Periodica Mathematica Hungarica Vol. 38 (3), (1999), pp. 179–211

ON LONG MINIMAL ZERO SEQUENCES IN FINITE ABELIAN GROUPS

WEIDONG GAO* (Beijing) and ALFRED GEROLDINGER (Graz)
[Communicated by: Attila Pethő]

1. Introduction

Additive number theory, graph theory and factorization theory provide inexhaustible sources for combinatorial problems in finite abelian groups (cf. [Ma1, Ma2, E-G, D-M, Na, An]). Among them zero sum problems have been of growing interest. Starting points of recent research in this area were the Theorem of Erdős–Ginzburg–Ziv and a question of H. Davenport on an invariant which today carries his name..

This paper centres around the following problem: let G be a finite abelian group and $D(G)$ Davenport's constant of G (cf. Section 3). Consider a long minimal zero sequence resp. a long zerofree sequence S; where in this context long means that $D(G) - |S|$ is small. What can be said about the structure of S? There are simple, well known answers for cyclic groups and elementary 2-groups (cf. Propositions 4.1 and 4.2). Our aim is to derive similar results for more general groups. In Section 5 we study the action of the automorphism group and in Section 6 we ask after the order of elements in S. If the rank of G is large, then all elements of S may be pairwise distinct (Section 7). Conversely, if the exponent is large, then one element occurs with high multiplicity (Section 8). In Section 9 we develop a polynomial method which will be applied successfully to elementary p-groups in Section 10.

Most of the raised problems seem to be deep and we just can provide first answers. However, such structural questions arise naturally e.g. in factorization theory. Furthermore, solutions to them will allow further progress in determining Davenport's constant, a starting problem in this area (cf. Properties B and C in Section 10).

Mathematics subject classification numbers, 11B50, 11B75.

Key words and phrases. Minimal zero sequences, finite abelian groups.

The author holds an Austrian Lise Meitner Fellowship (Project-Number M00397-MAT) and would like to thank the FWF for all the assistance.

0031-5303/99/$5.00
© *Akadémiai Kiadó, Budapest*
Akadémiai Kiadó, Budapest
Kluwer Academic Publishers, Dordrecht

2. Notations

Let $\mathbb{N}$ denote the non-negative integers, $\mathbb{N}_+$ the positive integers and $\mathbb{P} \subseteq \mathbb{N}_+$ the set of prime numbers. For a prime $p \in \mathbb{P}$, let $v_p \colon N_+ \to \mathbb{N}$ denote the p-adic exponent. Then $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ for every $n \in \mathbb{N}_+$.

Throughout, finite abelian groups will be written additively. For $n \in \mathbb{N}_+$, $C_n = \mathbb{Z}/n\mathbb{Z}$ denotes the cyclic group with n elements. Whenever it is convenient, the elementary abelian p-group C_p^r with $p \in \mathbb{P}$ and $r \in \mathbb{N}_+$ will be viewed as r-dimensional vector space over the field $\mathbb{F}_p$.

Let G be a finite abelian group. Then $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$, where $n_r = \exp(G)$ is the exponent of G and r is the rank of G. Indeed, r is the maximal p-rank of G resp. the minimal number of generators of G. An (ordered) *basis* of G is an r-tuple $(e_1, \ldots, e_r)$ with $\mathrm{ord}(e_i) = n_i$ for $1 \le i \le r$ such that $G = \oplus_{i=1}^r \langle e_i \rangle$. Then every $g \in G$ has a unique representation

$$g = \sum_{k=1}^{r} v_k(g) e_k$$

with $v_k(g) \in \{0, \ldots, n_k - 1\}$ for $1 \le k \le r$.

In general, our notations and terminology will be consistent with the usual one in factorization theory (cf. the survey articles by Chapman, Halter-Koch and the second author in [An]). Let $\mathcal{F}(G)$ denote the free abelian monoid with basis G. The elements of $\mathcal{F}(G)$ will be called *sequences*. The monoid homomorphism

$$\sigma \colon \mathcal{F}(G) \longrightarrow G$$
$$S = \prod_{\nu=1}^{l} g_\nu \mapsto \sum_{\nu=1}^{l} g_\nu$$

maps a sequence to the sum of its elements. Let $S = \prod_{\nu=1}^{l} g_\nu \in \mathcal{F}(G)$ be a sequence. Then S has a unique representation of the form

$$S = \prod_{g \in G} g^{v_g(S)} \in \mathcal{F}(G)$$

and $|S| = \Sigma_{g \in G} v_g(S) = l \in \mathbb{N}$ is called the *length* of S. We say that $T \in \mathcal{F}(G)$ is a subsequence of S (T divides S, S contains T) and write $T \mid S$, if $v_g(T) \le v_g(S)$ for every $g \in G$ (equivalently, $ST^{-1} \in \mathcal{F}(G)$). As usual, we say that $T, T' \in \mathcal{F}(G)$ are *disjoint subsequences* of S, if their product TT' divides S. Furthermore, we set

$$\gcd(S, T) = \prod_{g \in G} g^{\min\{v_g(S), v_g(T)\}}$$

The identity element $1 \in \mathcal{F}(G)$ will be called the *empty sequence*, and we have

$|1| = 0$. As usual, let

$$\begin{aligned}\Sigma(S) &= \{\sigma(T) \mid T \text{ a non-empty subsequence of } S\} \\ &= \Big\{\sum_{\nu\in I} g_\nu \mid \emptyset \neq I \subseteq \{1,\dots,l\}\Big\} \\ &= \Big\{\sum_{g\in G} m_g g \mid 0 \le m_g \le v_g(S)\,, \Sigma_{g\in G} m_g > 0\Big\}\end{aligned}$$

denote the set of sums of non-empty subsequences of S. We say that the sequence S is

squarefree, if $v_g(S) \le 1$ for every $g \in G$,

zerofree, if $0 \notin \Sigma(S)$,

a *zero sequence*, if $\sigma(S) = \sum_{\nu=1}^{l} g_\nu = 0$,

a *minimal zero sequence*, if it is a zero sequence and each proper subsequence is zerofree,

a *short zero sequence*, if it is a zero sequence with $1 \le |S| \le \exp(G)$.

In factorization theory zero sequences are called *blocks*. The set of blocks $\mathcal{B}(G) = \mathrm{Ker}(\sigma)$ is a submonoid of $\mathcal{F}(G)$. Its irreducible elements are just the minimal zero sequences, whose set will be denoted by $\mathcal{U}(G)$. For more information the reader is referred to [Ch] and the survey articles in [An], in particular to [Ch-Ge].

For every $1 \le k \le r$ we set

$$v_k(S) = \sum_{\nu=1}^{l} v_k(g_\nu) \in \mathbb{N}.$$

Clearly, S is a zero sequence if and only if

$$v_k(S) \equiv 0 \mod n_k$$

for all $1 \le k \le r$.

Every group homomorphism $\varphi\colon G \to H$ extends in a canonical way to a homomorphism

$$\begin{aligned}\varphi\colon \mathcal{F}(G) &\to \mathcal{F}(H) \\ S = \prod_{\nu=1}^{l} g_\nu &\mapsto \prod_{\nu=1}^{l} \varphi(g_\nu)\end{aligned}$$

and obviously, $|S| = |\varphi(S)|$.

3. Davenport's constant

In this section we summarize simple facts and well known theorems on Davenport's constant which will be used in the sequel without further quoting. A new result will be given at the end of the section.

For a finite abelian group G *Davenport's constant* $D(G)$ is defined as the minimum of all $d \in \mathbb{N}_+$ such that for every sequence $S \in \mathcal{F}(G)$ with $|S| \ge d$ it follows that $0 \in \Sigma(S)$.

We set

$$\mathcal{U}^*(G) = \{S \in \mathcal{U}(G) \,|\, |S| = D(G)\}.$$

LEMMA 3.1. *Let G be a finite abelian group.*

1.

$$\begin{aligned} D(G) &= \max\{|S| \mid S \in \mathcal{U}(G)\} \\ &= 1 + \max\{|S| \mid S \in \mathcal{F}(G), 0 \notin \Sigma(S)\} \\ &= 1 + \max\{|S| \mid S \in \mathcal{F}(G), \Sigma(S) = G \setminus \{0\}\}. \end{aligned}$$

2. *If $S = \prod_{\nu=1}^{D(G)} g_\nu \in \mathcal{U}(G)$, then $G = \langle g_1, \ldots, g_{D(G)-1} \rangle$.*

3. *If $H < G$ is a proper subgroup, then $D(H) < D(G)$.*

PROOF. **1.** Obvious.

2. Let $S = \prod_{\nu=1}^{D(G)} g_\nu \in \mathcal{U}(G)$. Then $T = \prod_{\nu=1}^{D(G)-1} g_\nu$ is zerofree and $\Sigma(T) = G \setminus \{0\}$ whence $G = < g_1, \ldots, g_{D(G)-1} >$.

3. For every zerofree sequence $S \in \mathcal{F}(H)$ and every $g \in G \setminus H$ the sequence $gS \in \mathcal{F}(G)$ is zerofree which implies the assertion. □

For a finite abelian group $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$ we set

$$M(G) = 1 + \sum_{i=1}^{r} (n_i - 1).$$

PROPOSITION 3.2. *Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$.*

1. $M(G) \le D(G) \le 1 + \exp(G)\left(1 + \log \frac{|G|}{\exp(G)}\right)$.

2. *If G is a p-group or $r \le 2$, then $M(G) = D(G)$.*

PROOF. **1.** If $(e_1, \ldots, e_r)$ is a basis of G with $\operatorname{ord}(e_i) = n_i$ for $1 \le i \le r$, then $S = \prod_{i=1}^{r} e_i^{n_i - 1}$ is zerofree whence $M(G) \le D(G)$. The upper bound was first proved by van Emde Boas and D. Kruyswijk (E-K], see also [A-G-P; Theorem 1.1] and [Me].

2. This was proved independently by J.E.Olson and D. Kruyswijk (cf. [Ol1, Ol2, E1]). □

There are groups with $M(G) < D(G)$ (cf. [G-S1] and [Ma]). However, the reason for this phenomenon is completely unclear. It is unknown, if $M(G) = D(G)$ holds for all groups of rank 3 (cf. *Property B* and [Ga5]). Furthermore, it is not known if there exists an $n \in \mathbb{N}_+$ such that $M(C_n^5) < D(C_n^5)$ (which implies $M(C_n^r) < D(C_n^r)$ for every $r \ge 5$) cf. [A-F-K; Conjecture A.5], [A-D1; Theorem 1.1] and [B-S]. Against this background the following result should be seen.

THEOREM 3.3. *$M(C_2^i \oplus C_{2n}^{5-i}) < D(C_2^i \oplus C_{2n}^{5-i})$ for every odd $n \geq 3$ and every $2 \leq i \leq 4$.*

PROOF. Let $i \in \{2,3,4\}$ and let $n \geq 3$ be odd. Further let $(e_1, \ldots, e_5)$ be a basis of $G = C_2^i \oplus C_{2n}^{5-i}$ with $\operatorname{ord}(e_1) = \cdots = \operatorname{ord}(e_i) = 2$ and $\operatorname{ord}(e_{i+1}) = \cdots = \operatorname{ord}(e_5) = 2n$. We construct a sequence S with $|S| = i+(5-i)(2n-1)+1 = M(G)$, and it has to be shown that $0 \notin \Sigma(S)$. The cases $i = 3$ and $i = 4$ were settled in [G-S]. Hence we just have to consider the case $i = 2$.

We define $g_j = e_1 + e_{j+2}$ for $1 \leq j \leq 3, g_j = e_2 + e_{j-1}$ for $4 \leq j \leq 6, g_7 = e_3 + 3e_4 - 5e_5$, $g_8 = e_1 + 2e_4 - 2e_5, g_9 = e_2 + 2e_3 + 3e_4 - 5e_5$ and $g_{10} = e_2 + (n-1)e_4 + (n+3)e_5$. We set

$$S = \prod_{i=1}^{7} g_i \cdot g_8^{2n-2} g_9^{2n-2} g_{10}^{2n-3}.$$

Assume that there are $l_1, \ldots, l_7 \in \{0,1\}, l_8, l_9 \in \{0, \ldots, 2n-2\}$ and $l_{10} \in \{0, \ldots, 2n-3\}$ such that $\sum_{i=1}^{10} l_i > 0$ and $\sum_{i=1}^{10} l_i g_i = 0$. This gives the following system of congruences.

I $\quad l_1 + l_2 + l_3 + l_8 \equiv 0 \mod 2$.

II $\quad l_4 + l_5 + l_6 + l_9 + l_{10} \equiv 0 \mod 2$.

III $\quad l_1 + l_4 + l_7 + 2l_9 \equiv 0 \mod 2n$.

IV $\quad l_2 + l_5 + 3l_7 + 2l_8 + 3l_9 + (n-1)l_{10} \equiv 0 \mod 2n$.

V $\quad l_3 + l_6 - 5l_7 - 2l_8 - 5l_9 + (n+3)l_{10} \equiv 0 \mod 2n$.

We set $a = l_1 + l_4 + l_7 + 2l_9$. Since $0 \leq a \leq 3 + 2(2n-2) = 4n-1$, equation III implies that $a \in \{0, 2n\}$.

CASE 1. $a = 0$. Then $l_1 = l_4 = l_7 = l_9 = 0$. Hence $l_2 = l_5$ by IV, and $l_3 = l_6$ by V. Adding IV and V we obtain $2l_2 + 2l_3 + 2l_{10} \equiv 0 \mod 2n$, and thus $l_2 + l_3 + l_{10} \equiv 0 \mod n$. From this we infer that $l_2 + l_3 + l_{10} \in \{0, n\}$. Since $l_2 + l_3 + l_{10}$ is even by equation II, it follows that $l_2 = l_3 = l_{10} = 0$. Finally I and IV imply that l_8 is even and $2l_8 \equiv 0 \mod 2n$, and so $l_8 = 0$. This is a contradiction to $\sum_{i=1}^{10} l_i > 0$.

CASE 2. $a = 2n$. Adding III, IV and V we obtain

$$b = l_1 + l_2 + l_3 + l_4 + l_5 + l_6 - l_7 + 2l_{10} \equiv 0 \mod 2n,$$

and therefore $b \in \{0, 2n, 4n\}$.

Assume $b = 0$. Then $l_{10} = 0$. From $l_7 = 1$, we infer that $l_9 = n - 1$ and $l_2 = l_5 = 0$; then IV implies $3 \equiv 0 \mod 2$, a contradiction. From $l_7 = 0$ it follows that $l_1 = \cdots = l_6 = 0$ and $l_9 = n$; hence $n \equiv 0 \mod 2$ by IV, a contradiction.

Assume $b = 4n$. Then $l_{10} = 2n - 3, l_1 = \cdots = l_6 = 1$ and $l_7 = 0$. Therefore $l_9 = n - 1$, and IV implies

$$2 + 2l_8 + (n - 3) - 3n + 3 \equiv 0 \mod 2n.$$

Hence $2l_8 + 2 \equiv 0 \mod 2n$ and thus $l_8 = n - 1$. Finally I gives $3 + (n - 1) \equiv 0 \mod 2$, a contradiction.

From now on we assume $b = 2n$ and distinguish the cases $l_7 = 0$ and $l_7 = 1$.

CASE 2.1. $l_7 = 1$. Since $a = 2n$, we obtain $l_1 + l_4 = 1$, $l_9 = n - 1$, and therefore $l_{10} = n - \frac{l_2+l_3+l_5+l_6}{2}$. Then IV yields $l_2 + l_5 = 1$, and V yields $l_3 + l_6 = 1$. Hence $l_{10} = n - 1$, and we consider IV:

$$1 + 3 + 2l_8 + n - 3 - n + 1 = 2l_8 + 2 \equiv 0 \mod 2n.$$

From this we conclude that $l_8 = n - 1$. Finally we add I and II to obtain $3 + 3(n - 1) \equiv 0 \mod 2$, a contradiction.

CASE 2.2. $l_7 = 0$. Since $a = 2n$, we obtain $l_1 = l_4$, $l_9 = n - l_1$, and therefore $l_{10} = n - l_1 - \frac{l_2+l_3+l_5+l_6}{2}$. Then IV yields $l_1 + l_2 + l_5 = 1$, and V yields $l_1 + l_3 + l_6 = 1$. If $l_1 = 1$, then $l_2 = l_5 = l_3 = l_6 = 0, l_9 = l_{10} = n - 1$, and from II it follows $1 + 2(n - 1) \equiv 0 \mod 2$, a contradiction. Thus $l_1 = 0$, which implies $l_9 = n$ and $l_{10} = n - 1$. Adding I and II it follows $2 + l_8 + n + (n - 1) \equiv 0 \mod 2$ i.e. l_8 is odd. Considering IV we obtain

$$1 + 2l_8 + n - n + 1 \equiv 0 \mod 2n,$$

which implies $l_8 = n - 1 \equiv 0 \mod 2$, a contradiction. □

4. Tools

PROPOSITION 4.1. *Let $G = C_2^r$ with $r \ge 1$ and $S \in \mathcal{F}(G)$.*

1. *S is zerofree if and only if $S = \prod_{i=1}^{k} e_i$ where $e_1, \ldots, e_k$ are linearly independent over $\mathbb{F}_2$.*
2. *$S \in \mathcal{U}^*(G)$ if and only if $S = \prod_{i=0}^{r} e_i$ where $(e_1, \ldots, e_r)$ is a basis of G and $e_0 = \sum_{i=1}^{r} e_i$.*

PROOF. Obvious; a detailed argument may be found in [Ge2; Lemma 3.10]. □

PROPOSITION 4.2. *Let $G = C_n$ with $n \ge 2$ and $S \in \mathcal{F}(G)$.*

1. *Suppose that S is zerofree of length $|S| \ge \frac{n+1}{2}$. Then S contains some $g \in G$ with $v_g(S) \ge 2|S| - n + 1$. Furthermore, if $|S| \ge \frac{3n}{4} - 1$, then $\mathrm{ord}(g) = n$.*

2. *If S is zerofree, then* $|\{h \in G \mid S \text{ contains } h\}| \le n - |S|$.

3. $S \in \mathcal{U}^*(G)$ *if and only if* $S = g^n$ *for some* $g \in G$ *with* $\operatorname{ord}(g) = n$.

PROOF. **1.** is proved in [B-E-N] and [Ga3; Lemma 2]. **2.** and **3.** are consequences of **1.** □

For a finite abelian group G let $\eta(G)$ denote the smallest integer $l \in \mathbb{N}_+$ such that every sequence $S \in \mathcal{F}(G)$ with $|S| \ge l$ contains a short zero subsequence.

LEMMA 4.3. *Let $G = C_p \oplus C_p$ for some prime p. Then we have*

1. $\eta(C_p \oplus C_p) \le 3p - 2$,

2. *Every sequence in G of length $3p-2$ contains a zero subsequence of length p or $2p$,*

3. *Every zero sequence $S \in G$ with $|S| \ge 2p$ contains a short zero subsequence.*

PROOF. **1.** and **2.** see [Ol2; Lemma 1.1].

3. This follows from [Ga4; Lemma 7] (with $H = C_p$ and $n = p$). □

LEMMA 4.4. $\eta(C_m \oplus C_m) \le 3m - 2$ *for every* $m \ge 2$.

PROOF. Let $m \ge 2$. We proceed by induction on the number of prime divisors on m. If m is a prime, the assertion follows from Lemma 4.3. Suppose $m = m_1 m_2$ with $1 < m_1, m_2 < m$ and consider the exact sequence

$$0 \longrightarrow C_{m_1} \oplus C_{m_1} \longrightarrow C_m \oplus C_m \xrightarrow{\varphi} C_{m_2} \oplus C_{m_2} \longrightarrow 0.$$

Let $S \in \mathcal{F}(G)$ be given with $|S| = 3m - 2$. Since

$$3m - 2 = (3m_1 - 3)m_2 + 3m_2 - 2 \text{ and } \eta(C_{m_2} \oplus C_{m_2}) \le 3m_2 - 2$$

we can find $3m_1 - 2$ disjoint subsequences $S_1, \ldots, S_{3m_1-2}$ of S with $|S_i| \le m_2$ and $\sigma(\varphi(S_i)) = 0$ for $1 \le i \le 3m_1 - 2$. Thus

$$\sigma(S_1), \ldots, \sigma(S_{3m_1-2}) \in \operatorname{Ker}(\varphi).$$

Since $\eta(C_{m_1} \oplus C_{m_1}) \le 3m_1 - 2$ there is a subset $I \subseteq \{1, \ldots, 3m_1 - 2\}$ with $|I| \le m_1$ such that $\prod_{i \in I} \sigma(S_i)$ is a zero sequence in $\operatorname{Ker}(\varphi) \subseteq C_m \oplus C_m$. Therefore $\prod_{i \in I} S_i$ is a zero subsequence of S with

$$\Big|\prod_{i \in I} S_i\Big| = \sum_{i \in I} |S_i| \le m_1 m_2 = m.$$ □

PROPOSITION 4.5. *Let G be a finite abelian group and $S \in \mathcal{F}(G)$.*

1. *If $|S| \ge |G|$, then S contains a zero subsequence T with $|T| \le \max\{v_g(S) \mid g \in G\}$.*

2. *If* $|S| \ge |G|$, *then* S *contains a zero subsequence* T *with* $|T| \le \max\{\mathrm{ord}(g) \mid g \in G \text{ with } v_g(S) > 0\}$.
3. *If* $|S| \ge |G| + \exp(G) - 1$, *then* S *contains a zero subsequence* T *with* $|T| = \exp(G)$.

PROOF. **1.** and **3.** are proved in [Ga-Y]. **2.** is a trivial consequence of **1.** □

5. The action of the automorphism group

Let G be a finite abelian group. Then the endomorphism ring $\mathrm{End}(G)$ acts on $\mathcal{F}(G)$ and on $\mathcal{B}(G)$. The automorphism group $\mathrm{Aut}(G) \subseteq \mathrm{End}(G)$ acts even on $\mathcal{U}(G)$ and on $\mathcal{U}^*(G)$. For $S \in \mathcal{F}(G)$ and $\tau \in \mathrm{Aut}(G)$ we write S^τ instead of $\tau(S)$.

In this section we deal with the following question: determine the groups G, for which $\mathrm{Aut}(G)$ acts transitively on $\mathcal{U}^*(G)$ (i.e., for each two sequences S, S' there exists some automorphism τ with $S^\tau = S'$). We answer the question for p-groups.

THEOREM 5.1. *Let* $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ *be a finite abelian group,* $(e_1, \ldots, e_r)$ *a basis of* G, $e_0 = \sum_{i=1}^r e_i$ *and* $A = e_0 \prod_{i=1}^r e_i^{n_i - 1} \in \mathcal{U}'(G) = \{S \in \mathcal{U}(G) \mid |S| = M(G)\}$. *Then the following conditions are equivalent:*

a) $\mathcal{U}'(G) = A^{\mathrm{Aut}(G)}$,

b) G *is either cyclic, an elementary 2-group or* $G \in \{C_3 \oplus C_3, C_2 \oplus C_4\}$.

PROOF. **b)** $\Rightarrow$ **a)** For cyclic groups and elementary 2-groups the assertion follows from Propositions 3.2, 4.1 and 4.2.

Suppose $G = C_3 \oplus C_3$ and $S \in \mathcal{U}'(G)$. Since by [M-W; Theorem 3.4] S is not squarefree, it follows that $S = g_1^2 g_2 S'$ with $g_2 \notin \langle g_1 \rangle$. By checking all possibilities it follows that $S' \in \{g_2(g_1 + g_2), (2g_1 + g_2)^2\}$ which implies the assertion.

Suppose $G = C_2 \oplus C_4$ and $S \in \mathcal{U}'(G)$. G has four elements of order four and every sum of two such elements is either zero or has order two. Since $D(C_2 \oplus C_2) = 3$, it follows that $S = h \prod_{i=1}^4 g_i$ with $\mathrm{ord}(h) = 2$ and $\mathrm{ord}(g_1) = \cdots = \mathrm{ord}(g_4) = 4$. Because $\prod_{i=1}^4 g_i$ is zerofree, one element, say $g = g_1$, occurs three times. Hence $S = hg^3(g + h)$, which implies the assertion.

a) $\Rightarrow$ **b)** Suppose that G is neither cyclic nor an elementary 2-group and $G \notin \{C_2 \oplus C_4, C_3 \oplus C_3\}$. Then $G = H \oplus C_n = \langle H, e_n \rangle$ with $n = \exp(G) \ge 3$. Let $\prod_{i=1}^d h_i \in \mathcal{U}(H)$ with $d = M(H)$.

For every $h \in H$ we set

$$S(h) = \prod_{i=1}^{d-1} h_i \cdot e_n^{n-3}(h + e_n)(-h + e_n)(h_d + e_n) \in \mathcal{U}'(G).$$

It is sufficient to find some $h \in H \setminus \{0\}$ such that $S(h) \notin S^{\mathrm{Aut}(G)}$ with $S = S(0)$.

CASE 1. $|H| \geq 4$. Take some $h \in H \setminus \{0, h_d, -h_d\}$. Then for every $\tau \in \mathrm{Aut}(G)$ we have

$$|\{g \in G \,|\, v_g(S^\tau) > 0\}| = |\{g \in G \,|\, v_g(S) > 0\}| < |\{g \in G \,|\, v_g(S(h)) > 0\}|$$

and hence $S(h) \neq S^\tau$.

CASE 2. $|H| \in \{2, 3\}$. Then $h_1 = \cdots = h_d, d = |H|$ and $n \geq 6$. Then for every $0 \neq h \in H$ we have

$$\max\{v_g(S) \,|\, g \in G\} = n - 1 > n - 3 = \max\{v_g(S(h)) \,|\, g \in G\}$$

and thus $S(h) \notin S^{\mathrm{Aut}(G)}$. □

COROLLARY 5.2. *For a p-group G the following conditions are equivalent:*

a) $\mathrm{Aut}(G)$ *acts transitively on* $\mathcal{U}^*(G)$,

b) G *is either cyclic or an elementary 2-group or* $G \in \{C_3^2, C_2 \oplus C_4\}$.

PROOF. Since for a p-group G Proposition 2.2 implies that $\mathcal{U}^*(G) = \mathcal{U}'(G)$, the assertion follows immediately from the previous Theorem. □

6. The order of elements in long minimal zero sequences

Let G be a finite abelian group. All explicitely constructed, minimal zero sequences $S \in \mathcal{U}(G)$ with $|S| \geq M(G)$, which hitherto appear in the literature (cf. [E1], [E2], [E3], [E-K], [Ma], [G-S1]), and all such sequences in this paper (cf. the proofs of the Theorems 3.3, 5.1 and 7.3) share the following property: they contain elements of order $\exp(G)$. Even more, some of them consist entirely of such elements. We start with the following conjecture which will be proved to hold true in various types of groups in Theorem 6.4.

CONJECTURE 6.1. *Let G be a finite abelian group and S a minimal zero sequence with $|S| = D(G)$. Then S contains some element $g \in G$ with* $\mathrm{ord}(g) = \exp(G)$.

A related question for a weighted form of Davenport's constant is studied in [G-S2]. A local version of 6.1 can be verified easily as the next result shows.

PROPOSITION 6.2. *Let G be a finite abelian group and S a minimal zero sequence with $|S| = D(G)$. Then* $\max\{v_p(\mathrm{ord}(g)) \,|\, g \in G \mathrm{with} g \,|\, S\} = v_p(\exp(G))$ *for every prime $p \in \mathbb{P}$.*

PROOF. Let T be a minimal zero sequence and suppose that there is a prime $p \in \mathbb{P}$ such that $\max\{v_p(\mathrm{ord}(g)) \,|\, g \in G \mathrm{with} g \,|\, S\} < v_p(\exp(G))$.

It is sufficient to construct a sequence $T' \in \mathcal{U}(G)$ having the following properties:

a) $|T| < |T'|$.

b) $\max\{v_p(\mathrm{ord}(g)) \mid g \mid T\} < \max\{v_p(\mathrm{ord}(g)) \mid g \mid T'\}$.

c) $\max\{v_q(\mathrm{ord}(g)) \mid g \mid T\} = \max\{v_q(\mathrm{ord}(g)) \mid g \mid T'\}$ for all primes $q \in \mathbb{P}\setminus\{p\}$.

Set $T = \prod_{i=1}^{l} g_i$ with $v_p(\mathrm{ord}(g_1)) \ge \cdots \ge v_p(\mathrm{ord}(g_l))$ and choose an element $g_0 \in G$ with $\mathrm{ord}(g_0) = p^{1+v_p(\mathrm{ord}(g_1))}$. It is easy to check that

$$T' = g_0^{p-1} \cdot (g_1 - (p-1)g_0) \cdot \prod_{i=2}^{l} g_i$$

satisfies the required properties. □

PROPOSITION 6.3. *Let $G = C_m \oplus C_n$ with $1 < m \mid n$ and S a minimal zero sequence with $|S| = D(G)$.*

1. *For every $g \in G$ with $g \mid S$ we have $m \mid \mathrm{ord}(g)$.*
2. *If $m < n$ and p is the smallest prime divisor of $\frac{n}{m}$, then S contains at least $m + n - \frac{n}{m}\left(\frac{2m-2}{p} + 1\right) \ge m$ elements of order n.*

PROOF. **1.** Set $S = gT$.

First we deal with the case $n = m$ and assume to the contrary that $\mathrm{ord}(g) = l < n = lk$. Consider the canonial epimorphism $\varphi : C_n \oplus C_n \to C_k \oplus C_k$ and the sequence $\varphi(T)$. Since $|T| = 2n-2 = (2l-3)k+(3k-2)$ and $\eta(C_k \oplus C_k) \le 3k-2$ by Lemma 4.4, there are $2l-2$ disjoint short zero subsequences $\varphi(S_1), \ldots, \varphi(S_{2l-2})$ of $\varphi(T) \in \mathcal{F}(C_k \oplus C_k)$. Set $S_{2l-1} = g$. Then $\sigma(S_i) \in \mathrm{Ker}(\varphi)$ for $1 \le i \le 2l-1$. Since $\mathrm{Ker}(\varphi) \simeq C_l \oplus C_l$ and $D(C_l \oplus C_l) = 2l-1$, there exists some $\emptyset \ne I \subseteq \{1, \ldots, 2l-1\}$ such that $\sum_{i \in I} \sigma(S_i) = 0 \in \mathrm{Ker}(\varphi)$. Thus $\prod_{i \in I} S_i$ is a proper zero subsequence of S, a contradiction.

Suppose now $m < n$ and consider the exact sequence

$$0 \longrightarrow C_{\frac{n}{m}} \hookrightarrow C_m \oplus C_n \xrightarrow{\varphi} C_m \oplus C_m \longrightarrow 0.$$

Then $|T| = m + n - 2 = m\left(\frac{n}{m} - 2\right) + (3m-2)$ and since $\eta(C_m \oplus C_m) \le 3m-2$ there are $\frac{n}{m} - 1$ disjoint short zero subsequences $\varphi(S_1), \ldots, \varphi(S_{\frac{n}{m}-1})$ of $\varphi(T)$. Set $T = S_0 \prod_{i=1}^{\frac{n}{m}-1} S_i$ and consider the sequence $\varphi(g \cdot S_0)$. Clearly, $\varphi(g \cdot S_0)$ is a zero sequence with length

$$|\varphi(g \cdot S_0)| = |g \cdot S_0| = 1 + |T| - \sum_{i=1}^{\frac{n}{m}-1} |T_i| \ge 1 + (m+n-2) - \left(\frac{n}{m} - 1\right) m = 2m - 1.$$

Since $\prod_{i=1}^{\frac{n}{m}-1} \sigma(S_i)$ is a zerofree sequence in $\mathcal{F}(\mathrm{Ker}(\varphi))$ and $D(\mathrm{Ker}(\varphi)) = \frac{n}{m}$, it follows that $\varphi(g \cdot S_0)$ is a minimal zero sequence. Therefore, the case $m = n$ implies that $\mathrm{ord}(\varphi(g)) = \exp(\varphi(G)) = m$ whence $m \mid \mathrm{ord}(g)$.

2. Suppose $m < n$, p the smallest prime divisor of $\frac{n}{m}$ and consider the exact sequence

$$0 \longrightarrow C_m \oplus C_m \hookrightarrow C_m \oplus C_n \xrightarrow{\varphi} C_{\frac{n}{m}} \longrightarrow 0.$$

We write S in the form $S = T \cdot U$ where T is the subsequence consisting of elements g with $\mathrm{ord}(g) < n$. Hence, if $g \mid T$, then by **1.** $m \mid \mathrm{ord}(g) \mid n = m\frac{n}{m}$. By assumption, $\frac{\mathrm{ord}(g)}{m}$ is a proper divisor of $\frac{n}{m}$ whence $\frac{\mathrm{ord}(g)}{m} \le \frac{n}{mp}$. Therefore $\mathrm{ord}(g) \le \frac{n}{p}$ whence $\mathrm{ord}(\varphi(g)) \le \frac{n}{mp}$. Assume that

$$|T| \ge \frac{n}{mp}(2m-2) + \frac{n}{m}.$$

By Proposition 4.5 (part **2.**) there exist $2m-1$ disjoint zero subsequences $\varphi(T_1), \ldots, \varphi(T_{2m-1})$ of $\varphi(T)$ with length $|\varphi(T_i)| \le \frac{n}{mp}$. Since $T' = \prod_{i=1}^{2m-1} \sigma(T_i) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ and $D(\mathrm{Ker}(\varphi)) = 2m-1$, T' and hence $\prod_{i=1}^{2m-1} T_i$ contains a non-empty zero subsequence. However, $\left|\prod_{i=1}^{2m-1} T_i\right| < 2m\frac{n}{mp} \le n < n+m-1 = |S|$ whence $\prod_{i=1}^{2m-1} T_i$ is a proper subsequence of S, a contradiction.

Therefore, we infer that

$$\begin{aligned} |U| &= |S| - |T| \\ &\ge (m+n-1) - \left(\frac{n}{mp}(2m-2) + \frac{n}{m} - 1\right) \\ &\ge m + n - \frac{n}{m}\left(\frac{2m-2}{p} + 1\right) \ge m. \end{aligned}$$

□

THEOREM 6.4. *Conjecture 6.1 holds for the following groups G:*

a) *G is a p-group,*

b) *G is cyclic,*

c) *G has rank two,*

d) *G is a direct sum of two elementary p-groups.*

PROOF. **a)** follows from Proposition 6.2, **b)** from Proposition 4.2 and **c)** from Proposition 6.3.

d) Let $G = C_p^r \oplus C_q^s$ and $S = \prod_{i=1}^{k} a_i \prod_{i=1}^{l} b_i \prod_{i=1}^{m} c_i \in \mathcal{U}^*(G)$ with $p, q \in \mathbb{P}, r, s \in \mathbb{N}_+, k, l, m \in \mathbb{N}, \mathrm{ord}(a_i) = p$, $\mathrm{ord}(b_i) = q$ and $\mathrm{ord}(c_i) = pq$. Then Lemma 3.1 implies that $m \ge 1$. □

7. Groups with large rank

Let G be a finite abelian group. Let $D_s(G)$ be defined as the minimum of all $d \in \mathbb{N}$ such that for every squarefree sequence $S \in \mathcal{F}(G)$ (equivalently, every subset $S \subseteq G$) with $|S| \ge d$ it follows that $0 \in \Sigma(S)$. This invariant was first

studied by Erdős and Heilbronn in 1964, for recent progress we refer to a paper by Hamidoune and Zemor (cf. [E-H, H-Z, Wh]). Note that by the very definition we have $D_s(G) \le D(G)$.

In this section we show by an explicit construction that groups with large rank r (e.g. with $r \ge 2\exp(G)$) have squarefree minimal zero sequences of length $M(G)$. As a consequence we obtain that $D_s(G) = M(G)$ for p-groups with large rank.

LEMMA 7.1. *Let G be a finite abelian group of order $|G| \ge 2$.*

1. *There exists a squarefree zero sequence $S \in \mathcal{F}(G)$ with $|S| = |G| - 1$.*
2. *Let $0 \ne g_0 \in G$ and $1 \le k \le \frac{|G|}{2} - 1$ with $k \ne 2$, if G is an elementary 2-group. Then there exists a squarefree zero sequence $S \in \mathcal{F}(G)$ with $g_0 \nmid S$ and $|S| = k$.*

PROOF. Let r be the 2-rank of G and $|G| = 2^r m$.

1. If $r \ne 1$, we set $g' = 0$; if $r = 1$, let g' denote the unique element of order 2. Then

$$S = \prod_{g \in G \setminus \{g'\}} g \in \mathcal{F}(G)$$

satisfies the required properties.

2. If $k = 1$, we set $S = 0 \in \mathcal{F}(G)$. From now on suppose $k \ge 2$. We distinguish two cases.

CASE 1. G is not an elementary 2-group. Then $m \ge 2$ and for $G' = \{g \in G \mid \mathrm{ord}(g) \ge 3\}$ we have

$$|G'| = |G| - 2^r = 2^r(m-1) = 2t \ge \frac{|G|}{2}$$

with $t \in \mathbb{N}_+$. Set

$$G' = \{-g_i, g_i \mid 1 \le i \le t\}$$

and suppose $g_0 = g_t$, if $g_0 \in G'$. Let $k \in \{2, \ldots, 2t-1\}$. For even k define

$$S = \prod_{i=1}^{k/2} (-g_i \cdot g_i)$$

and for odd$k$ define

$$S = 0 \cdot \prod_{i=1}^{(k-1)/2} (-g_i \cdot g_i).$$

Clearly, S is a squarefree zero sequence of length k with $g_0 \nmid S$.

CASE 2. G is an elementary 2-group. Hence $G = C_2^r$ and let $(g_0 = e_1, e_2, \ldots, e_r)$ be a basis of G. We treat the case $k = 3$. Since

$$3 \le \frac{|G|}{2} - 1 = 2^{r-1} - 1,$$

it follows $r \geq 3$. Clearly, $S = e_2 \cdot e_3 \cdot (e_2 + e_3)$ has the required properties. Now it is sufficient to verify the following assertion.

Assertion: for every $r \geq 4$ and every $k \in \{4, \ldots, 2^{r-1} - 1\}$ there exists a squarefree zero sequence $S \in \mathcal{F}(C_2^r)$ with $e_1 \nmid S$, $|S| = k$, $0 \nmid S$ for even k and $0 \mid S$ for odd$k$.

We proceed by induction on r. Let $r = 4$. For every $k \in \{4, \ldots, 7\}$ the following sequence S_k have the required properties:

$$S_4 = (e_2 + e_4)(e_3 + e_4)(e_2 + e_3 + e_4)e_4,$$
$$S_6 = (e_1 + e_2 + e_3)(e_2 + e_3)(e_1 + e_2 + e_3 + e_4)e_2 \cdot e_3 \cdot e_4,$$
$$S_5 = 0 \cdot S_4 \quad \text{and} \quad S_7 = 0 \cdot S_6.$$

Let $r \geq 5$; we conclude from $r - 1$ to r. Obviously, it suffices to show the assertion for even k. Let $4 \leq k = 2l \leq 2^{r-1} - 1$. If $k = 4$resp.6, take $S = S_4$ resp.$S = S_6$ as above. Suppose $k \geq 8$; then $4 \leq l \leq 2^{(r-1)-1} - 1$ and by induction hypothesis there exists a squarefree zero sequence $S' = \prod_{i=1}^{l} a_i \in \mathcal{F}(\langle e_1, \ldots, e_{r-1} \rangle)$ with $e_1 \nmid S'$, $0 \nmid S'$ for even l and $0 \mid S'$ for odd$l$.

If l is even, then

$$S = \prod_{i=1}^{l} a_i \prod_{i=1}^{l} (a_i + e_r)$$

satisfies the required properties. Let l be odd, suppose $a_1 = 0$ and choose some $b \in \langle e_1, \ldots, e_{r-1} \rangle \setminus \{0, a_2, \ldots, a_l, e_1 - a_2, a_3 - a_2, \ldots, a_l - a_2\}$. Then

$$S = e_r(b + e_r)(a_2 + b) \prod_{i=3}^{l} a_i \cdot \prod_{i=2}^{l} (a_i + e_r)$$

has the wanted properties. □

PROPOSITION 7.2. *Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$ and $H = \oplus_{i \in I} C_{n_i}$ with $I \subseteq \{1, \ldots r\}$ such that $\prod_{i=1}^{k} n_i \geq 2n_{k+1}$ for every $\max\{i \mid i \in I\} \leq k \leq r - 1$. If there exists a squarefree zerofree sequence $T \in \mathcal{F}(H)$ with $|T| = M(H) - 1$, then there exists a squarefree zero sequence S with $|S| = M(G)$.*

PROOF. It is sufficient to consider the case $G = H \oplus C_n$ where $\gcd\{n, \exp(H)\} = \min\{n, \exp(H)\}$, $M(G) = M(H) + n - 1$ and $|H| \geq 2n$. Then the general case follows by induction.

Let $\prod_{i=1}^{d} a_i \in \mathcal{F}(H)$ be a squarefree zerofree sequence with $d + 1 = M(H)$. Set $b_0 = -\sum_{i=1}^{d} a_i$ and $G = H \oplus < e_n >$. By the previous lemma there exists a squarefree zero sequence $\prod_{i=1}^{n-1} b_i \in \mathcal{F}(H)$ such that $b_0 \neq b_i$ for every $1 \leq i \leq n - 1$. Then, obviously

$$S = \prod_{i=1}^{d} a_i \prod_{i=0}^{n-1} (b_i + e_n)$$

is a squarefree minimal zero sequence with $|S| = M(G)$. □

THEOREM 7.3. *Let* $G = C_{n_1} \oplus \cdots \oplus C_{n_r} \oplus C_n^{s+1}$ *with* $r \ge 0, s \ge 0, 1 < n_1 \mid \ldots \mid n_r \mid n$ *and* $n_r \ne n$. *If* $r + \frac{s}{2} \ge n$, *then there exists a squarefree* $S \in \mathcal{U}(G)$ *with* $|S| = M(G)$.

PROOF. Set $n_{r+1} = \cdots = n_{r+s+1} = n_0 = n$ and let $(e_1, \ldots, e_{r+s}, e_{r+s+1} = e_0)$ be a basis of G with $\operatorname{ord}(e_i) = n_i$ for $1 \le i \le r+s+1$. By Lemma 7.1 there exist, for every $1 \le i \le r+s$, squarefree zero sequences $A_i = \prod_{j=1}^{n_i-1} a_j^{(i)} e_0 \in \mathcal{F}(< e_0 >)$ with $e_0 \nmid A_i$ if $n_i < n$. Define

$$S = \prod_{i=0}^{r+s} S_i \in \mathcal{F}(G)$$

where

$$S_i = \prod_{j=1}^{n_i-1} (e_i + a_j^{(i)} e_0) \quad \text{for} \quad 1 \le i \le r+s$$

and

$$S_0 = \prod_{j=1}^{\min\{r,n-1\}} (e_j + e_0) \prod_{j=1}^{n-1-r} (e_{r+2j-1} + e_{r+2j} + e_0) \cdot \Big(\sum_{j=\max\{n,2n-1-r\}}^{r+s} e_j + e_0 \Big)$$

We verify that S has the required properties. Clearly,

$$|S| = |S_0| + \sum_{i=1}^{r+s} |S_i| = n + \sum_{i=1}^{r+s} (n_i - 1) = M(G).$$

For every $1 \le i \le r+s$ we have

$$v_i(S) = v_i(S_i) + v_i(S_0) = (n_i - 1) + 1 \equiv 0 \mod n_i$$

and

$$v_0(S) = \sum_{i=1}^{r+s} \sum_{j=1}^{n_i-1} a_j^{(i)} + v_0(S_0) \equiv 0 \mod n.$$

Hence S is a zero sequence.

For every $1 \le i \le r+s$, the sequence S_i is squarefree since $|A_i| = |S_i| = n_i - 1$. By construction, $\prod_{i=1}^{r+s} S_i$ and S_0 are squarefree.

Since $e_0 \nmid A_i$ for $1 \le i \le r$, it follows that $\gcd\Big(\prod_{i=1}^{r+s} S_i, \prod_{j=1}^{\min\{r,n-1\}} (e_j + e_0)\Big) = 1$. Clearly, $\gcd\Big(\prod_{i=1}^{r+s} S_i, \prod_{j=1}^{n-1-r} (e_{r+2j-1} + e_{r+2j} + e_0)\Big) = 1$. Set

$$g = \sum_{j=\max\{n,2n-1-r\}}^{r+s} e_j + e_0;$$

if $r = n$ and $s = 0$, then $g = e_n + e_0 \nmid \prod_{i=1}^{r+s} S_i$, since $e_0 \nmid A_n = A_r$. In all other cases, our assumption $r + \frac{s}{2} \ge n$ implies

$$r + s - \big(\max\{n, 2n-1-r\} - 1\big) \ge 2$$

and hence $g \nmid \prod_{i=1}^{r+s} S_i$. Therefore, $\gcd\left(\prod_{i=1}^{r+s} S_i, S_0\right) = 1$ and hence S is squarefree.

It remains to show that S is a minimal zero sequence. For every $1 \le i \le r+s$,

$$v_i\left(\prod_{j=1}^{r+s} S_j\right) = v_i(S_i) = n_i - 1.$$

For every $g \in G$ with $g \mid \prod_{j=1}^{r+s} S_j$ there is an $i \in \{1, \dots, r+s\}$ with $v_i(g) \ge 1$. Thus $\prod_{j=1}^{r+s} S_j$ is zerofree. Let $1 \ne T = UV$ be a zero sequence with $U \mid \prod_{j=1}^{r+s} S_j$ and $V \mid S_0$. Since $\prod_{j=1}^{r+s} S_j$ is zerofree, it follows that $1 \le |V| \le |S_0| = n$. Let $1 \le i \le r+s$; if $v_i(V) > 0$ or $\gcd(S_i, U) \ne 1$, then $v_i(V) = v_i(S_0) = 1$ and $S_i \mid U$. However, this implies that

$$|V| = v_0(V) \equiv v_0(T) \equiv 0 \mod n.$$

Therefore, $|V| = n$ and $T = S$ follows. □

COROLLARY 7.4. *Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r} \oplus C_n^{s+1}$ with $r \ge 0, s \ge 0, 1 < n_1 \mid \dots \mid n_r \mid n$ and $n_r \ne n$. If G is a p-group and $r + \frac{s}{2} \ge n$, then $D_s(G) = M(G)$.*

PROOF. By the above Theorem we infer that

$$M(G) = D_s(G) \le D(G) = M(G).$$ □

8. Groups with large exponent

This section is dual to the previous one. We study groups with large exponent and present two results showing that long minimal zero sequences in such groups contain one element quite often.

THEOREM 8.1. *Let $G = C_m \oplus C_{mn}$ be a finite abelian group with integers $n > m+1 \ge 3$, $\varphi : G \to H = C_m \oplus C_m$ the canonical epimorphism and $S \in \mathcal{U}^*(G)$. If $h^k \mid \varphi(S)$ for some $k \ge m+1$ and some $h \in H$, then $g^k \mid S$ for some $g \in \varphi^{-1}(h)$.*

REMARK. Let all notations be as above and suppose $n \ge m^2$. Then $\frac{|S|}{|H|} = \frac{mn+m-1}{m^2} > m$ and hence there exists an element $h \in H$ such that $h^{m+1} \mid \varphi(S)$.

PROOF. Obviously, $\mathrm{Ker}(\varphi)$ is cyclic of order n and, by Proposition 3.2, $|S| = mn + m - 1$.

Using Lemma 4.4 one can find $n-1$ disjoint subsequences $W_1, \dots, W_{n-1}$ of S such that $\varphi(W_1), \dots, \varphi(W_{n-1})$ are short zero subsequences of $\varphi(S)$. In particular, we have $\sigma(W_i) \in \mathrm{Ker}(\varphi)$ for every $1 \le i \le n-1$.

Since S is a minimal zero sequence and $1 \le |W_1 \dots W_{n-1}| \le (n-1)m < |S|$ the sequences

$$W_1 \dots W_{n-1} \text{and hence } \sigma(W_1) \dots \sigma(W_{n-1})$$

are zerofree. Now it follows from Proposition 4.2, that

$$(*) \qquad \sigma(W_1) = \sigma(W_2) = \cdots = \sigma(W_{n-1}).$$

Suppose $h^k \mid \varphi(S)$ for some $k \geq m+1$ and some $h \in H$. Then S contains a subsequence $g_1 \ldots g_k$ with $\varphi(g_1) = \cdots = \varphi(g_k) = h$ and it suffices to verify that

$$g_1 = \cdots = g_k.$$

Assume to the contrary that this does not hold. Since $k \geq m+1$, one can find a subsequence U_1 of $g_1 \ldots g_k$ with length m such that $\sigma(U_1) \neq \sigma(W_1)$. However, $\varphi(g_i) = h$ for $1 \leq i \leq k$ implies that $\sigma(U_1) \in \mathrm{Ker}(\varphi)$.

Since $|U_1| = m < n-1$, we may assume that U_1 and W_1 are disjoint. Using Lemma 4.4 again we obtain $n-3$ disjoint subsequences $V_1, \ldots, V_{n-3}$ of $S(U_1W_1)^{-1}$ such that

$$\sigma(V_i) \in \mathrm{Ker}(\varphi) \quad \text{and} \quad 1 \leq |V_i| \leq m$$

for $1 \leq i \leq n-3$. Similarly to the proof of $(*)$ we infer that

$$\sigma(U_1) = \sigma(W_1) = \sigma(V_1) = \cdots = \sigma(V_{n-3}),$$

a contradiction. □

THEOREM 8.2. *Let $G = G' \oplus C_{mn}$ be a finite abelian group where G' is a direct summand with $\exp(G') \mid m$ and $n \geq 4|G'| > 4(m-2)$. Let $\varphi : G \to H = G' \oplus C_m$ denote the canonical epimorphism and let $S \in \mathcal{F}(G)$ be a zerofree sequence with $|S| = \exp(G) = mn$. Then S contains a subsequence T with $|T| \geq (n-2|G'|+1)m$ such that the following holds: if $h^k \mid \varphi(T)$ for some $k \geq m+1$ and some $h \in H$, then $g^k \mid T$ for some $g \in \varphi^{-1}(h)$.*

REMARK. Let all notations be as above and suppose that $n > m|G'| + 2|G'| - 1$. Then

$$\frac{|T|}{|H|} \geq \frac{(n-2|G'|+1)m}{m|G'|} = \frac{n-2|G'|+1}{|G'|} > m$$

and thus there exists an element $h \in H$ such that $h^{m+1} \mid \varphi(T)$.

PROOF. Throughout, we shall use that $\mathrm{Ker}(\varphi)$ is a cyclic group of order n.

Define Ω as the system containing all sets A of the following form:

A contains $n - |G'|$ disjoint subsequences $S_1, \ldots, S_{n-|G'|}$ of S such that

$$|S_i| = m \text{and} \sigma(S_i) \in \mathrm{Ker}(\varphi) \text{ for every} 1 \leq i \leq n - |G'|.$$

By applying Lemma 4.5 to $\varphi(S)$ we derive that $\Omega \neq \emptyset$.

Let $A = \{S_1, \ldots, S_{n-|G'|}\} \in \Omega$ and set $h_i = \sigma(S_i)$, for $1 \leq i \leq n - |G'|$. Since S is zerofree, the same is true for $h_1 h_2 \ldots h_{n-|G'|}$. Using $|G'| \leq \frac{n}{4}$ and Proposition 4.2 we infer that

$$h_1 \ldots h_{n-|G'|} = a^t g_1 \ldots g_{n-|G'|-t}$$

with $t \geq n - 2|G'| + 1$, $\operatorname{ord}(a) = n$ and $g_i \neq a$ for $i = 1, \ldots, n - |G'| - t$.

Note that

$$t + n - 2|G'| + 1 \geq 2(n - 2|G'| + 1) > n - |G'| = |h_1 \ldots h_{n-|G'|}|$$

therefore a is the unique element which occurs at least $n - 2|G'| + 1$ times in $h_1 \ldots h_{n-|G'|}$, denote t by $t(A)$, then $t(A)$ is determined by A.

Choose some $A \in \Omega$ with

$$t(A) = \min\{t(B) \mid B \in \Omega\}$$

and set $t = t(A)$. Suppose $S_1, \ldots, S_t$ be the t sequences in A so that

$$\sigma(S_1) = \cdots = \sigma(S_t) = a,$$

put $T = S_1 \ldots S_t$, then

$$|T| = |S_1| + \cdots + |S_t| = mt \geq (n - 2|G'| + 1)m.$$

We make the following assertion:

Assertion: If W is a subsequence of T with $\sigma(W) \in \operatorname{Ker}(\varphi)$ and $|W| = m$, then $\sigma(W) = a$.

First we show how the Assertion implies the Theorem. Suppose $h^k \mid \varphi(T)$ for some $k \geq m + 1$ and some $h \in H$. Then there are $g_1, \ldots, g_k \in \varphi^{-1}(h)$ such that $g_1 \ldots g_k \mid T$. Let $I \subseteq \{1, \ldots, k\}$ with $|I| = m$ and $W = \prod_{i \in I} g_i$. Then $\sum_{i \in I} \varphi(g_i) = mh = 0$ whence $\sum_{i \in I} g_i = \sigma(W) \in \operatorname{Ker}(\varphi)$. Thus the Assertion implies that $\sigma(W) = a$.

Since this is true for every such W it follows that $g_1 = \cdots = g_k$.

PROOF OF THE ASSERTION. Assume to the contrary, that there exists a subsequence W of T with length m such that $\sigma(W) \in \operatorname{Ker}(\varphi)$ but $\sigma(W) \neq a$. Without loss of generality, we may assume that $S_1, \ldots, S_u$ are the all sequences of $S_1, \ldots, S_t$ such that S_i and W are not disjoint for $1 \leq i \leq u$. Since $|W| = m$, we have $u \leq m$. Suppose $A = \{S_1, \ldots, S_u, S_{u+1}, \ldots, S_t, Q_1, \ldots, Q_{n-|G'|-t}\}$ and set

$$R = S(WS_{u+1} \ldots S_t Q_1 \ldots Q_{n-|G'|-t})^{-1}.$$

Applying Proposition 4.5 to R one can get $u - 1$ disjoint subsequences $P_1, \ldots, P_{u-1}$ of R having length m such that

$$\sigma(P_i) \in \operatorname{Ker}(\varphi)$$

for every $1 \leq i \leq u - 1$.

Obviously, $B = \{S_{u+1}, \ldots, S_t, Q_1, \ldots, Q_{n-|G'|-t}, W, P_1, \ldots, P_{u-1}\} \in \Omega$. By the choice of $S_1, \ldots, S_t$ we may infer that

$$\sigma(Q_i) \neq a$$

for every $1 \leq i \leq n - |G'| - t$. This together with $\sigma(W) \neq a$ shows that a occurs in

$$V \overset{\text{def}}{=} \sigma(S_{u+1}) \ldots \sigma(S_t)\sigma(Q_1) \ldots \sigma(Q_{n-|G'|-t})\sigma(W)\sigma(P_1) \ldots \sigma(P_{u-1})$$

at most $t-1$ times. Because $t(B) \ge t(A) > t-1$ there exists an element $b \neq a$ such that $b^{t(B)} \mid V$. Using $a^{t-u} \mid V$ we derive that

$$\begin{aligned} n - |G'| = |A| = |V| &\ge t(B) + t - u \ge 2t - m \\ &\ge 2(n - 2|G'| + 1) - m \\ &\ge n - |G'| + (n - 4|G'|) + (|G'| + 2 - m) \\ &> n - |G'|, \end{aligned}$$

a contradiction. □

9. A polynomial method

There exists a huge variety of techniques in which polynomials are applied for deriving consequences in additive group theory and combinatorial number theory (for a survey cf. [A11, A12, Na]). In this section we discuss a polynomial method for the investigation of the structure of zerofree sequences (cf. Proposition 9.2 and Theorem 10.3).

Let R be a commutative ring with identity, $l \in \mathbb{N}_+$, and $A \subseteq R[\mathbf{X}] = R[X_1, \ldots, X_l]$ a set of polynomials. Then the set

$$\mathcal{V}(A) = \{\boldsymbol{c} \in R^l \mid f(\boldsymbol{c}) = 0 \quad \text{for every} \quad f \in A\} \subseteq R^l$$

of all common zeros in R^l of the polynomials of A is called the *variety* of A. If $A = \{f_1, \ldots, f_m\}$, then we set $\mathcal{V}(f_1, \ldots, f_m) = \mathcal{V}(A)$. For $\boldsymbol{c} \in R^l$ let

$$\begin{aligned} \mathrm{ev}_{\boldsymbol{c}} : R[\boldsymbol{X}] &\longrightarrow R \\ f &\mapsto f(\boldsymbol{c}) \end{aligned}$$

denote the *evaluation homomorphism*.

Suppose now that for every $f \in A$ we have $\mathcal{V}(f) \neq R^l$ (i.e., f does not vanish identically on R^l). Then the set A is called *single-valued*, if $A \subseteq \mathrm{ev}_{\boldsymbol{c}}^{-1}(b)$ for some $\boldsymbol{c} \in R^l$ and some $b \in R \setminus \{0\}$. Define $\mathsf{r}(A)$ as the minimal $r \in \mathbb{N} \cup \{\infty\}$ such that $A = \bigcup_{i=1}^{r} A_i$ with single-valued sets A_i.

Since $\mathcal{V}(f) \neq R^l$, the set $\{f\}$ is single-valued whence A is a union of single-valued sets. Furthermore, we have $\mathsf{r}(A) = 0$ if and only if $A = \emptyset$ and $\mathsf{r}(A) = 1$ if and only if A is single-valued.

Define

$$A(l) = \Big\{ \sum_{i \in I} X_i \,|\, \emptyset \neq I \subseteq \{1, \ldots, l\} \Big\} \subseteq R[\boldsymbol{X}]$$

and for a sequence $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ in a finite abelian group G set

$$A(S) = \Big\{ \sum_{i \in I} X_i \in A(l) \,|\, \sum_{i \in I} g_i = 0, \emptyset \neq I \subseteq \{1, \ldots, l\} \Big\}.$$

Our aim is to study sequences S by studying the $\mathbf{r}$ invariant of $A(l)$ and $A(S)$. In this section we concentrate on $\mathbf{r}(A(l))$ and shift the applications to the next section.

Before going into details we give a geometric interpretation of the $\boldsymbol{r}$ invariant of a subset of homogenous linear polynomials, which was pointed out to us by the referee. Let R be a commutative ring with identity and $A \subset H = \{\sum_{j=1}^{l} c_j X_j \mid c_1, \ldots, c_l \in R\}$ a set of homogenous linear polynomials. Then there is a one-to-one correspondence between the set $A \subset R[\boldsymbol{X}]$ and the set of points $\overline{A} = \{(c_1, \ldots, c_l) \mid \sum_{j=1}^{l} c_j X_j \in A\} \subseteq R^l$. In particular, $A(l)$ corresponds to the $2^l - 1$ non-zero vertices of the unit cube $\{0,1\}^l \subseteq R^l$. If

$$A \subseteq \bigcup_{i=1}^{r} \mathrm{ev}_{\boldsymbol{a}_i}^{-1}(b_i)$$

with the above assumptions, then

$$\mathrm{ev}_{\boldsymbol{a}_i}^{-1}(b_i) \cap H = \left\{ \sum_{j=1}^{l} a_j X_j \in H \mid \sum_{j=1}^{l} a_j c_{i,j} = b_i \right\}$$

for every $1 \le i \le r$. Thus a point $\boldsymbol{a} \in R^l$ corresponds to a polynomial of the above set if and only if $\boldsymbol{a}$ lies on the affine hyperplane defined by $\sum_{j=1}^{l} c_{i,j} X_j = b_i$. Therefore, $\boldsymbol{r}(A)$ is the minimal number of hyperplanes covering $\overline{A}$ and $\boldsymbol{r}(A(l))$ is the minimal number of hyperplanes covering all non-zero vertices of the unit cube $\{0,1\}^l$ of the ring R. For some historical remarks of this covering problem we refer to the introduction in [Al-Fu]. In a recent paper ([Al2, Theorem 6.3]) Alon showed that $\boldsymbol{r}(A(l)) \ge l$ for integral domains R (for $R = Z/p\mathbb{Z}$ this was done by Gao in [Ga1] and for $R = \mathbb{R}$ the reals by Alon and Füredi in [Al-Fu, Theorem 1]). We study the $\boldsymbol{r}$ invariant of $A(l)$ by a fresh approach suitable for arbitrary commutative rings with identity which leads to a new proof of $\boldsymbol{r}(A(l)) = l$ for integral domains (see Prop. 9.4, part **3.**).

LEMMA 9.1. *Let R be a commutative ring with identity, $l \in \mathbb{N}_+$ and $A \subset R[\boldsymbol{X}]$ with $\mathcal{V}(f) \neq R^l$ for every $f \in A$.*

1. $\mathbf{r}(A) \le |A|$.
2. $\mathbf{r}(A) \le |\mathrm{ev}_{\mathbf{c}}(A)|$ *for every* $\mathbf{c} \in R^l$ *with* $0 \notin \mathrm{ev}_{\mathbf{c}}(A)$.
3. $\mathbf{r}(A \cup B) \le \mathbf{r}(A) + \mathbf{r}(B)$ *for every subset* $B \subseteq R[\mathbf{X}]$ *with* $\mathcal{V}(f) \neq R^l$ *for every* $f \in B$.
4. *If* $B \subseteq A$ *and* $\mathbf{r}(B) < \mathbf{r}(A)$, *then* $A \setminus B \neq \emptyset$.

PROOF. **1.** holds, since $A = \bigcup_{f \in A} \{f\}$ and $\{f\}$ is single-valued.

2. and **3.** are obvious.

To verify **4.** let $B \subseteq A$ with $\mathbf{r}(B) < \mathbf{r}(A)$. Then **3.** implies that $\mathbf{r}(B) < \mathbf{r}(A) \le \mathbf{r}(B) + \mathbf{r}(A \setminus B)$ whence $\mathbf{r}(A \setminus B) \neq 0$ and $A \setminus B \neq \emptyset$. □

PROPOSITION 9.2. *Let R be a commutative ring with identity, G a finite abelian group and $S \in \mathcal{F}(G)$ a sequence with length $l \in \mathbb{N}_+$. If $\mathsf{r}(A(l) \setminus A(S)) < \mathsf{r}(A(l))$, then S is not zerofree.*

PROOF. If $\mathsf{r}(A(l) \setminus A(S)) < \mathsf{r}(A(l))$, then Lemma 9.1.4 implies that $A(l) \setminus (A(l) \setminus A(S)) = A(S) \neq \emptyset$. Thus S contains a proper subsequence with sum zero i.e., S is not zerofree. □

LEMMA 9.3. *Let R be a commutative ring with identity and $l, k \in \mathbb{Z}$ with $l > k \geq 1$.*

1. *The following polynomial identity holds in $R[X, Y_{i,j} \mid 1 \leq i \leq k, 1 \leq j \leq l]$:*

$$\sum_{\emptyset \neq J \subseteq \{1,\ldots,l\}} (-1)^{|J|} \prod_{i=1}^{k} \Big(X - \sum_{j \in J} Y_{i,j} \Big) = -X^k .$$

2. *Let $C \in M_{k,l}(R)$ be a matrix with column vectors $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_l \in R^k$ and $\boldsymbol{b} = (b_1, \ldots, b_k) \in R^k$ a column vector such that $\prod_{i=1}^{k} b_i^k \neq 0$. Then there exists a subset $\emptyset \neq J \subseteq \{1, \ldots, l\}$ such that the vectors $\sum_{j \in J} \boldsymbol{c}_j$ and $\boldsymbol{b}$ are different in all coordinates.*

PROOF. **1.** Obviously,

$$\sum_{\emptyset \neq J \subseteq \{1,\ldots,l\}} (-1)^{|J|} \prod_{i=1}^{k} \Big(X - \sum_{j \in J} Y_{i,j} \Big) = \sum_{r=0}^{k} \sum_{\mathbf{i},\mathbf{j}} c(\mathbf{i},\mathbf{j}) Y_{i_1,j_1} \ldots Y_{i_r,j_r}$$

where $c(\mathbf{i},\mathbf{j}) \in R[X]$ and the sum runs over all $\mathbf{i} = (i_1, \ldots, i_r) \in \{1, \ldots, k\}^r$ and all $\mathbf{j} = (j_1, \ldots, j_r) \in \{1, \ldots, l\}^r$. If $r = 0$, then

$$c(\emptyset) = \sum_{\emptyset \neq J \subseteq \{1,\ldots,l\}} (-1)^{|J|} X^k = X^k \sum_{\nu=1}^{l} (-1)^{\nu} \binom{l}{\nu} = -X^k .$$

Let $1 \leq r \leq k, \mathbf{i} = (i_1, \ldots, i_r)$ and $\mathbf{j} = (j_1, \ldots, j_r)$. If not all of the $i_1, \ldots, i_r$ are pairwise distinct, then $c(\mathbf{i},\mathbf{j}) = 0$. Otherwise, if $\{j_1, \ldots, j_r\} = J'$ and $|J'| = d$ with $1 \leq d \leq r \leq k < l$, then

$$\begin{aligned} c(\mathbf{i},\mathbf{j}) &= \sum_{J' \subseteq J \subseteq \{1,\ldots,l\}} (-1)^{|J|} (-1)^r X^{k-r} \\ &= (-1)^r X^{k-r} \sum_{\nu=0}^{l-d} (-1)^{|J'|+\nu} \binom{l-d}{\nu} = 0 . \end{aligned}$$

2. For $1 \leq i \leq k$ and $1 \leq j \leq l$ we set

$$\boldsymbol{c}_j = \begin{pmatrix} c_{1,j} \\ \vdots \\ c_{k,j} \end{pmatrix}, \qquad x = \prod_{\nu=1}^{k} b_\nu \qquad \text{and} \qquad y_{i,j} = c_{i,j} \prod_{\substack{\nu=1 \\ \nu \neq i}}^{k} b_\nu .$$

Then **1.** implies that

$$\sum_{\emptyset \neq J \subseteq \{1,\ldots,l\}} (-1)^{|J|} \prod_{i=1}^{k} \Big(x - \sum_{j \in J} y_{i,j} \Big) = -x^k \neq 0 \,.$$

Therefore there exists a non-empty subset $J \subseteq \{1,\ldots,l\}$ such that

$$\prod_{i=1}^{k} \Big(x - \sum_{j \in J} y_{i,j} \Big) \neq 0$$

whence $x \neq \sum_{j \in J} y_{i,j}$ and $\sum_{j \in J} c_{i,j} \neq b_i$ for every $1 \leq i \leq k$. □

PROPOSITION 9.4. *Let R be a commutative ring with identity and $l \in \mathbb{N}_+$.*

1. *For every $1 \leq k \leq l$ we have*

$$1 \leq \mathsf{r}(A(k)) \leq \mathsf{r}(A(l)) \leq \mathsf{r}(A(k)) + (l-k) \leq l.$$

2. *If $\mathrm{char}(R) = n$, p a proper prime divisor of n and $l \geq p+1$, then $\mathsf{r}(A(l)) < l$.*

3. *If R is an integral domain, then $\mathsf{r}\big(A(l)\big) = l$.*

PROOF. **1.** Since $A(1) = \{X_1\}$ is single-valued, it follows that $\mathsf{r}(A(1)) = 1$. If $1 \leq k \leq l$, then $A(k) \subseteq A(l)$ whence $\mathsf{r}(A(k)) \leq \mathsf{r}(A(l))$ by Lemma 9.1.3. We show that $\mathsf{r}(A(l+1)) \leq \mathsf{r}(A(l)) + 1$ from which the remaining assertions follow by induction. Since $B = \{X_{l+1}\} + (A(l) \cup \{0\})$ is single-valued and $A(l+1) = A(l) \cup B$, Lemma 9.1.3 implies that $\mathsf{r}(A(l+1)) \leq \mathsf{r}(A(l)) + 1$.

2. Suppose $\mathrm{char}(R) = n$, $\mathbb{Z}/n\mathbb{Z} \hookrightarrow R$ and p a proper prime divisor of n. For $1 \leq i \leq p+1$ set $A_i = \big\{ \sum_{i \in I} X_i \mid I \subseteq \{1,\ldots,p+1\}, |I| = i \big\}$ whence $A(p+1) = \bigcup_{i=1}^{p+1} A_i$. For $1 \leq i \leq p+1$ we have $\mathsf{ev}_{\boldsymbol{c}}(A_i) = i + n\mathbb{Z} \neq n\mathbb{Z}$ where $\boldsymbol{c} = (1+n\mathbb{Z}, \ldots, 1+n\mathbb{Z})$ whence A_i is single-valued. Furthermore, $A_1 \cup A_{p+1}$ is single-valued, since $\mathsf{ev}_{\boldsymbol{c}}(A_1) = \frac{n}{p} + n\mathbb{Z} = \mathsf{ev}_{\boldsymbol{c}}(A_{p+1})$ where $\boldsymbol{c} = \Big(\frac{n}{p} + n\mathbb{Z}, \ldots, \frac{n}{p} + n\mathbb{Z} \Big)$. Since $A(p+1) = (A_1 \cup A_{p+1}) \cup \bigcup_{i=2}^{p} A_i$, it follows that $\mathsf{r}(A(p+1)) \leq p$. Thus **1.** implies that $\mathsf{r}(A(l)) \leq l-1$ for every $l \geq p+1$.

3. Let R be an integral domain and assume to the contrary, that $k = \mathsf{r}\big(A(l)\big) < l$. Then

$$A(l) = \bigcup_{j=1}^{k} A_j$$

with single-valued sets $A_1, \ldots, A_k$. Hence there are elements $\boldsymbol{c}_i = (c_{i,1}, \ldots, c_{i,l}) \in R^l$ such that for every $1 \leq i \leq k$,

$$\mathsf{ev}_{\boldsymbol{c}_i}(A_i) = b_i \qquad \text{for some} \qquad b_i \in R \setminus \{0\}.$$

Therefore, for every $\emptyset \neq J \subseteq \{1,\ldots,l\}$ there is some $i \in \{1,\ldots,k\}$ such that $\sum_{j \in J} X_j \in A_i$ and hence

$$\Big(\sum_{j \in J} X_j \Big)(\boldsymbol{c}_i) = \sum_{j \in J} c_{i,j} = b_i.$$

This is a contradiction to Lemma 9.3.2 (where the matrix C is built from the row vectors $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k \in R^l$ and $\boldsymbol{b} = (b_1, \ldots, b_k)$). □

10. Elementary abelian p-groups

Elementary p-groups may be viewed as vector spaces over the finite field $\mathbb{F}_p$. This allows to apply vector space methods and many combinatorial problems simplify considerably. Apart from being of interest for their own rights, a profound knowledge of elementary p-groups often makes it possible to study problems on arbitrary abelian groups by inductive methods i.e., if $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $p \mid n_1 \mid \ldots \mid n_r$, one considers the exact sequence

$$0 \longrightarrow C_p^r \longrightarrow G \longrightarrow \bigoplus_{i=1}^{r} C_{n_i/p} \longrightarrow 0.$$

Combinatorial properties of elementary p-groups have been studied very extensively. Hence we just can refer the reader to [A-L-M], [M-W] or [Pe] to catch an impression of the progress achieved in this area.

Our first aim is to derive a structural result (Theorem 10.3) for maximal zerofree sequences, which heavily depends on the work of Section 9. We start with a lemma.

LEMMA 10.1. *Let $G = C_p^r, R = \mathbb{Z}/p\mathbb{Z}$ with p prime, $r \in \mathbb{N}_+$ and $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)$. Then $\mathsf{r}(A(l) \setminus A(S)) \le r(p-1)$.*

PROOF. Let $(e_1, \ldots, e_r)$ be a basis of G and $g_i = \sum_{\nu=1}^{r} c_{\nu,i} e_\nu$ with $c_{\nu,i} \in \mathbb{Z}$ for every $1 \le i \le l$. For every $\nu \in \{1, \ldots, r\}$ and every $m \in \{1, \ldots, p-1\}$ the set

$$A_{\nu,m} = \Big\{ \sum_{i \in I} X_i \in A(l) \,|\, \emptyset \ne I \subseteq \{1, \ldots, l\} \text{ with } \sum_{i \in I} (c_{\nu,i} + p\mathbb{Z}) = m + p\mathbb{Z} \Big\}$$

is single-valued, since for $\mathbf{c}_\nu = (c_{\nu,1} + p\mathbb{Z}, \ldots, c_{\nu,l} + p\mathbb{Z}) \in R^l$ we have

$$\mathrm{ev}_{\mathbf{c}_\nu}(A_{\nu,m}) = \sum_{i \in I} (c_{\nu,i} + p\mathbb{Z}) = m + p\mathbb{Z} \in R \setminus \{0\}.$$

Obviously, it is sufficient to verify that

$$A(l) \setminus A(S) \subseteq \bigcup_{\nu=1}^{r} \bigcup_{m=1}^{p-1} A_{\nu,m}.$$

Let $f = \sum_{i \in I} X_i \in A(l) \setminus A(S)$ be given. Then $\sum_{i \in I} g_i \ne 0$ which implies that there is some $\nu \in \{1, \ldots, r\}$ such that $\sum_{i \in I} c_{\nu,i} e_\nu \ne 0$. Thus $\sum_{i \in I} (c_{\nu,i} + p\mathbb{Z}) = m + p\mathbb{Z}$ for some $m \in \{1, \ldots, p-1\}$ i.e., $f \in A_{\nu,m}$. □

In order to show how our method works we give a new proof of the following well known result.

COROLLARY 10.2. *$D(C_p^r) = r(p-1)+1$ for p prime and $r \in \mathbb{N}_+$.*

PROOF. By Proposition 3.2.1 it is sufficient to verify that $D(C_p^r) \le r(p-1)+1 = l$. Let $S = \prod_{i=1}^{l} g_i$ be a sequence in $\mathcal{F}(C_p^r)$. We have to show that S is not zerofree. Lemma 10.1 and Proposition 9.4 imply that

$$\mathbf{r}(A(l) \setminus A(S)) \le r(p-1) < l = \mathbf{r}(A(l)).$$

Hence S is not zerofree by Proposition 9.2. □

THEOREM 10.3. *Let G be an elementary p-group and $S \in \mathcal{F}(G)$ a zerofree sequence with $|S| = D(G)-1$. Then each two distinct elements of S are linearly independent.*

PROOF. Suppose $G = C_p^r$ with p prime, $r \in \mathbb{N}_+$, $R = \mathbb{Z}/p\mathbb{Z}$, $S = gg' \prod_{i=1}^{l} g_i$ with $l = D(G)-3 = r(p-1)-2$ and suppose that $\langle g \rangle = \langle g' \rangle$. We have to show that $g = g'$. For $r = 1$ this follows from Proposition 4.2. Suppose $r \ge 2$ and choose a basis $(g = e_1, e_2, \ldots, e_r)$ of G. Then $g_i = c_i e_1 + h_i$ with $c_i \in \mathbb{Z}$ and $h_i \in H = \langle e_2, \ldots, e_r \rangle$ for every $1 \le i \le l$ and let $T = \prod_{i=1}^{l} h_i \in \mathcal{F}(H)$. Then Lemma 10.1 implies that

$$\mathbf{r}(A(l) \setminus A(T)) \le (r-1)(p-1).$$

Lemma 9.1.3 and Proposition 9.4 yield that

$$l = \mathbf{r}\big(A(l)\big) \le \mathbf{r}(A(l) \setminus A(T)) + \mathbf{r}(A(T))$$

whence

$$\mathbf{r}(A(T)) \ge l - (r-1)(p-1) = p-3.$$

Since $0 \notin \Sigma\Big(\prod_{i=1}^{l} g_i\Big)$, it follows that

$$0 \notin \Big\{ \sum_{i \in I} c_i + p\mathbb{Z} \mid \emptyset \ne I \subseteq \{1, \ldots, l\} \text{ with } \sum_{i \in I} h_i = 0 \in H \Big\} = \mathrm{ev}_{\boldsymbol{c}}(A(T))$$

for $\boldsymbol{c} = (c_1 + p\mathbb{Z}, \ldots, c_l + p\mathbb{Z}) \in R^l$. Therefore by Lemma 9.1.2 we infer that

$$|\,\mathrm{ev}_{\boldsymbol{c}}(A(T))\,| \ge \mathbf{r}(A(T)) \ge p-3.$$

By assumption, $g' = cg$ with $c \in \{1, \ldots, p-1\}$ and hence $\Sigma(gg') = \{g, cg, (1+c)g\}$. Since $S = gg' \prod_{i=1}^{l} g_i$ is zerofree and $|\,\mathrm{ev}_{\boldsymbol{c}}(A(T))\,| \ge p-3$, it follows that $|\,\Sigma(gg')\,| \le 2$. This implies that $c = 1$ whence $g = g'$. □

The following result was anticipated by van Emde Boas in [E2; pp. 18].

PROPOSITION 10.4. *Let $G = C_p^r$ for some odd prime p and some $r \ge 2$. If $S \in \mathcal{U}^*(G)$ with $\max\{v_g(S) \mid g \in G\} = p-1$ and if $\max\{v_g(T) \mid g \in C_p^i\} = p-1$ for*

every $1 < i < r$ *and every* $T \in \mathcal{U}^*(C_p^i)$, *then*

$$S = \prod_{i=1}^{r-1}\Big(\prod_{j=1}^{p-1}\Big(e_i + \sum_{k=1}^{i-1} a_{k,j}^{(i)} e_k\Big)\Big) \prod_{j=1}^{p}\Big(e_r + \sum_{k=1}^{r-1} a_{k,j}^{(r)} e_k\Big)$$

for some basis $(e_1, \ldots, e_r)$ *of* G *and integers* $a_{k,j}^{(i)} \in \mathbb{Z}$ *such that* $\sum_{i=k+1}^{r-1} \sum_{j=1}^{p-1} a_{k,j}^{(i)} + \sum_{j=1}^{p} a_{k,j}^{(r)} \equiv 1 \mathrm{mod} p$ *for every* $1 \le k \le r-1$.

Conversely, every sequence of such a form lies in $\mathcal{U}^*(G)$.

PROOF. Consider a sequence S of the above form. For every $1 \le k \le r-1$ we have

$$v_k(S) = p - 1 + \sum_{i=k+1}^{r-1} \sum_{j=1}^{p-1} a_{k,j}^{(i)} + \sum_{j=1}^{p} a_{k,j}^{(r)} \equiv 0 \mathrm{mod} p$$

and obviously

$$v_r(S) = p \equiv 0 \mathrm{mod} p.$$

Hence S is a zero sequence. Let S' be a zero subsequence of S.. Let $m \in \{1, \ldots, r\}$ be maximal with $v_m(S') > 0$. Then $v_m(S') \equiv 0 \mathrm{mod} p$ implies that $m = r$. We consider step by step $v_r(S'), v_{r-1}(S') \ldots$ to infer that $S' = S$. Thus S is a minimal zero sequence and obviously $|S| = (r-1)(p-1) + p = D(G)$.

Conversely, let $S \in \mathcal{U}^*(G)$ be given with $\max\{v_g(S) \mid g \in G\} = p - 1$ and suppose that $\max\{v_g(T) \mid g \in C_p^i\} = p-1$ for every $1 < i < r$ and every $T \in \mathcal{U}^*(C_p^i)$. We proceed by induction on r.

Let $r = 2$. Suppose that $v_{e_1}(S) = p - 1$ for some $e_1 \in G$. Choose some $e_2' \in G \setminus \langle e_1 \rangle$. Thus (e_1, e_2') is a basis of G and

$$S = e_1^{p-1} \prod_{j=1}^{p} (a_j' e_1 + b_j e_2')$$

with integers $a_1', \ldots, a_p', b_1, \ldots, b_p$.

Since for every $1 \le j \le p$ the sequence $e_1^{p-1}(a_j' e_1) \in \mathcal{F}(C_p)$ contains a zero subsequence, it follows that $b_j \ne 0$ for all $1 \le j \le p$.

Assume to the contrary, that not all b_j are equal. Then, by Proposition 3.2 there exists some $\emptyset \ne I \subsetneq \{1, \ldots, p\}$ such that $\prod_{i \in I} b_i e_2'$ is a zero sequence in $\mathcal{F}(C_p)$. Then

$$e_1^k \prod_{i \in I} (a_i' e_1 + b_i e_2')$$

with $0 \le k \le p-1$ and $k \equiv -\sum_{i \in I} a_i' \mod p$, is a proper zero subsequence of S, a contradiction. Therefore, $b_1 = \cdots = b_p = b$.

Finally, set $e_2 = a_1' e_1 + b e_2'$. Then (e_1, e_2) is a basis and

$$S = e_1^{p-1} \prod_{j=1}^{p} (a_j e_1 + e_2)$$

with integers $a_1, \ldots, a_p$. Obviously, $\sum_{j=1}^{p} a_j \equiv 1 \mod p$.

To do the induction step, let $r \geq 3$ be given. We conclude from $r-1$ to r. Suppose $S = e_1^{p-1}T$ for some $0 \neq e_1 \in G$ and some $T \in \mathcal{F}(G)$. Extend e_1 to a basis $(e_1, \ldots, e_r)$ of $G = C_p^r$ and consider the canonical epimorphism

$$\varphi : G \to H = \oplus_{i=2}^{r} < e_i >$$

with $\varphi(e_1) = 0$ and $\varphi(e_i) = e_i$ for $2 \leq i \leq r$. Then $\varphi(S) = 0^{p-1}\varphi(T)$; clearly, $\varphi(T)$ is a zero sequence with $|\varphi(T)| = D(C_p^{r-1})$. Let T' be a subsequence of T such that $\varphi(T')$ is a minimal zero subsequence. Then there is some $l \in \{0, \ldots, p-1\}$ such that $e_1^l T'$ is a zero subsequence of S. This implies that $S = e_1^{p-1}T = e_1^l T'$ whence $T = T'$ and $\varphi(T)$ is a minimal zero sequence in C_p^{r-1}. Therefore, induction hypothesis reveals the structure of $\varphi(T)$ which implies the assertion. □

COROLLARY 10.5. *Let $G = C_p \oplus C_p$ for some odd prime p and $S = \prod_{i=1}^{s} g_i^{m_i} \in \mathcal{U}^*(G)$ with pairwise distinct g_i and $m_1 \geq \cdots \geq m_s \geq 1$.*

1. $3 \leq s \leq p+1$.
2. *If $m_1 = p-1$, then $S = e_1^{p-1} \prod_{i=1}^{p}(a_i e_1 + e_2)$ for some basis (e_1, e_2) of G and integers $a_1, \ldots, a_p \in \mathbb{Z}$ with $\sum_{i=1}^{p} a_i \equiv 1 \mod p$. Conversely, every sequence of such a form lies in $\mathcal{U}^*(G)$.*
3. *For every $j \in \{3, \ldots, p\}$ there is a sequence in $\mathcal{U}^*(G)$ containing exactly j distinct elements.*

PROOF. **1.** Since $|S| = D(G) = 2p-1 = \sum_{i=1}^{s} m_i \leq s(p-1)$, it follows that $s \geq 3$. If $p = 3$, then there are $g_1, \ldots, g_4 \in G$ with $G = \{0, g_1, -g_1, \ldots, g_4, -g_4\}$ whence $s \leq 4$. Suppose $p \geq 5$ and set $S = g_1 T$. By Theorem 10.3 $|\{g \in G \mid v_g(T) > 0\}|$ is bounded by the number of one-dimensional subspaces of $\mathbb{F}_p^2$ which equals $\frac{p^2-1}{p-1} = p+1$ whence

$$|\{g \in G \mid v_g(T) > 0\}| \leq p+1 < 2p-2 = |T|.$$

Therefore T is not squarefree which implies $m_1 \geq 2$ and thus $s = |\{g \in G \mid v_g(S) > 0| = |\{g \in G \mid v_g(T) > 0\}| \leq p+1$.

2. This follows from Proposition 10.4.

3. Let (e_1, e_2) be a basis of G and $j \in \{3, \ldots, p\}$. We give an explicit example of some $S_j \in \mathcal{U}^*(G)$ containing exactly j distinct elements. If j is odd, then

$$S_j = e_1^{p-1} e_2^{p-(j-2)} (e_1 + e_2) \prod_{i=2}^{\frac{j-1}{2}} (ie_1 + e_2)(-ie_1 + e_2)$$

has the required properties. For even j we set

$$S_j = e_1^{p-1} e_2^{p-(j-2)} \left(\frac{p-1}{2} e_1 + e_2\right) \left(\frac{p+3}{2} e_1 + e_2\right) \prod_{i=1}^{\frac{j-4}{2}} (ie_1 + e_2)(-ie_1 + e_2).$$

□

For every integer $n \geq 2$ we consider the following two properties:

PROPERTY B. *Every sequence* $S \in \mathcal{U}^*(C_n \oplus C_n)$ *contains some element* $(n-1)$ *times.*

PROPERTY C. *Every sequence* $S \in \mathcal{F}(C_n \oplus C_n)$ *of length* $3n-3$ *which does not contain a short zero subsequence has the form* $S = a^{n-1}b^{n-1}c^{n-1}$ *for some* $a, b, c \in C_n \oplus C_n$.

Recall that every element g contained in a sequence $S \in \mathcal{U}^*(C_n \oplus C_n)$ has order n by Proposition 6.3. By Theorem 10.3 a prime p satisfies property B if and only if every sequence $S \in \mathcal{U}^*(C_p \oplus C_p)$ contains $p-1$ elements of a proper subgroup $H \subsetneq C_p \oplus C_p$. If a prime p satisfies property B, then the structure of all sequences $S \in \mathcal{U}^*(C_p \oplus C_p)$ is completely determined by Corollary 10.5. *Property B* has been verified for $2, 3, 5$ and 7 and we conjecture that it holds for all primes.

In [E1] van Emde Boas studies a variant of *Property C* and conjectures that it holds for all primes (cf. page 4 and page 36). The equivalence of the van Emde Boas-Property and of *Property C* above was shown in [Ga5; Lemma 4.7]. *Property C* has been verified for $2, 3, 5$ and 7. Its significance stems from investigations of Davenport's constant for groups of rank 3 (cf. [E3] and [Ga5]). Furthermore, if two integers k, l satisfy *Property C*, then so does their product kl (cf. [Ga6]).

As a final result in this paper we show that every prime, which satisfies *Property B*, also satisfies *Property C*. Both properties hold for $p = 2$. Hence from now on we restrict to odd primes. Let p be an odd prime. For $a \in \mathbb{Z}$ let $|a|_p \in \{1, \ldots, p\}$ be such that $a \equiv |a|_p \bmod p$. The following fact follows from Lemma 4.3.3 and will be used several times: if a sequence in $\mathcal{F}(C_p \oplus C_p)$ has no short zero subsequence, then it does not contain a zero subsequence of length $2p$.

We start with a lemma.

LEMMA 10.6. *Let* $G = C_p \oplus C_p$ *for some odd prime* p *and* $S = a^{p-1}b^{p-1}\prod_{i=1}^{p} c_i \in \mathcal{F}(G)$ *a sequence which does not contain a short zero subsequence. If* p *satisfies Property B, then* $c_1 = \cdots = c_{p-1}$.

PROOF. Let S be as above and suppose that it does not contain a short zero subsequence. Then $(e_1 = a, e_2 = b)$ is a basis of G and S has the form

$$S = e_1^{p-1}e_2^{p-1}\prod_{i=1}^{p-1}(x_i e_1 + y_i e_2)$$

with $x_i, y_i \in \{1, \dots, p\}$. Since S has no zero subsequence of length p or $2p$, the same is true for

$$S_{e_2} = (e_1 - e_2)^{p-1} 0^{p-1} \prod_{i=1}^{p-1} (x_i e_1 + (y_i - 1)e_2) .$$

Therefore

$$(e_1 - e_2)^{p-1} \prod_{i=1}^{p-1} (x_i(e_1 - e_2) + (x_i + y_i - 1)e_2)$$

is zerofree. Therefore $\prod_{i=1}^{p-1}(x_i + y_i - 1)e_2$ is zerofree in $< e_2 > \simeq C_p$ whence

$$x_1 + y_1 \equiv \cdots \equiv x_{p-1} + y_{p-1} \mathrm{mod} p.$$

Since for every $1 \le i \le p-1$

$$e_1^{p-x_i} e_2^{p-y_i} (x_i e_1 + y_i e_2)$$

is a zero subsequence of S of length $2p + 1 - (x_i + y_i)$, it follows that $x_i + y_i \le p$. Thus

$$x_1 + y_1 = \cdots = x_{p-1} + y_{p-1} = m$$

for some m with $2 \le m \le p$.

If $m = 2$, then $x_1 = y_1 = \cdots = x_{p-1} = y_{p-1} = 1$ and the assertion is proved.

Suppose $m = p$. If $\prod_{i \in I} x_i e_1$ is a zero sequence for some $\emptyset \neq I \subseteq \{1, \dots, p-1\}$, then the same is true for $\prod_{i \in I} y_i e_2$ and thus $\prod_{i \in I}(x_i e_1 + y_i e_2)$ would be a zero sequence. Since S contains no short zero subsequence, $\prod_{i=1}^{p-1} x_i e_1$ is zerofree whence $x_1 = \cdots = x_{p-1}$. Therefore $y_1 = \cdots = y_{p-1}$ and the assertion is proved.

Suppose that $3 \le m \le p-1$. Then there is a unique $t \in \{2, \dots, p-2\}$ such that $t(m-1) \equiv 1 \mathrm{mod} p$; thus $|tm|_p = t + 1$. Obviously, it is sufficient to show that for every subset $I \subseteq \{1, \dots, p-1\}$ with $|I| = t$ all x_i resp. all y_i with $i \in I$ are equal.

Let $I \subseteq \{1, \dots, p-1\}$ with $|I| = t$ and consider the sequence

$$S_I = e_1^{p - |\Sigma_{i \in I} x_i|_p} e_2^{p - |\Sigma_{i \in I} y_i|_p} \prod_{i \in I} (x_i e_1 + y_i e_2) .$$

Clearly, S_I is a zero subsequence of S of length

$$\begin{aligned} |S_I| &= 2p + t - |\Sigma_{i \in I} x_i|_p - |\Sigma_{i \in I} y_i|_p \\ &= 2p + t - |\Sigma_{i \in I} x_i|_p - |tm - \Sigma_{i \in I} x_i|_p \\ &= \begin{cases} 2p + t - |tm|_p = 2p - 1 , & |tm|_p > |\Sigma_{i \in I} x_i|_p \\ 2p + t - (p + |tm|_p) = p - 1 , & |tm|_p \le |\Sigma_{i \in I} x_i|_p \end{cases} \end{aligned}$$

However, since S has no short zero subsequence, we infer that $|tm|_p > |\Sigma_{i \in I} x_i|_p$ and that S_I is a minimal zero sequence. Thus $S_I \in \mathcal{U}^*(G)$. Since $t \le p-2$ and $\{x_i e_1 + y_i e_2 \mid i \in I\} \cap \{e_1, e_2\} = \emptyset$, *Property B* implies that either

$$p - |\Sigma_{i \in I} x_i|_p = p - 1 \text{ or } p - |\Sigma_{i \in I} y_i| = p - 1 .$$

Therefore either

$$e_2^{p-|\Sigma_{i\in I}y_i|_p}\prod_{i\in I}y_ie_2 \text{ or } e_1^{p-|\Sigma_{i\in I}x_i|_p}\prod_{i\in I}x_ie_1$$

is a minimal zero sequence which implies that either all y_i are equal to 1 or all x_i are equal to 1. □

THEOREM 10.7. *Every prime having Property B also satisfies Property C.*

PROOF. We may suppose that p is an odd prime and set $G = C_p \oplus C_p$. Let $S \in \mathcal{F}(G)$ be a sequence of length $3p-3$ which does not contain a short zero subsequence. Since by Lemma 4.3.2 the sequence $0.S$ contains a zero subsequence of length p or $2p$, the sequence S contains a zero subsequence T of length $|T| \in \{p-1, p, 2p-1, 2p\}$. Therefore $|T| = 2p-1$ and T is a minimal zero sequence. Hence by *Property B* there is some $b \in G$ with $b^{p-1} \mid T$ and thus

$$S = b^{p-1}\prod_{i=1}^{2p-2} c_i\,.$$

Since S has no zero subsequence of length p or $2p$, the same is true for

$$S_b = 0^{p-1}\prod_{i=1}^{2p-2}(c_i-b)\,.$$

Therefore $\prod_{i=1}^{2p-2}(c_i-b)$ is zerofree and $c\prod_{i=1}^{2p-2}(c_i-b)\in\mathcal{U}^*(G)$ with $c=-\sum_{i=1}^{2p-2}(c_i-b)$. Next we use *Property B*. If there is some $g \in G$ such that $g^{p-1} \mid \prod_{i=1}^{2p-2}(c_i-b)$, then $b^{p-1}(g+b)^{p-1} \mid S$ and the assertion follows from Lemma 10.6. Hence suppose that

$$c^{p-2} \mid \prod_{i=1}^{2p-2}(c_i-b)$$

and without restriction we may further suppose that $c = c_1 - b$. Since S contains no short zero subsequence, we infer that $c+b \notin < b >$. Therefore $(e_1 = c_1 = c+b, e_2 = b)$ is a basis of G and S has the form

$$S = e_1^{p-2}e_2^{p-1}\prod_{i=1}^{p}(x_ie_1+y_ie_2)$$

with $x_i, y_i \in \{1,\dots,p\}$.

Setting

$$S_{e_2} = 0^{p-1}(e_1-e_2)^{p-2}\prod_{i=1}^{p}(x_ie_1+(y_i-1)e_2)$$

and arguing as above we infer that

$$(e_1-e_2)^{p-2}\prod_{i=1}^{p}(x_ie_1+(y_i-1)e_2)$$

is zerofree. Therefore

$$(e_1 - e_2)^{p-1} \prod_{i=1}^{p} \big(x_i(e_1 - e_2) + (x_i + y_i - 1)e_2\big)$$

is a minimal zero sequence, since

$$0 = c_1 - b + \sum_{i=1}^{2p-2} (c_i - b) = c_1 + b + \sum_{i=1}^{2p-2} c_i$$

$$= e_1 + e_2 + (p-2)e_1 + \sum_{i=1}^{p} (x_i e_1 + y_i e_2)\,.$$

Clearly, $(e_1 - e_2, e_2)$ is a basis of G whence $\prod_{i=1}^{p}(x_i + y_i - 1)e_2 \in \mathcal{U}^*(< e_2 >)$ which implies that

$$x_1 + y_1 \equiv \cdots \equiv x_p + y_p \mathrm{mod} p.$$

Let $1 \le i \le p$; if $x_i = 1$ and $y_i = p$, then $e_1^{p-1} e_2^{p-1} \mid S$ and the assertion follows from Lemma 10.6. We exclude this case and assert that

$$(*) \qquad 3 \le x_1 + y_1 = \cdots = x_p + y_p \le p - 1.$$

Assume to the contrary that $x_i + y_i \ge p + 1$. Then $x_i \ge 2$ and

$$e_1^{p-x_i} e_2^{p-y_i} (x_i e_1 + y_i e_2)$$

is a zero subsequence of S with length $2p + 1 - (x_i + y_i) \le p$, a contradiction. Thus

$$x_1 + y_1 = \cdots = x_p + y_p = m$$

for some m with $2 \le m \le p$.

Assume that $m = p$. There is a non-empty subset $I \subseteq \{1, \ldots, p\}$ such that $\Sigma_{i \in I} x_i e_1 = 0$. This implies that $\Sigma_{i \in I} y_i e_2 = 0$ whence $\prod_{i \in I}(x_i e_1 + y_i e_2)$ is a short zero subsequence of S, a contradiction.

Assume that $m = 2$; then $x_1 = y_1 = \ldots x_p = y_p = 1$ whence $\prod_{i=1}^{p}(x_i e_1 + y_i e_2)$ is a short zero subsequence of S, a contradiction.

Therefore $(*)$ is proved. Hence there is a unique $t \in \{2, \ldots, p-2\}$ such that $t(m-1) \equiv 1 \mathrm{mod} p$ and thus $|tm|_p = t + 1$.

Let $I \subseteq \{1, \ldots, p\}$ be a subset with $|I| = t$ and $\Sigma_{i \in I} x_i \not\equiv 1 \mathrm{mod} p$. Then $2 \le |\Sigma_{i \in I} x_i|_p \le p$,

$$S_I = e_1^{p - |\sum_{i \in I} x_i|_p} e_2^{p - |\sum_{i \in I} y_i|_p} \prod_{i \in I} (x_i e_1 + y_i e_2)$$

is a minimal zero subsequence of S with length $|S_I| = 2p - 1$; thus either all x_i are equal to 1 or all y_i are equal to 1 (argue as in Lemma 10.6).

Therefore, for every subset $I \subseteq \{1, \ldots, p\}$ with $|I| = t$ we have:

$$(**) \qquad \text{either} \Sigma_{i \in I} x_i \equiv 1 \mathrm{mod} p \text{ or all } x_i \text{are equal to 1 or} m - 1\,.$$

Assume to the contrary, that there are three distinct elements among $x_1, \ldots, x_p$; without restriction $x_{p-2} \neq x_{p-1} \neq x_p \neq x_{p-2}$. Since $t-1 \leq p-3$, it follows that $|\{x_j + \sum_{i=1}^{t-1} x_i \,|\, p-2 \leq j \leq p\}| = 3$, a contradiction to (**).

Therefore, $\prod_{i=1}^{p} x_i e_1 = (xe_1)^u (x'e_1)^v$ with $x, x' \in \{1, \ldots, p\}$, $x \neq x'$, $u+v=p$ and $0 \leq v \leq u$. If $v \leq 1$, then $u \geq p-1$ and Lemma 10.6 implies the assertion.

Assume to the contrary, that $2 \leq v \leq u$. If $t \geq 3$, one can choose $u_0 \in \{2, \ldots, u-1\}$ and $v_0 \in \{1, \ldots, v-1\}$ such that $u_0 + v_0 = t$ because $t \leq p-2 = u+v-2$. However,

$$u_0 x + v_0 x' \neq (u_0 - 1)x + (v_0 + 1)x'$$

which contradicts (**). Hence suppose $t = 2$. Using (**) we infer that $x + x' \equiv 1 \bmod p$. Thus $x + x \not\equiv x + x' \equiv 1 \bmod p$ whence $x \in \{1, m-1\}$. We argue in a similar way for x' and obtain $\{x, x'\} = \{1, m-1\}$. Therefore $m = x + x' \equiv 1 \bmod p$, a contradiction to $3 \leq m \leq p-1$. □

REFERENCES

[A-G-P] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmicheal numbers *Ann. Math.* **140** (1994), 703–722.

[Al1] N. Alon, Tools from higher Algebra, in: *Handbook of Combinatorics II*, North Holland, 1995, 1749–1783.

[Al2] N. Alon, Combinatorial Nullstellensatz.

[A-D1] N. Alon and M. Dubiner, A lattice point problem and additive number theory, *Combinatorica* **15** (1995), 301–309.

[A-D2] N. Alon and M. Dubiner, Zero-sum sets of prescribed size, in: *Combinatorics, Paul Erdős is Eighty*, Vol 1, J. Bolyai Math. Soc., 1993, 33–50.

[Al-Fu] N. Alon and F. Füredi, Covering the cube by affine hyperplanes *Europ. J. Combinatorics* **14** (1993), 79–83.

[A-F-K] N. Alon, S. Friedland and G. Kalai, Regular subgraphs of almost regular graphs, *J. Combin. Theory Ser. B* **37** (1984), 79–91.

[A-L-M] N. Alon, N. Linial and R. Meshulam, Additive bases of vector spaces over prime fields, *J. Comb. Th. Ser. A* **57** (1991), 203–210.

[An] D. D. Anderson, *Factorization in integral domains*, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker **189**, 1997.

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

[B-L] A. Bialostocki and M. Lotspeich, Some developments of the Erdős–Ginzburg–Ziv Theorem, in: *Sets, Graphs and Numbers*, Coll. Math. Soc. J. Bolyai **60**, 1992, 97–117.

[B-S] R. C. Baker and W. Schmidt, Diophantine problems in variables restricted to the values of 0 and 1, *J. Number Theory* **12** (1980), 460–486.

[Ca1] Y. Caro, Zero-sum subsequences in abelian non-cyclic groups *Israel J. Math.* **92** (1995), 221–233.

[Ca2] Y. CARO, Remarks on a zero-sum theorem *J. Comb. Th. Ser. A* **76** (1996), 315–322.

[Ca3] Y. CARO, Zero-sum problems — A survey, *Discrete Math.* **152** (1996), 93–113.

[Ch] S. CHAPMAN, On the Davenport's constant, the cross number and their application in factorization theory, in: *Zero-dimensional commutative rings*, Lecture Notes in Pure Appl. Math., Marcel Dekker, **171**, 1995, 167–190.

[Ch-Ge] S. CHAPMAN AND A. GEROLDINGER, Krull domains and monoids, their sets of lengths and associated combinatorial problems, in: *Factorization in Integral Domains*, Lecture Notes in Pure and Applied Mathematics **189**, Marcel Dekker, 1997, 73–112.

[D-M] G. T. DIDERRICH AND H. B. MANN, Combinatorial problems in finite abelian groups, in: *A survey of combinatorial theory*, edited by J. N. Srivastava, North-Holland, 1973.

[E1] P. VAN EMDE BOAS, A combinatorial problem on finite abelian groups II, *Reports* ZW-1969-007, Math. Centre, Amsterdam.

[E2] P. VAN EMDE BOAS, Some combinatorial properties of the group $C_3 \oplus C_3 \oplus C_3$, *Reports* ZW-1969-010, Math. Centre, Amsterdam.

[E3] P. VAN EMDE BOAS, An ALGOL-60 algorithm for the verification of a combinatorial conjecture on a finite abelian group, *Reports* ZW-1969-014, Math. Centre, Amsterdam.

[E-K] P. VAN EMDE BOAS AND D. KRUYSWIJK, A combinatorial problem on finite abelian groups III, *Reports* ZW-1969-008, Math. Centre, Amsterdam.

[E-G] P. ERDŐS AND R. L. GRAHAM, *Old and new problems and results in combinatorial number theory*, Monographie N. 28 de L'Enseignement Mathématique, Université de Genève, 1980.

[E-H] P. ERDŐS AND H. HEILBRONN, On the addition of residue classes mod p, *Acta Arith.* **9** (1964), 149–159.

[F-K] Z. FÜREDI AND D. J. KLEITMAN, The minimal number of zero sums, in: *Combinatorics, Paul Erdős is Eighty*, Vol 1, J. Bolyai Math. Soc., 1993, 159–172.

[Ga1] W. GAO, On the additivity of integers, *Adv. Math.* **19** (1990), 488–492.

[Ga2] W. GAO, Some problems in additive number theory and additive group theory, Ph. thesis, Sichuan University, 1994.

[Ga3] W. GAO, An addition theorem for finite cyclic groups, *Discrete Math.* **163** (1997), 257–265.

[Ga4] W. GAO, On a combinatorial problem connected with factorizations, *Colloq. Math.* **72** (1997), 251–268.

[Ga5] W. GAO, On Davenport's constant of finite abelian groups with rank three, *Discrete Math.*

[Ga6] W. GAO, Two zero-sum problems and multiple properties.

[Ga-Ge1] W. GAO AND A. GEROLDINGER, On the structure of zerofree sequences, *Combinatorica* **18** (1998), 519–527.

[Ga-Ge2] W. GAO AND A. GEROLDINGER, Half-factorial domains and half-factorial subsets of abelian groups, *Houston J. Math.* **24** (1998), 593–611.

[Ga-Ge3] W. GAO AND A. GEROLDINGER, Systems of sets of lengths II.

[Ga-Y] W. GAO AND Y. X. YANG, Note on a combinatorial constant, *J. Math. Res. and Expo.* **17** (1997), 139–140.

[Ge1] A. GEROLDINGER, On a conjecture of Kleitman and Lemke, *J. Number Th.* **44** (1993), 60–65.

[Ge2] A. GEROLDINGER, The catenary degree and tameness of factorizations in weakly Krull domains, in: *Factorization in Integral Domains*, Lecture Notes in Pure and Applied Mathematics **189**, Marcel Dekker, 1997, 113–153.

[G-S1] A. GEROLDINGER AND R. SCHNEIDER, On Davenport's constant, *J. Combin. Theory Ser. A* **61** (1992), 147–152.

[G-S2] A. GEROLDINGER AND R. SCHNEIDER, The cross number of finite abelian groups, III, *Discrete Math.* **150** (1996), 123–130.

[H-O-O] Y. O. HAMIDOUNE, O. ORDAZ AND A. ORTUNIO, On a combinatorial theorem of Erdős, Ginzburg and Ziv.

[H-Z] Y. O. HAMIDOUNE AND G. ZEMOR, On zero-free subset sums, *Acta Arith.* **78** (1996), 143–152.

[H-R] G. HARCOS AND I. Z. RUZSA, A problem on zero subsums in abelian groups, *Periodica Math. Hungarica* **35** (1997), 31–34.

[K-L] D. KLEITMAN AND P. LEMKE, An addition theorem on the integers modulo n, *J. Number Th.* **31** (1989), 335–345.

[Ma1] H. B. MANN, *Addition theorems: the addition theorems of group theory and number theory*, Interscience Publishers, J. Wiley& Sons, 1965.

[Ma2] H. B. MANN, Additive group theory — a progress report *Bull. American Math. Soc.* **79** (1973), 1069–1075.

[M-W] H. B. MANN AND YING FOU WOU, An addition theorem for the elementary abelian group of type (p,p), *Mh. Math.* **102** (1986), 273–308.

[Ma] M. MAZUR, A note on the growth of Davenport's constant *Manuscripta Math.* **74** (1992), 229–235.

[Me] R. MESHULAM, An uncertainty inequality and zero subsums, *Discr. Math.* **84** (1990), 197–200.

[Na] M. B. NATHANSON, *Additive Number Theory*, GTM **165**, Springer, 1996.

[Ol1] J. E. OLSON, A combinatorial problem on finite abelian groups, I, *J. Number Th.* **1** (1969), 8–10.

[Ol2] J. E. OLSON, A combinatorial problem on finite abelian groups, II, *J. Number Th.* **1** (1969), 195–199.

[Pe] C. PENG, Addition theorems in elementary abelian groups, I–II, *J. Number Th.* **27** (1987), 46–57, 58–62.

[Wh] È. T. WHITE, Ordered sums of group elements, *J. Comb. Th. Ser. A* **24** (1978), 118–121.

(Received: January 15, 1999)

WEIDONG GAO
DEPARTMENT OF COMPUTER SCIENCE AND TECHNOLOGY
UNIVERSITY OF PETROLEUM, BEIJING
SHUIKU ROAD, CHANGPING
BEIJING 102200, P.R. CHINA
E-MAIL: wdgao@mail.bjpeu.edu.cn

ALFRED GEROLDINGER
INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
HEINRICHSTRASSE 36
8010 GRAZ
AUSTRIA
E-MAIL: alfred.geroldinger@kfunigraz.ac.at