THE EGZ-CONSTANT AND SHORT ZERO-SUM SEQUENCES OVER FINITE ABELIAN GROUPS

WEIDONG GAO, DONGCHUN HAN, AND HANBIN ZHANG

Abstract. Let G be an additive finite abelian group with exponent $\exp(G)$. Let $\eta(G)$ be the smallest integer t such that every sequence of length t has a nonempty zero-sum subsequence of length at most $\exp(G)$. Let $\mathbf{s}(G)$ be the EGZ-constant of G, which is defined as the smallest integer t such that every sequence of length t has a zero-sum subsequence of length $\exp(G)$. Let p be an odd prime. We determine $\eta(G)$ for some groups G with $\mathbf{D}(G) \le 2\exp(G) - 1$, including the p-groups of rank three and the p-groups $G = C_{\exp(G)} \oplus C_{p^m}^r$. We also determine $\mathbf{s}(G)$ for the groups G above with more larger exponent than $\mathsf{D}(G)$, which confirms a conjecture by Schmid and Zhuang from 2010, where $\mathsf{D}(G)$ denotes the Davenport constant of G.

1. Introduction

Throughout this paper, let p denote a prime. Let G be an additive finite abelian group with exponent $\exp(G)$. Let $S = g_1 \cdot \ldots \cdot g_k$ be a sequence over G. We call S a zero-sum sequence if $0 = \Sigma_{i=1}^{k} g_i$. The Davenport's constant, denoted by $\mathsf{D}(G)$, is the minimal integer t such that such that every sequence S over G of length $|S| \ge t$ has a nonempty zero-sum subsequence. Let $\eta(G)$ be the minimal integer t such that every sequence of length t has a nonempty zero-sum subsequence of length less than or equal to $\exp(G)$. Let $\mathsf{s}(G)$ be the minimal integer t such that every sequence of length t has a zero-sum subsequence of length $\exp(G)$.

These are classical invariants in combinatorial number theory and have received a lot of attention(see [17], [18], [8], [2], [11]). For G is cyclic, we have $\eta(G) = |G|$, and $\mathsf{s}(G) = 2|G| - 1$ by the well known Erdős-Ginzurg-Ziv theorem [5]. For the case that G is of rank two, the key step of determine $\eta(G)$ (resp. $\mathsf{s}(G)$) is to determine $\eta(C_p^2)$ (resp. $\mathsf{s}(C_p^2)$). In 1969, Olson [17] proved $\eta(C_p^2) = 3p - 2$. While the determining of $\mathsf{s}(C_p^2)$ is very complicated. In 1983, Kemnitz [15] conjectured that $\mathsf{s}(C_p^2) = 4p - 3$ and it was confirmed by C. Reiher [18] in 2007. The precise values of $\eta(G)$ and $\mathsf{s}(G)$ for groups with rank at most two has been summarized in ([13, Theorem 5.8.3]) as follows.

If $G = C_m \oplus C_n$ with $1 \le m|n$, then $s(G) = \eta(G) + n - 1 = 2m + 2n - 3$.

The situation is very different for groups of higher rank. Even for the group $G = C_p^3$ with p being a prime, the precise value of the $\eta(G)$, $s(G)$ is unknown (for general p). Fan, Gao, Wang, and Zhong [8] determined the $\eta(G)$ and $s(G)$ for a special type groups with rank three. When $G = C_3^r$, the precise value of $\eta(G)$ and $s(G)$ has been determined for $r \le 6$ (see [4]). Apart the results mentioned above, Schmid and Zhuang [19] proved that if G is a finite abelian p-group with $\mathsf{D}(G) = 2\exp(G) - 1$, then $2\mathsf{D}(G) - 1 = \eta(G) + \exp(G) - 1 = s(G)$, which has

Gao.

been generalized recently by Geroldinger, Grynkiewcz and Schmid [12, Theorem 4.2]. Schmid and Zhuang further conjectured the following.

Conjecture 1.1. *([19]) Let G be a finite abelian p-group with $\mathsf{D}(G) \le 2\exp(G)-1$. Then*

$$2\mathsf{D}(G) - 1 = \eta(G) + \exp(G) - 1 = s(G).$$

In this paper we verify this conjecture for some p-groups with $\mathsf{D}(G) < 2\exp(G)-1$ and our main results are the following.

Theorem 1.2. *Let a, n be positive integers, let H be a finite abelian p-group, and let $G = C_{ap^n} \oplus H$. Suppose that $\mathsf{D}(C_{p^n} \oplus H)) \le 2p^n - 1$. If $p > 2r(H)$ then*

$$\eta(G) = 2\mathsf{D}(G) - ap^n = ap^n + 2\mathsf{D}(H) - 2$$

provided that H satisfies one of the following conditions:

(1) $\mathsf{D}(H) \le 2\exp(H)$.
(2) $\lceil (k+\frac{1}{2})\exp(H)\rceil < \mathsf{D}(H) \le (k+1)\exp(H)$ *for some integer $k \ge 2$.*

Theorem 1.3. *Let H be a finite abelian p-group with $\exp(H) = p^m$, and let $G = C_{ap^n} \oplus H$. If $p > 2r(H)$, $p^n \ge \mathsf{D}(H)$ and $a > |H|p^{2m-n}$, then*

$$s(G) = \eta(G) + ap^n - 1 = 2ap^n + 2\mathsf{D}(H) - 3$$

provided that H satisfies one of the following conditions:

(1) $\mathsf{D}(H) \le 2\exp(H)$.
(2) $\lceil (k+\frac{1}{2})\exp(H)\rceil < \mathsf{D}(H) \le (k+1)\exp(H)$ *for some integer $k \ge 2$.*

It is easy to see that the conditions of Theorem 1.2 are fulfilled by the following groups H and G.

- $r(H) = 2$ and $\mathsf{D}(C_{p^n} \oplus H) \le 2p^n - 1$.
- $\mathsf{D}(C_{p^n} \oplus H) \le 2p^n - 1$, $H = C_{p^m}^r$ and $p \ge 2r + 1$.

It is easy to see that the conditions of Theorem 1.3 are fulfilled by the following groups H and G.

- $r(H) = 2$, $\mathsf{D}(C_{p^n} \oplus H) \le 2p^n - 1$ and $a > |H|p^{2m-n}$.
- $\mathsf{D}(C_{p^n} \oplus H) \le 2p^n - 1$, $H = C_{p^m}^r$, $p \ge 2r + 1$ and $a > |H|p^{2m-n}$

2. Preliminaries

Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For a real number x, we denote by $\lfloor x \rfloor$ the largest integer that is less than or equals to x, and denote by $\lceil x \rceil$ the smallest integer that is greater than or equals to x.

Throughout, all abelian groups will be written additively. By the Fundamental Theorem of Finite Abelian Groups we have

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

where $r = \mathsf{r}(G) \in \mathbb{N}_0$ is the rank of G, $n_1, \ldots, n_r \in \mathbb{N}$ are integers with $1 < n_1 | \ldots | n_r$, moreover, $n_1, \ldots, n_r$ are uniquely determined by G, and $n_r = \exp(G)$ is the *exponent* of G. Let

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

For $g_1, \ldots, g_l \in G$(repetition allowed), we call $S = g_1 \cdot \ldots \cdot g_l$ a *sequence* over G. We write sequences S in the form

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

We call $\mathsf{v}_g(S)$ the *multiplicity* of g in S.

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

- $|S| = l = \Sigma_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0$ the *length* of S.
- $\sigma(S) = \Sigma_{i=1}^{l} g_i = \Sigma_{g \in G} \mathsf{v}_g(S) g \in G$ the *sum* of S.
- S is a *zero-sum sequence* if $\sigma(S) = 0$.
- S is a *short zero-sum sequence* if it is a zero-sum sequence of length $|S| \in [1, \exp(G)]$

Let $S = g_1 \cdot \ldots \cdot g_l$ be a sequence over G of length $|S| = l \in \mathbb{N}_0$ and let $g \in G$. For every $k \in \mathbb{N}_0$ let

$$N_g^k(S) = |\{I \subset [1, l] \mid \Sigma_{i \in I} g_i = g, |I| = k\}|$$

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).

For convenience, let $N^k(S)$ denote $N_0^k(S)$.

Lemma 2.1. *(*[4, Lemma 3.2]*) Let H be a finite abelian group, and let $G = C_n \oplus H$. If $\exp(H) \mid n$ then $\eta(G) \leq n + 2\mathsf{D}(H) - 2$.*

Lemma 2.2. ([16]) *Let G be a finite abelian p-group. Then*

$$\mathsf{D}(G) = \mathsf{D}^*(G).$$

Moreover, if S is a sequence over G with $|S| = l \geq \mathsf{D}^*(G)$, then

$$1 - N^1(S) + N^2(S) + \cdots + (-1)^l N^l(S) \equiv 0 \pmod{p}.$$

Lemma 2.3. *Let m be a positive integer, let G be a finite abelian p-group, and let S be a sequence over G of length $|S| \geq \mathsf{D}(G) + p^m - 1$. Let $t = \lfloor \frac{|S|}{p^m} \rfloor$. Then*

$$1 + \Sigma_{j=1}^{t} (-1)^j N^{jp^m}(S) \equiv 0 \pmod{p}.$$

Proof. Let $G \oplus C_{p^m} = G \oplus \langle e \rangle$ with $\langle e \rangle = C_{p^m}$. Let $\varphi : G \to G \oplus C_{p^m}$ be defined by $\varphi(g) = g + e$ for every $g \in G$. Let $S = g_1 \cdot \ldots \cdot g_l$. Then $\varphi(S) = (g_1 + e) \cdot \ldots \cdot (g_l + e)$ is a sequence over $G \oplus C_{p^m}$. Thus let $\varphi(T)$ be a subsequence of $\varphi(S)$ over $G \oplus C_{p^m}$, $\sigma(\varphi(T)) = 0$ if and only if $\sigma(T) = 0$ and $|T| \equiv 0 \pmod{p^m}$.

Apply lemma 2.2 to the sequence $\varphi(S)$, we get

$$1 + \Sigma_{j=1}^{t} (-1)^j N^{jp^m}(\varphi(S)) \equiv 0 \pmod{p},$$

hence

$$1 + \Sigma_{j=1}^{t} (-1)^j N^{jp^m}(S) \equiv 0 \pmod{p}.$$

This completes the proof.

$\square$

The following congruence is first used by Lucas [14], we give a proof for the convenience of the reader.

Lemma 2.4. *Let a, b be positive integers with $a = a_n p^n + \cdots + a_1 p + a_0$ and $b = b_n p^n + \cdots + b_1 p + b_0$ be the p-adic expansions, where p is a prime, define $\binom{k}{0} = 1$ for $k \geq 0$. Then*

$$\binom{a}{b} \equiv \binom{a_n}{b_n}\binom{a_{n-1}}{b_{n-1}} \cdots \binom{a_0}{b_0} \pmod{p}.$$

Proof. We have

$$\begin{aligned} (1+x)^a &= (1+x)^{a_n p^n + \cdots + a_1 p + a_0} \\ &= (1+x^{p^n})^{a_n} \cdots (1+x^p)^{a_1}(1+x)^{a_0} \pmod{p} \end{aligned}$$

Since $0 \leq a_i \leq p-1$, comparing the coefficient of x^b, we get the desired result. ∎

Lemma 2.5. *Let n and k be positive integers with $1 \leq 2k \leq n$, and let $A = \left(\binom{n-j}{i}\right)_{0 \leq i,j \leq k}$, that is*

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \binom{n}{1} & \binom{n-1}{1} & \cdots & \binom{n-k}{1} \\ \binom{n}{2} & \binom{n-1}{2} & \cdots & \binom{n-k}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{n}{k} & \binom{n-1}{k} & \cdots & \binom{n-k}{k} \end{pmatrix}_{(k+1)\times(k+1)}.$$

Then we have

$$det(A) = \frac{1}{\prod\limits_{1 \leq t \leq k} t!} \prod_{1 \leq i < j \leq k} (j-i).$$

Proof. Let

$$B = \begin{pmatrix} 1 & 1 & & 1 \\ n & n-1 & \cdots & n-k \\ n(n-1) & (n-1)(n-2) & & (n-k)(n-k-1) \\ \vdots & \vdots & \ddots & \vdots \\ n\cdots(n-k+1) & (n-1)\cdots(n-k) & \cdots & (n-k)\cdots(n-2k+1) \end{pmatrix}.$$

In what follows, we denote the ith row of B by $Row_B(i)$.

Firstly, replace $Row_B(3)$ by $Row_B(3)+Row_B(2)$, and we get the following matrix

$$\begin{pmatrix} 1 & 1 & & 1 \\ n & n-1 & \cdots & n-k \\ n^2 & (n-1)^2 & & (n-k)^2 \\ \vdots & \vdots & \ddots & \vdots \\ n\cdots(n-k+1) & (n-1)\cdots(n-k) & \cdots & (n-k)\cdots(n-2k+1) \end{pmatrix}.$$

by abuse of language we also denote the corresponding new matrix by B.

Similarly, let $f_i(x) = x(x-1)\cdots(x-i+2) = x^{i-1} + a_{i-2}x^{i-2} + \cdots + a_1 x$. Then replace $Row_B(i)$ by $Row_B(i) - a_{i-2}Row_B(i-1) - \cdots - a_1 Row_B(2)$ successively for

$4 \le i \le k+1$ and after each step also denote the corresponding new matrix by B, we can get the following matrix

$$C = \begin{pmatrix} 1 & 1 & & 1 \\ n & n-1 & \dots & n-k \\ n^2 & (n-1)^2 & & (n-k)^2 \\ \vdots & \vdots & \ddots & \vdots \\ n^k & (n-1)^k & \dots & (n-k)^k \end{pmatrix}.$$

It is well known that $det(C)$ is a Vandermonde determinant, then clearly

$$det(A) = \frac{1}{\prod\limits_{1 \le t \le k} t!} det(B) = \frac{1}{\prod\limits_{1 \le t \le k} t!} det(C) = \frac{1}{\prod\limits_{1 \le t \le k} t!} \prod_{1 \le i < j \le k} (j-i).$$

□

Lemma 2.6. [8, Theorem 1.2] *Let H be an arbitrary finite abelian group with* $\exp(H) = u \ge 2$, *and let $G = C_{vu} \oplus H$. If $v \ge \max\{u|H|+1, 4|H|+2u\}$, then* $s(G) = \eta(G) + \exp(G) - 1$.

Lemma 2.7. *(*[12, Page 7, (4.1)]*) Let K be subgroup of a finite abelian group G. Then, $\eta(G) \le \exp(G/K)(\eta(K)-1) + \eta(G/K)$.*

Lemma 2.8. *(*[3]*) Let a, n be a positive integer, let H be a finite abelian p-group with $D(H) \le p^n - 1$, and let $G = C_{ap^n} \oplus H$. Then, $\mathsf{D}(G) = ap^n + D(H) - 1$.*

3. Proof of the main theorems

Let $G = C_{p^n} \oplus H$ be a finite abelian p-group with $\exp(H) = p^m$. Let k be the integer with

$$kp^m \le \mathsf{D}(H) - 1 < (k+1)p^m,$$

and let

$$v = (k+1)p^m - \mathsf{D}(H).$$

The following technical result is crucial in the proof of Theorem 1.2.

Lemma 3.1. *Let $G = C_{p^n} \oplus H$ be a finite p-group with $\exp(H) = p^m$, and let S be a sequence over G of length $s = |S| = p^n + 2\mathsf{D}(H) - 2$. Suppose that S has no short zero-sum subsequence. If $p^n \ge 2\mathsf{D}(H) - 2$, then we have the following congruences:*

$$1 + \Sigma_{u=0}^{h} \binom{h}{u} \Sigma_{j=1}^{k} (-1)^{j-1} N^{p^n + jp^m - u}(S) \equiv 0 \pmod p \tag{3.1}$$

holds for every $h \in [0, v]$, and

$$\Sigma_{j=1}^{k} (-1)^{j-1} N^{p^n + jp^m - h}(S) \equiv 0 \pmod p \tag{3.2}$$

for every $h \in [1, v]$, and

$$\begin{aligned}&\tbinom{|S|}{ip^m} + \Sigma_{j=1}^{k} (-1)^{j-1} \Sigma_{u=0}^{v} \tbinom{|S| - p^n - jp^m + u}{ip^m} \tbinom{v}{u} N^{p^n + jp^m - u}(S) \\ &\equiv 0 \pmod p\end{aligned} \tag{3.3}$$

for every $i \in [0, k]$.

Proof. We first have the following claim.

Claim. $N^i(S) = 0$ for every $i \in [1, p^n] \cup [p^n + \mathsf{D}(H), |S|]$.

Since S has no short zero-sum subsequence, we obtain $N^i(S) = 0$ for every $i \in [1, p^n]$. Assume that $N^i(S) \neq 0$ for some $i \in [p^n + \mathsf{D}(H), |S|]$, then S has a zero-sum subsequence W of length $|W| = i \geq p^n + \mathsf{D}(H) = \mathsf{D}(G) + 1$, which implies W can be divided into two nonempty zero-sum subsequences $W = W_1 W_2$ with $|W_1| \leq |W_2|$. Since $2\mathsf{D}(H) - 2 \leq p^n$, we have

$$|W_1| \leq \frac{|W|}{2} \leq \frac{|S|}{2} = \frac{p^n + 2D(H) - 2}{2} \leq p^n = \exp(G),$$

it is a contradiction completing the proof of the Claim.

Consider the following homomorphism

$$\varphi : \; G = C_{p^n} \oplus H \to C_{p^n} \oplus H \oplus C_{p^m} = G \oplus \langle e \rangle$$

with $\varphi(g) = g + e$ for every $g \in G$, where $\langle e \rangle = C_{p^m}$. Let $S = g_1 \cdot \ldots \cdot g_s$. Then $\varphi(S) = (g_1 + e) \cdot \ldots \cdot (g_s + e)$ is a sequence over $G \oplus C_{p^m}$.

For $i \in [0, k]$, let T be an arbitrary subsequence of S of length

$$|T| = |S| - ip^m.$$

Note that

$$\begin{aligned} |T0^h| &= |T| + h = p^n + 2\mathsf{D}(H) - 2 - ip^m + h \geq p^n + \mathsf{D}(H) - 1 + p^m \\ &= \mathsf{D}(G) + p^m - 1 \end{aligned}$$

holds for $i \in [0, k-1]$ and $h \in [0, v]$, or $i = k$ and $h = v$. Applying Lemma 2.3 to the sequence $\varphi(T0^h)$ with $i \in [0, k-1]$ and $h \in [0, v]$, or $i = k$ and $h = v$, we get

$$1 + \Sigma_{j=1}^{t} (-1)^j N^{jp^m}(\varphi(T0^h)) \equiv 0 \pmod{p}. \tag{3.4}$$

where $t = \lfloor \frac{|T0^h|}{p^m} \rfloor$. Therefore,

$$1 + \Sigma_{j=1}^{t} (-1)^j (\Sigma_{u=0}^{h} \binom{h}{u} N^{jp^m - u}(T)) \equiv 0 \pmod{p}, \tag{3.5}$$

since $N^{jp^m}(\varphi(T0^h)) = \Sigma_{u=0}^{h} \binom{h}{u} N^{jp^m - u}(T)$ for every $j \in [1, t]$.

Note that $N^i(T) \leq N^i(S)$. Applying the claim above we obtain, $N^i(T) = 0$ for every $i \in [1, p^n] \cup [p^n + \mathsf{D}(H), |T|]$. Since $p^n + \mathsf{D}(H) = p^n + (k+1)p^m - v$, by (3.5), we obtain

$$1 + \Sigma_{u=0}^{h} \binom{h}{u} \Sigma_{j=1}^{k} (-1)^{j-1} N^{p^n + jp^m - u}(T) \equiv 0 \pmod{p} \tag{3.6}$$

holds for every pair of (h, i) with $h \in [0, v]$ and $i \in [0, k-1]$, or $h = v$ and $i = k$.

Taking $T = S$ in (3.6) we obtain (3.1).

Let $F(h) = 1 + \Sigma_{u=0}^{h} \binom{h}{u} \Sigma_{j=1}^{k} (-1)^{j-1} N^{p^n + jp^m - u}(S)$. By (3.1), we obtain that $F(h+1) - F(h) \equiv 0 \pmod{p}$. That is,

$$\begin{aligned} &\Sigma_{j=1}^{k} (-1)^{j-1} N^{p^n + jp^m - (h+1)}(S) = \\ &-\Sigma_{u=0}^{h} (\tbinom{h+1}{u} - \tbinom{h}{u}) \Sigma_{j=1}^{k} (-1)^{j-1} N^{p^n + jp^m - u}(S) \pmod{p}. \end{aligned} \tag{3.7}$$

Taking $h = 0$ in (3.7), we obtain

$$\Sigma_{j=1}^{k} (-1)^{j-1} N^{p^n + jp^m - 1}(S) \equiv 0 \pmod{p}.$$

This proves (3.2) for $h = 1$. Suppose that (3.2) is true for all $h < \ell$ $(\le v)$. Again by (3.7) taking $h = \ell - 1$, we obtain $\Sigma_{j=1}^{k}(-1)^{j-1}N^{p^n+jp^m-\ell}(S) \equiv 0 \pmod p$ completing the proof of (3.2). Now it remains to prove (3.3).

By (3.6) we have

$$\Sigma_{|T|=|S|-ip^m}\left(1+\Sigma_{u=0}^{v}\binom{v}{u}\Sigma_{j=1}^{k}(-1)^{j-1}N^{p^n+jp^m-u}(T)\right) \equiv 0 \pmod p, \tag{3.8}$$

where the sum is taken over all $T|S$ of length $|T| = |S| - ip^m$.

Note that each subsequence W of S of length $|W| \le |S| - ip^m$ can be extended to a subsequence T of length $|T| = |S| - ip^m$ in $\binom{|S|-|W|}{|T|-|W|} = \binom{|S|-|W|}{|S|-|T|} = \binom{|S|-|W|}{ip^m}$ way. Therefore, the left side of (3.8) equals

$$\binom{|S|}{ip^m} + \Sigma_{j=1}^{k}(-1)^{j-1}\Sigma_{u=0}^{v}\binom{|S|-p^n-jp^m+u}{ip^m}\binom{v}{u}N^{p^n+jp^m-u}(S).$$

Now (3.3) follows. □

Remark 3.2. Note that v could be 0 and the list of (3.2) is empty.

Proposition 3.3. *Let H be a finite abelian p-group with $2r(H) < p$, and let $G = C_{p^n} \oplus H$ with $\mathsf{D}(G) \le 2p^n - 1$. Let $\exp(H) = p^m$, and let $\mathsf{D}(H) - 1 = kp^m + t$ with k a integer and $t \in [0, p^m - 1]$. If $k = 1$ or $2t \ge p^m$, then*

$$\eta(G) = 2\mathsf{D}(G) - p^n = p^n + 2\mathsf{D}(H) - 2.$$

Proof. By Lemma 2.1, it suffices to prove that $\eta(G) \le p^n + 2\mathsf{D}(H) - 2$.

Let S be a sequence over G of length $s = |S| = p^n + 2\mathsf{D}(H) - 2 = p^n + 2kp^m + 2t$. We need to show S has a short zero-sum subsequence. Assume to the contrary that S has no short zero-sum sequence.

Case 1 $k = 1$**.**

Since $p > 2r(H)$, we know that p is a odd prime and $\mathsf{D}(H) = \mathsf{D}^*(H)$ is odd. Therefore,

$$v = 2p^m - \mathsf{D}(H) \ge 1.$$

In this case, (3.2) becomes

$$N^{p^n+p^m-h}(S) \equiv 0 \pmod p \tag{3.9}$$

for every $h \in [1, v]$.

By (3.3) taking $i = 1$, we obtain

$$\binom{p^n+2p^m+2t}{p^m} + \Sigma_{u=0}^{v}\binom{p^m+2t+u}{p^m}N^{p^n+p^m-u}(S) \equiv 0 \pmod p.$$

This together with (3.9) gives that

$$\binom{p^n+2p^m+2t}{p^m} + \binom{p^m+2t}{p^m}N^{p^n+p^m}(S) \equiv 0 \pmod p.$$

It follows from Lemma 2.4 that

$$\binom{2p^m+2t}{p^m} + \binom{p^m+2t}{p^m}N^{p^n+p^m}(S) \equiv 0 \pmod p. \tag{3.10}$$

Again by Lemma 2.4 and according to $2t < p^m$ or not, from (3.10) we know that either

$$2 + N^{p^n+p^m}(S) \equiv 0 \pmod p$$

or

$$3 + 2N^{p^n+p^m}(S) \equiv 0 \pmod p.$$

Both contradict to $1 + N^{p^n+p^m}(S) \equiv 0 \pmod p$ by (3.1).

Case 2: $2t \geq p^m$

From the assumption that $2r(H) < p$ we infer that $kp^m + t = \mathsf{D}(H) - 1 = \mathsf{D}^*(H) - 1 < r(H)p^m < \frac{p}{2} \times p^m$. Therefore,

$$2k < p.$$

Since

$$|S| - p^n - jp^m = p^n + 2kp^m + 2t - p^n - jp^m = (2k-j)p^m + 2t$$

and

$$\begin{aligned} |S| - p^n - jp^m + v &= p^n + 2kp^m + 2t - p^n - jp^m + (k+1)p^m - (kp^m + t + 1) \\ &= (2k-j)p^m + p^m + t - 1. \end{aligned}$$

By Lemma 2.4, $\binom{|S|-p^n-jp^m+u}{ip^m} = \binom{|S|-p^n-jp^m}{ip^m}$ for every $u \in [0, v]$. Thus in (3.3), we can treat $\Sigma_{u=0}^{v}\binom{v}{u}N^{p^n+jp^m-u}(S)$ as one variable.

Set $i = 0, \ldots, k$ respectively in (3.3), we get a group of linear equations in variables $1, \Sigma_{u=0}^{v}\binom{v}{u}N^{p^n+p^m-u}(S), \ldots, (-1)^{k-1}\Sigma_{u=0}^{v}\binom{v}{u}N^{p^n+kp^m-u}(S)$. That is

$$\begin{aligned} &\tbinom{2kp^m+2t}{ip^m} + \Sigma_{j=1}^{k}(-1)^{j-1}\tbinom{(2k-j)p^m+2t}{ip^m}\Sigma_{u=0}^{v}\tbinom{v}{u}N^{p^n+p^m-u}(S) \\ &\equiv 0 \pmod p \end{aligned} \tag{3.11}$$

for every $i \in [0, k]$.

Let $2t = p^m + d$ and $l = 2k + 1$, where $0 \leq d \leq p^m - 1$. Note that $2k < p$. By Lemma 2.4 we have

$$\binom{(2k-j)p^m + 2t}{ip^m} = \binom{2k+1-j}{i} = \binom{l-j}{i}$$

for all $i \in [0, k]$ and $j \in [0, k]$.

So, the coefficient matrix of the group of linear equations of (3.11) is $A = (\binom{l-j}{i})_{0 \leq i,j \leq k}$, that is

$$A = \begin{pmatrix} 1 & 1 & & 1 \\ \binom{l}{1} & \binom{l-1}{1} & \cdots & \binom{l-k}{1} \\ \binom{l}{2} & \binom{l-1}{2} & \cdots & \binom{l-k}{2} \\ & & \ddots & \\ \binom{l}{k} & \binom{l-1}{k} & \cdots & \binom{l-k}{k} \end{pmatrix}_{(k+1)\times(k+1)}.$$

By lemma 2.5 we have

$$det(A) = \frac{1}{\prod\limits_{1 \leq t \leq k} t!} \prod_{1 \leq i < j \leq k} (j - i) \not\equiv 0 \pmod p.$$

Therefore the linear equations above has only trivial solution

$$\begin{aligned} &1 \equiv \Sigma_{u=0}^{v}\tbinom{v}{u}N^{p^n+p^m-u}(S) \equiv \cdots \equiv (-1)^{k-1}\Sigma_{u=0}^{v}\tbinom{v}{u}N^{p^n+kp^m-u}(S) \\ &\equiv 0 \pmod p), \end{aligned}$$

a contradiction. □

Proof of Theorem 1.2. By Lemma 2.1 and Lemma 2.8, we only need to prove that $\eta(G) \le ap^n + 2\mathsf{D}(H) - 2$. Note that if $\eta(G) \le ap^n + 2\mathsf{D}(H) - 2$ for $a = 1$, then by Lemma 2.7 taking $K \simeq C_a$ as a subgroup of G, we obtain that $\eta(G) \le \exp(G/K)(\eta(K) - 1) + \eta(G/K) = p^n(a-1) + p^n + 2\mathsf{D}(H) - 2 = ap^n + 2\mathsf{D}(H) - 2$. So, it suffices to prove the theorem for $a = 1$ which we now assume.

(1): $\mathsf{D}(H) \le 2\exp(H)$.

Since $\mathsf{D}(H) - 1 \le 2\exp(H) - 1$, we have

$$k = 1.$$

Hence by Proposition 3.3, we get the desired result.

(2): $\lceil (k + \frac{1}{2})\exp(H) \rceil < \mathsf{D}(H) \le (k+1)\exp(H)$ for some integer $k \ge 2$.

Let $\mathsf{D}(H) - 1 = kp^m + t$. Since $\lceil (k + \frac{1}{2})\exp(H) \rceil < \mathsf{D}(H) \le (k+1)\exp(H)$, we have

$$2t \ge p^m.$$

Hence by Proposition 3.3, we get the desired result.

□

Proof of Theorem 1.3. If H is cyclic, then G is of rank at most two and the result is true as mentioned in the introduction. Now we assume that $r(H) \ge 2$. Since $p > 2r(H)$, we have $p \ge 5$ and $|H| \ge 25$ follows. Let $u = p^m$ and $v = ap^{n-m}$. Then $uv = ap^n$. By $a > p^{2m-n}|H|$ we obtain $v \ge m|H| + 1 = \max\{m|H| + 1, 4|H| + 2m\}$. It follows from Lemma 2.6 that $s(G) = \eta(G) + \exp(G) - 1$. Now the result follows from Theorem 1.2.

□

References

1. N. Alon and M. Dubiner, *A lattice point problem and additive number theory,* Combinatorica, 15 (1995) 301-309.
2. R. Chi, S.Y. Ding, W.D. Gao , A. Geroldinger and W.A. Schmid, *On zero-sum subsequences of restricted size IV.* Acta Math. Hung., 107(2005) 337- 344.
3. P. van Emde Boas, A combinatorial problem on finite abelian groups II, in *Reports of the Mathematisch Centrum Amsterdam*, ZW-1969-007.
4. Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham. *Zero-sum problems in finite abelian groups and affine caps.* Quarterly J. Math., Oxford II. Ser., 58(2007) 159-186.
5. P. Erdős, G. Ginzburg and A. Ziv, *Theorem in the additive number theory*, Bull. Res. Council Israel, 10F(1961) 41-43.
6. Y.S. Fan, W.D. Gao, G.Q. Wang, Q.H. Zhong and J.J. Zhuang, *On Short Zero-sum Subsequences of Zero-sum Sequences*, Electronic J. Combinatorics, 2012.
7. Y.S. Fan, W.D. Gao and Q.H. Zhong, *On the Erdős-Ginzburg-Ziv constant of finite abelian groups of high rank*, 131(2011) 1864-1874.
8. Y.S. Fan, W.D. Gao, L.L. Wang, Q.H. Zhong, *Two zero-sum invariants on finite abelian groups*, European J. Combinatorics, 34 (2013) 1331-1337.
9. W.D. Gao, *On zero-sum subsequences of restricted size III*, Ars. Combin., 61 (2001) 65-72.
10. W.D. Gao, *On zero-sum subsequences of restricted size II*, Discrete Math., 271 (2003) 51-59.
11. W.D. Gao and A. Geroldinger, *Zero-sum problems in abelian groups: A survey*, Expo. Math., 24 (2006) 337-369.
12. A. Geroldinger, D.J. Grynkiewicz and W.A. Schmid, *Zero-sum problems with congruence conditions.* Acta Math. Hung., 131(2011) 323- 345.

13. A. Geroldinger and F. Halter-Koch, Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
14. F.E.A. Lucas, *Sur les congruences des nombres eulériens et les coefficients différentiels des functions trigonométriques suivant un module premier.(French)*, Bull. Soc. Math. France, 6 (1878) 49-54.
15. A. kemnitz, *On a lattice point problem*, Ars Combin., 16b(1983) 151-160.
16. J.E. Olson, *A combinatorial problem on finite Abelian groups I*, J. Number Theory, 1(1969) 8-10.
17. J. E. Olson, *A combinatorial problem on finite Abelian groups II*, J. Number Theory, 1(1969) 195-199.
18. C. Reiher, *On Kemnitz' conjecture concerning lattice points in the plane*, Ramanujan J., 13(2007) 333-337.
19. W.A. Schmid and J.J. Zhuang, *On short zero-sum subsequences over p-groups*, Ars. Combin., 95(2010) 343-352.

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
E-mail address: wdgao1963@aliyun.com

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
E-mail address: han-qingfeng@163.com

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
E-mail address: nkuzhanghanbin@163.com