Jinsong Chen; Yi Jia Tan

On the maximal subgroup of the sandwich semigroup of generalized circulant Boolean matrices

Czechoslovak Mathematical Journal, Vol. 56 (2006), No. 4, 1117–1129

Persistent URL: http://dml.cz/dmlcz/128134

Czechoslovak Mathematical Journal, 56 (131) (2006), 1117–1129

ON THE MAXIMAL SUBGROUP OF THE SANDWICH SEMIGROUP OF GENERALIZED CIRCULANT BOOLEAN MATRICES

Jinsong Chen, Yijia Tan, Fuzhou

(Received October 6, 2003)

Abstract. Let n be a positive integer, and $C_n(r)$ the set of all $n\times n$ r-circulant matrices over the Boolean algebra $B=\{0,1\}$, $G_n=\bigcup\limits_{r=0}^{n-1} C_n(r)$. For any fixed r-circulant matrix C ($C\neq 0$) in G_n, we define an operation "$*$" in G_n as follows: $A*B=ACB$ for any A,B in G_n, where ACB is the usual product of Boolean matrices. Then $(G_n,*)$ is a semigroup. We denote this semigroup by $G_n(C)$ and call it the sandwich semigroup of generalized circulant Boolean matrices with sandwich matrix C. Let F be an idempotent element in $G_n(C)$ and $M(F)$ the maximal subgroup in $G_n(C)$ containing the idempotent element F. In this paper, the elements in $M(F)$ are characterized and an algorithm to determine all the elements in $M(F)$ is given.

Keywords: generalized ciculant Boolean matrix, sandwich semigroup, idempotent element, maximal subgroup

MSC 2000: 15A33

1. Introduction and preliminaries

Let $B=\{0,1\}$ be the binary Boolean algebra. The matrices which we consider in this paper are $n\times n$ matrices over B, called *Boolean matrices*. Let r be a nonnegative integer. An $n\times n$ *r-circulant* (*generalized circulant*) *Boolean matrix* is an $n\times n$ matrix over B in which each row, except the first, is obtained from the preceding row by shifting the elements cyclically r columns to the right, i.e., $a_{ij}=a_{i-1,j-r}$ for $i,j=0,1,\ldots,n-1$, where the indices are reduced to their least nonnegative remainder modulo n.

This work was supported by the Natural science Foundation of Fujian Province (Z0511012) and Foundation to the Educational Committee of Fujian (JB05041), China.

Let P be $n \times n$ 1-circulant with the first row $(0,1,0,\ldots,0)$. Then an r-circulant matrix A with the first row $(a_0,a_1,\ldots,a_{n-1})$ can be written in the from

$$A = \sum_{i=0}^{n-1} a_i Q_r P^i,$$

where Q_r is the r-circulant matrix with the first row $(1,0,0,\ldots,0)$. Let $\Delta(A) = \{i\colon\ a_i = 1,\ 0 \leqslant i \leqslant n-1\}$ for the matrix $A = \sum\limits_{i=0}^{n-1} a_i Q_r P^i$. Then A can be rewritten in the form

$$A = Q_r \sum_{i\in\Delta(A)} P^i.$$

It is very easy to verify that the matrix A satisfies

$$PA = AP^r. \tag{1.1}$$

Let $C_n(r)$ denote the set of all $n \times n$ r-circulant Boolean matrices, and $G_n = \bigcup\limits_{r=0}^{n-1} C_n(r)$. Then $C_n(1)$ and G_n form semigroups, called *the semigroup of circulant Boolean matrices* and *the semigroup of generalized circulant Boolean matrices*, respectively, under matrix multiplication and using Boolean operations for the entries of matrices. For an arbitrary but fixed element $C \in G_n$ $(C \neq 0)$, we can define an operation "$*$" in G_n as follows: For any $A, B \in G_n$, $A * B = ACB$, where ACB is the usual product of Boolean matrices. It can be easily proved that G_n is also a semigroup under the operation "$*$". We denote this semigroup by $G_n(C)$ and call it a *sandwich semigroup of generalized circulant Boolean matrices with sandwich matrix* C.

Let S be a semigroup. A subgroup M of S is called a maximal subgroup of S if it is not properly contained in any other subgroup of S. Clifford and Preston proved that a subgroup M of S containing an idempotent F is a maximal subgroup of S if and only if $M = M(F)$ and

$$M(F) = \{A \in S\colon\ FA = AF = A,\ XA = AY = F,\ \text{ for some }\ X, Y \in S\} \tag{1.2}$$

(see [4], pp. 22–23). Montague and Plemmons [5] dealt with maximal subgroups of the semigroup of relations. Kim and Schwarz [6] obtained the description of maximal subgroups of the semigroup of circulant Boolean matrices. Zhang [3] gave some necessary and sufficient conditions for an r-circulant Boolean matrix to be an element of a maximal subgroup of G_n and generalized the corresponding results in [6]. The purpose of this paper is to describe the maximal subgroups of $G_n(C)$. The main results obtained in this paper are generalizations of the corresponding results in [3].

The following notions and lemmas are used.

Let $\mathbb{Z}$ denote the set of all integers, and $r \in \mathbb{Z}$, $U, V, W \subseteq \mathbb{Z}$. Let $U + V = \{u + v \colon u \in U, v \in V\}$, $rU = \{ru \colon u \in U\}$, $u + V = \{u\} + V$ and let $\sigma(U)$ be the greatest common divisor of the elements in U. Let n be a positive integer. U is said to be *included in V modulo n*, denoted by $U \subseteq V \pmod{n}$, if for each $u \in U$ there exists a $v \in V$ such that $u \equiv v \pmod{n}$. U is said to be *congruent to V modulo n*, denoted by $U \equiv V \pmod{n}$ if $U \subseteq V \pmod{n}$ and $V \subseteq U \pmod{n}$. Clearly, this congruence relation is reflexive, symmetric, and transitive (see [1]). Let $M = \{m_0, m_1, \ldots, m_{t-1}\}$ be a set of integers. $M \pmod{n}$ denotes the set $\{\overline{m_0}, \overline{m_1}, \ldots, \overline{m_{t-1}}\}$, where $0 \leqslant \overline{m_k} \leqslant n-1$, and $\overline{m_k} \equiv m_k \pmod{n}$ for $k = 0, 1, \ldots, t-1$. A set $M = \{m_0, m_1, \ldots, m_{t-1}\}$ of integers is called an *arithmetic progression modulo n* with common difference d if the elements of $M \pmod{n}$ constitute an arithmetic progressions with the same common difference d and $dt = n$. We denote $\bigcup\limits_{u=0}^{e-1} \{i_u, i_u + d, \ldots, i_u + (m-1)d\}$, the union of e arithmetic progressions with the same common difference d, by $\bigcup\{i_0, i_1, \ldots, i_{e-1}, n, d, m\}$ (see [3]). (n, r) will denote the greatest common divisor of n and r.

Remark. Any integer set $U = \{j_0, j_1, \ldots, j_{t-1}\} \subseteq \{0, 1, \ldots, n-1\}$ can be represented as a union of some arithmetic progressions modulo n with the same common difference. The union of arithmetic progressions modulo n with the smallest common difference d is called the *final form of U* and we denote d by $d_n(U)$. For example, let $n = 12$ and $U = \{0, 1, 3, 4, 6, 7, 9, 10\}$. Then $U = \{0\} \cup \{1\} \cup \{3\} \cup \{6\} \cup \{7\} \cup \{9\} \cup \{10\}$, in this case, $d = 12$ and $m = 1$, and $U = \{0, 6\} \cup \{1, 7\} \cup \{3, 9\} \cup \{4, 10\}$, in this case, $d = 6$ and $m = 2$. Also $U = \{0, 3, 6, 9\} \cup \{1, 4, 7, 10\}$, in this case, $d = 3$ and $m = 4$. Obviously, $\{0, 3, 6, 9\} \cup \{1, 4, 7, 10\}$ is the final form of U and $d_{12}(U) = 3$. If $\bigcup\{i_0, i_1, \ldots, i_{e-1}, n, d, m\}$ is the final form of U and $\bigcup\{j_0, j_1, \ldots, j_{e_1-1}, n, d_1, m_1\}$ is not the final form of U, then it is easily verified that $d \mid d_1$.

Let c, r and d be positive integers. An integer s, $0 < s < d$, is called an *invertible integer relative to c, r and d* if s satisfies $s(cr-1) \equiv 0 \pmod{d}$ and there exists an integer s' such that $s'cs \equiv r \pmod{d}$.

Lemma 1.1 ([8], Proposition 3.3.1)**.** *Let s, d and r be integers, and $s, d \neq 0$. Then the congruence $sx \equiv r \pmod{d}$ has solutions if and only if $(s, d) \mid r$.*

Lemma 1.2. *Let c, d and r be positive integers, and $r(cr-1) \equiv 0 \pmod{d}$. If s_0 is the least positive integer such that $s_0(cr-1) \equiv 0 \pmod{d}$, then each integer s which satisfies $s(cr-1) \equiv 0 \pmod{d}$ is a multiple of s_0, and $s_0 = (r, d)$.*

Proof. Since $s_0(cr-1) \equiv 0 \pmod{d}$ and $s(cr-1) \equiv 0 \pmod{d}$, we have $s_0(cr-1) = kd$ and $s(cr-1) = k_1 d$ for some $k, k_1 \in \mathbb{Z}$, and so $skd = ss_0(cr-1) =$

$s_0s(cr-1) = s_0k_1d$. Therefore $sk = s_0k_1$. Since s_0 is the least positive integer such that $s_0(cr-1) \equiv 0 \pmod{d}$, we have $(s_0, k) = 1$. Therefore s is a multiple of s_0. In the following we will prove that $s_0 = (r, d)$.

Let $d_1 = (r, d)$, $r = pd_1$ and $d = hd_1$. Then $(p, h) = 1$. Since $r(cr-1) \equiv 0 \pmod{d}$, we have $r(cr-1) = md$ for some $m \in \mathbb{Z}$, and so $pd_1(cr-1) = r(cr-1) = md = mhd_1$. Therefore we have $p(cr-1) = mh$. But $(p, h) = 1$, so we have $m = m_1p$ for some $m_1 \in \mathbb{Z}$. Thus $phd_1(cr-1) = mhd = pm_1hd$, and so $d_1(cr-1) = m_1d$, i.e., $d_1(cr-1) \equiv 0 \pmod{d}$. Since s_0 is the least positive integer such that $s_0(cr-1) \equiv 0 \pmod{d}$, d_1 is a multiple of s_0. Now, suppose $d_1 = ts_0$, $t \in \mathbb{Z}$. Since $m_1d = d_1(cr-1) = ts_0(cr-1) = tkd$, we have $m_1 = tk$. Hence t is a common divisor of d_1 and m_1. On the other hand, since $(r, cr-1) = 1$ and $r = pd_1$, we have $(d_1, cr-1) = 1$. Since $d_1(cr-1) = m_1d = m_1d_1h$, we have $cr-1 = m_1h$. But $(d_1, cr-1) = 1$, so we have $(d_1, m_1) = 1$, and so $t = 1$. Therefore $s_0 = d_1 = (r, d)$. The proof is completed. □

Lemma 1.3. *Let c, r and d be positive integers, and $r(cr-1) \equiv 0 \pmod{d}$. Let s be an invertible integer relative to c, r and d, and l be an integer such that $l(cr-1) \equiv 0 \pmod{d}$. Then the equation $scz \equiv l \pmod{d}$ has solutions.*

Proof. First we shall show that for any invertible integer s relative to c, r and d, the equation $scx \equiv r \pmod{d}$ has solutions if and only if the equation $scy \equiv s_0 \pmod{d}$ has solutions, where s_0 is the least positive integer such that $s_0(cr-1) \equiv 0 \pmod{d}$. From Lemma 1.2 we know that $s_0 \mid s$ and $s_0 = (r, d)$. Let now $r = r_1s_0$, $d = d_1s_0$, $s = s_1s_0$, where r_1, d_1 and s_1 are positive integers. Then $(r_1, d_1) = 1$. If the equation $scx \equiv r \pmod{d}$ has some solution x_0, then $scx_0 \equiv r \pmod{d}$, and so $s_1cx_0 \equiv r_1 \pmod{d_1}$, i.e., $s_1cx_0 = r_1 + td_1$ for some $t \in \mathbb{Z}$. But $(r_1, d_1) = 1$, so we have $(s_1c, d_1) = 1$. Then there exist $p, q \in \mathbb{Z}$ such that $ps_1c + qd_1 = 1$. It follows that $(r_1-1)ps_1c + (r_1-1)qd_1 = r_1 - 1$. So $r_1 - (r_1-1)ps_1c - (r_1-1)qd_1 = r_1 - (r_1-1)$. By using $r_1 = s_1cx_0 - td_1$, we have $s_1cx_0 - td_1 - (r_1-1)ps_1c - (r_1-1)qd_1 = 1$ and so $s_0s_1cx_0 - s_0td_1 - (r_1-1)ps_0s_1c - (r_1-1)qd_1s_0 = s_0$. Hence $scx_0 - td - (r_1-1)psc - (r_1-1)qd = s_0$, and so $sc(x_0 - (r_1-1)p) \equiv s_0 \pmod{d}$. Let $y_0 = x_0 - (r_1-1)p$. Then y_0 is one of solutions for the equation $scy \equiv s_0 \pmod{d}$. Conversely, if y_0 is a solution of the equation $scy \equiv s_0 \pmod{d}$, then, it is clear that $x = r_1y_0$ is a solution of the equation $scx \equiv r \pmod{d}$.

In the following we show that the equation $scz \equiv l \pmod{d}$ has solutions. If $l = 0$, then 0 is a solution of this equation. We now suppose $l \neq 0$. Since s is an invertible integer relative to c, r and d, there exists an integer s' such that $scs' \equiv r \pmod{d}$, i.e., the equation $scx \equiv r \pmod{d}$ has solutions, and so the equation $scy \equiv s_0 \pmod{d}$ has solutions. Let y_0 be a solution of the equation $scy \equiv s_0 \pmod{d}$. Then $scy_0 \equiv s_0 \pmod{d}$. Since l satisfies $l(cr-1) \equiv 0 \pmod{d}$, by Lemma 1.2, we have

$l = qs_0$ for some $q \in \mathbb{Z}$. Let $z_0 = y_0q$. Then $scy_0q \equiv qs_0 \pmod d$, i.e., z_0 is a solution of the equation $scz \equiv l \pmod d$. This completes the proof. □

Lemma 1.4. *Let c, r and d be positive integers, and $r(cr-1) \equiv 0 \pmod d$, and s be an invertible integer relative to c, r and d. Then the equations $scx \equiv r \pmod d$ and $x(cr-1) \equiv 0 \pmod d$ have common solutions.*

Proof. Let s_0 be the least positive integer such that $s_0(cr-1) \equiv 0 \pmod d$. Since s is an invertible integer relative to c, r and d, we have $s(cr-1) \equiv 0 \pmod d$. From Lemma 1.2, we have $s_0 = (r,d)$ and $s_0 \mid s$. Let $s = s_1s_0$, $r = r_1s_0$ and $d = d_1s_0$, where $s_1, r_1, d_1 \in \mathbb{Z}$. Then $(r_1, d_1) = 1$. In the following we shall show that the equation $scz \equiv r_1 \pmod{d_1}$ has solutions. Since s is an invertible integer relative to c, r and d, there exists an integer s' such that $scs' \equiv r \pmod d$. Then we have $s_1s_0cs' - r_1s_0 = pd_1s_0$ for some $p \in \mathbb{Z}$, i.e., $s_1cs' - r_1 = pd_1$. But $(r_1, d_1) = 1$, so we have $(s_1c, d_1) = 1$. It follows that $(s_1, d_1) = 1$, and so $(s, d) = s_0$. Since $(r, cr-1) = 1$ and $s_0 \mid r$, we have $(s_0, cr-1) = 1$. Since $s(cr-1) \equiv 0 \pmod d$, we have $s(cr-1) = qd$ for some $q \in \mathbb{Z}$. Then $s_1s_0(cr-1) = qd_1s_0$, and so $s_1(cr-1) = qd_1$. But $(s_1, d_1) = 1$, so we have $d_1 \mid (cr-1)$. Since $(s_0, cr-1) = 1$, we have $(s_0, d_1) = 1$. Since $(s_1c, d_1) = 1$, we have $(s_1s_0c, d_1) = 1$, i.e., $(sc, d_1) = 1$. By Lemma 1.1, we have that the equation $scz \equiv r_1 \pmod{d_1}$ has solutions. Suppose that k ($k \in \mathbb{Z}$) is a solution of the equation $scz \equiv r_1 \pmod{d_1}$, i.e., $sck \equiv r_1 \pmod{d_1}$. Then $scks_0 \equiv r \pmod d$, and so ks_0 is a solution of the equation $scx \equiv r \pmod d$.

In the following we shall show that the equations $scx \equiv r \pmod d$ and $y(cr-1) \equiv 0 \pmod d$ have common solutions. Since s_0 is the least positive integer such that $s_0(cr-1) \equiv 0 \pmod d$, we have $ks_0(cr-1) \equiv 0 \pmod d$. Then ks_0 is a solution of the equation $x(cr-1) \equiv 0 \pmod d$. Therefore the equations $scx \equiv r \pmod d$ and $x(cr-1) \equiv 0 \pmod d$ have common solutions. This completes the proof. □

Lemma 1.5. *Let n, r, s and c be positive integers such that $r(cr-1) \equiv 0 \pmod d$ and $s(cr-1) \equiv 0 \pmod d$. Let U, V be two subsets of $\mathbb{Z}$. If $(\sigma(crU + rV), n) = d$, then $d \mid (\sigma(csU + sV), n)$.*

Proof. Let s_0 be the least positive integer such that $s_0(cr-1) \equiv 0 \pmod d$. Then, by Lemma 1.2, we have $s = qs_0$ and $s_0 = (r,d)$, where $q \in \mathbb{Z}$. Let $r = r_1s_0$, $d = d_1s_0$, where $r_1, d_1 \in \mathbb{Z}$. Then $(r_1, d_1) = 1$. Since $(\sigma(crU + rV), n) = d$, we have $d \mid (cru + rv)$ for any $u \in U$ and $v \in V$. And so $cru + rv = m_{uv}d$ for some $m_{uv} \in \mathbb{Z}$. It follows that $cru + rv = cr_1s_0u + r_1s_0v = m_{uv}d_1s_0$. Then we have $cr_1u + r_1v = m_{uv}d_1$. But $(r_1, d_1) = 1$, so we have $r_1 \mid m_{uv}$. Let $m_{uv} = m'_{uv}r_1$. Then $cu + v = m'_{uv}d_1$, and so $s_0(cu+v) = s_0m'_{uv}d_1 = m'_{uv}d$. Since $s = qs_0$, we have $s(cu+v) = qs_0(cu+v) = qm'_{uv}d$. Hence for any $u \in U$, $v \in V$, we have $d \mid (scu + sv)$, and so $d \mid (\sigma(csU + sV), n)$ (because $d \mid n$). The proof is completed. □

Lemma 1.6. *Let U be a union of some arithmetic progressions modulo n with common difference and $d = d_n(U)$. Let $k \in \mathbb{Z}$. Then $k + U \equiv U \pmod{n}$ if and only if $d \mid k$.*

Proof. The proof is omitted. □

Lemma 1.7 ([7], Lemma 1.2). *Let n be a positive integer. Let $M = \{m_0, m_1, \ldots, m_{t-1}\} \subseteq \mathbb{Z}$, where $0 \leqslant m_0 \leqslant m_1 \leqslant \ldots \leqslant m_{t-1} \leqslant n-1$, and let $N = \{n_0, n_1, \ldots, n_{l-1}\}$ be a set of nonnegative integers. Let $d = (\sigma(N), n)$, $s = n/d$. Then the following are equivalent:*

(1) $N + M \equiv M \pmod{n}$.

(2) *For all $f \in \{0, 1, \ldots, l-1\}$, we have $n_f + M \equiv M \pmod{n}$.*

(3) *M is a union of arithmetic progressions modulo n with common difference d.*

Lemma 1.8. *Let $U \subseteq \{0, 1, 2, \ldots, n-1\}$ be a union of some arithmetic progressions modulo n with common difference and $d = d_n(U)$. Let $A = Q_r\Bigl(\sum\limits_{i\in U} P^i\Bigr)$, $B = Q_s\Bigl(\sum\limits_{i\in U} P^i\Bigr) \in G_n$. Then $A = B$ if and only if $r \equiv s \pmod{d}$.*

Proof. Necessity: Let $A = B$. Obviously, we have $\Delta(A) = \Delta(B) = U$. We know that the second row of A is obtained from the first row of A by shifting the elements cyclically r columns to the right and the second row of B is obtained from the first row of B by shifting the elements cyclically s columns to the right. Since the second row of A is equal to that of B, we have $\Delta(A) + r \equiv \Delta(B) + s \pmod{n}$, i.e., $U + r \equiv U + s \pmod{n}$. It follows that $(r - s) + U \equiv U \pmod{n}$. By Lemma 1.7, U is an union of some arithmetic progressions modulo n with the same common difference $d_1 = (r - s, n)$. Since $d = d_n(U)$, we have $d \mid d_1$. Hence $d \mid (r - s)$, i.e., $r \equiv s \pmod{d}$.

Sufficiency: Let $r \equiv s \pmod{d}$, i.e., $d \mid (r-s)$. By Lemma 1.6, we have $(r-s)+U \equiv U \pmod{n}$. Since $\Delta(A) = \Delta(B) = U$, it follows that $\Delta(A)+r \equiv \Delta(B)+s \pmod{n}$. That is, the second row of A is the same as the second row of B. Similarly, we can prove that the ith row of A is the same as the ith row of B for $i = 3, 4, \ldots, n$. Therefore $A = B$. This proves the lemma. □

2. A characterization

In order to characterize the elements in $M(F)$, we need the following lemmas.

Lemma 2.1. *Let* $C = Q_c\Big(\sum\limits_{k\in\Delta(C)} P^k\Big) \in G_n$. *Then* F *is an idempotent of* $G_n(C)$ *if and only if* F *can be written in the form:*

$$F = Q_r\Bigg(\sum_{u=0}^{e_1-1}(P^{i_u} + P^{i_u+d_1} + \ldots + P^{i_u+(m_1-1)d_1})\Bigg),$$

where $d_1 = (\sigma(cr\Delta(F) + r\Delta(C)), n)$, $d_1 \mid (r^2c - r)$, *and* $n = m_1d_1$.

Proof. By Theorem 2.2 and Lemma 3.4 in [7], we can obtain the lemma. □

Lemma 2.2. *Let* n, c *and* r *be positive integers. Let* $C = Q_c\Big(\sum\limits_{k\in\Delta(C)} P^k\Big) \in G_n$ *and* $F = Q_r\Big(\sum\limits_{i\in\Delta(F)} P^i\Big)$ *be an idempotent of* $G_n(C)$. *If* $A = Q_s\Big(\sum\limits_{j\in\Delta(A)} P^j\Big)$ *is an element in the maximal subgroup* $M(F)$ *of* $G_n(C)$ *containing* F, *then* $\Delta(A) \equiv \Delta(F) + l \pmod n$ *for some integer* l.

Proof. Since A is an element of $M(F)$, by (1.2), we have $A * F = A$, and there exists an element in $G_n(C)$ such that $X * A = F$, i.e. $ACF = A$ and $XCA = F$. Let now $X = Q_t\Big(\sum\limits_{f\in\Delta(X)} P^f\Big)$. Then, by (1.1), we have

$$ACF = Q_{scr}\Bigg(\sum_{l\in cr\Delta(A)+r\Delta(C)+\Delta(F)} P^l\Bigg) = Q_s\Bigg(\sum_{j\in\Delta(A)} P^j\Bigg)$$

and

$$XCA = Q_{tcs}\Bigg(\sum_{l\in cs\Delta(X)+s\Delta(C)+\Delta(A)} P^l\Bigg) = Q_r\Bigg(\sum_{i\in\Delta(F)} P^i\Bigg).$$

Therefore, $cr\Delta(A)+r\Delta(C)+\Delta(F) \equiv \Delta(A) \pmod n$ and $cs\Delta(X)+s\Delta(C)+\Delta(A) \equiv \Delta(F) \pmod n$. Thus, $\forall\, l \in cr\Delta(A)+r\Delta(C)$ and $l' \in cs\Delta(X)+s\Delta(C)$, and we have

$$l + \Delta(F) \subseteq \Delta(A) \pmod n \quad \text{and} \quad l' + \Delta(A) \subseteq \Delta(F) \pmod n.$$

It follows that

$$l + l' + \Delta(A) \subseteq l + \Delta(F) \pmod n,$$

and so

$$l' + l + \Delta(A) \subseteq \Delta(A) \pmod n \quad (\text{because } l + \Delta(F) \subseteq \Delta(A) \pmod n).$$

Hence

$$l + l' + \Delta(A) \equiv \Delta(A) \pmod n.$$

Thus we have

$$\Delta(A) \equiv l + (l' + \Delta(A)) \pmod{n} \subseteq l + \Delta(F) \pmod{n} \subseteq \Delta(A) \pmod{n}.$$

Therefore $\Delta(A) \equiv \Delta(F) + l \pmod{n}$ for some integer l. This completes the proof. $\square$

Theorem 2.1. *Let $C = Q_c\Big(\sum\limits_{k\in\Delta(C)} P^k\Big) \in G_n$. Let $F = Q_0\Big(\sum\limits_{i\in\Delta(F)} P^i\Big)$ be an idempotent element in $G_n(C)$. Then the maximal subgroup in $G_n(C)$ containing the idempotent element F is $\{F\}$.*

Proof. If $F = 0$, clearly $M(F) = \{F\}$. Now suppose that $F \neq 0$. Let $A = Q_s\Big(\sum\limits_{j\in\Delta(A)} P^j\Big) \in M(F)$. By (1.2), we know that $A \neq 0$ and $A * F = ACF = A$. Hence

$$\begin{aligned} A = ACF &= Q_s\Big(\sum_{j\in\Delta(A)} P^j\Big)Q_c\Big(\sum_{k\in\Delta(C)} P^k\Big)Q_0\Big(\sum_{i\in\Delta(F)} P^i\Big) \\ &= Q_{s\cdot c\cdot 0}\Big(\sum_{j\in\Delta(A),\, k\in\Delta(C),\, i\in\Delta(F)} P^{0\cdot c\cdot j + 0\cdot k + i}\Big) \\ &= Q_0\Big(\sum_{i\in\Delta(F)} P^i\Big) = F. \end{aligned}$$

Conversely, if $A = F$, then clearly $A \in M(F)$. Therefore $M(F) = \{F\}$. This proves the theorem. $\square$

Theorem 2.2. *Let $C = Q_c\Big(\sum\limits_{k\in\Delta(C)} P^k\Big) \in G_n$, and let $F = Q_r\Big(\sum\limits_{i\in\Delta(F)} P^i\Big)$ ($r \neq 0$) be an idempotent element of $G_n(C)$. Then $A = Q_s\Big(\sum\limits_{j\in\Delta(A)} P_j\Big)$ is an element of the maximal subgroup $M(F)$ of $G_n(C)$ containing F if and only if*

(2.1) *s is an invertible integer relative to c, r and d;*

(2.2) *$\Delta(A) \equiv \Delta(F) + l \pmod{n}$ for some l with $0 \leqslant l \leqslant n-1$;*

(2.3) *the integer l in (2.2) satisfies $l(cr-1) \equiv 0 \pmod{d}$, where d is the common difference of $\Delta(F)$ in the final form. i.e., $d = d_n(\Delta(F))$.*

Proof. Sufficiency: Suppose that the conditions (2.1), (2.2) and (2.3) hold.

Since F is an idempotent in $G_n(C)$, by Lemma 2.1, we know that F can be written in the form: $F = Q_r\Big(\sum_{u=0}^{e_1-1}(P^{i_u} + P^{i_u+d_1} + \ldots + P^{i_u+(m_1-1)d_1})\Big)$, where $d_1 = (\sigma(cr\Delta(F) + r\Delta(C)), n)$, and $r^2c \equiv r \pmod{d_1}$, and $n = m_1d_1$.

Let $\bigcup\{i_0, i_1, \ldots, i_{e-1}, n, d, m\}$ be the final form of $\Delta(F)$. Then we have $d \mid d_1$. Hence $r^2c \equiv r \pmod{d}$ and $n = md$ for some m. In the following we will prove that (1.2) holds.

First, we show that $A * F = A$.

Since $F * F = F$, we have

$$F * F = FCF = Q_{r^2c}\Big(\sum_{t\in cr\Delta(F)+r\Delta(C)+\Delta(F)} P^t\Big) = F,$$

and so

$$rc\Delta(F) + r\Delta(C) + \Delta(F) \equiv \Delta(F) \pmod{n}. \tag{2.4}$$

Since $\Delta(F)$ can be represented as the union of some arithmetic progression modulo n with common difference d and $d = d_n(\Delta(F))$, by the condition (2.3) and Lemma 1.6, we have $crl + \Delta(F) \equiv l + \Delta(F) \pmod{n}$. By the condition (2.2), we have

$$\begin{aligned} rc\Delta(A) + r\Delta(C) + \Delta(F) &\equiv rc(\Delta(F) + l) + r\Delta(C) + \Delta(F) \pmod{n} \\ &\equiv rc\Delta(F) + r\Delta(C) + (crl + \Delta(F)) \pmod{n} \\ &\equiv rc\Delta(F) + r\Delta(C) + \Delta(F) + l \pmod{n} \\ &\equiv \Delta(F) + l \pmod{n} \quad \text{(by (2.4))}. \end{aligned}$$

Hence

$$A * F = ACF = Q_{scr}\Big(\sum_{t\in cr\Delta(A)+r\Delta(C)+\Delta(F)} P^t\Big) = Q_{scr}\Big(\sum_{t\in\Delta(F)+l} P^t\Big).$$

Since s is an invertible integer relative to c, r and d, we have $s(cr-1) \equiv 0 \pmod{d}$. By Lemma 1.8, we have

$$A * F = ACF = Q_{scr}\Big(\sum_{t\in\Delta(F)+l} P^t\Big) = Q_s\Big(\sum_{t\in\Delta(F)+l} P^t\Big) = Q_s\Big(\sum_{t\in\Delta(A)} P^t\Big) = A.$$

Secondly, we prove that $F * A = A$.

By the condition (2.1), we have $s(cr-1) \equiv 0 \pmod{d}$. Since $r^2c \equiv r \pmod{d}$ and $d \mid d_1 = (\sigma(cr\Delta(F)+r\Delta(C)), n)$, by Lemma 1.5, we have $d \mid (\sigma(cs\Delta(F)+s\Delta(C)), n)$. By Lemma 1.6, we have

$$sc\Delta(F) + s\Delta(C) + \Delta(F) \equiv \Delta(F) \pmod{n}. \tag{2.5}$$

Hence

$$\begin{aligned}
F * A = FCA &= Q_r\Big(\sum_{i\in\Delta(F)} P^i\Big)Q_c\Big(\sum_{k\in\Delta(C)} P^k\Big)Q_s\Big(\sum_{j\in\Delta(A)} P^j\Big)\\
&= Q_{scr}\Big(\sum_{t\in sc\Delta(F)+s\Delta(C)+\Delta(A)} P^t\Big)\\
&= Q_{scr}\Big(\sum_{t\in sc\Delta(F)+s\Delta(C)+\Delta(F)} P^t\Big)P^l \quad \text{(by the condition (2.2))}\\
&= Q_{scr}\Big(\sum_{t\in\Delta(F)} P^t\Big)P^l \quad \text{(by (2.5))}\\
&= Q_s\Big(\sum_{t\in\Delta(F)} P^t\Big)P^l \quad \text{(by Lemma 1.8)}\\
&= A.
\end{aligned}$$

Finally, we shall show that there exist $X, Y \in G_n(C)$ such that $X * A = F$ and $A * Y = F$.

Since s is an invertible integer relative to c, r and d, and $r^2c \equiv r \pmod d$, the equations $scx \equiv r \pmod d$ and $x(cr-1) \equiv 0 \pmod d$ have common solutions by Lemma 1.4. Let s' be a common solution of them, i.e., $s'cs \equiv r \pmod d$ and $s'(cr-1) \equiv 0 \pmod d$. By Lemma 1.3, we can find an integer w such that $scw \equiv l \pmod d$ and l satisfies the condition (2.3). Hence

$$\begin{aligned}
&cs\Delta(F) + s\Delta(C) + \Delta(F) + l + csd - csw\\
&\quad\equiv \Delta(F) + l - csw \pmod n \quad \text{(by (2.5))}\\
&\quad\equiv \Delta(F) \pmod n \quad (\text{because } csw \equiv l \pmod d).
\end{aligned}$$

Also, by Lemmas 1.5 and 1.6, we have

$$cs'\Delta(F) + s'\Delta(C) + \Delta(F) \equiv \Delta(F) \pmod n. \tag{2.6}$$

Let now $X = Q_{s'}\Big(\sum_{x\in\Delta(F)+d-w} P^x\Big)$ and $Y = Q_{s'}\Big(\sum_{y\in\Delta(F)-ls'c} P^y\Big) \in G_n(C)$. Then we have

$$\begin{aligned}
X * A = XCA &= Q_{s'}\Big(\sum_{x\in\Delta(F)+d-w} P^x\Big)Q_c\Big(\sum_{k\in\Delta(C)} P^k\Big)Q_s\Big(\sum_{j\in\Delta(A)} P^j\Big)\\
&= Q_{s'cs}\Big(\sum_{t\in cs\Delta(F)+s\Delta(C)+\Delta(A)+csd-csw} P^t\Big)
\end{aligned}$$

$$= Q_{s'cs}\Big(\sum_{t\in cs\Delta(F)+s\Delta(C)+\Delta(F)+l+csd-csw} P^t\Big) \quad \text{(by the condition (2.2))}$$

$$= Q_{s'cs}\Big(\sum_{t\in\Delta(F)} P^t\Big)$$

(by the fact that $cs\Delta(F)+s\Delta(C)+\Delta(F)+l+csd-csw \equiv \Delta(F) \pmod{n}$)

$$= Q_r\Big(\sum_{t\in\Delta(F)} P^t\Big) \quad \text{(by Lemma 1.8 and the fact that } s'cs\equiv r \pmod{d})$$

$$= F,$$

and

$$A*Y = ACY = Q_s\Big(\sum_{j\in\Delta(A)} P^j\Big)Q_c\Big(\sum_{k\in\Delta(C)} P^k\Big)Q_{s'}\Big(\sum_{y\in\Delta(F)-ls'c} P^y\Big)$$

$$= Q_{scs'}\Big(\sum_{t\in cs'\Delta(A)+s'\Delta(C)+\Delta(F)-ls'c} P^t\Big)$$

$$= Q_{scs'}\Big(\sum_{t\in cs'\Delta(F)+s'\Delta(C)+\Delta(F)} P^t\Big) \quad \text{(by the condition (2.2))}$$

$$= Q_{scs'}\Big(\sum_{t\in\Delta(F)} P^t\Big) \quad \text{(by (2.6))}$$

$$= Q_r\Big(\sum_{t\in\Delta(F)} P^t\Big) \quad \text{(by Lemma 1.8 and the fact that } s'cs\equiv r \pmod{d})$$

$$= F.$$

Therefore A is an element of the maximal subgroup $M(F)$ of $G_n(C)$.

Necessity: Suppose that A is an element in $M(F)$. By Lemma 2.2, we have $\Delta(A)\equiv\Delta(F)+l \pmod{n}$. This means that the condition (2.2) holds.

Since $A*F=A$ (by (1.2)) and $A*F=ACF=Q_{scr}\Big(\sum_{t\in cr\Delta(A)+r\Delta(C)+\Delta(F)} P^t\Big)=Q_{scr}\Big(\sum_{t\in cr\Delta(F)+r\Delta(C)+\Delta(F)+crl} P^t\Big)$ and $A=Q_s\Big(\sum_{j\in\Delta(A)} P^j\Big)=Q_s\Big(\sum_{j\in\Delta(F)+l} P^j\Big)$, we have $cr\Delta(F)+r\Delta(C)+\Delta(F)+crl\equiv\Delta(F)+l \pmod{n}$. By (2.4), we have $\Delta(F)+crl\equiv\Delta(F)+l \pmod{n}$. By Lemma 1.8, we have $scr\equiv s \pmod{d}$, i.e., $s(cr-1)\equiv 0 \pmod{d}$. By Lemma 1.6, we have $l(cr-1)\equiv 0 \pmod{d}$.

There exists an $X\in G_n(C)$ such that $X*A=F$. Let $X=Q_{s'}\Big(\sum_{x\in\Delta(X)} P^x\Big)$. Then $X*A=XCA=Q_{s'cs}\Big(\sum_{t\in sc\Delta(X)+s\Delta(C)+\Delta(A)} P^t\Big)$. Since $F=Q_r\Big(\sum_{i\in\Delta(F)} P^i\Big)$, we have $Q_{s'cs}\Big(\sum\limits_{t\in sc\Delta(X)+s\Delta(C)+\Delta(A)} P^t\Big) = Q_r\Big(\sum\limits_{i\in\Delta(F)} P^i\Big)$. Hence $scs' \equiv r \pmod d$ by Lemma 1.8. These mean that the condition (2.1) and the condition (2.3) hold. This proves Theorem 2.2. □

In Theorem 2.2, if $C = E$ (E is the identity matrix), then $G_n(C) = G_n$. In this case, we have the following corollary.

Corollary 2.1 ([3], Theorem 2). *Let* $F = Q_r\Big(\sum\limits_{u=0}^{e-1}(P^{i_u} + P^{i_u+d} + \ldots + P^{i_u+(m-1)d})\Big)$ *be an idempotent in* G_n. *Then* $A = Q_s\Big(\sum\limits_{j\in\Delta(A)} P^j\Big)$ *is an element of the maximal subgroup* $M(F)$ *of* G_n *containing* F *if and only if*

(1) *s is an invertible integer relative to r and d;*
(2) *there exists an integer l, $0 \leqslant l \leqslant n-1$, such that $\Delta(A) \equiv \Delta(F) + l \pmod n$;*
(3) *the integer l in (2) satisfies $l(cr-1) \equiv 0 \pmod d$.*

3. Algorithm and example

For any fixed r-circulant matrix $C \in G_n$ we will present an algorithm to find all the elements in the maximal subgroup $M(F)$ in the semigroup $G_n(C)$ containing F.

Let

$$C = Q_c\Big(\sum_{k\in\Delta(C)} P^k\Big),$$

$$F = Q_r\Big(\sum_{u=0}^{e-1}(P^{i_u} + P^{i_u+d} + \ldots + P^{i_u+(m-1)d})\Big), \quad n = md.$$

Step 1. Compute all the invertible integers relative to c, r and d, say $s_0, s_1, \ldots, s_{g-1}$.
Step 2. Compute all integers l such that $l(cr-1) \equiv 0 \pmod d$, say $l_0, l_1, \ldots, l_{h-1}$.
Step 3. Form all elements of

$$M(F) = \Big\{A_{pq} = Q_{s_p}\Big(\sum_{u=0}^{e-1}(P^{i_u} + P^{i_u+d} + \ldots + P^{i_u+(m-1)d})\Big)P^{l_q} : \\ p = 0, 1, \ldots, g-1, \ q = 0, 1, \ldots, h-1\Big\}.$$

Example. Let $n = 144$, $C = Q_2(P^3 + P^6) \in G_{144}$, we can verify that $F = Q_8\Big(\sum\limits_{u=0}^{5} P^{3+24u}\Big)$ is one of the idempotent elements in $G_{144}(C)$.

Step 1. The invertible integers relative to $2, 8$ and 24 are $\{8, 16\}$;

Step 2. All integers which satisfy $l(2\cdot 8-1)\equiv 0 \pmod{24}$ are $\{0, 8, 16\}$;

Step 3. $M(F)=\Big\{Q_{s_p}\sum\limits_{u=0}^{5}(P^{3+24u})P^{l_q}:\ s_p=8,16,\ \ l_q=0,8,16\Big\}.$

References

[1] *C.-Y. Chao, M.-C. Zhang*: On generalized circulants over a Boolean algebra. Linear Algebra Appl. *62* (1984), 195–206. Zbl 0553.15005

[2] *W.-C. Huang*: On the sandwich semigroups of circulant Boolean matrices. Linear Algebra Appl. *179* (1993), 135–160. Zbl 0768.20031

[3] *Mou-Chen Zhang*: On the maximal subgroup of the semigroup of generalized circulant Boolean matrices. Linear Algebra Appl. *151* (1991), 229–243. Zbl 0723.15009

[4] *A. H. Clifford, G. B. Preston*: The Algebra Theory of Semigroups, Vol. 1. Amer. Math. Soc., Providence, 1961.

[5] *J. S. Montague, R. J. Plemmons*: Maximal subgroup of semigroup of relations. J. Algebra *13* (1969), 575–587.

[6] K.-H. Kim, S. Schwarz The semigroup of circulant Boolean matrices. Czechoslovak Math. J. *26(101)* (1976), 632–635.

[7] *J.-S. Chen, Y.-J. Tan*: The idempotent elements in the sandwich semigroup of generalized elements Boolean mareices. J. Fuzhou Univ. Nat. Sci. *31* (2003), 505–509. Zbl 1052.15011

[8] *K. Ireland, M. Rosen*: A Classical Introduction to Modern Number Theory. Springer-Verlag, New York, 1982.

Authors' address: Jinsong Chen, Yijia Tan, College of Mathematics and Computer Science, Fuzhou University, Fuzhou, Fujian 350002, P.R. China, e-mail: yjtan@fzu.edu.cn.