symmetry

MDPI

Article

The Canonical Forms of Permutation Matrices

Wen-Wei Li [1,2], Xin Hou [3] and Qing-Wen Wang [4,*]

1 School of Mathematical Science, University of Science and Technology of China, Hefei 230026, China
2 School of Information and Mathematics, Anhui International Studies University, Hefei 231201, China
3 College of Elementary Education, Capital Normal University, Beijing 100048, China
4 Department of Mathematics, Shanghai University, Shanghai 200444, China
* Correspondence: wqw@shu.edu.cn

Abstract: We address classification of permutation matrices, in terms of permutation similarity relations, which play an important role in investigating the reducible solutions of some symmetric matrix equations. We solve the three problems. First, what is the canonical form of a permutation similarity class? Second, how to obtain the standard form of arbitrary permutation matrix? Third, for any permutation matrix A, how to find the permutation matrix T, such that $T^{-1}AT$ is in canonical form? Besides, the decomposition theorem of permutation matrices and the factorization theorem of both permutation matrices and monomial matrices are demonstrated.

Keywords: permutation matrix; monomial matrix; permutation similarity; canonical form; cycle matrix decomposition; cycle factorization

Citation: Li, W.-W.; Hou, X.; Wang, Q.-W. The Canonical Forms of Permutation Matrices. *Symmetry* **2023**, *15*, 332. https://doi.org/10.3390/sym15020332

Academic Editor: Aviv Gibali

Received: 5 January 2023
Revised: 19 January 2023
Accepted: 22 January 2023
Published: 25 January 2023

1. Introduction

The *incidence matrix* of a projective plane of order n is a 0-1 matrix of order $n^2 + n + 1$. Two projective planes are isomorphic if the incidence matrix of one projective plane can be transformed into the incidence matrix of the other one by permutation of rows and/or columns. After sorting the rows and columns, the incidence matrix of a projective plane can be reduced to (not unique) a standard form. In the reduced form, the incidence matrix can be split into blocks. Most blocks are permutation matrices (see [1]). If we keep the position of every block of the reduced form and perform permutations of the rows and columns, every permutation matrix is transformed into another matrix that is permutationally similar to the original one.

The members in the symmetry group S_n of order n are called permutations. They are tightly connected with permutation matrices of order n. Permutation matrices are powerful tools in the representation theory of groups, discrete mathematics, applied mathematics, and some engineering technology (see [2–5]). They play an important role in the study of the reducible solutions of matrix equations (see [6]). Since the elementary row (or column) transformations are inevitable in solving matrix equations, which are equivalent to the multiplication by permutation matrices or diagonal matrices. The tricks of matrix transformations (especially the row or column permutations) are applicable.

This paper is devoted to the permutational similarity relation and to the classification of the permutation matrices. In particular, we focus on the standard structure of a general permutation matrix, on the canonical form of a permutation similarity class, and on how to generate the canonical form. Furthermore, a theorem is presented about the decomposition of a permutation matrix into a diagonal matrix and some generalized cycle matrices of type II. A factorization theorem shows that an arbitrary non-identity permutation matrix is the product of some generalized cycle matrices of type I. These contents are represented in Section 3 which is the main part of this paper.

The number of permutational similarity classes of a permutation matrices of order n is discussed in Section 4. A similar factorization for monomial matrices is discussed at the end of the paper.

2. Preliminary

Let n be a positive integer, P be a square matrix of order n. If P is a binary matrix (i.e. elements are either 0 or 1, also referred to as 0-1 matrix or (0, 1) matrix) and there is a unique "1" in every row and every column, then P is called a *permutation matrix*. If we substitute the "1"s in a permutation matrix by other non-zero elements, we obtain a *monomial matrix*, also referred to as a *generalized permutation matrix*.

As a matter of fact, there is a reason for the name "*permutation matrix*". If a matrix T of size $n \times r$ is multiplied by a permutation matrix P of order n (from the left side of T), we obtain a permutation of the rows of T. If U is a matrix of size t by n, and P acts on U on the right, we have a permutation of the columns of U. The inverse of a permutation matrix P^{-1} coincides with the transpose P^{T} while P^{-1} itself is a permutation matrix.

Let k be a positive integer greater than 1, C be an invertible (0, 1) matrix of order k, if $C^k = I_k$ (I_k is the identity matrix of order k) and $C^i \neq I_k$ for any i ($1 \leq i < k$), then C will be referred to as a *cycle matrix* of order k. A cycle matrix of order k of the form

$$\begin{bmatrix} 0 & & & & 1 \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{bmatrix}$$

is a *standard cycle matrix*. The identity matrix of order 1 represents a cycle matrix of order 1.

If C_1 is a permutation matrix of order n, and there are exactly k zero diagonal elements (here $2 \leqslant k \leqslant n$), if $C^k = I_n$ and $C^i \neq I_n$ for any i ($1 \leqslant i < k$), then C_1 is termed a *generalized cycle matrix of Type* I with cycle order k.

If C_2 is a (0, 1) matrix of order n, rank $C_2 = k$, with k non-zero entries, ($2 \leqslant k \leqslant n$), if C^k is a diagonal of rank k, and C^i is non-diagonal ($1 \leqslant i < k$), then C_2 will be called a *generalized cycle matrix of type* II with cycle order k. Obviously, a generalized cycle matrix of type II plus some suitable diagonal (0, 1) matrix gives a generalized cycle matrix of type I with the same cycle order.

Let A and B be two monomial matrices of order n, if there is a permutation matrix T such that $B = T^{-1}AT$, then A and B are *permutationally similar*. The permutation similarity relation is an equivalence relation. Hence the set of the permutation matrices (or monomial matrices) or order n may be naturally split into equivalence classes.

3. Main Results

In this section, we attend to give 3 main theorems about the canonical form, the decomposition and the factorization of a permutation matrix, respectively.

Theorem 1 solves the following three problems (which arise naturally from the definitions),

(a) What is the canonical form of a permutation similarity class?
(b) How to generate the canonical form of a given permutation matrix?
(c) If B is the canonical form of the permutation matrix A, how to find the permutation matrix T, such that $B = T^{-1}AT$?

Now we give some theorems that would solve these problems.

Theorem 1. (*Similarity Theorem*) *For any permutation matrix A of order n, there is a permutation matrix T, such that,* $T^{-1}AT = \mathrm{diag}\,\{I_t, N_{k_1}, \cdots, N_{k_r}\}$, *where*

$$N_{k_i} = \begin{bmatrix} 0 & & & & 1 \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{bmatrix}$$

is a cycle matrix of order k_i in standard form, $(i = 1, 2, \cdots, r)$, $2 \leqslant k_1 \leqslant k_2 \cdots \leqslant k_r$, $0 \leqslant r \leqslant \left\lfloor \dfrac{n}{2} \right\rfloor$, $0 \leqslant t \leqslant n$, *and* $\sum\limits_{i=1}^{r} k_i + t = n$. *$T$, t, r, k_r are determined by A.*

If A is an identity matrix, then $t = n$, $r = 0$. When A is a cycle matrix, $t = 0$, $r = 1$, $k_1 = n$. In this theorem, the quasi-diagonal matrix (or block-diagonal matrices) diag $\{I_t, N_{k_1}, \cdots, N_{k_r}\}$ will be called the *canonical form* of a permutation matrix in permutational similarity relation.

The main idea of this proof is similar to that concerning the decomposition of a root subspace into cyclic subspaces.

In a root subspace V_λ associated with a linear transformation $\mathscr{B}$ and the eigenvalue λ of a matrix B, if v is a root vector of height n belonging to $\mathscr{B}$, then the subspace spanned by $\left\{ (\mathscr{B} - \lambda I)^{n-1}v, (\mathscr{B} - \lambda I)^{n-2}v, \cdots, (\mathscr{B} - \lambda I)v, v \right\}$ is a cyclic subspace, and V_λ is the direct sum of some cyclic subspaces.

Proof. For any permutation matrix A of order n, let $\mathscr{A}$ be a linear transformation defined on the vector space $\mathbb{R}^n$ with bases

$$\mathcal{B} = \{ e_1, e_2, \cdots, e_n \}, \tag{1}$$

where

$$e_i = (\underbrace{0, \cdots, 0}_{i-1}, 1, \underbrace{0, \cdots, 0}_{n-i})^{\mathrm{T}}, \quad (i = 1, 2, \cdots, n). \tag{2}$$

Here the regular letter "T" in the upper index means transposition. Suppose A is the matrix of the transformation $\mathscr{A}$ in the basis $\mathcal{B}$, and for any vector $\alpha \in \mathbb{R}^n$ with coordinates x (in the basis $\mathcal{B}$), the coordinates of $\mathscr{A}\alpha$ is Ax, i.e., $\mathscr{A}\alpha = \mathcal{B}Ax$. Here the coordinates are written as a column vector.

It is clear that the coordinates of e_i in the basis $\mathcal{B}$ is $(\underbrace{0, \cdots, 0}_{i-1}, 1, \underbrace{0, \cdots, 0}_{n-i})^{\mathrm{T}}$. Since A is a permutation matrix, Ae_i is the i'th column of A.

We decompose $\mathbb{R}^n$ into some subspaces. In each subspace V_i, there is a basis $\left\{ e_i, Ae_i, A^2e_i, \cdots, A^{k_i-1}e_i \right\}$, where $A^{k_i}e_i = e_i$. The positive k_i is the minimal integer satisfying this condition, i.e. the dimension of the cyclic subspace. Using this basis, the matrix of the transformation $\mathscr{A}$ restricted in V_i, can be written by

$$\begin{bmatrix} 0 & & & & 1 \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{bmatrix}_{k_i \times k_i}.$$

Let us now find all these cyclic subspaces. In order to describe the procedure precisely and concisely, we will use some auxiliary variables.

Step 1: Let $S = \{1, 2, \cdots, n\}$, $\mathcal{C} = \{e_i \mid i \in S\}$, $a_{11} = \min S$, $F_1 = [a_{11}]$, $G_1 = [e_{a_{11}}]$. (Here F_1 and G_1 are sequences, or sets equipped with precedence).

For the first cyclic subspace, of course $Ae_{a_{11}} \in \mathcal{C}$. If $Ae_{a_{11}} \neq e_{a_{11}}$, assume $e_{a_{12}} = Ae_{a_{11}}$, then put a_{12} and $e_{a_{12}}$ at the end of the sequences F_1 and G_1, respectively. If $Ae_{a_{1,j}} \neq e_{a_{11}}$, assume $e_{a_{1,(j+1)}} = Ae_{a_{1,j}}$, (i.e., $A^j e_{a_{11}} = e_{a_{1,(j+1)}}$), then add $a_{1,(j+1)}$ and $e_{a_{1,(j+1)}}$ at the end of sequences F_1 and G_1, respectively ($j = 1, 2, \cdots$). Since $Ae_i \in \mathcal{C}$ ($\forall i \in S$), there is an integer h_1 such that $Ae_{a_{1,h_1}} = e_{a_{11}}$ (otherwise the sequence $e_{a_{11}}, Ae_{a_{11}}, A^2e_{a_{11}}, A^3e_{a_{11}}, \cdots$ is infinite). Suppose that h_1 is the minimal integer satisfying this condition ($1 \leqslant h_1 \leqslant n$). It is clear that $A^{h_1}e_{a_{11}} = e_{a_{11}}$, $A^{h_1}e_{a_{1j}} = e_{a_{1j}}$, ($1 \leqslant j \leqslant h_1$). It is possible that $h_1 = 1$ or $h_1 = n$. At last $|F_1| = |G_1| = h_1$. Finally, remove the elements of G_1 from $\mathcal{C}$, and the elements of F_1 from S.

The first cyclic subspace is thus spanned by the basis $G_1 = \left[e_{a_{11}}, e_{a_{12}}, \cdots, e_{a_{1h_1}}\right]$. Usually, a basis of a linear space is denoted by braces, not brackets. However, braces denote sets, and this disregards the precedence. In order to avoid ambiguities, here we use brackets, which stand for sequences, where precedence is relevant. The dimension of this subspace is $|F_1| = h_1$. The matrix of the transformation $\mathscr{A}$, restricted to this cyclic subspace, is

$$N_{h_1} = \begin{bmatrix} 0 & & & & 1 \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{bmatrix}_{h_1 \times h_1}.$$

Let us now search for the next cyclic subspace, if it exists.

Step 2: If $S \neq \varnothing$, let $a_{21} = \min S$, $F_2 = [a_{21}]$, $G_2 = [e_{a_{21}}]$. It is clear that $Ae_{a_{21}} \in \mathcal{C}$. (Otherwise we would have $Ae_{a_{21}} \in G_1$. However, since all the elements in G_1 are removed from $\mathcal{C}$, then it exists k_0, s.t. $A^{k_0}e_{a_{11}} = Ae_{a_{21}}$ with $k_0 \neq 0$, so, $A^{k_0-1}e_{a_{11}} = e_{a_{21}}$ as A is invertible, which means that $e_{a_{21}} = A^{k_0-1}e_{a_{11}}$ is in the set G_1, which is a contradiction.) If $A^{i-1}e_{a_{21}} \neq e_{a_{21}}$, suppose $A^{i-1}e_{a_{21}} = e_{a_{2i}}$ ($i = 2, 3, \cdots$), then add a_{2i} and $e_{a_{2i}}$ at the end of the sequences F_2 and G_2, respectively. There will be a h_2, such that $A^{h_2}e_{a_{21}} = e_{a_{21}}$ (let h_2 be the minimal integer satisfying this condition. It is possible that $h_2 = 1$ or $h_2 = n - h_1$). Obviously, $A^{h_2}e_{a_{2i}} = e_{a_{2i}}$, ($1 \leqslant i \leqslant h_2$). Then remove the elements of G_2 from $\mathcal{C}$, and remove the elements of F_2 from S.

Now another cyclic subspace is spanned by the basis $G_2 = \left[e_{a_{21}}, e_{a_{22}}, \cdots, e_{a_{2h_2}}\right]$. The dimension of this subspace is $|F_2| = h_2$. The matrix of the transformation $\mathscr{A}$ restricted to this cyclic subspace is N_{h_2}.

Step 3: If $S \neq \varnothing$, goto step 2 and construct $F_3, F_4, \cdots$ and $G_3, G_4, \cdots$. This leads to other cyclic subspaces, their basis, and the matrices of the transformation $\mathscr{A}$ restricted to these cyclic subspaces. The procedure stops after a finite number of steps since n is finite.

Assume that we have $F_1, F_2, \cdots, F_u$ and $G_1, G_2, \cdots, G_u$, such that $\bigcup_{i=1}^{u} F_i = \{1, 2, \cdots, n\}$, $\bigcup_{i=1}^{u} G_i = \{e_1, e_2, \cdots, e_n\}$, $F_i \cap F_j = G_i \cap G_j = \varnothing$, ($1 \leqslant i \neq j \leqslant u$).

There is a possibility that $u = 1$ (when A is a cycle matrix of order n) or n (when A is an identity matrix).

Step 4: Sort $F_1, F_2, \cdots, F_u$ by candinality, s.t. $|F'_1| \leqslant |F'_2| \leqslant \cdots \leqslant |F'_u|$. Then sort G_i correspondingly, i.e., $G'_i = \{e_x \mid x \in F'_i\}$ ($i = 1, 2, \cdots, u$).

Suppose $|F'_1| = |F'_2| = \cdots = |F'_t| = 1$. If $t = n$ then A is an identity matrix. It is possible that $t = 0$.

Let $r = u - t$. Denote the unique element in G'_i by e'_i ($i = 1, 2, \cdots, t$). Let $k_j = \left|G'_{t+j}\right|$, and denote the elements in G'_{t+j} by $e'_{j,v}$ ($j = 1, 2, \cdots, r$; $v = 1, 2, \cdots, k_j$). Then, the matrix of $\mathscr{A}$ restricted to the subspace spanned by the bases $\mathcal{D}_0 = \{e'_1, e'_2, \cdots, e'_t\}$ } is I_t since $\mathscr{A}e'_i = e'_i$ ($i = 1, 2, \cdots, t$), or $\mathscr{A}\mathcal{D}_0 = \mathcal{D}_0 I_t$; and the matrix of $\mathscr{A}$ restricted in the subspace spanned by the bases $\mathcal{D}_j = G'_{t+j} = \left\{e'_{j,1}, e'_{j,2}, \cdots, e'_{j,k_j}\right\}$ ($j = 1, 2, \cdots, r$) is

$$N_{k_j} = \begin{bmatrix} 0 & & & & 1 \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{bmatrix},$$

which is a cycle matrix of order k_j, as $\mathscr{A}e'_{j,v} = e'_{j,v+1}$, ($v = 1, 2, \cdots, k_j - 1$), and $\mathscr{A}e'_{j,k_j} = e'_{j,1}$, i.e., $\mathscr{A}\mathcal{D}_j = \mathcal{D}_j N_{k_j}$ ($j = 1, 2, \cdots, r$). So, the matrix of $\mathscr{A}$ with bases

$$\mathcal{D} = \left\{e'_1, e'_2, \cdots, e'_t;\ e'_{1,1}, e'_{1,2}, \cdots, e'_{1,k_1};\ \cdots\cdots;\ e'_{r,1}, e'_{r,2}, \cdots, e'_{r,k_r}\right\} \tag{3}$$

is

$$B = I_t \oplus N_{k_1} \oplus \cdots \oplus N_{k_r} = \mathrm{diag}\{I_t, N_{k_1}, \cdots, N_{k_r}\}.$$

Since $\mathcal{D}$ is a reordering of $\mathcal{B}$, there is a permutation matrix T, such that $\mathcal{D} = \mathcal{B}T$. Then $B = T^{-1}AT$ and Theorem 1 is proved.

Take the matrix

$$P_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

as an example, and assume it is the matrix of a transformation $\mathscr{P}_2$ in the basis $\left\{e_1, e_2, e_3, \cdots, e_7\right\}$ in $\mathbb{R}^7$.

Let us now search for the first cyclic subspace.

Since $P_2e_1 = e_6$, $P_2e_6 = e_1$, we have $F_1 = [1, 6]$, and the first cyclic subspace is spanned by the basis $\left\{e_1, e_6\right\}$. Its dimension is $|F_1| = 2$. The matrix of the transformation $\mathscr{P}_2$ restricted to this cyclic subspace is $N_2 = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$.

Since $P_2e_2 = e_3$, $P_2e_3 = e_4$, $P_2e_4 = e_2$, so $F_2 = [2, 3, 4]$, $|F_2| = 3$. The second cyclic subspace is spanned by the basis $\left\{e_2, e_3, e_4\right\}$, and its dimension is $|F_2| = 3$. The matrix of the transformation $\mathscr{P}_2$ restricted to this cyclic subspace is $N_3 = \begin{bmatrix} & & 1 \\ 1 & & \\ & 1 & \end{bmatrix}$.

Since $P_2e_5 = e_5$, $F_3 = [5]$, $|F_3| = 1$. The third cyclic subspace is spanned by the basis $\left\{e_5\right\}$, and the dimension is $|F_3| = 1$. The matrix of $\mathscr{P}_2$ restricted to this cyclic subspace is $N_1 = [1]$. Finally, since $P_2e_7 = e_7$, $F_4 = [7]$, $|F_4| = 1$. The fourth cyclic subspace is spanned by the basis $\left\{e_7\right\}$, the dimension is $|F_4| = 1$. The matrix of $\mathscr{P}_2$ restricted to this cyclic subspace is $N_1 = [1]$.

Overall, we have that P_2 is permutationally similar to the canonical form

$$B_2 = \mathrm{diag}\,\{I_2, N_2, N_3\} = \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & 0 & 0 & 1 \\ & & & & 1 & 0 & 0 \\ & & & & 0 & 1 & 0 \end{bmatrix},$$

or

$$\begin{aligned} &P_2\{e_5; e_7;\ e_1, e_6;\ e_2, e_3, e_4\} \\ =&\{e_5; e_7;\ e_6, e_1;\ e_3, e_4, e_2\} \\ =&\{e_5; e_7;\ e_1, e_6;\ e_2, e_3, e_4\}\begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & 0 & 0 & 1 \\ & & & & 1 & 0 & 0 \\ & & & & 0 & 1 & 0 \end{bmatrix}. \end{aligned}$$

Now we find T_2, such that $B_2 = T_2^{-1} P_2 T_2$.
It follows from

$$(e_5, e_7, e_1, e_6, e_2, e_3, e_4) = (e_1, e_2, e_3, e_4, e_5, e_6, e_7)\begin{bmatrix} & & 1 & 0 & 0 & 0 & 0 \\ & & & 0 & 1 & 0 & 0 \\ & & & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & & & 0 & & & \\ 0 & & & 1 & & & \\ 0 & 1 & 0 & 0 & & & \end{bmatrix},$$

denote

$$T_2 = \begin{bmatrix} & & 1 & 0 & 0 & 0 & 0 \\ & & & 0 & 1 & 0 & 0 \\ & & & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & & & 0 & & & \\ 0 & & & 1 & & & \\ 0 & 1 & 0 & 0 & & & \end{bmatrix},$$

which implying

$$T_2^{-1} = T_2^{\mathrm{T}} = \begin{bmatrix} & & & & 1 & 0 & 0 \\ & & & & & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & & & & & 1 & 0 \\ 0 & 1 & & & & & \\ 0 & 0 & 1 & & & & \\ 0 & 0 & 0 & 1 & & & \end{bmatrix},$$

so $P_2 = T_2\, B_2\, T_2^{-1}$, that is,

$$\begin{bmatrix} 0&0&0&0&0&1&0\\ 0&0&0&1&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0\\ 1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1 \end{bmatrix}$$

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

Then, $B_2 = T_2^{-1} P_2 T_2$, i.e.,

$$\begin{bmatrix} 1& & & & & & \\ &1& & & & & \\ & &0&1& & & \\ & &1&0& & & \\ & & & &0&0&1\\ & & & &1&0&0\\ & & & &0&1&0 \end{bmatrix}$$

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

□

Theorem 2. (*Decomposition Theorem*) *For any permutation matrix A of order n, if A is not the identity, then there are some generalized cycle matrices $Q_1, Q_2, \cdots, Q_r$ of type* II *and a diagonal matrix D_t of rank t, such that, $A = Q_1 + Q_2 + \cdots + Q_r + D_t$, where the non-zero elements in D_t are all ones , $\sum\limits_{i=1}^{r} \mathrm{rank} Q_i + t = n$; $1 \leqslant r \leqslant \left\lfloor \frac{n}{2} \right\rfloor$, r, Q_i ($i = 1, 2, \cdots, r$) and D_t are determined by A.*

If the cycle order of Q_i is k_i, $(i = 1, 2, \cdots, r)$, then $2 \leqslant \sum\limits_{i=1}^{r} k_i \leqslant n$. If A is a cycle matrix, then $t = 0$, $r = 1$, $k_1 = n$.

The main idea of the proof may be summarized as follow.

Denote by O_m a zero square matrix of order m. By Theorem 1 , there is a permutation matrix T, such that, $T^{-1}AT = \mathrm{diag}\,\{I_t, N_{k_1}, \cdots, N_{k_r}\}$. Then consider the matrices

$M_0 = \mathrm{diag}\,\{I_t, O_{k_1}, \cdots, O_{k_r}\}$,
$M_1 = \mathrm{diag}\,\{O_t, N_{k_1}, O_{k_2}, \cdots, O_{k_r}\}$,
$M_2 = \mathrm{diag}\,\{O_t, O_{k_1}, N_{k_2}, O_{k_3}, \cdots, O_{k_r}\}$,
$\cdots\cdots$,
$M_r = \mathrm{diag}\,\{O_t, O_{k_1}, O_{k_2}, \cdots, O_{k_{r-1}}, N_{k_r}\}$,
clearly,

$$\mathrm{diag}\{I_t, N_{k_1}, \cdots, N_{k_r}\} = M_0 + M_1 + M_2 + \cdots + M_r,$$

and

$$
\begin{aligned}
A &= T\,\mathrm{diag}\,\{I_t, N_{k_1}, \cdots, N_{k_r}\}\,T^{-1} \\
&= TM_0T^{-1} + TM_1T^{-1} + TM_2T^{-1} + \cdots + TM_rT^{-1}.
\end{aligned}
$$

It is clear that rank $M_i = k_i$ ($i = 1, 2, \cdots, r$), and rank $M_0 = t$. The matrix M_i is a generalized cycle matrix of type II with cycle order k_i. Since T is invertible, rank TM_iT^{-1} = rank $M_i = k_i$. T and T^{-1} are permutation matrices, so $Q_i = TM_iT^{-1}$ is also a 0-1 matrix with the same rank. Since $N_{k_i}^{k_i} = I_{k_i}$,

$$
M_i^{k_i} = \mathrm{diag}\{O_t, O_{k_1}, \cdots, I_{k_i}, \cdots, O_{k_r}\},
$$

is a diagonal matrix of rank k_i, and $\left(TM_iT^{-1}\right)^{k_i} = TM_i^{k_i}T^{-1}$ is a diagonal matrix of rank k_i, too. If the exponent is less than k_i, the conclusion does not hold (but it will cost us some more words to prove this proposition). Then,

$$
Q_i = TM_iT^{-1} \tag{4}
$$

is a generalized cycle matrix of type II with cycle order k_i. Analogously,

$$
D_t = TM_0T^{-1} = T\,\mathrm{diag}\{I_t, O_{k_1}, \cdots, O_{k_r}\}\,T^{-1} \tag{5}
$$

is a diagonal matrix of rank t.

Following this idea, we may prove Theorem 2 in a different way. However, this requires to obtain Q_i and D_t directly, which may be challenging. We prefer to move on with another proof following the idea of the proof of Theorem 1. In this way, we construct Q_i and D_t more conveniently.

Proof. Starting from the F_i' generated above, one may construct a 0-1 matrix D_t of order n, such that the j'th column of D_t is the j'th column of A ($\forall j \in \bigcup\limits_{i=1}^{t} F_i'$) and the other columns of D_t are 0 vectors. Of course, D_t is a diagonal matrix of rank t, as the j'th column of A is e_j (by definition, $Ae_j = e_j$).

Then, construct a 0-1 matrix Q_i ($i = 1, 2, \cdots, r$) of order n, such that the j'th column of Q_i is the j'th column of A ($j \in F_{t+i}'$) and the other columns of Q_i are 0 vectors. As

$$
\left(\bigcup_{i=1}^{t} F_i'\right) \bigcup \left(\bigcup_{i=1}^{r} F_{t+i}'\right) = \bigcup_{i=1}^{u} F_i = \{1, 2, \cdots, n\}, \tag{6}
$$

and

$$
F_{i_1} \cap F_{i_2} = \varnothing \ \ (1 \leqslant i_1 \neq i_2 \leqslant u),
$$

every column of A appears exact once in a matrix (D_t or Q_i, denoted by M) in the expression $\sum\limits_{i=1}^{r} Q_i + D_t$, in the same position as it appears in A. Besides, the columns in the same position in the matrices other than M appeared in the sum $\sum\limits_{i=1}^{r} Q_i + D_t$ are all 0 vectors. Overall, we have

$$
\sum_{i=1}^{r} Q_i + D_t = A.
$$

Let us now prove that Q_i is a generalized cycle matrix of type II with cycle order k_i.

Assume that the members in F_{t+i}' ($i = 1, 2, \cdots, r$) are $a_{i,1}', a_{i,2}', \cdots, a_{i,k_i}'$, and that $F_{t+i}' = F_s$ for some s ($1 \leqslant s \leqslant u$). Then we have a relation about the members in G_{t+i}' and the members in a certain G_s, i.e., $e_{i,v}' = e_{a_{i,v}'} \in G_s, v = 1, 2, \cdots, k_i$. By the definition of F_s, we know that $Ae_{a_{i,v}'} = e_{a_{i,v+1}'}$, ($v = 1, 2, \cdots, k_i - 1$), $Ae_{a_{i,k_i}'} = e_{a_{i,1}'}$, so $e_{a_{i,v+1}'}$ is the $a_{i,v}'$'th column of A.

As Q_i is made of some 0 vectors and k_i columns of A, and the columns of A are linearly independent, the rank of Q_i is k_i. The $a'_{i,v}$'th column of Q_i is the $a'_{i,v}$'th column of A, so $Q_i e_{a'_{i,v}} = e_{a'_{i,v+1}}$, $(v = 1, 2, \cdots, k_i - 1)$, $Q_i e_{a'_{i,k_i}} = e_{a'_{i,1}}$, $Q_i e_l = 0$ $(\forall e_l \in \mathcal{D}\backslash G'_{t+i})$. Therefore $Q_i^v e_{a'_{i,1}} = e_{a'_{i,v+1}}$ $(v = 1, 2, \cdots, k_i - 1)$, $Q_i^{k_i} e_{a'_{i,1}} = e_{a'_{i,1}}$, (so Q_i^v is not diagonal as $Q_i^v e_{a'_{i,1}} = e_{a'_{i,v+1}} \neq e_{a'_{i,1}}$). Then

$$Q_i^{k_i} e_{a'_{i,v}} = Q_i^{v-1}\left(Q_i^{k_i - v+1} e_{a'_{i,v}}\right) = Q_i^{v-1}\left(e_{a'_{i,1}}\right) = e_{a'_{i,v}}, (v = 1, 2, \cdots, k_i).$$

Hence $Q_i^{k_i}$ is a diagonal matrix of rank k_i. Therefore Q_i is a generalized cycle matrix of type II with cycle order k_i. □

Theorem 3. (*Factorization Theorem*) *For any permutation matrix A of order n, if A is not the identity, then there are some generalized cycle matrices P_1, P_2, $\cdots$, P_r of type* I *, such that, $A = P_1 P_2 \cdots P_r$, where $1 \leqslant r \leqslant \left\lfloor \frac{n}{2} \right\rfloor$; r, P_i $(i = 1, 2, \cdots, r)$ are determined by A. P_{i_1} and P_{i_2} commute $(1 \leqslant i_1 \neq i_2 \leqslant r)$.*

If the cycle order of P_i is k_i, $(i = 1, 2, \cdots, r)$, then $2 \leqslant \sum\limits_{i=1}^{r} k_i \leqslant n$.
Since $T^{-1}AT = \text{diag}\ \{I_t, N_{k_1}, \cdots, N_{k_r}\}$, for convenience, we denote
$Y_1 = \text{diag}\ \{I_t, N_{k_1}, I_{k_2}, \cdots, I_{k_r}\}$,
$Y_2 = \text{diag}\ \{I_t, I_{k_1}, N_{k_2}, I_{k_3}, \cdots, I_{k_r}\}$,
$\cdots\cdots$,
$Y_r = \text{diag}\ \{I_t, I_{k_1}, I_{k_2}, \cdots, I_{k_{r-1}}, N_{k_r}\}$.
Obviously,

$$\text{diag}\{I_t, N_{k_1}, \cdots, N_{k_r}\} = Y_1 Y_2 \cdots Y_r$$

and

$$\begin{aligned} A &= T\ \text{diag}\{I_t, N_{k_1}, \cdots, N_{k_r}\}\ T^{-1} = TY_1 Y_2 \cdots Y_r T^{-1} \\ &= \left(TY_1 T^{-1}\right)\left(TY_2 T^{-1}\right) \cdots \left(TY_r T^{-1}\right). \end{aligned}$$

Obviously, $\left(N_{k_i}\right)^{k_i} = I_{k_i}$, $\left(N_{k_i}\right)^{k_i - j} \neq I_{k_i}$, $0 < j < k_i$.
So $(Y_i)^{k_i} = I_n$, $(Y_i)^{k_i - j} \neq I_n$, $0 < j < k_i$.
It is clear that Y_i is a generalized cycle matrix of type I with cycle order k_i $(i = 1, 2, \cdots, r)$, and it is thus sufficient to prove that

$$P_i = TY_i T^{-1} \tag{7}$$

is a generalized cycle matrix of type I with cycle order k_i. Rather obviously, $P_i^{k_i} = TY_i^{k_i} T^{-1} = TI_n T^{-1} = I_n$, however, it is not easy to prove that there are exact k_i vanishing entries in the diagonal of P_i, and that k_i is the minimal positive integer satisfying the condition $P_i^{k_i} = I_n$.

Proof. Let $D_t^{(b)} = I_n - D_t$, where D_t is determined by Equation (5). Then

$$\text{rank} D_t = t,\ \text{rank} D_t^{(b)} = n - t.$$

Now build a 0-1 matrix J_i^a $(i = 1, 2, \cdots, r)$ of order n, such that the j'th column of J_i^a is the j'th column of I_n $(j \in F'_{t+i})$, and the other columns of J_i^a are 0 vectors. So

$$\sum_{i=1}^{r} J_i^{(a)} + D_t = I_n.$$

Let $J_i^{(b)} = I_n - J_i^{(a)}$, then

$$\mathrm{rank}J_i^{(a)} = k_i,\ \mathrm{rank}J_i^{(b)} = n - k_i.$$

We have

$$\begin{aligned} D_t^{(b)}D_t = D_tD_t^{(b)} = 0, \quad J_i^{(a)}J_i^{(b)} = J_i^{(b)}J_i^{(a)} = 0, \quad Q_iJ_i^{(b)} = J_i^{(b)}Q_i = 0, \\ Q_{i_1}J_{i_2}^{(a)} = J_{i_2}^{(a)}Q_{i_1} = 0, \quad J_{i_1}^{(a)}J_{i_2}^{(a)} = J_{i_2}^{(a)}J_{i_1}^{(a)} = 0, \quad Q_{i_1}Q_{i_2} = Q_{i_2}Q_{i_1} = 0, \end{aligned}$$

and

$$Q_{i_1}J_{i_2}^{(b)} = J_{i_2}^{(b)}Q_{i_1} = Q_{i_1} \neq 0, \quad J_{i_1}^{(a)}J_{i_2}^{(b)} = J_{i_2}^{(b)}J_{i_1}^{(a)} = J_{i_1}^{(a)} \neq 0,$$

where $1 \leqslant i_1 \neq i_2 \leqslant r$, Q_i is defined above Equation (6) on page 8.

It is not difficult to prove that

$$J_{i_1}^{(b)}J_{i_2}^{(b)} = J_{i_2}^{(b)}J_{i_1}^{(b)} = I_n - J_{i_2}^{(a)} - J_{i_1}^{(a)}.$$

If we denote $P_i = Q_i + J_i^{(b)}$, we have

$$\mathrm{rank}P_i = n,\ I_n + Q_i = P_i + J_i^{(a)}.$$

Clearly,

$$P_{i_1}P_{i_2} = \left(Q_{i_1} + I_n - J_{i_1}^{(a)}\right)\left(Q_{i_2} + I_n - J_{i_2}^{(a)}\right) = Q_{i_1} + Q_{i_2} + I_n - J_{i_1}^{(a)} - J_{i_2}^{(a)},$$

and

$$P_{i_2}P_{i_1} = \left(Q_{i_2} + I_n - J_{i_2}^{(a)}\right)\left(Q_{i_1} + I_n - J_{i_1}^{(a)}\right) = Q_{i_2} + Q_{i_1} + I_n - J_{i_2}^{(a)} - J_{i_1}^{(a)}.$$

So, $P_{i_1}P_{i_2} = P_{i_2}P_{i_1}$, i.e., P_{i_1} and P_{i_2} commute.
Hence

$$\prod_{i=1}^{r} P_i = \prod_{i=1}^{r}\left(Q_i + I_n - J_i^{(a)}\right) = \sum_{i=1}^{r} Q_i + I_n - \sum_{i=1}^{r} J_i^{(a)} = \sum_{i=1}^{r} Q_i + D_t = A.$$

We can also prove the equality above in a different way.
Because $Q_{i_1}Q_{i_2} = 0$, $Q_{i_1}D_t = D_tQ_{i_1} = 0$, $(1 \leqslant i_1 \neq i_2 \leqslant r)$, then

$$(I_n + D_t)\prod_{i=1}^{r}(I_n + Q_i) = I_n + \sum_{i=1}^{r} Q_i + D_t = I_n + A. \tag{8}$$

Since $D_tQ_i = Q_iD_t = 0$, we have $D_tJ_i^{(a)} = J_i^{(a)}D_t = 0$.

By construction, when $1 \leqslant i \leqslant r$, $v \in F'_{t+i} \bigcup \left(\bigcup_{i=1}^{t} F'_i\right)$, the v'th column (or the v'th row) of P_j $(1 \leqslant j \leqslant r, j \neq i)$ is equal to the v'th column (or the v'th row) of I_n, so the v'th column (or the v'th row) of $\prod_{\substack{1\leqslant j\leqslant r \\ j\neq i}}^{r} P_j$ is equal to the v'th column (or the v'th row) of I_n.

Therefore, when $J_i^{(a)}$ is multiplied by $\prod\limits_{\substack{1\leqslant j\leqslant r\\ j\neq i}}^{r} P_j$, the v'th column does not change, while the other columns of $J_i^{(a)}$ are 0 vectors, such that

$$J_i^{(a)} \prod_{\substack{1\leqslant j\leqslant r\\ j\neq i}}^{r} P_j = J_i^{(a)}.$$

For the same reason, $D_t \prod\limits_{i=1}^{r} P_i = D_t$.

Noting that

$$\begin{aligned}
&(I_n + D_t)\prod_{i=1}^{r}(I_n + Q_i)\\
=&(I_n + D_t)\prod_{i=1}^{r}\left(P_i + J_i^{(a)}\right)\\
=&(I_n + D_t)\left(\prod_{i=1}^{r} P_i + \sum_{i=1}^{r}\left(J_i^{(a)} \prod_{\substack{1\leqslant j\leqslant r\\ j\neq i}}^{r} P_j\right)\right) \quad (J_{i_1}^{(a)} J_{i_2}^{(a)} = J_{i_2}^{(a)} J_{i_1}^{(a)} = 0,\ i_1 \neq i_2)\\
=&(I_n + D_t)\left(\prod_{i=1}^{r} P_i + \sum_{i=1}^{r} J_i^{(a)}\right)\\
=&\prod_{i=1}^{r} P_i + \sum_{i=1}^{r} J_i^{(a)} + D_t\prod_{i=1}^{r} P_i + D_t\sum_{i=1}^{r} J_i^{(a)}\\
=&\prod_{i=1}^{r} P_i + \sum_{i=1}^{r} J_i^{(a)} + D_t + 0 = \prod_{i=1}^{r} P_i + I_n,
\end{aligned}$$

we have that

$$(I_n + D_t)\prod_{i=1}^{r}(I_n + Q_i) = \prod_{i=1}^{r} P_i + I_n. \tag{9}$$

It follows from Equations (8) and (9), that

$$\prod_{i=1}^{r} P_i + I_n = I_n + A,$$

thus $\prod\limits_{i=1}^{r} P_i = A$.

Now, we prove that P_i is a generalized cycle matrix of type II with cycle order k_i.

Since $P_i = Q_i + J_i^{(b)}$, $Q_i J_i^{(b)} = J_i^{(b)} Q_i = 0$, then $P_i^m = Q_i^m + \left(J_i^{(b)}\right)^m = Q_i^m + J_i^{(b)}$ $(\forall m \in \mathbb{Z}^+)$, and $P_i^{k_i} = Q_i^{k_i} + J_i^{(b)}$.

It follows from $Q_i^{k_i} e_{a'_{i,v}} = A^{k_i} e_{a'_{i,v}} = e_{a'_{i,v}}$ $(v = 1, 2, \cdots, k_i)$ that

$$\forall e_l \in \mathcal{D}\backslash G'_{t+i},\ Q_i e_l = 0 \Longrightarrow Q_i^{k_i} e_l = 0.$$

Here $\mathcal{D}$ is defined in Equation (3).

On the other hand, $J_i^{(b)} e_{a'_{i,v}} = 0$ $(v = 1, 2, \cdots, k_i)$, $J_i^{(b)} e_l = e_l$, $(\forall e_l \in \mathcal{D}\backslash G'_{t+i})$.

So, for any e_l in $\mathcal{B}$, if $e_l \in G_i'$, then $\left(Q_i^{k_i} + J_i^{(b)}\right)e_l = Q_i^{k_i}e_l = e_l$; otherwise, $e_l \notin G_i'$, then $\left(Q_i^{k_i} + J_i^{(b)}\right)e_l = J_i^{(b)}e_l = e_l$.

This means that $P_i^{k_i}e_l = (Q_i^{k_i} + J_i^{(b)})e_l = e_l$ ($\forall e_l \in \mathcal{B}$), i.e. $P_i^{k_i}$ $(e_1, e_2, \cdots, e_n) = (e_1, e_2, \cdots, e_n)$, or $P_i^{k_i}$ $I_n = I_n$. (Actually, by $Q_i^{k_i} = J_i^{(a)}$, we have that $P_i^{k_i} = Q_i^{k_i} + J_i^{(b)} = J_i^{(a)} + J_i^{(b)} = I_n$.)

When $1 \leqslant m < k_i$, Q_i^m is not diagonal, and neither is $Q_i^m + J_i^{(b)} = P_i^m$. So, P_i is a generalized cycle matrix of type II with cycle order k_i. $\square$

4. On the Number of Permutation Similarity Classes

The number of permutation similarity classes of permutation matrices of order n is the partition number $p(n)$. There is a recursion formula for $p(n)$,

$$\begin{aligned} p(n) &= p(n-1) + p(n-2) - p(n-5) - p(n-7) + \cdots + \\ &\quad (-1)^{k-1}p\left(n - \frac{3k^2 \pm k}{2}\right) + \cdots\cdots \\ &= \sum_{k=1}^{k_1}(-1)^{k-1}p\left(n - \frac{3k^2+k}{2}\right) + \sum_{k=1}^{k_2}(-1)^{k-1}p\left(n - \frac{3k^2-k}{2}\right), \end{aligned} \tag{10}$$

(see [7], p. 55), where

$$k_1 = \left\lfloor \frac{\sqrt{24n+1}-1}{6} \right\rfloor, \; k_2 = \left\lfloor \frac{\sqrt{24n+1}+1}{6} \right\rfloor, \tag{11}$$

and $p(0) = 1$. In the above formula, $\lfloor x \rfloor$ denotes the floor function, i.e. the maximum integer that is less than or equal to the real number x.

Asymptotically, we have (see e.g., [8,9])

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\sqrt{\frac{2}{3}}\pi n^{1/2}\right). \tag{12}$$

This formula has been obtained by Godfrey H. Hardy and Srinivasa Ramanujan in 1918 [10] (In [11,12], one may find two different proofs. The evaluation of the constants can be found in [13]).

Formula (12) is relevant for theoretical analysis and very convenient to estimate the value of $p(n)$ by simple means. However, the accuracy of the asymptotic Formula (12) is limited when n is small. Another celebrated formula, given in term of a convergent series, has been found by Rademacher in 1937, based on the work of Hardy and Srinivasa Ramanujan, see [7,14].

In [15], several other formulae modified from Formula (12) have been obtained, showing high accuracy and yet expressed in terms of elementary functions, e.g.

$$p(n) \approx \left\lfloor \frac{\exp\left(\sqrt{\frac{2}{3}}\pi\sqrt{n}\right)}{4\sqrt{3}(n + C_2'(n))} + \frac{1}{2} \right\rfloor, \quad 1 \leqslant n \leqslant 80 \tag{13}$$

with a relative error less than 0.004%, where

$$C_2'(n) = \begin{cases} 0.4527092482 \times \sqrt{n+4.35278} - 0.05498719946, & n = 3, 5, 7, \cdots, 79; \\ 0.4412187317 \times \sqrt{n-2.01699} + 0.2102618735, & n = 4, 6, 8, \cdots, 80. \end{cases}$$

and

$$p(n) \approx \left\lfloor \frac{\exp\left(\sqrt{\frac{2}{3}}\pi\sqrt{n}\right)}{4\sqrt{3}(n+a_2\sqrt{n+c_2}+b_2)} + \frac{1}{2} \right\rfloor, \quad n \geqslant 80 \tag{14}$$

with a relative error less than 5×10^{-8} when $n \geqslant 180$, where $a_2 = 0.4432884566$, $b_2 = 0.1325096085$ and $c_2 = 0.274078$.

5. Results for Monomial Matrices

Any monomial matrix M can be written as a product of a permutation matrix P and an invertible diagonal matrix D. Turn all the non-zero elements of M into 1, then we have a permutation matrix P. Suppose that the unique non-zero elements in the i'th row of M is c_i, and the unique non-zero element in the i'th column of M is d_i, $i = 1, 2, \cdots, n$. Let D_1 = diag $\{ c_1, c_2, \cdots, c_n \}$, D_2 = diag $\{ d_1, d_2, \cdots, d_n \}$, then we have $M = PD_2 = D_1P$.

For the permutation matrix P, there is a permutation matrix T such that $T^{-1}PT = Y$ has the canonical form diag $\{I_t, N_{k_1}, \cdots, N_{k_r}\}$ as proved in Theorem 1. In the expression $T^{-1}PT$, the permutation matrix T^{-1} changes only the position of the rows, and T just changes the position of the columns of P. Since the non-zero elements of M and P share the same locations in the matrices, so do $T^{-1}MT$ and $T^{-1}PT$. Denote the unique non-zero element in the i'th row of $T^{-1}MT$ by a_i, and the unique non-zero element in the i'th column of $T^{-1}MT$ by b_i, $i = 1, 2, \cdots, n$. Let D_3 = diag $\{ a_1, a_2, \cdots, a_n \}$, D_4 = diag $\{ b_1, b_2, \cdots, b_n \}$, then $T^{-1}MT = D_3Y = YD_4$.

Finally, we have that

$$\begin{aligned} M = D_1T \begin{bmatrix} I_t & & & \\ & N_1 & & \\ & & \ddots & \\ & & & N_r \end{bmatrix} T^{-1} &= T \begin{bmatrix} I_t & & & \\ & N_1 & & \\ & & \ddots & \\ & & & N_r \end{bmatrix} T^{-1}D_2 \\ = TD_3 \begin{bmatrix} I_t & & & \\ & N_1 & & \\ & & \ddots & \\ & & & N_r \end{bmatrix} T^{-1} &= T \begin{bmatrix} I_t & & & \\ & N_1 & & \\ & & \ddots & \\ & & & N_r \end{bmatrix} D_4T^{-1}. \end{aligned}$$

D_1, D_2, D_3 and D_4 could be easily obtained from M directly. Their relations can be stated as below.

$D_2 = P^{-1}D_1P, \ D_3 = T^{-1}D_1T, D_4 = Y^{-1}D_3Y.$

6. Conclusions

For any permutation matrix A of order n, we can obtain its canonical form $B = \text{diag}\{I_t, N_{k_1}, \cdots, N_{k_r}\}$ and a permutation matrix T by the algorithm described in the proof of Theorem 1, such that, $B = T^{-1}AT$, where t, r, k_1, $\cdots$, k_r and T are uniquely determined from A. Any matrix permutationally similar to A has the same canonical form.

The permutation matrix A can be written as the sum of some generalized cycle matrices $Q_1, Q_2, \cdots, Q_r$ of type II and a diagonal matrix D_t of rank t, where t and r are the same as that mentioned above, $Q_1, Q_2, \cdots, Q_r$ and D_t are determined from A by Equations (4) and (5) in the proof of Theorem 2.

We can also denote A as the product of some generalized cycle matrices $P_1, P_2, \cdots, P_r$ of type I, where t is the same as that mentioned above, $P_1, P_2, \cdots, P_r$ can be constructed from the Equation (7) in the proof of Theorem 3.

7. Concluding Remark

We can also prove Theorem 1 by the combinatorial method, which may seem easier. But the other two theorems could not be easily proved in the same way. Theorem 1 could be written in the form of permutation transformations (which are the members of the symmetry group S_n). If L is a Latin square, every row (or column) of L could be considered as a permutation transformation. When searching for the invariant isotopism group of L, we will encounter the canonical form of the permutational similarity relations (of permutation matrices or of permutation transformations in S_n). So the conclusions obtained here could be applied in Latin squares or projective planes.

Author Contributions: Conceptualization, methodology, validation, writing—original draft—W.-W.L.; funding acquisition—Q.-W. W., W.-W.L. and X.H.; discussion, writing-final draft—X.H., Q.-W.W. and W.-W.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (No. 11971294), the College Natural Scientific Research Projects organized by Anhui Provincial Department of Education (No. KJ2021A1198, KJ2021ZD0143) and Beijing Natural Science Foundation (No. 1224036).

Institutional Review Board Statement: Not applicable

Data Availability Statement: Not applicable

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lam, C.W.H.; Kolesova, G.; Thiel, L. A computer search for finite projective planes of order 9. *Discret. Math.* **1991**, *92*, 187–195. [CrossRef]
2. Djordjević, B.D. Doubly stochastic and permutation solutions to $AXA = XAX$ when A is a permutation matrix. *Linear Algebra Its Appl.* **2023**, *661*, 79–105. [CrossRef]
3. Chen, J.X.; Zhu, Z.L.; Fu, C.; Yu, H.; Zhang, Y. Reusing the permutation matrix dynamically for efficient image cryptographic algorithm. *Signal Process.* **2015**, *111*, 294–307. [CrossRef]
4. Jaballi, A.; Sakly, A.; Hajjaji, A.E. Permutation matrix based robust stability and stabilization for uncertain discrete-time switched TS fuzzy systems with time-varying delays. *Neurocomputing* **2016**, *214*, 527–534. [CrossRef]
5. Diab, H.; El-semary, A.M. Cryptanalysis and improvement of the image cryptosystem reusing permutation matrix dynamically. *Signal Process.* **2018**, *148*, 172–192. [CrossRef]
6. Nie, X.R.; Wang, Q.W.; Zhang, Y. A System of Matrix Equations over the Quaternion Algebra with Applications. *Algebra Colloq.* **2017**, *24*, 233–253. [CrossRef]
7. Hall, M., Jr. A survey of combinatorial analysis. In *Some Aspects of Analysis and Probability*; Surveys in Applied Mathematics; Kaplansky, I., Hall, M., Jr., Eds.; John Wiley and Sons, Inc.: New York, NY, USA; Chapman and Hall, Limited: London, UK, 1958; Volume IV, pp. 35–104.
8. Weisstein, E.W. "Partition Function P." From MathWorld—A Wolfram Web Resource. 1999–2015. Available online: http://mathworld.wolfram.com/PartitionFunctionP.html (accessed on 20 November 2022).
9. Apostol, T.M. Functions of Number Theory, Additive Number Theory: Unrestricted Partitions. In *NIST Digital Library of Mathematical Functions (DLMF)*; Olver, F.W.J., Lozier, D.W., Boisvert, R.F., Eds.; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2022. Available online: http://dlmf.nist.gov/27.14 (accessed on 20 December 2022).
10. Hardy, G.H.; Ramanujan, S.R. Asymptotic Formulae in Combinatory Analysis. *Proc. Lond. Math. Soc.* **1918**, *2*, 75–115. [CrossRef]
11. Erdős, P. The Evaluation of the Constant in the Formula for the Number of Partitions of n. *Ann. Math. Second. Ser.* **1942**, *43*, 437–450. [CrossRef]
12. Newman, D.J. A simplified proof of the partition formula. *Mich. Math. J.* **1962**, *9*, 283–287. [CrossRef]
13. Newman, D.J. The Evaluation of the Constant in the Formula for the Number of Partitions of n. *Am. J. Math.* **1951**, *73*, 599–601. [CrossRef]
14. Rademacher, H. A Convergent Series for the Partition Function $p(n)$. *Proc. Natl. Acad. Sci. USA* **1937**, *23*, 78–84. [CrossRef] [PubMed]
15. Li, W.W. Estimation of the Partition Number: After Hardy and Ramanujan. *arXiv* **2016**, arXiv:1612.05526. [CrossRef]