Periodica Mathematica Hungarica Vol. 44 (1), 2002, pp. 63–73

ON THE ORDER OF ELEMENTS IN LONG MINIMAL ZERO-SUM SEQUENCES

WEIDONG GAO (Beijing) AND ALFRED GEROLDINGER (Graz)

[Communicated by: Attila Pethő]

Abstract

Let G be a finite abelian group and $S = \prod_{i=1}^{l} g_i$ a minimal zero-sum sequence in G of maximal length $|S| = l$. We study the order of the elements $g_1, \ldots, g_l$.

1. Introduction and Main Results

Let G be an additively written, finite abelian group. For every $n \in \mathbb{N}$ we denote by C_n the cyclic group with n elements. Then $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid \cdots \mid n_r$ if $|G| > 1$ and with $r = n_1 = 1$ if $|G| = 1$. Furthermore, $r = r(G)$ is the *rank* of G, $n_r = \exp(G)$ is the *exponent* of G and we set $M(G) = 1 + \sum_{i=1}^{r}(n_i - 1)$.

We study sequences in G and for convenience we recall some basic terminology (we use the same notations as in [GG99] and refer to this paper for details). Let $\mathcal{F}(G)$ denote the free abelian monoid with basis G and let $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ be a *sequence* in G. Then $|S| = l \in \mathbb{N}_0$ is called the *length* of S and $\sigma(S) = \sum_{i=1}^{l} g_i \in G$ the *sum* of S. We say that S is a *zero-sum sequence*, if $\sigma(S) = 0$ and that S is a *minimal zero-sum sequence* if no proper subsequence has sum zero. *Davenport's constant* $\mathcal{D}(G)$ of G is defined as the maximal length of a minimal zero-sum sequence in G.

It is a straightforward observation that $M(G) \le \mathcal{D}(G)$. About thirty years ago J.E. Olson and D. Kruyswijk proved independently that equality holds for p-groups and for groups G with rank $r(G) \le 2$ (see [vEB69], [Ols69a], [Ols69b]). It is still unknown whether equality holds for all groups with rank three (for some recent development see [Gao00]), but for every $r \ge 4$ there are infinitely many groups G with rank r and with $M(G) < \mathcal{D}(G)$ (see [GS92]). However, up to now there is no satisfactory explanation neither for the phenomenon $M(G) = \mathcal{D}(G)$ nor for $M(G) < \mathcal{D}(G)$.

In recent work it has been tried to obtain some information about the structure of minimal zero-sum sequences whose length is equal or close to $\mathcal{D}(G)$ (see [GG99]). A good knowledge about the structure of such sequences is of high importance for

Key words and phrases: finite abelian groups, zero-sum sequences

0031-5303/02/$5.00

Akadémiai Kiadó, Budapest
Kluwer Academic Publishers, Dordrecht

applications in factorization theory (see [And97]). Furthermore, it will allow further progress in determining Davenport's constant (see [Gao00]) and will provide a new insight in the phenomenon $M(G) = \mathcal{D}(G)$.

Among others the following property of finite abelian groups has been studied:

Property : Every minimal zero-sum sequence $S \in \mathcal{F}(G)$ with length $|S| = \mathcal{D}(G)$ contains some element g with $\mathrm{ord}(g) = \exp(G)$.

We conjecture that every finite abelian group G has this property and in [GG99] this was proved for p-groups and for groups with rank $r(G) \le 2$ among others. An analogous property plays an important role in the investigation of cross numbers of minimal zero-sum sequences (see [GS96], Lemma 1).

We discuss the following two refinements of the above question and ask for groups G satisfying one of the following two properties:

Property 1: Every minimal zero-sum sequence $S \in \mathcal{F}(G)$ with length $|S| = \mathcal{D}(G)$ consists entirely of elements g with $\mathrm{ord}(g) = \exp(G)$.

Property 2: There exists a minimal zero-sum sequence $S \in \mathcal{F}(G)$ with length $|S| = \mathcal{D}(G)$ which consists entirely of elements g with $\mathrm{ord}(g) = \exp(G)$.

Let $G = C_n$ be cyclic of order n. Then it is well known, that every minimal zero-sum sequence of length $\mathcal{D}(G) = n$ has the form g^n for some element g of order n. Hence cyclic groups have Property 1. In this note we characterize groups of rank two and p-groups having Property 1 resp. Property 2.

THEOREM 1.1. *Let $G = C_m \oplus C_n$ be a group with rank two where $1 < m \mid n$.*

(1) *G has Property 1 if and only if $m = n$.*
(2) *G has Property 2 if and only if either m or $\frac{n}{m}$ is odd.*

THEOREM 1.2. *Let $G = C_{p^{m_1}} \oplus \cdots \oplus C_{p^{m_r}}$ be a p-group where p is prime, $r \in \mathbb{N}$ and $1 \le m_1 \le \cdots \le m_r$.*

(1) *G has Property 1 if and only if $m_1 = m_r$.*
(2) *G has Property 2 if and only if G is not a 2-group with even rank r and with $m_{r-1} < m_r$.*

Furthermore, we give a complete characterization of all minimal zero-sum sequences with length $\mathcal{D}(G)$ in groups G of the form $G = C_2 \oplus C_{2n}$ (see Theorem 3.3). By the above Theorems these are the simplest groups which do not necessarily satisfy Property 2.

2. Preliminaries

Let G be a finite abelian group and $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ a sequence in G. Our terminology is consistent with the one used in [GG99]. In particular, we denote by $1 \in \mathcal{F}(G)$ the *empty sequence* and by $\mathrm{supp}(S) = \{g_i \mid 1 \le i \le l\}$ the *support* of S (hence S contains some element $g \in G$ if and only if $g \in \mathrm{supp}(S)$). The sequence S is called

- *zero-sumfree*, if $\sum_{i\in I} g_i \neq 0$ for every non-empty subset $I \subset \{1,\dots,l\}$. Clearly, S is zero-sumfree if and only if $-\sigma(S)\cdot S$ is a minimal zero-sum sequence.
- a *short zero-sum sequence*, if S is a zero-sum sequence with $1 \le |S| \le \exp(G)$.

Let $\eta(G)$ denote the smallest integer $\eta \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ with $|S| \ge \eta$ contains a short zero-sum subsequence.

LEMMA 2.1. *$\eta(C_n \oplus C_n) \le 3n-2$ for every $n \ge 2$.*

PROOF. This was proved in [GG99] Lemma 4.3. □

Let $\varphi : G \longrightarrow H$ be a group homomorphism. Then $\varphi(S) = \prod_{i=1}^{l} \varphi(g_i) \in \mathcal{F}(H)$ is a sequence in H with length $|\varphi(S)| = |S|$ and sum $\sigma(\varphi(S)) = \varphi(\sigma(S)) \in H$.

Elements $e_1,\dots,e_r \in G$ are called *independent*, if for every $m_1,\dots,m_r \in \mathbb{Z}$ the equation $\sum_{i=1}^{r} m_i e_i = 0$ implies that $m_i e_i = 0$ for every $1 \le i \le r$.

Furthermore, $(e_1,\dots,e_r)$ is called a *basis* of G, if $G = \bigoplus_{i=1}^{r} \langle e_i\rangle$, $\operatorname{ord}(e_i) = n_i$ for every $1 \le i \le r$ and $1 < n_1 \mid \dots \mid n_r$. Clearly, if $(e_1,\dots,e_r)$ is a basis of G, then $e_1,\dots,e_r$ are independent elements.

LEMMA 2.2. *Let G be an abelian group, $e_1,\dots,e_r \in G$ independent elements with $\operatorname{ord}(e_i) = n_i$ for $1 \le i \le r$ and $e_0 = \sum_{i=1}^{r} m_i e_i$ with $m_1,\dots,m_r \in \mathbb{Z}$.*

(1) $\operatorname{ord}(e_0) = \operatorname{lcm}\left\{ \dfrac{n_i}{\gcd\{m_i,n_i\}} \;\middle|\; 1 \le i \le r \right\}$.

(2) *If $n_1 = \dots = n_r = n$, then* $\operatorname{ord}(e_0) = \dfrac{n}{\gcd\{m_1,\dots,m_r,n\}}$.

PROOF. 1. For every $1 \le i \le r$ we have

$$\operatorname{ord}(m_i e_i) = \frac{\operatorname{ord}(e_i)}{\gcd\{\operatorname{ord}(e_i), m_i\}} = \frac{n_i}{\gcd\{n_i,m_i\}}.$$

Since $m_1e_1,\dots,m_re_r$ are independent elements, it follows that

$$\operatorname{ord}(e_0) = \operatorname{lcm}\{\operatorname{ord}(m_1e_1),\dots,\operatorname{ord}(m_re_r)\}$$

and the assertion follows.

2. If $n_1 = \dots = n_r = n$, then

$$\operatorname{ord}(e_0) = \operatorname{lcm}\left\{ \frac{n}{\gcd\{m_i,n\}} \;\middle|\; 1 \le i \le r \right\} = \frac{n}{\gcd\{m_1,\dots,m_r,n\}}. \qquad \square$$

3. Proof of Theorem 1.1

We start with a simple observation concerning the order of elements in long minimal zero-sum sequences.

LEMMA 3.1. *Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid \cdots \mid n_r$. Then there exists a minimal zero-sum sequence $S \in \mathcal{F}(G)$ with length $|S| = M(G)$ which contains some element g with $\mathrm{ord}(g) = n_1$.*

PROOF. Let $(e_1, \ldots, e_r)$ be a basis of G and set $e_0 = \sum_{i=1}^r e_i$. Then the sequence $\prod_{i=1}^r e_i^{n_i-1}$ is zero-sumfree whence $S = e_0 \cdot \prod_{i=1}^r e_i^{n_i-1}$ is a minimal zero-sum sequence with the required properties. □

THEOREM 3.2. *Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ be a finite abelian group with $1 < n_1 \mid \cdots \mid n_r$. Then the following conditions are equivalent:*

(1) *There exists a minimal zero-sum sequence $S \in \mathcal{F}(G)$ with length $|S| = M(G)$ such that $\mathrm{ord}(g) = \exp(G)$ for every $g \in \mathrm{supp}(S)$.*

(2) *$r = 1$ or $\sum_{i=1}^{r-1}(n_i - 1)$ is even or $\dfrac{n_r}{n_{r-1}}$ is odd.*

PROOF. 1. $\Longrightarrow$ 2. Suppose that $r \ge 2$, $\sum_{i=1}^{r-1}(n_i - 1)$ odd and $\frac{n_r}{n_{r-1}}$ is even. Then $H = \bigoplus_{i=1}^{r-1} C_{n_i}$ is non-trivial, $M(H)$ is even, $G = H \oplus \langle e \rangle$ with $\mathrm{ord}(e) = n_r = n$ and $l = M(G) = M(H) + n - 1$ is odd. Let

$$S = \prod_{i=1}^{l}(h_i + a_i e) \in \mathcal{F}(G)$$

be a minimal zero-sum sequence with all $h_i \in H$ and all $a_i \in \mathbb{Z}$. Assume to the contrary that $\mathrm{ord}(h_i + a_i e) = n$ for every $1 \le i \le l$. If some a_i would be even, then $\frac{n}{2}(a_i e) = 0$, $\frac{n}{2} h_i = 0$ since n_{r-1} divides $\frac{n}{2}$ and thus $\frac{n}{2}(h_i + a_i e) = 0$, a contradiction. Thus all a_i are odd whence $\sum_{i=1}^l a_i$ is odd. However, since S has sum zero, it follows that $\sum_{i=1}^l a_i \equiv 0 \mod n$, a contradiction.

2. $\Longrightarrow$ 1. Let $(e_1, \ldots, e_r)$ be a basis of G.

If $r = 1$, then $S = e_1^{n_1}$ has the required properties.

Suppose $r \ge 2$ and choose integers $a_{i,j} \in \mathbb{Z}$ with $\gcd\{n_r, a_{i,j}\} = 1$ for every $1 \le i \le r$ and every $1 \le j \le n_i - 1$. Then the sequence

$$\prod_{i=1}^{r-1} \prod_{j=1}^{n_i-1} (e_i + a_{i,j} e_r) \cdot e_r^{n_r-1}$$

is zero-sumfree whence

$$S = e_0 \cdot \prod_{i=1}^{r-1} \prod_{j=1}^{n_i-1} (e_i + a_{i,j} e_r) \cdot e_r^{n_r-1}$$

is a minimal zero-sum sequence with length $M(G)$ where

$$e_0 = \sum_{i=1}^{r-1} e_i + (1-a)e_r \quad \text{with} \quad a = \sum_{i=1}^{r-1}\sum_{j=1}^{n_i-1} a_{i,j}.$$

Since all $a_{i,j}$ are coprime to n_r, Lemma 2.2 implies that $\operatorname{ord}(e_i + a_{i,j}e_r) = n_r$. Hence it remains to show that $\operatorname{ord}(e_0) = n_r$. By Lemma 2.2 we have

$$\begin{aligned}\operatorname{ord}(e_0) &= \operatorname{lcm}\{\operatorname{ord}(e_1), \ldots, \operatorname{ord}(e_{r-1}), \operatorname{ord}((1-a)e_r)\} \\ &= \operatorname{lcm}\{n_{r-1}, \operatorname{ord}((1-a)e_r)\} \\ &= \operatorname{lcm}\left\{n_{r-1}, \frac{n_r}{\gcd\{n_r, 1-a\}}\right\}.\end{aligned}$$

If $\sum_{i=1}^{r-1}(n_i - 1) = 2k$ for some $k \in \mathbb{N}$, then choose k $a_{i,j}$'s equal to 1 and k $a_{i,j}$'s equal to -1. This implies that $a = 0$ whence $\operatorname{ord}(e_0) = n_r$.

If $\frac{n_r}{n_{r-1}}$ is odd and $\sum_{i=1}^{r-1}(n_i - 1) = 2k + 1$ for some $k \in \mathbb{N}_0$, then choose $k+1$ $a_{i,j}$'s equal to -1 and k $a_{i,j}$'s equal to 1. This implies that $1 - a = 2$ and $\operatorname{ord}(e_0) = n_r$. □

Proof of Theorem 1.1. Let $G = C_m \oplus C_n$ with $1 < m \mid n$.

1. If G has Property 1, then Lemma 3.1 implies that $m = n$. If $m = n$, then Property 1 holds by Proposition 6.3 in [GG99].

2. This follows from Theorem 3.2. □

In cyclic groups and elementary 2-groups it is an easy exercise to determine all minimal zero-sum sequences of maximal lengths (see Propositions 2.2 and 4.1 in [GG99]). Apart from these trivial cases this has been done for no other series of groups. Here we establish an explicit characterization of all minimal zero-sum sequences of maximal lengths in groups G of the form $G = C_2 \oplus C_{2n}$. Such explicit characterizations are of great relevance in zero sum theory (see the literature and problems in [Alo99], [Car96], [CFS99] or the discussions around Property B in [Gao00] and [GG99]) and in factorization theory (see e.g. [CG97] and [GG00]). In particular, we shall (explicitely) see that in groups $G = C_2 \oplus C_{4k}$ all minimal zero-sum sequences with length $\mathcal{D}(G)$ contain elements of order less that $\exp(G)$.

Theorem 3.3. *Let $G = C_2 \oplus C_{2n}$ for some $n \geq 2$ and $S \in \mathcal{F}(G)$ a minimal zero-sum sequence with length $|S| = \mathcal{D}(G)$. Then S has one of the following two forms:*

(1) *$S = g^{2n-1} \cdot h \cdot (g-h)$ for some $g \in G$ with $\operatorname{ord}(g) = 2n$ and some $h \in G \setminus \langle g \rangle$.*
(2) *$S = e \cdot g^v \cdot (g+e)^{2n-v}$ for some $g \in G$ with $\operatorname{ord}(g) = 2n$, $e \in G \setminus \langle g \rangle$ with $\operatorname{ord}(e) = 2$ and v odd with $3 \leq v \leq 2n-3$.*

Conversely, every sequence of form 1. *or* 2. *is a minimal zero-sum sequence with length* $\mathcal{D}(G)$.

PROOF. It is easy to verify that a sequence of form 1. or 2. is a minimal zero-sum sequence with length $2n+1 = \mathcal{D}(G)$.

Let (e_1, e_2) be a basis of G, $H = \langle 2e_2 \rangle \cong C_n$, $G/H = \{H = a_0, e_1 + H = a_1, e_2 + H = a_2, e_1 + e_2 + H = a_3\} \cong C_2 \oplus C_2$ and consider the exact sequence

$$0 \longrightarrow H \hookrightarrow G \xrightarrow{\varphi} G/H \longrightarrow 0.$$

We write S in the form

$$S = \prod_{i=0}^{3} S_i$$

such that $\varphi(S_i) = a_i^{|S_i|}$ for every $0 \le i \le 3$.

1. We assert that $S_0 = 1 \in \mathcal{F}(G)$, the empty sequence. Assume to the contrary that $S = g \cdot T$ with $\varphi(g) = a_0$. Since by Lemma 2.1 $\eta(C_2 \oplus C_2) \le 4$ and $|T| = 2n = 2(n-2) + 4$, there exist pairwise disjoint subsequences $T_1, \ldots, T_{n-1}$ of T such that all $\varphi(T_i)$ are short zero-sum subsequences of $\varphi(T)$. Therefore $U = g \cdot \prod_{i=1}^{n-1} \sigma(T_i) \in \mathcal{F}(H)$ and since $\mathcal{D}(H) = n$, it follows that U has a zero-sum subsequence. Therefore $V = g \cdot \prod_{i=1}^{n-1} T_i$ has a zero-sum subsequence. However, V is a subsequence of S with $|V| = 1 + \sum_{i=1}^{n-1} |T_i| \le 1 + 2(n-1) < |S|$, a contradiction.

2. We assert that $|S_i| \equiv 1 \mod 2$ for every $1 \le i \le 3$. For $i \in \{1,2,3\}$ set $|S_i| = 2q_i + r_i$ with $0 \le r_i \le 1$. Then $\varphi(S_i) = (a_i^2)^{q_i} \cdot a_i^{r_i}$ and obviously, a_i^2 is a short zero-sum subsequence of $\varphi(S_i)$. Therefore S contains $q = q_1 + q_2 + q_3$ pairwise disjoint subsequences T_i with $|T_i| = 2$ and $\sigma(\varphi(T_i)) = 0$. This implies that

$$T = \prod_{i=1}^{q} \sigma(T_i) \in \mathcal{F}(H).$$

Since $2n + 1 = |S| = 2q + \sum_{i=1}^{3} r_i$, it follows that $\sum_{i=1}^{3} r_i \in \{1, 3\}$. Assume to the contrary that $\sum_{i=1}^{3} r_i = 1$. Then it follows that

$$q = \frac{1}{2}\left(|S| - \sum_{i=1}^{3} r_i\right) = n$$

whence T contains a zero-sum subsequence and the same is true for $U = \prod_{i=1}^{q} T_i$. However, U is a subsequence of S with $|U| = \sum_{i=1}^{q} |T_i| \le 2n < |S|$, a contradiction. Thus $|S_i| = 2q_i + 1$ for every $1 \le i \le 3$ and $q = n - 1$.

3. We assert that for every $1 \le i \le 3$ there is some $g_i \in \varphi^{-1}(a_i) \subset G$ such that $S_i = g_i^{|S_i|}$. Furthermore, if $|S_1| \ge 3$ and $|S_2| \ge 3$, then $2g_1 = 2g_2$.

Let $i \in \{1,2,3\} = \{i,j,k\}$. If $|S_i| = 1$, there is nothing to prove. Suppose $S_i = \prod_{\nu=1}^{|S_i|} h_\nu$ with $|S_i| = 2q_i + 1 \ge 3$. We shall verify that $h_1 = h_2$.

First suppose that $|S_i| \ge 5$. For $1 \le \nu \le q_i$ the sequences $T_\nu = h_{2\nu} \cdot h_{2\nu+1}$ are pairwise distinct subsequences of S_i with $\sigma(T_\nu) \in H$. For $\mu \in \{j,k\}$ there are

q_μ such subsequences T_ν of S_μ. Set $S = T_{q+1} \cdot \prod_{\nu=1}^{q} T_\nu$. Then $q+1 = n$, $|T_n| = 3$ and $\varphi(T_n)$ has sum zero. Therefore

$$T = \prod_{\nu=1}^{n} \sigma(T_\nu) \in \mathcal{F}(H)$$

contains a zero-sum subsequence, and since S is a minimal zero-sum sequence, T is a minimal zero-sum sequence in a cyclic group of order n. Therefore, it follows that

$$\sigma(T_1) = \cdots = \sigma(T_n). \tag{1}$$

In particular, we obtain that

$$h_2 + h_3 = \sigma(T_1) = \sigma(T_2) = h_4 + h_5.$$

Repeating this construction (with a new numeration of the h_i's) we obtain that $h_1 + h_3 = h_4 + h_5$. Thus we obtain that $h_1 = h_2$.

Suppose now that $|S_i| = 3$ and assume that $|S_j| \geq |S_k|$. We distinguish the cases $|S_j| = 1$ and $|S_j| \geq 3$.

Suppose $|S_j| = 1$. Then $|S_k| = 1$ and $2n+1 = |S| = \sum_{\nu=1}^{3} |S_\nu| = 5$ whence $n = 2$. Thus we have $\varphi^{-1}(e_1 + H) = \{e_1, e_1 + 2e_2\}$, $\varphi^{-1}(e_2 + H) = \{e_2, 3e_2\}$ and $\varphi^{-1}(e_1 + e_2 + H) = \{e_1 + e_2, e_1 + 3e_2\}$. Assume to the contrary, that $|\mathrm{supp}(S_i)| > 1$ whence $S_i = g \cdot g \cdot (g + 2e_2)$ for some $g \in \varphi^{-1}(a_i)$. This implies that S_i is not zero-sumfree, a contradiction.

Suppose $|S_j| \geq 3$. Then $q_j + q_k = q - q_i = n-2$ and $S_j \cdot S_k = a \cdot b \cdot T_1 \cdot \ldots \cdot T_{n-2}$ with $|T_\mu| = 2$ and $\sigma(T_\mu) \in H$. Setting

$$S = T_1 \cdot \ldots \cdot T_{n-2} \cdot \underbrace{(h_1 \cdot h_3)}_{T_{n-1}} \cdot \underbrace{(a \cdot b \cdot h_2)}_{T_n}$$

we infer as above that

$$\sigma(T_1) = \cdots = \sigma(T_n). \tag{2}$$

In particular, we have $h_1 + h_3 = \sigma(T_1)$. Repeating the construction we obtain that $h_2 + h_3 = \sigma(T_1)$ which implies that $h_1 = h_2$.

Thus we proved that for every $1 \leq i \leq 3$ there are $g_i \in G$ such that $S_i = g_i^{|S_i|}$. Looking at (1) and (2) again we see that $2g_1 = 2g_2$ provided $|S_1| \geq 3$ and $|S_2| \geq 3$.

4. Set

$$g_1 = e_1 + 2ae_2, \quad g_2 = (2b+1)e_2 \quad \text{and} \quad g_3 = e_1 + (2c+1)e_2$$

with $a, b, c \in \{0, \ldots, n-1\} \subset \mathbb{Z}$ and $|S_i| = v_i$ for $1 \leq i \leq 3$. Then

$$S = g_1^{v_1} \cdot g_2^{v_2} \cdot g_3^{v_3}$$

and we have

$$v_1 2a + v_2(2b+1) + v_3(2c+1) \equiv 0 \mod 2n \tag{3}$$

$$v_1 \equiv v_2 \equiv v_3 \equiv 1 \mod 2 \tag{4}$$

$$|S| = v_1 + v_2 + v_3 = 2n + 1 \tag{5}$$

We assert that $1 \in \{v_1, v_2, v_3\}$. Assume to the contrary that $v_i > 1$ for every $1 \le i \le 3$. Then $v_i \ge 3$ for every $1 \le i \le 3$. Thus 3. implies that $2g_1 = 2g_2 = 2g_3$ whence

$$4a \equiv 4b + 2 \equiv 4c + 2 \mod 2n.$$

Therefore, n is odd, $2a \equiv 2b + 1 \mod n$ and $2a + n \equiv 2b + 1 \mod 2n$. Similarly, $2b+1 \equiv 2c+1 \mod n$ whence either $2b+1 \equiv 2c+1 \mod 2n$ or $2b+1 \equiv 2c+1+n \mod 2n$. Since $2a + n \not\equiv 2c + 1 + n \mod 2n$, we infer that

$$2b + 1 \equiv 2c + 1 \equiv 2a + n \mod 2n.$$

Using (3), (4) and (5) it follows that

$$v_1(2b + 1 + n) + v_2(2b + 1) + v_3(2b + 1) \equiv 0 \mod 2n,$$

$$(v_1 + v_2 + v_3)(2b + 1) + v_1 n \equiv 0 \mod 2n$$

and thus

$$(2b + 1) + n \equiv 0 \mod 2n.$$

Thus $2a \equiv 0 \mod 2n$ and g_1^2 is a proper zero-sum subsequence of S, a contradiction. Thus there are the following two cases.

Case 1: Two of the v_i's are equal to 1. Then S has form 1 of the formulation of the Theorem.

Case 2: Exactly one of the v_i's is equal to 1. In three subcases we show that S has the form

$$S = e \cdot g^v \cdot (g + e)^{2n-v} \tag{6}$$

with v odd, $3 \le v \le 2n - 3$ and $\mathrm{ord}(e) = 2$.

Case 2.1: $v_1 = 1$. Then $3 \le v_2, 3 \le v_3 = 2n - v_2$ and $2g_2 = 2g_3$ implies that $2(2b + 1) \equiv 2(2c + 1) \mod 2n$. If $2b + 1 \equiv 2c + 1 \mod 2n$, then v_2 is odd. Furthermore, $v_2 + v_3 = 2n$ and (3) imply that $2a \equiv 0 \mod 2n$ whence S has form (6) with $g_1 = e$.

If $2c+1 \equiv 2b+1+n \mod 2n$, then n is even, v_2 is odd, $2a \equiv n \mod 2n$ and S has form (6) with $g_1 = e$.

Case 2.2: $v_2 = 1$. Then $3 \le v_1, 3 \le v_3 = 2n - v_1$ and $2g_1 = 2g_3$ implies that $2(2a) \equiv 2(2c + 1) \mod 2n$. Thus n is odd, $2c + 1 \equiv 2a + n \mod 2n$, v_1 is odd and $2b + 1 \equiv n \mod 2n$ whence S has form (6) with $g_2 = e$.

Case 2.3: $v_3 = 1$. Then $3 \le v_1, 3 \le v_2 = 2n - v_1$ and $2g_1 = 2g_2$ implies that $2(2a) \equiv 2(2b + 1) \mod 2n$. Thus n is odd, $2b + 1 \equiv 2a + n \mod 2n$, v_1 is odd and $2c + 1 \equiv n \mod 2n$ whence S has form (6) with $g_3 = e$.

Hence we know that S has form (6), and it remains to show that $e \in G \setminus \langle g \rangle$ and $\mathrm{ord}(g) = 2n$.

Let $\mathrm{ord}(g) = m$ and $mm' = 2n$. If $e \in \langle g \rangle$, then $T = g^v \cdot (g + e)^{2n-v}$ is a sequence in $\langle g \rangle$, which contains a zero-sum subsequence, since $\mathcal{D}(\langle g \rangle) = m \le 2n$, a contradiction.

Assume to the contrary, that $m' > 1$. Since T is zero-sumfree, we infer that $v < \mathrm{ord}(g) = m$ and $2n - v < \mathrm{ord}(g + e) \le 2m$ whence $mm' = 2n < 3m$. Thus $m' = 2$, $m = n$, $2n - v > n$ and $e \cdot (g + e)^n$ contains a zero-sum sequence, a contradiction. □

COROLLARY 3.4. *Let $G = C_2 \oplus C_{2n}$ with $n \ge 2$, (e_1, e_2) a basis of G and $S \in \mathcal{F}(G)$ a minimal zero-sum sequence with length $|S| = \mathsf{D}(G)$. Then there exists a group automorphism $\varphi : G \to G$ such that $\varphi(S)$ has one of the following two forms:*

(1) $\varphi(S) = e_2^{2n-1} \cdot (e_1 + ae_2) \cdot (e_1 + (1-a)e_2)$ *with* $a \in \{0, \ldots, 2n-1\}$.
(2) $\varphi(S) = e_1 \cdot e_2^v \cdot (e_1 + e_2)^{2n-v}$ *with v odd and* $3 \le v \le 2n-3$.

PROOF. 1. Suppose $S = g^{2n-1} \cdot h \cdot (g - h)$ with $\mathrm{ord}(g) = 2n$ and $h \in G \setminus \langle g \rangle$. There exists some element $e \in G$ of order two such that $G = \langle g \rangle \dot\cup (e + \langle g \rangle)$ whence (e, g) is a basis of G. Then $h = e + ag$ for some $a \in \{0, \ldots, 2n-1\}$. Furthermore, there is some automorphism $\varphi : G \to G$ with $\varphi(e) = e_1$ and $\varphi(g) = e_2$ whence

$$\varphi(S) = e_2^{2n-1} \cdot (e_1 + ae_2) \cdot (e_1 + (1-a)e_2).$$

2. If $S = e \cdot g^v \cdot (g+e)^{2n-v}$ with $\mathrm{ord}(g) = 2n$ and $e \in G \setminus \langle g \rangle$ with $\mathrm{ord}(e) = 2$, then (e, g) is a basis of G and as above we obtain a group automorphism such that $\varphi(S)$ has the required form. □

Suppose that n is even. If $a \in \{0, \ldots, 2n-1\}$, then either a or $1 - a$ is even whence either $\mathrm{ord}(e_1 + ae_2) \le n$ or $\mathrm{ord}(e_1 + (1-a)e_2) \le n$. Thus every minimal zero-sum sequence in $C_2 \oplus C_{2n}$ contains some element g with $\mathrm{ord}(g) < \exp(G)$.

4. Proof of Theorem 1.2

Let G be an abelian p-group and $g \in G$. Then the (p-)*height* $h(g)$ of g (in G) is defined as the supremum of all $s \in \mathbb{N}_0 \cup \{\infty\}$ for which the equation $p^s \cdot x = g$ is solvable in G.

LEMMA 4.1. *Let G be a finite abelian p-group and $0 \ne g \in G$. Then* $\mathrm{ord}(g) \le \frac{\exp(G)}{p^{h(g)}}$ *and equality holds if $G = C_{p^m}^r$ for some $r, m \in \mathbb{N}$.*

PROOF. Let $x \in G$ with $p^s \cdot x = g$ with $s = h(g)$. Then $\mathrm{ord}(x) = p^t \le \exp(G)$ for some $t > s$ and it follows that

$$\mathrm{ord}(g) = \frac{p^t}{\gcd\{p^s, p^t\}} \le \frac{\exp(G)}{p^{h(g)}}.$$

Suppose that $G = (\mathbb{Z}/p^m\mathbb{Z})^r$ and $g = (a_1 + p^m\mathbb{Z}, \ldots, a_r + p^m\mathbb{Z})$ where $a_i = p^{m_i}b_i + p^m\mathbb{Z}$ and $p \nmid b_i$ for every $1 \le i \le r$. Setting $m_0 = \min\{m_1, \ldots, m_r\}$ we obtain that

$$g = p^{m_0} \cdot (p^{m_1 - m_0}b_1 + p^m\mathbb{Z}, \ldots, p^{m_r - m_0}b_r + p^m\mathbb{Z})$$

whence $h(g) \ge m_0$. By Lemma 2.2 we infer that

$$\mathrm{ord}(g) = \frac{p^m}{\gcd\{a_1, \ldots, a_r, p^m\}} = \frac{p^m}{p^{m_0}}.$$

Therefore it follows that

$$p^{m-m_0} = \mathrm{ord}(g) \le \frac{\exp(G)}{p^{h(g)}} \le p^{m-m_0}$$

and the assertion is proved. □

LEMMA 4.2. *Let G be a finite abelian p-group and $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ a sequence. If $\sum_{i=1}^{l} p^{h(g_i)} \ge M(G)$, then S is not zero-sumfree.*

PROOF. This was proved by J. E. Olson in [Ols69a], Theorem 2. □

PROPOSITION 4.3. *Let $G = C_{p^m}^r$ with p prime, $m, r \in \mathbb{N}$ and $S \in \mathcal{F}(G)$ a minimal zero-sum sequence. If $|S| \ge \mathcal{D}(G) - p + 2$, then $\mathrm{ord}(g) = \exp(G)$ for every $g \in \mathrm{supp}(S)$.*

PROOF. Suppose $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)$ is a minimal zero-sum sequence with $|S| = l \ge \mathcal{D}(G) - p + 2$ and assume to the contrary that there exists some $i \in \{1, \ldots, l\}$ with $\mathrm{ord}(g_i) < \exp(G)$. Without restriction we suppose that $i = 1$ and set $T = \prod_{i=1}^{l-1} g_i$. We show that T is not zero-sumfree which yields the wanted contradiction.

Lemma 4.1 implies that

$$\frac{\exp(G)}{p^{h(g_1)}} = \mathrm{ord}(g_1) < \exp(G)$$

whence $p^{h(g_1)} \ge p$. This implies that

$$\sum_{i=1}^{l-1} p^{h(g_i)} \ge p + \sum_{i=2}^{l-1} p^{h(g_i)} \ge p + (l-2) \ge \mathcal{D}(G) = M(G),$$

whence T is not zero-sumfree by Lemma 4.2. □

PROOF OF THEOREM 1.2. Let $G = C_{p^{m_1}} \oplus \cdots \oplus C_{p^{m_r}}$ be a p-group where p is prime, $r \in \mathbb{N}$ and $1 \le m_1 \le \cdots \le m_r$. Then we have $M(G) = \mathcal{D}(G)$. Thus 1. follows from Lemma 3.1 and Proposition 4.3.

Theorem 3.2 implies that G does not have Property 2 if and only if $r \ge 2$, $p = 2$, $m_r > m_{r-1}$ and $\sum_{i=1}^{r-1}(2^{m_i} - 1)$ is odd which is equivalent to r even, $p = 2$ and $1 \le m_1 \le \cdots \le m_{r-1} < m_r$. □

REFERENCES

[Alo99] N. Alon, Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing* **8** (1999), 7–29.

[And97] D. D. Anderson, *Factorization in integral domains*, Marcel Dekker, 1997.

[Car96] Y. Caro, Zero-sum problems – A survey, *Discrete Math.* **152** (1996), 93–113.

[CFS99] S. Chapman, M. Freeze and W. Smith, Minimal zero sequences and the strong Davenport constant, *Discrete Math.* **203** (1999), 271–277.

[CG97] 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 Appl. Math.* vol. 189, Marcel Dekker, 1997, 73–112.

[Gao00] W. Gao, On Davenport's constant of finite abelian groups with rank three, *Discrete Math.* **222** (2000), 111–124.

[GG99] W. Gao and A. Geroldinger, On long minimal zero sequences in finite abelian groups, *Periodica Math. Hungarica* **38** (1999), 179–211.

[GG00] W. Gao and A. Geroldinger, Systems of sets of lengths II, *Abhandl. Math. Sem. Univ. Hamburg* **70** (2000), 31–49.

[GS92] A. Geroldinger and R. Schneider, On Davenport's constant, *J. Comb. Th. Ser. A* **61** (1992), 147–152.

[GS96] A. Geroldinger and R. Schneider, The cross number of finite abelian groups III, *Discrete Math.* **150** (1996), 123–130.

[Ols69a] J.E. Olson, A combinatorial problem on finite abelian groups I, *J. Number Th.* **1** (1969), 8–10.

[Ols69b] J.E. Olson, A combinatorial problem on finite abelian groups II, *J. Number Th.* **1** (1969), 195–199.

[vEB69] P. van Emde Boas, A combinatorial problem on finite abelian groups II, in: *Reports ZW-1969-007*, Math. Centre, Amsterdam, 1969.

(Received: August 28, 2000)

Weidong Gao
Department of Computer Science and Technology
University of Petroleum, Beijing
Shuiku Road, Changping
Beijing 102200
P.R. China
E-mail: wdgao@public.fhnet.cn.net

Alfred Geroldinger
Institut für Mathematik
Karl-FranzensUniversität
Heinrichstrasse 36
8010 Graz
Austria
E-mail: alfred.geroldinger@uni-graz.at