Inverse theorems and approximate structure

Freddie Manners

January 30, 2024

Approximate homomorphisms

G_1, G_2: two finite abelian groups (e.g., $G_1 = G_2 = \mathbb{F}_2^n$).

Approximate homomorphisms

G_1, G_2: two finite abelian groups (e.g., $G_1 = G_2 = \mathbb{F}_2^n$).
$f : G_1 \to G_2$ a function.

Approximate homomorphisms

G_1, G_2: two finite abelian groups (e.g., $G_1 = G_2 = \mathbb{F}_2^n$).
$f : G_1 \to G_2$ a function.

f a homomorphism:

$$\forall x, y \in G_1 : \ f(x+y) = f(x) + f(y)$$

Approximate homomorphisms

G_1, G_2: two finite abelian groups (e.g., $G_1 = G_2 = \mathbb{F}_2^n$).
$f : G_1 \to G_2$ a function.

f a homomorphism:

$$\forall x, y \in G_1 : \ f(x+y) = f(x) + f(y)$$

f a *'99%' homomorphism:*

$$\mathbb{P}_{x,y \in G_1}\left[f(x+y) = f(x) + f(y)\right] \geq 1 - \varepsilon$$

Approximate homomorphisms

G_1, G_2: two finite abelian groups (e.g., $G_1 = G_2 = \mathbb{F}_2^n$).
$f : G_1 \to G_2$ a function.

f a homomorphism:

$$\forall x, y \in G_1 : \ f(x+y) = f(x) + f(y)$$

f a *'99%' homomorphism:*

$$\mathbb{P}_{x,y \in G_1}\left[f(x+y) = f(x) + f(y)\right] \geq 1 - \varepsilon$$

f a *'1% homomorphism'*:

$$\mathbb{P}_{x,y \in G_1}\left[f(x+y) = f(x) + f(y)\right] \geq \delta.$$

Approximate homomorphisms

G_1, G_2: two finite abelian groups (e.g., $G_1 = G_2 = \mathbb{F}_2^n$).
$f : G_1 \to G_2$ a function.

f a homomorphism:

$$\forall x, y \in G_1 : \ f(x+y) = f(x) + f(y)$$

f a *'99%' homomorphism:*

$$\mathbb{P}_{x,y \in G_1}\left[f(x+y) = f(x) + f(y)\right] \geq 1 - \varepsilon$$

f a *'1% homomorphism'*:

$$\mathbb{P}_{x,y \in G_1}\left[f(x+y) = f(x) + f(y)\right] \geq \delta.$$

Question

What do $\begin{cases} 99\% \\ 1\% \end{cases}$ *homomorphisms look like?*

The structure of 99% homomorphisms

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq 1-\varepsilon$$

The structure of 99% homomorphisms

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq 1-\varepsilon$$

Example

Take a true homomorphism $\phi\colon G_1\to G_2$ and modify $(\varepsilon/3)|G_1|$ of the values $\phi(x)$.

The structure of 99% homomorphisms

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq 1-\varepsilon$$

Example

Take a true homomorphism $\phi\colon G_1\to G_2$ and modify $(\varepsilon/3)|G_1|$ of the values $\phi(x)$.

Proposition

If

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq 1-\varepsilon$$

then there exists a homomorphism $\phi\colon G_1\to G_2$ *such that* $\mathbb{P}_{x\in G_1}[f(x)=\phi(x)]\geq 1-C\varepsilon$.

The structure of 99% homomorphisms

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq 1-\varepsilon$$

Example

Take a true homomorphism $\phi\colon G_1\to G_2$ and modify $(\varepsilon/3)|G_1|$ of the values $\phi(x)$.

Proposition

If

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq 1-\varepsilon$$

then there exists a homomorphism $\phi\colon G_1\to G_2$ *such that* $\mathbb{P}_{x\in G_1}[f(x)=\phi(x)]\geq 1-C\varepsilon$.

Application

Property testing.

The structure of 1% homomorphisms

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq\delta.$$

The structure of 1% homomorphisms

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq\delta.$$

Question

Is it true that there exists a homomorphism $\phi\colon G_1\to G_2$ *with* $\mathbb{P}_{x\in G_1}[f(x)=\phi(x)]\geq F(\delta)$*?*

The structure of 1% homomorphisms

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq\delta.$$

Question

Is it true that there exists a homomorphism $\phi\colon G_1\to G_2$ with $\mathbb{P}_{x\in G_1}[f(x)=\phi(x)]\geq F(\delta)$?

Example

Consider $f:\mathbb{Z}\to\mathbb{Z}$,

$$f(x)=\lfloor\sqrt{2}x\rfloor.$$

The structure of 1% homomorphisms

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq\delta.$$

Question

Is it true that there exists a homomorphism $\phi\colon G_1\to G_2$ with $\mathbb{P}_{x\in G_1}[f(x)=\phi(x)]\geq F(\delta)$?

Example

Consider $f:\mathbb{Z}\to\mathbb{Z}$,

$$f(x)=\lfloor\sqrt{2}x\rfloor.$$

We have

$$\mathbb{P}\left[\lfloor\sqrt{2}(x+y)\rfloor=\lfloor\sqrt{2}x\rfloor+\lfloor\sqrt{2}f(y)\rfloor\right]\approx 1/2$$

(depending on whether the carry bit is 0 or 1).

So no.

The structure of 1% homomorphisms (contd.)

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq\delta.$$

The structure of 1% homomorphisms (contd.)

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq\delta.$$

Theorem (Samorodnitsky 2007)

If $G_1=\mathbb{F}_2^n$, $G_2=\mathbb{F}_2^m$ then yes, $\mathbb{P}_{x\in G_1}[f(x)=\phi(x)]\geq F(\delta)$ for some homomorphism ϕ.

The structure of 1% homomorphisms (contd.)

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq\delta.$$

Theorem (Samorodnitsky 2007)

If $G_1=\mathbb{F}_2^n$, $G_2=\mathbb{F}_2^m$ then yes, $\mathbb{P}_{x\in G_1}[f(x)=\phi(x)]\geq F(\delta)$ for some homomorphism ϕ.

Conjecture (Ruzsa; Conjecture A)

You can take $F(\delta)=\delta^C$ for some constant $C>0$.

The structure of 1% homomorphisms (contd.)

$$\mathbb{P}_{x,y\in G_1}\left[f(x+y)=f(x)+f(y)\right]\geq\delta.$$

Theorem (Samorodnitsky 2007)

If $G_1=\mathbb{F}_2^n$, $G_2=\mathbb{F}_2^m$ then yes, $\mathbb{P}_{x\in G_1}[f(x)=\phi(x)]\geq F(\delta)$ for some homomorphism ϕ.

Conjecture (Ruzsa; Conjecture A)

You can take $F(\delta)=\delta^C$ for some constant $C>0$.

Weak (statistical structure) implies *strong* (algebraic) structure.

Approximate subgroups

Let G be an abelian group and $A \subseteq G$ a finite subset.

Approximate subgroups

Let G be an abelian group and $A \subseteq G$ a finite subset.

A is a *subgroup* if

$$\forall x, y \in A : x + y \in A$$

Approximate subgroups

Let G be an abelian group and $A \subseteq G$ a finite subset.

A is a *subgroup* if

$$\forall x, y \in A : x + y \in A$$

A is a *probabilist's* $\begin{cases} 99\% \\ 1\% \end{cases}$ *subgroup* if

$$\mathbb{P}_{x,y \in A}[x + y \in A] \geq \begin{cases} 1 - \varepsilon \\ \delta \end{cases}$$

Approximate subgroups

Let G be an abelian group and $A \subseteq G$ a finite subset.

A is a *subgroup* if

$$\forall x, y \in A : x + y \in A$$

A is a *probabilist's* $\begin{cases} 99\% \\ 1\% \end{cases}$ *subgroup* if

$$\mathbb{P}_{x,y \in A}[x + y \in A] \geq \begin{cases} 1 - \varepsilon \\ \delta \end{cases}$$

A is a *combinatorialist's* $\begin{cases} 99\% \\ 1\% \end{cases}$ *subgroup*

$$|\{x + y : x, y \in A\}| \leq \begin{cases} (1 + \varepsilon)|A| \\ K|A| \end{cases}$$

Approximate subgroups

Let G be an abelian group and $A \subseteq G$ a finite subset.

A is a *subgroup* if

$$\forall x, y \in A : x + y \in A$$

A is a *probabilist's* $\begin{cases} 99\% \\ 1\% \end{cases}$ *subgroup* if

$$\mathbb{P}_{x,y \in A}[x + y \in A] \geq \begin{cases} 1 - \varepsilon \\ \delta \end{cases}$$

A is a *combinatorialist's* $\begin{cases} 99\% \\ 1\% \end{cases}$ *subgroup*

$$|A + A| := |\{x + y : x, y \in A\}| \leq \begin{cases} (1 + \varepsilon)|A| \\ K|A| \end{cases}$$

Approximate subgroups (contd.)

Example

If $G = \mathbb{Z}$ and $A = \{1, \dots, n\}$ then

Approximate subgroups (contd.)

Example

If $G = \mathbb{Z}$ and $A = \{1, \dots, n\}$ then

$$A + A = \{2, \dots, 2n\}$$

Approximate subgroups (contd.)

Example

If $G = \mathbb{Z}$ and $A = \{1, \dots, n\}$ then

$$A + A = \{2, \dots, 2n\}$$

$$|A + A| \approx 2|A|$$

Approximate subgroups (contd.)

Example

If $G = \mathbb{Z}$ and $A = \{1, \dots, n\}$ then

$$A + A = \{2, \dots, 2n\}$$

$$|A + A| \approx 2|A|$$

$$\mathbb{P}_{x,y \in A}[x + y \in A] \approx 1/2.$$

Approximate subgroups (contd.)

Example

If $G = \mathbb{Z}$ and $A = \{1, \dots, n\}$ then

$$A + A = \{2, \dots, 2n\}$$

$$|A + A| \approx 2|A|$$

$$\mathbb{P}_{x,y \in A}[x + y \in A] \approx 1/2.$$

Question

What do $\begin{cases} 99\% \\ 1\% \end{cases}$ *subgroups look like in general?*

The structure of approximate subgroups

The structure of approximate subgroups

Proposition (Freiman (99%))

If $|A+A| < (1+\varepsilon)|A|$ *and* $\varepsilon < 1/2$ *then there is a subgroup* $H \leq G$ *and* $a \in G$ *such that* $A \subseteq a+H$ *and* $|H| \leq (1+\varepsilon)|A|$.

The structure of approximate subgroups

Proposition (Freiman (99%))

If $|A+A| < (1+\varepsilon)|A|$ *and* $\varepsilon < 1/2$ *then there is a subgroup* $H \leq G$ *and* $a \in G$ *such that* $A \subseteq a+H$ *and* $|H| \leq (1+\varepsilon)|A|$.

Theorem (Ruzsa (1%))

If $A \subseteq \mathbb{F}_2^n$ *and* $|A+A| \leq K|A|$ *then there exists a subgroup* $H \leq \mathbb{F}_2^n$ *and* $a \in \mathbb{F}_2^n$ *such that* $A \subseteq a+H$ *and* $|H| \leq K^2 2^{K^4}|A|$.

The structure of approximate subgroups

Proposition (Freiman (99%))

If $|A+A| < (1+\varepsilon)|A|$ and $\varepsilon < 1/2$ then there is a subgroup $H \leq G$ and $a \in G$ such that $A \subseteq a+H$ and $|H| \leq (1+\varepsilon)|A|$.

Theorem (Ruzsa (1%))

If $A \subseteq \mathbb{F}_2^n$ and $|A+A| \leq K|A|$ then there exists a subgroup $H \leq \mathbb{F}_2^n$ and $a \in \mathbb{F}_2^n$ such that $A \subseteq a+H$ and $|H| \leq K^2 2^{K^4}|A|$.

Conjecture (Marton; the "polynomial Freiman–Ruzsa conjecture"; Conjecture B)

If $A \subseteq \mathbb{F}_2^n$ and $|A+A| \leq K|A|$ then there exists a subgroup $H \leq \mathbb{F}_2^n$ and $a_1, \dots, a_m \in \mathbb{F}_2^n$ such that

$$A \subseteq \bigcup_{i=1}^{m} (a_i + H)$$

and $|H| \leq |A|$ and $m \leq 2K^C$.

The structure of approximate subgroups (contd.)

Proposition (Ruzsa)

Conjecture A (structure of 1% homomorphisms) and Conjecture B (structure of 1% subgroups) are equivalent.

The structure of approximate subgroups (contd.)

Proposition (Ruzsa)

Conjecture A (structure of 1% homomorphisms) and Conjecture B (structure of 1% subgroups) are equivalent.

. . . with many other equivalent forms.

The structure of approximate subgroups (contd.)

Proposition (Ruzsa)

Conjecture A (structure of 1% homomorphisms) and Conjecture B (structure of 1% subgroups) are equivalent.

. . . with many other equivalent forms.

Idea for $\Leftarrow$.

Given $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ consider its *graph*

$$\Gamma = \{(x, f(x)) : x \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^m.$$

Then Γ is a (probabilist's) 1% subgroup. □

The structure of approximate subgroups (contd.)

Proposition (Ruzsa)

Conjecture A (structure of 1% homomorphisms) and Conjecture B (structure of 1% subgroups) are equivalent.

. . . with many other equivalent forms.

Idea for $\Leftarrow$.

Given $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ consider its *graph*

$$\Gamma = \{(x, f(x)) : x \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^m.$$

Then Γ is a (probabilist's) 1% subgroup. □

Sanders (2012) got a *quasipolynomial* bound (much better than exponential).

The structure of approximate subgroups (contd.)

Proposition (Ruzsa)

Conjecture A (structure of 1% homomorphisms) and Conjecture B (structure of 1% subgroups) are equivalent.

. . . with many other equivalent forms.

Idea for $\Leftarrow$.

Given $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ consider its *graph*

$$\Gamma = \{(x, f(x)) : x \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^m.$$

Then Γ is a (probabilist's) 1% subgroup. □

Sanders (2012) got a *quasipolynomial* bound (much better than exponential).

Theorem (Gowers, Green, M., Tao 2024+)

Conjecture B is true (with $C = 12$).

Very brief outline of proof

Yet another notion of approximate structure:

Very brief outline of proof

Yet another notion of approximate structure:

Set $A \subseteq G$	Random variable X on G

Very brief outline of proof

Yet another notion of approximate structure:

Set $A \subseteq G$	Random variable X on G
$\lvert A \rvert$	Shannon entropy $H[X]$

Very brief outline of proof

Yet another notion of approximate structure:

Set $A \subseteq G$	Random variable X on G
$\lvert A \rvert$	Shannon entropy $H[X]$
$\lvert A + A \rvert \leq K \lvert A \rvert$	$H[X_1 + X_2] - \frac{1}{2}H[X_1] - \frac{1}{2}H[X_2] \leq k$

Very brief outline of proof

Yet another notion of approximate structure:

Set $A \subseteq G$	Random variable X on G
$\lvert A \rvert$	Shannon entropy $H[X]$
$\lvert A + A \rvert \leq K \lvert A \rvert$	$H[X_1 + X_2] - \frac{1}{2}H[X_1] - \frac{1}{2}H[X_2] \leq k$

Recursive proof: given X_1, X_2, either $k = 0$ or find X_1', X_2' with $k(X_1', X_2') \leq 0.99k(X_1, X_2)$.

Polynomials

Polynomials

Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function.

Polynomials

Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function. For $h \in \mathbb{Z}$, write $\partial_h f : x \mapsto f(x) - f(x+h)$ ("discrete derivative").

Polynomials

Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function. For $h \in \mathbb{Z}$, write $\partial_h f : x \mapsto f(x) - f(x+h)$ ("discrete derivative").

Observation

If f satisfies $\partial_{h_1} \dots \partial_{h_k} f(x) = 0$ for all $x, h_1, \dots, h_k$, then f is a polynomial of degree $\leq k - 1$.

Polynomials

Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function. For $h \in \mathbb{Z}$, write $\partial_h f : x \mapsto f(x) - f(x+h)$ ("discrete derivative").

Observation

If f satisfies $\partial_{h_1} \dots \partial_{h_k} f(x) = 0$ for all $x, h_1, \dots, h_k$, then f is a polynomial of degree $\leq k-1$.

$$\dots, \quad 3, \quad 7, \quad 13, \quad 21, \quad 31, \quad 43, \quad \dots$$

Polynomials

Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function. For $h \in \mathbb{Z}$, write $\partial_h f : x \mapsto f(x) - f(x+h)$ ("discrete derivative").

Observation

If f satisfies $\partial_{h_1} \dots \partial_{h_k} f(x) = 0$ for all $x, h_1, \dots, h_k$, then f is a polynomial of degree $\leq k-1$.

$$\begin{array}{ccccccccccc} \dots, & & 3, & & 7, & & 13, & & 21, & & 31, & & 43, & \dots \\ & \dots, & & 4, & & 6, & & 8, & & 10, & & 12, & \dots & \end{array}$$

Polynomials

Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function. For $h \in \mathbb{Z}$, write $\partial_h f : x \mapsto f(x) - f(x+h)$ ("discrete derivative").

Observation

If f satisfies $\partial_{h_1} \dots \partial_{h_k} f(x) = 0$ for all $x, h_1, \dots, h_k$, then f is a polynomial of degree $\leq k-1$.

$$\begin{array}{ccccccccccc} \dots, & 3, & & 7, & & 13, & & 21, & & 31, & & 43, & \dots \\ & \dots, & 4, & & 6, & & 8, & & 10, & & 12, & \dots & \\ & & \dots, & 2, & & 2, & & 2, & & 2, & \dots & & \end{array}$$

Polynomials

Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function. For $h \in \mathbb{Z}$, write $\partial_h f : x \mapsto f(x) - f(x+h)$ ("discrete derivative").

Observation

If f satisfies $\partial_{h_1} \dots \partial_{h_k} f(x) = 0$ for all $x, h_1, \dots, h_k$, then f is a polynomial of degree $\leq k-1$.

$$\begin{array}{ccccccccccc} \dots, & & 3, & & 7, & & 13, & & 21, & & 31, & & 43, & \dots \\ & \dots, & & 4, & & 6, & & 8, & & 10, & & 12, & \dots & \\ & & \dots, & & 2, & & 2, & & 2, & & 2, & \dots & & \\ & & & \dots, & & 0, & & 0, & & 0, & \dots & & & \end{array}$$

Polynomials

Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function. For $h \in \mathbb{Z}$, write $\partial_h f : x \mapsto f(x) - f(x+h)$ ("discrete derivative").

Observation

If f satisfies $\partial_{h_1} \dots \partial_{h_k} f(x) = 0$ for all $x, h_1, \dots, h_k$, then f is a polynomial of degree $\leq k-1$.

$$\begin{array}{ccccccccccc} \dots, & 3, & & 7, & & 13, & & 21, & & 31, & & 43, & \dots \\ & \dots, & 4, & & 6, & & 8, & & 10, & & 12, & \dots & \\ & & \dots, & 2, & & 2, & & 2, & & 2, & \dots & & \\ & & & \dots, & 0, & & 0, & & 0, & \dots & & & \end{array}$$

Definition

For G_1, G_2 abelian groups, call $f : G_1 \to G_2$ a *polynomial of degree* $\leq s$ if $\partial_{h_1} \dots \partial_{h_{s+1}} f(x) = 0 \ \forall x, h_1, \dots, h_{s+1} \in G_1$.

Approximate polynomials

Approximate polynomials

$f : G_1 \to G_2$ is a *probabilist's approximate polynomial* if

$$\mathbb{P}_{x,h_1,\dots,h_{s+1}\in G_1}[\partial_{h_1}\dots\partial_{h_{s+1}} f(x) = 0] \geq \delta.$$

Approximate polynomials

$f : G_1 \to G_2$ is a *probabilist's approximate polynomial* if
$$\mathbb{P}_{x,h_1,\dots,h_{s+1}\in G_1}[\partial_{h_1}\dots\partial_{h_{s+1}} f(x) = 0] \geq \delta.$$

$f : G_1 \to G_2$ is a *combinatorialist's approximate polynomial* if
$$\left|\left\{\partial_{h_1}\dots\partial_{h_{s+1}} f(x) : x, h_1, \dots, h_{s+1} \in G_1\right\}\right| \leq K.$$

Approximate polynomials

$f: G_1 \to G_2$ is a *probabilist's approximate polynomial* if
$$\mathbb{P}_{x,h_1,\dots,h_{s+1}\in G_1}[\partial_{h_1}\dots\partial_{h_{s+1}} f(x) = 0] \geq \delta.$$

$f: G_1 \to G_2$ is a *combinatorialist's approximate polynomial* if
$$\left|\left\{\partial_{h_1}\dots\partial_{h_{s+1}} f(x) : x, h_1, \dots, h_{s+1} \in G_1\right\}\right| \leq K.$$

$g: G \to \mathbb{C}$, $\|g\|_\infty \leq 1$ (e.g., $g(x) = e^{2\pi i f(x)}$) is an *analyst's approximate polynomial* if
$$\mathbb{E}_{x,h_1,\dots,h_{s+1}} \Delta_{h_1}\dots\Delta_{h_{s+1}} g(x) \geq \delta$$

where $\Delta_h g(x) = g(x)\overline{g(x+h)}$

Approximate polynomials

$f: G_1 \to G_2$ is a *probabilist's approximate polynomial* if
$$\mathbb{P}_{x,h_1,\dots,h_{s+1}\in G_1}[\partial_{h_1}\dots\partial_{h_{s+1}} f(x) = 0] \geq \delta.$$

$f: G_1 \to G_2$ is a *combinatorialist's approximate polynomial* if
$$\left|\left\{\partial_{h_1}\dots\partial_{h_{s+1}} f(x) : x, h_1, \dots, h_{s+1} \in G_1\right\}\right| \leq K.$$

$g: G \to \mathbb{C}$, $\|g\|_\infty \leq 1$ (e.g., $g(x) = e^{2\pi i f(x)}$) is an *analyst's approximate polynomial* if
$$\|g\|_{U^{s+1}}^{2^{s+1}} := \mathbb{E}_{x,h_1,\dots,h_{s+1}} \Delta_{h_1}\dots\Delta_{h_{s+1}} g(x) \geq \delta$$

where $\Delta_h g(x) = g(x)\overline{g(x+h)}$ and $\|g\|_{U^{s+1}}$ is called a *Gowers uniformity norm*.

Higher order Fourier analysis

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Higher order Fourier analysis

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Question

If $g\colon G\to\mathbb{C}$, $\|g\|_\infty\leq 1$, *obeys* $(\dagger)$, $\exists$ *a true polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(\delta)?$$

Higher order Fourier analysis

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Question

If $g\colon G\to\mathbb{C}$, $\|g\|_\infty\leq 1$, *obeys* $(\dagger)$, $\exists$ *a true polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(\delta)?$$

Example ($s=1$)

$$\mathbb{E}_{x,h_1,h_2\in G}g(x)\overline{g(x+h_1)g(x+h_2)}g(x+h_1+h_2)\geq\delta$$

Higher order Fourier analysis

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Question

If $g\colon G\to\mathbb{C}$, $\|g\|_\infty\leq 1$, *obeys* $(\dagger)$, $\exists$ *a true polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(\delta)?$$

Example ($s=1$)

$$\mathbb{E}_{x,h_1,h_2\in G}g(x)\overline{g(x+h_1)g(x+h_2)}g(x+h_1+h_2)\geq\delta$$

So there *does* exist $\chi\colon G\to\mathbb{R}/\mathbb{Z}$ such that

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\chi(x)}\right|\geq ?$$

Higher order Fourier analysis

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Question

If $g\colon G\to\mathbb{C}$, $\|g\|_\infty\leq 1$, *obeys* $(\dagger)$, $\exists$ *a true polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(\delta)?$$

Example ($s=1$)

$$\mathbb{E}_{x,h_1,h_2\in G}g(x)\overline{g(x+h_1)g(x+h_2)}g(x+h_1+h_2)\geq\delta$$

So there *does* exist $\chi\colon G\to\mathbb{R}/\mathbb{Z}$ such that

$$|\widehat{g}(\chi)|=|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\chi(x)}|\geq ?$$

Higher order Fourier analysis

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Question

If $g\colon G\to\mathbb{C}$, $\|g\|_\infty\leq 1$, *obeys* $(\dagger)$, $\exists$ *a true polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(\delta)?$$

Example ($s=1$)

$$\sum_{\chi\in\widehat{G}}|\widehat{f}(\chi)|^4=\mathbb{E}_{x,h_1,h_2\in G}g(x)\overline{g(x+h_1)g(x+h_2)}g(x+h_1+h_2)\geq\delta$$

So there *does* exist $\chi\colon G\to\mathbb{R}/\mathbb{Z}$ such that

$$|\widehat{g}(\chi)|=|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\chi(x)}|\geq\delta^{1/2}!$$

Higher order Fourier analysis

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Question

If $g\colon G\to\mathbb{C}$, $\|g\|_\infty\leq 1$, *obeys* $(\dagger)$, $\exists$ *a true polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(\delta)?$$

Example ($s=1$)

$$\sum_{\chi\in\widehat{G}}|\widehat{f}(\chi)|^4=\mathbb{E}_{x,h_1,h_2\in G}g(x)\overline{g(x+h_1)g(x+h_2)}g(x+h_1+h_2)\geq\delta$$

So there *does* exist $\chi\colon G\to\mathbb{R}/\mathbb{Z}$ such that

$$|\widehat{g}(\chi)|=|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\chi(x)}|\geq\delta^{1/2}!$$

So, the case $s=1$ is "just Fourier analysis".

Higher order Fourier analysis

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Question

If $g\colon G\to\mathbb{C}$, $\|g\|_\infty\leq 1$, *obeys* $(\dagger)$, $\exists$ *a true polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(\delta)?$$

Example ($s=1$)

$$\sum_{\chi\in\widehat{G}}|\widehat{f}(\chi)|^4=\mathbb{E}_{x,h_1,h_2\in G}g(x)\overline{g(x+h_1)g(x+h_2)}g(x+h_1+h_2)\geq\delta$$

So there *does* exist $\chi\colon G\to\mathbb{R}/\mathbb{Z}$ such that

$$|\widehat{g}(\chi)|=|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\chi(x)}|\geq\delta^{1/2}!$$

So, the case $s=1$ is "just Fourier analysis".

The case $s>1$ is called "higher-order Fourier analysis".

The inverse theorem(s)

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

The inverse theorem(s)

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Theorem (Tao–Ziegler (2011);)

If $g\colon\mathbb{F}_p^n\to\mathbb{C}$, $\|g\|_\infty\leq 1$ *and* $(\dagger)$ *holds,* $\exists$ *a degree* $\leq s$ *polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(p,\delta)$$

The inverse theorem(s)

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Theorem (Tao–Ziegler (2011); Gowers–Milicević (2022))

If $g\colon\mathbb{F}_p^n\to\mathbb{C}$, $\|g\|_\infty\leq 1$ *and* $(\dagger)$ *holds,* $\exists$ *a degree* $\leq s$ *polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(p,\delta) \text{ where}$$

$$F(p,\delta)\leq \underbrace{\exp(\exp(\dots\exp}_{c(s)}(C(p)/\delta)\dots)).$$

The inverse theorem(s)

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Theorem (Tao–Ziegler (2011); Gowers–Milicević (2022))

If $g\colon\mathbb{F}_p^n\to\mathbb{C}$, $\|g\|_\infty\leq 1$ *and* $(\dagger)$ *holds,* $\exists$ *a degree* $\leq s$ *polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(p,\delta) \text{ where}$$

$$F(p,\delta)\leq \underbrace{\exp(\exp(\dots\exp}_{c(s)}(C(p)/\delta)\dots)).$$

Theorem (Green–Tao–Ziegler (2012);)

If $g\colon\mathbb{Z}/n\mathbb{Z}\to\mathbb{C}$, $\|g\|_\infty\leq 1$ *and* $(\dagger)$ *holds, then there exists a "nilsequence"* $\psi\colon G\to\mathbb{C}$ *such that*

$$\left|\mathbb{E}_{x\in G}g(x)\overline{\psi(x)}\right|\geq F(\delta)$$

The inverse theorem(s)

$$\mathbb{E}_{x,h_1,\dots,h_{s+1}\in G}\Delta_{h_1}\dots\Delta_{h_{s+1}}g(x)\geq\delta \qquad (\dagger)$$

Theorem (Tao–Ziegler (2011); Gowers–Milicević (2022))

If $g\colon\mathbb{F}_p^n\to\mathbb{C}$, $\|g\|_\infty\leq 1$ *and* $(\dagger)$ *holds,* $\exists$ *a degree* $\leq s$ *polynomial* $\phi\colon G\to\mathbb{R}/\mathbb{Z}$,

$$\left|\mathbb{E}_{x\in G}g(x)e^{-2\pi i\phi(x)}\right|\geq F(p,\delta) \text{ where}$$

$$F(p,\delta)\leq \underbrace{\exp(\exp(\dots\exp}_{c(s)}(C(p)/\delta)\dots)).$$

Theorem (Green–Tao–Ziegler (2012); M. (2018))

If $g\colon\mathbb{Z}/n\mathbb{Z}\to\mathbb{C}$, $\|g\|_\infty\leq 1$ *and* $(\dagger)$ *holds, then there exists a "nilsequence"* $\psi\colon G\to\mathbb{C}$ *such that*

$$\left|\mathbb{E}_{x\in G}g(x)\overline{\psi(x)}\right|\geq F(\delta) \text{ where}$$

$$F(\delta)\leq\exp(\exp(C/\delta^C)).$$

The inverse theorem and approximate polynomials

Proposition

The structure theorem for probabilist's approximate polynomials in degree s
$\Rightarrow$ *the inverse theorem for the Gowers norms in degree $s+1$.*

The inverse theorem and approximate polynomials

Proposition

The structure theorem for probabilist's approximate polynomials in degree s
$\Rightarrow$ *the inverse theorem for the Gowers norms in degree $s+1$.*

In particular, the structure theorem for 1% linear functions
$\Rightarrow$ the inverse theorem for quadratic Fourier analysis (i.e., the U^3-norm).

Application to progressions

Question (Green–Tao)

Do there exist $x, a \in \mathbb{Z}$ *such that* $x, x+a, x+2a, x+3a$ *are all prime?*
How many (up to N*)?*

Application to progressions

Question (Green–Tao)

Do there exist $x, a \in \mathbb{Z}$ such that $x, x+a, x+2a, x+3a$ are all prime?
How many (up to N)?

Case 1: the primes $\mathcal{P} \cap [N]$ are "unstructured"; in particular, do not have *approximately quadratic structure*.

Application to progressions

Question (Green–Tao)

Do there exist $x, a \in \mathbb{Z}$ such that $x, x+a, x+2a, x+3a$ are all prime?
How many (up to N)?

Case 1: the primes $\mathcal{P} \cap [N]$ are "unstructured"; in particular, do not have *approximately quadratic structure*.
$\Rightarrow$ the number of solutions is (roughly) what you would expect from a random set.

Application to progressions

Question (Green–Tao)

Do there exist $x, a \in \mathbb{Z}$ such that $x, x+a, x+2a, x+3a$ are all prime?
How many (up to N)?

Case 1: the primes $\mathcal{P} \cap [N]$ are "unstructured"; in particular, do not have *approximately quadratic structure*.
$\Rightarrow$ the number of solutions is (roughly) what you would expect from a random set.
Case 2: the primes do have approximately quadratic structure.

Application to progressions

Question (Green–Tao)

Do there exist $x, a \in \mathbb{Z}$ such that $x, x+a, x+2a, x+3a$ are all prime?
How many (up to N)?

Case 1: the primes $\mathcal{P} \cap [N]$ are "unstructured"; in particular, do not have *approximately quadratic structure*.
$\Rightarrow$ the number of solutions is (roughly) what you would expect from a random set.
Case 2: the primes do have approximately quadratic structure.
$\Rightarrow$ the primes correlate with a quadratic nilsequence ($\approx e^{2\pi i \psi(x)}$).

Application to progressions

Question (Green–Tao)

Do there exist $x, a \in \mathbb{Z}$ such that $x, x+a, x+2a, x+3a$ are all prime?
How many (up to N)?

Case 1: the primes $\mathcal{P} \cap [N]$ are "unstructured"; in particular, do not have *approximately quadratic structure*.
$\Rightarrow$ the number of solutions is (roughly) what you would expect from a random set.
Case 2: the primes do have approximately quadratic structure.
$\Rightarrow$ the primes correlate with a quadratic nilsequence ($\approx e^{2\pi i \psi(x)}$).
$\Rightarrow \quad \Rightarrow\Leftarrow$.

[END]