Small Sumsets Modulo p

David J. Grynkiewicz

University of Memphis

July 18, 2025

Sumsets

Let G be an abelian group.

Definition

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

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

$3k - 4$ 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

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

$3k - 4$ 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

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

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

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

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 $|A+B| = |A| + |B| + r$.

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 $X \in \{A, B, C\}$.

- Note: $C \subseteq P_C$ with $|P_C| \leq |C| + r + 1$ is equivalent to $P_{A+B} := -(P_C)^{\mathrm{c}} \subseteq A + B$ with $|P_{A+B}| \geq |A| + |B| - 1$

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 $X \in \{A, B, C\}$.

- Note: $C \subseteq P_C$ with $|P_C| \leq |C| + r + 1$ is equivalent to $P_{A+B} := -(P_C)^c \subseteq A + B$ with $|P_{A+B}| \geq |A| + |B| - 1$

Conjecture

Assume **General Setup**. *If*

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

Small Doubling + *Low Density*,

then **Target Conclusions** *hold.*

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

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

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 $|A+B| \le p-r-3$ 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 $\alpha' = \alpha$.

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 it's 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 it's 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 with $\alpha = 1$ 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 with $\alpha = 1$ follow from more general "rectification" principles.
- $|A \cup B| \leq \log_4 p \quad \longrightarrow \quad$ 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

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

- "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), Candela, González-Sánchez and G. (2022)
  - $|A+A| \leq 2|A| + (0.4)|A| - 3$ 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 $10 \leq |A| < (0.00000125)p$
  - $|A+A| \leq 2|A| + (0.136)|A| - 3$ and $|A+A| \leq (0.75)p$

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), Candela, González-Sánchez and G. (2022)
  - $|A+A| \leq 2|A| + (0.4)|A| - 3$ 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 $10 \leq |A| < (0.00000125)p$
  - $|A+A| \leq 2|A| + (0.136)|A| - 3$ and $|A+A| \leq (0.75)p$
- $(0.001)|A|^{2/3} \leq |B| \leq |A|, \quad |A+B| \leq (|A|+|B|) + (0.03)|B|$ and $|A| < (0.0045)p \quad \longrightarrow \quad$ Huichochea (2022)

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* $|A| \geq 4$, $p > 2^{94}$,

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

then **Target Conclusions** *hold.*

Theorem (G. 2025)

Assume **General Setup**. *If*

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

then **Target Conclusions** *hold.*

Ideas for the Proof

Ideas for the Proof

- Additive Trio Formulation of DeVos (2015)

Ideas for the Proof

- Additive Trio Formulation of DeVos (2015)
- (modified) transfer argument of Huicochea (2017): If one of the sets A, B or C is a 'moderately' small subset of an arithmetic progression, then all three sets are very small subsets of arithmetic progressions with the same difference

Ideas for the Proof

- Additive Trio Formulation of DeVos (2015)
- (modified) transfer argument of Huicochea (2017): If one of the sets A, B or C is a 'moderately' small subset of an arithmetic progression, then all three sets are very small subsets of arithmetic progressions with the same difference
- $\log_2(A \cup B)$ density results: to handle small p

Ideas for the Proof

- Additive Trio Formulation of DeVos (2015)
- (modified) transfer argument of Huicochea (2017): If one of the sets A, B or C is a 'moderately' small subset of an arithmetic progression, then all three sets are very small subsets of arithmetic progressions with the same difference
- $\log_2(A \cup B)$ density results: to handle small p
- Freiman's original Fourier sum estimate: new variation better adapted for $A + B$ rather than $A + A$. Base Case.

Ideas for the Proof

- Additive Trio Formulation of DeVos (2015)
- (modified) transfer argument of Huicochea (2017): If one of the sets A, B or C is a 'moderately' small subset of an arithmetic progression, then all three sets are very small subsets of arithmetic progressions with the same difference
- $\log_2(A \cup B)$ density results: to handle small p
- Freiman's original Fourier sum estimate: new variation better adapted for $A + B$ rather than $A + A$. Base Case.
- Combinatorial Reduction Argument of Candela, González-Sánchez and G. (2022): extended from $A + A$ to $A + B$.

Ideas for the Proof

- Additive Trio Formulation of DeVos (2015)
- (modified) transfer argument of Huicochea (2017): If one of the sets A, B or C is a 'moderately' small subset of an arithmetic progression, then all three sets are very small subsets of arithmetic progressions with the same difference
- $\log_2(A \cup B)$ density results: to handle small p
- Freiman's original Fourier sum estimate: new variation better adapted for $A + B$ rather than $A + A$. Base Case.
- Combinatorial Reduction Argument of Candela, González-Sánchez and G. (2022): extended from $A + A$ to $A + B$.
- Hamidoune's Isoperimetric method: Inductive Step

Ideas for the Proof

- Additive Trio Formulation of DeVos (2015)
- (modified) transfer argument of Huicochea (2017): If one of the sets A, B or C is a 'moderately' small subset of an arithmetic progression, then all three sets are very small subsets of arithmetic progressions with the same difference
- $\log_2(A \cup B)$ density results: to handle small p
- Freiman's original Fourier sum estimate: new variation better adapted for $A + B$ rather than $A + A$. Base Case.
- Combinatorial Reduction Argument of Candela, González-Sánchez and G. (2022): extended from $A + A$ to $A + B$.
- Hamidoune's Isoperimetric method: Inductive Step
- Improved estimates for the size of an atom (G. 2013, Serra and Zémor 2000)

Ideas for the Proof

- Additive Trio Formulation of DeVos (2015)
- (modified) transfer argument of Huicochea (2017): If one of the sets A, B or C is a 'moderately' small subset of an arithmetic progression, then all three sets are very small subsets of arithmetic progressions with the same difference
- $\log_2(A \cup B)$ density results: to handle small p
- Freiman's original Fourier sum estimate: new variation better adapted for $A + B$ rather than $A + A$. Base Case.
- Combinatorial Reduction Argument of Candela, González-Sánchez and G. (2022): extended from $A + A$ to $A + B$.
- Hamidoune's Isoperimetric method: Inductive Step
- Improved estimates for the size of an atom (G. 2013, Serra and Zémor 2000)
- (modified) 'mid-range' version of Lev and Shkredov (2020)

Ideas for the Proof

- Additive Trio Formulation of DeVos (2015)
- (modified) transfer argument of Huicochea (2017): If one of the sets A, B or C is a 'moderately' small subset of an arithmetic progression, then all three sets are very small subsets of arithmetic progressions with the same difference
- $\log_2(A \cup B)$ density results: to handle small p
- Freiman's original Fourier sum estimate: new variation better adapted for $A + B$ rather than $A + A$. Base Case.
- Combinatorial Reduction Argument of Candela, González-Sánchez and G. (2022): extended from $A + A$ to $A + B$.
- Hamidoune's Isoperimetric method: Inductive Step
- Improved estimates for the size of an atom (G. 2013, Serra and Zémor 2000)
- (modified) 'mid-range' version of Lev and Shkredov (2020)
- Ruzsa-Plünnecke Bounds (1989) as used by Serra and Zémor (2009)

Ideas for the Proof

- Additive Trio Formulation of DeVos (2015)
- (modified) transfer argument of Huicochea (2017): If one of the sets A, B or C is a 'moderately' small subset of an arithmetic progression, then all three sets are very small subsets of arithmetic progressions with the same difference
- $\log_2(A \cup B)$ density results: to handle small p
- Freiman's original Fourier sum estimate: new variation better adapted for $A + B$ rather than $A + A$. Base Case.
- Combinatorial Reduction Argument of Candela, González-Sánchez and G. (2022): extended from $A + A$ to $A + B$.
- Hamidoune's Isoperimetric method: Inductive Step
- Improved estimates for the size of an atom (G. 2013, Serra and Zémor 2000)
- (modified) 'mid-range' version of Lev and Shkredov (2020)
- Ruzsa-Plünnecke Bounds (1989) as used by Serra and Zémor (2009)
- Lengthy Calculations...

Thanks!