ACTA ARITHMETICA
128.3 (2007)

Inverse zero-sum problems

by

Weidong Gao (Tianjin), Alfred Geroldinger (Graz) and
Wolfgang A. Schmid (Graz)

1. Introduction. Let G be an additive finite abelian group with exponent $\exp(G) = n$. We define some central invariants in zero-sum theory: Let

- $\mathsf{D}(G)$ denote the smallest integer $l \in \mathbb{N}$ such that every sequence S over G of length $|S| \ge l$ has a zero-sum subsequence.
- $\eta(G)$ denote 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 $|T| \in [1, n]$.
- $\mathsf{s}(G)$ denote 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 $|T| = n$.

All these three invariants have been studied since the 1960s; this was initiated by the works of P. Erdős et al. (see [17, 36], and for more detailed historical information see [23, 24]). For groups of rank at most two the precise values of all three invariants are well known (see Theorem 2.4). In groups of higher rank precise values are known only in very special cases (see [10, 24, 3] and the introduction of Section 3).

The investigation of inverse problems has a long tradition in combinatorial number theory (see [34]), and more recently it has been promoted by applications in the theory of non-unique factorizations (see [30]). In the present paper we study the inverse problems associated to the above invariants. More precisely, we investigate the structure of sequences of length $\mathsf{D}(G) - 1$ (respectively $\eta(G) - 1$ or $\mathsf{s}(G) - 1$) that do not have a zero-sum subsequence (of the required length). For cyclic groups these questions are completely settled. Indeed, the answer for the invariants $\mathsf{D}(G)$ and $\eta(G)$ is straightforward (see Theorem 2.1), and the inverse problem for the invariant $\mathsf{s}(G)$, with G cyclic, gave rise to a great variety of investigations (see [5, 8, 18, 9, 19, 4, 38, 26, 31, 29]). In this paper we study the problems for

2000 *Mathematics Subject Classification*: 11P70, 11B50.

groups G of the form $G = C_n^r$, with $n, r \ge 2$, where the emphasis is laid on groups of rank two.

Consider the following two properties.

PROPERTY **C**. Every sequence S over G of length $|S| = \eta(G) - 1$ that has no zero-sum subsequence of length in $[1, n]$ has the form $S = T^{n-1}$ for some sequence T over G.

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

Property **C** was first considered by P. van Emde Boas and Property **D** by W. D. Gao (see [16, 21]). At the beginning of Section 3 we discuss the state of knowledge on these properties. In [24, Conjecture 7.2] it is conjectured that every group $G = C_n^r$, where $r \in \mathbb{N}$ and $n \in \mathbb{N}_{\ge 2}$, has Property **D**. In Theorem 3.2 we show that Properties **C** and **D** are both multiplicative, and thus this conjecture is essentially reduced to the case of elementary p-groups.

Let $G = C_n \oplus C_n$ with $n \ge 2$. It is conjectured that every minimal zero-sum sequence S over G of length $|S| = \mathsf{D}(G)$ contains some element with multiplicity $n - 1$ (for several equivalent conditions see [30, Theorem 5.8.7]). If this conjecture is true, then G has Property **C** (see [23, Theorem 6.2] and [24, Theorem 6.7.2(b)]). In Theorem 4.1 we show that, if $\varepsilon > 0$ and n is a sufficiently large prime, then such a sequence S contains one element with multiplicity greater than $n^{1/4-\varepsilon}$. The proof rests on a variety of addition theorems, among them the theorem of Dias da Silva–Hamidoune (which settles the Erdős–Heilbronn conjecture).

In Section 5 we study the analogue of Property **D** for sets (that is, for squarefree sequences) in $G = C_p \oplus C_p$, where p is a prime. W. D. Gao and R. Thangadurai proved that the maximal size of a set $S \subset C_p \oplus C_p$, for primes $p \ge 67$, without a subset of size p that sums to zero, is $2p - 2$ (see [28]). In Theorem 5.1 we completely determine the structure of all extremal sets, and moreover, we slightly improve the bound to $p \ge 47$. The proof of the inverse result is analogue to the proof of the direct result, but additionally employs some (recent) ideas from the study of Brakemeier's function due to A. Bialostocki and M. Lotspeich [5] and F. Hennecart [31] (see Lemma 5.9).

A crucial idea in all our work on groups of rank two is to find suitable epimorphisms to cyclic groups, to use results known for cyclic groups and then to shift the information back to the groups of rank two. We make use of classical results, such as the Cauchy–Davenport theorem, and list the other needed results on cyclic groups at the end of Section 2 (see Theorems 2.1 to 2.3). Of course we need the solutions of the original direct problems, which are summarized in Theorem 2.4.

Throughout this article, let G be an additive finite abelian group.

2. Notations and some main tools. Our notations and terminology are consistent with [24] and [30]. Here we briefly gather some key notions and fix the notations concerning sequences over finite abelian groups. 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 real numbers $a, b \in \mathbb{R}$ we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$, and we denote by $\lfloor a \rfloor$ the largest integer that is less than or equal to a, and by $\lceil a \rceil$ the smallest integer that is greater than or equal to a.

Throughout, all abelian groups will be written additively. For $n \in \mathbb{N}$, let C_n denote a cyclic group with n elements. We have

$$G \cong C_{n_1} \oplus \cdots \oplus C_{n_r},$$

where $r = \mathsf{r}(G) \in \mathbb{N}_0$ is the *rank* of G, $n_1, \ldots, n_r \in \mathbb{N}$ are integers with $1 < n_1 \,|\, \ldots \,|\, n_r$ and $n_r = \exp(G)$ is the exponent of G. Let $s \in \mathbb{N}$. An s-tuple $(e_1, \ldots, e_s)$ of elements of G is said to be *independent* if $e_i \neq 0$ for all $i \in [1, s]$ and, for every s-tuple $(m_1, \ldots, m_s) \in \mathbb{Z}^s$,

$$m_1 e_1 + \cdots + m_s e_s = 0 \quad \text{implies} \quad m_1 e_1 = \cdots = m_s e_s = 0.$$

An s-tuple $(e_1, \ldots, e_s)$ of elements of G is called a *basis* if it is independent and $G = \langle e_1 \rangle \oplus \cdots \oplus \langle e_s \rangle$.

Let $\mathcal{F}(G)$ be the free abelian monoid, multiplicatively written, with basis G. The elements of $\mathcal{F}(G)$ are called *sequences* over G. We write sequences $S \in \mathcal{F}(G)$ in the form

$$S = \prod_{g \in G} g^{\mathsf{v}_g(S)}, \qquad \text{with } \mathsf{v}_g(S) \in \mathbb{N}_0 \text{ for all } g \in G.$$

We call $\mathsf{v}_g(S)$ the *multiplicity* of g in S, and we say that S *contains* g if $\mathsf{v}_g(S) > 0$. Further, S is called *squarefree* if $\mathsf{v}_g(S) \le 1$ for all $g \in G$. The unit element $1 \in \mathcal{F}(G)$ is called the *empty sequence*. A sequence S_1 is called a *subsequence* of S if $S_1 \,|\, S$ in $\mathcal{F}(G)$ (equivalently, $\mathsf{v}_g(S_1) \le \mathsf{v}_g(S)$ for all $g \in G$), and it is called a *proper subsequence* of S if it is a subsequence with $1 \neq S_1 \neq S$. If a sequence $S \in \mathcal{F}(G)$ is written in the form $S = g_1 \cdot \ldots \cdot g_l$, we tacitly assume that $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G$.

For a sequence

$$S = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G),$$

we call

- $|S| = l = \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0$ the *length* of S,
- $\mathsf{h}(S) = \max\{\mathsf{v}_g(S) \mid g \in G\} \in [0, |S|]$ the *maximum of the multiplicities* of S,
- $\operatorname{supp}(S) = \{g \in G \mid \mathsf{v}_g(S) > 0\} \subset G$ the *support* of S,

- $\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g\in G} \mathsf{v}_g(S)g \in G$ the *sum* of S,
- $\Sigma_k(S) = \{\sum_{i\in I} g_i \mid I \subset [1,l] \text{ with } |I| = k\}$ the *set of k-term subsums* of S, for all $k \in \mathbb{N}$,
- $\Sigma_{\le k}(S) = \bigcup_{j\in[1,k]} \Sigma_j(S)$, $\Sigma_{\ge k}(S) = \bigcup_{j\ge k} \Sigma_j(S)$,
- $\Sigma(S) = \Sigma_{\ge 1}(S)$ the *set of (all) subsums* of S.

The sequence S is called

- *zero-sumfree* if $0 \notin \Sigma(S)$,
- a *zero-sum sequence* if $\sigma(S) = 0$,
- a *minimal zero-sum sequence* if it is a non-empty zero-sum sequence and every proper subsequence is zero-sumfree,
- a *short zero-sum sequence* if it is a zero-sum sequence of length $|S| \in [1, \exp(G)]$.

Throughout the paper, we tacitly use the following argument: If $g \in G$ with $\mathrm{ord}(g) = \exp(G) = n$, then $S = g_1 \cdot \ldots \cdot g_l$ has a zero-sum subsequence of length n if and only if the shifted sequence $S' = (g_1 - g) \cdot \ldots \cdot (g_l - g)$ has a zero-sum subsequence of length n.

Every group homomorphism $\varphi\colon G \to H$ extends to a homomorphism $\varphi\colon \mathcal{F}(G) \to \mathcal{F}(H)$ where $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_l)$. Obviously, $\varphi(S)$ is a zero-sum sequence if and only if $\sigma(S) \in \mathrm{Ker}(\varphi)$. If $m \in \mathbb{N}$, $m \,|\, n_1$ and $\varphi\colon G \to G$ is the multiplication by m (defined by $\varphi(g) = mg$ for every $g \in G$), then $\mathrm{Ker}(\varphi) \cong C_m^r$ and $\varphi(G) \cong C_{n_1/m} \oplus \cdots \oplus C_{n_r/m}$.

Now we gather the results on cyclic groups that will be needed throughout this paper.

THEOREM 2.1. *Let G be cyclic of order $n \ge 3$ and $S \in \mathcal{F}(G)$ a zero-sumfree sequence of length $|S| \ge (n+1)/2$. Then there exists some $g \in \mathrm{supp}(S)$ such that $\mathsf{v}_g(S) \ge 2|S| - n + 1$. In particular, $\mathsf{D}(G) = n$ and the following statements hold*:

(a) *If $|S| = n - 1$, then $S = g^{n-1}$.*
(b) *If $|S| = n - 2$, then either $S = g^{n-3}(2g)$ or $S = g^{n-2}$.*
(c) *If $|S| = n - 3$, then S has one of the following forms*:

$$g^{n-5}(2g)^2, \quad g^{n-4}(2g), \quad g^{n-4}(3g), \quad g^{n-3}.$$

Proof. This is due to J. D. Bovey, P. Erdős and I. Niven (see [7] for the original paper and also [30, Theorem 5.4.5.2]). ∎

THEOREM 2.2. *Let G be prime cyclic of order $p \in \mathbb{P}$ and $S \in \mathcal{F}(G)$.*

(1) *Let $\mathsf{v}_0(S) = 0$ and $|S| = p$. Then $\Sigma_{\le \mathsf{h}(S)}(S) = G$, and in particular, S has a zero-sum subsequence of length at least $p - \mathsf{h}(S)$.*
(2) *Let $k \in [2, p-1]$, $|S| \ge 2p - k$ and $\mathsf{h}(S) \le p - k$. Then S has a zero-sum subsequence of length p.*

(3) *Let $p \ge 13$, $\mathsf v_0(S) = 0$, $k \in [(p+5)/2, p-4]$, $|S| \ge 2p-k-2$ and $\mathsf h(S) \le k$. Then S has a zero-sum subsequence T of length $|T| \in [p+2-k, p-2]$.*

Proof. (1)&(2) See [28, Lemma 2.6 and Theorem 2.7].

(3) Clearly, S has a subsequence S' of length $|S'| = p$ and with $\mathsf h(S') \le k-2$. By (1), S' has a zero-sum subsequence T of length $|T| \ge p - \mathsf h(S') \ge p+2-k$. If $|T| \le p-2$, then we are done. If $|T| \ge p-1$, then $\mathsf h(T) \le p-4$ and Theorem 2.1 imply that T is not a minimal zero-sum subsequence. Thus it has a proper zero-sum subsequence T' of length $|T'| \in [(p-1)/2, p-2] \subset [p+2-k, p-2]$. ∎

THEOREM 2.3. *Let G be prime cyclic of order $p \in \mathbb P$, $S \in \mathcal F(G)$ a squarefree sequence and $k \in [1, |S|]$.*

(1) $|\Sigma_k(S)| \ge \min\{p, k(|S|-k)+1\}$.
(2) *If $k = \lfloor |S|/2 \rfloor$, then* $|\Sigma_k(S)| \ge \min\{p, (|S|^2+3)/4\}$.
(3) *If $|S| = \lfloor \sqrt{4p-7} \rfloor + 1$ and $k = \lfloor |S|/2 \rfloor$, then $\Sigma_k(S) = G$.*

Proof. This is due to J. A. Dias da Silva and Y. O. Hamidoune (see [11] for the original paper, and also [2] and [34, Theorems 3.4 and 3.8]). Obviously, (2) and (3) are special cases of (1), which will be needed repeatedly in this form. ∎

THEOREM 2.4. *Let $G = C_{n_1} \oplus C_{n_2}$ with $1 \le n_1 \mid n_2$. Then*

$$\mathsf s(G) = 2n_1 + 2n_2 - 3, \quad \eta(G) = 2n_1 + n_2 - 2, \quad \mathsf D(G) = n_1 + n_2 - 1.$$

Proof. The result on $\mathsf D(G)$ goes back to D. Kruyswijk and J. E. Olson, and the result on $\mathsf s(G)$ is based on C. Reiher's result that $\mathsf s(C_p \oplus C_p) = 4p-3$ (see [35] and [30, Theorem 5.8.3]). ∎

3. Properties C and D in groups of the form C_n^r. Let $G = C_n^r$ with $n \ge 2$, $r \in \mathbb N$ and suppose that Property **D** holds. Then, by definition, there exists some $c(G) \in \mathbb N$ such that $\mathsf s(G) = c(G)(n-1)+1$. Moreover, a simple argument shows that Property **C** holds (see [24, Section 7]) and that $\eta(G) = (c(G)-1)(n-1)+1$ (see [13, Lemma 2.3]). For $r = 1$ we have $c(G) = 2$ and for $r = 2$ we have $c(G) = 4$ (see Theorem 2.4). In the case of higher ranks bounds for $c(G)$ were given by N. Alon and M. Dubiner (see [1]) and then by Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham (see [32, 15, 13, 12]).

We make use of the simple fact that $\eta(C_2^r) = 2^r$ and $\mathsf s(C_2^r) = 2^r + 1$ (see [30, Corollary 5.7.6]). It follows from the very definition that C_2^r satisfies Property **D**, and a straightforward argument shows that C_3^r satisfies Property **D** (see [13, Lemma 2.3.3] and the subsequent discussion). However, in general only very little is known about Property **D**. If $r = 2$ and $n \in \{2, 3, 5, 7\}$, then G has Property **D** by [37], and for first results in groups

of higher rank we refer to [25]. Property **C** was first studied for groups of rank two in connection with investigations of the Davenport constant of groups having rank three (see [16, 20], and also [24, Theorem 7.9]).

Theorem 3.2 shows that both Property **C** and Property **D** are multiplicative, provided that the $c(\cdot)$ invariants of all involved groups coincide (in contrast to this assumption see the investigation of C_6^3 in [25]). This result generalizes earlier work (see [21] and [27, Theorem 1]), and reduces the conjecture that all groups of the form C_n^r satisfy the discussed properties to the case of elementary p-groups (under the above assumption on the $c(\cdot)$ invariants).

We start with a lemma that is used in the proof of the following theorem. It is closely related to [27, Theorem 2].

LEMMA 3.1. *Let $G = C_n^r$ with $n \ge 2$, $r \in \mathbb{N}$ and let $S \in \mathcal{F}(G)$ be a sequence of length $|S| = \eta(G) + n - 2$ that has no zero-sum subsequence of length n. If G has Property* **C** *and $\mathsf{h}(S) \ge \lfloor (n-1)/2 \rfloor$, then $S = T^{n-1}$ for some $T \in \mathcal{F}(G)$.*

Proof. Suppose that G has Property **C** and let $g \in G$ be such that $\mathsf{v}_g(S) \ge \lfloor (n-1)/2 \rfloor$. We assume $g = 0$ and set $S = 0^v T$ with $v = \mathsf{v}_0(S)$ and $T \in \mathcal{F}(G)$. Since S has no zero-sum subsequence of length n, it follows that T has no zero-sum subsequence of length in $[n - v, n]$.

Assume to the contrary that $v \le n-2$. Since $|T| \ge \eta(G) + (n-2) - v \ge \eta(G)$, T has a short zero-sum subsequence, and let T_1 be a short zero-sum subsequence of maximal length. Then we get

$$|T_1| \le n - 1 - v, \quad |T_1^{-1}T| \ge \eta(G) - 1.$$

Since $\mathsf{h}(T_1^{-1}T) \le \mathsf{h}(S) = v \le n-2$ and G has Property **C**, it follows that $T_1^{-1}T$ has a short zero-sum subsequence T_2. Since T_1 has maximal length, we deduce that $|T_1T_2| \ge n+1$ and hence

$$\frac{n+1}{2} \le |T_1| \le n - 1 - v < n - 1 - \frac{n-3}{2} = \frac{n+1}{2},$$

a contradiction.

Therefore we have $v = n-1$ and $|T| = \eta(G) - 1$. Since T has no short zero-sum subsequence and G has Property **C**, it follows that S has the required form. ∎

THEOREM 3.2. *Let $G = C_{mn}^r$ with $m, n, r \in \mathbb{N}$ and let $c \in \mathbb{N}$.*

(1) *If both C_m^r and C_n^r have Property* **D** *and*

$$\frac{\mathsf{s}(C_m^r) - 1}{m-1} = \frac{\mathsf{s}(C_n^r) - 1}{n-1} = \frac{\mathsf{s}(C_{mn}^r) - 1}{mn-1} = c,$$

then G has Property **D**.

(2) *If both* C_m^r *and* C_n^r *have Property* **C** *and*

$$\frac{\eta(C_m^r)-1}{m-1}=\frac{\eta(C_n^r)-1}{n-1}=\frac{\eta(C_{mn}^r)-1}{mn-1}=c,$$

then G *has Property* **C**.

(3) *If* C_m^r *has Property* **D**, C_n^r *has Property* **C**, $\mathsf{s}(C_n^r)=\eta(C_n^r)+n-1$ *and*

$$\frac{\mathsf{s}(C_m^r)-1}{m-1}=\frac{\mathsf{s}(C_n^r)-1}{n-1}=\frac{\mathsf{s}(C_{mn}^r)-1}{mn-1}=c,\qquad m\ge\frac{n^r\lfloor(n-1)/2\rfloor+c}{cn},$$

then G *has Property* **D**.

Proof. The proofs of all three assertions are based on the inductive method.

We need the following terminology. Let $k\in\mathbb{N}$, $\mathsf{s}(C_k^r)=c(k-1)+1$ and $S\in\mathcal{F}(C_k^r)$. We say that S is of *Type* **D** if $|S|=c(k-1)$, S has no zero-sum subsequence of length k, and $S=T^{k-1}$ for some $T\in\mathcal{F}(C_k^r)$. Thus the group C_k^r has Property **D** if and only if every sequence of length $c(k-1)$ that has no zero-sum subsequence of length n is of Type **D**. Similarly, if $\eta(C_k^r)=c(k-1)+1$ and $S\in\mathcal{F}(C_k^r)$, then we say that S is of *Type* **C** if $|S|=c(k-1)$, S has no short zero-sum subsequence, and $S=T^{k-1}$ for some $T\in\mathcal{F}(C_k^r)$. Again, the group C_k^r has Property **C** if and only if every sequence of length $c(k-1)$ that has no short zero-sum subsequence is of Type **C**.

Obviously we may assume that $m,n\ge 2$. Let $\varphi\colon G\to G$ denote the multiplication by m. Then $\mathrm{Ker}(\varphi)\cong C_m^r$ and $\varphi(G)=mG\cong C_n^r$.

(1) Let $S\in\mathcal{F}(G)$ be of length $|S|=c(mn-1)$ and such that S has no zero-sum subsequence of length mn. We have to show that S is of Type **D**. Since $\mathsf{v}_g(S)\le mn-1$ for every $g\in G$, it suffices to show that $|\mathrm{supp}(S)|=c$.

Since $|S|=n(c(m-1))+c(n-1)$, it follows that S admits a product decomposition

$$S=S_1\cdot\ldots\cdot S_{c(m-1)}S',$$

where $S_1,\ldots,S_{c(m-1)},S'\in\mathcal{F}(G)$ and, for every $i\in[1,c(m-1)]$, $\varphi(S_i)$ has sum zero and length $|S_i|=n$ (see [30, Lemma 5.7.10]). Since S has no zero-sum subsequence of length mn, $\varphi(S')$ has no zero-sum subsequence of length n. Clearly, we have

$$|\varphi(S')|=|S'|=|S|-nc(m-1)=c(n-1),$$

and thus $\varphi(S')$ is of Type **D**, whence in particular $|\mathrm{supp}(\varphi(S'))|=c$. We continue with the following assertion:

A1. $|\mathrm{supp}(\varphi(S))|=|\mathrm{supp}(\varphi(S'))|$.

Proof of **A1**. It suffices to verify that for every $i \in [1, c(m-1)]$ there is some $h \in \mathrm{supp}(\varphi(S'))$ such that $\varphi(S_i) = h^n$. Assume to the contrary that there is some $i \in [1, c(m-1)]$ for which this does not hold. We assert that $\varphi(S_i S')$ is divisible by a product of two zero-sum subsequences of length n. This implies that $\varphi(S)$ is divisible by a product of $c(m-1)+1$ zero-sum subsequences of length n, whence S has a zero-sum subsequence of length mn, a contradiction. We distinguish two cases.

Case 1: $\mathrm{supp}(\varphi(S')) \cap \mathrm{supp}(\varphi(S_i)) \neq \emptyset$. Pick h in $\mathrm{supp}(\varphi(S')) \cap \mathrm{supp}(\varphi(S_i))$. Then $h^n \,|\, \varphi(S_i S')$. Since $\varphi(S_i)$ is a zero-sum sequence of length n and distinct from h^n, it follows that $|\mathrm{supp}(h^{-1}\varphi(S_i))| \geq 2$. Therefore $h^{-n}\varphi(S_i S')$ is not of Type **D**, and thus it has a zero-sum subsequence of length n.

Case 2: $\mathrm{supp}(\varphi(S')) \cap \mathrm{supp}(\varphi(S_i)) = \emptyset$. Pick $h \in \mathrm{supp}(\varphi(S_i))$ and let U be a zero-sum subsequence of $h\varphi(S')$ of length n. Then $\mathsf{v}_h(U) \geq 1$ and $|\mathrm{supp}(h^{-1}U)| \geq 2$. Consequently, $\mathrm{supp}(U^{-1}h\varphi(S')) = \mathrm{supp}(\varphi(S'))$ and hence $|\mathrm{supp}((U^{-1}h\varphi(S'))(h^{-1}\varphi(S_i)))| > |\mathrm{supp}(\varphi(S'))|$. Therefore $U^{-1}\varphi(S_i S')$ is not of Type **D**, and thus it has a zero-sum subsequence of length n.

It remains to show that

$$|\varphi^{-1}(h) \cap \mathrm{supp}(S)| = 1 \quad \text{for every } h \in \mathrm{supp}(\varphi(S)),$$

since we then obtain

$$|\mathrm{supp}(S)| = |\mathrm{supp}(\varphi(S))| = |\mathrm{supp}(\varphi(S'))| = c.$$

Let $h \in \mathrm{supp}(\varphi(S_1 \cdot \ldots \cdot S_{c(m-1)}))$, and assume to the contrary that there are two distinct elements $g, g' \in \mathrm{supp}(S)$ such that $\varphi(g) = \varphi(g') = h$. By **A1** we may suppose that $g \,|\, S_1 \cdot \ldots \cdot S_{c(m-1)}$ and $g' \,|\, S'$, say $g \,|\, S_1$. Since S has no zero-sum subsequence of length mn, the sequence $\sigma(S_1) \cdot \ldots \cdot \sigma(S_{c(m-1)}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no zero-sum subsequence of length m, whence it is of Type **D**. We consider $S_1' = g^{-1}g'S_1$. Then $\varphi(S_1') = \varphi(S_1)$ and hence $\sigma(S_1) \neq \sigma(S_1') \in \mathrm{Ker}(\varphi)$. Thus the sequence $\sigma(S_1')\sigma(S_2) \cdot \ldots \cdot \sigma(S_{c(m-1)}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ is not of Type **D** (note that in case $m = 2$ we have $c = |\mathrm{Ker}(\varphi)|$), whence it has a zero-sum subsequence of length m, a contradiction.

It remains to verify that $\mathrm{supp}(\varphi(S)) = \mathrm{supp}(\varphi(S_1 \cdot \ldots \cdot S_{c(m-1)}))$. We set

$$c' = |\mathrm{supp}(\varphi(S_1 \cdot \ldots \cdot S_{c(m-1)}))| \quad \text{and check that} \quad c = c'.$$

By **A1** we have $|\mathrm{supp}(\varphi(S))| = c$ and the above argument shows that $|\mathrm{supp}(S_1 \cdot \ldots \cdot S_{c(m-1)})| = |\mathrm{supp}(\varphi(S_1 \cdot \ldots \cdot S_{c(m-1)}))|$. Thus it follows that

$$\begin{aligned} c(mn-1) = |S| &= \sum_{g \in \mathrm{supp}(S)} \mathsf{v}_g(S) = \sum_{g \in \mathrm{supp}(S_1 \cdot \ldots \cdot S_{c(m-1)})} \mathsf{v}_g(S) \\ &\quad + (|\mathrm{supp}(\varphi(S))| - |\mathrm{supp}(\varphi(S_1 \cdot \ldots \cdot S_{c(m-1)}))|)(n-1) \\ &\leq c'(mn-1) + (c-c')(n-1), \end{aligned}$$

whence

$$(c-c')(mn-1) \le (c-c')(n-1) \quad \text{and} \quad c = c'.$$

(2) Let $S \in \mathcal{F}(G)$ be of length $|S| = c(mn-1)$ such that S has no zero-sum subsequence of length in $[1, mn]$. We have to show that S is of Type **C**. Since $\mathsf{v}_g(S) \le mn-1$ for every $g \in G$, it suffices to show that $|\mathrm{supp}(S)| = c$.

Since $|S| = n(c(m-1)) + c(n-1)$, it follows that S admits a product decomposition

$$S = S_1 \cdot \ldots \cdot S_{c(m-1)} S',$$

where $S_1, \ldots, S_{c(m-1)}, S' \in \mathcal{F}(G)$ and, for every $i \in [1, c(m-1)]$, $\varphi(S_i)$ has sum zero and length $|S_i| \in [1, n]$ (see [30, Lemma 5.7.10]). Since S has no zero-sum subsequence of length in $[1, mn]$, $\varphi(S')$ has no zero-sum subsequence of length in $[1, n]$ and every sequence $\varphi(S_i)$ is a minimal zero-sum sequence. Clearly, we have

$$|\varphi(S')| = |S'| \ge |S| - nc(m-1) = c(n-1),$$

and thus in fact $|S_i| = n$ for every $i \in [1, c(m-1)]$ and furthermore $\varphi(S')$ is of Type **C**, whence in particular $|\mathrm{supp}(\varphi(S'))| = c$. We continue with the following assertion:

A2. $|\mathrm{supp}(\varphi(S))| = |\mathrm{supp}(\varphi(S'))|$.

Proof of **A2**. It suffices to verify that for every $i \in [1, c(m-1)]$ there is some $h \in \mathrm{supp}(\varphi(S'))$ such that $\varphi(S_i) = h^n$. Assume to the contrary that there is some $i \in [1, c(m-1)]$ for which this does not hold. We assert that $\varphi(S_i S')$ is divisible by a product of two zero-sum subsequences of length in $[1, n]$. This implies that $\varphi(S)$ is divisible by a product of $c(m-1)+1$ zero-sum subsequences of length in $[1, n]$, whence S has a zero-sum subsequence of length in $[1, mn]$, a contradiction. We distinguish two cases.

Case 1: $\mathrm{supp}(\varphi(S')) \cap \mathrm{supp}(\varphi(S_i)) \ne \emptyset$. We recall that $|\varphi(S_i)| = n$. The remaining argument is analogous to the corresponding one in (1).

Case 2: $\mathrm{supp}(\varphi(S')) \cap \mathrm{supp}(\varphi(S_i)) = \emptyset$. Pick $h \in \mathrm{supp}(\varphi(S_i))$ and let U be a zero-sum subsequence of $h\varphi(S')$ of length in $[1, n]$. If $|U| < n$, then

$$|U^{-1}\varphi(S_i S')| \ge |S'| + 1 = c(n-1) + 1 = \eta(C_n^r),$$

and therefore $U^{-1}\varphi(S_i S')$ has a zero-sum subsequence of length in $[1, n]$. Suppose that $|U| = n$, and note that $\mathsf{v}_h(U) \ge 1$ and $|\mathrm{supp}(h^{-1}U)| \ge 2$. This implies the equality $\mathrm{supp}(U^{-1}h\varphi(S')) = \mathrm{supp}(\varphi(S'))$ and thus we get $|\mathrm{supp}((U^{-1}h\varphi(S'))(h^{-1}\varphi(S_i)))| > |\mathrm{supp}(\varphi(S'))|$. Therefore $U^{-1}\varphi(S_i S')$ is not of Type **C**, and thus it has a zero-sum subsequence of length in $[1, n]$.

It remains to show that

$$|\varphi^{-1}(h) \cap \mathrm{supp}(S)| = 1 \quad \text{for every } h \in \mathrm{supp}(\varphi(S)),$$

since we then obtain

$$|\mathrm{supp}(S)| = |\mathrm{supp}(\varphi(S))| = |\mathrm{supp}(\varphi(S'))| = c.$$

Let $h \in \mathrm{supp}(\varphi(S_1 \cdot \ldots \cdot S_{c(m-1)}))$, and assume to the contrary that there are two distinct elements $g, g' \in \mathrm{supp}(S)$ such that $\varphi(g) = \varphi(g') = h$. By **A2** we may suppose that $g \mid S_1 \cdot \ldots \cdot S_{c(m-1)}$ and $g' \mid S'$, say $g \mid S_1$. Since S has no zero-sum subsequence of length in $[1, mn]$, the sequence $\sigma(S_1) \cdot \ldots \cdot \sigma(S_{c(m-1)}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ has no zero-sum subsequence of length in $[1, m]$, whence it is of Type **C**. We consider $S_1' = g^{-1}g'S_1$. Then $\varphi(S_1') = \varphi(S_1)$ and hence $\sigma(S_1) \neq \sigma(S_1') \in \mathrm{Ker}(\varphi)$. Thus the sequence $\sigma(S_1')\sigma(S_2) \cdot \ldots \cdot \sigma(S_{c(m-1)}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ is not of Type **C** (note that in case $m = 2$ we have $c = |\mathrm{Ker}(\varphi)| - 1$), whence it has a zero-sum subsequence of length in $[1, m]$, a contradiction.

It remains to verify that $\mathrm{supp}(\varphi(S)) = \mathrm{supp}(\varphi(S_1 \cdot \ldots \cdot S_{c(m-1)}))$. This is achieved as in (1) using **A2** instead of **A1**.

(3) Since C_2^r has Property **D**, C_4^r has Property **D** by (1). Furthermore, C_3^r has Property **D** as mentioned at the beginning of this section. Thus for $n \in [2, 4]$, the assertion follows from (1). Since $c(n-1) + 1 = \mathsf{s}(C_n^r) \geq 2^r(n-1) + 1$ (see [13, Proposition 3.1]), we have $c \geq 2$.

Let $n \geq 5$ and let $S \in \mathcal{F}(G)$ be of length $|S| = c(mn-1)$ and such that S has no zero-sum subsequence of length mn. We have to show that S is of Type **D**, and again it suffices to show that $|\mathrm{supp}(S)| = c$.

There exists some $h \in \varphi(G)$ such that

$$\mathsf{v}_h(\varphi(S)) \geq \frac{|S|}{|\varphi(G)|} = \frac{c(mn-1)}{n^r} \geq \left\lfloor \frac{n-1}{2} \right\rfloor$$

and then

$$|h^{-\lfloor (n-1)/2 \rfloor}\varphi(S)| \geq n(c(m-1)-1) + \mathsf{s}(C_n^r).$$

By [30, Lemma 5.7.10], S admits a product decomposition of the form

$$S = S_1 \cdot \ldots \cdot S_{c(m-1)}S',$$

where $S_1, \ldots, S_{c(m-1)}, S' \in \mathcal{F}(G)$, $h^{\lfloor (n-1)/2 \rfloor}$ divides $\varphi(S')$ and, for every $i \in [1, c(m-1)]$, $\varphi(S_i)$ has sum zero and length $|S_i| = n$. Since S has no zero-sum subsequence of length mn, it follows that $\varphi(S')$ has no zero-sum subsequence of length n. Thus Lemma 3.1 implies that $\varphi(S')$ is of Type **D**, whence in particular $|\mathrm{supp}(\varphi(S'))| = c$. We continue with the following assertion:

A3. $|\mathrm{supp}(\varphi(S))| = |\mathrm{supp}(\varphi(S'))|$.

Proof of **A3**. It suffices to verify that for every $i \in [1, c(m-1)]$ there is some $h \in \mathrm{supp}(\varphi(S'))$ such that $\varphi(S_i) = h^n$. Assume to the contrary that there is some $i \in [1, c(m-1)]$ for which this does not hold. We assert that $\varphi(S_iS')$ is divisible by a product of two zero-sum subsequences of length n. This implies that $\varphi(S)$ is divisible by a product of $c(m-1)+1$ zero-sum

subsequences of length n, whence S has a zero-sum subsequence of length mn, a contradiction. We distinguish two cases.

CASE 1: $\operatorname{supp}(\varphi(S')) \cap \operatorname{supp}(\varphi(S_i)) \neq \emptyset$. Pick h in $\operatorname{supp}(\varphi(S')) \cap \operatorname{supp}(\varphi(S_i))$. Then $h^n \mid \varphi(S_iS')$. Since $\varphi(S_i)$ is a zero-sum sequence of length n and distinct from h^n, it follows that $|\operatorname{supp}(h^{-1}\varphi(S_i))| \geq 2$. Therefore $h^{-n}\varphi(S_iS')$ is not of Type **D**. Since $c \geq 2$, $h^{-n}\varphi(S_iS')$ contains some element with multiplicity $n-1$, and thus by Lemma 3.1 it has a zero-sum subsequence of length n.

CASE 2: $\operatorname{supp}(\varphi(S')) \cap \operatorname{supp}(\varphi(S_i)) = \emptyset$. Pick h in $\operatorname{supp}(\varphi(S_i))$ and let U be a zero-sum subsequence of $h\varphi(S')$ of length n. Then $\mathsf{v}_h(U) \geq 1$ and $|\operatorname{supp}(h^{-1}U)| \geq 2$. Thus $\operatorname{supp}(U^{-1}h\varphi(S')) = \operatorname{supp}(\varphi(S'))$ and

$$|\operatorname{supp}((U^{-1}h\varphi(S'))(h^{-1}\varphi(S_i)))| > |\operatorname{supp}(\varphi(S'))|.$$

Therefore $U^{-1}\varphi(S_iS')$ is not of Type **D**. Since $c \geq 2$, $U^{-1}\varphi(S_iS')$ contains some element with multiplicity at least $(n-1)/2$, and thus by Lemma 3.1 it has a zero-sum subsequence of length n.

It remains to show that

$$|\varphi^{-1}(h) \cap \operatorname{supp}(S)| = 1 \quad \text{for every } h \in \operatorname{supp}(\varphi(S)),$$

since we then obtain

$$|\operatorname{supp}(S)| = |\operatorname{supp}(\varphi(S))| = |\operatorname{supp}(\varphi(S'))| = c.$$

This can be achieved as in (1) using **A3** instead of **A1**. ∎

4. Properties B and C in groups of rank two. Let $G = C_n \oplus C_n$ with $n \geq 2$. We say that G has *Property* **B** if every minimal zero-sum sequence $S \in \mathcal{F}(G)$ of length $|S| = \mathsf{D}(G) = 2n-1$ contains some element with multiplicity $n-1$. This property was first addressed in [22], and it is conjectured that every group (of the above form) satisfies Property **B**. We already mentioned in the Introduction that Property **B** implies Property **C**. Various characterizations and further consequences of Property **B** may be found in [30, Section 5.8]. Here we only recall the following two recent results. If $n \geq 6$ and G has Property **B**, then $C_{2n} \oplus C_{2n}$ has Property **B** (see [23, Theorem 8.1]). If $S \in \mathcal{F}(G)$ is a minimal zero-sum sequence of length $2n-1$ and with $|\operatorname{supp}(S)| = 3$, then it contains some element with multiplicity $n-1$ (see [33, Theorem 1]).

As a main result in this section we show that, in case n is a large prime, every minimal zero-sum sequence of length $2n-1$ contains one element with high multiplicity (cf. also [33, Theorem 3]). Let $S \in \mathcal{F}(G)$ be a sequence of length $\eta(G)-1$ that has no short zero-sum subsequence. If G has Property **C**, then obviously $\operatorname{ord}(g) = n$ for all $g \in \operatorname{supp}(S)$. In Theorem 4.6 we establish this consequence without assuming that Property **C** holds.

THEOREM 4.1. *Let $G = C_p \oplus C_p$ with $p \in \mathbb{P}$ and let $S \in \mathcal{F}(G)$. If $\varepsilon > 0$ and p is sufficiently large (in dependence on ε), then the following statements hold*:

(1) *If S has length $|S| = \mathsf{D}(G) - 1$ but no zero-sum subsequence, then $\mathsf{h}(S) > p^{1/4-\varepsilon}$.*
(2) *If S has length $|S| = \eta(G) - 1$ but no short zero-sum subsequence, then $\mathsf{h}(S) > p^{1/4-\varepsilon}$.*

By inspecting the proof of this result it can be noted that only in (4.7) does the size of p have to depend on that of ε. Though at some other places it is required that p is not too small, all these bounds are absolute and of a fairly moderate size. By some calculation it can be seen that the result holds for $p > \exp(-8\log(\varepsilon)/\varepsilon)$. Yet no effort was made to optimize the value of this constant.

We need a series of lemmas. For a prime $p \in \mathbb{P}$ we denote by $\mathbb{F}_p$ a field with p elements. The group $C_p \oplus C_p$ can be viewed as a vector space over $\mathbb{F}_p$. In particular, the notions of "independent elements" and "basis", as stated in Section 2, coincide with the notions of "linearly independent (over $\mathbb{F}_p$)" and "$\mathbb{F}_p$-basis".

LEMMA 4.2. *Let $G = C_p \oplus C_p$ with $p \in \mathbb{P}$, (e_1, e_2) a basis of G and*

$$S = \prod_{i=1}^{l} (a_i e_1 + b_i e_2) \in \mathcal{F}(G), \qquad \text{where } a_1, b_1, \ldots, a_l, b_l \in \mathbb{F}_p,$$

a zero-sumfree sequence of length $|S| = l \ge p$. Then

$$\Big|\Big\{ \sum_{i\in I} b_i \,\Big|\, \emptyset \ne I \subset [1,l] \text{ with } \sum_{i\in I} a_i = 0 \Big\}\Big| \ge l - p + 1.$$

Proof. The proof is based on recent results from the theory of coverings. We recall the required terminology. A subset $A \subset \mathbb{F}_p^l$ is called a *proper coset* if $A = a + N$ for some subspace $N \subset \mathbb{F}_p^l$ and some $a \in \mathbb{F}_p^l \setminus N$. For a subset $A \subset \mathbb{F}_p^l$ let $\mathsf{s}(A, \mathbb{F}_p^l)$ denote the smallest $s \in \mathbb{N}_0 \cup \{\infty\}$ such that $A \setminus \{0\}$ is contained in a union of s proper cosets.

Let $(X_1, \ldots, X_l)$ be an $\mathbb{F}_p$-basis of $\mathbb{F}_p^l$, and

$$D = \Big\{ \sum_{i\in I} X_i \,\Big|\, I \subset [1,l], \sum_{i\in I} a_i \ne 0 \Big\} \subset \mathbb{F}_p^l,$$

$$D_0 = \Sigma(X_1 \cdot \ldots \cdot X_l) \setminus D = \Big\{ \sum_{i\in I} X_i \,\Big|\, I \subset [1,l], \sum_{i\in I} a_i = 0 \Big\} \subset \mathbb{F}_p^l.$$

Then $\mathsf{s}(\Sigma(X_1 \cdot \ldots \cdot X_l), \mathbb{F}_p^l) = l$ by [30, Theorem 5.6.6] and $\mathsf{s}(D, \mathbb{F}_p^l) \le p - 1$ by [30, Lemma 5.6.7]. If $\theta \in \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_p^l, \mathbb{F}_p)$ is the unique homomorphism

satisfying $\theta(X_i) = b_i$ for all $i \in [1, l]$, then $0 \notin \Sigma(S)$ implies

$$0 \notin \theta(D_0) = \Big\{ \sum_{i \in I} b_i \,\Big|\, \emptyset \neq I \subset [1, l] \text{ with } \sum_{i \in I} a_i = 0 \Big\}.$$

Therefore [30, Lemma 5.6.2.1] implies that

$$|\theta(D_0)| \ge \mathsf{s}(D_0, \mathbb{F}_p^l) \ge \mathsf{s}(\Sigma(X_1 \cdot \ldots \cdot X_l), \mathbb{F}_p^l) - \mathsf{s}(D, \mathbb{F}_p^l) \ge l - (p-1). \blacksquare$$

LEMMA 4.3. *Let $G = C_p \oplus C_p$ with $p \in \mathbb{P}$ and let $S \in \mathcal{F}(G)$ be a zero-sumfree sequence of length $|S| = 2p-2$. Then any two distinct elements of* $\operatorname{supp}(S)$ *are independent.*

Proof. See [30, Corollary 5.6.9]. ∎

LEMMA 4.4. *Let $G = C_n \oplus C_n$ with $n \ge 2$ and $S \in \mathcal{F}(G)$.*

(1) *If $|S| = 3n-2$, then S has a zero-sum subsequence T of length $|T| \in \{n, 2n\}$.*
(2) *If $|S| = 3n-3$ and S has no short zero-sum subsequence, then S has a minimal zero-sum subsequence T of length $|T| = 2n-1$.*

Proof. (1) See [24, Theorem 6.7].

(2) Suppose that $|S| = 3n-3$ and S has no short zero-sum subsequence; set $W = 0S \in \mathcal{F}(G)$. Then (1) implies that W has a zero-sum subsequence U of length $|U| \in \{n, 2n\}$, and by our assumption on S we get $|U| = 2n$. If U is a subsequence of S, then $\mathsf{D}(G) = 2n-1$ implies that $U = U_1U_2$, where both U_1 and U_2 are non-empty zero-sum sequences. Therefore, either U_1 or U_2 is a short zero-sum subsequence of S, a contradiction. Therefore, $U = 0T$ with $|T| = 2n-1$, and since S has no short zero-sum subsequence, it follows that T is a minimal zero-sum sequence. ∎

Proof of Theorem 4.1. By Theorem 2.4 we have $\mathsf{D}(G) = 2p-1$ and $\eta(G) = 3p-2$. By Lemma 4.4 it suffices to prove the first assertion. Let (e_1, e_2) be a basis of G and, for $i \in [1, 2]$, let $\varphi_i \colon G \to \langle e_i \rangle$ denote the canonical projections. Let $\varepsilon > 0$, let p be sufficiently large and assume to the contrary that there exists a zero-sumfree sequence

$$S = \prod_{i=1}^{2p-2} (a_i e_1 + b_i e_2) \in \mathcal{F}(G), \quad \text{with } a_1, b_1, \ldots, a_{2p-2}, b_{2p-2} \in [0, p-1],$$

of length $|S| = 2p-2$ and with $\mathsf{h}(S) \le p^{1/4-\varepsilon}$. Let T denote a maximal squarefree subsequence of S and set $h = \mathsf{h}(\varphi_1(T))$. After renumbering if necessary we may assume that

$$T = \prod_{i=1}^{|T|} (a_i e_1 + b_i e_2), \quad a_1 = \cdots = a_h = a.$$

Now we set

$$W = \prod_{i=1}^{h}(ae_1 + b_ie_2), \quad S_1 = SW^{-1},$$

and distinguish three cases.

CASE 1: $h \ge \lfloor\sqrt{4p-7}\rfloor + 1$. We set $k = \lfloor\sqrt{4p-7}\rfloor + 1$, $l = \lfloor k/2\rfloor$ and

$$S_2 = \prod_{i=k+1}^{2p-2}(a_ie_1 + b_ie_2).$$

Theorem 2.3(3) implies that

$$\Sigma_l\Big(\prod_{i=1}^{k} b_ie_2\Big) = \langle e_2\rangle. \tag{4.1}$$

Consider the sequence $\varphi_1(S_2) = \prod_{i=k+1}^{2p-2} a_ie_1$. If $a_i = a_j = 0$ for some $i, j \in [k+1, 2p-2]$, then by Lemma 4.3 we obtain $b_i = b_j$. Therefore,

$$\mathsf{v}_0(\varphi_1(S_2)) \le \mathsf{h}(S)$$

and

$$\begin{aligned}|\varphi_1(S_2)| - \mathsf{v}_0(\varphi_1(S_2)) &= 2p-2-k-\mathsf{v}_0(\varphi_1(S_2))\\ &> 2p-2-\lfloor\sqrt{4p-7}\rfloor - 1 - p^{1/4} \ge p-1\end{aligned}$$

where the last inequality holds since $p \ge 11$. Thus Theorem 2.2(1) implies that $\Sigma(\varphi_1(S_2)) = \langle e_1\rangle$. In particular, S_2 has a non-empty subsequence S_3 such that $\sigma(\varphi_1(S_3)) = -lae_1$. By equation (4.1) there is a subset $I \subset [1,k]$ such that $\sum_{i\in I} b_ie_2 = -\sigma(\varphi_2(S_3))$ and $|I| = l$. Therefore, $S_3\prod_{i\in I}(ae_1+b_ie_2)$ is a non-empty zero-sum subsequence of S, a contradiction.

CASE 2: $5p^{1/4} \le h \le \lfloor\sqrt{4p-7}\rfloor$. We set $k = \lfloor h/2\rfloor$ and $h_1 = \mathsf{h}(\varphi_1(S_1))$. Theorem 2.3(2) implies that

$$\Big|\Sigma_k\Big(\prod_{i=1}^{h} b_ie_2\Big)\Big| \ge \frac{h^2+3}{4}, \tag{4.2}$$

and by the assumption of Case 2 we get

$$h_1 \le \mathsf{h}(\varphi_1(T))\mathsf{h}(S) < hp^{1/4}.$$

Therefore, since $p \ge 53$,

$$|\varphi_1(S_1)| - \mathsf{v}_0(\varphi_1(S_1)) \ge |S_1| - h_1 = 2p-2-h-h_1 > 2p-2-h-hp^{1/4} \ge p-1,$$

whence Theorem 2.2(1) implies

$$\Sigma_{\le h_1}(\varphi_1(S_1)) = \langle e_1\rangle.$$

In particular, S_1 has a non-empty subsequence S_4 such that

$$\sigma(\varphi_1(S_4)) = -kae_1, \quad |S_4| \le h_1. \tag{4.3}$$

By equations (4.2) and (4.3) we infer that

$$\sigma(S_4)+\Sigma_k(W)\subset\langle e_2\rangle,\quad |\sigma(S_4)+\Sigma_k(W)|\ge\frac{h^2+3}{4}. \tag{4.4}$$

Set $S_5=S(S_4W)^{-1}$. By Lemma 4.2,

$$|\Sigma(S_5)\cap\langle e_2\rangle|\ge|S_5|-p+1.$$

Therefore,

$$\begin{aligned}|\sigma(S_4)+\Sigma_k(W)|+|\Sigma(S_5)\cap\langle e_2\rangle|&\\ \ge\frac{h^2+3}{4}+|S_5|-p+1&=\frac{h^2+3}{4}+2p-2-|S_4|-|W|-p+1\\ \ge\frac{h^2+3}{4}+p-1-h_1-h&>\frac{h^2+3}{4}+p-1-hp^{1/4}-h\ge p,\end{aligned}$$

where the last inequality holds since $p\ge 5^4$. It follows from the Cauchy–Davenport theorem that

$$(\sigma(S_4)+\Sigma_k(W))+(\Sigma(S_5)\cap\langle e_2\rangle)=\langle e_2\rangle,$$

whence $0\in(\sigma(S_4)+\Sigma_k(W))+(\Sigma(S_5)\cap\langle e_2\rangle)\subset\Sigma(S)$, a contradiction.

Case 3: $h<5p^{1/4}$. Let $m=\lfloor 5p^{1/4}\rfloor$. Note that $|\mathrm{supp}(T)\cap(ae_1+\langle e_2\rangle)|=h$. Thus we may suppose that, for every subgroup $H\subset G$ with $|H|=p$ and every $g\in G$,

$$|\mathrm{supp}(T)\cap(g+H)|\le m, \tag{4.5}$$

since otherwise we choose a different basis (e_1',e_2') of G and are back to Case 1 or Case 2.

Let $\widehat{G}=\mathrm{Hom}(G,\mathbb{C}^\times)$ be the character group of G with complex values, $\chi_0\in\widehat{G}$ the principal character, and for any $\chi\in\widehat{G}$ let

$$f(\chi)=\prod_{i=1}^{2p-2}(1+\chi(a_ie_1+b_ie_2)).$$

Clearly, we have

$$f(\chi)=1+\sum_{g\in\Sigma(S)}c_g\chi(g),$$

where $c_g=|\{\emptyset\ne I\subset[1,2p-2]\mid\sum_{i\in I}(a_ie_1+b_ie_2)=g\}|$.

Since S is zero-sumfree, we have $0\notin\Sigma(S)$ and the Orthogonality Relations (see [30, Lemma 5.5.2]) imply that

$$\sum_{\chi\in\widehat{G}}f(\chi)=\sum_{\chi\in\widehat{G}}\Big(1+\sum_{g\in\Sigma(S)}c_g\chi(g)\Big)=|\widehat{G}|+\sum_{g\in\Sigma(S)}c_g\sum_{\chi\in\widehat{G}}\chi(g)=|G|.$$

Obviously, $f(\chi_0)=2^{|S|}$. Let $\chi\in\widehat{G}\setminus\{\chi_0\}$. We set $M=m\mathsf{h}(S)$ and

$$|S|=(2k-1)M+q\quad\text{with } q\in[0,2M-1],$$

and continue with the following assertion:

A1. $|f(\chi)| \le 2^{|S|}\exp(-\pi^2 r/2p^2)$ with $r = 2M(1^2+2^2+\cdots+(k-1)^2)+qk^2$.

Proof of **A1**. Let $j \in [-(p-1)/2,(p-1)/2]$ and $g \in G$ with $\chi(g) = \exp(2\pi ij/p)$. Note that for any real x with $|x| < \pi/2$, we have $\cos x \le \exp(-x^2/2)$. Thus

$$|1+\chi(g)| = 2\cos\left(\frac{\pi j}{p}\right) \le 2\exp\left(-\frac{\pi^2 j^2}{2p^2}\right). \tag{4.6}$$

If $H = \mathrm{Ker}(\chi)$, then $|H| = p$ and $g+H = \chi^{-1}(\exp(2\pi ij/p))$. Thus (4.5) implies that there are at most m elements $h \in \mathrm{supp}(S)$ such that $\chi(h) = \exp(2\pi ij/p)$. Consequently, the upper bound for $|f(\chi)|$, obtained by repeated application of (4.6), is maximal if the values $0, 1, -1, \ldots, k-1$, $-(k-1)$ are accepted M times each and the values $k, -k$ are accepted q times as images of $\chi(g)$ for $g \in \mathrm{supp}(S)$. Therefore

$$|f(\chi)| \le 2^{|S|}\exp(-\pi^2 r/2p^2).$$

Since $|S| = (2k-1)M+q$, we get $k = (2M)^{-1}(|S|-q+M)$ and hence

$$r = 2M\sum_{j=1}^{k-1} j^2 + qk^2 = 2M\,\frac{(k-1)k(2k-1)}{6} + qk^2$$

$$= \frac{(|S|-q-M)(|S|-q+M)(|S|-q)+3q(|S|-q+M)^2}{12M^2}.$$

Since $q \in [0, 2M-1]$ and $q \le |S|$, it follows that

$$r = \frac{|S|(|S|^2-M^2)}{12M^2} + \frac{q(2M-q)(2M+3|S|-2q)}{12M^2} \ge \frac{|S|(|S|^2-M^2)}{12M^2}.$$

We deduce that (here we need p sufficiently large)

$$\exp\left(\frac{\pi^2 r}{2p^2}\right) \ge \exp\left(\frac{\pi^2|S|(|S|^2-M^2)}{24M^2p^2}\right) > 2p^2. \tag{4.7}$$

Therefore it follows that

$$p^2 = |G| = \sum_{\chi\in\widehat{G}} f(\chi) \ge f(\chi_0) - \sum_{\chi\ne\chi_0}|f(\chi)|$$

$$\ge 2^{|S|}\left(1-(p^2-1)\exp\left(\frac{-\pi^2 r}{2p^2}\right)\right) > 2^{|S|}\left(1-\frac{p^2-1}{2p^2}\right) > 2^{|S|-1} > p^2,$$

a contradiction. ∎

The special case $T = 1$ of the following lemma may be found in [30, Proposition 5.7.11].

LEMMA 4.5. *Let $S \in \mathcal{F}(G)$ be a sequence, $H \subset G$ a subgroup and $T \in \mathcal{F}(H)$ a subsequence of S such that*

$$|S| \ge \exp(G/H)(\eta(H)-1)+\eta(G/H)-(\exp(G/H)-1)|T|.$$

Then S has a zero-sum subsequence S' of length $|S'| \in [1, \exp(H)\exp(G/H)]$.

Proof. If $|T| \ge \eta(H)$, then T (and hence S) has a zero-sum subsequence S' of length $|S'| \in [1, \exp(H)]$. Suppose that $|T| < \eta(H)$, and let $\varphi\colon G \to G/H$ denote the canonical epimorphism. Since the sequence $T^{-1}S$ has length

$$|T^{-1}S| \ge \exp(G/H)(\eta(H) - |T| - 1) + \eta(G/H),$$

it admits a product decomposition of the form $T^{-1}S = T_1 \cdot \ldots \cdot T_{\eta(H)-|T|}T'$, where $T_1, \ldots, T_{\eta(H)-|T|}, T' \in \mathcal{F}(G)$ and, for every $i \in [1, \eta(H) - |T|]$, $\varphi(T_i)$ has sum zero and length $|T_i| \in [1, \exp(G/H)]$ (see [30, Lemma 5.7.10]). Then the sequence $T\sigma(T_1) \cdot \ldots \cdot \sigma(T_{\eta(H)-|T|}) \in \mathcal{F}(H)$ has a short zero-sum subsequence V, say

$$V = T_0 \prod_{i \in I} \sigma(T_i), \quad \text{where } T_0 \,|\, T \text{ and } I \subset [1, \eta(H) - |T|].$$

Thus the sequence

$$S' = T_0 \prod_{i \in I} T_i$$

is a zero-sum subsequence of S of length $|S'| \le |T_0| + |I| \exp(G/H) \le \exp(H) \exp(G/H)$. ∎

THEOREM 4.6. *Let $G = C_n \oplus C_n$ with $n \ge 2$ and $S \in \mathcal{F}(G)$. If there is some subsequence T of S and some divisor m of n such that $\mathrm{ord}(g) \,|\, m$ for every $g \in \mathrm{supp}(T)$ and*

$$|S| \ge 3n - 2 - \left(\frac{n}{m} - 1\right)|T|,$$

then S has a short zero-sum subsequence. In particular, if S has length $|S| = 3n - 3$ but no short zero-sum subsequence, then $\mathrm{ord}(g) = n$ for every $g \in \mathrm{supp}(S)$.

Proof. Let T and m be as above, and let $\varphi\colon G \to G$ denote the multiplication by m. Then $H = \mathrm{Ker}(\varphi) \cong C_m^2$, $G/H \cong C_{n/m}^2$ and $T \in \mathcal{F}(H)$. By Theorem 2.4 we infer that

$$\begin{aligned} |S| &\ge 3n - 2 - \left(\frac{n}{m} - 1\right)|T| = \frac{n}{m}(3m - 3) + \left(3\frac{n}{m} - 2\right) - \left(\frac{n}{m} - 1\right)|T| \\ &= \frac{n}{m}(\eta(C_m^2) - 1) + \eta(C_{n/m}^2) - \left(\frac{n}{m} - 1\right)|T|. \end{aligned}$$

Thus Lemma 4.5 implies that S has a short zero-sum subsequence.

Let $|S| = 3n-3$ and $g \in \mathrm{supp}(S)$. If S has no short zero-sum subsequence, then $|S| = 3n - 3 < 3n - 2 - (n/\mathrm{ord}(g) - 1)$ implies that $\mathrm{ord}(g) = n$. ∎

5. Extremal zero-sumfree subsets in $C_p \oplus C_p$. Let $\mathsf{g}(G)$ denote 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 $|T| = \exp(G)$.

Some elementary properties of $\mathsf{g}(G)$ are outlined in [24, Section 10], and a (straightforward) connection with Property **D** (for groups of the form C_n^r) may be found in [13, Lemma 2.3]. Moreover, if G is a vector space over a finite field, then the invariant $\mathsf{g}(G)$ allows an interpretation in finite geometry. Indeed, $\mathsf{g}(C_3^r) - 1$ is the maximal size of a cap in $\mathrm{AG}(r, 3)$ (see [13, Lemma 5.2] and also [25, Section 5.2]), and in this connection it found a lot of attention by finite geometers (see [14, 6] and the literature cited there).

In [28] it is conjectured that $\mathsf{g}(C_n \oplus C_n)$ is equal to $2n-1$ for every odd $n \ge 3$ and equal to $2n+1$ for every even $n \ge 3$, and it is observed that these values are lower bounds. Moreover, it is proved (see [28, Theorem 1]) that $\mathsf{g}(C_p \oplus C_p) = 2p-1$ for all primes $p \ge 67$. Now Theorem 5.1 completely solves the associated inverse problem by giving an explicit characterization of all squarefree sequences of length $2p-2$ without a zero-sum subsequence of length p.

First we give a proof of Theorem 5.1 which is based on the following Proposition 5.2. Note that for the implication (b)⇒(a) we need no assumption on the size of the prime p. We also outline how the inverse result gives back the direct result that $\mathsf{g}(G) = 2p-1$. Then the main work will be to derive Proposition 5.2. If $G = C_p \oplus C_p$ for some prime $p \in \mathbb{P}$ and $H \subset G$ is a subgroup of order p, then a homomorphism $\varphi\colon G \to H$ is called a *projection* if $\varphi|H = \mathrm{id}_H$ and $G = H \oplus \mathrm{Ker}(\varphi)$.

THEOREM 5.1. *Let $G = C_p \oplus C_p$ for some $p \in \mathbb{P}$ with $p \ge 47$ and let $S \in \mathcal{F}(G)$ be a squarefree sequence of length $|S| = 2p-2$. Then the following statements are equivalent*:

(a) *S has no zero-sum subsequence of length p.*

(b) *There exists a subgroup $K \subset G$ of order p such that one of the following conditions is satisfied*:

(b1) $\mathrm{supp}(S) = \{g, h\} + K \setminus \{g + k_1, h + k_2\}$,

(b2) $\mathrm{supp}(S) = (\{g, h\} + K \setminus \{g + k_1, g + k_1', h + k_2\}) \cup \{2g - h + k_1 + k_1' - k_2\}$,

(b3) $\mathrm{supp}(S) = (\{g, h\} + K \setminus \{g + k_1, g + k_1', h + k_2, h + k_2'\}) \cup \{2g - h + k_1 + k_1' + k_2^{(\prime)}, 2h - g + k_2 + k_2' + k_1^{(\prime)}\}$,

where $g, h \in G$ with $g + K \ne h + K$ and $k_1, k_1', k_2, k_2' \in K$ with $k_i \ne k_i'$ and $k_i^{(\prime)} \in \{k_i, k_i'\}$ for $i \in \{1, 2\}$.

In particular, we have $\mathsf{g}(G) = 2p-1$.

PROPOSITION 5.2. *Let $G = C_p \oplus C_p$ for some $p \in \mathbb{P}$ with $p \ge 47$ and let $S \in \mathcal{F}(G)$ be a squarefree sequence of length $|S| = 2p-2$ that has no zero-sum subsequence of length p. Then there exist a subgroup $H \subset G$ of order p, a projection $\varphi\colon G \to H$ and distinct elements $g, h \in H$ such that*

$\varphi(S)$ has one of the following forms:

$$g^{p-1}h^{p-1}, \quad g^{p-2}h^{p-1}(2g-h) \quad \text{or} \quad g^{p-2}h^{p-2}(2g-h)(2h-g).$$

Proof of Theorem 5.1 (using Proposition 5.2). (a)⇒(b). By Proposition 5.2 there exists a subgroup $H \subset G$ of order p and a projection $\varphi\colon G \to H$ such that $\varphi(S)$ has one of the indicated forms. Then $G = H \oplus K$ with $K = \mathrm{Ker}(\varphi)$. If $\varphi(S) = g^{p-1}h^{p-1}$ with distinct elements $g, h \in H$, then obviously

$$\mathrm{supp}(S) = (g+K) \cup (h+K) \setminus \{g+k_1, h+k_2\} \quad \text{for some } k_1, k_2 \in K.$$

The remaining cases are similar (cf. the proof of (b)⇒(a) below).

(b)⇒(a). Assume to the contrary that S has a zero-sum subsequence T of length $|T| = p$. Without restriction we may assume that $h = 0$. Then $g \notin K$, $G = \langle g\rangle \oplus K$ and let $\varphi\colon \langle g\rangle \oplus K \to \langle g\rangle$ denote the canonical projection. Clearly, $\varphi(T)$ is a zero-sum subsequence of $\varphi(S)$ of length p.

If (b1) holds, then $\varphi(S) = g^{p-1}0^{p-1}$. This sequence has no zero-sum subsequence of length p, a contradiction.

If (b2) holds, then $\varphi(S) = g^{p-2}0^{p-1}(2g)$ and $\varphi(T) = g^{p-2}0(2g)$. Let $k' \in \mathrm{supp}(T)$ with $\varphi(k') = 0$. We have $(\mathrm{id} - \varphi)(T) = (\prod_{k \in K \setminus \{k_1, k_1'\}} k)k'(k_1 + k_1' - k_2)$. Since $\sigma(T) = 0$ it follows that $0 = \sigma((\mathrm{id} - \varphi)(T)) = (-k_1 - k_1') + k' + (k_1 + k_1' - k_2)$, whence $k' = k_2$, a contradiction to $k_2 \notin \mathrm{supp}(S)$.

If (b3) holds, then $\varphi(S) = g^{p-2}0^{p-2}(2g)(-g)$ and $\varphi(T) = g^{p-2}0(2g)$ or $\varphi(T) = g0^{p-2}(-g)$. First, suppose that $\varphi(T) = g^{p-2}0(2g)$. Let $k' \in \mathrm{supp}(T)$ with $\varphi(k') = 0$. We have $(\mathrm{id} - \varphi)(T) = (\prod_{k \in K \setminus \{k_1, k_1'\}} k)k'(k_1 + k_1' - k_2^{(\prime)})$. It follows that $0 = \sigma((\mathrm{id} - \varphi)(T)) = (-k_1 - k_1') + k' + (k_1 + k_1' - k_2^{(\prime)})$, whence $k' = k_2^{(\prime)}$, a contradiction.

Now, suppose that $\varphi(T) = g0^{p-2}(-g)$. Let $k' \in \mathrm{supp}(T)$ with $\varphi(k') = g$. We have $(\mathrm{id} - \varphi)(T) = (\prod_{k \in K \setminus \{k_2, k_2'\}} k)k'(k_2 + k_2' - k_1^{(\prime)})$. It follows that $0 = \sigma((\mathrm{id} - \varphi)(T)) = (-k_2 - k_2') + k' + (k_2 + k_2' - k_1^{(\prime)})$, whence $k' = k_1^{(\prime)}$, a contradiction.

It remains to verify the additional statement, and for that it suffices to prove that $\mathsf{g}(G) \le 2p-1$. Let $R \in \mathcal{F}(G)$ be a squarefree sequence of length $|R| = 2p-1$, and assume to the contrary that R has no zero-sum subsequence of length p. Let T be a subsequence of R of length $|T| = 2p-2$. By (b), there exist a subgroup $K_T \subset G$ of order p and two elements $g_T, h_T \in G$ such that, for $A_T = \mathrm{supp}(T) \cap (g_T + K_T)$ and $B_T = \mathrm{supp}(T) \cap (h_T + K_T)$, we have

$$|A_T| \ge p-2, \quad |B_T| \ge p-2, \quad g_T - h_T \notin K_T.$$

Next we verify that K_T, g_T and h_T are independent of T. Let T' be a subsequence of R of length $|T'| = 2p-2$. Then $|A_{T'} \cap A_T| \ge 2$ or $|A_{T'} \cap B_T|$

≥ 2, since otherwise we would have

$$\begin{aligned}|A_{T'}| &= |A_T \cup A_{T'} \cup B_T| - |A_T| - |B_T| + |A_{T'} \cap A_T| + |A_{T'} \cap B_T| \\ &\le (2p-1) - (p-2) - (p-2) + 1 + 1 = 5 < p-2,\end{aligned}$$

a contradiction. Hence, $|A_{T'} \cap A_T| \ge 2$ or $|A_{T'} \cap B_T| \ge 2$. This implies that $K_T = K_{T'}$, and we set $K = K_T$. If there are three distinct elements in $\{g_T, h_T, g_{T'}, h_{T'}\}$, then

$$2p-1 = |\mathrm{supp}(R)| \ge 3(p-2), \quad \text{a contradiction.}$$

Therefore it follows that $\{g_T, h_T\} = \{g_{T'}, h_{T'}\}$, and we set $\{g, h\} = \{g_T, h_T\}$.

Thus for every subsequence T of R of length $|T| = 2p-2$ we have

$$|\mathrm{supp}(T) \cap (g+K)| \ge p-2, \quad |\mathrm{supp}(T) \cap (h+K)| \ge p-2, \quad g-h \notin K.$$

This implies that $|\mathrm{supp}(R) \cap (g+K)| \ge p-1$ and $|\mathrm{supp}(R) \cap (h+K)| \ge p-1$. Without restriction we may suppose that $h = 0$. Since by assumption R has no zero-sum subsequence of length p, we infer that

$$|\mathrm{supp}(R) \cap K| = |\mathrm{supp}(R) \cap (g+K)| = p-1$$

and

$$R = (mg + g_p) \prod_{i=1}^{p-1} k_i \prod_{i=1}^{p-1} (g + g_i),$$

where $k_i \in K$ for every $i \in [1, p-1]$, $g_i \in K$ for every $i \in [1, p]$ and $m \in [2, p-1]$. Theorem 2.3 and the Cauchy–Davenport theorem imply

$$\begin{aligned}&\Big|\Sigma_{m-1}\Big(\prod_{i=1}^{p-1} k_i\Big) + \Sigma_{p-m}\Big(\prod_{i=1}^{p-1} g_i\Big)\Big| \\ &\ge \min\{p, ((m-1)(p-m)+1) + ((p-m)(p-1-(p-m))+1) - 1\} = p,\end{aligned}$$

and hence there are some $I \subset [1, p-1]$ with $|I| = m-1$ and some $J \subset [1, p-1]$ with $|J| = p-m$ such that

$$(mg + g_p) \prod_{i \in I} k_i \prod_{j \in J} (g + g_j)$$

is a zero-sum subsequence of R of length p, a contradiction. ∎

The rest of this section is devoted to the proof of Proposition 5.2. It is based on a series of lemmas, and its strategy can be seen best by browsing through the (short) *Proof of Proposition 5.2* at the very end of the section. We fix our notations which remain valid throughout what follows:

Let $G = C_p \oplus C_p$ for some odd prime $p \in \mathbb{P}$, $H \subset G$ a subgroup of order p, $\varphi\colon G \to H$ a projection and let $S \in \mathcal{F}(G)$ be a squarefree sequence.

LEMMA 5.3.

(1) *If $\varphi(S)$ has a zero-sum subsequence T such that*

$$\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \ge p-1\,,$$

then S has a zero-sum subsequence T^* of length $|T^*| = |T|$.

(2) *If $|S| = 2p-2$ and $\mathsf{h}(\varphi(S)) \in [(p+5)/2, p-4]$, then S has a zero-sum subsequence of length p.*

(3) *If $\mathsf{h}(\varphi(S)) \ge p$, then S has a zero-sum subsequence of length p.*

Proof. (1) See [25, Lemma 5.2].

(2) Let $g \in \operatorname{supp}(\varphi(S))$ with $\mathsf{v}_g(\varphi(S)) = \mathsf{h}(\varphi(S)) = h$. We assume $g = 0$ and set $\varphi(S) = 0^h T$. By Theorem 2.2(3) the sequence T has a zero-sum subsequence R of length $|R| \in [p+2-h, p-2]$. Now the assertion follows from (1), applied with $T = 0^{p-|R|}R$.

(3) Let T be a subsequence of S such that $\varphi(T) = g^p$. Since $K = \operatorname{Ker}(\varphi) \subset G$ is a subgroup of order p and T is squarefree, it follows that $T = \prod_{k\in K}(g+k)$ and hence $\sigma(T) = 0$. ∎

LEMMA 5.4. *Let $p \ge 7$, $|S| = 2p-2$ and $\mathsf{h}(\varphi(S)) = p-1$. If S has no zero-sum subsequence of length p, then there exist distinct elements $g, h \in H$ such that*

$$\varphi(S) = g^{p-1}h^{p-1} \quad \text{or} \quad \varphi(S) = g^{p-2}h^{p-1}(2g-h).$$

Proof. Let $h \in \operatorname{supp}(\varphi(S))$ with $\mathsf{v}_h(\varphi(S)) = \mathsf{h}(\varphi(S))$. We assume $h = 0$ and set $\varphi(S) = 0^{p-1}T$. If T is zero-sumfree or a minimal zero-sum sequence, then Theorem 2.1 implies that $\varphi(S)$ has the required form. If T has a zero-sum subsequence R of length $|R| \in [3, p-2]$, then $0^{p-|R|}R$ is a zero-sum subsequence of $\varphi(S)$ of length p, and hence, by Lemma 5.3(1), S has a zero-sum subsequence of length p. Thus it remains to consider the case that all zero-sum subsequences R of T have length $|R| = 2$ and $R^{-1}T$ is zero-sumfree. Let R be such a sequence, say $R = (-g)g$ for some $g \in H$. Since $R^{-1}T$ is a zero-sumfree sequence of length $p-3$, Theorem 2.1 implies that there is some $e \in H$ such that $R^{-1}T$ has one of the following forms: e^{p-3}, $e^{p-4}(2e)$, $e^{p-4}(3e)$ or $e^{p-5}(2e)^2$. Since T has no zero-sum subsequence of length greater than 2, it follows that $e \in \{-g, g\}$. Now we again apply Lemma 5.3(1) with $0^{p-|R|}R$ and infer that S has a zero-sum subsequence of length p. ∎

LEMMA 5.5. *Let $p \ge 11$, $|S| = 2p-2$ and $\mathsf{h}(\varphi(S)) = p-2$. If S has no zero-sum subsequence of length p, then there exist distinct elements $g, h \in H$ such that $\varphi(S) = g^{p-2}h^{p-2}(-g+2h)(2g-h)$.*

Proof. Let $h \in \operatorname{supp}(\varphi(S))$ with $\mathsf{v}_h(\varphi(S)) = \mathsf{h}(\varphi(S))$. We assume $h = 0$ and set $\varphi(S) = 0^{p-2}T$. If T has a zero-sum subsequence R of length $|R| \in$

$[4, p-2]$, then S has a zero-sum subsequence of length p by Lemma 5.3(1). Suppose that T has no such zero-sum subsequences, and let R denote a zero-sum subsequence of T of maximal length. We distinguish two cases.

Case 1: $|R| \ge p-1$. We may assume that R is a minimal zero-sum subsequence, since otherwise there exists a zero-sum subsequence of length in $[4, p-2]$. Since $\mathsf{h}(\varphi(S)) = p-2$, Theorem 2.1 implies that $R = e^{p-2}(2e)$ for some $e \in H$. Let $g \in H$ be such that $T = Rg$. We note that $g \neq e$. If $g \notin \{-e, -2e\}$, it follows that T has a zero-sum subsequence of length in $[4, p-2]$, a contradiction. If $g = -2e$, then $(-2e)e^2 0^{p-3}$ is a zero-sum subsequence of $\varphi(S)$ of length p, and Lemma 5.3(1) implies that S has a zero-sum subsequence of length p. If $g = -e$, then $\varphi(S)$ has the asserted form.

Case 2: $|R| \le 3$. Suppose that $|R| = 2$, say $R = (-g)g$ for some $g \in H$. Then $R^{-1}T$ is a zero-sumfree sequence of length $p-2$ and thus by Theorem 2.1 equal to $e^{p-3}(2e)$ or e^{p-2} for some $e \in H$. Note that in the latter case necessarily $g \neq e$. However, this implies that the sequence T has a zero-sum subsequence of length greater than 2, a contradiction. Thus we obtain $|R| = 3$. The sequence $R^{-1}T$ is a zero-sumfree sequence of length $p-3$. By Theorem 2.1 there exists some $e \in H$ such that $R^{-1}T$ has one of the following forms: $e^{p-5}(2e)^2$, $e^{p-4}(2e)$, $e^{p-4}(3e)$, or e^{p-3}. If there exists some $g \in \operatorname{supp}(R)$ such that $g \notin \{-2e, -e, e, 2e\}$, then there exists a zero-sum subsequence of T of length greater than 3, a contradiction. If $-2e \in \operatorname{supp}(R)$, then $(-2e)e^2 0^{p-3}$ is a zero-sum subsequence of $\varphi(S)$ of length p, and Lemma 5.3(1) implies that S has a zero-sum subsequence of length p. Therefore we deduce that $\operatorname{supp}(R) \subset \{-e, e, 2e\}$, $R = (2e)(-e)^2$ and thus $(-e)^2e^2$ is a zero-sum subsequence of T of length 4, a contradiction. ∎

Lemma 5.6. *Let $p \ge 11$, $|S| = 2p-2$ and $\mathsf{h}(\varphi(S)) = p-3$. Then S has a zero-sum subsequence of length p.*

Proof. Let $h \in \operatorname{supp}(\varphi(S))$ with $\mathsf{v}_h(\varphi(S)) = \mathsf{h}(\varphi(S))$. We assume $h = 0$ and set $\varphi(S) = 0^{p-3}T$. Let R be a zero-sum subsequence of T of maximal length. If $|R| \in [5, p-2]$, the result follows by Lemma 5.3(1). If $|R| \ge p-1$, then we may assume that R is a minimal zero-sum subsequence. However, since $\mathsf{h}(\varphi(S)) = p-3$ this is impossible by Theorem 2.1.

It remains to consider the case that $|R| \le 4$. Since R has maximal length, $R^{-1}T$ is zero-sumfree. Since $\mathsf{h}(\varphi(S)) = p-3$, we have $|T| = p+1$, and thus Theorem 2.1 implies that $|R| \ge 3$. We distinguish two cases.

Case 1: $|R| = 3$. By Theorem 2.1 we have $R^{-1}T = e^{p-3}(2e)$. We note that $\operatorname{supp}(R) \not\subset \{-e, -2e\}$. However, this implies that there exists a zero-sum subsequence of T of length greater than 3.

CASE 2: $|R| = 4$. The sequence $R^{-1}T$ is a zero-sumfree sequence of length $p-3$. By Theorem 2.1 it is equal to e^{p-3}, $e^{p-4}(2e)$, $e^{p-4}(3e)$, or $e^{p-5}(2e)^2$ for some $e \in H$. Since T has no zero-sum subsequence of length greater than 4, we infer that $\mathrm{supp}(R) \subset \{-3e, -2e, -e, e, 2e\}$. If $-3e \in \mathrm{supp}(R)$, then $(-3e)e^3 0^{p-4}$ is a zero-sum subsequence of $\varphi(S)$ of length p, and the assertion follows by Lemma 5.3(1). Thus, we may assume $\mathrm{supp}(R) \subset \{-2e, -e, e, 2e\}$. If $(-2e)^2 \mid R$, then $(-2e)^2 e^4$ is a zero-sum subsequence of T of length 6. Therefore R is equal to $(-2e)(-e)(2e)e$ or to $(-e)^2 e^2$, and in both cases we have $\mathsf{v}_e(R) > 0$. Applying Lemma 5.3(1) with $R0^{p-4}$ we conclude that S has a zero-sum subsequence of length p. ∎

In all the remaining lemmas we use the following notation:

Let

$$\varphi(S) = R'R^3U^2V \quad \textit{where } R', R, U, V \in \mathcal{F}(H),$$

R, U, V *are squarefree*, $\mathrm{supp}(V)$ *consists of those elements* $h \in H$ *with* $\mathsf{v}_h(\varphi(S)) = 1$, $\mathrm{supp}(U)$ *of those* $h \in H$ *with* $\mathsf{v}_h(\varphi(S)) = 2$ *and* $\mathrm{supp}(R)$ *of those* $h \in H$ *with* $\mathsf{v}_h(\varphi(S)) \ge 3$.

LEMMA 5.7. *Let* $p \ge 5$, $|\mathrm{supp}(\varphi(S))| \le (p+3)/2$ *and suppose that* $R'RUV$ *has a zero-sum subsequence of length* p. *Then* S *has a zero-sum subsequence of length* p.

Proof. Let W be a zero-sum subsequence of $R'RUV$ of length p. We set $W = W_1W_2$, where W_1 is the subsequence of elements occurring with multiplicity 1 in W, and thus $W_2 \mid RR'$. Since $|W_1| + |W_2| = p$, $|\mathrm{supp}(W_1)| + |\mathrm{supp}(W_2)| \le (p+3)/2$ and W_1 is squarefree, it follows that $W_2 \ne 1$, $|W_1| = |\mathrm{supp}(W_1)| \le (p+1)/2$ and $|W_2| \ge (p-1)/2$. Since

$$\begin{aligned}\sum_{g\in H} \mathsf{v}_g(W)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(W)) &\ge \sum_{g\in\mathrm{supp}(W_2)} \mathsf{v}_g(W)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(W)) \\ &\ge \sum_{g\in\mathrm{supp}(W_2)} 2(\mathsf{v}_g(\varphi(S)) - 2) \\ &\ge \sum_{g\in\mathrm{supp}(W_2)} 2\mathsf{v}_g(W) = 2|W_2| \ge p-1,\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p. ∎

LEMMA 5.8. *Let* $p \ge 5$, $|S| = 2p-2$ *and* $2|\mathrm{supp}(\varphi(S))| + \mathsf{h}(\varphi(S)) \le p$. *Then* S *has a zero-sum subsequence of length* p.

Proof. We set $s = |\mathrm{supp}(\varphi(S))|$ and note that $s \le (p-1)/2$ whence $\mathsf{h}(\varphi(S)) \ge 3$ and $s \le (p-3)/2$. Since

$$|R'RUV| = |\varphi(S)| - 2|R| - |U| \ge 2p - 2 - 2s$$

and

$$\mathsf h(R'RUV) = \mathsf h(\varphi(S)) - 2 \le p - 2 - 2s,$$

Theorem 2.2(2) implies that $R'RUV$ has a zero-sum subsequence of length p, and therefore the assertion follows from Lemma 5.7. ∎

LEMMA 5.9. *Let* $p \ge 47$, $|S| = 2p-2$, $\mathsf h(\varphi(S)) \le (p+3)/2$ *and* $|\mathrm{supp}(\varphi(S))| \in [(p-1)/4, (p-1)/3]$. *Then* S *has a zero-sum subsequence of length* p.

Proof. By Lemma 5.7 it suffices to show that $R'RUV$ has a zero-sum subsequence of length p. We set $s = |\mathrm{supp}(\varphi(S))| = |RUV|$, and obtain

$$|R'RUV| = |S| - 2|R| - |U| \ge 2p - 2 - 2s, \quad |R'| \ge 2p - 2 - 3s.$$

By Theorem 2.3(1) we have $|\Sigma_{\lceil s/2\rceil}(RUV)| \ge \min\{p, \lceil s/2\rceil \lfloor s/2\rfloor + 1\} = t$. Since $\mathsf h(R') = \mathsf h(\varphi(S)) - 3 \le (p-3)/2$ and $|R'| \ge p-1$, R' allows a product decomposition of the form

$$R' = Q' \prod_{i\in I} Q_i,$$

where all Q_i are squarefree sequences of length 2, $|I| = \lfloor |R'|/2\rfloor$ and $|Q'| \in \{0,1\}$.

We assert that $|I| \ge p - t$. This is clear for $t = p$, and we suppose that $t = \lceil s/2\rceil \lfloor s/2\rfloor + 1$. Since $t \ge (s^2-1)/4 + 1$, $s \ge (p-1)/4$ and $p \ge 37$, it follows that

$$|I| = \lfloor |R'|/2\rfloor \ge \frac{p-1}{2} \ge p - \frac{((p-1)/4)^2 - 1}{4} - 1 \ge p - t.$$

If $J \subset I$, then

$$\Sigma_{|J|}\Big(\prod_{i\in J} Q_i\Big) \supset \sum_{i\in J} \mathrm{supp}(Q_i),$$

and therefore the Cauchy–Davenport theorem implies that

$$\Big|\Sigma_{|J|}\Big(\prod_{i\in J} Q_i\Big)\Big| \ge \Big|\sum_{i\in J} \mathrm{supp}(Q_i)\Big| \ge \min\{p, |J|+1\}.$$

If $J \subset I$ with $|J| = p - t$, then

$$\Sigma_{p-t+\lceil s/2\rceil}\Big(RUV \prod_{i\in J} Q_i\Big) \supset \Sigma_{\lceil s/2\rceil}(RUV) + \Sigma_{|J|}\Big(\prod_{i\in J} Q_i\Big).$$

The Cauchy–Davenport theorem and the previous estimate imply that $\min\{p, t + (|J|+1) - 1\} = p$ is a lower bound for the cardinality of the latter sumset, whence both sets are equal to H.

Now we choose some $J \subset I$ with $|J| = p - t$, set

$$R^* = R'\Big(\prod_{i\in J} Q_i\Big)^{-1}$$

and assert that

$$|R^*| \ge t - \lceil s/2 \rceil.$$

Suppose that this is proved. Then R^* has a subsequence Y of length $t - \lceil s/2 \rceil$. Since $RUV \prod_{i \in J} Q_i$ has a subsequence X of length $p - t + \lceil s/2 \rceil$ with $\sigma(X) = -\sigma(Y)$, it follows that XY is a zero-sum sequence of $R'RUV$ of length $|XY| = p$.

Since

$$|R^*| = |R'| - 2|J| = |R'| - 2(p-t) \ge 2p - 2 - 3s - 2p + 2t = 2t - 2 - 3s,$$

it suffices to show that

$$t - 2 - 3s \ge -\lceil s/2 \rceil.$$

Since $s \le (p-1)/3$ and $s \ge (p-1)/4 \ge 2$, this is clear for $t = p$. For $t = \lceil s/2 \rceil \lfloor s/2 \rfloor + 1$ we have to show that

$$\lceil s/2 \rceil \lfloor s/2 \rfloor - 1 - 3s + \lceil s/2 \rceil \ge 0.$$

Since $p \ge 47$, we have $s \ge (p-1)/4 \ge 23/2$, and thus the inequality holds. ∎

LEMMA 5.10. *Let $p \ge 41$, $|S| = 2p - 2$ and $|\mathrm{supp}(\varphi(S))| \in [(p+1)/3, p-5]$. Then S has a zero-sum subsequence of length p.*

Proof. Let W be a subsequence of RUV of length $|W| = \lceil p/3 \rceil$ such that $|\gcd(W, R)|$ is minimal. Then W is squarefree, and Theorem 2.3(1) implies that $\Sigma_4(W) = H$. Since $|\gcd(W, R)|$ is minimal, we have either $W \,|\, UV$ or $UV \,|\, W$. If $W \,|\, UV$, then $\gcd(W, R) = 1$ and

$$|\gcd(W, R)^{-1} RR'RU| = |RR'RU| = 2p - 2 - |RUV| \ge p + 3.$$

If $UV \,|\, W$, then $|\gcd(W, R)| = |W| - |UV|$, and since $|R| \le (2p-2)/3$, we obtain

$$|\gcd(W, R)^{-1} RR'RU| = 2p - 2 - (|R| + \lceil p/3 \rceil) \ge p - 2.$$

In both cases $\gcd(W, R)^{-1} RR'RU$ has a subsequence Y of length $p-4$ such that $RU \,|\, Y$. Let X be a subsequence of W of length 4 such that $\sigma(X) = -\sigma(Y)$. Then $T = XY$ is a zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\begin{aligned}
&\sum_{g \in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\quad = \sum_{g \in \mathrm{supp}(R)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) + \sum_{g \in \mathrm{supp}(U)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\quad \ge \sum_{g \in \mathrm{supp}(R)} (\mathsf{v}_g(\varphi(S)) - 1) + \sum_{g \in \mathrm{supp}(U) \setminus \mathrm{supp}(X)} 1 \\
&\quad = |R'R^2| + |U| - 4 = |\varphi(S)| - |\mathrm{supp}(S)| - 4 \ge p - 1,
\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p. ∎

LEMMA 5.11. *Let $p \ge 17$, $|S| = 2p-2$ and $|\mathrm{supp}(\varphi(S))| = p-4$. Then S has a zero-sum subsequence of length p.*

Proof. Let W be a subsequence of RUV of length $(p+3)/2$ such that $|\gcd(W,R)|$ is minimal. We distinguish two cases.

CASE 1: $|\gcd(W,R)| \le 4$. Since

$$\begin{aligned}|\gcd(W,R)^{-1}RR'RU| &= |R'R^2| + |U| - |\gcd(W,R)| \\ &\ge 2p-2-(p-4)-4 = p-2,\end{aligned}$$

$\gcd(W,R)^{-1}RR'RU$ has a subsequence Y of length $p-2$ such that $RU \,|\, Y$. By Theorem 2.3(1) we have $\Sigma_2(W) = H$, and thus W has a subsequence X of length 2 such that $\sigma(X) = -\sigma(Y)$. Then $T = XY$ is a zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\begin{aligned}&\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\ &\quad= \sum_{g\in \mathrm{supp}(R)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) + \sum_{g\in \mathrm{supp}(U)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\ &\quad\ge \sum_{g\in \mathrm{supp}(R)} (\mathsf{v}_g(\varphi(S)) - 1) + \sum_{g\in \mathrm{supp}(U)\setminus\mathrm{supp}(X)} 1 \\ &\quad= |R'R^2| + |U| - 2 = |\varphi(S)| - |\mathrm{supp}(S)| - 2 \ge p,\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p.

CASE 2: $|\gcd(W,R)| \ge 5$. By the minimality of $|\gcd(W,R)|$ we have $UV \,|\, W$. Then $|UV| = |W| - |\gcd(W,R)| \le (p+3)/2 - 5$ and $|RUV| = p-4$. Thus it follows that $|R| \ge (p-1)/2$. Therefore Theorem 2.3(1) implies that $\Sigma_4(R) = H$. Let X be a subsequence of R of length 4 such that $T = XRUV$ is a zero-sum sequence. Then $|T| = p$, and since

$$\begin{aligned}&\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\ &\quad= \sum_{g\in \mathrm{supp}(R)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) + \sum_{g\in \mathrm{supp}(U)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\ &\quad\ge \sum_{g\in \mathrm{supp}(R)} (\mathsf{v}_g(\varphi(S)) - 1) + \sum_{g\in \mathrm{supp}(U)} 1 \\ &\quad= |R'R^2| + |U| = |\varphi(S)| - |\mathrm{supp}(S)| \ge p+2,\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p. ∎

LEMMA 5.12. *Let $p \ge 23$, $|S| = 2p-2$ and $|\mathrm{supp}(\varphi(S))| = p-3$. Then S has a zero-sum subsequence of length p.*

Proof. We have $|R'R^2U| = |S| - |\mathrm{supp}(\varphi(S))| = p+1$, in particular $R \neq 1$. We distinguish two cases.

Case 1: $|R| \geq 7$. By the Cauchy–Davenport theorem and by Theorem 2.3(1), we obtain

$$\begin{aligned}|\Sigma_4(R) - \mathrm{supp}(UV)| &\geq \min\{p, 4(|R|-4)+|U|+|V|\}\\ &= \min\{p, 3|R|-16+|\mathrm{supp}(\varphi(S))|\} = p,\end{aligned}$$

and therefore $\Sigma_4(R) - \mathrm{supp}(UV) = H$. Thus there exist a subsequence R^* of R of length 4 and some $x \in \mathrm{supp}(UV)$ such that $T = R^*x^{-1}RUV$ is a zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\begin{aligned}\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) &\geq \sum_{g\in \mathrm{supp}(R)} (\mathsf{v}_g(\varphi(S))-1) + \sum_{g\in \mathrm{supp}(U)\setminus\{x\}} 1\\ &\geq |R'R^2| + |U| - 1 = p,\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p.

Case 2: $|R| \leq 6$. We choose some $r \in \mathrm{supp}(R)$ and distinguish two cases.

Case 2.1: $|U| \geq (p+3)/2$. Then $\Sigma_2(U) = H$. Thus U has a subsequence X of length 2 such that $T = rRUVX$ is a zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \geq |R'R^2| + |U| - 2 = p-1,$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p.

Case 2.2: $|U| \leq (p+1)/2$. Since $|R'R^2U| = p+1$, $|R| \leq 6$ and $p \geq 23$, it follows that $|R'R| \geq (p+1)/2 - 6 \geq 6$, and hence $R'R$ has a subsequence R^* of length 5. Since $|UV| \geq |RUV| - 6 = p-9 \geq (p+3)/2$, it follows that $\Sigma_2(UV) = H$, and hence UV has a subsequence X of length 2 such that $T = R^*RUVX^{-1}$ is a zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \geq |R'R^2| + |U| - 2 = p-1,$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p. ∎

Lemma 5.13. *There exist a subgroup $H^* \subset G$ of order p and a projection $\varphi^*\colon G \to H^*$ such that*

$$\sum_{h\in H} \binom{\mathsf{v}_h(\varphi^*(S))}{2} \geq \binom{|S|}{2}(p+1)^{-1}.$$

In particular, $|S| = 2p-2$ and $p \geq 7$ imply that $\mathsf{h}(\varphi^*(S)) \geq 3$.

Proof. For a subgroup $H' \subset G$ of order p we define

$$A_{H'} = |\{gg' \in \mathcal{F}(G) \mid gg' \text{ is a subsequence of } S \text{ and } g - g' \in H'\}|.$$

Since G has $p+1$ subgroups of order p and S has $\binom{|S|}{2}$ subsequences of length 2, it follows that there exists some subgroup $K \subset G$ such that $A_K \ge \binom{|S|}{2}/(p+1)$. Let $\kappa\colon G \to K$ denote a projection. We define $\varphi^* = \mathrm{id} - \kappa$ and $H^* = \mathrm{Im}(\mathrm{id} - \kappa) = \mathrm{Ker}(\kappa)$. Note that $g - g' \in K$ if and only if $\varphi^*(g) = \varphi^*(g')$. Since there exist $\sum_{h \in H} \binom{\mathsf{v}_h(\varphi^*(S))}{2}$ subsequences gg' of S such that $\varphi^*(g) = \varphi^*(g')$, the first assertion follows.

Let $|S| = 2p-2$, $p \ge 7$ and assume to the contrary that $\mathsf{h}(\varphi^*(S)) \le 2$. Then

$$\binom{2p-2}{2}(p+1)^{-1} \le \sum_{h \in H} \binom{\mathsf{v}_h(\varphi^*(S))}{2} \le |\mathrm{supp}(\varphi^*(S))| \le p,$$

a contradiction. ∎

A pair (H^*, φ^*) consisting of a subgroup $H^* \subset G$ and a projection $\varphi^*\colon G \to H^*$ is called *suitable* (with respect to S) if it has the property given in Lemma 5.13.

In the following lemmas there is a trade-off between the length of the argument and the range of primes for which the results are valid. Some arguments could be slightly shortened when allowing p to be larger, and conversely, with more involved proofs some of the results could be obtained for (slightly) smaller primes. Our aim is to obtain results (at least) for primes p with $p \ge 47$, which is the bound given by Lemma 5.9.

LEMMA 5.14. *Let $p \ge 23$, $|S| = 2p-2$, $|\mathrm{supp}(\varphi(S))| = p$ and (H, φ) suitable. Then S has a zero-sum subsequence of length p.*

Proof. Since $|RUV| = p$ and $|R^3U^2V| \le |S| = 2p-2$, it follows that $|R^2U| \le p-2$ and thus $|R| \le (p-3)/2$. This implies that $|UV| \ge (p+3)/2$ and hence $\Sigma_2(UV) = H$ by Theorem 2.3(1). Furthermore, we have $|R'R^2U| = |S| - |\mathrm{supp}(\varphi(S))| = p-2$.

We assert that one of the following three statements holds:

- $\mathsf{h}(\varphi(S)) \ge 6$.
- There exist two distinct elements $r_1, r_2 \in H$ whose multiplicities in $\varphi(S)$ are at least 5 and 4, respectively.
- There exist three distinct elements $r_1, r_2, r_3 \in H$ whose multiplicities in $\varphi(S)$ are at least 4.

Assume to the contrary that none of these statements holds. Since (H, φ) is suitable, we have

$$2p-6 \le \binom{|S|}{2}(p+1)^{-1} \le \sum_{h \in H} \binom{\mathsf{v}_h(\varphi(S))}{2}.$$

Since none of the statements holds, the last sum is bounded above either by

$$\binom{5}{2} + (|R|-1)\binom{3}{2} + |U|\binom{2}{2} = 7 + 3|R| + |U|$$

or by

$$2\binom{4}{2} + (|R|-2)\binom{3}{2} + |U|\binom{2}{2} = 6 + 3|R| + |U|.$$

Since $|R^3U^2V| \le 2p-2$, it follows that either $|UV| \le 11$ or $|UV| \le 10$, a contradiction to $|UV| \ge (p+3)/2$.

Now we distinguish three cases.

Case 1: $\mathsf{h}(\varphi(S)) \ge 6$. Let $r \in \operatorname{supp}(R)$ with $\mathsf{v}_r(\varphi(S)) = \mathsf{h}(\varphi(S))$, and let X be a subsequence of UV of length 2 such that $T = r^2RUVX^{-1}$ is a zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\begin{aligned}
&\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\qquad = 3(\mathsf{v}_r(\varphi(S)) - 3) + \sum_{g\in \operatorname{supp}(R)\setminus\{r\}} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\qquad\quad + \sum_{g\in \operatorname{supp}(U)\setminus\operatorname{supp}(X)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\qquad \ge 3(\mathsf{v}_r(\varphi(S)) - 3) + \sum_{g\in \operatorname{supp}(R)\setminus\{r\}} (\mathsf{v}_g(\varphi(S)) - 1) + |U| - 2 \\
&\qquad = 2\mathsf{v}_r(\varphi(S)) - 8 + |R'R^2| + |U| - 2 \ge |R'R^2| + |U| + 2 = p,
\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p.

Case 2: There exist distinct elements $r_1, r_2 \in H$ with $\mathsf{v}_{r_1}(\varphi(S)) \ge 5$ and $\mathsf{v}_{r_2}(\varphi(S)) \ge 4$. Let X be a subsequence of UV of length 2 such that $T = r_1r_2RUVX^{-1}$ is a zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\begin{aligned}
&\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\qquad = 2(\mathsf{v}_{r_1}(\varphi(S)) - 2) + 2(\mathsf{v}_{r_2}(\varphi(S)) - 2) \\
&\qquad\quad + \sum_{g\in \operatorname{supp}(R)\setminus\{r_1,r_2\}} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\qquad\quad + \sum_{g\in \operatorname{supp}(U)\setminus\operatorname{supp}(X)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\qquad \ge \mathsf{v}_{r_1}(\varphi(S)) + \mathsf{v}_{r_2}(\varphi(S)) - 6 + |R'R^2| + |U| - 2 \\
&\qquad \ge |R'R^2| + |U| + 1 = p - 1,
\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p.

Case 3: There exist three distinct elements $r_1, r_2, r_3 \in H$ with $\mathsf{v}_{r_i}(\varphi(S)) \ge 4$ for all $i \in [1,3]$. As $|RUV| = p$ and $3+|R^3U^2V| \le |R'R^3U^2V| = 2p-2$, we infer that $|R^2U| \le p-5$, $|R| \le (p-5)/2$ and therefore $|UV| \ge (p+5)/2$. Note that $V \ne 1$, and we choose some $v \in \mathrm{supp}(V)$. Then $\Sigma_2(UVv^{-1}) = H$, and therefore UVv^{-1} has a subsequence X of length 2 such that $T = r_1r_2r_3RUVv^{-1}X^{-1}$ is a zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\begin{aligned}
&\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\quad = \sum_{i=1}^{3} 2(\mathsf{v}_{r_i}(\varphi(S)) - 2) + \sum_{g\in \mathrm{supp}(R)\setminus\{r_1,r_2,r_3\}} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\qquad + \sum_{g\in \mathrm{supp}(U)\setminus\mathrm{supp}(X)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\quad \ge \sum_{i=1}^{3} (\mathsf{v}_{r_i}(\varphi(S)) - 3) + |R'R^2| + |U| - 2 \ge |R'R^2| + |U| + 1 = p-1,
\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p. ∎

Lemma 5.15. *Let $p \ge 23$, $|S| = 2p-2$, $|\mathrm{supp}(\varphi(S))| = p-1$ and (H,φ) suitable. Then S has a zero-sum subsequence of length p.*

Proof. Since $|RUV| = p-1$ and $|R^3U^2V| \le |S| = 2p-2$, it follows that $|R^2U| \le p-1$ and thus $|R| \le (p-1)/2$. This implies that $|UV| \ge (p-1)/2$ and hence $\Sigma_3(UV) = H$.

Since $p \ge 23$ and (H,φ) is suitable, one of the following five statements holds:

- There exists an element $r_1 \in H$ whose multiplicity in $\varphi(S)$ is at least 7.
- There exist two distinct elements $r_1, r_2 \in H$ whose multiplicities in $\varphi(S)$ are at least 6 and 3, respectively.
- There exist two distinct elements $r_1, r_2 \in H$ whose multiplicities in $\varphi(S)$ are at least 5.
- There exist three distinct elements $r_1, r_2, r_3 \in H$ whose multiplicities in $\varphi(S)$ are at least 5, 4 and 3, respectively.
- There exist four distinct elements $r_1, r_2, r_3, r_4 \in H$ whose multiplicities in $\varphi(S)$ are at least 4, 4, 4 and 3, respectively.

Corresponding to the five cases let R^* be one of the following five sequences:

$$r_1^4, \quad r_1^3r_2, \quad r_1^2r_2^2, \quad r_1^2r_2r_3, \quad \text{or} \quad r_1r_2r_3r_4.$$

Let X be a subsequence of UV of length 3 such that $T = R^*RUVX^{-1}$ is a

zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\begin{aligned}
&\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\quad = \sum_{g\in \mathrm{supp}(R^*)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\qquad + \sum_{g\in \mathrm{supp}(R)\setminus\mathrm{supp}(R^*)} (\mathsf{v}_g(\varphi(S)) - 1) + \sum_{g\in \mathrm{supp}(U)\setminus\mathrm{supp}(X)} 1 \\
&\quad = \sum_{g\in \mathrm{supp}(R^*)} (\mathsf{v}_g(T) - 1)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T) - 1) \\
&\qquad + \sum_{g\in \mathrm{supp}(R)} (\mathsf{v}_g(\varphi(S)) - 1) + \sum_{g\in \mathrm{supp}(U)\setminus\mathrm{supp}(X)} 1 \\
&\quad \ge \sum_{g\in \mathrm{supp}(R^*)} (\mathsf{v}_g(T) - 1)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T) - 1) + |R'R^2| + |U| - 3 \\
&\quad = \sum_{g\in \mathrm{supp}(R^*)} (\mathsf{v}_g(T) - 1)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T) - 1) + (p-4) \ge p-1,
\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p. ∎

LEMMA 5.16. *Let $p \ge 23$, $|S| = 2p-2$, $|\mathrm{supp}(\varphi(S))| = p-2$ and (H,φ) suitable. Then S has a zero-sum subsequence of length p.*

Proof. We have $|R'R^2U| = |S| - |\mathrm{supp}(\varphi(S))| = p$. We distinguish two cases.

CASE 1: $|R| \ge 6$. By the Cauchy–Davenport theorem and by Theorem 2.3(1),

$$\begin{aligned}
|\Sigma_3(R) - \mathrm{supp}(UV)| &\ge \min\{p, 3(|R|-3) + |U| + |V|\} \\
&= \min\{p, 2|R| - 9 + |\mathrm{supp}(\varphi(S))|\} = p,
\end{aligned}$$

and therefore $\Sigma_3(R) - \mathrm{supp}(UV) = H$. Thus there exist a subsequence R^* of R of length 3 and some $x \in \mathrm{supp}(UV)$ such that $\sigma(R^*) - x = -\sigma(RUV)$ and hence $T = R^*x^{-1}RUV$ is a zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\begin{aligned}
\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) &\ge \sum_{g\in \mathrm{supp}(R)} (\mathsf{v}_g(\varphi(S)) - 1) + \sum_{g\in \mathrm{supp}(U)\setminus\{x\}} 1 \\
&\ge |R'R^2| + |U| - 1 = p-1,
\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p.

CASE 2: $|R| \le 5$. Since $p \ge 23$ and (H,φ) is suitable, one of the following six statements holds:

- There exists an element $r_1 \in H$ whose multiplicity in $\varphi(S)$ is at least 7.
- There exist two distinct elements $r_1, r_2 \in H$ whose multiplicities in $\varphi(S)$ are at least 6 and 3, respectively.
- There exist two distinct elements $r_1, r_2 \in H$ whose multiplicities in $\varphi(S)$ are at least 5 and 4, respectively.
- There exist three distinct elements $r_1, r_2, r_3 \in H$ whose multiplicities in $\varphi(S)$ are at least 5, 3 and 3, respectively.
- There exist three distinct elements $r_1, r_2, r_3 \in H$ whose multiplicities in $\varphi(S)$ are at least 4, 4 and 3, respectively.
- There exist four distinct elements $r_1, r_2, r_3, r_4 \in H$ whose multiplicities in $\varphi(S)$ are at least 4, 3, 3 and 3, respectively.

Corresponding to the six cases let R^* be one of the following six sequences:

$$r_1^4, \quad r_1^3 r_2, \quad r_1^2 r_2^2, \quad r_1^2 r_2 r_3, \quad r_1 r_2^2 r_3 \quad \text{or} \quad r_1 r_2 r_3 r_4.$$

Since $|UV| \ge |RUV| - 5 = p - 7 \ge (p+3)/2$, it follows that $\Sigma_2(UV) = H$, and hence UV has a subsequence X of length 2 such that $T = R^* RUV X^{-1}$ is a zero-sum subsequence of $\varphi(S)$ of length p. Since

$$\begin{aligned}
&\sum_{g\in H} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\quad = \sum_{g\in \mathrm{supp}(R^*)} \mathsf{v}_g(T)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T)) \\
&\qquad + \sum_{g\in \mathrm{supp}(R)\setminus\mathrm{supp}(R^*)} (\mathsf{v}_g(\varphi(S)) - 1) + \sum_{g\in \mathrm{supp}(U)\setminus\mathrm{supp}(X)} 1 \\
&\quad = \sum_{g\in \mathrm{supp}(R^*)} (\mathsf{v}_g(T) - 1)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T) - 1) \\
&\qquad + \sum_{g\in \mathrm{supp}(R)} (\mathsf{v}_g(\varphi(S)) - 1) + \sum_{g\in \mathrm{supp}(U)\setminus\mathrm{supp}(X)} 1 \\
&\quad \ge \sum_{g\in \mathrm{supp}(R^*)} (\mathsf{v}_g(T) - 1)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T) - 1) + |R'R^2| + |U| - 2 \\
&\quad = \sum_{g\in \mathrm{supp}(R^*)} (\mathsf{v}_g(T) - 1)(\mathsf{v}_g(\varphi(S)) - \mathsf{v}_g(T) - 1) + p - 2 \ge p - 1,
\end{aligned}$$

Lemma 5.3(1) implies that S has a zero-sum subsequence of length p. ∎

Proof of Proposition 5.2. Let $p \in \mathbb{P}$ with $p \ge 47$ and let $S \in \mathcal{F}(G)$ be a squarefree sequence of length $|S| = 2p - 2$. By Lemma 5.13 there exists a subgroup $H \subset G$ of order p and a projection $\varphi\colon G \to H$ such that (H, φ) is suitable and thus in particular $\mathsf{h}(\varphi(S)) \ge 3$.

If $\mathsf{h}(\varphi(S)) \ge p$, then S has a zero-sum subsequence of length p by Lemma 5.3(3). If $\mathsf{h}(\varphi(S)) = p-1$, then S either has a zero-sum subsequence of length p or it is of the asserted form by Lemma 5.4. If $\mathsf{h}(\varphi(S)) = p-2$, then S either has a zero-sum subsequence of length p or it is of the asserted form by Lemma 5.5. If $\mathsf{h}(\varphi(S)) = p-3$, then S has a zero-sum subsequence of length p by Lemma 5.6. If $\mathsf{h}(\varphi(S)) \in [(p+5)/2, p-4]$, then S has a zero-sum subsequence of length p by Lemma 5.3(2).

Now suppose that $\mathsf{h}(\varphi(S)) \in [3, (p+3)/2]$. Then S has a zero-sum subsequence of length p: Indeed,

- for $|\mathrm{supp}(\varphi(S))| = p$, see Lemma 5.14,
- for $|\mathrm{supp}(\varphi(S))| = p-1$, see Lemma 5.15,
- for $|\mathrm{supp}(\varphi(S))| = p-2$, see Lemma 5.16,
- for $|\mathrm{supp}(\varphi(S))| = p-3$, see Lemma 5.12,
- for $|\mathrm{supp}(\varphi(S))| = p-4$, see Lemma 5.11,
- for $|\mathrm{supp}(\varphi(S))| \in [(p+1)/3, p-5]$, see Lemma 5.10,
- for $|\mathrm{supp}(\varphi(S))| \in [(p-1)/4, (p-1)/3]$, see Lemma 5.9,
- for $|\mathrm{supp}(\varphi(S))| \le (p-3)/4$, see Lemma 5.8. ∎

Acknowledgements. The first author is supported by NSFC, Project No. 10671011 and by the 973 Program, Project No. 2006CB805900. The second and the third authors are supported by the Austrian Science Fund FWF, Project No. P18779-N13. This paper was completed during a one-month stay of the second author at the Center for Combinatorics, Nankai University. He would like to thank for the excellent working conditions and for all the hospitality.

References

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

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

[3] G. Bhowmik and J.-C. Schlage-Puchta, *Davenport's constant for groups of the form* $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$, manuscript.

[4] A. Bialostocki, P. Dierker, D. Grynkiewicz, and M. Lotspeich, *On some developments of the Erdős–Ginzburg–Ziv Theorem II*, Acta Arith. 110 (2003), 173–184.

[5] A. Bialostocki and M. Lotspeich, *Some developments of the Erdős–Ginzburg–Ziv Theorem I*, in: Sets, Graphs and Numbers, Colloq. Math. Soc. János Bolyai 60, North-Holland, 1992, 97–117.

[6] J. Bierbrauer and Y. Edel, *Bounds on affine caps*, J. Combin. Des. 10 (2002), 111–115.

[7] J. D. Bovey, P. Erdős, and I. Niven, *Conditions for zero sum modulo n*, Canad. Math. Bull. 18 (1975), 27–29.

[8] Y. Caro, *On zero-sum Ramsey numbers—stars*, Discrete Math. 104 (1992), 1–6.

[9] —, *Zero-sum problems—a survey*, ibid. 152 (1996), 93–113.

[10] 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.
[11] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc. 26 (1994), 140–146.
[12] Y. Edel, *Sequences in abelian groups G of odd order without zero-sum subsequences of length* $\exp(G)$, Des. Codes Cryptography, to appear.
[13] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, and L. Rackham, *Zero-sum problems in finite abelian groups and affine caps*, Q. J. Math., to appear.
[14] Y. Edel, S. Ferret, I. Landjev, and L. Storme, *The classification of the largest caps in* $\mathrm{AG}(5,3)$, J. Combin. Theory Ser. A 99 (2002), 95–110.
[15] C. Elsholtz, *Lower bounds for multidimensional zero sums*, Combinatorica 24 (2004), 351–358.
[16] P. van Emde Boas, *A combinatorial problem on finite abelian groups II*, report ZW-1969-007, Math. Centre, Amsterdam, 1969.
[17] P. Erdős, A. Ginzburg, and A. Ziv, *Theorem in the additive number theory*, Bull. Res. Council Israel Sect. F Math. Phys. 10 (1961), 41–43.
[18] C. Flores and O. Ordaz, *On the Erdős–Ginzburg–Ziv theorem*, Discrete Math. 152 (1996), 321–324.
[19] W. D. Gao, *An addition theorem for finite cyclic groups*, ibid. 163 (1997), 257–265.
[20] —, *On Davenport's constant of finite abelian groups with rank three*, ibid. 222 (2000), 111–124.
[21] —, *Two zero sum problems and multiple properties*, J. Number Theory 81 (2000), 254–265.
[22] W. D. Gao and A. Geroldinger, *On long minimal zero sequences in finite abelian groups*, Period. Math. Hungar. 38 (1999), 179–211.
[23] —, —, *On zero-sum sequences in* $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, Integers 3 (2003), A08, 45pp.
[24] —, —, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. 24 (2006), 337–369.
[25] W. D. Gao, Q. H. Hou, W. A. Schmid, and R. Thangadurai, *On short zero-sum subsequences II*, Integers 7 (2007), A21, 22 pp.
[26] W. D. Gao, A. Panigrahi, and R. Thangadurai, *On the structure of p-zero-sum free sequences and its application to a variant of Erdős–Ginzburg–Ziv theorem*, Proc. Indian Acad. Sci. Math. Sci. 115 (2005), 67–77.
[27] W. D. Gao and R. Thangadurai, *On the structure of sequences with forbidden zero-sum subsequences*, Colloq. Math. 98 (2003), 213–222.
[28] —, —, *A variant of Kemnitz conjecture*, J. Combin. Theory Ser. A 107 (2004), 69–86.
[29] W. D. Gao, R. Thangadurai, and J. Zhuang, *Addition theorems on the cyclic groups of order* p^l, Discrete Math., to appear.
[30] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. 278, Chapman & Hall/CRC, 2006.
[31] F. Hennecart, *La fonction de Brakemeier dans le problème d'Erdős–Ginzburg–Ziv*, Acta Arith. 117 (2005), 35–50.
[32] S. Kubertin, *Nullsummen in* $\mathbb{Z}_p^d$, master's thesis, Technical Univ. Clausthal, 2002.
[33] G. Lettl and W. A. Schmid, *Minimal zero-sum sequences in* $C_n \oplus C_n$, Eur. J. Comb. 28 (2007), 742–753.
[34] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.
[35] C. Reiher, *On Kemnitz' conjecture concerning lattice points in the plane*, Ramanujan J. 13 (2007), 333–337.

[36] K. Rogers, *A combinatorial problem in abelian groups*, Proc. Cambridge Philos. Soc. 59 (1963), 559–562.

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

[38] C. Wang, *Note on a variant of the Erdős–Ginzburg–Ziv problem*, Acta Arith. 108 (2003), 53–59.

Center for Combinatorics
Nankai University
Tianjin 300071, P.R. China
E-mail: wdgao_1963@yahoo.com.cn

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

Received on 9.11.2006
and in revised form on 19.2.2007 (5317)