Upper Bounds for the Davenport Constant

R. Balasubramanian, Gautami Bhowmik

UPPER BOUNDS FOR THE DAVENPORT CONSTANT

R. Balasubramanian and Gautami Bhowmik

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

I. 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 $ZS(G)$ 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. $ZS(G) = |G| + D(G) - 1$. 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, eg, [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 $M(G) = 1 + \sum_{i=1}^{r}(d_i - 1)$ 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, $ZS(G) \leq 2n - 1$ [EGZ] has been improved. Alon, Bialostocki and Caro [cited in OQ] proved that $ZS(G) \leq 3n/2$ if G is non-cyclic. Caro improved this bound to $ZS(G) \leq 4n/3 + 1$ if G is neither cyclic nor of the form $\mathbb{Z}_2 \oplus \mathbb{Z}_{2t}$. On excluding $\mathbb{Z}_3 \oplus \mathbb{Z}_{3t}$ as well, Ordaz and Quiroz [OQ] tightened the bound to $5n/4+2$. It is easy to see that though it is true for $k = 1, 2, 3$

The 2.6.2006

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 $\mathbb{Z}_u \oplus \mathbb{Z}_{ut}, u < k$.

On the other hand , Alfred, Granville and Pomerance [AGP] in 1994 used the bound $D(G) \leq m(1+\log \frac{n}{m})$, 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 contains a zero sum subsequence of length atmost s.

Olson calculated $D^p(\mathbb{Z}_p \oplus \mathbb{Z}_p)$ 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 $D^p(\mathbb{Z}_p^r)$ for $r \geq 3$. But Alon and Dubiner [AD] proved a remarkable bound in 1995, i.e. $D^p(\mathbb{Z}_p^r) \leq c(r)p$. In fact $c(r)$ can be taken to be $(cr\log r)^r$where c is an absolute constant. Dimitrov [D] used the Alon Dubiner constant to prove that $D(G) \leq M(G)(Kr\log r)^r$ 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 $G \sim \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_1a_2} \oplus \mathbb{Z}_{a_1a_2a_3}$, we have

$$D(G) \leq M(G)(1 + \frac{K}{a_2a_3}),$$

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 $D^p(\mathbb{Z}_p^r)$.

II. 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 $D(\mathbb{Z}_s^3)$ can be calculated, for example when s is a power of a prime..

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

$$\begin{aligned} h = \quad h_{a,b} \quad &= D(\mathbb{Z}_a \oplus \mathbb{Z}_{ab}), && a \neq 1 \\ &= D(\mathbb{Z}_b), && a = 1. \end{aligned}$$

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

$$D(\mathbb{Z}_s \oplus \mathbb{Z}_{sa} \oplus \mathbb{Z}_{sab}) \leq B(h_{a,b}),$$

where $B(h_{a,b}) = (h_{a,b} - u - 1)s + A$.

Proof.

Let S be a set of $B(h)$ elements of $\mathbb{Z}_s \oplus \mathbb{Z}_{sa} \oplus \mathbb{Z}_{sab}$. Every sequence of length atleast $D^s(\mathbb{Z}_s \oplus \mathbb{Z}_s \oplus \mathbb{Z}_s)$ 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 $D^s(\mathbb{Z}_s^3)$ elements left in $B(h)$. Thus there exist disjoint subsets $A_1, A_2, \cdots A_{h-u-1}$ in S such that $|A_j| \leq s$ 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 $B(h) - (h-u-1)s \geq D^s(\mathbb{Z}_s^3)$ 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 $D^s(\mathbb{Z}_s^3)$. Now

$$B(h) - (h-u)s \geq A - s \geq uD(\mathbb{Z}_p^3).$$

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 $(a_j s, b_j s, c_j s)$. Suppose that $a \neq 1$ and for $j \leq h$ let $C_j = (b_j, c_j)$. 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 $\mathbb{Z}_a \oplus \mathbb{Z}_{ab}$. The corresponding subcollection of A_j will suit our purpose in $\mathbb{Z}_s \oplus \ Z_{sa} \oplus \ Z_{sab}$.

If $a = 1$, we take $C_j = (c_j)$ and proceed as before.

□

To get precise bounds it is often necessary to actually evaluate $D(\mathbb{Z}_s^3)$ or atleast find reasonable bounds. This is possible for small values of s as follows :

Lemma 2. We have,

$$\begin{aligned} D^s(\ Z_s \oplus \mathbb{Z}_s \oplus \mathbb{Z}_s) \quad &= 8,\ s = 2 \\ &= 17,\ s = 3,. \\ &\leq 43,\ s = 4. \end{aligned}$$

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.

For $s = 4$, consider the 7 following elements : $x_1 = (2,0,0), x_2 = (0,2,0), x_3 = (0,0,2), x_4 = (2,2,0), x_5 = (2,0,2), x_6 = (0,2,2)$ and $x_7 = (2,2,2)$.

Let $A_i = \{y : 2y = x_i\}$. with $|A_i| = 8$. Let $B_i = A_i \cup \{x_i\}$ and if possible let S be a set of 43 elements with no zero sum subsequence.

Now consider $C_i = S \cap B_i$. Since $\cup_{i=1}^7 B_i$ has all the non zero elements of $\mathbb{Z}_4^3$, we have $|\cup_{i=1}^7 C_i| = 43$. Thus there exists an i such that $|C_i| \geq 7$ and c_i has no zero sum subsequence.

We shall show that this leads to a contradiction. We take $i = 1$ for convenience, the arguments would work for a general i. Thus

$$A_1 = \{(1,0,0), (3,0,0), (1,2,0), (3,2,0), (1,0,2), (3,0,2), (1,2,2), (3,2,2)\}.$$

Since C_1 is zero sum free, the following pairs of elements cannot occur in C_1 : $((1,0,0),(3,0,0)), ((1,2,0),(3,2,0)), ((1,0,2),(3,0,2)), ((1,2,2),(3,2,2))$.

Thus C_1 has at most 5 distinct elements. Further the multiplicity of any element in C_1 is atmost 3 and x_1 can occur atmost once. Atmost one element can have multiplicity 2, since $2y_1 + 2y_2 = 2x_1 = 0$. Further, if an element y_1 has multiplicity greater than 1, then $2y_1 + x_1 = 0$ and x_1 does not belong to C_1.

So we see that there exists no such C_i, and hence no such S. □

Sometimes we cannot find an effective bound for $D(\mathbb{Z}_s^3)$ 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

$$D(\mathbb{Z}_{s^a}^{r-1} \oplus \mathbb{Z}_{s^a} t) \leq D(\mathbb{Z}_{s^a}^r)t.$$

For some estimates, it is necessary to use the constant $D_k(G)$ which is the smallest integer t such that every sequence of t elemnts of G contains k disjoint zero sum sequences.

Lemma 4. We have $D_2(\mathbb{Z}_3^3) \leq 13$.

Proof. Consider the set $S = \{x_1, \cdots, x_{13}\}$. Now either S has a zero sum sequence of length less than 7, in which case it has another such sequence among the remaining $D(\mathbb{Z}_3^3)$ elements. Or S contains no zero sum sequence of length upto 6. Consider the set $T_i = \{x_1, \cdots, x_6, x_i\}$ with $7 \leq i \leq 13$. Now T_i contains a zero sum sequence of length exactly 7. Thus $\sum_{j=1}^{6} x_j + x_i = 0$ where $7 \leq i \leq 13$. This gives $x_7 = \cdots = x_{13}$ and $x_7 + x_8 + x_9 = 0$ in $\mathbb{Z}_3^3$. □

Remark. By the same method we could prove that $D_k(\mathbb{Z}_p^a) \leq k(D(\mathbb{Z}_p^a) - 1) + 1$.

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-Ginzburg-Ziv [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

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

and the condition $m(1 + \log \frac{n}{m}) \leq \frac{n}{k} + k - 1$ 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 : 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,

$$D(\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus K) \leq 2D(K) + 3.$$

Taking K to be $\mathbb{Z}_2 \oplus \mathbb{Z}_{2t}$, we get $D(G) \leq 4t+5 \leq \frac{32}{k}t + k - 1$ for $k = 5, 6, 7$.

Case 2 : $\text{rank}(G) = 4$.

The condition $\frac{n}{m} = a_1^3 a_2^2 a_3 < 31$ is satisfied only for the following groups of rank 4 that would violate the AGP condition would be of the form

$$G_1 \sim \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2t},$$

$$G_2 \sim \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{4t},$$

$$G_3 \sim \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{6t},$$

and

$$G_4 \sim \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3t}.$$

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] and 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 $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{4t}$. Then $D(H) = M(H)$ (see [vE]). Thus $D(G_2) \leq 8t+8$ 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

$$D(G_4) \leq 9t \leq \frac{81}{7}t + 6$$

for $k = 7$. Since $\frac{n}{m} = 27$ the inequality is already satisfied by the AGP bound for $k = 5, 6$.

Case 3 : $\text{rank}(G) = 3$.

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 $G_5 \sim \mathbb{Z}_2 \oplus \mathbb{Z}_{2u} \oplus \mathbb{Z}_{2ut}$, $1 < u < 8$, $G_6 \sim \mathbb{Z}_3 \oplus \mathbb{Z}_{3v} \oplus \mathbb{Z}_{3vt}, v = 1, 2, 3$; $G_7 \sim \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{4t}$ and $G_8 \sim \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{5t}$.

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

$$D(\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3t}) \leq 3t + 8 \leq \frac{27}{k}t + k - 1,$$

whenever $t \geq 2$.

When $t = 1$, we have a p-group and the BO conjecture is satisfied.

For $k = 7$ we now verify the inequality

$$D(\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_6) \leq 13 < \frac{54}{7} + 6.$$

We consider a set of 13 elements of $\mathbb{Z}_3^2 \oplus \mathbb{Z}_6$. From Lemma 4 we know that it contains two disjoint zero sum sequences in $\mathbb{Z}_3^3$, say T_1 and T_2. Let their sums be $(3a, 3b, 3c)$ and $(3k, 3l, 3m)$ respectively. Now if either c or m is even, we obtain a zero sum sequence in $\mathbb{Z}_3^2 \oplus \mathbb{Z}_6$, while if both are odd, $T_1 \cup T_2$ is the required zero sum sequence.

For the case $v = 2, 3$ in G_6, the BO condition is realised [vE] and we are within the claimed bound.

For G_7 we use Lemmas 1 and 2 with $s = 4, a = 1, b = t$ to obtain that

$$D(G_7) \leq 4t + 27 \leq \frac{64}{7}t + 6$$

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 : $\text{rank}(G) = 2$.

It is well known that $D(G) = a_1 + a_1a_2 - 1$ and the inequation

$$a_1 + a_1a_2 - 1 \leq \frac{a_1^2 a_2}{k} + k - 1$$

is always true for $a_1 = \frac{n}{m} \geq k$.

□

Remark. This bound is tight, since $D(\mathbb{Z}_k \oplus \mathbb{Z}_{kt}) = kt + k - 1$.

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.

III. 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 $M(G) = a_1a_2a_3 + a_1a_2 + a_1 - 2$. Our method also gives a minor improvement for the higher rank cases.

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

$$\begin{aligned} h &= D(\mathbb{Z}_{a/d} \oplus \mathbb{Z}_{ab/d} \oplus \mathbb{Z}_{abc/d}), a \neq d, \\ &= D(\mathbb{Z}_b \oplus \mathbb{Z}_{bc}) \ , \qquad a = p \ , \ b \neq 1, \\ &= D(\mathbb{Z}_c) \ , \qquad a = d, b = 1, c \neq 1. \end{aligned}$$

Then

$$D(\mathbb{Z}_a \oplus \mathbb{Z}_{ab} \oplus \mathbb{Z}_{abc}) \leq B(h),$$

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 $G \sim \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_1a_2} \oplus \mathbb{Z}_{a_1a_2a_3}$. Then

$$D(G) \leq a_1a_2a_3 + a_1a_2 + Ka_1,$$

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,

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

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

For fixed a_2, a_3 we write $h(a_1) = D(\mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_1a_2} \oplus \mathbb{Z}_{a_1a_2a_3})$.

Using Lemma 3 we see that if p divides a_1 ,

$$h(a_1) \leq h((a_1/p) + K)p.$$

Let $a_1 = p_1p_2 \cdots p_t$ with $p_i \geq p_{i+1}$. Thus

$$h(p_1p_2 \cdots p_t) \leq h((p_2 \cdots p_t) + K)p.$$

Repeating the above process we get

$$h(a_1) \leq a_1h(1) + K(p_1p_2 \cdots p_t + p_1p_2 \cdots p_{t-1} + \cdots + p_1)$$

But

$$p_1p_2 \cdots p_t + p_1p_2 \cdots p_{t-1} + \cdots + p_1 = a_1(1 + \frac{1}{p_t} + \frac{1}{p_tp_{t-1}} + \cdots + \frac{1}{p_tp_{t-1} \cdots p_2}) \leq 2a_1.$$

This gives $D(\mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_1a_2} \oplus \mathbb{Z}_{a_1a_2a_3}) \leq a_1D(\mathbb{Z}_{a_2} \oplus \mathbb{Z}_{a_2a_3}) + 2Ka_1$,
i.e.

$$D(\mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_1a_2} \oplus \mathbb{Z}_{a_1a_2a_3}) \leq a_1a_2a_3 + a_1a_2 + (2K-1)a_1.$$

□

Remark. For the case of a general r we get $D(G) \leq M(G)(1 + \frac{K_r}{a_{r-1}a_r})$ and the improvement from the existing bound comes into 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 on 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 $\mid A \mid /4W$ 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

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

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

This gives

$$M(ja) = L(ja) + L(-ja) \leq \frac{2jW}{5p} \mid Y \mid .$$

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

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

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

$$T(b) = \frac{1}{|G|}\sum_x (1 - l^{\bar{b}.\bar{x}})|\sum_y l^{\bar{x}.\bar{y}}|^2,$$

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

Then

$$T(b) = \frac{1}{|G|}\sum_x (1 - l^{\bar{b}.\bar{x}}) \sum_{y_1, y_2} l^{\bar{x}.(\bar{y}_1 - \bar{y}_2)}.$$

$$= \frac{1}{|G|}\sum_{y_1,y_2}(\sum_x l^{\bar{x}.(\bar{y}_1-\bar{y}_2)} - \sum_x l^{\bar{x}.(\bar{y}_1-\bar{y}_2-\bar{b})}).$$

$$= B - D.$$

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

$$M(ja) = L(ja) + L(-ja) = T(ja) + T(-ja) = \sum_x (2 - l^{j\bar{a}.\bar{x}} - l^{-j\bar{a}.\bar{x}})|\sum_y l^{\bar{x}.\bar{y}}|^2.$$

$$= \frac{4}{|G|}\sum_x \sin^2(\frac{\pi}{p}j\bar{a}.\bar{x})|\sum_y l^{\bar{x}.\bar{y}}|^2.$$

Then

$$S = \frac{4}{|G|}\sum_{x\neq 0}\sum_a\sum_j \sin^2(\frac{\pi}{p}j\bar{a}.\bar{x})|\sum_y l^{\bar{x}.\bar{y}}|^2$$

$$\geq \frac{4}{|G|}\sum_{x\neq 0} R|\sum_y l^{\bar{x}.\bar{y}}|^2$$

where R is a minorisation of $\sum_a \sum_j \sin^2(\frac{\pi}{p}j\bar{a}.\bar{x})$ for $x \neq 0$.

We then have

$$S \geq \frac{4R}{|G|}\sum_{x\in G}|\sum_y l^{\bar{x}.\bar{y}}|^2 - \frac{4R}{|G|}\sum_{x=0}|\sum_y l^{\bar{x}.\bar{y}}|^2$$

$$\geq 4R|Y| - \frac{4R}{|G|}|Y|^2 \geq 2R|Y|,$$

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 $j\bar{a}.\bar{x}$ as small as possible. Thus the condition that no hyperplane contains more than $\frac{|A|}{4W}$ elements implies that $\bar{a}.\bar{x} \geq W$ 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.

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

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. Alfred, 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] *"$(C_2 \oplus C_2 \oplus C_2 \oplus C_{2n})$! 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"* S-T. 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* .

[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) .**

Authors' Address:

1.Institute of Mathematical Sciences, Chennai,India.Email:balu@imsc.res.in

2.Université de Lille 1, Laboratoire de Math. U.M.R. CNRS 8524, 59655 Villeneuve d'Ascq Cedex, France.Email:bhowmik@math.univ-lille1.fr