# ZERO-SUM PROBLEMS IN FINITE ABELIAN GROUPS AND AFFINE CAPS

YVES EDEL, CHRISTIAN ELSHOLTZ,
ALFRED GEROLDINGER, SILKE KUBERTIN, LAURENCE RACKHAM

Abstract. For a finite abelian group $G$ let $\mathsf{s}(G)$ denote the smallest integer $l$ such that every sequence $S$ over $G$ of length $|S| \ge l$ has a zero-sum subsequence of length $\exp(G)$. We derive new upper and lower bounds for $\mathsf{s}(G)$ and all our bounds are sharp for special types of groups. The results are not restricted to groups $G$ of the form $G = C_n^r$ but they respect the structure of the group. In particular, we show $\mathsf{s}(C_n^4) \ge 20n - 19$ for all odd $n$ which is sharp if $n$ is a power of 3. Moreover, we investigate the relationship between extremal sequences and maximal caps in finite geometry.

## 1. Introduction and Main Results

Let $G$ be a finite abelian group. We denote by $\mathsf{s}(G)$ (or $\eta(G)$ respectively) the smallest integer $l \in \mathbb{N}$ such that every sequence $S$ over $G$ of length $|S| \ge l$ has a zero-sum subsequence $T$ of length $|T| = \exp(G)$ (or a zero-sum subsequence $T$ of length $|T| \in [1, \exp(G)]$ respectively); for details on terminology and notations we refer to Section 2. The investigation of these invariants has a long tradition in combinatorial number theory as well as in finite geometry (for an overview see [32, Section 5.7] and Section 5). As already pointed out by H. Harborth, $\mathsf{s}(C_n^r)$ is the smallest integer $l$ such that every set of $l$ lattice points in the $r$-dimensional euclidean space contains $n$ elements which have a centroid with integral coordinates. This geometric interpretation was a main reason why emphasis was formerly placed on groups of the form $C_n^r$. In the meantime new applications (for example in the theory of non-unique factorizations, see [32]) caused the need for investigations of the invariants $\mathsf{s}(G)$ and $\eta(G)$ for general finite abelian groups.

In the present paper such investigations are carried out for the first time in a systematic way. In Theorems **A** and **B** we briefly summarize the present state of knowledge, and then we discuss the new results.

For finite abelian groups of rank at most two, both invariants $\eta(G)$ and $\mathsf{s}(G)$ are completely determined.

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

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

A proof of Theorem **A** was recently given in [32, Theorem 5.8.3]. It contains the result by C. Reiher, which states that $\mathsf{s}(C_p \oplus C_p) = 4p - 3$ for all $p \in \mathbb{P}$ (see [56] and [59]), and it contains

2000 *Mathematics Subject Classification.* 11B50, 20K01, 51E22.
*Key words and phrases.* zero-sum sequences, finite abelian groups, affine caps.

the Theorem of Erdős-Ginzburg-Ziv (set $n_1 = 1$; see [19] for the original paper; for various proofs see [1] and [51, Section 2.4]).

From now on we consider finite abelian groups of rank larger than two, and we start with the discussion of lower bounds.

**Theorem B.** *Let $n, r \in \mathbb{N}$.*

1. $\eta(C_n^r) \ge (2^r - 1)(n-1) + 1$ *and* $\mathsf{s}(C_n^r) \ge 2^r(n-1) + 1$.
2. *If $n$ is odd, then there exists a sequence $T \in \mathcal{F}(C_n^3)$ of length $|T| = 9$ such that $T^{n-1}$ has no zero-sum subsequence of length $n$. In particular, we have $\eta(C_n^3) \ge 8n - 7$ and $\mathsf{s}(C_n^3) \ge 9n - 8$.*

The first result is due to H. Harborth (see [34, Hilfssatz 1] or Proposition 3.1 for a generalization) and the second due to C. Elsholtz ([17], see also Lemma 3.4 for a simpler alternative proof). Note that in these papers only the result for $\mathsf{s}(C_n^r)$ is formulated but the proofs and Lemma 2.3.2 (below) show the lower bound for $\eta(C_n^r)$.

In [27] W. Gao and R. Thangadurai conjecture that the lower bounds given in Theorem **B**.2 are the precise values, that is

$$\eta(C_n^3) = 8n - 7 \quad \text{and} \quad \mathsf{s}(C_n^3) = 9n - 8 \quad \text{for all odd} \quad n \in \mathbb{N}_{\ge 3}$$

(see also Corollary 4.5).

Before discussing our new results we consider the inverse problems associated to the invariants $\mathsf{s}(G)$ and $\eta(G)$. In other words, we study the structure of sequences $S \in \mathcal{F}(G)$ of length $|S| = \mathsf{s}(G) - 1$ (or $|S| = \eta(G) - 1$ respectively) which have no zero-sum subsequence $T$ of length $|T| = \exp(G)$ (or no zero-sum subsequence $T$ of length $|T| \in [1, \exp(G)]$ respectively). These problems were first studied for groups of the form $G = C_n \oplus C_n$ by P. van Emde Boas (see [18]). Suppose that $G = C_n^r$ with $n \ge 2$ and $r \in \mathbb{N}$. It is generally believed that $G$ has the following two properties:

**Property C.** Every sequence $S \in \mathcal{F}(G)$ of length $|S| = \eta(G) - 1$ which has no short zero-sum subsequence has the form $S = T^{n-1}$ for some sequence $T \in \mathcal{F}(G)$.

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

If $n \ge 2$ and $r = 1$, then Property **C** holds (trivially) and so does Property **D**, as was proved independently by several authors (see [54], [4], [24, Theorem 1]). For a detailed discussion of these two properties in the case $r = 2$ see [26] and in the case $r \ge 3$ see [28]. Clearly, if Property **D** holds, then $n-1$ divides $\mathsf{s}(C_n^r) - 1$ and, by Lemma 2.3.2 (below) we have $\eta(C_n^r) = \mathsf{s}(C_n^r) - n + 1$.

In Theorem 1.1 we present new lower bounds for $\eta(C_n^4)$ and for $\mathsf{s}(C_n^4)$, and we conjecture that these lower bounds give the precise value for all odd $n \in \mathbb{N}_{\ge 3}$ (see Corollary 4.5). The sequence $S$ we construct for the proof of Theorem 1.1 has the form $S = T^{n-1}$ for some $T \in \mathcal{F}(C_n^r)$, supporting the conjecture that Property **D** holds for $C_n^4$. The proof of Theorem 1.1 is given in Section 3, and subsequently we show how to lift the bounds of Theorem 1.1 and Theorem **B** to groups of higher rank (see Proposition 3.5 and Corollary 3.6).

**Theorem 1.1.** *Let $n$ be an odd integer with $n \ge 3$. Then there exists a sequence $T \in \mathcal{F}(C_n^4)$ of length $|T| = 20$ such that $T^{n-1}$ has no zero-sum subsequence of length $n$. In particular, we have $\eta(C_n^4) \ge 19n - 18$ and $\mathsf{s}(C_n^4) \ge 20n - 19$.*

Now we discuss upper bounds. W. Gao and Y.X. Yang proved that $\mathsf{s}(G) \le |G| + \exp(G) - 1$ for every finite abelian group $G$ (see [30] for the original paper (in Chinese) or [32, Theorem 5.7.4]). Upper bounds for groups $G$ of the form $G = C_n^r$ were given by N. Alon, M. Dubiner and recently by S. Kubertin (see Remarks 3.7).

We derive new upper bounds both for $\eta(G)$ and $\mathsf{s}(G)$. The first (Theorem 1.2) rests on upper bounds for $\mathsf{s}(C_p^r)$ for primes $p \in \mathbb{P}$ dividing $\exp(G)$, and the second (Theorem 1.3) is valid for groups with large exponent (as usual, $\mathsf{D}(G)$ denotes the Davenport constant of $G$, see Definition 2.1 and the subsequent remarks).

**Theorem 1.2.** *Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $r = \mathsf{r}(G)$ and $1 < n_1 \mid \ldots \mid n_r$. Let $c_1, \ldots, c_r \in \mathbb{N}$ such that for all primes $p \in \mathbb{P}$ with $p \mid n_r$ and all $i \in [1, r]$ we have $\mathsf{s}(C_p^i) \le c_i(p-1) + 1$. Then*

$$\mathsf{s}(G) \le \sum_{i=1}^{r} (c_{r+1-i} - c_{r-i}) n_i \ - c_r + 1 \quad \text{where} \quad c_0 = 0\,.$$

*In particular, if $n_1 = \ldots = n_r = n$, then $\mathsf{s}(G) \le c_r(n-1) + 1$.*

**Theorem 1.3.** *Let $G = H \oplus C_n$ be a finite abelian group where $H \subset G$ is a subgroup, $\exp(G) = n \ge 2$ and $\mathsf{D}(G) \le 2n - 1$.*

1. *If $\mathsf{D}(G \oplus C_n) \le 3n - 1$, then $2\big(\mathsf{D}(H) - 1\big) + n \le \eta(G) \le \mathsf{D}(G \oplus C_n)$.*
2. *If $G$ is a $p$-group for some odd prime $p$, then*

$$\mathsf{D}(G \oplus C_n) + \mathsf{D}(H) - 1 \le \mathsf{s}(G) \le \mathsf{D}(G \oplus C_n) + n\,.$$

The proofs of the Theorems 1.2 and 1.3 will be given in Section 4. Theorem 1.2 is proved by the induction method, and provides the best known upper bound for groups $G$ which are not of the form $G = C_n^r$. The main part of Theorem 1.3 is the upper bound in 1.3.2 which generalizes (for odd primes) recent results of W. Gao and J. Zhou (see [31, Theorem 1.5], and also [23, Proposition 3.1]). Its proof uses the polynomial method, first developed by L. Rónyai and later generalized by Z.W. Sun and S. Kubertin (see [57], [61], [45]).

After the proof of Theorem 1.3 we present special types of groups for which the lower and upper bounds derived in this paper coincide (see Corollaries 4.4, 4.5 and 4.6). The quality of the bounds in Theorem 1.3 can immediately be seen by considering the following most simple case. If (in Theorem 1.3) $H = C_m$ for some $m$ dividing $n$, then $2\big(\mathsf{D}(H) - 1\big) + n = 2m + n - 2 = \eta(G)$ (see Theorem **A**). Moreover, if $H = C_n$ and $n$ is a prime power, then (again by Theorem **A**) $\eta(G) = 3n - 2 = \mathsf{D}(G \oplus C_n)$ and $\mathsf{s}(G) = 4n - 3 = \mathsf{D}(G \oplus C_n) + n - 1 = \mathsf{D}(G \oplus C_n) + \mathsf{D}(H) - 1$.

In Section 5 we discuss further applications of the invariants $\mathsf{s}(G)$ and $\eta(G)$. Special emphasis is given to the role of the invariant $\mathsf{s}(C_n^r)$ in finite geometry and problems on arithmetic progressions. We give a detailed discussion of the history of the associated geometric problems.

## 2. Notations and some preparatory results

Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of all prime numbers and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For integers $a, b \in \mathbb{Z}$ we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$, and for $c \in \mathbb{N}$ let $\mathbb{N}_{\ge c} = \mathbb{N} \setminus [1, c-1]$. Throughout, all abelian groups will be written additively and for $n \in \mathbb{N}$ let $C_n$ denote a cyclic group with $n$ elements. For $p \in \mathbb{P}$ let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and for a power $q$ of $p$ let $\mathbb{F}_q$ denote a field with $q$ elements such that $\mathbb{F}_q \supset \mathbb{F}_p$.

Let $G$ be an additive finite abelian group. If $|G| > 1$, then there are uniquely determined integers $r, n_1, \ldots, n_r$ with $1 < n_1 \mid \ldots \mid n_r$ such that $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$. Then $r = \mathsf{r}(G)$ is the rank of $G$, and $n_r = \exp(G)$ is the exponent of $G$. An $r$-tuple $(e_1, \ldots, e_r)$ in $G \setminus \{0\}$ is called a basis of $G$ if $G = \langle e_1 \rangle \oplus \ldots \oplus \langle e_r \rangle$. For $n \in \mathbb{N}$ we set $nG = \{ng \mid g \in G\}$.

We denote by $\mathcal{F}(G)$ the free (abelian, multiplicative) monoid with basis $G$. An element $S \in \mathcal{F}(G)$ is called a *sequence over* $G$ and will be written in the form

$$S = \prod_{g \in G} g^{\mathsf{v}_g(S)} = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)\,,$$

where $\mathsf{v}_g(S)$ is called the *multiplicity of* $g$ *in* $S$. A sequence $S' \in \mathcal{F}(G)$ is called a *subsequence of* $S$ if there exists some $S'' \in \mathcal{F}(G)$ such that $S = S'S''$ (equivalently, $S' \mid S$ or $\mathsf{v}_g(S') \le \mathsf{v}_g(S)$ for every $g \in G$). If this holds, then $S'' = {S'}^{-1}S$. As usual,

$$\sigma(S) = \sum_{g \in G} \mathsf{v}_g(S)g = \sum_{i=1}^{l} g_i \ \in \ G$$

denotes the *sum of* $S$,

$$\mathrm{supp}(S) = \{g \in G \mid \mathsf{v}_g(S) > 0\} \subset G$$

is the *support of* $S$ and

$$|S| = \sum_{g \in G} \mathsf{v}_g(S) = l \in \mathbb{N}_0$$

denotes the *length of* $S$. Clearly, $|S| = 0$ if and only if $S = 1$ is the empty sequence. We say that the sequence $S$ is

- *a zero-sum sequence* (resp. *has sum zero*) if $\sigma(S) = 0$.
- *short* (in $G$) if $|S| \in [1, \exp(G)]$.
- *squarefree* if $\mathsf{v}_g(S) \le 1$ for all $g \in G$.

**Definition 2.1.** We denote by

- $\mathsf{D}(G)$ the smallest integer $l \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a zero-sum subsequence. $\mathsf{D}(G)$ is called the *Davenport constant of* $G$.
- $\eta(G)$ the smallest integer $l \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a short zero-sum subsequence.
- $\mathsf{s}(G)$ the smallest integer $l \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a zero-sum subsequence $T$ of length $|T| = \exp(G)$.
- $\mathsf{g}(G)$ the smallest integer $l \in \mathbb{N}$ such that every squarefree sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a zero-sum subsequence $T$ of length $|T| = \exp(G)$.

A thorough treatment of the Davenport constant, a central invariant in zero-sum theory, may be found in [32, Chapter 5], and for some recent results we refer to [11]. Apart from basic properties we use the following classical results on $\mathsf D(G)$ (originally due to D. Kruyswijk and J.E. Olson): If $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$, where $r = \mathsf r(G)$ and $1 < n_1 \mid \ldots \mid n_r$, then

$$1 + \sum_{i=1}^{r} (n_i - 1) \le \mathsf D(G)\,,$$

and equality holds if either $r \le 2$ or $G$ is a $p$-group (see [32, Theorems 5.5.9 and 5.8.3]).

Let $\varphi\colon G \to G'$ be a map of abelian groups. Then there is a unique homomorphism $\overline{\varphi}\colon \mathcal F(G) \to \mathcal F(G')$ with $\overline{\varphi} \mid G = \varphi$. We simply write $\varphi$ instead of $\overline{\varphi}$, whence if $S = g_1 \cdot \ldots \cdot g_l \in \mathcal F(G)$, then $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_l) \in \mathcal F(G')$.

We start with a simple observation which will be used tacitly throughout the paper. Then we continue with a lemma relating the invariants $\eta(G)$, $\mathsf s(G)$ and $\mathsf g(G)$. In the Sections 3 and 4 we concentrate on $\eta(G)$ and $\mathsf s(G)$ and in Section 5 we mainly deal with $\mathsf g(G)$.

**Lemma 2.2.** *Let $G$ be a finite abelian group with $\exp(G) = n \ge 2$, $g \in G$, $\varphi\colon G \to G$ an automorphism and $f\colon G \to G$ a map defined by $f(x) = \varphi(x) - g$ for every $x \in G$.*

1. *A sequence $S \in \mathcal F(G)$ has a zero-sum subsequence of length $n$ if and only if $f(S)$ has a zero-sum subsequence of length $n$.*
2. *Let $S = h^{n-1}T \in \mathcal F(G)$ with $h \in G$, $f(h) = 0$ and $T \in \mathcal F(G)$. Then $S$ has a zero-sum subsequence of length $n$ if and only if $f(T)$ has a short zero-sum subsequence.*

*Proof.* 1. Let $S = g_1 \cdot \ldots \cdot g_l \in \mathcal F(G)$ and $T = \prod_{i\in I} g_i$ be a subsequence of $S$ where $I \subset [1, l]$ with $|I| = n$. Then

$$\sigma(f(T)) = \sum_{i\in I} \big(\varphi(g_i) - g\big) = \varphi(\sigma(T))$$

whence $\sigma(T) = 0$ if and only if $\sigma(f(T)) = 0$.

2. By 1., $S$ has a zero-sum subsequence of length $n$ if and only if $f(S)$ has a zero-sum subsequence of length $n$. Since $f(S) = 0^{n-1}f(T)$, the assertion follows. □

**Lemma 2.3.** *Let $G$ be a finite abelian group with $\exp(G) = n \ge 2$, $S \in \mathcal F(G)$ a sequence which has no zero-sum subsequence of length $n$ and $h = \max\{\mathsf v_g(S) \mid g \in G\}$.*

1. $\mathsf D(G) \le \eta(G) \le \mathsf s(G) - n + 1$.
2. *If $h = n - 1$, then $\eta(G) \ge |S| - n + 2$. In particular, if $|S| = \mathsf s(G) - 1$, then $\eta(G) = \mathsf s(G) - n + 1$.*
3. $\mathsf g(G) \le \mathsf s(G) \le \big(\mathsf g(G) - 1\big)(n - 1) + 1$. *If $G = C_n^r$, with $n \ge 2$ and $r \in \mathbb N$, and $\mathsf s(G) = \big(\mathsf g(G) - 1\big)(n - 1) + 1$, then $G$ has Property* **D**.
4. *If $H$ is a finite abelian group with $|H| \ge h$ and $f\colon [1, h] \to H$ an injective map, then*

$$\prod_{g\in G} \prod_{i=1}^{\mathsf v_g(S)} (g + f(i)) \in \mathcal F(G \oplus H)$$

*is a squarefree sequence which has no zero-sum subsequence of length $n$. In particular, if $\exp(H) \mid n$ then $\mathsf g(G \oplus H) \ge \mathsf s(G)$, and $\mathsf g(C_n^{r+1}) \ge \mathsf s(C_n^r)$.*

*Proof.* 1. Straightforward (for a detailed proof see [32, Lemma 5.7.2]).

2. Let $S = g^{n-1}T$, with $g \in G$ and $T \in \mathcal{F}(G)$, and consider the map $f\colon G \to G$ defined by $f(x) = x - g$ for all $x \in G$. By Lemma 2.2.2, $f(T)$ has no short zero-sum subsequence whence $\eta(G) \ge |f(T)| + 1 = |S| - n + 2$. If $|S| = \mathsf{s}(G) - 1$, then $\eta(G) \ge \mathsf{s}(G) - n + 1$ whence 1. implies that $\eta(G) = \mathsf{s}(G) - \exp(G) + 1$.

3. The first inequality follows by definition. Let

$$U = g_1^{k_1} \cdot \ldots \cdot g_l^{k_l} \in \mathcal{F}(G), \quad \text{where} \quad l, k_1, \ldots, k_l \in \mathbb{N} \quad \text{and} \quad g_1, \ldots, g_l \in G \quad \text{are distinct},$$

be a sequence of length $|U| = \mathsf{s}(G) - 1$ which has no zero-sum subsequence of length $n$. Clearly, $T = g_1 \cdot \ldots \cdot g_l$ is a squarefree sequence which has no zero-sum subsequence of length $n$ whence $l \le \mathsf{g}(G) - 1$. Therefore, we obtain that

$$\mathsf{s}(G) - 1 = |U| = \sum_{i=1}^{l} k_i \le l(n-1) \le \big(\mathsf{g}(G) - 1\big)(n-1)\,.$$

Furthermore, if $G = C_n^r$ and equality holds, then $k_1 = \ldots = k_l = n - 1$ whence $G$ has Property **D**.

4. By construction, the given sequence has all asserted properties. □

All sequences $S$ constructed in this paper which have no zero-sum subsequence of length $\exp(G)$ have the additional property of Lemma 2.3.2. (that is, they have some element with multiplicity $\exp(G) - 1$) whence we always get $\eta(G) \ge |S| - \exp(G) + 2$. W. Gao conjectured that for all finite abelian groups $G$ we have $\eta(G) = \mathsf{s}(G) - \exp(G) + 1$. Among others this holds true for all groups $G$ with $\mathsf{r}(G) \le 2$ (see Theorem **A**) and for all groups $G$ with $\exp(G) \le 4$ (see [25]). Let $G = C_n^r$ with $n \ge 2$ and $r \in \mathbb{N}$ and consider the inequality $\mathsf{s}(G) \le \big(\mathsf{g}(G)-1\big)(n-1)+1$. Then equality holds for $n = 2$ (trivial) and for $n = 3$ (see [34, Hilfssatz 3]). If $p$ is a prime with $p \ge 67$, then $\mathsf{g}(C_p \oplus C_p) = \mathsf{s}(C_p) = 2p - 1$ (see Theorem **A** and [29]).

## 3. Lower bounds

All lower bounds for the invariants $\eta(G)$ and $\mathsf{s}(G)$ are established by explicit constructions of sequences $S \in \mathcal{F}(G)$ having no zero-sum subsequences with the required properties. The first two results will be used several times whereas the specific preparations for the proof of Theorem 1.1 start from Lemma 3.3 on. A geometric interpretation of the sequences given in Lemma 3.4 and in Theorem 1.1 will be offered after Lemma 5.4. Note that in the special setting of $p$-groups the bounds given in Lemma 3.2 were first proved in [31, Theorem 1.5].

**Proposition 3.1.** *Let* $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$, *where* $r = \mathsf{r}(G)$ *and* $1 < n_1 \mid \ldots \mid n_r$, *and let* $(e_1, \ldots, e_r)$ *be a basis of* $G$ *with* $\mathrm{ord}(e_i) = n_i$ *for every* $i \in [1, r]$. *For a subset* $I \subset [1, r]$ *we set* $e_I = \sum_{i \in I} e_i$ (*in particular,* $e_\emptyset = 0$).

1. *Let*

$$U = \prod_{k=1}^{r} \prod_{I \subset [k+1, r]} (e_k + e_I)^{n_k - 1} \quad \in \mathcal{F}(G)\,.$$

*Then the following statements are equivalent*:

(a) $U$ *has no short zero-sum subsequence.*

(b) $r = 1$ *or* $(r \ge 2$ *and* $n_2 = n_r)$.

2. *Let* $H$ *be a finite abelian group with* $\exp(H) = n$ *being a multiple of* $n_r$ *and* $T \in \mathcal{F}(H)$ *such that* $T^{n-1}$ *has no zero-sum subsequence of length* $n$. *Then the sequence*

$$S = \prod_{g \in T} \left( g^{n-1} \prod_{i=1}^{r} (g + e_i)^{n_i - 1} \right) \in \mathcal{F}(G \oplus H)$$

*has no zero-sum subsequence of length* $n$, *and hence*

$$\mathsf{s}(G \oplus H) \ge \eta(G \oplus H) + n - 1 \ge 1 + |T| \big( n - 1 + \sum_{i=1}^{r} (n_i - 1) \big) .$$

*Furthermore, if* $m \in \mathbb{N}$ *and* $I_1, \ldots, I_m \subset [1, r]$ *are pairwise disjoint sets with* $\sum_{i \in I_\mu} (n_i - 1) \ge n$ *for all* $\mu \in [1, m]$, *then*

$$\overline{S} = S \prod_{g \in T} \prod_{\mu=1}^{m} (g + e_{I_\mu}) \quad \in \mathcal{F}(G \oplus H)$$

*has no zero-sum subsequence of length* $n$.

3. *If* $\overline{G} = G \oplus C_n^k$ *with* $k, n \in \mathbb{N}$ *and* $n_r \mid n$, *then*

$$\mathsf{s}(\overline{G}) \ge \eta(\overline{G}) + n - 1 \ge 1 + 2^k \big( n - 1 + \sum_{i=1}^{r} (n_i - 1) \big) .$$

*Proof.* 1. (a) $\Rightarrow$ (b) If $r \le 2$, then there is nothing to show. If $r \ge 3$ and $n_2 < n_r$, then

$$U' = e_r^{n_r - n_2 - 1} (e_2 + e_r)^{n_2 - n_1 + 1} (e_1 + e_r)(e_1 + e_2 + e_r)^{n_1 - 1}$$

is a short zero-sum subsequence of $U$, a contradiction.

(b) $\Rightarrow$ (a) If $r = 1$, then the assertion is clear. Suppose that $r \ge 2$ and $n_2 = n_r = n$. Then

$$U = \prod_{I \subset [2,r]} (e_1 + e_I)^{n_1 - 1} \prod_{\emptyset \ne I \subset [2,r]} e_I^{n-1} \quad \in \mathcal{F}(G) ,$$

and we consider a zero-sum subsequence

$$U' = \prod_{\nu=1}^{k} (e_1 + e_{I_\nu}) \prod_{\nu=k+1}^{l} e_{I_\nu}$$

of $U$ with $0 \le k \le l \le n$, subsets $I_1, \ldots, I_k \subset [2, r]$ and non-empty subsets $I_{k+1}, \ldots, I_l \subset [2, r]$. We have to show that $|U'| = l = 0$. Assume to the contrary that $l \ge 1$. Since $\mathsf{v}_{e_1}(U') \le \mathsf{v}_{e_1}(U) = n_1 - 1$, there exists some $\nu \in [1, l]$ such that $I_\nu$ is non-empty. Let $i \in I_\nu$ and

$$\alpha = |\{ j \in [1, l] \mid i \in I_j \}| .$$

Since $\alpha \equiv 0 \mod n$ and $1 \le \alpha \le l \le n$, it follows that $\alpha = l = n$. Since $U'$ has sum zero, we infer that $I_1 = \ldots = I_n$ whence

$$U' = (e_1 + e_{I_1})^k e_{I_1}^{n-k} .$$

Then $k \equiv 0 \mod n_1$ and $k \le \mathsf{v}_{e_1 + e_{I_1}}(U) = n_1 - 1$ imply that $k = 0$ whence $U' = e_{I_1}^n$ is a subsequence of $U$, a contradiction.

2. Assume to the contrary that $S$ has a zero-sum subsequence $S'$ of length $n$. Since every zero-sum subsequence of $T^m$, for any $m \ge n$, of length $n$ has the form $g^n$ for some $g \in \mathrm{supp}(T)$, the sequence $S'$ has the form

$$S' = g^{l_g} \prod_{i=1}^{r} (g+e_i)^{l_i} \,,$$

with $g \in \mathrm{supp}(T)$, $l_g \in [0, n-1]$ and $l_i \in [0, n_i - 1]$ for all $i \in [1, r]$. But $l_g < n$, implies that there is some $i \in [1, r]$ with $l_i \in [1, n_i - 1]$ and hence $\sigma(S') \neq 0$, a contradiction. Now the lower bounds for $\mathsf{s}(G \oplus H)$ and $\eta(G \oplus H)$ follow from Lemma 2.3.

If $\overline{S}$ has a zero-sum subsequence $\overline{S}'$ of length $n$, then

$$\overline{S}' = g^{l_g} \prod_{i=1}^{r} (g+e_i)^{l_i} \prod_{\mu=1}^{m} (g+e_{I_\mu})^{\delta_\mu} \,,$$

with $\delta_\mu \in \{0, 1\}$ and all other parameters as before. Since $\overline{S}'$ is not a subsequence of $S$, there is some $\mu \in [1, m]$ with $\delta_\mu = 1$. This implies that $\overline{S}'$ must contain the sequence

$$\overline{S}'' = (g+e_{I_\mu}) \prod_{i \in I_\mu} (g+e_i)^{n_i - 1} \,,$$

and hence $n = |\overline{S}'| \ge |\overline{S}''| \ge 1 + \sum_{i \in I_\mu} (n_i - 1) \ge n+1$, a contradiction.

3. Applying 1. to the group $C_n^k$ we obtain a sequence $T = 0T'$ of length $|T| = 2^k$ such that $U = {T'}^{n-1}$ has no short zero-sum subsequence and hence $T^{n-1}$ has no zero-sum subsequence of length $n$. Then 2. gives us a sequence $S \in \mathcal{F}(\overline{G})$ of length $|S| = |T|(n - 1 + \sum_{i=1}^{r} (n_i - 1))$ which has no zero-sum subsequence of length $n$. Now the assertion follows from Lemma 2.3. □

**Lemma 3.2.** *Let $G$ be a finite abelian group with $\exp(G) = n \ge 2$ and $G = H \oplus \langle e \rangle$ where $H \subset G$ is a subgroup and $e \in G$ with $\mathrm{ord}(e) = n$. Then*

$$\eta(G) \ge 2\big(\mathsf{D}(H) - 1\big) + n \quad \textit{and} \quad \mathsf{s}(G) \ge 2\big(\mathsf{D}(H) - 1\big) + 2n - 1 \,.$$

*Proof.* If $T = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(H)$ is a sequence of length $|T| = l = \mathsf{D}(H) - 1$ which has no zero-sum subsequence, then obviously the sequence

$$S = e^{n-1} \prod_{i=1}^{l} g_i \prod_{i=1}^{l} (g_i + e) \ \in \mathcal{F}(G)$$

has no short zero-sum subsequence. This implies that

$$\eta(G) \ge |S| + 1 = 2\big(\mathsf{D}(H) - 1\big) + n \,,$$

and by Lemma 2.3.1 we have $\mathsf{s}(G) \ge 2\big(\mathsf{D}(H) - 1\big) + 2n - 1$. □

For the rest of this section we introduce the following notation. Let $G = C_n^r$, with $n \ge 2$ and $r \in \mathbb{N}$, and let $(e_1, \ldots, e_r)$ be a basis of $G$. In order to stress the geometric aspect of the theory we write the elements $g \in G$ as coordinate vectors, this means for an element $g \in G$ with $g = a_1 e_1 + \ldots + a_r e_r$ we set

$$\begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} = a_1 e_1 + \ldots a_r e_r = g$$

where $a_1, \ldots, a_r \in [0, n-1]$. For $i \in [1, r]$ we call $a_i$ the *$i$-th coordinate of $g$* and $a_1 + \ldots + a_r \in \mathbb{N}_0$ the *weight of $g$*.

**Lemma 3.3.** *Let $G = C_n^2$ with $n \geq 3$ odd,*

$$V_2 = \binom{0}{0}^{n-1} S \quad \text{with} \quad S = \binom{0}{2}^{n-1} \binom{2}{0}^{n-1} \binom{2}{2}^{n-1}$$

*and*

$$W_2 = \binom{0}{1}^{n-1} \binom{1}{0}^{n-1} \binom{1}{2}^{n-1} \binom{2}{1}^{n-1}.$$

*Then neither $V_2$ nor $W_2$ has a zero-sum subsequence of length $n$.*

*Proof.* Let $f\colon G \to G$ be defined by

$$\binom{a}{b} \mapsto \begin{pmatrix} \frac{n+1}{2} & \frac{n+1}{2} \\ \frac{n-1}{2} & \frac{n+1}{2} \end{pmatrix} \binom{a}{b} + \binom{0}{1}.$$

Then it is easy to check that $f(V_2) = W_2$. By Proposition 3.1.1, $S$ has no short zero-sum subsequence. Thus Lemma 2.2 implies that $V_2$ and $f(V_2)$ have no zero-sum subsequence of length $n$. □

**Lemma 3.4.** *Let $G = C_n^3$ with $n \geq 3$ odd,*

$$V_3 = \tilde{V}_3^{n-1} \quad \text{with} \quad \tilde{V}_3 = \binom{1}{0}{0} \binom{1}{0}{2} \binom{1}{2}{0} \binom{1}{2}{2} \binom{2}{0}{1} \binom{2}{1}{0} \binom{2}{1}{2} \binom{2}{2}{1} \binom{3}{1}{1}$$

*and*

$$W_3 = \tilde{W}_3^{n-1} \quad \text{with} \quad \tilde{W}_3 = \binom{2}{0}{0} \binom{2}{0}{2} \binom{2}{2}{0} \binom{2}{2}{2} \binom{1}{0}{1} \binom{1}{1}{0} \binom{1}{1}{2} \binom{1}{2}{1} \binom{0}{1}{1}.$$

*Then neither $V_3$ nor $W_3$ has a zero-sum subsequence of length $n$. In particular, we have $\eta(C_n^3) \geq 8n - 7$ and $\mathsf{s}(C_n^3) \geq 9n - 8$.*

*Proof.* Let $f\colon G \to G$ be defined by

$$\binom{a}{b}{c} \mapsto \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \binom{a}{b}{c} + \binom{3}{0}{0}.$$

Then it is easy to verify that $f(V_3) = W_3$. Thus by Lemma 2.2.1 and by Lemma 2.3.2 it suffices to prove that $V_3$ has no zero-sum subsequence of length $n$. Assume to the contrary that there is a zero-sum subsequence $V_3'$ of $V_3$ of length $n$.

We first suppose $V_3'$ contains only those elements of $V_3$ that have first coordinate 1 or 2. Then the sum of the first coordinates of the elements of $V_3'$ is $n$ or $2n$. This is only possible if all the elements of $V_3'$ have the same entry in the first coordinate. If all elements of $V_3'$ have first coordinate 1, then the sequence formed by the remaining two coordinates is a zero-sum subsequence of $V_2$ of length $n$, a contradiction to Lemma 3.3. Similarly, if all elements of $V_3'$ have first coordinate 2, then the sequence formed by the remaining two coordinates is a zero-sum subsequence of $W_2$ of length $n$, a contradiction to Lemma 3.3.

Thus $V_3'$ must contain the element $g = \begin{pmatrix}3\\1\\1\end{pmatrix}$. Since the second coordinate of $g$ equals 1, the sum of the second coordinates of the elements of $V_3'$ must be $n$. The same is true for the third coordinate. Since the first coordinate of $g$ equals 3, the sum of the first coordinates of the elements of $V_3'$ must be $2n$. Thus the sum of all coordinates of the $n$ elements of $V_3'$ equals $n+n+2n$ which is even. On the other hand, since all elements of $V_3$ have odd weight, this is the sum of an odd number of odd weights whence it should be odd, a contradiction. □

*Proof of Theorem 1.1.* Let $G = C_n^4$ with $n \ge 3$ odd. We set

$$T(n) = T = \begin{pmatrix}1\\1\\0\\0\end{pmatrix}\begin{pmatrix}1\\1\\0\\2\end{pmatrix}\begin{pmatrix}1\\1\\2\\0\end{pmatrix}\begin{pmatrix}1\\1\\2\\2\end{pmatrix}\begin{pmatrix}1\\2\\0\\1\end{pmatrix}\begin{pmatrix}1\\2\\1\\0\end{pmatrix}\begin{pmatrix}1\\2\\1\\2\end{pmatrix}\begin{pmatrix}1\\2\\2\\1\end{pmatrix}\begin{pmatrix}1\\3\\1\\1\end{pmatrix}$$
$$\begin{pmatrix}2\\2\\0\\0\end{pmatrix}\begin{pmatrix}2\\2\\0\\2\end{pmatrix}\begin{pmatrix}2\\2\\2\\0\end{pmatrix}\begin{pmatrix}2\\2\\2\\2\end{pmatrix}\begin{pmatrix}2\\1\\0\\1\end{pmatrix}\begin{pmatrix}2\\1\\1\\0\end{pmatrix}\begin{pmatrix}2\\1\\1\\2\end{pmatrix}\begin{pmatrix}2\\1\\2\\1\end{pmatrix}\begin{pmatrix}2\\0\\1\\1\end{pmatrix}\begin{pmatrix}0\\2\\1\\1\end{pmatrix}\begin{pmatrix}3\\1\\1\\1\end{pmatrix}$$

and assert that $V_4 = T^{n-1}$ has no zero-sum subsequence of length $n$. Then $\mathsf{s}(G) \ge |S| + 1 = 20n - 19$, and Lemma 2.3.2 implies that $\eta(G) \ge 19n - 18$. Assume to the contrary that there is a zero-sum subsequence $V_4'$ of $V_4$ of length $n$. We consider the elements

$$g = \begin{pmatrix}0\\2\\1\\1\end{pmatrix}, \quad h = \begin{pmatrix}3\\1\\1\\1\end{pmatrix}, \quad g' = \begin{pmatrix}2\\0\\1\\1\end{pmatrix} \quad \text{and} \quad h' = \begin{pmatrix}1\\3\\1\\1\end{pmatrix}.$$

We first suppose that $\mathsf{v}_g(V_4') + \mathsf{v}_h(V_4') = 0$ whence $V_4'$ contains only those elements of $V_4$ that have first coordinate 1 or 2. Then the sum of the first coordinates of the elements of $V_4'$ is $n$ or $2n$. This is only possible if all the elements of $V_4'$ have the same entry in the first coordinate. If all elements of $V_4'$ have first coordinate 1, then the sequence formed by the remaining three coordinates is a zero-sum subsequence of $V_3$ of length $n$, a contradiction to Lemma 3.4. Similarly, if all elements of $V_4'$ have first coordinate 2, then the sequence formed by the remaining three coordinates is a zero-sum subsequence of $W_3$ of length $n$, a contradiction to Lemma 3.4.

Thus it follows that $\mathsf{v}_g(V_4') + \mathsf{v}_h(V_4') > 0$. Since both $g$ and $h$ have a 1 in the third coordinate and all other elements of $V_4$ have a 0 a 1 or a 2 in the third coordinate, the sum of the third coordinates of the elements of $V_4'$ must be $n$. The same is true for the fourth coordinate. The sum of the first coordinates of the elements of $V_4'$ can neither be 0 nor $3n$ whence it must be either $n$ or $2n$. The same is true for the second coordinate. We distinguish three cases.

CASE 1: The sum of the first coordinates and the sum of the second coordinates are both $n$.

Since for all elements of $V_4$ the sum of the first and the second coordinate is at least 2, $V_4'$ can only contain elements whose first two coordinates sum to exactly 2. This implies that $\mathsf{v}_g(V_4') = \mathsf{v}_{g'}(V_4')$. Any other elements of $V_4'$ have an even number in the third coordinate. Thus the sum of the third coordinates is even, contradicting $n$ is odd.

CASE 2 : The sum of the first coordinates and the sum of the second coordinates are both $2n$.

Since for all elements of $V_4$ the sum of the first and the second coordinate is at most 4, $V_4'$ can only contain elements whose first two coordinates sum to exactly 4. This implies that $\mathsf{v}_h(V_4') = \mathsf{v}_{h'}(V_4')$. Any other elements of $V_4'$ have an even number in the third coordinate. Thus the sum of the third coordinates is even, contradicting $n$ is odd.

CASE 3 : The sum of the first coordinates equals $n$ and the sum of the second coordinates equals $2n$, or conversely.

Then the sum of all coordinates of the $n$ elements of $V_4'$ equals $n+n+n+2n = 5n$, which is odd. On the other hand, since all elements of $V_4$ have even weight, the sum of all coordinates of the $n$ elements of $V_4'$ should be even, a contradiction. □

Next we show how to lift the lower bounds for $\mathsf{s}(C_n^2), \mathsf{s}(C_n^3)$ and $\mathsf{s}(C_n^4)$ to lower bounds for $\mathsf{s}(C_n^r)$ with $r \ge 5$. Then we compare these bounds with upper bounds for $\mathsf{s}(C_n^r)$. Although these lifting results give the best lower bounds which are currently available, a lifting of a sharp bound for $\mathsf{s}(C_n^r)$ will in general not give sharp bounds for larger ranks.

**Proposition 3.5.** *Let $G$ be a finite abelian group with $\exp(G) = n \ge 2$.*

1. *Let $G = G_1 \oplus G_2$ with subgroups $G_1, G_2 \subset G$ such that $\exp(G_1) = \exp(G_2) = n$. If for every $i \in \{1,2\}$ there is some $T_i = g_{i,1} \cdot \ldots \cdot g_{i,l_i} \in \mathcal{F}(G_i)$ such that $T_i^{n-1}$ has no zero-sum subsequence of length $n$, then the sequence $T^{n-1}$, where*

$$T = \prod_{\substack{\lambda \in [1,l_1] \\ \nu \in [1,l_2]}} \big(g_{1,\lambda} + g_{2,\nu}\big) \quad \in \mathcal{F}(G)\,,$$

*has no zero-sum subsequence of length $n$. In particular,*

$$\mathsf{s}(G) \ge |T|(n-1)+1 \quad \text{and} \quad \eta(G) \ge (|T|-1)(n-1)+1\,.$$

2. *Let $G = C_n^r$ with $r \ge 2$ and let $r = r_1 + \ldots + r_s$ be any partition of $r$ with $s, r_1, \ldots, r_s \in \mathbb{N}$. If for every $i \in [1,s]$ there exists some $T_i \in \mathcal{F}(C_n^{r_i})$ such that $T_i^{n-1}$ has no zero-sum subsequence of length $n$, then*

$$\mathsf{s}(G) \ge \Big(\prod_{i=1}^{s} |T_i|\Big)(n-1)+1 \quad \text{and} \quad \eta(G) \ge \Big(\prod_{i=1}^{s} |T_i| - 1\Big)(n-1)+1\,.$$

*Proof.* 1. Assume to the contrary that $T^{n-1}$ has a zero-sum subsequence $T'$ of length $n$, say

$$T' = \prod_{j=1}^{n} \big(g_{1,\lambda_j} + g_{2,\nu_j}\big) \quad \text{where} \quad \lambda_1, \ldots, \lambda_n \in [1,l_1] \quad \text{and} \quad \nu_1, \ldots, \nu_n \in [1,l_2]\,.$$

Then the sequences

$$T_1' = \prod_{j=1}^{n} g_{1,\lambda_j} \quad \text{and} \quad T_2' = \prod_{j=1}^{n} g_{2,\nu_j}$$

have sum zero. Thus for every $i \in \{1,2\}$, the sequence $T_i'$ is not a subsequence of $T_i^{n-1}$ whence $\lambda_1 = \ldots = \lambda_n$, $\nu_1 = \ldots = \nu_n$ and

$$T' = \big(g_{1,\lambda_1} + g_{2,\nu_1}\big)^n\,,$$

a contradiction to the assumption that $T'$ is a subsequence of $T^{n-1}$.

Now the lower bound for $\mathsf{s}(G)$ follows by the very definition, and the lower bound for $\eta(G)$ follows from Lemma 2.3.2.

2. This follows from 1. by induction on $s$. □

**Corollary 3.6.** *Let $n \ge 3$ be an odd integer and $r \in \mathbb{N}$.*

1. *For $r \in [5, 12]$ we have $\mathsf{s}(C_n^r) \ge c_r(n-1)+1$ where $c_5 = 40, c_6 = 81, c_7 = 180, c_8 = 400, c_9 = 800, c_{10} = 1620, c_{11} = 3600, c_{12} = 8000$.*
2. *If $r = 4s + d$ with $s \in \mathbb{N}_0$ and $d \in [1, 4]$ and if $\mathsf{s}(C_n^d) \ge c_d(n-1)+1$ with $c_1, c_2, c_3, c_4 \in \mathbb{N}$, then $\mathsf{s}(C_n^r) \ge 20^s c_d(n-1)+1$.*

*Proof.* Let $d \in [1, 4]$. We assert that there is some sequence $T \in \mathcal{F}(C_n^d)$ such that $T^{n-1}$ has no zero-sum subsequence of length $n$ and $|T| = c_d$ with $c_1 = 2$, $c_2 = 4$, $c_3 = 9$ and $c_4 = 20$. For $d = 1$ the sequence $T = 0g$ has this property for every $g \in C_n$ with $\mathrm{ord}(g) = n$. For $d = 2$ this follows from Proposition 3.1.2 with $G = H = C_n$. For $d = 3$ this follows by Lemma 3.4 and for $d = 4$ this follows by Theorem 1.1. Now 1. and 2. follow from Proposition 3.5.2 (for 1. use the partitions $5 = 1+4, 6 = 3+3, 7 = 4+3, 8 = 4+4, 9 = 1+4+4, 10 = 3+3+4, 11 = 3+4+4, 12 = 4+4+4$). □

**Remarks 3.7.** 1. N. Alon and M. Dubiner proved the following upper bounds for $\mathsf{s}(C_n^r)$: For every $r \in \mathbb{N}$ and every prime $p$ one has $\mathsf{s}(C_p^r) \le c_r p$ where $c_r$ is recursively defined as follows: $c_1 = 2$ and $c_r = 256r(\log_2 r + 5)c_{r-1} + (r+1)$ for $r \ge 2$ (note that there is a misprint in the formula (6) in [2, page 306]; since in the meantime it is known that $\mathsf{s}(C_p^2) \le 4p$, one can also start the recursion with $c_2 = 4$). Furthermore, there exists an absolute constant $M > 0$ such that $\mathsf{s}(C_n^r) \le (Mr \log_2 r)^r n$ for all $r, n \in \mathbb{N}$ (see [2, Theorem 1.1]).

2. Using some refinements S. Kubertin gave the following upper bounds: For sufficiently large $p$ and $n$ we have $\mathsf{s}(C_p^r) \le c_r p$ and $\mathsf{s}(C_n^r) \le 2c_r n$ with $c_1 = 2$, $c_2 = 4$ and $c_r = 79.3224 \log(4.2637(1.4715r)^r)c_{r-1} + \frac{r+3}{2}$ (see [44, Satz 5.2]).

3. Upper and lower bounds for $\mathsf{s}(C_3^r)$ (equivalently, bounds for the maximal size of affine caps) are discussed in detail in Section 5.

## 4. Upper bounds and Consequences

We first deal with Theorem 1.2. Note that the results of N. Alon, M. Dubiner and S. Kubertin (discussed in Remarks 3.7) provide the starting values $c_1, \ldots, c_r$ mentioned in the assumption of Theorem 1.2. Although the proof of this theorem is straightforward, it provides the first reasonable upper bound for $\mathsf{s}(G)$ in case where $G$ has not the form $C_n^r$ (see Corollary 4.6). We start with the following lemma which generalizes [34, Hilfssatz 2] (see also [12]).

**Lemma 4.1.** *Let $G$ be a finite abelian group, $H \subset G$ a subgroup and $S \in \mathcal{F}(G)$ a sequence of length $|S| \ge (\mathsf{s}(H) - 1)\exp(G/H) + \mathsf{s}(G/H)$. Then $S$ has a zero-sum subsequence of length $\exp(H)\exp(G/H)$. In particular, if $\exp(G) = \exp(H)\exp(G/H)$, then*

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

*Proof.* This follows from [32, Proposition 5.7.11]. □

*Proof of Theorem 1.2.* We proceed by induction on $\exp(G)$. If $\exp(G) = p \in \mathbb{P}$, then $G = C_p^r$ and the assertion holds by assumption.

Let $p \in \mathbb{P}$ with $p \mid n_1$, $p < n_r$ and let $m_i = p^{-1}n_i$ for $i \in [1, r]$. We consider the groups

$$pG \cong C_{m_1} \oplus \ldots \oplus C_{m_r} \qquad \text{and} \qquad G/pG \cong C_p^r \,.$$

Note that we may have $m_1 = 1$, but in any case the induction hypothesis implies that

$$\mathsf{s}(pG) \le \sum_{i=1}^{r} (c_{r+1-i} - c_{r-i})m_i \ - c_r + 1 \,.$$

By Lemma 4.1 (with $H = pG$) we infer that

$$\begin{aligned} \mathsf{s}(G) &\le (\mathsf{s}(H) - 1)\exp(G/H) + \mathsf{s}(G/H) \\ &\le \Big(\sum_{i=1}^{r} (c_{r+1-i} - c_{r-i})m_i \ - c_r\Big)p + c_r(p-1) + 1 \\ &\le \sum_{i=1}^{r} (c_{r+1-i} - c_{r-i})n_i \ - c_r + 1 \,. \end{aligned}$$

□

For the proof of Theorem 1.3 we need the following two well-known lemmas. For convenience we provide the short proof of the second one.

**Lemma 4.2.** *Let $G$ be a finite abelian group, $k, n \in \mathbb{N}$, $\mathsf{D}(G \oplus C_n) \le 3n - 1$ and $S \in \mathcal{F}(G)$ a zero-sum sequence of length $|S| = (2k-1)n$. Then $S$ has a zero-sum subsequence of length $n$.*

*Proof.* This follows from [32, Proposition 5.7.7.3]. □

We introduce some more notation. Let $R$ be a commutative ring and $l \in \mathbb{N}$. We set $R[\boldsymbol{X}] = R[X_1, \ldots, X_l]$, and if

$$f = \sum_{\boldsymbol{m}=(m_1,\ldots,m_l)\in\mathbb{N}_0^l} a_{\boldsymbol{m}} X_1^{m_1} \cdot \ldots \cdot X_l^{m_l} \ \in R[\boldsymbol{X}]$$

is a non-zero polynomial, then we denote by

$$\deg(f) = \max\{m_1 + \ldots + m_l \mid \boldsymbol{m} \in \mathbb{N}_0^l \text{ with } a_{\boldsymbol{m}} \ne 0\} \in \mathbb{N}_0$$

the total degree of $f$.

**Lemma 4.3.** *Let $R$ be a commutative ring, $l \in \mathbb{N}$, $M = \langle \prod_{i\in I} X_i \mid I \subset [1,l]\rangle_R \subset R[\boldsymbol{X}]$ the submodule generated by the multi-linear monomials, $C = \{0_R, 1_R\}^l \subset R^l$ the cube in $R^l$ and $R^C$ the set of all maps $\varphi\colon C \to R$. Then the map*

$$\theta\colon M \to R^C, \quad \text{defined by} \quad f \ \mapsto \ \theta(f)\colon \begin{cases} C & \longrightarrow R \\ \boldsymbol{c} & \longmapsto f(\boldsymbol{c}) \end{cases}$$

*is an $R$-module isomorphism.*

*Proof.* Clearly, $M$ is a free $R$-module of rank $2^l$ and $R^C$ is a free $R$-module of rank $2^l$ having the set of all characteristic functions as an $R$-basis. If $\boldsymbol{c} = (c_1, \ldots, c_l) \in C$, $\chi_{\boldsymbol{c}} \in R^C$ the characteristic function of $\boldsymbol{c}$ and

$$f = \prod_{\substack{j \in [1,l] \\ c_j = 1}} X_j \prod_{\substack{j \in [1,l] \\ c_j = 0}} (1 - X_j) \in M \,,$$

then $\theta(f) = \chi_{\boldsymbol{c}}$ whence $\theta$ is an isomorphism. □

*Proof of Theorem 1.3.* 1. The lower bound follows by Lemma 3.2 and the upper bound by [32, Proposition 5.7.7.2]).

2. Since $\mathsf D(G \oplus C_n) = \big(\mathsf D(H) - 1\big) + \mathsf D(C_n \oplus C_n) = \big(\mathsf D(H) - 1\big) + 2n - 1$, the lower bound follows by Lemma 3.2, and it remains to prove the upper bound.

Let $p \in \mathbbm P$ be an odd prime, $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ a $p$-group, where $r = \mathsf r(G)$ and $1 < n_1 \mid \ldots \mid n_r$, and let $(e_1, \ldots, e_r)$ be a basis of $G$ with $\mathrm{ord}(e_i) = n_i$ for every $i \in [1, r]$. Then

$$\mathsf D(G) = 1 + \sum_{i=1}^r (n_i - 1) \quad \text{and} \quad \mathsf D(G \oplus C_n) = n + \sum_{i=1}^r (n_i - 1) \,.$$

Assume to the contrary that there exists a sequence $S = g_1 \cdot \ldots \cdot g_l \in \mathcal F(G)$ of length $|S| = l = \mathsf D(G \oplus C_n) + n$, which has no zero-sum subsequence of length $n$. Since $\mathsf D(G) \le 2n - 1$ by assumption, Lemma 4.2 implies that $S$ has no zero-sum subsequence of length $3n$. For every $i \in [1, l]$ we set

$$g_i = a_{i,1} e_1 + \ldots + a_{i,r} e_r \quad \text{with} \quad a_{i,\rho} \in [0, n_\rho - 1] \quad \text{for all} \quad \rho \in [1, r] \,.$$

We define the polynomial

$$P = \left( \binom{\sum_{i=1}^l X_i}{n} - 2 \right) Q \prod_{\rho=1}^r R_\rho \in \mathbb Q[\boldsymbol X]$$

where, for all $\rho \in [1, r]$,

$$R_\rho = \binom{\sum_{i=1}^l a_{i,\rho} X_i - 1}{n_\rho - 1} \in \mathbb Q[\boldsymbol X] \quad \text{and} \quad Q = \binom{\sum_{i=1}^l X_i - 1}{n - 1} \in \mathbb Q[\boldsymbol X] \,.$$

We set $C = \{0, 1\}^l \subset \mathbb Q^l$ and start with the following assertion.

*Assertion*: $P(C) \subset \mathbb Z$, $P(\boldsymbol 0) \not\equiv 0 \mod p$ and $P(\boldsymbol c) \equiv 0 \mod p$ for all $\boldsymbol c \in C \setminus \{\boldsymbol 0\}$.

*Proof of the Assertion*: Clearly, $P(\boldsymbol 0) \in \{-2, 2\}$ whence $P(\boldsymbol 0) \not\equiv 0 \mod p$ because $p$ is odd. Let $\boldsymbol 0 \ne \boldsymbol c = (c_1, \ldots, c_l) \in \{0, 1\}^l \subset \mathbb Q^l$. We have to show that $P(\boldsymbol c) \equiv 0 \mod p$.

We need the following two facts on binomial coefficients. Let $k, m \in \mathbb N$.

**F1.** If $p^k \nmid m$, then $\binom{m-1}{p^k - 1} \equiv 0 \mod p$.

**F2.** $\binom{mn}{n} \equiv m \mod p$.

We consider the sequence

$$S_{\boldsymbol c} = \prod_{i=1}^l g_i^{c_i} \in \mathcal F(G) \,.$$

Clearly, $S_{\boldsymbol c}$ is a subsequence of $S$ of length $|\boldsymbol c| = c_1 + \ldots + c_l \le l$. We distinguish two cases.

CASE 1: $S_{\boldsymbol{c}}$ is not a zero-sum sequence.
Then there exists some $\rho \in [1, r]$ such that

$$\sum_{\substack{i=1\\ c_i=1}}^{l} a_{i,\rho} \not\equiv 0 \mod n_\rho \,.$$

Then **F1** implies that $R_\rho(\boldsymbol{c}) \equiv 0 \mod p$ whence $P(\boldsymbol{c}) \equiv 0 \mod p$.

CASE 2: $S_{\boldsymbol{c}}$ is a zero-sum sequence.
If $|S_{\boldsymbol{c}}|$ is not divisible by $n$, then **F1** implies that $Q(\boldsymbol{c}) \equiv 0 \mod p$ whence $P(\boldsymbol{c}) \equiv 0 \mod p$. Suppose that $|S_{\boldsymbol{c}}|$ is divisible by $n$. Then by assumption we have $|S_{\boldsymbol{c}}| = 2n$ whence **F2** and the first factor of $P$ imply that $P(\boldsymbol{c}) \equiv 0 \mod p$.
Thus the proof of the Assertion is complete.

Now we use Lemma 4.3 with $R = \mathbb{Q}$ and with $\theta$ and $M$ as defined there.
Let $P_0 \in \mathbb{Q}[\boldsymbol{X}]$ be the polynomial arising from $P$ after replacing the powers $X_i^k$ by $X_i$ for all $i \in [1, l]$ and all $k \in \mathbb{N}$. Then $P_0 \in M$, $\deg(P_0) \le \deg(P)$ and $P(\boldsymbol{c}) = P_0(\boldsymbol{c})$ for all $\boldsymbol{c} \in C$.
For every $\boldsymbol{c} = (c_1, \ldots, c_l) \in C$ we define

$$\chi_{\boldsymbol{c}} = \prod_{\substack{i=1\\ c_i=1}}^{l} X_i \prod_{\substack{i=1\\ c_i=0}}^{l} (1 - X_i) \in M \subset \mathbb{Q}[\boldsymbol{X}]$$

and

$$\widetilde{P_0} = \sum_{\boldsymbol{c} \in C} P_0(\boldsymbol{c}) \chi_{\boldsymbol{c}} \in M \subset \mathbb{Q}[\boldsymbol{X}] \,.$$

Then $\theta(\chi_{\boldsymbol{c}})\colon C \to \mathbb{Q}$ is the characteristic function of $\boldsymbol{c}$ and we have $\theta(\widetilde{P_0})(\boldsymbol{c}) = \theta(P_0)(\boldsymbol{c})$ for all $\boldsymbol{c} \in C$. Therefore, by Lemma 4.3 we get $\widetilde{P_0} = P_0$. The Assertion implies that the coefficient of $\prod_{i=1}^{l} X_i$ in $\widetilde{P_0}$ and the coefficient of $\prod_{i=1}^{l} X_i$ in $P_0(\boldsymbol{0})\chi_{\boldsymbol{0}}$ are both integers which are congruent modulo $p$ but not divisible by $p$. In particular, the coefficient of $\prod_{i=1}^{l} X_i$ in $\widetilde{P_0}$ is non-zero whence $\deg(\widetilde{P_0}) = l$, and we get

$$\begin{aligned} l = \deg(\widetilde{P_0}) &= \deg(P_0) \le \deg(P) \\ &\le n + \deg(Q) + \sum_{\rho=1}^{r} \deg(R_\rho) \le 2n - 1 + \sum_{\rho=1}^{r} (n_\rho - 1) \\ &= \mathsf{D}(G \oplus C_n) + n - 1 < l \,, \end{aligned}$$

a contradiction. □

We end this section with a series of corollaries. Among others they provide some special types of groups for which the lower bounds derived in Section 3 and the upper bounds of this section give the precise values of $\eta(G)$ and $\mathsf{s}(G)$. The first corollary generalizes [34, Satz 1].

**Corollary 4.4.** *Let $G = C_{2^{k_1}} \oplus C_{2^k}^{r-1}$ where $k, r \in \mathbb{N}$, $r \ge 2$ and $k_1 \in [1, k]$. Then*

$$\eta(G) + 2^k - 1 = \mathsf{s}(G) = 2^{r-1}(2^{k_1} + 2^k - 2) + 1 \,.$$

*Proof.* For every $i \in [1, r]$ we have $\mathsf{s}(C_2^i) = 2^i + 1 = c_i(2-1) + 1$ with $c_i = 2^i$ (this can be seen directly from the definition, or see [32, Corollary 5.7.6]). Thus Theorem 1.2 implies that

$$\begin{aligned}\mathsf{s}(G) &\le (2^r - 2^{r-1})2^{k_1} + \sum_{i=2}^{r-1}(2^{r+1-i} - 2^{r-i})2^k + 2 \cdot 2^k - 2^r + 1 \\ &= 2^{r-1}2^{k_1} + 2^k 2^{r-1} - 2^r + 1 \\ &= 2^{r-1}(2^{k_1} + 2^k - 2) + 1\,.\end{aligned}$$

On the other hand, Proposition 3.1.3 (with $G = C_{2^{k_1}}$ and $C_n^k = C_{2^k}^{r-1}$) implies that

$$1 + 2^{r-1}(2^k - 1 + 2^{k_1} - 1) \le \eta(G) + 2^k - 1\,,$$

whence the assertion follows by Lemma 2.3.1. □

**Corollary 4.5.** *Let $P \subset \mathbb{P}$ be a non-empty set of odd primes and let $n \in \mathbb{N}$ be a product of prime powers with primes from $P$.*

1. *If $\mathsf{s}(C_p^3) = 9p - 8$ for all $p \in P$, then $8n - 7 = \eta(C_n^3) = \mathsf{s}(C_n^3) - n + 1$.*
2. *If $\mathsf{s}(C_p^4) = 20p - 19$ for all $p \in P$, then $19n - 18 = \eta(C_n^4) = \mathsf{s}(C_n^4) - n + 1$.*
3. *Let $r, c_r \in \mathbb{N}$ and let $m$ be a power of 2. If $\mathsf{s}(C_p^r) \le c_r(p-1) + 1$ for all $p \in P$, then $\mathsf{s}(C_{mn}^r) \le 2^r(m-1)n + c_r(n-1) + 1$.*

*Proof.* 1. By Lemma 3.4 and Lemma 2.3.1 we have

$$8n - 7 \le \eta(C_n^3) \le \mathsf{s}(C_n^3) - n + 1\,.$$

On the other hand, Theorem 1.2 (with $r = 3$ and $c_r = 9$) implies that $\mathsf{s}(C_n^3) \le 9n - 8$.

2. By Theorem 1.1 and Lemma 2.3.1 we have

$$19n - 18 \le \eta(C_n^4) \le \mathsf{s}(C_n^4) - n + 1\,.$$

On the other hand, Theorem 1.2 (with $r = 4$ and $c_r = 20$) implies that $\mathsf{s}(C_n^4) \le 20n - 19$.

3. We set $G = C_{mn}^r$ and $H = nG \cong C_m^r$ whence $G/H \cong C_n^r$. Since $\mathsf{s}(C_p) \le \mathsf{s}(C_p^2) \le \ldots \le \mathsf{s}(C_p^r) \le c_r(p-1) + 1$, Theorem 1.2 implies that $\mathsf{s}(G/H) \le c_r(n-1) + 1$, and Corollary 4.4 implies that $\mathsf{s}(H) = 2^r(m-1) + 1$. Using Lemma 4.1 we infer that

$$\begin{aligned}\mathsf{s}(G) &\le (\mathsf{s}(H) - 1)\exp(G/H) + \mathsf{s}(G/H) \\ &= 2^r(m-1)n + c_r(n-1) + 1\,.\end{aligned}$$

□

**Corollary 4.6.** *Let $G = C_{n_1} \oplus C_{n_2} \oplus C_{n_3}$ where $1 < n_1 \mid n_2 \mid n_3$ and let $P \subset \mathbb{P}$ denote the set of primes dividing $n_3$.*

1. *If $\mathsf{s}(C_p^3) \le 9p - 8$ for all $p \in P$, then $\mathsf{s}(G) \le 5n_1 + 2n_2 + 2n_3 - 8$. If $n_2 = n_3$, then $4n_1 + 4n_3 - 7 \le \mathsf{s}(G)$.*
2. *If $G$ is a 2-group, then $\mathsf{s}(G) \le 4n_1 + 2n_2 + 2n_3 - 7$, and equality holds if $n_2 = n_3$.*

*Proof.* For every prime $p$ we have $\mathsf{s}(C_p) = 2p-1$ and $\mathsf{s}(C_p^2) = 4p-3$ by Theorem **A**. Corollary 4.4 shows that $\mathsf{s}(C_2^3) = 8(2-1)+1$. Thus Theorem 1.2 implies the upper bounds. The lower bound in 1. follows from Proposition 3.1.3 (with $k=2$ and $n=n_3$). If $G$ is a 2-group and $n_2 = n_3$, then Corollary 4.4 implies equality in 2. □

**Remarks 4.7.** 1. For $r \in \{3,4,5\}$ the precise values of $\mathsf{s}(C_3^r)$ and $\mathsf{g}(C_3^r)$ (see the discussion after Lemma 2.3) were found (independently) by many authors (see the historical remarks after Lemma 5.2). We have $\mathsf{s}(C_3^3) = 19$, $\mathsf{s}(C_3^4) = 41$ and $\mathsf{s}(C_3^5) = 91$ whence $P = \{3\}$ satisfies both assumptions in Corollary 4.5, and $P = \{2,3\}$ satisfies the assumption in Corollary 4.6.1. Note that the sequence $(2,4,9,20,45) = (\mathsf{g}(C_3)-1, \ldots, \mathsf{g}(C_3^5)-1)$ has number $A090245$ in the On-Line Encyclopedia of Integer Sequences [60].

2. Applying Corollary 4.5.3 (with $P = \{3\}, r = 3, m = 2, c_3 = 9$) and Proposition 3.1 we obtain $41 \le \mathsf{s}(C_6^3) \le 43$. Thus if the group $C_6^3$ has Property **D**, then $\mathsf{s}(C_6^3) = 41$.

3. In general, neither the upper bound in Theorem 1.2 nor the upper bound in Corollary 4.6.1 are sharp. Indeed, for certain groups the upper bound from Theorem 1.3.2 is smaller than the upper bound from Corollary 4.6.1.

## 5. On a geometric aspect of the invariant $\mathsf{s}(G)$

It seems conceivable that all phenomena controlling the invariant $\mathsf{s}(C_n^r)$, for $n \ge 3$ odd and $r \in \mathbb{N}$, already occur in the special case where $n = 3$ (see the discussion after Lemma 5.4 and note that in all situations known so far, we have $\mathsf{s}(C_n^r) = \frac{\mathsf{s}(C_3^r)-1}{2}(n-1)+1$). But the problem to determine $\mathsf{s}(C_3^r)$ is equivalent to the (well investigated) problem of maximal caps in affine geometry (see Lemma 5.2 and the subsequent remarks). Even though this relationship may have been implicitly known, we hope that the discussion below gives directions for future research.

We start with some elementary facts from finite geometry. For a short introduction and collection of basic properties of finite geometries we refer to [48, Appendix B] and for more material to [39]. A recent survey on extremal problems in finite geometry is given in [40].

Let $q$ be a prime power and $r \in \mathbb{N}$. Recall that the $s$-dimensional subspaces of a projective space $PG(r,q)$ can be identified with the $(s+1)$-subspaces of the vector space $\mathbb{F}_q^{r+1}$. The incidence in the projective geometry is defined by the inclusion of the corresponding vector spaces. The 0-dimensional subspaces of a projective space $PG(r,q)$ are called the points, so $PG(r,q)$ has $q^r + q^{r-1} + \ldots + q + 1$ points. The 1-dimensional subspaces are called the lines and the $(r-1)$-dimensional subspaces are called the hyperplanes. The points of a set $S \subset PG(r,q)$ are called collinear if there is a line $L$ so that $S \subset L$.

One of the hyperplanes of $PG(r,q)$ can be thought of as the hyperplane at infinity. The complement of this hyperplane in $PG(r,q)$ is the affine geometry $AG(r,q)$ which consists of $q^r$ points. These points can be thought of as lying on $q$ parallel hyperplanes of $q^{r-1}$ points each. As the automorphism group of $PG(r,q)$, $PGL(r,q)$, operates transitively on the hyperplanes we can assume without loss of generality that the hyperplane at infinity is the hyperplane $x_{r+1} = 0$. So we can always choose this standard embedding of $AG(r,q)$, i.e. the points $(x:1)$ in $PG(r,q)$

So one can also think of $AG(r,q)$ as $\mathbb{F}_q^r$, as the point $(x:1)$ is uniquely determined by $x \in \mathbb{F}_q^r$. It is also convenient to call $x$ itself a point of $AG(r,q)$. The geometric structure of $AG(r,q)$ is

induced from $PG(r,q)$ by restriction. A line in projective space has $q+1$ points, a line in affine space has $q$ points. One of the classic objects of interest in finite geometry are caps.

**Definition 5.1.**

1. An *$m$-cap* $C \subset PG(r,q)$ is a set of $|C| = m$ points no three of which are collinear.
2. An $m$-cap in $PG(r,q)$ is called *maximal* if there exists no $m+1$-cap in $PG(r,q)$.
3. A cap $C \subset PG(r,q)$ is called *affine* if there is a hyperplane $H$ so that $C \cap H = \emptyset$.
4. An $m$-cap in $PG(r,q)$ is called *maximal affine* if there exists no affine $m+1$-cap in $PG(r,q)$.

**Lemma 5.2.** *Let $G = \mathbb{F}_3^r$ with $r \in \mathbb{N}$.*

1. *The map $f$, defined by $f(T) = \mathrm{supp}(T)$, is a bijection from the set*

$$\{T \in \mathcal{F}(G) \mid T \quad \text{is squarefree and has no zero-sum subsequence of length } 3\}$$

   *onto the set $\{C \subset G \mid C \quad \text{is a cap}\}$.*
2. $\mathsf{g}(G) - 1$ *is the maximal size of a cap in $AG(r,3)$.*
3. $\mathsf{s}(G) = 2\mathsf{g}(G) - 1$, *and every sequence $S \in \mathcal{F}(G)$ of length $|S| = \mathsf{s}(G) - 1$ which has no zero-sum subsequence of length 3 has the form $S = T^2$ where* $\mathrm{supp}(T)$ *is a maximal cap in $G$. Conversely, if $T \in \mathcal{F}(G)$ is squarefree and has no zero-sum subsequence of length 3, then $T^2$ has no zero-sum subsequence of length 3.*

*Proof.* We identify $G$ with the affine space $AG(r,3) \subset PG(r,3)$.

1. Three different points $(x:1), (y:1), (z:1) \in AG(r,3)$ are not on a line if and only if the vectors $(x,1), (y,1), (z,1) \in \mathbb{F}_3^{r+1}$ are linearly independent, i.e. if there is no nontrivial linear combination $\lambda x + \mu y + \nu z = 0$ with $\lambda + \mu + \nu = 0$. The only possible coefficients $\{\lambda, \mu, \nu\}$ are $\{1,1,1\}$, $\{2,2,2\}$ or permutations of $\{0,1,2\}$. The case $\{0,1,2\}$ is impossible as it would imply that two points are equal. An affine relation with respect to coefficients $\{2,2,2\}$ is equivalent to the relation with respect to $\{1,1,1\}$ by a scalar multiplication. So three different points are not on a line if and only if the corresponding sequence has no zero-sum of length three.

2. This follows from 1.

3. In [34, Hilfssatz 3] it is proved that $\mathsf{s}(G) = 2\mathsf{g}(G) - 1$. Therefore Lemma 2.3.3 implies that $G$ has Property **D** whence the first assertion follows from 1. Let $T \in \mathcal{F}(G)$ be a squarefree sequence without a zero-sum subsequence of length 3. Assume to the contrary that $T^2$ has a zero-sum subsequence $S'$ of length 3. Since $S'$ is not a subsequence of $T$, we have $S' = h^2 h'$ for some $h, h' \in G$. But then $2h + h' = 0$ implies that $h = h'$, a contradiction. □

Let us briefly discuss some further connections to related problems. As the lemma above already shows the same type of problem has been studied in various different parts of mathematics, such as number theory, combinatorics, and finite geometry.

1. A sequence $g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(\mathbb{F}_p^r)$ is called an arithmetic progression of length $l$ if there exist $a, b \in \mathbb{F}_p^r$ such that $g_i = a + ib$ for all $i \in [0, l-1]$. The problem of studying sets without arithmetic progressions in $\mathbb{F}_p^r$ has been studied for example by B.J. Green [33] and V. Lev [47].

In analogy to Lemma 5.2 one can state:
The map $f$, defined by $f(T) = \mathrm{supp}(T)$, is a bijection from the set

$$\{T \in \mathcal{F}(G) \mid T \quad \text{is squarefree and has no zero-sum subsequence of length } 3\}$$

onto the set $\{C \subset G \mid C \quad \text{does not contain an arithmetic progression of length } 3\}$. Thus $\mathsf{g}(G) - 1$ is the maximal size of a set in $G$ without an arithmetic progression of length 3.

This follows from Lemma 5.2.1. by observing that three points in $\mathbb{F}_3^r$ define an arithmetic progression of length 3 if and only if they are collinear.

The problem of sets without progressions in $\mathbb{F}_3^r$ is closely connected to the famous Erdős-Turán problem on sets of integers without arithmetic progressions. Using harmonic analysis, K. Roth [58] was the first to show that the maximal cardinality $r_3(n)$ of sets without a progression of length 3 in $[1, n]$ is $r_3(n) = O\left(\frac{n}{\log\log n}\right)$. Further progress was due to D.R. Heath-Brown [35], E. Szemerédi [62], and J. Bourgain [8], leading to $r_3(n) = O\left(\frac{n(\log\log n)^{1/2}}{(\log n)^{1/2}}\right)$. As B.J. Green [33] shows all four proofs can be adapted to give an upper bound of $O\left(\frac{3^r}{r}\right)$ for the cardinality of maximal sets in $\mathbb{F}_3^r$ without an arithmetic progression of length 3. This bound was first proved by R. Meshulam [49], based on Roth's method. For precursors see [10] and [21], [22], for a generalization see [47]. For explicit bounds on $\mathsf{g}(C_3^r)$ see below.

2. B.L. Davis and D. Maclagan (see [13]) wrote an interesting article on the card game SET which carefully explains the connections between this card game and affine caps. In short, cards consists of several properties such as colour and symbol. A "SET" is a set of 3 cards where these properties are either the same (like 3 times the same colour) or all different (like all three different colours occur). This corresponds to arithmetic progression of length 3 or 3 collinear points. Since this card game is very popular, a growing number of manuscripts appears on the internet rediscovering results that are equivalent to the values of $\mathsf{g}(C_3^3) = 10$ or $\mathsf{g}(C_3^4) = 21$, here we only mention the computer programme by D. E. Knuth (see [43]).
3. The problem of finding lattice points with no 3 collinear has an interesting application to graph drawings. Given a finite simple graph $G$, a drawing of $G$ represents each vertex by an integer gridpoint in $\mathbb{Z}^3$, where the edges are drawn as the straight line segments between the adjacent vertices. Edges are not allowed to pass through other vertices. One is interested in drawings with minimal volume of the bounding box of the vertices. The connection to the problem of no 3 collinear points follows by the observation that a set $V \subset \mathbb{Z}^3$ of $n$ points induces a drawing of the complete graph $K_n$ if and only if no three points of $V$ are collinear. For more details see A. Pór and D.R. Wood [55]. Also, their open problem 3 on $vol(n, d, 1)$ is a question on dense $d$-dimensional point configurations without 3 points on a line, and their comment that this problem is trivial for $d \geq \log_2 n$ follows from the trivial cap consisting of the $2^d$ points with coordinates 0 and 1 only.

We now describe the connection to caps in some more detail and discuss explicit bounds on $\mathsf{g}(C_3^r)$.

The determination of the maximal size of caps in projective geometry $PG(r, q)$ or affine geometry $AG(r, q)$, as well as their complete characterization, appears to be a difficult problem. Only few exact results are known. We refer to [40, 5] for the known results and here only summarize some details we need for caps in $AG(r, 3)$.

Let $q$ be an odd prime power. In $PG(2,q)$ there are $(q+1)$-caps, the ovals, known to be maximal [7]. An oval avoids several hyperplanes, so the maximal size of a cap in $AG(2,3)$ is 4. In $PG(3,q)$ there is a unique maximal $(q^2+1)$-cap, the ovoid, see [7, 3, 52]. The ovoid contains an affine $q^2$-cap. As every $q^2$-cap in $PG(3,q)$ can be embedded in the unique $(q^2+1)$-cap (see [20]) and as the automorphism group of the ovoid is transitive, also the affine $q^2$-cap is projectively unique. In $PG(4,3)$ there exist exactly 9 types of maximal 20-caps, one of these is affine, see [53, 38].

The values, $\mathsf{s}(C_3^3) = 19$, $\mathsf{g}(C_3^3) = 10$, $\mathsf{s}(C_3^4) = 41$ and $\mathsf{g}(C_3^4) = 21$, were rediscovered several times. It appears they were first found by finite geometers. R.C. Bose [7] found the size of the maximal affine caps in dimension 3, and the uniqueness was proved by A. Barlotti, G. Panella [3, 52]. In $AG(4,3)$ the existence and the maximality of a cap of size 20 was proved by G. Pellegrino [53], and the uniqueness was proved by R. Hill [38]. The size of the unique maximal cap in $AG(5,3)$ is 45, as proved by Y. Edel, S. Ferret, I. Landjev, and L. Storme [16]. In $AG(6,3)$ a 112-cap can be constructed by applying the elementary doubling construction due to A.C. Mukhopadhyay [50] to the 56 points of the Hill cap in PG(5,3), see [36, 37]. The size of a cap in $AG(6,3)$ can be at most 114, see [6]. P. Frankl, R.L. Graham and V. Rödl [21] connected the problem of no 3 points in arithmetic progression in $\mathbb{F}_3^r$ to sunflowers and proved, based on a construction in $r = 18$, that there are affine caps in $AG(3,r)$ of size at least $2.179^r$, for sufficiently large $r$.

In the combinatorics community the problem of determining the invariants $\mathsf{s}(C_n^r)$ and $\mathsf{g}(C_n^r)$ was posed and popularized by H. Harborth and A. Kemnitz. H. Harborth verified that $\mathsf{s}(C_3^3) = 19$, and A. Kemnitz proved $\mathsf{s}(C_3^4) = 41$ (see [34], [41], [42] and also [9], [10], [63]).

For larger $r$ lower bounds for the size of an affine cap in $AG(r,3)$, i.e. bounds for $\mathsf{g}(C_3^r) - 1$, can be obtained from projective caps by choosing a hyperplane (which will be the hyperplane at infinity of the affine cap) and delete all points of the projective cap in this hyperplane.

The lower bounds for $r \le 12$ in the table below are obtained by choosing a hyperplane that contains the minimal number of points of the projective caps found at [14]. The bounds for $r = 62$ and $r = 480$ are constructed in [15]. The latter shows, that there are affine caps in $AG(3,r)$ of size at least $2.217389^r$, for sufficiently large $r$.

For the upper bounds we recursively use the following lemma, which is an adaption of [6, Theorem 2] (see also [49]) to our situation. The upper bounds in the table are obtained by starting with the maximal cap in $AG(5,3)$, that is with $\mathsf{g}(C_3^5) - 1 = 45$ [16].

**Lemma 5.3.** *If $r \ge 3$, then*

$$(\mathsf{g}(C_3^r) - 1) \le 3^r \frac{3(\mathsf{g}(C_3^{r-1}) - 1) + 1}{3(\mathsf{g}(C_3^{r-1}) - 1) + 3^r},$$

$$\begin{aligned}
236 &\le \mathsf{g}(C_3^7) - 1 \le 296, \\
476 &\le \mathsf{g}(C_3^8) - 1 \le 783, \\
1068 &\le \mathsf{g}(C_3^9) - 1 \le 2099, \\
2228 &\le \mathsf{g}(C_3^{10}) - 1 \le 5691, \\
5232 &\le \mathsf{g}(C_3^{11}) - 1 \le 15573, \\
10848 &\le \mathsf{g}(C_3^{12}) - 1 \le 42944, \\
2.57342 \cdot 10^{21} \sim 2^{41}7^9 29 &\le \mathsf{g}(C_3^{62}) - 1 \le 6.11654 \cdot 10^{27}, \\
1.0095 \cdot 10^{166} \sim 32^{80} + 8^5 \tbinom{10}{5} 112^{75} 12^5 &\le \mathsf{g}(C_3^{480}) - 1 \le 2.17081 \cdot 10^{226}.
\end{aligned}$$

The upper bound coming from Lemma 5.3 tends to $\frac{3^r}{r}$, as $r$ tends to infinity. Note that R. Meshulam [49] states his bound with an extra factor of 2.

**Lemma 5.4.** *For $r \in \{3,4,5\}$ the maximal affine cap in $AG(r,3)$ is unique up to affine transformation (that means, every maximal cap can be written as $MC+a$ where $C$ is a fixed example of the maximal cap, $M$ a nonsingular $r \times r-$Matrix over $\mathbb{F}_3$ and $a \in \mathbb{F}_3^r$).*

*Proof.* In the preceding discussion we have seen that the caps in question are projectively unique. These caps avoid only one hyperplane (e.g. easily verified by computer). As there is only one avoided hyperplane a projective homomorphism fixing the cap must also fix this hyperplane.

This hyperplane must be the "hyperplane at infinity" that defines the embedding of the affine geometry into the projective geometry. As we motivated in the introduction we can use the standard embedding of $AG(r,3)$ (that is, all points are of the form $(x:1)^t$ in $PG(r,3)$).

A projective homomorphism fixing the"hyperplane at infinity", $x_{r+1}=0$, must be equivalent to a multiplication with a matrix of the form

$$\begin{pmatrix} M & a \\ 0 & 1 \end{pmatrix}$$

with $M$ a nonsingular $r \times r-$Matrix over $\mathbb{F}_3$ and $a \in \mathbb{F}_3^r$, i.e. be an affine transformation. □

In the remainder of this section we discuss some geometric aspects of the sequence constructed in [17] and of the sequence given in Theorem 1.1 (we use the notations introduced before Lemma 3.3). If $n \geq 3$ is odd and

$$T = \binom{2}{1}\binom{0}{0}\binom{0}{1}\binom{0}{1}\binom{1}{0}\binom{1}{0}\binom{1}{1}\binom{1}{2}\binom{2}{2}\binom{0}{0},$$

then the sequence $T^{n-1} \in \mathcal{F}(C_n^3)$ has no zero-sum subsequence of length $n$. This was first proved in [17] for all odd $n \geq 3$. The case $n=3$ was studied in [34, Proof of Satz 4]. In that case, the underlying set $\mathrm{supp}(T)$ is a cap in $AG(3,3)$, and hence unique up to affine transformation (see Lemma 5.2.1, and Lemma 5.4). A computer based search produced the following squarefree sequences $T_1,\ldots,T_6$ with the following properties: in case $n=3$ all underlying sets are representations of the cap in $AG(3,3)$, and for all odd $n \geq 3$ the sequences $T_1^{n-1},\ldots,T_6^{n-1}$ have no zero-sum subsequence of length $n$.

$$T_1 = \binom{2}{0}\binom{1}{1}\binom{1}{1}\binom{2}{2}\binom{1}{0}\binom{2}{1}\binom{1}{0}\binom{2}{1}\binom{0}{0},$$

$$T_2 = \binom{2}{1}\binom{1}{0}\binom{1}{1}\binom{2}{1}\binom{1}{0}\binom{2}{0}\binom{1}{1}\binom{2}{2}\binom{0}{0},$$

$$T_3 = \binom{1}{1}\binom{0}{0}\binom{2}{1}\binom{2}{1}\binom{1}{0}\binom{1}{0}\binom{0}{1}\binom{2}{2}\binom{0}{0},$$

$$T_4 = \binom{1}{1}\binom{1}{0}\binom{0}{1}\binom{1}{1}\binom{1}{0}\binom{2}{0}\binom{0}{1}\binom{0}{2}\binom{0}{0},$$

$$T_5 = \binom{2}{0}\binom{0}{1}\binom{0}{1}\binom{0}{2}\binom{1}{0}\binom{1}{1}\binom{1}{0}\binom{1}{1}\binom{0}{0} \quad \text{and}$$

$$T_6 = \binom{2}{1}\binom{0}{0}\binom{1}{1}\binom{1}{1}\binom{2}{0}\binom{2}{0}\binom{0}{1}\binom{1}{2}\binom{0}{0}.$$

Of these seven examples the sequence $T$ is distinguished by being the only one with the canonical affine basis (containing $0, e_1, e_2, e_3$) and moreover is one of those sequences with a minimal sum of entries.

We now come back to the example in $C_n^4$. Consider the support

$$S(n) = \operatorname{supp}\big(T(n)\big) \subset (\mathbb{Z}/n\mathbb{Z})^4 \quad \text{where} \quad n \ge 3 \quad \text{is odd},$$

of the squarefree sequence given in the proof of Theorem 1.1.

By Lemma 5.2.1, $S(3)$ is a cap in $AG(4,3)$, and by Lemma 5.4, it is unique up to affine transformation. However, there are representations $\mathbb{T}$ of $S(3)$ such that the sequence $S = T^{n-1}$ (now considered as a sequence in $C_n^r$), with $\operatorname{supp}(T) = \mathbb{T}$, has a zero-sum subsequence of length $n$. For example, by [13] the set

$$\left\{ \binom{0}{0}\binom{0}{0}, \binom{2}{0}\binom{0}{0}, \binom{0}{2}\binom{0}{0}, \binom{2}{2}\binom{0}{0}, \binom{1}{0}\binom{2}{0}, \binom{0}{1}\binom{2}{0}, \binom{1}{2}\binom{2}{0}, \binom{2}{1}\binom{2}{0}, \binom{1}{1}\binom{1}{0}, \binom{1}{1}\binom{0}{1}, \right.$$
$$\left. \binom{0}{0}\binom{2}{2}, \binom{2}{0}\binom{2}{2}, \binom{0}{2}\binom{2}{2}, \binom{2}{2}\binom{2}{2}, \binom{1}{0}\binom{0}{2}, \binom{0}{1}\binom{0}{2}, \binom{1}{2}\binom{0}{2}, \binom{2}{1}\binom{0}{2}, \binom{1}{1}\binom{1}{2}, \binom{1}{1}\binom{2}{1} \right\}$$

is a representation of the cap $S(3)$. For every odd $n > 3$, the sequence $S$ consisting of $n-1$ copies of any of the above points has the following zero-sum subsequence $S'$ of length $n$ where

$$S' = \binom{1}{0}\binom{1}{1}\binom{1}{1}\binom{0}{1}\binom{2}{2}^{\frac{n-3}{2}}\binom{0}{0}^{\frac{n-5}{2}}.$$

Actually, using a computer we tried many representations of the cap $S(3)$, but we did not find any that have no zero sums of length $n$ modulo other odd integers $n$ and use the entries $0, 1, 2$ only. As the proof of Theorem 1.1 shows the example can be thought of as two twisted copies of caps in $AG(3,3)$ and two further points. The example we found may be one of the easiest ones, since it uses only the 4 entries $0, 1, 2, 3$, with only two 3's, and because of the symmetry discussed in the proof of Theorem 1.1, and below.

Finally we study the automorphism group of the set $S(n)$ (that is the group of all affine transformations $f\colon (\mathbb{Z}/n\mathbb{Z})^4 \to (\mathbb{Z}/n\mathbb{Z})^4$ with $f\big(S(n)\big) = S(n)$). It is hoped for that the study of the automorphism group helps to construct maximal caps in $AG(r,q)$ for $r > 4$.

The following automorphisms are easy to spot.

$$\begin{aligned} S(n) &\to S(n) \\ (a,b,c,d) &\mapsto (b,a,c,d) \\ (a,b,c,d) &\mapsto (a,b,d,c) \\ (a,b,c,d) &\mapsto (3,3,2,2) - (a,b,c,d) \end{aligned}$$

Combinations of these already generate up to 8 points for one given point $(a,b,c,d)$. A complete computer based search revealed that the full automorphism group of $S(5) \subset \mathbb{F}_5^4$ and of $S(7) \subset \mathbb{F}_7^4$ has 96 elements. The maps

$$\begin{aligned} g_1 : (a,b,c,d) &\mapsto (0,0,2,2) + (b,a,-c,-d) \\ g_2 : (a,b,c,d) &\mapsto (3,3,2,2) - (a,b,c,d) \\ g_3 : (a,b,c,d) &\mapsto (f,f,f,f+2) - (d,c,b,d+c+b), \\ &\qquad \text{with } f := (a+b+c+d)(n+1)/2 \\ g_4 : (a,b,c,d) &\mapsto (0,0,2,0) + (a,b,-d,c) \end{aligned}$$

fix the set $S(n)$, as can be seen by explicit verification. The map $g_1$ as well as $g_2$ is of order 2 and commutes with all other maps. The maps $g_3$ and $g_4$ are of order 3 and 4, respectively. The maps $g_3$ and $g_4$ generate a group of order 24 without a centre and with more than two elements of order 3. Thus $\langle g_3, g_4\rangle$ is a group which is isomorphic to the symmetric group $S_4$ (see [46, Lemma 4.3.4]). Therefore the automorphism group of $S(n)$ must contain the group $C_2 \oplus C_2 \oplus S_4$ as a subgroup. It is well known that in case $n = 3$ the full automorphism group has order 2880. For $n \in \{5,7\}$ a computer search shows that $G = C_2 \oplus C_2 \oplus S_4$ is the full automorphism group and we do not expect any further automorphisms for $n > 7$. Under the group action of $\langle g_1, g_2, g_3, g_4\rangle$ the set $S(n)$ is split into two orbits which are given in the following lemma.

**Lemma 5.5.** *Let $n \geq 3$ be odd.*

1. *The group $G(n) = \langle g_1, g_2, g_3, g_4\rangle$ is isomorphic to $C_2 \oplus C_2 \oplus S_4$. $G(n)$ is a subgroup of the automorphism group of $S(n)$, and for $n \in \{5,7\}$ it is the full automorphism group.*
2. *Under the group action of $G(n)$ the set $S(n)$ is split into two orbits of length* 12 *(the first* 12 *below) and* 8 *(the last* 8*) respectively .*

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 1 | 3 | 0 | 2 | | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 |
| 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 3 | 1 | 2 | 0 | | 2 | 2 | 2 | 2 | 1 | 1 | 1 | 1 |
| 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 1 | 1 | 1 | 1 | | 0 | 1 | 1 | 2 | 0 | 1 | 1 | 2 |
| 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 1 | 1 | 1 | 1 | | 1 | 0 | 2 | 1 | 1 | 0 | 2 | 1 |

*Proof.* 1. has been outlined above and 2. is checked by a direct computation. □

## References


[1] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size*, Combinatorics, Paul Erdős is Eighty, vol. 1, J. Bolyai Math. Soc., 1993, pp. 33 – 50.

[2] ———, *A lattice point problem and additive number theory*, Combinatorica **15** (1995), 301 – 309.

[3] A. Barlotti, *Un'estensione del teorema di Segre-Kustaanheimo*, Boll. Unione Mat. Ital., III **10** (1955), 498 – 506.
[4] A. Bialostocki and P. Dierker, *On the Erdős-Ginzburg-Ziv theorem and the Ramsey numbers for stars and matchings*, Discrete Math. **110** (1992), 1 – 8.
[5] J. Bierbrauer, *Large caps*, J. Geom. **76** (2003), 16 – 51.
[6] J. Bierbrauer and Y. Edel, *Bounds on affine caps*, J. Comb. Des. **10** (2002), 111 – 115.
[7] R.C. Bose, *Mathematical theory of symmetrical factorial design*, Sankhya **8** (1947), 107 – 166.
[8] J. Bourgain, *On triples in arithmetic progression*, Geom. Funct. Anal. **9** (1999), 968 – 984.
[9] J.L. Brenner, J.E. Cruthirds, L.E. Mattics, I.M. Isaacs, and F. Quinn, *Problem 6298*, Am. Math. Mon. **89** (1982), 279 – 280.
[10] T.C. Brown and J.P. Buhler, *A density version of a geometric Ramsey theorem*, J. Comb. Theory, Ser. A **32** (1982), 20 – 34.
[11] S.T. Chapman, M. Freeze, W. Gao, and W.W. Smith, *On Davenport's constant of finite abelian groups*, Far East J. Math. Sci. **5** (2002), 47 – 54.
[12] R. Chi, S. Ding, W. Gao, A. Geroldinger, and W.A. Schmid, *On zero-sum subsequences of restricted size IV*, Acta Math. Hung. **107** (2005), 337 – 344.
[13] B.L. Davis and D. Maclagan, *The card game SET*, Math. Intell. **25** (2003), 33 – 40.
[14] Y. Edel, *Caps, generators and further information*, http://www.mathi.uni-heidelberg.de/∼yves/Matrizen/CAPs/CAPMatIndex.html#Mat.
[15] ———, *Extensions of generalized product caps*, Des. Codes Cryptography **31** (2004), 5 – 14.
[16] Y. Edel, S. Ferret, I. Landjev, and L. Storme, *The classification of the largest caps in $AG(5,3)$*, J. Comb. Theory, Ser. A **99** (2002), 95 – 110.
[17] C. Elsholtz, *Lower bounds for multidimensional zero sums*, Combinatorica **24** (2004), 351 – 358.
[18] P. van Emde Boas, *A combinatorial problem on finite abelian groups II*, Reports ZW-1969-007, Math. Centre, Amsterdam, 1969.
[19] P. Erdős, A. Ginzburg, and A. Ziv, *Theorem in the additive number theory*, Bull. Research Council Israel **10** (1961), 41 – 43.
[20] G. Faina, S. Marcugini, A. Milani, and F. Pambianco, *The sizes $k$ of the complete $k$-caps in $PG(n,q)$, for small $q$ and $3 \leq n \leq 5$*, Ars Comb. **50** (1998), 235 – 243.
[21] P. Frankl, R.L. Graham, and V. Rödl, *On subsets of abelian groups with no 3-term arithmetic progression*, J. Comb. Theory, Ser. A **45** (1987), 157 – 161.
[22] H. Furstenberg and Y. Katznelson, *A density version of the Hales-Jewett theorem for $k = 3$*, Discrete Math. **75** (1989), 227 – 241.
[23] W. Gao, *On zero-sum subsequences of restricted size*, J. Number Theory **61** (1996), 97 – 102.
[24] ———, *An addition theorem for finite cyclic groups*, Discrete Math. **163** (1997), 257 – 265.
[25] ———, *On zero sum subsequences of restricted size II*, Discrete Math. **271** (2003), 51 – 59.
[26] W. Gao and A. Geroldinger, *On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$*, Integers **3** (2003), Paper A08, 45p.
[27] W. Gao and R. Thangadurai, *On zero-sum sequences of prescribed length*, Aequationes Math., to appear.
[28] ———, *On the structure of sequences with forbidden zero-sum subsequences*, Colloq. Math. **98** (2003), 213 – 222.
[29] ———, *A variant of Kemnitz conjecture*, J. Comb. Theory, Ser. A **107** (2004), 69 – 86.
[30] W. Gao and Y.X. Yang, *Note on a combinatorial constant*, J. Math. Res. and Expo. **17** (1997), 139 – 140.
[31] W. Gao and J. Zhou, *On short zero-sum subsequences*, Ars Comb. **74** (2005), 231 – 238.
[32] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 700 pages, 2006.
[33] B.J. Green, *Finite field models in additive combinatorics*, Surveys in Combinatorics 2005, London Math. Soc. Lecture Note Ser., vol. 327, Cambridge University Press, 2005, pp. 1 – 27.
[34] H. Harborth, *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math. **262** (1973), 356 – 360.
[35] D.R. Heath-Brown, *Integer sets containing no arithmetic progressions*, J. London Math. Soc. **35** (1987), 385 – 394.
[36] R. Hill, *On the largest size of a cap in $S_{5,3}$*, Atti Accad. Naz. Lincei Rend. **54** (1973), 378 – 384.
[37] ———, *Caps and codes*, Discrete Math. **22** (1978), 111 – 137.
[38] ———, *On Pellegrino's 20-caps in $S_{4,3}$*, Ann. Discrete Math. **18** (1983), 433 – 447.

[39] J.W.P. Hirschfeld, *Projective geometries over finite fields, 2nd ed.*, Oxford Mathematical Monographs, Clarendon Press, 1998.
[40] J.W.P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces: Update* 2001, Finite Geometries, Kluwer Academic Publishers, 2001, pp. 201 – 246.
[41] A. Kemnitz, *Extremalprobleme für Gitterpunkte*, Ph.D. thesis, Technische Universität Braunschweig, 1982.
[42] ———, *On a lattice point problem*, Ars Comb. **16-B** (1983), 151 – 160.
[43] D.E. Knuth, *Computerprogramme*, http://www-cs-faculty.stanford.edu/∼knuth/programs/setset-all.w.
[44] S. Kubertin, *Nullsummen in* $\mathbb{Z}_p^d$, Master's thesis, Technical University Clausthal, 2002.
[45] ———, *Zero-sums of length kq in* $\mathbb{Z}_q^d$, Acta Arith. **116** (2005), 145 – 152.
[46] H. Kurzweil and B. Stellmacher, *The Theory of Finite Groups. An Introduction*, Springer, 2004.
[47] V.F. Lev, *Progression-free sets in finite abelian groups*, J. Number Theory **104** (2004), 162 – 169.
[48] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.
[49] R. Meshulam, *On subsets of finite abelian groups with no* 3*-term arithmetic progressions*, J. Comb. Theory, Ser. A **71** (1995), 168 – 172.
[50] A.C. Mukhopadhyay, *Lower bounds on* $m_t(r, s)$, J. Comb. Theory, Ser. A **25** (1978), 1 – 13.
[51] M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.
[52] G. Panella, *Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito*, Boll. Unione Mat. Ital., III **10** (1955), 507 – 513.
[53] G. Pellegrino, *The maximal order of the spherical cap in* $S_{4,3}$, Matematiche **25** (1971), 149 – 157.
[54] B. Peterson and T. Yuster, *A generalization of an addition theorem for solvable groups*, Can. J. Math. **36** (1984), 529 – 536.
[55] A. Pór and D.R. Wood, *No-three-in-line-in-3D*, Proceedings of the 12th International Symposium on Graph Drawing, Lecture Notes in Computer Science, vol. 3383, Springer, 2005, pp. 395 – 402.
[56] C. Reiher, *On Kemnitz' conjecture concerning lattice points in the plane*, Ramanujan J. **13** (2007), 333 – 337.
[57] L. Rónyai, *On a conjecture of Kemnitz*, Combinatorica **20** (2000), 569 – 573.
[58] K.F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104 – 109.
[59] S. Savchev and F. Chen, *Kemnitz' conjecture revisited*, Discrete Math. **297** (2005), 196 – 201.
[60] N.J.A Sloane, *On-line Encyclopedia of Integer Sequences*, http://www.research.att.com/projects/OEIS?Anum=A090245.
[61] Zhi-Wei Sun, *Unification of zero-sum problems, subset sums and covers of* $\mathbb{Z}$, Electron. Res. Announc. Am. Math. Soc. **9** (2003), 51 – 60.
[62] E. Szemerédi, *Integer sets containing no arithmetic progressions*, Acta Math. Hung. **56** (1990), 155 – 158.
[63] R. Thangadurai, *On a conjecture of Kemnitz*, C.R. Math. Rep. Acad. Sci. Canada **23** (2001), 39 – 45.

Mathematisches Institut der Universität, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany
*E-mail address*: y.edel@mathi.uni-heidelberg.de

Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK
*E-mail address*: christian.elsholtz@rhul.ac.uk, L.Rackham@rhul.ac.uk

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria
*E-mail address*: alfred.geroldinger@uni-graz.at

Zur Seebecke 6, 31311 Uetze-Hänigsen, Germany
*E-mail address*: silke.kubertin@web.de