

On short zero-sum subsequences over p -groups

W. A. Schmid* J. J. Zhuang†

Abstract

Let G be a finite abelian group with exponent n . Let $s(G)$ denote the smallest integer l such that every sequence over G of length at least l has a zero-sum subsequence of length n . For p -groups whose exponent is odd and sufficiently large (relative to Davenport's constant of the group) we obtain an improved upper bound on $s(G)$, which allows to determine $s(G)$ precisely in special cases. Our results contain Kemnitz' conjecture, which was recently proved, as a special case.

Keywords: Davenport's constant, finite abelian group, Kemnitz' conjecture, zero-sum sequence

MSC (2000): 11B75, 11P21, 20K01

1 Introduction

Let G be a finite abelian group. In this paper we investigate the invariant $s(G)$. Two further invariants, $\eta(G)$ and $D(G)$, will be of importance as well. We recall their definitions.

Definition 1.1. Let G be a finite abelian group with exponent n .

1. Let $s(G)$ denote the smallest integer l such that every sequence over G of length at least l has a zero-sum subsequence of length n .
2. Let $\eta(G)$ denote the smallest integer l such that every sequence over G of length at least l has a non-empty zero-sum subsequence of length at most n .

*Institut für Mathematik und wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstraße 36, 8010 Graz, Austria, email: wolfgang.schmid@uni-graz.at. Supported by the FWF (P18779-N13).

†The corresponding author. Department of Mathematics, Dalian Maritime University, Dalian, 116024, China, email: jjzhuang1979@yahoo.com.cn. Supported by the NSFC with grant No. 10826026.

3. Let $D(G)$ denote the smallest integer l such that every sequence over G of length at least l has a non-empty zero-sum subsequence. (This invariant is called Davenport's constant of G .)

The investigation of $s(G)$ has a long tradition. It was initiated at the beginning of the 1960s when P. Erdős, A. Ginzburg, and A. Ziv [3] proved $s(G) = 2n - 1$ if G is a cyclic group. First results for more general groups are due to H. Harborth [10]. We refer to [2] for an overview of the numerous contributions to this problem.

Still, the precise value of $s(G)$ is known only if G has rank at most 2, G is a special type of 2-group, or a very special type of 3-group with rank at most 5. Indeed, the case of groups of rank 2 was settled only recently when C. Reiher [12] proved, the longstanding Kemnitz' conjecture, $s(C_p^2) = 4p - 3$ (cf. [13, 4, 7] for earlier contributions and variants and [9, Theorem 5.8.3] for the general result on groups of rank at most 2). For the precise results for 2- and 3-groups cf. [2] (in particular Corollary 4.4 and Remarks 4.7).

Here, we obtain the following result on $s(G)$.

Theorem 1.2. *Let p be an odd prime and let G be a finite abelian p -group with $\exp(G) = n$ and $D(G) \leq 2n - 1$. Then*

$$2D(G) - 1 \leq \eta(G) + n - 1 \leq s(G) \leq D(G) + 2n - 2.$$

In particular, if $D(G) = 2n - 1$, then

$$s(G) = \eta(G) + n - 1 = 4n - 3.$$

We emphasize that the lower bounds on $s(G)$ are already known (see [8, Theorem 1.5] or [2, Lemma 3.2]). The contribution of this paper is a new upper bound on $s(G)$, which sharpens recent results obtained in [8, Theorem 1.5] and [2, Theorem 1.3.2], and allows to obtain the precise value of $s(G)$ for certain groups. Our result confirms a conjecture of W.D. Gao. He conjectured (cf. [6, Conjecture 2.3]) that

$$s(G) = \eta(G) + \exp(G) - 1$$

for every finite abelian group. This conjecture holds for every group for which $s(G)$ has been determined so far (cf. above), and additionally it is known to hold for groups with $\exp(G) \leq 4$ (see [6, Theorem 2.5]) and for C_5^3 (see [5]).

It is well-known that $D(C_p^2) = 2p - 1$ (cf. Lemma 2.3). Thus, our result contains the result of C. Reiher (cf. above) as a special case. In fact, recently S. Savchev and F. Chen [14] obtained a result that gives some structural insight into the variety of zero-sum subsequences of "long" sequences in C_p^2 that, among others, implies Reiher's result. We adapt their method to

our more general situation and obtain an analogue of their result (Theorem 3.1) that in turn yields Theorem 1.2.

In the following section, we recall and introduce some notation, and recall some well-known results that we will apply in our proofs. Then, we state Theorem 3.1 and derive Theorem 1.2 from it. We end the paper with a conjecture on the precise value of $s(G)$ for the groups considered in Theorem 1.2.

2 Notation and some results

Throughout, let G denote an, additively written, finite abelian group.

We denote by \mathbb{Z} the integers, and by \mathbb{N} and \mathbb{N}_0 the positive and non-negative integers respectively. For $r, s \in \mathbb{Z}$, we denote by $[r, s] = \{z \in \mathbb{Z} : r \leq z \leq s\}$ the interval of integers. For $r, n \in \mathbb{N}$ we denote by C_n a cyclic group of order n and by C_n^r the direct sum of r copies of C_n .

If $|G| > 1$, then there exist uniquely determined $1 < n_1 | \dots | n_r$ such that $G \cong C_{n_1} \oplus \dots \oplus C_{n_r}$. We denote by $\exp(G) = n_r$ the exponent of G and r is called the rank of G . We call G a p -group if $\exp(G) = p^k$ where p is a prime and $k \in \mathbb{N}$.

We denote by $\mathcal{F}(G)$ the multiplicatively written free abelian monoid over G . We refer to its elements as sequences (over G). Let $S \in \mathcal{F}(G)$. By definition, S is equal to a (formal, commutative) product $S = \prod_{i=1}^l g_i$ with $l \in \mathbb{N}_0$ and $g_i \in G$; this representation is unique up to the order of the factors. We denote by $|S| = l \in \mathbb{N}_0$ the length of S and by $\sigma(S) = \sum_{i=1}^l g_i \in G$ its sum. We say that $T \in \mathcal{F}(G)$ is a subsequence of S if T divides S (in $\mathcal{F}(G)$), i.e., there exists some $T' \in \mathcal{F}(G)$ such that $S = TT'$; we use the notation $T^{-1}S$ to denote this sequence T' . A sequence whose sum is equal to 0 is called a zero-sum sequence. The unit element of $\mathcal{F}(G)$ is called the empty sequence; its length and sum equal 0 (in \mathbb{N}_0 and G respectively).

2.1 Induced subsequences with prescribed sum

The “counting” of certain subsequences will play a main role in our proofs. Therefore, we introduce some notation related to this problem. Similar considerations can be found in [14].

Let $S = g_1 \dots g_l \in \mathcal{F}(G)$. For $I \subset [1, l]$, let $S_I = \prod_{i \in I} g_i$ denote the subsequence induced by I . Let $d \in \mathbb{N}$, $\mathbf{i} = (i_1, \dots, i_d) \in \mathbb{Z}^d$ and $\mathbf{h} = (h_1, \dots, h_d) \in G^d$. We denote by

$$N_{\mathbf{h}}^{\mathbf{i}}(S) = |\{(I_1, \dots, I_d) : I_j \subset [1, l], |I_j| = i_j, \sigma(S_{I_j}) = h_j, \\ I_j \cap I_k = \emptyset \text{ for all } j, k \in [1, d]\}| ,$$

i.e., the number of (ordered) d -tuples of disjoint subsets of $[1, l]$ with prescribed number of elements and prescribed sum of the induced subsequence. For $d = 1$ this coincides with the usual terminology, cf. [9, Definition 5.3.7]. For $\mathbf{0} = (0, \dots, 0)$, we omit the subscript and write $N^i(S)$ instead of $N_{\mathbf{0}}^i(S)$.

Though we defined $N_{\mathbf{h}}^i(S)$ with respect to a particular representation of S as a product of elements g_i , $N_{\mathbf{h}}^i(S)$ is clearly invariant under permutation of the factors of this product and actually just depends on S . If any of the i_j is negative, then $N_{\mathbf{h}}^i(S) = 0$.

In the following lemma we record some basic properties of $N_{\mathbf{h}}^i(S)$ that we will use frequently.

Lemma 2.1. *Let $S \in \mathcal{F}(G)$ with $|S| = l$, and let $d \in \mathbb{N}$, $\mathbf{i} = (i_1, \dots, i_d) \in \mathbb{Z}^d$ and $\mathbf{h} = (h_1, \dots, h_d) \in G^d$.*

1. *Suppose $d \geq 2$. Let $k \in [1, d]$, and $\mathbf{i}_k = (i_1, \dots, \widehat{i_k}, \dots, i_d) \in \mathbb{Z}^{d-1}$ and $\mathbf{h}_k = (h_1, \dots, \widehat{h_k}, \dots, h_d) \in G^{d-1}$ where the $\widehat{}$ indicates that the coordinate is omitted. Then*

$$N_{\mathbf{h}}^{\mathbf{i}}(S) = \sum_{I \subset [1, l], |I| = \mathbf{i}_k, \sigma(S_I) = \mathbf{h}_k} N_{\mathbf{h}_k}^{\mathbf{i}_k}(S_I^{-1}S).$$

2. *Let $\mathbf{i} = \sum_{j=1}^d i_j$ and $\mathbf{h} = \sum_{j=1}^d h_j$. Then*

$$N_{\mathbf{h}}^{\mathbf{i}}(S) = \sum_{I \subset [1, l], |I| = \mathbf{i}, \sigma(S_I) = \mathbf{h}} N_{\mathbf{h}}^{\mathbf{i}}(S_I).$$

Proof. The first assertion is a direct consequence of the definition. To get the second one, we observe that d disjoint sets I_1, \dots, I_d with $|I_j| = i_j$ are contained in a unique set I with $|I| = \mathbf{i}$ and that necessarily $\sigma(S_I) = \sum_{j=1}^d \sigma(S_{I_j}) = \mathbf{h}$. \square

2.2 Two results

We recall two well-known results. Important special cases of the following result can be found in [1] and [8].

Lemma 2.2. *Let $S \in \mathcal{F}(G)$ and suppose $D(G \oplus C_n) < 3n$. If $N^n(S) = 0$, then $N^{(2i+1)n}(S) = 0$ for each $i \in \mathbb{N}_0$.*

Proof. See Proposition 5.7.7.3 in [9]. \square

The following result is due to J.E. Olson [11] and D. Kruyswijk (cf. [15]).

Lemma 2.3. Let $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$ be a p -group. Then $D(G) = 1 + \sum_{i=1}^r (n_i - 1)$. Moreover, if $|S| \geq D(G)$, then for each $g \in G$

$$\sum_{i \in \mathbb{Z}} (-1)^i N_g^i(S) \equiv 0 \pmod{p}.$$

Proof. See Proposition 5.5.8.2 in [9]. □

3 Main technical result

The following theorem is the main technical result of this paper.

Theorem 3.1. Let p be an odd prime and let G be a finite abelian p -group with $\exp(G) = n$ and $D(G) \leq 2n - 1$. Further, let $l \in [1, n]$ and $S \in \mathcal{F}(G)$ with $D(G) + (n - 2) + l \leq |S| < 4n$.

1. For each $\{0\} \subset I \subset [0, l - 1]$ we have

$$\begin{aligned} \sum_{i \in I} (-1)^i (N^{(i, n-i)}(S) + N^{(i, 3n-i)}(S)) + \sum_{i \in [0, n-1] \setminus I} (-1)^i N^{(i, 2n-i)}(S) \\ \equiv 1 + 2^{-1} N^{(n, n)}(S) \pmod{p}. \end{aligned}$$

2. One of the following two statements holds:

- (a) S has a zero-sum subsequence B with $|B| = n$.
- (b) S has a zero-sum subsequence B with $|B| = 2n$ such that B has a zero-sum subsequence B' with $|B'| \in [l, n - 1]$.

Now, using Theorem 3.1, we prove Theorem 1.2.

Proof of Theorem 1.2. For a proof of the lower bound on $\eta(G)$ we refer to [2, Lemma 3.2], and a proof that $\eta(G) + n - 1 \leq s(G)$ may be found in [9, Lemma 5.7.2].

To show the upper bound on $s(G)$, let $S \in \mathcal{F}(G)$ be a sequence of length $|S| \geq D(G) + 2n - 2$. We may suppose that $|S| = D(G) + 2n - 2$; otherwise we consider a subsequence of S of that length. We apply Theorem 3.1.2 with $l = n$. Since in case $l = n$ statement (b) cannot hold, we infer that S has a zero-sum subsequence of length n . Consequently, $s(G) \leq D(G) + 2n - 2$.

Obviously, the assertion on the case of equality follows from the upper and lower bound. □

The rest of the section is concerned with the proof of Theorem 3.1.

3.1 Auxiliary results

Lemma 3.2. *Let p be an odd prime and let G be a p -group. Let $d \in \mathbb{N}$ and $k \in [1, d]$. Further, let $\mathbf{i} = (i_j)_{j=1}^d \in \mathbb{Z}^d$ and $\mathbf{h} = (h_j)_{j=1}^d \in G^d$, and let $\mathbf{e}_k = (\delta_{j,k})_{j=1}^d \in \mathbb{Z}^d$ denote the k -th unit vector. If $|S| \geq D(G) + p^m - 1 + \sum_{j \in [1, d] \setminus \{k\}} i_j$, then*

$$\sum_{j \in \mathbb{Z}} (-1)^j N_{\mathbf{h}}^{i_1 + j p^m \mathbf{e}_k}(S) \equiv 0 \pmod{p}.$$

Proof. We prove the result by induction on d . For $d = 1$ we have to show that if $|S| \geq D(G) + p^m - 1$, then $\sum_{j \in \mathbb{Z}} (-1)^j N_{h_1}^{i_1 + j p^m}(S) \equiv 0 \pmod{p}$. Thus, suppose that $|S| \geq D(G) + p^m - 1$. Let $G \oplus C_{p^m} = G \oplus \langle e \rangle$ and let

$$\varphi : \begin{cases} G & \rightarrow G \oplus C_{p^m} \\ g & \mapsto g + e \end{cases}.$$

By Lemma 2.3 $|\varphi(S)| \geq D(G \oplus C_{p^m})$ and for each $g' \in G \oplus C_{p^m}$,

$$\sum_{j \in \mathbb{Z}} (-1)^j N_{g'}^j(\varphi(S)) \equiv 0 \pmod{p}. \quad (1)$$

We note that for $g' = g_1 + i_1 e$,

$$N_{g'}^j(\varphi(S)) = \begin{cases} N_{g_1}^j(S) & \text{if } j \equiv i_1 \pmod{p^m} \\ 0 & \text{otherwise} \end{cases}.$$

Consequently by (1),

$$\sum_{j \in \mathbb{Z}} (-1)^{i_1 + j p^m} N_{h_1}^{i_1 + j p^m}(S) \equiv 0 \pmod{p}.$$

Since p is odd, $(-1)^{j p^m} = (-1)^j$ and the claim follows.

Now, let $d \geq 2$ and we assume that the result holds for $d - 1$. Let $l \in [1, d] \setminus \{k\}$. By Lemma 2.1.1 we have

$$\begin{aligned} & \sum_{j \in \mathbb{Z}} (-1)^j N_{\mathbf{h}}^{i_1 + j p^m \mathbf{e}_k}(S) \\ &= \sum_{j \in \mathbb{Z}} (-1)^j \sum_{I \subset [1, |S|], \sigma(S_I) = h_1, |I| = i_1} N_{h_1}^{(i_1 + j p^m \mathbf{e}_k)_I}(S_I^{-1} S) \\ &= \sum_{I \subset [1, |S|], \sigma(S_I) = h_1, |I| = i_1} \sum_{j \in \mathbb{Z}} (-1)^j N_{h_1}^{(i_1 + j p^m \mathbf{e}_k)_I}(S_I^{-1} S), \end{aligned}$$

where, as in Lemma 2.1.1, $(i + jp^m \mathbf{e}_k)_l \in \mathbb{Z}^{d-1}$ and $\mathbf{h}_l \in G^{d-1}$ are obtained by omitting the l -th coordinate. If $|S| \geq D(G) + p^m - 1 + \sum_{j \in [1, d] \setminus \{k\}} i_j$, then $|S_l^{-1} S| = |S| - i_l \geq D(G) + p^m - 1 + \sum_{j \in [1, d] \setminus \{k, l\}} i_j$ and consequently each sum $\sum_{j \in \mathbb{Z}} (-1)^j N_{\mathbf{h}_l}^{(i + jp^m \mathbf{e}_k)_l}(S_l^{-1} S)$ is equal to 0 modulo p by the induction hypothesis. \square

Lemma 3.3. *Let G be a p -group, $g \in G$, and $S \in \mathcal{F}(G)$. Further, let $l \in \mathbb{N}$ such that $2l \geq D(G)$.*

1. *If $|S| = 2l$ and $\sigma(S) = 2g$, then*

$$2 \sum_{i=0}^{l-1} (-1)^i N_g^i(S) \equiv (-1)^{l-1} N_g^l(S) \pmod{p}.$$

2.

$$2 \sum_{i=0}^{l-1} (-1)^i N_{(g,g)}^{(i, 2l-i)}(S) \equiv (-1)^{l-1} N_{(g,g)}^{(l,l)}(S) \pmod{p}.$$

Proof. 1. Suppose $|S| = 2l$ and $\sigma(S) = 2g$. By Lemma 2.3

$$\sum_{i=0}^{2l} (-1)^i N_g^i(S) \equiv 0 \pmod{p}.$$

We note that $N_g^i(S) = N_{\sigma(S)-g}^{|S|-i}(S) = N_g^{2l-i}(S)$ for each $i \in \mathbb{Z}$. Since clearly $i \equiv 2l - i \pmod{2}$, the result follows.

2. We have

$$\begin{aligned} 2 \sum_{i=0}^{l-1} (-1)^i N_{(g,g)}^{(i, 2l-i)}(S) &= 2 \sum_{i=0}^{l-1} (-1)^i \sum_{I \subset [1, l], \sigma(S_I)=2g, |I|=2l} N_g^i(S_I) \\ &= \sum_{I \subset [1, l], \sigma(S_I)=2g, |I|=2l} 2 \sum_{i=0}^{l-1} (-1)^i N_g^i(S_I) \\ &\equiv \sum_{I \subset [1, l], \sigma(S_I)=2g, |I|=2l} (-1)^{l-1} N_g^l(S_I) \\ &= (-1)^{l-1} N_{(g,g)}^{(l,l)}(S) \end{aligned}$$

where the congruence holds modulo p and we applied Lemma 2.1.2 to obtain the first and the last equality, and the first assertion of this lemma to get the congruence. \square

3.2 Proof of Theorem 3.1

Proof of Theorem 3.1. 1. Since $2n \geq D(G)$, Lemma 3.3.2 yields (note that $n - 1$ is even)

$$2 \sum_{i=0}^{n-1} (-1)^i N^{(i, 2n-i)}(S) \equiv N^{(n, n)}(S) \pmod{p}. \quad (2)$$

For each $k \in [0, l - 1]$, by Lemma 3.2 (with $p^m = n$),

$$\sum_{j \in \mathbb{Z}} (-1)^j N^{(k, jn-k)}(S) \equiv 0 \pmod{p}. \quad (3)$$

Since $|S| < 4n$, for $k = 0$ this simplifies to

$$N^{(0, 0)}(S) - N^{(0, n)}(S) + N^{(0, 2n)}(S) - N^{(0, 3n)}(S) \equiv 0 \pmod{p}.$$

Since $N^{(0, 0)}(S) = 1$, substituting in (2) gives

$$2(-1 + N^{(0, n)}(S) + N^{(0, 3n)}(S)) + \sum_{i=1}^{n-1} (-1)^i N^{(i, 2n-i)}(S) \equiv N^{(n, n)}(S) \pmod{p},$$

which yields the claimed congruence in the special case $I = \{0\}$. To obtain the general case, it suffices to note that (3) for $k \in [1, l - 1]$ implies

$$N^{(k, n-k)}(S) + N^{(k, 3n-k)}(S) \equiv N^{(k, 2n-k)}(S) \pmod{p}.$$

2. We note that (a) is equivalent to $N^n(S) \neq 0$ and (b) to $N^{(k, 2n-k)}(S) \neq 0$ for some $k \in [l, n - 1]$. By the first assertion of this theorem (with $I = [0, l - 1]$) at least one of the following has to hold:

- $N^{(n, n)}(S) \neq 0$.
- $N^{(k, n-k)}(S) \neq 0$ or $N^{(k, 3n-k)}(S) \neq 0$ for some $k \in [0, l - 1]$.
- $N^{(k, 2n-k)}(S) \neq 0$ for some $k \in [l, n - 1]$.

If the first or the last assertion holds, then (a) or (b) respectively holds. If $N^{(k, n-k)}(S) \neq 0$ for $k \in [0, l - 1]$, then there exist two zero-sum subsequences of S of length k and $n - k$ respectively and their product is a zero-sum subsequence of S of length n . Similarly, if $N^{(k, 3n-k)}(S) \neq 0$, then $N^{3n}(S) \neq 0$ and, since by Lemma 2.3 $D(G \oplus C_n) = D(G) + n - 1 < 3n$, by Lemma 2.2 $N^n(S) \neq 0$. \square

4 Concluding remark

In view of the known results the following conjecture on $s(G)$ (and $\eta(G)$) for p -groups with “large” exponent seems conceivable.

Conjecture 4.1. Let G be a finite abelian p -group with $\exp(G) = n$ and $D(G) \leq 2n - 1$. Then

$$2D(G) - 1 = \eta(G) + n - 1 = s(G).$$

In other words, equality holds at the lower bounds in Theorem 1.2.

This conjecture is confirmed in case G has rank at most 2 (cf. [9, Theorem 5.8.3]) and in case $D(G) = 2n - 1$ by Theorem 1.2.

References

- [1] N. Alon and M. Dubiner. Zero-sum sets of prescribed size. In *Combinatorics, Paul Erdős is eighty, Vol. 1*, Bolyai Soc. Math. Stud., pages 33–50. János Bolyai Math. Soc., Budapest, 1993.
- [2] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, and L. Rackham. Zero-sum problems in finite abelian groups and affine caps, submitted. Preprint available at Elsholtz’ website:
<http://www.ma.rhul.ac.uk/~elsholtz/>
- [3] P. Erdős, A. Ginzburg, and A. Ziv. Theorem in the additive number theory. *Bull. Res. Council Israel*, 10F:41–43, 1961.
- [4] W. D. Gao. Note on a zero-sum problem. *J. Combin. Theory Ser. A*, 95(2):387–389, 2001.
- [5] W. D. Gao and A. Geroldinger. Zero-sum problems in finite abelian groups: a survey, submitted.
- [6] W. D. Gao. On zero-sum subsequences of restricted size. II. *Discrete Math.*, 271(1-3):51–59, 2003.
- [7] W. D. Gao and R. Thangadurai. A variant of Kemnitz conjecture. *J. Combin. Theory Ser. A*, 107(1):69–86, 2004.
- [8] W. D. Gao and J. Zhou. On short zero-sum subsequences. *Ars Combin.*, 74:231–238, 2005.
- [9] A. Geroldinger and F. Halter-Koch. *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*. Pure and Applied Mathematics vol. 278, Chapman & Hall/CRC, 2006.

- [10] H. Harborth. Ein Extremalproblem für Gitterpunkte. *J. Reine Angew. Math.*, 262/263:356–360, 1973.
- [11] J. E. Olson. A combinatorial problem on finite Abelian groups. I. *J. Number Theory*, 1:8–10, 1969.
- [12] C. Reiher. On Kemnitz' conjecture concerning lattice points in the plane. *Ramanujan J.*, to appear.
- [13] L. Rónyai. On a conjecture of Kemnitz. *Combinatorica*, 20(4):569–573, 2000.
- [14] S. Savchev and F. Chen. Kemnitz' conjecture revisited. *Discrete Math.*, 297(1-3):196–201, 2005.
- [15] P. van Emde Boas. A combinatorial problem on finite Abelian groups. II. Technical report, Math. Centrum, Amsterdam, Afd. Zuivere Wisk. ZW 1969-007, 60 p., 1969.