ZERO SUMS IN FINITE CYCLIC GROUPS

W. D. Gao[1]
Department of Computer Science and Technology, University of Petroleum, Beijing, China, 102200.

Received: 12/12/99, Accepted: 10/31/00, Published: 11/6/00

Abstract

Let C_n be the cyclic group of n elements, and let $S = (a_1, \cdots, a_k)$ be a sequence of elements in C_n. We say that S is a *zero sequence* if $\sum_{i=1}^{k} a_i = 0$ and that S is a *minimal zero-sequence* if S is a zero sequence and S contains no proper zero subsequence. In this paper we prove, among other results, that if S is a minimal zero sequence of elements in C_n and $|S| \geq n - [\frac{n+1}{3}] + 1$, then there exists an integer m coprime to n such that $|ma_1| + \cdots + |ma_k| = n$, where $|x|$ denotes the least positive inverse image under the natural homomorphism from the additive group of integers Z onto C_n. On the other hand, we give some explicit minimal zero sequences of length $[\frac{n+1}{2}] + 1$ not having this property above.

1. Introduction

Let G be a finite abelian group. Let $S = (a_1, \cdots, a_k)$ be a sequence of elements in G. By $\sigma(S)$ we denote the sum $\sum_{i=1}^{k} a_i$. We say that S is a *zero sequence* if $\sigma(S) = 0$, that S is a *zero-free sequence* if S contains no nonempty zero subsequence, and that S is a *minimal zero sequence* if S is a zero sequence and S contains no proper zero subsequence. By $\sum(S)$ we denote the set consisting of all elements which can be expressed as a sum over a nonempty subsequence of S, i.e.

$$\sum(S) = \{\sigma(T) | T \text{ is a nonempty subsequence of } S\}$$

Sometimes we also write $S = \prod_{i=1}^{k} a_i$. If T is a subsequence of S, by ST^{-1} we denote the subsequence W such that $WT = S$. We say subsequences $S_1, \cdots, S_r$ of S are disjoint if $S_1 \cdots S_r$ is a subsequence of S. For every $g \in G$, we use $v_g(S)$ to denote the number of the times that g occurs in S.

Let C_n be the cyclic group of order n. For every $x \in C_n$, we define $|x|$ to be the least positive inverse image under the natural homomorphism from the additive group of integers Z onto C_n. For example, $|0| = n$. Let $S = (a_1, \cdots, a_k)$ be a sequence of elements in C_n, by $|S|_n$ we denote the sum $\sum_{i=1}^{k} |a_i|$. Define

$$Index(S) = \min_{(m,n)=1} \{|mS|_n\}$$

[1]This work has been supported partly by the National Natural Science Foundation of China and the Foundation of Education Committee of China.

$Index(C_n)$ was first introduced by Chapman, Freeze, and Smith in [2]. It is well known that if S is a minimal zero sequence of n elements in C_n, then $S = (\underbrace{a, \cdots, a}_{n})$ for some a generating C_n. Hence, $Index(S) = n$. From a result of ([3], Lemma 2) we can easily derive that every minimal zero sequence S of elements in C_n with $|S| \geq n - [n/4]$ satisfies $Index(S) = n$. In Section 2 of this paper, we prove that the last conclusion holds for the restriction of $|S| \geq n - [n/4]$ replaced by $|S| \geq n - [n/3] + 1$; In Sectoin 3 we study the sums of divisors of a positive integer n; the final section 4 contains some conculding remarks.

2. On $Index(S)$

Definition. Let $l(C_n)$ be the minimal integer t such that every minimal sequence S of at least t elements in C_n satisfies $Index(S) = n$.

Theorem 2.1 *(1).* $[\frac{n+1}{2}] + 1 \leq l(C_n) \leq n - [\frac{n+1}{3}] + 1$ *holds for all* $n \geq 8$.
(2). $l(C_n) = 1$ *for* $n = 1, 2, 3, 4, 5, 7$ *and* $l(C_6) = 5$.

Lemma 2.2 *([1]) Let* $n - 2k \geq 1$, *and let* $S = (a_1, \cdots, a_{n-k})$ *be a zero-free sequence of* $n - k$ *elements in* C_n. *Then there is an element* $g \in C_n$ *such that* $v_g(S) \geq n - 2k + 1$.

Lemma 2.3 *([4]) Let* S *be a zero-free sequence of elements in* C_n, *and let* $g \in C_n$ *with* $order(g) = n/m$. *Suppose that* $|S| > n/2$. *Then* $v_g(S) < \frac{n-|S|}{m-1}$.

Lemma 2.4 *([4]) Let* S *be a zero-free sequence of elements in an abelian group, and let* $S_1, \cdots, S_k$ *be disjoint subsequences of* S. *Then,* $|\sum(S)| \geq \sum_{i=1}^{k} |\sum(S_i)|$.

Let $S = (a_1, \cdots, a_k)$ and $T = (b_1, \cdots, b_k)$ be two sequences of elements in C_n with the same length. We say S is *similiar* to T if there exists an integer m coprime to n and a permutation δ of $\{1, \cdots, k\}$ such that $a_i = mb_{\delta(i)}$ for $i = 1, \cdots, k$. Denote it by $S \sim T$.

Lemma 2.5 *Let* $1 \leq k \leq [\frac{n+1}{3}]$, *and let* S *be a zero-free sequence of* $n - k$ *elements in* C_n. *Then*

$$S \sim (\underbrace{1, \cdots, 1}_{n-2k+1}, x_1, \cdots, x_{k-1})$$

with $\sum_{i=1}^{k-1} |x_i| \leq 2k - 2$. *Therefore,* $Index(S) < n$.

Proof. By Lemma 2.2, there is an element $g \in C_n$ such that $v_g(S) \geq n - 2k + 1 \geq k = n - |S|$. It follows from Lemma 2.3 that $order(g) = n$. Without loss of generality, we may assume that

$g = 1$. Set $l = v_g(S)$. Suppose $S = 1^l \prod_{i=1}^{t} a_i$, where $l + t = |S|$. Since S is zero-free, we clearly have

$$1 \le |a_i| \le n - l - 1 \text{ for } i = 1, \cdots, t. \tag{1}$$

If $|a_t| \ge l+1$, then $|\sum(1^l a_t)| = 2l+1$. By Lemma 2.4, $n-1 \ge |\sum(S)| \ge |\sum(1^l a_t)| + t - 1 \ge 2l + t = n - k + l \ge n - k + n - 2k + 1 \ge n$, a contradiction. Hence,

$$1 \le |a_i| \le l \text{ for } i = 1, \cdots, t \tag{2}$$

Since S is zero-free, $1 \le |a_1 + a_2| \le n - l - 1$. By (1) and (2), $|a_1| + |a_2| \le n - 1$. Therefore, $|a_1| + |a_2| = |a_1 + a_2| \le n - l - 1$. Similarly, one can get $|a_1| + |a_2| + |a_3| = |a_1 + a_2| + |a_3| = |a_1 + a_2 + a_3| \le n - l - 1$. Finally, we must get $\sum_{i=1}^{t} |a_i| = |\sum_{i=1}^{t} a_i| \le n - l - 1$. Therefore, $Index(S) \le n - 1$. □

Proof of Theorem 2.1. (1). We first prove the upper bounds. Let S be a minimal zero sequence of elements in C_n with $|S| \ge n - [\frac{n+1}{3}] + 1$. Take an arbitrary element x from S. Then Sx^{-1} is zero-free. By Lemma 2.5, $Index(S) \le Index(Sx^{-1}) + n - 1 \le n - 1 + n - 1 < 2n$. Hence, $Index(S) = n$.

To prove the lower bounds we distinguish four cases.

Case 1. n is odd. Set $S = (\underbrace{1, \cdots, 1}_{\frac{n-5}{2}}, \frac{n+3}{2}, \frac{n+3}{2}, \frac{n-1}{2})$. Note that for $n \ge 9$, clearly $Index(S) = 2n$. Therefore, $\frac{n+1}{2} + 1 \le l(C_n)$.

Case 2. n is even and $n \ge 12$. Set

$S = (\underbrace{1, \cdots, 1}_{\frac{n-6}{2}}, \frac{n+4}{2}, \frac{n+4}{2}, \frac{n-2}{2})$. Clearly $Index(S) = 2n$. Therefore, $[\frac{n+1}{2}] + 1 \le l(C_n)$.

Case 3. $n = 8$, set $S = (1, 4, 5, 6)$. It is easy to check that S is a minimal zero sequence and that $Index(S) = 16$. Therefore $[9/2] + 1 = 4 + 1 \le l(C_8)$.

Case 4. $n = 10$, set $S = (1, 5, 8, 3, 3)$. It is easy to check that S is a minimal zero sequence and that $Index(S) = 20$. Therefore $[11/2] + 1 = 5 + 1 \le l(C_{10})$.

(2). It is proved in [2] that $l(C_n) = 1$ for $n = 1, 2, 3, 5, 7$. For $n = 4$, it is easy to see that $l(C_4) = 1$. For $n = 6$, by Lemma 2.5, we clearly have $l(C_6) \le 5$. For $S = (1, 3, 4, 4)$ it is clear that $Index(S) = 12$. Therefore $l(C_6) = 5$. □

Let S be a zero-free (resp. minimal zero) sequence of elements in an abelian group G. We say S is *splitable* if there exists an element $a \in S$ and two elements $x, y \in G$ such that $x + y = a$ and such that $Sa^{-1}xy$ is zero-free (resp. minimal zero) sequence as well.

Proposition 2.6 *Let S be a minimal zero subsequence with $|S| = l(C_n) - 1$. Suppose that $Index(S) > n$. Then S is not splitable.*

Proof. Assume to the contrary that S is splitable. Then there exist $a \in S$ and $x, y \in C_n$ such that $Sa^{-1}xy$ is also a minimal zero squenece. Since, $|Sa^{-1}xy| = l(C_n)$, by the definition of $l(C_n)$, $Index(Sa^{-1}xy) = n$. Therefore, $Index(S) \leq Index(Sa^{-1}xy) = n$, a contradiction. This proves the proposition. □

Conjecture 2.7 *Let S be a minimal zero subsequence with $|S| = l(C_n) - 1$. Suppose that S is not splitable. Then $Index(S) = 2n$.*

This conjecture, if true, would be useful for determining $l(C_n)$.

Theorem 2.8 *Let G be a finite abelian group and let $G = C_{n_1} \oplus \cdots \oplus C_{n_k}$ be a decomposition of G into direct summands, where all $n_i > 1$. Let $C_{n_i} = \langle e_i \rangle$ for $i = 1, \cdots, k$. Then the sequence $S = (e_1 + \cdots + e_k) \prod_{i=1}^{k} e_i^{n_i - 1}$ is not splitable.*

Proof. Clear. □

Conjecture 2.9 *Let $G = C_{n_1} \oplus \cdots \oplus C_{n_k}$ be a finite non-cyclic abelian group with $1 < n_1 | \cdots | n_k$, and let S be a minimal zero sequence of elements in G. Suppose that $\langle S \rangle = G$ and suppose that S is not splitable. Then S contains at least $k+1$ distinct elements.*

Definition. Let $sp(G)$ be the largest integer t such that every minimal zero sequence of elements in G with $|S| \leq t$ is splitable.

Problem. Determine $sp(G)$.

We clearly have, $\log_2(\frac{|G|}{2}) \leq sp(G) \leq l(G) - 1$.

Conjecture 2.10 *$sp(G) \leq c \ln |G|$ for some absolute constant c.*

Define

$$I(C_n) = \max_S \{Index(S)\},$$

where S runs over all minimal zero sequences of elements in C_n.

Proposition 2.11 *$I(C_n) \geq \frac{n+1}{2}(1 + [\log_3(\frac{n}{3})]) + 1$.*

Lemma 2.12 *If a is an element in C_n, then $|ma| + |m(n - 2a)| > n/2$ holds for every integer m coprime to n.*

Proof. If $|ma| > n/2$ then we are done. Otherwise, $|ma| < n/2$, then

$$|ma| + |m(n-2a)| = |ma| + n - 2|na| = n - |ma| > n/2. \qquad \square$$

Proof of Proposition 2.11. Let $t = [\log_3(\frac{n}{3})]$, set $T = (1, 3, 3^2, \cdots, 3^t, n-2, n-6, n-18, \cdots, n-2\times 3^t) = \prod_{i=0}^{t}(3^i, n-2\times 3^i)$. Since $3^{i+1} > 2\sum_{j=1}^{i} 3^i$ for $i = 0, \cdots, t-1$ and $2\sum_{i=1}^{t} 3^i = 3^{t+1}-1 < n$, T is zero-free. Let m be the positive integer coprime to n such that $Index(T) = |mT|$. By Lemma 2.12, $Index(T) = |mT| = \sum_{i=0}^{t}(|m3^i|+|m(n-2\times 3^i)| \geq \frac{n+1}{2}(t+1)$. Set $S = T\cdot(-\sigma(T))$. Then S is a minimal zero sequence with $Index(S) \geq Index(T) + 1 \geq \frac{n+1}{2}(t+1) + 1$. $\square$

3. Sums of Divisors of n

In [5], Lemke and Kleitman proved, among other results, that if $S = (a_1, \cdots, a_n)$ is a sequence of positive integer and $a_i|n$ holds for every $i = 1, \cdots, n$ then there is a subsequence T of S with $\sigma(T) = n$. Here we shall show a generaliztion of this result.

Theorem 3.1 *Let $S = (a_1, \cdots, a_k, b_1, \cdots, b_{n-k})$ be a sequence of n positive integers. Suppose that $a_i|n$ for $i = 1, \cdots, k$, and suppose that all of b_i are distinct and $b_i \leq n$ for $i = 1, \cdots, n-k$. Then, there is a subsequence T of S with $\sigma(T) = n$.*

Lemma 3.2 *Let A be a subset of $[0, n]$, and $B \setminus \{0\}$ a set of positive divisors of n. Suppose that $0 \in A \cap B$ and suppose that $n \notin A + B$. Then, $|(A + B) \cap [0, n]| \geq |A| + |B| - 1$, where $[0, n] = \{0, 1, 2, \cdots, n-1, n\}$.*

Proof. We proceed by induction on $|B|$. $|B| = 1$ implies $B = \{0\}$ and the lemma is trivial. Assume that the lemma is true for $|B| < k$ $(k \geq 2)$, we want to prove it is true also for $|B| = k$. Take an arbitrary $b \in B \setminus \{0\}$. Then $b|n$. Since $n \notin A + B$, $(\frac{n}{b} - 1)b \notin A$. Let r be the least nonnegative integer such that $rb \notin A$. Then $1 \leq r < \frac{n}{b}$. Therefore $(r-1)b \in A$ but $b + (r-1)b \notin A$. Set $a = (r-1)b$. Set $B_0 = \{b' \in B | a + b' \notin A \text{ and } a + b' < n\}$. Then $B_0 \neq \emptyset$. Now set $A_1 = A \cup (a + B_0)$ and set $B_1 = B \setminus B_0$. Clearly, $(A_1 + B_1) \cap [0, n] \subset (A + B) \cap [0, n]$. Note that $|B_1| < k$. By the inductive assumption we have $|(A + B) \cap [0, n]| \geq |(A_1 + B_1) \cap [0, n]| \geq |A_1| + |B_1| - 1 = |A| + |B| - 1$. $\square$

Proof of Theorem 3.1. Set $A_0 = \{0, b_1, \cdots, b_{n-k}\}$ and set $A_i = \{0, a_i\}$ for $i = 1, \cdots, k$. Assume to the contrary that $n \notin \sum(S)$. By Lemma 3.2 we have, $|(A_0 + A_1) \cap [1, n]| = |(A_0 + A_1) \cap [0, n]| - 1 \geq |A_0| + |A_1| - 2$. Similiarly, one can get $|(A_0 + A_1 + A_2) \cap [1, n] \geq |(A_0 + A_1) \cap [0, n]| + |A_2| - 1 \geq |A_0| + |A_1| + |A_2| - 3$, and finally, we must get $|(A_0 + A_1 + A_2 + \cdots + A_k) \cap [1, n]| \geq |A_0| + |A_1| + \cdots + |A_k| - k - 1 = |S| = n$, a contradiction on $n \notin \sum(S)$. $\square$

Kleitman and Lemke [5] suggested that

Conjecture 3.3 *Every sequence of n elements in C_n contains a nonempty subsequence T such that $Index(T) = n$.*

They pointed out that this conjecture is open even for n prime.

Conjecture 3.4 *Let $S = (a_1, \cdots, a_k)$ be a sequence of elements in C_n. Suppose that S contains no subsequence T with $Index(T) = n$. Then, $|\{\sigma(T)|\lambda \neq T \subset S$ and $Index(T) < n\}| \geq k$, where λ denotes the empty sequence.*

This conjecture, if true, would clearly imply Conjecture 2.4.

4. Concluding Remarks

Let $S = (a_1, \cdots, a_k)$ be a sequence of elements in C_n. For a positive integer l, we say S is a *partition* of l if $\sum_{i=1}^{k} |a_i| = l$. By the definition of $Index(S)$ we have that every sequence S of elements in C_n is similiar to a partition of $Index(S)$. By the definition of $I(C_n)$ we have that every minimal zero sequence of elements in C_n is similiar to a partition of ln for some $l \leq I(C_n)/n$. Hence, if $Index(S) > I(C_n)$, then S contains a proper zero subsequence. From Theorem 1.1 we see that every minimal zero sequence of at least $n - [\frac{n+1}{3}] + 1$ elements in C_n is similiar to a partition of n. For every positive integer $k \leq n - 1$, we define

$$I_k(C_n) = \max_{|T|=k}\{Index(T)\},$$

where T runs over all zero-free sequences of k elements in C_n.

Proposition 4.1 *(1). If p is the smallest positive divisor of n then $I_1(C_n) = n/p$.*
(2). If $n \geq 3$ is a prime then $I_2(C_n) = \frac{n+1}{2}$.

Proof. (1). Clear.

(2). By Lemma 1.12, $I_2(C_n) \geq \frac{n+1}{2}$. To prove the upper bound, let x, y be two nonzero elements (not necessarily distinct) with $x + y \neq 0$. Set $z = -x - y$. Then (x, y, z) is a minimal zero sequence. Let t be the positive intger such that $tz = \frac{p+1}{2}$ and $1 \leq t \leq p - 1$. Then $(p-t)z = \frac{p-1}{2}$. Since $|tx|+|ty|+|tz|+|(p-t)x|+|(p-t)y|+|(p-t)z| = 3p$, $|tx|+|ty|+|tz| = p$ or $|(p-t)x|+|(p-t)y|+|(p-t)z| = p$. Therefore, $|ty|+|tz| = \frac{p-1}{2}$ or $|(p-t)x|+|(p-t)y| = \frac{p+1}{2}$.
□

Conjecture 4.2 $I(C_n) \leq c \ln n$ *for some absolute constant c.*

References

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

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

[3] W. D. Gao, *An addition theorem for finite cyclic groups,* Discrete Math., 163(1997), 257-265.

[4] W. D. Gao and A. Geroldinger, *On the structure of zero-free sequences*, Combinatoria, 18(1998), 519-527.

[5] D. J. Kleitman and P. Lemke, *An addition theorem on the integers modulo n,* J.Number Theory, 31(1989), 335-345.