Proc. Indian Acad. Sci. (Math. Sci.) Vol. 119, No. 3, June 2009, pp. 275–281.

Remarks on some zero-sum theorems

S D ADHIKARI, SANOLI GUN* and PURUSOTTAM RATH*

Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211 019, India
*Department of Mathematics and Statistics, Queen's University, Jeffrey Hall, 99 University Avenue, Kingston, ON, Canada K7L 3N6
E-mail: adhikari@mri.ernet.in; sanoli@mast.queensu.ca; rath@mast.queensu.ca

MS received 30 April 2008

Abstract. In the present paper, we give a new proof of a weighted generalization of a result of Gao in a particular case. We also give new methods for determining the weighted Davenport constant and another similar constant for some particular weights.

Keywords. Davenport constant; Gao's theorem; permanent.

1. Introduction

For a finite abelian group G, the Davenport constant $D(G)$ is the smallest natural number k such that any sequence of k elements in G has a non-empty subsequence whose sum is zero. Similarly, for an abelian group G of cardinality n, another combinatorial invariant is defined to be the smallest number k such that any sequence of k elements in G has a subsequence of length n whose sum is zero; this is denoted as $E(G)$. The following result of Gao [8] connects these two constants:

$$E(G) = D(G) + n - 1. \tag{1}$$

In [4] and [5], certain generalisations of the above constants were considered for the particular group $\mathbb{Z}/n\mathbb{Z}$. In a recent work [3], the following generalisations of both $E(G)$ and $D(G)$ for an arbitrary finite abelian group G of order n have been introduced. For a more elaborate account of this theme and further references, we refer to [2].

For a finite abelian group G and a finite subset $A \subseteq \mathbb{Z}$, the Davenport constant of G with weight A, denoted by $D_A(G)$, is defined to be the smallest number k such that for any sequence $(x_1, \ldots, x_k)$ of k elements in G, there exists a non-empty subsequence $(x_{j_1}, \ldots, x_{j_r})$ and $a_1, \ldots, a_r \in A$ such that

$$\sum_{i=1}^{r} a_i \, x_{j_i} = 0.$$

To avoid trivial cases, one assumes that the weight set A does not contain 0 and it is non-empty. Further, if $|G| = n$, one can assume that $A \subset \{1, 2, \ldots, n-1\}$.

Similarly, for any such A and an Abelian group G with $|G| = n$, the constant $E_A(G)$ is the smallest number k such that any sequence $(x_1, \ldots, x_k)$ of k elements in G, there exists $x_{j_1}, \ldots, x_{j_n}$ such that

$$\sum_{i=1}^{n} a_i \, x_{j_i} = 0$$

with $a_i \in A$.

When G is the cyclic group $\mathbb{Z}/n\mathbb{Z}$, we denote $E_A(G)$ and $D_A(G)$ by $E_A(n)$ and $D_A(n)$ respectively. Taking $A = \{1\}$, we retrieve the classical constants $D(G)$ and $E(G)$.

A result similar to the above result (1) of Gao is expected in the weighted set up too. Here one of the few general results known is the following one due to Adhikari and Chen [3]; one notes that it does not include the result (1) of Gao which corresponds to the case $|A| = 1$.

Theorem A. *Let G be a finite abelian group of order n and $A = \{a_1, \ldots, a_r\}$ be a finite subset of $\mathbb{Z}$ with $r \geq 2$. If $\gcd(a_2 - a_1, \ldots, a_r - a_1, n) = 1$, then*

$$E_A(G) = D_A(G) + n - 1. \tag{2}$$

Clearly Theorem A implies the following result.

Theorem 1. *Whenever the weight set A satisfies $|A| \geq 2$, we have*

$$E_A(p) = D_A(p) + p - 1.$$

However, it is clear that the argument used in the proof of Theorem 2 of [5] yields a proof of the above theorem. Here we give a new proof of Theorem 1 which is interesting on its own. It uses the theory of permanents. It should be mentioned that the idea of using permanents to tackle this type of problems was initiated by Alon (see [6] for instance, see also [1]).

In the present paper, we also give a new proof of the following result which had been proved in [5].

Theorem 2. *Let A be the set of quadratic residues. Then we have*

$$E_A(p) = p + 2,$$

and

$$D_A(p) = 3.$$

In the final section of this paper, we shall have few more remarks involving new proofs of some more zero-sum results.

2. Proof of the theorems

For the proof of Theorem 1, we require a result on permanents. We recall the definition of permanent of a matrix A. Given a matrix $A = (a_{i,j})$ of order $n \times n$, the permanent of A, denoted by $\mathrm{Per}(A)$, is defined by

$$\mathrm{Per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Thus it is similar to the determinant of A except that the sign of the permutations is absent. We state the following special case of the *permanent lemma* [6]; we sketch a proof of the result for the sake of completeness.

Lemma 1. *For a prime p, let $A = (a_{i,j})$ be a $(p-1) \times (p-1)$ matrix over the finite field $\mathbb{F}_p$. Suppose that its permanent* $\mathrm{Per}(A)$ *is non-zero. Then given any sequence of elements $b_1, b_2, \ldots, b_{p-1}$ in $\mathbb{F}_p$, there exists $\epsilon_1, \epsilon_2, \ldots \epsilon_{p-1} \in \{0, 1\}$ such that*

$$\sum_{j=1}^{p-1} \epsilon_j a_{ij} \neq b_i, \ \forall i.$$

For the proof of the above lemma, we need the following result which follows easily by induction on the number of variables m.

Lemma 2. *Let R be a commutative ring with unity. Let*

$$P(x_1, \ldots, x_m) = \sum_{I \subset \{1,\ldots,m\}} C_I \prod_{i \in I} x_i$$

be a multilinear polynomial with co-efficients in R. Then

$$P(x_1, \ldots, x_m) = 0, \quad \forall (x_1, \ldots, x_m) \in \{0, 1\}^m$$

implies that

$$C_I = 0, \quad \forall I,$$

that is, the polynomial P is identically zero.

Proof of Lemma 1. Suppose there is no $(\epsilon_1, \epsilon_2, \ldots \epsilon_{p-1}) \in \{0, 1\}^{p-1}$ satisfying the hypothesis. Then for all $(x_1, \ldots, x_{p-1}) \in \{0, 1\}^{p-1}$,

$$P(x_1, \ldots, x_{p-1}) := \prod_{i=1}^{p-1} \left(\sum_{j=1}^{p-1} x_j a_{ij} - b_i \right) = 0.$$

We then consider the polynomial $Q(x_1, \ldots, x_{p-1})$ which is obtained from P by expanding it and then replacing any higher power x_i^r of any variable x_i occurring in some monomial of $P(x_1, \ldots, x_{p-1})$ by x_i. For instance, a term of the form $cx_1^3 x_2 x_3^2$ with $c \in \mathbb{F}_p$ is replaced by $cx_1x_2x_3$ in this process. Now Q is multilinear and observing that $P(x_1, \ldots, x_{p-1}) = Q(x_1, \ldots, x_{p-1})$, for all $(x_1, \ldots, x_{p-1}) \in \{0, 1\}^{p-1}$, it follows from Lemma 2 that $Q(x_1, \ldots, x_{p-1})$ is the zero polynomial. However, the coefficient of $x_1 \ldots x_{p-1}$ in $Q(x_1, \ldots, x_{p-1})$ is the same as that in $P(x_1, \ldots, x_{p-1})$, which is $\mathrm{per}(A)$. This leads to a contradiction since $\mathrm{Per}(A)$ is assumed to be non-zero. This proves the lemma.

We now proceed to give a proof of Theorem 1.

Proof of Theorem 1. We begin by noting that for any non-empty weight set $A \subseteq \{1, \ldots, p-1\}$,

$$E_A(p) \geq D_A(p) + p - 1. \tag{3}$$

This follows by appending a sequence of $p-1$ zeros to a sequence S of length $D_A(p) - 1$ which does not have any subsequence which sums up to zero with weights in A.

Let A contain a, b with $1 \leq a < b \leq p-1$. Let $c_1, \ldots, c_m$ be any sequence of m elements of $\mathbb{F}_p$ where $m = D_A(p) + p - 1$.

First we assume that the number of non-zero elements in the above sequence is at least $p-1$. Without loss of generality, we assume that $c_i \neq 0$ for $1 \leq i \leq p-1$. Consider the matrix $A = (a_{ij})_{(p-1)\times(p-1)}$ where for all i,

$$a_{ij} = (b-a)c_j, \quad 1 \leq j \leq p-1.$$

Consider the element $-a(c_1 + \cdots + c_p)$ in F_p and let $b_1, \ldots, b_{p-1}$ be the remaining elements of F_p. Since $\mathrm{per}(A) = (p-1)!(b-a)^{p-1}c_1c_2\ldots c_{p-1} \neq 0$, by using Lemma 1, there exists $\epsilon_1, \epsilon_2, \ldots \epsilon_{p-1} \in \{0, 1\}$ such that

$$\sum_{j=1}^{p-1} \epsilon_j(b-a)c_j = -a(c_1 + \cdots + c_p),$$

which can be re-written as

$$\sum_{j=1}^{p-1} (\epsilon_j(b-a)c_j + ac_j) + ac_p = 0.$$

Clearly, this shows that a sum of the subsequence $(c_1, \ldots, c_p)$ with coefficients in $\{a, b\}$ is zero.

Now we address the case when the given sequence has less than $p-1$ non-zero elements in it. We re-order the sequence in such a way that $c_1 = c_2 = \cdots = c_t = 0$ and the remaining elements are non-zero. We have $m - t < p - 1$. Let $B = \{r_1, \ldots, r_l\}$ be a subset of $\{t+1, \ldots, m\}$ which is maximal with respect to the property that there exists $a_1, \ldots, a_l \in A$ with

$$\sum_{j=1}^{l} a_j c_{r_j} = 0.$$

We claim that $l + t \geq p$. Indeed, if this were not the case, then the complement set

$$\{t+1, \ldots, m\} \setminus \{r_1, \ldots, r_l\}$$

would contain $m - t - l \geq D_A(p)$ elements and hence the corresponding sequence c_i with $i \in \{t+1, \ldots, m\} \setminus \{r_1, \ldots, r_l\}$ will contain a subsequence whose sum with weights from A is equal to zero. Appending this subsequence to the subsequence associated to B will violate the maximality of B. Hence $l + t \geq p$. Therefore, appending the sequence $\{c_i : i \in B\}$ to $c_1 = c_2 = \cdots = c_{p-l} = 0$, we get a sequence of length p with the desired property.

Thus we have

$$E_A(p) \leq D_A(p) + p - 1.$$

This together with (3) proves Theorem 1.

Proof of Theorem 2. We would require the following version of *Cauchy–Davenport inequality* (see [11] or [1] for instance):

$$|A_1 + A_2 + \cdots + A_h| \geq \min\left\{p, \sum_{i=1}^{h} |A_i| - h + 1\right\},$$

where $A_1, \ldots, A_h$ are non-empty subsets of $\mathbb{F}_p$.

First, we proceed to prove that

$$E_A(p) \leq p + 2.$$

If $p \leq 3$, noting that $2p - 1 \leq p + 2$, by EGZ theorem [7] (see also [1], [11] for instance) we have

$$E_A(p) \leq p + 2.$$

However, in these cases, we may retrieve the above by elementary pigeon-hole principle. For instance, if $p = 2$, then any sequence of $p + 2 = 4$ elements in $\mathbb{F}_2$ will have at least one element repeated twice.

If $p = 3$, then given any sequence of $p + 2 = 5$ elements, if all the elements of $\mathbb{F}_3$ occur, then we have $0 + 1 + 2 = 0$. Otherwise, one of the elements of $\mathbb{F}_3$ must occur at least thrice and once again we are done. So $E_A(p) \leq p + 2$, for $p \leq 3$.

From now onwards, we assume $p \geq 5$.

Let $X = \{a_1, \ldots, a_{p+2}\}$ be a sequence of $p + 2$ elements in $\mathbb{F}_p$. If

$$\#\{i | a_i = 0\} \geq p\ ,$$

then we are done. Thus without loss of generality, we may assume that there are at least three non-zero elements in X.

Case 1 (*There are more than three non-zero elements*). Without loss of generality, we assume that $a_i \neq 0$ for $i = 1, 2, 3, 4$.

Since $|A_i| = (p - 1)/2$, for $i = 1, \ldots, 4$, by Cauchy–Davenport inequality stated above, we have

$$\begin{aligned} |Aa_1 + Aa_2 + Aa_3 + Aa_4| &\geq \min\{p,\ 2p - 5\} \\ &= p \ \text{(since } p \geq 5). \end{aligned}$$

Thus

$$Aa_1 + Aa_2 + Aa_3 + Aa_4 = \mathbb{Z}/p\mathbb{Z}.$$

So there exists $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 \in A$ such that

$$\epsilon_1 a_1 + \epsilon_2 a_2 + \epsilon_3 a_3 + \epsilon_4 a_4 = -a_5 - a_6 - \cdots - a_p.$$

This implies that

$$\epsilon_1 a_1 + \epsilon_2 a_2 + \epsilon_3 a_3 + \epsilon_4 a_4 + a_5 + a_6 + \cdots + a_p = 0.$$

Case 2 (*There are exactly three non-zero elements*). Without loss of generality, we assume that $a_i \neq 0$ for $i = 1, 2, 3$. We have $a_4 = a_5 = \cdots = a_{p+2} = 0$.

Let $B_1 = Aa_1 \cup \{0\}$, $B_2 = Aa_2 \cup \{0\}$ and $B_3 = Aa_3$. Then $|B_1| = |B_2| = \frac{p-1}{2} + 1$ and $|B_3| = \frac{p-1}{2}$.

Once again by the Cauchy–Davenport inequality, we have

$$\begin{aligned} |B_1 + B_2 + B_3| &\geq \min\left\{p,\ \frac{3(p-1)}{2}\right\} \\ &= p \ \text{(since } p \geq 5). \end{aligned} \tag{4}$$

Then

$$\epsilon_1 a_1' + \epsilon_2 a_2' + \epsilon_3 a_3' = -a_6 - \cdots - a_{p+2},$$

where $a_1' \in \{a_1, a_4 = 0\}$, $a_2' \in \{a_2, a_5 = 0\}$.

Hence in all cases, we have

$$E_A(p) \leq p + 2.$$

On the other hand, by considering the sequence $\{a, -b\}$, where a is a square and b is a non-square, one observes that $D_A(p) \geq 3$ and hence by (3),

$$E_A(p) \;\geq\; D_A(p) + p - 1 \;\geq\; p + 2.$$

From the above two inequalities,

$$p + 2 \;\geq\; E_A(p) \;\geq\; D_A(p) + p - 1 \;\geq\; p + 2.$$

Hence the theorem.

3. Further remarks

Taking A to be the set of units in $\mathbb{Z}/n\mathbb{Z}$, it was conjectured in [4] that $D_A(n) = \Omega(n) + 1$ and $E_A(n) = n + \Omega(n)$, where $\Omega(n)$ is the number of prime divisors of n counted with multiplicity. It was first proved by Luca [10] and later it was also proved by Griffiths [9]. We give here very simple and new proofs of the above results in some particular cases.

When $n = p$, a prime, given any sequence $a_1, a_2, \ldots, a_{p+1}$ of elements of $\mathbb{F}_p$, considering the system of equations

$$\sum_{i=1}^{p+1} a_i x_i = 0,$$
$$\sum_{i=1}^{p+1} x_i^{p-1} = 0,$$

by *Chevalley–Warning theorem* (see [1], [11], for instance), the system has a non-trivial solution, say $\alpha_1, \ldots, \alpha_{p-1}$.

If $I = \{i | \alpha_i \neq 0\}$, then clearly $|I| = p$ and $\sum_{i \in I} a_i \alpha_i = 0$ and we have $E_A(p) \leq p+1$.

Since trivially $D_A(p) \geq 2$, we have $E_A(p) \geq D_A(p) + p - 1 \geq p + 1$ and we are through.

Now consider the case when $n = p^r$ is a prime power, this will give another proof of the case $n = p$.

Here we have $\Omega(n) = r$.

Any sequence of $r + 1$ non-zero elements will have at least two elements a, b in it such that $gcd(a, p^r) = gcd(b, p^r) = p^s$, say, where $s \in \{0, \ldots, r - 1\}$. Let $a = a_1 p^s$ and $b = b_1 p^s$, where a_1 and b_1 are in A. Clearly $b_1 a - a_1 b = 0$ and we have $D_A(n) \leq r + 1$. Since considering the sequence $1, p, \ldots, p^{r-1}$, we have $D_A(n) \geq r+1$ and $D_A(n) = r+1$.

If p is an odd prime, then since $\{1, 2\} \subseteq A$, Theorem A is applicable and we have $E_A(p^r) = D_A(p^r) + p^r - 1 = p^r + r$.

Acknowledgements

This work was done when the first author was visiting the Department of Mathematics and Statistics, Queen's University. He wishes to thank Professor M Ram Murty for the invitation. The authors are also grateful to Professor Murty for his time and encouraging remarks.

References

[1] Adhikari Sukumar Das, Aspects of combinatorics and combinatorial number theory (New Delhi: Narosa Publishing House) (2002)

[2] Adhikari S D, Balasubramanian R and Rath P, Some combinatorial group invariants and their generalizations with weights, Additive combinatorics, 327–335, CRM Proc. Lecture Notes, 43, Amer. Math. Soc. (RI: Providence) (2007)

[3] Adhikari S D and Chen Y G, Davenport constant with weights and some related questions II., *J. Combin. Theory Ser. A* **115(1)** (2008) 178–184

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

[5] Adhikari Sukumar Das and Rath Purusottam, Davenport constant with weights and some related questions, *Integers* **6(A30)** (2006) 6

[6] Alon Noga, Combinatorial Nullstellensatz, Recent trends in combinatorics (Mátraháza, 1995), *Combin. Probab. Comput.* **8(1–2)** (1999) 7–29

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

[8] Gao W D, A combinatorial problem on finite abelian groups, *J. Number Theory* **58(1)** (1996) 100–103

[9] Griffiths Simon, The Erdős-Ginzburg-Ziv theorem with units, *Discrete Math.* **308(23)** (2008) 5473–5484, doi:10.1016/j.disc.2007.09.060

[10] Luca Florian, A generalization of a classical zero-sum problem, *Discrete Math.* **307(13)** (2007) 1672–1678

[11] Nathanson Melvyn B, Additive number theory. Inverse problems and the geometry of sumsets, Graduate Texts in Mathematics, 165 (New York: Springer-Verlag) (1996)