On Semigroup of Permutation Factor Circulant Boolean Matrices

ZHOU Min-na

(College of Science and Technology, Ningbo University, Ningbo 315211, China)

Abstract: Let $PM_n(B)$ denote the set of all $n\times n$ permutation factor circulant matrices over the Boolean algebra $B=\{0,1\}$, then $PM_n(B)$ forms a semigroup under the usual matrix product. In this paper, all idempotents in $PM_n(B)$ are characterized, the Euler-Fermat theorem for the semigroup $PM_n(B)$ is also established.

Key words: Boolean algebra; permutation factor circulant Boolean matrix; semigroups; idempotent; Euler-Ferment theorem

CLC number: O153.1 **Document code:** A **Article ID:** 1001-5132（2011）03-0038-03

1 Introduction and preliminaries

As an important class of special matrices, circulant matrices have a wide range of interesting applications[1-2]. The circulant matrices have in recent years been extended in many directions[1-9]. The permutation factor circulant matrices are another natural extension of this well-studied class, and can be found in [8-9]. Let $B=\{0,1\}$ be the Boolean algebra. We denote by $M_n(B)$ the set of all $n\times n$ matrices over *B*. Clearly, $M_n(B)$ forms a semigroup under the usual matrix product. We call $M_n(B)$ the Boolean matrix semigroup. Let $A=(a_{ij}),\ B=(b_{ij})\in M_n(B)$. Define $A\leqslant B$ by $a_{ij}\leqslant b_{ij}$ for all $i,j=1,2,\cdots,n$.

Let $C=(c_{ij})\in M_n(B)$ by $c_{1n}=1=c_{ii+1}(i\neq n)$ and $c_{ij}=0$ for all other *i* and *j*. Let

$$C_n(B)=\{A\,|\,A=a_0E+a_1C+\cdots+a_{n-1}C^{n-1}\in M_n(B)\},$$

where *E* is the unit matrix in $M_n(B)$. Then $C_n(B)$ is a commutative subsemigroup of $M_n(B)$. For $A\in C_n(B)$, *A* is called a circulant Boolean matrix. $C_n(B)$ is called the semigroup of circulant Boolean matrices. K-Hang K et al studied the semigroup $C_n(B)$ in [10-11]. Chao C Y et al studied the semigroup of generalized-circulant Boolean matrices in [5-7]. In this paper, we shall study the semigroup of the following permutation factor Boolean matrices.

Definition 1[9] An $n\times n$ permutation matrix *P* over *B* is called a basic permutation factor circulant Boolean matrix if and only if

$$P^n=E\,, \tag{1}$$

n is the smallest positive integer which satisfies the above equation (1).

Definition 2[9] An $n\times n$ matrix *A* over *B* is called a permutation factor circulant Boolean matrix if

$$A=a_0E+a_1P+\cdots+a_{n-1}P^{n-1}\,. \tag{2}$$

In view of the structure of the powers of the basic permutation factor circulant Boolean matrix *P* in $M_n(B)$ and Definition 1, it is clear that *A* is a permutation factor circulant Boolean matrix in $M_n(B)$ if and only if *A* commutes with *P*, that is, *AP*=*PA*. Let $Z_n=\{\overline{0},\overline{1},\cdots,\overline{n-1}\}$ be the residue classes additive group module *n*. Write

$$Supp(A)=\{\,\overline{i}\mid a_i=1\,\}\subseteq Z_n\,,$$

Then, *A* can be denoted by

$$A=\sum\nolimits_{\overline{i}\in Suup(A)}P^i\,. \tag{3}$$

The set of all permutation factor circulant

Received date: 2011–03–31. JOURNAL OF NINGBO UNIVERSITY (NSEE): http://3xb.nbu.edu.cn
Author's biography: ZHOU Min-na (1960–), female, Ningbo Zhejiang, associate professor, research domain: algebra. E-mail: cjmclj@mail.nbptt.zj.cn

Boolean matrix in $M_n(B)$ is denoted by $PM_n(B)$. Then, $PM_n(B)$ is also a commutative subsemigroup of $M_n(B)$. If $P=C$, $PM_n(B)=C_n(B)$. Therefore, the permutation factor circulant Boolean matrix is a generalized of the circulant Boolean matrix.

Definition 3 Let $A\in M_n(B)$. A is said to be an idempotent Boolean matrix if $A^2=A$.

We shall characterize all idempotents in $PM_n(B)$, and also establish the Euler-Fermat theorem for the semigroup $PM_n(B)$. All results in this paper are generalizations of results in [10-11].

2 The idempotents in $PM_n(B)$

Theorem 1 Let $A=\sum_{\bar{i}\in Suup(A)}P^i$. Then A is an idempotent in $PM_n(B)$ if and only if $D = Suup(A)$ is a subgroup of Z_n. Thus, if $A\neq E$, A takes the following form:

$$A=E+P^d+\cdots+P^{(n/d-1)d}, \tag{4}$$

where d is some positive factor of n.

Proof Necessity. Since $A^2=A$ and

$$A^2=\sum_{\bar{i}\in D}P^i\sum_{\bar{j}\in D}P^j=\sum_{\bar{i},\bar{j}\in D}P^{i+j}=\sum_{\bar{k}\in D+D}P^k=A=\sum_{\bar{i}\in D}P^i,$$

$D+D=Suup(A^2)=Suup(A)=D$. Therefore, the subset $D=Suup(A)$ of Z_n is a subgroup of the residue classes additive group Z_n.

Sufficiency. Since $D=Suup(A)$ is a subgroup of the residue classes additive group Z_n, D+D=D. Then we have

$$A^2=\sum_{\bar{i},\bar{j}\in D}P^{i+j}=\sum_{\bar{k}\in D+D}P^k=\sum_{\bar{k}\in D}P^k=A.$$

Therefore, A is an idempotent in $PM_n(B)$.

Also, if $A=\sum_{\bar{i}\in Suup(A)}P^i$ is an idempotent in, D= $Suup(A)$ is a subgroup of Z_n. Thus, if $D\neq 0$, there exist a positive factor d of n such that

$$D=<\bar{d}>=\{\bar{0},\bar{d},\cdots,\overline{(n/d-1)d}\}.$$

Then

$$A=E+P^d+\cdots+P^{(n/d-1)d}.$$

This proves the theorem.

Theorem 2 The number of idempotent in $PM_n(B)$ is the number of subgroup of the residue classes additive group Z_n, that is, $D(n)$+1 where $D(n)$ denotes the number of positive factor of n.

Proof By Theorem 1, A is an idempotent in $PM_n(B)$ if and only if D=$Suup(A)$ is a subgroup of Z_n. For a subgroup D of Z_n, if $D\neq 0$, there exist a positive factor d of n such that $D=<\bar{d}>$.

Conversely, for a positive factor d of n, there exist only subgroup D of Z_n such that $D=<\bar{d}>$. Thus, Theorem 2 holds.

3 Euler-Fermat theorem for the semigroup $PM_n(B)$

In [11], Schwarz studied the Euler-Fermat theorem for the semigroup $C_n(B)$ of circulant Boolean matrices, and obtained the following result.

Theorem 3[11] For any $A\in C_n(B)$, we have $A^{n-1}=A^{2n-1}$. This result is the best possible, i.e., none of the exponents can be replaced by a smaller number.

The purpose of this section is to generalize this result in the semigroup $PM_n(B)$. We need the following lemma.

Lemma 1[12] Let n be a positive integer. Then for any $2n-1$ integers, there exist n integers such that their sum is a multiple of n.

Theorem 4 For any $A\in PM_n(B)$, we have $A^{n-1}=A^{2n-1}$. This result is the best possible, i.e., none of the exponents can be replaced by a smaller number.

Proof Let $A=\sum_{i=0}^{n-1}a_iP^i\in PM_n(B)$ and $A^k=\sum_{i=0}^{n-1}a_i^{(k)}P^i\in PM_n(B)$, where k is any positive integer. Then, for any i, $a_i^{(k)}$ is a sum of terms Q of the form:

$$Q=a_{i_1}a_{i_2}\cdots a_{i_k},$$

with k indices $i_1,i_2,\cdots,i_k$ such that $\bar{i}_1+\bar{i}_2+\cdots+\bar{i}_k=\bar{i}$, i.e.,

$$a_i^{(k)}=\sum_{\bar{i}_1+\bar{i}_2+\cdots+\bar{i}_k=\bar{i}}a_{i_1}a_{i_2}\cdots a_{i_k},$$

Since for any h, $n\bar{h}=\bar{0}$. Therefore, for any i, we have

$$a_i^{(n-1)}=\sum_{\bar{i}_1+\bar{i}_2+\cdots+\overline{i_{n-1}}=\bar{i}}a_{i_1}a_{i_2}\cdots a_{i_{n-1}}=$$

$$\sum_{\bar{i}_1+\bar{i}_2+\cdots+\bar{i}_{n-1}+n\overline{i_{n-1}}=\bar{i}} a_{i_1}a_{i_2}\cdots a_{i_{n-1}}(a_{i_{n-1}})^n \leqslant$$

$$\sum_{\bar{i}_1+\bar{i}_2+\cdots+\bar{i}_{n-1}+\bar{i}_n+\cdots+\overline{i_{2n-1}}=\bar{i}} a_{i_1}a_{i_2}\cdots a_{i_{n-1}}a_{i_n}\cdots a_{i_{2n-1}} = a_i^{(2n-1)},$$

hence, $A^{n-1} \leqslant A^{2n-1}$.

Conversely, for any term $Q = a_{i_1}a_{i_2}\cdots a_{i_k}a_{i_{k+1}}\cdots a_{i_{2n-1}}$ of $a_i^{(2n-1)}$, by Lemma 1, we can select n elements from indices $\bar{i}_1, \bar{i}_2, \cdots, \overline{i_{2n-1}}$ such that their sum is $\bar{0}$. We can assume without loss of generality that the n integers are $i_n, \cdots, i_{2n-1}$. Then

$$a_i^{(2n-1)} = \sum_{\bar{i}_1+\bar{i}_2+\cdots+\overline{i_{n-1}}+\bar{i}_n+\cdots+\overline{i_{2n-1}}=\bar{i}} a_{i_1}a_{i_2}\cdots a_{i_{n-1}}a_{i_n}\cdots a_{i_{2n-1}} =$$

$$\sum_{\bar{i}_1+\bar{i}_2+\cdots+\overline{i_{n-1}}=\bar{i}} a_{i_1}a_{i_2}\cdots a_{i_{n-1}}a_{i_n}\cdots a_{i_{2n-1}} \leqslant$$

$$\sum_{\bar{i}_1+\bar{i}_2+\cdots+\overline{i_{n-1}}=\bar{i}} a_{i_1}a_{i_2}\cdots a_{i_{n-1}} = a_i^{(n-1)}.$$

Hence, $A^{2n-1} \leqslant A^{n-1}$, and we have $A^{n-1} = A^{2n-1}$. When P=C, $PM_n(B) = C_n(B)$, by Theorem 3, we can see that this result is the best possible, i.e., none of the exponents can be replaced by a smaller number. This proves the theorem.

References:

[1] Ruiz-Claeyssen J. Factor block circulant and periodic solutions of undamped matrix differential equations[J]. Math Appl Comput, 1983, 3(1):81-92.

[2] Claeyssen J C R, Leal L A S. Diagonalization and spectral decomposition of factor block circulant matrices [J]. Linear Algebra and its Applications, 1988, 99:41-61.

[3] Davis P. Circulant matrices[M]. New York: Wiley and Sons, 1979:20-22.

[4] Jiang Zhaolin, Zhou Zhangxin. Circulant Matrices[M]. Chengdu: Chengdu Technology University Publishing Company, 1999:50-60.

[5] Chao C Y, Zhang M C. On generalized circulants over a Boolean algebra[J]. Linear Algebra and its Applications, 1984, 62:195-206.

[6] Cen Jianmiao. On the Sandwich semigroup of group Boolean matrices[J]. SIAM J Matrix Anal Appl, 1998, 19(2):416-428.

[7] Tan Yijia. The semigroup of primitive generalized circulant Boolean matrices[J]. Semigroup Forum, 2007, 74:77-92.

[8] Stuart Jefrey L. Diagonally scaled permutations and circulant matrices[J]. Linear Algebra and its Applications, 1994, 212/213:397-411.

[9] Jiang Zhaolin, Xu Zongben, Gao Shuping. Algorithms for finding the minimal polynomials and inverses of permutation factor circulant matrices[J]. Chinese Journal of Engineering Mathematics, 2006, 23(6):1088-1094.

[10] K-Hang K, Schwarz S. The semigroup of circulant Boolean matrices[J]. Czech Math J, 1976, 26(4):632-635.

[11] Schwarz S. The Euler-Fermat theorem for the semigroup of circulant Boolean matrices[J]. Czech Math J, 1980, 30(105):135-141.

[12] Zun S. On a conjecture of elementary number theory[J]. Advances in Mathematics (in Chinese), 1983, 12(4):299-301.

关于置换因子循环布尔矩阵半群

周敏娜

（宁波大学 科学技术学院, 浙江 宁波 315211）

摘要： $PM_n(B)$ 表示布尔代数 $B=\{0,1\}$ 上的所有 $n\times n$ 置换因子循环矩阵组成的集合. $PM_n(B)$ 对于矩阵乘法成为一个半群. 刻画了 $PM_n(B)$ 中的幂等元, 并给出了半群 $PM_n(B)$ 中的 Euler-Fermat 定理.

关键词： 布尔代数; 置换因子循环矩阵; 半群; 幂等元; Euler-Fermat 定理

（责任编辑 史小丽）