MODIFICATIONS OF SOME METHODS IN THE STUDY OF ZERO-SUM CONSTANTS

Sukumar Das Adhikari
Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad, India
adhikari@hri.res.in

Eshita Mazumdar
Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad, India
eshitam@hri.res.in

Received: 7/9/13, Revised: 1/2/14, Accepted: 4/5/14, Published: 5/30/14

Abstract

For a finite abelian group G with $\exp(G) = n$, the arithmetical invariant $\mathsf{s}_{mn}(G)$ is defined to be the least integer k such that any sequence S with length k of elements in G has a zero-sum subsequence of length mn. When $m = 1$, it is the *Erdős-Ginzburg-Ziv constant* and is denoted by $\mathsf{s}(G)$. There are weighted versions of these constants. Here, to obtain bounds on some particular constants of these types corresponding to the cyclic group $\mathbb{Z}_n$, we shall modify a polynomial method used by Rónyai for making some progress towards the Kemnitz conjecture, and also a method of Griffiths which had been used to attack a problem for some weighted version of the constant.

1. Introduction

Consider a finite abelian group G (written additively). By a sequence over G we mean a finite sequence of terms from G which is unordered and repetition of terms is allowed. We view sequences over G as elements of the free abelian monoid $\mathcal{F}(G)$ and use multiplicative notation (so our notation is consistent with [[13], [15], [17]]).

A sequence $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$ is called a *zero-sum sequence* if $g_1 + \cdots + g_l = 0$, where 0 is the identity element of the group.

If G is a finite abelian group with $\exp(G) = n$, then *the Erdős-Ginzburg-Ziv constant* $\mathsf{s}(G)$ is defined to be the least integer k such that any sequence S with length k of elements in G has a *zero-sum subsequence* of length $\exp(G) = n$; to know some known facts about this constant, one may look into the expository article of Gao and Geroldinger [13] and Section 4.2 in the survey of Geroldinger [14].

For integers $m < n$, we shall use the notation $[m, n]$ to denote the set $\{m, m+1, \ldots, n\}$. For a finite set A, we denote its size by $|A|$, which is the number of elements of A.

If G is a finite abelian group with $\exp(G) = n$, then for a non-empty subset A of $[1, n-1]$, one defines $\mathsf{s}_A(G)$ to be the least integer k such that any sequence S with length k of elements in G has an A-*weighted zero-sum subsequence* of length $\exp(G) = n$, that is, for any sequence $x_1 \cdot \ldots \cdot x_k$ with $x_i \in G$, there exists a subset $I \subset [1, k]$ with $|I| = n$ and, for each $i \in I$, some element $a_i \in A$ such that

$$\sum_{i \in I} a_i x_i = 0.$$

Taking $A = \{1\}$, one recovers the classical Erdős-Ginzburg-Ziv constant $\mathsf{s}(G)$. The above weighted version and some other invariants with weights were initiated by Adhikari, Chen, Friedlander, Konyagin and Pappalardi [4], Adhikari and Chen [3] and Adhikari, Balasubramanian, Pappalardi and Rath [2]. For developments regarding bounds on the constant $\mathsf{s}_A(G)$ in the case of abelian groups G with higher rank and related references, we refer to the recent paper of Adhikari, Grynkiewicz and Sun [6].

When $A = \mathbb{Z}_n^* = \{a \in [1, n-1] | (a, n) = 1\}$, the set of units of $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, Luca [21] and Griffiths [16] proved independently the following result which had been conjectured in [4]:

$$\mathsf{s}_A(\mathbb{Z}_n) \leq n + \Omega(n), \tag{1}$$

where $\Omega(n)$ denotes the number of prime factors of n, counted with multiplicity.

An example in [4] had already established the inequality in the other direction:

$$\mathsf{s}_A(\mathbb{Z}_n) \geq n + \Omega(n).$$

Now we state the following result of Griffiths [16] which generalizes the result (1) for an odd integer n:

Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be an odd integer and let $a = \sum_s a_s$. For each s, let $A_s \subset \mathbb{Z}_{p_s^{a_s}}$ be a subset with its size $|A_s| > p_s^{a_s}/2$, and let $A = A_1 \times \cdots \times A_k$. Then for $m > a$, every sequence $x_1 \cdot \ldots \cdot x_{m+a}$ over $\mathbb{Z}_n$ has 0 as an A-weighted m-sum.

Griffiths [16] also had a similar result when n is even; we only need to mention the case when n is odd.

With suitable modifications of the method of Griffiths [16], we establish the following result:

Theorem 1. *Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be an odd integer and let $a = \sum_s a_s$. For each s, let $A_s \subset \mathbb{Z}_{p_s^{a_s}}$ be a subset with $|A_s| > (4/9)p_s^{a_s}$, and let $A = A_1 \times \cdots \times A_k$. Then for $m > 2a$, every sequence $x_1 \cdot \ldots \cdot x_{m+2a}$ over $\mathbb{Z}_n$ has 0 as an A-weighted m-sum.*

Since $n \geq 3^a > 2a$, from Theorem 1 it follows that any sequence of length $n+2a$ of elements of $\mathbb{Z}_n$ has 0 as an A-weighted n-sum. In other words, if A is as in the statement of Theorem 1, $\mathsf{s}_A(\mathbb{Z}_n) \leq n + 2\Omega(n)$.

Clearly, Theorem 1 covers many subsets $A = A_1 \times \cdots \times A_k$ with $A_s \subset \mathbb{Z}_{p_s^{a_s}}$, which are not covered by the result of Griffiths. We proceed to give one such example where it determines the exact value of $\mathsf{s}_A(\mathbb{Z}_n)$.

When $n = p$, a prime, and A is the set of quadratic residues $\pmod p$, Adhikari and Rath [7] proved that

$$\mathsf{s}_A(\mathbb{Z}_p) = p + 2. \tag{2}$$

For general n, considering the set A of squares in the group of units in the cyclic group $\mathbb{Z}_n$, it was proved by Adhikari, Chantal David and Urroz [5] that if n is a square-free integer, coprime to 6, then

$$\mathsf{s}_A(\mathbb{Z}_n) = n + 2\Omega(n). \tag{3}$$

Later, removing the requirement that n is a square-free, Chintamani and Moriya [8] showed that if n is a power of 3 or n is coprime to $30 = 2 \times 3 \times 5$, then the result (3) holds, where A is again the set of squares in the group of units in $\mathbb{Z}_n$. However, Chintamani and Moriya [8] had only to prove that $\mathsf{s}_A(\mathbb{Z}_n) \leq n + 2\Omega(n)$, the corresponding inequality in the other direction for odd n (and so for n coprime to 30) had already been established by Adhikari, Chantal David and Urroz [5]. We mention that a lower bound for $\mathsf{s}_A(\mathbb{Z}_n)$ when n is even has been given by Grundman and Owens [18].

Considering an odd integer $n = p_1^{a_1} \cdots p_k^{a_k}$, the set A of squares in the group of units in $\mathbb{Z}_n$ is $A = A_1 \times \cdots \times A_k$, where A_s is the set of squares in the group of units in $\mathbb{Z}_{p_s^{a_s}}$ and it satisfies $|A_s| = \frac{p_s^{a_s}}{2}\left(1 - \frac{1}{p_s}\right)$. Observing that $\frac{1}{2}\left(1 - \frac{1}{p_s}\right) > (4/9)$, if $p_s \geq 11$, Theorem 1 gives the required upper bound in the above mentioned result of Chintamani and Moriya [8] when n is coprime to $2 \times 3 \times 5 \times 7$.

In the next section we shall give a proof of our Theorem 1.

To describe the result in Section 3, we need the following definition. For a finite abelian group G with $\exp(G) = n$, $\mathsf{s}_{mn}(G)$ is defined (see [13], for instance) to be the least integer k such that any sequence S with length k of elements in G has a zero-sum subsequence of length mn. Putting $m = 1$, one observes that the constant $\mathsf{s}(G)$ is the same as $\mathsf{s}_n(G)$.

As before, for a non-empty subset A of $[1, n-1]$, one defines $\mathsf{s}_{mn,A}(G)$ to be the least integer k such that any sequence S with length k of elements in G has an A-weighted zero-sum subsequence of length mn.

In Section 3, we obtain an upper bound for $\mathsf{s}_{3p,A}(\mathbb{Z}_p^3)$, where p is an odd prime and $A = \{\pm 1\}$.

We state some known results for the case $A = \{\pm 1\}$.

When $A = \{\pm 1\}$, for any positive integer n it was proved by Adhikari, Chen, Friedlander, Konyagin and Pappalardi [4] that

$$\mathsf{s}_{\{\pm 1\}}(\mathbb{Z}_n) = n + \lfloor \log_2 n \rfloor.$$

When n is odd, and $A = \{\pm 1\}$, it was observed by Adhikari, Balasubramanian, Pappalardi and Rath [2] that

$$\mathsf{s}_{\{\pm 1\}}(\mathbb{Z}_n^2) = 2n - 1.$$

Later, for any finite abelian group G of rank r and even exponent it was proved by Adhikari, Grynkiewicz and Zhi-Wei Sun [6], that there exists a constant k_r, dependent only on r, such that

$$\mathsf{s}_{\{\pm 1\}}(G) \leq \exp(G) + \log_2 |G| + k_r \log_2 \log_2 |G|.$$

In Section 3, we shall take up the problem for the rank 3 case and after some preliminary remarks, we shall observe that a suitable modification of a polynomial method used by Rónyai [24] yields the following.

Theorem 2. *For $A = \{\pm 1\}$, and an odd prime p, we have*

$$\mathsf{s}_{3p,A}(\mathbb{Z}_p^3) \leq \frac{(9p-3)}{2}.$$

We remark that a polynomial method has been successfully employed to tackle questions in additive number theory and, in particular, to zero-sum problems; we refer to the monographs [15, Chapter 5.5] and [17, Chapters 17 and 22].

There is much recent work on $\mathsf{s}(G)$ (e.g., [10], [26], [12], [9], [11]). The plus-minus weighted analogue of a different constant has been taken up in the recent paper [22]. While many of the ideas in the above papers do not work in our situation, we feel that it will be worth investigating the method in [26]; more precisely one may look into plugging in some ideas from the paper [25], which would involve some structural insight into weighted zero-sum subsequences. However, adapting some of these ideas in the weighted case will not be straightforward as one will run into obvious difficulties; for instance while in the classical case, existence of a zero sum subsequence of length $2p$ of a sequence of length $3p$ implies the existence a zero sum subsequence of length p, that will no longer be valid in the weighted case. It will be worthwhile to explore the possibility of suitable modifications of some ideas in some of the above papers in the weighted situation.

2. Proof of Theorem 1

For our proof of Theorem 1, we shall closely follow the method of Griffiths [16]. Though we shall be able to use many of the ideas in [16] with straight forward modifications, some modifications need some work and some new observations have to be made to make things work.

We start this section with a couple of basic lemmas.

Lemma 1. *Let p^a be an odd prime power and $A \subset \mathbb{Z}_{p^a}$ be a subset such that $|A| > \frac{4}{9}p^a$. If $x, y, z \in \mathbb{Z}_{p^a}^*$, the group of units in $\mathbb{Z}_{p^a}$, then given any $t \in \mathbb{Z}_{p^a}$, there exist $\alpha, \beta, \gamma \in A$ such that*

$$\alpha x + \beta y + \gamma z = t.$$

Proof. Considering the sets

$$A_1 = \{\alpha x : \alpha \in A\},\ B_1 = \{\beta y : \beta \in A\},\ C_1 = \{\gamma z : \gamma \in A\},$$

and observing that $|A_1| = |B_1| = |C_1| = |A|$, by Kneser's theorem ([20], may also see Chapter 4 of [23]) we have

$$|A_1 + B_1| \geq |A_1| + |B_1| - |H| > \frac{8p^a}{9} - |H|, \tag{4}$$

where $H = H(A_1 + B_1)$ is the stabilizer of $A_1 + B_1$.

Now, $H = \mathbb{Z}_{p^a}$ would imply $A_1 + B_1 = \mathbb{Z}_{p^a}$, which in turn would imply that $A_1 + B_1 + C_1 = \mathbb{Z}_{p^a}$ and we are through.

Otherwise, $|H|$ being a power of an odd prime $p \geq 3$, we have

$$|H| \leq p^{a-1} = \frac{p^a}{p} \leq \frac{p^a}{3}$$

and hence from (4),

$$|A_1 + B_1| > \frac{8p^a}{9} - \frac{p^a}{3} = \frac{5p^a}{9}.$$

Therefore, we have

$$|A_1 + B_1| + |t - C_1| > \frac{5p^a}{9} + \frac{4p^a}{9} = p^a,$$

which implies that the sets $A_1 + B_1$ and $t - C_1$ intersect and we are through. $\square$

Lemma 2. *Let p^a be an odd prime power and let $A \subset \mathbb{Z}_{p^a}$ be such that $|A| > (4/9)p^a$. Let $x_1 \cdot \ldots \cdot x_m$ be a sequence over $\mathbb{Z}_{p^a}$ such that for each $b \in [1, a]$, writing $T_b = \{i | x_i \not\equiv 0 \pmod{p^b}\}$, its cardinality $|T_b| \notin \{1, 2\}$. Then $x_1 \cdot \ldots \cdot x_m$ is an A-weighted zero-sum sequence.*

Proof. Let c be minimal such that $\{i|x_i \not\equiv 0 \pmod{p^c}\}$ is non-empty. If no such c exists then $T_b = \emptyset$ for all b and we are done.

Therefore, $\{i|x_i \not\equiv 0 \pmod{p^c}\}$ has at least three elements; without loss of generality let $x_1, x_2, x_3 \not\equiv 0 \pmod{p^c}$.

Set

$$x'_i = x_i/p^{c-1} \in \mathbb{Z}_{p^{a-(c-1)}},$$

for $i \in [1, m]$.

If elements of A meets less than $(4/9)p^{a-(c-1)}$ congruence classes modulo $p^{a-(c-1)}$, then $|A| < (4/9)p^{a-(c-1)} \times p^{(c-1)} = (4/9)p^a$, which is a contradiction to our assumption.

Therefore, the elements of A must meet more than $(4/9)p^{a-(c-1)}$ congruence classes modulo $p^{a-(c-1)}$.

Picking up arbitrarily $\alpha_4, \alpha_5, \cdots, \alpha_m \in A$, by Lemma 1, there exist $\alpha_1, \alpha_2, \alpha_3 \in A$ satisfying

$$\alpha_1 x'_1 + \alpha_2 x'_2 + \alpha_3 x'_3 = -\alpha_4 x'_4 - \cdots - \alpha_m x'_m$$

in $\mathbb{Z}_{p^{a-(c-1)}}$, and hence

$$\alpha_1 x_1 + \cdots + \alpha_m x_m = 0$$

in $\mathbb{Z}_{p^a}$. $\square$

Let $n = p_1^{a_1} \cdots p_k^{a_k}$. Then, $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$ and an element $x \in \mathbb{Z}_n$ can be written as $x = (x^{(1)}, \ldots, x^{(k)})$, where $x^{(s)} \equiv x \pmod{p_s^{a_s}}$ for each s. As has been observed in [16], it is not difficult to see that if $A = A_1 \times A_2 \times \cdots \times A_k$ is a subset of $\mathbb{Z}_n$, where $A_s \subset \mathbb{Z}_{p_s^{a_s}}$ for each $s \in [1, k]$, then a sequence of $x_1 \cdot \ldots \cdot x_m$ over $\mathbb{Z}_n$ is an A-weighted zero-sum sequence in $\mathbb{Z}_n$ if and only if for each $s \in [1, k]$, the sequence $x_1^{(s)} \cdot \ldots \cdot x_m^{(s)}$ is an A_s-weighted zero-sum sequence in $\mathbb{Z}_{p_s^{a_s}}$.

We shall need the following definitions.

Given subsets $X_1, \cdots, X_a$ of the set $V = [1, m + 2a]$, a *path* is a sequence of distinct vertices $v_1, \cdots, v_l$ and distinct sets $X_{i_1}, \cdots, X_{i_{l+1}}$ such that $v_1 \in X_{i_1} \cap X_{i_2}, \cdots, v_l \in X_{i_l} \cap X_{i_{l+1}}$. A *cycle* is a sequence of distinct vertices $v_1, \cdots, v_l$ and distinct sets $X_{i_1}, \cdots, X_{i_l}$ such that $v_1 \in X_{i_1} \cap X_{i_2}, \cdots, v_l \in X_{i_l} \cap X_{i_1}$.

Lemma 3. *Given subsets $X_1, \cdots, X_a$ of the set $V = [1, m + 2a]$, where $m > 2a$, there exists a set $I \subset [1, m + 2a]$ with $|I| = m$ and $|I \cap X_s| \notin \{1, 2\}$, for all $s = 1, \cdots, a$.*

Proof. Given a ground set $V = [1, m+2a]$ and subsets $X_1, \cdots, X_a$ of V, for $I \subset V$, we define $S(I)$ to be the set $\{s : |I \cap X_s| \geq 3\}$ and I will be called *valid* if $|I \cap X_s| \notin \{1, 2\}$, for all $s \in [1, a]$.

We proceed by induction on a.

In the case $a = 1$, we have $V = [1, m + 2]$ where $m > 2$.

If $0 \leq |X_1| \leq 2$, then we can take $I \subset V \setminus X_1$, such that $|I| = m$ and we have $|I \cap X_1| = 0 \notin \{1, 2\}$.

Now, let $|X_1| > 2$. If $|X_1| \geq m$, we take $I \subset X_1$ such that $|I| = m$, so that $|I \cap X_1| = m > 2$. If $|X_1| < m$, we choose I with $|I| = m$ and $X_1 \subset I \subset V$ so that $|I \cap X_1| = |X_1| > 2$.

Now, assume that $a > 1$ and the statement is true when the number of subsets is not more than $a - 1$.

If one of the sets, say X_a, has no more than two elements, then without loss of generality, let $X_a \subset \{m + 2a, m + 2a - 1\}$ and consider the sets $X'_i = X_i \cap [1, m + 2(a - 1)]$, for $i \in [1, a - 1]$. Since $m > 2a > 2(a - 1)$, by the induction hypothesis there exists $I \subset [1, m+2(a-1)]$ with $|I| = m$ and $|I \cap X'_i| \notin \{1, 2\}$, for $i \in [1, a-1]$. Clearly, $|I \cap X_i| \notin \{1, 2\}$, for $i \in [1, a - 1]$ and $|I \cap X_a| = 0$. So, we are through.

Hence we assume that

$$|X_s| \geq 3, \quad \text{for all } s.$$

If there exists a non-empty valid set $J \subset V = [1, m+2a]$ such that $2|S(J)| \geq |J|$, then considering the ground set $V \setminus J$ and the subsets $\{X_s : s \notin S(J)\}$, observing that $|V \setminus J| = m + 2a - |J| \geq m + 2(a - |S(J)|)$, by the induction hypothesis there is a set $J' \subset V \setminus J$ with $|J'| = m - |J|$ such that $|J' \cap X_s| \notin \{1, 2\}$, for all $s \notin S(J)$.

Since $J \subset V$ is valid, $J \cap X_s$ is empty for any X_s with $s \notin S(J)$. Therefore, it is clear that $I = J \cup J'$ is valid for the ground set $V = [1, m + 2a]$ and subsets $X_1, \cdots, X_a$. Since $|I| = m$, we are through.

Now, let $J (\neq \emptyset)$ be a subset of V such that $2|S(J)| \geq |J|$. If J is not valid, then there exists X_s such that $|J \cap X_s| \in \{1, 2\}$.

If $|J \cap X_s| = 1$, then since $|X_s| \geq 3$, we can choose $i, j \in X_s \setminus J$ and consider the set $K = J \cup \{i, j\}$. Then, $|K| = |J| + 2$ and $|S(K)| \geq |S(J)| + 1$ so that $2|S(K)| \geq 2|S(J)| + 2 \geq |J| + 2 = |K|$.

Similarly, if $|J \cap X_s| = 2$, we can choose $i \in X_s \setminus J$ and consider the set $K = J \cup \{i\}$. We have $|K| = |J| + 1$ and $|S(K)| \geq |S(J)| + 1$ so that $2|S(K)| \geq 2|S(J)| + 2 \geq |J| + 2 > |K|$.

Therefore, iterating this process we arrive at a valid set L with $2|S(L)| \geq |L|$ and by our previous argument L can be extended to a valid set I with $|I| = m$.

So, we assume that for all non-empty $J \subset [1, m + 2a]$ we have

$$2|S(J)| < |J|.$$

If there are X_u, X_v, $u \neq v$, such that $i, j \in X_u \cap X_v$, then taking $k \in X_u \setminus \{i, j\}$ and $l \in X_v \setminus \{i, j\}$ and considering $I = \{i, j, k, l\}$, we have $2|S(I)| \geq 4 \geq |I|$, contradicting the above assumption. So, we assume that for every pair X_u, X_v for $u \neq v$, we have

$$|X_u \cap X_v| \leq 1.$$

If there is a cycle, consisting of distinct vertices $v_1, \cdots, v_l$ and distinct sets $X_{i_1}, \cdots, X_{i_l}$ such that $v_1 \in X_{i_1} \cap X_{i_2}, \cdots, v_l \in X_{i_l} \cap X_{i_1}$, then considering the set $K = \{v_1, \cdots, v_l\}$ and observing that $|X_s| \geq 3$ for all s, we can choose $t_j \in X_{i_j}$ for $j \in [1, l]$ so that taking $J = K \cup \{t_1, \cdots, t_l\}$, $|X_{i_j} \cap J| \geq 3$ for all $j \in [1, l]$. Then $2|S(J)| \geq 2l \geq |J|$, which is a contradiction to our assumption.

Therefore, it is assumed that there is no cycle.

Define a *leaf* to be a set X_s such that $|X_s \cap (\cup_{t \neq s} X_t)| \leq 1$.

We claim that there must be at least two leaves.

If the sets X_s are pairwise disjoint, then for any s, $|X_s \cap (\cup_{t \neq s} X_t)| = 0$; since $a > 1$, we have two leaves. So we assume that there are two sets which meet. Without loss of generality, let $X_1 \cap X_2 \neq \emptyset$.

Now we consider a path of maximum length involving X_1; by the assumption above, its length is at least 2. Let $X_{i_1}, \cdots, X_{i_l}$ be the distinct sets corresponding to this path, where X_{i_1}, X_{i_l} are end sets and $v_1 \in X_{i_1} \cap X_{i_2}, \cdots, v_{i_{l-1}} \in X_{i_{l-1}} \cap X_{i_l}$. By the maximality condition, $X_{i_1} \setminus \{v_1\}$ and $X_{i_l} \setminus \{v_{l-1}\}$ cannot intersect with the sets not on the path and since there are no cycles, they cannot intersect with the sets on the path as well. Therefore, $|X_{i_1} \cap (\cup_{t \neq i_1} X_t)| = 1$ and similarly, $|X_{i_l} \cap (\cup_{t \neq i_l} X_t)| = 1$. This establishes the claim that there are at least two leaves.

Consider the case $a = 2$ so that $m \geq 2a + 1 = 5$. If either $X_{a-1} \cap X_a \neq \emptyset$, or $X_{a-1} \cap X_a = \emptyset$ and $m \geq 6$, in both these cases, one can easily find $I \subset V$, such that $|I| = m \geq 5$ and $|I \cap X_i| \geq 3$ for $i = 1, 2$. If $X_{a-1} \cap X_a = \emptyset$ and $m = 5$, then $m + 2a = 9$ and at least one of the sets X_{a-1}, X_a, say X_a, has no more than 4 elements. Therefore there is $I \subset V \setminus X_a$ with $|I| = 5 = m$ such that $|I \cap X_{a-1}| \geq 3$, $|I \cap X_a| = 0$ and we are through. So, henceforth we assume that $a > 2$.

We call a point $t \in X_i$ a *free vertex* if $t \notin \cup_{j \neq i} X_j$.

First we consider the case where there are two sets, say X_{a-1}, X_a, each having at least four free vertices. Let $m+2a, m+2a-1, m+2a-2, m+2a-3$ be free vertices in X_a and $m+2a-4, m+2a-5, m+2a-6, m+2a-7$ be free vertices in X_{a-1}. Considering the set $W = [1, m+2a-8]$, by the induction hypothesis there is a set $J \subset W$ such that $|J| = m-4$ and $|J \cap X_i| \notin \{1, 2\}$, for $i \in [1, a-2]$. If J intersects both X_{a-1} and X_a, we take $I = J \cup \{m+2a, m+2a-1, m+2a-4, m+2a-5\}$. If J does not intersect at least one of them, say X_a, we take $I = J \cup \{m+2a-4, m+2a-5, m+2a-6, m+2a-7\}$. Clearly, I is a valid set with $|I| = m$.

Next, suppose there is exactly one set, say X_a, which has more than three free vertices. Let $m+2a, m+2a-1, m+2a-2, m+2a-3$ be free vertices in X_a. As there are two leaves, there must be one leaf among the other sets; let X_{a-1} be a leaf, without loss of generality. Now, $|X_{a-1}| \geq 3$ and $|X_{a-1} \cap (\cup_{t \neq a-1} X_t)| \leq 1$. Since by our assumption X_{a-1} does not have more than three free vertices, $|X_{a-1}| \in \{3, 4\}$.

If X_{a-1} has three elements, say $m + 2a - 4, m + 2a - 5, m + 2a - 6$, by the induction hypothesis there exists $J \subset [1, m+2a-7]$ such that $|J| = m-3 > 2(a-2)$ and $|J \cap X_i| \notin \{1, 2\}$ for $i \in [1, a-2]$. Since J does not intersect X_{a-1}, taking $I = J \cup \{m + 2a, m + 2a - 1, m + 2a - 2\}$, I is a valid set with $|I| = m$.

If X_{a-1} has four elements, say $m+2a-4, m+2a-5, m+2a-6, m+2a-7$, by the induction hypothesis there exists $J \subset [1, m+2a-8]$ such that $|J| = m-4 > 2(a-2)$ and $|J \cap X_i| \notin \{1, 2\}$ for $i \in [1, a-2]$. Since J does not intersect X_{a-1}, taking $I = J \cup \{m + 2a, m + 2a - 1, m + 2a - 2, m + 2a - 3\}$, I is a valid set with $|I| = m$.

Now we assume that no set X_s has more than three free vertices.

We claim that for $a > 1$,

$$| \cup_s X_s| \leq 4a - 1.$$

We proceed by induction. For $a = 2$, since no set has more than three free vertices and $|X_1 \cap X_2| \leq 1$, $|X_1 \cup X_2| \leq 7 = 4a - 1$.

Now, assume $a > 2$. By the induction hypothesis, $|X_1 \cup \cdots \cup X_{a-1}| \leq 4(a-1)-1 = 4a-5$. Since no set has more than three free vertices, $|\cup_s X_s| \leq 4a-5+3 = 4a-2 \leq 4a - 1$. Hence the claim is established.

Since, $m > 2a$, for $a > 1$, we have $4a - 1 < 4a < m + 2a$ and hence there are two vertices, say $m + 2a, m + 2a - 1$, which are not in any of the sets $X_1, \cdots, X_a$.

Let X_a be one of the leaves. As had been observed earlier, by our assumptions, $|X_a| \in \{3, 4\}$.

If $|X_a| = 3$, then X_a has two free vertices, say $m + 2a - 2, m + 2a - 3$. By the induction hypothesis there exists $J \subset [1, m+2a-4]$ such that $|J| = m-2 > 2(a-1)$ and $|J \cap X_i| \notin \{1, 2\}$ for $i \in [1, a-1]$. If J meets X_a, we take $I = J \cup \{m + 2a - 2, m + 2a - 3\}$ and if J does not meet X_a, we take $I = J \cup \{m + 2a, m + 2a - 1\}$ and in either case we obtain a valid set I with $|I| = m$.

Now, let $|X_a| = 4$ so that X_a has three free vertices; let $m + 2a - 2, m + 2a - 3, m+2a-4$ be free vertices in X_a. As we have at least two leaves, let the other leaf be X_{a-1}. By the above argument we are done except when $|X_{a-1}| = 4$ in which case X_{a-1} has three free vertices; and let $m + 2a - 5, m + 2a - 6, m + 2a - 7$ be free vertices in X_{a-1}.

By the induction hypothesis there exists $J \subset [1, m + 2a - 8]$ such that $|J| = m - 4 > 2(a - 2)$ and $|J \cap X_i| \notin \{1, 2\}$ for $i \in [1, a - 2]$. If J meets both X_a, X_{a-1}, we take $I = J \cup \{m+2a-2, m+2a-3, m+2a-5, m+2a-6\}$. If J does not meet one of these two sets, say X_{a-1}, we take $I = J \cup \{m+2a-2, m+2a-3, m+2a-4, m+2a\}$. In either case we obtain a valid set I with $|I| = m$. $\square$

Proof of Theorem 1. Given a sequence $x_1 \cdot \ldots \cdot x_{m+2a}$ over $\mathbb{Z}_n$, we define $X_b^{(s)} \subset [1, m+2a]$ for $s \in [1,k]$ and $b \in [1, a_s]$ by

$$X_b^{(s)} = \{i : x_i \not\equiv 0 \pmod{p_s^b}\}.$$

By Lemma 3, there exists $I \subset [1, m+2a]$ with $|I| = m$ and $|I \cap X_b^{(s)}| \notin \{1, 2\}$ for all s,b. Let $I = \{i_1, \cdots, i_m\}$. Then by Lemma 2 and the observation made after the proof of Lemma 2, it follows that $x_{i_1}, \cdots, x_{i_m}$ is an A-weighted zero-sum sequence. □

3. Proof of Theorem 2

Throughout this section, p will be an odd prime and we shall have $A = \{\pm 1\}$. Here, an A-weighted zero-sum sequence will be called a plus-minus zero-sum sequence.

Before we proceed to prove Theorem 2, we make some observations regarding $\mathsf{s}_{rp,A}(\mathbb{Z}_p^3)$ for $r = 1, 2, 3$.

Let (e_1, e_2, e_3) be a basis of $\mathbb{Z}_p^3$ and let $e_0 = e_1 + e_2 + e_3$.

Observation 1. The sequence

$$S = \prod_{\nu=0}^{3} e_\nu^{p-1}$$

has no plus-minus zero-sum subsequence of length p since obtaining $(0, 0, 0)$ happens either by adding an element with its additive inverse (if the inverse is not in the sequence, but the element repeats, it can be obtained by multiplying with (-1)) or by adding the sum of the elements e_1, e_2, e_3 with the additive inverse of e_0. Each involves an even number of elements in the sequence and p is an odd prime.

Thus,

$$\mathsf{s}_{p,A}(\mathbb{Z}_p^3) \geq 4p - 3. \tag{5}$$

Observation 2. We consider the sequence

$$T = e_0^3 \prod_{\nu=1}^{3} e_\nu^{p-1}.$$

Since T is a subsequence of S, it does not have a plus-minus zero-sum subsequence of length p. However, multiplying one of the e_0's by (-1) and then adding with the remaining elements, it follows that the sequence is a plus-minus zero-sum sequence of length $3p$.

However, observing that the sequence

$$S = \mathbf{0}^{3p-1} \prod_{\nu=0}^{r} (2^\nu e_1) \prod_{\nu=0}^{r} (2^\nu e_2) \prod_{\nu=0}^{r} (2^\nu e_3)$$

where r is defined by $2^{r+1} \leq p < 2^{r+2}$, does not have any plus-minus zero-sum subsequence of length $3p$, we obtain:

$$\mathsf{s}_{3p,A}(\mathbb{Z}_p^3) \geq 3p + 3\lfloor \log_2 p \rfloor. \tag{6}$$

Similarly, one can observe that

$$\mathsf{s}_{2p,A}(\mathbb{Z}_p^3) \geq 2p + 3\lfloor \log_2 p \rfloor. \tag{7}$$

Observation 3. Given a sequence $\prod_{i=1}^{t} w_i$ over $\mathbb{Z}_p^3$, where $t = \frac{(5p-3)}{2}$ and $w_i = (a_i, b_i, c_i)$ with a_i, b_i, c_i in $\mathbb{Z}_p$, consider the following system of equations over $\mathbb{F}_p$, where $\mathbb{F}_p$ is the finite field with p elements.

$$\sum_{i=1}^{t} a_i x_i^{\frac{p-1}{2}} = 0, \ \sum_{i=1}^{t} b_i x_i^{\frac{p-1}{2}} = 0, \ \sum_{i=1}^{t} c_i x_i^{\frac{p-1}{2}} = 0, \ \sum_{i=1}^{t} x_i^{p-1} = 0.$$

Since sum of the degrees of the polynomials on the left hand side is $\frac{(5p-5)}{2} < t$ and $x_1 = x_2 = \cdots = x_t = 0$ is a solution, by Chevalley-Warning theorem (see [1], [19] or [23], for instance) there is a nontrivial solution $(y_1, \cdots, y_t)$ of the above system. By Fermat's little theorem, writing $I = \{i : y_i \neq 0\}$, from the first three equations it follows that $\sum_{i \in I} \epsilon_i (a_i, b_i, c_i) = (0, 0, 0)$, where $\epsilon_i \in \{1, -1\}$ and from the second equation we have $|I| = p$ or $|I| = 2p$.

Thus, *a sequence of $\frac{(5p-3)}{2}$ elements of $\mathbb{Z}_p^3$ must have a plus-minus zero-sum subsequence of length p or $2p$.*

Observation 4. Suppose we are given a sequence $\prod_{i=1}^{t} w_i$ over $\mathbb{Z}_p^3$, where $t = \frac{(7p-3)}{2}$ and $w_i = (a_i, b_i, c_i)$, with a_i, b_i, c_i in $\mathbb{Z}_p$.

By Observation 3, the subsequence $\prod_{i=1}^{k} w_i$, where $k = \frac{(5p-3)}{2}$, must have a plus-minus zero-sum subsequence of length p or $2p$. If it does not have a plus-minus zero-sum subsequence of length $2p$, after removing a plus-minus zero-sum subsequence of length p from the original sequence, the length of the remaining subsequence is $\frac{(5p-3)}{2}$, and by Observation 3, it must have a plus-minus zero-sum subsequence of length p or $2p$ and in either case, the original sequence has a plus-minus zero-sum subsequence of length $2p$.

Therefore, we have

$$\mathsf{s}_{2p,A}(\mathbb{Z}_p^3) \leq \frac{(7p-3)}{2}. \tag{8}$$

Remarks. One can observe that there is a big gap between the lower bound $3p+3\lfloor\log_2 p\rfloor$ of $\mathsf{s}_{3p,A}(\mathbb{Z}_p^3)$ given in (6) and the corresponding upper bound $\frac{(9p-3)}{2}$ in the statement of Theorem 2.

Similarly, there is a gap between the upper and lower bounds of $\mathsf{s}_{2p,A}(\mathbb{Z}_p^3)$ given respectively in (8) and (7).

For the constant $\mathsf{s}_{p,A}(\mathbb{Z}_p^3)$, obtaining any reasonable upper bound would be rather difficult.

For the proof of Theorem 2, we shall modify the proof of a result of Rónyai [24]. More precisely, we shall work with monomials of the form $\prod_{i\in I} x_i^{r_i}, r_i \in \{0,1,2\}$, where I is a finite set, in place of monomials of the form $\prod_{i\in I} x_i^{r_i}, r_i \in \{0,1\}$ as had been employed in [24].

Lemma 4. *Given a sequence $(a_1,b_1,c_1)\cdot\ldots\cdot(a_t,b_t,c_t)$ over $\mathbb{Z}_p^3$, where $t=\frac{(9p-3)}{2}$, if it has a plus-minus zero-sum subsequence of length p then it must have a plus-minus zero-sum subsequence of length $3p$.*

Proof. Since after removing a plus-minus zero-sum subsequence of length p, the length of the remaining subsequence is $\frac{(7p-3)}{2}$, the result follows from (8). □

Lemma 5. *Let F be a field which is not of characteristic 2 and m a positive integer. Then the monomials $\prod_{1\le i\le m} x_i^{r_i}, r_i \in \{0,1,2\}$ constitute a basis of the F-linear space of all functions from $D=\{0,1,-1\}^m$ to F.*

Proof. It is easy to observe that the dimension of the space spanned by the monomials $\prod_{1\le i\le m} x_i^{r_i}, r_i \in \{0,1,2\}$ over F is 3^m which is the same as that of the F-linear space of all functions from $D=\{0,1-1\}^m$ to F.

If U,V,W are disjoint subsets of $[1,m]$, such that their union is $[1,m]$, then the function

$$f_{U,V,W}(x_1,x_2,\cdots,x_m)=\prod_{j\in U} x_j(1+x_j)/2\prod_{j\in V} x_j(x_j-1)/2\prod_{j\in W}(1-x_j^2)$$

takes the value 1 precisely at the point $(x_1,x_2,\cdots,x_m)$ of D where $x_j=0$ for $j\in W$, $x_j=1$ for $j\in U$ and $x_j=-1$ for $j\in V$.

Since the functions $f_{U,V,W}$ clearly span the linear space of functions from D to F, we are through. □

Proof of Theorem 2. Let $S=(a_1,b_1,c_1)\cdot\ldots\cdot(a_m,b_m,c_m)$ be a sequence over $\mathbb{Z}_p^3$ where $m=\frac{(9p-3)}{2}$. We proceed to show that it must have a plus-minus zero-sum subsequence of length $3p$.

If possible, let there be no such subsequence. By Lemma 4, there is no plus-minus zero-sum subsequence of length p.

Let

$$\sigma(x_1, x_2, \cdots, x_m) := \sum_{I \subset [1,m], |I| = p} \prod_{i \in I} x_i^2,$$

the p-th elementary symmetric polynomial of the variables x_1^2, x_2^2, $\cdots, x_m^2$.

Next we consider the following polynomial in $\mathbb{F}_p[x_1, x_2, \cdots, x_m]$:

$$\begin{aligned} & P(x_1, x_2, \cdots, x_m) \\ := \; & \left(\left(\sum_{i=1}^m a_i x_i \right)^{p-1} - 1 \right) \left(\left(\sum_{i=1}^m b_i x_i \right)^{p-1} - 1 \right) \left(\left(\sum_{i=1}^m c_i x_i \right)^{p-1} - 1 \right) \\ & \left(\left(\sum_{i=1}^m x_i^2 \right)^{p-1} - 1 \right) (\sigma(x_1, x_2, \cdots, x_m) - 4)(\sigma(x_1, x_2, \cdots, x_m) - 2). \end{aligned}$$

Given $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_m)$ in $\{0, 1, -1\}^m$, if the number of non-zero entries of α is $2p$, then $\sigma(\alpha) = \binom{2p}{p} = 2 \in \mathbb{F}_p$ and therefore the last factor in P vanishes for $(x_1, x_2, \cdots, x_m) = \alpha$. Similarly, if the number of non-zero entries of α is $4p$, then $\sigma(\alpha) = \binom{4p}{p} = 4 \in \mathbb{F}_p$ and therefore the fifth factor in P vanishes for $(x_1, x_2, \cdots, x_m) = \alpha$ in this case.

If the number of non-zero entries of α is p or $3p$, then by our assumption,

$$\left(\left(\sum_{i=1}^m a_i x_i \right)^{p-1} - 1 \right) \left(\left(\sum_{i=1}^m b_i x_i \right)^{p-1} - 1 \right) \left(\left(\sum_{i=1}^m c_i x_i \right)^{p-1} - 1 \right) = 0,$$

for $(x_1, x_2, \cdots, x_m) = \alpha$.

Finally, the fourth factor in P vanishes unless the number of non-zero entries of α is divisible by p.

Therefore, P vanishes on all vectors in $\{0, 1, -1\}^m$ except at $\mathbf{0}$ and $P(\mathbf{0}) = 8$. Thus, with the notations used in the proof of Lemma 5, we have $P = 8 f_{\emptyset, \emptyset, [m]}$ as functions on $\{0, 1, -1\}^m$. We observe that deg $P \leq 3(p-1) + 2(p-1) + 2p + 2p = 9p - 5$.

We now reduce P into a linear combination of monomials of the form $\prod_{1 \leq i \leq m} x_i^{r_i}$, $r_i \in \{0, 1, 2\}$ by replacing each x_i^r, $r \geq 1$ by x_i if r is odd and by x_i^2 if r is even and let Q denote the resulting expression.

We note that as functions on $\{0, 1, -1\}^m$, P and Q are the same. Therefore, as a function on $\{0, 1, -1\}^m$, $Q = 8 f_{\emptyset, \emptyset, [m]}$. Also, since reduction can not increase the degree, we have deg $Q \leq 9p - 5$. But, because of the uniqueness part, Q has to be identical with $8(1-x_1^2)(1-x_2^2)\cdots(1-x_m^2)$. This leads to a contradiction since the later has degree $2m = 9p-3$. $\square$

Acknowledgements. We thank the referee for several suggestions to improve the presentation of the paper and also for informing us about some related references.

References

[1] S. D. Adhikari, *Aspects of Combinatorics and Combinatorial Number Theory*, Narosa, New Delhi, 2002.

[2] S. D. Adhikari, R. Balasubramanian, F. Pappalardi and P. Rath, *Some zero-sum constants with weights*, Proc. Indian Acad. Sci. (Math. Sci.) **118** (2008), 183–188.

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

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

[5] S. D. Adhikari, Chantal David and Jorge Jiménez Urroz, *Generalizations of some zero-sum theorems*, Integers **8** (2008), #A52.

[6] S. D. Adhikari, David J. Grynkiewicz and Zhi-Wei Sun, *On weighted zero-sum sequences*, Advances in Applied Mathematics **48** (2012), 506–527.

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

[8] M. N. Chintamani and Bhavin K. Moriya, *Generalizations of some zero sum theorems*, Proc. Indian Acad. Sci. (Math. Sci.) **122**, No. 1 (2012), 15–21.

[9] M. N. Chintamani, B. K. Moriya, W. D. Gao, P. Paul and R. Thangadurai, *New upper bounds for the Davenport and for the Erdős-Ginzburg-Ziv constants*, Arch. Math. **98** (2012), 133-142.

[10] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham, *Zero-sum problems in finite abelian groups and affine caps*, Quart. J. Math. **58** (2007), 159–186.

[11] Yushuang Fan, W. Gao, Linlin Wang and Qinghai Zhong, *Two zero-sum invariants on finite abelian groups*, Europ. J. Comb. **34** (2013), 1331–1337.

[12] Yushuang Fan, W. Gao and Qinghai Zhong, *On the Erdős-Ginzburg-Ziv constant of finite abelian groups of high rank*, J. Number Theory **131** (2011), 1864–1874.

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

[14] A. Geroldinger, *Additive group theory and non-unique factorizations*, in: A. Geroldinger, I. Ruzsa (Eds.), Combinatorial Number Theory and Additive Group Theory, in: Adv. Courses Math. CRM Barcelona, Birkhäuser Verlag, Basel, 2009.

[15] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics (Boca Raton), 278, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[16] S. Griffiths, *The Erdős-Ginzburg-Ziv theorem with units*, Discrete Math. **308**, No. 23 (2008), 5473–5484.

[17] D. J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics, Springer, 2013.

[18] H. G. Grundman and C. S. Owens, *On bounds for two Davenport-type constants*, Integers **13** (2013), #A7.

[19] Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition, Springer-Verlag, 1990.

[20] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z. **58** (1953), 459–484.

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

[22] L. E. Marchan, O. Ordaz, D. Ramos and W. A. Schmid, *Some exact values of the Harborth constant and its plus-minus weighted analogue*, Arch. Math. **101** (2013), 501–512.

[23] Melvyn B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

[24] L. Rónyai, *On a conjecture of Kemnitz*, Combinatorica **20** (4) (2000), 569–573.

[25] S. Savchev and Fang Chen, *Kemnitz conjecture revisited*, Discrete Math. **297** (2005), 196–201.

[26] W. A. Schmid and Zhuang, *On short zero-sum subsequences over p-groups*, Ars Comb. **95** (2010), 343–352.