Maximum exponent of boolean circulant matrices with constant number of nonzero entries in their generating vector

M.I. Bueno,*

Department of Mathematics and The College of Creative Studies
University of California, Santa Barbara, USA;
mbueno@math.ucsb.edu

S. Furtado,†

Faculdade de Economia do Porto
Rua Dr. Roberto Frias 4200-464 Porto, Portugal;
sbf@fep.up.pt

N. Sherer ‡

The College of Creative Studies
University of California, Santa Barbara, USA;
nsherer@sbcglobal.net

Submitted: Sep 11, 2008; Accepted: May 19, 2009; Published: May 29, 2009
Mathematics Subject Classification: 11P70, 05C25, 05C50

Abstract

It is well-known that the maximum exponent that an n-by-n boolean primitive circulant matrix can attain is $n-1$. In this paper, we find the maximum exponent attained by n-by-n boolean primitive circulant matrices with constant number of nonzero entries in their generating vector. We also give matrices attaining such exponents. Solving this problem we also solve two equivalent problems: 1) find the maximum exponent attained by primitive Cayley digraphs on a cyclic group whose vertices have constant outdegree; 2) determine the maximum order of a basis for $\mathbb{Z}_n$ with fixed cardinality.

*Supported by a Faculty Career Development Award granted by UCSB in Summer 2008 and supported by Dirección General de Investigación (Ministerio de Ciencia y Tecnología) of Spain under grant MTM2006-06671.

†This work was done within the activities of Centro de Estruturas Lineares e Combinatorias da Universidade de Lisboa.

‡Supported by a Summer Undergraduate Research Fellowship granted by the College of Creative Studies at UCSB.

1 Introduction

A boolean matrix is a matrix over the binary Boolean algebra $\{0, 1\}$. An n-by-n boolean matrix C is said to be circulant if each row of C (except the first) is obtained from the preceding row by shifting the elements cyclically 1 column to the right. In other words, the entries of a circulant matrix $C = (c_{ij})$ are related in the manner: $c_{i+1,j} = c_{i,j-1}$, where $0 \leq i \leq n-2$, $0 \leq j \leq n-1$, and the subscripts are computed modulo n. The first row of C is called the generating vector. Here and throughout we number the rows and columns of an n-by-n matrix from 0 to $n-1$.

Let

$$P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Any circulant boolean matrix C can be expressed as $C = P^{j_0} + P^{j_1} + ... + P^{j_{r-1}}$, with $0 \leq j_0 < j_1 < ... < j_{r-1} < n$. We define $P^0 = I_n$, where I_n denotes the identity matrix.

An n-by-n boolean circulant matrix C is said to be primitive if there exists a positive integer k such that $C^k = J_n$, where J_n is the n-by-n matrix whose entries are all ones and the product is computed in the algebra $\{0, 1\}$. The smallest such k is called the exponent of C, and we denote it by $exp(C)$.

The set of all n-by-n boolean circulant matrices forms a multiplicative commutative semigroup C_n with $|C_n| = 2^n$ [3, 5]. In 1974, K.H. Kim-Buttler and J.R. Krabill [4], and S. Schwarz [7] investigated the semigroup C_n. They obtained the following result:

Lemma 1.1 *Let $C \in C_n$, $n > 1$, and assume that the nonzero entries in its generating vector are placed in columns $\{j_0, j_1, ..., j_{r-1}\}$. Then, C is primitive if and only if $r \geq 2$ and $gcd(j_1 - j_0, ..., j_{r-1} - j_0, n) = 1$. Moreover, if C is primitive, then $exp(C) \leq n - 1$.*

In the literature, the problem of computing all possible exponents attained by primitive matrices in C_n has been considered. However, not much progress has been done. In [2] and [9], it is shown that if $C \in C_n$ is primitive, then its exponent is either $n-1$, $\lfloor n/2 \rfloor$, $\lfloor n/2 \rfloor - 1$ or does not exceed $\lfloor n/3 \rfloor + 1$. The matrices with exponents $n-1$, $\lfloor n/2 \rfloor$, $\lfloor n/2 \rfloor - 1$ are also characterized.

Based on numerous numerical experiments, we state the following conjecture:

Conjecture 1 *Given a positive integer n, let c be the smallest positive integer such that $\lfloor \frac{n}{c+1} \rfloor + c > \lfloor \frac{n}{c} \rfloor$. If $C \in C_n$, then*

$$exp(C) = \left\lfloor \frac{n}{j} \right\rfloor + k, \quad k = -1, 0, 1, ..., j-2 \tag{1}$$

for some $j \in \{1, 2, ..., c-1\}$ or $exp(C) \leq \lfloor n/c \rfloor + c - 2$. Moreover, there exist matrices in C_n attaining all the exponents in the interval $[1, \lfloor n/c \rfloor + c - 2]$.

The previous conjecture would explain the gaps in the set of exponents attained by primitive matrices in C_n for a given n.

In order to prove this conjecture, it is relevant to study the set of exponents attained by n-by-n boolean primitive circulant matrices whose generating vector has exactly r nonzero entries. We denote this set by $C_{n,r}$. In particular, we find important to give an answer to the following question: Given two positive integers n and r, where $2 \leq r \leq n$, find the maximum exponent attained by matrices in $C_{n,r}$ and give matrices attaining such exponent. In this paper we solve this question.

Note that matrices in $C_{n,r}$ are r-regular, that is, the number of nonzero entries in each row and each column of the matrix is exactly r. Therefore, the problem we study in this paper is also connected to the problem of finding the exponent attained by boolean r-regular primitive matrices, which was considered in [1].

Our problem can also be stated in terms of Cayley digraphs.

A boolean primitive circulant matrix can be seen as a Cayley digraph on a cyclic group. A digraph D is called primitive if there exists a positive integer k such that for each ordered pair a, b of vertices there is a directed walk from a to b of length k in D. The smallest such integer k is called the exponent of the primitive digraph D. Thus, our problem is equivalent to finding the maximum exponent attained by primitive Cayley digraphs on a cyclic group whose vertices have outdegree r, and giving digraphs attaining such exponents.

In this paper we use techniques from Additive Number Theory to solve our problem. We can restate our question in Number Theory terms in the following way: Let n be a positive integer and let S be a nonempty subset of $\mathbb{Z}_n$. The set S is said to be a basis for $\mathbb{Z}_n$ if there exists a positive integer k such that the sumset $kS = S + \cdots + S = \mathbb{Z}_n$, where the sum is computed modulo n. The smallest such k is called the order of S. As we will show later on, the problem we study in this paper can also be stated in the following way: Determine the maximum order of bases for $\mathbb{Z}_n$ with fixed cardinality r and give bases of such order.

The main result in this paper is given in Section 3. There we prove: Let n and r be two positive integers such that $2 \leq r \leq n$. Let $m_0 = 1$ and let $\{m_1, ..., m_t\}$ be the set of proper divisors of n smaller than $r - 1$. Then,

$$\max\{exp(C) : C \in C_{n,r}\} = \max\left\{\left\lceil \frac{n - m_i}{(\lceil r/m_i \rceil - 1)m_i} \right\rceil, i = 0, 1, ..., t\right\}.$$

2 Results from Additive Number Theory

In this section, we present some results from Additive Number Theory that will be useful to solve our problem in terms of basis for finite cyclic subgroups.

Let $S_1, S_2, ..., S_k$ be nonempty subsets of $\mathbb{Z}_n$. We define the sumset

$$S_1 + S_2 + ... + S_k = \{a_1 + a_2 + ... + a_k : a_i \in S_i, i = 1, ..., k\},$$

where the sum is computed modulo n. If S is a subset of $\mathbb{Z}_n$ and $S_i = S$ for $i = 1, ..., k$, then we denote the sumset $S_1 + ... + S_k$ by kS . Thus, the k-fold sumset kS is the set of all sums of k elements of S, with repetitions allowed.

If $S \subseteq \mathbb{Z}_n$ is a basis for $\mathbb{Z}_n$, we denote by $order(S)$ the order of S. In general, we say that S is a basis for $\mathbb{Z}_n$ if $kS = \mathbb{Z}_n$ for some positive integer k.

Definition 2.1 *Let $A \subseteq \mathbb{Z}_n$ be nonempty. We call the stabilizer $H(A)$ of A the set given by*

$$H(A) := \{h \in \mathbb{Z}_n : h + A = A\}.$$

The next lemma gives some useful properties of the stabilizer $H(A)$ of a given nonempty set $A \subseteq \mathbb{Z}_n$.

Lemma 2.2 *Let $A \subseteq \mathbb{Z}_n$ be nonempty. Then,*

i) *$H(A)$ is an additive subgroup of $\mathbb{Z}_n$;*

ii) *A is a union of cosets of $H(A)$;*

iii) *$H(kA) \subseteq H((k+1)A)$, for all $k \geq 1$.*

iv) *if $0 \in A$, $H(A) \subseteq A$;*

Proof. i) Let $h_1, h_2 \in H(A)$. Let us show that $h_1 + h_2 \in H(A)$. Since $h_2 \in H(A)$,

$$h_1 + h_2 + A = h_1 + A.$$

Similarly, since $h_1 \in H(A)$,

$$h_1 + A = A$$

and the result follows.

ii) First we note that if $a \in A$ then, by the definition of $H(A)$, $a + H(A) \subseteq A$. Thus, the union of cosets of $H(A)$ of the form $a+H(A)$, with $a \in A$, is a subset of A. Conversely, if $a \in A$ then $a \in a + H(A)$. Thus, A is contained in the union of the cosets of $H(A)$ of the form $a + H(A)$ with $a \in A$.

iii) Let $h \in H(kA)$. Then, $h+kA = kA$, which implies that $h+(k+1)A = (h+kA)+A = kA + A = (k+1)A$ and the result follows.

iv) Let $h \in H(A)$. Then, $h + A = A$. In particular, $h + 0 = h \in A$. ◻

The next result is an immediate consequence of ii) in Lemma 2.2. We denote by $|M|$ the cardinality of the set M.

Corollary 2.3 *Let $A \subseteq \mathbb{Z}_n$ be nonempty. Then $|H(A)|$ divides $|A|$.*

Next we show that the order is invariant under addition of a constant to a basis for $\mathbb{Z}_n$.

Lemma 2.4 *Let S_1 and S_2 be two subsets of $\mathbb{Z}_n$. Suppose that $S_1 = s + S_2$, where $s \in \mathbb{Z}_n$. Then, S_1 is a basis for $\mathbb{Z}_n$ if and only if S_2 is a basis for $\mathbb{Z}_n$. Moreover, if S_1 is a basis for $\mathbb{Z}_n$, then $order(S_1) = order(S_2)$.*

Proof. Since

$$kS_1 = (ks) + (kS_2),$$

we have

$$|kS_1| = |kS_2| \quad \text{for all } k \geq 1,$$

and the result follows. ◻

The following results give a lower and an upper bound for the cardinality of a k-fold sumset kS. The first result is a version of Kneser's Theorem for finite abelian groups.

Theorem 2.5 (Kneser's theorem) *[6] Let $S \subseteq \mathbb{Z}_n$ be nonempty. Let $H_k = H(kS)$ be the stabilizer of kS, $k \geq 1$. Then,*

$$|kS| \geq k|S + H_k| - (k-1)|H_k|.$$

Theorem 2.6 *[6] Let $k \geq 2$. Let $S \subseteq \mathbb{Z}_n$ and $r = |S|$. Then,*

$$|kS| \leq \binom{k+r-1}{k}.$$

3 Maximum exponent attained by matrices in $C_{n,r}$.

Let $C \in C_n$ and let $S \subseteq \mathbb{Z}_n$ be the set of positions of the nonzero entries in the generating vector of C. We will show that S is a basis for $\mathbb{Z}_n$ if and only if C is primitive. Moreover, if C is primitive, then the exponent of C is the order of S. Thus, we show that the study of the maximum exponent attained by matrices in $C_{n,r}$ is equivalent to the study of the maximum order of bases for $\mathbb{Z}_n$ with cardinality r.

The notation $C(:,j)$ and $C(i,:)$ denote the j-th column and the i-th row of the matrix C, respectively.

Lemma 3.1 *Let $C \in C_n$. Let $S \subseteq \mathbb{Z}_n$ be the set of positions of the nonzero entries in the generating vector of C. Then, for $k \geq 1$, kS is the set of positions of the nonzero entries in the generating vector of C^k.*

Proof. The proof is by induction on k. If $k = 1$ the result is trivially true. Now suppose that the result is true for some $k \geq 1$, that is,

$$C^k(0,j) \neq 0 \text{ if and only if } j \in kS.$$

Suppose that $S = \{j_0, ..., j_{r-1}\}$ and $kS = \{b_1, ..., b_t\}$. Note that $C^{k+1}(0,j) = C^k(0,:)C(:,j) \neq 0$ if and only if $C(b_i,j) \neq 0$ for some $i = 1,..,t$. Also, note that, since C is circulant, the positions of the nonzero entries in the b_i-th row of C are given by $j_0 + b_i$ (mod n), $\ldots, j_{r-1} + b_i$ (mod n). Then, the nonzero entries in the generating vector of C^{k+1} are in the positions corresponding to the elements in $(k+1)S$. ◻

Theorem 3.2 *Let $C \in C_n$ and let $S \subseteq \mathbb{Z}_n$ be the set of positions of the nonzero entries in the generating vector of C. Then, S is a basis for $\mathbb{Z}_n$ if and only if C is primitive. Moreover, if C is primitive, then*

$$exp(C) = order(S).$$

Proof. From Lemma 3.1, the generating vector of C^k is positive if and only if S is a basis of order k for $\mathbb{Z}_n$. Now the result follows taking into account that the generating vector of C^k is positive if and only if C^k is positive, as C^k is also a circulant matrix. ⌑

Next, given n and $r \in \{2, \ldots, n\}$, we determine the maximum order of bases for $\mathbb{Z}_n$ with constant cardinality r. We also give subsets of $\mathbb{Z}_n$ with such an order. Since we are only interested in the order of the bases for $\mathbb{Z}_n$, based on Lemma 2.4, from now on we exclusively consider bases S such that $0 \in S$. In particular, notice that if $S = \{0, j_1, ..., j_{r-1}\}$, then, the set $n - S$ and the sets $j_i - S$, $i = 1, ..., r-1$, contain 0 and have the same order as S.

Let us denote by $S_{n,r}$ the set of bases for $\mathbb{Z}_n$ that contain 0 and have cardinality r, with $2 \leq r \leq n$. Note that for each pair (n, r), $S_{n,r}$ is nonempty. Clearly, if $n = r$ and $S \in S_{n,r}$, then $S = \mathbb{Z}_n$ and $order(S) = 1$.

First we define the m-representation of a basis S for $\mathbb{Z}_n$, where m is a divisor of n smaller than n or $m = 0$. This representation will allow us to study the structure of a basis S and will facilitate the computation of its order.

Definition 3.3 *Let n be a positive integer and $m < n$ be a divisor of n. Then,*

$$\mathbb{Z}_n = \langle m \rangle \cup (1 + \langle m \rangle) \cup ... \cup (m - 1 + \langle m \rangle),$$

where $\langle m \rangle$ denotes the cyclic subgroup of $\mathbb{Z}_n$ generated by m. Let $S \subseteq \mathbb{Z}_n$ be nonempty. Let us denote $S_i = S \cap (i + \langle m \rangle)$. Then, we call the set

$$\{S_0, S_1, ..., S_{m-1}\},$$

the m-representation of S, where some S_i can be the empty set. We also define the 0-representation of $S = \{j_0, j_1, ..., j_{r-1}\}$ as the set $\{\{j_0\}, \{j_1\}, ..., \{j_{r-1}\}\}$.

We denote by $f_m(S)$ the number of subsets S_i in the m-representation of S which are nonempty.

Note that $f_0(S) = |S|$ and $f_1(S) = 1$. Moreover, if S is a basis for $\mathbb{Z}_n$, taking into account Lemma 1.1, $f_m(S) \geq 2$ for all proper divisors m of n and for $m = 0$. By a proper divisor of a positive integer n we mean any positive integer divisor of n larger than 1 and smaller than n. For convenience, we define $f_n(S) = f_0(S)$.

The next lemma follows in a straightforward way from the previous observation and the definition of m-representation.

Lemma 3.4 *Let $S \in S_{n,r}$ and $m < n$ be a divisor of n. Then, $f_{n/m}(S) \geq \max\{2, \lceil r/m \rceil\}$.*

Consider a basis $S \in S_{n,r}$, where $r < n$. In what follows we denote by H the stabilizer $H(kS) \neq \mathbb{Z}_n$ such that if $H(kS)$ is strictly contained in $H(k'S)$ then $H(k'S) = k'S = \mathbb{Z}_n$. Notice that if h is such that $H(hS) = H$, then, because of iv) in Lemma 2.2, $H(kS) = H$ for all $k \geq h$ such that $|kS| < n$.

Lemma 3.5 *Let $S \in S_{n,r}$, $r < n$. Assume that m is the generator of H. Then,*

$$order(S) \leq \left\lceil \frac{n - |H|}{(f_m(S) - 1)|H|} \right\rceil.$$

Proof. Because of Theorem 2.5, we get

$$|kS| \geq k|S + H| - (k-1)|H|, \quad \text{for all } k \text{ such that } H(kS) = H.$$

Notice that $|S + H| = f_m(S)|H|$. Thus,

$$|kS| \geq k(f_m(S)|H| - |H|) + |H|.$$

By considering $k(f_m(S)|H| - |H|) + |H| \geq n$ we get the result. $\sqcup\!\sqcap$

An immediate corollary of the previous lemma can be obtained for bases S for $\mathbb{Z}_n$ such that $H = H(S)$.

Corollary 3.6 *Let $S \in S_{n,r}$, $r < n$. Assume that $H = H(S)$ and let $d = |H(S)|$. Then,*

$$order(S) \leq \left\lceil \frac{n - d}{r - d} \right\rceil.$$

Proof. It is an immediate consequence of Lemma 3.5 given that $f_m(S)|H| = |S|$ when $H = H(S) = \langle m \rangle$. $\sqcup\!\sqcap$

Note that, it follows from the previous corollary that if n is prime, then $order(S) \leq \lceil \frac{n-1}{r-1} \rceil$ for all $S \in S_{n,r}$, $r < n$, as $H = H(S) = \{0\}$.

The previous results can be used to determine an upper bound for the order of bases for $\mathbb{Z}_n$ containing 0, with given cardinality.

Theorem 3.7 *Let n and r be two positive integers such that $2 \leq r \leq n$. Let $m_0 = 1$ and $\{m_1, ..., m_t\}$ be the set of proper divisors of n smaller than $r - 1$, which may be empty. Let $S \in S_{n,r}$. Then,*

$$order(S) \leq \max\left\{ \left\lceil \frac{n - m_i}{(\lceil r/m_i \rceil - 1)m_i} \right\rceil, i \in \{0, 1, ..., t\} \right\}.$$

Proof. Clearly, if $r = n$, the left side of the inequality is one. Now suppose that $r < n$. Let $h = |H|$. Note that h divides n and, by Lemma 3.4, the n/h-representation of S has at least two subsets. Therefore, by Lemma 3.5, $order(S) \leq \lceil \frac{n-h}{h} \rceil$. Notice that

$$\left\lceil \frac{n - h}{h} \right\rceil \leq \left\lceil \frac{n - 1}{r - 1} \right\rceil, \quad \text{for all } h \geq r - 1.$$

Thus, if the smallest proper divisor of n is larger than or equal to $r-1$, since $h \geq r-1$, the result follows.

If $h = m_i$ for some $i \in \{0, 1, ..., t\}$, then by Lemma 3.4 the n/h-representation of S has at least $\lceil r/h \rceil$ subsets and therefore, by Lemma 3.5,

$$order(S) \leq \left\lceil \frac{n - m_i}{(\lceil r/m_i \rceil - 1)m_i} \right\rceil.$$

and the result follows. ⊔⊓

Next we show that the upper bound for the set of exponents of matrices in $S_{n,r}$ given by Theorem 3.7 is, in fact, a maximum.

Lemma 3.8 *Let n and r be positive integers such that $2 \leq r \leq n$. Let $S = \{0, 1, ..., r-1\} \subseteq \mathbb{Z}_n$. Then, $order(S) = \left\lceil \frac{n-1}{r-1} \right\rceil$.*

Proof. Notice that

$$kS = \{0, 1, ..., k(r-1)\},$$

and $|kS| \geq n$ if and only if $k(r-1)+1 \geq n$, which implies the result. ⊔⊓

Lemma 3.9 *Let n and r be positive integers such that $2 \leq r \leq n$. Suppose that n has a proper divisor m smaller than $r-1$. Moreover, suppose that $m \geq 3$ or both $m = 2$ and r is even. Let $t := \lceil r/m \rceil$ and $r = tq + p$ for some positive integers q and p such that $0 \leq p < t$. Let*

$$S = \bigcup_{i=0}^{p-1} \{i, n/m + i, ..., qn/m + i\} \cup \bigcup_{i=p}^{t-1} \{i, n/m + i, ..., (q-1)n/m + i\}).$$

where the first union is empty if $p = 0$. Then,

$$order(S) = \left\lceil \frac{n - m}{(\lceil r/m \rceil - 1)m} \right\rceil.$$

Proof. Since $t = \lceil r/m \rceil$ and $m < r-1$, then $t \geq 2$ and

$$r > m(t-1). \tag{2}$$

Taking this into account and considering that $r = tq + p$, we deduce that

$$q = \frac{r-p}{t} > \frac{m(t-1)}{t} - \frac{p}{t} = m - \frac{m+p}{t}.$$

Observe that, since $p < t$ and $t \geq 2$, then

$$\frac{m+p}{t} < \frac{m+t}{t} \leq 1 + \frac{m}{2}.$$

Therefore,

$$q \geq m - \frac{m}{2} = \frac{m}{2}. \tag{3}$$

Let us denote

$$S_i = \{i, n/m + i, ..., qn/m + i\}$$

for $i = 0, 1, ..., p-1$ and

$$\tilde{S}_j = \{j, n/m + j, ..., (q-1)n/m + j\})$$

for $j = p, p+1, ..., t-1$.

Notice that

$$S_i + S_j = \{i + j, i + j + n/m, ..., i + j + 2qn/m\} = i + j + \langle n/m \rangle, \tag{4}$$

where the last equality follows because, from (3), $2qn/m \geq n$.

Analogously,

$$S_i + \tilde{S}_j = \{i + j, i + j + n/m, ..., i + j + (2q-1)n/m\} = i + j + \langle n/m \rangle, \tag{5}$$

where the last equality follows because, from (3), $(2q-1)n/m \geq (m-1)n/m$.

Also,

$$\tilde{S}_i + \tilde{S}_j = \{i + j, i + j + n/m, ..., i + j + (2q-2)n/m\}.$$

In this case, $(2q-2)n/m \geq (m-2)n/m$ and we need to consider two cases:

- Case 1: Suppose that $(2q-2)n/m > (m-2)n/m$. Then, $\tilde{S}_i + \tilde{S}_j = i + j + \langle n/m \rangle$. This fact together with (4) and (5) imply that $H(2S) = \langle n/m \rangle$ and therefore,

  $$kS = \bigcup_{i=0}^{kt-k} (i + \langle n/m \rangle), \quad \text{for } k \geq 2,$$

  or, in other words, $order(S) = order\{0, 1, ..., t-1\}$ in $\mathbb{Z}_{n/m}$, which, from Lemma 3.8, is

  $$\left\lceil \frac{n/m - 1}{t-1} \right\rceil.$$

- Case 2: Suppose that $(2q-2)n/m = (m-2)n/m$. In this case, $q = m/2$, which implies that m is even. Next we show that this case cannot happen under the hypothesis of the theorem.

  Notice that

  $$t = \left\lceil \frac{r}{m} \right\rceil = \left\lceil \frac{t}{2} + \frac{p}{m} \right\rceil.$$

  Therefore,

  $$t - 1 < \frac{t}{2} + \frac{p}{m} \leq t,$$

which implies, as $p < t$,

$$m\left(\frac{t}{2}-1\right) < p \leq \min\left\{t-1, \frac{mt}{2}\right\}. \quad (6)$$

Taking into account that $p < t$, we get

$$m\left(\frac{t}{2}-1\right) < t.$$

Thus,

$$t < \frac{2m}{m-2}, \quad \text{if } m > 2. \quad (7)$$

If $m \geq 6$, then $2 < \frac{2m}{m-2} \leq 3$. Therefore, for $m \geq 6$, $t = 2$. Also, from (6), $p = 1$, which implies that $r = m+1$. But this is impossible since $m < r-1$.

If $m = 4$, from (7) we deduce that $t = 2$ or 3. If $t = 3$, from (6), we get $p > 2$, which is impossible since $p < t$. If $t = 2$, from (6), we get $p = 1$, and then $r = 5$, which contradicts the fact that $m < r-1$ again.

Finally, if $m = 2$, from (6) we deduce that $p = t-1$ and, hence, $r = 2t-1$. But this contradicts the fact that r is even when $m = 2$.

□

The next theorem gives the main result in this paper.

Theorem 3.10 *Let n and r be two positive integers such that $2 \leq r \leq n$. Let $m_0 = 1$ and let $\{m_1, ..., m_t\}$ be the set of proper divisors of n smaller than $r-1$. Then,*

$$\max\{order(S) : S \in S_{n,r}\} = \max\left\{\left\lceil \frac{n-m_i}{(\lceil r/m_i \rceil - 1)m_i} \right\rceil, i = 0, 1, ..., t\right\}.$$

Proof. By Theorem 3.7,

$$\max\{order(S) : S \in S_{n,r}\} \leq \max\left\{\left\lceil \frac{n-m_i}{(\lceil r/m_i \rceil - 1)m_i} \right\rceil, i = 0, 1, ..., t\right\}.$$

Note that, if n is even and r is odd, then

$$\left\lceil \frac{n-1}{r-1} \right\rceil \geq \left\lceil \frac{n-2}{(\lceil r/2 \rceil - 1)2} \right\rceil.$$

Taking into account this observation, the result follows either from Lemma 3.8 or Lemma 3.9. □

The next corollary is a consequence of Theorem 3.10.

Corollary 3.11 *Let n, r_1, and r_2 be positive integers such that $2 \leq r_1 < r_2 \leq n$. Then,*

$$\max\{order(S) : S \in S_{n,r_1}\} \geq \max\{order(S) : S \in S_{n,r_2}\}.$$

Proof. Let $m_0 = 1$, and let $\{m_1, ..., m_{t_1}\}$ and $\{m_1, ..., m_{t_1}, .., m_{t_2}\}$ be, respectively, the sets of proper divisors of n smaller than $r_1 - 1$ and $r_2 - 1$. Notice that, for $i = 0, 1, ..., t_1$,

$$\left\lceil \frac{n - m_i}{(\lceil r_1/m_i \rceil - 1)m_i} \right\rceil \geq \left\lceil \frac{n - m_i}{(\lceil r_2/m_i \rceil - 1)m_i} \right\rceil.$$

Also, if $t_2 > t_1$, for any i such that $t_1 < i \leq t_2$, since $m_i \geq r_1 - 1$ and $\lceil r_2/m_i \rceil \geq 2$,

$$\left\lceil \frac{n-1}{r_1 - 1} \right\rceil \geq \left\lceil \frac{n - m_i}{(\lceil r_2/m_i \rceil - 1)m_i} \right\rceil.$$

Taking into account these observations, the result follows from Theorem 3.10. ◻

Next we present some particular cases of Theorem 3.10 by considering several values for r.

Corollary 3.12 *For $n \geq 2$,*

$$\max\{order(S) : S \in S_{n,2}\} = n - 1.$$

For $n \geq 3$,

$$\max\{order(S) : S \in S_{n,3}\} = \left\lceil \frac{n-1}{2} \right\rceil.$$

Proof. Since there are not proper divisors of n smaller than $r - 1$ in both cases, the result follows in a straightforward way from Theorem 3.10. Moreover, by Lemma 3.8 sets attaining the maximum order in $S_{n,2}$ and $S_{n,3}$, respectively, are $\{0, 1\}$ and $\{0, 1, 2\}$. ◻

Corollary 3.13 *For $n \geq 4$,*

$$\max\{order(S) : S \in S_{n,4}\} = \begin{cases} \lceil \frac{n-1}{3} \rceil & \textit{if } n \not\equiv 0 \ (\textit{mod } 2) \\ \lceil \frac{n-2}{2} \rceil & \textit{if } n \equiv 0 \ (\textit{mod } 2). \end{cases}$$

Proof. Note that 2 is the only possible positive proper divisor of n smaller than $r - 1$. Applying Theorem 3.10 and taking into account that

$$\left\lceil \frac{n-1}{3} \right\rceil \leq \left\lceil \frac{n-2}{2} \right\rceil, \quad \text{for all } n \geq 4$$

the result follows. By Lemma 3.8, a set attaining the maximum order when n is odd is $\{0, 1, 2, 3\}$. By Lemma 3.9, a set attaining the maximum exponent when n is even is $\{0, 1, n/2, 1 + n/2\}$. ◻

Corollary 3.14 *For $n \geq 5$,*

$$\max\{order(S) : S \in S_{n,5}\} = \begin{cases} \lceil \frac{n-1}{4} \rceil & \textit{if } n \not\equiv 0 \ (\textit{mod } 3) \textit{ or } n = 6 \\ \lceil \frac{n-3}{3} \rceil & \textit{if } n \equiv 0 \ (\textit{mod } 3), \ n \geq 9. \end{cases}$$

Proof. Note that 2 and 3 are the only possible proper divisors of n smaller than $r-1$. Applying Theorem 3.10 and taking into account that

$$\left\lceil \frac{n-2}{4} \right\rceil \leq \left\lceil \frac{n-1}{4} \right\rceil, \quad \text{for all } n,$$

and

$$\left\lceil \frac{n-1}{4} \right\rceil \leq \left\lceil \frac{n-3}{3} \right\rceil \quad \text{if and only if} \quad n \geq 7,$$

the result follows. By Lemma 3.8, a set attaining the maximum order when $n \not\equiv 0 \pmod 3$ or $n = 6$ is $\{0, 1, 2, 3, 4\}$. By Lemma 3.9, a set attaining the maximum exponent when $n \equiv 0 \pmod 3$ is $\{0, 1, n/3, 1 + n/3, 2n/3\}$. ∎

Regarding a lower bound for the set of exponents of $S_{n,r}$, based on Theorem 2.6, we get the following result.

Corollary 3.15 *Let $k \geq 2$. Let $S \subseteq \mathbb{Z}_n$ for some positive integer n. Let $r = |S|$. Then,*

$$\min\{order(S) : S \in S_{n,r}\} \geq \min\left\{k : \frac{(k+r-1)...(k+2)(k+1)}{(r-1)!} \geq n\right\}.$$

Next we give a new proof for a well-known result.

Corollary 3.16 *Let S be a basis for $\mathbb{Z}_n$. Then, $order(S)$ is either $n-1$ or does not exceed $\left\lfloor \frac{n}{2} \right\rfloor$.*

Proof. By Corollary 3.12,

$$\max\{order(S) : S \subseteq S_{n,2}\} = n - 1.$$

From Corollary 3.15,

$$\min\{order(S) : S \in S_{n,2}\} \geq \min\{k : k + 1 \geq n\} = n - 1.$$

Therefore, if $S \subseteq S_{n,2}$, $order(S) = n - 1$.

Moreover, from Corollary 3.12,

$$\max\{order(S) : S \subseteq S_{n,3}\} = \left\lfloor \frac{n}{2} \right\rfloor.$$

Taking into account Corollary 3.11, the result follows. ∎

References

[1] M.I. Bueno and S. Furtado, *On the exponent of r-regular primitive matrices*. Electr. Journal of Linear Algebra 17(2008), 28-47.

[2] H. Daode, *On Circulant Boolean Matrices*, Linear Algebra and its Applications, 136(1990), 107-117.

[3] P.J. Davis, *Circulant matrices*, Wiley-Interscience, NY, 1979.

[4] K.H. Kim-Buttler and J.R. Krabill, *Circulant Boolean relation matrices*, Czechoslovak Math. J. 24(1974), 247-251.

[5] P. Lancaster, *Theory of matrices*, Academic Press, NY, 1969.

[6] M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics, Vol. 165, Springer-Verlag, New York, 1996.

[7] S. Schwarz, *Circulant Boolean relation matrices*, Czechoslovak Math. J. 24(1974), 252-253.

[8] Y. Tan and M. Zhang, *Primitivity of Generalized Circulant Boolean Matrices*, Linear Algebra and its Applications, 234(1996), 61-69.

[9] J.Z. Wang and J.X. Meng, *The exponent of the primitive Cayley digraphs on finite Abelian groups*, Discrete Appl. Math., 80(1997), 177-191.