The Weighted Davenport constant of a group and a related extremal problem

Niranjan Balachandran
Department of Mathematics
Indian Institute of Technology, Bombay
Mumbai, India
niranj@math.iitb.ac.in

Eshita Mazumdar
Center for Combinatorics
Nankai University
Tianjin, P. R. China
eshitamazumdar@yahoo.com

Submitted: Jul 11, 2018; Accepted: Sept 23, 2019; Published: Dec 20, 2019

Abstract

For a finite abelian group G written additively, and a non-empty subset $A \subset [1, \exp(G) - 1]$ the weighted Davenport Constant of G with respect to the set A, denoted $D_A(G)$, is the least positive integer k for which the following holds: Given an arbitrary sequence $(x_1, \ldots, x_k)$ with $x_i \in G$, there exists a non-empty subsequence $(x_{i_1}, \ldots, x_{i_t})$ along with $a_j \in A$ such that $\sum_{j=1}^{t} a_j x_{i_j} = 0$. In this paper, we pose and study a natural new extremal problem that arises from the study of $D_A(G)$: For an integer $k \geqslant 2$, determine $f_G^{(D)}(k) := \min\{|A| : D_A(G) \leqslant k\}$ (if the problem posed makes sense). It turns out that for k 'not-too-small', this is a well-posed problem and one of the most interesting cases occurs for $G = \mathbb{Z}_p$, the cyclic group of prime order, for which we obtain near optimal bounds for all k (for sufficiently large primes p), and asymptotically tight (up to constants) bounds for $k = 2, 4$.

Mathematics Subject Classifications: 11B50, 11B75, 05D40.

1 Introduction

Suppose $a < b$ are positive integers. By $[a, b]$ we denote the set $\{a, a+1, \ldots, b\} \subset \mathbb{N}$. Throughout this paper, we shall use the Landau asymptotic notation: For functions f, g, we write $f(n) = O(g(n))$ if there exists an absolute constant $C > 0$ and an integer n_0 such that for all $n \geqslant n_0$, $|f(n)| \leqslant C|g(n)|$. We write $f = \Theta(g)$ if $f = O(g)$ and $g = O(f)$. If the constant $C = C(k)$ depends on another parameter k (but not on n) then we shall denote this by writing $f = O_k(g)$, so for instance when we write $O_k(1)$, we simply mean a constant that depends on the parameter k.

By $f \ll g$ we mean $\frac{f(n)}{g(n)} \to 0$ as $n \to \infty$. We shall also use some of the standard notation from additive combinatorics: For sets $A, B \subseteq \mathbb{Z}_n$, $A+B := \{a+b : a \in A, b \in B\}$ and $\alpha A = \{\alpha a : a \in A\}$. Also, for sets A, the cardinality of A is denoted by $|A|$ as usual, but we shall also use the notation $\#A$ to denote the same, especially when A is a set of k-tuples of elements from some set, for some $k \geqslant 2$.

Let G be a finite abelian group written additively. By a G-sequence of length k, we shall mean a sequence $(x_1, \dots, x_k)$ with $x_i \in G$ for each i. By a *zero-sum* G-sequence (or simply, zero-sum sequence) we shall mean a G-sequence $(x_1, \dots, x_k)$ such that $\sum_i x_i = 0$, where 0 is the identity element of G. The *Davenport Constant* $D(G)$, introduced by Rogers [12], is defined as the smallest k such that every G-sequence of length k contains a non-trivial zero-sum subsequence. As it turns out, the Davenport constant is an important invariant of the ideal class group of the ring of integers of an algebraic number field (see [11] for more details).

A weighted version of the Davenport constant which first appeared in a paper by Adhikari *et al* ([3]), and was later generalized by Adhikari and Chen ([2]), goes as follows. Suppose G is a finite abelian group, and let $A \subset \mathbb{Z} \setminus \{0\}$ be a non-empty subset of the integers. The weighted Davenport Constant of G *with respect to the set* A is the least positive integer k for which the following holds: Given an arbitrary G-sequence $(x_1, \dots, x_k)$, there exists a non-empty subsequence $(x_{i_1}, \dots, x_{i_t})$ along with $a_j \in A$ such that $\displaystyle\sum_{j=1}^{t} a_j x_{i_j} = 0$. Here we adopt the convention that $ax := \overbrace{x + \cdots + x}^{a \text{ times}}$ for a positive, and $ax := (-a)(-x)$ for a negative. It is clear that if G has exponent n, then one may restrict A to be a subset of $[1, n-1]$.

As one might expect, the Davenport constant is best understood when G is a finite cyclic group. Here are some well-known results:

1. $D_{\pm}(\mathbb{Z}_n) = \lfloor \log_2 n \rfloor + 1$. Here our notation is a shorthand to denote that the set $A = \{-1, 1\}$. ([3])

2. $D_A(\mathbb{Z}_n) = 2$ if $A = \mathbb{Z}_n \setminus \{0\}$. ([3])

3. $D_A(\mathbb{Z}_n) = a + 1$ if $A = \mathbb{Z}_n^*$ and $a = \sum_{i=1}^{k} a_i$ for $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ ([10]). Here, $\mathbb{Z}_n^*$ denotes the set of primitive elements of $\mathbb{Z}_n$, i.e., the 'invertible' elements of $\mathbb{Z}_n$ when $\mathbb{Z}_n$ is viewed as a ring.

4. $D_A(\mathbb{Z}_n) = \lceil \frac{n}{r} \rceil$ if $A = \{1, \dots, r\}$ for some $1 \leqslant r \leqslant n-1$. ([4], [5])

For other results, see [1, 5].

The focal point of this paper stems from a natural extremal problem in light of the known results on the Davenport constant of a group. Suppose G is a finite abelian group of exponent n, and let $k \geqslant 2$ be an integer. Define

$$\begin{aligned} f_G^{(D)}(k) &:= \min\{|A| : \emptyset \neq A \subseteq [1, n-1] \text{ satisfies } D_A(G) \leqslant k\}, \\ &:= \infty \text{ if there is no such } A. \end{aligned}$$

Here is a natural extremal problem: Given a finite abelian group G, determine $f_G^{(D)}(k)$ for $k \in \mathbb{N}$.

It is important to note that if k is 'too small' relative to the group, then the parameter as defined above is in fact infinite. For instance, consider the group $G = \mathbb{Z}_p^r$ for p prime, and the sequence $\mathbf{x} := (e_1, \ldots, e_r)$ where $e_i = (0, \ldots, 0, 1, 0 \ldots, 0)$ has a 1 in the i^{th} coordinate, for $1 \leqslant i \leqslant r$. Then for any subset $A \subset \mathbb{Z}_p^*$ and any sequence $(a_1, a_2, \ldots, a_r)$ with $a_i \in A$ the element $\sum_{i=1}^{r} a_i e_i = 0$ implies $a_i = 0$ for each i, which implies that $f_G^{(D)}(k) = \infty$ for $k \leqslant r$. However, for $k > r$ we do have $f_G^{(D)}(k) < \infty$. A consequence of one of our results implies that for every group, if k is not too small (this will be more clear when we see the statement of the theorem) then $f_G^{(D)}(k) < \infty$, so this is indeed a non-trivial parameter. For $G = \mathbb{Z}_n$, we shall write $f^{(D)}(n, k) := f_G^{(D)}(k)$ for convenience.

As it turns out, the nature of this extremal problem of determining $f_G^{(D)}(k)$ is most interesting for the case when G is a cyclic group of prime order, and in that case, we establish the following bounds.

Theorem 1. Let $k \in \mathbb{N}$, $k \geqslant 2$. There exists an integer $p_0(k)$ and an absolute constant $C = C(k) > 0$ such that for all prime $p > p_0(k)$

$$p^{1/k} - 1 \leqslant f^{(D)}(p, k) \leqslant C(p \log p)^{1/k}.$$

As some of our preliminary results will illustrate, this also determines asymptotically (up to a logarithmic factor) $f_G^{(D)}(k)$ for $G = \mathbb{Z}_p^r$ and $G = \mathbb{Z}_{p^r}$ and these in turn 'almost' determine $f_G^{(D)}(k)$ in all cases up to a logarithmic factor for all integers $k \geqslant 2$.

In a couple of special cases, viz., $k = 2, 4$, we are able to obtain an asymptotically sharper upper bound which is tight upto constant factors. In fact, for the case $k = 2$, the extremal problem even achieves tight bounds in certain special cases.

Theorem 2. Let p be an odd prime.

1. If $p = q^2 + q + 1$ for some prime q then $f^{(D)}(p, 2) = \lceil \sqrt{p-1} \rceil$.

2. $f^{(D)}(p, 2) \leqslant 2\lceil \sqrt{p} \rceil$.

3. $f^{(D)}(p, 4) \leqslant C_0 p^{1/4}$ for some constant $C_0 > 0$.

In particular, this theorem establishes that $f^{(D)}(p, k)$ is of the order of $p^{1/k}$ for $k = 2, 4$ upto a constant factor. As for the tightness result, there is an old conjecture of Hardy-Littlewood that there are infinitely many prime pairs (p, q) such that $p = q^2 + q + 1$.

The rest of the paper is organized as follows. We begin with some preliminaries before launching into a formal description in section 3 of the extremal problem. In section 4 we prove theorems 1 and 2. We conclude the paper with some remarks and open questions.

Before we end this section, we set up some notation and terminology. For a sequence $\mathbf{x} = (x_1, \ldots, x_m)$ and a subset $I \subseteq [1, m]$ of the set of indices, we shall denote by $\mathbf{x}_I$ the sum $\sum_{i \in I} x_i$. For sequences $\mathbf{x} = (x_1, \ldots, x_m), \mathbf{y} = (y_1, \ldots, y_m)$, we shall denote the sum $\sum_{i=1}^{m} x_i y_i$ by $\langle \mathbf{x}, \mathbf{y} \rangle$, and $\mathbf{0}_k$ shall denote the k-tuple $(0, \ldots, 0)$.

2 Preliminaries

In this section, we state a few well known results that we serve as important tools in the proofs of theorems 1 and 2.

We start with recalling Janson's inequality (see [7], for instance), which is our main probabilistic tool in the proof of theorem 1. The version of the inequality that we shall use is given below for the sake of completeness.

Suppose Ω is a finite set, and let R a random subset of Ω where each $r \in \Omega$ is chosen independently with probability p_r. Let $A_i \subset \Omega$ for $i = 1, 2 \ldots, t$, and let $\mathcal{E}_i$ denote the event: $A_i \subset R$. Let $N = \#\{i : A_i \subset R\}, \mu := \mathbb{E}(N),\ \Delta := \sum_{i \sim j} \mathbb{P}(\mathcal{E}_i \wedge \mathcal{E}_j)$, where we write $i \sim j$ if $A_i \cap A_j \neq \emptyset$. Then one of the forms of Janson's inequality states that

$$\mathbb{P}(N = 0) \leqslant \exp(-\mu + \frac{\Delta}{2})$$

and this is what we shall use.

For the proof of theorem 2, we need the notion of a Difference set in an abelian group (see [9]).

Definition 3. **Difference Set:** Suppose G is an abelian group of order v. A set $D \subset G \backslash \{0\}$ is called a (v, k, λ) difference set if

1. $|D| = k$ and
2. for each $g \in G, g \neq 0$, there are exactly λ pairs $(d, d') \in D \times D$ such that $d - d' = g$.

If $\lambda = 1$, then D is called a *Perfect Difference Set.*

The relevant theorem in our context is a classical result due to Singer ([13]):

Theorem 4. (Singer, [13]) Suppose $n = q^2 + q + 1$ for q prime, then the cyclic group $G = \mathbb{Z}_n$ admits a perfect difference set of size $q + 1$.

3 The extremal problem of $f_G^{(D)}(k)$

Let $k \geqslant 2$ be an integer. We start by recalling the definition of $f_G^{(D)}(k)$:

$$f_G^{(D)}(k) := \min\{|A| : A \subseteq [1, n-1] \text{ satisfies } D_A(G) \leqslant k\}. \tag{1}$$

We shall (as mentioned in the introduction) write $f^{(D)}(n, k)$ to denote $f_G^{(D)}(k)$ for $G = \mathbb{Z}_n$.

Proposition 3.1. Let $G = H_1 \times \cdots \times H_r$ be the product of p_i-groups H_i with $p_1 < p_2 < \cdots < p_r$. Then for all k, $f_G^{(D)}(k) \leqslant \min\{f_{H_i}^{(D)}(k) : 1 \leqslant i \leqslant r\}$. In particular, if $G = \mathbb{Z}_p \times H$ is a finite abelian group with $p \nmid |H|$, then for any integer k, $f_G^{(D)}(k) \leqslant f^{(D)}(p, k)$.

Proof. Write $n_i = \exp(H_i)$, and let $n := \exp(G) = \prod_{i=1}^{r} n_i$.

Suppose $f_{H_i}^{(D)}(k) = \ell$, and let $A_i := \{a_1, \dots, a_\ell\} \subset [1, n_i - 1]$ be such that $D_{A_i}(H_i) \leqslant k$. Then consider the set

$$A = \{(n/n_i)a_1, \dots, (n/n_i)a_\ell\} \subset [1, n-1].$$

We claim that for any G-sequence $\mathbf{g} = (g_1, \dots, g_k)$ of length k there exists an $\mathbf{a} = (a_1, \dots, a_k) \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$, for which $\langle \mathbf{g}, \mathbf{a} \rangle = 0$ in G.

Write $g_j = (x_j, y_j)$ for $j \in [1, k]$, where $x_j \in H_i$ and $y_j \in H := \prod_{r \neq i} H_r$. Since $\exp(H) = n/n_i$ we have $(n/n_i)y_j = 0$ for all j. Furthermore, by the assumption, there exists $\mathbf{a} = (a_1, \dots, a_k) \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ such that $\langle \mathbf{x}, \mathbf{a} \rangle = 0$, where $\mathbf{x} = (x_1, \dots, x_k)$. Consequently,

$$\sum_{j=1}^{k} \frac{na_j}{n_i}(x_j, y_j) = \left(\sum_{j=1}^{k} \frac{na_j}{n_i} x_j, \sum_{j=1}^{k} \frac{na_j}{n_i} y_j \right) = (0, 0)$$

and that completes the proof.

The second part of the statement is an immediate consequence of the first part. □

The next proposition compares groups G, H with the same exponent.

Proposition 3.2. Let $k \geqslant 2$. Suppose G and H are finite abelian groups with $H = G \times G'$ and $\exp(G) = \exp(H)$. Then

$$f_G^{(D)}(k) \leqslant f_H^{(D)}(k).$$

In particular, if $G_n = (\mathbb{Z}_p)^n$ and we write $f_n := f_{G_n}^{(D)}(k)$, then the sequence $\{f_n\}_{n \geqslant 1}$ is increasing.

Proof. Let $f_H^{(D)}(k) = \ell$. Let $A \subset [1, \exp(G) - 1]$ with $|A| = \ell$ such that for all H-sequences $\mathbf{x}$ of length k, there exists $\mathbf{a} \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ such that $\langle \mathbf{x}, \mathbf{a} \rangle = 0$. Let $\mathbf{y} = (y_1, \dots, y_k)$ be a G-sequence of length k, and consider the sequence $\mathbf{x} = (x_1, \dots, x_k)$, where $x_i = (y_i, 0) \in H$. Let $\mathbf{a} = (a_1, \dots, a_k) \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ be such that $\langle \mathbf{x}, \mathbf{a} \rangle = 0$ in H. But since $\exp(G) = \exp(H)$, this implies that $\langle \mathbf{y}, \mathbf{a} \rangle = 0$ in G as well. This completes the proof.

The second part is again a straightforward consequence of the first statement. □

The next theorem contrasts $f^{(D)}(p, k)$ with $f_G^{(D)}(k)$ for $G = \mathbb{Z}_{p^m}$.

Theorem 5. Let p be a prime and $m \geqslant 1, k \geqslant 2$ be positive integers. Then for $G = \mathbb{Z}_{p^m}$,

$$p^{1/k} - 1 \leqslant f_G^{(D)}(k) = f^{(D)}(p, k).$$

Proof. We first prove that $f_G^{(D)}(k) = f^{(D)}(p, k)$. Let $f^{(D)}(p, k) = \ell$. Then there exists $A = \{a_1, \dots, a_\ell\} \subset \mathbb{Z}_p^*$ of size ℓ such that for every $\mathbb{Z}_p$-sequence $\mathbf{x} := (x_1, \dots, x_k)$ of length k, there exists $\mathbf{a} = (a_{i_1}, \dots, a_{i_k}) \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ such that $\langle \mathbf{a}, \mathbf{x} \rangle = 0$. Set $A' = p^{m-1}A \subset [1, p^m - 1]$. Consider a $\mathbb{Z}_{p^m}$-sequence $\mathbf{x}' := (x_1', \dots, x_k')$ of length k and let x_i denote the projection of x_i' on $\mathbb{Z}_p$. By our assumption, there exist $(a_{i_1}, \dots, a_{i_k}) \in$

$(A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$, such that $\langle \mathbf{a}, \mathbf{x}' \rangle = 0$. Consequently, $\langle p^{m-1} \cdot \mathbf{a}, \mathbf{x}' \rangle = 0$ in G. This establishes that $f_G^{(D)}(k) \leqslant f^{(D)}(p,k)$.

We shall now prove the reverse inequality, i.e., $f_G^{(D)}(k) \geqslant f^{(D)}(p,k)$ by means of contradiction. Clearly, $m \geqslant 2$, or there is nothing to prove. Suppose if possible that there exists $A \subset [1, p^m - 1]$ with $|A| < f^{(D)}(p,k)$ such that for every G-sequence $\mathbf{x} = (x_1, \ldots, x_k)$ of length k there exists $\mathbf{a} \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ such that $\langle \mathbf{a}, \mathbf{x} \rangle = 0$ in G. Let us write

$$A = A_0 \cup (p \cdot A_1) \cup \cdots \cup \left(p^{m-1} \cdot A_{m-1}\right)$$

with $A_i \subset \mathbb{Z}_{p^{m-i}}^*$ for each $0 \leqslant i \leqslant m-1$. Let $A_i' := A_i \pmod{p}$, and let $B = \cup_{i=0}^{m-1} A_i'$. Clearly, $B \subset [1, p-1]$ and $|B| \leqslant |A| < f^{(D)}(p,k)$.

Let $\mathbf{y} = (y_1 \ldots, y_k)$ be a $\mathbb{Z}_p$-sequence of length k. Viewing this as a G-sequence, and using the property of A, it follows that there exists $\mathbf{a} \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ such that

$$\sum_{A_0} a_i y_i + p \cdot \sum_{A_1} a_i y_i + \cdots + p^{m-1} \sum_{A_{m-1}} a_i y_i \equiv 0 \pmod{p^m}. \tag{2}$$

In this notation, if all the a_i listed in a particular summand are zero, then we treat that summand as empty.

Now, if the first summand is non-empty, then we must have $\sum_{A_0'} a_i' y_i = 0$ in $\mathbb{Z}_p$; here by a_i' we mean the corresponding projection of a_i into the set A_0'. In general, if the first non-empty summand in (2) is $p^j \sum_{A_j} a_i y_i$, then considering (2) modulo p^j it follows that $\sum_{A_j'} a_i' y_i = 0$ in $\mathbb{Z}_p$. Since at least one summand is non-empty, this yields a non-empty subsequence of $\mathbf{y}$ that admits a B-weighted zero-sum subsequence in $\mathbb{Z}_p$, contradicting that $|B| < f^{(D)}(p,k)$. This completes the other inequality, and thereby establishes $f_G^{(D)}(k) = f^{(D)}(p,k)$ for $G = \mathbb{Z}_{p^m}$.

We finally prove that $f^{(D)}(p,k) \geqslant p^{1/k} - 1$. Consider a bipartite graph $\mathcal{G} = (V, E)$ with $V = \mathcal{X} \cup \mathcal{Y}$, where $\mathcal{X}$ consists of all k-tuples $\mathbf{a} \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ and $\mathcal{Y}$ consists of all k-tuples $\mathbf{x} = (x_1, x_2, \ldots, x_k)$ where all the x_i's are non-zero elements in $\mathbb{Z}_p$, and $\mathbf{a}, \mathbf{x}$ are adjacent in $\mathcal{G}$ if and only if $\langle \mathbf{a}, \mathbf{x} \rangle = 0$ in $\mathbb{Z}_p$. By the hypothesis on A, it follows that every vertex of $\mathcal{Y}$ is adjacent to at least one vertex of $\mathcal{X}$, so $\mathcal{G}$ has at least $(p-1)^k$ edges. On the other hand, fix $\mathbf{a} \in \mathcal{X}$, and assume without loss of generality that $a_1 \neq 0$. Then for any possible choices for $x_2, \ldots, x_k \in \mathbb{Z}_p^*$, the equation $a_1 x_1 = -(a_2 x_2 + \cdots + a_k x_k)$ admits a unique solution for $x_1 \in \mathbb{Z}_p$, so that the vertex $\mathbf{a} \in \mathcal{X}$ has degree at most $(p-1)^{k-1}$. Hence

$$|\mathcal{X}|(p-1)^{k-1} \geqslant |E| \geqslant (p-1)^k,$$

and since $|\mathcal{X}| = (|A|+1)^k - 1$, it follows that

$$|A| = f^{(D)}(p,k) \geqslant p^{1/k} - 1$$

and that completes the proof.

□

The last part of the proof of theorem 5 in fact can be modified *mutatis mutandis* to also show that $f_G^{(D)}(k) \geqslant |G|^{1/k} - 1$ holds for $G = \mathbb{Z}_p^s$. To reiterate a point we mentioned in the introduction, $f_G^{(D)}(k) = \infty$ for $k \leqslant s$. In light of the remark above, it is somewhat natural that we turn our attention to the case $G = \mathbb{Z}_n^s$. The following proposition shows that for $k > s+1$ and p reasonably large, the parameter $f_G^{(D)}(k) < \infty$.

Proposition 3.3. Let $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$, where $1 < n_1 \mid \cdots \mid n_s$. Let $1 \leqslant r < (n-1)/2$, and let $A = \{\pm 1, \pm 2, \cdots, \pm r\}$. Then

$$\begin{aligned} 1 + \sum_{i=1}^{s} \left\lceil \log_{r+1} n_i \right\rceil \geqslant D_A(G) &\geqslant 1 + \sum_{i=1}^{s} \left\lfloor \log_{r+1} n_i \right\rfloor \text{ for } s \geqslant 2 \\ D_A(\mathbb{Z}_n) &= \left\lfloor \log_{r+1} n \right\rfloor + 1. \end{aligned}$$

Consequently, $f^{(D)}(n,k) \leqslant 2(n^{1/(k-1)} - 1)$, and $f_G^{(D)}(k) \leqslant 2(|G|^{1/(k-s-1)} - 1)$ for $s > 1$.

Proof. Consider the following sequence of elements of G:

$$\begin{aligned} \mathbf{a} :=& (1, \ldots, 0), ((r+1), \ldots, 0), \cdots, ((r+1)^{t_1}, \ldots, 0), \cdots, (0, \ldots, 1), \\ & (0, \ldots, (r+1)), \cdots, (0, \ldots, (r+1)^{t_s}), \end{aligned}$$

where t_i is defined by $(r+1)^{t_i+1} \leqslant n_i < (r+1)^{t_i+2}$ for $1 \leqslant i \leqslant s$. If t is such that $(r+1)^{t+1} \leqslant n < (r+1)^{t+2}$ then by the choice of t, all integers of the form $a_0 + a_1(r+1) + \cdots + a_t(r+1)^t$ where $a_i \in [r]$ are strictly less than n, and are distinct in $\mathbb{Z}_n$, it follows that no element of the form $a_0 + a_1(r+1) + \cdots + a_t(r+1)^t$ where $a_i \in A$ equals zero in $\mathbb{Z}_n$. In particular, it follows that the sequence $\mathbf{a}$ admits no non-trivial zero sum subsequence. Furthermore, since $\mathbf{a}$ has $\sum_{i=1}^{s}(t_i+1) = \sum_{i=1}^{s} \left\lfloor \log_{r+1} n_i \right\rfloor$ elements, we have $D_A(\mathbb{Z}_n) \geqslant \sum_{i=1} \left\lfloor \log_{r+1} n_i \right\rfloor + 1$.

To prove the upper bound, consider a sequence $\mathbf{x} = (x_1, \ldots, x_t)$ of length

$$t = \sum_{i=1}^{s} \left\lceil \log_{r+1} n_i \right\rceil + 1,$$

where $x_i = (\alpha_1^{(i)}, \alpha_2^{(i)}, \ldots, \alpha_s^{(i)})$ for $i = 1, \ldots, t$.

Let

$$N = \left\{ \sum_{\ell=1}^{r} \ell \mathbf{x}_{I_\ell} : I_\ell \subseteq [1,t], I_i \cap I_j = \emptyset \text{ for } i \neq j \right\}.$$

Now if we show that $|N| \geqslant n_1 \cdots n_s$ then it follows that $D_A(\mathbb{Z}_n) \leqslant t$. Indeed, since $|G| = n_1 \cdots n_s$, it would follow that for some distinct collections of sets $\{I_j\}_{j \in [1,r]}, \{J_j\}_{j \in [1,r]}$ with $I_i \cap I_j = J_i \cap J_j = \emptyset$ whenever $i \neq j$, we have

$$\sum_{j=1}^{r} j \mathbf{x}_{I_j} = \sum_{j=1}^{r} j \mathbf{x}_{J_j}$$

as elements in G. But then this yields a relation of the form $\sum_{j=1}^{r} a_j \mathbf{x}_{I_j} = 0$ with $a_j \in \{\pm 1, \ldots, \pm r\}$ and that is what we seek.

It is now a straightforward exercise to check that $|N| = (r+1)^t$. Since

$$t = \sum_{i=1}^{s} \lceil \log_{r+1} n_i \rceil + 1 > \sum_{i=1}^{s} \log_{r+1} n_i,$$

we have $|N| \geqslant n_1 \cdots n_s$ and the proof is complete. □

We quickly return to a point we made in the introduction about the finiteness of the parameter $f_G^{(D)}(k)$. By propositions 3.1, 3.2, 3.3, it is easy to see that when k is not 'too small' (and we shall prefer to be somewhat vague about what 'small' means exactly, though it can easily be expounded in more precise terms), we necessarily have $f_G^{(D)}(k) < \infty$. But as we shall see, the bound in proposition 3.3 is far from best possible, even in the case when G is a cyclic group of prime order.

Before we conclude this section, we make one other digressive remark. If $A \subset [1, \exp(G)-1]$ is somewhat 'large', (so that $D_A(G)$ is 'small') then it is probably tempting to conclude that one must have $D_B(G)$ large where $B = [1, \exp(G)-1] \setminus A$; that is however false, as the following example shows.

Let p be prime and consider $G = \mathbb{Z}_p, A_r = \{\pm 1, \pm 2, \ldots, \pm r\}$, and $B_r = \mathbb{Z}_p \setminus \{0, \pm 1, \pm 2, \ldots, \pm r\}$. We claim that $D_{B_r}(\mathbb{Z}_p) \leqslant 2$ for $r < \frac{p-1}{4}$. Then by the previous proposition, for somewhat large r, say $r = \Omega(p)$, we have $D_{A_r}(\mathbb{Z}_p) = D_{B_r}(\mathbb{Z}_p) = 2$.

To see this, consider the sequence $\mathbf{x} := (1, \alpha)$ with $\alpha \neq 0$. If $\alpha \in \frac{1}{i} B_r$ for some i satisfying $(r+1) \leqslant i \leqslant p-(r+1)$, then it is easy to see that there exist $a, b \in B_r$ such that $a.1 + b.\alpha = 0$. So the only interesting case is when $\alpha \in \bigcap_{i=r+1}^{p-(r+1)} \frac{1}{i} A_r$. The main observation now is that if $r < \frac{p-1}{4}$, then $\bigcap_{i=r+1}^{p-(r+1)} \frac{1}{i} A_r = \emptyset$. Indeed, consider an array whose rows are indexed by the elements of B_r, the columns by the elements of A_r, and whose $(i,j)^{th}$ entry is j/i. An element of the intersection corresponds to picking a transversal for this array, i.e., a set of entries, one from each row, such that no two chosen elements are in the same column. But this is impossible if $p - 2r - 1 > 2r$, i.e., if $r < \frac{p-1}{4}$.

4 Proofs of theorem 1 and theorem 2

In this section, we prove theorems 1 and 2, which shall appear in the two subsections of this section.

The main idea behind the proof of theorem 1 is to consider random sets A. To make this more specific, suppose $0 < \theta < 1$. By a *θ-random subset of* $[a, b]$, we mean a random subset $A \subseteq [a, b]$ obtained by picking each $i \in [a, b]$ independently with probability θ. Also, for a probability space we say that a sequence of events $\mathcal{E}_n$ occurs *with high probability* (abbreviated as *whp*) if $\lim_{n\to\infty} \mathbb{P}(\mathcal{E}_n) = 1$. In our results, the parameter n will be clear from their corresponding contexts, so we do shall not draw attention to it explicitly.

Before we state our main result more precisely, we note that one can prove a more general upper bound for $f_G^{(D)}(k)$ for *all* abelian groups. In fact, the following proposition also shows that $f_G^{(D)}(k)$ is a relevant problem only for $k \leqslant \lceil \log_2 |G| \rceil + 1$.

Proposition 4.1. Suppose G is a finite abelian group of exponent n, and let A be a θ-random subset of $[1, n-1]$, where $\theta \geqslant \frac{\omega(n)}{\sqrt{n}}$, where $\omega(n) \to \infty$ as $n \to \infty$. Then $D_A(G) \leqslant \lfloor \log_2 |G| \rfloor + 1$ *whp.*

Proof. Suppose the set A contains $x, n-x$, for some $x \in [1, n-1]$. Let $\mathbf{y} = (y_1, \dots, y_s)$ be a G-sequence, and suppose $s > \log_2 |G|$. Consider the set $\{\mathbf{y}_I : I \subseteq [1, s]\}$; as I varies over all subsets of $[1, s]$ and as there are $2^s > |G|$ such summands, it follows that there exist $J_1, J_2 \subseteq [1, s]$ with $J_1 \neq J_2$ such that $\mathbf{y}_{J_1} = \mathbf{y}_{J_2}$. Set $J = (J_1 \cup J_2) \setminus (J_1 \cap J_2)$ and define the sequence $\mathbf{a}$ by setting $a_j = x$ for $j \in J_1 \setminus J_2$ and $a_j = n - x$ if $j \in J_2 \setminus J_1$. Then clearly, $\langle \mathbf{y}, \mathbf{a} \rangle_J = 0$, so it follows that for such A, we have $D_A(G) \leqslant \lfloor \log_2 |G| \rfloor + 1$.

Let A be a θ-random subset of $[1, n-1]$. For each $x \in [1, n-1]$, let $\mathcal{E}_x$ denote the event that both $x, n-x$ are in A, and let $\mathcal{E} = \bigwedge_x \overline{\mathcal{E}_x}$. Since A is θ-random, it follows that

$$\mathbb{P}(\mathcal{E}) = (1 - \theta^2)^{\frac{n-1}{2}} \leqslant e^{-\theta^2 (n-1)}.$$

By assumption, $\theta \gg 1/\sqrt{n}$, so it follows that $\mathbb{P}(\mathcal{E}) \to 0$ as $n \to \infty$ and so we are done. □

Remark: A quick consequence of proposition 4.1 is the following: Set $\theta = \sqrt{\frac{\log n}{n}}$. Then *whp* a θ-random subset of $[1, n-1]$ satisfies $D_A(G) \leqslant \lfloor \log_2 |G| \rfloor + 1$. In particular, for any $k \leqslant \lfloor \log_2 |G| \rfloor + 1$, we have $f_G^{(D)}(k) \leqslant O(\sqrt{n \log n})$.

4.1 Proof of theorem 1

As mentioned earlier, the proof of theorem 1 involves understanding the asymptotic behaviour of $D_A(\mathbb{Z}_p)$ for random $A \subset [1, p-1]$. The following theorem in this subsection details the nature of $D_A(\mathbb{Z}_p)$ when A is θ-random, for prime p:

Theorem 6. Suppose p is a prime and A is a θ-random subset of $[1, p-1]$. Let $\omega(p), \omega'(p)$ be arbitrary functions satisfying $\omega(p), \omega'(p) \to \infty$ as $p \to \infty$. Also, suppose p is sufficiently large.

1. If $\theta > \sqrt{\frac{2 \log p + \omega(p)}{p}}$, then *whp* $D_A(\mathbb{Z}_p) = 2$.

2. If $k \geqslant 3$ is an integer and θ satisfies

$$\frac{(3kp(\log p + \omega(p)))^{1/k}}{p} < \theta < \frac{p^{1/(k-1)}}{p\, \omega'(p)},$$

then *whp* $D_A(\mathbb{Z}_p) = k$.

Remark: One could have incorporated the first part of theorem 6 into the second more general part, but we state the theorem as we do, because the proof of the first part is simpler, and motivates and elucidates the general strategy better; the difference comes in the finer details.

It is clear that theorem 6 implies the result of theorem 1. Also, theorem 6 is clearly not tight as in that the theorem makes a statement only for $\frac{(p\log p)^{1/k}}{p} \ll \theta \ll \frac{p^{1/(k-1)}}{p}$. The constant 3 in the statement of the theorem is definitely not tight (even by our method of proof), but we make no attempt to improve it to find the best possible constant in order to make the presentation more lucid.

Proof. 1. First observe that $D_A(\mathbb{Z}_n) \geqslant 2$ follows trivially by considering the sequence $\mathbf{x} = (1)$. Fix a sequence $\mathbf{x} = (x_1, x_2)$ of length 2 in $\mathbb{Z}_p$. Without loss of generality, we may assume that both $x_i \in \mathbb{Z}_p^*$. Write $u = x_2/x_1 \neq 0$.

For this given sequence, consider the graph $G_u = (V_u, E_u)$, where $V_u = \mathbb{Z}_p^*$ and for $a, b \in V_u$, $\{a, b\} \in E_u$ if and only if $a = -bu$ or $b = -au$. If $A \subset [1, p-1]$ is regarded a subset of the vertex set of G_u, and if A is not independent in G_u, then by the definition of G_u, it follows that the sequence (x_1, x_2) admits a pair $a, b \in A$ such that $ax_1 + bx_2 = 0$.

Suppose A is a θ-random subset of $[1, p-1]$ and let $N_u = |\{e \in E_u : e \subset A\}|$. Since each vertex of G_u has degree 2, G_u is a union of cycles, so it is straightforward to see that

$$\mathbb{E}(N_u) = (p-1)\theta^2, \quad \mathit{\Delta} := \sum_{\substack{e\cap e'\neq\emptyset \\ e\neq e'\in E_u}} \mathbb{P}(e, e' \subset A) = (p-1)\theta^3.$$

By Janson's Inequality we have $\mathbb{P}(N_u = 0) \leqslant e^{-(p-1)\theta^2(1-\theta/2)}$. Hence by the hypothesis on θ,

$$\begin{aligned}\mathbb{P}(\text{There exists } u \in \mathbb{Z}_p^* \text{ such that } N_u = 0) &\leqslant \exp(-(p-1)\theta^2(1-\theta/2) + \log p) \\ &\leqslant \exp\left(-\omega(p)\right),\end{aligned}$$

and that completes the proof.

2. The proof of this part is very similar to the proof of part 1, with the crucial difference being that rather than evaluate μ, Δ precisely (which is messy), we shall use appropriate bounds in this case.

Let $\mathcal{X}$ be the set of all k-tuples $\mathbf{x} = (x_1, \ldots, x_k)$ of elements in $\mathbb{Z}_p$ such that $\mathbf{x}_I \neq 0$ for all non-trivial subsets $I \subseteq [1, k]$.

Fix $\mathbf{x} \in \mathcal{X}$ and call a k-tuple $\mathbf{a} = (a_1, \ldots, a_k) \in (\mathbb{Z}_p^*)^k$ *good for* $\mathbf{x}$ if $\langle \mathbf{x}, \mathbf{a} \rangle = 0$. For each $i \in [1, k]$, let $\mathcal{N}_i := \mathcal{N}_i(\mathbf{x})$ denote the set of good k-tuples $(a_1, \ldots, a_k)$ with exactly i distinct a_j's, and let $n_i = |\mathcal{N}_i|$. We claim that

(a) If $i < k$ then $n_i = O_k(p^{i-1})$.

(b) $n_k \geqslant (p-1)(p-2)\cdots(p-k+1) - O_k(p^{k-2}) \geqslant p^{k-1}/2$ for $p \gg k$.

To see why, first let $i < k$; suppose $\mathbf{a} \in \mathcal{N}_i$ is good for $\mathbf{x}$, and let $a, b_1, \ldots, b_{i-1}$ be the distinct elements of $\mathbf{a}$. Then there is a corresponding partition $[1,k] = \cup_{j=0}^{i-1} I_j$ into i non-empty, disjoint sets satisfying $a\mathbf{x}_{I_0} + b_1\mathbf{x}_{I_1} + \cdots + b_{i-1}\mathbf{x}_{I_{i-1}} = 0$. Fix such a partition of $[1,k]$ and consider the aforementioned equation. For each set of pairwise distinct choices for $b_1, \ldots, b_{i-1} \in \mathbb{Z}_p^*$, there is a unique $a \in \mathbb{Z}_p$ that satisfies this equation. In other words, every set of pairwise distinct $b_1, \ldots, b_{i-1}$ gives rise to at most one set $\{a, b_1, \ldots, b_{i-1}\}$ that satisfy the equation above. Since each element of $\mathcal{N}_i$ arises from some such set of i distinct elements, and since each such set of i distinct elements gives rise to at most k^k different elements of $\mathcal{N}_i$, it follows that for $p \gg k$, $n_i = O_k(p^{i-1})$.

For $i = k$, again, for distinct choices of $b_1, \ldots, b_{k-1}$, the equation $ax_1 + b_1x_2 + \cdots + b_{k-1}x_k = 0$ admits a unique solution for $a \in \mathbb{Z}_p$. Hence the number of $(k-1)$-tuples $(b_1, \ldots, b_{k-1})$ of pairwise distinct elements of $\mathbb{Z}_p^*$ either counts some $\mathbf{a} \in \mathcal{N}_k$ (if $a \neq 0, b_i$ for any of the b_i) or enumerates a sequence $\mathbf{b} \in \mathcal{N}_{k-1}(\mathbf{y})$ for the sequence $\mathbf{y} = (x_2, \ldots, x_k)$ of length $(k-1)$ (if $a = 0$), or enumerates a sequence in $\mathcal{N}_{k-1}(\mathbf{x})$. Hence by induction on k for instance, and the preceding discussion, we have

$$n_k \geqslant (p-1)(p-2)\cdots(p-k+1) - O_k(p^{k-2}) \geqslant \frac{p^{k-1}}{2}$$

and that proves the claim.

Let $N_{\mathbf{x}}$ denote the number of good k-tuples for $\mathbf{x}$ arising from the θ-random set A. Then

$$\mu = \mathbb{E}(N_{\mathbf{x}}) = \sum_{i=1}^{k} n_i\theta^i \geqslant \frac{1}{2}p^{k-1}\theta^k,$$

by the discussion above, for p sufficiently large.

To give an upper bound for Δ, we set up some additional notation. For k-tuples $\mathbf{a}, \mathbf{b}$, we write $\mathbf{a} \sim \mathbf{b}$ if there is some common element (not necessarily in the same position) in the sequences, and by $|\mathbf{a} \cap \mathbf{b}|$ we shall denote the number of common elements in the two k-tuples.

First, observe that

$$\Delta = \sum_{\substack{\mathbf{a}\sim\mathbf{b}\\ \mathbf{a},\mathbf{b}\text{ good}}} \mathbb{P}(\mathbf{a},\mathbf{b} \subset A) = \sum_{2\leqslant j\leqslant i\leqslant k} \sum_{\ell=1}^{j} \sum_{\substack{\mathbf{a}\sim\mathbf{b}\\ \mathbf{a}\in\mathcal{N}_i, \mathbf{b}\in\mathcal{N}_j\\ |\mathbf{a}\cap\mathbf{b}|=\ell}} \mathbb{P}(\mathbf{a},\mathbf{b} \subset A) \tag{3}$$

$$= \sum_{2\leqslant j\leqslant i\leqslant k} \sum_{\ell=1}^{j} \#\big\{(\mathbf{a},\mathbf{b}) \in \mathcal{N}_i \times \mathcal{N}_j : |\mathbf{a}\cap\mathbf{b}| = \ell\big\} \cdot \theta^{i+j-\ell} \tag{4}$$

To bound this expression, we claim

(a) For all $j \leqslant i \leqslant k$ and all $1 \leqslant \ell \leqslant j$ we have

$$\#\big\{(\mathbf{a},\mathbf{b}) \in \mathcal{N}_i \times \mathcal{N}_j : |\mathbf{a} \cap \mathbf{b}| = \ell\big\} = O_k(p^{i+j-\ell-2}).$$

(b) In the special case $i = j = k, \ell = 1$, we have

$$\#\big\{(\mathbf{a},\mathbf{b}) \in \mathcal{N}_k \times \mathcal{N}_k : |\mathbf{a} \cap \mathbf{b}| = 1\big\} \leqslant k^2 p^{2k-3}.$$

Indeed, there are $n_i = O_k(p^{i-1})$ choices for $\mathbf{a} \in \mathcal{N}_i$. Fix $\mathbf{a} \in \mathcal{N}_i$, and let $\{a_{i_1}, \ldots, a_{i_\ell}\}$ be a set of ℓ distinct elements that appear in $\mathbf{a}$. Choose a subset $L \subset [1,k]$ of size ℓ, and consider an arrangement $(b_1, \ldots, b_\ell)$ of these elements in the positions of L. Now for a partition $[1,k] = \cup_{t=1}^{j} I_t$ with $b_t \in I_t$ for $t \in L$ it follows that there are at most $p^{j-\ell-1}$ sequences $\mathbf{b}$ that are good for $\mathbf{x}$ and extend the partial sequence $(b_1, \ldots, b_\ell)$. Since there are $O_k(1)$ choices for the sequence $(a_{i_1}, \ldots, a_{i_\ell})$, $O_k(1)$ choices for the set L, $O_k(1)$ choices for the arrangement $(b_1, \ldots, b_\ell)$ and a further $O_k(1)$ choices for the partition $(I_1, \ldots, I_j)$ with $b_t \in I_t$ for each $t \in L$, it follows that there are at most $O_k(1)p^{j-\ell-1}$ sequences $\mathbf{b}$ that are good for $\mathbf{x}$ which satisfy $\mathbf{a} \sim \mathbf{b}$ and $|\mathbf{a} \cap \mathbf{b}| = \ell$. Since this holds for each $\mathbf{a}$, the first claim holds.

For the second claim, we only need to note that in the case $i = j = k$, and $\ell = 1$, there are k choices for picking the common element a_i, and a further k choices for choosing a position for that a_i in the sequence $\mathbf{b} = (b_1 \ldots, b_k)$. The rest of the argument is exactly as before.

Now, piecing all the observations from above, and using the expression for Δ (see (4) above), it follows that for p sufficiently large, we have

$$\Delta = \sum_{\substack{\mathbf{a}\sim\mathbf{b} \\ \mathbf{a},\mathbf{b} \text{ good}}} \mathbb{P}(\mathbf{a},\mathbf{b} \subset A) \leqslant 2k^2\theta^{2k-1}p^{2k-3}.$$

Consequently, by Janson's Inequality

$$\mathbb{P}(N_{\mathbf{x}} = 0) \leqslant e^{-\mu+\frac{\Delta}{2}} \leqslant \exp\left(-\frac{1}{2}\theta^k p^{k-1} + 2k^2\theta^{2k-1}p^{2k-3}\right).$$

So, again as before,

$$\begin{aligned}\mathbb{P}(\text{There exists } \mathbf{x} \text{ such that } N_{\mathbf{x}} = 0) &\leqslant \exp\left(-\frac{1}{2}\theta^k p^{k-1} + 2k^2\theta^{2k-1}p^{2k-3} + k\log p\right) \\ &< \exp\left(-C\omega(p)\right)\end{aligned}$$

for some absolute constant $C > 0$, by the bounds on θ.

For the final part of the theorem, consider the sequence $\mathbf{1}_{k-1} := (\underbrace{1, \ldots, 1}_{k-1 \text{ times}})$. We claim that *whp* there is no sequence $\mathbf{a} \in (A(\cup\{0\})^{(k-1)} \setminus \{\mathbf{0}_{k-1}\}$ such that $\langle \mathbf{1}_{k-1}, \mathbf{a}\rangle = 0$.

Again, let T_{k-1} denote the number of $(k-1)$-tuples $\mathbf{a} = (a_1, \ldots, a_{k-1}) \in \mathbb{Z}_p^{k-1} \setminus \{\mathbf{0}_{k-1}\}$ satisfying $\langle \mathbf{1}_{k-1}, \mathbf{a} \rangle = 0$. Again, let N_i denote the number of $(k-1)$-tuples $\mathbf{a}$ with exactly i distinct elements that are enumerated in T_{k-1}. Then by arguments very similar to the one outlined earlier, it is straightforward to see that

$$\begin{aligned} \mathbb{E}(N_{k-1}) &\leqslant p^{k-2}\theta^{k-1}, \\ \mathbb{E}(N_i) &\leqslant \mathbb{E}(N_{k-1}) \text{ for all } 2 \leqslant i \leqslant k-1, \end{aligned}$$

so that we have

$$\mathbb{E}(T_{k-1}) \leqslant kp^{k-2}\theta^{k-1} < \frac{k}{\omega'(p)^{k-1}}$$

where the last inequality holds by the hypothesis on θ. Consequently $\mathbb{E}(T_{k-1}) \to 0$ as $p \to \infty$, and so it follows that there exists no $\mathbf{a} \in (A \cup \{0\})^{k-1} \setminus \{\mathbf{0}_{k-1}\}$ for which $\langle \mathbf{1}_{k-1}, \mathbf{a} \rangle = 0$ *whp*. This completes the proof of theorem 6. □

4.2 Proof of theorem 2

1. *Proof.* (of part 1) First by theorem 5 we have $f^{(D)}(p, 2) \geqslant \sqrt{p} - 1$. However, a closer inspection of the same proof for the case $k = 2$ reveals that the corresponding set $\mathcal{X}$ (in the proof of theorem 5) consists of all pairs $(a_1, a_2) \in A^2$ itself, so we actually have a (slightly) better bound, viz., $f^{(D)}(p, 2) \geqslant \sqrt{p-1}$, so $f^{(D)}(p, 2) \geqslant \left\lceil \sqrt{p-1} \right\rceil$.

   Suppose $p = q^2 + q + 1$ and let $D \subset \mathbb{Z}_p^*$ be a perfect difference set of size $q+1$, which is assured by Singer's theorem. Set $A = \{\theta^i : i \in D\}$, where θ is a primitive element of $\mathbb{Z}_p^*$. We claim that $D_A(\mathbb{Z}_p) = 2$, so that this establishes that $f^{(D)}(p, 2) \leqslant \left\lceil \sqrt{p-1} \right\rceil$ and completes the proof.

   In order to show that $D_A(\mathbb{Z}_p) = 2$, it suffices to show that for every $u \in \mathbb{Z}_p^*$, the sequence $(1, u)$ admits a pair $(a_1, a_2) \in A^2$ such that $a_1 + ua_2 = 0$. Write $-u = \theta^{i_u}$ for a unique $i_u \in [1, q^2 + q]$, and since D is a perfect difference set, write $i_u = d_1(u) - d_2(u)$ for a unique pair $(d_1(u), d_2(u))$ in D. Then if we set $a_i = \theta^{d_i(u)}$ then we have $-u = a_1/a_2$, or equivalently, $a_1 + ua_2 = 0$. This completes the proof of the first part. □

2. *Proof.* (of part 2) For $k = 2$, and all primes p, we now prove the more general bound $f^{(D)}(p, 2) \leqslant 2\sqrt{p} - 1$. Again, we ignore the ceiling/floor notation for simplicity. In what follows, if A is a set containing 0 then by A_* we shall mean $A \setminus \{0\}$. If $a, b \in \mathbb{Z}_p$ and $b \neq 0$, then $\frac{a}{b}$ shall denote ab^{-1} where b^{-1} is the unique element of $\mathbb{Z}_p$ satisfying $bb^{-1} = 1$. For sets $A, B \subset \mathbb{Z}_p$ with $0 \notin B$, $\frac{A}{B}$ shall denote the set $\{\frac{a}{b} : a \in A, b \in B\}$.

   Observation 4.2. Suppose $A, B \subset \mathbb{Z}_p^*$ and satisfy $|A| \cdot |B| > p$. Then $\frac{B-B}{(A-A)_*} = \mathbb{Z}_p$.

   To prove the observation, for each $x \in \mathbb{Z}_p^*$, consider the map $\phi_x : A \times B \to \mathbb{Z}_p^*$ given by $\phi_x(a, b) := ax + b$. Then by the assumption that $|A| \cdot |B| > p$ it follows that this map is not injective, so there exist pairs $(a, b) \neq (a', b')$ such that $\phi_x(a, b) = \phi_x(a', b')$. By the definition of ϕ_x, this implies that $a \neq a'$, which then implies that $x = \frac{b'-b}{a-a'} \in \frac{B-B}{(A-A)_*}$, and since x was arbitrary, the proof of the observation is complete.

Let $\ell = \lceil \sqrt{p} \rceil$, and consider the set $A = [-\ell, \ell]_*$. Then note that $A = (B-B)_*$ where $B = [1, \ell]$. Since $|B|^2 > p$, by observation 4.2, we have $\frac{A}{A} = \frac{(B-B)_*}{(B-B)_*} = \mathbb{Z}_p^*$. Consequently, for every $u \in \mathbb{Z}_p^*, -u \in \frac{A}{A}$, and as we have seen above, this implies that $D_A(\mathbb{Z}_p) = 2$. Since $|A| = 2\ell$, the proof is complete. □

3. *Proof.* (of part 3) Before we start with the proof of the 3rd part of this theorem, we shall state a reformulation of what we seek: For any $k \geqslant 1$, to find an upper bound for $f^{(D)}(p, 2k)$, it suffices to construct a set $A \subset \mathbb{Z}_p^*$ of the requisite size such that for any $\alpha_1, \dots, \alpha_{k-1}, \beta_1, \dots, \beta_{k-1} \in \mathbb{Z}_p^*$,

$$\mathbb{Z}_p^* \subseteq \frac{A + \alpha_1 A + \cdots + \alpha_{k-1} A}{A + \beta_1 A + \cdots + \beta_{k-1} A}. \tag{5}$$

To see why, note that $D_A(\mathbb{Z}_p) = 2k$ implies that for any sequence $(x_1, \dots, x_{2k})$ with $x_i \in \mathbb{Z}_p^*$ for all i, we have $0 \in Ax_1 + \cdots + Ax_{2k}$, or equivalently,

$$-\frac{x_1}{x_{k+1}} = \frac{a_{k+1} + a_{k+2}(x_{k+2}/x_{k+1}) + \cdots + a_{2k}(x_{2k}/x_{k+1})}{a_1 + a_2(x_2/x_1) + \cdots + a_k(x_k/x_1)},$$

and if (5) holds, then this is indeed satisfied. So in order to show that $f^{(D)}(p, 4) \leqslant O(p^{1/4})$, it suffices to construct a set $A \subset \mathbb{Z}_p^*$ with $|A| \leqslant C_0 p^{1/4}$ for some constant $C_0 > 0$ such that

$$\mathbb{Z}_p^* \subseteq \frac{A + \alpha A}{A + \beta A} \tag{6}$$

for all $\alpha, \beta \in \mathbb{Z}_p^*$.

Let $L = \lfloor 30 p^{1/4} \rfloor$. For a positive integer t, let

$$X_t := t[-L, L] = \{-Lt, \dots, -t, 0, t, \dots, Lt\}.$$

The following observations regarding X_t are evident:

Observation 4.3. (i). $\alpha X_t = X_{\alpha t}$.

(ii). For $s \neq t$, $X_s + X_t$ contains a subset $Y_{s,t}$ of size at least $|X_s + X_t|/4$ such that $Y_{s,t} - Y_{s,t} \subseteq X_s + X_t$. This follows from the simple fact that this is a *generalized arithmetic progression (GAP)* of rank 2, and this is a general property of GAPs. (see for instance [14], chapter 2. However, this property is easily verified, and does not need any specialized tools).

We shall denote by I, the set $X_1 = [-L, \dots, -1, 0, 1, \dots, L]$, for convenience.

We shall now introduce some further terminology. For integers $\xi, \eta \in [1, p-1]$, we shall regard the sets $[-\xi, \xi] = \{-\xi, -\xi+1, \ldots, -1, 0, 1, \ldots \xi - 1, \xi\}$ and $[1, \eta] = \{1, 2, \ldots, \eta\}$ as subsets of $\mathbb{Z}_p$. Define

$$S(\xi, \eta) := \frac{[-\xi, \xi]_*}{[1, \eta]}.$$

For a given $t \in \mathbb{Z}_p^*$, we say that $\alpha \in \mathbb{Z}_p^*$ *is good for* t if $|(I + \alpha X_t)_*| \geqslant \frac{L^2}{200}$. For $t, s \in [1, (p-1)/2]$, since $|X_s + \alpha X_t| = |I + \alpha X_{(t/s)}|$ it follows that

$$|X_s + \alpha X_t| \geqslant \frac{L^2}{200} \text{ if and only if } \alpha \text{ is good for } (t/s).$$

Lemma 7. Suppose $\alpha \in \mathbb{Z}_p^*$ is not good for t, then $\alpha \in t^{-1} S(2L, \frac{L}{200})$.

Proof. (**of the lemma**): Since $\alpha X_t = X_{\alpha t}$, it will suffice if we show the following: If $|I + X_t| < \frac{L^2}{200}$ then $t \in S(2L, L/200)$.

Set $X_t^+ = \{0, t, \ldots, Lt\}$. Note that $I + X_t^+ = \bigcup_{i=0}^{L} [it - L, it + L]$. Set $\mathcal{X}_0 = [-L, L]$, and recursively define $\mathcal{X}_{i+1} = \mathcal{X}_i \cup [it - L, it + L]$ for $0 \leqslant i \leqslant L - 1$. We say that the set $\mathcal{X}_i$ is *valid* if it is the union of pairwise disjoint intervals each of length $2L$ and centred around an element of X_t^+. Clearly, $\mathcal{X}_0$ is valid. If $\mathcal{X}_i$ is valid for all $i \leqslant L/200$, then in particular, for $M = \lceil L/400 \rceil$, we have $|\mathcal{X}_M| = 2LM \geqslant (2L)\frac{L}{400} \geqslant \frac{L^2}{200}$ contradicting the hypothesis. Hence there is a smallest i such that $\mathcal{X}_i$ is not valid. Since i is the least such index, it follows that the addition of the latest interval $[it - L, it + L]$ non-trivially intersects some other such interval so that there exists $j < i$ with $[it - L, it + L] \cap [jt - L, jt + L] \neq \emptyset$. But this implies that there exist $\xi_1, \xi_2 \in [-L, L]$ such that $it + \xi_1 = jt + \xi_2$, or equivalently, $t = \frac{\xi_2 - \xi_1}{i - j} \in \frac{[-2L, 2L]}{[1, L/200]}$ and that completes the proof of the lemma. □

We now return to complete the proof of the last part of theorem 2. Recall that $L = \lfloor 30 p^{1/4} \rfloor$. We shall now denote by S the set $S(2L, \frac{L}{200})$.

Consider the hypergraph $\mathcal{H} = (V, E)$ whose vertex set $V = \mathbb{Z}_p^*$ and whose edge set consists of all dilates of S, i.e., $E(\mathcal{H}) = \{xS : x \in \mathbb{Z}_p^*\}$.

Claim 1. *If there exist* $x_1, \ldots, x_N \in \mathbb{Z}_p^*$ *such that* $\bigcap_{i=1}^{N} x_i S = \emptyset$ *then the set*

$$A = \left(I \cup \bigcup_{i=1}^{N} X_{x_i^{-1}} \right)_* \subset [1, p-1]$$

satisfies $D_A(\mathbb{Z}_p) \leqslant 4$. *In particular,* $f^{(D)}(p, 4) \leqslant (2L+1)N$.

(*Proof of claim 1*) We shall show that for any $\alpha \in \mathbb{Z}_p^*$, $|I + \alpha X_{x_i^{-1}}| > 4\sqrt{p}$ for some $1 \leqslant i \leqslant N$. Then by observation 4.3, there exists $\tilde{Y_\alpha} \subset I + \alpha X_{x_i^{-1}}$ with $|\tilde{Y_\alpha}| > p^{1/2}$ such that $\tilde{Y_\alpha} - \tilde{Y_\alpha} \subseteq I + X_{x_i^{-1}}$. Since this holds for all $\alpha, \beta \in \mathbb{Z}_p^*$, it follows by observation 4.2 that $\mathbb{Z}_p^* \subseteq \frac{A+\alpha A}{A+\beta A}$ and that completes the proof of claim 1.

Suppose $\alpha \in \mathbb{Z}_p^*$. Since $\displaystyle\bigcap_0^N x_i S = \emptyset$, $\alpha \notin x_i S$ for some i. This in turn (by lemma 7) implies that α is good for x_i^{-1}, or equivalently, $|I+\alpha X_{x_i^{-1}}| \geqslant \frac{L^2}{200} > 4p^{1/2}$ as required.

For $x \in \mathbb{Z}_p^*$, define

$$N(x) = \#\left\{(s_1, s_2) : s_i \in S \text{ satisfying } x = \frac{s_1}{s_2}\right\}$$

and let NORMAL $:= \{x \in \mathbb{Z}_p^* : N(x) \leqslant 650\}$.

Claim 2. *Now suppose $x \in$ NORMAL. Then $|S \cap xS| \leqslant 650$.*

(*Proof of claim 2*) Indeed, if $S \cap xS = \emptyset$ then there is nothing to prove. Let $S \cap xS = \{y_1, \dots, y_k\}$. Then $y_i = xs_i = s_i'$ for some $s_i, s_i' \in S$ where $1 \leqslant i \leqslant k$, and the s_i are all distinct. Hence $x = \frac{s_i'}{s_i}$ for $1 \leqslant i \leqslant k$, which implies that x can be expressed as the ratio of two elements of S in at least k different ways. Since $x \in$ NORMAL, it follows that $k \leqslant 650$ and proves claim 2.

Claim 3. *There exists $N = O(1)$ such that the hypergraph $\mathcal{H}$ is not N-intersecting, i.e., there exist $x_1, \dots, x_N \in \mathbb{Z}_p^*$ such that $\displaystyle\bigcap_{i=1}^N x_i S = \emptyset$.*

(*Proof of claim 3*) Suppose x is chosen uniformly at random from $\mathbb{Z}_p^*$. Then

$$\mathbb{E}(N(x)) = \sum_{(s_1,s_2)\in S^2} \mathbb{P}\left(x = \frac{s_1}{s_2}\right) = \frac{|S|^2}{p-1} < 325$$

whenever $p > 325$. Hence by the Markov Inequality,

$$\mathbb{P}(x \notin \text{NORMAL}) \leqslant \frac{1}{2} \tag{7}$$

for a uniformly randomly chosen $x \in \mathbb{Z}_p^*$. Consequently,

$$|\text{NORMAL}| \geqslant \frac{p-1}{2}. \tag{8}$$

Let $x_1 \in$ NORMAL be an arbitrary element. By the preceding discussion, $|S \cap x_1 S| \leqslant 650$. Write $S \cap x_1 S = \{a_1, \dots, a_k\}$ for some $k \leqslant 650$. Now inductively, having picked $x_1, \dots, x_{i-1} \in \mathrm{NORMAL}$ pick $x_i \in \mathrm{NORMAL} \setminus \{x_1, \dots, x_{i-1}\}$ such that $a_{i-1} \notin x_i S$ (so we pick at most $k+1 \leqslant 651$ such x_i). Since $|S| \leqslant 18\sqrt{p}$ the number of forbidden choices (at each step of this process) is at most $|S| + k \leqslant 18\sqrt{p} + 651 \lll \frac{p-1}{2} \leqslant |\mathrm{NORMAL}|$ (by (8)) for sufficiently large p, so there is always a valid choice for x_i.

Now observe that $S \bigcap x_1 S \bigcap \cdots \bigcap x_{k+1} S = \emptyset$ since any element x in the intersection must be a_i for some i, but by the choices of the x_i, we have $a_i \notin x_{i+1} S$, and that is a contradiction. In summary, we may take $N = 651$ in the statement of claim 3. This completes the proof of claim 3, and hence also the proof of part 3 of theorem 2 with $C_0 = 40000$, for instance, when p is sufficiently large. □

Remark: We have not made any attempts to determine an optimal value for the constant C_0 in the proof of the last part of the theorem above. We believe that in reality $f^{(D)}(p, 4) \leqslant (1+\varepsilon))p^{1/4}$ (for all $\varepsilon > 0$; please see the first remark in the next section) and it doesn't seem possible to be able to prove this by optimizing for C_0 along these lines.

5 Concluding Remarks

- As we have stated earlier, we believe that $f^{(D)}(p, k) = \Theta(p^{1/k})$ for all sufficiently large p. But in fact, we are also inclined to believe that in fact $f^{(D)}(p, k) \leqslant (1 + o(1))p^{1/k}$ though we can prove neither statement now.

- The best upper bound for $f^{(D)}(p, 2)$ that one could prove (for all prime p) is $(2/\sqrt{3})\sqrt{p} = 1.154\ldots\sqrt{p}$. This needs some recent results on the existence of small differences bases for $[1, n]$, (see [8]), which again crucially rely on Singer's theorem on the existence of perfect difference sets in $\mathbb{Z}_n$ for $n = q^2 + q + 1$.

- One may frame the problem of obtaining an upper bound for $f^{(D)}(p, 2k-1)$ (in an analogous manner to that in the proof of theorem 2) by constructing a set A such that for any $\alpha_1 \dots, \alpha_k, \beta_1, \dots, \beta_{k-1} \in \mathbb{Z}_p^*$ such that

$$\mathbb{Z}_p^* \subseteq \frac{A + \alpha_1 A + \cdots + \alpha_k A}{A + \beta_1 A + \cdots + \beta_{k-1} A}.$$

  So, for instance, to prove that $f^{(D)}(p, 3) \leqslant O(p^{1/3})$ amounts to constructing a set of the appropriate size such that $\mathbb{Z}_p^* \subseteq \frac{A + \alpha A}{A}$. But this asymmetry in the framing makes the problem of $f^{(D)}(p, 2k)$ easier to approach in this manner.

- One very natural counterpart to the problem that is the focus of this paper is the corresponding dual problem: For a given finite group G, determine

$$\max\{D_A(G) : |A| = k, A \subseteq [1, \exp(G) - 1]\}.$$

  For instance, it is known that $D_A(\mathbb{Z}_p) = \lceil p/k \rceil$ if $A = \{1, \dots, k\}$ for $1 \leqslant k \leqslant p-1$ (see [4], [5]), so this corresponding maximum is at least $\lceil p/k \rceil$. It turns out, that for

p prime, one can show that this maximum is at most $\lceil p/k \rceil$ as follows (this result also appears in [1], with a different proof):

Suppose A is a set of size k. We shall show that for any sequence $\mathbf{x}$ of length $\lceil p/k \rceil$, there exist $\mathbf{a} \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ such that $\langle \mathbf{x}, \mathbf{a} \rangle = 0$. Write $p = (m-1)k + r$ for $0 < r < k$, so that $m = \lceil p/k \rceil$. Let $\mathcal{X} := (x_1 \dots x_m)$ be a sequence of non-zero elements of $\mathbb{Z}_p$, and let $S = A \cup \{0\}$. Consider the polynomial $g(X_1, \cdots, X_m) = ((\sum_{i=1}^m x_i X_i)^{p-1} - 1)\, X_1^{k+1-r}$. The coefficient of $\prod_{i=1}^m X_i^k$ in g equals $\binom{p-1}{r-1, k, \cdots, k} x_1^{r-1} \prod_{i=2}^m x_i^k \neq 0$, since $x_i \neq 0$, so by the Combinatorial Nullstellensatz (see [6]) it follows that there is a choice of $a_i \in S$ for each $1 \leqslant i \leqslant m$ with $a_1 \neq 0$ (since $k+1-r > 0$) such that $\sum_i a_i x_i = 0$. In fact this proof also works even when we assign arbitrary lists S_i of size $\lceil p/k \rceil$ for each non-zero element of $\mathbb{Z}_p$ and we are only allowed to pick coefficients from the corresponding list of each element, so that a corresponding list-weighted version of the Davenport constant also admits the same upper bound.

The same ideas can be extended to show that if $n = p_1 \cdots p_r$ is square-free, and A is a subset of $[1, n-1]$ of size k such that the set $A \pmod{p_i} := \{a \pmod{p_i} : a \in A\}$ also has size k, then any sequence $(x_1 \dots, x_m)$ in $\mathbb{Z}_n$ with $m \geqslant \frac{\lceil p_i/k \rceil n}{p_i}$ admits an A-weighted zero-sum subsequence. Indeed, suppose $A_i := A \pmod{p_i}$ has size k. Since n is square-free, $\mathbb{Z}_n \cong \mathbb{Z}_{p_i} \times \mathbb{Z}_{n/p_i}$. Write $p_i = k\lambda_i + r_i$, for some λ_i, r_i where $0 \leqslant r_i < k$, so that $\lceil p_i/k \rceil = \lambda_i + 1$. Let $\mathcal{X} = (x_1, \dots, x_{m_i})$ be a sequence of elements in $\mathbb{Z}_n$, where $m_i = \frac{n \lceil p_i/k \rceil}{p_i}$. Write $x_j = (y_j, z_j) \in \mathbb{Z}_{p_i} \times \mathbb{Z}_{n/p_i}$ for each $j = 1, \dots, m_i$; similarly, write $a = (a', a'')$ where $a' \in \mathbb{Z}_{p_i}$ and $a'' \in \mathbb{Z}_{n/p_i}$. Regroup the sequence $\mathcal{X}$ into n/p_i segments of length $\lceil p_i/k \rceil$ each. It follows that for each $1 \leqslant j \leqslant n/p_i$ and $1 \leqslant \ell \leqslant \lceil p_i/k \rceil$, there exist $a'_{\ell,j} \in A_i \cup \{0\}$, not all zero, such that

$$\sum_{\ell=(j-1)\lceil p_i/k \rceil + 1}^{j \lceil p_i/k \rceil} a'_{\ell,j} y_\ell = 0$$

in $\mathbb{Z}_{p_i}$. Writing $t = \lceil p_i/k \rceil$ for convenience, we note that in particular, we have the sequence (from our regrouping)

$$\mathcal{Y} = \left(\left(0, \sum_{\ell=1}^{t} a''_{\ell,1} z_\ell \right), \left(0, \sum_{\ell=t+1}^{2t} a''_{\ell,2} z_\ell \right), \dots, \left(0, \sum_{j=(n/p_i-1)t+1}^{nt/p_i} a''_{\ell,(n/p_i-1)} z_\ell \right) \right)$$

in $\mathbb{Z}_{p_i} \times \mathbb{Z}_{n/p_i}$ of length n/p_i. Note that the first coordinates are all zero by our choices of $a \in A_i \cup \{0\}$. But since $D(\mathbb{Z}_m) = m$, every sequence of length n/p_i in $\mathbb{Z}_{n/p_i}$ admits a non-trivial zero-sum subsequence, so we are through. An immediate consequence of this is the following:

For $N := \max \left\{ \left\lceil \frac{p_i}{\sqrt{k}} \right\rceil \frac{n}{p_i} : 1 \leqslant i \leqslant r \right\}$, any set $A \subset [1, n-1]$ of size k, and any $\mathbb{Z}_n$-sequence $\mathbf{x} = (x_1, \dots, x_N)$ of length N, there exists $\mathbf{a} \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ such that $\langle \mathbf{x}, \mathbf{a} \rangle = 0$, so in particular,

$$\max\{D_A(\mathbb{Z}_n) : |A| = k\} \leqslant \max\left\{ \left\lceil \frac{p_i}{\sqrt{k}} \right\rceil \frac{n}{p_i} : 1 \leqslant i \leqslant r \right\}.$$

Acknowledgements

The second author's research was supported by NSFC with grant no. 11681217. Authors would like to thank referees for their valuable comments.

References

[1] S. D. Adhikari, R. Balasubramanian, F. Pappalardi, and P. Rath, Some zero-sum constants with weights, *Proc. Indian Acad. Sci. Math. Sci.* **118**(2008), no. 2, 183-188.

[2] S. D. Adhikari, and Y. G. Chen, Davenport constant with weights and some related question II, *J. Combin. Theory Ser. A* **115**(2008), No. 1, 178-184.

[3] S. D. Adhikari, Y. G. Chen, J. B. Friedlander, S. V. Konyagin, and F. Pappalardi, Contributions to zero-sum problems. *Discrete Math.* **306** (2006), no. 1, 1-10.

[4] S. D. Adhikari, C. David, and J. Urroz, Generalizations of some zero-sum theorems, *Integers*, **8**(2008), Article A52.

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

[6] N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.* **8**(1999), 7-29.

[7] N. Alon, and J. Spencer, *The Probabilistic Method*, Wiley Series in Discrete Mathematics and Optimization, 4th edition, 2016.

[8] T. Banakh, and V. Gavrylkiv, Difference bases in cyclic groups, arXiv:1702.02631.

[9] T. Beth, D. Jungnickel, H. Lenz, *Design Theory, Volume 1*, Second ed., Cambridge University Press, 1999.

[10] S. Griffiths, The Erdős-Ginzburg-Ziv Theorem with units. *Discrete Math.* **308** (2008), no. 23, 5473-5484.

[11] F. Halter-Koch, Arithmetical interpretation of weighted Davenport constants, *Arch. Math.* **103** (2014), 125-131.

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

[13] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43**(1938), 377-385.

[14] T. Tao, and V. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.