Electronic Journal of Linear Algebra

Volume 20 *ELA Volume 20 (2010)* Article 46

2010

On the gaps in the set of exponents of boolean primitive circulant matrices

Maribel I. Bueno
mbueno@math.ucsb.edu

Susana Furtado

Recommended Citation
Bueno, Maribel I. and Furtado, Susana. (2010), "On the gaps in the set of exponents of boolean primitive circulant matrices", *Electronic Journal of Linear Algebra*, Volume 20.
DOI: https://doi.org/10.13001/1081-3810.1399

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

ON THE GAPS IN THE SET OF EXPONENTS OF BOOLEAN PRIMITIVE CIRCULANT MATRICES*

MARIBEL I. BUENO† AND SUSANA FURTADO‡

Abstract. In this paper, we consider the problem of describing the possible exponents of boolean primitive circulant matrices. We give a conjecture for the possible such exponents and prove this conjecture in several cases. In particular, we consider in greater detail the case of matrices whose generating vector has three nonzero entries.

Key words. Circulant primitive matrices, Exponent of primitive matrices, Circulant digraphs, Basis for a group.

AMS subject classifications. 11P70, 05C25, 05C50.

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 one) 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 $n-1$.

The set of all n-by-n Boolean circulant matrices forms a multiplicative commutative semigroup C_n with $|C_n| = 2^n$ [3, 8]. In 1974, K.H. Kim-Buttler and J.R. Krabill [6], and S. Schwarz [9] investigated this semigroup thoroughly.

An n-by-n Boolean 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 $\exp(C)$. Let us also denote by E_n the set $\{\exp(C) : C \in C_n,\ C \text{ is primitive}\}$.

In [1], we stated the following question: Given a positive integer n, what is the set E_n?

The previous question can easily be restated in terms of circulant graphs or bases for finite cyclic groups, as we show next.

*Received by the editors December 7, 2009. Accepted for publication August 22, 2010. Handling Editor: Bryan L. Shader.

†Department of Mathematics, University of California, Santa Barbara, CA, USA (mbueno@math.ucsb.edu). Supported by Dirección General de Investigación (Ministerio de Ciencia y Tecnología) of Spain under grant MTM2009-09281.

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

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

Let C be a Boolean primitive circulant matrix, and let S be the set of positions corresponding to the nonzero entries in the generating vector of C, where the columns are counted starting with zero instead of one. C is the adjacency matrix of the circulant digraph $Cay(\mathbb{Z}_n, S)$. The vertex set of this graph is $\mathbb{Z}_n$ and there is an arc from u to $u + a \pmod n$ for every $u \in \mathbb{Z}_n$ and every $a \in S$. 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, a circulant digraph is primitive if and only if its adjacency matrix is. Moreover, if they are primitive, they have the same exponent. Therefore, finding the set E_n is equivalent to finding the possible exponents of circulant digraphs of order n.

Let S be a nonempty subset of the additive group $\mathbb{Z}_n$. For a positive integer k, we denote by kS the set given by

$$kS = \{s_1 + s_2 + \cdots + s_k : s_i \in S\} \subset \mathbb{Z}_n.$$

The set kS is called the *k-fold sumset* of S.

The set S is said to be a *basis* for $\mathbb{Z}_n$ if there exists a positive integer k such that $kS = \mathbb{Z}_n$. The smallest such k is called the *order* of S, denoted by $\text{order}(S)$. It is well known that the set $S = \{s_0, s_1, \ldots, s_r\} \subset \mathbb{Z}_n$ is a basis if and only if $\gcd(s_1 - s_0, \ldots, s_r - s_0, n) = 1$. We denote by S_n the set of all bases for $\mathbb{Z}_n$.

In [1], we proved that, given a matrix C in C_n, if S is the set of positions corresponding to the nonzero entries in the generating vector of C, then C is primitive if and only if S is a basis for $\mathbb{Z}_n$. Moreover, if C is primitive, then $\exp(C) = \text{order}(S)$. Therefore, finding the set E_n is equivalent to finding the possible orders of bases for the cyclic group $\mathbb{Z}_n$. This question is quite interesting by itself.

Note that the only primitive matrix in C_2 is the 2-by-2 matrix with all entries equal to 1, so $E_2 = \{1\}$. From now on, we assume that $n \geq 3$. In [1], we presented a conjecture concerning the possible exponents attained by n-by-n Boolean primitive circulant matrices which we consider here in greater detail.

Given a positive integer $n \geq 3$, let c be the smallest positive integer such that

$$\left\lfloor \frac{n}{c} \right\rfloor < \left\lfloor \frac{n}{c+1} \right\rfloor + c. \tag{1.1}$$

We call c the *critical point* of n and we denote it by c_n. Clearly, $c_n \leq \left\lfloor \frac{n}{2} \right\rfloor + 1$.

CONJECTURE 1. If C is an n-by-n Boolean primitive circulant matrix, then either

$$\exp(C) = \left\lfloor \frac{n}{j} \right\rfloor + k, \tag{1.2}$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

for some $j \in \{1, 2, \ldots, c_n - 1\}$ and $k \in \{-1, 0, 1, \ldots, j-2\}$, or

$$\exp(C) \leq \left\lfloor \frac{n}{c_n} \right\rfloor + c_n - 2. \tag{1.3}$$

Moreover, for every $m \leq \lfloor n/c_n \rfloor + c_n - 2$, there exists a matrix whose exponent is m.

In the literature, the problem of computing all possible exponents attained by circulant primitive matrices or, equivalently, by circulant digraphs, has been considered. In [2] and [11], it is shown that if a circulant matrix C is primitive, then its exponent is either $n-1$, $\lfloor n/2 \rfloor$, $\lfloor n/2 \rfloor - 1$ or does not exceed $\lfloor n/3 \rfloor + 1$. Matrices with exponents $n-1$, $\lfloor n/2 \rfloor$, $\lfloor n/2 \rfloor - 1$ are also characterized. All these results can be immediately translated into results about the possible orders of bases for a finite cyclic group. In a recent preprint [5], the authors prove that if S is a basis for $\mathbb{Z}_n$ of order greater than k for some positive integer k, then there exists d_k such that the order of S is within d_k of n/l for some integer $l \in [1, k]$. Notice that the result we present in Conjecture 1 produces gaps in the set of orders which are larger than the ones encountered in [5]. Moreover, we show that our gaps should be maximal. In [5], the authors also prove the existence of the additional gap $[\lfloor n/4 \rfloor + 3, \lfloor n/3 \rfloor - 2]$ although they do not use the techniques presented in the same paper. See [4] for a detailed proof of the existence of such gap.

In this paper, we give partial results related with Conjecture 1 and give a class of matrices for which it is shown that the conjecture holds. All the results in the paper are given in terms of bases for $\mathbb{Z}_n$ since the equivalent formulation of the problem in these terms resulted more fruitful than the original statement of the problem in terms of matrices.

In Section 2, we give the explicit value of the critical point c_n, as well as some of its interesting properties. In Section 3, we define Maximal Generalized Gaps and show that the set of gaps that follow from Conjecture 1 are maximal. In Section 4, we introduce some concepts and give some results concerning the order of general bases for $\mathbb{Z}_n$. In Section 5, we give some results about the order of bases for $\mathbb{Z}_n$ with cardinality 3. These results will allow us to prove Conjecture 1 for some classes of bases for $\mathbb{Z}_n$ in Section 6. In Section 7, we extend some of the results given in Sections 5 and 6 to general bases for $\mathbb{Z}_n$. Finally, in Section 8, we present the conclusions as well as some open questions.

2. The critical point. In this section, we prove that c_n is either $\lfloor \sqrt[3]{n} \rfloor$ or $\lfloor \sqrt[3]{n} \rfloor + 1$.

We first show that $c_n \leq \lfloor \sqrt[3]{n} \rfloor + 1$.

LEMMA 2.1. *Let n be a positive integer and $r = \lfloor \sqrt[3]{n} \rfloor$. Then*

$$\left\lfloor \frac{n}{r+1} \right\rfloor < \left\lfloor \frac{n}{r+2} \right\rfloor + r + 1. \tag{2.1}$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

Proof. Suppose that

$$\left\lfloor \frac{n}{r+1} \right\rfloor \geq \left\lfloor \frac{n}{r+2} \right\rfloor + r + 1. \tag{2.2}$$

We have

$$n = (r+2)m + t,$$

where $m = \left\lfloor \frac{n}{r+2} \right\rfloor$ and $0 \leq t < r+2$. Then (2.2) is equivalent to

$$\left\lfloor \frac{t+m}{r+1} \right\rfloor \geq r+1$$

which implies that

$$(r+1)^2 - t \leq m,$$

or, equivalently, multiplying by $r+2$ and adding t,

$$(r+1)^2(r+2) - t(r+2) + t \leq n.$$

Let us show that

$$(r+1)^3 \leq (r+1)^2(r+2) - t(r+2) + t \tag{2.3}$$

which leads to a contradiction, as $n < (r+1)^3$. Notice that

$$(r+1)^2 - t(r+1) \geq (r+1)^2 - (r+1)(r+1) = 0,$$

which implies (2.3). □

Next we show that $c_n \geq \lfloor \sqrt[3]{n} \rfloor$.

LEMMA 2.2. *Let n be a positive integer and $r = \lfloor \sqrt[3]{n} \rfloor$. Let p be an integer such that $0 < p < r$. Then*

$$\left\lfloor \frac{n}{p} \right\rfloor > \left\lfloor \frac{n}{p+1} \right\rfloor + p. \tag{2.4}$$

Proof. Suppose that

$$\left\lfloor \frac{n}{p+1} \right\rfloor + p \geq \left\lfloor \frac{n}{p} \right\rfloor.$$

Then

$$n \geq \left(\left\lfloor \frac{n}{p} \right\rfloor - p \right)(p+1).$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

We will show that $\left(\left\lfloor \frac{n}{p} \right\rfloor - p\right)(p+1) > n$, which gives a contradiction. Thus, (2.4) holds.

We have

$$\begin{aligned}\left(\left\lfloor \frac{n}{p} \right\rfloor - p\right)(p+1) &= \left\lfloor \frac{n}{p} \right\rfloor p + \left\lfloor \frac{n}{p} \right\rfloor - p^2 - p \\ &> n - p + \left\lfloor \frac{n}{p} \right\rfloor - p^2 - p \\ &= n + \left\lfloor \frac{n}{p} \right\rfloor - p^2 - 2p > n,\end{aligned}$$

where the last inequality follows because $\left\lfloor \frac{n}{p} \right\rfloor - p^2 - 2p > 0$, as

$$n \geq (p+1)^3 = p^3 + 3p^2 + 3p + 1 > p^3 + 2p^2 + p. \quad \square$$

It follows from Lemmas 2.1 and 2.2 that the smallest c_n such that $\left\lfloor \frac{n}{c_n} \right\rfloor < \left\lfloor \frac{n}{c_n+1} \right\rfloor + c_n$ is either $\lfloor \sqrt[3]{n} \rfloor$ or $\lfloor \sqrt[3]{n} \rfloor + 1$.

THEOREM 2.3. *Let n be a positive integer and $r = \lfloor \sqrt[3]{n} \rfloor$. If*

$$\left\lfloor \frac{n}{r} \right\rfloor < \left\lfloor \frac{n}{r+1} \right\rfloor + r \tag{2.5}$$

then $c_n = \lfloor \sqrt[3]{n} \rfloor$, otherwise $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$.

We now give some properties of c_n that will be useful later.

LEMMA 2.4. *Let n be a positive integer. Then $n \leq (c_n+1)^2(c_n-1)$.*

Proof. If $n = (c_n+1)^2(c_n-1) + k$ for some positive integer k, then

$$\left\lfloor \frac{n}{c_n+1} \right\rfloor + c_n = c_n^2 + c_n - 1 + \left\lfloor \frac{k}{c_n+1} \right\rfloor \leq c_n^2 + c_n - 1 + \left\lfloor \frac{k-1}{c_n} \right\rfloor = \left\lfloor \frac{n}{c_n} \right\rfloor,$$

which is a contradiction by the definition of c_n. $\square$

Before presenting the next results we introduce the following notation: If a and b are integers, with $b \geq a$, then $[a,b]$ denotes the set of integers in the real interval $[a,b]$. Moreover, $[a]$ denotes the set containing just the integer a. If $b < a$, then $[a,b] = \varnothing$.

The next lemma shows that, if $c_n \geq 3$, the interval $[\lfloor n/c_n \rfloor + 2, \lfloor n/(c_n-1) \rfloor - 1]$ is nonempty if and only if $n = 14$ or $n \geq 16$.

LEMMA 2.5. *Let n be a positive integer such that $c_n \geq 3$. Then $\lfloor n/(c_n-1) \rfloor \geq \lfloor n/c_n \rfloor + 3$ if and only if $n = 14$ or $n \geq 16$.*

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

Proof. If $c_n = 3$ or $c_n = 4$, then the result can be verified by a direct computation. Suppose that $c_n \geq 5$. Let $k - (c_n - 1)^3$. By Theorem 2.3, $k \geq 0$. Note that

$$\left\lfloor \frac{n}{c_n - 1} \right\rfloor \geq \left\lfloor \frac{n}{c_n} \right\rfloor + 3 \tag{2.6}$$

if and only if

$$\left\lfloor \frac{k}{c_n - 1} \right\rfloor \geq \left\lfloor \frac{k-1}{c_n} \right\rfloor + 5 - c_n.$$

Since $\left\lfloor \frac{k}{c_n - 1} \right\rfloor - \left\lfloor \frac{k-1}{c_n} \right\rfloor \geq 0$, if $c_n \geq 5$, then the result holds. □

The next lemma gives an upper bound for the length of the interval $\left[\left\lfloor \frac{n}{c_n} \right\rfloor, \left\lfloor \frac{n}{c_n - 1} \right\rfloor \right]$.

LEMMA 2.6. *Let n be a positive integer such that $c_n \geq 3$.*

- *If $c_n = \lfloor \sqrt[3]{n} \rfloor$, then*

$$\left\lfloor \frac{n}{c_n - 1} \right\rfloor - \left\lfloor \frac{n}{c_n} \right\rfloor \leq c_n + 3.$$

- *If $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $n = c_n^3 - 1$, then*

$$\left\lfloor \frac{n}{c_n - 1} \right\rfloor - \left\lfloor \frac{n}{c_n} \right\rfloor = c_n + 2.$$

- *If $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $n \leq c_n^3 - 2$, then*

$$\left\lfloor \frac{n}{c_n - 1} \right\rfloor - \left\lfloor \frac{n}{c_n} \right\rfloor \leq c_n + 1.$$

Proof. Let $n = pc_n + q$, where $p = \lfloor n/c_n \rfloor$ and $0 \leq q < c_n$. Notice that

$$\left\lfloor \frac{n}{c_n - 1} \right\rfloor - \left\lfloor \frac{n}{c_n} \right\rfloor = \left\lfloor \frac{p+q}{c_n - 1} \right\rfloor. \tag{2.7}$$

Suppose that $c_n = \lfloor \sqrt[3]{n} \rfloor$. By Lemma 2.4, $n \leq (c_n + 1)^2(c_n - 1)$, and therefore,

$$\left\lfloor \frac{n}{c_n} \right\rfloor \leq c_n^2 + c_n - 2.$$

Hence,

$$p + q \leq \left\lfloor \frac{n}{c_n} \right\rfloor + c_n - 1 \leq c_n^2 + 2c_n - 3 = (c_n - 1)(c_n + 3),$$

which implies that

$$\left\lfloor \frac{p+q}{c_n - 1} \right\rfloor \leq c_n + 3.$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

Suppose that $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$. Then $(c_n - 1)^3 \leq n \leq c_n^3 - 1$. If $n = c_n^3 - 1$,

$$p = \left\lfloor \frac{n}{c_n} \right\rfloor = c_n^2 - 1, \quad q = c_n - 1 \quad \text{and} \quad p + q = c_n^2 + c_n - 2 = (c_n - 1)(c_n + 2).$$

Then

$$\left\lfloor \frac{p+q}{c_n - 1} \right\rfloor = c_n + 2.$$

If $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $c_n^3 - c_n \leq n < c_n^3 - 1$, then $p = c_n^2 - 1$ and $q \leq c_n - 2$. Therefore,

$$p + q \leq c_n^2 - 1 + c_n - 2,$$

which implies

$$\left\lfloor \frac{p+q}{c_n - 1} \right\rfloor \leq c_n + 1.$$

If $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $n \leq c_n^3 - c_n - 1$, then

$$p + q \leq c_n^2 - 2 + c_n - 1,$$

which implies

$$\left\lfloor \frac{p+q}{c_n - 1} \right\rfloor \leq c_n + 1. \quad \square$$

LEMMA 2.7. *Let n be a positive integer such that $c_n \geq 3$. Then*

- *if $c_n = \lfloor \sqrt[3]{n} \rfloor$, then $4c_n \leq \lfloor n/c_n \rfloor + 3$;*
- *if $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $n = c_n^3 - 1$, then $3c_n \leq \lfloor n/c_n \rfloor + 2$.*

Proof. If $c_n = \lfloor \sqrt[3]{n} \rfloor$, then $n \geq c_n^3$, which implies that

$$\left\lfloor \frac{n}{c_n} \right\rfloor \geq c_n^2 \geq 4c_n - 3,$$

for $c_n \geq 3$. If $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $n = c_n^3 - 1$, then

$$\left\lfloor \frac{n}{c_n} \right\rfloor = c_n^2 - 1 \geq 3c_n - 2,$$

for $c_n \geq 3$. $\square$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

3. Maximal generalized gaps. Let n be a positive integer. Let $E_n = \{\text{order}(S) : S \in S_n\}$. It is well known [2] that $E_n \subset [1, n-1]$. We call a *gap* in E_n a nonempty interval $A \subset [1, n-1]$ such that $A \cap E_n = \emptyset$. We say that a gap A in E_n is maximal if $A' \cap E_n \neq \emptyset$ for any interval $A' \subset [1, n-1]$, with A strictly contained in A'.

For each positive integer n and each $j \in \{1, 2, \ldots, c_n - 1\}$, if

$$\left\lfloor \frac{n}{j+1} \right\rfloor + j \leq \left\lfloor \frac{n}{j} \right\rfloor - 2,$$

let

$$B_{j,n} = \left[\left\lfloor \frac{n}{j+1} \right\rfloor + j, \left\lfloor \frac{n}{j} \right\rfloor - 2 \right], \tag{3.1}$$

otherwise let $B_{j,n} = \emptyset$.

Clearly, if Conjecture 1 is true and $B_{j,n}$ is nonempty, $B_{j,n}$ is a gap in E_n. Though the intervals $B_{j,n}$ are not necessarily maximal gaps in E_n, the next theorem shows that, for each positive integer j, there is an integer n, with $j \leq c_n - 1$, such that $B_{j,n}$ is a maximal gap in E_n. Here, we use the result that, if $b > 1$ is a divisor of n, then $\text{order}(\{0, 1, b\}) = \lfloor \frac{n}{b} \rfloor + b - 2$, which is a particular case of Corollary 5.4. If $a \in \mathbb{Z}_n$, we denote by $\langle a \rangle$ the cyclic group generated by a in $\mathbb{Z}_n$.

THEOREM 3.1. *For each positive integer j, there is an integer n, with $j \leq c_n - 1$, such that $B_{j,n}$ is a maximal gap in E_n.*

Proof. We show that for each j there is an integer n, with $j \leq c_n - 1$, and two bases for $\mathbb{Z}_n$, say S_1 and S_2, such that $\text{order}(S_1) = \left\lfloor \frac{n}{j+1} \right\rfloor + j - 1$ and $\text{order}(S_2) = \left\lfloor \frac{n}{j} \right\rfloor - 1$.

Let $n = j(j+1)(j+3)$. First, we show that $c_n - 1 \geq j$. If $j = 1$, then $n = 8$ and $c_n = 3$. If $j > 1$, then $n - (j+1)^3 = j^2 - 1 > 0$, which implies that $\sqrt[3]{n} > j + 1$. Then $c_n - 1 \geq \lfloor \sqrt[3]{n} \rfloor - 1 \geq \sqrt[3]{n} - 2 > j - 1$, where the first inequality follows from Theorem 2.3.

Since $j+1$ divides n, by Corollary 5.4, for $S_1 = \{0, 1, j+1\}$, $\text{order}(S_1) = \left\lfloor \frac{n}{j+1} \right\rfloor + j - 1$. If $j > 1$, let $S_2 = \langle (j+1)(j+3) \rangle \cup (1 + \langle (j+1)(j+3) \rangle)$. Then, for $k > 0$,

$$kS_2 = \bigcup_{i=1}^{k} \left(i + \langle (j+1)(j+3) \rangle \right).$$

If $j = 1$, let $S_2 = \{0, 1\}$. In any case, it is easy to see that $\text{order}(S_2) = (j+1)(j+3) - 1 = \left\lfloor \frac{n}{j} \right\rfloor - 1$. □

4. Order of bases for $\mathbb{Z}_n$. Let T be a subset of the additive group $\mathbb{Z}_n$, and let $q \in \mathbb{Z}_n$. We define $q + T = \{q + t : t \in T\}$ and $q * T = \{qt : t \in T\}$.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

Clearly, if $S \subset \mathbb{Z}_n$ and $q \in \mathbb{Z}_n$, S is a basis for $\mathbb{Z}_n$ if and only if $q+S$ is a basis for $\mathbb{Z}_n$. Moreover, if S is a basis, order$(S) =$ order$(q+S)$.

LEMMA 4.1. *Let n and q be positive integers. If $S \in S_n$ and $\gcd(q,n) = 1$, then $q * S \in S_n$ and* order$(S) =$ order$(q * S)$.

Proof. It is enough to show that, for all $k \geq 1$, $|q * kS| = |kS|$, as $k(q * S) = q * (kS)$. Let $T = kS$. Clearly, $|q * T| \leq |T|$. Now suppose that $t_1, t_2 \in T$ with $t_1 \neq t_2$. Suppose that $qt_1 = qt_2 \pmod n$. Then $(t_1 - t_2)q = 0 \pmod n$, or equivalently, $(t_1 - t_2)q = kn$ for some positive integer k. Since $\gcd(q,n) = 1$, $t_1 - t_2 = 0 \pmod n$. As $0 \leq t_1, t_2 < n$, then $t_1 - t_2 = 0$, which is a contradiction. Thus, $|q * T| \geq |T|$, which completes the proof. □

We note that, if $\gcd(n,q) \neq 1$, then $q * S$ is not a basis for $\mathbb{Z}_n$.

Let $S_1, S_2 \subset \mathbb{Z}_n$. We say that S_1 and S_2 are equivalent, and we write $S_1 \sim S_2$, if there exist integers q_1 and q_2, where $\gcd(q_1, n) = 1$, such that $S_2 = q_2 + q_1 * S_1$. Note that $\sim$ is an equivalence relation. Clearly, from the observations above, if $S_1 \in S_n$ and $S_1 \sim S_2$, then $S_2 \in S_n$ and order$(S_1) =$ order(S_2).

Note that if $S = \{s_1, s_2, \ldots, s_t\} \in S_n$, then $S \sim \{0, s_2 - s_1, \ldots, s_t - s_1\}$. Therefore, in what follows we assume that $0 \in S$.

REMARK 1. Let $S = \{0, a\} \in S_n$. Then order$(S) = n - 1$ since $S \sim \{0, 1\}$, as a is a unit for $\mathbb{Z}_n$.

We now introduce some definitions that will be used in the next sections.

Let $S = \{0, s_1, \ldots, s_t\} \in S_n$. Then any element $q \in \mathbb{Z}_n$ can be expressed as $x_1 s_1 + \cdots + x_t s_t \pmod n$, for some nonnegative integers $x_1, \ldots, x_t$. Moreover, if $q \neq 0$, the smallest k such that $q \in kS$ is the minimum $x_1 + \cdots + x_t$ among all the solutions $(x_1, \ldots, x_t)$, $x_i \geq 0$, to $x_1 s_1 + \cdots + x_t s_t = q \pmod n$.

DEFINITION 4.2. Let $S = \{0, s_1, \ldots, s_t\} \in S_n$ and $q \in \mathbb{Z}_n$. If $q = 0$, then we define $\exp(q; S, n) = 1$; otherwise we define

$$\exp(q; S, n) := \min\{x_1 + \cdots + x_t : x_1 s_1 + \cdots + x_t s_t = q \pmod n,\ x_i \geq 0\}.$$

Clearly, if S is a basis for $\mathbb{Z}_n$ and $0 \in S$, order$(S) = \max\{\exp(q; S, n) : q \in \mathbb{Z}_n\}$.

DEFINITION 4.3. Let $S = \{0, s_1, \ldots, s_t\} \in S_n$, $q \in \mathbb{Z}_n$ and k be a positive integer. If $q \neq 0$, we say that q is $(k; S, n)$-periodic if k is the smallest nonnegative integer for which there are nonnegative integers $x_1, \ldots, x_t$ satisfying

$$x_1 + \cdots + x_t = \exp(q; S, n) \quad \text{and} \quad x_1 s_1 + \cdots + x_t s_t = q + kn.$$

If $q = 0$, we say that q is $(0; S, n)$-periodic. We say that S is K-periodic if there exist

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

$(K; S, n)$-periodic elements in $\mathbb{Z}_n$ and there are no $(k; S, n)$-periodic elements in $\mathbb{Z}_n$ for $k > K$.

REMARK 2. If the minimum nonzero element of a basis S of $\mathbb{Z}_n$, say b, is not 1, then S is not 0-periodic as any b', with $0 < b' < b$, is not $(0; S, n)$-periodic.

We finish this section with the following lemma.

LEMMA 4.4. [2] *Let $S \in S_n$ and m be a divisor of n. Suppose that S contains an element of order m. Then*

$$\text{order}(S) \leq \frac{n}{m} + m - 2.$$

By Remark 1, all bases for $\mathbb{Z}_n$, $n \geq 3$, with cardinality 2 have order $n-1$, and therefore, they satisfy Conjecture 1. In the next section we focus on bases with cardinality 3.

5. Order of bases for $\mathbb{Z}_n$ with cardinality 3. By $S_{n,r}$ we denote the set of all bases for $\mathbb{Z}_n$ with cardinality r.

For a given positive integer n, we define p_n as follows:

$$p_n = \begin{cases} \lfloor n/2 \rfloor + 1, & \text{if n is odd} \\ \lfloor n/2 \rfloor, & \text{if n is even.} \end{cases} \tag{5.1}$$

LEMMA 5.1. *Let $S = \{0, s_1, s_2\} \in S_{n,3}$. If $\gcd(s_1, n) = 1$ or $\gcd(s_2, n) = 1$ or $\gcd(s_2 - s_1, n) = 1$, then there exists $b \in \mathbb{Z}_n$ such that $b \leq p_n$ and $S \sim \{0, 1, b\}$.*

Proof. Without loss of generality, suppose that either $\gcd(s_1, n) = 1$ or $\gcd(s_2 - s_1, n) = 1$. In the first case, s_1 is a unit in $\mathbb{Z}_n$ and

$$S \sim S_1 = s_1^{-1} S = \{0, 1, s_1^{-1} s_2\}.$$

If $s_1^{-1} s_2 \leq \lfloor n/2 \rfloor$, the claim holds with $b = s_1^{-1} s_2$. If $s_1^{-1} s_2 > \lfloor n/2 \rfloor$, then

$$S \sim S_2 = 1 - S_1 = \{0, 1, n + 1 - s_1^{-1} s_2\}$$

and the claim holds with $b + 1 - s_1^{-1} s_2$. In the second case, that is, $\gcd(s_2 - s_1, n) = 1$, let

$$S_1 = -s_1 + S = \{0, s_2 - s_1, n - s_1\}.$$

Then $S \sim S_2 = s' S_1$, where $s' = (s_2 - s_1)^{-1}$. Now the argument used above applies to show the result. □

We note that if $\gcd(s_1, n) \neq 1$, $\gcd(s_2, n) \neq 1$ and $\gcd(s_2 - s_1, n) \neq 1$ and one of s_1, s_2, $s_2 - s_1$, $n - s_1$, $n - s_2$, $n - s_2 + s_1$ is a product of a divisor of n and a unit in $\mathbb{Z}_n$, then

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

there exist $a, b \in \mathbb{Z}_n$ such that a is a divisor of n, $a \neq 1$ and $S = \{0, s_1, s_2\} \sim \{0, a, b\}$. To see this, assume, without loss of generality, that $s_1 < s_2$. Note that

$$\begin{aligned} S \sim S_1 &= -s_1 + S = \{0, n - s_1, s_2 - s_1\} \\ &\sim S_2 = -s_2 + S = \{0, n + s_1 - s_2, n - s_2\}. \end{aligned}$$

Suppose that s_1 is a product of a divisor of n and a unit. The proof is analogous in the other mentioned cases, eventually by considering S_1 or S_2 instead of S. If $s_1|n$, then the result is clear; otherwise $s_1 = d_1 t_1$, where $d_1|n$ and $\gcd(n, t_1) = 1$. Then

$$S \sim t_1^{-1} S = \{0, d_1, t_1^{-1} s_2\},$$

and the result follows.

We were not able to prove that every basis $S \in S_{n,3}$ that is not equivalent to a basis of the form $\{0, 1, b\}$ is equivalent to a basis $\{0, a, b\}$ with $a \neq 1$ a divisor of n. However, numerical experiments show that if these bases exist, they are rare.

THEOREM 5.2. *Let $S = \{0, a, b\} \in S_{n,3}$, where a is a divisor of n and $a \neq 1$. Then*

$$a - 1 \leq \text{order}(S) \leq \frac{n}{a} + a - 2.$$

Proof. The inequality on the right follows from Lemma 4.4.

Consider the quotient map $f : \mathbb{Z}_n \to \mathbb{Z}_a$. Notice that $T = f(S) = \{0, f(b)\}$. Since S is a basis and a divides n, $\gcd(a, b) = 1$ and $f(b) \neq 0$. Therefore, T is a basis for $\mathbb{Z}_a$. Moreover, by Remark 1, order$(T) = a - 1$. Since order$(S) \geq$ order(T), we get order$(S) \geq a - 1$. □

>From now on, we consider bases S of $S_{n,3}$ of the form $\{0, 1, b\}$. For convenience, we write $\exp(q; b, n)$ instead of $\exp(q; S, n)$; we also say that S is 0-periodic instead of $(0; S, n)$-periodic.

If $S = \{0, 1, b\} \in S_{n,3}$, then, considering the standard addition and multiplication in $\mathbb{Z}$, for $k \geq 1$,

$$kS = [0, k] \cup [b, b + k - 1] \cup [2b, 2b + k - 2] \cup \cdots \cup [(k - 1)b, (k - 1)b + 1] \cup [kb].$$

For $j = 0, 1, \ldots, k$, let

$$I_{j,k} = [jb, jb + k - j]. \tag{5.2}$$

THEOREM 5.3. *Let $S = \{0, 1, b\} \in S_{n,3}$. Then*

$$\left\lfloor \frac{n}{b} \right\rfloor \leq \text{order}(S) \leq \left\lfloor \frac{n}{b} \right\rfloor + b - 2.$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

Proof. Let $n = mb + t$, with $m = \left\lfloor \frac{n}{b} \right\rfloor$ and $0 \leq t < b$. Considering the standard addition and multiplication in $\mathbb{Z}$, the largest element in kS is kb. Thus, if $k = \text{order}(S)$, then $kb \geq n - 1 = mb + t - 1$, which implies the inequality on the left.

We have $I_{0,b-1} \cup I_{1,b-1} = [0, 2b-2] \subset (b-1)S$. Moreover, $\{0, b, \ldots, (m-1)b\} \subset (m-1)S$. Thus,

$$((b-1) + (m-1))S = (b-1)S + (m-1)S = \mathbb{Z}_n.$$

which implies the inequality on the right. □

We now focus on 0-periodic bases of $S_{n,3}$.

COROLLARY 5.4. *Let $S = \{0, 1, b\} \in S_{n,3}$. If S is 0-periodic, then*

$$\text{order}(S) = \left\lfloor \frac{n}{b} \right\rfloor + b - 2.$$

Proof. Suppose $kS = \mathbb{Z}_n$. Let $j_0 = \left\lfloor \frac{n}{b} \right\rfloor - 1$. Note that $k \geq j_0$. Since S is 0-periodic, necessarily $[j_0 b, j_0 b + b - 1] \subset I_{j_0,k}$, which implies that

$$\left(\left\lfloor \frac{n}{b} \right\rfloor - 1\right) b + k - \left(\left\lfloor \frac{n}{b} \right\rfloor - 1\right) \geq \left\lfloor \frac{n}{b} \right\rfloor b - 1,$$

that is, $k \geq \left\lfloor \frac{n}{b} \right\rfloor + b - 2$. Then $\text{order}(S) \geq \left\lfloor \frac{n}{b} \right\rfloor + b - 2$. Since, by Theorem 5.3, $\text{order}(S) \leq \left\lfloor \frac{n}{b} \right\rfloor + b - 2$, the result follows. □

We next characterize the 0-periodic bases in $S_{n,3}$. Note that, by Remark 2, we may assume that these bases are of the form $\{0, 1, b\}$. First, we add a technical lemma.

It is clear that if b and w are positive integers, with $b \geq 2$, then the minimum $x + y$ among all the solutions of $x + by = w$, with $x, y \geq 0$, is obtained when y is $y_0 = \left\lfloor \frac{w}{b} \right\rfloor$. Since $x = w - by$, the minimum value of $x + y$ is $x_0 + y_0 = w - \left\lfloor \frac{w}{b} \right\rfloor (b-1)$. Note also that $x_0 = w - by_0 < b$. We then have the following lemma.

LEMMA 5.5. *Let $b, q \in \mathbb{Z}_n$, with $b \geq 2$ and $q \neq 0$. Then*

$$\exp(q; b, n) = \min\left\{ q + kn - (b-1)\left\lfloor \frac{q + kn}{b} \right\rfloor,\ k \geq 0 \right\}.$$

Note that

$$\exp(q; b, n) \leq q - (b-1)\left\lfloor \frac{q}{b} \right\rfloor \leq q,$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

where the first inequality follows from Lemma 5.5.

LEMMA 5.6. *Let $S = \{0, 1, b\} \in S_{n,3}$. Then S is 0-periodic if and only if either b divides n or*

$$(b-1)\left(\left\lfloor \frac{n}{b} \right\rfloor + 1\right) \leq n. \tag{5.3}$$

Proof. Suppose that S is 0-periodic and b is not a divisor of n. Let $q = \left\lfloor \frac{n}{b} \right\rfloor b - 1$. By Lemma 5.5 and Definition 4.3,

$$q - (b-1)\left\lfloor \frac{q}{b} \right\rfloor \leq q + n - (b-1)\left\lfloor \frac{n+q}{b} \right\rfloor. \tag{5.4}$$

As $n + q = 2\left\lfloor \frac{n}{b} \right\rfloor b + (t-1)$, for some $1 \leq t < b$, it follows that $\left\lfloor \frac{n+q}{b} \right\rfloor = 2\left\lfloor \frac{n}{b} \right\rfloor$. Also, $\left\lfloor \frac{q}{b} \right\rfloor = \left\lfloor \frac{n}{b} \right\rfloor - 1$. Thus, (5.4) is equivalent to (5.3).

To prove the converse note that, from Lemma 5.5, if b divides n, S is 0-periodic, as, for any $k > 0$,

$$kn - (b-1)\frac{kn}{b} > 0.$$

Now suppose that (5.3) holds. According to Lemma 5.5, we need to show that, for any $k > 0$ and any $q \in \mathbb{Z}_n \backslash \{0\}$,

$$q - (b-1)\left\lfloor \frac{q}{b} \right\rfloor \leq q + kn - (b-1)\left\lfloor \frac{q+kn}{b} \right\rfloor,$$

or equivalently,

$$(b-1)\left(\left\lfloor \frac{q+kn}{b} \right\rfloor - \left\lfloor \frac{q}{b} \right\rfloor\right) \leq kn.$$

Because of (5.3), it is enough to show that

$$\left\lfloor \frac{q+kn}{b} \right\rfloor - \left\lfloor \frac{q}{b} \right\rfloor \leq k\left(\left\lfloor \frac{n}{b} \right\rfloor + 1\right).$$

For $n = \left\lfloor \frac{n}{b} \right\rfloor b + t$, $0 \leq t < b$,

$$kn + q = k\left\lfloor \frac{n}{b} \right\rfloor b + kt + q = \left(k\left\lfloor \frac{n}{b} \right\rfloor + \left\lfloor \frac{q}{b} \right\rfloor + k\right) b + k(t-b) + \left(q - \left\lfloor \frac{q}{b} \right\rfloor b\right).$$

As, $k(t-b) + (q - \left\lfloor \frac{q}{b} \right\rfloor b) < b$, then

$$\left\lfloor \frac{q+kn}{b} \right\rfloor \leq k\left\lfloor \frac{n}{b} \right\rfloor + \left\lfloor \frac{q}{b} \right\rfloor + k,$$

completing the proof. □

THEOREM 5.7. *Let $S = \{0, 1, b\} \in S_{n,3}$. Then S is 0-periodic if and only if one of the following conditions is satisfied:*

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

i) b *is a divisor of* n;
ii) $b = \left\lfloor \frac{n}{j} \right\rfloor + 1$, *for some nonnegative integer* j. *In this case,* j *is unique and is given by* $\lfloor n/b \rfloor + 1$.

Proof. If b is a divisor of n, then Lemma 5.6 implies that S is 0-periodic. Now suppose that b is not a divisor of n. Let $i = \lfloor n/b \rfloor$ and $n = bi + t$, with $0 < t < b$. If $t < i$ then $b = \lfloor \frac{n}{i} \rfloor$, otherwise $b < \lfloor \frac{n}{i} \rfloor$. Since $n = (i+1)b + (t-b)$ and $t - b < 0$, it follows that $\lfloor \frac{n}{i+1} \rfloor < b$. Therefore,

$$\left\lfloor \frac{n}{i+1} \right\rfloor < b \leq \left\lfloor \frac{n}{i} \right\rfloor.$$

Suppose that $b = \left\lfloor \frac{n}{i+1} \right\rfloor + 1$. Since

$$b - 1 = \left\lfloor \frac{n}{i+1} \right\rfloor \leq \frac{n}{i+1},$$

we have

$$n \geq (b-1)(i+1).$$

Therefore, by Lemma 5.6, S is 0-periodic.

Now suppose that $\left\lfloor \frac{n}{i} \right\rfloor \geq b \geq \left\lfloor \frac{n}{i+1} \right\rfloor + 2$. Then

$$\frac{n}{i+1} < b - 1$$

and, by Lemma 5.6, S is not 0-periodic. □

6. The conjecture for bases in $S_{n,3}$. In this section, we prove the following result.

THEOREM 6.1. *Let* $S \in S_{n,3}$, $n \geq 3$. *Conjecture 1 holds if* S *satisfies one of the following conditions:*

i) S *is equivalent to* $\{0, a, b\}$, *where* a *is a divisor of* n *and* $a \geq c_n$;
ii) S *is equivalent to* $\{0, 1, b\}$ *for some* $b \leq \min\left\{p_n, \left\lfloor \frac{n}{c_n - 1} \right\rfloor - 1\right\}$;
iii) S *is equivalent to a* 0*-periodic basis.*

The rest of this section is dedicated to the proof of Theorem 6.1.

We first observe that, in general, if i and j are positive numbers, then

$$\frac{n}{i} + i < \frac{n}{j} + j$$

can be written as

$$(i - j)(n - ij) > 0,$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

which is equivalent to

$$j < \min\left\{i, \frac{n}{i}\right\} \vee j > \max\left\{i, \frac{n}{i}\right\}.$$

LEMMA 6.2. *Let $S = \{0, a, b\} \in S_{n,3}$, where a is a divisor of n such that $a \geq c_n$. Then either* order$(S) \leq \left\lfloor \frac{n}{c_n} \right\rfloor + c_n - 2$ *or*

$$\frac{n}{j} - 1 \leq \text{order}(S) \leq \frac{n}{j} + j - 2, \tag{6.1}$$

for some $j \in \{1, 2, \ldots, c_n - 1\}$.

Proof. Note that $n \neq 3$. If $n = 4$ then $c_n = a = 2$ and order$(S) = 2$, which implies that order$(S) \leq \left\lfloor \frac{n}{c_n} \right\rfloor + c_n - 2$. If $n = 8$ then $c_n = 3$ and $a = 4$; a direct computation considering all possible values of b, namely $1, 3, 5, 7$, shows that order$(S) = 4$ (in fact, in this case, $S \sim \{0, 1, b'\}$ for some $b' \in \mathbb{Z}_n$). Then (6.1) holds with $j = 2$. Now suppose that $n \neq 4$ and $n \neq 8$. Suppose that order$(S) > \left\lfloor \frac{n}{c_n} \right\rfloor + c_n - 2$. By Theorem 5.2,

$$a - 1 \leq \text{order}(S) \leq \frac{n}{a} + a - 2.$$

Then

$$\frac{n}{c_n} + c_n < \frac{n}{a} + a.$$

Taking into account the observation before this lemma and the fact that for $n \neq 3, 4, 8$, $c_n < n/c_n$, it follows that $a > n/c_n$, as, by hypothesis, $a \geq c_n$. Then, because a divides n, $a = \frac{n}{i}$ for some $i \in \{2, 3, \ldots, c_n - 1\}$. Then (6.1) holds with $j = i$. □

LEMMA 6.3. *Let $S = \{0, 1, b\} \in S_{n,3}$, with $b \leq p_n$. If S is 0-periodic and $b \geq \lfloor n/c_n \rfloor + 2$, then there exists $i \in [2, c_n - 1]$ such that*

$$i + \left\lfloor \frac{n}{i} \right\rfloor - 3 \leq \text{order}(S) \leq i + \left\lfloor \frac{n}{i} \right\rfloor - 2,$$

Proof. Note that $n > 3$ and $n \neq 8$. If b is a divisor of n, then $b = n/i$ for some $i \in [2, c_n - 1]$. By Corollary 5.4, order$(S) = \frac{n}{i} + i - 2$.

If b is not a divisor of n, then, taking into account Theorem 5.7 , $b = \lfloor n/i \rfloor + 1$ for some $i \in [2, c_n - 1]$. Let $m = \lfloor n/i \rfloor$ and $n = mi + t$, $0 \leq t < i$. By Corollary 5.4,

$$\text{order}(S) = \left\lfloor \frac{mi + t}{m + 1} \right\rfloor + \left\lfloor \frac{n}{i} \right\rfloor - 1 = \left\lfloor \frac{t - i}{m + 1} \right\rfloor + i + \left\lfloor \frac{n}{i} \right\rfloor - 1.$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

If $m+1 \geq i-t$, then

$$\left\lfloor \frac{t-i}{m+1} \right\rfloor = -1.$$

If $m+1 < i-t$, then

$$\left\lfloor \frac{t-i}{m+1} \right\rfloor = -2,$$

as $i - t \leq i \leq c_n - 1 \leq \left\lfloor \frac{n}{c_n} \right\rfloor - 1 \leq b - 3 \leq 2b = 2m + 2$. Note that $c_n \leq \left\lfloor \frac{n}{c_n} \right\rfloor$ for $n \neq 3, 8$. Thus, the result follows. □

LEMMA 6.4. *Let* $S = \{0, 1, b\} \in S_{n,3}$. *If* $b \in \left[c_n + 1, \left\lfloor \frac{n}{c_n} \right\rfloor + 1\right]$, *then* order$(S) \leq \left\lfloor \frac{n}{c_n} \right\rfloor + c_n - 2$.

Proof. By Theorem 5.3, order$(S) \leq \lfloor \frac{n}{b} \rfloor + b - 2$. Thus, it is enough to show that

$$b + \left\lfloor \frac{n}{b} \right\rfloor \leq c_n + \left\lfloor \frac{n}{c_n} \right\rfloor. \tag{6.2}$$

Taking into account the observation before Lemma 6.2, if $c_n < \min\{b, \frac{n}{b}\}$ then

$$b + \left\lfloor \frac{n}{b} \right\rfloor \leq b + \frac{n}{b} < c_n + \frac{n}{c_n},$$

which implies (6.2), as c_n is an integer. Since

$$c_n < \min\left\{b, \frac{n}{b}\right\} \Leftrightarrow \begin{cases} c_n < b \leq \left\lfloor \frac{n}{c_n} \right\rfloor & \text{if } c_n \text{ is not a divisor of } n \\ c_n < b \leq \frac{n}{c_n} - 1 & \text{if } c_n \text{ is a divisor of } n \end{cases},$$

we now need to show that (6.2) holds if either $b = \left\lfloor \frac{n}{c_n} \right\rfloor + 1$ or $b = \frac{n}{c_n}$ and c_n divides n. The latter is immediate. For the first case, note that

$$\left\lfloor \frac{n}{\left\lfloor \frac{n}{c_n} \right\rfloor + 1} \right\rfloor = c_n - 1,$$

as, if $n = \left\lfloor \frac{n}{c_n} \right\rfloor c_n + t$, with $0 \leq t < c_n$, then

$$n = (c_n - 1)\left(\left\lfloor \frac{n}{c_n} \right\rfloor + 1\right) + \left(t - c_n + \left\lfloor \frac{n}{c_n} \right\rfloor + 1\right),$$

with $0 \leq t - c_n + \left\lfloor \frac{n}{c_n} \right\rfloor + 1 < \left\lfloor \frac{n}{c_n} \right\rfloor + 1$. □

Next we give a result that allows us to show that the conjecture holds if $S = \{0, 1, b\}$, with $b \leq p_n$ and $b \in [\lfloor n/c_n \rfloor + 2, \lfloor n/(c_n - 1) \rfloor - 1]$. Note that $\lfloor n/c_n \rfloor + 2 \leq p_n$ if and only

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

if $c_n \geq 3$. Also, by Lemma 2.5, for $c_n \geq 3$ the previous interval is nonempty if and only if $n = 14$ or $n \geq 16$. Finally, observe that $\lfloor n/b \rfloor = c_n - 1$.

We think the method used to prove the conjecture in this case might be generalizable to the cases in which $b \in [\lfloor \frac{n}{c_n - k} \rfloor, \lfloor \frac{n}{c_n - k + 1} \rfloor - 1]$, with $1 \leq k \leq c_n - 3$, when this interval is nonempty. Some results presented in Section 2 will be used.

LEMMA 6.5. *Let n be a positive integer such that $c_n \geq 3$, $b \in \left[\lfloor \frac{n}{c_n} \rfloor + 2, \lfloor \frac{n}{c_n - 1} \rfloor - 1\right]$ and $t = n - (c_n - 1)b$. If*

$$\left\lfloor \frac{n}{c_n} \right\rfloor + 1 < b - t, \tag{6.3}$$

then either $c_n = \lfloor \sqrt[3]{n} \rfloor$, or $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $n = c_n^3 - 1$. Moreover, $3c_n \leq \lfloor n/c_n \rfloor + 2$.

Proof. Let $m = c_n - 1$ and $r = \lfloor n/c_n \rfloor + c_n - 2$. First we show that if (6.3) holds, then $b = \left\lfloor \frac{n}{c_n - 1} \right\rfloor - 1$. Suppose that $b \leq \left\lfloor \frac{n}{c_n - 1} \right\rfloor - 2$. Then $t \geq 2(c_n - 1)$ and, taking into account Lemma 2.6, we get

$$b - t \leq \left\lfloor \frac{n}{c_n - 1} \right\rfloor - 2 - 2(c_n - 1) \leq \left\lfloor \frac{n}{c_n} \right\rfloor + 1,$$

a contradiction. Now suppose that $b = \left\lfloor \frac{n}{c_n - 1} \right\rfloor - 1$ and (6.3) holds. Then $t \geq c_n - 1$. If $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $n \leq c_n^3 - 2$, then, taking into account Lemma 2.6,

$$b - t \leq \left\lfloor \frac{n}{c_n - 1} \right\rfloor - 1 - (c_n - 1) \leq \left\lfloor \frac{n}{c_n} \right\rfloor + 1,$$

a contradiction. Thus, $c_n = \lfloor \sqrt[3]{n} \rfloor$ or $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $n = c_n^3 - 1$. Taking into account Lemma 2.7, the result follows. □

LEMMA 6.6. *Let $S = \{0, 1, b\} \in S_{n,3}$, with $c_n \geq 3$. Suppose that $b \in [\lfloor n/c_n \rfloor + 2, \lfloor n/(c_n - 1) \rfloor - 1]$. Then*

$$\text{order}(\{0, 1, b\}) \leq \left\lfloor \frac{n}{c_n} \right\rfloor + c_n - 2.$$

Proof. Note that $n = 14$ or $n \geq 16$ for the interval $[\lfloor n/c_n \rfloor + 2, \lfloor n/(c_n - 1) \rfloor - 1]$ not to be empty. Let $r = \left\lfloor \frac{n}{c_n} \right\rfloor + c_n - 2$ and $n = (c_n - 1)b + t$ for some $0 < t < b$. Note that $t \geq c_n - 1$. Let $m = \lfloor n/b \rfloor = c_n - 1$. Since $c_n \leq \lfloor n/c_n \rfloor$, $2m \leq r$.

Let

$$k_1(i) = ib \text{ and } k_2(i) = i(b - 1) + r, \text{ for } i \in \{0, 1, \ldots, m\},$$

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

$$k_1(i) = ib - n \text{ and } k_2(i) = i(b-1) + r - n, \text{ for } i \in \{m+1, m+2, \ldots, 2m\},$$

and

$$k_1(i) = ib - 2n \text{ and } k_2(i) = i(b-1) + r - 2n, \text{ for } i \in \{2m+1, 2m+2, \ldots, 3m\}.$$

Consider the following intervals in $\mathbb{Z}$: $I_i = [k_1(i), k_2(i)]$, $i \in \{0, 1, \ldots, 3m\}$. Note that, for each $i = 0, 1, \ldots, 3m$, $k_1(i) < k_2(i)$ and $k_1(i) < n$. Also, $0 \leq k_1(i)$, for $i = 0, 1, \ldots, 3m$, $i \neq 2m+1$. We have $rS \equiv \bigcup_{i=0}^{r} I_i \pmod n$. We next show that if

$$b - t \leq \lfloor n/c_n \rfloor + 1, \tag{6.4}$$

then $\bigcup_{i=0}^{2m} I_i \equiv \mathbb{Z}_n \pmod n$; if

$$\lfloor n/c_n \rfloor + 1 < b - t, \tag{6.5}$$

then $\bigcup_{i=0}^{3m} I_i \equiv \mathbb{Z}_n \pmod n$, which implies $rS = \mathbb{Z}_n$. Note that $2m < r$ and, by Lemma 6.5, if (6.5) holds, $3m \leq r$.

Consider the intervals I_i, $i = 0, 1, \ldots, 3m$, ordered in the following way:

$$I_0, I_{2m+1}, I_{m+1}, I_1, I_{2m+2}, I_{m+2}, \ldots, I_{3m}, I_{2m}, I_m.$$

Clearly, for $j = 1, 2, \ldots, m$,

$$k_1(j-1) \leq k_1(m+j) \leq k_1(j) \text{ and } k_1(2m+j) \leq k_1(m+j).$$

We show that, for each $j = 1, 2, \ldots, m$,

(i) $k_2(m+j) + 1 \geq k_1(j)$;
(ii) $k_2(j-1) + 1 \geq k_1(m+j)$ if (6.4) holds;
(iii) $k_2(j-1) + 1 \geq k_1(2m+j) \geq k_1(j-1)$ if (6.5) holds;
(iv) $k_2(2m+j) + 1 \geq k_1(m+j)$ if (6.5) holds;
(v) $k_2(m) \geq n - 1$,

which completes the proof.

Condition (i) follows easily taking into account that $c_n + t \leq \lfloor \frac{n}{c_n} \rfloor + 1$, as

$$t - (c_n - 1)b \leq n - (c_n - 1)\left(\left\lfloor \frac{n}{c_n} \right\rfloor + 2\right) = \left(n - c_n \left\lfloor \frac{n}{c_n} \right\rfloor\right) + \left\lfloor \frac{n}{c_n} \right\rfloor - 2(c_n - 1)$$

$$\leq c_n - 1 + \left\lfloor \frac{n}{c_n} \right\rfloor - 2(c_n - 1) = \left\lfloor \frac{n}{c_n} \right\rfloor - c_n + 1.$$

Condition (ii) follows from a simple calculation.

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

Now suppose that (6.5) holds. The first inequality in condition (iii) holds as

$$b - 2t \leq \left\lfloor \frac{n}{c_n - 1} \right\rfloor - 1 - 2(c_n - 1) \leq \left\lfloor \frac{n}{c_n} \right\rfloor + 1 \leq \left\lfloor \frac{n}{c_n} \right\rfloor + c_n - j,$$

where the second inequality follows from Lemma 2.6. Since we have shown in (i) that $t \leq \left\lfloor \frac{n}{c_n} \right\rfloor - c_n + 1$, then

$$b > \lfloor n/c_n \rfloor + 1 + t > 2t,$$

which implies the second inequality.

Condition (iv) holds if $2c_n + t \leq \lfloor n/c_n \rfloor + 2$. By Lemma 6.5 either $c_n = \lfloor \sqrt[3]{n} \rfloor$ or $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $n = c_n^3 - 1$. If $c_n = \lfloor \sqrt[3]{n} \rfloor$, by Lemma 2.6,

$$t \leq \left\lfloor \frac{n}{c_n - 1} \right\rfloor - 1 - \left\lfloor \frac{n}{c_n} \right\rfloor - 1 \leq c_n + 3 - 2.$$

Thus, taking into account Lemma 2.7,

$$2c_n + t \leq 3c_n + 1 \leq \left\lfloor \frac{n}{c_n} \right\rfloor + 2.$$

If $c_n = \lfloor \sqrt[3]{n} \rfloor + 1$ and $n = c_n^3 - 1$, by Lemma 2.6,

$$t \leq \left\lfloor \frac{n}{c_n - 1} \right\rfloor - 1 - \left\lfloor \frac{n}{c_n} \right\rfloor - 1 \leq c_n + 2 - 2.$$

By Lemma 2.7,

$$2c_n + t \leq 3c_n \leq \left\lfloor \frac{n}{c_n} \right\rfloor + 2.$$

Finally, note that condition (v) is equivalent to $t \leq \lfloor n/c_n \rfloor$, which holds as $c_n \geq 3$ and we have shown that $t + c_n \leq \lfloor n/c_n \rfloor + 1$. □

Proof of Theorem 6.1. It follows from Lemma 6.2 that if condition i) holds then Conjecture 1 is satisfied.

Now suppose that $S = \{0, 1, b\}$, with $b \leq p_n$. If $b \leq c_n$, Conjecture 1 holds by Theorem 5.3; if $b \in [c_n + 1, \left\lfloor \frac{n}{c_n} \right\rfloor + 1]$, the conjecture holds by Lemma 6.4; if $b \in \left[\left\lfloor \frac{n}{c_n} \right\rfloor + 2, \left\lfloor \frac{n}{c_n - 1} \right\rfloor - 1 \right]$ then $c_n \geq 3$ and Conjecture 1 holds by Lemma 6.6. Finally, if $b \geq \lfloor n/c_n \rfloor + 2$ and S is 0 -periodic, Conjecture 1 holds by Lemma 6.3. Since two equivalent bases have the same order, the result follows. □

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

7. The conjecture for bases with cardinality larger than 3. In this section, we include some partial results regarding Conjecture 1 for bases with cardinality larger than 3.

The next lemma shows that to prove Conjecture 1 it is enough to consider bases S for $\mathbb{Z}_n$ such that

$$|S| \leq \max\left\{\frac{n}{d}\left(\left\lfloor\frac{d-2}{\lfloor n/c_n\rfloor + c_n - 3}\right\rfloor + 1\right) : d|n,\ d \geq \lfloor n/c_n\rfloor + c_n - 1\right\}.$$

LEMMA 7.1. [7] *Let n be a positive integer and $r \in [2, n-1]$. Let $S \in S_n$ be such that* order$(S) \geq r$. *Then*

$$|S| \leq \max\left\{\frac{n}{d}\left(\left\lfloor\frac{d-2}{r-1}\right\rfloor + 1\right) : d|n,\ d \geq r+1\right\}.$$

COROLLARY 7.2. *If $S \in S_n$ is equivalent to $\{0, 1, s_1, \ldots, s_r\} \in S_n$, with $1 < s_1 < \cdots < s_r$, then*

$$\left\lfloor\frac{n}{s_r}\right\rfloor \leq \text{order}(S) \leq \min_{i\in\{1,2,\ldots,r\}}\left\{\left\lfloor\frac{n}{s_i}\right\rfloor + s_i - 2\right\}.$$

Proof. The proof of the inequality on the left is analogous to the one given in the proof of the left inequality in Theorem 5.3. The inequality on the right follows from the fact that order$(S) \leq \min_i\{\text{order}(\{0, 1, s_i\})\}$ and Theorem 5.3. □

We then have the following consequence of Corollary 7.2, Lemmas 6.4 and 6.6 and Theorem 5.3.

COROLLARY 7.3. *If $S \in S_n$ is equivalent to $\{0, 1, s_1, \ldots, s_r\}$ and there exists $i \in \{1, 2, \ldots, r\}$ such that $s_i \in \left[c_n, \left\lfloor\frac{n}{c_n - 1}\right\rfloor - 1\right]$, then S satisfies Conjecture 1.*

COROLLARY 7.4. *If $S \in S_n$ is equivalent to $S' = \{0, s_1, \ldots, s_r\}$ and S' contains an element of order m, with $m \in \{c_n, \ldots, \frac{n}{c_n}\}$, then S satisfies Conjecture 1.*

Proof. By Lemma 4.4,

$$\text{order}(S) \leq \frac{n}{m} + m - 2.$$

Taking into account the observation before Lemma 6.2, if m is a divisor of n such that $m \in \{c, \ldots, \frac{n}{c}\}$, then $\frac{n}{m} + m \leq \frac{n}{c_n} + c_n$, which implies that $\frac{n}{m} + m \leq \left\lfloor\frac{n}{c_n}\right\rfloor + c_n$ and the result follows. □

Electronic Journal of Linear Algebra ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 20, pp. 640-660, October 2010

ELA
http://math.technion.ac.il/iic/ela

8. Conclusions and open problems. Given a positive integer $n \geq 3$, we defined the critical point c_n and conjectured that all intervals of the form $[\lfloor n/i \rfloor + i - 1, \lfloor n/(i-1) \rfloor - 2]$, with $2 \leq i < c_n$, are gaps in the set E_n of orders of bases for $\mathbb{Z}_n$. It was already known that bases with cardinality 2 have order $n-1$, and therefore, they satisfy our conjecture.

In this paper, we have proven some partial results regarding bases of cardinality 3 and larger. The main result is Theorem 23. However, there are many open questions still to answer. For bases with cardinality 3, it needs to be proven that the conjecture holds when a basis S is equivalent to $\{0, 1, b\}$ with $b \in [\lfloor n/(c_n - 1) \rfloor, p_n]$, where p_n is defined in (5.1). We think that in order to prove this result the concept of K-periodicity needs to be studied in greater detail. If a basis S is equivalent to $\{0, a, b\}$, where a is a divisor of n, $a \neq 1$, it is still an open question if the conjecture holds when $a < c_n$. Though we did not show that all bases for $\mathbb{Z}_n$ with cardinality 3 are equivalent to a set of the form $\{0, 1, b\}$ or $\{0, a, b\}$, where $a \neq 1$ is a divisor of n, at least for almost all bases this seems to happen. If there exist bases for $\mathbb{Z}_n$ which are not equivalent to sets of any of those two types, the conjecture should also be proven for them.

Finally, we have only proven that the conjecture holds for very specific bases for $\mathbb{Z}_n$ with cardinality larger than 3, so there is a lot to be done concerning those bases.

REFERENCES

[1] M.I. Bueno, S. Furtado, and N. Sherer. Maximum exponent of Boolean circulant matrices with constant number of nonzero entries in its generating vector. *Electron. J. Combin.*, 16(1), Research Paper no. 66, 2009.
[2] H. Daode. On circulant boolean matrices. *Linear Algebra Appl.*, 136:107–117, 1990.
[3] P.J. Davis. *Circulant Matrices*. Wiley-Interscience, New York, 1979.
[4] P. Dukes and S. Herke. The structure of the exponent set for finite cyclic groups. ArXiv: 0810.0881v1, 2008.
[5] P. Dukes, P. Hegarty, and S. Herke. On the possible orders of a basis for a finite cyclic group. Preprint, 2010.
[6] K.H. Kim-Buttler and J.R. Krabill. Circulant Boolean relation matrices. *Czechoslovak Math. J.*, 24:247–251, 1974.
[7] B. Klopsch and V.F. Lev. Generating Abelian groups by addition only. *Forum Math.*, 21:23–41, 2009.
[8] P. Lancaster. *Theory of Matrices*. Academic Press, New York, 1969.
[9] S. Schwarz. Circulant Boolean relation matrices. *Czechoslovak Math. J.*, 24:252–253, 1974.
[10] Y. Tan and M. Zhang. Primitivity of generalized circulant Boolean matrices. *Linear Algebra Appl.*, 234:61–69, 1996.
[11] J.Z. Wang and J.X. Meng. The exponent of the primitive Cayley digraphs on finite Abelian groups. *Discrete Appl. Math.*, 80:177–191, 1997.