Going beyond 2.4 in Freiman's 2.4k-Theorem

Pablo Candela Oriol Serra **Christoph Spiegel**

CANT 2018

New York, May 2018

The City University of New York
UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH
BGSMath BARCELONA GRADUATE SCHOOL OF MATHEMATICS

The sumset

Definition

Given a set $A \subset G$ in some additive group G, we define its *sumset* as

$$A + A = 2A = \{a + a' : a, a' \in A\} \subset G. \quad (1)$$

The sumset

Definition

Given a set $A \subset G$ in some additive group G, we define its *sumset* as

$$A + A = 2A = \{a + a' : a, a' \in A\} \subset G. \tag{1}$$

This should not be confused with the dilate $2 \cdot A = \{2a : a \in A\}$.

The sumset

Definition

Given a set $A \subset G$ in some additive group G, we define its *sumset* as

$$A + A = 2A = \{a + a' : a, a' \in A\} \subset G. \quad (1)$$

This should not be confused with the dilate $2 \cdot A = \{2a : a \in A\}$.

Example

Consider the following two sets of size k:

The sumset

Definition

Given a set $A \subset G$ in some additive group G, we define its *sumset* as

$$A + A = 2A = \{a + a' : a, a' \in A\} \subset G. \quad (1)$$

This should not be confused with the dilate $2 \cdot A = \{2a : a \in A\}$.

Example

Consider the following two sets of size k:

1. For $A = \{0, \ldots, k-1\} \subset \mathbb{Z}$ we have $|2A| = 2k - 1$.

The sumset

Definition

Given a set $A \subset G$ in some additive group G, we define its *sumset* as

$$A + A = 2A = \{a + a' : a, a' \in A\} \subset G. \tag{1}$$

This should not be confused with the dilate $2 \cdot A = \{2a : a \in A\}$.

Example

Consider the following two sets of size k:

1. For $A = \{0, \dots, k-1\} \subset \mathbb{Z}$ we have $|2A| = 2k - 1$.
2. For $A = \{0, 1, 2, 4, \dots, 2^{k-2}\} \subset \mathbb{Z}$ we have $|2A| = \binom{k}{2} + 2$.

The sumset

Definition

Given a set $A \subset G$ in some additive group G, we define its *sumset* as

$$A + A = 2A = \{a + a' : a, a' \in A\} \subset G. \tag{1}$$

This should not be confused with the dilate $2 \cdot A = \{2a : a \in A\}$.

Example

Consider the following two sets of size k:

1. For $A = \{0, \ldots, k-1\} \subset \mathbb{Z}$ we have $|2A| = 2k - 1$.
2. For $A = \{0, 1, 2, 4, \ldots, 2^{k-2}\} \subset \mathbb{Z}$ we have $|2A| = \binom{k}{2} + 2$.

Inverse Problems: We are interested in understanding the structure of A when the *doubling* $|2A|/|A|$ is small.

Some classic results

Proposition

Any set $A \subset \mathbb{Z}$ *satisfies* $|2A| \geq 2|A| - 1$.

Some classic results

Proposition

Any set $A \subset \mathbb{Z}$ *satisfies* $|2A| \geq 2|A| - 1$. *Equality holds if and only if* A *is an arithmetic progression.*

Some classic results

Proposition

Any set $A \subset \mathbb{Z}$ satisfies $|2A| \geq 2|A| - 1$. Equality holds if and only if A is an arithmetic progression.

Theorem (Davenport '35; Cauchy 1813)

Any set $\mathcal{A} \subseteq \mathbb{Z}_p$ satisfies $|2\mathcal{A}| \geq \min(2|\mathcal{A}| - 1, p)$.

Some classic results

Proposition

Any set $A \subset \mathbb{Z}$ *satisfies* $|2A| \geq 2|A| - 1$. *Equality holds if and only if* A *is an arithmetic progression.*

Theorem (Davenport '35; Cauchy 1813)

Any set $\mathcal{A} \subseteq \mathbb{Z}_p$ *satisfies* $|2\mathcal{A}| \geq \min(2|\mathcal{A}| - 1, p)$.

Theorem (Vosper '56)

Any set $\mathcal{A} \subseteq \mathbb{Z}_p$ *satisfying* $|\mathcal{A}| \geq 2$ *and* $|2\mathcal{A}| = 2|\mathcal{A}| - 1 \leq p - 2$ *must be an arithmetic progression.*

Some classic results

Proposition

Any set $A \subset \mathbb{Z}$ satisfies $|2A| \geq 2|A| - 1$. Equality holds if and only if A is an arithmetic progression.

Theorem (Davenport '35; Cauchy 1813)

Any set $\mathcal{A} \subseteq \mathbb{Z}_p$ satisfies $|2\mathcal{A}| \geq \min(2|\mathcal{A}| - 1, p)$.

Theorem (Vosper '56)

Any set $\mathcal{A} \subseteq \mathbb{Z}_p$ satisfying $|\mathcal{A}| \geq 2$ and $|2\mathcal{A}| = 2|\mathcal{A}| - 1 \leq p - 2$ must be an arithmetic progression.

Theorem (Kneser '53)

Any set $\mathcal{A} \subseteq \mathbb{Z}_n$ satisfies $|2\mathcal{A}| \geq 2|\mathcal{A} + H| - |H|$ where $H = \{x \in \mathbb{Z}_n : x + 2\mathcal{A} \subset 2\mathcal{A}\}$ is the stabilizer of the sumset.

Some classic results

Proposition

Any set $A \subset \mathbb{Z}$ *satisfies* $|2A| \geq 2|A| - 1$. *Equality holds if and only if* A *is an arithmetic progression.*

Theorem (Davenport '35; Cauchy 1813)

Any set $\mathcal{A} \subseteq \mathbb{Z}_p$ *satisfies* $|2\mathcal{A}| \geq \min(2|\mathcal{A}| - 1, p)$.

Theorem (Vosper '56)

Any set $\mathcal{A} \subseteq \mathbb{Z}_p$ *satisfying* $|\mathcal{A}| \geq 2$ *and* $|2\mathcal{A}| = 2|\mathcal{A}| - 1 \leq p - 2$ *must be an arithmetic progression.*

Theorem (Kneser '53)

Any set $\mathcal{A} \subseteq \mathbb{Z}_n$ *satisfies* $|2\mathcal{A}| \geq 2|\mathcal{A} + H| - |H|$ *where* $H = \{x \in \mathbb{Z}_n : x + 2\mathcal{A} \subset 2\mathcal{A}\}$ *is the stabilizer of the sumset.*

The corresponding inverse statement is due to Kemperman '60.

Freiman's $3k - 4$ Theorem in $\mathbb{Z}$

Theorem (Freiman '66)

Any set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3|A| - 4$ is contained in an arithmetic progression of size at most $|2A| - |A| + 1$.

Freiman's $3k-4$ Theorem in $\mathbb{Z}$

Theorem (Freiman '66)

Any set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3|A| - 4$ is contained in an arithmetic progression of size at most $|2A| - |A| + 1$.

Proof due to Lev and Smeliansky '95.

Freiman's $3k-4$ Theorem in $\mathbb{Z}$

Theorem (Freiman '66)

Any set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3|A| - 4$ is contained in an arithmetic progression of size at most $|2A| - |A| + 1$.

Proof due to Lev and Smeliansky '95.

1. Normalize A, that is consider $\big(A - \min(A)\big) / \gcd\big(A - \min(A)\big)$.

Freiman's $3k - 4$ Theorem in $\mathbb{Z}$

Theorem (Freiman '66)

Any set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3|A| - 4$ is contained in an arithmetic progression of size at most $|2A| - |A| + 1$.

Proof due to Lev and Smeliansky '95.

1. Normalize A, that is consider $\big(A - \min(A)\big)/\gcd\big(A - \min(A)\big)$.
2. To simplify the proof, assume that $a = \max(A)$ is prime.

Freiman's $3k-4$ Theorem in $\mathbb{Z}$

Theorem (Freiman '66)

Any set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3|A| - 4$ is contained in an arithmetic progression of size at most $|2A| - |A| + 1$.

Proof due to Lev and Smeliansky '95.

1. Normalize A, that is consider $\big(A - \min(A)\big)/\gcd\big(A - \min(A)\big)$.
2. To simplify the proof, assume that $a = \max(A)$ is prime.
3. Let $\mathcal{A}$ denote the canonical projection of A into $\mathbb{Z}_a$.

Freiman's $3k-4$ Theorem in $\mathbb{Z}$

Theorem (Freiman '66)

Any set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3|A|-4$ is contained in an arithmetic progression of size at most $|2A|-|A|+1$.

Proof due to Lev and Smeliansky '95.

1. Normalize A, that is consider $\big(A-\min(A)\big)/\gcd\big(A-\min(A)\big)$.
2. To simplify the proof, assume that $a = \max(A)$ is prime.
3. Let $\mathcal{A}$ denote the canonical projection of A into $\mathbb{Z}_a$.
4. $|2A| = |2\mathcal{A}| + \#\big\{x \in [0,a) : x, a+x \in 2A\big\} + 1 \geq |2\mathcal{A}| + |A|$.

Freiman's $3k-4$ Theorem in $\mathbb{Z}$

Theorem (Freiman '66)

Any set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3|A| - 4$ is contained in an arithmetic progression of size at most $|2A| - |A| + 1$.

Proof due to Lev and Smeliansky '95.

1. Normalize A, that is consider $\big(A - \min(A)\big)/\gcd\big(A - \min(A)\big)$.
2. To simplify the proof, assume that $a = \max(A)$ is prime.
3. Let $\mathcal{A}$ denote the canonical projection of A into $\mathbb{Z}_a$.
4. $|2A| = |2\mathcal{A}| + \#\big\{x \in [0,a) : x, a+x \in 2A\big\} + 1 \geq |2\mathcal{A}| + |A|$.
5. If $|2\mathcal{A}| = \max(A)$ we are done. If not, then Cauchy-Davenport gives us the contradiction $|2A| \geq 2|\mathcal{A}| - 1 + |A| = 3|A| - 3$. □

Freiman's $3k - 4$ Theorem in $\mathbb{Z}$

Theorem (Freiman '66)

Any set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3|A| - 4$ is contained in an arithmetic progression of size at most $|2A| - |A| + 1$.

Proof due to Lev and Smeliansky '95.

1. Normalize A, that is consider $\big(A - \min(A)\big) / \gcd\big(A - \min(A)\big)$.
2. To simplify the proof, assume that $a = \max(A)$ is prime.
3. Let $\mathcal{A}$ denote the canonical projection of A into $\mathbb{Z}_a$.
4. $|2A| = |2\mathcal{A}| + \#\big\{x \in [0, a) : x, a + x \in 2A\big\} + 1 \geq |2\mathcal{A}| + |A|$.
5. If $|2\mathcal{A}| = \max(A)$ we are done. If not, then Cauchy-Davenport gives us the contradiction $|2A| \geq 2|\mathcal{A}| - 1 + |A| = 3|A| - 3$. $\square$

Example

For $k \geq 3$ and $x > 2(k-2)$ the sets $A_x = \{0, \ldots, k-2\} \cup \{x\}$ all satisfy $|2A_x| = 3|A_x| - 3$ but require arbitrarily large APs to be covered.

Obtaining an analogue in $\mathbb{Z}_p$

A similar result is conjectured to hold in $\mathbb{Z}_p$.

Obtaining an analogue in $\mathbb{Z}_p$

A similar result is conjectured to hold in $\mathbb{Z}_p$.

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$ as well as _________ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Obtaining an analogue in $\mathbb{Z}_p$

A similar result is conjectured to hold in $\mathbb{Z}_p$.

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$ as well as _________ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Corollary to Green, Ruzsa '06 $|\mathcal{A}| \leq p/10^{250}$

Obtaining an analogue in $\mathbb{Z}_p$

A similar result is conjectured to hold in $\mathbb{Z}_p$.

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$ as well as ________ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Corollary to Green, Ruzsa '06 $|\mathcal{A}| \leq p/10^{250}$

Serra, Zémor '08 $|2\mathcal{A}| \leq (2+\epsilon)|\mathcal{A}| - 4$ and $|2\mathcal{A}| \leq p - \left(|2\mathcal{A}| - 2|\mathcal{A}| + 1\right)$

Obtaining an analogue in $\mathbb{Z}_p$

A similar result is conjectured to hold in $\mathbb{Z}_p$.

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$ as well as ________ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Corollary to Green, Ruzsa '06 $|\mathcal{A}| \leq p/10^{250}$

Serra, Zémor '08 $|2\mathcal{A}| \leq (2+\epsilon)|\mathcal{A}| - 4$ and $|2\mathcal{A}| \leq p - \big(|2\mathcal{A}| - 2|\mathcal{A}| + 1\big)$

Freiman '66 $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/35$

Obtaining an analogue in $\mathbb{Z}_p$

A similar result is conjectured to hold in $\mathbb{Z}_p$.

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$ as well as _________ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Corollary to Green, Ruzsa '06 $|\mathcal{A}| \leq p/10^{250}$

Serra, Zémor '08 $|2\mathcal{A}| \leq (2+\epsilon)|\mathcal{A}| - 4$ and $|2\mathcal{A}| \leq p - \big(|2\mathcal{A}| - 2|\mathcal{A}| + 1\big)$

Freiman '66 $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/35$

Rødseth '06 $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/10.7$

Obtaining an analogue in $\mathbb{Z}_p$

A similar result is conjectured to hold in $\mathbb{Z}_p$.

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$ as well as _________ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Corollary to Green, Ruzsa '06 $|\mathcal{A}| \leq p/10^{250}$

Serra, Zémor '08 $|2\mathcal{A}| \leq (2+\epsilon)|\mathcal{A}| - 4$ and $|2\mathcal{A}| \leq p - \big(|2\mathcal{A}| - 2|\mathcal{A}| + 1\big)$

Freiman '66 $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/35$

Rødseth '06 $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/10.7$

Candela, Serra, S. '18+ $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ and $|\mathcal{A}| \leq p/10^{10}$

Obtaining an analogue in $\mathbb{Z}_p$

A similar result is conjectured to hold in $\mathbb{Z}_p$.

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$ as well as __________ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Corollary to Green, Ruzsa '06 $|\mathcal{A}| \leq p/10^{250}$

Serra, Zémor '08 $|2\mathcal{A}| \leq (2+\epsilon)|\mathcal{A}| - 4$ and $|2\mathcal{A}| \leq p - \left(|2\mathcal{A}| - 2|\mathcal{A}| + 1\right)$

Freiman '66 $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/35$

Rødseth '06 $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/10.7$

Candela, Serra, S. '18+ $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ and $|\mathcal{A}| \leq p/10^{10}$

All but the second result use *rectification*, that is they Freiman-isomorphically map (part of) the set into the integers.

Proof outline of Freiman's $2.4k$-Theorem

Theorem (Freiman '66)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/35$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

Proof outline of Freiman's $2.4k$-Theorem

Theorem (Freiman '66)

Any set $\mathcal{A} \subset \mathbb{Z}$ *satisfying* $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ *and* $|\mathcal{A}| \leq p/35$ *is contained in an arithmetic progression of size at most* $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

1. Show that a small sumset implies a large Fourier coefficient of the indicator function $\mathbb{1}_{\mathcal{A}}$.

Proof outline of Freiman's $2.4k$-Theorem

Theorem (Freiman '66)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/35$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

1. Show that a small sumset implies a large Fourier coefficient of the indicator function $\mathbb{1}_{\mathcal{A}}$.
2. As a consequence of this large Fourier coefficient, one can *rectify* a large part $\mathcal{A}'$ of the set $\mathcal{A}$. Call the result of that rectification A'.

Proof outline of Freiman's $2.4k$-Theorem

Theorem (Freiman '66)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/35$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

1. Show that a small sumset implies a large Fourier coefficient of the indicator function $\mathbb{1}_{\mathcal{A}}$.
2. As a consequence of this large Fourier coefficient, one can *rectify* a large part $\mathcal{A}'$ of the set $\mathcal{A}$. Call the result of that rectification A'.
3. Apply the $3k - 4$-Theorem to that part A', obtaining an efficient covering of both A' and $\mathcal{A}'$ through an AP with some step size d.

Proof outline of Freiman's $2.4k$-Theorem

Theorem (Freiman '66)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/35$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

1. Show that a small sumset implies a large Fourier coefficient of the indicator function $\mathbb{1}_{\mathcal{A}}$.
2. As a consequence of this large Fourier coefficient, one can *rectify* a large part $\mathcal{A}'$ of the set $\mathcal{A}$. Call the result of that rectification A'.
3. Apply the $3k - 4$-Theorem to that part A', obtaining an efficient covering of both A' and $\mathcal{A}'$ through an AP with some step size d.
4. Shrink $\mathcal{A}'$ into a small segment in $\mathbb{Z}_p$ by dilating $\mathcal{A}$ by d^{-1}.

Proof outline of Freiman's $2.4k$-Theorem

Theorem (Freiman '66)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/35$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

1. Show that a small sumset implies a large Fourier coefficient of the indicator function $\mathbb{1}_{\mathcal{A}}$.
2. As a consequence of this large Fourier coefficient, one can *rectify* a large part $\mathcal{A}'$ of the set $\mathcal{A}$. Call the result of that rectification A'.
3. Apply the $3k - 4$-Theorem to that part A', obtaining an efficient covering of both A' and $\mathcal{A}'$ through an AP with some step size d.
4. Shrink $\mathcal{A}'$ into a small segment in $\mathbb{Z}_p$ by dilating $\mathcal{A}$ by d^{-1}.
5. Using the cardinality of $2\mathcal{A}$, argue that some $p/2$-segment of $\mathbb{Z}_p$ is free of elements of $\mathcal{A}$. Hence all of $\mathcal{A}$ can be rectified.

Proof outline of Freiman's $2.4k$-Theorem

Theorem (Freiman '66)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.4|\mathcal{A}| - 3$ and $|\mathcal{A}| \leq p/35$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

1. Show that a small sumset implies a large Fourier coefficient of the indicator function $\mathbb{1}_{\mathcal{A}}$.
2. As a consequence of this large Fourier coefficient, one can *rectify* a large part $\mathcal{A}'$ of the set $\mathcal{A}$. Call the result of that rectification A'.
3. Apply the $3k-4$-Theorem to that part A', obtaining an efficient covering of both A' and $\mathcal{A}'$ through an AP with some step size d.
4. Shrink $\mathcal{A}'$ into a small segment in $\mathbb{Z}_p$ by dilating $\mathcal{A}$ by d^{-1}.
5. Using the cardinality of $2\mathcal{A}$, argue that some $p/2$-segment of $\mathbb{Z}_p$ is free of elements of $\mathcal{A}$. Hence all of $\mathcal{A}$ can be rectified.
6. Apply the $3k-4$-Theorem to all of $\mathcal{A}$, obtaining the covering. $\square$

Proof outline of our result

Theorem (Candela, Serra, S. '18+)

Any set $\mathcal{A} \subset \mathbb{Z}$ *satisfying* $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ *and* $|\mathcal{A}| \leq p/10^{10}$ *is contained in an arithmetic progression of size at most* $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof outline of our result

Theorem (Candela, Serra, S. '18+)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ and $|\mathcal{A}| \leq p/10^{10}$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

$\mathbb{Z}_n$	*modular reduction*	$\mathbb{Z}$	*rectification*	$\mathbb{Z}_p$

Proof outline of our result

Theorem (Candela, Serra, S. '18+)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ and $|\mathcal{A}| \leq p/10^{10}$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

$\mathbb{Z}_n$	*modular reduction*	$\mathbb{Z}$	*rectification*	$\mathbb{Z}_p$
'2k-1 Theorem' *Kneser '53*	$\rightarrow$	3k-4 Theorem *Freiman '66* *Lev, Smeliansky '95*	$\rightarrow$	2.4k-3 Theorem *Freiman '66*

Proof outline of our result

Theorem (Candela, Serra, S. '18+)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ and $|\mathcal{A}| \leq p/10^{10}$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

$\mathbb{Z}_n$	*modular reduction*	$\mathbb{Z}$	*rectification*	$\mathbb{Z}_p$
'2k-1 Theorem' *Kneser '53*	$\rightarrow$	3k-4 Theorem *Freiman '66* *Lev, Smeliansky '95*	$\rightarrow$	2.4k-3 Theorem *Freiman '66*
2.04k Theorem *Freiman, Deshoullier '03*				

Proof outline of our result

Theorem (Candela, Serra, S. ’18+)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ and $|\mathcal{A}| \leq p/10^{10}$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

$\mathbb{Z}_n$	*modular reduction*	$\mathbb{Z}$	*rectification*	$\mathbb{Z}_p$
‘2k-1 Theorem’ *Kneser ’53*	$\to$	3k-4 Theorem *Freiman ’66* *Lev, Smeliansky ’95*	$\to$	2.4k-3 Theorem *Freiman ’66*
2.04k Theorem *Freiman, Deshoullier ’03*	$\to$	’weak’ 3.04k Theorem		

Proof outline of our result

Proposition

Any 1-dimensional set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3.04|A| - 3$ can be covered by an arithmetic progression of length at most $10^9|A|$.

Proof outline of our result

Proposition

Any 1-dimensional set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3.04|A| - 3$ can be covered by an arithmetic progression of length at most $10^9|A|$.

Theorem (Freiman, Deshouiller '03)

With some exceptions, for any set $\mathcal{A} \subset \mathbb{Z}_n$ satisfying $|\mathcal{A}| \leq 10^{-9}n$ and $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$ there exists a subgroup $H < \mathbb{Z}$ so that $\mathcal{A}$ is contained in an ℓ-term arithmetic progression of cosets of H where $(\ell - 1)|H| \leq |2\mathcal{A}| - |\mathcal{A}|$.

Proof outline of our result

Proposition

Any 1-dimensional set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3.04|A| - 3$ can be covered by an arithmetic progression of length at most $10^9|A|$.

Theorem (Freiman, Deshouiller '03)

With some exceptions, for any set $\mathcal{A} \subset \mathbb{Z}_n$ satisfying $|\mathcal{A}| \leq 10^{-9}n$ and $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$ there exists a subgroup $H < \mathbb{Z}$ so that $\mathcal{A}$ is contained in an ℓ-term arithmetic progression of cosets of H where $(\ell - 1)|H| \leq |2\mathcal{A}| - |\mathcal{A}|$.

1. Normalize A and let $\mathcal{A}$ denote the projection of A into $\mathbb{Z}_{\max(A)}$.

Proof outline of our result

Proposition

Any 1-dimensional set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3.04|A| - 3$ can be covered by an arithmetic progression of length at most $10^9|A|$.

Theorem (Freiman, Deshouiller '03)

With some exceptions, for any set $\mathcal{A} \subset \mathbb{Z}_n$ satisfying $|\mathcal{A}| \leq 10^{-9}n$ and $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$ there exists a subgroup $H < \mathbb{Z}$ so that $\mathcal{A}$ is contained in an ℓ-term arithmetic progression of cosets of H where $(\ell - 1)|H| \leq |2\mathcal{A}| - |\mathcal{A}|$.

1. Normalize A and let $\mathcal{A}$ denote the projection of A into $\mathbb{Z}_{\max(A)}$.
2. Again $|2A| \geq |2\mathcal{A}| + |A|$ and therefore $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$.

Proof outline of our result

Proposition

Any 1-dimensional set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3.04|A| - 3$ can be covered by an arithmetic progression of length at most $10^9|A|$.

Theorem (Freiman, Deshouiller '03)

With some exceptions, for any set $\mathcal{A} \subset \mathbb{Z}_n$ satisfying $|\mathcal{A}| \leq 10^{-9}n$ and $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$ there exists a subgroup $H < \mathbb{Z}$ so that $\mathcal{A}$ is contained in an ℓ-term arithmetic progression of cosets of H where $(\ell - 1)|H| \leq |2\mathcal{A}| - |\mathcal{A}|$.

1. Normalize A and let $\mathcal{A}$ denote the projection of A into $\mathbb{Z}_{\max(A)}$.
2. Again $|2A| \geq |2\mathcal{A}| + |A|$ and therefore $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$.
3. If $|\mathcal{A}| > 10^{-9}\max(A)$ we are done.

Proof outline of our result

Proposition

Any 1-dimensional set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3.04|A| - 3$ can be covered by an arithmetic progression of length at most $10^9|A|$.

Theorem (Freiman, Deshouiller '03)

With some exceptions, for any set $\mathcal{A} \subset \mathbb{Z}_n$ satisfying $|\mathcal{A}| \leq 10^{-9}n$ and $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$ there exists a subgroup $H < \mathbb{Z}$ so that $\mathcal{A}$ is contained in an ℓ-term arithmetic progression of cosets of H where $(\ell - 1)|H| \leq |2\mathcal{A}| - |\mathcal{A}|$.

1. Normalize A and let $\mathcal{A}$ denote the projection of A into $\mathbb{Z}_{\max(A)}$.
2. Again $|2A| \geq |2\mathcal{A}| + |A|$ and therefore $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$.
3. If $|\mathcal{A}| > 10^{-9}\max(A)$ we are done. If not, then we note that $\ell < m/2$ where $m = \max(A)/|H|$.

Proof outline of our result

Proposition

Any 1-dimensional set $A \subset \mathbb{Z}$ satisfying $|2A| \leq 3.04|A| - 3$ can be covered by an arithmetic progression of length at most $10^9|A|$.

Theorem (Freiman, Deshouiller '03)

With some exceptions, for any set $\mathcal{A} \subset \mathbb{Z}_n$ satisfying $|\mathcal{A}| \leq 10^{-9}n$ and $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$ there exists a subgroup $H < \mathbb{Z}$ so that $\mathcal{A}$ is contained in an ℓ-term arithmetic progression of cosets of H where $(\ell - 1)|H| \leq |2\mathcal{A}| - |\mathcal{A}|$.

1. Normalize A and let $\mathcal{A}$ denote the projection of A into $\mathbb{Z}_{\max(A)}$.
2. Again $|2A| \geq |2\mathcal{A}| + |A|$ and therefore $|2\mathcal{A}| \leq 2.04|\mathcal{A}|$.
3. If $|\mathcal{A}| > 10^{-9}\max(A)$ we are done. If not, then we note that $\ell < m/2$ where $m = \max(A)/|H|$.
4. It follows that the projection of A into $\mathbb{Z}_m$ is rectifiable. Letting $\phi : \mathbb{Z} \to \mathbb{Z}_m$ denote the projection and $\psi : \mathbb{Z}_m \to \mathbb{Z}$ the rectification, we note that $\{(a, \psi(\phi(a))) : a \in A\} \subset \mathbb{Z}^2$ is F_2-isomorphic to A and not contained in a hyperplane, contradicting $\dim(A) = 1$. $\square$

Proof outline of our result

Theorem (Candela, Serra, S. '18+)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ and $|\mathcal{A}| \leq p/10^{10}$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

$\mathbb{Z}_n$	*modular reduction*	$\mathbb{Z}$	*rectification*	$\mathbb{Z}_p$
'2k-1 Theorem' *Kneser '53*	$\rightarrow$	3k-4 Theorem *Freiman '66* *Lev, Smeliansky '95*	$\rightarrow$	2.4k-3 Theorem *Freiman '66*
2.04k Theorem *Freiman, Deshoullier '03*	$\rightarrow$	'weak' 3.04k Theorem		

Proof outline of our result

Theorem (Candela, Serra, S. '18+)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ and $|\mathcal{A}| \leq p/10^{10}$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

$\mathbb{Z}_n$	*modular reduction*	$\mathbb{Z}$	*rectification*	$\mathbb{Z}_p$
'2k-1 Theorem' *Kneser '53*	$\rightarrow$	3k-4 Theorem *Freiman '66* *Lev, Smeliansky '95*	$\rightarrow$	2.4k-3 Theorem *Freiman '66*
2.04k Theorem *Freiman, Deshoullier '03*	$\rightarrow$	'weak' 3.04k Theorem	$\searrow$	
		2-dim 3.3k Theorem *Freiman '66*	$\rightarrow$	

Proof outline of our result

Theorem (Candela, Serra, S. '18+)

Any set $\mathcal{A} \subset \mathbb{Z}$ satisfying $|2\mathcal{A}| \leq 2.48|\mathcal{A}| - 7$ and $|\mathcal{A}| \leq p/10^{10}$ is contained in an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Proof Outline.

$\mathbb{Z}_n$	*modular reduction*	$\mathbb{Z}$	*rectification*	$\mathbb{Z}_p$
'2k-1 Theorem' *Kneser '53*	$\rightarrow$	3k-4 Theorem *Freiman '66* *Lev, Smeliansky '95*	$\rightarrow$	2.4k-3 Theorem *Freiman '66*
2.04k Theorem *Freiman, Deshoullier '03*	$\rightarrow$	'weak' 3.04k Theorem	$\searrow$	
		2-dim 3.3k Theorem *Freiman '66*	$\rightarrow$	2.48k-7 Theorem

What should a complete statement look like?

What should a complete statement look like?

Theorem (Vosper '56)

Any set $\mathcal{A} \subseteq \mathbb{Z}_p$ satisfying $|\mathcal{A}| \geq 2$ and $|2\mathcal{A}| = 2|\mathcal{A}| - 1 \leq p - 2$ must be an arithmetic progression.

What should a complete statement look like?

Theorem (Vosper '56)

Any set $\mathcal{A} \subseteq \mathbb{Z}_p$ *satisfying* $|\mathcal{A}| \geq 2$ *and* $|2\mathcal{A}| = 2|\mathcal{A}| - 1 \leq p - 2$ *must be an arithmetic progression.*

Theorem (Serra, Zémor '08)

Any set $\mathcal{A} \subseteq \mathbb{Z}_n$ *satisfying* $|2\mathcal{A}| \leq \min(3|\mathcal{A}| - 4, (2 + \epsilon)|\mathcal{A}|)$ *as well as*

$$|2\mathcal{A}| \leq p - (|2\mathcal{A}| - 2|\mathcal{A}| + 3) \tag{2}$$

can be covered by an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

What should a complete statement look like?

Theorem (Vosper '56)

Any set $\mathcal{A} \subseteq \mathbb{Z}_p$ satisfying $|\mathcal{A}| \geq 2$ and $|2\mathcal{A}| = 2|\mathcal{A}| - 1 \leq p - 2$ must be an arithmetic progression.

Theorem (Serra, Zémor '08)

Any set $\mathcal{A} \subseteq \mathbb{Z}_n$ satisfying $|2\mathcal{A}| \leq \min(3|\mathcal{A}| - 4, (2+\epsilon)|\mathcal{A}|)$ as well as

$$|2\mathcal{A}| \leq p - (|2\mathcal{A}| - 2|\mathcal{A}| + 3) \qquad (2)$$

can be covered by an arithmetic progression of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Conjecture (Serra, Zémor '08)

If $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$ and $|2\mathcal{A}| \leq p - (|2\mathcal{A}| - 2|\mathcal{A}| + 3)$ then $\mathcal{A}$ can be covered by an AP of size at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

What should a complete statement look like?

Example

Consider $\mathcal{A} = \{0, 1, 2, 3, 5, 10\}$ in $\mathbb{Z}_{19}$.

What should a complete statement look like?

Example

Consider $\mathcal{A} = \{0, 1, 2, 3, 5, 10\}$ in $\mathbb{Z}_{19}$. We have $|2A| = 14$, so that $|2\mathcal{A}| = 3|A| - 4$ as well as $|2\mathcal{A}| = p - (|2\mathcal{A}| - 2|\mathcal{A}| + 3)$ but $\mathcal{A}$ is not contained in an arithmetic progressions of size $9 = |2\mathcal{A}| - |\mathcal{A}| + 1$.

What should a complete statement look like?

Example

Consider $\mathcal{A} = \{0, 1, 2, 3, 5, 10\}$ in $\mathbb{Z}_{19}$. We have $|2\mathcal{A}| = 14$, so that $|2\mathcal{A}| = 3|\mathcal{A}| - 4$ as well as $|2\mathcal{A}| = p - (|2\mathcal{A}| - 2|\mathcal{A}| + 3)$ but $\mathcal{A}$ is not contained in an arithmetic progressions of size $9 = |2\mathcal{A}| - |\mathcal{A}| + 1$.

Conjecture (Candela, de Roton '17; Hamidoune, Serra, Zémor '05)

If $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$ *and* $|2\mathcal{A}| \leq p - (|2\mathcal{A}| - 2|\mathcal{A}| + \mathbf{4})$ *then* $\mathcal{A}$ *can be covered by an AP of size at most* $|2\mathcal{A}| - |\mathcal{A}| + 1$*.*

What should a complete statement look like?

Example

Consider $\mathcal{A} = \{0, 1, 2, 3, 5, 10\}$ in $\mathbb{Z}_{19}$. We have $|2A| = 14$, so that $|2\mathcal{A}| = 3|A| - 4$ as well as $|2\mathcal{A}| = p - (|2\mathcal{A}| - 2|\mathcal{A}| + 3)$ but $\mathcal{A}$ is not contained in an arithmetic progressions of size $9 = |2\mathcal{A}| - |\mathcal{A}| + 1$.

Conjecture

Let a set $\mathcal{A} \subset \mathbb{Z}_p$ be given. If either

(i) $0 \le |2\mathcal{A}| - \big(2|\mathcal{A}| - 1\big) \le \min(|\mathcal{A}| - 4, p - |2\mathcal{A}| - 2)$ *or*

(ii) $0 \le |2\mathcal{A}| - \big(2|\mathcal{A}| - 1\big) = |\mathcal{A}| - 3 \le p - |2\mathcal{A}| - 3$

then $\mathcal{A}$ can be covered by an AP of length at most $|2\mathcal{A}| - |\mathcal{A}| + 1$.

Thank you for your attention!