Inverse Sumset Results mod p at High Density

David J. Grynkiewicz

University of Memphis

June 14, 2024

Sumsets

Let G be an abelian group.

Definition

For $A, B \subseteq G$, their sumset is

$$A + B = \{a + b : \ a \in A, \ b \in B\}, \quad 2A := A + A$$

Sumsets

Let G be an abelian group.

Definition

For $A, B \subseteq G$, their sumset is

$$A + B = \{a + b : \ a \in A, \ b \in B\}, \quad 2A := A + A$$

Small Sumset $\implies$ "Structure"

Sumsets

Let G be an abelian group.

Definition

For $A, B \subseteq G$, their sumset is

$$A + B = \{a + b : \; a \in A, \; b \in B\}, \quad 2A := A + A$$

Small Sumset $\implies$ "Structure"

Theorem (Folklore)

For finite, nonempty A, $B \subseteq \mathbb{Z}$, we have

$$|A + B| \geq |A| + |B| - 1.$$

If equality holds, then A and B are arithmetic progressions with common difference (or $|A| = 1$ or $|B| = 1$).

$3k - 4$ Theorem

Theorem ($3k - 4$ Theorem)

Let $A, B \subseteq \mathbb{Z}$ be finite and nonempty with $|A| \geq |B|$ and

$$|A + B| = |A| + |B| + r \leq |A| + 2|B| - 3 - \delta,$$

where

$$\delta = \begin{cases} 1 & \textit{if} \quad A = (\min A - \min B) + B, \\ 0 & \textit{otherwise.} \end{cases}$$

$3k - 4$ Theorem

Theorem ($3k - 4$ Theorem)

Let $A, B \subseteq \mathbb{Z}$ be finite and nonempty with $|A| \geq |B|$ and

$$|A+B| = |A| + |B| + r \leq |A| + 2|B| - 3 - \delta,$$

where

$$\delta = \begin{cases} 1 & \text{if} \quad A = (\min A - \min B) + B, \\ 0 & \text{otherwise.} \end{cases}$$

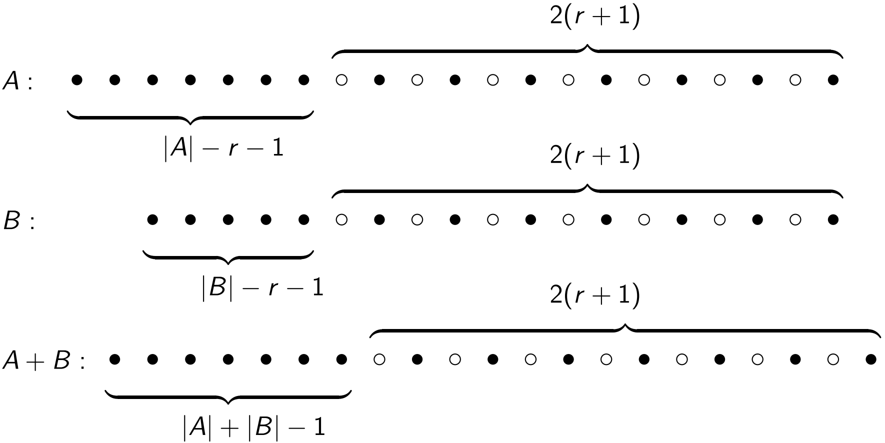
Then there are arithmetic progressions P_A, P_B, $P_{A+B} \subseteq \mathbb{Z}$ having common difference such that

$$X \subseteq P_X \quad \text{and} \quad |P_X| \leq |A| + r + 1 \qquad \text{for all } X \in \{A, B\},$$

$$P_{A+B} \subseteq A + B \quad \text{and} \quad |P_{A+B}| \geq |A| + |B| - 1.$$

Freiman (1962); Lev and Smeliansky (1995); Freiman (2009); Bardaji and G (2010); G (2013)

Some Examples: r is tight



Extension modulo p

Definition (General Setup)

$G = \mathbb{Z}/p\mathbb{Z}$ with $p \geq 2$ prime, $A, B \subseteq G$ nonempty, $A + B \neq G$,
$|A| \geq |B|$, $C := -(A+B)^c = -G \setminus (A+B)$ and $|A+B| = |A| + |B| + r$.

Extension modulo p

Definition (General Setup)

$G = \mathbb{Z}/p\mathbb{Z}$ with $p \geq 2$ prime, $A, B \subseteq G$ nonempty, $A + B \neq G$, $|A| \geq |B|$, $C := -(A+B)^{\mathrm{c}} = -G \setminus (A+B)$ and $|A+B| = |A| + |B| + r$.

Definition (Target Conclusion)

There exist arithmetic progressions P_A, P_B, $P_C \subseteq G$ of common difference with $X \subseteq P_X$ and $|P_X| \leq |X| + r + 1$ for all $X \in \{A, B, C\}$.

Extension modulo p

Definition (General Setup)

$G = \mathbb{Z}/p\mathbb{Z}$ with $p \geq 2$ prime, $A, B \subseteq G$ nonempty, $A + B \neq G$, $|A| \geq |B|$, $C := -(A+B)^{\mathrm{c}} = -G \setminus (A+B)$ and $|A+B| = |A| + |B| + r$.

Definition (Target Conclusion)

There exist arithmetic progressions P_A, P_B, $P_C \subseteq G$ of common difference with $X \subseteq P_X$ and $|P_X| \leq |X| + r + 1$ for all $X \in \{A, B, C\}$.

Conjecture

Assume **General Setup**. *If*

$$|A+B| \leq (|A| + |B|) + |B| - 3 - \delta_B \quad \text{and} \quad |A+B| \leq p - r - 3 - \delta_C,$$

then **Target Conclusions** *hold.*

Extension modulo p

Definition (General Setup)

$G = \mathbb{Z}/p\mathbb{Z}$ with $p \geq 2$ prime, $A, B \subseteq G$ nonempty, $A + B \neq G$,
$|A| \geq |B|$, $C := -(A+B)^{\mathrm{c}} = -G \setminus (A+B)$ and $|A+B| = |A| + |B| + r$.

Definition (Target Conclusion)

There exist arithmetic progressions P_A, P_B, $P_C \subseteq G$ of common difference with $X \subseteq P_X$ and $|P_X| \leq |X| + r + 1$ for all $X \in \{A, B, C\}$.

Conjecture

Assume **General Setup**. *If*

$$|A+B| \leq (|A| + |B|) + |B| - 3 - \delta_B \quad \textit{and} \quad |A+B| \leq p - r - 3 - \delta_C,$$

then **Target Conclusions** *hold.*

- Upshot: $3k - 4$ Theorem should in $\mathbb{Z}/p\mathbb{Z}$ too so long as $A + B$ isn't too large

Extension modulo p

Definition (General Setup)

$G = \mathbb{Z}/p\mathbb{Z}$ with $p \geq 2$ prime, $A, B \subseteq G$ nonempty, $A + B \neq G$, $|A| \geq |B|$, $C := -(A+B)^c = -G \setminus (A+B)$ and $|A+B| = |A| + |B| + r$.

Definition (Target Conclusion)

There exist arithmetic progressions P_A, P_B, $P_C \subseteq G$ of common difference with $X \subseteq P_X$ and $|P_X| \leq |X| + r + 1$ for all $X \in \{A, B, C\}$.

Conjecture

Assume **General Setup**. *If*

$$|A+B| \leq (|A| + |B|) + |B| - 3 - \delta_B \quad \textit{and} \quad |A+B| \leq p - r - 3 - \delta_C,$$

then **Target Conclusions** *hold.*

- Upshot: $3k - 4$ Theorem should in $\mathbb{Z}/p\mathbb{Z}$ too so long as $A + B$ isn't too large
- Much partial Progress. General Idea: Impose additional small doubling and density constraints to obtain **Target Conclusions**.

P_C vs. P_{A+B}

- Why does P_C replace P_{A+B}?

P_C vs. P_{A+B}

- Why does P_C replace P_{A+B}?
- For $X \subseteq G$, let $X^{\mathrm{c}} := G \setminus X$.

P_C vs. P_{A+B}

- Why does P_C replace P_{A+B}?
- For $X \subseteq G$, let $X^c := G \setminus X$.
- Recall $C = -(A+B)^c$.

P_C vs. P_{A+B}

- Why does P_C replace P_{A+B}?
- For $X \subseteq G$, let $X^c := G \setminus X$.
- Recall $C = -(A+B)^c$.
- Set $P_{A+B} = -(P_C)^c$

P_C vs. P_{A+B}

- Why does P_C replace P_{A+B}?
- For $X \subseteq G$, let $X^c := G \setminus X$.
- Recall $C = -(A+B)^c$.
- Set $P_{A+B} = -(P_C)^c$
- $C \subseteq P_C \qquad \iff \qquad -(P_C)^c \subseteq -C^c$

P_C vs. P_{A+B}

- Why does P_C replace P_{A+B}?
- For $X \subseteq G$, let $X^c := G \setminus X$.
- Recall $C = -(A+B)^c$.
- Set $P_{A+B} = -(P_C)^c$
- $C \subseteq P_C \qquad \iff \qquad P_{A+B} = -(P_C)^c \subseteq -C^c = A + B$

P_C vs. P_{A+B}

- Why does P_C replace P_{A+B}?
- For $X \subseteq G$, let $X^c := G \setminus X$.
- Recall $C = -(A+B)^c$.
- Set $P_{A+B} = -(P_C)^c$
- $C \subseteq P_C \iff P_{A+B} = -(P_C)^c \subseteq -C^c = A+B$
- $|P_C| \leq |C| + r + 1 \iff |P_{A+B}| \geq |A| + |B| - 1$

$$|P_{A+B}| = p - |P_C| \geq p - |C| - r - 1 = |A+B| - r - 1 = |A| + |B| - 1$$

Ideal Density implies $(1 - \epsilon)$ Density

- Suppose **Target Conclusions** holds if $|A + B| \leq p - r - 3$ and $|A + B| \leq (|A| + |B|) + \alpha|B| - 3$

Ideal Density implies $(1-\epsilon)$ Density

- Suppose **Target Conclusions** holds if $|A+B| \leq p-r-3$ and $|A+B| \leq (|A|+|B|)+\alpha|B|-3$
- Goal: Given any small $\epsilon > 0$, we want to show there is some $\alpha' > 0$ such that $|A+B| \leq (1-\epsilon)p$ and $|A+B| = (|A|+|B|)+r \leq (|A|+|B|)+\alpha'|B|-3$ also yields **Target Conclusions**.

Ideal Density implies $(1-\epsilon)$ Density

- Suppose **Target Conclusions** holds if $|A+B| \leq p-r-3$ and $|A+B| \leq (|A|+|B|)+\alpha|B|-3$
- Goal: Given any small $\epsilon > 0$, we want to show there is some $\alpha' > 0$ such that $|A+B| \leq (1-\epsilon)p$ and $|A+B| = (|A|+|B|)+r \leq (|A|+|B|)+\alpha'|B|-3$ also yields **Target Conclusions**.
- If $(1-\epsilon)p \leq p-r-3$, we can take $\alpha' = \alpha$.

Ideal Density implies $(1 - \epsilon)$ Density

- Suppose **Target Conclusions** holds if $|A + B| \leq p - r - 3$ and $|A + B| \leq (|A| + |B|) + \alpha|B| - 3$
- Goal: Given any small $\epsilon > 0$, we want to show there is some $\alpha' > 0$ such that $|A + B| \leq (1 - \epsilon)p$ and $|A + B| = (|A| + |B|) + r \leq (|A| + |B|) + \alpha'|B| - 3$ also yields **Target Conclusions**.
- If $(1 - \epsilon)p \leq p - r - 3$, we can take $\alpha' = \alpha$.
- So we need $r + 3 \leq \epsilon p$

Ideal Density implies $(1-\epsilon)$ Density

- Suppose **Target Conclusions** holds if $|A+B| \leq p-r-3$ and $|A+B| \leq (|A|+|B|)+\alpha|B|-3$
- Goal: Given any small $\epsilon > 0$, we want to show there is some $\alpha' > 0$ such that $|A+B| \leq (1-\epsilon)p$ and $|A+B| = (|A|+|B|)+r \leq (|A|+|B|)+\alpha'|B|-3$ also yields **Target Conclusions**.
- If $(1-\epsilon)p \leq p-r-3$, we can take $\alpha' = \alpha$.
- So we need $r+3 \leq \epsilon p$
- Since $A+B \neq G$, easy pigeonhole argument shows $2|B| \leq |A|+|B| \leq p$. Hence $|B| \leq \frac{p}{2}$.

Ideal Density implies $(1-\epsilon)$ Density

- Suppose **Target Conclusions** holds if $|A+B| \leq p-r-3$ and $|A+B| \leq (|A|+|B|)+\alpha|B|-3$
- Goal: Given any small $\epsilon > 0$, we want to show there is some $\alpha' > 0$ such that $|A+B| \leq (1-\epsilon)p$ and $|A+B| = (|A|+|B|)+r \leq (|A|+|B|)+\alpha'|B|-3$ also yields **Target Conclusions**.
- If $(1-\epsilon)p \leq p-r-3$, we can take $\alpha' = \alpha$.
- So we need $r+3 \leq \epsilon p$
- Since $A+B \neq G$, easy pigeonhole argument shows $2|B| \leq |A|+|B| \leq p$. Hence $|B| \leq \frac{p}{2}$.
- Thus $r+3 \leq \alpha'|B| < \alpha'\frac{p}{2}$, so its true for $\alpha' \leq 2\epsilon$

Ideal Density implies $(1-\epsilon)$ Density

- Suppose **Target Conclusions** holds if $|A+B| \le p-r-3$ and $|A+B| \le (|A|+|B|)+\alpha|B|-3$
- Goal: Given any small $\epsilon > 0$, we want to show there is some $\alpha' > 0$ such that $|A+B| \le (1-\epsilon)p$ and $|A+B| = (|A|+|B|)+r \le (|A|+|B|)+\alpha'|B|-3$ also yields **Target Conclusions**.
- If $(1-\epsilon)p \le p-r-3$, we can take $\alpha' = \alpha$.
- So we need $r+3 \le \epsilon p$
- Since $A+B \neq G$, easy pigeonhole argument shows $2|B| \le |A|+|B| \le p$. Hence $|B| \le \frac{p}{2}$.
- Thus $r+3 \le \alpha'|B| < \alpha'\frac{p}{2}$, so its true for $\alpha' \le 2\epsilon$
- Summary:

$$|A+B| \le (|A|+|B|)+2\epsilon|B|-3 \quad \text{and} \quad |A+B| \le (1-\epsilon)p$$

ensure A, B and C contained in small length arithmetic progressions (for small $\epsilon < \frac{1}{2}\alpha$.)

Partial Progress: Low Density

$$|A + B| = |A| + |B| + r \leq (|A| + |B|) + \alpha|B| - 3, \qquad \text{where } \alpha \in (0, 1]$$

- Results for very low density follow from more general "rectification" principles.

Partial Progress: Low Density

$$|A + B| = |A| + |B| + r \leq (|A| + |B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0, 1]$$

- Results for very low density follow from more general “rectification” principles.
- Low density implies “isomorphic” to a sumset $A' + B' \subseteq \mathbb{Z}$.

Partial Progress: Low Density

$$|A+B| = |A| + |B| + r \leq (|A|+|B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0,1]$$

- Results for very low density follow from more general "rectification" principles.
- Low density implies "isomorphic" to a sumset $A' + B' \subseteq \mathbb{Z}$.
- $|A \cup B| \leq \log_4 p \quad \longrightarrow \quad$ Bilu, Lev, Ruzsa (1998)
- $|A \cup B| \leq \lceil \log_2 p \rceil \quad \longrightarrow \quad$ Lev (2008), + technical issue G. (2013)
- $A = B$ and $|A| \leq cp$ with $c = (1/96)^{108} \quad \longrightarrow \quad$ Green, Ruzsa (2006)

Partial Progress: Mid-Range Density

$$|A + B| = |A| + |B| + r \leq (|A| + |B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0, 1]$$

- "Balanced" approach with tangible constants both for the density and small doubling constraints

Partial Progress: Mid-Range Density

$$|A+B| = |A| + |B| + r \leq (|A| + |B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0,1]$$

- "Balanced" approach with tangible constants both for the density and small doubling constraints
- $A = B$: Freiman (1960s), Rodseth (2006), Candela, Serra and Spiegel (2020), Lev and Shkredov (2020), Lev and Serra (2020)
  - $|A+A| \leq 2|A| + (0.4)|A| - 3$ and $|A| \leq (0.02857)p$
  - $|A+A| \leq 2|A| + (0.4)|A| - 3$ and $|A| \leq (0.093457)p$
  - $|A+A| \leq 2|A| + (0.48)|A| - 7$ and $|A| < (0.0000000001)p$
  - $|A+A| \leq 2|A| + (0.59)|A| - 3$ and $101 \leq |A| < (0.0045)p$
  - $|A+A| < 2|A| + (0.7652)|A| - 3$ and $10 \leq |A| < (0.00000125)p$

Partial Progress: Mid-Range Density

$$|A+B| = |A| + |B| + r \leq (|A| + |B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0,1]$$

- "Balanced" approach with tangible constants both for the density and small doubling constraints
- $A = B$: Freiman (1960s), Rodseth (2006), Candela, Serra and Spiegel (2020), Lev and Shkredov (2020), Lev and Serra (2020)
  - $|A+A| \leq 2|A| + (0.4)|A| - 3$ and $|A| \leq (0.02857)p$
  - $|A+A| \leq 2|A| + (0.4)|A| - 3$ and $|A| \leq (0.093457)p$
  - $|A+A| \leq 2|A| + (0.48)|A| - 7$ and $|A| < (0.0000000001)p$
  - $|A+A| \leq 2|A| + (0.59)|A| - 3$ and $101 \leq |A| < (0.0045)p$
  - $|A+A| < 2|A| + (0.7652)|A| - 3$ and $10 \leq |A| < (0.00000125)p$
- In many cases, "flexible" versions are available: density restriction grows stronger as small doubling constraint gets weaker.

Partial Progress: Mid-Range Density

$$|A+B| = |A| + |B| + r \leq (|A| + |B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0,1]$$

- "Balanced" approach with tangible constants both for the density and small doubling constraints
- $A = B$: Freiman (1960s), Rodseth (2006), Candela, Serra and Spiegel (2020), Lev and Shkredov (2020), Lev and Serra (2020)
  - $|A+A| \leq 2|A| + (0.4)|A| - 3$ and $|A| \leq (0.02857)p$
  - $|A+A| \leq 2|A| + (0.4)|A| - 3$ and $|A| \leq (0.093457)p$
  - $|A+A| \leq 2|A| + (0.48)|A| - 7$ and $|A| < (0.0000000001)p$
  - $|A+A| \leq 2|A| + (0.59)|A| - 3$ and $101 \leq |A| < (0.0045)p$
  - $|A+A| < 2|A| + (0.7652)|A| - 3$ and $10 \leq |A| < (0.00000125)p$
- In many cases, "flexible" versions are available: density restriction grows stronger as small doubling constraint gets weaker.
- $(0.001)|A|^{2/3} \leq |B| \leq |A|, \quad |A+B| \leq (|A| + |B|) + (0.03)|B|$ and $|A| < (0.0045)p \quad \longrightarrow \quad$ Huichochea (2022)

Partial Progress: High/Ideal Density

$$|A+B| = |A| + |B| + r \leq (|A| + |B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0,1]$$

- $A = B$, $|A+A| \leq 2|A| + (0.136)|A| - 3$ and $|A+A| \leq (0.75)p$.
  $\longrightarrow$ Candela, González-Sánchez and G. (2022)

Partial Progress: High/Ideal Density

$$|A+B| = |A| + |B| + r \leq (|A|+|B|) + \alpha|B| - 3, \qquad \text{where } \alpha \in (0,1]$$

- $A = B$, $|A+A| \leq 2|A| + (0.136)|A| - 3$ and $|A+A| \leq (0.75)p$.
  $\longrightarrow$ Candela, González-Sánchez and G. (2022)
- $r \leq cp - 1.2$ with $c = 1.4 \times 10^{-63951}$

Partial Progress: High/Ideal Density

$$|A+B| = |A| + |B| + r \leq (|A|+|B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0,1]$$

- $A = B$, $|A+A| \leq 2|A| + (0.136)|A| - 3$ and $|A+A| \leq (0.75)p$.
  $\longrightarrow$ Candela, González-Sánchez and G. (2022)
- $r \leq cp - 1.2$ with $c = 1.4 \times 10^{-63951}$
- Why does a $r \leq cp$ restriction count as High density?

Partial Progress: High/Ideal Density

$$|A+B| = |A| + |B| + r \leq (|A| + |B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0,1]$$

- $A = B$, $|A+A| \leq 2|A| + (0.136)|A| - 3$ and $|A+A| \leq (0.75)p$.
  $\longrightarrow$ Candela, González-Sánchez and G. (2022)
- $r \leq cp - 1.2$ with $c = 1.4 \times 10^{-63951}$
- Why does a $r \leq cp$ restriction count as High density?
- $A + B \neq G$ implies $|B| \leq \frac{p}{2}$ (easy pigeonhole argument)

Partial Progress: High/Ideal Density

$$|A+B| = |A| + |B| + r \leq (|A|+|B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0,1]$$

- $A = B$, $|A+A| \leq 2|A| + (0.136)|A| - 3$ and $|A+A| \leq (0.75)p$.
  $\longrightarrow$ Candela, González-Sánchez and G. (2022)
- $r \leq cp - 1.2$ with $c = 1.4 \times 10^{-63951}$
- Why does a $r \leq cp$ restriction count as High density?
- $A + B \neq G$ implies $|B| \leq \frac{p}{2}$ (easy pigeonhole argument)
- If $\alpha \leq 2c$, small doubling hypothesi rephrases as
  $r \leq \alpha|B| - 3 \leq (2c)\frac{p}{2} - 3 = cp - 3$.

Partial Progress: High/Ideal Density

$$|A+B| = |A| + |B| + r \leq (|A|+|B|) + \alpha|B| - 3, \quad \text{where } \alpha \in (0,1]$$

- $A = B$, $|A+A| \leq 2|A| + (0.136)|A| - 3$ and $|A+A| \leq (0.75)p$.
  $\longrightarrow$ Candela, González-Sánchez and G. (2022)
- $r \leq cp - 1.2$ with $c = 1.4 \times 10^{-63951}$
- Why does a $r \leq cp$ restriction count as High density?
- $A + B \neq G$ implies $|B| \leq \frac{p}{2}$ (easy pigeonhole argument)
- If $\alpha \leq 2c$, small doubling hypothesi rephrases as
  $r \leq \alpha|B| - 3 \leq (2c)\frac{p}{2} - 3 = cp - 3$.
- This gives no density restriction for $|A+B| \leq |A| + (1+2c)|B| - 3$.

Ideal Density

Theorem (Serra and Zémor 2009)

Assume **General Setup**. *If* $|A| \geq 4$, $p > 2^{94}$,

$$|A+A| \leq 2|A| + (0.0001)|A| \quad \textit{and} \quad |A+A| \leq p - r - 3,$$

then **Target Conclusions** *hold.*

Ideal Density

Theorem (Serra and Zémor 2009)

Assume **General Setup**. *If* $|A| \geq 4$, $p > 2^{94}$,

$$|A + A| \leq 2|A| + (0.0001)|A| \quad \textit{and} \quad |A + A| \leq p - r - 3,$$

then **Target Conclusions** *hold.*

Theorem (G. 2024)

Assume **General Setup**. *If*

$$|A + B| \leq (|A| + |B|) + (0.01)|A| - 3 \quad \textit{and} \quad |A + B| \leq p - r - 3,$$

then **Target Conclusions** *hold.*

Ideas for the Proof: Additive Trios

Definition (Boothbay, DeVos, Montejano 2015)

Let G be a finite abelian group; let $A, B, C \subseteq G$ be nonempty sets. Then (A, B, C) is and **additive trio** if $A + B + C \neq G$ with $\mathrm{r}(A, B, C) := |G| - |A| - |B| - |C|$.

Ideas for the Proof: Additive Trios

Definition (Boothbay, DeVos, Montejano 2015)

Let G be a finite abelian group; let $A, B, C \subseteq G$ be nonempty sets. Then (A, B, C) is and **additive trio** if $A + B + C \neq G$ with $\mathrm{r}(A, B, C) := |G| - |A| - |B| - |C|$.

Example

$A, B \subseteq G$, $C := -(A + B)^{\mathrm{c}}$, $|A + B| = |A| + |B| + r$. Then (A, B, C) is an additive trio, since

$$0 \notin (A + B) - (A + B)^{\mathrm{c}} = A + B + C,$$

with $\mathrm{r}(A, B, C) = |G| - |A| - |B| - (|G| - |A| - |B| - r) = r$

Ideas for the Proof: Additive Trios

Definition (Boothbay, DeVos, Montejano 2015)

Let G be a finite abelian group; let $A, B, C \subseteq G$ be nonempty sets. Then (A, B, C) is and **additive trio** if $A + B + C \neq G$ with $\mathrm{r}(A, B, C) := |G| - |A| - |B| - |C|$.

Example

$A, B \subseteq G$, $C := -(A+B)^{\mathrm{c}}$, $|A+B| = |A| + |B| + r$. Then (A, B, C) is an additive trio, since

$$0 \notin (A+B) - (A+B)^{\mathrm{c}} = A + B + C,$$

with $\mathrm{r}(A, B, C) = |G| - |A| - |B| - (|G| - |A| - |B| - r) = r$

- $|A+B| = |A| + |B| + r \leq (|A| + |B|) + \alpha|B| - 3$ and $|A+B| \leq p - \alpha(r+3)$ equivalent to $|A|, |B|, |C| \geq \alpha^{-1}(r+3)$.

Ideas for the Proof: Huicochea's Reduction

Definition

For $A \subseteq G$ and $d \in G$, let $\ell_d(A)$ be the minimal length of an arithmetic progression with difference d containing A.

Theorem (Huicochea 2017; modified by G. 2024)

Let $G = \mathbb{Z}/p\mathbb{Z}$ with $p \geq 2$ prime, let (A, B, C) be an additive trio from G, and let $r,\ h \in \mathbb{Z}$ be integers.

1. *If $\ell_d(A) \leq |A| + h$ for some $d \in G \setminus \{0\}$, $r(A, B, C) \leq r$, $|A| \geq r + 3 + h$ and $|B| \geq r + 3 + 2h$ with strict inequality in one of these estimates, and $|C| \geq r + 3$, then*

   $$\ell_d(A) \leq |A| + r + 1,\ \ell_d(B) \leq |B| + r + 1, \quad \text{and} \quad \ell_d(C) \leq |C| + r + 1.$$

2. *If $\ell_d(A) \leq |A| + h$ for some $d \in G \setminus \{0\}$, $r(A, B, C) \leq h - 1$, $h + 2 \leq |A| \leq \max\{|B|, |C|\}$, $|B|, |C| \geq h + 3$ and $35h + 10 \leq p$, then*

   $$\ell_d(B) \leq |B| + h \quad \text{and} \quad \ell_d(C) \leq |C| + h.$$

Ideas for the Proof: Fourier Analysis

- Original Idea of Freiman: Use fourier analysis on G to get a "large" subset $A' \subseteq A$ contained in an AP with length $\leq \frac{p+1}{2}$.

Ideas for the Proof: Fourier Analysis

- Original Idea of Freiman: Use fourier analysis on G to get a "large" subset $A' \subseteq A$ contained in an AP with length $\leq \frac{p+1}{2}$.
- This ensures $A' + A'$ canonically isomorphic to an integer sumset.

Ideas for the Proof: Fourier Analysis

- Original Idea of Freiman: Use fourier analysis on G to get a "large" subset $A' \subseteq A$ contained in an AP with length $\leq \frac{p+1}{2}$.
- This ensures $A' + A'$ canonically isomorphic to an integer sumset.
- Apply the $3k - 4$ Theorem in $\mathbb{Z}$ to $A' + A'$ to get A' contained in an even smaller arithmetic progression

Ideas for the Proof: Fourier Analysis

- Original Idea of Freiman: Use fourier analysis on G to get a "large" subset $A' \subseteq A$ contained in an AP with length $\leq \frac{p+1}{2}$.
- This ensures $A' + A'$ canonically isomorphic to an integer sumset.
- Apply the $3k - 4$ Theorem in $\mathbb{Z}$ to $A' + A'$ to get A' contained in an even smaller arithmetic progression
- Choose $A' \subseteq A$ maximal and show via a combinatorial argument $A' = A$ forced.

Ideas for the Proof: Fourier Analysis

- Original Idea of Freiman: Use fourier analysis on G to get a "large" subset $A' \subseteq A$ contained in an AP with length $\leq \frac{p+1}{2}$.
- This ensures $A' + A'$ canonically isomorphic to an integer sumset.
- Apply the $3k - 4$ Theorem in $\mathbb{Z}$ to $A' + A'$ to get A' contained in an even smaller arithmetic progression
- Choose $A' \subseteq A$ maximal and show via a combinatorial argument $A' = A$ forced.
- Problem 1: Simple extremal combinatorial argument for showing $A = A'$ fails at higher densities $|A + A| > \frac{p+1}{2}$.

Ideas for the Proof: Fourier Analysis

- Original Idea of Freiman: Use fourier analysis on G to get a "large" subset $A' \subseteq A$ contained in an AP with length $\leq \frac{p+1}{2}$.
- This ensures $A' + A'$ canonically isomorphic to an integer sumset.
- Apply the $3k - 4$ Theorem in $\mathbb{Z}$ to $A' + A'$ to get A' contained in an even smaller arithmetic progression
- Choose $A' \subseteq A$ maximal and show via a combinatorial argument $A' = A$ forced.
- Problem 1: Simple extremal combinatorial argument for showing $A = A'$ fails at higher densities $|A + A| > \frac{p+1}{2}$.
- Problem 2: Issues with Fourier calculation estimates when $A \neq B$ and adapting the combinatorial argument for showing $A = A'$.

Ideas for the Proof: Combinatorial Reduction

- Problem 1 resolved by Candela, González-Sánchez and G. (2022) for $A = B$ using vosper duality (i.e., additive trios).

Ideas for the Proof: Combinatorial Reduction

- Problem 1 resolved by Candela, González-Sánchez and G. (2022) for $A = B$ using vosper duality (i.e., additive trios).
- These arguments needed to be adapted from $A + A$ to $A + B$ (G. 2024)

Theorem (G. 2024)

Let p be prime, let A, $B \subseteq \mathbb{Z}/p\mathbb{Z}$ be nonempty subsets with

$$|A + B| = |A| + |B| + r \leq \frac{3}{4}(p + 1) \quad \text{and} \quad p \geq 4r + 9,$$

and set $C = -(A + B)^c$. Suppose there exist subsets $A' \subseteq A$ and $B' \subseteq B$ or $A' \subseteq B$ and $B' \subseteq A$ such that $A' + B'$ rectifies, $|B'| \leq |A'|$ and

$$|A'| + 2|B'| - 4 \geq |A + B|. \tag{1}$$

Then **Target Conclusions** *hold.*

Ideas for the Proof: Fourier Analysis

Ideas for the Proof: Fourier Analysis

- Problem 2 resolved by modifying standard fourier sum estimates for $A + A$ to improve constants for $A + B$.

Ideas for the Proof: Fourier Analysis

- Problem 2 resolved by modifying standard fourier sum estimates for $A + A$ to improve constants for $A + B$.

Definition

For $A \subseteq G = \mathbb{Z}/p\mathbb{Z}$, let $S_A(x) = \sum_{a \in A} \exp(ax/p)$, where $\exp(x) = e^{2\pi i x} \in \mathbb{C}$.

Ideas for the Proof: Fourier Analysis

- Problem 2 resolved by modifying standard fourier sum estimates for $A + A$ to improve constants for $A + B$.

Definition

For $A \subseteq G = \mathbb{Z}/p\mathbb{Z}$, let $S_A(x) = \sum_{a \in A} \exp(ax/p)$, where $\exp(x) = e^{2\pi i x} \in \mathbb{C}$.

Lemma

If $z_1, \ldots, z_N \in \mathbb{C}$ is a sequence of points lying on the complex unit circle such that every open half-arc contains at most n of the terms z_i for $i \in [1, N]$, then $|\sum_{i=1}^{N} z_i| \leq 2n - N$.

The “Base Case”

Theorem (G. 2024)

Assume **General Setup**. *Let* $\beta \in [0.731, 1]$ *and* $\alpha \in (0, 0.212]$ *be real numbers. Suppose*

$$|A + B| \le |A| + (1 + \alpha)|B| - 3 \quad \textit{and} \quad \beta|A| \le |B| \le |A| \le f(\alpha, \beta)\, p.$$

Then **Target Conclusions hold**.

Ideas for the proof: The Isoperimetric Method

- G abelian group, $B \subseteq G$ finite and nonempty, $k \geq 1$

Ideas for the proof: The Isoperimetric Method

- G abelian group, $B \subseteq G$ finite and nonempty, $k \geq 1$
- B is k-separable if there is some finite $X \subseteq G$ with

$$|X| \geq k \quad \text{and} \quad |(X+B)^{\mathsf{c}}| \geq k.$$

Ideas for the proof: The Isoperimetric Method

- G abelian group, $B \subseteq G$ finite and nonempty, $k \geq 1$
- B is k-separable if there is some finite $X \subseteq G$ with

$$|X| \geq k \quad \text{and} \quad |(X+B)^{\mathsf{c}}| \geq k.$$

- A k-**fragment** is a subset $X \subseteq G$ (satisfying above constraints) with $|X+B| - |X|$ minimal.

Ideas for the proof: The Isoperimetric Method

- G abelian group, $B \subseteq G$ finite and nonempty, $k \geq 1$
- B is k-separable if there is some finite $X \subseteq G$ with

$$|X| \geq k \quad \text{and} \quad |(X+B)^{\mathsf{c}}| \geq k.$$

- A k-**fragment** is a subset $X \subseteq G$ (satisfying above constraints) with $|X+B| - |X|$ minimal.
- A minimal cardinality k-fragment is called a k-**atom**. We will need good upper bounds for their size. (Serra and Zémor 2000, G. 2013).

Ideas for the proof: The Isoperimetric Method

- G abelian group, $B \subseteq G$ finite and nonempty, $k \geq 1$
- B is k-separable if there is some finite $X \subseteq G$ with

$$|X| \geq k \quad \text{and} \quad |(X+B)^{\mathrm{c}}| \geq k.$$

- A k-**fragment** is a subset $X \subseteq G$ (satisfying above constraints) with $|X+B| - |X|$ minimal.
- A minimal cardinality k-fragment is called a k-**atom**. We will need good upper bounds for their size. (Serra and Zémor 2000, G. 2013).
- $|A+B| = |A| + |B| + r \leq p - r - 3$ with $|B| \geq r+3$ shows B is $(r+3)$-separable.

Ideas for the proof: The Isoperimetric Method

- G abelian group, $B \subseteq G$ finite and nonempty, $k \geq 1$
- B is k-separable if there is some finite $X \subseteq G$ with

$$|X| \geq k \quad \text{and} \quad |(X+B)^{\mathrm{c}}| \geq k.$$

- A k-**fragment** is a subset $X \subseteq G$ (satisfying above constraints) with $|X+B| - |X|$ minimal.
- A minimal cardinality k-fragment is called a k-**atom**. We will need good upper bounds for their size. (Serra and Zémor 2000, G. 2013).
- $|A+B| = |A| + |B| + r \leq p - r - 3$ with $|B| \geq r+3$ shows B is $(r+3)$-separable.
- Replace A by a $(r+3)$-atom X. Then $|X+B| \leq |X| + |B| + r$ and $|X+B| \leq p - r - 3$.

Ideas for the proof: The Isoperimetric Method

- G abelian group, $B \subseteq G$ finite and nonempty, $k \geq 1$
- B is k-separable if there is some finite $X \subseteq G$ with

$$|X| \geq k \quad \text{and} \quad |(X+B)^c| \geq k.$$

- A k-**fragment** is a subset $X \subseteq G$ (satisfying above constraints) with $|X+B| - |X|$ minimal.
- A minimal cardinality k-fragment is called a k-**atom**. We will need good upper bounds for their size. (Serra and Zémor 2000, G. 2013).
- $|A+B| = |A| + |B| + r \leq p - r - 3$ with $|B| \geq r+3$ shows B is $(r+3)$-separable.
- Replace A by a $(r+3)$-atom X. Then $|X+B| \leq |X| + |B| + r$ and $|X+B| \leq p - r - 3$.
- Repeat and replace B with a $(r+3)$-atom Y for X.

Ideas for the proof: The Isoperimetric Method

- G abelian group, $B \subseteq G$ finite and nonempty, $k \geq 1$
- B is k-separable if there is some finite $X \subseteq G$ with

$$|X| \geq k \quad \text{and} \quad |(X+B)^{\mathrm{c}}| \geq k.$$

- A k-**fragment** is a subset $X \subseteq G$ (satisfying above constraints) with $|X+B| - |X|$ minimal.
- A minimal cardinality k-fragment is called a k-**atom**. We will need good upper bounds for their size. (Serra and Zémor 2000, G. 2013).
- $|A+B| = |A| + |B| + r \leq p - r - 3$ with $|B| \geq r + 3$ shows B is $(r+3)$-separable.
- Replace A by a $(r+3)$-atom X. Then $|X+B| \leq |X| + |B| + r$ and $|X+B| \leq p - r - 3$.
- Repeat and replace B with a $(r+3)$-atom Y for X.
- Strengthen the hypotheses and use $9(r+3)$-atoms instead. Then $X+Y$ satisfies the "base case" result hypotheses (calculation).

Ideas for the proof: The Isoperimetric Method

- G abelian group, $B \subseteq G$ finite and nonempty, $k \geq 1$
- B is k-separable if there is some finite $X \subseteq G$ with

$$|X| \geq k \quad \text{and} \quad |(X+B)^{\mathrm{c}}| \geq k.$$

- A k-**fragment** is a subset $X \subseteq G$ (satisfying above constraints) with $|X+B| - |X|$ minimal.
- A minimal cardinality k-fragment is called a k-**atom**. We will need good upper bounds for their size. (Serra and Zémor 2000, G. 2013).
- $|A+B| = |A| + |B| + r \leq p - r - 3$ with $|B| \geq r + 3$ shows B is $(r+3)$-separable.
- Replace A by a $(r+3)$-atom X. Then $|X+B| \leq |X| + |B| + r$ and $|X+B| \leq p - r - 3$.
- Repeat and replace B with a $(r+3)$-atom Y for X.
- Strengthen the hypotheses and use $9(r+3)$-atoms instead. Then $X+Y$ satisfies the "base case" result hypotheses (calculation).
- Used Huichochea reduction argument transfers desired structure back to A, B and C.

Near Optimal Density

Theorem (G. 2024)

Assume **General Setup**. *If*

$$|A+B| \leq (|A|+|B|) + \frac{1}{9}|B| - 3 \quad \textit{and} \quad |A+B| \leq p - 29(r+3),$$

then **Target Conclusions** *hold.*

Moving from near-optimal to optimal density

- Replace B by a $(r + 3)$-atom X.

Moving from near-optimal to optimal density

- Replace B by a $(r+3)$-atom X.
- Then $|A+X| \leq |A| + |X| + r$ and $|X| \lesssim 3.077(r+3)$

Moving from near-optimal to optimal density

- Replace B by a $(r+3)$-atom X.
- Then $|A+X| \leq |A|+|X|+r$ and $|X| \lesssim 3.077(r+3)$

Theorem (Ruzsa-Plünnecke Bounds)

Let G be an abelian group, let $A, B \subseteq G$ be finite, nonempty subsets and let $A' \subseteq A$ be a nonempty subset attaining the minimum

$$\alpha := \min\left\{\frac{|A'+B|}{|A'|} : \emptyset \neq A' \subseteq A\right\} \leq \frac{|A+B|}{|A|}.$$

Then $|A'+nB| \leq \alpha^n|A'| \leq \alpha^n|A|$ for all $n \geq 0$.

Moving from near-optimal to optimal density

- Replace B by a $(r+3)$-atom X.
- Then $|A+X| \leq |A|+|X|+r$ and $|X| \lesssim 3.077(r+3)$

Theorem (Ruzsa-Plünnecke Bounds)

Let G be an abelian group, let $A, B \subseteq G$ be finite, nonempty subsets and let $A' \subseteq A$ be a nonempty subset attaining the minimum

$$\alpha := \min\left\{\frac{|A'+B|}{|A'|} : \emptyset \neq A' \subseteq A\right\} \leq \frac{|A+B|}{|A|}.$$

Then $|A'+nB| \leq \alpha^n|A'| \leq \alpha^n|A|$ for all $n \geq 0$.

- Apply Ruzsa-Plünnecke and Vosper's Theorem to estimate $|A'+nX|$:

$$|A'+nX| \leq |A'|+(|A'|/|A|)n(|X|+r)\Big(1+0.01434\cdot n\Big) \quad \text{for all } n \in [2,8].$$

Moving from near-optimal to optimal density

- Replace B by a $(r+3)$-atom X.
- Then $|A+X| \le |A| + |X| + r$ and $|X| \lesssim 3.077(r+3)$

Theorem (Ruzsa-Plünnecke Bounds)

Let G be an abelian group, let A, $B \subseteq G$ be finite, nonempty subsets and let $A' \subseteq A$ be a nonempty subset attaining the minimum

$$\alpha := \min\left\{\frac{|A'+B|}{|A'|} : \emptyset \neq A' \subseteq A\right\} \le \frac{|A+B|}{|A|}.$$

Then $|A'+nB| \le \alpha^n |A'| \le \alpha^n |A|$ for all $n \ge 0$.

- Apply Ruzsa-Plünnecke and Vosper's Theorem to estimate $|A'+nX|$:

  $$|A'+nX| \le |A'| + (|A'|/|A|)n(|X|+r)\Big(1+0.01434\cdot n\Big) \quad \text{for all } n \in [2,8].$$

- If A' contained in short AP, then apply Huicochea to $A'+X$, then to $A+X$, then to $A+B$ to get A, B and C all in short AP's.

Moving from near-optimal to optimal density

- Replace B by a $(r+3)$-atom X.
- Then $|A+X| \leq |A|+|X|+r$ and $|X| \lesssim 3.077(r+3)$

Theorem (Ruzsa-Plünnecke Bounds)

Let G be an abelian group, let A, $B \subseteq G$ be finite, nonempty subsets and let $A' \subseteq A$ be a nonempty subset attaining the minimum

$$\alpha := \min\left\{\frac{|A'+B|}{|A'|} : \emptyset \neq A' \subseteq A\right\} \leq \frac{|A+B|}{|A|}.$$

Then $|A'+nB| \leq \alpha^n|A'| \leq \alpha^n|A|$ for all $n \geq 0$.

- Apply Ruzsa-Plünnecke and Vosper's Theorem to estimate $|A'+nX|$:

$$|A'+nX| \leq |A'|+(|A'|/|A|)n(|X|+r)\Big(1+0.01434\cdot n\Big) \quad \text{for all } n \in [2,8].$$

- If A' contained in short AP, then apply Huicochea to $A'+X$, then to $A+X$, then to $A+B$ to get A, B and C all in short AP's.
- Use near-ideal density result on $A'+nX$ to improve lower bound for $|A'+nX|$, thus improving upper bound for $|nX|$:

$$|A'+nX| > |A'| + \frac{10}{9}|nX| - 3$$

Moving from near-optimal to optimal density

- Apply Lev-Shkredov Result (modified doubling constant ~ 2.55) to $X + X$ or $4X = 2X + 2X$ or $8X = 4X + 4X$.

Moving from near-optimal to optimal density

- Apply Lev-Shkredov Result (modified doubling constant ~ 2.55) to $X + X$ or $4X = 2X + 2X$ or $8X = 4X + 4X$.
- Upper bound for $8X$ ensures that we can apply this result to at least one of these sumsets (long calculation).

Moving from near-optimal to optimal density

- Apply Lev-Shkredov Result (modified doubling constant ~ 2.55) to $X + X$ or $4X = 2X + 2X$ or $8X = 4X + 4X$.
- Upper bound for $8X$ ensures that we can apply this result to at least one of these sumsets (long calculation).
- Conclusion implies $\ell_d(2X) < \frac{p}{2}$, so $2X + 2X$ isomorphic to integer sumset

Moving from near-optimal to optimal density

- Apply Lev-Shkredov Result (modified doubling constant ~ 2.55) to $X + X$ or $4X = 2X + 2X$ or $8X = 4X + 4X$.
- Upper bound for $8X$ ensures that we can apply this result to at least one of these sumsets (long calculation).
- Conclusion implies $\ell_d(2X) < \frac{p}{2}$, so $2X + 2X$ isomorphic to integer sumset
- We now apply the integer version of the $3k - 4$ to $X + X$ and $2X + 2X$.

Moving from near-optimal to optimal density

- Apply Lev-Shkredov Result (modified doubling constant ~ 2.55) to $X+X$ or $4X = 2X+2X$ or $8X = 4X+4X$.
- Upper bound for $8X$ ensures that we can apply this result to at least one of these sumsets (long calculation).
- Conclusion implies $\ell_d(2X) < \frac{p}{2}$, so $2X+2X$ isomorphic to integer sumset
- We now apply the integer version of the $3k-4$ to $X+X$ and $2X+2X$.
- If $|X+X| < 3|X|-3$, we apply huicochea to $X+A$ then $A+B$ to complete the proof. Thus

$$|2X| \geq 2|X| - 3$$

.

Moving from near-optimal to optimal density

- Apply Lev-Shkredov Result (modified doubling constant ~ 2.55) to $X + X$ or $4X = 2X + 2X$ or $8X = 4X + 4X$.
- Upper bound for $8X$ ensures that we can apply this result to at least one of these sumsets (long calculation).
- Conclusion implies $\ell_d(2X) < \frac{p}{2}$, so $2X + 2X$ isomorphic to integer sumset
- We now apply the integer version of the $3k - 4$ to $X + X$ and $2X + 2X$.
- If $|X + X| < 3|X| - 3$, we apply huicochea to $X + A$ then $A + B$ to complete the proof. Thus

$$|2X| \geq 2|X| - 3$$

.

- Repeat for $4X = 2X + 2X$ to get improved lower bound for $|4X|$.

Moving from near-optimal to optimal density

- Apply Lev-Shkredov Result (modified doubling constant ~ 2.55) to $X+X$ or $4X = 2X+2X$ or $8X = 4X+4X$.
- Upper bound for $8X$ ensures that we can apply this result to at least one of these sumsets (long calculation).
- Conclusion implies $\ell_d(2X) < \frac{p}{2}$, so $2X+2X$ isomorphic to integer sumset
- We now apply the integer version of the $3k-4$ to $X+X$ and $2X+2X$.
- If $|X+X| < 3|X|-3$, we apply huicochea to $X+A$ then $A+B$ to complete the proof. Thus

$$|2X| \geq 2|X| - 3$$

.

- Repeat for $4X = 2X+2X$ to get improved lower bound for $|4X|$.
- Compare with upper bound, and obtain a contradiction.

Thanks!