

Permutation Matrices of Reverse r-th Stride

I. Ž. Milovanović, E.R. Glogić, E. I. Milovanović, M. P. Bekakos, M. K. Stojčev

Abstract: A new class of permutation matrices is defined in this paper. It is based on a tensor product of permutation matrices of reverse cyclic stride. Recurrent relation for generation of these matrices is derived.

Keywords: Permutation matrices, tensor product.

1 Introduction

A binary matrix is a matrix with elements from the set $\{0, 1\}$. Examples of these matrices include adjacency matrices, incidence matrices, ordered and unordered matrices, permutation matrices, etc. These are met in graph theory, discrete mathematics, cryptography (see [1, 2, 3, 8]), digital signal processing, numerical analysis [4, 5, 6], etc. In focus of our interest are permutation matrices. A permutation matrix is a square matrix which has one and only one unit element in each row and column. These matrices provide stability and well conditionality of computations (e.g. solving systems of linear equations and LR factorization based on Gaussian method with pivoting [6]). In addition they are used in parallel computing systems for memory referencing (see for example [7, 9]), during systolic array synthesis for optimization of space and time parameters (see [9, 10]).

In this paper a new class of permutation matrices obtained by tensor product of permutation matrices of reverse cyclic stride is presented.

Manuscript received January 22, 2013; accepted May 15, 2013.

I. Ž. Milovanović, E. I. Milovanović and M. K. Stojčev with the Faculty of Electronic Engineering, Niš, Serbia; E.R. Glogić is with the State University of Novi Pazar, Novi Pazar, Serbia; M. P. Bekakos is with Democritus University of Thrace, Xanthi, Greece.

2 Permutation matrices of reverse cyclic stride

Denote with I_r an identity matrix of order $r \times r$, and by \hat{I}_r a reverse identity matrix defined as

$$\hat{I}_r = \begin{bmatrix} 0 & \dots & 0 & 1 \\ 0 & \dots & 1 & 0 \\ \vdots & & & \\ 1 & \dots & 0 & 0 \end{bmatrix}.$$

Further, denote by $\hat{I}_r^{(k \rightarrow)}$, $0 \leq k \leq r-1$, a permutation matrix obtained by cyclic shifting of columns of \hat{I}_r to the right, i.e.

$$\hat{I}_r \equiv \hat{I}_r^{(0 \rightarrow)} = \begin{bmatrix} 0 & \dots & 0 & 1 \\ 0 & \dots & 1 & 0 \\ \vdots & & & \\ 1 & \dots & 0 & 0 \end{bmatrix}, \quad \hat{I}_r^{(1 \rightarrow)} = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 \\ \vdots & & & & \\ 0 & 1 & \dots & 0 & 0 \end{bmatrix}, \dots,$$

$$\hat{I}_r^{(k \rightarrow)} = \begin{bmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & \dots & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ \vdots & & & & & & & & \\ 1 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ \vdots & & & & & & & & \\ 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 & 0 \end{bmatrix}.$$

Similarly, a permutation matrix obtained by cyclic shifting of columns of \hat{I}_r to the left, denoted as $\hat{I}_r^{(\leftarrow k)}$, can be defined. Some crucial properties of these matrices are

$$\begin{aligned} \hat{I}_r^{(k \rightarrow)} &= \hat{I}_r^{(\leftarrow (r-k))}, & \hat{I}_r^{(k \rightarrow)} \cdot \hat{I}_r^{(k \rightarrow)} &= I_r, \\ \hat{I}_r^{(k \rightarrow)} &= I_r^{(k \rightarrow)} \cdot \hat{I}_r^{(0 \rightarrow)}, & \hat{I}_r^{(k \rightarrow)} \cdot \hat{I}_r^{(t \rightarrow)} &= \hat{I}_r^{((t-k) \bmod r \rightarrow)} \end{aligned}$$

for each $0 \leq k \leq r-1$ and $0 \leq t \leq r-1$, where $I_r^{(0 \rightarrow)} \equiv I_r^{(\leftarrow 0)} \equiv I_r$, and $I_r^{(k \rightarrow)}$ ($I_r^{(\leftarrow k)}$) are matrices obtained by cyclic shifting of columns of identity matrix to the right (left).

Let $\vec{x} = [x_1 \ x_2 \ \dots \ x_r]^T$ be an arbitrary vector. By multiplying vector \vec{x} with $\hat{I}_r \equiv \hat{I}_r^{(0 \rightarrow)}$, we obtain vector

$$\vec{x}^* = [x_r \ x_{r-1} \ \dots \ x_1]^T.$$

Similarly, by multiplying \vec{x} with $\hat{I}_r^{(k \rightarrow)}$, $0 \leq k \leq r-1$, we obtain

$$\vec{x}^{*(k \rightarrow)} = [x_k \ x_{k-1} \ \dots \ x_1 \ x_r \ x_{r-1} \ \dots \ x_{k+1}]^T,$$

and by matrix $\hat{I}_r^{(\leftarrow k)}$

$$\vec{x}^{*(\leftarrow k)} = [x_{r-k} \ \dots \ x_1 \ x_r \ \dots \ x_{r-k+1}]^T.$$

This implies that elements of vector \vec{x} are first rearranged in reverse order and then cyclicly shifted for k positions to the right (left).

3 Permutation matrices of reverse r -th stride

Let $r \geq 2$ and $m \geq 2$ are given natural numbers. For each k , $0 \leq k \leq r^m - 1$, there exist unique non negative integers k_i , $0 \leq k_i \leq r - 1$, $i = 0, 1, \dots, m - 1$, so that the following presentation is valid

$$k = k_{m-1}r^{m-1} + k_{m-2}r^{m-2} + \dots + k_0r^0 = (k_{m-1}k_{m-2}\dots k_0)_r \quad (1)$$

According to the above representation of non negative integer (i.e. representation n power number system of radix r) and tensor product of permutation matrices of reverse stride, we will define a new class of permutation matrices.

Definition 1 Let r , k and m be non negative integers for which (1) is valid. For each k , $k = 0, 1, \dots, r^m - 1$ permutation matrix of reverse r -th right stride, $S_{r^m}^{(k \rightarrow)}$, are defined as

$$S_{r^m}^{(k \rightarrow)} = \hat{I}_r^{(k_{m-1} \rightarrow)} \otimes \hat{I}_r^{(k_{m-2} \rightarrow)} \otimes \dots \otimes \hat{I}_r^{(k_0 \rightarrow)}, \quad (2)$$

where \otimes denotes tensor product of two matrices.

Notice 1 According to (1) the following class of permutation matrices can be defined

$$\begin{aligned} S_{r^m}^{(\leftarrow k)} &= \hat{I}_r^{(\leftarrow k_{m-1})} \otimes \hat{I}_r^{(\leftarrow k_{m-1})} \otimes \dots \otimes \hat{I}_r^{(\leftarrow k_0)}, \\ R_{r^m}^{(k \rightarrow)} &= \hat{I}_r^{(k_0 \rightarrow)} \otimes \hat{I}_r^{(k_1 \rightarrow)} \otimes \dots \otimes \hat{I}_r^{(k_{m-1} \rightarrow)}, \\ R_{r^m}^{(\leftarrow k)} &= \hat{I}_r^{(\leftarrow k_0)} \otimes \hat{I}_r^{(\leftarrow k_1)} \otimes \dots \otimes \hat{I}_r^{(\leftarrow k_{m-1})} \end{aligned}$$

Matrices $S_{r^m}^{(\leftarrow k)}$ form a class of permutation matrices of reverse r -th left stride. Matrices $R_{r^m}^{(k \rightarrow)}$ (i.e. $R_{r^m}^{(\leftarrow k)}$) form a class of permutation matrices of inverse stride with respect to $S_{r^m}^{(k \rightarrow)}$ (i.e. $S_{r^m}^{(\leftarrow k)}$).

New arrangement of elements of vector \vec{x} , after multiplication by permutation matrix of reverse r -th stride, will be explained on the concrete example.

Example: Let $r = 3$ and $m = 2$. For each k , $0 \leq k \leq 8$, according to (1), the following is valid

$$\begin{array}{lll} 0 = 0 \cdot 3^1 + 0 \cdot 3^0, & 1 = 0 \cdot 3^1 + 1 \cdot 3^0, & 2 = 0 \cdot 3^1 + 2 \cdot 3^0 \\ 3 = 1 \cdot 3^1 + 0 \cdot 3^0, & 4 = 1 \cdot 3^1 + 1 \cdot 3^0, & 5 = 1 \cdot 3^1 + 2 \cdot 3^0, \\ 6 = 2 \cdot 3^1 + 0 \cdot 3^0, & 7 = 2 \cdot 3^1 + 1 \cdot 3^0, & 8 = 2 \cdot 3^1 + 2 \cdot 3^0 \end{array}$$

Let $\vec{x} = [x_1 \ x_2 \ x_3 \ | \ x_4 \ x_5 \ x_6 \ | \ x_7 \ x_8 \ x_9]^T$ be a given vector and $\vec{x}^* = [x_9 \ x_8 \ x_7 \ | \ x_6 \ x_5 \ x_4 \ | \ x_3 \ x_2 \ x_1]^T$ a vector accompanied to \vec{x} . Vector \vec{x}^* is decomposed into three blocks. Based on the equalities

$$S_{3^2}^{(1 \rightarrow)} \cdot \vec{x} = \begin{bmatrix} 0 & 0 & \hat{I}_3^{(1 \rightarrow)} \\ 0 & \hat{I}_3^{(1 \rightarrow)} & 0 \\ \hat{I}_3^{(1 \rightarrow)} & 0 & 0 \end{bmatrix} \cdot \vec{x} = [x_7 \ x_9 \ x_8 \ | \ x_4 \ x_6 \ x_5 \ | \ x_1 \ x_3 \ x_2]^T,$$

$$S_{3^2}^{(3 \rightarrow)} \cdot \vec{x} = \begin{bmatrix} \hat{I}_3^{(0 \rightarrow)} & 0 & 0 \\ 0 & 0 & \hat{I}_3^{(0 \rightarrow)} \\ 0 & \hat{I}_3^{(0 \rightarrow)} & 0 \end{bmatrix} \cdot \vec{x} = [x_3 \ x_2 \ x_1 \ | \ x_9 \ x_8 \ x_7 \ | \ x_6 \ x_5 \ x_4]^T,$$

$$S_{3^2}^{(1 \rightarrow)} \cdot \vec{x} = \begin{bmatrix} 0 & \hat{I}_3^{(1 \rightarrow)} & 0 \\ \hat{I}_3^{(1 \rightarrow)} & 0 & 0 \\ 0 & 0 & \hat{I}_3^{(1 \rightarrow)} \end{bmatrix} \cdot \vec{x} = [x_4 \ x_6 \ x_5 \ | \ x_1 \ x_3 \ x_2 \ | \ x_7 \ x_9 \ x_8]^T,$$

we obtain three different arrangement of elements of vector \vec{x} . To explain this reordering it is necessary to start from vector \vec{x}^* . If $k_0 = 0$, elements within blocks of \vec{x}^* remain at the same locations. If $1 \leq k \leq 2$, then elements within blocks are cyclically shifted for k_0 positions to the right. If $k_1 = 0$, blocks of \vec{x}^* stay at their original positions. If $1 \leq k_1 \leq 2$, blocks of \vec{x}^* are cyclically shifted for k_1 positions to the right.

Let m and $r, r \geq 2$ are two natural numbers, and k non negative integer with the property $0 \leq k \leq r^m - 1$ represented in form (1). Further, let $S_{r^m}^{(k \rightarrow)}$ be a permutation matrix of reverse r -th stride, and $\vec{x} = [x_1 \ x_2 \ \dots \ x_{r^m}]^T$ a vector to which vector $\vec{x}^* = [x_{r^m} \ x_{r^m-1} \ \dots \ x_1]^T$ is accompanied. Our goal is to determine the arrangement of elements in vector $\vec{x}^{(k)} = S_{r^m}^{(k \rightarrow)} \vec{x}$. Therefore, we first decompose vector \vec{x}^* into r blocks, each with r^{m-1} elements. These blocks belong to a class-block $(m-1)$. Further, each block from class $(m-1)$ is divided into r blocks. Now, we have r^2 blocks with r^{m-2} elements each. These blocks form class-block $(m-2)$. We continue with this procedure until class-block (1) with r^{m-1} blocks of size r is obtained. Now, the following can be concluded:

- If $k_0 = 0$, elements in class-block (1) retain their positions. If $1 \leq k_0 \leq r-1$, elements within each block of class (1) are cyclically shifted for k_0 positions to the right;
- If $k_i = 0, i = 1, 2, \dots, m-2$ blocks from class (i) retain their positions within blocks from class $(i+1)$. If $1 \leq k_i \leq r-1$, blocks from class (i) are cyclically shifted for k_i positions to the right within a block from class $(i+1)$;

- If $k_{m-1} = 0$, blocks from class $(m-1)$ retain their positions within vector \vec{x}^* . If $1 \leq k_{m-1} \leq r-1$, then these blocks are cyclically shifted for k_{m-1} positions to the right within vector \vec{x}^* .

The following theorem defines a recursive procedure for generating permutation matrices of reverse r -th stride.

Theorem 1 *Let $r \geq 2$ and $m \geq 2$ are given natural numbers. Then for each non negative integer k , $0 \leq k \leq r^m - 1$, the following equality is valid*

$$S_{r^m}^{(k \rightarrow)} = \hat{I}_r^{(t \rightarrow)} \otimes S_{r^{m-1}}^{(n \rightarrow)}, \quad (3)$$

where $t = \left\lfloor \frac{k}{r^{m-1}} \right\rfloor$ and $n = k \bmod r^{m-1}$.

Proof. Suppose that r , m and k satisfy the conditions of Theorem 1. Since

$$k_{m-2}r^{m-2} + \dots + k_0r^0 \leq (r-1)\frac{r^{m-1}-1}{r-1} = r^{m-1} - 1 < r^{m-1},$$

according to (1), we have that

$$t \left\lfloor \frac{k}{r^{m-1}} \right\rfloor = k_{m-1} \quad \text{and} \quad n = k \bmod r^{m-1} = k_{m-2}r^{m-2} + \dots + k_0r^0,$$

so the equality (3) directly follows from (2). \square

4 Conclusion

We have defined four new classes of permutation matrices in this paper, called permutation matrices of reverse r -th stride. For these classes of permutation matrices, we have described a procedure which defines rearrangement of elements of a given vector \vec{x} after the multiplication by a permutation matrix.

Acknowledgement

This work was supported by the Serbian Ministry of Education and Science, Project No TR 32009.

References

- [1] D. CVETKOVIĆ, M. MILIĆ, *Graph theory and its applications*, Beograd, 1977 (In Serbian)
- [2] I. Ž. MILOVANOVIĆ, E. I. MILOVANOVIĆ, *Discrete mathematics*, University of Niš, Faculty of Electronic Engineering, Niš, 2000. (In Serbian)
- [3] A. DUJELLA, M. MARETIĆ, *Cryptography*, Element, Zagreb, 2007. (In Croatian)
- [4] E. JE. DAGMAN, G. A. KUHAREV, *Fast discrete orthogonal transformations*, Nauka, Novosibirsk, 1983. (In Russian)
- [5] M. STOJIC, M. STANKOVIĆ, R. STANKOVIĆ, *Discrete transformations in applications*, Naučna knjiga, Beograd, 1985. (In Serbian)
- [6] G. V. MILOVANOVIĆ, *Numerical analysis*, Naučna knjiga, Beograd, 1988. (In Serbian)
- [7] S. G. AKL, *The design and analysis of parallel algorithms*, Prentice-Hall Inter. Edit., 1989.
- [8] J. A. ANDERSON, *Discrete mathematics with combinatorics*, Pearson, Prentice Hall, New Jersey, 2004.
- [9] I. Ž. MILOVANOVIĆ, M. P. BEKAKOS, I. N. TSELEPIS, E. I. MILOVANOVIĆ, *Forty three ways of systolic matrix multiplication*, Intern. J. Comput. Math., Vol. 87, 6 (2010), 1264-1276.
- [10] M. K. STOJČEV, E. I. MILOVANOVIĆ, I. Ž. MILOVANOVIĆ, *An algorithm for multiplication of concatenated matrices*, Parall. Comput., Vol. 13, (1990), 211-223.