry, J. (1997) Weighing matrices and their applications. *Journal of Statistical Planning and Inference*, 62 (1), 91–101.

[5] Sachkov, V. N., & Tarakanov, V. E. (2002) *Combinatorics of Nonnegative Matrices*. Translations of Mathematical Monographs. American Mathematical Society.

[6] Tarakanov, V. E. (1985) *Combinatorial Problems and* $(0, 1)$*-matrices*. Nauka, Moscow (in Russian).

[7] Yordzhev, K. (2017) On the cardinality of a factor set of binary matrices. *Linear Algebra and Its Applications*, 534, 122–134.