Subspaces in difference sets

Thái Hoàng Lê & Zhenchao Ge

University of Mississippi

Nov. 11, 2018

Mississippi Discrete Math Workshop 2018

For two sets A, B in an abelian group G, we denote

$$A \pm B = \{a \pm b : a \in A, b \in B\}.$$

If $A \subset G$, we let

$$|A| = \#\{a : a \in A\}.$$

By the *density* of A in G, we mean $\frac{|A|}{|G|}$.

A motivation from analysis

For functions $f, g : \mathbb{R} \to \mathbb{R}$, the *convolution* of f and g, in symbole $f * g$, is defined as

$$(f * g)(x) = \int_{\mathbb{R}} f(y)g(x - y)\, dy.$$

A motivation from analysis

For functions $f, g : \mathbb{R} \to \mathbb{R}$, the *convolution* of f and g, in symbole $f * g$, is defined as

$$(f * g)(x) = \int_{\mathbb{R}} f(y)g(x - y)\, dy.$$

If f is supported on A, g is supported on B, then $f * g$ is supported on $A + B$.

A motivation from analysis

For functions $f, g : \mathbb{R} \to \mathbb{R}$, the *convolution* of f and g, in symbole $f * g$, is defined as

$$(f * g)(x) = \int_{\mathbb{R}} f(y)g(x - y)\, dy.$$

If f is supported on A, g is supported on B, then $f * g$ is supported on $A + B$.

The convolution $f * g$ is in general more smooth than both f and g.

A motivation from analysis

For functions $f, g : \mathbb{R} \to \mathbb{R}$, the *convolution* of f and g, in symbole $f * g$, is defined as

$$(f * g)(x) = \int_{\mathbb{R}} f(y)g(x-y)\,dy.$$

If f is supported on A, g is supported on B, then $f * g$ is supported on $A + B$.

The convolution $f * g$ is in general more smooth than both f and g.

Correspondingly, we expect $A + B$, and in particular $A - A$, to contain nice structures.

Theorem (Steinhaus 1920)

If $A \subset \mathbb{R}$ has positive Lebesgue measure, then $A - A$ contains an interval centered at 0.

Theorem (Steinhaus 1920)

If $A \subset \mathbb{R}$ has positive Lebesgue measure, then $A - A$ contains an interval centered at 0.

Theorem (Steinhaus 1920)

If $A \subset \mathbb{R}$ has positive Lebesgue measure, then $A - A$ contains an interval centered at 0.

If $A \subset \mathbb{Z}$ has positive upper density, then $A - A$ contains many nice structures (e.g. long arithmetic progressions (Bourgain), squares (Furstenberg, Sárközy)).

We are interested in the analogous phenomenon in $G := \mathbb{F}_2^n$ or $\mathbb{F}_p^n$.
Throughout, we let A be a subset of G with density α.

We are interested in the analogous phenomenon in $G := \mathbb{F}_2^n$ or $\mathbb{F}_p^n$. Throughout, we let A be a subset of G with density α.

Analogous to Steinhaus' theorem, if $\alpha > 0$, then $A - A$ should contain a large subspace.

We are interested in the analogous phenomenon in $G := \mathbb{F}_2^n$ or $\mathbb{F}_p^n$. Throughout, we let A be a subset of G with density α.

Analogous to Steinhaus' theorem, if $\alpha > 0$, then $A - A$ should contain a large subspace.

Proposition

If $\alpha > 1/2$ then $A - A = G$.

We are interested in the analogous phenomenon in $G := \mathbb{F}_2^n$ or $\mathbb{F}_p^n$. Throughout, we let A be a subset of G with density α.

Analogous to Steinhaus' theorem, if $\alpha > 0$, then $A - A$ should contain a large subspace.

Proposition

If $\alpha > 1/2$ then $A - A = G$.

We are interested in the analogous phenomenon in $G := \mathbb{F}_2^n$ or $\mathbb{F}_p^n$. Throughout, we let A be a subset of G with density α.

Analogous to Steinhaus' theorem, if $\alpha > 0$, then $A - A$ should contain a large subspace.

Proposition

If $\alpha > 1/2$ then $A - A = G$.

Proof.

Let x be arbitrary in G. Then A and $x + A$ both have density $> 1/2$, thus $A \cap (x + A) \neq \varnothing$. Thus $x \in A - A$. □

Theorem (Green 2005, Sanders 2010)

In $G = \mathbb{F}_2^n$, if $0 < \alpha < 1$, then $A - A$ contains a subspace of dimension $\Omega(\alpha n)$.

Theorem (Green 2005, Sanders 2010)

In $G = \mathbb{F}_2^n$, if $0 < \alpha < 1$, then $A - A$ contains a subspace of dimension $\Omega(\alpha n)$.

Theorem (Green 2005, Sanders 2010)

In $G = \mathbb{F}_2^n$, if $0 < \alpha < 1$, then $A - A$ contains a subspace of dimension $\Omega(\alpha n)$.

However, finite codimension (i.e. dimension $n - c(\alpha)$) is impossible.

Theorem (Green 2005, Sanders 2010)

In $G = \mathbb{F}_2^n$, if $0 < \alpha < 1$, then $A - A$ contains a subspace of dimension $\Omega(\alpha n)$.

However, finite codimension (i.e. dimension $n - c(\alpha)$) is impossible.

Theorem (Ruzsa 1991, Green 2005)

In $G = \mathbb{F}_2^n$, for any $0 < \alpha < 1/2$, there exists $A \subset G$ of density $\geq \alpha$ such that $A - A$ does not contain any subspace of codimension $c(\alpha)\sqrt{n}$ (i.e. dimension $n - c(\alpha)\sqrt{n}$).

Theorem (Bogolyubov 1939)

In $G = \mathbb{F}_p^n$, if $0 < \alpha < 1$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

Theorem (Bogolyubov 1939)

In $G = \mathbb{F}_p^n$, if $0 < \alpha < 1$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

Theorem (Bogolyubov 1939)

In $G = \mathbb{F}_p^n$, if $0 < \alpha < 1$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

- Bogolyubov's proof gives $c(\alpha) = O\left(\frac{1}{\alpha^2}\right)$.

Theorem (Bogolyubov 1939)

In $G = \mathbb{F}_p^n$, if $0 < \alpha < 1$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

- Bogolyubov's proof gives $c(\alpha) = O\left(\frac{1}{\alpha^2}\right)$.
- Sanders 2010: $c(\alpha) = O\left(\log^4 \frac{1}{\alpha}\right)$.

Theorem (Bogolyubov 1939)

In $G = \mathbb{F}_p^n$, if $0 < \alpha < 1$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

- Bogolyubov's proof gives $c(\alpha) = O\left(\frac{1}{\alpha^2}\right)$.
- Sanders 2010: $c(\alpha) = O\left(\log^4 \frac{1}{\alpha}\right)$.

Theorem (Bogolyubov 1939)

In $G = \mathbb{F}_p^n$, if $0 < \alpha < 1$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

- Bogolyubov's proof gives $c(\alpha) = O\left(\frac{1}{\alpha^2}\right)$.
- Sanders 2010: $c(\alpha) = O\left(\log^4 \frac{1}{\alpha}\right)$.

It is easy to see that we cannot do better than $O\left(\log \frac{1}{\alpha}\right)$.

Q: What happens when $\alpha = 1/2$, or is close to $1/2$?

Q: What happens when $\alpha = 1/2$, or is close to $1/2$?

Theorem (Sanders 2010)

In $G = \mathbb{F}_2^n$, if $\alpha > \frac{1}{2} - \frac{c}{\sqrt{n}}$, then $A - A$ contains a subspace of codimension 1.

Q: What happens when $\alpha = 1/2$, or is close to $1/2$?

Theorem (Sanders 2010)

In $G = \mathbb{F}_2^n$, if $\alpha > \frac{1}{2} - \frac{c}{\sqrt{n}}$, then $A - A$ contains a subspace of codimension 1.

Q: What happens when $\alpha = 1/2$, or is close to $1/2$?

Theorem (Sanders 2010)

In $G = \mathbb{F}_2^n$, if $\alpha > \frac{1}{2} - \frac{c}{\sqrt{n}}$, then $A - A$ contains a subspace of codimension 1.

This is best possible by taking A to be a subspace of codimension 1.

Q: What happens when $\alpha = 1/2$, or is close to $1/2$?

Theorem (Sanders 2010)

In $G = \mathbb{F}_2^n$, if $\alpha > \frac{1}{2} - \frac{c}{\sqrt{n}}$, then $A - A$ contains a subspace of codimension 1.

This is best possible by taking A to be a subspace of codimension 1.

The proof uses McDiarmid's inequality in probability.

Q: What happens when $\alpha = 1/2$, or is close to $1/2$?

Theorem (Sanders 2010)

In $G = \mathbb{F}_2^n$, if $\alpha > \frac{1}{2} - \frac{c}{\sqrt{n}}$, then $A - A$ contains a subspace of codimension 1.

This is best possible by taking A to be a subspace of codimension 1.

The proof uses McDiarmid's inequality in probability.

With Lê, we found a simple and elementary proof which also works in $\mathbb{F}_p^n$, inspired by a theorem of Wirsing.

Theorem (Wirsing 1979)

Let $A \subset \{1, 2, 3, 4, 5, \ldots, 2^n\}, H = \{0\} \cup \{\pm 2^i : i \geq 0\}$. *Then*

$$|(A + H) \cap [1, 2^n]| \geq |A| + \sqrt{\frac{2}{n}}|A|\left(1 - \frac{|A|}{2^n}\right).$$

Theorem (Wirsing 1979)

Let $A \subset \{1, 2, 3, 4, 5, \dots, 2^n\}$, $H = \{0\} \cup \{\pm 2^i : i \geq 0\}$. *Then*

$$|(A + H) \cap [1, 2^n]| \geq |A| + \sqrt{\frac{2}{n}}|A|\left(1 - \frac{|A|}{2^n}\right).$$

Theorem (Lê-G. 2018)

Let $G = \mathbb{F}_p^n$, $e_1, \dots, e_n$ *be a basis of* $\mathbb{F}_p^n$, $H = \{0, e_1, \dots, e_n\}$. *Then for any* $A \subset G$, *we have*

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{|G|}\right).$$

Theorem (Lê-G. 2018)

Let $G = \mathbb{F}_p^n$, $e_1, \ldots, e_n$ be a basis of $\mathbb{F}_p^n$, $H = \{0, e_1, \ldots, e_n\}$. Then for any $A \subset G$, we have

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{|G|}\right).$$

Theorem (Lê-G. 2018)

Let $G = \mathbb{F}_p^n$, $e_1, \dots, e_n$ be a basis of $\mathbb{F}_p^n$, $H = \{0, e_1, \dots, e_n\}$. Then for any $A \subset G$, we have

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{|G|}\right).$$

- The factor $\sqrt{n}$ is best possible.

Theorem (Lê-G. 2018)

Let $G = \mathbb{F}_p^n$, $e_1, \ldots, e_n$ be a basis of $\mathbb{F}_p^n$, $H = \{0, e_1, \ldots, e_n\}$. Then for any $A \subset G$, we have

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{|G|}\right).$$

- The factor $\sqrt{n}$ is best possible.
- Our proof gives $c(p) = \Omega(p^{-3/2})$. The truth may be $\Omega(p^{-1})$.

Theorem (Lê-G. 2018)

Let $G = \mathbb{F}_p^n$, $e_1, \ldots, e_n$ be a basis of $\mathbb{F}_p^n$, $H = \{0, e_1, \ldots, e_n\}$. Then for any $A \subset G$, we have

$$|A+H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{|G|}\right).$$

- The factor $\sqrt{n}$ is best possible.
- Our proof gives $c(p) = \Omega(p^{-3/2})$. The truth may be $\Omega(p^{-1})$.
- When $p = 2$, one can probably deduce the theorem from vertex isoperimetric inequalities for hypercubes. Harper 1966: among sets $A \subset \{0,1\}^n$ of the same size, $|A+H|$ is minimized when A is a Hamming ball.

Theorem (Lê-G. 2018)

Let $G = \mathbb{F}_p^n$, $e_1, \ldots, e_n$ be a basis of $\mathbb{F}_p^n$, $H = \{0, e_1, \ldots, e_n\}$. Then for any $A \subset G$, we have

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{|G|}\right).$$

- The factor $\sqrt{n}$ is best possible.
- Our proof gives $c(p) = \Omega(p^{-3/2})$. The truth may be $\Omega(p^{-1})$.
- When $p = 2$, one can probably deduce the theorem from vertex isoperimetric inequalities for hypercubes. Harper 1966: among sets $A \subset \{0, 1\}^n$ of the same size, $|A + H|$ is minimized when A is a Hamming ball.
- Wirsing's argument is extremely simple and works in a general setting.

Proof of generalized Sanders' theorem

Theorem (Sanders 2010 ($p = 2$), Lê-G. (all p))

($G = \mathbb{F}_p^n$) *If* $\alpha > \frac{1}{2} - \frac{c'(p)}{\sqrt{n}}$*, then* $A - A$ *contains a subspace of codimension 1.*

We will show that $A - A$ contains $G \setminus V$ where V is an *affine* subspace of codimension 1.

Proof of generalized Sanders' theorem

Theorem (Sanders 2010 ($p = 2$), Lê-G. (all p))

($G = \mathbb{F}_p^n$) If $\alpha > \frac{1}{2} - \frac{c'(p)}{\sqrt{n}}$, then $A - A$ contains a subspace of codimension 1.

We will show that $A - A$ contains $G \setminus V$ where V is an *affine* subspace of codimension 1.

Proof of generalized Sanders' theorem

Theorem (Sanders 2010 ($p = 2$), Lê-G. (all p))

($G = \mathbb{F}_p^n$) *If* $\alpha > \frac{1}{2} - \frac{c'(p)}{\sqrt{n}}$*, then* $A - A$ *contains a subspace of codimension 1.*

We will show that $A - A$ contains $G \setminus V$ where V is an *affine* subspace of codimension 1. With further work, we can show $0 \notin V$, which implies generalized Sanders' theorem.

Proof of generalized Sanders' theorem

Theorem (Sanders 2010 ($p = 2$), Lê-G. (all p))

($G = \mathbb{F}_p^n$) If $\alpha > \frac{1}{2} - \frac{c'(p)}{\sqrt{n}}$, then $A - A$ contains a subspace of codimension 1.

We will show that $A - A$ contains $G \setminus V$ where V is an *affine* subspace of codimension 1. With further work, we can show $0 \notin V$, which implies generalized Sanders' theorem.

Equivalently, $S := (A - A)^c$ is contained in an affine subspace of codimension 1.

Goal: if $\alpha > \frac{1}{2} - \frac{c}{\sqrt{n}}$, then $S := (A - A)^c$ is contained in an affine subspace of codimension 1.

Goal: if $\alpha > \frac{1}{2} - \frac{c}{\sqrt{n}}$, then $S := (A - A)^c$ is contained in an affine subspace of codimension 1.

Suppose this is not true. Let $s \in S$. Then $S - s$ contains n linearly independent vectors $e_1, \ldots, e_n$. Let $H = \{0, e_1, \ldots, e_n\}$.

Goal: if $\alpha > \frac{1}{2} - \frac{c}{\sqrt{n}}$, then $S := (A - A)^c$ is contained in an affine subspace of codimension 1.

Suppose this is not true. Let $s \in S$. Then $S - s$ contains n linearly independent vectors $e_1, \ldots, e_n$. Let $H = \{0, e_1, \ldots, e_n\}$.

By definition $S \cap (A - A) = \varnothing$. Thus $(S + A) \cap A = \varnothing$ and

Goal: if $\alpha > \frac{1}{2} - \frac{c}{\sqrt{n}}$, then $S := (A - A)^c$ is contained in an affine subspace of codimension 1.

Suppose this is not true. Let $s \in S$. Then $S - s$ contains n linearly independent vectors $e_1, \dots, e_n$. Let $H = \{0, e_1, \dots, e_n\}$.

By definition $S \cap (A - A) = \varnothing$. Thus $(S + A) \cap A = \varnothing$ and

$$1 \geq \frac{|A|}{|G|} + \frac{|S + A|}{|G|} \geq \frac{|A|}{|G|} + \frac{|H + A|}{|G|} \geq \alpha + \alpha + \frac{c(p)}{\sqrt{n}} \alpha(1 - \alpha).$$

Goal: if $\alpha > \frac{1}{2} - \frac{c}{\sqrt{n}}$, then $S := (A - A)^c$ is contained in an affine subspace of codimension 1.

Suppose this is not true. Let $s \in S$. Then $S - s$ contains n linearly independent vectors $e_1, \dots, e_n$. Let $H = \{0, e_1, \dots, e_n\}$.

By definition $S \cap (A - A) = \varnothing$. Thus $(S + A) \cap A = \varnothing$ and

$$1 \geq \frac{|A|}{|G|} + \frac{|S + A|}{|G|} \geq \frac{|A|}{|G|} + \frac{|H + A|}{|G|} \geq \alpha + \alpha + \frac{c(p)}{\sqrt{n}}\alpha(1 - \alpha).$$

This is a contradiction if $\alpha > \frac{1}{2} - \frac{c'(p)}{\sqrt{n}}$.

Wirsing's argument

Theorem (Lê-G. 2018)

Let $G = \mathbb{F}_p^n$, $e_1, \ldots, e_n$ be a basis of $\mathbb{F}_p^n$, $H = \{0, e_1, \ldots, e_n\}$. Then for any $A \subset G$, we have

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{|G|}\right).$$

Wirsing's argument

Theorem (Lê-G. 2018)

Let $G = \mathbb{F}_p^n$, $e_1, \ldots, e_n$ be a basis of $\mathbb{F}_p^n$, $H = \{0, e_1, \ldots, e_n\}$. Then for any $A \subset G$, we have

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{|G|}\right).$$

Wirsing's argument

Theorem (Lê-G. 2018)

Let $G = \mathbb{F}_p^n$, $e_1, \dots, e_n$ be a basis of $\mathbb{F}_p^n$, $H = \{0, e_1, \dots, e_n\}$. Then for any $A \subset G$, we have

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{|G|}\right).$$

Suppose $p = 2$. We prove by induction on n that for any $A \subset \mathbb{F}_2^n$, $H_n := \{0, e_1, e_2, \dots, e_n\}$, we have

$$|A + H_n| \geq |A| + c_n|A|\left(1 - \frac{|A|}{2^n}\right)$$

for some constant c_n.

Wirsing's argument

Theorem (Lê-G. 2018)

Let $G = \mathbb{F}_p^n$, $e_1, \ldots, e_n$ be a basis of $\mathbb{F}_p^n$, $H = \{0, e_1, \ldots, e_n\}$. Then for any $A \subset G$, we have

$$|A + H| \geq |A| + \frac{c(p)}{\sqrt{n}}|A|\left(1 - \frac{|A|}{|G|}\right).$$

Suppose $p = 2$. We prove by induction on n that for any $A \subset \mathbb{F}_2^n$, $H_n := \{0, e_1, e_2, \ldots, e_n\}$, we have

$$|A + H_n| \geq |A| + c_n|A|\left(1 - \frac{|A|}{2^n}\right)$$

for some constant c_n.

$n = 1$: Easy to see that this is true when $c_1 \leq 2$.

$n-1 \Rightarrow n$: We partition

$$A = A_0 \oplus \{0\} \bigcup A_1 \oplus \{1\}$$

where $A_0, A_1 \subset \mathbb{F}_2^{n-1}$.

$n-1 \Rightarrow n$: We partition

$$A = A_0 \oplus \{0\} \bigcup A_1 \oplus \{1\}$$

where $A_0, A_1 \subset \mathbb{F}_2^{n-1}$. Two easy observations:

1. $A + H_n \supset A_0 \oplus \{0, 1\}$. Therefore, $|A + H_n| \geq 2|A_0|$. Similarly, $|A + H_n| \geq 2|A_1|$.

$n-1 \Rightarrow n$: We partition

$$A = A_0 \oplus \{0\} \bigcup A_1 \oplus \{1\}$$

where $A_0, A_1 \subset \mathbb{F}_2^{n-1}$. Two easy observations:

1. $A + H_n \supset A_0 \oplus \{0,1\}$. Therefore, $|A + H_n| \geq 2|A_0|$. Similarly, $|A + H_n| \geq 2|A_1|$.
2. $A + H_n \supset (A_0 + H_{n-1}) \oplus \{0\} \bigcup (A_1 + H_{n-1}) \oplus \{1\}$. Therefore, $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

$n-1 \Rightarrow n$: We partition

$$A = A_0 \oplus \{0\} \bigcup A_1 \oplus \{1\}$$

where $A_0, A_1 \subset \mathbb{F}_2^{n-1}$. Two easy observations:

1. $A + H_n \supset A_0 \oplus \{0,1\}$. Therefore, $|A + H_n| \geq 2|A_0|$. Similarly, $|A + H_n| \geq 2|A_1|$.
2. $A + H_n \supset (A_0 + H_{n-1}) \oplus \{0\} \bigcup (A_1 + H_{n-1}) \oplus \{1\}$. Therefore, $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

$n-1 \Rightarrow n$: We partition

$$A = A_0 \oplus \{0\} \bigcup A_1 \oplus \{1\}$$

where $A_0, A_1 \subset \mathbb{F}_2^{n-1}$. Two easy observations:

1. $A + H_n \supset A_0 \oplus \{0, 1\}$. Therefore, $|A + H_n| \geq 2|A_0|$. Similarly, $|A + H_n| \geq 2|A_1|$.
2. $A + H_n \supset (A_0 + H_{n-1}) \oplus \{0\} \bigcup (A_1 + H_{n-1}) \oplus \{1\}$. Therefore, $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Case 1: If one of $|A_0|$ and $|A_1|$ is significantly larger than the other, then use Observation 1.

$n-1 \Rightarrow n$: We partition

$$A = A_0 \oplus \{0\} \bigcup A_1 \oplus \{1\}$$

where $A_0, A_1 \subset \mathbb{F}_2^{n-1}$. Two easy observations:

1. $A + H_n \supset A_0 \oplus \{0,1\}$. Therefore, $|A + H_n| \geq 2|A_0|$. Similarly, $|A + H_n| \geq 2|A_1|$.
2. $A + H_n \supset (A_0 + H_{n-1}) \oplus \{0\} \bigcup (A_1 + H_{n-1}) \oplus \{1\}$. Therefore, $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Case 1: If one of $|A_0|$ and $|A_1|$ is significantly larger than the other, then use Observation 1.

Case 2: If $|A_0|$ and $|A_1|$ are close, then use Observation 2 and induction hypothesis.

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Case 1: $|A_0| - |A_1| \geq c_n|A|\left(1 - \frac{|A|}{2^n}\right)$.

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Case 1: $|A_0| - |A_1| \geq c_n |A| \left(1 - \frac{|A|}{2^n}\right)$. Then

$$|A + H_n| \geq 2|A_0| = (|A_0| + |A_1|) + (|A_0| - |A_1|) = |A| + (|A_0| - |A_1|)$$

and the goal follows.

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Observations:

1. $|A+H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A+H_n| \geq |A_0+H_{n-1}| + |A_1+H_{n-1}|$.

Case 2: $0 \leq |A_0| - |A_1| \leq c_n|A|\left(1-\frac{|A|}{2^n}\right)$.

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Case 2: $0 \leq |A_0| - |A_1| \leq c_n|A|\left(1 - \frac{|A|}{2^n}\right)$.

Then by induction hypothesis,

$$|A + H_n| \quad \geq \quad |A_0| + c_{n-1}|A_0|\left(1 - \frac{|A_0|}{2^{n-1}}\right) + |A_1| + c_{n-1}|A_1|\left(1 - \frac{|A_1|}{2^{n-1}}\right)$$

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Case 2: $0 \leq |A_0| - |A_1| \leq c_n|A|\left(1 - \frac{|A|}{2^n}\right)$.

Then by induction hypothesis,

$$\begin{aligned} |A + H_n| &\geq |A_0| + c_{n-1}|A_0|\left(1 - \frac{|A_0|}{2^{n-1}}\right) + |A_1| + c_{n-1}|A_1|\left(1 - \frac{|A_1|}{2^{n-1}}\right) \\ &= |A| + c_{n-1}|A| - \frac{c_{n-1}}{2^{n-1}}\left(|A_0|^2 + |A_1|^2\right) \end{aligned}$$

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Case 2: $0 \leq |A_0| - |A_1| \leq c_n|A|\left(1 - \frac{|A|}{2^n}\right)$.

Then by induction hypothesis,

$$\begin{aligned}
|A + H_n| &\geq |A_0| + c_{n-1}|A_0|\left(1 - \frac{|A_0|}{2^{n-1}}\right) + |A_1| + c_{n-1}|A_1|\left(1 - \frac{|A_1|}{2^{n-1}}\right) \\
&= |A| + c_{n-1}|A| - \frac{c_{n-1}}{2^{n-1}}\left(|A_0|^2 + |A_1|^2\right) \\
&= |A| + c_{n-1}|A| - \frac{c_{n-1}}{2^{n-1}}\left(\frac{|A|^2}{2} + \frac{(|A_0| - |A_1|)^2}{2}\right)
\end{aligned}$$

Observations:

1. $|A + H_n| \geq 2\max(|A_0|, |A_1|)$.
2. $|A + H_n| \geq |A_0 + H_{n-1}| + |A_1 + H_{n-1}|$.

Case 2: $0 \leq |A_0| - |A_1| \leq c_n|A|\left(1 - \frac{|A|}{2^n}\right)$.

Then by induction hypothesis,

$$\begin{aligned}
|A + H_n| &\geq |A_0| + c_{n-1}|A_0|\left(1 - \frac{|A_0|}{2^{n-1}}\right) + |A_1| + c_{n-1}|A_1|\left(1 - \frac{|A_1|}{2^{n-1}}\right) \\
&= |A| + c_{n-1}|A| - \frac{c_{n-1}}{2^{n-1}}\left(|A_0|^2 + |A_1|^2\right) \\
&= |A| + c_{n-1}|A| - \frac{c_{n-1}}{2^{n-1}}\left(\frac{|A|^2}{2} + \frac{(|A_0| - |A_1|)^2}{2}\right) \\
&\geq |A| + |A|\left(1 - \frac{|A|}{2^n}\right)\left(c_{n-1} - \frac{c_n^2}{4}\right).
\end{aligned}$$

Thus the goal follows if $c_{n-1}\left(1-\frac{c_n^2}{4}\right) \geq c_n$.

Thus the goal follows if $c_{n-1}\left(1-\frac{c_n^2}{4}\right)\geq c_n$. This is satisfied if $c_n=\sqrt{\frac{2}{n}}$.

Thus the goal follows if $c_{n-1}\left(1-\frac{c_n^2}{4}\right) \geq c_n$. This is satisfied if $c_n = \sqrt{\frac{2}{n}}$.

When $G = \mathbb{F}_p^n$, we partition A into p fibers and argue similarly. We also use Plünnecke's inequality.

Thus the goal follows if $c_{n-1}\left(1-\frac{c_n^2}{4}\right) \geq c_n$. This is satisfied if $c_n = \sqrt{\frac{2}{n}}$.

When $G = \mathbb{F}_p^n$, we partition A into p fibers and argue similarly. We also use Plünnecke's inequality.

Theorem (Plünnecke 1970, Rusza 1989, Petridis 2011)

Let A, B be finite subsets of a commutative group G. Define

$$\mu_i = \min\left\{\frac{|X+iB|}{|X|} : X \subset A\right\}.$$

Then the sequence $\{\mu_i^{1/i}\}$ is decreasing.

Thank You!