INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 7 (2007), #A21

ON SHORT ZERO-SUM SUBSEQUENCES II

W. D. Gao
Center for Combinatorics, Nankai University, Tianjin 300071, China
gao@cfc.nankai.edu.cn

Q. H. Hou
Center for Combinatorics, Nankai University, Tianjin 300071, China
hou@nankai.edu.cn

W. A. Schmid
Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstraße 36, 8010 Graz, Austria
wolfgang.schmid@uni-graz.at

R. Thangadurai
School of Mathematics, Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad - 211019, India
thanga@mri.ernet.in

Received: 7/7/06, Accepted: 4/11/07, Published: 4/18/07

Abstract

Let G be a finite abelian group of exponent n. In this paper we investigate the structure of the maximal (in length) sequences over G that contain no zero-sum subsequence of length [at most] n. Among others, we obtain a result on the multiplicities of elements in these sequences, which support well-known conjectures on the structure of these sequences. Moreover, we investigate the related invariants $\mathsf{s}(G)$ and $\eta(G)$, which are defined as the smallest integer l such that every sequence over G of length at least l has a zero-sum subsequence of length n (at most n, respectively). In particular, we obtain the precise value of $\mathsf{s}(G)$ for certain groups of rank 3.

1. Introduction and Main Results

Let G be a finite abelian group. By $\mathsf{s}(G)$ (or $\eta(G)$ respectively) we denote the smallest integer $l \in \mathbb{N}$ such that every sequence S over G of length $|S| \geq l$ has a zero-sum subsequence T of length $|T| = \exp(G)$ (or $1 \leq |T| \leq \exp(G)$ respectively). For details on terminology and notation we refer to Section 2. The investigation of these invariants has a long tradition, and in recent years the investigation of these invariants and of the according inverse problems, i.e., the investigation of the structure of extremal sequences with, and in particular without, the respective properties, received an increasing amount of attention. Among others, this is due to applications in the theory of non-unique factorizations. We refer to the monograph [21], in particular to Chapter 5, for a detailed account of results on these invariants and their applications in the theory of non-unique factorizations, and to the recent survey article [16] for an exposition of the state of the knowledge and numerous references.

Still, many questions are wide open. The precise value of $\mathsf{s}(G)$ for cyclic groups is known by the classical Erdős–Ginzburg–Ziv theorem [9], but $\mathsf{s}(G)$ for groups of rank 2 has only recently been determined by C. Reiher [26], and the precise value of $\mathsf{s}(G)$ is unknown for most groups of rank greater than 2, as is the value of $\eta(G)$. In Theorem 2.2 we recall these and some further results on $\mathsf{s}(G)$ and $\eta(G)$ that we apply in our investigations.

A main motivation for the investigations of this paper is the following conjecture.

Conjecture 1.1. ([14, Conjecture 2.3]) Let G be a finite abelian. Then

$$\mathsf{s}(G) = \eta(G) + \exp(G) - 1.$$

It is well-known and not difficult to see that $\mathsf{s}(G) \geq \eta(G) + \exp(G) - 1$ (cf., e.g., [21, Lemma 5.7.2]). Moreover, several (in general unproven) assertions, which we recall below, on the structure of maximal sequences without zero-sum subsequences of length $\exp(G)$ would imply this conjecture.

Open Problems 1.2. Let G be a finite abelian group with $\exp(G) = n$. Are the following claims true?

(C1) Every sequence $S \in \mathcal{F}(G)$ of length $\mathsf{s}(G) - 1$ that has no zero-sum subsequence of length n contains some element $g \in G$ with multiplicity $\mathsf{v}_g(S) \geq \lfloor (n-1)/2 \rfloor$.

(C2) Every sequence $S \in \mathcal{F}(G)$ of length $\mathsf{s}(G) - 1$ that has no zero-sum subsequence of length n contains some element $g \in G$ with multiplicity $\mathsf{v}_g(S) = n - 1$.

(C3) Suppose $G \cong C_n^r$. Every sequence $S \in \mathcal{F}(G)$ of length $\eta(G) - 1$ that has no non-empty zero-sum subsequence of length at most n is of the form $S = T^{n-1}$ for some $T \in \mathcal{F}(G)$, i.e., each element contained in S is contained in it with multiplicity $n - 1$. (A group for which this is true is said to have Property C.)

(C4) Suppose $G \cong C_n^r$. Every sequence $S \in \mathcal{F}(G)$ of length $\mathsf{s}(G) - 1$ that has no zero-sum subsequence of length n is of the form $S = T^{n-1}$ for some $T \in \mathcal{F}(G)$. (A group for which this is true is said to have Property D.)

Apparently, these four claims are closely related. Obviously, (C2) is a stronger claim than (C1), and for $G \cong C_n^r$ the claim (C4) is stronger than (C2). And, it is known that if for a group (C1) is true, then so is Conjecture 1.1 (see [14, Proposition 2.7]). Moreover, it is known that (C4) implies (C3). Conversely, if for a group both (C1) and (C3) are true, then so is (C4) (see [18, Theorem 2]).

No counterexample to Conjecture 1.1 or to these claims is known and there are several results that support them (see, e.g., [13, 15, 18, 7]). However, they are only confirmed for very few types of groups. It is easy to see that elementary 2-groups have Property D and H. Harborth [22, Beweis von Hilfssatz 3] showed (not using this terminology) that elementary 3-groups have Property D as well. Furthermore, for cyclic groups the inverse problems are well investigated (see, e.g., [12, 11, 29, 17]), and in particular it is known that cyclic groups have Property D. Yet, for groups of rank 2 only Conjecture 1.1 is confirmed in general (cf. Theorem 2.2); the more general claims are confirmed only in special cases: for instance it is known that C_n^2 has Property D if n is not divisible by a prime greater than 7 (see [28] and the references there). Additionally, Conjecture 1.1 is confirmed for certain 2- and 3-groups (see [7]), in particular for groups of exponent 4 (see [14]), for C_5^3 (see [16, Theorem 6.6.4]), and for a special type of p-group with "large" exponent (see [27]).

In this paper, we confirm Conjecture 1.1 and the claims in Open Problems 1.2 for certain groups and obtain results that support them for more general groups. Moreover, we determine the precise value of $\mathsf{s}(G)$ for certain groups of rank 3. Below, we outline the results of this paper in more detail.

First, we obtain two results valid for fairly general groups. The first gives some information on the structure of "long" sequences without a zero-sum subsequence of length equal to the exponent of the group.

Theorem 1.3. *Let G be a finite abelian group with $\exp(G) = n$. Let $S \in \mathcal{F}(G)$ such that $|S| \geq \eta(G) + n - 2$ and S has no zero-sum subsequence of length n.*

1. *$\mathsf{v}_g(S) \neq n - 2$ for each $g \in G$.*
2. *If $n - 3 \geq \lfloor (n-1)/2 \rfloor$ and $\gcd(2, n) = 1$, then $\mathsf{v}_g(S) \neq n - 3$ for each $g \in G$.*
3. *If $n - 4 \geq \lfloor (n-1)/2 \rfloor$ and $\gcd(6, n) = 1$, then $\mathsf{v}_g(S) \neq n - 4$ for each $g \in G$.*

This theorem directly yields the following result.

Corollary 1.4. *Let G be a finite abelian group with $\exp(G) = n$. Let $S \in \mathcal{F}(G)$ such that either $|S| = \mathsf{s}(G) - 1$ and S has no zero-sum subsequence of length n, or $|S| = \eta(G) - 1$ and S has no non-empty zero-sum subsequence of length at most n. Then assertions 1., 2., and 3. of Theorem 1.3 hold.*

This result, in particular, implies that if (C2) (or Properties C or D) should not hold for some group, then the structure of the extremal sequences has to differ considerably from the "expected" one. Furthermore, it immediately implies that C_3^r has Property D for every $r \in \mathbb{N}$.

The second result is an upper bound on $\mathsf{s}(G)$, which supports Conjecture 1.1. For now, we only state a special case; for the more technical results see Section 4.

Theorem 1.5. *Let G be a finite abelian group and let $H \subset G$ be a subgroup such that $\exp(G) = \exp(H)\exp(G/H)$. If $\exp(G) \ge |G/H|^2$, then*

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

At first it might not be clear that this results actually supports Conjecture 1.1 and, thus, we add the following explanation. We recall a result that generalizes a classical result of H. Harborth [22]; also see Theorem 1.2 and Lemma 4.1 in [7] for other and more general results of this type.

Lemma 1.6. ([5, Proposition 3.1]) *Let G be a finite abelian group and let $H \subset G$ be a subgroup such that $\exp(G) = \exp(H)\exp(G/H)$. Then*

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

Consequently, if Conjecture 1.1 is true for G/H, then the upper bound of Theorem 1.5 follows immediately. Conversely, we can use Theorem 1.5 to confirm, under certain conditions, Conjecture 1.1 (see Section 4 for details).

Then, we focus on specific groups of rank 3 and obtain the following results.

Theorem 1.7. *Let $n = 3^a 5^b$ for $a, b \in \mathbb{N}_0$. Then*

$$\mathsf{s}(C_n^3) = \eta(C_n^3) + n - 1 = 9n - 8.$$

Thus, equality holds at the lower bound obtained by C. Elsholtz [8] (cf. Theorem 2.2.3 for his actual result, which is more general), so far this was known only for $n = 3^a$.

Theorem 1.8. *Let $n = 2^a 3$ with $a \in \mathbb{N}$. Then*

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

Thus, equality holds at the classical lower bound due to H. Harborth [22] (cf. Theorem 2.2.2). The crucial point in the proofs of these two results is the investigation of C_5^3 and C_6^3, respectively. In these investigations Theorem 1.3 plays a key role. However, considerable additional effort and the aid of a computer is needed to obtain the results. In particular, we also prove that (C2) holds for C_6^3 (see Proposition 6.3) and moreover obtain the following result.

Theorem 1.9. *Let $a \in \mathbb{N}$. The group $C_{5^a}^3$ has Property D.*

In view of these results, we formulate the following conjecture.

Conjecture 1.10. Let $n \in \mathbb{N}$. Then

$$\mathsf{s}(C_n^3) = \begin{cases} 8n - 7 & \text{if } n \text{ is even} \\ 9n - 8 & \text{if } n \text{ is odd}\,. \end{cases}$$

As mentioned above, $8n - 7$ and $9n - 8$, respectively, are known to be lower bounds. Moreover, if n is even, C_n^3 has Property D, and $\mathsf{s}(C_m^3) = 9m - 8$ where m denotes the maximal odd divisor of n, then $\mathsf{s}(C_n^3) = 8n - 7$; this follows by Lemma 1.6 and the well-known fact that this conjecture is true for powers of 2 (cf. Theorem 2.2.2).

The organization of the paper is as follows: in Section 2 we recall basic terminology and results, and each of the other sections is devoted to the proof of one or two of the above mentioned theorems. Following [7], we use geometrical methods.

2. Preliminaries

Our terminology and notation is consistent with the monograph [21]. For convenience we recall some key notions.

Let $\mathbb{N}$ and $\mathbb{N}_0$ denote the positive and non-negative integers, respectively. Throughout, all finite abelian groups are written additively. For $r, n \in \mathbb{N}$, we denote by C_n a cyclic group of order n and by C_n^r the direct sum of r copies of C_n.

Let G denote a finite abelian group. If $|G| > 1$, then there exist uniquely determined integers $1 < n_1 \mid \cdots \mid n_r$ such that $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$, and $\exp(G) = n_r$ is called the exponent of G and $\mathsf{r}(G) = r$ the rank of G. For $|G| = 1$, let $\exp(G) = 1$ and $\mathsf{r}(G) = 0$. We call G a p-group if $\exp(G) = p^k$ for p a prime number and $k \in \mathbb{N}$, and we call G an elementary p-group if $\exp(G) = p$.

We denote by $\mathcal{F}(G)$ the (multiplicatively written) free abelian monoid with basis G. An element $S \in \mathcal{F}(G)$ is called a sequence over G and is written in the following ways:

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

where $\mathsf{v}_g(S) \in \mathbb{N}_0$, and $l \in \mathbb{N}_0$ and $g_i \in G$. The neutral element of $\mathcal{F}(G)$ is called the empty sequence. We call $|S| = l \in \mathbb{N}_0$ the length, $\sigma(S) = \sum_{i=1}^{l} g_i \in G$ the sum, and $\operatorname{supp}(S) = \{g \in G \colon \mathsf{v}_g(S) > 0\}$ the support of S. Moreover, $\mathsf{v}_g(S)$ is called the multiplicity of g in S.

A sequence is called a zero-sum sequence if $\sigma(S) = 0$, it is called squarefree if $\mathsf{v}_g(S) \le 1$ for each $g \in G$, and it is called short (with respect to G) if $1 \le |S| \le \exp(G)$. A sequence T is called a subsequence of S (in symbols $T \mid S$) if T divides S (in $\mathcal{F}(G)$), i.e., there exists a sequence $T' \in \mathcal{F}(G)$ such that $TT' = S$; clearly the sequence T' is uniquely determined by T and S and we denote it by $T^{-1}S$.

As mentioned in Section 1, we investigate the invariants $\mathsf{s}(\cdot)$ and $\eta(\cdot)$. In our investigations we make use of an other related invariant as well. We summarize their definitions.

Definition 2.1 Let G be a finite abelian group. We denote by

- $\eta(G)$ the smallest $l \in \mathbb{N}$ 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 $l \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a zero-sum subsequence of length $\exp(G)$.
- $\mathsf{g}(G)$ the smallest $l \in \mathbb{N}$ such that every squarefree sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ has a zero-sum subsequence of length $\exp(G)$.

We point out that, though, in case G is an elementary 2-group or a cyclic group of even order no squarefree zero-sum sequences over G of length $\exp(G)$ exist, the invariant $\mathsf{g}(G)$ is nevertheless well-defined (cf. [16, Lemma 10.1]).

In the following theorem we recall known results on these invariants that we use in this paper.

Theorem 2.2. *Let $m, n, r \in \mathbb{N}$ with $m \mid n$.*

1. $\eta(C_m \oplus C_n) = 2m + n - 2$ *and* $\mathsf{s}(C_m \oplus C_n) = 2m + 2n - 3$.
2. $\eta(C_n^r) \ge (2^r - 1)(n - 1) + 1$ *and* $\mathsf{s}(C_n^r) \ge 2^r(n - 1) + 1$. *If n is a power of 2, then equality holds.*
3. *If n is odd, then* $\eta(C_n^3) \ge 8n - 7$ *and* $\mathsf{s}(C_n^3) \ge 9n - 8$. *If n is a power of 3, then equality holds.*
4. $\mathsf{g}(C_5^2) = 9$ *and* $\mathsf{g}(C_3^3) = 10$.

Proof.

1. The result is based on work of C. Reiher [26] and may be found in [21, Theorem 5.8.3].
2. The result is due to H. Harborth [22, Hilfsatz 1 and Satz 1], also see [7, Proposition 3.1].
3. The lower bound is due to C. Elsholtz [8, Theorem] (actually, he obtained an improvement on (2) for odd n for arbitrary $r \ge 3$; moreover see [7] for further improvements for $r \ge 4$). Equality for powers of 3 holds by Lemma 1.6, since $\mathsf{s}(C_3^3) = 19$ (see [22, Satz 4]); also cf. [7,

Corollary 4.5].
4. The results are due to A. Kemnitz [24, Theorem 3] and H. Harborth [22, Beweis von Satz 4], respectively. The latter result was also obtained in other contexts; see [7, Section 5] for details. □

Let G' be a finite abelian group. For every map $\phi : G \to G'$ there exists a unique continuation to a monoid homomorphism $\mathcal{F}(G) \to \mathcal{F}(G')$, which we thus denote by ϕ as well; it is given by $\phi(\prod_{i=1}^{l} g_i) = \prod_{i=1}^{l} \phi(g_i)$. In particular, $|S| = |\phi(S)|$ and $\phi(\mathrm{supp}(S)) = \mathrm{supp}(\phi(S))$, and if $\phi : G \to G'$ is a homomorphism, then $\sigma(\phi(S)) = \phi(\sigma(S))$.

We call a map $\alpha : G \to G'$ affine if there exists a homomorphism $\phi_\alpha : G \to G'$ and an element $h_\alpha \in G'$ such that $\alpha(g) = \phi_\alpha(g) + h_\alpha$ for every $g \in G$; furthermore, we call a bijective affine map an affinity. Obviously, for α an affine map, ϕ_α and h_α are uniquely determined, and α is an affinity if and only if ϕ_α is an isomorphism.

We will frequently and freely make use of the following result (see [7, Lemma 2.2]).

Lemma 2.3. *Let G and G' be finite abelian groups, let $S \in \mathcal{F}(G)$, and let $\phi : G \to G'$. Suppose that ϕ is an affinity (in particular $\exp(G') = \exp(G)$). Then S has a zero-sum subsequence of length $\exp(G)$ if and only if $\phi(S)$ has a zero-sum subsequence of length $\exp(G)$.*

Elementary p-groups are in a natural way vector spaces over $\mathbb{F}_p$, the field with p elements; whenever it is convenient we consider elementary p-groups as vector spaces over $\mathbb{F}_p$. Clearly, in this case our definition of an affinity coincides with the usual one.

As in [7], we use the following well-known geometric notion in our investigations (cf., e.g., the monograph [23, Chapters 16 and 18]): a set of points C (in some geometry) is called a cap if no three distinct points in C are collinear. Considering elementary p-groups as vector spaces these are naturally affine geometries. Explicitly, a subset C of an elementary p-group is a cap if and only if for each three distinct elements $f, g, h \in C$ we have $\langle g - f \rangle \neq \langle h - f \rangle$. At one point, in Lemma 6.1, we need to embed an elementary p-group into a projective geometry in order to apply geometric results; we give the details there.

As discussed in [7] in detail, the investigation of (the maximal cardinality) of caps and of $\mathsf{s}(G)$ and $\mathsf{g}(G)$ for elementary p-groups is closely related. In particular, for $p = 3$ these problems are equivalent. We make use of this relation in Sections 5 and 6.

3. Proof of Theorem 1.3 and its Corollary

First, we prove Theorem 1.3 and then Corollary 1.4.

Proof of Theorem 1.3. We prove the three statements separately. In each case, we suppose that n fulfills the respective condition and assume to the contrary that $\mathsf{v}_g(S) = n - i$ for some $g \in G$, where i equals 2, 3, and 4, respectively. By Lemma 2.3 we may assume that $g = 0$.

1. For $n = 1$ the claim is trivial and we thus assume $n \geq 2$. Let $S = 0^{n-2}T$. We have $|T| \geq \eta(G)$. Thus, by definition of $\eta(G)$, there exists a short zero-sum subsequence $W \mid T$ and, since $0 \nmid T$, we have $|W| \geq 2$. Therefore, $W0^{n-|W|}$ is a subsequence of S, and its sum equals 0 and its length equals n, a contradiction.

2. Let $S = 0^{n-3}T$. We have $|T| \geq \eta(G) + 1$. Thus, there exists a short zero-sum subsequence $W \mid T$. If $|W| \geq 3$, the sequence $W0^{n-|W|}$ yields a contradiction. Thus, since $|W| > 1$, we have $|W| = 2$, i.e., $W = (-g)g$ for some $g \in G$. Indeed, we may assume that every short zero-sum subsequence of T has length 2. Consequently, since $n \geq 5$, the sequence $W^{-1}T$ has no short zero-sum subsequence. However, the sequences $g^{-1}T = (-g)W^{-1}T$ and $(-g)^{-1}T = gW^{-1}T$, since they are of length $\eta(G)$, each have a short zero-sum subsequence, which consequently contains $-g$ and g, respectively. By assumption, these short zero-sum sequences are of length 2 and thus are both equal to $(-g)g$. Consequently, $g \mid g^{-1}T$ and $-g \mid (-g)^{-1}T$. Since $2 \nmid n$, we have $-g \neq g$ and therefore $(-g)^2g^2$ is a short zero-sum subsequence of T of length 4, a contradiction.

3. Let $S = 0^{n-4}T$. The sequence T has a short zero-sum subsequence W, which is of length at least 2. If $|W| \geq 4$, then $W0^{n-|W|}$ is a subsequence of S, which yields a contradiction. Moreover, if $W^{-1}T$ contains a short zero-sum sequence W', then, since $n \geq 7$, we get that W, W', or WW' is a short zero-sum subsequence of T of length at least 4. Thus, we may assume that $W^{-1}T$ has no short zero-sum subsequence, and consequently $|W^{-1}T| < \eta(G)$ and $|W| > 2$.

In other words, we may assume that for each short zero-sum subsequence V of T

- $|V| = 3$ and
- $V^{-1}T$ has no short zero-sum subsequence (in particular, if V' is a short zero-sum subsequence of T, then $\operatorname{supp}(V) \cap \operatorname{supp}(V') \neq \emptyset$).

Now, we distinguish two cases.

Case 1. Every short zero-sum subsequence of T is squarefree. Let V be a short zero-sum subsequence of T and let $g \in \operatorname{supp}(V)$. Since $V^{-1}T$ does not have a short zero-sum subsequence, $gV^{-1}T$ has a short zero-sum subsequence V' and $g \in \operatorname{supp}(V')$. By assumption V' is squarefree. Thus, it follows that $\mathsf{v}_g(T) = 1$, since otherwise $V' \mid V^{-1}T$, a contradiction. We write $V = g_1g_2g_3$. By the above reasoning, for each $1 \leq j \leq 3$, there exists a short zero-sum subsequence $U_j \mid g_jV^{-1}T$ with $g_j \in \operatorname{supp}(U_j)$. We distinguish two subcases.

Subcase 1.1. $\bigcap_{j=1}^{3} \operatorname{supp}(U_j) \neq \emptyset$. The intersection contains a unique element; we denote it by $h \in G$. We note that $h \notin \operatorname{supp}(V)$. For $1 \leq j \leq 3$, let $h_j \in G$ such that $U_j = g_jhh_j$. There exists a short zero-sum subsequence $R \mid h_1U_1^{-1}T$ with $h_1 \in \operatorname{supp}(R_1)$. We have $\operatorname{supp}(R) \cap \operatorname{supp}(V) = \{g_j\}$ for some $1 \leq j \leq 3$, and, since $g_1 \notin \operatorname{supp}(R)$, we have $j \in \{2, 3\}$. Let $i \in \mathbb{N}$ such that $\{i, j\} = \{2, 3\}$. We note that $\{h, g_i\} \cap \operatorname{supp}(R) = \emptyset$ and $g_j \notin \operatorname{supp}(U_i)$. Thus $\operatorname{supp}(R) \cap \operatorname{supp}(U_i) = \{h_i\}$ and $R = h_1h_ig_j$. We note that $VU_1U_i = R(g_1hg_i)^2$. Since

$\sigma(V) = \sigma(U_1) = \sigma(U_i) = \sigma(R) = 0$, we infer that $2\sigma(g_1hg_i) = \sigma((g_1hg_i)^2) = 0$. Thus, since $2 \nmid n$, we have $\sigma(g_1hg_i) = 0$. However, this implies $h = -g_1 - g_i = g_j$, a contradiction, since U_j is squarefree.

Subcase 1.2. $\bigcap_{j=1}^3 \operatorname{supp}(U_j) = \emptyset$. Since $|\operatorname{supp}(U_i) \cap \operatorname{supp}(U_j)| = 1$ for $1 \le i < j \le 3$, we infer that $|\bigcup_{j=1}^3 \operatorname{supp}(U_i) \setminus \operatorname{supp}(V)| = 3$, and each of these 3 elements is contained in exactly 2 of the U_js. Thus $U_1U_2U_3 = VR^2$ for some squarefree sequence R with $\operatorname{supp}(R) \cap \operatorname{supp}(V) = \emptyset$. Furthermore, $2\sigma(R) = \sigma(R^2) = 0$ and thus $\sigma(R) = 0$. Consequently, R is a short zero-sum subsequence of $V^{-1}T$, a contradiction.

Case 2. There exists a short zero-sum subsequence V of T that is not squarefree. Since $|V| = 3$ and since $3 \nmid n$, we have $V = gh^2$ with distinct elements $g, h \in G$. There exists a short zero-sum subsequence $U \mid gV^{-1}T$ with $g \in \operatorname{supp}(U)$. We distinguish three cases.

Subcase 2.1. $\mathsf{v}_h(U) \ge 1$. This implies $\mathsf{v}_h(U) = 2$, $U = V$, and $\mathsf{v}_h(T) \ge 4$. Consequently $\mathsf{v}_g(T) = 1$. Let $R \mid hV^{-1}T$ a short zero-sum sequence with $h \in \operatorname{supp}(R)$. Since $g \notin \operatorname{supp}(R)$ and since $R \ne h^3$, we infer that $R \mid V^{-1}T$, a contradiction.

Subcase 2.2. $\mathsf{v}_g(U) = 1$ (and $\mathsf{v}_h(U) = 0$). We have $\mathsf{v}_g(T) = 1$, otherwise $U \mid V^{-1}T$. Moreover, since $\mathsf{v}_g(U) = 1$ and $2 \nmid n$, we know that U is squarefree. Let $R \mid hV^{-1}T$ be a short zero-sum sequence with $h \in \operatorname{supp}(R)$. We have $\mathsf{v}_g(R) = 0$ and thus $\mathsf{v}_h(R) = 1$. Since $\operatorname{supp}(R) \cap \operatorname{supp}(U) \ne \emptyset$, we have $U = gff_1$ and $R = hff_2$ with $f, f_1, f_2 \in G$. Clearly $f_1 \ne f_2$. Let $Q \mid f_1U^{-1}T$ be a short zero-sum sequence with $f_1 \in \operatorname{supp}(Q)$. Since $\operatorname{supp}(Q) \cap \operatorname{supp}(V) \ne \emptyset$, we have $Q = f_1hf_3$. We have $f_3 \ne h$. Moreover, since $f \ne f_1$ and $f + f_2 = f_1 + f_3$, we have $f_2 \ne f_3$. Thus $Q \mid R^{-1}T$, a contradiction.

Subcase 2.3. $\mathsf{v}_g(U) \ge 2$ (and $\mathsf{v}_h(U) = 0$). Let $U = g^2f$ with $f \in G$, and we have $g \ne f$. Let $R \mid fU^{-1}T$ a short zero-sum sequence with $f \in \operatorname{supp}(R)$. We may assume that $\mathsf{v}_f(R) \ge 2$ and $\mathsf{v}_g(R) = 0$, otherwise we are in the situation of Subcase 2.1 or 2.2. Let $R = f^2f'$. On the one hand we have $g \ne f$, and furthermore

$$g + 2h = 2g + f = 2f + f' = 0,$$

which implies

- $f \ne h$, since otherwise $g = h$, a contradiction,
- $f' \ne g$, since otherwise $f = g$, a contradiction,
- $f' \ne h$, since otherwise $3(f+g+h) = 0$ and $f+g+h = 0$, a contradiction as $(fgh)^2 \mid T$.

On the other hand, we have $\operatorname{supp}(R) \cap \operatorname{supp}(V) \ne \emptyset$, that is $\{g, h\} \cap \{f, f'\} \ne \emptyset$, a contradiction. $\square$

Proof of Corollary 1.4. If $|S| = \mathsf{s}(G) - 1$ and S has no zero-sum subsequence of length n, then, since $\mathsf{s}(G) \ge \eta(G) + n - 1$, the result is obvious by Theorem 1.3. If $|S| = \eta(G) - 1$ and

S has no short zero-sum subsequence, then we note that $0^{n-1}S$ has no zero-sum subsequence of length n and again the claim is obvious by Theorem 1.3. $\square$

4. Proof of Theorem 1.5 and Related Results

To prove Theorem 1.5, we first derive a technical result (Proposition 4.1). From this result, using known upper and lower bounds for the involved quantities, we derive Theorem 1.5. Moreover, we discuss some other ways to derive "explicit" results from the technical one.

Proposition 4.1. *Let G be a finite abelian group and let $H \subset G$ be a subgroup such that $\exp(G) = \exp(H)\exp(G/H)$. We denote $\exp(G/H)$ by n. Then*

$$\begin{aligned}\mathsf{s}(G) \le \max\Big\{&|G/H|\Big(n-2+\Big(\frac{n}{\lceil\frac{n+1}{2}\rceil}-1\Big)\big(\mathsf{s}(G/H)-\eta(G/H)-1\big)\Big),\\ &n\,\mathsf{s}(H)+\eta(G/H)-1\Big\}.\end{aligned}$$

Proof. Let $S \in \mathcal{F}(G)$ such that S is at least as long as the claimed upper bound on $\mathsf{s}(G)$. We have to show that S has a zero-sum subsequence of length $\exp(G)$. Let $\phi : G \to G/H$ be the canonical epimorphism. Without restriction we assume that $\mathsf{v}_0(\phi(S)) = \max\{\mathsf{v}_g(\phi(S))\colon g \in G/H\}$; let $\mathsf{v}_0(\phi(S)) = v$. We have $v \ge |S|/|G/H|$. We write $\phi(S) = 0^v T$. Let $T_1 \dots T_a \mid T$ such that $\sigma(T_i) = 0 \in G/H$ and $|T_i| = n$ for each $1 \le i \le a$. We assume that a is maximal, i.e., $W = T(\prod_{i=1}^a T_i)^{-1}$ has no zero-sum subsequence of length n, and thus $|W| \le \mathsf{s}(G/H)-1$. Further, let $W_1 \dots W_b \mid W$ such that each W_i is a short zero-sum sequence. We may assume that $|W_1| \ge \dots \ge |W_b|$ and that $|W_i| \ge \lceil (n+1)/2\rceil$ for each $1 \le i \le b-1$. Moreover, we assume that $|W| - \sum_{i=1}^b |W_i| \le \eta(G/H)-1$, and in case $b \ge 1$ that $|W| - \sum_{i=1}^{b-1}|W_i| \ge \eta(G/H)$.

If $\sum_{i=1}^b (n-|W_i|) \le v$, then $T_1 \dots T_a (W_1 0^{n-|W_1|}) \dots (W_b 0^{n-|W_b|}) \mid \phi(S)$, i.e., we can "extend" the W_is to zero-sum subsequences of length n of $\phi(S)$. We assert that indeed $\sum_{i=1}^b (n-|W_i|) \le v$. If $b=0$, this is trivial. If $b=1$, then $n-|W_b| \le n-2 \le |S|/|G/H| \le v$. We assume $b \ge 2$. We have $(b-1)|W_{b-1}| \le \sum_{i=1}^{b-1}|W_i| \le \mathsf{s}(G/H)-1-\eta(G/H)$. Thus

$$\begin{aligned}\sum_{i=1}^b (n-|W_i|) &\le (n-|W_b|)+(b-1)(n-|W_{b-1}|)\\ &\le n-2+\frac{\mathsf{s}(G/H)-\eta(G/H)-1}{|W_{b-1}|}(n-|W_{b-1}|)\\ &\le n-2+\big(\mathsf{s}(G/H)-\eta(G/H)-1\big)\frac{n-\lceil\frac{n+1}{2}\rceil}{\lceil\frac{n+1}{2}\rceil}\\ &\le \frac{|S|}{|G/H|} \le v.\end{aligned}$$

Now, we set $c = \lfloor (v - \sum_{i=1}^{b}(n - |W_i|))/n \rfloor$ and have

$$T_1 \dots T_a (W_1 0^{n-|W_1|}) \dots (W_b 0^{n-|W_b|})(0^n)^c \mid \phi(S).$$

Thus, we have $a+b+c$ zero-sum subsequences of length n of $\phi(S)$.

We assert that $a+b+c > \mathsf{s}(H) - 1$. We have

$$(a+b)n = \sum_{i=1}^{a} |T_i| + \sum_{i=1}^{b} |W_i| + \sum_{i=1}^{b} (n - |W_i|)$$

and $|S| - v - \sum_{i=1}^{a} |T_i| - \sum_{i=1}^{b} |W_i| \le \eta(G/H) - 1$. Moreover, $nc \ge v - \sum_{i=1}^{b}(n - |W_i|) - (n-1)$. Consequently,

$$\begin{aligned} & n(a+b+c) \ge \\ & \quad |S| - v - \eta(G/H) + 1 + \sum_{i=1}^{b}(n - |W_i|) + v - \sum_{i=1}^{b}(n - |W_i|) - (n-1) \ge \\ & \quad n\, \mathsf{s}(H) + \eta(G/H) - 1 - \eta(G/H) + 1 - (n-1) = \\ & \quad n\, \mathsf{s}(H) - (n-1) > n(\mathsf{s}(H) - 1). \end{aligned}$$

Let $S_1 \dots S_{a+b+c} \mid S$ such that $\phi(S_i)$ is equal to T_i, $W_{i-a} 0^{n-|W_{i-a}|}$ or 0^n according as $1 \le i \le a$, $a+1 \le i \le a+b$ or $a+b+1 \le i$. Since $\prod_{i=1}^{a+b+c} \sigma(S_i) \in \mathcal{F}(H)$ is a sequence of length at least $\mathsf{s}(H)$, it has a zero-sum subsequence of length $\exp(H)$. Let $I \subset \{1, \dots, a+b+c\}$ a subset of cardinality $\exp(H)$ such that $\sum_{i \in I} \sigma(S_i) = 0$. Then $\prod_{i \in I} S_i$ is a zero-sum subsequence of S of length $n \exp(H) = \exp(G)$. □

From this result we can derive the following corollary, which is slightly less precise but more convenient for the present purpose.

Corollary 4.2. *Let G be a finite abelian group and let $H \subset G$ be a subgroup such that $\exp(G) = \exp(H)\exp(G/H)$ and*

$$\mathsf{s}(H) \ge \frac{|G/H|}{\exp(G/H)} \big(\mathsf{s}(G/H) - \eta(G/H) + \exp(G/H) - 3 \big).$$

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

Proof. We denote $\exp(G/H)$ by n. For $n = 1$ the result is trivial and we assume $n \ge 2$. By Proposition 4.1, it suffices to prove that

$$|G/H| \big(n - 2 + \big(\frac{n}{\lceil \frac{n+1}{2} \rceil} - 1 \big) \big(\mathsf{s}(G/H) - \eta(G/H) - 1 \big) \big) \le n\, \mathsf{s}(H) + \eta(G/H) - 1.$$

This follows by an easy calculation. □

In order to obtain Theorem 1.5 we need the following bounds on $\mathsf{s}(\cdot)$ and $\eta(\cdot)$. The lower bounds are fairly obvious. The upper bounds for $\mathsf{s}(\cdot)$ and $\eta(\cdot)$ were obtained in [20] (also cf. [21, Theorem 5.7.4]). All bounds are sharp for cyclic groups.

Proposition 4.3. *Let G be a finite abelian group with $\exp(G) = n$.*

1. $n \le \eta(G) \le |G|$.
2. $2n - 1 \le \mathsf{s}(G) \le |G| + n - 1$.

Having all auxiliary results at hand, we prove Theorem 1.5.

Proof of Theorem 1.5. By Corollary 4.2 it suffices to assert that $\mathsf{s}(H) \ge |G/H|(\mathsf{s}(G/H) - \eta(G/H) + n - 3)/n$. Furthermore, using the bounds recalled in Proposition 4.3 it thus suffices to show the inequality $2\exp(H) - 1 \ge |G/H|(|G/H| - 1 + n - 3)/n$. By assumption $n\exp(H) = \exp(G)$, thus if $\exp(G) \ge |G/H|^2$ this inequality holds. □

For various types of groups refined upper and lower bounds for $\mathsf{s}(\cdot)$ and $\eta(\cdot)$ are known, see, e.g., [1] and [7]. Using these bounds or known precise values for $\mathsf{s}(\cdot)$ and $\eta(\cdot)$, instead of the general bounds, we can obtain refined versions of Theorem 1.5 for various types of groups. As an example, we state the following result.

Corollary 4.4. *Let $m, n, r \in \mathbb{N}$ with $r \ge 3$. If $m \ge n^{2r-1}/2^r$, then $\mathsf{s}(C_{mn}^r) \le n\ \mathsf{s}(C_m^r) + \eta(C_n^r) - 1$.*

Proof. For $n = 1$ the assertion is obvious. Let $n \ge 2$. Let $H \subset C_{mn}^r$ denote the subgroup of elements whose order divides m; it is isomorphic to C_m^r and $C_{mn}^r/H \cong C_n^r$. Using the classical lower bounds, recalled in Theorem 2.2.2, for $\eta(C_n^r)$ and $\mathsf{s}(C_m^r)$, and the upper bound of Proposition 4.3 for $\mathsf{s}(C_n^r)$, the result follows by Corollary 4.2. □

As indicated in Section 1, the results of this section can be applied to confirm Conjecture 1.1 for certain groups. In particular, this is the case if there exists a "large" subgroup for which equality holds in Lemma 1.6.

Corollary 4.5. *Let G be a finite abelian group and let $H \subset G$ be a subgroup such that $\exp(G) = \exp(H)\exp(G/H)$ and $\exp(G) \ge |G/H|^2$. If $\mathsf{s}(G) = \exp(G/H)\mathsf{s}(H) + \mathsf{s}(G/H) - \exp(G/H)$, then $\mathsf{s}(G/H) = \eta(G/H) + \exp(G/H) - 1$.*

Proof. By Theorem 1.5 we have $\mathsf{s}(G) \le \exp(G/H)\mathsf{s}(H) + \eta(G/H) - 1$. Since $\mathsf{s}(G) = \exp(G/H)\mathsf{s}(H) + \mathsf{s}(G/H) - \exp(G/H)$, we infer $\mathsf{s}(G/H) \le \eta(G/H) + \exp(G/H) - 1$. However, it is well-known that $\mathsf{s}(G/H) \ge \eta(G/H) + \exp(G/H) - 1$. □

Corollary 4.6. *Let $n, r \in \mathbb{N}$ such that there exists a constant $c = c(n, r)$ with $\mathsf{s}(C_{n^a}^r) = c(n^a - 1) + 1$ for every $a \in \mathbb{N}$. Then $\mathsf{s}(C_{n^a}^r) = \eta(C_{n^a}^r) + n^a - 1$ for every $a \in \mathbb{N}$.*

Proof. Let $a \in \mathbb{N}$. We need to show $\mathsf{s}(C_{n^a}^r) = \eta(C_{n^a}^r) + n^a - 1$. Let $b = (2r - 1)a$ and let $G = C_{n^{a+b}}^r$. By assumption we have $\mathsf{s}(G) = c(n^{a+b} - 1) + 1$. Let $H \subset G$ be the subgroup isomorphic to $C_{n^b}^r$. Clearly $G/H \cong C_{n^a}^r$. We have $\mathsf{s}(G) = \exp(G/H)\mathsf{s}(H) + \mathsf{s}(G/H) - \exp(G/H)$ and, since $n^{a+b} \ge (n^{ar})^2$, it follows by Corollary 4.5 that $\mathsf{s}(G/H) = \eta(G/H) + \exp(G/H) - 1$. □

We point out that r and n that fulfil the condition of Corollary 4.6 actually exist. It is well-known that the conditions hold for $r \le 2$ and arbitrary n, where however also the conclusion of Corollary 4.6 is known; but, in the following section we prove that they hold for $r = 3$ and every n whose only prime divisor are 3 and 5 as well, and we conjecture that they hold in further cases as well (cf. Conjecture 1.10).

5. Proof of Theorem 1.7 and Theorem 1.9

We recall and prove several auxiliary results. We start with the more general ones.

5.1 General Auxiliary Results

Let G be a finite abelian group and let $\emptyset \ne A, B \subset G$. Then $A + B = \{a + b \colon a \in A,\ b \in B\}$ is called the sum of A and B, and $\sum_k A = \{\sum_{a \in A'} a \colon A' \subset A,\ |A'| = k\}$ is called the set of k-term subsums. In the following proposition we recall two well-known results on set addition. The first result is the classical Theorem of Cauchy–Davenport and the second one was conjectured by P. Erdős and H. Heilbronn [10] and proved by J. Dias da Silva and Y. ould Hamidoune [6], and differently by N. Alon, M. B. Nathanson, and I. Ruzsa [2, 3]. We refer to the monograph [25], in particular Theorem 2.2 and Theorem 3.4, for a detailed account.

Proposition 5.1. *Let p be a prime number, $k \in \mathbb{N}$, and $\emptyset \ne A, A_1, \ldots, A_r \subset C_p$.*

1. $|A_1 + \cdots + A_r| \ge \min\{p, \sum_{i=1}^{r} |A_i| - (r-1)\}$.
2. $|\sum_k A| \ge \min\{p, k(|A| - k) + 1\}$.

Now, we use these results to establish the following lemma, which was proved in [19] in the special case $r = 2$.

Lemma 5.2. *Let p be a prime number and $r \ge 2$. Let $\pi : C_p^r \to C_p^r$ be a linear projection onto a subgroup of rank $r - 1$. Further, let $S \in \mathcal{F}(C_p^r)$ be a squarefree sequence. If there exists a zero-sum subsequence $T \mid \pi(S)$ such that $\sum_{h \in \mathrm{im}(\pi)} \mathsf{v}_h(T)(\mathsf{v}_h(\pi(S)) - \mathsf{v}_h(T)) \ge p - 1$, then there exists a zero-sum subsequence $T^* \mid S$ with $|T^*| = |T|$.*

Proof. Let $H = \mathrm{im}(\pi)$. We assume that $T \mid \pi(S)$ is a zero-sum sequence such that $\sum_{h \in H} \mathsf{v}_h(T)(\mathsf{v}_h(\pi(S)) - \mathsf{v}_h(T)) \ge p - 1$

For $h \in H$, let $S_h \mid S$ such that $\pi(S_h) = h^{\mathsf{v}_h(\pi(S))}$. Since S is squarefree, we know that $(\mathrm{id} - \pi)(S_h) \in \mathcal{F}(\ker(\pi))$ is squarefree. Clearly $\ker(\pi) \cong C_p$. Therefore, by Proposition 5.1.2,

$$|\{\sigma((\mathrm{id} - \pi)(T_h)) \colon T_h \mid S_h,\ |T_h| = \mathsf{v}_h(T)\}| \ge \min\{p, \mathsf{v}_h(T)(|S_h| - \mathsf{v}_h(T)) + 1\}.$$

Furthermore,

$$\begin{aligned}
&\{\sigma((\mathrm{id}-\pi)(T')) \colon T' \mid S,\ \pi(T')=T\} = \\
&\{\sigma((\mathrm{id}-\pi)(\prod_{h\in H} T_h)) \colon T_h \mid S_h,\ |T_h| = \mathsf{v}_h(T) \text{ for each } h \in H\} = \\
&\{\sum_{h\in H} \sigma((\mathrm{id}-\pi)(T_h)) \colon T_h \mid S_h,\ |T_h| = \mathsf{v}_h(T) \text{ for each } h \in H\} = \\
&\sum_{h\in H} \{\sigma((\mathrm{id}-\pi)(T_h)) \colon T_h \mid S_h,\ |T_h| = \mathsf{v}_h(T)\} = A.
\end{aligned}$$

Now, by Proposition 5.1.1, the above inequality, and the assumption, we have

$$\begin{aligned}
|A| &\geq \min\big\{p, \sum_{h\in H} |\{\sigma((\mathrm{id}-\pi)(T_h)) \colon T_h \mid S_h,\ |T_h| = \mathsf{v}_h(T)\}| - (|H|-1)\big\} \\
&\geq \min\big\{p, \sum_{h\in H} \min\{p, \mathsf{v}_h(T)(|S_h| - \mathsf{v}_h(T)) + 1\} - (|H|-1)\big\} \\
&\geq \min\{p, 1 + \sum_{h\in H} \mathsf{v}_h(T)(|S_h| - \mathsf{v}_h(T))\} \\
&= p.
\end{aligned}$$

Thus, $A = \ker(\pi) \supset \{0\}$ and consequently there exists a sequence $T^* \mid T$ such that $\pi(T^*) = T$ and $\sigma((\mathrm{id}-\pi)(T^*)) = 0$. Since by definition $\sigma(\pi(T^*)) = \sigma(\pi(T)) = 0$, we have $\sigma(T^*) = 0$ and clearly $|T| = |T^*|$. □

5.2 Results for Elementary 5-groups

For elementary 3-groups it is known that the support of a sequence without a zero-sum subsequence of length equal to the exponent is a cap (cf. [7, Lemma 5.2]). Though, this cannot hold in general for elementary 5-groups, we prove that this is true for the sequences that are of maximal length.

Proposition 5.3. *Let $r \in \mathbb{N}$ and let $S \in \mathcal{F}(C_5^r)$.*

1. *If $|S| = \mathsf{s}(C_5^r) - 1$ and S has no zero-sum subsequence of length 5, then $\mathrm{supp}(S)$ is a cap.*

2. *If $|S| = \eta(C_5^r) - 1$ and S has no short zero-sum subsequence, then $\mathrm{supp}(S)$ is a cap.*

Proof. 1. We suppose that $|S| = \mathsf{s}(C_5^r) - 1$ and S has no zero-sum subsequence of length 5. Let $f, g, h \in \mathrm{supp}(S)$ be distinct elements. We have to show that $\langle g - f \rangle \neq \langle h - f \rangle$. By Lemma 2.3 we may assume that $f = 0$, and we assume to the contrary that $h \in \{2g, -2g, -g\}$. By Corollary 1.4 we know that $v = \mathsf{v}_0(S) \in \{1, 4\}$. Let $S = 0^v T$. We distinguish several cases.

Case 1. $v = 1$ and $h = -g$. The sequence $(gh)^{-1}T$ has a short zero-sum subsequence $|W|$. We have $2 \leq |W| \leq 5$. Thus, $gh0W$, ghW, $0W$, or W is a zero-sum subsequence of S of length 5.

Case 2. $v = 1$ and $h = 2g$. By Corollary 1.4 we have $\mathsf{v}_g(T) \in \{1, 4\}$. If $\mathsf{v}_g(T) = 4$, then g^3h0 is a zero-sum subsequence of S of length 5. Thus, we assume $\mathsf{v}_g(T) = 1$. The sequence $h^{-1}g^2T$ has a zero-sum subsequence W of length 5; this follows by Corollary 1.4, since the sequence has length $\mathsf{s}(C_5^r) - 1$ and the multiplicity of g is 3. Since $W \nmid T$, we have $g^2 \mid W$ and therefore $0hg^{-2}W$ is a zero-sum subsequence of S of length 5.

Case 3. $v = 4$ and $h = -g$. The sequence $gh0^3$ is a zero-sum subsequence of length 5 of S.

Case 4. $v = 4$ and $h = 2g$. If $\mathsf{v}_g(T) = 4$, then $0g^3h \mid S$ and we are done. Thus, again, we assume $\mathsf{v}_g(T) = 1$ and proceed similarly to Case 2.

Case 5. $v = 1$ or $v = 4$, and $h = -2g$. Since $g = 2h$, this follows by Case 2 and Case 4, respectively.

2. The argument is similar. We omit the details. $\square$

Since clearly each sequence over C_5^r without a zero-sum subsequences of length 5, contains no element with multiplicity exceeding 4, Proposition 5.3 yields four times the maximal cardinality of a cap in C_5^r as an upper bound for $\mathsf{s}(C_5^r) - 1$. One could combine this observation with results on caps in C_5^r (see, e.g., [4, Section 8]) to obtain bounds for $\mathsf{s}(C_5^r)$. However, to bound $\mathsf{s}(C_n^r)$ by $n - 1$ times the maximal cardinality of a cap, for $n = 5$, opposed to the situation for $n = 3$, seems to introduce a considerable error. Here, being interested in exact values, we do not pursue this approach any further. Yet, we make use of Proposition 5.3, in a different way, in the present investigations.

Now, we turn to the investigation of C_5^3.

Lemma 5.4. *Let $S \in \mathcal{F}(C_5^3)$ such that $|S| = \mathsf{s}(C_5^3) - 1$ and S has no zero-sum subsequence of length 5. Further, let $T \mid S$ be a squarefree sequence. There exists a linear projection $\pi : C_5^3 \to C_5^3$ onto a subgroup of rank 2 such that $\pi(T) = U^2V$ where UV is a squarefree sequence and $|U| \geq |T|(|T| - 1)/62$.*

Proof. Let N be a subgroup of C_5^3 of order 5. Let
$$q_N = \big|\big\{\{g, h\} \colon \{g, h\} \subset \operatorname{supp}(T),\ g - h \in N \setminus \{0\}\big\}\big|.$$
We have
$$\sum_{N < C_5^3,\ |N| = 5} q_N = \binom{|T|}{2},$$
where $N < C_5^3$ means that N is a subgroup. We note that C_5^3 has $(5^3 - 1)/(5 - 1) = 31$ subgroups of order 5. Thus, there exists some N' such that
$$q_{N'} \geq \frac{1}{31} \frac{|T|(|T| - 1)}{2}.$$

Let $\pi' : C_5^3 \to C_5^3$ be a linear projection onto N' and let $\pi = \mathrm{id} - \pi'$, which is a projection onto $\ker(\pi') = H$, a subgroup of C_5^3 of rank 2. We observe that

$$q_{N'} = \sum_{h \in H} \binom{\mathsf{v}_h(\pi(T))}{2}.$$

By Proposition 5.3, each triple of distinct elements in $\mathrm{supp}(S)$ does not lie on a line. Consequently, π maps no three distinct elements in $\mathrm{supp}(S)$ to the same element. Since $T \mid S$ is squarefree, this implies that $\mathsf{v}_h(\pi(T)) \le 2$ for each $h \in H$. Thus, $\mathsf{v}_h(\pi(T)) = 2$ for $q_{N'} \ge |T|(|T|-1)/62$ elements $h \in H$, and the result follows. □

Next, we prove a result on the structure of sequences over C_5^3 without a zero-sum subsequence of length 5 of maximal length. In particular, this result shows that (C2) is true for the group C_5^3.

Proposition 5.5. *Let $S \in \mathcal{F}(C_5^3)$ such that $|S| = \mathsf{s}(C_5^3) - 1$ and S has no zero-sum subsequence of length 5. Then $(e_0e_1e_2e_3g)^4 \mid S$ for some affine basis $\{e_0, e_1, e_2, e_3\}$ of C_5^3 and some $g \in C_5^3$.*

Proof. By Corollary 1.4 we have $\mathsf{v}_h(S) \in \{0, 1, 4\}$ for each $h \in C_5^3$. First, we prove that at least 5 distinct elements have multiplicity 4 in S. We assume that this is not the case. Then $|\mathrm{supp}(S)| \ge 36 - 3 \cdot 4 = 24$. Let $T \mid S$ denote the maximal squarefree subsequence. By Lemma 5.4 there exists a linear projection π onto a subgroup of rank 2 such that $\pi(T) = U^2V$ where UV is a squarefree sequence and $|U| \ge 24 \cdot 23/62 > 8$. Thus by Theorem 2.2.4 there exists a zero-sum subsequence $W \mid U$ with $|W| = 5$. Let $U' \mid T$ such that $\pi(U') = U^2$. By Lemma 5.2, applied to U' and W, there exists a zero-sum subsequence W^* of U', and thus of S, of length $|W| = 5$, a contradiction. Thus, we have $S = (g_1g_2g_3g_4g_5)^4S'$ with $g_i \in G$. It remains to show that $\{g_1, g_2, g_3, g_4, g_5\}$ contains an affine basis of C_5^3. If this is not the case, then $\{g_1, g_2, g_3, g_4, g_5\}$ is contained in an affine plane of C_5^3. Yet, by Lemma 2.3, since $\mathsf{s}(C_5^2) = 17$ (see Theorem 2.2.1), this implies that $(g_1g_2g_3g_4g_5)^4$ has a zero-sum subsequence of length 5, a contradiction. □

We use this (incomplete) structural result as "initial value" for a program, which we describe below, that yields the following result.

Proposition 5.6. *$\mathsf{s}(C_5^3) = 37$ and C_5^3 has Property D.*

Proof and description of program. Let $S \in \mathcal{F}(C_5^3)$ such that $|S| = \mathsf{s}(C_5^3) - 1$ and S has no zero-sum subsequence of length 5. We have to show that $|S| = 36$ and $S = T^4$ for some $T \in \mathcal{F}(C_5^3)$.

Roughly speaking, our program recursively constructs sequences without a zero-sum subsequence of length 5, i.e., for $S' \in \mathcal{F}(C_5^3)$ without a zero-sum subsequence of length 5 it determines all $g \in G$ such that $S'g$ has no zero-sum subsequence of length 5 (we refer to these elements as admissible elements of S'). It turns out that the set of admissible elements of (all) sequences of length 36 without a zero-sum subsequence of length 5 is empty, i.e.

$\mathsf{s}(C_5^3) - 1 \le 36$ and moreover every sequence of length 36 without a zero-sum subsequence of length 5 is equal to T^4 for some $T \in \mathcal{F}(C_5^3)$.

However, actually our program does not start "from scratch" when constructing these sequences. By Proposition 5.5 we know that for every $S \in \mathcal{F}(C_5^3)$ with $|S| = \mathsf{s}(C_5^3) - 1$ and without a zero-sum subsequence of length 5 there exists some $U \in \mathcal{F}(C_5^3)$ such that $U^4 \mid S$, $|U| = 5$, and $\operatorname{supp}(U)$ contains an affine basis C_5^3. Moreover, by Lemma 2.3 we may assume that this affine basis is equal to $\{0, e_1, e_2, e_3\}$ for some (fixed) basis $\{e_1, e_2, e_3\}$ of C_5^3. Thus, since we are only interested in sequences of length $\mathsf{s}(C_5^3) - 1$ we can restrict to considering sequences that have a subsequence with the above mentioned properties. Therefore, instead of starting the recursive construction with the empty sequence we can start it with a fixed sequence of length 16, and additionally we can make use of the fact that at least one (further) element has to occur with multiplicity 4.

To implement this procedure we represent the elements of C_5^3 by (unsigned) integers in the following way: Every $g \in C_5^3$ has a unique representation $a_g e_1 + b_g e_2 + c_g e_3$ with $0 \le a_g, b_g, c_g \le 4$. For each $g \in C_5^3$ let $n_g = 25a_g + 5b_g + c_g$. (Note that we are only interested in sums of at most 5 elements of C_5^3.) For the complete code and the detailed output of the program see `http://www.combinatorics.net.cn/homepage/hou/C53.html`. $\square$

Finally, we use the results on C_5^3 to prove Theorems 1.7 and 1.9.

Proof of Theorem 1.7. By Theorem 2.2.4 $\mathsf{s}(C_3^3) = 27 - 8$ and by Proposition 5.6 $\mathsf{s}(C_5^3) = 45 - 8$. Thus, the claim follows by [7, Corollary 4.5]; having all auxiliary results at hand, we sketch the argument for a more self-contained exposition: By Theorem 2.2.3 we known that $\mathsf{s}(C_n^3) \ge 9n - 8$ and we have to prove that $9n - 8$ is an upper bound as well. We know this for C_3^3 and C_5^3. Using Lemma 1.6, the general case follows by induction on $a + b$. Finally, noting that $\mathsf{s}(C_n^3) - n + 1 \ge \eta(C_n^3) \ge 8n - 7$, the proof is complete. $\square$

Proof of Theorem 1.9. By Proposition 5.6 we know that C_5^3 has Property D. By [18, Theorem 1], this implies that $C_{5^a}^3$ has Property D for every $a \in \mathbb{N}$. $\square$

6. Proof of Theorem 1.8

Throughout this section we use the following convention and notation. We consider C_6^3 as $C_3^3 \oplus C_2^3$, and we denote by $\pi_3 : C_6^3 \to C_3^3$ and $\pi_2 : C_6^3 \to C_2^3$ the canonical epimorphisms.

We need a further results on caps in C_3^3, or in other words squarefree sequences without a zero-sum subsequence of length 3. It is essentially well-known (cf. the monograph of J.W.P. Hirschfeld [23]), however only in the context of projective geometries. For convenience, we provide a detailed "translation."

Lemma 6.1. *Let $A \subset C_3^3$ be a cap with $|A| = 8$. Then there exists at most one cap $B \subset C_3^3$ with $A \subsetneq B$.*

Proof. If A is inclusion-maximal the statement is obvious. Thus, we assume that A is not inclusion-maximal. We embed C_3^3 into $\mathrm{PG}(3,3)$, the projective space of dimension 3 over the field of order 3; we denote the embedding by ι. We recall (cf. [23, Theorem 16.1.5]) that the maximal cardinality of a cap in $\mathrm{PG}(3,3)$ is 10, and a cap with maximal cardinality is called an ovaloid.

First, we assert that $\iota(A)$ is contained in some ovaloid. Since A is not an inclusion maximal cap, $\iota(A)$ is not an inclusion-maximal cap, and there exists a cap $C \subset \mathrm{PG}(3,3)$ such that $\iota(A) \subsetneq C$. Since $|C| \ge 9$, it follows by [23, Theorem 18.4.2] or [23, Theorem 16.1.7] that C is contained in a (unique) elliptic quadric E. The quadric E is an ovaloid (cf. [23, Proof of Theorem 16.1.5]) and obviously $\iota(A) \subset E$.

Now, let $B \subset C_3^3$ be a cap with $A \subsetneq B$. Then $\iota(A) \subsetneq \iota(B)$ and, since $\iota(A) \subset E$ and $|\iota(A)| = 8$, it follows by [23, Theorem 18.4.2] that $\iota(B) \subset E$. Since $A, B \subset C_3^3$, we have $\iota(A) \subsetneq \iota(B) \subset (E \cap \iota(C_3^3)) \subsetneq E$; the last inclusion is proper, since every plane and thus in particular the plane "at infinity" intersects E (cf. [23, Lemma 16.1.6]). Since $|\iota(A)| = 8$ and $|E| = 10$, this implies $\iota(B) = E \cap \iota(C_3^3)$. Consequently, $\iota(B)$ and thus B is unique. $\square$

In the following lemma we obtain basic properties of sequences over C_6^3 without a zero-sum subsequence of length 6.

Lemma 6.2. *Let $S \in \mathcal{F}(C_6^3)$ such that S has no zero-sum subsequence of length 6.*

1. *Let $S_1 \dots S_m \mid S$ with $|S_i| = 3$ and $\sigma(\pi_3(S_i)) = 0$ for each $1 \le i \le m$. If $|S| \ge 40 + \varepsilon$, with $\varepsilon \in \{0,1,2\}$, then there exists a squarefree sequence $T \in \mathcal{F}(C_3^3)$ of length $7 + \varepsilon$ such that $T^2 \mid \pi_3(S(\prod_{i=1}^m S_i)^{-1})$. In particular, $m \le 8$.*
2. *For $g \in C_3^3$, let $S_g \mid S$ such that $\mathrm{supp}(\pi_3(S_g)) = \{g\}$. If $|S| \ge 40 + \varepsilon$, with $\varepsilon \in \{0,1\}$, and $|S_g| \ge 4$, then $|\mathrm{supp}(S_g)| \le 2 - \varepsilon$.*

Proof. 1. Without restriction we may assume that $\pi_3(S(\prod_{i=1}^m S_i)^{-1})$ has no zero-sum subsequence of length 3. On the one hand, we have $|\pi_3(S(\prod_{i=1}^m S_i)^{-1})| \le 18 = \mathsf{s}(C_3^3) - 1$, $|\mathrm{supp}(\pi_3(S(\prod_{i=1}^m S_i)^{-1}))| \le 9 = \mathsf{g}(C_3^3) - 1$ (see Theorem 2.2), and $\mathsf{v}_g(\pi_3(S(\prod_{i=1}^m S_i)^{-1})) \le 2$ for each $g \in C_3^3$. On the other hand, since S has no zero-sum subsequence of length 6, the sequence $\prod_{i=1}^m \sigma(S_i) \in \mathcal{F}(C_2^3)$ has no zero-sum sequence of length 2 and thus $m \le \mathsf{s}(C_2^3) - 1 = 8$, which implies $|\pi_3(S(\prod_{i=1}^m S_i)^{-1})| = |S| - 3m \ge 16 + \varepsilon$. These conditions imply that $\pi_3(S(\prod_{i=1}^m S_i)^{-1})$ contains at least $7 + \varepsilon$ distinct elements with multiplicity 2, which is just what we claimed.

2. We suppose that $|S| \ge 40 + \varepsilon$ with $\varepsilon \in \{0,1\}$ and $|S_g| \ge 4$ for some $g \in C_3^3$, and assume to the contrary that $|\mathrm{supp}(S_g)| \ge 3 - \varepsilon$. Let $T_g \mid S_g$ with $|T_g| = 4$ and $|\mathrm{supp}(T_g)| \ge 3 - \varepsilon$. Let $W = T_g^{-1} S$. Since $|W| \ge 36 + \varepsilon = (18 + \varepsilon) + \mathsf{s}(C_3^3) - 1$, it follows that there exist $W_1 \dots W_{6+\varepsilon} \mid W$ such that $\sigma(\pi_3(W_i)) = 0$ and $|W_i| = 3$ for each $1 \le i \le 6 + \varepsilon$. Since W has no zero-sum subsequence of length 6, we have $|\{\sigma(W_i) \colon 1 \le i \le 6 + \varepsilon\}| = 6 + \varepsilon$. Since $\pi_3(T_g) = g^4$, it is clear that $\sigma(\pi_3(W')) = 0$ for every subsequence $W' \mid T_g$ of length 3.

However, since $|\mathrm{supp}(T_g)| \geq 3-\varepsilon$, we infer that there exist subsequences $W'_1, \ldots, W'_{3-\varepsilon}$ of T_g of length 3 with pairwise distinct sums. Thus, $\{\sigma(W'_i)\colon 1 \leq i \leq 3-\varepsilon\} \cap \{\sigma(W_i)\colon 1 \leq i \leq 6+\varepsilon\} \neq \emptyset$ and consequently S has a zero-sum subsequence of length 6, a contradiction. $\square$

The following proposition, in particular, shows that (C2) holds for C_6^3. Moreover, it is a key tool in the proof of Theorem 1.8.

Proposition 6.3. *Let $S \in \mathcal{F}(C_6^3)$ such that $|S| = 40$ and S has no zero-sum subsequence of length 6. Then there exists a squarefree $T \in \mathcal{F}(C_6^3)$ with $|T| = 6$ such that $T^5 \mid S$. Moreover, at least one of the following statements holds:*

1. *for some $g \in G$, we have $\mathsf{v}_g(T^{-5}S) = 5$.*

2. *for distinct $g, g' \in G$, we have $\mathsf{v}_g(T^{-5}S) = \mathsf{v}_{g'}(T^{-5}S) = 4$.*

3. *for some $h \in C_3^3$, we have $\mathsf{v}_h(\pi_3(S)) \geq 6$.*

Proof. Since $|S| = 22 + \mathsf{s}(C_3^3) - 1$, we have $S_1 \ldots S_8 \mid S$ such that $\sigma(\pi_3(S_i)) = 0$ and $|S_i| = 3$ for each i. Since S has no zero-sum subsequence of length 6, we have $|\{\sigma(S_i)\colon 1 \leq i \leq 8\}| = 8$ and $W = \pi_3(S(\prod_{i=1}^{8} S_i)^{-1})$ has no zero-sum subsequence of length 3. Thus, $|\mathrm{supp}(W)| \leq 9$ and $\mathsf{v}_g(W) \leq 2$ for each $g \in \mathrm{supp}(W)$. Consequently, $W = T^2rs$ where T is squarefree $|T| = 7$ and $r, s \notin \mathrm{supp}(T)$. We distinguish two cases.

Case 1. $r \neq s$. For each $1 \leq j \leq 8$, we consider the sequence $\pi_3(S_j)W$.

Subcase 1.1. $\pi_3(S_j)$ is squarefree, say $\pi_3(S_j) = h_1h_2h_3$. If $|\mathrm{supp}(T) \cap \{h_1, h_2, h_3\}| \geq 2$, say $h_1h_2 \mid T$, then $h_1^3h_2^3 \mid \pi_3(S_j)W$, a contradiction to Lemma 6.2.1, since the product of 9 zero-sum sequence of length 3 would divide $\pi_3(S)$. If $|\mathrm{supp}(T) \cap \{h_1, h_2, h_3\}| = 1$, say $h_1 \mid T$, then $h_2h_3 \neq rs$, say $h_2 \nmid rs$. By Lemma 6.1, the sequence $h_1^{-1}Trsh_2$ has a zero-sum subsequence U of length 3, and consequently $h_1^3U \mid \pi_3(S_j)W$, a contradiction. Thus, $|\mathrm{supp}(T) \cap \{h_1, h_2, h_3\}| = 0$. If $rs \nmid h_1h_2h_3$, say $h_1, h_2 \notin \{r, s\}$, then by Lemma 6.1 Trh_1 and Tsh_2 both have a zero-sum subsequence of length 3, a contradiction. Therefore, $\pi_3(S_j) = rs(-r-s)$.

Subcase 1.2. $\pi_3(S_j)$ is not squarefree, and thus $\pi_3(S_j) = h_j^3$ for some $h_j \in C_3^3$. If $h_j \nmid W$, then Trh_j and Tsh_j both have a zero-sum subsequence of length 3, a contradiction. Thus $h_j \mid W$. We assert that $|\pi_3^{-1}(h_j) \cap \mathrm{supp}(S)| = 1$. The argument is similar to Lemma 6.2.2. Let $S' = S_jS(\prod_{i=1}^{8} S_i)^{-1}$. First, we assert that $|\pi_3^{-1}(h_j) \cap \mathrm{supp}(S')| = 1$. Assume this is not true. We note that $\mathsf{v}_{h_j}(\pi_3(S')) \geq 4$. There exist subsequences U and U' of S' such that $\pi_3(U) = \pi_3(U') = h_j^3$ and $\sigma(U) \neq \sigma(U')$. Since $\{\sigma(S_i)\colon 1 \leq i \leq 8,\, i \neq j\} \cap \{\sigma(U), \sigma(U')\} \neq \emptyset$, we get a zero-sum subsequence of S of length 6, a contradiction. Now, we assume there exists some $k \neq j$ such that $h_j \mid \pi_3(S_k)$, say $g_k \mid S_k$ and $\pi_3(g_k) = h_j$. Let $g_j \mid S_j$, and define $S'_k = g_k^{-1}g_jS_k$ and $S'_j = g_kg_j^{-1}S_j$. By the above argument $|\pi_3^{-1}(h_j) \cap \mathrm{supp}(S'_j)| = 1$. This proves the assertion.

Thus for each $1 \le j \le 8$, either we have $\pi_3(S_j) = rs(-r-s)$ or we have $\pi_3(S_j) = h_j^3$ and $|\pi_3^{-1}(h_j) \cap \mathrm{supp}(S)| = 1$. We note that we may assume that the former is the case at most once, since, if $j \ne j'$ such that $\pi_3(S_j) = \pi_3(S_j') = rs(-r-s)$, then $S_jS_{j'}W = r^3s^3T^2(-r-s)^2$ and we are in the situation of Case 2.

If none of the sequences $\pi_3(S_j)$ is equal to $rs(-r-s)$, we get $S = (\prod_{i=1}^{6+\varepsilon} g_i^5)(\prod_{i=7+\varepsilon}^{8} g_i^4)R$, where $g_i \in C_6^3$, $\varepsilon \in \{0,1\}$, and $|R| = 2-\varepsilon$. We note that $\mathrm{supp}(R) \cap \{g_1, \ldots, g_8\} = \emptyset$ and thus the result holds with 1. or 2. according as ε equals 1 or 0. If one of the sequences $\pi_3(S_j)$ is equal to $rs(-r-s)$, we get $S = (\prod_{i=1}^{7} g_i^5)R$, where $|R| = 5$, and the result holds with 1.

Case 2. $r = s$. Let $T_0 = Tr$, then $W = T_0^2$. Again, we consider $\pi_3(S_j)W$.

Subcase 2.1. $\pi_3(S_j)$ is squarefree, say $\pi_3(S_j) = h_1h_2h_3$. By Lemma 6.1, there exists at most one $k \in \{1,2,3\}$ such that the sequence T_0h_k has no zero-sum subsequence of length 3, a contradiction.

Subcase 2.2. $\pi_3(S_j) = h_j^3$. If $h_j \mid T_0$, then, as in Subcase 1.2, we get $|\pi_3^{-1}(h_j) \cap \mathrm{supp}(S)| = 1$. If $h_j \nmid T_0$, it follows that T_0h_j has no zero-sum subsequence of length 3, and by Lemma 6.1 h_j is thus uniquely determined by T_0.

Thus, either we have $\pi_3(S_j) = h_0^3$ for some $h_0 \in C_3^3$ that is independent of j, or $\pi_3(S_j) = h_j^3$ and $|\pi_3^{-1}(h_j) \cap \mathrm{supp}(S)| = 1$. Let $n = |\{j \colon \pi_3(S_j) = h_0^3\}|$. We note that $n \le 3$, since by Lemma 6.2.2 $|\pi_3^{-1}(h_0) \cap \mathrm{supp}(S)| \le 2$ and clearly every element has multiplicity at most 5 in S. If $n = 0$, we get $S = (\prod_{i=1}^{8} g_i^5)$. If $n = 1$, we get $S = (\prod_{i=1}^{7} g_i^5)R$ where $|R| = 5$. If $n = 2$, we get $S = (\prod_{i=1}^{6} g_i^5)R$ where $|R| = 10$. If $n = 3$, we get $S = (\prod_{i=1}^{5} g_i^5)g_6^5g_7^4R$ where $|R| = 6$. Thus, for $0 \le n \le 1$ the result holds with 1. and for $2 \le n \le 3$ it holds with 3. $\square$

In the next result, we show that for even longer sequences over C_6^3 without a zero-sum subsequence of length 6 we would obtain very precise structural results. However, actually we use this result to prove that such sequences do not exist.

Proposition 6.4. *Let $S \in \mathcal{F}(C_6^3)$ such that $|S| = \mathsf{s}(C_6^3) - 1$ and S has no zero-sum subsequence of length* 6*. If $|S| \ge 41$, then there exists a $T \in \mathcal{F}(C_6^3)$ with $|T| = 8$ such that $T^5 \mid S$.*

Proof. Obviously, $\mathsf{v}_g(S) \le 5$ for each $g \in G$. For $U \in \mathcal{F}(G)$, let $\mathsf{m}(U) = |\{g \in G \colon \mathsf{v}_g(U) = 5\}|$. We have to show that $\mathsf{m}(S) = 8$. We assume to the contrary $\mathsf{m}(S) \le 7$.

If $|S| \ge 42$, then there exists a subsequence S' of S of length 40 such that $\mathsf{m}(S') \le 5$, a contradiction to Proposition 6.3. Thus, we assume $|S| = 41$. Let $S' \mid S$ of length 40 such that $\mathsf{m}(S') = 6$. By Lemma 6.2.2 we know that $\mathsf{v}_h(\pi_3(S)) \le 5$ for each $h \in C_3^3$. Thus by Proposition 6.3 $\mathsf{v}_g(S') = \mathsf{v}_{g'}(S') = 4$ for distinct $g, g' \in C_6^3$. Consequently, $\mathsf{v}_g(S)$ or $\mathsf{v}_{g'}(S)$ is equal to 4, a contradiction to Theorem 1.3.1. $\square$

Finally, we are ready to prove Theorem 1.8.

Proof of Theorem 1.8. By Theorem 2.2.2 we known that $\mathsf{s}(C_n^3) \ge 8n-7$. We prove that $\mathsf{s}(C_n^3) \le 8n-7$. In view of Lemma 1.6, it suffices to prove the result for $a=1$; the general case follows by induction.

Thus, we have to prove that $\mathsf{s}(C_6^3) \le 41$. We assume to the contrary that $\mathsf{s}(C_6^3) \ge 42$. Let $S \in \mathcal{F}(C_6^3)$ such that $|S| = \mathsf{s}(C_6^3) - 1$ and S has no zero-sum subsequence of length 6. By Proposition 6.4 we have $S = T^5 R$ with $|T| = 8$ and $|R| \ge 1$. Let $g_0 \mid R$ and let $T = \prod_{i=1}^8 g_i$. Since $\pi_3(g_i^3)$ is a zero-sum subsequence of $\pi_3(S)$ for each $1 \le i \le 8$, it follows by Lemma 6.2.1 that $\pi_3(g_0 T^2)$ has no zero-sum subsequence of length 3, in particular $\mathrm{supp}(\pi_3(g_0T^2)) = \{\pi_3(g_i) \colon 0 \le i \le 8\}$ is a cap of cardinality 9. We note that $\sigma(g_i^3) = 3\pi_2(g_i) = \pi_2(g_i)$. Thus $|\{\pi_2(g_i) \colon 1 \le i \le 8\}| = 8$. Let $1 \le j \le 8$ such that $\pi_2(g_0) = \pi_2(g_j)$.

We consider the sequence $W = (\prod_{i=1}^8 \sigma(g_i^2)^2)\sigma(g_jg_0) \in \mathcal{F}(C_3^3)$. Since S has no zero-sum subsequence of length 6, W has no zero-sum subsequence of length 3. Thus, we have $\sigma(g_jg_0) \notin \{\sigma(g_i^2) \colon 1 \le i \le 8\}$ and $\{\sigma(g_jg_0)\} \cup \{\sigma(g_i^2) \colon 1 \le i \le 8\}$ is a cap in C_3^3 of cardinality 9. We observe that $\sigma(g_i^2) = -\pi_3(g_i)$ and thus by Lemma 6.1 we have $\sigma(g_jg_0) = -\pi_3(g_0)$. However, since $\sigma(g_jg_0) = \pi_3(g_j) + \pi_3(g_0)$, this implies $\pi_3(g_j) = -2\pi_3(g_0) = \pi_3(g_0)$, a contradiction.

Since $\mathsf{s}(C_n^3) - n + 1 \ge \eta(C_n^3) \ge 7n-6$, the result follows. $\square$

Acknowledgments

This work has been supported partially by NSFC with grant no. 10271080. This work was done while the last author was visiting the Center for Combinatorics, Nankai University, Tianjin. He is thankful to the center for providing excellent atmosphere for research and their hospitality. The penultimate author is supported by the FWF (P18779-N13).

References

1. N. Alon and M. Dubiner. A lattice point problem and additive number theory. *Combinatorica*, 15(3):301–309, 1995.

2. N. Alon, M. B. Nathanson, and I. Ruzsa. Adding distinct congruence classes modulo a prime. *Amer. Math. Monthly*, 102(3):250–255, 1995.

3. N. Alon, M. B. Nathanson, and I. Ruzsa. The polynomial method and restricted sums of congruence classes. *J. Number Theory*, 56(2):404–417, 1996.

4. J. Bierbrauer. Large caps. *J. Geom.*, 76:16–51, 2003.

5. R. Chi, S. Ding, W. Gao, A. Geroldinger, and W. A. Schmid. On zero-sum subsequences of restricted size. IV. *Acta Math. Hungar.*, 107(4):337–344, 2005.

6. J. A. Dias da Silva and Y. ould Hamidoune. Cyclic spaces for Grassmann derivatives and additive theory. *Bull. London Math. Soc.*, 26(2):140–146, 1994.

7. Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, and L. Rackham. Zero-sum problems in finite abelian groups and affine caps. *Quart. J. Math. Oxford Ser. (2)*, to appear. Preprint available at: `http://www.ma.rhul.ac.uk/~elsholtz/`

8. C. Elsholtz. Lower bounds for multidimensional zero sums. *Combinatorica*, 24(3):351–358, 2004.

9. P. Erdős, A. Ginzburg, and A. Ziv. Theorem in the additive number theory. *Bull. Res. Council Israel*, 10F:41–43, 1961.

10. P. Erdős and H. Heilbronn. On the addition of residue classes mod p. *Acta Arith.*, 9:149–159, 1964.

11. L. Gallardo, G. Grekos, L. Habsieger, F. Hennecart, B. Landreau, and A. Plagne. Restricted addition in $\mathbb{Z}/n\mathbb{Z}$ and an application to the Erdős-Ginzburg-Ziv problem. *J. London Math. Soc. (2)*, 65(3):513–523, 2002.

12. W. D. Gao. An addition theorem for finite cyclic groups. *Discrete Math.*, 163(1-3):257–265, 1997.

13. W. D. Gao. Note on a zero-sum problem. *J. Combin. Theory Ser. A*, 95(2):387–389, 2001.

14. W. D. Gao. On zero-sum subsequences of restricted size. II. *Discrete Math.*, 271(1-3):51–59, 2003.

15. W. D. Gao and A. Geroldinger. On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. *Integers*, 3:A8, 45 pp. (electronic), 2003.

16. W. D. Gao and A. Geroldinger. Zero-sum problems in finite abelian groups: a survey. *Expo. Math.*, 24(4):337–369, 2006.

17. W. D. Gao, A. Panigrahi, and R. Thangadurai. On the structure of p-zero-sum free sequences and its application to a variant of Erdös–Ginzburg–Ziv theorem. *Proc. Indian Acad. Sci. Math. Sci.*, 115(1):67–77, 2005.

18. W. D. Gao and R. Thangadurai. On the structure of sequences with forbidden zero-sum subsequences. *Colloq. Math.*, 98(2):213–222, 2003.

19. W. D. Gao and R. Thangadurai. A variant of Kemnitz conjecture. *J. Combin. Theory Ser. A*, 107(1):69–86, 2004.

20. W. D. Gao and Y. X. Yang. Note on a combinatorial constant. *J. Math. Res. Exposition*, 17(1):139–140, 1997.

21. A. Geroldinger and F. Halter-Koch. *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*. Chapman & Hall/CRC, 2006.

22. H. Harborth. Ein Extremalproblem für Gitterpunkte. *J. Reine Angew. Math.*, 262/263:356–360, 1973.

23. J. W. P. Hirschfeld. *Finite projective spaces of three dimensions*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1985.

24. A. Kemnitz. On a lattice point problem. *Ars Combin.*, 16(B):151–160, 1983.

25. M. B. Nathanson. *Additive number theory. Inverse problems and the geometry of sumsets.*, volume 165 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

26. C. Reiher. On Kemnitz' conjecture concerning lattice points in the plane. *Ramanujan J.*, 13(1-3):333–337, 2007.

27. W. A. Schmid and J. J. Zhuang. On short zero-sum subsequences over p-groups. *Ars Combin.*, to appear. Preprint available at:
`http://www.uni-graz.at/~wschmid/personal/research.html`

28. B. Sury and R. Thangadurai. Gao's conjecture on zero-sum sequences. *Proc. Indian Acad. Sci. Math. Sci.*, 112(3):399–414, 2002.

29. R. Thangadurai. Non-canonical extensions of Erdős-Ginzburg-Ziv theorem. *Integers*, 2:Paper A7, 14 pp. (electronic), 2002.