(This is a sample cover image for this issue. The actual cover is not yet available at this time.)

Journal of Number Theory 131 (2011) 1864–1874

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the Erdős–Ginzburg–Ziv constant of finite abelian groups of high rank

Yushuang Fan, Weidong Gao *, Qinghai Zhong

Center for Combinatorics, LPMC-TJKLC, Nankai University, Tianjin 300071, PR China

ARTICLE INFO

Article history:
Received 24 October 2010
Revised 14 February 2011
Accepted 14 February 2011
Available online xxxx
Communicated by Ronald Graham

MSC:
11B30
11P70
20K01

Keywords:
Erdős–Ginzburg–Ziv constant
Zero-sum sequences
Inverse zero-sum problems

ABSTRACT

Let G be a finite abelian group. The Erdős–Ginzburg–Ziv constant $\mathsf{s}(G)$ of G is defined as the smallest integer $l \in \mathbb{N}$ such that every sequence S over G of length $|S| \geqslant l$ has a zero-sum subsequence T of length $|T| = \exp(G)$. If G has rank at most two, then the precise value of $\mathsf{s}(G)$ is known (for cyclic groups this is the theorem of Erdős–Ginzburg–Ziv). Only very little is known for groups of higher rank. In the present paper, we focus on groups of the form $G = C_n^r$, with $n, r \in \mathbb{N}$ and $n \geqslant 2$, and we tackle the study of $\mathsf{s}(G)$ with a new approach, combining the direct problem with the associated inverse problem.

1. Introduction and main result

Let G be an additive finite abelian group. We denote by

- $\mathsf{D}(G)$ the smallest integer $l \in \mathbb{N}$ such that every sequence S over G of length $|S| \geqslant l$ has a non-empty zero-sum subsequence.
- $\mathsf{s}(G)$ the smallest integer $l \in \mathbb{N}$ such that every sequence S over G of length $|S| \geqslant l$ has a zero-sum subsequence T of length $|T| = \exp(G)$.

Then $\mathsf{D}(G)$ is called the *Davenport constant* and $\mathsf{s}(G)$ the *Erdős–Ginzburg–Ziv constant* of G. These are classical invariants in the Combinatorial Number Theory, and their precise values are known for groups with rank at most two. Indeed, we have (see [15, Theorem 5.8.3])

* Corresponding author.
E-mail addresses: fys850820@163.com (Y. Fan), wdgao1963@yahoo.com.cn (W. Gao), zhongqinghai@yahoo.com.cn (Q. Zhong).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2011.02.017

Theorem A. *Let $G = C_{n_1} \oplus C_{n_2}$ with $1 \leqslant n_1 | n_2$. Then*

$$\mathsf{D}(G) = n_1 + n_2 - 1 \quad \text{and} \quad \mathsf{s}(G) = 2n_1 + 2n_2 - 3.$$

The result for $\mathsf{D}(G)$ dates back to the 1960s, and the special case $n_1 = 1$ and $\mathsf{s}(C_{n_2}) = 2n_2 - 1$ is the well-known theorem of Erdős–Ginzburg–Ziv proved in 1961 [6]. However, the special case where $n_1 = n_2$ is a prime was only settled in 2007 by C. Reiher [19]. More information can be found in the surveys [9,13]. Both the Davenport constant and the Erdős–Ginzburg–Ziv constant have found far reaching generalizations, and for these generalized versions, the precise values have been determined for groups with rank at most two (see [15, Section 6.1], [7], [14, Theorem 5.2], [17]).

The situation is very different for groups of higher rank. Even for the group $G = C_n \oplus C_n \oplus C_n$ with $n \geqslant 2$, the precise value of the Davenport constant is unknown (for general n) and the same is true for the Erdős–Ginzburg–Ziv constant. In what follows, we focus our discussion on the Erdős–Ginzburg–Ziv constant, which will be the main topic of the present paper. In 1995, N. Alon and M. Dubiner [1] proved that for every positive integer r there is a constant $c(r)$ depending only on r such that $\mathsf{s}(C_n^r) \leqslant c(r)n$ for all $n \geqslant 2$. To illustrate the difficulties for obtaining precise values, let us consider the special case $G = \mathbb{F}_3^r$, where $\mathbb{F}_3$ is the finite field with three elements. Then $(\mathsf{s}(G) - 1)/2$ equals the maximal size of a cap in the affine space $\mathbb{F}_3^r$. The maximal size of such caps has been studied in finite geometry for decades, and the precise value is known so far only for $r \leqslant 6$ (see [18,2]). The connection to affine caps will be addressed in greater detail in Section 4. In the next theorem, we gather the cases where precise values for $\mathsf{s}(G)$ are known (more on upper and lower bounds will be given in Section 2).

Theorem B. *Let G be a finite abelian group, n, r positive integers, and a, b nonnegative integers.*

- *If $G = C_{2^a} \oplus C_{2^b}^{r-1}$ where $r \geqslant 2$, $b \geqslant 1$ and $a \in [1, b]$, then* $\mathsf{s}(G) = 2^{r-1}(2^a + 2^b - 2) + 1$ [3, Corollary 4.4].
- $\mathsf{s}(C_{3^a 5^b}^3) = 9(3^a 5^b - 1) + 1$, *where* $a + b \geqslant 1$ [11, Theorem 1.7].
- $\mathsf{s}(C_{3^a}^4) = 20(3^a - 1) + 1$, *where* $a \geqslant 1$ (*the precise value for* $\mathsf{s}(C_3^4)$ *was found independently several times, see* [3, Section 5]; *then use* [3, Theorems 1.3 and 1.4]).
- $\mathsf{s}(C_3^5) = 91$ *and* $\mathsf{s}(C_3^6) = 225$ (*see* [4, Theorem 1.2], [18, Theorem 16] *and Proposition* 4.1).
- $\mathsf{s}(C_{3\times 2^a}^3) = 8(3 \times 2^a - 1) + 1$, *where* $a \geqslant 1$ [11, Theorem 1.8].
- *If G is a p-group for some odd prime p with* $\mathsf{D}(G) = 2\exp(G) - 1$, *then* $\mathsf{s}(G) = 4\exp(G) - 3$ [21, Theorem 1.2].
- *If there exists some odd $q \in \mathbb{P}$ such that* $\mathsf{D}(G_q) - \exp(G_q) + 1 | \exp(G_q)$ *and G_p is cyclic for each $p \in \mathbb{P} \setminus \{q\}$, then* $\mathsf{s}(G) = 2(\mathsf{D}(G_q) - \exp(G_q)) + 2\exp(G) - 1$ ([14, Theorem 4.2]; *G_p denotes the p-Sylow subgroup of G*).

This shows that precise results for $\mathsf{s}(G)$ are extremely sparse (a few more precise results and upper bounds for groups G which are not of the form C_n^r can be found in [3,14]). In the present paper, we focus on groups of the form $G = C_n^r$, with $n, r \in \mathbb{N}$ and $n \geqslant 2$, and we tackle the study of $\mathsf{s}(G)$ with a new approach, combining the direct problem with the associated inverse problem. We outline this in the next paragraph.

Let $G = C_n^r$ with $n, r \in \mathbb{N}$ and $n \geqslant 2$. The inverse problem associated with $\mathsf{s}(G)$ asks for the structure of sequences of length $\mathsf{s}(G) - 1$ that do not have a zero-sum subsequence of length n. The standing conjecture is that every group of above form satisfies the following Property D (see [9, Conjecture 7.2]).

Property D. *Every sequence S over G of length $|S| = \mathsf{s}(G) - 1$ that has no zero-sum subsequence of length n has the form $S = T^{n-1}$ for some sequence T over G.*

In the case $r = 2$, Property D was first studied by the second author in [8], and only recently W.A. Schmid completely determined the structure of the sequences having Property D (it was even

done for general groups of rank two; see [20, Theorem 3.1]). A detailed overview of Property D and its relationship with further inverse problems can be found in the survey paper [13, Section 5].

Suppose that $G = C_n^r$ satisfies Property D. Then $\mathsf{s}(G) = c(n-1)+1$ where $c = |T|$, and we say that G satisfies Property D with respect to c. If $\mathsf{s}(G) = c(n-1)+1$ for some $c \in \mathbb{N}$, then G satisfies the following Property D0.

Property D0. *(With respect to some $c \in \mathbb{N}$.) Every sequence S over G of the form $S = gT^{n-1}$ has a zero-sum subsequence of length n, where $g \in G$ and T is a sequence of length $|T| = c$.*

Now we can state our main result.

Theorem 1.1. *Suppose that C_m^r has Property* D *with respect to c and that C_n^r has Property* D0 *with respect to c, where $m, n, r, c \in \mathbb{N}$. If $\mathsf{s}(C_n^r) \leqslant c(n-1)+n+1$,*

$$n \geqslant (c-1)^2+1 \quad \text{and} \quad m \geqslant \frac{(c(n-1)+n)(n-1)(n^r-(c-1))-(c-1)^2}{n-(c-1)^2},$$

then

$$\mathsf{s}\big(C_{mn}^r\big) \leqslant c(mn-1)+1.$$

The proof of Theorem 1.1 will be given in Section 3. After the proof we will discuss how to apply Theorem 1.1, and we will provide an explicit list of groups satisfying the assumptions of Theorem 1.1. For all of them we will get that $\mathsf{s}(C_{mn}^r) = c(mn-1)+1$.

2. Preliminaries

Our notation and terminology are consistent with [9] and [13]. We briefly gather some key notions and fix the notation concerning sequences over finite abelian groups. Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, we set $[a,b] = \{x \in \mathbb{Z} \mid a \leqslant x \leqslant b\}$. Throughout this article, all abelian groups will be written additively, and for $n \in \mathbb{N}$, we denote by C_n a cyclic group with n elements.

Let G be a finite abelian group and $\exp(G)$ its exponent. A sequence S over G will be written in the form

$$S = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G} g^{\mathsf{v}_g(S)}, \quad \text{with } \mathsf{v}_g(S) \in \mathbb{N}_0 \text{ for all } g \in G,$$

and we call

$$|S| = l \in \mathbb{N}_0 \quad \text{the } \textit{length} \quad \text{and} \quad \sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g \in G} \mathsf{v}_g(S)g \in G \quad \text{the } \textit{sum} \text{ of } S.$$

The sequence S is called a *zero-sum sequence* if $\sigma(S) = 0$. For every element $g \in G$, we set $g+S = (g+g_1) \cdot \ldots \cdot (g+g_l)$. Every map of abelian groups $\varphi : G \to H$ extends to a map from the sequences over G to the sequences over H by setting $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_l)$. If φ is a homomorphism, then $\varphi(S)$ is a zero-sum sequence if and only if $\sigma(S) \in \mathrm{Ker}(\varphi)$.

Lemma 2.1. *Let G be a finite abelian group.*

1. $\mathsf{s}(G) \leqslant |G| + \exp(G) - 1$.

2. *If $H \subset G$ is a subgroup with $\exp(G) = \exp(H)\exp(G/H)$, then*

$$\mathsf{s}(G) \leqslant \big(\mathsf{s}(H) - 1\big)\exp(G/H) + \mathsf{s}(G/H).$$

Proof. 1. This was first proved by the second author in his thesis (in Chinese). A proof can also be found in [13, Theorem 4.2.7].

2. See [15, Proposition 5.7.11]. □

Lemma 2.2. *Let $n \in \mathbb{N}$ with $n \geqslant 2$.*

1. *$\mathsf{s}(C_n^r) \geqslant 2^r(n-1)+1$ for every $r \in \mathbb{N}$.*
2. *If n is odd, then $\mathsf{s}(C_n^3) \geqslant 9n-8$ and $\mathsf{s}(C_n^4) \geqslant 20n-19$.*

Proof. 1. See [16, Hilfssatz 1].

2. See [5] and [3, Lemma 3.4 and Theorem 1.1]. □

The above mentioned lower bounds for $\mathsf{s}(C_n^3)$ and $\mathsf{s}(C_n^4)$ are due to C. Elsholtz and Y. Edel et al. The standing conjecture is that equality holds for all odd integers (see also [11]).

Lemma 2.3. *Let $G = C_{mn}^r$ with $m, n, r \in \mathbb{N}$ and let $c \in \mathbb{N}$.*

1. *If both C_m^r and C_n^r have Property* D *with respect to c and $\mathsf{s}(G) = c(mn-1)+1$, then G has Property* D.
2. *If both C_m^r and C_n^r have Property* D0 *with respect to c, then G has Property* D0 *with respect to c.*

Proof. 1. See [10, Theorem 3.2].

2. Let $S = g_0 \prod_{i=1}^{c} g_i^{mn-1}$ be a sequence over C_{mn}^r. We need to show that S has a zero-sum subsequence of length mn.

Let $\varphi : G \to G$ denote the multiplication by m. Then $\mathrm{Ker}(\varphi) \cong C_m^r$, $\varphi(G) = mG \cong C_n^r$, and

$$\varphi(S) = \varphi(g_0)\prod_{i=1}^{c}\varphi(g_i)^{mn-1}$$

is a sequence over $\varphi(G)$. For every $i \in [1,c]$ and every $j \in [1, m-1]$, we set $S_{(i-1)(m-1)+j} = g_i^n$. For the sequence $T = S(\prod_{i=1}^{c}\prod_{j=1}^{m-1} S_{(i-1)(m-1)+j})^{-1}$ we get $\varphi(T) = \varphi(g_0)\prod_{i=1}^{c}\varphi(g_i)^{n-1}$, and since $\varphi(G)$ has Property D0, T has a subsequence S_0 such that $\varphi(S_0)$ is a zero-sum sequence of length n. Since $\mathrm{Ker}(\varphi)$ has Property D0 and

$$\prod_{k=0}^{c(m-1)}\sigma(S_k) = \sigma(S_0)\prod_{i=1}^{c}\prod_{j=1}^{m-1}\sigma(S_{(i-1)(m-1)+j}) = \sigma(S_0)\prod_{i=1}^{c}(ng_i)^{m-1}$$

is a sequence over $\mathrm{Ker}(\varphi)$, it has a zero-sum subsequence of length m. Therefore there is a subset $I \subset [0, c(m-1)]$ such that $|I| = m$ and $\sum_{k\in I}\sigma(S_k) = 0$, which implies that $\prod_{k\in I} S_k$ is a zero-sum subsequence of S of length mn. □

Lemma 2.4. *Let $a, b \in \mathbb{N}_0$.*

1. *$C_{2^a}^r$ has Property* D *with respect to 2^r for every $r \in \mathbb{N}$.*
2. *$C_{3^a}^4$ has Property* D *with respect to* 20.
3. *$C_{3^a5^b}^3$ has Property* D *with respect to* 9.

Proof. 1. Obviously, C_2^r has Property D, and Theorem B shows that Property D holds with respect to 2^r. Using Lemma 2.3 and Theorem B again, we infer that $C_{2^a}^r$ has Property D with respect to 2^r.

2. C_3^r has Property D by [16, Hilfssatz 3] and [3, Lemma 2.3.3]. It follows from Lemma 2.3 and Theorem B that $C_{3^a}^4$ has Property D with respect to 20.

3. As mentioned above, C_3^3 has Property D, and Theorem B shows that Property D holds with respect to 9. It has been proved in [11, Theorem 1.9] that C_5^3 has Property D with respect to 9. Thus $C_{3^a5^b}^3$ has Property D with respect to 9 again by Lemma 2.3 and Theorem B. □

Lemma 2.5. *Let $n \in \mathbb{N}$ be an odd integer which is only divisible by primes $p \in \{3, 5, 7, 11, 13\}$. Then C_n^3 has Property* D0 *with respect to* 9.

Proof. By Lemma 2.3, it suffices to show that C_p^3 has Property D0 with respect to 9 for all $p \in \{3, 5, 7, 11, 13\}$. For $p \in \{3, 5\}$, this follows from Lemma 2.4. For the other primes this has been verified by a computer program written in C language (the running time was about 0.03, 17 and 31 computer hours, respectively). □

3. Proof of Theorem 1.1 and some applications

Proof of Theorem 1.1. Let $G = C_{mn}^r$ with $m, n, r \in \mathbb{N}$, and let all assumptions be as in Theorem 1.1. Assume to the contrary, there exists a sequence S over G with $|S| = c(mn-1)+1$ such that S has no zero-sum subsequence of length mn. Let $\varphi : G \to G$ denote the multiplication by m. Then $\mathrm{Ker}(\varphi) \cong C_m^r$ and $\varphi(G) = mG \cong C_n^r$. We start with a simple observation which will be used several times in the proof.

A1 Suppose that $S = T_1 \cdot \ldots \cdot T_{c(m-1)}T'$, where $T_1, \ldots, T_{c(m-1)}, T'$ are sequences over G and, for every $i \in [1, c(m-1)]$, $\varphi(T_i)$ has sum zero and length $|T_i| = \exp(\varphi(G)) = n$. Then

$$\sigma(T_1) \cdot \ldots \cdot \sigma(T_{c(m-1)}) = \prod_{i=1}^{c} a_i^{m-1},$$

where $a_1, \ldots, a_{c(m-1)} \in \mathrm{Ker}(\varphi)$ are pairwise distinct.

Proof of A1. Since S has no zero-sum subsequence of length mn, the sequence $\sigma(T_1) \cdot \ldots \cdot \sigma(T_{c(m-1)})$ has no zero-sum subsequence of length m. Since $\mathrm{Ker}(\varphi)$ has Property D, the assertion follows. □

First we show that S has a product decomposition as in assertion A1. Note that

$$\big|\varphi(S)\big| = c(mn-1)+1 = \big(c(m-1)-1\big)n + c(n-1) + n + 1.$$

Since $\mathsf{s}(C_n^r) \leqslant c(n-1)+n+1$, S allows a product decomposition $S = T_1 \cdot \ldots \cdot T_{c(m-1)}T'$, where $T_1, \ldots, T_{c(m-1)}, T'$ are sequences over G and, for every $i \in [1, c(m-1)]$, $\varphi(T_i)$ has sum zero and length $|T_i| = \exp(\varphi(G)) = n$ (for details see [15, Proposition 5.7.10]).

We set

$$\varphi(S) = h_1^{r_1} \cdot \ldots \cdot h_t^{r_t} \quad \text{and} \quad S = S_1 \cdot \ldots \cdot S_t,$$

where $h_1, \ldots, h_t \in \varphi(G)$ are pairwise distinct, $r_1, \ldots, r_t \in \mathbb{N}$, and $\varphi(S_i) = h_i^{r_i}$ for all $i \in [1, t]$. After renumbering if necessary there exists an integer $f \in [0, t]$ satisfying

$$\begin{cases} r_i \geqslant \big(c(n-1)+n\big)(n-1), & \text{if } i \in [1, f], \\ r_i \leqslant \big(c(n-1)+n\big)(n-1)-1, & \text{otherwise.} \end{cases} \tag{1}$$

A2 For every $i \in [1,t]$ we have $r_i \leqslant mn + c(m-1) - m$, and $f \geqslant c$.

Proof of A2. Assume to the contrary, there exists some $i \in [1,t]$ such that $r_i \geqslant mn + c(m-1) - m + 1$. By the definition of S_i, we have $S_i = (g+g_1)\cdot\ldots\cdot(g+g_{r_i})$ for some $g \in G$ with $\varphi(g) = h_i$ and $g_j \in \mathrm{Ker}(\varphi)$ for every $j \in [1, r_i]$. Since $\mathsf{s}(C_m^r) = c(m-1)+1$ and $r_i \geqslant m(n-1) + c(m-1) + 1$, we can write $g_1\cdot\ldots\cdot g_{r_i} = R_0R_1\cdot\ldots\cdot R_n$ where R_j is a zero-sum sequence of length $|R_j| = m$ for every $j \in [1,n]$. Then the shifted sequence $g + R_1\cdot\ldots\cdot R_n$ is a subsequence of S_i such that $|g+R_1\cdot\ldots\cdot R_n| = |R_1\cdot\ldots\cdot R_n| = mn$ and $\sigma(g+R_1\cdot\ldots\cdot R_n) = mng + \sum_{j=1}^n \sigma(R_j) = 0$, a contradiction to the assumption that S has no such zero-sum subsequence.

Combining the upper bounds on r_i with the assumptions that $m \geqslant \frac{(c(n-1)+n)(n-1)(n^r-(c-1))-(c-1)^2}{n-(c-1)^2}$ and $n > (c-1)^2$, we deduce that the c-th largest r_i is at least

$$\frac{|S| - (c-1)(mn + c(m-1) - m)}{n^r - (c-1)} \geqslant \big(c(n-1)+n\big)(n-1).$$

Thus it follows that $f \geqslant c$. □

A3 For every $i \in [1, f]$, $S_i = g_i^{v_i} W_i$ for some $g_i \in G$ and $|W_i| \leqslant 1$.

Proof of A3. Let $i \in [1, f]$. Since $|S_i| = r_i \geqslant (c(n-1)+1)(n-1) > 2n$, we may choose an arbitrary subsequence L of S_i with $|L| = 2n$. We set $L = L_1L_2$ where $|L_1| = |L_2| = n$, and since $\varphi(S_i) = h_i^{r_i}$, it follows that $\sigma(L_1), \sigma(L_2) \in \mathrm{Ker}(\varphi)$.

Since $|S| = c(mn-1)+1$, SL^{-1} admits a product decomposition $SL^{-1} = V_0V_1\cdot\ldots\cdot V_{cm-c-2}$, where $|V_i| = n$ and $\sigma(V_i) \in \mathrm{Ker}(\varphi)$ for all $i \in [1, cm-c-2]$ (we use again [15, Proposition 5.7.10]). Now by A1, $\sigma(L_1)\sigma(L_2)\sigma(V_1)\cdot\ldots\cdot\sigma(V_{cm-c-2}) = \prod_{i=1}^c a_i^{m-1}$, where all $a_i \in \mathrm{Ker}(\varphi)$ are pairwise distinct. After renumbering if necessary we may assume that $\sigma(V_1)\cdot\ldots\cdot\sigma(V_{cm-c-2}) = a_1^{k_1}a_2^{k_2}\prod_{i=3}^c a_i^{m-1}$, where $k_1, k_2 \in [m-3, m-1]$ and $k_1 + k_2 = 2m-4$. Therefore, $\sigma(L_1), \sigma(L_2) \in \{a_1, a_2\}$.

Since $m \geqslant 4$, L_1 is an arbitrary subsequence of L and L an arbitrary subsequence of S_i, we infer that L and therefore S_i has at most two distinct elements. Therefore there exists some element $g_i \in G$ which occurs at least $\frac{r_i}{2} = \frac{(c(n-1)+n)(n-1)}{2} \geqslant 2(n-1)$ times in S_i. We set $S_i = g_i^{v_i}W_i$ where $v_i = \mathsf{v}_{g_i}(S_i)$ and $W_i = a^{|W_i|}$. Assume to the contrary that $|W_i| \geqslant 2$. We set

$$L_1 = g_i^n \quad \text{and} \quad L_2 = g_i^{n-2}a^2,$$

and as above we obtain a product decomposition of $S(L_1L_2)^{-1}$, say $S(L_1L_2)^{-1} = V_0V_1\cdot\ldots\cdot V_{cm-c-2}$, where $|V_i| = n$ and $\sigma(V_i) \in \mathrm{Ker}(\varphi)$ for all $i \in [1, cm-c-2]$. Now by A1, $\sigma(L_1)\sigma(L_2)\sigma(V_1)\cdot\ldots\cdot\sigma(V_{cm-c-2}) = \prod_{i=1}^c a_i^{m-1}$, where all $a_i \in \mathrm{Ker}(\varphi)$ are pairwise distinct. Let $L_1' = L_1ag_i^{-1}$ and $L_2' = L_2g_ia^{-1}$. Since $m \geqslant 4$, again by A1, we infer that

$$\sigma\big(L_1'\big)\sigma\big(L_2'\big)\sigma(V_1)\cdot\ldots\cdot\sigma(V_{cm-c-2}) = \sigma(L_1)\sigma(L_2)\sigma(V_1)\cdot\ldots\cdot\sigma(V_{cm-c-2}) = \prod_{i=1}^c a_i^{m-1}.$$

It follows that $\{\sigma(L_1), \sigma(L_2)\} = \{\sigma(L_1'), \sigma(L_2')\}$, which implies that $\sigma(L_1) = \sigma(L_1')$ or $\sigma(L_1) = \sigma(L_2')$, and thus $g_i = a$, a contradiction. □

Now we have

$$S = g_1^{v_1}\cdot\ldots\cdot g_f^{v_f}T \quad \text{where } T = W_1\cdot\ldots\cdot W_fS_{f+1}\cdot\ldots\cdot S_t.$$

A4 $|\operatorname{supp}(\sigma(g_1^n)\cdot\ldots\cdot\sigma(g_f^n))|\geqslant c$.

Proof of A4. Assume to the contrary that $|\operatorname{supp}(\sigma(g_1^n)\cdot\ldots\cdot\sigma(g_f^n))|\leqslant c-1$. By the definition of f we have that $|T|=|W_1\cdot\ldots\cdot W_f|+|S_{f+1}\cdot\ldots\cdot S_t|\leqslant f+[(c(n-1)+n)(n-1)-1](n^r-f)$. Since

$$\begin{aligned} m &\geqslant \frac{(c(n-1)+n)(n-1)(n^r-(c-1))-(c-1)^2}{n-(c-1)^2}\\ &\geqslant \frac{n^{r+1}+2n+(c(n-1)+n)(n-1)n^r-cn+c-1}{n}, \end{aligned}$$

a straightforward calculation shows that

$$|T|\leqslant \big(c(mn-1)+1\big)-\big[(c-1)(m-1)+1+f\big]n.$$

Thus we get $v_1+\cdots+v_f\geqslant((c-1)(m-1)+1+f)n$, and hence

$$\left\lfloor\frac{v_1}{n}\right\rfloor+\cdots+\left\lfloor\frac{v_f}{n}\right\rfloor\geqslant\left(\frac{v_1}{n}-1\right)+\cdots+\left(\frac{v_f}{n}-1\right)=\frac{v_1+\cdots+v_f}{n}-f\geqslant(c-1)(m-1)+1.$$

By the pigeonhole principle, there are at least m sequences $C_1,\ldots,C_m$ among of the $\lfloor\frac{v_1}{n}\rfloor+\cdots+\lfloor\frac{v_f}{n}\rfloor$ sequences

$$\underbrace{g_1^n,\ldots,g_1^n}_{\lfloor\frac{v_1}{n}\rfloor},\underbrace{g_2^n,\ldots,g_2^n}_{\lfloor\frac{v_2}{n}\rfloor},\ldots,\underbrace{g_f^n,\ldots,g_f^n}_{\lfloor\frac{v_f}{n}\rfloor}$$

such that $\sigma(C_1)=\cdots=\sigma(C_m)$. This implies that $C_1\cdot\ldots\cdot C_m$ is a zero-sum subsequence of S of length mn, a contradiction. □

After renumbering if necessary we may suppose that $|\operatorname{supp}(\sigma(g_1^n)\cdot\ldots\cdot\sigma(g_c^n))|=c$. Let Q be the subsequence of S with $\varphi(Q)=h_{c+1}^{r_{c+1}}\cdot\ldots\cdot h_t^{r_t}$. Then we get $\varphi(S)=h_1^{r_1}\cdot\ldots\cdot h_c^{r_c}\varphi(Q)$, and we distinguish two cases.

Case 1. $h_1^{n-1}\cdot\ldots\cdot h_c^{n-1}$ has no zero-sum subsequence of length n.

Let $l\in\mathbb{N}_0$ be maximal such that Q admits a product decomposition of the form $Q=Q'U_1\cdot\ldots\cdot U_l$, where $|U_i|=n$ and $\varphi(U_i)$ is a zero-sum sequence for every $i\in[1,l]$. It follows that

$$\big|Q'\big|=\left|\varphi\left(Q\left(\prod_{i=1}^{l}U_i\right)^{-1}\right)\right|\leqslant \mathsf{s}\big(\varphi(G)\big)-1\leqslant c(n-1)+n.$$

Since $\varphi(G)\cong C_n^r$ has Property D0 with respect to c, every sequence of the form $h_1^{n-1}\cdot\ldots\cdot h_c^{n-1}\varphi(x)$ with $x\in Q'$ has a zero-sum subsequence of length n. Thus for every $x\in\operatorname{supp}(Q')$, one can find a sequence $U_{l+1}=xU'_{l+1}$, where $U'_{l+1}|SQ^{-1}$, $|U_{l+1}|=n$ and $\varphi(U_{l+1})$ has sum zero. Since

$$r_i\geqslant\big(c(n-1)+n\big)(n-1)\geqslant(n-1)\big|Q'\big|\quad\text{for all } i\in[1,c],$$

we can do so for every $i\in[1,|Q'|]$, and we obtain a product decomposition $S=Q''U_1\cdot\ldots\cdot U_lU_{l+1}\cdot\ldots\cdot U_{l+|Q'|}$ where the sequences $U_{l+1},\ldots,U_{l+|Q'|}$ have the above properties. Obviously, we have

$\varphi(Q'') = h_1^{q_1} \cdot \ldots \cdot h_c^{q_c}$. Next we choose $\lambda = [\frac{q_1}{n}] + \cdots + [\frac{q_c}{n}]$ subsequences $U_{l+|Q'|+1}, \ldots, U_{l+|Q'|+\lambda}$ of Q'' such that $\varphi(U_{l+|Q'|+i}) \in \{h_1^n, \ldots, h_c^n\}$ for all $i \in [1, \lambda]$ and $S = Q''' \prod_{i=1}^{l+|Q'|+\lambda} U_i$. Obviously, we have $\varphi(Q''') = h_1^{q_1'} \cdot \ldots \cdot h_c^{q_c'}$ with $q_i' \in [0, n-1]$ for all $i \in [1, c]$. Therefore we get

$$l + \big|Q'\big| + \lambda = \frac{|S| - |Q'''|}{n} \geqslant \frac{c(mn-1) + 1 - c(n-1)}{n} \geqslant c(m-1) + 1 = \mathsf{s}\big(C_m^r\big).$$

Since $\sigma(U_i) \in \mathrm{Ker}(\varphi) \cong C_m^r$ for all $i \in [1, l + |Q'| + \lambda]$, the sequence $\prod_{i=1}^{l+|Q'|+\lambda} \sigma(U_i)$ has a zero-sum subsequence of length m, and hence S has a zero-sum subsequence of length mn, a contradiction.

Case 2. $h_1^{n-1} \cdot \ldots \cdot h_c^{n-1}$ has a zero-sum subsequence of length n.

Let

$$h_1^{x_1} \cdot \ldots \cdot h_c^{x_c}$$

be a zero-sum subsequence of $h_1^{n-1} \cdot \ldots \cdot h_c^{n-1}$ with $x_i \in [0, n-1]$ and $x_1 + \cdots + x_c = n$. Then $\sigma(g_1^{x_1} \cdot \ldots \cdot g_c^{x_c}) \in \mathrm{Ker}(\varphi)$. Since $|\mathrm{supp}(\sigma(g_1^n) \cdot \ldots \cdot \sigma(g_c^n))| = c$, A1 implies that $\sigma(g_1^{x_1} \cdot \ldots \cdot g_c^{x_c}) = \sigma(g_k^n)$ for some $k \in [1, c]$, say $\sigma(g_1^{x_1} \cdot \ldots \cdot g_c^{x_c}) = \sigma(g_1^n)$. Next we write S in the form

$$S = \big(g_1^n\big)^{s_1} \cdot \ldots \cdot \big(g_c^n\big)^{s_c} g_1^{y_1} \cdot \ldots \cdot g_c^{y_c} M,$$

where $s_i \in \mathbb{N}$ and $y_i \in [0, n-1]$ for all $i \in [1, c]$. We set

$$M_1 = g_1^{y_1} \cdot \ldots \cdot g_c^{y_c} M \quad \text{and} \quad M_2 = \big(g_1^n\big)^{s_1} \cdot \ldots \cdot \big(g_c^n\big)^{s_c},$$

and consider M_2 as a product of $s_1 + s_2 + \cdots + s_c$ subsequences of the form $g_1^n, \ldots, g_c^n$. On the other hand, M_1 admits a product decomposition of the form

$$M_1 = M_1' A_1 \cdot \ldots \cdot A_{c(m-1)-(s_1+s_2+\cdots+s_c)}$$

such that $|A_i| = n$ and $\sigma(A_i) \in \mathrm{Ker}(\varphi)$ for all $i \in [1, c(m-1) - (s_1 + \cdots + s_c)]$. Since $\sigma(g_1^n), \ldots, \sigma(g_c^n)$ are pairwise distinct, A1 implies that the sequence $\sigma(A_1) \cdot \ldots \cdot \sigma(A_{c(m-1)-(s_1+\cdots+s_c)})$ contains the element $\sigma(g_1^n)$ exactly $m - 1 - s_1$ times. By renumbering if necessary we assume that

$$\sigma(A_j) = \sigma\big(g_1^n\big)$$

for every $j \in [1, m-1-s_1]$.

Next we provide a further construction of more than s_1 subsequences of M_2 of length n and with sum $\sigma(g_1^n)$, which allows us to find more than s_1 such subsequences and derive a contradiction. Since $\sigma(g_1^{x_1} \cdot \ldots \cdot g_c^{x_c}) = \sigma(g_1^n)$ and $s_i > x_i$, we can write M_2 in the form $M_2 = M_2' B_1 \cdot \ldots \cdot B_n$ where $B_1 = \cdots = B_n = g_1^{x_1} \cdot \ldots \cdot g_c^{x_c}$. Next we write $M_2' = M_2'' B_{n+1} \cdot \ldots \cdot B_{n+[\frac{ns_1 - nx_1}{n}]}$ where $B_j = g_1^n$ for all $j \in [n+1, n+s_1-x_1]$.

Thus altogether there are $N = n + s_1 - x_1$ subsequences $B_1, \ldots, B_N$ such that $\sigma(B_j) = \sigma(g_1^n)$ and $|B_j| = n$ for all $j \in [1, N]$. Since $N = n + s_1 - x_1 > s_1$, the sequence $A_1 \cdot \ldots \cdot A_{m-s_1-1} B_1 \cdot \ldots \cdot B_{s_1+1}$ is a zero-sum subsequence of S of length mn, a contradiction. □

Now we discuss how to apply Theorem 1.1. Let r, c and n_0 be positive integers and $p \in \mathbb{P}$ a prime. Suppose that C_p^r has Property D with respect to c, and that $C_{n_0}^r$ has Property D0 with respect to c. By Lemma 2.3, $\mathrm{s}(C_m^r) = c(m-1)+1$ and C_m^r has Property D for every $m = p^a$ and every $a \in \mathbb{N}$. By Lemma 2.1.2 we get,

$$\mathrm{s}\big(C_{mn_0}^r\big) \leqslant n_0\big(\mathrm{s}\big(C_m^r\big)-1\big)+\mathrm{s}\big(C_{n_0}^r\big) = n_0c(m-1)+\mathrm{s}\big(C_{n_0}^r\big) = c(mn_0-1)-cn_0+c+\mathrm{s}\big(C_{n_0}^r\big).$$

Therefore, for every fixed n_0 and p, we can choose a sufficiently large such that for $m_0 = p^a$ we get $\mathrm{s}(C_{m_0n_0}^r) \leqslant c(m_0n_0-1)+m_0n_0+1$ and $m_0n_0 \geqslant (c-1)^2+1$. Then we can apply Theorem 1.1 with $n = m_0n_0$ and $m = p^b$ where b is sufficiently large such that m is greater than or equal to the lower bound in n.

We work out a few explicit cases. Let a, b, c, d, e be nonnegative integers. By the above arguments, we can prove that $\mathrm{s}(C_{mn}^r) = c(mn-1)+1$ in each of the following situations.

1. Let $r=3$, $c=9$, $n \geqslant 65$ an odd integer such that C_p^3 has Property D0 with respect to 9 for all prime divisors p of n, and let $m = 3^a5^b$ with
$$m \geqslant \frac{5(n^2-7)\{(50n(n^2-7)-9)(5n(n^2-7)-1)(125n^3(n^2-7)^3-8)-64\}}{(n^2-7)n-64}.$$
2. Let $r=4$, $c=20$, $n \geqslant 362$ an odd integer such that C_p^4 has Property D0 with respect to 20 for all prime divisors p of n, and let $m = 3^a$ with
$$m \geqslant \frac{3(n^3-18)\{(63n(n^3-18)-20)(3n(n^3-18)-1)(81n^4(n^3-18)^4-19)-361\}}{(n^3-18)n-361}.$$
3. $r \geqslant 1$, $c = 2^r$, $n \geqslant (2^r-1)^2+1$ an even integer such that C_n^r has Property D0 with respect to 2^r, and let $m = 2^a$ with
$$m \geqslant \frac{2n^{r-1}\{(2n^r(2^r+1)-2^r)(2n^r-1)((2n^r)^r-(2^r-1))-(2^r-1)^2\}}{n^r-(2^r-1)^2}.$$
4. Let $r=3$, $c=9$, $n = 7^c11^d13^e \geqslant 65$, and let $m = 3^a5^b$ with
$$m \geqslant \frac{5(n^2-7)\{(50n(n^2-7)-9)(5n(n^2-7)-1)(125n^3(n^2-7)^3-8)-64\}}{(n^2-7)n-64}.$$

Proof. 1. By Lemma 2.2.2, $\mathrm{s}(C_k^3) \geqslant 9k-8$ for all odd positive integers k. So, it suffices to prove the upper bound. Let $a_0, b_0 \in \mathbb{N}_0$ with $a_0 \in [0,a]$ and $b_0 \in [0,b]$ such that,

$$n^2-7 \leqslant 3^{a_0}5^{b_0} < 5\big(n^2-7\big).$$

Let $m_0 = 3^{a_0}5^{b_0}$ and $n' = m_0n$. By Lemma 2.1.1 and Lemma 2.1.2, $\mathrm{s}(C_{n'}^3) \leqslant n(\mathrm{s}(C_{m_0}^3)-1)+\mathrm{s}(C_n^3) = n(9m_0-9)+\mathrm{s}(C_n^3) \leqslant 9m_0n-9n+n^3+n-1 \leqslant 9(n'-1)+n'+1$ (the last inequality holds because $m_0 = 3^{a_0}5^{b_0} \geqslant n^2-7$). Let $m' = \frac{m}{m_0}$. By Lemma 2.4, $C_{m'}^3$ has Property D, and by Lemma 2.3.2, $C_{n'}^3$ has Property D0 with respect to 9. Now 1. follows from Theorem 1.1 with n' replacing n and m' replacing m.

2. can be proved in a similar way to 1. and we omit it in detail.
3. can be proved in a similar way to 1. by using Lemma 2.2.1 and we omit it in detail.
4. It follows from 1. and Lemma 2.5. □

4. Concluding remarks and open problems

We recall the relationship between the Erdős–Ginzburg–Ziv constant and the maximal size of caps in the affine space over $\mathbb{F}_3$.

Let G be a finite abelian group, and let $\mathsf{g}(G)$ denote the smallest integer $l \in \mathbb{N}$ such that every squarefree sequence S over G (or in other terms, every subset $S \subset G$) of length $|S| \geqslant l$ has a zero-sum subsequence T of length $|T| = \exp(G)$. The constant $\mathsf{g}(G)$ has been studied for groups of rank two (see [12] and [10, Section 5]). Moreover, it found a lot of attention because of its connection to finite geometry, which we summarize below.

Proposition 4.1. *Let G be a finite abelian group with $\exp(G) = n \geqslant 2$.*

1. $\mathsf{g}(G) \leqslant \mathsf{s}(G) \leqslant (\mathsf{g}(G)-1)(n-1)+1$. *If $G = C_n^r$, with $n \geqslant 2$ and $r \in \mathbb{N}$, and $\mathsf{s}(G) = (\mathsf{g}(G)-1)(n-1)+1$, then G has Property* D.
2. *Suppose that $G = \mathbb{F}_3^r$. Then the maximal size of a cap in G equals $\mathsf{g}(G)-1$, and we have $\mathsf{s}(G) = (\mathsf{g}(G)-1)(3-1)+1 = 2\mathsf{g}(G)-1$.*

Proof. 1. The first inequality is clear. For the second statement see [3, Lemma 2.3].

2. This was first observed by H. Harborth [16]. For a proof in the present terminology see [3, Lemma 5.2]. □

Let $G = C_n^r$ with $n \geqslant 3$ odd and $r \in \mathbb{N}$. As already observed in [3, Section 5], in all situations known so far we have $\mathsf{s}(G) = (\mathsf{g}(C_3^r)-1)(n-1)+1$, and we would like to formulate this as a conjecture (obviously, it implies that C_n^r satisfies Property D0 with respect to $\mathsf{g}(C_3^r)-1$).

Conjecture 4.2. *For all $n \geqslant 3$ odd and all $r \in \mathbb{N}$, we have $\mathsf{s}(C_n^r) = (\mathsf{g}(C_3^r)-1)(n-1)+1$.*

Finally we consider groups with even exponent. Let n, r and a be positive integers. By Theorem B, Lemma 2.1.2 and Lemma 2.1.1 we obtain that

$$\mathsf{s}\big(C_{2^a n}^r\big) \leqslant n\big(2^r\big(2^a-1\big)\big) + n^r + n - 1 = 2^r\big(2^a n\big) + n^r + n - 2^r n - 1,$$

and by Lemma 2.2.1 we have

$$2^r\big(2^a n - 1\big) + 1 \leqslant \mathsf{s}\big(C_{2^a n}^r\big) \leqslant 2^r\big(2^a n - 1\big) + 1 + n^r - 2^r n + 2^r + n - 2.$$

Therefore there exists an $\alpha \in [0, n^r - 2^r n + 2^r + n - 2]$ such that

$$\mathsf{s}\big(C_{2^a n}^r\big) = 2^r\big(2^a n - 1\big) + 1 + \alpha \quad \text{for infinitely many } a \in \mathbb{N}.$$

We are not aware of any even n such that $\mathsf{s}(C_n^r) > 2^r(n-1)+1$, and end with the following conjecture.

Conjecture 4.3. *For all $n, r \in \mathbb{N}$ we have*

$$\mathsf{s}\big(C_{2^a n}^r\big) = 2^r\big(2^a n - 1\big) + 1 \quad \textit{for all sufficiently large } a \in \mathbb{N}.$$

Acknowledgments

This work was supported by the PCSIRT Project of the Ministry of Science and Technology, and the National Science Foundation of China. We would like to thank the referees for all their comments which helped to improve the presentation of the paper.

References

[1] N. Alon, M. Dubiner, Zero-sum sets of prescribed size, in: Combinatorics, Paul Erdős is Eighty, vol. 1, János Bolyai Math. Soc., 1993, pp. 33–50.
[2] Y. Edel, Sequences in abelian groups G of odd order without zero-sum subsequences of length $\exp(G)$, Des. Codes Cryptogr. 47 (2008) 125–134.
[3] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, L. Rackham, Zero-sum problems in finite abelian groups and affine caps, Q. J. Math. 58 (2007) 159–186.
[4] Y. Edel, S. Ferret, I. Landjev, L. Storme, The classification of the largest caps in $AG(5,3)$, J. Combin. Theory Ser. A 99 (2002) 95–110.
[5] C. Elsholtz, Lower bounds for multidimensional zero sums, Combinatorica 24 (2004) 351–358.
[6] P. Erdős, A. Ginzburg, A. Ziv, Theorem in the additive number theory, Bull. Res. Council Israel 10 (1961) 41–43.
[7] M. Freeze, W.A. Schmid, Remarks on a generalization of the Davenport constant, Discrete Math. 310 (2010) 3373–3389.
[8] W. Gao, Two zero sum problems and multiple properties, J. Number Theory 81 (2000) 254–265.
[9] W. Gao, A. Geroldinger, Zero-sum problems in finite abelian groups: a survey, Expo. Math. 24 (2006) 337–369.
[10] W. Gao, A. Geroldinger, W.A. Schmid, Inverse zero-sum problems, Acta Arith. 128 (2007) 245–279.
[11] W. Gao, Q.H. Hou, W.A. Schmid, R. Thangadurai, On short zero-sum subsequences II, Integers 7 (2007), paper A21, 22 pp.
[12] W. Gao, R. Thangadurai, A variant of Kemnitz conjecture, J. Combin. Theory Ser. A 107 (2004) 69–86.
[13] A. Geroldinger, Additive group theory and non-unique factorizations, in: A. Geroldinger, I. Ruzsa (Eds.), Combinatorial Number Theory and Additive Group Theory, in: Adv. Courses Math. CRM Barcelona, Birkhäuser, 2009, pp. 1–86.
[14] A. Geroldinger, D.J. Grynkiewicz, W.A. Schmid, Zero-sum problems with congruence conditions, Acta Math. Hungar. 131 (2011) 323–345.
[15] A. Geroldinger, F. Halter-Koch, Non-unique Factorizations. Algebraic, Combinatorial and Analytic Theory, Pure Appl. Math., vol. 278, Chapman & Hall/CRC, 2006.
[16] H. Harborth, Ein Extremalproblem für Gitterpunkte, J. Reine Angew. Math. 262 (1973) 356–360.
[17] A. Plagne, W.A. Schmid, An application of coding theory to estimating Davenport constants, Des. Codes Cryptogr., doi:10.1007/s10623-010-9441-5, in press.
[18] A. Potechin, Maximal caps in $AG(6,3)$, Des. Codes Cryptogr. 46 (2008) 243–259.
[19] C. Reiher, On Kemnitz' conjecture concerning lattice points in the plane, Ramanujan J. 13 (2007) 333–337.
[20] W.A. Schmid, Restricted inverse zero-sum problems in groups of rank two, Q. J. Math., doi:10.1093/qmath/haq042, in press.
[21] W.A. Schmid, J.J. Zhuang, On short zero-sum subsequences over p-groups, Ars Combin. 95 (2010) 343–352.