Proc. Indian Acad. Sci. (Math. Sci.) Vol. 117, No. 2, May 2007, pp. 147–158.

A variant of Davenport's constant

R THANGADURAI

Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211 019, India
E-mail: thanga@hri.res.in

MS received 25 July 2006; revised 27 September 2006

Abstract. Let p be a prime number. Let G be a finite abelian p-group of exponent n (written additively) and A be a non-empty subset of $]n[:= \{1, 2, \ldots, n\}$ such that elements of A are incongruent modulo p and non-zero modulo p. Let $k \geq D(G)/|A|$ be any integer where $D(G)$ denotes the well-known Davenport's constant. In this article, we prove that for any sequence $g_1, g_2, \ldots, g_k$ (not necessarily distinct) in G, one can always extract a subsequence $g_{i_1}, g_{i_2}, \ldots, g_{i_\ell}$ with $1 \leq \ell \leq k$ such that

$$\sum_{j=1}^{\ell} a_j g_{i_j} = 0 \text{ in } G,$$

where $a_j \in A$ for all j. We provide examples where this bound cannot be improved. Furthermore, for the cyclic groups, we prove some sharp results in this direction. In the last section, we explore the relation between this problem and a similar problem with prescribed length. The proof of Theorem 1 uses group-algebra techniques, while for the other theorems, we use elementary number theory techniques.

Keywords. Davenport's constant; zero-sum problems; abelian groups.

1. Introduction

Let G be a finite abelian group additively written. Let n be the exponent of G. Let $\emptyset \neq A \subset]n[$ where $]n[:= \{1, 2, \ldots, n\}$. The set of all integers is denoted by $\mathbb{Z}$, while the set of all positive integers is denoted by $\mathbb{N}$. Also, let p be a prime number. The finite field with p elements is denoted by $\mathbb{F}_p$ or $\mathbb{Z}_p$. Also, direct sum of d copies of $\mathbb{Z}_p$ is denoted by $\mathbb{Z}_p^d$. For any integer $x \geq 1$, we denote $]x[$ for $\{1, 2, \ldots, x\}$.

Since G is an abelian group, G is a $\mathbb{Z}$-module. As a $\mathbb{Z}$-module, one has $m_1 g_1 + m_2 g_2 + \cdots + m_k g_k \in G$ where $g_i \in G$ and $m_i \in \mathbb{Z}$. Note that when $m_i \geq n$, then we can write $m_i = \ell n + r$ with $r < n$. Since n is the exponent of G, for any $g \in G$, we get, $m_i g = \ell n g + r g = r g$. Also, if $m_i < 0$, then $m_i g = |m_i|(-g)$. Therefore, it is enough to vary the subset A among the subsets of $]n[$ instead of the set of all integers. Hence, among the relations of the form $m_1 g_1 + m_2 g_2 + \cdots + m_k g_k$ with $m_i \in]n[$, there may be many such linear combinations equal to 0 in G. This motivates us to make the following definition.

DEFINITION

Davenport's constant for G with respect to A is denoted by $d_A(G)$ and is defined to be the least positive integer t such that given any sequence $S = (g_1, g_2, \ldots, g_t)$ in G, we can always extract a subsequence $g_{i_1}, g_{i_2}, \ldots, g_{i_\ell}$ with $1 \leq \ell \leq t$ such that

$$\sum_{j=1}^{\ell} a_j g_{i_j} = 0 \text{ in } G, \tag{1}$$

where $a_j \in A$ for all j.

When $A = \{a\} \subset]n[$ with $(a, n) = 1$, the definition of $d_A(G)$ is nothing but the well-known Davenport's constant which is denoted by $D(G)$. It is easy to prove that $D(\mathbb{Z}_n) = n$.

Olson, in [6] and [7], proved that

(i) when $G \sim \mathbb{Z}_m \oplus \mathbb{Z}_n$, where $1 < m|n$ integers, we have $D(G) = m + n - 1$;
(ii) when $G \sim \mathbb{Z}_{p^{e_1}} \oplus \mathbb{Z}_{p^{e_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_l}}$, where $1 \le e_1 \le e_2 \le \cdots \le e_l$ are integers, $D(G) = 1 + \sum_{i=1}^{l}(p^{e_i} - 1)$.

It is seemingly a difficult problem to find the exact value of $D(G)$ for all G other than the above mentioned groups.

If $n \in A \subset]n[$, then, clearly, $d_A(G) = 1$. Thus, we can always assume that $A \subset]n[$ and $1 \le |A| < n$ and $n \notin A$.

Problem. Find the value of $d_A(G)$ for all non-empty subsets A of $]n[$ and for all finite abelian groups G of exponent n.

In this article, we prove the following theorem.

Theorem 1. *Let $G \sim \mathbb{Z}_{p^{e_1}} \oplus \mathbb{Z}_{p^{e_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_l}}$ where $1 \le e_1 \le e_2 \le \cdots \le e_l$ are integers. Then, for any non-empty subset A of $]p^{e_l}[$ such that the elements of A are incongruent modulo p and non-zero modulo p, we have*

$$d_A(G) \le \left\lceil \frac{1}{|A|}\left(1 + \sum_{i=1}^{l}(p^{e_i} - 1)\right)\right\rceil$$

where $\lceil x \rceil$ denotes the smallest positive integer greater than or equal to x.

COROLLARY 1.1

Let $G \sim \mathbb{Z}_p^d$, where $d \ge 1$ integer. Then for any non-empty subset A of $]p - 1[$, we have

$$d_A(G) \le \left\lceil \frac{1}{|A|}(d(p-1) + 1)\right\rceil.$$

COROLLARY 1.2

Let $G \sim \mathbb{Z}_p^d$, where $d \ge 1$ integer. If

(a) $A =]p - 1[\subset]p[$, *then* $d_A(G) = d + 1$;
(b) $A_1 = \{a \in]p - 1[: a \equiv x^2 (\mathrm{mod}\ p)$ *for some* $x \in]p[\}$, *then* $d_{A_1}(G) = 2d + 1$;
(c) $A_2 = \{a \in]p - 1[: a \not\equiv x^2 (\mathrm{mod}\ p)$ *for all* $x \in]p[\}$, *then* $d_{A_2}(G) = 2d + 1$;
(d) $A_3 = \{a \in]p - 1[: a$ *generates* $\mathbb{F}_p^*\}$, *then* $d_{A_3}(G) = 2d + 1$;
(e) $A_4 = \{a \in]p - 1[: a \in A_2 \backslash A_3\}$, *then* $d_{A_4}(G) = 2d + 1$ *holds for all primes* $p \ne 2^{2^m} + 1$ *for some* $m \in \mathbb{N}$.
(f) $A_5 \subset]p - 1[$ *such that* $|A_5| = (p - 1)/2$ *and if* $x \in A_5$, *then* $p - x \notin A_5$, *then* $d_{A_5}(\mathbb{Z}_p^d) = 2d + 1$.

(g) $A =]r[\subset]p[$ *and* $r \geq d$, *then*

$$d_A(G) = \left\lceil \frac{d(p-1)+1}{r} \right\rceil.$$

From Corollary 1.2(a), (b), (c), (f) and (g), it is clear that the bound stated in Corollary 1.1 is tight for many subsets $A \subset]p[$, while for the subsets A_3 and A_4, Corollary 1.1 provides a weaker bound, as $|A_3| = \phi(p-1)$ and $|A_4| = (p-1)/2 - \phi(p-1)$.

Open problem. For any finite abelian group G of exponent n, classify all the non-empty subsets A of $]n[$ such that

$$d_A(G) \leq \left\lceil \frac{D(G)}{|A|} \right\rceil.$$

In §3, we prove some elementary but sharp results for the cyclic groups. In fact, one of the results says that when $A = \{a \in]n[: (a, n) = 1\}$, then $d_A(\mathbb{Z}_n) = 1 + \Omega(n)$. It is easy to see that $1 + \Omega(n) > d_A(\mathbb{Z}_n)/|A| = n/\phi(n)$ whenever $n = p^r$ for all integers $r \geq r_0$. Therefore, in the above open problem, the upper bound does not hold for all non-empty subsets A.

In §4, we explore the relation between $d_A(G)$ and the associated constants for the existence of similar weighted sum of length $|G|$ or the exponent of G. We prove some results and state a conjecture related to this relation.

2. Proof of Theorem 1

Let p be any prime number. Throughout this section, we assume that G is a finite abelian p-group written *multiplicatively*. Therefore, $G \sim \mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_l}}$, where $1 \leq e_1 \leq e_2 \leq \cdots \leq e_l$ are integers. Let $n := p^{e_l}$ be its exponent. Also, we denote the identity element of G by $\mathbf{e}$. We shall start with two lemmas which are crucial for the proof of Theorem 1.

Lemma 1.1 [8]. *Let p be a prime number and $r \geq 1$ be an integer. Let $B = \{0, b_1, b_2, \ldots, b_r\}$ be a non-empty subset of $]p-1[\cup \{0\}$ such that $b_i \not\equiv b_j \pmod{p}$ for all $i \neq j$. Then there exists a polynomial*

$$f(x) = c_0 + c_{b_1}x^{b_1} + \cdots + c_{b_r}x^{b_r} \in \mathbb{F}_p[x]$$

such that $(1-x)^r$ divides $f(x)$ and $c_0 = f(0) \neq 0$.

We recall that the group algebra $\mathbb{F}_p[G]$ is a $\mathbb{F}_p$-vector space with G as its basis. Hence, any element $\tau \in \mathbb{F}_p[G]$ can be written as $\tau = \sum_{g \in G} a_g g$, where $a_g \in \mathbb{F}_p$. Also, note that $\tau = 0 \in \mathbb{F}_p[G]$ if and only if $a_g = 0$ for all $g \in G$.

Lemma 1.2 [6]. *If $g_1, g_2, \ldots, g_s$ is a sequence in G with $s \geq 1 + \sum_{i=1}^{l}(p^{e_i} - 1)$, then the element*

$$\prod_{i=1}^{s}(1 - g_i) = 0 \in \mathbb{F}_p[G].$$

Proof of Theorem 1. Let $A = \{a_1, a_2, \ldots, a_r\} \subset]n[$ such that $a_1 < a_2 < \cdots < a_r$ and $a_i \not\equiv a_j \pmod{p}$ for $i \neq j$. Set $B = A \cup \{0\}$. Consider the group algebra $\mathbb{F}_p[G]$. Let $k \geq (1 + \sum_{i=1}^{l}(p^{e_i} - 1))/r$ be any integer where $r = |A|$. Let $S = (g_1, g_2, \ldots, g_k)$ be any given sequence in G of length k. To prove the theorem, it is enough to prove the existence of a subsequence $g_{i_1}, \ldots, g_{i_\ell}$ with $1 \leq \ell \leq k$ such that

$$\prod_{j=1}^{\ell} g_{i_j}^{a_{i_j}} = \mathbf{e} \text{ in } G,$$

where $a_{i_j} \in A$ for all j.

By Lemma 1.1, we have a polynomial $f(x) \in \mathbb{F}_p[x]$ associated with B and $f(x) = (1-x)^r F(x)$ for some polynomial $F(x) \in \mathbb{F}_p[x]$.

Let $\sigma = \prod_{i=1}^{k} f(g_i)$. Clearly σ is the element in the group algebra $\mathbb{F}_p[G]$. In fact, as G is abelian, we have

$$\sigma = \prod_{i=1}^{k} F(g_i) \prod_{i=1}^{k} (1 - g_i)^r \in \mathbb{F}_p[G].$$

Since $kr \geq 1 + \sum_{i=1}^{l}(p^{e_i} - 1)$, by Lemma 1.2, we see that

$$\prod_{i=1}^{k} (1 - g_i)^r = 0 \text{ in } \mathbb{F}_p[G]$$

and hence, $\sigma = 0$ in $\mathbb{F}_p[G]$.

Set $a_0 = 0$ and

$$f(x) = \lambda_{a_0} + \lambda_{a_1} x^{a_1} + \cdots + \lambda_{a_r} x^{a_r} \in \mathbb{F}_p[x].$$

Then, on the other hand, we can expand the product and see that σ is of the following form:

$$0 = \sigma = \prod_{j=1}^{k} f(g_j) = \prod_{j=1}^{k} \left(\sum_{i=0}^{r} \lambda_{a_i} g_j^{a_i} \right) \in \mathbb{F}_p[G]. \tag{2}$$

The constant term of the above product is $\lambda_{a_0}^k \mathbf{e}$. Since, by Lemma 1.1, we know that $\lambda_{a_0} \neq 0$, the constant term in (2) is non-zero. But since $\sigma = 0 \in \mathbb{F}_p[G]$, we conclude that there is some other contribution to $\mathbf{e}$ in the above product. That is, we have

$$\prod_{j=1}^{\ell} g_{i_j}^{a_{i_j}} = \mathbf{e} \text{ with } a_{i_j} \in A.$$

Hence the theorem. □

Proof of Corollary 1.1. Since $G \sim \mathbb{Z}_p^d$, and $A \subset]p-1[$, any two elements of A are incongruent modulo p. Hence, by Theorem 1, we get the result. □

Proof of Corollary 1.2. (a). The upper bound follows from Corollary 1.1. Indeed, since $A =]p-1[$, we have $|A| = p - 1$. Therefore, by Corollary 1.1, we get

$$d_A(\mathbb{Z}_p^d) \leq \left\lceil \frac{d(p-1)+1}{p-1} \right\rceil = d + 1.$$

For the lower bound, consider the sequence $(e_1, e_2, \ldots, e_d)$ in $\mathbb{Z}_p^d$ with $e_j = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ where 1 appears in the jth coordinate and 0 elsewhere. Then clearly, eq. (1) is not satisfied for $A =]p-1[$.

To prove the assertions (b)–(e) at one stroke, we prove the following claim.

Claim. Let $S = (g_1, g_2, \ldots, g_{2d+1})$ be any sequence in $\mathbb{Z}_p^d$ of length $2d+1$. Let $c \in \mathbb{Z}_p$ be a fixed non-zero element such that

$$c \in \begin{cases} A_1 & \text{for proving (b)} \\ A_2 & \text{for proving (c)} \\ A_3 & \text{for proving (d)} \\ A_4 & \text{for proving (e)} \end{cases}. \tag{3}$$

Then, for each $i = 1, 2, 3, 4$, the sequence S satisfies (1) with coefficients a_j in A_i whenever $c \in A_i$.

First note that this claim clearly implies that $d_{A_i}(\mathbb{Z}_p^d) \leq 2d+1$ for all $i = 1, 2, 3, 4$. Also note that $A_4 = \emptyset$ whenever p is of the form $2^{2^m}+1$. Hence while proving (e), we need to assume that $p \neq 2^{2^m}+1$.

Since $g_j \in \mathbb{Z}_p^d$ for each $j = 1, 2, \ldots, 2d+1$, we put $g_j = (g_{1j}, g_{2j}, \ldots, g_{dj})$ where $g_{lj} \in \mathbb{Z}_p$ for all $l = 1, 2, \ldots, d$. Let

$$f_l(X_1, X_2, \ldots, X_{2d+1}) = \sum_{j=1}^{2d+1} g_{lj} c X_j^2$$

for all $l = 1, 2, \ldots$ and d be the system of homogeneous equations over $\mathbb{Z}_p$. Since the total degree of f_l's is equal to $2d <$ the number of variables involved, by the Chevalley–Warning theorem, there exists a non-zero solution in $\mathbb{Z}_p^{2d+1}$ to the system. Let $(y_1, y_2, \ldots, y_{2d+1}) \in \mathbb{Z}_p^{2d+1}$ be a non-zero solution and let

$$I = \{j \in \{1, 2, \ldots, 2d+1\} : y_j \not\equiv 0 (\mathrm{mod}\ p)\},$$

which is non-empty. Therefore, we get

$$0 \equiv \sum_{j \in I} g_{lj} c y_j^2 (\mathrm{mod}\ p) \ \text{ for all } l = 1, 2, \ldots, d.$$

By putting $k_j = c y_j^2$ for all $j \in I$, we have

$$\sum_{j \in I} g_{1j} k_j \equiv 0 (\mathrm{mod}\ p), \sum_{j \in I} g_{2j} k_j \equiv 0 (\mathrm{mod}\ p), \ldots, \sum_{j \in I} g_{dj} k_j \equiv 0 (\mathrm{mod}\ p)$$

and hence we arrive at

$$\sum_{j \in I} g_j k_j = (0, 0, \ldots, 0) \text{ in } \mathbb{Z}_p^d.$$

Now, note that for each $i = 1, 2, 3, 4$, if $c \in A_i$, then $k_j \in A_i$ for all $j \in I$. Hence, the sequence S satisfies the claim.

To prove the assertions (b)–(e), it is enough to prove the lower bound.
Let c be a fixed non-zero element in $\mathbb{Z}_p$ such that

$$c = \begin{cases} \text{a quadratic non-residue modulo } p, & \text{if } p \equiv 1 (\text{mod } 4) \\ 1, & \text{if } p \equiv 3 (\text{mod } 4) \end{cases}.$$

Consider the sequence $S = (e_1, e_2, \ldots, e_d, f_1, f_2, \ldots, f_d)$ in $\mathbb{Z}_p^d$ of length $2d$ where $e_j = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ and $f_j = (0, 0, \ldots, 0, c, 0, \ldots, 0)$ (in e_j (similarly, in f_j), the element 1 (similarly, c) appears in the jth coordinate and 0 elsewhere). If any subsequence of S satisfies eq. (1), then, in the jth coordinate, we have the following:

$$a + cb \equiv 0 (\text{mod } p), \quad \text{where } a, b \in A_i.$$

Note that a and $a^{-1} \in \mathbb{Z}_p^*$ are either both quadratic residues or both quadratic non-residues. Therefore, ab^{-1} is a quadratic residue modulo p, as $a, b \in A_i$. We know that $p \equiv 1 (\text{mod } 4)$ if and only if -1 is a quadratic residue modulo p. Therefore, we get $-ab^{-1}$ is a quadratic residue modulo p, whenever $p \equiv 1 (\text{mod } 4)$ and $-ab^{-1}$ is a quadratic non-residue, if $p \equiv 3 (\text{mod } 4)$. This contradicts the fact that $c \equiv -ab^{-1} (\text{mod } p)$ is a quadratic non-residue modulo p, in the case when $p \equiv 1 (\text{mod } 4)$, while if $p \equiv 3 (\text{mod } 4)$, $c = 1$ is a quadratic residue. Hence, for each $i = 1, 2, 3, 4$, the sequence S does not satisfy eq. (1) with coefficients $a_j \in A_i$. Thus, we arrive at the assertions (b)–(e).

(f) By assumption $A_5 \subset]p - 1[$ and $|A_5| = (p - 1)/2$. Also, if $x \in A_5$, then $p - x \notin A_5$. Therefore, to get the lower bound, consider the sequence $(e_1, e_1, e_2, e_2, \ldots, e_d, e_d)$ in $\mathbb{Z}_p^d$ of length $2d$ and clearly, eq. (1) is not satisfied for A_5. Since $|A_5| = (p - 1)/2$, the upper bound, by Corollary 1.1, is $d_{A_5}(G) \leq 2d + 1$ and thus the result.

(g) The upper bound follows from Corollary 1.1. To prove the lower bound, consider the sequence

$$S = (\underbrace{e_1, \ldots, e_1}_{m \text{ times}}, \ldots, \underbrace{e_d, \ldots, e_d}_{m \text{ times}})$$

in $\mathbb{Z}_p^d$ length dm where $m = \left\lceil \frac{p}{r} \right\rceil - 1 = \left\lfloor \frac{p}{r} \right\rfloor$. Clearly, any subsequence of S does not satisfy (1) and hence $d_A(G) \geq dm + 1 = d \left\lfloor \frac{p}{r} \right\rfloor + 1$. Since $r \geq d$, we have

$$d \left\lfloor \frac{p}{r} \right\rfloor + 1 = \left\lceil \frac{d(p-1)+1}{r} \right\rceil.$$

Thus, the corollary follows. □

3. Elementary results for the cyclic group

Let n be any composite positive integer.

Theorem 2. *For all $a \in]n[$, we have*

(i) $d_{\{a\}}(\mathbb{Z}_n) = n/(a, n)$ *where* (a, n) *denotes the gcd of* n *and* a;
(ii) $d_{\{a, n-a\}}(\mathbb{Z}_n) = 1 + \lfloor \log_2 n \rfloor$, *whenever* $(a, n) = 1$;

(iii) *whenever* $A = \{a\colon (a, n) = 1\} \subset]n[$, *we have*, $d_A(\mathbb{Z}_n) = 1 + \Omega(n)$, *where* $\Omega(n)$ *denotes the number of prime power divisors* > 1 *of* n;
(iv) *whenever* $A =]n-1[\subset]n[$, *we have*, $d_A(\mathbb{Z}_n) = 2$.

Proof.

(i) Whenever $(n, a) = 1$, the classical Davenport constant $D(\mathbb{Z}_n)$ and $d_{\{a\}}(\mathbb{Z}_n)$ are same and therefore the result follows easily. Hence, we assume that $(n, a) = d > 1$. Let $S = (a_1, a_2, \ldots, a_l)$ be any sequence in $\mathbb{Z}_n$ of length $l = n/d$.

We have to find a subsequence of S satisfying equation (1). That is, we need to find a subsequence, say, $a_{i_1}, a_{i_2}, \ldots, a_{i_r}$ such that

$$a\sum_{j=1}^{r} a_{i_j} \equiv 0(\text{mod } n) \Longrightarrow \frac{a}{d}\sum_{j=1}^{r} a_{i_j} \equiv 0 \bmod \left(\frac{n}{d}\right).$$

Since $(a/d, n/d) = 1$, it is enough to find a subsequence of S whose sum is divisible by n/d. Since $l \geq n/d$, this is possible by the classical Davenport constant for the group $\mathbb{Z}_{n/d}$. Thus, we have the required upper bound. The lower bound follows from the sequence $(a, a, \ldots, a)$ where a appears exactly $-1 + n/(n, a)$ times.

(ii) Given that $A = \{a, n-a\}$ with $(a, n) = 1$. To prove the lower bound, let $s = \lfloor \log_2 n \rfloor$. Then clearly, $2^s \leq n < 2^{s+1}$. Consider the sequence $S = (1, 2, 2^2, \ldots, 2^{s-1})$ in $\mathbb{Z}_n$ of length s. Then any zero sum with coefficients in A leads to an equation of the type

$$a(x - y) \equiv 0(\text{mod } n),$$

where

$$x = \sum_{i\in I} 2^i \quad \text{and} \quad y = \sum_{j\in J} 2^j$$

and $I \cup J$ is a partition of $\{1, 2, \ldots, s\}$. Since a is coprime to n, we get that $x \equiv y(\text{mod } n)$ and since both x and y are nonnegative integers smaller than n we get $x = y$, which is impossible because of the uniqueness of the binary expansion of a nonnegative integer. Hence, the sequence S does not satisfy (1).

For the upper bound, let $S = (a_1, a_2, \ldots, a_s)$ be any sequence in $\mathbb{Z}_n$ of length $s = 1 + \lfloor \log_2 n \rfloor$. Consider the set

$$\sum(S) := \left\{ \sum_{i\in I} aa_i\colon\ I \subset \{1, 2, \ldots, s\} \right\}.$$

Clearly, the set $\sum(S)$ contains 2^s elements. Since $n < 2^s$, it follows that there exist $I \neq J$ subsets of $\{1, 2, \ldots, s\}$ and satisfying

$$\sum_{i\in I} aa_i \equiv \sum_{j\in J} aa_j(\text{mod } n) \Longrightarrow \sum_{i\in I} aa_i + \sum_{i\in I}(n-a)a_i \equiv 0(\text{mod } n).$$

Note that if $i \in I \cap J$, then, in the above congruence, we have $aa_i + (n-a)a_i = na \equiv 0(\text{mod } n)$. Hence, we can assume that $I \cap J = \emptyset$ and this proves the upper bound.

(iii) To see the lower bound, let $n = p_1 p_2 \cdots p_s$ where p_is are prime divisors (not necessarily distinct) of n. The sequence $S = (1, p_1, p_1p_2, \ldots, p_1p_2 \ldots p_{s-1})$ in $\mathbb{Z}_n$ of length $\Omega(n)$ does not satisfy eq. (1).

For the upper bound[1], we use a result of Luca [5] stated in the next section. Let $k = 1 + \Omega(n)$, $g_1, g_2, \ldots, g_k$ be any elements in $\mathbb{Z}_n$ and consider the sequence $S = (g_1, \ldots, g_k, \underbrace{0, \ldots, 0}_{n-1 \text{ times}})$ in $\mathbb{Z}_n$ of length $n + \Omega(n)$. By Luca's result, there is a linear combination with coefficients in A of precisely n elements from S which is 0. Of those n elements, at most $n-1$ elements are 0's. Hence, we have zero sum of g_i's with coefficients in A which proves the upper bound.

(iv) The lower bound follows by taking $k = 1$ and $g_1 = 1$. For the upper bound, let g_1, g_2 be any two elements in $]n[$. If one of them is n, say $g_1 = n$, then $1 \cdot g_1 = 0$. If both are $< n$, then $(n - g_2)g_1 + g_1 \cdot g_2 \equiv 0 (\mathrm{mod}\ n)$ so we can take $a_1 = n - g_2$ and $a_2 = g_1$, both in $]n-1[$, which proves the result. Hence, the corollary follows. □

4. Relation between $d_A(G)$ and zero-sums of length $|G|$

Let G be a finite abelian group of exponent n and A be any non-empty subset of $]n[$.

By $ZS_A(G)$ (similarly, $s_A(G)$), we denote the least positive integer t such that for any given sequence $S = (g_1, g_2, \ldots, g_t)$ in G of length t has a non-empty subsequence, say, $g_{i_1}, g_{i_2}, \ldots, g_{i_m}$ satisfying

$$\sum_{j=1}^{m} a_j g_{i_j} = 0 \text{ in } G, \tag{4}$$

where $a_j \in A$ for all j and $m = |G|$ (similarly, $m = n$).

The following results are known for various subsets A and some groups:

1. When $A = \{a\}$ and $(a, n) = 1$, we have
$$ZS_A(G) = D(G) + |G| - 1$$
by [4], which generalizes the famous theorem of Erdös, Ginzburg and Ziv [3].
2. When $A = \{a, n-a\} \subset]n[$ and $(a, n) = 1$, we have
$$s_A(\mathbb{Z}_n) = ZS_A(\mathbb{Z}_n) = n + \lceil \log_2 n \rceil$$
by [1].
3. When $A = \{a \in]n[: (n, a) = 1\}$, we have
$$s_A(\mathbb{Z}_n) = ZS_A(\mathbb{Z}_n) = n + \Omega(n)$$
by [5].
4. When $A =]r[\subset]p[$, we have
$$s_A(\mathbb{Z}_p) = ZS_A(\mathbb{Z}_p) = p + [p/r]$$
by [2].

Note that, by the definition, $s_A(\mathbb{Z}_n) = ZS_A(\mathbb{Z}_n)$. Also, we have $ZS_A(G) > d_A(G) + |G| - 2$. Indeed, by the definition of $d_A(G)$, we have a sequence S in G of length $d_A(G) - 1$ and does not satisfy (1). Now consider the sequence

$$T = (S, \underbrace{0, 0, \ldots, 0}_{|G|-1 \text{ times}})$$

[1] One can also give a direct and elementary proof.

in G of length $d_A(G) + |G| - 2$. Clearly, by the construction, T does not satisfy (4) with $m = |G|$. Therefore, $ZS_A(G) \geq d_A(G) + |G| - 1$. We feel that the lower bound seems to be tight. More precisely, we have Theorems 3 and 4.

Conjecture 1. For any finite abelian group G with exponent n and for any non-empty subset A of $]n[$, we have

$$ZS_A(G) = |G| - 1 + d_A(G).$$

Using Theorem 2 and the results 1–4 stated above, we see that Conjecture 1 holds for those A's and G's. In support of Conjecture 1, we prove Theorems 3 and 4.

Lemma 3.1. *If* $s_A(\mathbb{Z}_n^d) = d_A(\mathbb{Z}_n^d) + n - 1$ *for some* $A \subset]n[$, *then we have*

$$ZS_A(\mathbb{Z}_n^d) = d_A(\mathbb{Z}_n^d) + n^d - 1.$$

Proof. Consider a sequence $S = (g_1, g_2, \ldots, g_\ell)$ in $\mathbb{Z}_n^d$ of length $\ell = d_A(\mathbb{Z}_n^d) + n^d - 1$. To prove the lemma, we have to prove that S has a subsequence satisfying (4) with $m = n^d$. By hypothesis, we know that $s_A(\mathbb{Z}_n^d) = d_A(\mathbb{Z}_n^d) + n - 1$. Since $\ell \geq s_A(\mathbb{Z}_n^d)$, clearly, there exists a subsequence S_1 of S of length n satisfying (4) with $m = n$. Since

$$|S| = \ell = d_A(\mathbb{Z}_n^d) + n^d - 1 = d_A(\mathbb{Z}_n^d) + n(n^{d-1} - 1) + n - 1,$$

we can extract disjoint subsequences $S_1, S_2, \ldots, S_k$ of S with $|S_i| = n$ for all $i = 1, 2, \ldots, k$ where $k = n^{d-1}$ satisfies (4). Note that the total length of the subsequence S_i is $n^{d-1}n = n^d$. Thus, we get

$$\sum_{i=1}^{k} \sum_{j=1}^{n} a_{ij} g_{ij} \equiv 0 (\mathrm{mod}\, n),$$

where $a_{ij} \in A$ and $g_{ij} \in S_i$ for all $i = 1, 2, \ldots, k$ and for all $j = 1, 2, \ldots, n$. Hence, we arrive at a subsequence L of S of length n^d satisfying (4). □

Theorem 3. *Let* $d \geq 1$ *be any integer. Let* p *be a prime number such that* $p \geq 2d + 1$. *Then*

$$s_{A_i}(\mathbb{Z}_p^d) = d_{A_i}(\mathbb{Z}_p^d) + p - 1 = 2d + p,$$

where A_i*'s* (*for* $i = 1, 2, 3, 4$) *are as defined in Corollary* 1.2.

Proof. Choose $c \in]p - 1[$ as in (3). Let $S = (g_1, g_2, \ldots, g_{2d+p})$ be a given sequence in $\mathbb{Z}_p^d$ of length $2d + p$. To conclude the proof of this theorem, we have to prove that for each $i = 1, 2, 3, 4$ the sequence S has a subsequence which satisfies (4) for A_i with $m = p$.

Since $g_i \in \mathbb{Z}_p^d$, we have

$$g_i = (g_{i1}, g_{i2}, \ldots, g_{id}) \text{ where } g_{ij} \in \mathbb{Z}_p \text{ for all } j = 1, 2, \ldots, d.$$

Now consider the homogeneous equations over the finite field $\mathbb{F}_p$ as follows:

$$f_j(X_1, X_2, \ldots, X_{2d+p}) = \sum_{i=1}^{2d+p} c g_{ij} X_i^2 \quad \text{for all } j = 1, 2, \ldots, d$$

and

$$g(X_1, X_2, \ldots, X_{2d+p}) = \sum_{i=1}^{2d+p} X_i^{p-1}.$$

Note that sum of the degrees of f_j and g is $2d + p - 1$ which is strictly less than the number of variables X_i's. Hence, by the Chevalley–Warning theorem, we have a non-trivial simultaneous solution over $\mathbb{F}_p$. Let $(y_1, y_2, \ldots, y_{2d+p}) \in \mathbb{F}_p^{2d+p}$ be a non-trivial solution and let

$$I = \{i \in \{1, 2, \ldots, 2d + p\} : y_i \not\equiv 0 (\text{mod } p)\} \neq \emptyset.$$

Then, we get

$$0 \equiv \sum_{i \in I} c g_{ij} y_i^2 (\text{mod } p)$$

and

$$0 \equiv \sum_{i \in I} y_i^{p-1} \equiv \sum_{i \in I} 1 = |I| (\text{mod } p),$$

as $y_i \not\equiv 0 (\text{mod } p)$ whenever $i \in I$ and by Fermat Little theorem, the above follows. Note that $|I| \neq 0$ and $|I| \leq 2d + p < 2p$. Thus, using this fact and the second congruence above, we get $|I| = p$. From the first congruence, we get

$$\sum_{i \in I} g_i c y_i^2 \equiv 0 (\text{mod } p),$$

where $(g_i)_{i \in I}$ is a subsequence of the given sequence with $|I| = p$. Also, note that $cy_i^2 \in A_j$ for all $i \in I$, whenever $c \in A_j$. Hence, the theorem follows. □

COROLLARY 3.1

Let $d \geq 1$ be an integer and $p \geq 2d + 1$ be any prime number. Then

$$ZS_{A_i}(\mathbb{Z}_p^d) = d_{A_i}(\mathbb{Z}_p^d) + p^d - 1 = p^d + 2d,$$

for all A_i's where $i = 1, 2, 3, 4$ as defined in Corollary 1.2(b), (c), (d) *and* (e).

Proof. Proof follows from Lemma 3.1 and Theorem 3. □

COROLLARY 3.2

Let $d \geq 1$ be any integer. Let $p \equiv 3 (\text{mod } 4)$ be a prime such that $p \geq 2d + 1$. Then

$$ZS_{A_5}(\mathbb{Z}_p^d) = d_{A_5}(\mathbb{Z}_p^d) + p^d - 1 = 2d + p^d,$$

where A_5 is defined in Corollary 1.2(f).

Proof. Since $p \equiv 3 (\text{mod } 4)$, we know that $-1 = p - 1$ is a quadratic non-residue modulo p. Therefore, x is a quadratic residue modulo p, $p - x$ is a quadratic non-residue modulo p and vice versa. Thus, we can re-write

$$A_5 = \{a \in]p - 1[: a \equiv x^2 (\text{mod } p) \text{ for some } x \in]p - 1[\},$$

or its compliment in $]p - 1[$. Hence, the result follows by Corollary 3.1. □

Theorem 4. *Let* $S = (g_1, g_2, \ldots, g_k)$ *be a sequence in* G *of length* $k = |G| + d_A(G) - 1$. *If* $0 \in G$ *appears in* S *at least* $d_A(G) - 1$ *times, then* S *satisfies eq.* (4) *with* $m = |G|$.

Proof. By rearranging the terms of S, we may assume that

$$S = (\underbrace{0, 0, \ldots, 0}_{h \text{ times}}, g_1, g_2, \ldots, g_{k-h}),$$

where $g_i \neq 0 \in G$. If $h \geq |G|$, then eq. (4) is trivially satisfied. Assume that $h \leq |G| - 1$. Therefore, we have

$$k - h = |G| + d_A(G) - 1 - h \geq d_A(G).$$

Therefore, by the definition of $d_A(G)$, we can find $W_1 = (g_{i_1}, g_{i_2}, \ldots, g_{i_r})$, a subsequence of S with $g_{i_j} \neq 0$ and $a_{i_j} \in A$ for $j = 1, 2, \ldots, r$ satisfying eq. (1) with $r \geq 1$. Choose W_1 to be the maximal subsequence having the above property. If $k - h - |W_1| \geq d_A(G)$, then again we choose another subsequence W_2 with non-zero elements g_is satisfying eq. (1). Hence, $W_1 W_2$ together satisfy eq. (1) which contradicts the maximality of W_1. This forces that $k - h - |W_1| \leq d_A(G) - 1$. Hence, we arrive at $|W_1| \geq |G| - h$. Therefore,

$$|G| - h \leq |W_1| \leq k - h \leq |G|.$$

Since we have at least h number of 0's outside W_1, eq. (4) is satisfied with $m = |G|$. Thus, the result is proved. □

Acknowledgment

The author is grateful to the referee for his/her extensive comments to improve the presentation of the paper.

References

[1] Adhikari S D, Chen Y G, Friedlander J B, Konyagin S V and Pappalardi F, Contributions to zero-sum problems, *Discrete Math.* **306** (2006) 1–10

[2] Adhikari S D and Rath P, Davenport constant with weights and some related questions, *Integers* **6** (2006) A30, pp. 6

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

[4] Gao W D, Addition theorems for finite abelian groups, *J. Number Theory* **53(2)** (1995) 241–246

[5] Luca F, A generalization of a classical zero-sum problem, *Discrete Math.* **307** (2007) 1672–1678

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

[7] Olson J E, A combinatorial problem on finite abelian groups, II, *J. Number Theory* **1** (1969) 195–199

[8] Troi G and Zannier U, On a theorem of J. E. Olson and an application (Vanishing sums in finite abelian p-groups), *Finite Fields and their Applications* **3** (1997) 378–384

Note added. It seems that much before H Davenport introduced the problem of Davenport's constant in 1966 (see for instance, H Davenport, Proceedings of the Midwestern Conference on Group Theory and Number Theory, Ohio State University, April, 1966), the problem was, historically, first studied and introduced by K Rogers in 1962 (K Rogers, A combinatorial problem in abelian groups, *Proc. Cambridge Philos. Soc.* **59** (1963) 559–562). Somehow this reference was overlooked and never quoted by the later authors.