On zero-sum subsequence of length not exceeding a given number

Chunlin Wang[1] and Kevin Zhao[2]

[1,2] Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China

[1]c-l.wang@outlook.com, [2]zhkw-hebei@163.com

Abstract. Let G be an additive finite abelian group. For a positive integer k, let $s_{\leq k}(G)$ denote the smallest integer l such that each sequence of length l has a non-empty zero-sum subsequence of length at most k. Among other results, we determine $s_{\leq k}(G)$ for all finite abelian group of rank two.

Keywords: Davenport constant, zero-sum sequence, Abelian group.
2010 Mathematics Subject Classification: 11B75, 11R27.

1 Introduction

Let C_n denote the cyclic group of n elements. Let G be an additive finite abelian group. It is well known that $|G| = 1$ or $G = C_{n_1} \oplus C_{n_2} \cdots \oplus C_{n_r}$ with $1 < n_1 | n_2 \cdots | n_r$. Then, $r(G) = r$ is the rank of G and the exponent $\exp(G)$ of G is n_r. Let

$$S := g_1 \cdots g_l$$

be a sequence with elements in G. We call S a zero-sum sequence if $g_1 + \cdots + g_l = 0$. The Davenport constant $D(G)$ is the minimal integer $l \in N$ such that every sequence S over G of length $|S| \geq l$ has a nonempty zero-sum subsequence. Set

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

Then $D(G) \geq D^*(G)$. Let $\eta(G)$ denote the smallest integer $l \in N$ such that every sequence S over G of length $|S| \geq l$ has a nonempty zero-sum subsequence T of length $|T| \leq \exp(G)$. In this paper, we investigate a following generalization of $D(G)$ and $\eta(G)$.

Definition 1.1. *Denote by $s_{\leq k}(G)$ the smallest element $l \in N \cup \{+\infty\}$ such that each sequence of length l has a non-empty zero-sum subsequence of length at most k ($k \in N$).*

The constant $s_{\leq k}(G)$ was introduced by Delorme, Ordaz and Quiroz [2]. It is trivial to see that $s_{\leq k}(G) = D(G)$ if $k \geq D(G)$, $s_{\leq k}(G) = \eta(G)$ if $k = \exp(G)$ and $s_{\leq k}(G) = \infty$ if $1 \leq k < \exp(G)$. For general, the problem of determining $s_{\leq k}(G)$ is not at all trivial. Recently, the exact number of $s_{\leq 3}(C_2^r)$ is known by the work of Freeze and Schmid [3], namely, $1 + 2^{r-1}$. Besides its own interesting, Cohen and Zemor [1] pointed out a connection between $s_{\leq k}(C_2^r)$ and coding theory. In this paper, we shall determine $s_{\leq k}(G)$ for some groups. Our main results are the followings:

Theorem 1.2. *Let $G = C_m \oplus C_n$ with $m|n$ be an abelian group. Set $d := D(G)$. Then for all $0 \leq k \leq m-1$, one has*

$$s_{\leq d-k}(G) = d + k.$$

Theorem 1.3. *Let r be a positive integer. Then we have that $s_{\leq r-k}(C_2^r) = r + 2$ for all positive integers $r - k \in [\lceil \frac{2r+2}{3} \rceil, r]$.*

2 Preliminaries

In this paper, our notations are coincident with [5] and we briefly present some key concepts. Let N denote the set of positive integers and $N_0 = N \cup \{0\}$.

Let $\mathscr{F}(G)$ be the free abelian monoid, multiplicatively written, with basis G. The elements of $\mathscr{F}(G)$ are called sequences over G. Let

$$S = g_1 \cdots g_l \in \mathscr{F}(G),$$

we denote $g_1 + \cdots + g_l$ by $\sigma(S)$. Every map of abelian groups $\varphi : G \to H$ extends to a map from $\mathscr{F}(G)$ to $\mathscr{F}(H)$ by setting

$$\varphi(S) = \varphi(g_1) \cdots \varphi(g_l).$$

If φ is a homomorphism, then $\varphi(S)$ is a zero-sum sequence if and only if $\sigma(S) \in \ker \varphi$. Let $G = H \oplus K$ be a finite abelian group. And let $\varphi : G \to H$ be a homomorphism with $\ker \varphi = K$ and $\psi : G \to K$ be a homomorphism with $\ker \psi = H$. If $S \in \mathscr{F}(G)$ such that $\sigma(\varphi(S)) = 0$, then $\sigma(S) = \sigma(\psi(S))$.

We have the following lemmas:

Lemma 2.1 ([5])**.** *For G be a p-group or $G = C_m \oplus C_n$ with $1 \leq m$ and $m|n$, we have*

$$D(G) = D^*(G).$$

Lemma 2.2 ([5])**.** *Let m and n be positive integers with $m \mid n$. Then*

$$\eta(C_m \oplus C_n) = 2m + n - 2.$$

Definition 2.3. *Let $S = g_1 \cdots g_l \in \mathscr{F}(G)$ be a sequence of length $|S| = l \in N_0$ and let $g \in G$.*

1. *For every $k \in N_0$ let*

$$N_g^k(S) := \#\Big\{I \subset [1,l] : \sum_{i\in I} g_i = g \text{ and } |I| = k\Big\}.$$

denote the number of subsequences T of S having sum $\sigma(T) = g$ and length $|T| = k$ (counted with the multiplicity of their appearance in S). When $g = 0$, $N_g^k(S)$ is denoted by $N^k(S)$ for short.

2. *We define*

$$N_g(S) := \sum_{k\geq 0} N_g^k(S),\ \ N_g^+(S) := \sum_{k\geq 0} N_g^{2k}(S) \text{ and } N_g^-(S) := \sum_{k\geq 0} N_g^{2k+1}(S)$$

Thus $N_g(S)$ denotes the number of subsequences T of S having sum $\sigma(T) = g$, $N_g^+(S)$ denotes the number of all such subsequences of even length, and $N_g^-(S)$ denotes the number of all such subsequences of odd length (each counted with the multiplicity of its appearance in S).

Lemma 2.4 ([5])**.** *Let p be a prime, G be a p-group, $S = g_1 \cdots g_l \in \mathscr{F}(G)$. If $l \geq D(G)$, then $N_g^+(S) \equiv N_g^-(S)$ mod p for all $g \in G$. In particular, $N_0^+(S) \equiv N_0^-(S)$ mod p.*

3 Proof of Theorem 1.2

In this section, we prove Theorem 1.2.

Proof. Suppose that $\{e_1, e_2\}$ is a basis of G. That is,

$$C_m \oplus C_n = \langle e_1\rangle \oplus \langle e_2\rangle$$

with $\mathrm{ord}(e_1) = m$ and $\mathrm{ord}(e_2) = n$. For a integer k with $1 \leq k \leq m-1$, let

$$S := e_1^{m-1} e_2^{n-1}(e_1+e_2)^{k-2}.$$

Then S is a sequence of length $d+k-1$. It is easy to see that S has no zero-sum subsequence of length in $[1, d-k]$. It follows that

$$s_{\leq d-k}(G) \geq d+k. \tag{3.1}$$

Then to prove Theorem 1.2, it suffices to show that

$$s_{\leq d-k}(G) \leq d+k, \tag{3.2}$$

holds, which will be done in the following.

Let p be a prime number. First we show that (3.2) is true for the case $m = n = p$. Suppose conversely that (3.2) is false. Then there exits a sequence S of length $|S| = d+k$ such that S has no zero-sum subsequence of length in $[1, d-k]$. Thus $N^i(S) = 0$ for integers $i \in [1, d-k]$. It is easy to see that any zero-sum sequence of length i with $i \in [d+1, 2d-2k+1]$ has a nonempty zero-sum subsequence of length at most $d-k$. Then we conclude that $N^i(S) = 0$ for $d+1 \le i \le \min(|S|, 2d-2k+1)$.

Let $|S| \le 2d-2k+1$. Then $0 \le k \le \frac{d+1}{3} = \frac{2p}{3}$. Let T be a subsequence of S with $|T| = |S|-t$, where t is a integer such that $0 \le t \le k$. Obviously $0 \le N^i(T) \le N^i(S) = 0$ holds for $1 \le i \le d+1$ and $d+1 \le i \le |T|$. Then by lemma 2.4, we have the following equation:

$$1 + (-1)^{d-k+1}N^{d-k+1}(T) + \cdots + (-1)^d N^d(T) \equiv 0 \ (p).$$

It follows that

$$\sum_{T|S,\ |T|=|S|-t} \big(1 + (-1)^{d-k+1}N^{d-k+1}(T) + \cdots + (-1)^d N^d(T)\big) \equiv 0 \ (p).$$

Analysing the number of times each subsequence is counted, one obtains

$$\begin{aligned} &\binom{|S|}{|T|} + (-1)^{d-k+1}\binom{|S|-(d-k+1)}{|T|-(d-k+1)}N^{d-k+1}(S) + \cdots + (-1)^d\binom{|S|-d}{|T|-d}N^d(S) \\ =&\binom{|S|}{t} + (-1)^{2p-k}\binom{2k-1}{t}N^{2p-k}(S) + \cdots + (-1)^{2p-1}\binom{k}{t}N^{2p-1}(S) \equiv 0 \ (p). \end{aligned} \tag{3.3}$$

Let $b := (\binom{|S|}{0}, \binom{|S|}{1}, \cdots, \binom{|S|}{k})^T$ and

$$A := \begin{pmatrix} \binom{2k-1}{0} & \cdots & \binom{k}{0} \\ \binom{2k-1}{1} & \cdots & \binom{k}{1} \\ \cdots & \cdots & \cdots \\ \binom{2k-1}{k} & \cdots & \binom{k}{k} \end{pmatrix}$$

On the one hand, it can be deduced from (3.3) that the following equation

$$AX + b \equiv 0 \ (p)$$

has a solution

$$X = ((-1)^{2p-k}N^{2p-k}(S), \cdots, (-1)^{2p-1}N^{2p-1}(S))^T.$$

Let (A,b) denote the augmented matrix. Then one can deduce that

$$r((A,b)) = r(A) \le k.$$

On the other hand, since $k < p$, by Lucas Theorem we have

$$\binom{|S|}{t} \equiv \binom{k-1}{t} \ (p) \ \text{ for } \ 0 \le t \le k.$$

It follows that

$$|\det((A,b))| \equiv \begin{vmatrix} \binom{k-1}{0} & \binom{k}{0} & \cdots & \binom{2k-1}{0} \\ \binom{k-1}{1} & \binom{k}{1} & \cdots & \binom{2k-1}{1} \\ \cdots & \cdots & \cdots & \cdots \\ \binom{k-1}{k} & \binom{k}{k} & \cdots & \binom{2k-1}{k} \end{vmatrix} = \begin{vmatrix} \binom{k-1}{0} & 0 & \cdots & 0 \\ \binom{k-1}{1} & \binom{k-1}{0} & \cdots & \binom{2k-2}{0} \\ \cdots & \cdots & \cdots & \cdots \\ \binom{k-1}{k} & \binom{k-1}{k-1} & \cdots & \binom{2k-2}{k-1} \end{vmatrix} = 1 \not\equiv 0 \ (p).$$

Thus $r((A,b)) = k+1$, a contradiction.

Let $|S| > 2d-2k+1$, that is $\frac{2p}{3} < k \le p-1$. If $d \le |T| \le 2(d-k)+1$, then we have that (3.3) holds. If $2(d-k+1) \le |T| \le |S|-1$, then we have

$$\begin{aligned} &1 + (-1)^{d-k+1} N^{d-k+1}(T) + \cdots + (-1)^d N^d(T) \\ &\quad + (-1)^{2(d-k+1)} N^{2(d-k+1)}(T) + \cdots + (-1)^{|T|} N^{|T|}(T) \equiv 0 \ (p). \end{aligned}$$

It follows that

$$\begin{aligned} &\sum_{T|S,\ |T|=|S|-t} \Big(1 + (-1)^{d-k+1} N^{d-k+1}(T) + \cdots + (-1)^d N^d(T) \\ &+ (-1)^{2(d-k+1)} N^{2(d-k+1)}(T) + \cdots + (-1)^{|T|} N^{|T|}(T)\Big) \equiv 0 \ (p). \end{aligned}$$

Analysing the number of times each subsequence is counted, one obtains

$$\begin{aligned} &\binom{|S|}{t} + (-1)^{2p-k}\binom{2k-1}{t} N^{2p-k}(S) + \cdots + (-1)^{2p-1}\binom{k}{t} N^{2p-1}(S) \\ &+(-1)^{2(2p-k)}\binom{3k-2p-1}{t} N^{2(2p-k)}(S) + \cdots + (-1)^{|S|}\binom{0}{t} N^{|S|}(S) \equiv 0 \ (p). \end{aligned}$$

So we have the following equation:

$$b + BY \equiv 0 \ (p)$$

where $b := (\binom{|S|}{0}, \binom{|S|}{1}, \cdots, \binom{|S|}{k})^T$,

$$\begin{aligned} Y := ((-1)^{2p-k} N^{2p-k}(S), \cdots, &(-1)^{2p-1} N^{2p-1}(S), \\ &(-1)^{2(2p-k)} N^{2(2p-k)}(S), \cdots, (-1)^{|S|} N^{|S|}(S))^T \end{aligned}$$

and

$$B = \begin{pmatrix} \binom{2k-1}{0} & \cdots & \binom{k}{0} & \binom{3k-2p-1}{0} & \cdots & \binom{0}{0} \\ \binom{2k-1}{1} & \cdots & \binom{k}{1} & \binom{3k-2p-1}{1} & \cdots & \binom{0}{1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{2k-1}{k} & \cdots & \binom{k}{k} & \binom{3k-2p-1}{k} & \cdots & \binom{0}{k} \end{pmatrix}.$$

Obviously (B,b) contains (A,b) as a sub-matrix. Hence

$$r((B,b)) = r((A,b)) = k+1.$$

Since $k \leq 3k-p-i \leq 2k-1$ and

$$\binom{3k-2p-i}{t} \equiv \binom{3k-p-i}{t} \ (p)$$

for $0 \leq t \leq k$ and $1 \leq i \leq 3k-2p$, it follows that

$$r(B) = r(A) \leq k.$$

This derives a contradiction. So (3.2) is true for $G = C_p \oplus C_p$.

In the following, we show (3.2) is true for all positive integers m and n with $1 < m|n$. Equivalently, we show that for every sequence S of length $d+k$, it has a zero-sum subsequence of length less or equal to $d-k$. We proceed by induction on m and n. Suppose that (3.2) is true for all $C_{m'} \oplus C_{n'}$ with $m'|m, n'|n$ and $m'|n'$. We show in the following that (3.2) is true for $C_m \oplus C_n$. Let p is a prime number such that $m = pm_1$, $n = pn_1$. We consider the epimorphism

$$\varphi : \ C_m \oplus C_n \to C_p \oplus C_p,$$

defined by $\varphi(g_1 + g_2) = m_1 g_1 + n_1 g_2$ with $g_1 \in C_m$, $g_2 \in C_n$. Then $\ker(\varphi) \cong C_{m_1} \oplus C_{n_1}$. Let S be a sequence with $|S| = d+k$. Set $d_1 := D(C_{m_1} \oplus C_{n_1})$ and $k := vp + p_0$ with $0 \leq p_0 \leq p-1$. Let

$$l := \lfloor \frac{|S| - 3p + 2}{p} \rfloor + 1 = d_1 - 1 + v.$$

Then l is the least integer such that $|S| - pl < 3p-2$. Since $\eta(C_p \oplus C_p) = 3p-2$, there is a decomposition

$$S = (T_1 \cdots T_l)T$$

with $\sigma(\varphi(T_i)) = 0$, $|T_i| \leq p$ for all $i \in [1, l]$ and $|T| \geq 2p - 1 + p_0$. By using

$$s_{\leq 2p-1-p_0}(C_p \oplus C_p) = 2p - 1 + p_0,$$

which we showed earlier, there is a subsequence $T_{l+1}|T$ such that

$$\sigma(\varphi(T_{l+1})) = 0 \ \text{ and } \ |T_{l+1}| \leq 2p - 1 - p_0.$$

Since $\sigma(T_i) \in \ker(\varphi)$ for all $i \in [1, l+1]$, it follows that

$$S_1 = \sigma(T_1) \cdots \sigma(T_l)\sigma(T_{l+1})$$

is a sequence in $C_{m_1} \oplus C_{n_1}$ with $|S_1| = d_1 + v$. By the induction assumption, one has

$$s_{\leq d_1 - v}(C_{m_1} \oplus C_{n_1}) = d_1 + v.$$

It implies that there is a zero-sum subsequence $S_1'|S_1$ with $|S_1'| \leq d_1 - v$. Let

$$S' = \prod_{\sigma(T_i)|S_1'} T_i.$$

Then S' is a zero-sum subsequence of S. If $\sigma(T_{l+1}) \nmid S_1'$, then

$$|S'| \leq (d_1 - v)p \leq d - k.$$

If $\sigma(T_{l+1}) \mid S_1'$, then

$$|S'| \leq (d_1 - 1 - v)p + 2p - 1 - p_0 = d - k.$$

Hence there is a zero-sum subsequence $S'|S$ with $|S'| \leq d-k$. This shows that (3.2) holds for any $C_m \oplus C_n$ and ends the proof of Theorem 1.2. ∎

4 Proof of Theorem 1.3

Before proving Theorem 1.3, we need a following lemma.

Lemma 4.1. *If G is a finite abelian group with $r(G) \geq 2$. Then $s_{\leq D(G)-1}(G) = D(G)+1$.*

Proof. By the definition of $D(G)$, there is a minimal zero-sum sequence S with $|S| = D(G)$. Then S apparently has no zero-sum subsequence of length $\leq D(G) - 1$. So,

$$s_{\leq D(G)-1}(G) \geq D(G) + 1.$$

It remainds to show that

$$s_{\leq D(G)-1}(G) \leq D(G) + 1.$$

Let T be any sequence of length $D(G) + 1$. It is enough to show that T has a zero-sum subsequence of length not exceeding $D(G)-1$. Conversely, suppose that T has no zero-sum subsequence of length at most $D(G) - 1$. Then the length of all zero-sum subsequences of T is $D(G)$. For any $g|T$, let $T' = T - g$. Since $|T'| = D(G)$, T' has a zero-sum subsequence. On the other hand, any zero-sum subsequence of T is of length $D(G)$. Thus T' itself is zero-sum. Hence we conclude that $g = \sigma(T)$ for any $g|T$. So $T = g^{D(G)+1}$, which implies that T has a minimal zero-sum subsequence $g^{\mathrm{ord}(g)}$. Since $r(G) \geq 2$, it follows that $\mathrm{ord}(g) \leq \exp(G) < D(G)$, a contrary. Thus $s_{\leq D(G)-1}(G) = D(G) + 1$. The proof of Lemma 4.1 is complete. ∎

In the following, we give the proof of Theorem 1.3.

Proof. We proceed by induction on k. Since $D(C_2^r) = r + 1$, by Lemma 4.1, one has $s_{\leq r}(C_2^r) = r + 2$. So, the theorem is true for $k = 0$. Let k be a positive integer with $r - k \in [\lceil \frac{2r+2}{3} \rceil, r]$, and assume $s_{\leq r-l} = r+2$ for $0 \leq l \leq k-1$, we show that $s_{\leq r-k} = r+2$. Since $s_{\leq r-k}(C_2^r) \geq s_{\leq r-k+1}(C_2^r) = r + 2$, it suffices to show that

$$s_{\leq r-k}(C_2^r) \leq r + 2.$$

Suppose to the contrary that there is a sequence S of length $r + 2$ without zero-sum subsequences of length in $[1, r-k]$. By the induction assumption, we have $s_{\leq r-k+1}(C_2^r) =$

$r+2$. Thus, there is a zero-sum subsequence $T|S$ with $|T| = r-k+1$ and T has to be a minimal zero-sum subsequence. Let $\{e_1, ..., e_r\}$ be a basis of C_2^r. Without loss of generality, one can suppose that

$$T = \prod_{i=1}^{r-k} e_i(e_1 + e_2 + \cdots + e_{r-k}).$$

Thus $S = TS_1$, where $S_1 := \prod_{j=1}^{k+1} a_j$.

Let $\varphi : C_2^r \to C_2^k$ with $\ker(\varphi) =< e_1, e_2, \cdots, e_{r-k} >$. Then $\varphi(S_1) = \prod_{j=1}^{k+1} \varphi(a_j)$ is a sequence of length $k+1$ in C_2^k. Since $D(C_2^k) = k+1$, there is a subsequence $T_1|S_1$ with $|T_1| \leq k+1$ and $\sigma(T_1) \in \ker(\varphi)$. Again without loss of generality, suppose that $\sigma(T_1) = e_1 + e_2 + \cdots + e_s$ with $s \leq r-k$. Then

$$T_1' = T_1 \prod_{i=1}^{s} e_i \text{ and } T_2' = \prod_{i=s+1}^{r-k} e_i T_1(e_1 + e_2 + \cdots + e_{r-k-1})$$

are zero-sum subsequences of S. Since $r-k \in [\lceil \frac{2r+2}{3} \rceil, r]$, we have $\min\{|T_1'|, |T_2'|\} \leq r-k$. Thus S has a zero-sum sequence of length $\leq r-k$. Hence we come to a contrary. Theorem 1.3 is proved. ∎

Remark. By Similar discussion as in the proof of Theorem 1.3, we can show that $s_{\leq r-k}(C_2^r) = r+3$ holds for all $r-k \in [\lceil \frac{4r+4}{7} \rceil, \lceil \frac{2r+2}{3} \rceil - 1]$ if $r \not\equiv 4$ (7) and for all $r-k \in [\lceil \frac{4r+7}{7} \rceil, \lceil \frac{2r+2}{3} \rceil - 1]$ if $r \equiv 4$ (7).

References

[1] G. Cohen and G. Zemor, Subset sums and coding theory, *Asterisque* 258 (1999), 327-339.

[2] C. Delorme, O. Ordaz, and D. Quiroz, Some remarks on Davenport constant, *Discrete Math.*, 237 (2001), 119-128.

[3] M. Freeze and W. Schmid, Remarks on a generalization of the Davenport constant, *Discrete Math.*, 310 (2010), 3373-3389.

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

[5] A.Geroldinger and F.Halter-Koch, Non-unique factorizations, Algebraic, Combinatorial and Analytic Theory, Chapman and Hall/CRC, 2006.