Zero sum problems in abelian groups and related extremal problems

Niranjan Balachandran

Mathematics Department,
Indian Institute of Technology Bombay (IITB)

A meeting on operator theory, topology and combinatorics: Celebrating Bhaskar Bagchi's career at ISI Bangalore.

(Based on joint work with Eshita Mazumdar and Kevin Zhao)

January 29, 2019

Bhaskar Bagchi

Bhaskar Bagchi, COO, IndiaHomes ...
indiahomesblog.wordpress.com


Bhaskar Bagchi - Homepage
cse.iitkgp.ac.in


Bhaskar Bagchi - Quora
quora.com


Bhaskar Bagchi | Indian Insti...
researchgate.net


Subodh Sarkar With Bhaskar Bagchi ...
youtube.com


PropTiger sacks 200 to integrate ...
livemint.com


Top 10 Bhaskar Bagchi profil...
in.linkedin.com


Top 10 Bhaskar Bagchi profil...
in.linkedin.com

BOLO JUNGALMAHAL BHASKAR BAGCHI WIT...
youtube.com


BHASKAR DASGUPTA WITH BHAS...
youtube.com


DR. SANATAN DUTTA WITH BHAS...
youtube.com


PRABIR SARKAR WITH BHASKAR ...
youtube.com


SANAT NIYAGI WITH BHASKAR B...
youtube.com

SAIKAT RAKSHIT WITH BHASKAR BAGCHI ...
youtube.com


bhaskar bagchi (@RocksB...
twitter.com


APARAJITA HAJRA WITH BHASKAR ...
youtube.com


bhaskar bagchi (@RocksBhaskar) | Twitter
twitter.com


BISWADEEP SARKAR WITH BHASKAR ...
youtube.com

Dynamic Linkages and Vol...
kobo.com

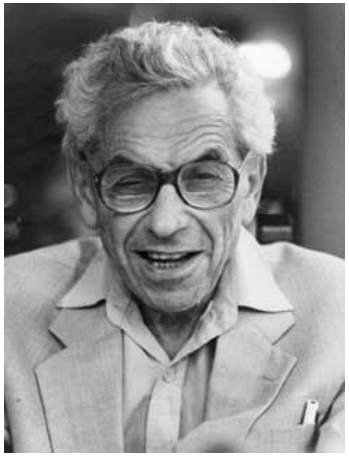

Bhaskar Bagchi - Country Man...
linkedin.com


BHASKAR BAGCHI - Google+
plus.google.com


MAHADEB DEY WITH BHASKAR BAGC...
youtube.com

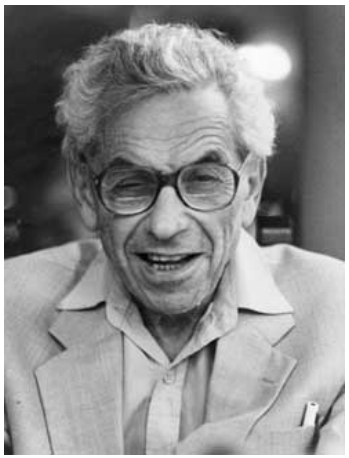
Bhaskar Bagchi, ISI Bangalore

An Erdős problem for 'Epsilons'



Given a sequence of n integers $(a_1, \ldots, a_n)$ there exists a nontrivial subsequence of these integers whose sum equals zero modulo n.

An Erdős problem for 'Epsilons'



Given a sequence of n integers $(a_1, \ldots, a_n)$ there exists a nontrivial subsequence of these integers whose sum equals zero modulo n.

This is tight: $\underbrace{(1, \ldots, 1)}_{n-1 \text{ times}}$ does not have a nontrivial zero sum subsequence.

Zero sum problems in finite abelian groups

Suppose $G = G(+, 0)$ is a finite abelian group.

Zero sum problems in finite abelian groups

Suppose $G = G(+, 0)$ is a finite abelian group.

- G-sequence of length m: $(x_1, \ldots, x_m)$ with $x_i \in G$ for each i.

Zero sum problems in finite abelian groups

Suppose $G = G(+, 0)$ is a finite abelian group.

- G-sequence of length m: $(x_1, \ldots, x_m)$ with $x_i \in G$ for each i.
- *Zero-sum* G-sequence: G-sequence $(x_1, \ldots, x_m)$ such that $\sum_i x_i = 0$.

Zero sum problems in finite abelian groups

Suppose $G = G(+, 0)$ is a finite abelian group.

- G-sequence of length m: $(x_1, \ldots, x_m)$ with $x_i \in G$ for each i.
- *Zero-sum* G-sequence: G-sequence $(x_1, \ldots, x_m)$ such that $\sum_i x_i = 0$.

Definition

The Davenport constant $D(G)$ of the group G is the smallest m such that every G-sequence of length m contains a non-trivial zero-sum G-subsequence.

Zero sum problems in finite abelian groups

Suppose $G = G(+, 0)$ is a finite abelian group.

- G-sequence of length m: $(x_1, \ldots, x_m)$ with $x_i \in G$ for each i.
- *Zero-sum* G-sequence: G-sequence $(x_1, \ldots, x_m)$ such that $\sum_i x_i = 0$.

Definition

The Davenport constant $D(G)$ of the group G is the smallest m such that every G-sequence of length m contains a non-trivial zero-sum G-subsequence.

The Erdős problem $\Leftrightarrow D(\mathbb{Z}_n) = n$.

The Davenport constant in Algebraic Number theory

The Davenport constant is an important invariant of the ideal class group:

If R is the ring of integers of an algebraic number field and G its ideal class group, then $D(G)$ is the max no. of prime ideals occurring in the prime ideal decomposition of an irreducible in R.

Other (Combinatorial) Invariants:

- Erdős-Ginzburg-Ziv constant (EGZ), $\mathfrak{s}(G)$: $\min m \in \mathbb{N}$ such that every sequence of elements from G of length m contains a zero-sum subsequence of length $\exp(G)$.

Other (Combinatorial) Invariants:

- Erdős-Ginzburg-Ziv constant (EGZ), $\mathfrak{s}(G)$: $\min m \in \mathbb{N}$ such that every sequence of elements from G of length m contains a zero-sum subsequence of length $\exp(G)$.

- Harborth constant, $\mathrm{g}(G)$: $\min\ m$ such that every *subset* of size m of G admits a zero-sum subsequence of size $\exp(G)$.

A Weighted Davenport constant

Notation: Suppose $\mathbf{x} = (x_1, \ldots, x_m)$ is a G-sequence and $\mathbf{a} = (a_1, \ldots, a_m)$ is a sequence of integers. Let $\mathbf{0}_m = \underbrace{(0, \ldots, 0)}_{m \text{ times}} \in \mathbb{Z}^m$.

$$\langle \mathbf{a}, \mathbf{x} \rangle := \sum_i a_i x_i.$$

Here $nx := \underbrace{x + \cdots + x}_{n \text{ times}}$ if $n > 0$, and for n negative, $nx := (-n)(-x)$.

A Weighted Davenport constant

Notation: Suppose $\mathbf{x} = (x_1, \ldots, x_m)$ is a G-sequence and $\mathbf{a} = (a_1, \ldots, a_m)$ is a sequence of integers. Let $\mathbf{0}_m = \underbrace{(0, \ldots, 0)}_{m \text{ times}} \in \mathbb{Z}^m$.

$$\langle \mathbf{a}, \mathbf{x} \rangle := \sum_i a_i x_i.$$

Here $nx := \underbrace{x + \cdots + x}_{n \text{ times}}$ if $n > 0$, and for n negative, $nx := (-n)(-x)$.

An equivalent description of the Davenport constant: Least m such that for every G-sequence $\mathbf{x} = (x_1, \ldots, x_m)$, there exists $\mathbf{e} = (\varepsilon_1, \ldots, \varepsilon_m) \in \{0, 1\}^m$ with $\mathbf{e} \neq \mathbf{0}_m$ (nontrivial $\mathbf{e}$) such that

$$\langle \mathbf{e}, \mathbf{x} \rangle = 0.$$

A Weighted Davenport constant - contd.

Theorem

(Adhikari, et al, 2006) Let $m = \lfloor \log_2 n \rfloor + 1$. *Then every* $\mathbb{Z}_n$*-sequence* $\mathbf{x} = (x_1, \ldots, x_m)$ *admits a nontrivial* $\mathbf{e} = (\varepsilon_1, \ldots, \varepsilon_m)$ *with* $\varepsilon_i \in \{-1, 0, 1\}$ *such that*

$$\langle \mathbf{e}, \mathbf{x} \rangle = 0.$$

A Weighted Davenport constant - contd.

Theorem

(Adhikari, et al, 2006) Let $m = \lfloor \log_2 n \rfloor + 1$. *Then every* $\mathbb{Z}_n$*-sequence* $\mathbf{x} = (x_1, \ldots, x_m)$ *admits a nontrivial* $\mathbf{e} = (\varepsilon_1, \ldots, \varepsilon_m)$ *with* $\varepsilon_i \in \{-1, 0, 1\}$ *such that*

$$\langle \mathbf{e}, \mathbf{x} \rangle = 0.$$

This is also tight: Consider $\mathbf{x} = (1, 2, 2^2, \ldots, 2^{r-1})$ where $2^r \leq n < 2^{r+1}$.

A Weighted Davenport constant - contd.

Theorem

(Adhikari, et al, 2006) Let $m = \lfloor \log_2 n \rfloor + 1$. *Then every* $\mathbb{Z}_n$*-sequence* $\mathbf{x} = (x_1, \ldots, x_m)$ *admits a nontrivial* $\mathbf{e} = (\varepsilon_1, \ldots, \varepsilon_m)$ *with* $\varepsilon_i \in \{-1, 0, 1\}$ *such that*

$$\langle \mathbf{e}, \mathbf{x} \rangle = 0.$$

This is also tight: Consider $\mathbf{x} = (1, 2, 2^2, \ldots, 2^{r-1})$ where $2^r \leq n < 2^{r+1}$.

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

Weighted Davenport constant w.r.t weight set A

Suppose $A \subset \mathbb{N}$ be a non-empty subset of the integers.

Weighted Davenport constant w.r.t weight set A

Suppose $A \subset \mathbb{N}$ be a non-empty subset of the integers.

Definition

Suppose G is an abelian group. The Weighted Davenport constant of G w.r.t A, denoted $D_A(G)$, is the least k such that:

For any G-sequence $(x_1, \ldots, x_k)$, there exists a nontrivial $\mathbf{a} \in (A \cup \{0\})^k$ such that

$$\langle \mathbf{a}, \mathbf{x} \rangle = 0.$$

Weighted Davenport constant w.r.t weight set A

Suppose $A \subset \mathbb{N}$ be a non-empty subset of the integers.

Definition

Suppose G is an abelian group. The Weighted Davenport constant of G w.r.t A, denoted $D_A(G)$, is the least k such that:

For any G-sequence $(x_1, \ldots, x_k)$, there exists a nontrivial $\mathbf{a} \in (A \cup \{0\})^k$ such that

$$\langle \mathbf{a}, \mathbf{x} \rangle = 0.$$

We may always assume $A \subset [1, n-1]$ where $n = \exp(G)$.

Weighted Davenport constant $D_A(G)$

An interpretation of this for $G = \mathbb{F}_p^n$:

Weighted Davenport constant $D_A(G)$

An interpretation of this for $G = \mathbb{F}_p^n$:

If $A = [1, p-1]$, then this is precisely the dimension n.

For arbitrary $A \subset [1, p-1]$, $D_A(G)$ measures how large a sequence of vectors in $\mathbb{F}_p^n$ can be, if the sense of 'independence' restricts the coefficients of the vectors to A.

Some known results

- $D_{\pm}(\mathbb{Z}_n) = \lfloor \log_2 n \rfloor + 1$. (Adhikari *et al*, 2006)
- $D_A(\mathbb{Z}_n) = 2$ for $A = \mathbb{Z}_n \setminus \{0\}$. (Adhikari *et al*, 2006)
- $D_A(\mathbb{Z}_n) = a + 1$ for $A = \mathbb{Z}_n^*$ where $a = \sum_{i=1}^{k} a_i$ and $n = p_1^{a_1} \cdots p_k^{a_k}$. (Griffiths, 2008)
- $D_A(\mathbb{Z}_n) = \lceil \frac{n}{r} \rceil$ if $A = \{1, \ldots, r\}$ for $1 \leq r \leq n-1$. (Adhikari, David, Urroz, 2006; Adhikari, Rath, 2008)

A related extremal problem

Suppose G is a finite abelian group with $\exp(G) = n$, and suppose $k \geq 2$ is an integer.

Definition

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

Notation: If $G = \mathbb{Z}_n$, then denote $f_G^{(D)}(k)$ by $f^{(D)}(n, k)$.

A related extremal problem

Suppose G is a finite abelian group with $\exp(G) = n$, and suppose $k \geq 2$ is an integer.

Definition

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

Notation: If $G = \mathbb{Z}_n$, then denote $f_G^{(D)}(k)$ by $f^{(D)}(n, k)$.

Natural extremal problem: Given a finite abelian group G, and $k \geq 2$,

$$\text{Determine } f_G^{(D)}(k).$$

The function $f_G^{(D)}(k)$

Proposition

If $G = \mathbb{Z}_p \times H$ is a finite abelian group with $p \nmid |H|$, then for any integer k, $f_G^{(D)}(n,k) \leq f^{(D)}(p,k)$. More generally, if $G = H_1 \times \cdots \times H_r$ where H_i is a p_i-group with $p_1 < \cdots < p_r$, then for all k,

$$f_G^{(D)}(k) \leq \min\left\{ f_{H_i}^{(D)}(k) : 1 \leq i \leq r \right\}.$$

The function $f_G^{(D)}(k)$

Proposition

If $G = \mathbb{Z}_p \times H$ is a finite abelian group with $p \nmid |H|$, then for any integer k, $f_G^{(D)}(n,k) \leq f^{(D)}(p,k)$. More generally, if $G = H_1 \times \cdots \times H_r$ where H_i is a p_i-group with $p_1 < \cdots < p_r$, then for all k,

$$f_G^{(D)}(k) \leq \min\left\{ f_{H_i}^{(D)}(k) : 1 \leq i \leq r \right\}.$$

Proposition

Let $k \geq 2$. Suppose G and H are finite abelian groups with $H = G \times G'$ and $\exp(G) = \exp(H)$. Then $f_G^{(D)}(k) \leq f_H^{(D)}(k)$.

The function $f_G^{(D)}(k)$

Proposition

If $G = \mathbb{Z}_p \times H$ is a finite abelian group with $p \nmid |H|$, then for any integer k, $f_G^{(D)}(n,k) \leq f^{(D)}(p,k)$. More generally, if $G = H_1 \times \cdots \times H_r$ where H_i is a p_i-group with $p_1 < \cdots < p_r$, then for all k,

$$f_G^{(D)}(k) \leq \min\left\{ f_{H_i}^{(D)}(k) : 1 \leq i \leq r \right\}.$$

Proposition

Let $k \geq 2$. Suppose G and H are finite abelian groups with $H = G \times G'$ and $\exp(G) = \exp(H)$. Then $f_G^{(D)}(k) \leq f_H^{(D)}(k)$.

If $G_n = (\mathbb{Z}_p)^n$, $f_n := f_G^{(D)}(k)$, then $f_1 \leq f_2 \leq \cdots$

Theorem

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

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

Thus for all k,

$$f^{(D)}(p, k) = f_{\mathbb{Z}_{p^2}}^{(D)}(k) = f_{\mathbb{Z}_{p^3}}^{(D)}(k) = \cdots$$

Concrete Upper bounds for $f_G^{(D)}(k)$

Theorem

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

$$1 + \sum_{i=1}^{s} \left\lceil \log_{r+1} n_i \right\rceil \geq D_A(G) \geq 1 + \sum_{i=1}^{s} \left\lfloor \log_{r+1} n_i \right\rfloor \text{ for } s \geq 2$$

$$D_A(\mathbb{Z}_n) = \left\lfloor \log_{r+1} n \right\rfloor + 1.$$

Concrete Upper bounds for $f_G^{(D)}(k)$

Theorem

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

$$1 + \sum_{i=1}^{s} \left\lceil \log_{r+1} n_i \right\rceil \geq D_A(G) \quad \geq \quad 1 + \sum_{i=1}^{s} \left\lfloor \log_{r+1} n_i \right\rfloor \text{ for } s \geq 2$$

$$D_A(\mathbb{Z}_n) \quad = \quad \left\lfloor \log_{r+1} n \right\rfloor + 1.$$

Consequently, $p^{1/k} - 1 \leq f^{(D)}(p,k)$

Concrete Upper bounds for $f_G^{(D)}(k)$

Theorem

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

$$1 + \sum_{i=1}^{s} \left\lceil \log_{r+1} n_i \right\rceil \geq D_A(G) \quad \geq \quad 1 + \sum_{i=1}^{s} \left\lfloor \log_{r+1} n_i \right\rfloor \text{ for } s \geq 2$$

$$D_A(\mathbb{Z}_n) \quad = \quad \left\lfloor \log_{r+1} n \right\rfloor + 1.$$

Consequently, $p^{1/k} - 1 \leq f^{(D)}(p,k) \leq 2(p^{1/(k-1)} - 1)$.

Almost tight upper bound for $f^{(D)}(p,k)$

Theorem

Let $k \geq 2$. There exists an integer $p_0(k)$ and an absolute constant $C = C(k) > 0$ such that for all prime $p > p_0(k)$

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

Almost tight upper bound for $f^{(D)}(p,k)$

Theorem

Let $k \geq 2$. There exists an integer $p_0(k)$ and an absolute constant $C = C(k) > 0$ such that for all prime $p > p_0(k)$

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

So we have

$$p^{1/k} - 1 \leq f^{(D)}(p,k) \leq C(p \log p)^{1/k} \text{ for all sufficiently large } p.$$

A better upper bound for $k = 2$ and $k = 4$

Theorem

Let p be an odd prime.

A better upper bound for $k = 2$ and $k = 4$

Theorem

Let p be an odd prime.

- $f^{(D)}(p, 2) \leq 2\sqrt{p} - 1$. *Our general bound gives* $O(\sqrt{p \log p})$.

A better upper bound for $k = 2$ and $k = 4$

Theorem

Let p be an odd prime.

- $f^{(D)}(p, 2) \leq 2\sqrt{p} - 1$. *Our general bound gives* $O(\sqrt{p \log p})$.

- *If* $p = q^2 + q + 1$ *for some prime* q *then*

$$f^{(D)}(p, 2) = \lceil \sqrt{p - 1} \rceil.$$

A better upper bound for $k = 2$ and $k = 4$

Theorem

Let p be an odd prime.

- $f^{(D)}(p, 2) \leq 2\sqrt{p} - 1$. *Our general bound gives* $O(\sqrt{p \log p})$.
- *If* $p = q^2 + q + 1$ *for some prime* q *then*

$$f^{(D)}(p, 2) = \lceil \sqrt{p - 1} \rceil.$$

- *There exists an absolute constant* $C > 0$ *such that*

$$f^{(D)}(p, 4) \leq C p^{1/4}.$$

Something about the proofs

$f^{(D)}(p,k) \geq p^{1/k} - 1$:

Consider $\mathcal{G} = (V, E)$ with $V = \mathcal{X} \cup \mathcal{Y}$, where $\mathcal{X} = \{\mathbf{a} \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ and $\mathcal{Y} = \{\mathbf{x} : x_i \neq 0, x_i \in \mathbb{Z}_p\}$ and $\mathbf{a} \leftrightarrow \mathbf{x}$ in $\mathcal{G}$ if and only if $\langle \mathbf{a}, \mathbf{x} \rangle = 0$. Let A be an optimal sized set.

Something about the proofs

$f^{(D)}(p,k) \geq p^{1/k} - 1$:

Consider $\mathcal{G} = (V, E)$ with $V = \mathcal{X} \cup \mathcal{Y}$, where $\mathcal{X} = \{\mathbf{a} \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ and $\mathcal{Y} = \{\mathbf{x} : x_i \neq 0, x_i \in \mathbb{Z}_p\}$ and $\mathbf{a} \leftrightarrow \mathbf{x}$ in $\mathcal{G}$ if and only if $\langle \mathbf{a}, \mathbf{x} \rangle = 0$. Let A be an optimal sized set.

By the hypothesis on A: Every $\mathbf{x} \in \mathcal{Y}$ has degree at least one in $\mathcal{G}$. So $e(\mathcal{G}) \geq (p-1)^k$.

Something about the proofs

$f^{(D)}(p,k) \geq p^{1/k} - 1$:

Consider $\mathcal{G} = (V, E)$ with $V = \mathcal{X} \cup \mathcal{Y}$, where $\mathcal{X} = \{\mathbf{a} \in (A \cup \{0\})^k \setminus \{\mathbf{0}_k\}$ and $\mathcal{Y} = \{\mathbf{x} : x_i \neq 0, x_i \in \mathbb{Z}_p\}$ and $\mathbf{a} \leftrightarrow \mathbf{x}$ in $\mathcal{G}$ if and only if $\langle \mathbf{a}, \mathbf{x} \rangle = 0$. Let A be an optimal sized set.

By the hypothesis on A: Every $\mathbf{x} \in \mathcal{Y}$ has degree at least one in $\mathcal{G}$. So $e(\mathcal{G}) \geq (p-1)^k$.

Fix $\mathbf{a} \in \mathcal{X}$, and wlog let $a_1 \neq 0$. For any $x_2, \ldots, x_k \in \mathbb{Z}_p^*$, 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 $\mathbf{a} \in \mathcal{X}$ has degree at most $(p-1)^{k-1}$. Hence $|\mathcal{X}|(p-1)^{k-1} \geq |E| \geq (p-1)^k$. Now use

$$|\mathcal{X}| = (|A| + 1)^k - 1.$$

About the proofs

$f^{(D)}(p,k) \leq O((p \log p)^{1/k})$:

Theorem

Suppose $p \gg 0$ 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 $p \to \infty$.

About the proofs

$f^{(D)}(p,k) \leq O((p \log p)^{1/k})$:

Theorem

Suppose $p \gg 0$ 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 $p \to \infty$.

1. *If $\theta > \sqrt{\frac{2 \log p + \omega(p)}{p}}$, then whp $D_A(\mathbb{Z}_p) = 2$.*
2. *If $k \geq 3$ 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 $D_A(\mathbb{Z}_p) = k$.

About the proofs

$f^{(D)}(p,k) \leq O((p \log p)^{1/k})$:

Theorem

Suppose $p \gg 0$ 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 $p \to \infty$.

1. *If $\theta > \sqrt{\frac{2 \log p + \omega(p)}{p}}$, then whp $D_A(\mathbb{Z}_p) = 2$.*
2. *If $k \geq 3$ 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 $D_A(\mathbb{Z}_p) = k$.

Janson's Inequality.

About the proofs: Why is the upper bound harder?

For sets $A, B \in \mathbb{Z}_p$ with $0 \notin B$, $\frac{A}{B} := \{\frac{a}{b} : a \in A, b \in B\}$.

About the proofs: Why is the upper bound harder?

For sets $A, B \in \mathbb{Z}_p$ with $0 \notin B$, $\frac{A}{B} := \{\frac{a}{b} : a \in A, b \in B\}$.

To prove a good upper bound for $f^{(D)}(p, 2)$, we need a 'small' $A \subseteq \mathbb{Z}_p^*$ such that $\frac{A}{A} = \mathbb{Z}_p^*$. Here $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

About the proofs: Why is the upper bound harder?

For sets $A, B \in \mathbb{Z}_p$ with $0 \notin B$, $\frac{A}{B} := \{\frac{a}{b} : a \in A, b \in B\}$.

To prove a good upper bound for $f^{(D)}(p, 2)$, we need a 'small' $A \subseteq \mathbb{Z}_p^*$ such that $\frac{A}{A} = \mathbb{Z}_p^*$. Here $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

A **Difference Base** in a finite abelian group G is a set $B \subseteq G \setminus 0$ such that for every $g \neq 0$, $g = b - b'$ for some $b, b' \in B$. An upper bound for $f^{(D)}(p, 2)$ comes from a 'small' difference base for $\mathbb{Z}_p$.

About the proofs: Why is the upper bound harder?

For sets $A, B \in \mathbb{Z}_p$ with $0 \notin B$, $\frac{A}{B} := \{\frac{a}{b} : a \in A, b \in B\}$.

To prove a good upper bound for $f^{(D)}(p, 2)$, we need a 'small' $A \subseteq \mathbb{Z}_p^*$ such that $\frac{A}{A} = \mathbb{Z}_p^*$. Here $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

A **Difference Base** in a finite abelian group G is a set $B \subseteq G \setminus 0$ such that for every $g \neq 0$, $g = b - b'$ for some $b, b' \in B$. An upper bound for $f^{(D)}(p, 2)$ comes from a 'small' difference base for $\mathbb{Z}_p$.

A difference base D is said to be **Perfect** if for every $g \neq 0$, there exists a unique pair $(b, b') \in D \times D$ s.t. $g = b - b'$.

Upper bound for $f^{(D)}(p, 2)$

Singer's theorem: There exists a Perfect Difference Set for $\mathbb{Z}_{p^2+p+1}$ of order $p+1$ for p prime.

Upper bound for $f^{(D)}(p, 2)$

Singer's theorem: There exists a Perfect Difference Set for $\mathbb{Z}_{p^2+p+1}$ of order $p+1$ for p prime.

The best known upper bound for a size of a difference base in $\mathbb{Z}_n$ is $\frac{2}{\sqrt{3}}\sqrt{n} \leq 1.15471\sqrt{n}$ for $n \gg 0$. (Banakh-Gavrylkiv, 2017)

Upper bound for $f^{(D)}(p, 2k)$

For $A, B \subseteq \mathbb{Z}_p$, and $\alpha \in \mathbb{Z}_p^*$, $\alpha A := \{\alpha a : a \in A\}$, and $A + B := \{a + b : a \in A, b \in B\}$.

Upper bound for $f^{(D)}(p, 2k)$

For $A, B \subseteq \mathbb{Z}_p$, and $\alpha \in \mathbb{Z}_p^*$, $\alpha A := \{\alpha a : a \in A\}$, and $A + B := \{a + b : a \in A, b \in B\}$.

Towards an optimal upper bound for $f^{(D)}(p, 2k)$: A set $A \subseteq \mathbb{Z}_p^*$ of 'optimal' size such that for any $\alpha_1, \ldots, \alpha_{k-1}, \beta_1, \ldots, \beta_{k-1} \in \mathbb{Z}_p^*$,

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

Upper bound for $f^{(D)}(p, 2k)$

For $A, B \subseteq \mathbb{Z}_p$, and $\alpha \in \mathbb{Z}_p^*$, $\alpha A := \{\alpha a : a \in A\}$, and $A + B := \{a + b : a \in A, b \in B\}$.

Towards an optimal upper bound for $f^{(D)}(p, 2k)$: A set $A \subseteq \mathbb{Z}_p^*$ of 'optimal' size such that for any $\alpha_1, \ldots, \alpha_{k-1}, \beta_1, \ldots, \beta_{k-1} \in \mathbb{Z}_p^*$,

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

Theorem

There exists a set $A \subseteq \mathbb{Z}_p^*$ with $|A| \leq Cp^{1/4}$ for some absolute constant $C > 0$ s.t. for all $\alpha, \beta \in \mathbb{Z}_p^*$

$$\mathbb{Z}_p^* \subseteq \frac{A + \alpha A}{(A + \beta A)^*}.$$

Another related extremal problem

Suppose G is a finite abelian group with $\exp(G) = n$, and suppose $k \geq 2$ is an integer. Determine

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

Another related extremal problem

Suppose G is a finite abelian group with $\exp(G) = n$, and suppose $k \geq 2$ is an integer. Determine

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

We know $D_A(\mathbb{Z}_n) = \lceil n/k \rceil$ if $A = \{1, \ldots, k\}$ for $1 \leq k \leq n-1$, so this maximum is at least $\lceil n/k \rceil$.

Another related extremal problem

Theorem

- $$\max\{D_A(\mathbb{Z}_p) : |A| = k, A \subset [1, p-1]\} = \lceil p/k \rceil$$

  for p prime.

Another related extremal problem

Theorem

- $$\max\{D_A(\mathbb{Z}_p) : |A| = k, A \subset [1, p-1]\} = \lceil p/k \rceil$$

  for p prime.

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

Another related extremal problem

Theorem

- $$\max\{D_A(\mathbb{Z}_p) : |A| = k, A \subset [1, p-1]\} = \lceil p/k \rceil$$

  for p prime.

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

Combinatorial Nullstellensatz. Also works for a 'list version' of this result.

The Harborth Constant

Harborth constant, $\mathsf{g}(G)$: $\min\ m$ such that every *subset* of size m of G admits a zero-sum subsequence of size $\exp(G)$.

The Harborth Constant

Harborth constant, $\mathsf{g}(G)$: $\min\ m$ such that every *subset* of size m of G admits a zero-sum subsequence of size $\exp(G)$.

This is not always well defined: If $G = \mathbb{Z}_{2n}$, $\exp(G) = 2n$. But

$$\sum_{x \in \mathbb{Z}_{2n}} x = n.$$

In these cases, we adopt the convention: $\mathsf{g}(G) = |G| + 1$.

Some known results on the Harborth constant

Theorem

(Marchan, Ordaz, Ramos, Schmid, 2013) Let $n \in \mathbb{N}$. We have

- $$\mathsf{g}(\mathbb{Z}_2 \oplus \mathbb{Z}_{2n}) = \begin{cases} 2n+2 & \text{if } 2 \mid n, \\ 2n+3 & \text{otherwise.} \end{cases}$$

- $$\mathsf{g}_{\pm 1}(\mathbb{Z}_n) = \begin{cases} n+1 & \text{if } n \equiv 2 \pmod 4, \\ n & \text{otherwise.} \end{cases}$$

- *If $n \geq 3$, then $\mathsf{g}_{\pm 1}(\mathbb{Z}_2 \oplus \mathbb{Z}_{2n}) = 2n+2$.*

Harborth constant for the dihedral groups

Recall

$$D_{2n} = \langle x, y \mid x^2 = y^n = (xy)^2 = 1 \rangle.$$

Harborth constant for the dihedral groups

Recall

$$D_{2n} = \langle x, y \mid x^2 = y^n = (xy)^2 = 1 \rangle.$$

Theorem

(B., Mazumdar, Zhao, 2018)
For any integer $n \geq 3$ and $G = D_{2n}$,

$$\mathrm{g}(G) = \begin{cases} n+2 & \text{if } 2 \mid n, \\ 2n+1 & \text{otherwise.} \end{cases}$$

Main ingredient lemmas

Lemma

Suppose n *is even and let* $s \geq 2$. *Let* $S = \{xy^{\alpha_1}, \ldots, xy^{\alpha_{2s}}\}$ *with* $\alpha_i \neq \alpha_j$. *Then*

$$\left|\prod\nolimits_{2s}(S)\right| \geq s.$$

If equality holds, then $2s$ *divides* n *and* $\{\alpha_1, \ldots, \alpha_{2s}\}$ *is a coset of the subgroup of* $\mathbb{Z}_n$ *of order* $2s$.

Main ingredient lemmas

Lemma

Suppose n is even and let $s \geq 2$. Let $S = \{xy^{\alpha_1}, \ldots, xy^{\alpha_{2s}}\}$ with $\alpha_i \neq \alpha_j$. Then

$$\left|\prod_{2s}(S)\right| \geq s.$$

If equality holds, then $2s$ divides n and $\{\alpha_1, \ldots, \alpha_{2s}\}$ is a coset of the subgroup of $\mathbb{Z}_n$ of order $2s$.

Lemma

Suppose n is even and let $S = \{xy^{\alpha_1}, \ldots, xy^{\alpha_{2s+1}}\}$ with $\alpha_i \neq \alpha_j$. Then

$$\left|\prod_{2s+1}(S)\right| \geq s + 1.$$

If equality holds then $2s+2$ divides n and there is a coset K of the subgroup H of $\mathbb{Z}_n$ of order $2s+2$ such that $\{\alpha_1, \ldots, \alpha_{2s+1}\} \subset K$.

Open Questions

- Our conjecture:

Conjecture

$f^{(D)}(p,k) = \Theta(p^{1/k})$ *for all sufficiently large* p.

Stronger conjecture:

$$f^{(D)}(p,k) \leq (1+o(1))p^{1/k}.$$

- We believe

$$\max\{D_A(G) : |A| = k, A \subset [1, \exp(G) - 1]\} = \left\lceil \frac{|G|}{k} \right\rceil$$

holds for $G = \mathbb{Z}_n$, and also for $G = (\mathbb{Z}_n)^\ell$ for all n and all ℓ.

THANK YOU