COLLOQUIUM MATHEMATICUM

VOL. 98 2003 NO. 2

ON THE STRUCTURE OF SEQUENCES WITH FORBIDDEN ZERO-SUM SUBSEQUENCES

BY

W. D. GAO (Beijing) and R. THANGADURAI (Allahabad)

Abstract. We study the structure of longest sequences in $\mathbb{Z}_n^d$ which have no zero-sum subsequence of length n (or less). We prove, among other results, that for $n = 2^a$ and d arbitrary, or $n = 3^a$ and $d = 3$, every sequence of $c(n,d)(n-1)$ elements in $\mathbb{Z}_n^d$ which has no zero-sum subsequence of length n consists of $c(n,d)$ distinct elements each appearing $n-1$ times, where $c(2^a,d) = 2^d$ and $c(3^a,3) = 9$.

1. Introduction. Many authors have studied the structure of sequences which have no zero-sum subsequences of prescribed lengths. The motivation for this study stems from problems in non-unique factorization theory. See, for example, [9], [13], [14].

Let H be a finite abelian group (written additively). Then $H = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_d}$ with $1 < n_1 \mid n_2 \mid \ldots \mid n_d$, where $n_d = \exp(H) =: n$ is the *exponent* of H and where d is the *rank* of H. When $n_1 = n_2 = \ldots = n_d = n$, we denote H by $\mathbb{Z}_n^d$.

By a *sequence* $S = \{g_i\}$ in H of *length* l, we mean a multi-set S whose elements are from H and the cardinality of S with multiplicity is l. We also denote l by $|S|$. For convenience, we write any sequence S in H of length l as $S = \prod_{i=1}^{l} g_i$. Also, $v_g(S)$ denotes the number of times g appears in S. Let $\sigma(S) = \sum_{i=1}^{l} g_i$.

We say that the sequence $S = \prod_{i=1}^{l} g_i$ in H is a

- *zero-sum sequence* if $\sigma(S) = 0$ in H,
- *short zero-sum sequence* if $\sigma(S) = 0$ and $1 \le |S| \le \exp(H) = n$.

Definition 1.1. A pair (n,d) of positive integers is said to have *Property* D if $(n-1) \mid (s(\mathbb{Z}_n^d) - 1)$ and every sequence S in $\mathbb{Z}_n^d$ of length $s(\mathbb{Z}_n^d) - 1$ having no zero-sum subsequence of length n is of the form $\prod_{i=1}^{c} a_i^{n-1}$, where $c = (s(\mathbb{Z}_n^d) - 1)/(n-1)$ and $s(\mathbb{Z}_n^d)$ denotes the smallest positive integer t such that every sequence T in $\mathbb{Z}_n^d$ with $|T| = t$ has a zero-sum subsequence of length n.

2000 *Mathematics Subject Classification*: Primary 11B75; Secondary 20K99.

Key words and phrases: structure of sequences, zero-sum problems, finite abelian groups.

The constant $s(\mathbb{Z}_n^d)$ was first introduced by Harborth [16] in 1973. Using the pigeonhole principle, he proved that

$$2^d(n-1)+1 \le s(\mathbb{Z}_n^d) \le n^d(n-1)+1$$

and

$$s(\mathbb{Z}_{mn}^d) \le \min\{s(\mathbb{Z}_n^d)+n(s(\mathbb{Z}_m^d)-1), s(\mathbb{Z}_m^d)+m(s(\mathbb{Z}_n^d)-1)\}. \tag{1}$$

It follows that

$$s(\mathbb{Z}_{2^l}^d) = 2^d(2^l-1)+1 \tag{2}$$

for every integer $l \ge 1$. But it is known that $s(\mathbb{Z}_3^3) = 19 = 9(3-1)+1$ (see [16]), which is greater than the above lower bound. Recently, C. Elsholtz [4] proved that for every odd integer $n \ge 3$, we have

$$s(\mathbb{Z}_n^d) \ge (1.125)^{\lfloor d/3 \rfloor} 2^d(n-1)+1. \tag{3}$$

In particular, $s(\mathbb{Z}_n^3) \ge 9(n-1)+1$ for every odd integer $n \ge 3$. In 1995, Alon and Dubiner [1] proved that

$$s(\mathbb{Z}_n^d) \le (c(d) d \log_2 d)^d n,$$

where $c(d)$ is an absolute constant.

For every integer $n \ge 2$, the pair $(n, 1)$ has Property D; this follows from the theorems of Erdős, Ginzburg and Ziv [5] (which says that $s(\mathbb{Z}_n) = 2n-1$) and Peterson and Yuster [19] (and also Bialostocki and Dierker [3] independently) (which says that any sequence T of $\mathbb{Z}_n$ of length $2n-2$ having no zero-sum subsequences of length n is of the form $a^{n-1}b^{n-1}$ for some $a, b \in \mathbb{Z}_n$).

The following two conjectures imply that for any integer $n \ge 2$, the pair $(n, 2)$ has Property D.

Conjecture 1.1 (Kemnitz, 1983, [17]). *For every integer $n \ge 2$, we have $s(\mathbb{Z}_n^2) = 4n-3$.*

Conjecture 1.2 (W. D. Gao, 2000, [8]). *Let S be a sequence in $\mathbb{Z}_n^2$ of length $4n-4$. If S does not have a zero-sum subsequence of length n, then S is of the form $a^{n-1}b^{n-1}u^{n-1}v^{n-1}$ for some distinct $a, b, u, v \in \mathbb{Z}_n^2$.*

Conjecture 1.1 has been proved for prime $n \le 7$. It is also known that it is "multiplicative". The best known result on Conjecture 1.1 is due to W. D. Gao [11]: For every prime p and every integer $k \ge 1$, we have $s(\mathbb{Z}_{p^k}^2) \le 4p^k - 2$. There are many further partial results (see, for example, [2], [6], [7], [17], [20], [21]–[23]).

Gao [8] proved that Conjecture 1.2 is "multiplicative". Also, he verified Conjecture 1.2 for $n = 2, 3$ and 5. Recently, Sury and Thangadurai [21] verified it for $n = 7$.

Thus, for any integer n of the form $n = 2^a 3^b 5^u 7^v$ where $a, b, u, v \geq 0$, we know that, unconditionally, the pair $(n, 2)$ has Property D.

Definition 1.1 is just a generalization of the definition given in [15] for the group $\mathbb{Z}_n^2$; so is the following definition:

DEFINITION 1.2. A pair (n, d) of positive integers is said to have *Property* C if $(n-1) \mid (\varrho(\mathbb{Z}_n^d) - 1)$ and every sequence S in $\mathbb{Z}_n^d$ of length $\varrho(\mathbb{Z}_n^d) - 1$ having no short zero-sum subsequences is of the form $\prod_{i=1}^{b} a_i^{n-1}$, where $b = (\varrho(\mathbb{Z}_n^d) - 1)/(n-1)$ and $\varrho(\mathbb{Z}_n^d)$ denotes the smallest positive integer t such that every sequence T in $\mathbb{Z}_n^d$ with $|T| = t$ has a non-empty short zero-sum subsequence.

It is trivial that $\varrho(\mathbb{Z}_n) = n$. Also, if S is a sequence in $\mathbb{Z}_n$ of length $n-1$ with no proper zero-sum subsequence, then $S = a^{n-1}$ for some $a \in \mathbb{Z}_n$. Thus, for any integer $n \geq 2$, the pair $(n, 1)$ has Property C. The constant $\varrho(H)$ was first studied by Olson [18] and van Emde Boas [25] for $H = \mathbb{Z}_n^2$; they proved (independently) that $\varrho(\mathbb{Z}_n^2) = 3n - 2$ and van Emde Boas conjectured the following.

CONJECTURE 1.3 (van Emde Boas, 1969, [25]). *Let S be a sequence in $\mathbb{Z}_n^d$ of length $3n-3$. Suppose S does not have a short zero-sum subsequence. Then $S = a^{n-1}u^{n-1}v^{n-1}$ for some $a, u, v \in \mathbb{Z}_n^2$.*

This conjecture has been verified by van Emde Boas [25] for any prime $n \leq 7$. Moreover, Gao [8] proved that Conjecture 1.3 is "multiplicative". Thus, it is true for all integers n of the form $2^a 3^u 5^v 7^w$.

Clearly, from the above discussion the pairs $(n, 1)$ and $(2^a 3^u 5^v 7^w, 2)$ have Property C.

Similarly to the definition of $s(\mathbb{Z}_n^d)$ and $\varrho(\mathbb{Z}_n^d)$ we can analogously define $s(H)$ and $\varrho(H)$ for any finite abelian group H. Also, one can easily prove that $\varrho(H) \leq s(H) - n + 1$. When $H = \mathbb{Z}_n$, we know from the above results that $\varrho(H) = s(H) - n + 1$. By Conjecture 1.1 and by the value of $\varrho(\mathbb{Z}_n^2)$, we see that this equality also holds for $H = \mathbb{Z}_n^2$. Gao suggested the following conjecture.

CONJECTURE 1.4 (W. D. Gao, 2002, [12]). *If H is a finite abelian group of exponent n, then $s(H) = \varrho(H) + n - 1$.*

Gao [12] verified Conjecture 1.4 for all groups H with exponent $n \leq 4$. More precisely, he proved the following: Let S be a sequence in H of length $\varrho(H) + n - 1$. Suppose there exists $g \in H$ such that $v_g(S) \geq n - [n/2] - 1$. Then S has a zero-sum subsequence of length n.

OPEN PROBLEM 1. Does every pair (n, d) of positive integers have Property C and Property D?

The main result of this paper gives a partial answer to this problem and we study the relationship between the two properties. We prove the following theorems.

THEOREM 1. *Suppose that the pair* (n, d) *of positive integers has Property* D. *If* $s(\mathbb{Z}_{n^r}^d) = c(n^r - 1) + 1$ *for every* r (*where* c *is a constant depending only on* n *and* d), *then the pair* (n^r, d) *has Property* D *for every positive integer* r.

COROLLARY 1.1. *The pairs* $(2^a, d), (3^a, 3)$ *and* $(3, d)$ *have Property* D *for any positive integers* a *and* d.

COROLLARY 1.2. *If a pair* (n, d) *has Property* D, *then* (i) $s(\mathbb{Z}_n^d) = \varrho(\mathbb{Z}_n^d) + n - 1$ *and* (ii) (n, d) *has Property* C *and hence the pairs* $(2^a, d)$, $(3^a, 3)$ *and* $(3, d)$ *have Property* C.

THEOREM 2. *Suppose there exists a sequence* S *in* $\mathbb{Z}_n^d$ *of length* $s(\mathbb{Z}_n^d) - 1$ *such that* $v_g(S) > [(n-3)/2]$ *for some* $g \in \mathbb{Z}_n^d$ *and* S *does not have a zero-sum subsequence of length* n. *If the pair* (n, d) *has Property* C, *then* (i) $s(\mathbb{Z}_n^d) = \varrho(\mathbb{Z}_n^d) + n - 1$ *and* (ii) $S = \prod_{i=1}^{c} a_i^{n-1}$, *where* $c = (s(\mathbb{Z}_n^d) - 1)/(n-1)$.

2. Proofs of Theorems

Proof of Theorem 1. We proceed by induction on r. The case $r = 1$ is just the hypothesis of the theorem.

Suppose that the assertion is true for $r - 1$. We want to prove that it is also true for r. Set $m = n^{r-1}$. Let $S = \prod_{i=1}^{c(nm-1)} a_i$ be a sequence of length $c(nm - 1)$ in $\mathbb{Z}_{nm}^d$ such that S contains no zero-sum subsequence of length nm. We have to prove that $S = \prod_{i=1}^{c} a_i^{nm-1}$ (say).

Let

$$\phi : \mathbb{Z}_{nm}^d \to \mathbb{Z}_n^d$$

be the natural homomorphism with $\ker \phi = \mathbb{Z}_m^d$. Since $s(\mathbb{Z}_n^d) = c(n-1) + 1$ by assumption and $c(nm-1) = (c(m-1))n + c(n-1)$, one can find $c(m-1)$ disjoint zero-sum subsequences $S_1, \ldots, S_{c(m-1)}$ such that $|S_1| = \ldots = |S_{c(m-1)}| = n$ and $\sigma(\phi(S_1)) = \ldots = \sigma(\phi(S_{c(m-1)})) = 0$. Therefore, $\sigma(S_i) \in \ker\phi = \mathbb{Z}_m^d$ for $i = 1, \ldots, c(m-1)$. Since S contains no zero-sum subsequence of length nm and $s(\mathbb{Z}_{nm}^d) = c(nm-1) + 1$, the sequence $\phi(S(S_1 \ldots S_{c(m-1)})^{-1})$ contains no zero-sum subsequence of length n. As the pair (n, d) has Property D, we have $\phi(S(S_1 \ldots S_{c(m-1)})^{-1}) = \prod_{i=1}^{c} b_i^{n-1}$, where b_i's are pairwise distinct. Therefore, $\phi(S)$ contains at least c distinct elements.

CLAIM 1. *$\phi(S)$ contains exactly c distinct elements.*

Assume that, on the contrary, $\phi(S)$ contains $k > c$ distinct elements. Suppose $\phi(S) = \prod_{i=1}^{k} h_i^{t_i}$ with $t_1, \dots, t_k \geq 1$ and $t_1 + \dots + t_k = c(nm-1)$. Let $T_i = \prod_{\phi(a_j)=h_i} a_j$. Then $S = T_1 \dots T_k$. Now we distinguish two cases.

CASE 1: $n \mid t_i$ for some $1 \leq i \leq k$. Without loss of generality we assume that $i = 1$. We divide T_1 into k_1/n disjoint subsequences $W_1, \dots, W_{k_1/n}$ each having length n. By applying $s(\mathbb{Z}_n^d) = c(n-1)+1$ repeatedly, one can find $c(m-1) - k_1/n$ disjoint subsequences of ST_1^{-1}, namely, $W_{k_1/n+1}, \dots,$ $W_{c(m-1)}$ each having length n and each having sum in $\mathbb{Z}_m^d$. As above, one can derive that $\phi(S(W_1 \dots W_{c(m-1)})^{-1}) = \prod_{i=1}^{c} b_i^{n-1}$, where b_i's are pairwise distinct. Set $W = S(W_1 \dots W_{c(m-1)})^{-1}$. Then $\phi(W_1 W) = b^n \prod_{i=1}^{c} b_i^{n-1}$. Let U_1 be a zero-sum subsequence of $b^{n-1} \prod_{i=1}^{c} b_i^{n-1}$ of length n. Then $(b^{n-1} \prod_{i=1}^{c} b_i^{n-1}) U_1^{-1}$ contains exactly $c+1$ distinct elements. Therefore, $(b^n \prod_{i=1}^{c} b_i^{n-1}) U_1^{-1}$ contains a zero-sum subsequence U_2 of length n. Let V_i be the subsequence of S such that $\phi(V_i) = U_i$ for $i = 1, 2$. Now, we get $c(m-1)+1$ disjoint subsequences V_1, V_2, W_2, $\dots$, $W_{c(m-1)}$ each having length n and having sum in $\mathbb{Z}_m^d$. Since $s(\mathbb{Z}_m^d) = c(m-1)+1$, we can obtain a zero-sum subsequence of S of length nm, a contradiction.

CASE 2: $n \nmid t_i$ for every $i = 1, \dots, k$. Write $t_i = nq_i + r_i$ with $1 \leq r_i \leq n-1$. Then

$$\phi(S) = \prod_{i=1}^{k} h_i^{t_i} = \prod_{i=1}^{k} (h_i^n)^{q_i} \prod_{i=1}^{k} h_i^{r_i},$$

where $k > c$. Also since $t_1 + \dots + t_k = c(nm-1) = c(m-1)n + c(n-1)$ and $1 \leq r_1, \dots, r_k \leq n-1$, we see that $r_1 + \dots + r_k = c(n-1) + ln$ for some integer $l \geq 0$. If we can prove that $\prod_{i=1}^{k} h_i^{r_i}$ contains $l+1$ disjoint zero-sum subsequences each having length n, then as above, one can derive that S contains a zero-sum subsequence of length nm and we are done.

SUBCLAIM 1. *If $k > c$, $1 \leq r_1, \dots, r_k \leq n-1$ and $r_1 + \dots + r_k = c(n-1) + ln$ for some integer $l \geq 0$, then a sequence of the form $\prod_{i=1}^{k} h_i^{r_i}$ in $\mathbb{Z}_n^d$ contains $l+1$ disjoint zero-sum subsequences each having length n.*

To prove the subclaim, we proceed by induction on l. If $l = 0$, then $r_1 + \dots + r_k = c(n-1)$. Since (n, d) has Property D and $k > c$, by definition, the sequence $\prod_{i=1}^{k} h_i^{r_i}$ contains a zero-sum subsequence of length n. Assuming the subclaim is true for $l-1$, we want to prove it for l. Without loss of generality, we may assume that $n-1 \geq r_1 \geq \dots \geq r_k \geq 1$. Then there is an integer $u \geq 0$ such that $r_1 = \dots = r_u = n-1$ and $n-1 > r_{u+1} \geq \dots \geq r_k \geq 1$. Since (n, d) has Property D, the sequence $\prod_{i=1}^{k} h_i^{r_i}$ contains a zero-sum subsequence T of length n. Since the subsequence h_i^{n-1} is not a subsequence of T for any $i = 1, \dots, u$, and $h_i \mid (\prod_{i=1}^{k} h_i^{r_i})T^{-1}$ for every $i = 1, \dots, u$, we see that the sequence $(\prod_{i=1}^{k} h_i^{r_i})T^{-1}$ contains at least

$$\begin{aligned} u + \frac{r_{u+1} + r_{u+2} + \ldots + r_k - n}{n-2} &= u + \frac{c(n-1) + ln - u(n-1) - n}{n-2} \\ &\geq u + \frac{(c-u)(n-1)}{n-2} > c \end{aligned}$$

distinct elements and by the induction hypothesis, it contains $l - 1 + 1$ disjoint zero-sum subsequences each having length n. Thus, including T, we have $l + 1$ disjoint zero-sum subsequences of length n; hence Subclaim 1, and therefore Claim 1, follows.

Now we have $\phi(S) = \prod_{i=1}^{c} h_i^{t_i}$ with $t_1, \dots, t_c \geq 1$ and $t_1 + \ldots + t_c = c(nm-1)$. Let $T_i = \prod_{\phi(a_j)=h_i} a_j$. Then $S = T_1 \ldots T_c$. Write $t_i = nq_i + r_i$ with $0 \leq r_i \leq n-1$ for $i = 1, \dots, c$. Then $r_1 + \ldots + r_c \geq c(n-1)$. Hence, $r_1 = \ldots = r_c = n-1$. Choosing q_i disjoint zero-sum subsequences of T_i each having length n, we get altogether $q_1 + \ldots + q_c = c(m-1)$ disjoint subsequences $W_1, \dots, W_{c(m-1)}$ of S each having length n and having sum in $\mathbb{Z}_m^d$. Since (m,d) has Property D, we have $\sigma(W_1)\sigma(W_2)\ldots\sigma(W_{c(m-1)}) = g_1^{m-1} g_2^{m-1} \ldots g_{c(m-1)}^{m-1}$, where $g_1, \dots, g_{c(m-1)}$ are pairwise distinct.

Claim 2. *If $q_i \geq 1$, then $T_i = x^{t_i}$ for some $x \in \mathbb{Z}_{nm}^d$.*

Note that $t_i = q_i n + n - 1$. Without loss of generality we may assume that $W_1, \dots, W_{q_i}$ are subsequences of T_i. Also, for every $x \mid T_i(W_1 \ldots W_{q_i})^{-1}$ and every $y \mid W_1$, set $W_1' = W_1 y^{-1} x$. Since (m,d) has Property D,

$$\sigma(W_1')\sigma(W_2)\ldots\sigma(W_{c(m-1)}) = (g_1')^{m-1}(g_2')^{m-1}\ldots(g_{c(m-1)}')^{m-1}.$$

Therefore, $\sigma(W_1') = \sigma(W_1)$ and $x = y$ follows. Hence, $W_1 = x^n$. Similarly one can prove that $W_2 = W_3 = \ldots = W_{q_i} = x^n$, and thus $T = x^{t_i}$.

Since S contains no zero-sum subsequence of length nm, it follows from Claim 2 that $t_i \leq nm - 1$. But $t_1 + \ldots + t_c = c(nm-1)$, and we infer that $t_1 = \ldots = t_c = nm - 1$. Again by Claim 2, we have $T_i = x_i^{nm-1}$ for every $i = 1, \dots, c$. Now the proof is complete. ∎

Proposition 1.1. *Let H be a finite abelian group of exponent n, and let S be a sequence in H of length $s(H) - 1$. Suppose that S contains no zero-sum subsequence of length n. Then $v_g(S) \neq n - 2$ for every $g \in H$.*

Proof. Suppose that $v_g(S) = n - 2$ for some $g \in H$. Without loss of generality, we assume that $g = 0$. Consider the sequence $S' = S(g^{n-2})^{-1}$. Clearly, $|S'| = |S| - n + 2 = s(H) - n + 1$. Since $\varrho(H) \leq s(H) - n + 1$, one sees that S' has a short zero-sum subsequence T with $2 \leq |T| \leq n$. If we let $|T| = t$, then we get a zero-sum sequence $T' = Tg^{n-t}$ of S of length n, which contradicts the hypothesis. ∎

Proof of Corollary 1.1. (i) From (1), we know that $s(\mathbb{Z}_2^d) = 2^d(2-1)+1$. Now, consider a sequence S in $\mathbb{Z}_2^d$ of length 2^d having no zero-sum subsequence of length 2. It is clear that if $v_g(S) \neq 0$ then $v_g(S) = 1$. That is, S is of the required form showing that $(2, d)$ has Property D. Therefore, by Theorem 1, $(2^a, d)$ has Property D for any integer $a \geq 1$.

(ii) We know that $s(\mathbb{Z}_3^3) = 19 = 9(3-1)+1$. Therefore, from (2) and (3), we have $s(\mathbb{Z}_{3^a}^3) = 9(3^a-1)+1$. If we prove that $(3,3)$ has Property D, then so does $(3^a, 3)$ by Theorem 1. So consider a sequence $S = \prod_{i=1}^{18} a_i$ in $\mathbb{Z}_3^3$ of length 18 having no zero-sum subsequence of length 3. Then $v_g(S) \leq 2$. Also, by Proposition 1.1, if $v_g(S) \neq 0$, then $v_g(S) \neq 1$. Thus, $S = \prod_{i=1}^{9} a_i^2$, which shows that $(3,3)$ has Property D.

(iii) Let S be a sequence in $\mathbb{Z}_3^d$ of length $s(\mathbb{Z}_3^d) - 1$. Suppose S does not have a zero-sum subsequence of length 3. Then by Proposition 1.1, $S = \prod_{i=1}^{t} a_i^2$ (as above) and hence $|S| = s(\mathbb{Z}_3^d) - 1 = (3-1)t$. Thus, $(3, d)$ has Property D. ∎

Proof of Corollary 1.2. (i) Suppose (n, d) has Property D. It is easy to prove that $\varrho(\mathbb{Z}_n^d) \leq s(\mathbb{Z}_n^d) - n + 1$. So, to prove our first assertion, it is enough to show that $s(\mathbb{Z}_n^d) \leq \varrho(\mathbb{Z}_n^d) + n - 1$.

Consider a sequence S in $\mathbb{Z}_n^d$ of length $s(\mathbb{Z}_n^d) - 1$ such that S does not have a zero-sum subsequence of length n. Since (n, d) has Property D, we see that $S = \prod_{i=1}^{c} a_i^{n-1}$ for some $a_i \in \mathbb{Z}_n^d$ (for all i) and $c = (s(\mathbb{Z}_n^d)-1)/(n-1)$. Let $S' = \prod_{i=1}^{c} b_i^{n-1} = 0^{n-1}\prod_{i=2}^{c} b_i^{n-1}$, where $b_i = a_i - a_1$ for every i. Since S does not have a zero-sum subsequence of length n, it is clear that $T = \prod_{i=2}^{c} b_i$ does not have a short zero-sum subsequence. Therefore,

$$\varrho(\mathbb{Z}_n^d) - 1 \geq |T| - (n-1) = s(\mathbb{Z}_n^d) - 1 - (n-1).$$

That is, $s(\mathbb{Z}_n^d) \leq \varrho(\mathbb{Z}_n^d) + n - 1$ as desired.

(ii) Since (n, d) has Property D, by (i) we see that $(n-1) \mid (\varrho(\mathbb{Z}_n^d) - 1)$. Thus to finish the proof of (ii), it is enough to show that any sequence S in $\mathbb{Z}_n^d$ of length $\varrho(\mathbb{Z}_n^d) - 1$ having no short zero-sum subsequence is of the form $\prod_{i=1}^{c-1} a_i^{n-1}$.

Consider $S' = ST$, where $T = 0^{n-1}$ and 0 is the zero element in $\mathbb{Z}_n^d$. Clearly, $|S'| = s(\mathbb{Z}_n^d) - 1$ and S' does not have a zero-sum subsequence of length n. Since (n, d) has Property D, we have $S' = \prod_{i=1}^{c} a_i^{n-1}$. As $T = 0^{n-1}$, this implies the assertion. ∎

Proof of Theorem 2. (i) We know that in general $s(\mathbb{Z}_n^d) \geq \varrho(\mathbb{Z}_n^d) + n - 1$. So, to prove (i) it is enough to show that $s(\mathbb{Z}_n^d) \leq \varrho(\mathbb{Z}_n^d) + n - 1$.

Let S be as in the hypothesis. If $|S| \geq \varrho(\mathbb{Z}_n^d) + n - 1$, then by the result of Gao (stated just after Conjecture 1.4 in the introduction), S has a zero-sum subsequence of length n, which is impossible by hypothesis. Therefore, $|S| = s(\mathbb{Z}_n^d) - 1 \leq \varrho(\mathbb{Z}_n^d) + n - 2$. That is, $s(\mathbb{Z}_n^d) \leq \varrho(\mathbb{Z}_n^d) + n - 1$.

(ii) As (n,d) has Property C, we know that $(n-1) \mid (\varrho(\mathbb{Z}_n^d)-1)$ and hence by (i), we get $(n-1) \mid (s(\mathbb{Z}_n^d)-1)$. Hence $c = (s(\mathbb{Z}_n^d)-1)/(n-1)$ is a positive integer.

Let $S = a^s \prod_{i=1}^{c(n-1)-s} a_i$ be the given sequence in $\mathbb{Z}_n^d$ with $|S| = c(n-1)$ and $s > [(n-3)/2]$. Translating the given $cn-c$ elements by a, we get $S-a = 0^s \prod_{i=1}^{cn-c-s} b_i$, where $b_i = a_i - a \neq 0$ in $\mathbb{Z}_n^d$. Let $S^* = \prod_{i=1}^{cn-c-s} b_i$, which is a subsequence of $S-a$.

In order to prove this part of the theorem, we shall show that when $s = n-1$, the sequence $S-a$ is of the form $0^{n-1}\prod_{i=1}^{c-1} a_i^{n-1}$ in $\mathbb{Z}_n^d$. When $s < n-1$, we will produce a zero-sum subsequence of $S-a$ of length n, so that this case cannot happen.

Case I: $s = n-1$. Since S does not have a zero-sum subsequence of length n, S^* does not have a short zero-sum subsequence. Also, by (i), we know that $\varrho(\mathbb{Z}_n^d) = s(\mathbb{Z}_n^d) - n + 1 = (c-1)(n-1)+1$. Since (n,d) has Property C, we know that $S^* = \prod_{i=1}^{c-1} b_i^{n-1}$ and hence S is of the desired form.

Case II: $[(n-3)/2] < s \leq n-2$. In this case, $|S^*| = cn - c - s \geq (c-1)(n-1)+1$. Therefore, S^* contains a short zero-sum subsequence T, by the definition of $\varrho(\mathbb{Z}_n^d)$. In fact, $|T| < n - s$. That is,

$$|T| + s \leq n-1. \tag{4}$$

Otherwise, T together with $n-|T|$ zeros would produce a zero-sum subsequence of length n, contrary to assumption.

Since $|S^*| \geq (c-1)(n-1)+1$, we can fix T as above of maximal length. Now, the deleted sequence S^*T^{-1} has length $c(n-1)-(s+t) \geq (c-1)(n-1)$. Since there is no subsequence R of S^*T^{-1} of the form a^{n-1} for any $a \in \mathbb{Z}_n^d$, and (n,d) has Property C, there exists a short zero-sum subsequence K of S^*T^{-1} (in fact, if $|S^*T^{-1}| \geq (c-1)(n-1)+1$, we can use the definition of ϱ). Because of maximality of $|T|$, we have

$$|K| \leq |T|. \tag{5}$$

Also, if $|T|+|K| \leq n$, then TK is a short zero-sum subsequence of S^* with $|T| < |TK|$, contradicting the choice of T. Thus

$$n+1 \leq |T| + |K|. \tag{6}$$

Now, multiplying (4) by 2, we get $2s \leq 2n-2-2|T|$. If we add (5) and (6), we obtain $2|T| \geq n+1$. Combining these two results gives $2s \leq 2n-2-2|T| \leq n-3$, which is a contradiction. ∎

Remarks. It would be interesting to prove the following generalization of Theorem 1. *Suppose the pairs (n,r) and (m,r) have Property* D *and* $s(\mathbb{Z}_{mn}^r) \equiv 1 \pmod{mn-1}$. *Then (nm,r) has Property* D.

Acknowledgments. This work has been supported in part by NSFC and by MOEC under grant 02047. The work was started while the second author was visiting the Department of Computer Science and Technology, University of Petroleum, Beijing. He is grateful for the kind hospitality during his stay. Also, we thank the referee for many useful comments.

REFERENCES

[1] N. Alon and M. Dubiner, *A lattice point problem and additive number theory*, Combinatorica 15 (1995), 301–309.

[2] —, —, *Zero-sum sets of prescribed size*, in: Combinatorics, Paul Erdős is Eighty, Vol. 1, Bolyai Soc. Math. Stud., János Bolyai Math. Soc., Budapest, 1993, 33–50.

[3] A. Bialostocki and P. Dierker, *On the Erdős–Ginzburg–Ziv theorem and the Ramsey numbers for stars and matchings*, Discrete Math. 110 (1992), 1–8.

[4] C. Elsholtz, *Lower bounds for multi-dimensional zero sums*, Combinatorica (to appear).

[5] P. Erdős, A. Ginzburg and A. Ziv, *Theorem in the additive number theory*, Bull. Res. Council Israel 10 F (1961), 41–43.

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

[7] —, *Addition theorems and group rings*, J. Combin. Theory Ser. A 77 (1997), 98–109.

[8] —, *Two zero-sum problems and multiple properties*, J. Number Theory 81 (2000), 254–265.

[9] —, *On a combinatorial problem connected with factorization*, Colloq. Math. 72 (1997), 251–268.

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

[11] —, *A note on a zero-sum problem*, J. Combin. Theory Ser. A 95 (2001), 387–389.

[12] —, *On zero-sum subsequences of restricted size—II*, Discrete Math. 271 (2003), 51–59.

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

[14] —, —, *On long minimal zero sequences in finite abelian groups*, Period. Math. Hungar. 38 (1999), 179–211.

[15] —, —, *On zero-sum sequences in* $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, Integers 3 (2003), Paper A8, 45 pp. (electronic).

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

[17] A. Kemnitz, *On a lattice point problem*, Ars Combin. 16B (1983), 151–160.

[18] J. E. Olson, *On a combinatorial problem of finite Abelian groups*, *I*, *II*, J. Number Theory 1 (1969), 8–10, 195–199.

[19] B. Peterson and T. Yuster, *A generalization of an addition theorem for solvable groups*, Canad. J. Math. 36 (1984), 529–536.

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

[21] B. Sury and R. Thangadurai, *Gao's conjecture on zero-sum sequences*, Proc. Indian Acad. Sci. Math. Sci. 112 (2002), 399–414.

[22] R. Thangadurai, *On a conjecture of Kemnitz*, C. R. Math. Acad. Sci. Soc. R. Canad. 23 (2001), 39–45.

[23] R. Thangadurai, *Interplay between four different conjectures on certain zero-sum problems*, Expo. Math. 20 (2002), 215–229.

[24] —, *Non-canonical extensions of Erdős–Ginzburg–Ziv theorem*, Integers 2 (2002), Paper A7, 14 pp. (electronic).

[25] P. van Emde Boas, *A combinatorial problem on finite Abelian groups II*, Math. Centrum-Amsterdam Afd. Zuivere Wisk. 1969, ZW-014.

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

School of Mathematics
Harish Chandra Research Institute
Chhatnag Road, Jhusi
Allahabad 211019, India
E-mail: thanga@mri.ernet.in

Received 13 May 2003;
revised 3 November 2003 (4343)