## On Davenport's Constant [1]

P. Rath, K. Srilakshmi and R. Thangadurai

**Abstract**

In this paper, using the idea of Alford, Granville and Pomerance in [1] (or Emde Boas and Kruyswijk [6]) we obtain an upper bound for the Davenport Constant of an Abelian group $G$ in terms of the number of repeatations of the group elements in any given sequence. In particular, our result implies,

$$D(G) \leq n\left(k + 1 + \log\left[\left(\frac{n-2}{n}\right)^k \frac{|G|}{n}\right]\right) - k,$$

where $n$ is the exponent of $G$ and $k \geq 0$ denotes the number of distinct elements of $G$ that are repeated at least twice in the given sequence.

# 1. Introduction

Let $G$ be a finite abelian group. By the structure theorem, we know $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_d}$ where $n_i$'s are integers satisfying $1 < n_1|n_2|\cdots|n_d$ and $n_d$ is the *exponent* (denoted by $\exp(G)$) of $G$ and $d$ is the *rank* of $G$. Let $M(G) = 1 + \sum_{i=1}^{d}(n_i - 1)$. Through-out this paper, we follow standard notations followed in the book of Geroldinger and Halter-Koch [12].

The **Davenport constant** of a finite abelian group $G$ (denoted by $D(G)$) is defined to be the least positive integer $t$ such that any sequence (not necessarily distinct) of $t$ elements in $G$ contains a subsequence whose sum is the zero element in $G$. This constant is finite and doesn't exceed the cardinality of the group $G$.

This constant, though attributed to Davenport, seems to have been first studied by K. Rogers [20] in 1962. This particular reference was somehow missed-out by most of the authors in this area.

Apart from their interest in zero-sum problems of additive number theory and non-unique factorization in algebraic number theory, these constants play important role in graph theory (see, for instance, [4] or [10]). One of the prime examples is the proof of the infinitude of Carmichael numbers where some knowledge of zero-sum sequences in the group of units of $\mathbb{Z}_n$ is required. For more details we refer to [1].

Determining the Davenport constant for a general finite abelian group, however, seems to belong to the realms of distant future. We are not even sure

[1] Subject Classification: Primary 11B75, Secondary 20K01

what exactly are the invariants which should appear in a general formula for all abelian groups. It is perceived, from whatever little is known, that the following invariants ought to have a bearing in such a general formula: (1) The rank of the group; (2)The number of prime factors of the order of the group; (3) The distribution of orders of the various group elements, for instance the ratio of the largest and the smallest (greater than 1) possible orders.

It is trivial to see that $M(G) \leq D(G) \leq |G|$ and the equality holds if and only if $G = \mathbb{Z}_n$, the cyclic group of order $n$. Olson ([18] and [19]) proved that $D(G) = M(G)$ for all finite abelian groups of rank 2 and for all $p$-groups. Recently, G. Bhowmik and J-C. Schlage-Puchta [3] proved that $D(\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}) = 3d + 4 = M(\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d})$. It is also known that $D(G) > M(G)$ for infinitely many finite abelian groups of rank $d > 3$. (See for instance, [13]).

Chronologically, Emde Boas and Kruyswijk [6], Baker and Schmidt [2] and Meshulam [15] gave upper bounds for Davenport Constant which involves the exponent of the group and the cardinality of the group $G$. In this direction, the best known bound is due to Emde Boas and Kruyswijk [6] who proved that

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

where $n$ is the exponent of $G$. This was again proved by Alford, Granville and Pomerance [1].

Obtaining a good upper bound for the Davenport constant constitutes a very important question about which the current state of knowledge is rather limited. However, we do have the following conjectures.

## Conjectures.

1. $D(G) = M(G)$ for all $G$ with rank $d = 3$ or $G = \mathbb{Z}_n^d$. ([7] and [8]).
2. $D(G) \leq \sum_{i=1}^{d} n_i$ ([17]).

In their paper, Alford, Granville and Pomerance [1] (Here referee pointed out that the idea of this proof goes back to Emde Boas and Kruyswijk [6]) obtained the above mentioned bound (1) for an arbitrary abelian group $G$ by constructing a suitable group algebra $K[G]$, where $K$ is a finite field and by an ingenious enumeration of the characters on $K[G]$ based on the greedy algorithm. However, their enumerative procedure does not take into account the fact that group elements are allowed to recur in the sequence; i.e., they do not distinguish between a set or a sequence of group elements.

In our work, we modify their method so as to take into account repeatations and hence obtain a different upper bound. Since most of the examples giving "good" lower bound involve repeatations, one would expect better answers once repeatation is assumed which turns out to be the case for us. Of course we do away with the trivial case where some element occurs at least $\exp(G)$ times. We prove the following theorem.

**Theorem 1.** *Let $G$ be a finite abelian group of rank $d$ and of exponent $n$. Let $\ell_1, \ell_2, \cdots, \ell_k$ and $r$ be integers such that $1 \leq \ell_i \leq n-2$ for all $i = 1, 2, \cdots, k$ for some integer $k \geq 0$ and the positive integer*

$$r := \begin{cases} n + \left[ n \left( \sum_{i=1}^{k} \log \ell_i - \log \frac{n^{k+1}}{|G|} \right) \right] & \text{if } \prod_{i=1}^{k} \ell_i > \frac{n^{k+1}}{|G|} \\ n & \text{otherwise} \end{cases}$$

*Let*

$$S = \prod_{i=1}^{k} g_i^{n-\ell_i} \prod_{j=1}^{r} c_j$$

*be a sequence in $G$ of length $\rho = \sum_{i=1}^{k}(n - \ell_i) + r$. Then $S$ has a subsequence whose sum is zero.*

**Remark 1.** From Theorem 1, we have the following upper bound for the Davenport Constant of an Abelian group $G$ in terms of the number of repeatations of the group elements in any given sequence.

$$D(G) \leq \begin{cases} \sum_{i=1}^{k} (n \log \ell_i - \ell_i) + (k+1)n - n \log \frac{n^{k+1}}{|G|} & \text{if } \prod_{i=1}^{k} \ell_i > \frac{n^{k+1}}{|G|} \\ (k+1)n - \sum_{i=1}^{k} \ell_i & \text{otherwise} \end{cases}.$$

Hence, we get,

$$\begin{aligned} D(G) &\leq \sum_{i=1}^{k} (n \log(n-2) - \ell_i) + (k+1)n - n \log \frac{n^{k+1}}{|G|} \\ &\leq n \log(n-2)^k + (k+1)n + n \log \frac{|G|}{n^{k+1}} - k. \end{aligned}$$

which implies

$$D(G) \leq n \left( k + 1 + \log \left( \frac{n-2}{n} \right)^k \frac{|G|}{n} \right) - k.$$

Thus, we see that when no repeatation is assumed, i.e., when $k = 0$, we recover the bound (1) of Alford *et al.* which is to be expected as they did not use the fact that the group elements can repeat in a given sequence.

**Remark 2.** *Let $d \geq 3$ be any integer. Let $S$ be any sequence in $\mathbb{Z}_n^d$ of length $d(n-1)+1$. Suppose there exist at least $d-1$ distinct elements of $\mathbb{Z}_n^d$ which* *are repeated* $n-1$ *times in* $S$*. Then* $S$ *contains a non-empty subsequence whose product is* 1 *in* $\mathbb{Z}_n^d$*.*

We get the above by applying Theorem 1 with $G=\mathbb{Z}_n^d$, $k=d-1$ and $\ell_i=1$. Moreover, this length is tight because the sequence

$$S=e_1^{n-1}e_2^{n-1}\cdots e_d^{n-1} \text{ in } \mathbb{Z}_n^d$$

of length $d(n-1)$ has no subsequence whose product is identity where $e_i=(0,0,\cdots,0,1,0,\cdots,0)$ with 1 in the $i$-th position.

## 2. Proof of Theorem 1

First we prove the following general lemma which would be of relevance in our proof.

**Lemma 1.** *Let* $G$ *be a finite abelian group,* $K$ *a field and* $X\subset Hom(G,K^*)$*.*

1. *If* $k\in\mathbb{N}$ *and* $g_1,\cdots,g_k\in G$*, then there exist* $a_1,a_2,\cdots,a_k\in K^*$ *such that*

$$|\{\chi\in X\mid \chi(g_i)\neq a_i \text{ for all } i\in[1,k]\ \}|\leq |X|\prod_{i=1}^{k}\left(1-\frac{1}{ord(g_i)}\right).$$

2. *If* $g\in G$ *with* $ord(g)=n\geq 2$ *and* $l\in[1,n-1]$*, then there exists* $a^{(1)},\cdots,a^{(\ell)}\in K^*$ *such that*

$$|\{\chi\in X\mid \chi(g)\neq a^{(j)} \text{ for all } j\in[1,\ell]\ \}|\leq |X|\prod_{j=0}^{\ell-1}\left(1-\frac{1}{n-j}\right).$$

3. *If* $k\in\mathbb{N}$ *and* $g_1,\cdots,g_k\in G$ *with* $ord(g_i)=n_i\geq 2$ *and* $\ell_i\in[1,n_i-1]$ *for all* $i\in[1,k]$*, then there exists* $a_1^{(1)},\cdots,a_1^{(\ell_1)},\cdots,a_k^{(1)},\cdots,a_k^{(\ell_k)}\in K^*$ *such that*

$$|\{\chi\in X\mid \chi(g_i)\neq a_i^{(j)} \text{ for all } j\in[1,\ell_i] \text{ and for all } i\in[1,k]\}|$$

$$\leq |X|\prod_{i=1}^{k}\prod_{j=0}^{\ell_i-1}\left(1-\frac{1}{n_i-j}\right).$$

*Proof.* For the proof of the first assertion, see ([12] , Lemma 5.5.3).

2. We proceed by induction on $\ell$. The case $\ell=1$ follows from above. Let $\ell\geq 2$ and $a^{(1)},a^{(2)},\cdots,a^{(\ell-1)}\in K^*$ be such that the cardinality of the set $X_1=\{\chi\in X\mid \chi(g)\neq a^{(j)}$ for all $j\in[1,\ell-1]\ \}$ satisfies

$$|X_1|\leq |X|\prod_{j=0}^{\ell-2}\left(1-\frac{1}{n-j}\right).$$

The set $\{\chi(g) \mid \chi \in X_1\}$ is contained in a cyclic subgroup of order n in $K^*$ and does not intersect $\{a^{(1)}, a^{(2)}, \cdots, a^{(\ell-1)}\}$. Hence there exists an $a^{(\ell)}$ in $K^*$ such that

$$|\{\chi \in X_1 \mid \chi(g) = a^{(\ell)}\}| \geq \frac{|X_1|}{n-(\ell-1)}.$$

Thus, we have

$$|\{\chi \in X \mid \chi(g) \neq a^{(i)} \text{ for all } i \in [1,\ell]\}| = |\{\chi \in X_1 \mid \chi(g) \neq a^{(\ell)}\}|$$

$$\leq |X_1|\left(1 - \frac{1}{n-\ell+1}\right) \leq |X| \prod_{j=0}^{\ell-1}\left(1 - \frac{1}{n-j}\right)$$

3. We proceed by induction on $k$. The case $k = 1$ follows from part 2. Let $k \geq 2$ and $a_1^{(1)}, \cdots, a_1^{(\ell_1)}, \cdots, a_{k-1}^{(1)}, \cdots, a_{k-1}^{(\ell_{k-1})} \in K^*$ be such that the set

$$X_1 = \{\chi \in X \mid \chi(g_i) \neq a_i^{(j)} \text{ for all } j \in [1,\ell_i] \text{ for all } i \in [1,k-1]\}$$

satisfies

$$|X_1| \leq |X| \prod_{i=1}^{k-1}\prod_{j=0}^{\ell_i-1}\left(1 - \frac{1}{n_i - j}\right).$$

Again by part 2, there are $a_k^{(1)}, \cdots, a_k^{(\ell_k)} \in K^*$ such that

$$|\{\chi \in X_1 \mid \chi(g_k) \neq a_k^{(j)} \text{ for all } j \in [1,\ell_k]\}| \leq |X_1| \prod_{j=0}^{\ell_k-1}\left(1 - \frac{1}{n_k - j}\right).$$

Thus,

$$\begin{aligned}
|\{\chi \in X \quad &| \quad \chi(g_i) \neq a_i^{(j)} \text{ for all } j \in [1,\ell_i] \text{ and for all } i \in [1,k]\ \}| \\
&= \quad |\{\chi \in X_1 \mid \chi(g_k) \neq a_k^{(j)} \text{ for all } j \in [1,\ell_k]\}| \\
&\leq \quad |X_1| \prod_{j=0}^{\ell_k-1}\left(1 - \frac{1}{n_k - j}\right) \leq |X| \prod_{i=1}^{k}\prod_{j=0}^{\ell_i-1}\left(1 - \frac{1}{n_i - j}\right).
\end{aligned}$$

Thus the lemma is proved. □

*Proof of Theorem 1.* We adopt the strategy applied in [1]. Let

$$S = \prod_{i=1}^{k} g_i^{n-\ell_i} \prod_{j=1}^{r} c_j$$

be the sequence in $G$ of length $\rho$.

Let $q$ be a prime such that $n|(q-1)$. Let $\mathbb{F}_q[G]$ be the group algebra over $\mathbb{F}_q$ with basis $G$ and we write the elements in it as

$$f = \sum_{g \in G} c_g X^g.$$

Our goal is to find $\rho$ elements $a_1^{(i_1)}, a_2^{(i_2)}, \cdots, a_k^{(i_k)}, b_1, b_2, \cdots, b_r \in \mathbb{F}_q^*$ where each $i_j$ varies from 1 to $n - \ell_j$ for $j = 1, 2, \cdots, k$ such that the product

$$\prod_{i=1}^{n-\ell_1} (X^{g_1} - a_1^{(i)}) \prod_{i=1}^{n-\ell_2} (X^{g_2} - a_2^{(i)}) \cdots \prod_{i=1}^{n-\ell_k} (X^{g_k} - a_k^{(i)})) \prod_{i=1}^{r} (X^{c_i} - b_i)$$

is equal to zero in $\mathbb{F}_q[G]$. This clearly ensures the existence of a subsequence of $S$ whose sum is zero. To show that an element $a \in \mathbb{F}_q[G]$ is the zero element, it suffices to prove $\chi(a) = 0$ for all $\chi \in Hom(G, \mathbb{F}_q^*)$ where each such $\chi$ is extended naturally to $\mathbb{F}_q[G]$. Indeed, by definition,

$$\chi(f) := \chi(\sum_{g \in G} c_g X^g) = \sum_{g \in G} c_g \chi(g).$$

By Lemma 1, we see that there exists non-zero elements

$$a_1^{(1)}, \cdots, a_1^{(n-\ell_1)}, \cdots, a_k^{(1)}, \cdots, a_k^{(n-\ell_k)} \in \mathbb{F}_q^*$$

such that the following set

$$B_k^{(n-\ell_k)} \quad := \quad \left\{ \chi \in Hom(G, \mathbb{F}_q^*) \mid \chi(g_i) \neq a_i^{(j)}, \ \forall\ i \in [1, k], j \in [1, n - \ell_i] \right\}.$$

has cardinality

$$\left| B_k^{(n-\ell_k)} \right| \quad \leq \quad |G| \prod_{i=1}^{k} \left[ \prod_{j=0}^{n-\ell_i-1} \left(1 - \frac{1}{n-j}\right) \right].$$

Since $\prod_{j=0}^{n-z-1} \left(\frac{n-j-1}{n-j}\right) = \frac{z}{n}$, we get

$$\left| B_k^{(n-\ell_k)} \right| \leq |G| \prod_{i=1}^{k} \frac{\ell_i}{n} = \ell_1 \ell_2 \cdots \ell_k \frac{|G|}{n^k}.$$

**Case (i)** $\displaystyle\prod_{i=1}^{k} \ell_i \leq \frac{n^{k+1}}{|G|}$

In this case, it is clear that $\left| B_k^{(n-\ell_k)} \right| \leq n$. Also note that we are still left with $r = n$ elements of the sequence. Set $B_a := B_k^{(n-\ell_k)}$.

**Case (ii)** $\displaystyle\prod_{i=1}^{k} \ell_i > \frac{n^{k+1}}{|G|}$

In this case, we can continue the process (because of the definition of $r$) and use

$$m = \left[ n \left( \sum_{i=1}^{k} \log \ell_i - \log \frac{n^{k+1}}{|G|} \right) \right] + 1$$

number of $c_i$'s to find elements $b_1, b_2, \cdots, b_m$ in $\mathbb{F}_q^*$ such that at the final step, we have the following set

$$B_a := \left\{ \chi \in B_k^{(n-\ell_k)} \mid \chi(c_i) \neq b_i, \ \forall\, i \in [1, m] \right\}$$

with

$$|B_a| \leq \ell_1 \ell_2 \cdots \ell_k \frac{|G|}{n^k} \left(1 - \frac{1}{n}\right)^m .$$

By the choice of $m$, we have $|B_a| < n$. In this case, we are still left with at least $n-1$ elements of the sequence.

Let $B_a = \{\chi_{m+1}, \chi_{m+2}, \cdots, \chi_{m+s}\}$. Then in case (i), we have $|B_a| = s \leq n$ and in case (ii), we have $|B_a| = s \leq n-1$. We take $b_i = \chi_i(c_i)$ for all $i = m+1, m+2 \cdots, m+s$ and the remaining (if any) $b_i$'s can be chosen arbitrarily. Thus, the required product vanishes for all the characters in the group algebra $\mathbb{F}_q[G]$ and hence the result. $\square$

## 3. Remarks.

1. It is our perception that the method adopted here is unlikely to yield an upper bound qualitatively superior to whatever has been obtained. The main reason is that the method here only takes into account the maximal order of the group elements and does not take into account the distribution of the orders of the other group elements. For instance, the method does not distinguish between the groups $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_d}$ and $G = \mathbb{Z}_n^d$, a serious drawback.

2. If one does not allow repeatations in the definition of Davenport's constant, then the corresponding constant is referred to as *Olson's constant* (denoted by $Ol(G)$). Clearly $Ol(G) \leq D(G)$. However, equality is expected for groups with large rank $d$ (See for instance [9] and [11]). But for smaller values of $d$, it is expected to be much smaller than $D(G)$. In [14], it is proved that $Ol(\mathbb{Z}_p) \leq \sqrt{2p} + 5\log p$ for all primes $p$ while in [11], it is proved that $Ol(\mathbb{Z}_p^2) = p - 1 + Ol(\mathbb{Z}_p)$ for all primes $p > 4.67 \times 10^{34}$. Recently, J. M. Deshouillers and G. Prakash ([5]) proved for large enough prime $p$ that

$$Ol(\mathbb{Z}_p) \leq \sqrt{2p} + \frac{1}{2} + \frac{7}{16}\sqrt{\frac{2}{p}}.$$

   Other than these results, hardly anything is known as regards its exact value. This also constitutes an important open question in Combinatorial group theory.

3. Many generalization of Davenport's constant is known now. For instance, one may refer to Theorem 5.1.5 in [12]. Also, very recently the last author proved a variation of Davenport's constant in [21].

**Acknowledgments.** We are grateful to the referee for suggesting us the Lemma 1 which brought clarity to the proof of our theorem and for drawing our attention to some of the relevant references. This work was done while the first two authors were at Harish-Chandra Research Institute, Allahabad. They are thankful to the institute for the warm hospitality during their stay.

## References

[1] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math., **139** (2) (1994), no. 3, 703-722.

[2] R. C. Baker and W. Schmidt, *Diophantine problems in variables restricted to the values of* 0 *and* 1, J. Number Theory, **12** (1980), 460-486.

[3] G. Bhowmik and J-C. Schlage-Puchta, *Davenport's constant for groups of the form* $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$, Preprint, 2006.

[4] Y. Caro, *Zero-sum problems - a survey*, Discrete Math., **152** (1996), 93-113.

[5] J. M. Deshouillers and G. Prakash, Preprint, 2006.

[6] P. van Emde Boas and D. Kruswjik, *A combinatorial problem on finite abelian group III*, Z. W.1969-008 (Math. Centrum, Amsterdam).

[7] W. D. Gao, *On Davenport's constant of finite abelian groups with rank three*, Discrete Math., **222** (2000), no. 1-3, 111-124.

[8] W. D. Gao and A. Geroldinger, *Zero-sum problems and coverings by proper cosets*, European J. Combinatorics, **24** (2003), 531-549.

[9] W. D. Gao and A. Geroldinger, *On long minimal zero sequences in finite abelian groups*, Period. Math. Hungar. **38** (3) (1999), 179-211.

[10] W. D. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups; a survey*, Expo. Math., **24** (4), (2006), 337-369.

[11] W. D. Gao, I. Z. Ruzsa and R. Thangadurai, *Olson's constant for the group* $\mathbb{Z}_p \oplus \mathbb{Z}_p$, J. Combin. Theory, Ser. A, **107** (2004), 49-67.

[12] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations, Algebraic, Combinatorial and Analytic Theory,* Pure and Applied Mathematics, vol.278, Chapman and Hall/CRC,

[13] A. Geroldinger and R. Schneider, *On Davenport's constant*, J. Combin. Theory, Ser. A, **61** (1992), no. 1, 147-152.

[14] Y. O. Hamidoune and G. Zémor, *On zero-free subset sums*, Acta Arith., **78** (2) (1996), 143-152.

[15] R. Meshulam, *An uncertainty inequality and zero subsums*, Discrete Math., **84** (1990), no. 2, 197-200.

[16] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer Verlag, 1990.

[17] W. Narkiewicz and J. Śliwa, *Finite abelian groups and factorization problems - II*, Colloq. Math., **46** (1982), 115-122.

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

[19] J. E. Olson, *A combinatorial problem in finite abelian groups, II*, J. Number Theory, **1** (1969), 195-199.

[20] K. Rogers, *A Combinatorial problem in Abelian groups,* Proc. Cambridge Phil. Soc., (1963) **59**, 559-562.

[21] R. Thangadurai, *A variant of Davenport's Constant*, To appear in: Proc. Indian Acad. Sci. (Math. Sci).

**Addresses of Authors.**

P. Rath
Institute of Mathematical Sciences
C. I. T. Campus, Taramani
Chennai 600113. INDIA
Email: rath@imsc.res.in

K. Srilakshmi
Department of Pure Mathematics
University of Sheffield
Hicks Building, Hounsfield Road
Sheffield S3 7RH, United Kingdom.
Email: pmp06sk@shef.ac.uk

R. Thangadurai
Harish-Chandra Research Institute
School of Mathematics
Chhatnag Road, Jhunsi
Allahabad 211019, INDIA
Email: thanga@hri.res.in