On Short Zero-Sum Subsequences

W. D. Gao* J. Zhou †

April 26, 2004

Abstract

Let G be a finite abelian group of exponent m. By $s(G)$ we denote the smallest integer t such that, every sequence of t elements in G contains a zero-sum subsequence of length m. Among other results, we prove that, let p be a prime, and let $H = C_{p^{e_1}} \oplus \cdots \oplus C_{p^{e_l}}$ be a p-group. Suppose that $1 + \sum_{i=1}^{l}(p^{e_i} - 1) = p^k$ for some positive integer k. Then, $4p^k - 3 \leq s(C_{p^k} \oplus H) \leq 4p^k - 2$.

1 Introduction

Let G be a finite abelian group. We call $S = (a_1, \cdots, a_k)$ *a sequence in* G if all $a_i \in G$. We call S *a zero-sum sequence* if the sum $\sum_{i=1}^{k} a_i = 0$. We call S a *zero-free sequence* if S contains no nonempty zero-sum subsequence. Let m be the exponent of G, i.e., the maximal order of an element in G. We call a zero-sum sequence S in G *a short zero-sum sequence* if $1 \leq |S| \leq m$. In this paper we will study the following invariants on short zero-sum sequences which play important roles in zero-sum problems ([3], [9]).

Definition 1.1 *Define $\rho(G)$ to be the smallest integer t such that every sequence S in G with $|S| \geq t$ contains a short zero-sum subsequence.*

*This work has been supported partly by NSFC with grant number 19971058 and by MOEC with grant number 02047. Department of Computer Science and Technology, University of Petroleum, Beijing, 102200, China

†Tsinghua High School, Beijing, 100084, China

Definition 1.2 *Define $s(G)$ to be the smallest integer t such that every sequence S in G with $|S| \geq t$ contains a zero-sum subsequence of length m.*

Definition 1.3 *Define $D(G)$ to be the smallest integer d such that every sequence S in G with $|S| \geq d$ contains a nonempty zero-sum subsequence.*

Let m, k be positive integers. By C_m we denote the finite cyclic group of m elements, and by C_m^k we denote the direct sum of k copies of C_m. So far, many studies have been made on $\rho(G)$ and $s(G)$. Here we list some known results on them.

Theorem 1.4 *Let p be a prime, and let G be a finite abelian group of exponent m. Then,*

1. $s(C_m) = 2m - 1$. [4]
2. $\rho(G) \leq |G|$. [8]
3. $s(G) \leq |G| + m - 1$. [10]
4. $s(C_m^k) \leq c(k)m$, *where* $c(k) \leq 256(k \log_2 k)^k$. [2]
5. $s(G) \geq \rho(G) + m - 1$. [8]
6. $s(C_{p^d}^2) \leq 4p^d - 2$. [5]
7. $s(C_m^2) \leq \frac{41}{10}m$. [14]
8. $s(C_m^2) = 4m-3$ *provided that* $m = 2^a3^b5^c7^dn$ *and* $n \leq \frac{5}{2}(2^a3^b5^c7^d)^{1/2}$. ([6], [7], [12])
9. $s(C_3^3) = 19$. [12]
10. $s(C_3^4) = 41$. [12]
11. $s(C_3^k) = \rho(C_3^k) + 2$. [7]
12. $s(C_{2^d}^k) = 2^k(2^d - 1) + 1$. [11]

Let G be a finite abelian group with $|G| > 1$. It is well known that $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 | \cdots | n_r$. Set $M(G) = 1 + \sum_{i=1}^{r}(n_i - 1)$. Let p be a prime. We call G a finite abelian p-group if $|G|$ is a power of p. It seems difficult to determine $\rho(G)$ ($s(G)$) for further G, especially for the case that $r \geq 3$ and n_r is not a power of two. In this paper we prove the following.

Theorem 1.5 *Let p be a prime, and H a finite abelian p-group. Let k be a positive integer with $p^k \geq M(H)$. Set $G = H \oplus C_{p^k}$. Then,*

1. $\rho(G) \geq p^k + 2M(H) - 2$.
2. $s(G) \geq 2p^k + 2M(H) - 3$.
3. *If $p^k = M(H)$ then $4p^k - 3 \leq s(G) \leq 4p^k - 2$.*

We will show Theorem 1.5 by improving the method used in [5] and we need some preliminaries.

Let G be a finite abelian group. By λ we denote the empty sequence and adopt the convention that λ is a zero-sum sequence. $T \subset S$ means that T is a subsequence of S. By $f_E(S)$ ($f_O(S)$) we denote the number of zero-sum subsequences T of S with $2||T|$ ($2 \not| |T|$). Clearly, $f_E(S) \geq f_E(\lambda) = 1$.

Lemma 1.6 [13] *Let p be a prime, and G a finite abelian p-group. Let S be a sequence in G. Suppose that $|S| \geq M(G)$. Then, $f_E(S) \equiv f_O(S)(\ mod\ p)$.*

Lemma 1.7 *Let p be a prime, and H a finite abelian p-group. Let k be a positive integer with $p^k \geq M(H)$. Set $G = H \oplus C_{p^k}$. If S is a zero-sum sequence of $3p^k$ elements in G then S contains a zero-sum subsequence of length p^k.*

Proof. Suppose $S = (a_1, \cdots, a_{3p^k})$ with $a_i \in G$ for $i = 1, \cdots, 3p^k - 2$. Set $c_i = (1, a_i)$ with $1 \in C_{p^k}$ for $i = 1, \cdots, 3p^k - 2$. Then, $c_i \in C_{p^k} \oplus G$. Put $U = (c_1, \cdots, c_{3p^k-2})$. Note that $D(C_{p^k} \oplus G) = M(C_{p^k} \oplus G) = M(H) + p^k - 1 + p^k - 1 \leq 3p^k - 2$. Therefore, there is a nonempty zero-sum subsequence V of U. By the definition of U we have $p^k||V|$. Since $|V| \leq |U| = 3p^k - 2$, $|V| = p^k$ or $2p^k$. Let T be the subsequence of S correspond to V. Then, either T or $S \setminus T$ is a zero sum subsequence of length p^k. □

Let T be a sequence in G. By $r(T)$ we denote the number of zero-sum subsequences W of T with $|W| = 2p^k$.

Lemma 1.8 *With the same assumption on G, H, p and k as in Lemma 1.7 let T be a sequence in G with $3p^k - 2 \leq |T| \leq 4p^k - 1$. Suppose that T contains no zero-sum subsequence of length p^k. Then, $r(T) \equiv -1(\ mod\ p)$.*

Proof. Set $t = |T|$. Suppose $T = (b_1, \cdots, b_t)$. Set $c_i = (1, b_i)$ with $1 \in C_{p^k}$ for $i = 1, \cdots, t$. Then, $c_i \in C_{p^k} \oplus G$. Put $U = (c_1, \cdots, c_t)$. Let V be a zero-sum subsequence of U. We clearly have, $p^k || V|$. Since $|V| \leq |T| \leq 4p^k - 1$, $|V| = p^k, 2p^k$ or $3p^k$. Since T contains no zero-sum subsequence of length p^k, by Lemma 1.7 we get $|V| = 2p^k$. It follows from Lemma 1.6 that $r(T)+1 \equiv f_E(T) \equiv f_O(T) \equiv 0(\mod p)$. Therefore, $r(T) \equiv -1(\mod p)$. □

Let $W = (w_1, \cdots, w_r)$ and $Q = (q_1, \cdots, q_t)$ be two sequences in G, by WQ we denote the sequence $(w_1, \cdots, w_r, q_1, \cdots, q_t)$. Sometimes we also write $W = \prod_{i=1}^{r} w_i$.

Proof of Theorem 1.5. 1. Let $a_1, \cdots, a_{M(H)-1}$ be a zero-free sequence in H. Let $S = (0_H, 1)^{p^k-1} \prod_{i=1}^{M(H)-1}(a_i, 1) \prod_{i=1}^{M(H)-1}(a_i, 0)$ with $0 \in C_{p^k}, 1 \in C_{p^k}$ and 0_H is the identity of H. Then, S is a sequence in G. It is easy to check that S contains no short zero-sum subsequence. This shows that $\rho(G) \geq |S| + 1 = p^k + 2M(H) - 2$.

2. Since we have already proved that $\rho(G) \geq p^k + 2M(H) - 2$. It follows from 5. of Theorem 1.4 that $s(G) \geq 2p^k + 2M(H) - 3$.

3. By 2., $4p^k - 3 = 2p^k + 2M(H) - 3 \leq s(G)$. So, it remains to prove the upper bound. Assume to the contrary that, there is a sequence S in G with $|S| = 4p^k - 2$ and S contains no zero -sum subsequence of length p^k. By Lemma 1.8 we have

$$r(T) \equiv -1(\mod p)$$

holds for every subsequence T of S with $|T| \geq 3p^k - 2$.
We clearly have

$$\sum_{T \subset S, |T| = 3p^k - 2} r(T) = \begin{pmatrix} 4p^k - 2 - 2p^k \\ 3p^k - 2 - 2p^k \end{pmatrix} r(S).$$

Therefore,

$$\sum_{T \subset S, |T| = 3p^k - 2} (-1) \equiv \begin{pmatrix} 2p^k - 2 \\ p^k - 2 \end{pmatrix} (-1)(\mod p).$$

This gives that

$$\begin{pmatrix} 4p^k-2 \\ 3p^k-2 \end{pmatrix} \equiv \begin{pmatrix} 2p^k-2 \\ p^k-2 \end{pmatrix} (\bmod p).$$

Therefore,

$$\begin{aligned} 3 &\equiv \begin{pmatrix} 4p^k-2 \\ p^k \end{pmatrix} \equiv \begin{pmatrix} 4p^k-2 \\ 3p^k-2 \end{pmatrix} \equiv \begin{pmatrix} 2p^k-2 \\ p^k-2 \end{pmatrix} \\ &\equiv \begin{pmatrix} 2p^k-2 \\ p^k \end{pmatrix} \equiv 1 (\bmod p), \end{aligned}$$

a contradiction. Now the proof is completed. □

Corollary 1.9 *With the same assumptions as in Theorem 1.5 we have,* $2p^k + 2M(H) - 3 \leq s(G) \leq 4p^k - 2$.

Proof. Suppose $H = C_{p^{e_1}} \oplus \cdots \oplus C_{p^{e_l}}$. Then, $p^k = 1 + \sum_{i=1}^{l}(p^{e_i} - 1) + (p-1)\frac{p^k - 1 - \sum_{i=1}^{l}(p^{e_i}-1)}{p-1}$. Set $N = H \oplus C_p^{\frac{p^k-1-\sum_{i=1}^{l}(p^{e_i}-1)}{p-1}}$. Then, $p^k = M(N)$. It follows from Theorem 1.5 that $s(C_{p^k} \oplus N) \leq 4p^k - 2$. Note that the exponent of G is p^k. We have, $2p^k + 2M(H) - 3 \leq s(G) \leq s(C_{p^k} \oplus N) \leq 4p^k - 2$. □

From the proof of Corollary 1.9 we see that

Corollary 1.10 *Let p be a prime and k a positive integer. Let H be a finite abelian p-group with $M(H) \leq p^k$. Then, there is a finite abelian p-group N such that $4p^k - 3 \leq s(H \oplus N \oplus C_{p^k}) \leq 4p^k - 2$.*

Remark 1.11 *Taking $H = C_{p^k}$ in Theorem 1.5 we get 5. of Theorem 1.4. Let G be a finite abelian group of exponent m, H a subgroup of G. It is easy to see that, if the exponent of H is m or H is a direct summand of G then $s(H) \leq s(G)$. The following example shows that H is a subgroup of G is not enough to ensure that $s(H) \leq s(G)$. Note that $p^k = (p-1)\frac{p^k-1}{p-1} + 1$, let $H = C_p^{\frac{p^k-1}{p-1}}$. Then, $M(H) = p^k$. By Theorem 1.5, $4p^k - 3 \leq s(G) \leq 4p^k - 2$, where $G = C_{p^k} \oplus H$. On the other hand, it is easy to see that $s(H) \geq 2^{\frac{p^k-1}{p-1}}(p-1) + 1$ ([11], [1]). So, if $k \geq 2$ and $p \geq 3$, we have $s(H) > s(G)$.*

2 Concluding remarks and open problems

The problem to determine $s(G)$ and $\rho(G)$ remains widely open. In [1] it is suggested

Conjecture 2.1 *$s(C_n^d) \leq c^d n$ holds for some absolute constant n.*

Proposition 2.2 *If n, k are positive integers then $\rho(C_n^d) \geq n + \sum_{i=1}^{d-1}(s(C_n^i) - 1)$*

Proof. For every $1 \leq i \leq d-1$, set $s_i = s(C_n^i) - 1$, and let $(a_{i1}, \cdots, a_{is_i})$ be a sequence in C_n^i which contains no zero-sum subsequence of length n. Set $b = (\underbrace{0, \cdots, 0}_{d-1}, 1) \in C_n^d$, and set $b_{ij} = (\underbrace{0, \cdots, 0}_{d-i-1}, 1, a_{ij}) \in C_n^d$ for $j = 1, \cdots, s_i, i = 1, \cdots, d-1$. Let $S = b^{n-1} \prod_{i=1}^{d-1} \prod_{j=1}^{s_i} b_{ij}$. Then, S is a sequence in C_n^d with $|S| = n - 1 + \sum_{i=1}^{d-1}(s(C_n^i) - 1)$. We clearly have, S contains no short zero-sum subsequence. Therefore, $\rho(C_n^d) \geq 1 + |S| = n + \sum_{i=1}^{d-1}(s(C_n^i) - 1)$. □

From Proposition 2.2 we see that, Conjecture 2.1 is equivalent to

Conjecture 2.3 *$\rho(C_n^d) \leq c^d n$ holds for some absolute constant c.*

Let p be a prime, we can regard C_p^d as a vector space over F_p, the p-element field. For every $1 \leq k \leq d$, by $l(p, d, k)$ we denote the smallest integer t such that every subset A of C_p^d with $|A| \geq t$ contains some k distinct elements which are linearly dependent.

Proposition 2.4 *$s(C_3^d) \leq 2l(3, d+1, 3) - 1$.*

Proof. By $g(C_3^d)$ we denote the smallest integer t such that, every subset B of C_3^d with $|B| \geq t$ contains three distinct elements with zero-sum. It is proved that $s(C_3^d) = 2g(C_3^d) - 1$ in [12]. Let C be a subset of C_3^d such that $|C| = g(C_3^d) - 1$ and such that C contains no three distinct elements with sum zero. Suppose $C = (c_1, \cdots, c_r)$, where $r = g(C_3^d) - 1$. Set $a_i = (1, c_i)$ with $1 \in C_3$ for $i = 1, \cdots, r$. Set $A = (a_1, \cdots, a_r)$. We assert that

A contains no three distinct elements which are linearly dependent.

Assume to the contrary that A contains three distinct elements which are linearly dependent. With rearranging the subscripts we may assume that a_1, a_2, a_3 are linearly dependent. That is, there are three elements $f_1, f_2, f_3 \in F_3$ such that $f_1a_1+f_2a_2+f_3a_3 = 0 \in C_3^{d+1}$ and at least one of f_1, f_2, f_3 is not zero. By the definition of a_i we infer that $f_1 + f_2 + f_3 = 0$. Therefore, $\{f_1, f_2, f_3\} = \{0, 1, -1\}$ or $f_1 = f_2 = f_3 \neq 0$. If $\{f_1, f_2, f_3\} = \{0, 1, -1\}$, we infer that $c_1 = c_2$, or $c_1 = c_3$, or $c_2 = c_3$, a contradiction. If $f_1 = f_2 = f_3 \neq 0$, we derive that $c_1 + c_2 + c_3 = 0$, also a contradiction. This proves the assertion. Thus, $g(C_3^d) - 1 = r < l(3, d+1, 3)$. Hence, $g(C_3^d) \leq l(3, d+1, 3)$. Therefore, $s(C_3^d) = 2g(C_3^d) - 1 \leq 2l(3, d+1, 3) - 1$. □

Proposition 2.4 suggests that

Conjecture 2.5 $s(C_3^d) < 2^{d+3}$.

Conjecture 2.6 [7] *Let G be a finite abelian group of exponent m. Then, $s(G) = \rho(G) + m - 1$.*

Although several authors (see [1], [5], [6], [14]) have made considerable progress on the following conjecture, it remains open in general,

Conjecture 2.7 [12] $s(C_m^2) = 4m-3$ *holds for every positive integer m.*

Acknowledgements The authors would like to thank the referees for several very helpful comments and suggestions.

References

[1] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size*, in "Combinatorics, Paul Erdös is eighty, Vol.1, Keszthely," pp.33-50, Bolyai Soc.Math.Stud., Janos Bolyai Math. Soc., Budapest, 1993.

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

[3] P. van Emde Boas, *A combinatorial problem on finite abelain groups II*, Math. Centre report ZW-1969-007, Amsterdam.

[4] P. Erdös, A. Ginzburg and A. Ziv, *A theorem in the additive number theory*, Bull. Res. Council. Israel, 10F(1961), 41-43.

[5] W. D. Gao, *Note on a zero-sum problem* , J. Combinatorial Theory, Series A, 95(2001), 387-389.

[6] W. D. Gao, *On zero-sum subsequences of restricted size*, J. Number Theory, 61(1996), 97-102.

[7] W. D. Gao, *On zero-sum subsequences of restricted size, II*, Discrete Mathematics, 271(2003), 51-59.

[8] W. D. Gao, *Some problems in additive number theory and additive group theory*, Ph. D. thesis, Sichuan Univ., 1994.

[9] W. D. Gao and Alfred Geroldinger, *Half factorial domains and half-factorial subsets in abelian groups*, Houston J. Math., 24(1998), 593-611.

[10] W. D. Gao and Y. X. Yang, *Note on a combinatorial constant*, J. Math. Res. and Expo., 17(1997), 139-140.

[11] H. Harborth, *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math., 262/263 (1973), 356-360.

[12] A. Kemnitz, *On a lattice point problem*, Ars Combin., 16b(1983), 151-160.

[13] J. E. Olson, *A combinatorial problem on finite abelian groups I*, J. Number theory, 1(1969), 8-11.

[14] L. Rónyai, *On a conjecture of Kemnitz*, Combinatorica, 20(2000), 569-573.