Davenport Constant and Non-Abelian Version of Erdős-Ginzburg-Ziv Theorem

W. D. Gao and R. Thangadurai

Center for Combinatorics,
Nankai University,
Tianjin 300071,
China.
e-mail:
wdgao_1963@yahoo.com.cn

and

School of Mathematics, Harish-Chandra
Research Institute,
Chhatnag Road,Jhunsi,
Allahabad - 211019, India.
e-mail:
thanga@hri.res.in

Dedicated to Professor K. Ramachandra on his 70th birthday

Abstract

In this article, apart from giving a survey of known results on Davenport constant for finite groups, we shall prove the following new result. Let G be a non-abelian group with $\mathbf{Z}(G)$ as its center. Let $S = (a_1, a_2, \ldots, a_\ell)$ be a sequence in G of length $\ell = |G|+D(G)-1$, where $D(G)$ is the Davenport constant (see below, definition 1) for the group G. Suppose that there exists $g \in \mathbf{Z}(G)$ such that g appears in S maximum number of times. Then, there exist distinct integers $i_1, i_2, \ldots, i_{|G|}$ from $1, 2, \ldots, \ell$ such that the product $a_{i_1}a_{i_2}\ldots a_{i_{|G|}}$ is the identity element in G.

1 Introduction

In 1961, Erdős, Ginzburg and Ziv [2] proved that given any sequence a_1, a_2, $\ldots, a_{2n-1}$ (not necessarily distinct) of elements in $\mathbb{Z}_n$, the cyclic group of order n, there exists a subsequence with n elements whose sum is the identity in $\mathbb{Z}_n$. Moreover, they proved that $2n-1$ cannot be replaced by $2n-2$.

This theorem is a cornerstone of many questions in 'Zero-sum Problems' which is now one of the active fields of research in Combinatorial Number Theory. The above theorem has many generalizations (See [25] for instance).

From now onwards, we denote any finite group (not necessarily abelian) by G which is additively written.

Definition 1. By $D(G)$, we denote the smallest positive integer t such that given any sequence $g_1, g_2, \ldots, g_\ell$ in G with $\ell \geq t$ there exist distinct integers $1 \leq i_1 < i_2 < \cdots < i_r \leq \ell$ and a permutation π on the symbols $\{1, 2, \ldots, r\}$ such that $g_{i_{\pi(1)}} + g_{i_{\pi(2)}} + \cdots + g_{i_{\pi(r)}} = 0$ in G.

1991 *Mathematics Subject Classification.* Primary 11B75, Secondary 20K99.

Key words and phrases. zero-sum sequences, non-abelian groups, Erdős, Ginzburg and Ziv Theorem

When G is abelian, $D(G)$ is nothing but the well-known *Davenport constant*. This above generalization is considered, for example, in [3]. Clearly, we have $D(G) \leq |G|$.

In the definition 1, if we take π to be identity, then $D(G)$ is called the Strong Davenport constant and we denote it by $d(G)$.

Definition 2. By $ZS(G)$, we denote the smallest positive integer t such that given any sequence $g_1, g_2, \ldots, g_\ell$ in G with $\ell \geq t$ there exists distinct integers $1 \leq i_1 < i_2 < \cdots < i_{|G|} \leq \ell$ and a permutation π on the symbols $\{1, 2, \ldots, |G|\}$ such that $g_{i_{\pi(1)}} + g_{i_{\pi(2)}} + \cdots + g_{i_{\pi(|G|)}} = 0$ in G.

When G is abelian, the first author [7] proved that

$$ZS(G) = |G| - 1 + D(G),$$

which had been earlier conjectured by Hamidoune. When $G = \mathbb{Z}_n$, this result is nothing but the Erdös, Ginzburg and Ziv theorem.

An interesting problem is to prove or disprove the following conjecture.

Conjecture 1. (Gao and Zhuang, [12]) For every finite group G, we have $ZS(G) = |G| - 1 + D(G)$.

J. E. Olson [21] proved that $ZS(G) \leq 2|G| - 1$. Recently, Dimitrov [4] gave a very simple proof of this fact for all solvable groups. In 1984, Peterson and Yuster [23] proved that $ZS(G) \leq 2|G| - 2$ for a non-cyclic group G. In 1988, for a positive integer r, with the restriction that $|G| \geq 600((r-1)!)^2$, Yuster [27] proved that $ZS(G) \leq 2|G| - r$; for a non-cyclic solvable group G and 1996, the first author [8] proved that $ZS(G) \leq \frac{11}{6}|G| - 1$ for a non-cyclic solvable group G. In 2003, Dimitrov [5] proved a stronger result when G is a non-cyclic p group. More precisely, he proved:

Let $s \geq \left(1 + \frac{2p-1}{p^2}\right)|G| - 1$ *be any integer. Then for any sequence* $S = (a_1, a_2, \ldots, a_s)$ *in* G*, there exist* $1 \leq i_1 < i_2 < \cdots < i_{|G|} \leq s$ *such that* $a_{i_1} + a_{i_2} + \cdots + a_{i_{|G|}} = 0$ *in* G.

Using the method of the proof of the above result, in [6], Dimitrov mentions that $ZS(G) \leq \frac{7}{4}|G| - 1$ for all non-cyclic nilpotent groups G. More recently, Gao and Juan [12] proved Conjecture 1 for any Dihedral G of large prime index.

In this article, we shall survey the known results and conjectures on Davenport constant for all finite groups and prove the following new result which is related to Conjecture 1.

Main Theorem. *Let* G *be a finite non-abelian group and* $S = (a_1, a_2, \ldots, a_\ell)$ *a sequence in* G *of length* $\ell = |G| + D(G) - 1$. *Suppose that there exists* $g \in \mathbf{Z}(G)$, *where* $\mathbf{Z}(G)$ *is the center of* G *such that* g *appears in* S *maximum number of times. Then, there exist distinct integers* $i_1, i_2, \ldots, i_{|G|}$ *from* $1, 2, \ldots, |G| - 1 + D(G)$ *such that* $a_{i_1} + a_{i_2} + \cdots + a_{i_{|G|}} = 0$ *in* G.

Notations. Let $S = (a_1, a_2, \ldots, a_\ell)$ be a sequence in G. We denote the length ℓ of S by $|S|$. If T is a subsequence of S, then ST^{-1} is a sequence obtained by deleting the terms of T from S. If T_1 and T_2 are two disjoint subsequence of S, then we write

T_1T_2 for a subsequence of S after a permutation on T_1 and T_2. We call a sequence S of length ℓ to be a *zero-sum sequence* if there is a permutation π on the symbols $\{1, 2, \ldots, \ell\}$ such that $g_{\pi(1)} + g_{\pi(2)} + \cdots + g_{\pi(\ell)} = 0$ in G. We call a sequence in G a *zero-free sequence* if none of its subsequences is a zero-sum sequence. We call an element g of G to be a *hole* of S if $g \notin \sum(S) \cup \{0\}$, where $\sum(S)$ denotes the set of all possible finite sums of elements of S.

2 Davenport Constant for any finite group

One can easily see that $D(G) \leq |G|$ for any finite group G.

2.1 Davenport constant for abelian groups.

Since G is a finite abelian group, by the structure theorem, we have

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}$$

where $1 < n_1 | n_2 | \cdots | n_r$ and $|G| = n_1 n_2 \ldots n_r$. Here r is called the *rank* (denoted by $r(G)$) of G and n_r is called the *exponent* (denoted by $\exp(G)$) of G. Define

$$M(G) = 1 + \sum_{i=1}^{r}(n_i - 1) \tag{1}$$

and

$$\kappa(G) = \sum_{i=1}^{r} n_i. \tag{2}$$

It is easy to see that $D(G) = |G|$, whenever G is cyclic. Olson ([21] and [22]) proved that $D(G) = M(G)$ for all p-groups G and for all G with rank 2. These are the major classes of groups for which this constant is known explicitly. The first author [9] studied this constant when G is of rank 3 and he conjectured that

Conjecture 2. (Gao, [9]) *For all groups G of rank 3, we have $D(G) = M(G)$.*

It is known from the results in [13], [11] and [16] that $D(G) > M(G)$ for infinitely many groups G.

Recently, P. Rath, K. Srilakshmi and the second author proved the following theorem in [24].

Theorem 1. *Let G be a finite abelian group of rank r and of exponent n. Let $\ell_1, \ell_2, \ldots, \ell_{r-1}$ and d be integers such that $1 \leq \ell_i \leq n - 1$ for all $i = 1, 2, \ldots, r - 1$ and the positive integer*

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

Let

$$S = \left(\underbrace{g_1, \dots, g_1}_{(n-\ell_1)\ times}, \dots, \underbrace{g_{r-1}, \dots, g_{r-1}}_{(n-\ell_{r-1})\ times}, c_1, c_2, \dots, c_d \right)$$

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

Corollary 1. *We have*

$$D(G) \leq n_r \left(1 + \log \left(\frac{n_r - 1}{n_r} \right)^{r-1} \left(\frac{|G|}{n_r} \right) \right).$$

The Corollary 1 improves the previous best upper bound due to Alford, Granville and Pomerance[1] and Meshulam [17] in 1993. Also, Corollary 1 can be improved if one proves the following conjectural bound suggested by W. Narkiewicz and J. Śliwa, [18] in 1982.

Conjecture 3. (Narkiewicz and Śliwa, [18]) *For all finite abelian group* G*, we have,* $D(G) \leq \kappa(G)$.

Conjecture 3 has been verified for many particular groups; for more information one can refer to [10]. In 2003, Dimitrov [4] proved that $D(G) \leq c(r)\kappa(G)$ where $c(r)$ is a positive constant which depends only on r. Recently the second author [25] improved this bound to

$$D(G) < \begin{cases} (c(r) - r - 3)\kappa(G) & \text{if } \ 4 \leq n_1 \leq 2^{r-1} - 1 \\ (c(r) - r\ell_r)\kappa(G) & \text{if } \ n_1 \geq 2^{r-1}, \end{cases}$$

where $c(r)$ is a constant depending only on r and

$$\ell_r = \frac{(2^{r-1} - 1)(r - 1) + 1}{r(r - 1)}.$$

Definition 3. We denote by $\nu(G)$ the smallest non-negative integer t such that every zero-free sequence S in G of length $t \geq \nu$ has all its holes in some proper coset of G, i.e., $G \setminus (\sum(S) \cup \{0\}) \subset a + H$ for some proper subgroup H and for some $a \in G \setminus H$.

Note that $\nu(\mathbb{Z}_2) = 0$. The first author [9] proved that $\nu(G) + 1 \leq D(G) \leq \nu(G) + 2$. Also, it is known by the result of van Emde Boas [28] that if G is either cyclic or a p-group, then $D(G) = \nu(G) + 2$. The following was conjectured by the first author;

Conjecture 4. (Gao, [9]) *For every finite abelian group* G*, we have* $D(G) = \nu(G) + 2$.

In 2003, Dimitrov gave an upper bound for $D(G)$ when $G = \mathbb{Z}_n^d$ using covering systems modulo n. More precisely, we define the terminology as follows;

Definition 4. Let $n > 1$ be any positive integer. Let

$$M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \dots & & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mr} \end{pmatrix} a_{ij} \in \mathbb{Z}_n$$

be an $m \times r$ matrix over $\mathbb{Z}_n$. Let $R = (a_1 a_2 \dots a_m)$ be a $m \times 1$ column vector over $\mathbb{Z}_n$. We call the tuple (M, R) to be a *covering system* if for every r-tuple $(x_1, x_2, \dots, x_r) \in \mathbb{Z}^r$, there exists $i \in \{1, 2, \dots, m\}$ such that

$$\sum_{j=1}^{r} a_{ij} x_j \equiv a_i \pmod{n}$$

has a solution.

A finite dimensional matrix M over $\mathbb{Z}_n$ is said to be a *cover* if it is the matrix of some covering system.

For any given positive integers r and n, we denote $c(n, r)$ to the least positive integer t such that all $t \times r$ matrices over $\mathbb{Z}_n$ are covers.

Using these notions, Dimitrov [4] proved that for all positive integers r and $n > 1$, we have,

$$D(\mathbb{Z}_n^r) \leq c(n, r).$$

and he conjectured the following.

Conjecture 5. (Dimitrov, [4]) For all positive integers r and $n > 1$, we have

$$D(\mathbb{Z}_n^r) = c(n, r).$$

2.2 Davenport constant for non-abelian groups.

Olson and White [22] proved that $D(G) \leq (|G| + 1)/2$ for any non-cyclic group G. Also, trivially one observes that $D(G) \leq d(G)$. Since every group of order p is cyclic, the first non-trivial class of non-abelian group is of order $2p$ where p is an odd prime. If G is of order $2p$, then the first author and Zhuang [12] proved that $D(G) = p + 1$. Recently, Dimitrov [4] proved that $D(G \oplus \mathbb{Z}_{|G|}) \leq 2|G| - 1$ for any finite solvable group G. If H is a normal subgroup of G, then Delorme *et al.*, [3] proved that $D(G) \geq D(H) + D(G/H) - 1$. It is obvious from the definition that $D(G) \leq d(G)$. So, any reasonable bound for $d(G)$ gives a bound for $D(G)$ as well. But, providing a reasonable bound for $d(G)$ seems to be another hard problem. We have the following conjecture of Dimitrov [6].

Conjecture 6. (Dimitrov, [6]) Let G be any finite group whose complex irreducible representations (up to equivalence) have degrees $d_1, d_2, \dots, d_r$, then

$$d(G) \leq \sum_{i=1}^{r} d_i.$$

When G is a non-abelian p-group, then we have better known result for $d(G)$. Since G is a p-group, $\mathbb{F}_pG$ is a group algebra. Its Jacobson radical J is an augmentation ideal and is nilpotent. Then its nilpontency class is called the *Loewy length* of $\mathbb{F}_pG$ and is denoted by $L(G)$. Dimitrov [5] proved that

$$d(G) \leq L(G).$$

He conjectured the following;

Conjecture 7. (Dimitrov, [5]) For all finite p-group G, we have $d(G) = L(G)$.

Note that Conjecture 7 is true for abelian p-group by the result of Olson [21] and Jennings [14].

3 Proof of Main Theorem

We start this section with the statement of the following deep theorem of Kemperman [15].

Theorem 2. *If A and B are two non-empty finite subsets of a group G such that $0 \in A \cap B$, and $0 = a + b, a \in A, b \in B$ implies that $a = b = 0$. Then,*

$$|A + B| \geq |A| + |B| - 1.$$

Lemma 1. *Let S be a sequence in G of length at least $|G|$. Let $g \in G$ be the element appearing in S maximum number of, say h, times. Then $0 \in \sum_{\leq h}(S)$ where $\sum_{\leq h}(S) = \cup_{i=1}^{h} \sum_i(S)$ and $\sum_i(S)$ denotes the set of all possible sums of i elements of S.*

Proof: One can distribute S into h non-empty subsets $B_1, B_2, \ldots, B_h$, such that $\sum |B_i| = |S|$. For any two nonempty subsets A, B of G, let $A \oplus B = A \cup B \cup (A + B)$, and this definition can be generalized to three or more subsets by induction.

Assume to the contrary that $0 \notin \sum_{\leq h}(S)$, then $0 \notin B_i$ and

$$0 \notin B_1 \oplus B_2 \subset B_1 \oplus B_2 \oplus B_3 \subset \cdots \subset B_1 \oplus B_2 \oplus B_3 \oplus \cdots \oplus B_h.$$

Set $A_i = \{0\} \cup B_i$ for $i = 1, \ldots, h$. Then, by Theorem 2, we obtain, $|A_1 + A_2| \geq |A_1| + |A_2| - 1 = |B_1| + |B_2| + 1$. Since $0 \notin B_1 \oplus B_2 \oplus B_3$, one can apply Theorem 2 to $A_1 + A_2 = \{0\} \cup (B_1 \oplus B_2)$ and $A_3 = \{0\} \cup B_3$ to get

$$|A_1+A_2+A_3| \geq |A_1+A_2|+|A_3|-1 \geq |B_1|+|B_2|+1+|B_3|+1-1 = |B_1|+|B_2|+|B_3|+1.$$

Continuing this process, finally we arrive at:

$$|A_1 + A_2 + \cdots + A_h| \geq |B_1| + |B_2| + \cdots + |B_h| + 1 = |G| + 1,$$

a contradiction. □

Proof of the Main Theorem: Let $S = (a_1, a_2, \ldots, a_\ell)$ where $\ell = |G| + D(G) - 1$ be a sequence in G. By our hypothesis, we know that some element, say, $a_\ell \in \mathbf{Z}(G)$ is repeated maximum number of, say h, times in S. We can assume that $h \leq |G| - 1$; otherwise, we are done. As $a_\ell \in \mathbf{Z}(G)$, we have $a_\ell + x = x + a_\ell$ for every $x \in G$. Therefore, we can translate, if necessary, the given sequence by a_ℓ and can assume that 0, the zero element is repeated h times. Thus, we have,

$$S = \left(a_1, a_2, \ldots, a_{\ell-h}, \underbrace{0, 0, \ldots, 0)}_{h \text{ times}} \text{ and } S_1 = (a_1, a_2, \ldots, a_{\ell-h} \right).$$

Clearly, $\ell - h = |G| - 1 + D(G) - h \geq D(G)$.

We distinguish two cases here.

Case (i). $(\ell - h \leq |G|)$

Since $\ell - h \geq D(G)$, by the definition of $D(G)$, there exist distinct indices $i_1, i_2, \ldots, i_k$ from $1, 2, \ldots, \ell - h$ such that $a_{i_1} + a_{i_2} + \cdots + a_{i_k} = 0$. Choose k to be the maximal possible integer t such that this happens in S_t. This can be done by applying all possible permutations on the indices $\{1, 2, \ldots, \ell - h\}$. Hence by the maximality of k, it is clear that $|G| - 1 + D(G) - h - k \leq D(G) - 1$, in turn this implies $k \geq |G| - h$ and hence $|G| - h \leq k \leq |G|$. Therefore, we can get

$$\underbrace{0 + 0 + \cdots + 0}_{|G|-k \text{ times}} + a_{i_1} + a_{i_2} + \cdots + a_{i_k} = 0 \text{ in } G,$$

as desired.

Case (ii) $(\ell - h \geq |G| + 1)$

By Lemma 1, one can find t disjoint zero-sum subsequences $T_1, \ldots, T_t$ of S_1 such that $2 \leq |T_i| \leq h$, and that $|S_1(T_1 \ldots T_t)^{-1}| \leq |G| - 1$. Let W be the maximal zero-sum subsequence of $S_1(T_1 \ldots T_t)^{-1}$ (if it exists). If $|W| \geq |G| - h$, then we are done, by the argument as in Case (i). Otherwise, $|W| \leq |G| - h - 1$. By the maximality of W, we see that $|S_1(T_1 \ldots T_t)^{-1}W^{-1}| \leq D(G) - 1$. Therefore,

$$|W| + |T_1| + \cdots + |T_t| \geq \ell - h - (D(G) - 1) \geq |G| - h.$$

Note that since $2 \leq |T_i| \leq h$, we infer that, $|G| - h \leq |W| + |T_1| + \cdots + |T_k| \leq |G|$ for some $k \in \{1, 2, \ldots, t\}$. But $WT_1 \ldots T_k$ is zero-sum and we are done, as we have h number of 0's outside S_1. $\square$

Acknowledgment. The first author is supported by NSFC with grant number 10271080. We are grateful to the referee for many useful suggestions for the better presentation of the paper. Also we are thankful to him/her for pointing out typos.

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

[3] C. Delorme, O. Ordaz and D.Quiroz, Some remarks on Davenport constant, *Discrete Math.,* **237** (2001), 119-128.

[4] V. Dimitrov, Zero-sum problems in finite groups, Research Science Institute Students Reports, 2003, *The center for excellence in education, Vienna*, pg. 9-18.

[5] V. Dimitrov, On the strong Davenport constant of non-abelian finite p-groups, *Math. Balkanica (N.S.)*, **18** (2004), no. 1-2, 131-140.

[6] V. Dimitrov, A zero-sum result for non-abelian finite groups, *Preprint*, 2004.

[7] W. D. Gao, A combinatorial problem on finite abelian group, *J. Number Theory*, **58** (1996), 100-103.

[8] W. D. Gao, An improvement of Erdős-Ginzburg-Ziv theorem, *Acta Math. Sinca*, **39** (1996), 514-523.

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

[10] W. D. Gao, On a combinatorial problem connected with factorizations. *Colloq. Math.*, **72** (1997), no. 2, 251-268.

[11] W. D. Gao and A. Geroldinger, On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, *Integers*, **3** (2003), A8, 45 pp. (electronic).

[12] W. D. Gao and J. Zhuang, Erdős-Ginzburg-Ziv theorem for Dihedral groups of large prime index, To appear in: *European J. Combinatorics.*

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

[14] S. A. Jennings, The structure of the group ring of a p-group over modular field, *Trans. Amer. Math. Soc.*, **50** (1941), 175-185.

[15] J. H. Kemperman, On complexes in a semigroup, *Nederl. Akad. Wetensch. Proc. Ser. A.*, **59** (1956), 247-254.

[16] M. Mazur, A note on the growth of Davenport's constant, *Manuscripta Math.*, **74** (1992), no. 3, 229-235.

[17] R. Meshulam, An uncertainity inequality and zero subsums, *Discrete Math.*, **84** (1990), 197-200.

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

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

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

[21] J. E. Olson, On a Combinatorial Problem of Erdős, Ginzburg, and Ziv, *J. Number Theory*, **8** (1976), 52-57.

[22] J. E. Olson and E. T. White, Sums from a sequence of group elements, *Number theory and algebra,*, Academic Press, New York, (1977), 215-222.

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

[24] P. Rath, K. Srilakshmi and R. Thangadurai, On Davenport's constant, *Preprint*, 2006.

[25] R. Thangadurai, Non-canonical extensions of Erdő-Ginzburg-Ziv Theorem, *Integers*, (2002), A7, 14pp (electronic).

[26] R. Thangadurai, A remark on an upper bound for Davenport's constant, Preprint, 2004.

[27] T. Yuster, Bounds for counter-example to addition theorem in solvable groups, *Arch. Math.*, **51** (1988), 223-231.

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

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