On the possible orders of a basis for a finite cyclic group

Peter Dukes*
Mathematics and Statistics
University of Victoria, Victoria BC, Canada V8W3R4
dukes@uvic.ca

Peter Hegarty†
Mathematical Sciences
Chalmers University of Technology and University of Gothenburg
41296 Gothenburg, Sweden
hegarty@chalmers.se

Sarada Herke‡
Mathematics and Statistics
University of Victoria, Victoria BC, Canada V8W3R4
sarada@uvic.ca

Submitted: Sep 22, 2009; Accepted: Apr 27, 2010; Published: XX
Mathematics Subject Classification: 11B13, 11B75 (primary), 05C20 (secondary)

Abstract

We prove a result concerning the possible orders of a basis for the cyclic group $\mathbb{Z}_n$, namely: For each $k \in \mathbb{N}$ there exists a constant $c_k > 0$ such that, for all $n \in \mathbb{N}$, if $A \subseteq \mathbb{Z}_n$ is a basis of order greater than n/k, then the order of A is within c_k of n/l for some integer $l \in [1, k]$. The proof makes use of various results in additive number theory concerning the growth of sumsets. Additionally, exact results are summarized for the possible basis orders greater than $n/4$ and less than $\sqrt{n}$. An equivalent problem in graph theory is discussed, with applications.

*Research supported by NSERC
†Research supported by Swedish Science Research Council (Vetenskapsrådet)
‡Research supported by NSERC

1 Introduction

Let G be an abelian group, written additively, and A a subset of G. For a positive integer h we denote by hA the subset of G consisting of all possible sums of h not necessarily distinct elements of A, i.e.:

$$hA = \{a_1 + \cdots + a_h : a_i \in A\}. \tag{1.1}$$

This set is called the *h-fold sumset* of A. We say that A is a *basis* for G if $hA = G$ for some $h \in \mathbb{N}$. Define the function $\rho : 2^G \to \mathbb{N} \cup \{\infty\}$ as follows:

$$\rho(A) := \begin{cases} \min\{h : hA = G\}, & \text{if } A \text{ is a basis for } G, \\ \infty, & \text{otherwise.} \end{cases} \tag{1.2}$$

In the case where $\rho(A) < \infty$, this invariant is usually referred to as the *order*[1] of the basis A.

Now let us specialise to the case $G = \mathbb{Z}_n$, a finite cyclic group. Throughout this paper we will write $\rho_n(A)$ when referring to a subset A of $\mathbb{Z}_n$. Clearly a subset $A \subseteq \mathbb{Z}_n$ is a basis if and only if the greatest common divisor of its elements is relatively prime to n. Also, it is easy to see that, if $\rho_n(A) < \infty$ then $\rho_n(A) \leq n - 1$, with equality if and only if $A = \{a_1, a_2\}$ is a 2-element set with $\gcd(a_2 - a_1, n) = 1$. Hence the range of the function ρ_n is contained inside $[1, n-1] \cup \{\infty\}$. It has been known for some time that, for large enough n, the range of ρ_n does not contain the entire interval of integers $[1, n-1]$. For instance, in somewhat different language, it was shown in [D] that roughly half of this interval, specifically $[\lfloor \frac{n}{2} \rfloor + 1, n-2]$, is disjoint from the range of ρ_n. An additional gap $[\lfloor \frac{n}{3} \rfloor + 2, \lfloor \frac{n}{2} \rfloor - 2]$ in the range of ρ_n was discovered by Wang and Meng in [WM]. These gaps, when considered in light of earlier work on sumsets (see Section 2) and exponents of primitive digraphs (see Section 5), led us to believe in an infinite sequence of gaps, between about $\frac{n}{k+1}$ and $\frac{n}{k}$. This is essentially our main result, stated precisely below.

Theorem 1.1. *For each $k \in \mathbb{N}$ there exists an absolute constant $c_k > 0$ such that the following holds:*

For any $n \in \mathbb{N}$, if A is a basis for $\mathbb{Z}_n$ for which $\rho_n(A) \geq n/k$, then there is some integer $l \in [1, k]$ such that $|\rho_n(A) - n/l| < c_k$.

Observe that Theorem 1.1 implies the somewhat surprising fact that the range of ρ_n is asymptotically sparse.

Corollary 1.2.

$$\lim_{n\to\infty} \frac{|\{\rho_n(A) : A \subseteq \mathbb{Z}_n\}|}{n} = 0. \tag{1.3}$$

Theorem 1.1 is a negative result for basis orders. It is not hard to explicitly construct certain bases A of $\mathbb{Z}_n$ with $\rho_n(A)$ achieving various special values. For instance, it was previously mentioned that $n-1$ is realizable as a basis order for every $n \in \mathbb{N}$. If $n \geq 3$, we have

[1] In [KL] the term *positive diameter* appears, with different notation.

$\rho_n(\{0,1,2\}) = \lfloor \frac{n}{2} \rfloor$. And in the recent manuscript [HMV], the interval $[1, \sqrt{n}]$ of small basis orders are obtained.

The primary purpose of our note is to prove Theorem 1.1. The background results from additive number theory are given in Section 2. These concern the structure of sets with small doubling. The technical aspects of the proof are given in Section 3, roughly as follows. On the one hand, the statement of the theorem says something about the possible orders of a basis for $\mathbb{Z}_n$ when that order is large, namely of order n. On the other hand, various results from additive number theory imply that if A is a basis for $\mathbb{Z}_n$, then the iterated sumsets hA cannot grow in size 'too slowly' and, if the growth rate is close to the slowest possible, then A has a very restricted structure. Putting these two things together allows us to describe closely the structure of (a small multiple of) a basis A of large order, and from there we can establish the result.

Despite our main theorem and previous existence results, we remain far from a complete characterization of the possible basis orders for $\mathbb{Z}_n$. However, in Section 4, we give a summary of known results leading to an exact list for all $n \leq 64$. Section 5 concludes with some applications in the language of graph theory.

2 Preliminaries

Here we state three results from the additive number theory literature which will be used in our proof of Theorem 1.1.

The first result is part of Theorem 2.5 of [KL]:

Theorem 2.1. (Klopsch-Lev) *Let $n \in \mathbb{N}$ and $\rho \in [2, n-1]$. Let A be a basis for $\mathbb{Z}_n$ such that $\rho_n(A) \geq \rho$. Then*

$$|A| \leq \max \left\{ \frac{n}{d} \left(\left\lfloor \frac{d-2}{\rho - 1} \right\rfloor + 1 \right) : d \mid n,\ d \geq \rho + 1 \right\}, \tag{2.1}$$

In particular, for each fixed $k \in \mathbb{N}$, if $\rho_n(A) \geq n/k$ and n is large enough, then $|A| \leq 2k$.

The second result concerns the structure of subsets of $\mathbb{Z}_n$ with small doubling and is Theorem 1 of [DF]:

Theorem 2.2. (Deshouillers-Freiman) *Let $n \in \mathbb{N}$ and A be a non-empty subset of $\mathbb{Z}_n$ such that $|A| < 10^{-9}n$ and $|2A| < 2.04|A|$. Then there is a subgroup $H \subsetneq G$ such that one of the following three cases holds:*

(i) if the number of cosets of H met by A, let us call it s, is different from 1 and 3, then A is included in an arithmetic progression of l cosets modulo H such that

$$(l-1)|H| \leq |2A| - |A|. \tag{2.2}$$

(ii) if A meets exactly three cosets of H, then (2.2) holds with l replaced by $\min\{l, 4\}$.

(iii) if A is included in a single coset of H, then $|A| > 10^{-9}|H|$.

Furthermore, when $l \geq 2$, there exists a coset of H which contains more than $\frac{2}{3}|H|$ elements from A, a relation superseded by (2.2) when $l \geq 4$.

Remark 2.3. In [DF] the authors remark that they expect that the same structure theorem holds for larger constants than 2.04 and 10^{-9} respectively. This is known to be the case when n is prime, according to the so-called *Freiman-Vosper theorem*. For a proof of that 'classical' result, see Theorem 2.10 in [N].

The third and last result from the literature that we shall use is a special case of a result of Lev [L], generalising an earlier result of Freiman [F], concerning the growth of sumsets of a large subset of an arithmetic progression of integers:

Theorem 2.4. (Freiman, Lev) *Let $A \subseteq \mathbb{Z}$ satisfy*

$$|A| = n, \quad A \subseteq [0, l], \quad \{0, l\} \subseteq A, \quad \gcd(A) = 1. \tag{2.3}$$

If $2n - 3 \geq l$ then, for every $h \in \mathbb{N}$ one has

$$|hA| \geq n + (h-1)l. \tag{2.4}$$

3 Proof of the main theorem

First some notation. Let G be an abelian group and $A \subseteq G$. For $g \in G$ we denote

$$A + g := \{a + g : a \in A\}, \tag{3.1}$$

and for $h \in \mathbb{Z}$ we denote

$$h \cdot A := \{ha : a \in A\}. \tag{3.2}$$

Lemma 3.1. *Let $A \subseteq \mathbb{Z}_n$ and $u, v \in \mathbb{Z}$ such that $\gcd(u, n) = 1$. Then $\rho_n(A) = \rho_n[(u \cdot A) + v]$.*

Proof. This is clear. □

Lemma 3.2. *Theorem 1.1 holds for bases consisting of at most 3 elements.*

Proof. Let $n \in \mathbb{N}$ and A be a basis for $\mathbb{Z}_n$ such that $|A| \leq 3$. If $|A| = 1$ then $n = 1$, so the Theorem is vacuous. If $|A| = 2$ then $\rho_n(A) = n - 1$, as already noted in the Introduction. The Theorem clearly holds in that case (say with $k = 2$, $l = 1$, $c_2 = 2$). Suppose $|A| = 3$. By Lemma 3.1, there is no loss of generality in assuming that $A = \{0, a, b\}$ for some $a, b \in \mathbb{Z}_n$. First suppose that at least one of a, b and $b - a$ is a unit in $\mathbb{Z}_n$ (we will see later that the general case can essentially be reduced to this one). By Lemma 3.1 again, we may assume without loss of generality that $A = \{0, 1, t\}$ for some $t \in \mathbb{Z}_n$. In what follows we adopt the following notation: If $x \in \mathbb{Z}$ and $n \in \mathbb{N}$ then $||x||_n$ denotes the numerically least residue of x modulo n, that is, the unique integer $x_0 \in (n/2, n/2]$ such that $x \equiv x_0 \pmod{n}$.

So fix $k, t \in \mathbb{N}_{>1}$ and consider $A = \{0, 1, t\}$. Let $n \in \mathbb{N}$, which we think of as being very large. We suppose that $\rho_n(A) > n/k$ and shall show that Theorem 1.1 holds. First of all, by the pigeonhole principle, there must exist distinct integers $j_1, j_2 \in \{1, ..., k\}$ such that $||j_1 t - j_2 t|| = ||(j_1 - j_2)t|| \leq n/k$. Hence, there is an integer $c \in [1, k-1]$ such that

$||ct||_n \leq n/k$. Put $r := ||ct||_n$ and $s := |r|$. Clearly, if $s \neq 0$ then the order of the basis $\{0, 1, s\}$ is at most $s + n/s$, whereas if $s = 0$ then its order is $n - 1$. In terms of A, this implies that

$$\rho_n(A) \leq \min\{n - 1, s + \frac{cn}{s}\}. \tag{3.3}$$

The function $f(s) = s + cn/s$ has a local minimum at $s = \sqrt{cn}$. Note also that $f(ck) = f(n/k) = n/k + ck$. It follows that, for $n \gg 0$, if $\rho_n(A) > n/k + ck$ then $s \leq ck$. In terms of t, the latter implies that

$$t = \frac{dn + e}{c}, \tag{3.4}$$

for some integers $d \in [0, c)$, $e \in [-ck, ck]$. In this representation of t, we may assume that $\gcd(d, c) = 1$. The important point is that each of c, d, e is $O(k)$. First suppose $e \geq 0$. Clearly then, the number of terms from A needed to represent every number from 0 through $n - 1$ is at most $O(k)$ greater than the number of terms needed to represent every number from 0 through $\lfloor n/c \rfloor$. But since $ct \equiv e \pmod n$ it is easy to see in turn that the latter number of terms is within $O(k)$ of n/l, where $l = \max\{c, e\}$. Thus $|\rho_n(A) - n/l| = O(k)$, which implies Theorem 1.1.

If $e < 0$, then replace A by $1 - A = \{0, 1, 1 - t\} \pmod n$ and argue as before. This completes the proof of the lemma for bases $\{0, 1, t\}$.

Now let us deal with the general case of a 3-element basis $A = \{0, a, b\}$. Again, fix $k \in \mathbb{N}$, let n be very large and assume that $\rho_n(A) > n/k$. Let $a_1 := \text{GCD}(a, n)$. Since A is a basis we must have $\text{GCD}(a_1, b) = 1$. Then noting that, as m runs from 1 through $a_1 - 1$, the numbers mb run through all non-zero congruence classes modulo a_1, we easily deduce that

$$a_1 - 1 \leq \rho_n(A) \leq \frac{n}{a_1} + (a_1 - 1). \tag{3.5}$$

Clearly, then, we will be done unless $a_1 < k$. Supposing that this is the case, we wish to give a more precise inequality than (3.5), as follows. Let $a' := a/a_1$ and let b' be the unique integer in $[0, n/a_1)$ such that $b' \equiv b \pmod{n/a_1}$. Let $A' := \{0, a', b'\}$. This set can be considered as a basis for $\mathbb{Z}_{n/a_1}$, and the latter can be naturally identified with the subring of $\mathbb{Z}_n$ consisting of the multiples of a_1. Then we have the inequality

$$\rho'(A') \leq \rho_n(A) \leq \rho'(A') + (a_1 - 1), \tag{3.6}$$

where $\rho'(A')$ denotes the order of the basis A' for Z_{n/a_1}, but with the twist that every use of the number b' is weighted by a factor of a_1 (see the example below). Recall that $a_1 < k$, so that if $\rho_n(A) > \frac{n}{k} + (k - 2)$ then $\rho'(A') > \frac{n}{k}$. So we may assume the latter. Also, since a' is a unit in $\mathbb{Z}_{n/a_1}$, there is no loss of generality (by Lemma 3.1) in assuming $a' = 1$. We now complete the proof of Lemma 3.2 by imitating the argument given to deal with the special case of bases $\{0, 1, t\}$ above (now $t = b'$). The weighting mentioned above in fact implies that that argument goes through verbatim in the current setting, and this suffices to complete the proof of Lemma 3.2. □

Example 3.3. Let $n = 30$, $a = 4$, $b = 9$ and $A = \{0, 4, 9\}$. Then $\rho_{30}(A) = 9$ since, for example, the number $11 \in \mathbb{Z}_{30}$ can most efficiently be represented as $11 \equiv 8 \cdot 4 + 1 \cdot 9 \pmod{30}$. We have $a_1 = \text{GCD}(4, 30) = 2$, $a' = a/a_1 = 2$ and $b' = b = 9$. Then $A' = \{0, 2, 9\}$ is a basis for $\mathbb{Z}_{30/2} = \mathbb{Z}_{15}$. Multiplying by the unit $8 \in \mathbb{Z}_{15}$, let's work instead with the equivalent basis $A'' = \{0, 1, 12\} \equiv \{0, 1, -3\}$. One readily verifies that $\rho_{15}(A'') = 5$, and that the most difficult element of $\mathbb{Z}_{15}$ to represent with this basis is $8 \equiv 2 \cdot 1 + 3 \cdot (-3)$. When computing ρ', each use of the number -3 must be weighted by $a_1 = 2$, hence this same representation of 8 is now given total weight $2 + 2 \cdot 3 = 8$. Hence $\rho'(A'') = \rho'(A') = 8$, and the right-hand inequality of (3.6) is satisfied (with equality).

We can now complete the proof of Theorem 1.1. Fix $k \in \mathbb{N}$. All constants $c_{i,k}$ appearing below depend on k only. Let n be a positive integer which we think of as being very large. Let A be a basis for $\mathbb{Z}_n$ such that $\rho_n(A) > n/k$. By Lemma 3.1 we may assume, without loss of generality, that $0 \in A$. This is a convenient assumption, as it implies that $hA \subseteq (h+1)A$ for every h. From Theorem 2.1 it is easy to deduce the existence of positive constants $c_{1,k}, c_{2,k}$, such that

$$|A| \leq c_{1,k} \tag{3.7}$$

and, for some integer $j \in [1, c_{2,k}]$ one must have

$$|2^{j+1}A| < 2.04|2^j A|. \tag{3.8}$$

Set $h := 2^j$. For n sufficiently large, we'll certainly have $|hA| < 10^{-9}n$ and so we can apply Theorem 2.2. Let H be the corresponding subgroup of $\mathbb{Z}_n$ and $\pi : \mathbb{Z}_n \to \mathbb{Z}_n/H$ the natural projection. We can identify H with $\mathbb{Z}_m$ for some proper divisor m of n, and then identify $\mathbb{Z}_n/H$ with $\mathbb{Z}_{n/m}$. Let $B := hA$. Since A is a basis for $\mathbb{Z}_n$, then so is B and hence $\pi(B)$ is a basis for $\mathbb{Z}_{n/m}$. This means that either case (i) or case (ii) of Theorem 2.2 must apply. Moreover, since some coset of H contains at least $\frac{2}{3}|H|$ elements from B, it follows that $m = |H| = O(|B|) = O(k)$. Thus

$$m \leq c_{3,k}, \tag{3.9}$$

say. Since

$$\rho_{n/m}(\pi(A)) \leq \rho_n(A) \leq \rho_{n/m}(\pi(A)) + m, \tag{3.10}$$

this together with (3.8) and (3.9) imply that

$$|\rho_n(A) - h\rho_{n/m}(\pi(B))| \leq c_{4,k}. \tag{3.11}$$

To prove Theorem 1.1, it thus suffices to show that

$$|\rho_{n/m}(\pi(B)) - n/q| \leq c_{5,k}, \quad \text{for some multiple } q \text{ of } h. \tag{3.12}$$

Let s be the number of cosets of H met by B and s' the number met by A.

CASE 1: $s = 3$.

Then $s' \leq 3$. We don't need (3.12) in this case and can instead deduce Theorem 1.1 directly from (3.10) and Lemma 3.2.

CASE 2: $s \neq 3$.

Then Case (i) of Theorem 2.2 must apply. Let l be the minimum length of an arithmetic progression in $\mathbb{Z}_{n/m}$ containing $\pi(B)$. Note that $l \leq c_{6,k}$, by (2.1). By Lemma 3.1, there is no loss of generality in assuming that $\pi(B)$ is contained inside an interval of length $l-1$. Since $\pi(A) \subseteq \pi(B)$ and $l = O(k)$ we can now also see that $l-1$ is a multiple of h, provided n is large enough. Thus it suffices to prove that

$$\left| \rho_{n/m}(\pi(B)) - \frac{n}{l-1} \right| \leq c_{7,k}. \tag{3.13}$$

It is here that we use Theorem 2.4. Indeed (3.13) is easily seen to follow from that theorem provided that $2s - 3 \geq l - 1$. But this inequality is in turn easily checked to result from (2.1) (as applied to B), (3.8) and the fact that $|B| \leq s|H|$.

Thus the proof of Theorem 1.1 is complete.

Remark 3.3. Explicit values for each of the constants $c_{i,k}$, $i = 1, ..., 7$, can easily be obtained from the argument given above. Similarly, one can obtain bounds for all the $O(k)$ terms in the proof of Lemma 3.2. All of this will in turn yield explicit constants c_k in Theorem 1.1. We refrain from carrying out this messy procedure, however, since the more interesting question is what the optimal values are for the c_k. Note that $c_k \geq (k-2) + \frac{1}{k}$, which can be seen by considering the basis $\{0, 1, k\}$ for $\mathbb{Z}_n$, when $n \equiv -1 \pmod{k}$.

4 Some specific basis orders and gaps

It remains to determine exactly which integers are in the range of ρ_n. (Theorem 1.1 essentially finishes this question 'up to constants'.) It is worth briefly summarizing the known basis orders and exact gaps. The first two gaps were separately discovered in [D, WM].

Theorem 4.1. (Daode, Wang-Meng) *Let A be a basis for $\mathbb{Z}_n$. Then*

$$\rho_n(A) \notin \left[\left\lfloor \frac{n}{3} \right\rfloor + 2, \left\lfloor \frac{n}{2} \right\rfloor - 2 \right] \cup \left[\left\lfloor \frac{n}{2} \right\rfloor, n-2 \right].$$

In fact, the arguments for these gaps actually apply more generally to finite abelian groups G of order n.

Extending the argument in [WM], it is possible to exactly determine a third gap. We only outline the proof, leaving details to the interested reader.

Theorem 4.2. *Let A be a basis for $\mathbb{Z}_n$. Then*

$$\rho_n(A) \notin \left[\left\lfloor \frac{n}{4} \right\rfloor + 3, \left\lfloor \frac{n}{3} \right\rfloor - 2 \right].$$

Proof. By Lemma 3.1, assume $0 \in A$. We may suppose that the only other elements in A have orders in $\{2, 3, n/3, n/2, n\}$. Elements in A of order 2 or 3 lead to $\rho_n(A) \geq \frac{n}{2} - 1$ or $\frac{n}{3} - 1$, respectively. If A contains an element of order n, use Lemma 3.1 to assume without loss of generality that $\{0, 1, t\} \subseteq A$, $t \leq \frac{n}{2}$. After some arithmetic, one has $\rho_n(A) \leq \rho_n(\{0, 1, t\}) \leq \frac{n}{4} + 2$, unless $t \in \{2, 3, \lfloor \frac{n}{3} \rfloor, \lfloor \frac{n}{3} \rfloor + 1, \lfloor \frac{n}{2} \rfloor\}$. If 2 or $3 \mid n$, the cases $t = \frac{n}{2}, \frac{n}{3}$ produce an element of order 2 or 3, respectively. If $3 \mid n$ and $t = \frac{n}{3} + 1$, one has $\frac{2n}{3} \in (-1) \cdot A + 1$, again an element of order 3. Otherwise, consider either $2 \cdot A$ or $3 \cdot A$ and arrive at a case equivalent to one of

- $A = \{0, 1, 2\}$, with order $\lfloor \frac{n}{2} \rfloor$,
- $A = \{0, 1, 3\}$, with order $\lfloor \frac{n}{3} \rfloor + 1$, or
- $A = \{0, 1, 2, 3\}$, with order $\lceil \frac{n-1}{3} \rceil \geq \lfloor \frac{n}{3} \rfloor - 1$.

Finally, suppose that all nonzero elements of A have orders in $\{n/2, n/3\}$. For A to be a basis, we must have an element of each of these orders. Therefore, $6 \mid n$. Multiplying by a unit, we may assume $\{0, 2, 3t\} \subseteq A$. Then $A - 2$ contains $3t - 2$, reducing to a previously considered case. □

Table 1: Basis orders for $\mathbb{Z}_n$, $5 \leq n \leq 64$.

n	basis orders	n	basis orders	n	basis orders
5	1 2 4	25	1..9 12 24	45	1..16 22 44
6	1 2 3 5	26	1..9 12 13 25	46	1..13 15 16 22 23 45
7	1 2 3 6	27	1..10 13 26	47	1..13 16 23 46
8	1..4 7	28	1..10 13 14 27	48	1..17 23 24 47
9	1..4 8	29	1..10 14 28	49	1..14 16 17 24 48
10	1..5 9	30	1..11 14 15 29	50	1..14 17 24 25 49
11	1..5 10	31	1..11 15 30	51	1..14 16 17 18 25 50
12	1..6 11	32	1..11 15 16 31	52	1..15 17 18 25 26 51
13	1..6 12	33	1..12 16 32	53	1..15 18 26 52
14	1..7 13	34	1..12 16 17 33	54	1..15 19 26 27 53
15	1..7 14	35	1..10 12 17 34	55	1..15 19 27 54
16	1..8 15	36	1..13 17 18 35	56	1..16 19 27 28 55
17	1..6 8 16	37	1..13 18 36	57	1..16 19 20 28 56
18	1..9 17	38	1..11 13 18 19 37	58	1..16 20 28 29 57
19	1..7 9 18	39	1..14 19 38	59	1..16 20 29 58
20	1..7 9 10 19	40	1..14 19 20 39	60	1..17 21 29 30 59
21	1..8 10 20	41	1..12 14 20 40	61	1..17 20 21 30 60
22	1..8 10 11 21	42	1..15 20 21 41	62	1..17 21 30 31 61
23	1..8 11 22	43	1..12 14 15 21 42	63	1..17 21 22 31 62
24	1..9 11 12 23	44	1..13 15 21 22 43	64	1..18 22 31 32 63

In Table 1, we summarize the situation for small finite cyclic groups. The realizable basis orders are obtained in many cases by easy constructions, while in some cases by a very short computer search. The non-realizable basis orders are those resulting from Theorems 4.1 and 4.2.

5 Applications and Concluding Remarks

A *directed graph*, or *digraph* is an ordered pair $D = (V, E)$ where V is a nonempty set of *vertices*, and $E \subseteq V \times V$ is a set of *arcs*. In most investigations, V is taken to be a finite set. If V is a set of points, the arc (x, y) is drawn as an arrow from x to y. A *loop* is an arc of the form $(x,\ x)$. Among other things, digraphs are used to model finite networks.

A (*directed*) *walk* in D from vertex x to vertex y is a sequence of vertices

$$x = x_0, x_1, x_2, \ldots, x_L = y$$

where $(x_i, x_{i+1}) \in E$ for all $0 \leq i < L$. Such a walk has *length* L. A walk with no repeated vertices is called a *path*; clearly, the shortest walk from x to y is always a path.

A digraph D is *primitive* if, for some positive integer k, there is a walk in D of length k between any pair of vertices u and v in D. The smallest such k is the *exponent* of D, and is denoted by $\gamma(D)$. A related notion is the *diameter* $\mathrm{diam}(D)$, defined to be the maximum, over all $x, y \in V$, of the shortest path (walk) from x to y, this taken to be ∞ if some pair of vertices are not joined by a walk.

If D is primitive, one obviously has $\mathrm{diam}(D) \leq \gamma(D)$. Conversely, if D has finite diameter and loops at every vertex, then $\gamma(D) = \mathrm{diam}(D)$.

There is a history of research on exponents of digraphs. In 1950, Wielandt [W] stated that for primitive digraphs D on n vertices,

$$\gamma(D) \leq w_n := (n-1)^2 + 1. \tag{5.1}$$

Later, Lewin and Vitek [LV] found a sequence of gaps in $[1, w_n]$ as non-realizable exponenets of primitive digraphs on n vertices.

Let $n \in \mathbb{N}$ and $A \subseteq \mathbb{Z}_n$. The *circulant* $C = \mathtt{Circ}(n, A)$ is a digraph with vertex set $\mathbb{Z}_n$ and (x, y) an arc if and only if $y - x \in A$. Bounds on the diameter of certain circulants has proved useful in quantum information theory; see [BPS]. Other applications can be found in the references of [LV, WM].

In any case, the connection with basis orders in $\mathbb{Z}_n$ is now clear.

Proposition 5.1. $\gamma(\mathtt{Circ}(n, A)) = \rho_n(A)$.

There exists a similar connection between the possible basis orders for general finite groups G and the possible exponents of *Cayley* digraphs. Therefore, the problem of extending Theorem 1.1 to general groups merits some attention.

Acknowledgements

We wish to thank Renling Jin for very helpful discussions, the referee for his/her comments and David Gil for pointing out an error in an earlier version of the paper.

References

[BPS] M. Bašić, M.D. Petrović and D. Stevanović, *Perfect state transfer in integral circulant graphs*, Applied Math. Lett. **7** (2009), 1117–1121.

[D] H. Daode, *On circulant Boolean matrices*, Linear Algebra Appl. **136** (1990), 107–117.

[DF] J.-M. Deshouillers and G.A. Freiman, *A step beyond Kneser's theorem for abelian finite groups*, Proc. London Math. Soc. (3) **86** (2003), 1–28.

[F] G.A. Freiman, *Foundations of a Structural Theory of Set Addition* (Russian), Kazan. Gos. Ped. Inst., Kazan (1966) ; also Translations of Math. Monographs **37**, AMS Providence, RI (1973).

[KL] B. Klopsch and V.F. Lev, *Generating abelian groups by addition only*, Forum Math. **21** (2009), 23–41.

[L] V.F. Lev, *Structure theorem for multiple addition and the Frobenius problem*, J. Number Theory **58** (1996), 79–88.

[LV] M. Lewin and Y. Vitek, *A system of gaps in the exponent set of primitive matrices*, Illinois J. Math. **25** (1981), 87–98.

[HMV] S. Herke, G. MacGillivray and P. van den Driessche, *Exponents of primitive digraphs*, preprint.

[N] M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, New York (1996).

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

[W] H. Wielandt, *Unzerlegbare, nicht negative Matrizen*, Math. Zeit. **52** (1950), 642–645.