COLLOQUIUM MATHEMATICUM

VOL. 72 1997 NO. 2

ON A COMBINATORIAL PROBLEM CONNECTED WITH FACTORIZATIONS

BY

WEIDONG GAO (BEIJING)

0. Let K be an algebraic number field with classgroup G and integer ring R. For $k \geq 1$ and a real number $x > 0$, let $a_k = a_k(G)$ be the maximal number of nonprincipal prime ideals which can divide a squarefree element of R with at most k distinct factorizations into irreducible elements, and let $F_k(x)$ be the number of elements $\alpha \in R$ (up to associates) having at most k different factorizations into irreducible elements of R. W. Narkiewicz [8] derived the asymptotic expression

$$F_k(x) \sim c_k x(\log)^{-1+1/|G|}(\log\log x)^{a_k},$$

where c_k is positive and depends on k and K.

Recently, F. Halter-Koch [6–7] used the characterizations of $a_k(G)$ to study nonunique factorizations.

In [8], Narkiewicz showed that $a_k(G)$ depends only on k and G, gave a combinatorial definition of it and proposed the problem of determining $a_k(G)$ (Problem 1145).

Let G be a finite abelian group (written additively). The *Davenport constant* $D(G)$ of G is defined to be the minimal integer d such that for every sequence of d elements in G there is a nonempty subsequence with sum zero. Narkiewicz and Śliwa [8–9] derived several properties of $a_1(G)$ involving $D(G)$ and proposed the following conjecture:

CONJECTURE 1. *Let $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$. Then $a_1(G) = n_1 + \ldots + n_r$, where C_n denotes the cyclic group of order n.*

They affirmed Conjecture 1 for $G = C_2^n, C_2^n \oplus C_4, C_2^n \oplus C_4^2$ or C_3^n.

In this paper we derive several properties of $a_k(G)$, affirm this conjecture for a more general case and determine $a_2(C_2^n)$ and $a_k(C_n)$ provided that n is substantially larger than k. The paper is organized in the following way: In Section 1 we repeat the combinatorial definition of $a_k(G)$ due to Narkiewicz [8] and give some preliminaries on $a_1(G)$ and $D(G)$. In Section 2 we derive some new properties of $a_1(G)$ and show the following:

1991 *Mathematics Subject Classification*: Primary 20D60.

THEOREM 1. *Let* $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ *with* $1 < n_1 \mid \ldots \mid n_r$, *let* p *be a prime with* $2 \le p \le 151$, *and let us adopt the convention* $C_n^0 = C_1$. *Then* $a_1(G) = n_1 + \ldots + n_r$ *provided that* G *is of one of the following forms* ($m \ge 1$):

(1) $C_{2^t3^s} \oplus C_{2^t3^sm}$, $0 \le t \le 1$ *or* $0 \le s \le 1$,
(2) $C^2_{2^t3^sp}$, $0 \le t \le 1$ *or* $0 \le s \le 1$,
(3) C^2_{4p},
(4) $C_{2^tp} \oplus C_{2^tpm}$, $0 \le t \le 1$,
(5) $C_{2^t5^s} \oplus C_{2^t5^sm}$, $0 \le t \le 1$,
(6) $C^2_{3\times 5^s}$,
(7) $C^2_{4\times 5^s}$,
(8) $C_2^n \oplus C_4^t \oplus C_{2^m}$, $0 \le t \le 1$,
(9) $C_2^n \oplus C_4^t \oplus C_{2^ml}$, $0 \le t \le 1, l \ge 4$ *and* $2^m \ge n + 3t + 1$,
(10) $C_3^n \oplus C_9^t \oplus C_{3^m}$, $0 \le t \le 1$,
(11) $C_3^n \oplus C_9^t \oplus C_{3^ml}$, $0 \le t \le 1, l \ge 4$, *and* $3^m \ge 2n + 8t + 1$,
(12) $C_5^2 \oplus C_{25m}, m = 1$ *or* $m \ge 4$.

In Section 3 we derive some properties of $a_k(G)$ and show the following

THEOREM 2. *If* $k \ge 2$ *and if*

$$k \le \frac{-\log_2 n + \sqrt{(\log_2 n)^2 + n}}{2} + 1,$$

then $a_k(C_n) = n$.

Remark 1. It is proved in [8, Proposition 9] that $\max\{D(G), \sum_{i=1}^r n_i\} \le a_k(G) \le a_l(G)$ for $1 \le k \le l$; therefore if Conjecture 1 is true, then $D(G) \le n_1 + \ldots + n_r$ and the best known estimation (see [3])

$$D(G) \le n_r\left(1 + \frac{\log |G|}{\log n_r}\right)$$

would be improved. So it seems very difficult to settle Conjecture 1 in general.

1. In what follows we always let G denote a finite abelian group.

For a sequence $S = (a_1, \ldots, a_m)$ of elements in G, we use $\sum S$ to denote the sum $\sum_{i=1}^m a_i$. By λ we denote the empty sequence and adopt the convention that $\sum \lambda = 0$. We say S a *zero-sum sequence* if $\sum S = 0$. A subsequence T of S is a sequence $T = (a_{i_1}, \ldots, a_{i_l})$ with $\{i_1, \ldots, i_l\} \subset \{1, \ldots, m\}$; we denote by I_T the index set $\{i_1, \ldots, i_l\}$, and identify two subsequences S_1 and S_2 if $I_{S_1} = I_{S_2}$. We say two subsequences S_1 and S_2 are *disjoint* if $I_{S_1} \cap I_{S_2} = \emptyset$ (the empty set) and define multiplication of two disjoint subsequences by juxtaposition.

A nonempty sequence B of nonzero elements in G is called a *block* in G provided that $\sum B = 0$; we call a block *irreducible* if it cannot be written as a product of two blocks.

By a *factorization* of a block $B = (b_1, \dots, b_k)$ we shall understand any surjective map

$$\varphi : \{1, \dots, k\} \to \{1, \dots, t\}$$

with a certain positive integer $t = t(\varphi)$ such that, for $j = 1, \dots, t$, the sequences $B_j = (b_i : \varphi(i) = j)$ are blocks. If they are all irreducible, we speak about an *irreducible factorization* of B. Obviously, we have $B = B_1 \dots B_t$. Two such factorizations φ and ψ are called *strongly equivalent* if $t(\varphi) = t(\psi)$ $(= t$ say$)$ and for a suitable permutation δ the sets $\{i : \varphi(i) = j\}$ and $\{\psi(i) = \delta(j)\}$ coincide for $j = 1, \dots, t$. For $k \geq 1$, we define $B_k(G)$ to be the set consisting of all blocks which have at most k strongly inequivalent irreducible factorizations, and let $a_k(G) = \max\{|B| : B \in B_k(G)\}$.

For a sequence S of elements in G, we use $\sum(S)$ to denote the set consisting of all elements in G which can be expressed as a sum over a nonempty subsequence of S, i.e.,

$$\sum(S) = \Big\{ \sum T : \lambda \neq T,\ T \subseteq S \Big\},$$

where $T \subseteq S$ means that T is a subsequence of S.

Lemma 1 ([9, Proposition 2]). *Let $B = B_1 \dots B_r \in B(G)$ and let $B_1, \dots, B_r$ be irreducible blocks. Then $B \in B_1(G)$ if and only if for all disjoint nonempty subsets X, Y of $\{1, \dots, r\}$ we have*

$$\sum \Big(\prod_{i \in X} B_i \Big) \cap \sum \Big(\prod_{i \in Y} B_i \Big) = \{0\}.$$

Lemma 2 ([9, Proposition 6]). *If $B = B_1 \dots B_r \in B_1(G)$ and if $B_1, \dots, B_r$ are irreducible blocks, then $|B_1| \dots |B_r| \leq |G|$.*

Lemma 3 ([9, Proposition 3]). *Let $B = B_1 \dots B_r \in B_1(G)$ and let $B_1, \dots, B_r$ be irreducible blocks. Then $|B| \leq D(G) + r - 1$.*

For a sequence S of elements in G, let $f_{\mathrm{E}}(S)$ (resp. $f_{\mathrm{O}}(S)$) denote the number of zero-sum subsequences T of S with $2 \mid |T|$ (resp. $2 \nmid |T|$), where we count $f_{\mathrm{E}}(S)$ including the empty sequence; hence, we have $f_{\mathrm{E}}(S) \geq 1$.

Lemma 4. *Let p be a prime. Then the following hold.*

(i) $D(C_{n_1} \oplus C_{n_2}) = n_1 + n_2 - 1$ $(n_1 \mid n_2)$ ([11]).
(ii) $D(C_{2p^t}^3) = 6p^t - 2$ ([2]).
(iii) $D(C_{3 \times 2^t}^3) = 9 \times 2^t - 2$ ([3]).
(iv) $D(\bigoplus_{i=1}^k C_{p^{e_i}}) = 1 + \sum_{i=1}^k (p^{e_i} - 1)$ ([10]).

(v) *If* S *is a sequence of elements in* $\bigoplus_{i=1}^{k} C_{p^{e_i}}$ *with* $|S| \geq 1 + \sum_{i=1}^{k}(p^{e_i}-1)$, *then* $f_{\mathrm{E}}(S) \equiv f_{\mathrm{O}}(S) \pmod p$ ([2], [10]).

LEMMA 5. *Let* $H = C_{n_1} \oplus \ldots \oplus C_{n_l}$ *with* $1 < n_1 \mid \ldots \mid n_l$, $n_l \mid n$, *and* $D(H \oplus C_n^2) = 2(n-1) + D(H)$. *Then* $D(H \oplus C_n) = n - 1 + D(H)$.

Proof. By the definition of Davenport's constant one can choose a sequence $T = (a_1, \ldots, a_{D(H\oplus C_n)-1})$ of $D(H \oplus C_n) - 1$ elements in $H \oplus C_n$ such that $0 \notin \sum(T)$. Put $b_i = (a_i, 0)$ with $0 \in C_n$ for $i = 1, \ldots, D(H \oplus C_n) - 1$, and put $b_i = (0, 1)$ with $0 \in H \oplus C_n$ and $1 \in C_n$ for $i = D(H \oplus C_n), \ldots, D(H \oplus C_n) + n - 2$. Clearly, $b_i \in H \oplus C_n^2$ for $i = 1, \ldots, D(H \oplus C_n) + n - 2$ and the sequence $b_1, \ldots, b_{D(H\oplus C_n)+n-2}$ contains no nonempty zero-sum subsequence. This implies that

$$D(H \oplus C_n) + n - 1 \leq D(H \oplus C_n^2).$$

Similarly, one can prove that

$$D(H) + n - 1 \leq D(H \oplus C_n),$$

so we have

$$D(H) + 2(n-1) \leq D(H \oplus C_n) + n - 1 \leq D(H \oplus C_n^2) = D(H) + 2(n-1).$$

This forces that $D(H \oplus C_n) = D(H) + n - 1$ as desired.

LEMMA 6. *Let* $H = C_{n_1} \oplus \ldots \oplus C_{n_l}$ *with* $1 < n_1 \mid \ldots \mid n_l$, *and* $n_l \mid n$. *Suppose that* $n \geq D(H)$ *and* $D(H \oplus C_n^2) = 2(n-1) + D(H)$. *Then any sequence* S *of* $2(n-1) + D(H)$ *elements in* $H \oplus C_n$ *contains a nonempty zero-sum subsequence* T *with* $|T| \leq n$.

Proof. Suppose $S = (a_1, \ldots, a_{2(n-1)+D(H)})$. For $i = 1, \ldots, 2(n-1) + D(H)$ we define $b_i = (a_i, 1)$ with $1 \in C_n$. Clearly, $b_i \in H \oplus C_n^2$. Since $D(H \oplus C_n^2) = 2(n-1) + D(H)$, the sequence $b_1, \ldots, b_{2(n-1)+D(H)}$ contains a nonempty zero-sum subsequence T. By the definition of b_i, we must have $n \mid |T|$. But $n \geq D(H) - 1$, so $|T| \leq 2(n-1) + D(H) \leq 3n - 1$, and this forces that

$$|T| = n \quad \text{or} \quad |T| = 2n.$$

If $|T| = n$ we are done. Otherwise, $|T| = 2n$. By Lemma 5, $D(H \oplus C_n) = n - 1 + D(H) \leq 2n - 1$, so one can find a nonempty zero-sum subsequence M of T with $|M| < |T|$. Setting W equal to the shorter of M and $T - M$ (the subsequence with index set $I_T - I_M$) completes the proof.

LEMMA 7. *Let* $H = C_{n_1} \oplus \ldots \oplus C_{n_l}$ *with* $1 < n_1 \mid \ldots \mid n_l$, *and* $n_l \mid n$. *Suppose that* $n \geq D(H)$ *and* $D(H \oplus C_n^2) = 2(n-1) + D(H)$. *Then any zero-sum sequence* S *of elements in* $H \oplus C_n$ *with* $|S| \geq n + D(H)$ *contains a zero-sum subsequence* T *with* $|S| - n \leq |T| < |S|$.

P r o o f. We distinguish three cases.

C a s e 1: $|S| \geq 2(n-1)+D(H)$. Then the lemma follows from Lemma 6.

C a s e 2: $n + D(G) \leq |S| \leq 2n$. By Lemma 5, we have $D(H \oplus C_n) = n - 1 + D(G)$, thus there exists a zero-sum subsequence W of S with $1 \leq |W| < |S|$. Setting T equal to the longer of W and $S - W$ proves the lemma in this case.

C a s e 3: $2n + 1 \leq |S| \leq 2n - 3 + D(H)$. We define

$$b_i = \begin{cases} (a_i, 1) \text{ with } 1 \in C_n & \text{if } i = 1, \ldots, |S|, \\ (0, 1) \text{ with } 0 \in H \oplus C_n \text{ and } 1 \in C_n & \text{if } i = |S| + 1, \ldots, 2(n-1) + D(H), \end{cases}$$

and similarly to the proof of Lemma 6 we find a zero-sum subsequence W of $b_1, \ldots, b_{2(n-1)+D(H)}$ with $|W| = n$ or $2n$. Put

$$J = \begin{cases} \{1, \ldots, |S|\} - I_W & \text{if } |W| = n \text{ (not necessarily } I_W \subseteq \{1, \ldots, |S|\}), \\ I_W - \{|S| + 1, \ldots, 2(n-1) + D(H)\} & \text{if } |W| = 2n, \end{cases}$$

and let T be the subsequence of S with $I_T = J$. Clearly, $\sum T = 0$ and $|S| - n \leq |T| < |S|$. This completes the proof.

We say two nonempty sequences $S = (a_1, \ldots, a_m)$ and $T = (b_1, \ldots, b_m)$ of elements in C_n with the same size m are *similar* (written $S \sim T$) if there exist an integer c coprime to n and a permutation σ of $1, \ldots, m$ such that $a_i = cb_{\sigma(i)}$ for $i = 1, \ldots, m$. Clearly, $\sim$ is an equivalence relation. For any $x \in C_n$, we denote by $|x|_n$ the minimal nonnegative inverse image of x under the natural homomorphism from the additive group of integers onto C_n.

LEMMA 8 ([1], [4]). *Let $S = (a_1, \ldots, a_{n-k})$ be a sequence of $n-k$ elements in C_n with $n \geq 2$. Suppose that $0 \notin \sum(S)$ and suppose that $k \leq n/4 + 1$. Then*

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

with all $x_i \neq 0$.

2. In this section we derive some properties of $a_1(G)$ and prove Theorem 1.

PROPOSITION 1. *Let $G = \bigoplus_{i=1}^{k} C_{p^{e_i}}$ with p an odd prime, let $B = B_1 \ldots B_r \in B_1(G)$ and let $B_1, \ldots, B_r$ be irreducible blocks. Suppose that exactly t of $|B_1|, \ldots, |B_r|$ are odd. Then $|B| \leq D(G) + t - 1$.*

P r o o f. Without loss of generality, we assume that $|B_1|, \ldots, |B_t|$ are odd and that $|B_{t+1}|, \ldots, |B_r|$ are even. Let $D_i \subseteq B_i$ with $|D_i| = |B_i| - 1$ for $i = 1, \ldots, t$, and put $S = D_1 \ldots D_t B_{t+1} \ldots B_r$. By the choice of $D_1, \ldots, D_t$ and the hypothesis of the proposition, all zero-sum subsequences of S consist of all products of the form $B_{i_1}\ldots B_{i_l}$ with $l\ge 0$ and $t+1\le i_1<\ldots<i_l\le r$. This gives

$$f_{\mathrm{E}}(S)=\binom{r-t}{0}+\binom{r-t}{1}+\binom{r-t}{2}+\ldots+\binom{r-t}{r-t}=2^{r-t}$$

and $f_{\mathrm{O}}(S)=0$. But $p\nmid 2$, therefore $f_{\mathrm{E}}(S)\not\equiv f_{\mathrm{O}}(S) \pmod p$. Now it follows from Lemma 4(v) that $|B|-t=|S|\le\sum_{i=1}^{k}(p^{e_i}-1)=D(G)-1$, that is, $|B|\le D(G)+t-1$.

PROPOSITION 2. *Let $H=C_{n_1}\oplus\ldots\oplus C_{n_l}$ be a finite abelian group with $1<n_1\,|\,\ldots\,|\,n_l$, and let $G=H\oplus C_{nm}$ with $n_l\,|\,n$. Suppose that* (i) *$m\ge 4$ and $n\ge D(H)$, and* (ii) *$D(H\oplus C_n^2)=2(n-1)+D(H)$. Then $a_1(G)\le a_1(H\oplus C_n)+nm-n$; moreover, if $a_1(H\oplus C_n)=n+n_1+\ldots+n_l$ then $a_1(G)=nm+n_1+\ldots+n_l$.*

Remark 2. From Lemma 4(ii)–(iv) we see that there exists a large class of pairs of (H,n) satisfying conditions (i) and (ii) of Proposition 2.

LEMMA 9. *Let s, r, a, b be positive integers such that $a\ge 2$, $2a<b$ and $(r-1)b\ge s\ge ar$. Let $l,x_1,\ldots,x_l$ be positive integers satisfying*

(i) $l\ge r$,
(ii) $x_1+\ldots+x_l=s$,
(iii) $a\le x_1,\ldots,x_l\le b$.

Suppose $x_1=n_1,\ldots,x_l=n_l$ are such that the product $x_1\ldots x_l$ attains its minimal possible value. Then (a) *there is at most one i such that $a\ne n_i\ne b$; and we may assume* (b) *$l=r$.*

Proof. (a) If there are i,j with $1\le i\ne j\le l$ such that $a<n_i,n_j<b$, without loss of generality, we assume that $a<n_i\le n_j<b$. Then $(n_i-1)(n_j+1)<n_in_j$, therefore if we take $x_i=n_i-1, x_j=n_j+1$ and $x_k=n_k$ for $k\ne i,j$, then $x_1\ldots x_l<n_1\ldots n_l$, a contradiction. This proves (a).

(b) Let l be the smallest integer satisfying $l\ge r$ and the hypothesis of the lemma. If $l\ge r+1$, then since $s\le(r-1)b$, there are at most $r-2$ distinct indices i such that $n_i=b$, so by (a), there are at least two indices i and j such that $n_i=n_j=a$; without loss of generality, we assume $n_{l-1}=n_l=a$. Now let $x_i=n_i$ for $i=1,\ldots,l-2$ and set $x_{l-1}=n_{l-1}+n_l=2a\le b$. Then $x_1\ldots x_{l-1}\le n_1\ldots n_l$, a contradiction. This proves (b) and completes the proof.

Proof of Proposition 2. Let $t=a_1(G)-nm-n_1-\ldots-n_l\ge 0$. It is sufficient to prove that there exists a block in $B_1(H\oplus C_n)$ of length not less than $n_1+\ldots+n_l+n+t$. To do this we consider a block $A=A_1\ldots A_r\in B_1(G)$ with $|A|=a_1(G)=nm+n_1+\ldots+n_l+t$, where $A_1,\ldots,A_r$ are irreducible blocks.

By rearranging the indices we may assume that

$$A = (a_1, \dots, a_{mn+n_1+\dots+n_l+t-r}, b_1, \dots, b_r)$$

with $b_i \in A_i$ for $i = 1, \dots, r$.

We assert that

$$r \le n_1 + \dots + n_l. \tag{1}$$

Assume $r > n_1 + \dots + n_l$. Since it is well known that $D(H) \ge n_1 + \dots + n_l - l + 1$ (see for example [2]), we have $n \ge D(H) \ge n_1 + \dots + n_l - l + 1$. Now by Lemma 9,

$$\begin{aligned} |A_1| \dots |A_r| &\ge (nm + n_1 + \dots + n_l + t - 2r)2^r \\ &> (mn + t - n_1 - \dots - n_l)2^{n_1+\dots+n_l} \\ &\ge ((m-1)n - l + 1)2^{n_1} \dots 2^{n_l} \\ &\ge ((m-1)n - l + 1)(2n_1) \dots (2n_l) \\ &\ge mnn_1 \dots n_l = |G|; \end{aligned}$$

this contradicts Lemma 2 and proves (1).

It is well known that there exists a homomorphism φ from $H \oplus C_{nm}$ onto $H \oplus C_n$ with $\ker \varphi = C_m$ (up to isomorphism).

For a sequence $S = (s_1, \dots, s_u)$ of elements of $H \oplus C_{nm}$, let $\varphi(S)$ denote the sequence $(\varphi(s_1), \dots, \varphi(s_u))$ of elements of $H \oplus C_n$. Since $nm + n_1 + \dots + n_l + t - r \ge nm = (m-2)n + 2n$ and $n \ge D(H)$, by Lemmas 6 and 7 one can find $m - 1$ disjoint nonempty subsequences $B_1, \dots, B_{m-1}$ of $(a_1, \dots, a_{mn+n_1+\dots+n_l+t-r})$ with $\sum \varphi(B_i) = 0$ for $i = 1, \dots, m-1$, and $|B_i| \le n$ for $i = 1, \dots, m-2$. Therefore

$$\sum B_i \in \ker \varphi = C_m$$

for $i = 1, \dots, m-1$.

Since $A = A_1 \dots A_r$ is the unique irreducible factorization of A and $b_i \in A_i$ for $i = 1, \dots, r$, the sequence $\sum B_1, \dots, \sum B_{m-1}$ contains no nonempty zero-sum subsequence, and it follows from Lemma 8 that $\sum B_1 = \dots = \sum B_{m-1} = a$ (say) and a generates C_m.

Let $A_{i_1}, \dots, A_{i_v}$ $(v \ge 0)$ be all irreducible blocks contained in $A - B_1 - \dots - B_{m-2}$. Since $A \in B_1(G)$, it follows that $A_{i_1}, \dots, A_{i_v}$ are disjoint, so one can write

$$A - B_1 - \dots - B_{m-2} = A_{i_1} \dots A_{i_v} B'.$$

Then B' contains no nonempty zero-sum subsequence and

$$\sum B' = \sum A - \sum B_1 - \dots - \sum B_{m-2} - \sum A_{i_1} - \dots - \sum A_{i_v} = 2a.$$

Now we split the proof into steps.

Step 1: *$\varphi(B_1),\ldots,\varphi(B_{m-2})$ and $\varphi(A_{i_1}),\ldots,\varphi(A_{i_v})$ are irreducible blocks in $H\oplus C_n$.* If for some i with $1\le i\le m-2, \varphi(B_i)$ is not an irreducible block in $H\oplus C_n$, then there exist two disjoint nonempty subsequences B_i', B_i'' of B_i such that $\sum\varphi(B_i')=\sum\varphi(B_i'')=0$ (in $H\oplus C_n$) and $B_i=B_i'B_i''$. Then $\sum B_i'\in C_m, \sum B_i''\in C_m$, and the sequence $\sum B_1,\ldots,\sum B_{i-1},\sum B_i',\sum B_i''$, $\sum B_{i+1},\ldots,\sum B_{m-1}$ contains a nonempty zero-sum subsequence. This contradicts $b_i\in A_i$ for $i=1,\ldots,r$ and proves $\varphi(B_1),\ldots,\varphi(B_{m-2})$ are irreducible blocks.

If for some j, $\varphi(A_{i_j})$ is not an irreducible block in $H\oplus C_n$, then there exist two disjoint nonempty subsequences A_{i_j}', A_{i_j}'' of A_{i_j} such that $\sum\varphi(A_{i_j}')=\sum\varphi(A_{i_j}'')=0$ (in $H\oplus C_n$) and $A_{i_j}=A_{i_j}'A_{i_j}''$. It follows from $A\in B_1(G)$ that $\sum B_1,\ldots,\sum B_{m-2},\sum A_{i_j}'$ contains no nonempty zero-sum subsequence, so by Lemma 8, $\sum A_{i_j}'=a$, and therefore, $\sum B'A_{i_j}'B_1\ldots B_{m-3}=0$. This clearly contradicts $A=A_1\ldots A_r\in B_1(G)$ and completes the proof of this step.

Step 2: $\varphi(B_1)\varphi(A_{i_1})\ldots\varphi(A_{i_v})\in B_1(H\oplus C_n)$. Assume otherwise. Then there exist $B_1'\subseteq B_1, A_{i_1}'\subseteq A_{i_1},\ldots,A_{i_v}'\subseteq A_{i_v}$ such that $\sum\varphi(B_1')=\sum\varphi(A_{i_1}'\ldots A_{i_v}')$ and $A_{i_j}\ne A_{i_j}'\ne\lambda$ for at least one j with $1\le j\le v$. Therefore, $\sum B_1'-\sum A_{i_1}'\ldots A_{i_v}'\in C_m$, so $\sum(B_1-B_1')A_{i_1}'\ldots A_{i_v}'\in C_m$. Noting that $m\ge 4, \sum B_2=a$ and $\sum B'=2a$, it follows from Lemma 8 that the sequence $\sum(B_1-B_1')A_{i_1}'\ldots A_{i_v},\sum B_2,\ldots,\sum B_{m-2},\sum B'$ contains a nonempty zero-sum subsequence. Clearly, such a subsequence must contain the term $\sum(B_1-B_1')A_{i_1}'\ldots A_{i_v}'$, contrary to $A\in B_1(G)$.

Step 3: We distinguish two cases.

Case 1: $|B'|\le 2n$. Then

$$\begin{aligned}|\varphi(B_1)\varphi(A_{i_1})\ldots\varphi(A_{i_v})| &= |B_1A_{i_1}\ldots A_{i_v}|\\ &= |A|-|B'|-|B_2|-\ldots-|B_{m-2}|\\ &\ge |A|-2n-(m-3)n\ge n+n_1+\ldots+n_l+t,\end{aligned}$$

as desired.

Case 2: $|B'|>2n$. Then $|B'|>n+D(H)$. By Lemma 7, there exists a subsequence T of B' such that $\sum\varphi(T)=0$ and $|B'|-n\le|T|<|B'|$. Put $W=B'-T$. Then

$$1\le|W|\le n.$$

Since a generates C_m and B' contains no nonempty zero-sum subsequence, $\sum T=fa$ with $1\le f\le m-1$. If $3\le f\le m-1$, let $A_{u_1},\ldots,A_{u_h}$ be all irreducible blocks which meet T (i.e. $I_{A_{u_i}}\cap I_T\ne\emptyset$ for $i=1,\ldots,h$). Since $\sum TB_1\ldots B_{m-f}=\sum TB_2\ldots B_{m-f+1}=0$, it follows from $A=A_1\ldots A_r\in$

$B_1(G)$ that $B_1 \ldots B_{m-f} = A_{u_1} \ldots A_{u_h} - T = B_2 \ldots B_{m-f+1}$. This contradicts the disjointness of $B_1, \ldots, B_{m-2}$. Hence

$$\sum T = a \text{ or } 2a.$$

But $\sum T + \sum W = 2a$ and $\sum W \neq 0$, so we must have $\sum T = \sum W = a$. Let T' be a nonempty subsequence of T with $\sum \varphi(T') = 0$. Then by using the same method one can prove that $\sum T' = a$. This forces that $T' = T$ and implies that

$$\varphi(T) \text{ is an irreducible block in } H \oplus C_n.$$

We assert that

$$\varphi(T)\varphi(A_{i_1}) \ldots \varphi(A_{i_v}) \in B_1(H \oplus C_n).$$

Assume to the contrary that there exist $T' \subseteq T, A'_{i_1} \subseteq A_{i_1}, \ldots, A'_{i_v} \subseteq A_{i_v}$ such that $\sum \varphi(T'A'_{i_1} \ldots A'_{i_v}) = 0$ and $A_{i_j} \neq A'_{i_j} \neq \lambda$ for some $1 \leq j \leq v$. Then $\sum T'A'_{i_1} \ldots A'_{i_v} \in C_m$. Notice that the sequence $\sum B_1, \ldots, \sum B_{m-2}$, $\sum W, \sum T'A'_{i_1} \ldots A'_{i_v}$ must contain a nonempty zero-sum subsequence and such a subsequence must contain the term $\sum T'A'_{i_1} \ldots A'_{i_v}$. This clearly contradicts $A = A_1 \ldots A_r \in B_1(G)$ and proves the assertion. Now the theorem follows from $|\varphi(T)\varphi(A_{i_1}) \ldots \varphi(A_{i_v})| = nm + n_1 + \ldots + n_l + t - |B_1| - \ldots - |B_{m-2}| - |W| \geq n + n_1 + \ldots + n_l + t$. This completes the proof.

PROPOSITION 3. *If* $D(C_n^3) = 3n - 2$, *then*

(i) $a_1(C_n \oplus C_{2n}) \leq a_1(C_n^2) + n$;
(ii) $a_1(C_n \oplus C_{3n}) \leq a_1(C_n^2) + 2n$;
(iii) $a_1(C_{2n}^2) \leq a_1(C_n^2) + 2n$, *and*
(iv) $a_1(C_{3n}^2) \leq a_1(C_n^2) + 4n$.

P r o o f. Put $H = C_k \oplus C_n$ and $G = C_{lk} \oplus C_{nm}$. It is well known that there exists a homomorphism φ from G onto H such that $\ker \varphi = C_l \oplus C_m$ (up to isomorphism). We use the same notation $A = A_1 \ldots A_r \in B_1(G)$, φ, $\varphi(S)$ as in the proof of Proposition 2.

(i) $k = 1$, $l = n$, $m = 2$. Let $t = a_1(C_n \oplus C_{2n}) - 3n$. Clearly, it is sufficient to prove that there exists a block in $B_1(C_n^2)$ of length not less than $2n + t$. If $t = 0$, then the proposition follows from Remark 1, so we may assume that $t \geq 1$, and $r \geq 3$ follows from Lemma 3. We assert that

$$\max\{|A_1|, \ldots, |A_r|\} \geq 2n + t.$$

Otherwise by Lemma 9 we get $|A_1| \ldots |A_r| > (2n+t)n > 2n^2 = |C_n \oplus C_{2n}|$; this contradicts Lemma 2 and proves the assertion. So we may assume that

$$|A_r| \geq 2n + t.$$

By using Lemmas 7 and 4(i) one can find a subsequence B_1 of A_r such that $\sum \varphi(B_1) = 0$ and $|A_r| - n \leq |B_1| < |A_r|$. Put $B_2 = A_r - B_1$. Then

$\sum \varphi(B_2) = 0$. So $\sum B_1 \in C_2, \sum B_2 \in C_2$, and clearly $\sum B_1 = \sum B_2 = 1$. It is easy to prove that $\varphi(B_1), \varphi(B_2), \varphi(A_1), \ldots, \varphi(A_{r-1})$ are all irreducible blocks in C_n^2, and similarly to the proof of Proposition 2 one can get $\varphi(B_1)\varphi(A_1)\ldots\varphi(A_{r-1}) \in B_1(C_n^2)$. Now (i) follows from $|\varphi(B_1)\varphi(A_1)\ldots \ldots, \varphi(A_{r-1})| \geq 2n + t$.

(ii) $k = 1$, $l = n, m = 3$. Let $t = a_1(C_n \oplus C_{3n}) - 4n$. Similarly to (i) we may assume that $t \geq 1$ and by Lemma 3 we have $r \geq 3$, and similarly to (i) we get $\max\{|A_1|, \ldots, |A_r|\} \geq 3n + t$, so we may assume that $|A_r| \geq 3n + t$. By using Lemmas 4(i), 6, and 7 we get three disjoint subsequences B_1, B_2, B_3 of A_r such that $\sum \varphi(B_1) = \sum \varphi(B_2) = \sum \varphi(B_3) = 0$ and $|B_1| \leq n, |A_r - B_1| - n \leq |B_2| < |A_r - B_1|$, and $B_3 = A_r - B_1 - B_2$. Clearly, $\sum B_1 = \sum B_2 = \sum B_3 = a$ (say) and $a = 1$ or 2. Now (ii) follows in a similar way to (i).

(iii) $k = n$, $l = m = 2$. Let $t = a_1(C_{2n}^2) - 4n$. If $t = 0$, then (iii) follows from Remark 1, so we may assume that $t \geq 1$. Clearly, it is sufficient to prove that there exists a block in $B_1(C_n^2)$ of length not less than $2n + t$.

Since $a_1(C_{2n}^2) \geq 4n + 1$, by Lemmas 3 and 4(i) we have $r \geq 3$. If $\max\{|A_1|, \ldots, |A_r|\} < 3n$, then by Lemma 9 we have $|A_1| \ldots |A_r| \geq 2(n + 2 - 2)(3n - 1) > 4n^2 = |C_{2n}^2|$. This contradicts Lemma 2, so we may assume that $|A_r| \geq 3n$, and by using Lemmas 6 and 7 we find three disjoint subsequences B_1, B_2, B_3 of A_r such that $\sum \varphi(B_1) = \sum \varphi(B_2) = \sum \varphi(B_3) = 0$ and $|B_1| \leq n, |A_r - B_1| - n \leq |B_2| < |A_r - B_1|$, and $B_3 = A_r - B_1 - B_2$. Noticing that $D(C_2^2) = 3$ we can prove (iii) similarly to (i).

(iv) $k = n$, $l = m = 3$. Let $t = a_1(C_{3n}) - 6n$. Similarly to (iii) we may assume that $t \geq 1$, and $r \geq 3$ follows from Lemmas 3 and 4(i). Furthermore, we may assume $n \geq 3$ for otherwise (iv) reduces to (iii). If max $\{|A_1|, \ldots, |A_r|\} < 5n$, then by Lemma 9 we have $|A_1| \ldots |A_r| \geq 2(n + 2 - 2)(5n - 1) > 9n^2 = |C_{3n}^2|$. This contradicts Lemma 2 and proves that max $\{|A_1|, \ldots, |A_r|\} \geq 5n$. Now (iv) follows in a similar way to (iii) upon noting that $D(C_3^2) = 5$. This completes the proof.

COROLLARY 1. *If* $a_1(C_n^2) = 2n$ *and* $D(C_n^3) = 3n - 2$, *then*

(i) $a_1(C_n \oplus C_{2n}) = 3n$;
(ii) $a_1(C_n \oplus C_{3n}) = 4n$;
(iii) $a_1(C_{2n}^2) = 4n$, *and*
(iv) $a_1(C_{3n}^2) = 6n$.

P r o o f. This follows from Remark 1 and Proposition 3.

LEMMA 10 ([2, Theorem (2.8)]). *Let* p *be a prime*, H *a finite abelian* p*-group*, *and let* S *be a sequence of* $D(H) - 2$ *elements in* H. *Suppose that* $f_{\mathrm{E}}(S) - f_{\mathrm{O}}(S) \not\equiv 0 \pmod p$. *Then all elements not in* $\sum(S)$ *are contained in a fixed proper coset of a subgroup of* H.

P. van Emde Boas ([2, Theorem (2.8)]) stated the conclusion of Lemma 10 for the case $f_{\mathrm{E}}(S) = 1$ and $f_{\mathrm{O}}(S) = 0$, but his method does work for the general case. For covenience, we repeat the proof here.

P r o o f o f L e m m a 10. In the proof we shall use mutiplicative notation for H, and in all other cases in this paper, additive notation will be used.

Let $H = C_{p^{e_1}} \oplus \ldots \oplus C_{p^{e_r}}$ with $1 \le e_1 \le \ldots \le e_r$, and suppose $S = (g_1, \ldots, g_k)$, where $k = D(H) - 2 = -k - 1 + \sum_{i=1}^{k} p^{e_i}$. Put $N(S, g) := N_{\mathrm{even}} - N_{\mathrm{odd}}$ where $N_{\mathrm{even(odd)}}$ is the number of solutions of the equation

$$g_1^{m_1} g_2^{m_2} \ldots g_k^{m_k} = g, \qquad m_i = 0, 1,$$

with $\sum_{i=1}^{k} m_i$ even (odd).

We denote by F_p the p-element field. We multiply out the product

$$(1 - g_1)(1 - g_2) \ldots (1 - g_k)$$

in the group ring $F_p[H]$. Then

$$\prod_{i=1}^{k} (1 - g_i) = \sum_{g \in H} N(S, g) g. \tag{2}$$

If $g^{p^n} = 1$ $(g \in H)$, then it is well known that the following equalities hold in $F_p[H]$:

$$(1 - g)^{p^n} = 0, \tag{3}$$

$$(1 - g)^{p^n - 1} = \sum_{v=0}^{p^n - 1} g^v, \tag{4}$$

$$(1 - g)^{p^n - 2} = \sum_{v=1}^{p^n - 1} v g^{v-1}. \tag{5}$$

Let $x_1, \ldots, x_r$ be a basis for H where x_i has order p^{e_i}. Then $g_i = x_1^{f_{i1}} \ldots x_r^{f_{ir}}$, $0 \le f_{ij} \le p^{e_j} - 1$, $i = 1, \ldots, k$, $j = 1, \ldots, r$. Now, we have

$$\begin{aligned}
\prod_{i=1}^{k} (1 - g_i) &= \prod_{i=1}^{k} (1 - x_1^{f_{i1}} \ldots x_r^{f_{ir}}) \\
&= \prod_{i=1}^{k} (1 - (1 - (1 - x_1))^{f_{i1}} \ldots (1 - (1 - x_r))^{f_{ir}}) \\
&= \prod_{i=1}^{k} \sum_{j=1}^{r} (f_{ij}(1 - x_j) + h_{ij}(1 - x_j)^2 + \alpha_{ij}(1 - x_j)^3),
\end{aligned}$$

where $h_{ij} = \frac{1}{2}(f_{ij}-1)f_{ij}$ and $\alpha_{ij} \in F_p[H]$. Now from (3) and $k = -1 + \sum_{i=1}^{r}(p^{e_i}-1)$ we derive that

$$\prod_{i=1}^{k}(1-g_i) = \prod_{i=1}^{k}\sum_{j=1}^{r}(f_{ij}(1-x_j) + h_{ij}(1-x_j)^2),$$

and it follows from (3)–(5) that

$$\prod_{i=1}^{k}(1-g_i) = c_0\prod_{i=1}^{r}\sum_{j=0}^{p^{e_i}-1} x_i^j + \sum_{i=1}^{r} c_i\Big(\sum_{v=1}^{p^{e_i}-1} v x_i^{v-1}\Big)\prod_{\substack{j=1\\ j\neq i}}^{r}\sum_{v=0}^{p^{e_j}-1} x_j^v \tag{6}$$

where $c_i \in F_p$.

For every $g \in H$, write $g = x_1^{\tau_1(g)}\dots x_r^{\tau_r(g)}$. Then from (6) we derive that

$$\prod_{i=1}^{k}(1-g_i) = \sum_{g\in H}(c_0 + c_1(\tau_1(g)+1) + \dots + c_r(\tau_r(g)+1))g.$$

This together with (2) implies

$$N(S,g) = \sum_{i=1}^{r} c_i\tau_i(g) + \sum_{i=0}^{r} c_i.$$

Now by the hypothesis of the lemma we have

$$\sum_{i=0}^{r} c_i = N(S,1) = f_{\mathrm{E}}(S) - f_{\mathrm{O}}(S) \neq 0 \quad \text{(in } F_p).$$

It follows that all elements g not in $\sum(S)$ satisfy the equation

$$\sum_{i=1}^{r} c_i\tau_i(g) = -\sum_{i=0}^{r} c_i \neq 0,$$

and this equation defines a proper coset. This completes the proof.

Lemma 11. *Let p be an odd prime, and let $A = A_1\dots A_r \in B_1(C_p^2)$ with $A_1,\dots,A_r$ irreducible blocks. Suppose that $|A| = 2p+t$ and $t \geq 1$. Then at least $4+t$ of $|A_1|,\dots,|A_r|$ are odd.*

Proof. Suppose that exactly l of $|A_1|,\dots,|A_r|$ are odd. Then $l \geq 2+t$ follows from Proposition 1 and Lemma 4(iv).

Assume the conclusion of the lemma is false. Then $l = 2+t$ follows from the obvious fact $l \equiv 2p+t \equiv t \pmod 2$. Without loss of generality, we may assume that $|A_1|,\dots,|A_{2+t}|$ are odd and that $|A_{3+t}|,\dots,|A_r|$ are even. We next show that

$$p \mid |A_1|.$$

We fix $a_i \in A_i$ for $i = 1, \dots, 2+t$, take any $x \in A_1 - (a_1)$, and set

$$S = (A_1 - (a_1, x))(A_2 - (a_2)) \dots (A_{2+t} - (a_{2+t}))A_{3+t} \dots A_r.$$

Clearly, $f_{\mathrm{E}}(S) = 2^{r-2-t}$, $f_{\mathrm{O}}(S) = 0$, $|S| = 2p - 3 = D(C_p^2) - 2$, and

$$\{-a_1, -a_1 - a_2, \dots, -a_1 - a_{2+t}, -x, -x - a_2, \dots, -x - a_{2+t}\} \cap \sum(S) = \emptyset.$$

Now it follows from Lemma 10 that there exist a subgroup H of C_p^2 and an element $g \in C_p^2 - H$ such that

$$\{-a_1, -a_1 - a_2, \dots, -a_1 - a_{2+t}, -x, -x - a_2, \dots - x - a_{2+t}\} \subset g + H.$$

This implies that $x - a_1 = (-a_1) - (-x) \in H, a_2 = (-a_1) - (-a_1 - a_2) \in H$, so we have $H = \langle a_2 \rangle$. Since x was arbitrary, any element of A_1 is in $a_1 + H = g + H$. Now $|A_1|(g + H) = 0$ (in C_p^2/H) follows from $\sum A_1 = 0$; but $g + H \neq 0$ (in C_p^2/H), hence, $p \mid |A_1|$. Similarly, one can prove that $p \mid |A_2|, \dots, p \mid |A_{2+t}|$. This yields $|A| \geq |A_1| + \dots + |A_{2+t}| \geq (2+t)p > 2p + t$, a contradiction. This completes the proof.

LEMMA 12. *Let p be a prime with $2 \leq p \leq 151$. Then $a_1(C_p^2) = 2p$.*

Proof. We may assume that $p \geq 5$; for $p \leq 3$ see [9].

Assume to the contrary that $a_1(C_p^2) \neq 2p$. Then one can find a block $A = A_1 \dots A_r \in B_1(C_p^2)$ with $|A| = 2p + t$ and $t \geq 1$, where $A_1, \dots, A_r$ are irreducible blocks. Suppose exactly l of $|A_1|, \dots, |A_r|$ are odd. Then $l \geq 4 + t$ follows from Lemma 11.

If $p = 5$, then $2 \times 5 + t = |A| \geq 3l \geq 3(4 + t) > 10 + t$, a contradiction. Hence, $7 \leq p \leq 151$ and it follows from $l \geq 4 + t \geq 5$ that $|A_1| \dots |A_r| \geq 3^4(2p + 1 - 12) = 162(p - 5.5) > p^2$, a contradiction to Lemma 2. This completes the proof.

LEMMA 13. $a_1(C_{5^s}^2) = 2 \times 5^s$.

Proof. We proceed by induction on s. If $s = 1$, then the assertion follows from Lemma 12.

Taking $s \geq 2$ we assume that the lemma is true for $s - 1$. Assume to the contrary that $a_1(C_{5^s}^2) \neq 2 \times 5^s$. Then one can find a block $A = A_1 \dots A_r \in B_1(C_{5^s}^2)$ with $|A| = 2 \times 5^s + t$ and $t \geq 1$, where $A_1, \dots, A_r$ are irreducible blocks. By Proposition 1, at least three of $|A_1|, \dots, |A_r|$ are odd. If $\max\{|A_1|, \dots, |A_r|\} < 9 \times 5^{s-1}$, then by Lemma 9 we have $|A_1| \dots |A_r| \geq 3 \times (5^{s-1} - 1)(9 \times 5^{s-1} - 1) > (5^s)^2 = |C_{5^s}^2|$. This contradicts Lemma 2 and shows that $\max\{|A_1|, \dots, |A_r|\} \geq 9 \times 5^{s-1}$. Note $D(C_5^2) = 9$ and similarly to the proof of Proposition 3 one can derive a contradiction. So we complete the proof.

Proof of Theorem 1. Obviously, (1)–(7) follow from Corollary 1, Lemma 12, Lemma 13, Lemma 4 and Proposition 2. So to prove the theorem we only need to consider (8)–(12).

(8) We only consider the case of $t=1$; one can deal with the case of $t=0$ similarly. Assume to the contrary that $a_1(C_2^n \oplus C_4 \oplus C_{2^m}) \neq 2n+4+2^m$. Then one can find a block $A = A_1 \ldots A_r \in B_1(C_2^n \oplus C_4^t \oplus C_{2^m})$ with $|A| = 2n+4+2^m+t$ and $t \geq 1$, where $A_1, \ldots, A_r$ are irreducible blocks. It follows from Lemma 3 that $r \geq n+3$ and this implies that $|A_1| \ldots |A_r| \geq 2^{n+2}(2^m+1) > |C_2^n \oplus C_4 \oplus C_{2^m}|$, a contradiction to Lemma 2.

(9) follows from Proposition 2, Lemma 4 and the conclusion of (8).

(10) As in (8) we only consider the case of $t=1$. Assume to the contrary that $a_1(C_3^n \oplus C_9 \oplus C_{3^m}) \neq 3n+9+3^m$. Then one can find a block $A = A_1 \ldots A_r \in B_1(C_2^n \oplus C_9 \oplus C_{3^m})$ with $|A| = 3n+9+3^m+t$ and $t \geq 1$, where $A_1, \ldots, A_r$ are irreducible blocks. It follows from Proposition 1 that at least $n+3$ of $|A_1|, \ldots, |A_r|$ are odd. This implies that $|A_1| \ldots |A_r| \geq 3^{n+3}(3^m+1) > |C_3^n \oplus C_9 \oplus C_{3^m}|$, a contradiction to Lemma 2.

(11) follows from Proposition 2, Lemma 4 and the conclusion of (10).

(12) The proof is similar to that of (10) and we omit it here. Now the proof is complete.

3. In this section we consider $a_k(G)$ with $k \geq 2$.

PROPOSITION 4. *Let $B \in B_2(G) - B_1(G)$, and let $B = \prod_{i=1}^{r_i} B_{i_j}, i = 1, 2$, be the two strongly inequivalent irreducible factorizations of B, where $B_{i_j}, 1 \leq i \leq 2$, $1 \leq j \leq r_i$, are all irreducible blocks. Then*

$$|B| \leq \max\{r_1, r_2\} + D(G) - 1.$$

P r o o f. Suppose $r_1 \geq r_2$ and $B = (b_1, \ldots, b_k)$. Put $E_j = I_{B_{1_j}}$ for $j = 1, \ldots, r_1$ and $F_j = I_{B_{2_j}}$ for $j = 1, \ldots, r_2$. We have $B_{1_j} = (b_i : i \in E_j)$ and $B_{2_j} = (b_i : i \in F_j)$.

For $j = 1, \ldots, r_2$, we define D_j to be the set $\{i : E_i \cap F_j \neq \emptyset,\ 1 \leq i \leq r_1\}$. We assert that

$$D_1, \ldots, D_{r_2} \text{ has a system of distinct representatives.}$$

Deny the assertion; by Hall's Theorem ([5], p. 45) there exists a nonempty subset $\{i_1, \ldots, i_t\}$ of $\{1, \ldots, r_2\}$ such that

$$|D_{i_1} \cup \ldots \cup D_{i_t}| < t.$$

Suppose $D_{i_1} \cup \ldots \cup D_{i_t} = \{f_1, \ldots, f_m\}$. Then $m < t$. By the definition of D_j, $1 \leq j \leq r_2$, we have

$$F_{i_1} \cup \ldots \cup F_{i_t} \subseteq E_{f_1} \cup \ldots \cup E_{f_m}.$$

Set $E = (E_{f_1} \cup \ldots \cup E_{f_m}) - (F_{i_1} \cup \ldots \cup F_{i_t})$ and $B_0 = (b_i : i \in E)$. Clearly, B_0 is a block or the empty sequence, and we have

$$B = B_0 B_{2_{i_1}} \ldots B_{2_{i_t}} \prod_{l \neq f_1, \ldots, f_m} B_{1_l}.$$

This implies that B can be factored into a product of at least $r_1 - m + t > r_1$ irreducible blocks. Obviously, such an irreducible factorization is not strongly equivalent to $B = \prod_{j=1}^{r_1} B_{1_j}$ or $B = \prod_{j=1}^{r_2} B_{2_j}$, a contradiction to $B \in B_2(G)$. This proves the assertion.

Let $\{s_1, \ldots, s_{r_2}\}$ be a system of distinct representatives of $D_1, \ldots, D_{r_2}$. Then $F_j \cap E_{s_j} \neq \emptyset$, $j = 1, \ldots, r_2$. Take $u_i \in E_i$ for $i = 1, \ldots, r_1$ so that $u_{s_j} \in F_j \cap E_{s_j}$ for $j = 1, \ldots, r_2$. Put $M = \{1, \ldots, k\} - \{u_1, \ldots, u_{r_1}\}$. Clearly, no nonempty subset of M can be expressed as a union of some E_i or as a union of some F_i. This implies that for any nonempty subset W of M, the sequence $(b_i : i \in W)$ is not a block, so $|M| \leq D(G) - 1$ and $|B| = |M| + r_1 \leq r_1 + D(G) - 1$. This completes the proof.

COROLLARY 2. *$a_2(C_2^n) = 2n$.*

Proof. Since it is proved in [9] that $a_1(C_2^n) = 2n$, we have $a_2(C_2^n) \geq a_1(C_2^n) = 2n$.

To prove the upper bound we consider any $B \in B_2(C_2^n)$ and show that $|B| \leq 2n$.

If $B \in B_1(C_2^n)$, the estimate is trivial.

If $B \in B_2(C_2^n) - B_1(C_2^n)$, suppose $B = \prod_{i=1}^{r_i} B_{i_j}, i = 1, 2$, are the two strongly inequivalent irreducible factorizations of B, where $B_{i_j}, 1 \leq i \leq 2, 1 \leq j \leq r_i$, are irreducible blocks. We assume without loss of generality that $r_1 \geq r_2$. It follows from Proposition 4 that $D(C_2^n) + r_1 - 1 \geq |B| = \sum_{j=1}^{r_1} |B_{1_j}| \geq 2r_1$, thus, $r_1 \leq D(C_2^n) - 1$, and $|B| \leq 2(D(C_2^n) - 1) = 2n$ by Lemma 4(iv). This completes the proof.

LEMMA 14. *Let $B \in B_k(G) - B_{k-1}(G)$ with $k \geq 2$, and let $B = \prod_{j=1}^{r_i} B_{i_j}, i = 1, \ldots, k$, be the k strongly inequivalent irreducible factorizations of B, where $B_{i_j}, 1 \leq i \leq k, 1 \leq j \leq r_i$ are irreducible blocks. Suppose that $r_1 = \max\{r_1, \ldots, r_k\} \geq k$. Then there exists a subset X of $\{1, \ldots, r_1\}$ such that $\prod_{j \in X} B_{1_j} \in B_1(G)$ and $|X| \geq r_1 - k + 1$.*

Proof. Clearly, for any $i = 2, \ldots, k$ there exists an $f = f(i)$ such that $I_{B_{1_f}} \neq I_{B_{i_t}}$ for any $t = 1, \ldots, r_i$. Put $Y = \bigcup_{2 \leq i \leq k} \{f(i)\}$. Then $|Y| \leq k - 1$. Set $X = \{1, \ldots, r_1\} - Y$. Clearly, $\prod_{j \in X} B_{1_j} \in B_1(G)$ and $|X| \geq r_1 - k + 1$. This completes the proof.

LEMMA 15. *Let G be a finite abelian group of order n, let $B \in B_k(G) - B_{k-1}(G)$ with $k \geq 2$, and let $B = \prod_{j=1}^{r_i} B_{i_j}, i = 1, \ldots, k$, be the k strongly inequivalent irreducible factorizations of B, where $B_{i_j}, 1 \leq i \leq k, 1 \leq j \leq r_i$, are irreducible blocks. Then*

$$\max\{r_1, \ldots, r_k\} \leq k - 1 + \log_2 n.$$

Proof. Without loss of generality, assume that $r_1 = \max\{r_1, \ldots, r_k\} \geq k$. By using Lemma 14 one can find a subset X of $\{1, \ldots, r_1\}$ such that $\prod_{j\in X} B_{1_j} \in B_1(G)$ and $|X| \ge r_1 - k + 1$. Now $\prod_{j\in X} |B_{1_j}| \le n$ follows from Lemma 2. Note that all $|B_{1_j}| \ge 2$, we have $|X| \le \log_2 n$, and $r_1 \le k - 1 + \log_2 n$ follows. This completes the proof.

Proof of Theorem 2. Assume to the contrary that $a_k(C_n) \ne n$. Since $a_k(C_n) \ge a_{k-1}(C_n) \ge \ldots \ge a_1(C_n) = n$, we have $a_k(C_n) = n+1+t$ for some $t \ge 0$. Let $B \in B_k(C_n)$ with $|B| = n+1+t$. Since $a_1(C_n) = n$, we must have $B \in B_m(C_n) - B_{m-1}(C_n)$ for some $2 \le m \le k$. Let $B = \prod_{j=1}^{r_i} B_{i_j}, 1 \le i \le m$, be the m strongly inequivalent irreducible factorizations of B, where $B_{i_j}, 1 \le i \le m, 1 \le j \le r_i$, are irreducible blocks.

Suppose $B = (b_1, \ldots, b_s)$. Put $E_{i_j} = I_{B_{i_j}}$ for $i = 1, \ldots, m$ and $j = 1, \ldots, r_i$. For $j = 1, \ldots, r_2$, we define D_j to be the set $\{t : E_{1_t} \cup E_{2_j} \ne \emptyset, 1 \le t \le r_1\}$. Similarly to the proof of Proposition 4 one can show that $D_1, \ldots, D_{r_2}$ has a system of distinct representatives. Therefore one can find an r_1-subset of $\{1, \ldots, s\}$ which meets all E_{1_j} and all E_{2_j}. Hence, one can find an $(r_1 + r_3 + \ldots + r_k)$-subset I of $\{1, \ldots, s\}$ such that $I \cap E_{i_j} \ne \emptyset$ for $i = 1, \ldots, m$ and $j = 1, \ldots, r_i$. Put $J = \{1, \ldots, s\} - I$ and let T be the subsequence of B with $I_T = J$. Clearly, T contains no nonempty zero-sum subsequence. Put $l = n - |T|$. Notice that

$$\begin{aligned} l &= n - |T| = n - |J| = n - (n + 1 + t - |I|) \le |I| - 1 \\ &= r_1 + r_3 + \ldots + r_m - 1 \le (m-1)r_1 - 1 \\ &\le (m-1)(m-1+\log_2 n) - 1 \qquad \text{(by Lemma 15)} \\ &\le (k-1)(k-1+\log_2 n) \le n/4 \qquad \text{(by the hypothesis of the theorem)}, \end{aligned}$$

so by using Lemma 8 we see that, T contains an $(n-2l+1)$-subsequence which is similar to the sequence $(\underbrace{1, \ldots, 1}_{n-2l+1})$. Therefore, B contains an $(n-2l+1)$-subsequence which is similar to the sequence $(\underbrace{1, \ldots, 1}_{n-2l+1})$; without loss of generality, we may assume that

$$B = (\underbrace{1, \ldots, 1}_{n-2l+1}, x_1, \ldots, x_{t+2l}).$$

If $|x_i|_n \ge 2l$, since $(\underbrace{1, \ldots, 1}_{n-|x_i|_n}, x_i)$ is an irreducible block and

$$\binom{n-2l+1}{n-|x_i|_n} \ge n - 2l + 1 \ge n/2 + 1 > k$$

(from the hypothesis of the theorem), we must have $B \notin B_k(C_n)$, a contradiction. Hence,

$$1 \le |x_i|_n \le 2l - 1$$

for $i = 1, \dots, t + 2l$, and so $2 \le |x_1|_n + |x_2|_n \le 4l - 2 \le n - 2$, hence, $2 \le |x_1 + x_2|_n = |x_1|_n + |x_2|_n \le n - 2$.

If $|x_1 + x_2|_n \ge 2l$, since $(\underbrace{1, \dots, 1}_{n - |x_1 + x_2|_n}, x_1, x_2)$ is an irreducible block and

$$\binom{n - 2l + 1}{n - |x_1 + x_2|_n} \ge n - 2l + 1 > k,$$

we have $B \notin B_k(G)$, a contradiction. Hence, $|x_1|_n + |x_2|_n = |x_1 + x_2|_n \le 2l - 1$. Continuing the same process we finally get

$$\sum_{i=1}^{2l+t} |x_i|_n = \Big|\sum_{i=1}^{2l+t} x_i\Big|_n \le 2l - 1;$$

but

$$\sum_{i=1}^{2l+t} |x_i|_n \ge 2l + t \ge 2l,$$

a contradiction. This completes the proof.

Acknowledgements. The author is grateful to the referee for helpful suggestions and comments.

REFERENCES

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

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

[3] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups III*, ZW-1969-008, Math. Centre, Amsterdam.

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

[5] M. Hall Jr., *Combinatorial Theory*, Blaisdell, London, 1967.

[6] F. Halter-Koch, *Typenhalbgruppen und Faktorisierungsprobleme*, Results Math. 22 (1992), 545–549.

[7] —, *Factorization problems in class number two*, Colloq. Math. 65 (1993), 255–265.

[8] W. Narkiewicz, *Finite abelian groups and factorization problems*, ibid. 42 (1979), 319–330.

[9] W. Narkiewicz and J. Śliwa, *Finite abelian groups and factorization problems II*, ibid. 46 (1982), 115–122.

[10] J. E. Olson, *A combinatorial problem on finite abelian groups I*, J. Number Theory 1 (1969), 8–10.

[11] —, *A combinatorial problem on finite abelian groups II*, ibid. 1 (1969), 195–199.

Department of Information Engineering
Beijing University of Posts and Telecommunications
Beijing 100088, China
E-mail: zmhu@bupt.edu.cn

Received 9 March 1995;
revised 10 February 1996