# UPPER BOUNDS FOR THE DAVENPORT CONSTANT 

R. Balasubramanian<br>Institute of Mathematical Sciences, C.I.T. Campus, Taramani, Chennai 600 113, India. balu@imsc.res.in<br>Gautami Bhowmik<br>Université de Lille 1, UMR CNRS 8524,59655 Villeneuve d’Ascq Cedex, France. bhowmik@math.univ-lille1.fr

Received: 1/5/06, Accepted: 4/4/06


#### Abstract

We prove that for all but a certain number of abelian groups of order $n$ the Davenport constant is at most $\frac{n}{k}+k-1$ for positive integers $k \leq 7$. For groups of rank three we improve on the existing bound involving the Alon-Dubiner constant.


## 1. Introduction

Let $G$ be an abelian group of order $n$. A sequence of elements (not necessarily distinct) of $G$ is called a zero sum sequence of $G$ if the sum of its components is 0 . The zero-sum constant $Z S(G)$ of $G$ is defined to be the smallest integer $t$ such that every sequence of length $t$ of $G$ contains a zero-sum subsequence of length $n$, while the Davenport constant $D(G)$ is the smallest integer $d$ such that every sequence of length $d$ of $G$ contains a zero-sum subsequence.

The study of the zero-sum constant dates back to the Erdös-Ginzburg-Ziv theorem of 1961 [EGZ]. On the other hand Davenport in 1966 introduced $D(G)$ as the maximum possible number of prime ideals (with multiplicity) in the prime ideal decomposition of an irreducible element of the ring of integers of an algebraic number field whose ideal class group is $G$. More recently, Gao [G] proved that these two constants are closely related, i.e., $Z S(G)=|G|+D(G)-1$. It is thus enough to study any one of these constants.

Apart from their interest in zero sum problems of additive number theory and non-unique
factorisations in algebraic number theory, these constants play an important role in graph theory (see, e.g., [Ch]). However their determination is still an open problem.

We consider the cyclic decomposition of a group of rank $r$, i.e., $G \sim \mathbb{Z}_{d_{1}} \oplus \mathbb{Z}_{d_{2}} \oplus \cdots \oplus \mathbb{Z}_{d_{r}}$, where $d_{i}$ divides $d_{i+1}$. It is clear that $M(G)=1+\sum_{i=1}^{r}\left(d_{i}-1\right)$ is a lower bound for $D(G)$.

It was proved that $D(G)=M(G)$ for $p$ groups and for groups of rank 1 or 2 , independently by Olson [O] and Kruswijk [B1] and the equality is also known to hold for several other groups. Olson and Baayen both conjectured that the equality holds for all finite abelian groups. The conjecture however turned out to be false. Geroldinger and Schneider [GS] in 1992 in fact showed that for all groups of rank greater than 3 , there exist infinitely many cases where $D(G)>M(G)$.

As far as upper bounds are concerned, the Erdös-Ginzburg-Ziv theorem that asserts that for a finite abelian group of order $n, Z S(G) \leq 2 n-1$ [EGZ] has been improved. Alon, Bialostocki and Caro [cited in OQ] proved that $Z S(G) \leq 3 n / 2$ if $G$ is non-cyclic. Caro improved this bound to $Z S(G) \leq 4 n / 3+1$ if $G$ is neither cyclic nor of the form $\mathbb{Z}_{2} \oplus \mathbb{Z}_{2 t}$. On excluding $\mathbb{Z}_{3} \oplus \mathbb{Z}_{3 t}$ as well, Ordaz and Quiroz [OQ] tightened the bound to $5 n / 4+2$. It is easy to see that though it is true for $k=1,2,3$ and 4 ; for a general positive integer $k$ we cannot say that $D(G) \leq \frac{n}{k}+(k-1)$ whenever $G$ is not of the form $\mathbb{Z}_{u} \oplus \mathbb{Z}_{u t}, u<k$.

On the other hand, Alford, Granville and Pomerance [AGP] in 1994 used the bound $D(G) \leq$ $m\left(1+\log \frac{n}{m}\right)$, where $m$ is the exponent of $G$, to prove the existence of infinitely many Carmichael numbers.

In this paper, we combine the two types of upper bounds to prove that

Theorem. If $G$ is an abelian group of order $n$ and exponent $m$, then for $k \leq 7$, its Davenport constant $D(G) \leq \frac{n}{k}+(k-1)$ whenever $\frac{n}{m} \geq k$.

Thus when the ratio $\frac{n}{m}$ is small, we get an improvement on the [AGP] bound.

We expect the above result to be true for all $k \leq \sqrt{n}$.
To study the Davenport constant, it is sometimes useful to use another constant $D^{s}(G)$ which is the smallest integer $t$ such that every sequence of $G$ with length $t$ contains a zero sum subsequence of length atmost $s$.

Olson calculated $D^{p}\left(\mathbb{Z}_{p} \oplus \mathbb{Z}_{p}\right)$ for a prime number $p$ and used it to determine $D(G)$ for the rank 2 case. As yet, no precise result is known for $D^{p}\left(\mathbb{Z}_{p}^{r}\right)$ for $r \geq 3$. But Alon and Dubiner $[\mathrm{AD}]$ proved a remarkable bound in 1995, i.e., $D^{p}\left(\mathbb{Z}_{p}^{r}\right) \leq c(r) p$. In fact $c(r)$ can be taken to be $(c r \log r)^{r}$ where $c$ is an absolute constant. Dimitrov [D] used the Alon Dubiner constant to prove that $D(G) \leq M(G)(K r \log r)^{r}$ for an absolute constant $K$. In the general case we
have only a slight improvement of Dimitrov's result. It is for the rank 3 case that our result is interesting.

Theorem. If $G \sim \mathbb{Z}_{a_{1}} \oplus \mathbb{Z}_{a_{1} a_{2}} \oplus \mathbb{Z}_{a_{1} a_{2} a_{3}}$, we have

$$
D(G) \leq M(G)\left(1+\frac{K}{a_{2} a_{3}}\right)
$$

where $K$ is a constant of the same order of magnitude as that obtained by Alon-Dubiner.
At the end we give an elementary proof of a result of Alon Dubiner that helped them obtain the bound for $D^{p}\left(\mathbb{Z}_{p}^{r}\right)$.

## 2. A General Bound

We first prove a lemma which would help us find bounds for the Davenport constant when reasonable bounds can be found for $D^{s}(G)$ and when $D\left(\mathbb{Z}_{s}^{3}\right)$ can be calculated, for example when $s$ is a power of a prime.

Lemma 1. Let $D^{s}\left(\mathbb{Z}_{s}^{3}\right) \leq A, u=\left[\frac{A-s}{D\left(\mathbb{Z}_{s}^{3}\right)}\right]$, and let

$$
h=h_{a, b}= \begin{cases}D\left(\mathbb{Z}_{a} \oplus \mathbb{Z}_{a b}\right), & a \neq 1 \\ D\left(\mathbb{Z}_{b}\right) & , a=1\end{cases}
$$

Then, if $h \geq u+1$,

$$
D\left(\mathbb{Z}_{s} \oplus \mathbb{Z}_{s a} \oplus \mathbb{Z}_{s a b}\right) \leq B\left(h_{a, b}\right)
$$

where $B\left(h_{a, b}\right)=\left(h_{a, b}-u-1\right) s+A$.
Proof. Let $S$ be a set of $B(h)$ elements of $\mathbb{Z}_{s} \oplus \mathbb{Z}_{s a} \oplus \mathbb{Z}_{s a b}$. Every sequence of length atleast $D^{s}\left(\mathbb{Z}_{s} \oplus \mathbb{Z}_{s} \oplus \mathbb{Z}_{s}\right)$ contains a zero sum subsequence of length atmost $s$. Thus $B(h)$ contains one zero sum subsequence of length atmost $s$. On removing this zero sum sequence, we would still have more than $D^{s}\left(\mathbb{Z}_{s}^{3}\right)$ elements left in $B(h)$. Thus there exist disjoint subsets $A_{1}, A_{2}, \cdots A_{h-u-1}$ in $S$ such that $\left|A_{j}\right| \leq s$ and the sum of the elements of $A_{j}$ is $(0,0,0)$ in $\mathbb{Z}_{s}^{3}$. If these sets are removed from $B(h)$, we still have more than $B(h)-(h-u-1) s \geq D^{s}\left(\mathbb{Z}_{s}^{3}\right)$ elements from which we can extract another subset $A_{h-u}$ disjoint from the others of length $\leq s$ and still of sum $(0,0,0)$ in $D^{s}\left(\mathbb{Z}_{s}^{3}\right)$. Now

$$
B(h)-(h-u) s \geq A-s \geq u D\left(\mathbb{Z}_{p}^{3}\right)
$$

So we can extract $u$ more subsets $A_{h-u+1}, \cdots, A_{h}$ disjoint from the rest the sum of whose elements is still zero in $\mathbb{Z}_{s}^{3}$.

Thus we have $h$ disjoint subsets whose sum in $\mathbb{Z}_{s}^{3}$ is $(0,0,0)$, i.e., the sum is of the form $\left(a_{j} s, b_{j} s, c_{j} s\right)$. Suppose that $a \neq 1$ and for $j \leq h$ let $C_{j}=\left(b_{j}, c_{j}\right)$. Now $a_{j} s$ is 0 in $\mathbb{Z}_{s}$ and since we have taken the sum over $h$ sets, there exists a subcollection of $C_{j}$ whose sum is $(0,0)$ in $\mathbb{Z}_{a} \oplus \mathbb{Z}_{a b}$. The corresponding subcollection of $A_{j}$ will suit our purpose in $\mathbb{Z}_{s} \oplus Z_{s a} \oplus Z_{\text {sab }}$.

If $a=1$, we take $C_{j}=\left(c_{j}\right)$ and proceed as before.
To get precise bounds it is often necessary to actually evaluate $D\left(\mathbb{Z}_{s}^{3}\right)$ or at least find reasonable bounds. This is possible for small values of $s$ as follows :

Lemma 2. We have,

$$
D^{s}\left(Z_{s} \oplus \mathbb{Z}_{s} \oplus \mathbb{Z}_{s}\right)=\left\{\begin{array}{r}
8, s=2 \\
17, s=3 \\
22, s=4
\end{array}\right.
$$

Proof. The first two assertions can be verified directly. We notice that any 9 distinct elements in $\mathbb{Z}_{3}^{3}$ contain a zero sum subsequence. The third follows essentially from Harborth $[\mathrm{H}]$.

Sometimes we cannot find an effective bound for $D\left(\mathbb{Z}_{s}^{3}\right)$ but we might be able to use the following weaker bound which can be proved in the same way as Lemma 1.

Lemma 3. We have $D\left(\mathbb{Z}_{s^{a}}^{r-1} \oplus \mathbb{Z}_{s^{a} t}\right) \leq D\left(\mathbb{Z}_{s^{a}}^{r}\right) t$.
Theorem 1. If $G$ is an abelian group of order $n$ and exponent $m$, then for every positive integer $k \leq 7$, its Davenport constant $D(G)$ is atmost $\frac{n}{k}+(k-1)$ whenever $\frac{n}{m} \geq k$.

Proof. We notice that the exceptions to the bounds stated in the theorems of Erdös-GinzburgZiv [EGZ], Alon-Bialostocki-Caro [ABC], Caro [C] and Ordaz-Quiroz [OZ] can be reformulated as the cases where $\frac{n}{m} \geq k$ to assert our result for $k=1,2,3$ and 4 , respectively.

It is known [AGP] that

$$
D(G) \leq m\left(1+\log \frac{n}{m}\right)
$$

and the condition $m\left(1+\log \frac{n}{m}\right) \leq \frac{n}{k}+k-1$ is satisfied whenever $\frac{n}{m} \geq 31$ for $k=7$. Thus it suffices to examine the groups where $\frac{n}{m} \leq 31$.

Case 1: $\operatorname{rank}(G) \geq 5$.
We notice that for a group of rank greater than $5, \frac{n}{m}$ is always greater than 31. Let

$$
G \sim \mathbb{Z}_{a_{1}} \oplus \mathbb{Z}_{a_{1} a_{2}} \oplus \mathbb{Z}_{a_{1} a_{2} a_{3}} \oplus \mathbb{Z}_{a_{1} a_{2} a_{3} a_{4}} \oplus \mathbb{Z}_{a_{1} a_{2} a_{3} a_{4} a_{5}}
$$

Here $n=a_{1}^{5} a_{2}^{4} a_{3}^{3} a_{4}^{2} a_{5}$, and $m=a_{1} a_{2} a_{3} a_{4} a_{5}$. Since $a_{1} \geq 2, \frac{n}{m} \leq 31$ only when $a_{1}=2, a_{2}=$
$a_{3}=a_{4}=1$. Now, a result of [OQ] says that for any abelian group $K$,

$$
D\left(\mathbb{Z}_{2} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{2} \oplus K\right) \leq 2 D(K)+3
$$

Taking $K$ to be $\mathbb{Z}_{2} \oplus \mathbb{Z}_{2 t}$, we get $D(G) \leq 4 t+5 \leq \frac{32}{k} t+k-1$ for $k=5,6,7$.
Case $2: \operatorname{rank}(G)=4$.
The condition $\frac{n}{m}=a_{1}^{3} a_{2}^{2} a_{3}<31$ is satisfied only by groups of rank 4 of the form

$$
\begin{aligned}
& G_{1} \sim \mathbb{Z}_{2} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{2 t} \\
& G_{2} \sim \mathbb{Z}_{2} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{4} \oplus \mathbb{Z}_{4 t} \\
& G_{3} \sim \mathbb{Z}_{2} \oplus \mathbb{Z}_{2} \oplus \mathbb{Z}_{6} \oplus \mathbb{Z}_{6 t}
\end{aligned}
$$

and

$$
G_{4} \sim \mathbb{Z}_{3} \oplus \mathbb{Z}_{3} \oplus \mathbb{Z}_{3} \oplus \mathbb{Z}_{3 t}
$$

However, the first case satisfies the stronger condition of the Baayen-Olson conjecture, i.e., $D(G)=M(G)$. This was proved for odd $t$ [B2]. For even $t$ it follows from the fact that in this case

$$
G_{1}=H \oplus \mathbb{Z}_{p^{k} u}
$$

$H$ being a $p$-group and $p^{k} \geq M(H)$, a case that satisfies the BO conjecture [vE].
For $G_{2}$ we split it as a sum of two groups $H$ and $K$ and use the estimate (see eg [C]),

$$
D(H+K) \leq(D(H)-1)|K|+D(K)
$$

We take $H$ to be $\mathbb{Z}_{2} \oplus \mathbb{Z}_{4} \oplus \mathbb{Z}_{4 t}$. Then $D(H)=M(H)$ (see [vE]). Thus $D\left(G_{2}\right) \leq 8 t+8$ which is less than $\frac{n}{k}+k-1$ for all $t$ when $k=5$ and for $t>1$ when $k=6,7$. But for $t=1$ we have a p-group.

The same argument works for $G_{3}$. For $G_{4}$ we use Lemma 3 and get

$$
D\left(G_{4}\right) \leq 9 t \leq \frac{81}{7} t+6
$$

for $k=7$. Since $\frac{n}{m}=27$ the inequality is already satisfied by the AGP bound for $k=5,6$.
Case $3: \operatorname{rank}(G)=3$.
Since $a_{1}^{2} a_{2} \geq 31$ ensures that $D(G) \leq \frac{n}{k}+k-1$, and $\frac{n}{m} \geq k$ we are left with the cases $G_{5} \sim \mathbb{Z}_{2} \oplus \mathbb{Z}_{2 u} \oplus \mathbb{Z}_{2 u t}, 1<u<8, G_{6} \sim \mathbb{Z}_{3} \oplus \mathbb{Z}_{3 v} \oplus \mathbb{Z}_{3 v t}, v=1,2,3 ; G_{7} \sim \mathbb{Z}_{4} \oplus \mathbb{Z}_{4} \oplus \mathbb{Z}_{4 t}$ and $G_{8} \sim \mathbb{Z}_{5} \oplus \mathbb{Z}_{5} \oplus \mathbb{Z}_{5 t}$.

Now $G_{5}$ satisfies the BO conjecture. This follows from the fact that $u$ has no prime divisor greater than 11, which is a sufficient condition from a result of van Emde Boas [vE].

With $s=3, a=1, b=t$ in Lemmas 1 and 2, we obtain, for $k=5$ or 6 that

$$
D\left(\mathbb{Z}_{3} \oplus \mathbb{Z}_{3} \oplus \mathbb{Z}_{3 t}\right) \leq 3 t+8 \leq \frac{27}{k} t+k-1
$$

whenever $t \geq 2$.
When $t=1$, we have a $p$-group and the BO conjecture is satisfied.
For $k=7$ we know that for $\mathbb{Z}_{3} \oplus \mathbb{Z}_{3} \oplus \mathbb{Z}_{6}$ the BO condition is realized [vEK] and we are within the claimed bound. The same is true for the cases $v=2,3$ in $G_{6}[\mathrm{vE}]$. For $G_{7}$ we use Lemmas 1 and 2 with $s=4, a=1, b=t$ to obtain

$$
D\left(G_{7}\right) \leq 4 t+27 \leq \frac{64}{7} t+6
$$

for $t>4, k=7$. Lemma 3 gives the desired bound for $k=5$ or $6, t \leq 3, k=7$ in $G_{7}$ as well as for all cases of $G_{8}$.

Case 4: $\operatorname{rank}(G)=2$.
It is well known that $D(G)=a_{1}+a_{1} a_{2}-1$ and the inequation

$$
a_{1}+a_{1} a_{2}-1 \leq \frac{a_{1}^{2} a_{2}}{k}+k-1
$$

is always true for $a_{1}=\frac{n}{m} \geq k$.
Remark. This bound is tight, since $D\left(\mathbb{Z}_{k} \oplus \mathbb{Z}_{k t}\right)=k t+k-1$.
Conjecture. We believe that Theorem 1 is true for all $k \leq \sqrt{n}$. Notice that this is a weaker claim than the Narkiewicz-Śliwa conjecture that $D(G) \leq M(G)+r-1$ for a group of rank $r$.

## 3. Rank 3 Case

We now use the Alon-Dubiner theorem for improving the existing bound for the Davenport constant when the rank of the group is 3 which is [D]

$$
D(G) \leq K_{3} M(G),
$$

where $K_{3}$ is a constant of the same order of magnitude as that of Alon-Dubiner, and $M(G)=$ $a_{1} a_{2} a_{3}+a_{1} a_{2}+a_{1}-2$. Our method also gives a minor improvement for the higher rank cases.

INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 7(2) (2007), \#A03 7
We state a Lemma which can be seen as a generalisation of Olson's result for the rank 2 case.

Lemma 5. Let $d$ be a divisor of $a$ and let

$$
h= \begin{cases}D\left(\mathbb{Z}_{a / d} \oplus \mathbb{Z}_{a b / d} \oplus \mathbb{Z}_{a b c / d}\right) & , a \neq d \\ D\left(\mathbb{Z}_{b} \oplus \mathbb{Z}_{b c}\right) & , a=p, b \neq 1 \\ D\left(\mathbb{Z}_{c}\right) & , a=d, b=1, c \neq 1\end{cases}
$$

Then

$$
D\left(\mathbb{Z}_{a} \oplus \mathbb{Z}_{a b} \oplus \mathbb{Z}_{a b c}\right) \leq B(h)
$$

where $B(h)=(h-u-1) d+A$, and $A$ and $u$ are as defined in Lemma 1 .
Proof. Same as that of Lemma 1.
Theorem 2. Let $G \sim \mathbb{Z}_{a_{1}} \oplus \mathbb{Z}_{a_{1} a_{2}} \oplus \mathbb{Z}_{a_{1} a_{2} a_{3}}$. Then

$$
D(G) \leq a_{1} a_{2} a_{3}+a_{1} a_{2}+K a_{1}
$$

where $K$ is a constant of the same order of magnitude as that of Alon-Dubiner.
Proof. We use Lemma 3 above and the Alon Dubiner bound,

$$
D^{p}\left(\mathbb{Z}_{p}^{r}\right) \leq c(r) p,
$$

where $c(r)$ is a constant. In particular, for $r=3$, we write $D^{p}\left(\mathbb{Z}_{p}{ }^{3}\right) \leq(K+3) p$ with $(K+3) p \geq$ $7 p-4$. Thus $h p+K p \geq h p+4 p-4$.

For fixed $a_{2}, a_{3}$ we write $h\left(a_{1}\right)=D\left(\mathbb{Z}_{a_{1}} \oplus \mathbb{Z}_{a_{1} a_{2}} \oplus \mathbb{Z}_{a_{1} a_{2} a_{3}}\right)$.
Using Lemma 3 we see that if $p$ divides $a_{1}$,

$$
h\left(a_{1}\right) \leq h\left(\left(a_{1} / p\right)+K\right) p .
$$

Let $a_{1}=p_{1} p_{2} \cdots p_{t}$ with $p_{i} \geq p_{i+1}$. Thus

$$
h\left(p_{1} p_{2} \cdots p_{t}\right) \leq h\left(\left(p_{2} \cdots p_{t}\right)+K\right) p .
$$

Repeating the above process we get

$$
h\left(a_{1}\right) \leq a_{1} h(1)+K\left(p_{1} p_{2} \cdots p_{t}+p_{1} p_{2} \cdots p_{t-1}+\cdots+p_{1}\right)
$$

But

$$
p_{1} p_{2} \cdots p_{t}+p_{1} p_{2} \cdots p_{t-1}+\cdots+p_{1}=a_{1}\left(1+\frac{1}{p_{t}}+\frac{1}{p_{t} p_{t-1}}+\cdots+\frac{1}{p_{t} p_{t-1} \cdots p_{2}}\right) \leq 2 a_{1} .
$$

This gives $D\left(\mathbb{Z}_{a_{1}} \oplus \mathbb{Z}_{a_{1} a_{2}} \oplus \mathbb{Z}_{a_{1} a_{2} a_{3}}\right) \leq a_{1} D\left(\mathbb{Z}_{a_{2}} \oplus \mathbb{Z}_{a_{2} a_{3}}\right)+2 K a_{1}$, i.e.,

$$
D\left(\mathbb{Z}_{a_{1}} \oplus \mathbb{Z}_{a_{1} a_{2}} \oplus \mathbb{Z}_{a_{1} a_{2} a_{3}}\right) \leq a_{1} a_{2} a_{3}+a_{1} a_{2}+(2 K-1) a_{1}
$$

Remark. For the case of a general $r$ we get $D(G) \leq M(G)\left(1+\frac{K_{r}}{a_{r-1} a_{r}}\right)$ and the improvement from the existing bound comes into the picture only when $a_{r-1}$ and $a_{r}$ are large.

The proof of Theorem 2 uses an inequality of [Proposition 2.4, AD]. Here we give a slightly improved constant for the inequality. The proof goes along the same lines as [AD] but uses no graph theory. We include it here for the sake of completion.

Theorem 3. Let $A$ be a subset of $\mathbb{Z}_{p}^{d}$ such that no hyperplane contains more than $|A| / 4 W$ elements of $A$. Then for all subsets $Y$ of $\mathbb{Z}_{p}^{d}$ containing at most $p^{d} / 2$ elements, there is an element $a \in A$ such that

$$
|(a+Y) \backslash Y| \geq \frac{W}{5 p}|Y|
$$

Proof. If possible, let there exist no such $a$. Then $L(a)=|(a+Y) \backslash Y| \leq \frac{W}{5 p}|Y|$ for all $a \in A$. Since $L(j a) \leq j L(a)$, we get $L(j a) \leq \frac{j W}{5 p}|Y|$ for all $j \leq p / W$.

This gives

$$
M(j a)=L(j a)+L(-j a) \leq \frac{2 j W}{5 p}|Y| .
$$

Let $J=\left[\frac{p}{W}\right]$. Then

$$
S=\sum_{a} \sum_{1 \leq j \leq J} M(j a) \leq J(J+1) \frac{W}{5 p}|Y||A| .
$$

On the other hand we shall get a lower bound for $S$. For any $b$ define

$$
T(b)=\frac{1}{|G|} \sum_{x}\left(1-l^{\bar{b} \cdot \bar{x}}\right)\left|\sum_{y} l^{\bar{x} \cdot \bar{y}}\right|^{2},
$$

where for notational convenience we write $l$ for $e^{\frac{2 i \pi}{p}}$ and $G$ for the group $\mathbb{Z}_{p}^{d}$.
Then

$$
\begin{aligned}
& T(b)=\frac{1}{|G|} \sum_{x}\left(1-l^{\bar{b}} \cdot \bar{x}\right) \sum_{y_{1}, y_{2}} l^{\bar{x} .\left(\bar{y}_{1}-\bar{y}_{2}\right)} . \\
& =\frac{1}{|G|} \sum_{y_{1}, y_{2}}\left(\sum_{x} l^{\bar{x} \cdot\left(\bar{y}_{1}-\bar{y}_{2}\right)}-\sum_{x} l^{\bar{x} \cdot\left(\bar{y}_{1}-\bar{y}_{2}-\bar{b}\right)}\right) .
\end{aligned}
$$

$$
=B-D
$$

Clearly $B=|Y|$ and $D$ is the number of solutions of the equation $\bar{y}_{1}-\bar{y}_{2}=\bar{b}$ which is the same as $(b+Y) \cap Y$.

Thus, $B-D=|(b+Y) \backslash Y|=L(b)$. Thus,

$$
\begin{aligned}
M(j a)=L(j a)+L(-j a) & =T(j a)+T(-j a)=\sum_{x}\left(2-l^{j \bar{a} \cdot \bar{x}}-l^{-j \bar{a} \cdot \bar{x}}\right)\left|\sum_{y} l^{\bar{x} \cdot \bar{y}}\right|^{2} \\
= & \frac{4}{|G|} \sum_{x} \sin ^{2}\left(\frac{\pi}{p} j \bar{a} \cdot \bar{x}\right)\left|\sum_{y} l^{\bar{x} \cdot \bar{y}}\right|^{2} .
\end{aligned}
$$

Then

$$
\begin{gathered}
S=\frac{4}{|G|} \sum_{x \neq 0} \sum_{a} \sum_{j} \sin ^{2}\left(\frac{\pi}{p} j \bar{a} \cdot \bar{x}\right)\left|\sum_{y} l^{\bar{x} \cdot \bar{y}}\right|^{2} \\
\geq \frac{4}{|G|} \sum_{x \neq 0} R\left|\sum_{y} l^{\bar{x} \cdot \bar{y}}\right|^{2},
\end{gathered}
$$

where $R$ is a minorization of $\sum_{a} \sum_{j} \sin ^{2}\left(\frac{\pi}{p} j \bar{a} \cdot \bar{x}\right)$ for $x \neq 0$.
We then have

$$
\begin{gathered}
S \geq \frac{4 R}{|G|} \sum_{x \in G}\left|\sum_{y} l^{\bar{x} \cdot \bar{y}}\right|^{2}-\frac{4 R}{|G|} \sum_{x=0}\left|\sum_{y} l^{\bar{x} \cdot \bar{y}}\right|^{2} \\
\geq 4 R|Y|-\frac{4 R}{|G|}|Y|^{2} \geq 2 R|Y|,
\end{gathered}
$$

since $|Y| \leq \frac{|G|}{2}$. On the other hand, to get a lower bound for $R$ we note that the least value is obtained by taking $j \bar{a} \cdot \bar{x}$ as small as possible. Thus the condition that no hyperplane contains more than $\frac{|A|}{4 W}$ elements implies that $\bar{a} \cdot \bar{x} \geq W$ for atleast $\frac{|A|}{2}$ values of $a$. Considering only these values, we have $R \geq \frac{|A||J|}{8}$ and $S \geq \frac{|A||J|}{4}|Y|$. This gives a contradiction.

## References

[ABC] "Extremal zero sum problem" N. Alon, A. Bialostocki \& Y . Caro Manuscript, cited in [OQ] .
[AD] "A Lattice Point Problem and Additive Number Theory" N. Alon \& M. Dubiner Combinatorica 15 (1995), pages 301-309.
[AGP] "There are infinitely many Carmichael numbers" W.R. Alford, A. Granville \& C . Pomerance Annals of Math (1994), pages 703-722.
[B1] "Een combinatorisch probleem voor eindige Abelse groepen" P.C Baayen Colloq. Discrete Wiskunde Caput 3, Math Centre, Amsterdam (1968).
[B2] " $\left(C_{2} \oplus C_{2} \oplus C_{2} \oplus C_{2 n}\right)$ ! Is True for Odd n" P.C Baayen Report ZW-1969-006, Math Centre, Amsterdam (1969) .
[C] "On zero sum subsequences in abelian non-cyclic groups" Y. Caro Israel Jour. of Math 92 (1995), pages 221-233.
[Ch] "On the Davenport Constant, the Cross Number, and their Application in Factorization Theory" ST. Chapman Lecture Notes in Pure and Applied Maths,Dekker, eds Anderson \& Dobbs 171 (1995) , pages 167-190.
[D] "Zero-sum problems in finite groups" V. Dimitrov (2003).
[EGZ] "Theorem in Additive Number Theory" P. Erdös,A. Ginzburg \& A. Ziv Bull. Research Council Israel 10 (1961) , pages 41-43.
[G] "Addition theorems for finite abelian groups" W. Gao J. Number Theory 53 (1995), pages 241-246.
[GS] "On Davenport's Constant" A. Geroldinger \& R. Schneider J. Combinatorial Theory, Series A 61 (1992) , pages 147-152.
[H] "Ein extremalproblem für Gitterpunkte" H. Harborth J. Reine Angew.Math. 262 (1973) , pages 356-360 .
[O] "A combinatorial problem on finite Abelian groups I, II" J.E. Olson J. Number Theory 1 (1969), pages 8-11, 195-199.
[OQ] "The Erdös-Ginzburg-Ziv Theorem in Abelian non-Cyclic Groups" O. Ordaz \& D . Quiroz Divulgaciones Matematicas 8, no. 2 (2000), pages 113-119.
[vE] "A combinatorial problem on finite Abelian groups II" P. van Emde Boas Report ZW-1969-007 Math Centre, Amsterdam (1969) .
[vEK] "A combinatorial problem on finite Abelian groups III" P. van Emde Boas \& D.Kruyswijk Report ZW-1969-008 Math Centre, Amsterdam (1969) •

## Acknowledgement

The authors are grateful to CEFIPRA (Project 2801-1) for its financial support to visit each others' institute.

