On the Sandwich Semigroups of Circulant Boolean Matrices

Wenchao Huang
Department of Mathematics
University of Wisconsin—Madison
Madison, Wisconsin 53706

Submitted by Hans Schneider

ABSTRACT

Let $C_n$ be the semigroup of all the $n \times n$ ($n \geq 2$) circulant Boolean matrices, and $R$ a nonzero element in $C_n$. The sandwich semigroup of $C_n$ with the sandwich element $R$ is denoted by $C_n(R)$. The purpose of this paper is to discuss the Green's classes, idempotent elements, regular elements, and maximal subgroups in $C_n(R)$. In Section 4, a necessary and sufficient condition on the Green's class $\mathcal{J}_R(A)$ is given, where $\mathcal{J}_R(A)$ is the Green's class in the sandwich semigroup $C_n(R)$ containing $A$, and $A$ is an arbitrary circulant Boolean matrix in $C_n(R)$. In Sections 5 and 6, the idempotent elements and the maximal subgroups containing an idempotent element in $C_n(R)$ are discussed. Some necessary and sufficient conditions which characterize the idempotent elements and maximal subgroups are obtained. In Section 7, we use the results of Sections 5 and 6 to obtain a necessary and sufficient condition which characterizes the regular elements in $C_n(R)$. Otherwise, some counting theorems about the idempotent elements, the regular elements, and the maximal subgroups are given.

1. INTRODUCTION

Let $B = \{0, 1\}$ be a Boolean algebra, and $C_n$ the set of all the $n \times n$ ($n \geq 2$) circulant matrices over $B$. The elements of $C_n$ are all the matrices of the form

$$A = \begin{bmatrix}
  a_0 & a_1 & \cdots & a_{n-1} \\
  a_{n-1} & a_0 & \cdots & a_{n-2} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_1 & a_2 & \cdots & a_0
\end{bmatrix}, \quad \text{where} \quad a_i \in B \ (i = 0, 1, 2, \ldots, n - 1).$$

© Elsevier Science Publishing Co., Inc., 1993
655 Avenue of the Americas, New York, NY 10010 0024-3795/93/$5.00
Denote three special matrices in $C_n$ as follows:

$$
P = \begin{bmatrix}
0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 1 \\
1 & 0 & 0 & \cdots & 0 & 0
\end{bmatrix},
$$

$$
E = \begin{bmatrix}
1 \\
1 \\
\vdots \\
1
\end{bmatrix}, \quad \text{and} \quad
H = \begin{bmatrix}
1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 1
\end{bmatrix}.
$$

Then, for any $A \in C_n$, $A$ can be written as

$$
A = a_0E + a_1P + a_2P^2 + \cdots + a_{n-1}P^{n-1}, \quad a_i \in B.
$$

We define $P^0 = E$. It is obvious that $P^n = E$. Under the usual multiplication operation of Boolean matrices, the set $C_n$ forms a commutative semigroup and is still denoted by $C_n$. Clearly, every nonzero elements in $C_n$ has a unique representation in the form (1.1) The zero element is $C_n$ is devoted by $Z$.

For an arbitrary but fixed element $R \in C_n$, we can define an operation $*$ in $C_n$ as follows: For arbitrary $A, B \in C_n$, $A * B = ARB$, where $ARB$ is the usual product of Boolean matrices. It can be easily proved that $C_n$ is also a commutative semigroup under the operation $*$. We denote this semigroup by $C_n(R)$ and call it a sandwich semigroup of circulant Boolean matrices with sandwich matrix $R$. The purpose of this paper is to discuss Green's relations, idempotent elements, regular elements, and maximal subgroups for $C_n(R)$ with $R \neq Z$.

2. NOTATION AND DEFINITIONS

For convenience, some notation and definitions are given in the following.

**Definition 2.1.** For any finite set $M \neq \emptyset$, denote

$$
|M| = \text{the cardinality of } M.
$$

**Definition 2.2.** Let $a_1, \ldots, a_m$ be $m$ ($m \geq 2$) integers. The greatest
common divisor $d$ of $a_1, \ldots, a_m$ is denoted by

$$d = (a_1, \ldots, a_m).$$

The number of all the different positive common divisors of $a_1, \ldots, a_m$ is denoted by

$$d^+(a_1, \ldots, a_m).$$

If $m = 1$, let $d^+(a_1)$ denote the number of all the different positive divisors of $a_1$.

**Definition 2.3.** Let $M = \{m_1, \ldots, m_s\}$ and $N = \{n_1, \ldots, n_t\}$ be two sets of integers. Let $m$ be an integer. Write

$$m + N = \{m + n_1, \ldots, m + n_t\}$$

and

$$M + N = \{m_i + n_j | i = 1, 2, \ldots, s; j = 1, 2, \ldots, t\}.$$ 

**Definition 2.4.** Let $M$ and $N$ be two sets of integers, $n$ a positive integer. If each integer in $M$ is congruent to some integer in $N$ modulo $n$, we write $M \subseteq N \pmod{n}$. We write $M = N \pmod{n}$ if $M \subseteq N \pmod{n}$ and $N \subseteq M \pmod{n}$.

**Definition 2.5.** Let $n$ be a positive integer and $Z \not\equiv A \in C_n$. If $A = p_1^n + \cdots + p_t^n$ and $0 < n_1 < \cdots < n_t < n$, then $\{n_1, \ldots, n_t\}$ is said to be the set of support numbers of $A$. It is denoted by

$$\text{SN}(A) = [n_1, \ldots, n_t].$$

**Definition 2.6.** For $A \in C_n(R)$, denote

$$C_n(R) * A = \{CRA | C \in C_n(R)\}.$$ 

**Definition 2.7.** For any $A \in C_n(R)$, the $\mathcal{L}_R$-class of $C_n(R)$ containing
A is denoted by $\mathcal{L}_R(A)$, i.e.,

$$\mathcal{L}_R(A) = \{ B | B \in C_n(R), B \mathcal{L}_R A \}.$$

(The definitions of Green’s relations and Green’s classes can be seen in [5]. In this paper, $\mathcal{L}$ denotes the $\mathcal{L}$-relation in $C_n$, and $\mathcal{L}_R$ denotes the $\mathcal{L}$-relation in $C_n(R)$.)

3. PRELIMINARIES ON INTEGERS

Many problems on Boolean matrices can be studied by using the properties of integers. In this paper, the integer method is applied almost everywhere. As preparation, several lemmas and a proposition on integers are proved in the following.

**Lemma 3.1.** Let $M_1, \ldots, M_k$ and $N_1, \ldots, N_k$ be $2k$ sets of integers ($k \geq 2$), and $n$ be a positive integer. If

$$M_i \equiv N_i \pmod{n}, \quad i = 1, 2, \ldots, k,$$

then

$$\sum_{i=1}^{k} M_i \equiv \sum_{i=1}^{k} N_i \pmod{n}.$$

**Proof.** It is easy to prove by the Definition 2.3.

The following lemma is due to C. Y. Chao and M. C. Zhang in [1]. But it is stated and proved in different manner as follows:

**Lemma 3.2.** Let $n$, $s_1$, $s_2$, $d_1$, and $d_2$ be positive integers such that $n = s_1d_1 = s_2d_2$. For an arbitrary nonnegative integer $r$, let

$$C = \bigcup_{i=0}^{s_1-1} \bigcup_{j=0}^{s_2-1} \{ r + id_1 + jd_2 \}.$$

Then

$$C \equiv \{ r, r + d, \ldots, r + (s - 1)d \} \pmod{n},$$

where $d = (d_1, d_2)$ and $n = sd$. 
Proof. Let $C_1 = \{r, r + d, \ldots, r + (s - 1)d\}$. Since $d = (d_1, d_2, \ldots)$, there exist two integers $x$ and $y$ such that $d = xd_1 + yd_2$. For any $r + ad \in C_1$ ($0 \leq a \leq s - 1$), suppose $ax = t_1s_1 + i$ and $ay = t_2s_2 + j$, where $t_1, t_2, i,$ and $j$ are integers and $0 \leq i \leq s_1 - 1$, $0 \leq j \leq s_2 - 1$. Then

$$r + ad = r + axd_1 + ayd_2 = r + id_1 + jd_2 + (t_1 + t_2)n \equiv r + id_1 + jd_2 \pmod{n}.$$  

This shows that $C_1 \subseteq C \pmod{n}$. Conversely, for any $r + id_1 + jd_2 \in C$ ($0 \leq i \leq s_1 - 1$, $0 \leq j \leq s_2 - 1$), suppose $d_1 = q_1d$ and $d_2 = q_2d$; then

$$r + id_1 + jd_2 = r + (iq_1 + jq_2)d.$$  

Suppose $iq_1 + jq_2 = ts + a$, where $t$ and $a$ are two integers and $0 \leq a \leq s - 1$. Then

$$r + id_1 + jd_2 = r + tn + ad \equiv r + ad \pmod{n}.$$  

This shows that $C_1 \subseteq C \pmod{n}$. Hence $C \equiv C_1 \pmod{n}$.  

**Lemma 3.3.** Let $n, s_1, \ldots, s_k, d_1, \ldots, d_k$ be positive integers such that $n = s_id_i$ ($k \geq 2$, $i = 1, 2, \ldots, k$). For an arbitrary nonnegative integer $r$, let

$$C = \bigcup_{i_1=0}^{s_1-1} \cdots \bigcup_{i_k=0}^{s_k-1} \{r + i_1d_1 + \cdots + i_kd_k\}.$$  

Then

$$C \equiv \{r, r + d, \ldots, r + (s - 1)d\} \pmod{n},$$  

where $d = (d_1, d_2, \ldots, d_k)$ and $n = sd$.  

**Proof.** The proof is by induction on $k$. For the case of $k = 2$, it is the result of Lemma 3.2. Hypothesize that the statement is true for the case of $k - 1$. Now we discuss the case of $k$. Let $d' = (d_1, d_2, \ldots, d_{k-1})$ and $n = s'd'$. By the induction hypothesis, we have

$$\bigcup_{i_1=0}^{s_1-1} \cdots \bigcup_{i_{k-1}=0}^{s_{k-1}-1} \{r + i_1d_1 + \cdots + i_{k-1}d_{k-1}\} \equiv \{r, r + d', \ldots, r + (s' - 1)d'\} \pmod{n}. \quad (3.3.1)$$  

LEMMA 3.3. Let $n, s_1, \ldots, s_k, d_1, \ldots, d_k$ be positive integers such that $n = s_id_i$ ($k \geq 2$, $i = 1, 2, \ldots, k$). For an arbitrary nonnegative integer $r$, let

$$C = \bigcup_{i_1=0}^{s_1-1} \cdots \bigcup_{i_k=0}^{s_k-1} \{r + i_1d_1 + \cdots + i_kd_k\}.$$  

Then

$$C \equiv \{r, r + d, \ldots, r + (s - 1)d\} \pmod{n},$$  

where $d = (d_1, d_2, \ldots, d_k)$ and $n = sd$.  

**Proof.** The proof is by induction on $k$. For the case of $k = 2$, it is the result of Lemma 3.2. Hypothesize that the statement is true for the case of $k - 1$. Now we discuss the case of $k$. Let $d' = (d_1, d_2, \ldots, d_{k-1})$ and $n = s'd'$. By the induction hypothesis, we have

$$\bigcup_{i_1=0}^{s_1-1} \cdots \bigcup_{i_{k-1}=0}^{s_{k-1}-1} \{r + i_1d_1 + \cdots + i_{k-1}d_{k-1}\} \equiv \{r, r + d', \ldots, r + (s' - 1)d'\} \pmod{n}. \quad (3.3.1)$$
Since \((d', d_k) = ((d_1, d_2, \ldots, d_{k-1}), d_k) = d\), by Lemma 3.2 we have
\[
\bigcup_{i=0}^{s' \cdot 1} \bigcup_{i_k=0}^{s_k \cdot 1} \{r + id' + i_k d_k\} \equiv \{r, r + d, \ldots, r + (s - 1)d\} \pmod{n}.
\]

Let
\[
C' = \bigcup_{i=0}^{s'-1} \bigcup_{i_k=0}^{s_k-1} \{r + id' + i_k d_k\}.
\]

For any \(r + id' + i_k d_k \in C'\) (\(0 \leq i \leq s' - 1, 0 \leq i_k \leq s_k - 1\)), by (3.3.1) there are \(i_1, \ldots, i_{k-1}\) (\(0 \leq i_j \leq s_j - 1, j = 1, 2, \ldots, k - 1\)) such that
\[
r + id' = r + i_1 d_1 + \cdots + i_{k-1} d_{k-1} \pmod{n},
\]
and then
\[
r + id' + i_k d_k \equiv r + i_1 d_1 + \cdots + i_{k-1} d_{k-1} + i_k d_k \pmod{n}.
\]

This shows that \(C' \subseteq C \pmod{n}\). Similarly, by (3.3.1), we can prove that \(C \subseteq C' \pmod{n}\). Hence \(C \equiv C' \equiv \{r, r + d, \ldots, r + (s - 1)d\} \pmod{n}\). 

Through the rest of this paper, the concept "arithmetic series" with respect to a given positive integer \(n\) is used. For a given positive integer \(n\):

(i) Any single integer is considered to be an arithmetic series with common difference \(n\) only (i.e., if an integer \(m\) is said to be a arithmetic series with common difference \(d\), then \(d\) equals \(n\)).

(ii) Let \(M\) be a finite set of integers \(|M| \geq 2\). Then \(M\) is said to be an arithmetic series with common difference \(d\) if all the integers of \(M\) can be arranged as
\[
m_1, \ldots, m_t
\]
such that \(m_{i+1} - m_i = d, i = 1, 2, \ldots, t - 1\).

**Lemma 3.4.** Let \(n\) be a positive integer, \(M\) a finite set of nonnegative integers. Let \(m\) be an integer. If \(M\) is an arithmetic series with common difference \(d\) and \(|M| = s\), where \(d\) is a positive common divisor of \(m\) and \(n\), and \(n = sd\), then \(m + M = M \pmod{n}\).

**Proof.** Suppose \(M = \{k, k + d, \ldots, k + (s - 1)d\}\) and \(m = rd\). For any \(m + k + ad \in m + M\) (\(0 \leq a \leq s - 1\)), we have \(m + k + ad = k + (a
+ r)d, and this implies \( m + M \subseteq M \) (mod \( n \)). Conversely, for any \( k + ad \in M \) (0 \( \leq a \leq s - 1 \)), we have \( k + ad = m + k + (a - r)d \equiv m + k + (qs + a - r)d \) (mod \( n \)) for every integer \( q \). We claim that there exists an integer \( q \) such that 0 \( \leq qs + a - r \leq s - 1 \). The above argument shows that \( M \subseteq m + M \) (mod \( n \)). Hence \( m + M \equiv M \) (mod \( n \)). 

**Proposition 3.5.** Let \( n \) be a given positive integer. Let \( M = \{n_1, \ldots, n_t\} \) satisfying \( n_1 < n_2 < \cdots < n_t \), 0 \( \leq n_i < n \) for every \( i \). Let \( m_1, \ldots, m_t \) be \( l \) different nonnegative integers. Then

\[
m_f + M \equiv M \pmod n \quad (f = 1, 2, \ldots, t)
\]

if and only if, for \( d = (m_1, \ldots, m_t, n) \) and \( n = sd \),

\[
M = M_1 \cup \cdots \cup M_h,
\]

where \( M_i \cap M_j = \emptyset \) whenever \( i \neq j \), \( M_j \) \((j = 1, 2, \ldots, h)\) is an arithmetic series with common difference \( d \), and \( |M_1| = \cdots = |M_h| = s \).

**Proof.** "Only if": Suppose \( d_f = (m_f, n) \) and \( n = sf d_f \) \((f = 1, 2, \ldots, l)\).

Let

\[
A_f(n_i) = \{n_i, n_i + m_f, \ldots, n_i + (s_f - 1)m_f\} \quad \text{and}
\]

\[
B_f(n_i) = \{n_i, n_i + d_f, \ldots, n_i + (s_f - 1)d_f\},
\]

\[
i = 1, 2, \ldots, t, \quad f = 1, 2, \ldots, l.
\]

Since \( s_f \) is the smallest positive integer such that \( sf m_f \equiv 0 \) (mod \( n \)), for any \( n_i \) and \( f \) the integers in \( A_f(n_i) \) \( \text{if} \ |A_f(n_i)| \geq 2 \) are not congruent to each other modulo \( n \). Clearly, for any \( n_i \) and \( f \), the integers in \( B_f(n_i) \) \( \text{if} \ |B_f(n_i)| \geq 2 \) are not congruent to each other modulo \( n \). On the other hand, for any \( n_i + am_f \in A_f(n_i) \) \((0 \leq a \leq s_f - 1)\), the integer \( n_i + am_f = n_i + a(m_f/d)d_f \) is congruent to some integer in \( B_f(n_i) \). Since \( |A_f(n_i)| = |B_f(n_i)| \) for any \( n_i \) and \( f \), synthesizing the above argument, we claim that

\[
A_f(n_i) = B_f(n_i) \pmod n, \quad i = 1, 2, \ldots, t, \quad f = 1, 2, \ldots, l. \quad (3.4.1)
\]

Choose \( n_{i_1} = \min(M) = n_1 \), and let

\[
M_1 = \{n_{i_1}, n_{i_1} + 1, \ldots, n_{i_1} + (s - 1)d\}.
\]
where \( d = (m_1, \ldots, m_i, n) \) and \( n = sd \). Since \( d = ((m_1, n), (m_2, n), \ldots, (m_i, n)) = (d_1, d_2, \ldots, d_l) \), by Lemma 3.3 we have

\[
M_1 = \bigcup_{i=0}^{s_1-1} \bigcup_{i=0}^{s_l-1} \{ n_{i_1} + i_1d_1 + \cdots + i_l d_l \} \pmod{n}.
\]

By (3.4.1), (3.4.2), and \( m_1 + M = M \pmod{n} \) \( (f = 1, 2, \ldots, l) \), we have \( M_1 \subseteq M \pmod{n} \). In fact, we have \( M_1 \subseteq M \). To prove this, it is sufficient to prove \( n_{i_1} + (s - 1)d < n \). If \( n_{i_1} + (s - 1)d \geq n \), then since \( n_{i_1}, s - 1 < n \) and \( M_1 \subseteq M \pmod{n} \), we suppose \( n_{i_1} + (s - 1)d = n + n_j \) for some \( n_j \in M \). By the choice of \( n_{i_1} \), we have \( n_{i_1} < n_j \). This implies \( n_{i_1} + (s - 1)d > n + n_j \) and then \( n_{i_1} - d > n_j \). Since \( d > 0 \), this is impossible. Hence \( M_1 \subseteq M \).

Assume that \( M_1, \ldots, M_{k-1} \ (k \geq 2) \) have been constructed such that

\[
M_j \subseteq M
\]

and

\[
M_j = \{ n_{i_j}, n_{i_j} + d, \ldots, n_{i_j} + (s - 1)d \} \quad (j = 1, 2, \ldots, k - 1).
\]

We can construct \( M_k \) as follows: Choose

\[
n_{ik} = \min \left\{ M \setminus \bigcup_{j=1}^{k-1} M_j \right\},
\]

and let

\[
M_k = \{ n_{ik}, n_{ik} + d, \ldots, n_{ik} + (s - 1)d \}.
\]

By the same reasoning as for \( M_1 \subseteq M \pmod{n} \), we can prove \( M_k \subseteq M \pmod{n} \).

To prove \( M_k \subseteq M \), we first prove the following:

STATEMENT I. None of the integers in \( M_k \) is congruent to any integer in \( \bigcup_{k=1}^{k-1} M_j \) modulo \( n \).

Suppose the contrary, and assume that there exist \( a \) and \( b \), \( 0 \leq a, b < s \), such that

\[
n_{ik} + ad \equiv n_{ij} + bd \pmod{n},
\]
where \( n_{ij} \in M_j \) \((1 \leq j \leq k - 1)\). This implies that one of following three cases is true:

(i) \( n_{ik} + ad = n_{ij} + bd \);
(ii) \( n_{ik} + ad = n + n_{ij} + bd \);
(iii) \( n + n_{ik} + ad = n_{ij} + bd \).

Suppose (i) is true. By the choices of \( n_{ij} \) and \( n_{ik} \), we have \( n_{ik} > n_{ij} \). This implies \( b > a \), then \( 0 < b = n_{ij} + (b - a)d \leq M_j \). This is impossible. So (i) cannot be true. Suppose (ii) is true. Since \( n_{ik} = n_{ij} + (s + b - a)d \), it follows that \( s + b - a > 0 \). If \( 0 < s + b - a < s \), we have \( n_{ik} \in M_j \). But that is impossible according to the choice of \( n_{ik} \). If \( s + b - a \geq s \), then \( (s + b - a)d \geq sd = n \), and then \( n_{ik} = n_{ij} + (s + b - a)d \geq n + n \). This contradicts the condition of this proposition. So (ii) cannot be true. Since \( n_{ij} + bd \in M_j \), we have \( n_{ij} + Bd < n \). But \( n + n_{ik} + ad > n \). These imply that (iii) cannot be true. According to above argument, Statement I holds.

To prove \( M_k \subseteq M \), it is sufficient to prove \( n_{ik} + (s - 1)d < n \). Assume \( n_{ik} + (s - 1)d = n \). Since \( M_k \subseteq M \) (mod \( n \)), we can suppose \( n_{ik} + (s - 1)d = n + n_j \) for some \( n_j \in M \). By Statement I and the choice of \( n_{ik} \), we have \( n_{ik} < n_j \). But \( n_{ik} + (s - 1)d = n + n_j \) and \( sd = n \) imply \( n_{ik} > n_j \). This is a contradiction. So \( M_k \subseteq M \).

By the same process, after a finite number of steps, we can construct \( M_1, M_2, \ldots, M_h \) such that

\[
M_j = \{n_{ij}, n_{ij} + d, \ldots, n_{ij} + (s - 1)d\} \subseteq M \quad (j = 1, 2, \ldots, h)
\]

and

\[
M \setminus \bigcup_{j=1}^{h} M_j = \emptyset.
\]

Hence

\[
M = \bigcup_{j=1}^{h} M_j.
\]

Clearly, \( M_j \) \((j = 1, 2, \ldots, h)\) is an arithmetical series with common difference \( d \) and \( |M_j| = \cdots = |M_k| = s \). By Statement I, \( M_i \cap M_j = \emptyset \) whenever \( i \neq j \). The proof of "only if" is completed.
"If": For any $f$ and $j$, $1 \leq f \leq l$, $1 \leq j \leq h$, by Lemma 3.4 we have

$$m_f + M_j \equiv M_j \pmod{n}.$$ 

Since

$$\bigcup_{j=1}^{h} (m_f + M_j) = m_f + \bigcup_{j=1}^{h} M_j = m_f + M,$$

by Lemma 3.1 we have $m_f + M \equiv M \pmod{n}$, $f = 1, 2, \ldots, l$. \qed

**Remark.** If the condition "$m_1, \ldots, m_l$ are $l$ different nonnegative integers" in Proposition 3.5 is replaced by "$m_1, \ldots, m_l$ are $l$ different integers," the proposition is still true.

4. $\mathcal{L}_n$-RELATION IN $C_n(R)$

We now recall some concepts for a semigroup $S$ (they can be found in [5]). For a general semigroup $S$, there are five Green's relations $\mathcal{L}$, $\mathcal{R}$, $\mathcal{D}$, $\mathcal{H}$, and $\mathcal{I}$ for $S$. It can be easily proved that, for a commutative semigroup, we have $\mathcal{L} = \mathcal{R} = \mathcal{D} = \mathcal{H} = \mathcal{I}$. Since $C_n(R)$ is commutative, all the Green's relations in $C_n(R)$ coincide with each other. So it is sufficient to discuss the Green's relation $\mathcal{L}$ in this paper.

Let $n \geq 2$ be a positive integer. In this section, Proposition 3.5 in Section 3 will be applied to discuss the Green's relation $\mathcal{L}_n$ in $C_n(R)$. A necessary and sufficient condition on $\mathcal{L}_n$ is given. The condition is characterized by the properties of integers in $\text{SN}(A)$. For the special case of $R = E$, it is exactly the result of Butler and Schwarz in [6]. First, some properties on $C_n(R)$ (or $C_n$) are discussed as preparation for the main investigation.

For convenience, we recall some results on semigroup theory in the following (see [5]).

Let $S$ be a semigroup (it need not contain the identity element), and $a, b \in S$. Then

(i) if $a \in Sb$ and $b \in Sa$, then $a \mathcal{L} b$;

(ii) if $a \neq b$, then $a \mathcal{L} b$ if and only if $a \in Sb$ and $b \in SA$.

Let $R \neq Z$ be a fixed element in $C_n$. For convenience, assume $\text{SN}(R) = [k_1, \ldots, k_l]$ throughout this paper.
Lemma 4.1. Let $Z \neq A$, $Q \in C_n$. Then the following are equivalent:

1. $QA = A$;
2. $SN(Q) + SN(A) \equiv SN(A) \pmod{n}$;
3. for every $a \in SN(Q)$, $a + SN(A) \equiv SN(A) \pmod{n}$;
4. for every $a \in SN(Q)$, $P^aA = A$.

Proof. (1) $\Rightarrow$ (2): Since $P^i = P^j$ is and only if $i \equiv j \pmod{n}$, by the unique representation (1.1) of any nonzero element in $C_n$ we have $SN(QA) \equiv SN(Q) + SN(A) \pmod{n}$. So (2) holds.

(2) $\Rightarrow$ (3): For every $a \in SN(Q)$, obviously $a + SN(A) \subseteq SN(A) \pmod{n}$. Since any two integers in $a + SN(A)$ and $SN(A)$ are not congruent to each other modulo $n$, and $|a + SN(A)| = |SN(A)|$, it must follow $a + SN(A) \equiv SN(A) \pmod{n}$.

(3) $\Rightarrow$ (4): For every $a \in SN(Q)$, since $SN(P^aA) \equiv a + SN(A) \equiv SN(A) \pmod{n}$, we have $P^aA = A$.

(4) $\Rightarrow$ (1): Since $P^aA = A$ for every $a \in SN(Q)$, we have

$$A = \sum_{a \in SN(Q)} P^aA = \left( \sum_{a \in SN(Q)} P^a \right) A = QA.$$ 

Proposition 4.2. There exists an identity element in $C_n(R)$ if and only if $|SN(R)| = 1$.

Proof. "Only if": Assume $|SN(R)| \geq 2$ and

$$T = \sum_{q \in SN(T)} P^q$$

is an identity element of $C_n(R)$. Then $RT = E$. By Lemma 4.1, for $q \in SN(T)$, we have

$$q + k_i \equiv 0 \pmod{n}, \quad i = 1, 2, \ldots, l.$$ 

This implies $k_1 \equiv k_2 \pmod{n}$, but that is impossible.

"If": If $|SN(R)| = 1$, then $R = P^k$. Clearly $I = P^{n-k}$ is an identity element of $C_n(R)$.

Lemma 4.3 (Kim Ki-Hang Butler and Stefan Schwarz [6]). If $A, B \in C_n$, then $A \not\subseteq B$ if and only if there exists an element $P^m \in C_n$ such that $B = P^mA$.

For any $Z \neq R \in C_n$, it is obvious that $A \not\subseteq R B$ implies $A \not\subseteq B$. Hence, it is necessary for $A \not\subseteq_R B$ that there exists $P^m$ such that $B = P^mA$. For this
reason, the following question is considered in this section:
Let $Z \neq A \in C_n(R)$. What is the necessary and sufficient condition for $P^mA \mathcal{L}_R A$ for all $0 \leq m \leq n - 1$?
Clearly, if $A = Z$ or $H$, $P^mA \mathcal{L}_R A$ holds for $0 \leq m \leq n - 1$. Hence, the above question will be discussed for the case of $A \neq Z, H$.

**Lemma 4.4.** Let $Z \neq A \in C_n(R)$. Then $P^kA = A$ for all $0 \leq k \leq n - 1$ if and only if $A = H$.

**Proof.** "Only if": If $P^kA = A$ for all $0 \leq k \leq n - 1$, then

$$A = (E + P + P^2 + \cdots + P^{n-1}) A = HA = H.$$ 

"If": This is obvious. \hfill \blacksquare

**Lemma 4.5.** Let $Z, H \neq A \in C_n(R)$. Then the following are equivalent:

1. $A \in C_n(R) * A$.
2. For all $0 \leq m \leq n - 1$, $P^mA \mathcal{L}_R A$.
3. There exists $m_0$, $0 \leq m_0 \leq n - 1$, such that $A \neq P^{m_0}A$ and $P^{m_0}A \mathcal{L}_R A$.

**Proof.** (1) $\Rightarrow$ (2): If $A \in C_n(R) * A$, then there exists $C \in C_n(R)$ such that $A = CRA$. For any $0 \leq m \leq n - 1$, since $P^mA = (P^mC)RA = (P^mC) * A$, hence $P^mA \in C_n(R) * A$. On the other hand, $A = (P^{n-m}C)R(P^mA) = (P^{n-m}C) * (P^mA)$, and this implies $A \in C_n(R) * P^mA$. Hence $P^mA \mathcal{L}_R A$ for all $0 \leq m \leq n - 1$.

(2) $\Rightarrow$ (3): By the hypothesis $A \neq Z, H$ and Lemma 4.4, there exists $m_0$, $1 \leq m_0 \leq n - 1$, such that $A \neq P^{m_0}A$. By (2), then (3) holds.

(3) $\Rightarrow$ (1): Since $A \neq P^{m_0}A$ and $P^{m_0}A \mathcal{L}_R A$, we have $A \in C_n(R) * (P^{m_0}A)$, and then $A \in C_n(R) * A$. Hence (1) holds. \hfill \blacksquare

**Theorem 4.6.** Let $Z, H \neq A \in C_n(R)$, and $\text{sn}(R) = [k_1, \ldots, k_l]$. Then the following are equivalent:

1. For all $0 < m < n - 1$, $P^mA \mathcal{L}_R A$.
2. There exists a nonnegative integer $q$ such that, for $d = (q + k_1, \ldots, q + k_l, n)$ and $n = sd$,

$$\text{sn}(A) = M_1 \cup \cdots \cup M_h,$$

where $M_i \cup M_j = \emptyset$ whenever $i \neq j$, $M_j$ ($j = 1, 2, \ldots, h$) is an arithmetic series with common difference $d$, and $|M_1| = \cdots = |M_h| = s$. 

Proof. Suppose \( A \neq P^{m_0}A \) for some \( m_0, 1 \leq m_0 \leq n - 1 \). By Lemma 4.5, (1) holds if and only if \( P^{m_0}A \preceq \mathcal{L}_R A \), and if and only if \( A \in C_n(R) \ast A \), i.e., there exists \( C \in C_n(R) \) such that \( A = CRA \). By Lemma 4.1, \( A \in C_n(R) \ast A \) if and only if there exists a nonnegative integer \( q \) such that \( A = P^qRA \), and if and only if there exists a nonnegative integer \( q \) such that \( q + k_i + \text{sn}(A) = \text{sn}(A) \pmod{n}, \quad i = 1, 2, \ldots, l. \) (4.5.1)

By Proposition 3.5, there exists a nonnegative integer \( q \) such that (4.5.1) holds if and only if (2) holds. The proof is completed.

Remarks.

(i) According to the proof of (1) \( \rightarrow \) (2) in Lemma 4.5, (2) \( \rightarrow \) (1) in Theorem 4.5 still holds without the condition \( A \neq H \).

(ii) When \( A = H \), it is possible to choose a nonnegative integer \( q \) such that \( (q + k_1, \ldots, q + k_l, n) = 1 \), and \( \text{sn}(A) \) is an arithmetical series with common difference 1 and \( |\text{sn}(A)| = n \). Hence, (2) holds.

(i) and (ii) show that Theorem 4.5 is still true without the condition \( A \neq H \).

According to Lemma 4.4 and Theorem 4.6. The following theorem on \( \mathcal{L}_R \)-classes is true.

**Theorem 4.7.** Let \( A \in C_n(R) \). Then either \( \mathcal{L}_R(A) = \{A\} \) or \( |\mathcal{L}_R(A)| \geq 2 \) with \( \mathcal{L}_R(A) = \{A, PA, \ldots, P^{n-1}A\} \).

**Example 4.1.** Let \( n = 18 \) and \( R = E + P^3 + P^6 + P^9 + P^{15} \). Suppose \( A = P + P^2 + P^4 + P^5 + P^7 + P^8 + P^{10} + P^{11} + P^{13} + P^{14} + P^{16} + P^{17} \).

Choose \( q = 3 \). For

\[
d = (3 + 0, 3 + 3, 3 + 6, 3 + 9, 3 + 15, 18) = 3 \quad \text{and} \quad n = 6d,
\]

we have

\[
\text{sn}(A) = \{1, 4, 7, 10, 13, 16\} \cup \{2, 5, 8, 11, 14, 17\}.
\]

Here \( M_1 = \{1, 4, 7, 10, 13, 16\} \) and \( M_2 = \{2, 5, 8, 11, 14, 17\} \) are two arith-
metrical series with common difference \( d = 3 \) and \( |M_1| = |M_2| = 6 \). By Theorem 4.6, \( \mathcal{S}_R(A) = \{A, PA, \ldots, P^{17}A\} \). By calculating, \( \mathcal{S}_R(A) = \{A, PA, P^2A\} \) and \( |\mathcal{S}_R(A)| = 3 \).

In the following, several special cases for Theorem 4.6 are discussed.

Case 1. Suppose \( |\text{SN}(R)| = 1 \) and \( \text{SN}(R) = \{k\} \). For arbitrary \( A \in C_n(R) \), let \( \text{SN}(A) = \{n_1, \ldots, n_t\} \). Choose \( q = n - k \). For \( d = (q + k, n) = n \) and \( s = 1 \), \( \text{SN}(A) = \{n_1\} \cup \cdots \cup \{n_t\} \) is a union satisfying (2) of Theorem 4.6. This shows that \( \mathcal{S}_R(A) = \{A, PA, \ldots, P^{n-1}A\} \) for all \( A \in C_n(R) \), and leads to the following corollary.

**Corollary 4.8.** Let \( R = P^k \) \((0 \leq k \leq n - 1)\). If \( A, B \in C_n(R) \), then \( A \mathcal{S}_R B \) if and only if \( B = P^mA \) for some \( P^m \in C_n(R) \).

When \( k = 0 \), Corollary 4.9 coincides with Lemma 4.3, which is due to Butler and Schwarz [6].

Case 2. Suppose \( n \) is a prime and \( |\text{SN}(A)| \geq 2 \). For any nonnegative integer \( q \), since \( |\text{SN}(A)| \geq 2 \), we have \( d = (q + k_1, \ldots, q + k_t, n) = 1 \) and \( s = n \) \((n = sd)\). This shows that for any \( Z, H \neq A \in C_n(R) \), \( A \) cannot satisfy condition (2) of Theorem 4.6. By Lemma 4.5, all the \( \mathcal{S}_R \)-classes in \( C_n(R) \) are trivial, i.e., \( \mathcal{S}_R(A) = \{A\} \) for all \( A \in C_n(R) \).

Case 3. Suppose \( |\text{SN}(A)| \geq 2 \) and \( (k_i - k_j, n) = 1 \) for some \( k_i, k_j \in \text{SN}(R) \). By the same reasoning as the discussion in Case 2, all the \( \mathcal{S}_R \)-classes in \( C_n(R) \) are trivial.

5. IDEMPOTENT ELEMENTS IN \( C_n(R) \)

Let \( S \) be a semigroup and \( a \in S \). Then \( a \) is said to be an idempotent element of \( S \) if \( a^2 = a \). In this section, the structure theorems for the nonzero idempotent elements of \( C_n(R) \) are given.

**Lemma 5.1.** Let \( k \) be a positive integer, and \( B_1, \ldots, B_k, A \) be \( k + 1 \) nonzero elements in \( C_n(R) \). Then the following are equivalent:

1. \( B_1 \cdots B_k A = A \);
2. \( \Sigma_{i=1}^k \text{SN}(B_i) + \text{SN}(A) \equiv \text{SN}(A) \pmod{n} \);
3. for any \( b_i \in \text{SN}(B_i) \), \( i = 1, 2, \ldots, k \), one has \( (\Sigma_{i=1}^k b_i) + \text{SN}(A) \equiv \text{SN}(A) \pmod{n} \).
Proof. (1) $\Rightarrow$ (2): When $k = 1$, this is true by Lemma 4.1. Since
\[
\sum_{i=1}^{k} SN(B_i) \equiv SN(B_1, \cdots, B_k) \pmod{n}
\]
for any positive integer $k$, statement (2) holds by induction on $k$.

(2) $\Rightarrow$ (3): For any $b_i \in SN(B_i)$, $i = 1, 2, \ldots, k$, by (2), we have $(\sum_{i=1}^{k} b_i) + SN(A) \subseteq SN(A) \pmod{n}$. Since no two integers in $\sum_{i=1}^{k} b_i + SN(A)$ are congruent modulo $n$, and no two integers in $SN(A)$ are congruent modulo $n$, we have $|\sum_{i=1}^{k} b_i + SN(A)| = |SN(A)|$. This implies $(\sum_{i=1}^{k} b_i) + SN(A) = SN(A) \pmod{n}$.

(3) $\Rightarrow$ (1): For any $b_i \in SN(B_i)$, $i = 1, 2, \ldots, k$, since
\[
SN(P_{\sum_{i=1}^{k} b_i} A) \equiv SN(P_{\sum_{i=1}^{k} b_i} A) + SN(A) \equiv \sum_{i=1}^{k} b_i + SN(A) \equiv SN(A) \pmod{n},
\]
we have $P_{\sum_{i=1}^{k} b_i} A = A$. Hence, we have
\[
A = \sum_{b_i \in SN(B_i)} \cdots \sum_{b_k \in SN(B_k)} (P_{\sum_{i=1}^{k} b_i} A)
= \sum_{b_1 \in SN(B_1)} \cdots \sum_{b_k \in SN(B_k)} (P^{b_1} P^{b_2} \cdots P^{b_k} A)
= \left(\sum_{b_1 \in SN(B_1)} P^{b_1}\right) \cdots \left(\sum_{b_k \in SN(B_k)} P^{b_k}\right) A
= B_1 \cdots B_k A.
\]

Lemma 5.2. Let $Z \neq I \in C_n(R)$ and $SN(I) = \{n_1, \ldots, n_t\}$. Then the following are equivalent:

1. $I$ is an idempotent element in $C_n(R)$;
2. For $d = (\cdots, n_\mu + k_\nu, \ldots, n)$ and $n = sd$, one has $SN(I) = M_1 \cup \cdots \cup M_h$, where $M_i \cap M_j = \emptyset$ whenever $i \neq j$, $M_j (j = 1, 2, \ldots, h; h \geq 1)$ is an arithmetic series with common difference $d$, and $|M_1| = \cdots = |M_h| = s$.

---

1. The greatest common divisor $d$ of $n$ and $n_\mu + k_\nu$ ($\mu = 1, 2, \ldots, t; \nu = 1, 2, \ldots, l$) is indicated by $d = (\ldots, n_\mu + k_\nu, \ldots, n)$. Throughout the rest of this paper, this notation will be used.
Proof. I being an idempotent element in \( C_n(R) \) means \( IRI = I \). By Lemma 5.1, \( I = IRI \) if and only if

\[
n_{\mu} + k_\nu + \text{sn}(I) \equiv \text{sn}(I) \pmod{n} \quad (\mu = 1, 2, \ldots, t; \nu = 1, 2, \ldots, l).
\]

(5.2.1)

By proposition 3.5, (5.2.1) holds if and only if (2) holds.

**Theorem 5.3.** Let \( Z \neq I \in C_n(R) \) and \( \text{sn}(I) = [n_1, \ldots, n_t] \). Then the following are equivalent:

1. \( I \) is an idempotent element in \( C_n(R) \).
2. \( \text{sn}(I) = [n_1, \ldots, n_t] \).

Proof. (1) \( \Rightarrow \) (2): Suppose \( I \) is an idempotent element in \( C_n(R) \). By Lemma 5.2, for \( d = (\ldots, n_{\mu} + k_\nu, \ldots, n) \) and \( n = sd \), we have \( \text{sn}(I) = M_1 \cup \cdots \cup M_h \), where \( M_i \cap M_j = \emptyset \) whenever \( i \neq j \), \( M_j \) \((j = 1, 2, \ldots, h; h \geq 1)\) is an arithmetic series with common difference \( d \), and \( |M_1| = \cdots = |M_h| = s \). We will prove \( h = 1 \). Suppose \( h \geq 2 \). Let

\[
M_1 = \{n_{i1}, n_{i1} + d, \ldots, n_{i1} + (s - 1)d\} \quad \text{and} \quad M_2 = \{n_{i2}, n_{i2} + d, \ldots, n_{i2} + (s - 1)d\},
\]

where \( n_{i1}, n_{i2} \in \text{sn}(I) \). Since \( d \) is a common divisor of \( n_{i1} + k_1, n_{i2} + k_1 \), and \( n \), by Lemma 3.4 we have \( n_{i1} + k_1 + M_1 \equiv M_1 \pmod{n} \) and \( n_{i2} + k_1 + M_2 \equiv M_2 \pmod{n} \). These show that there exist integers \( a \) and \( b \), \( 0 \leq a, b \leq s - 1 \), such that

\[
n_{i1} + k_1 + (n_{i1} + ad) \equiv n_{i1} \pmod{n} \quad \text{and} \quad n_{i2} + k_1 + (n_{i2} + bd) \equiv n_{i2} \pmod{n}.
\]

These imply \( n_{i1} + ad \equiv n_{i2} + bd \pmod{n} \). Since \( 0 \leq n_{i1} + ad, n_{i2} + bd \leq n - 1 \), it follows that \( n_{i1} + ad = n_{i2} + bd \). This implies \( n_{i1} \in M_2 \), i.e., \( M_1 \cap M_2 \neq \emptyset \), which contradicts \( M_1 \cap M_2 = \emptyset \). Hence, \( h = 1 \), and it follows that \( s = t \). Therefore, (2) holds.

(2) \( \Rightarrow \) (1): This is the conclusion of Lemma 5.2.
SANDWICH SEMIGROUP

**Theorem 5.4 (The first structure theorem for idempotent elements).** Suppose \( 0 \in \text{sn}(R) \). Let \( d \) be a positive common divisor of \( k_1, \ldots, k_t, n \) and \( n = td \). Then

\[
I = E + p^d + p^{2d} + \cdots + p^{(t-1)d}
\]

is a nonzero idempotent element in \( C_n(R) \). All the nonzero idempotent elements in \( C_n(R) \) are obtained in this manner.

**Proof.**

(a) If \( t = 1 \) and \( d = n \), it follows that \( |\text{sn}(R)| = 1 \). Since \( 0 \in \text{sn}(R) \), we have \( R = E \). Clearly, \( I = E \) is an idempotent element in \( C_n(E) \). Suppose \( t \geq 2 \) (then \( d < n \)). Clearly, \( \text{sn}(I) = [0, d, 2d, \ldots, (t-1)d] \). Let

\[
d' = (\ldots, (\mu - 1)d + k_v, \ldots, n).
\]

Since \( d'|k_1 \) and \( d'|d + k_1 \), we have \( d'|d \). Since \( d \) is a positive common divisor of \( n \) and \( (\mu - 1)d + k_v \) (\( \mu = 1, 2, \ldots, t; v = 1, 2, \ldots, l \)), we have \( d|d' \). Therefore, \( d = d' \). Since \( \text{sn}(I) \) is an arithmetic series with common difference \( d \), \( n = td \), and \( |\text{sn}(I)| = t \), it follows by Theorem 5.3 that \( I \) is an idempotent element in \( C_n(R) \).

(b) Conversely, let \( I \) be an arbitrary nonzero idempotent element in \( C_n(R) \). By Theorem 5.3, for some nonnegative integer \( c \) we have

\[
\text{sn}(I) = [c, c + d, \ldots, c + (t - 1)d],
\]

where \( d = (\ldots, c + (\mu - 1)d + k_v, \ldots, n) \) and \( n = td \). Since \( 0 \in \text{sn}(R) \), we have \( d|c \). Let \( c = rd \), where \( r \) is a nonnegative integer. Because \( c + (t - 1)d = (r + t - 1)d < n = td \), we have \( (r - 1)d < 0 \). This shows \( r < 1 \). Hence, \( r = 0 \), and then \( c = 0 \). Therefore, \( \text{sn}(I) = [0, d, 2d, \ldots, (t - 1)d] \), where \( n = td \) and \( d \) is a positive common divisor of \( k_1, \ldots, k_t, n \). The proof is completed.

The following corollary is an immediate conclusion of Theorem 5.4.

**Corollary 5.5.** If \( 0 \in \text{sn}(R) \), there exist exactly \( d^*(k_1, \ldots, k_t, n) \) different nonzero idempotent elements in \( C_n(R) \).

**Remark.** For the case of \( \text{sn}(R) = \{0\} \), Theorem 5.4 coincides with the result of Butler and Schwarz in [6].
If \( 0 \in \text{sn}(R) \), according to Theorem 5.4, we can find out all the nonzero idempotent elements in \( C_n(R) \). This can be demonstrated by the following example.

**Example 5.1.** Let \( n = 30 \) and \( R = E + P^6 + P^{12} + P^{18} + P^{24} \). Then \( \text{sn}(R) = [0, 6, 12, 18, 24] \). All the positive common divisors of 0, 6, 12, 18, 24, 30 are 1, 2, 3, and 6. By Theorem 5.4, there exist exactly four nonzero idempotent elements in \( C_n(R) \) as follows:

\[
I_1 = H, \quad I_2 = E + P^2 + P^4 + \cdots + P^{28}, \\
I_3 = E + P^3 + P^6 + \cdots + P^{27}, \quad I_4 = E + P^6 + P^{12} + \cdots + P^{24}.
\]

In the following, we discuss the idempotent elements in \( C_n(R) \) for the general case [without the condition \( 0 \in \text{sn}(R) \)].

**Lemma 5.6.** Let \( I \in C_n(R) \). If \( \text{sn}(I) = [0, d, 2d, \ldots, (t-1)d] \), where \( d \) is a positive common divisor of \( k_1, \ldots, k_i, n \) and \( n = td \), then \( I \) is an idempotent element in \( C_n(R) \).

**Proof.** The proof is the same as part (a) of the proof of Theorem 5.4. ■

**Theorem 5.7.** There exist exactly \( d^+(k_1, \ldots, k_i, n) \) different nonzero idempotent elements \( I \) in \( C_n(R) \) satisfying \( 0 \in \text{sn}(I) \).

**Proof.** By Lemma 5.6, there exist at least \( d^+(k_1, \ldots, k_i, n) \) different nonzero idempotent elements \( I \) in \( C_n(R) \) satisfying \( 0 \in \text{sn}(I) \). Conversely, let \( I \) be a nonzero idempotent element in \( C_n(R) \) satisfying \( 0 \in \text{sn}(I) \). By Theorem 5.3, we have

\[
\text{sn}(I) = [0, d, 2d, \ldots, (t-1)d],
\]

where \( d = (\ldots, (\mu - 1)d + k_\mu, \ldots, n) \) and \( n = td \). Obviously, \( d \) is a positive common divisor of \( k_1, \ldots, k_i, n \). This shows that each nonzero idempotent element \( I \) in \( C_n(R) \) satisfying \( 0 \in \text{sn}(I) \) corresponds to a positive common divisor of \( k_1, \ldots, k_i, n \). Combining the above discussion, we have proved this theorem. ■

**Theorem 5.8.** Let \( Z \neq I \in C_n(R) \) and \( 0 \notin \text{sn}(I) \). Then the following are equivalent:

1. \( I \) is an idempotent element in \( C_n(R) \).
2. There exists an integer \( c (0 < c < n) \) such that, for a positive common
Proof. (1) ⇒ (2): Suppose I is an idempotent element in $C_n(R)$. By Theorem 5.3, there exists $c(0 < c < n)$ such that, for

$$d = (\ldots, c + (\mu - 1)d + k_\nu, \ldots, n)$$

and $n = td$.

SN(I) = [c, c + d, \ldots, c + (t - 1)d].$ Since $0 \notin SN(I)$, we have $0 < c < n$.

Obviously, $d$ is a positive common divisor of $c + k_1, \ldots, c + k_\nu, n$.

(2) ⇒ (1): If $t = 1$ and $d = n$, then $SN(I) = [c]$. Since $n$ is a common divisor of $c + k_1, \ldots, c + k_\nu, 0 < c < n$, and $0 < k_1 < k_2 < \ldots < k_\nu < n$, we have $|SN(R)| = 1$. Therefore, $SN(R) = [k_1]$ and $c + k_1 = n$, i.e., $R = P^{k_1}$ and $I = P^c$. Then $IRI = P^{c+k_1+c} = P^c = I$, and $I$ is an idempotent element in $C_n(R)$.

Suppose $t > 2 (d < n)$. Let

$$d' = (\ldots, c + (\mu - 1)d + k_\nu, \ldots, n).$$

Since $t > 2$, $d'$ is a common divisor of $c + k_1$ and $c + d + k_1$. This shows $d'|d$. Because $d$ is a common divisor of $c + k_1, \ldots, c + k_\nu, n$, $d$ is also a common divisor of $c + (\mu - 1)d + k_\nu (\mu = 1, 2, \ldots, t; \nu = 1, 2, \ldots, l)$. This shows $d|d'$. Since $d > 0$, $d = d'$. By Theorem 5.3, $I$ is an idempotent element in $C_n(R)$.

Theorem 5.9 (The second structure theorem for idempotent elements). Let $g = (\ldots, k_\mu - k_\nu, \ldots, n)$ and $c$ be an integer satisfying $0 < c < g$. Let $d$ be a positive common divisor of $c + k_1, \ldots, c + k_\nu, n$ and $n = td$. Then

$$I = P^c + P^{c+d} + P^{c+2d} + \ldots + P^{c+(t-1)d}$$

is a nonzero idempotent element in $C_n(R)$. All the nonzero idempotent elements in $C_n(R)$ are obtained in this manner.

Proof.

(a) If $c = 0$, then by Lemma 5.6, $I = E + P^d + P^{2d} + \ldots + P^{(t-1)d}$ (where $d$ is a positive common divisor of $k_1, \ldots, k_\nu, n$ and $n = td$) is an idempotent element in $C_n(R)$. Suppose $0 < c < g$. If $c + (t - 1)d < n$, then $SN(I) = [c, c + d, \ldots, c + (t - 1)d]$ and $I$ satisfy the conditions of Theorem 5.8. Therefore, $I$ is an idempotent element in $C_n(R).$ If $c + (t -$
1) $d \geq n$, let $q (0 \leq q < t - 1)$ be the greatest integer such that $c + qd < n$, i.e., $c + qd < n$ but $c + (g + 1)d \geq n$. Indicating $c' = c - (t - q - 1)d$, we have $c' \geq 0$. Since $n = td$, it is easy to prove

$$\{c', c' + d, \ldots, c' + (t - 1)d\} \equiv \{c, c + d, \ldots, c + (t - 1)d\} \pmod{n}.$$  

This means

$$I = p^{c'} + p^{c'+d} + p^{c'+2d} + \cdots + p^{c'+(t-1)d}.$$  

Because $c' \geq 0$ and $c' + (t - 1)d < n$, we have $\text{sn}(I) = [c', c' + d, \ldots, c' + (t - 1)d]$. If $c' = 0$, then by Lemma 5.6, $I$ is an idempotent element in $C_n(R)$. If $c' > 0$, then $0 \notin \text{sn}(I)$. Since $d$ is also a positive common divisor of $c' + k_1, \ldots, c' + k_t, n$, by Theorem 5.8 $I$ is an idempotent element in $C_n(R)$.

(b) Conversely, let $I$ be a nonzero idempotent element in $C_n(R)$. If $0 \notin \text{sn}(I)$, then by the proof of Theorem 5.7, $\text{sn}(I) = [0, d, 2d, \ldots, (t - 1)d]$, where $d$ is a positive common divisor of $k_1, k_2, \ldots, k_t, n$ and $n = td$. If $0 \in \text{sn}(I)$, by Theorem 5.8, there exists an integer $c (0 < c < n)$ such that, for a positive common divisor $d$ of $c + k_1, \ldots, c + k_t, n$ and $n = td$, $\text{sn}(I) = [c, c + d, \ldots, c + (t - 1)d]$. Since $d$ is also a common divisor of $n$ and $k_\mu - k_\nu (\mu, \nu = 1, 2, \ldots, t)$, we have $d | g$. Hence $d \leq g$. Since $c + (t - 1)d < n$, we have $c < d$. Therefore, $0 < c < g$. The proof is completed.

The idempotent element obtained in Theorem 5.9 is denoted by $I(c, d)$. Obviously, $I(c, 1) = H$ for any possible $c$.

**Lemma 5.10.** In $C_n(R)$, $I(c, d) = I(c', d')$ if and only if $d = d'$.

**Proof.** “Only if”: Suppose $I(c, d) = I(c', d')$. Since $\text{sn}(I(c, d)) = \text{sn}(I(c', d'))$, we have $t = t'(n - td - t'd')$, and then $d = d'$.

“If”: Let $n = td$. By Theorem 5.9, we have $c + k_1 \equiv 0 \pmod{d}$ and $c' + k_1 \equiv 0 \pmod{d}$. Hence $c \equiv c' \pmod{d}$. Therefore, it is easy to prove

$$\{c, c + d, \ldots, c + (t - 1)d\} \equiv \{c', c' + d, \ldots, c' + (t - 1)d\} \pmod{n}.$$  

This shows $\text{sn}(I(c, d)) = \text{sn}(I(c', d'))$, i.e., $I(c, d) = I(c', d')$.

**Lemma 5.11.** If $g = (\ldots, k_\mu - k_\nu, \ldots, n)$, then for any positive divisor $d$ of $g$, there exists an integer $c, 0 \leq c < g$, such that $I(c, d)$ which is obtained in the manner of Theorem 5.9 is an idempotent element in $C_n(R)$.  


Proof. It is sufficient to prove that, for any positive divisor \( d \) of \( g \), there exists an integer \( c \), \( 0 < c < g \), such that \( d \) is a common divisor of \( c + k, \ldots, c + k_i, n \). Choosing \( c \) to be the least nonnegative integer such that \( c + k_1 \equiv 0 \pmod{d} \), we can prove \( 0 < c < g \). Suppose the contrary, and assume \( g \leq c \). Let \( c = qg + r \), where \( q \) and \( r \) are nonnegative integers satisfying \( 0 \leq r < g \). Clearly, it follows that \( c > r \). On the other hand, \( c + k_1 = qg + k_1, \ d \mid g, \) and \( d \mid c + k_1 \) imply \( r + k_1 \equiv 0 \pmod{d} \). This contradicts the choice of \( c \). Hence, \( 0 \leq c < g \). For any \( k_i \in \text{SN}(R) \), since \( k_i - k_1 \equiv 0 \pmod{n} \), we have \( c + k_i \equiv c + k_1 \equiv 0 \pmod{n} \). This shows that \( d \) is a common divisor of \( c + k_1, \ldots, c + k_i, n \). Therefore, we can obtain the idempotent element \( I(c, d) \) in \( C_n(R) \) in the manner of Theorem 5.9.

The set of all the idempotent elements in \( C_n(R) \) is denoted by \( \text{Id}(C_n(R)) \). We have the following counting theorem on \( \text{Id}(C_n(R)) \).

**Theorem 5.12.** Let \( n \) be a positive integer and \( Z \neq R \subseteq C_n \). If \( g = (\ldots, k_\mu - k_v, \ldots, n) \), then \( |\text{Id}(C_n(R))| = d^+(g) + 1 \).

Proof. By Theorem 5.9, Lemma 5.10, and Lemma 5.11, the number of nonzero idempotent elements in \( C_n(R) \) is exactly \( d^+(g) \). Clearly, \( Z \) is also an idempotent element in \( C_n(R) \).

According to Theorem 5.9, Lemma 5.10, Lemma 5.11, and Theorem 5.12, we can find out all the idempotent elements in \( C_n(R) \) for any \( Z \neq R \subseteq C_n \). The proof of Lemma 5.11 tells us how to compute every idempotent element. An algorithm for obtaining all the idempotent elements in \( C_n(R) \) is given as follows.

**Algorithm.** Let \( n \) be a positive integer and \( \text{SN}(R) = [k_1, \ldots, k_\mu] \).

\begin{itemize}
  \item **Step 1.** Compute \( g = (\ldots, k_\mu - k_v, \ldots, n) \).
  \item **Step 2.** Compute all positive divisors of \( g \), say \( d_1, \ldots, d_\ell \).
  \item **Step 3.** Compute all positive integers \( t_i \) such that \( n = t_i d_i \) (\( i = 1, 2, \ldots, k \)), say \( t_1, \ldots, t_k \).
  \item **Step 4.** Compute all the least nonnegative integers \( c_i \) such that \( c_i - k_1 \equiv 0 \pmod{d_i} \) (\( i = 1, 2, \ldots, k \)), say \( c_1, \ldots, c_k \).
  \item **Step 5.** Form all idempotent elements of

\[
\text{Id}(C_n(R)) = \{Z\} \cup \left\{ I(c_i, d_i) = \sum_{e=0}^{t_i-1} p^{c_i+ed_i} \mid i = 1, 2, \ldots, k \right\}.
\]
\end{itemize}
Example 5.2. Let \( n = 60 \) and \( R = P^{17} + P^{20} \). We will determine all the idempotent elements in \( C_n(R) \).

Step 1: \( g = (29 - 17, 60) = 12 \).

Step 2: All the positive divisors \( d_i \) of 12 are \( \{1, 2, 3, 4, 6, 12\} \).

Step 3: All the positive integers \( t_i \) such that \( n = t_id_i \) are \( \{60, 30, 20, 15, 10, 5\} \).

Step 4: All the least nonnegative integers \( c_i \) such that \( c_i + k_1 = 0 \pmod{d_i} \) are \( \{0, 1, 1, 3, 1, 7\} \).

Step 5: \( \text{Id}(C_n(R)) = \{Z, I(0, 1) = H, I(1, 2), I(1, 3), I(3, 4), I(1, 6), I(7, 12)\} \), where

\[
I(1, 2) = P + P^3 + P^5 + \cdots + P^{59}, \quad I(1, 3) = P + P^4 + P^7 + \cdots + P^{58},
\]

\[
I(3, 4) = P^3 + P^7 + P_{11} + \cdots + P^{59}.
\]

\[
I(1, 6) = P + P^7 + P^{13} + \cdots + P^{55}, \quad \text{and}
\]

\[
I(7, 12) = P^7 + P^{19} + P^{31} + \cdots + P^{55}.
\]

We obtain exactly \( d^+(12) = 6 \) nonzero idempotent elements in \( C_n(R) \).

6. MAXIMAL SUBGROUPS IN \( C_n(R) \)

Let \( I \) be an idempotent element in \( C_n(R) \). The maximal subgroup of \( C_n(R) \) containing \( I \) is denoted by \( G_I(R) \) (The definition of the maximal subgroup of a semigroup can be seen in [5].) In this section, we will investigate the structure of \( G_I(R) \). Since \( C_n(R) \) is commutative, all the Green's relations for \( C_n(R) \) coincide with each other. Therefore, for any idempotent element \( I \) in \( C_n(R) \) we have \( G_I(R) = \mathcal{L}_n^*(I) \).

Lemma 6.1. If \( I \) is an idempotent element in \( C_n(R) \), then for any \( k \), \( 0 \leq k \leq n - 1 \), one has \( P^kI \in \mathcal{L}_n^*(I) \).

Proof. If \( I = Z \), the conclusion is obviously true. Suppose \( I \neq Z \). It is sufficient to prove

\[
P^kI \in C_n(R) \ast I \text{ and } I \in C_n(R) \ast (P^kI), \quad 0 \leq k \leq n - 1. \quad (6.1.1)
\]

Since \( I = IRI \), we have \( P^kI = (P^kI)RI \) and \( I = (P^{n-k}I)R(P^kI) \). This shows that (6.1.1) is true.
For $A, B \in C_n(R)$, clearly, if $A$ and $B$ are $\mathcal{L}$-equivalent in $C_n(R)$, then $A$ and $B$ are $\mathcal{L}$-equivalent in $C_n$. According to Lemma 1 in [6] and Lemma 6.1, for any idempotent element $I$ in $C_n(R)$, we have $\mathcal{L}_n(I) = \{I, PI, \ldots, P^{n-1}I\}$.

**Theorem 6.2.** (Structure theorem for maximal subgroups). Let $I = I(c, d) = P^c + P^{c+d} + \cdots + P^{c+(t-1)d}$ be a nonzero idempotent element in $C_n(R)$ obtained in the manner of Theorem 5.9. Then

$$G_{\mathcal{I}}(R) = \{I, PI, \ldots, P^{d-1}I\} \quad \text{and} \quad |G_{\mathcal{I}}(R)| = d.$$  

**Proof.** By the above investigation, $G_{\mathcal{I}}(R) = \{I, PI, \ldots, P^{n-1}I\}$. Firstly, we prove that $P^iI \neq P^jI$ when $i \neq j$ and $0 \leq i, j \leq d - 1$. Assume $P^iI = P^jI$ for $i$ and $j$. $0 \leq i < j \leq d - 1$. Then $i + \text{SN}(I) \equiv j + \text{SN}(I) \pmod{n}$. Hence, there exists $a$ ($0 \leq a \leq t - 1$) such that $i + c \equiv j + c + ad \pmod{n}$. This shows $(j - i) + ad \equiv 0 \pmod{n}$. Since $0 \leq j - i < d, 0 \leq ad \leq (t - 1)d$, and $n = td$ it follows that $(j - i) + ad = 0$. Therefore, $j - i = 0$, i.e., $i = j$. This is impossible.

Secondly, we prove that for any $j$ ($d < j \leq n - 1$), there exists $i$ ($0 \leq i < d - 1$) such that $P^iI = P^jI$. Suppose $j = kd + i$ where $k$ and $i$ are nonnegative integers and $0 \leq i \leq d - 1$. Clearly,

$$\text{SN}(P^jI) \equiv j + \text{SN}(I)$$

$$= i + kd + \text{SN}(I)$$

$$\equiv i + \{c + kd, c + (k + 1)d, \ldots, c + (k + t - 1)d\} \pmod{n}.$$  

Since $n = td$, it is easy to prove

$$\{c, c + d, \ldots, c + (t - 1)d\}$$

$$\equiv \{c + kd, c + (k + 1)d, \ldots, c + (k + t - 1)d\} \pmod{n}.$$  

Hence,

$$\text{SN}(P^jI) \equiv i + \{c, c + d, \ldots, c + (t - 1)d\} \equiv i + \text{SN}(I) \pmod{n}.$$  

This shows $P^iI = P^jI$. 

Combining the above discussion, we conclude

\[ G_{I}(R) = \{ I, PI, \ldots, P^{d-1}I \} \quad \text{and} \quad |G_{I}(R)| = d. \]

According to Theorem 6.2, all the maximal subgroups of \( C_{n}(R) \) containing a nonzero idempotent element can be determined. Considering \( G_{Z}(R) \), there are exactly \( d^{+}(g) + 1 \) maximal subgroups in \( C_{n}(R) \), where \( g = (\ldots, k_{\mu} - k_{\nu}, \ldots, n) \). For example, in Example 5.2, six nonzero idempotent elements are obtained in \( C_{n}(R) \), where \( n = 60 \) and \( R = P^{17} + P^{19} \). So there are seven maximal subgroups in \( C_{n}(R) \) as follows:

\[ G_{Z}(R), G_{H}(R), G_{I(1,2)}(R), G_{I(1,3)}(R), G_{I(3,4)}(R), \]
\[ G_{I(1,6)}(R), \text{ and } G_{I(7,12)}(R). \]

The following theorem gives an answer for the problem about trivial maximal subgroups in \( C_{n}(R) \).

**Theorem 6.3.** For arbitrary \( Z \neq R \in C_{n} \), \( C_{n}(R) \) contains exactly two trivial maximal subgroups, which are \( G_{Z}(R) \) and \( G_{H}(R) \).

**Proof.** Let \( I = I(c, d) \) be a nonzero idempotent element determined in the manner of Theorem 5.9. If \( G_{I}(R) \) is trivial, then by Theorem 6.2, \( |G_{I}(R)| = d = 1 \). So \( I = P^{c} + P^{c+1} + P^{c+2} + \cdots + P^{c+(n-1)} \). It is easy to prove

\[ \{ c, c + 1, \ldots, c + (n - 1) \} \equiv \{ 0, 1, 2, \ldots, n - 1 \} \pmod{n}. \]

Hence \( I = E + P + P^{2} + \cdots + P^{n-1} = H \). Therefore, \( G_{Z}(R) \) and \( G_{H}(R) \) are the only trivial maximal subgroups in \( C_{n}(R) \).

7. REGULAR ELEMENTS IN \( C_{n}(R) \)

In this section, we will determine all the regular elements in \( C_{n}(R) \). Let \( S \) be a semigroup and \( a \in S \). Then \( a \) is said to be a regular element of \( S \) if \( axa = a \) for some \( x \in S \). By referring to [5], we can obtain:

(i) if \( A \in C_{n}(R) \) is regular, then all the elements in \( \mathcal{L}_{r}(A) \) are regular; 
(ii) \( A \in C_{n}(R) \) is regular if and only if \( \mathcal{L}_{r}(A) \) contains an idempotent element.
Theorem 7.1. Let \( A \in C_n(R) \). Then the following are equivalent:

1. \( A \) is a regular element in \( C_n(R) \).
2. There exist \( P^m \) and \( I \) in \( C_n(R) \), where \( I \) is an idempotent element of \( C_n(R) \), such that \( A = P^mI \).
3. There exists an idempotent element \( I \) of \( C_n(R) \) such that \( A \in C_I(R) \).

The set of all the regular elements in \( C_n(R) \) is denoted by \( \text{Reg}(C_n(R)) \).

Corollary 7.2. For \( C_n(R) \), the following is true:

1. \( \text{Reg}(C_n(R)) = \bigcup I \in \text{Id}(C_n(R)) C_I(R) \);
2. \( |\text{Reg}(C_n(R))| = 1 + \sum_{d \mid g, d > 0} d \), where \( g = (\ldots, k_m - k_l, \ldots, n) \).

Proof. (1) is the immediate result of Theorem 7.1.

(2): Since \( C_I(R) \cap C_{I'}(R) = \emptyset \) whenever \( I \neq I' \), by (1) we have

\[
|\text{Reg}(C_n(R))| = \sum_{I \in \text{Id}(C_n(R))} |C_I(R)| = 1 + \sum_{I \in \text{Id}(C_n(R)) \setminus \bigcup I} |C_I(R)|. \quad (7.2.1)
\]

By Theorem 6.2 and the Algorithm presented in Section 5, we claim

\[
\sum_{I \in \text{Id}(C_n(R)) \setminus \bigcup I} |C_I(R)| = \sum_{d \mid g, d > 0} d. \quad (7.2.2)
\]

(7.2.1) and (7.2.2) show that (2) holds.

According to Corollary 7.2, we can determine all the regular elements in \( C_n(R) \) by computing all the idempotent elements in \( C_n(R) \). For example, for \( C_6(R) \) where \( n = 60 \) and \( R = P^{17} + P^{29} \), we have \( g = (29 - 17, 60) = 12 \).

By Corollary 7.2,

\[
|\text{Reg}(C_n(R))| = 1 + \sum_{d \mid 12, d > 0} d = 29.
\]

So there exist exactly 29 regular elements in \( C_6(R) \) which are the matrices in all the maximal subgroups \( G_2(R), G_9(R), G_{9,1}(R), G_{9,1,3}(R), G_{9,1,4}(R), G_{9,1,6}(R), G_{9,12}(R) \).

The author thanks Professor Mou-Cheng Zhang and Professor Hans Schneider for their help and suggestions.
REFERENCES


*Received 28 January 1991; final manuscript accepted 27 December 1991*