Roth's theorem on arithmetic progressions

Tom Sanders

University of Oxford

1st July 2013

solve equations in sets of integers *e.g.* primes, squares, . . .

solve equations in sets of integers *e.g.* primes, squares, ...

general framework: Ruzsa

$A \subset \mathbb{Z}$ 'the' set of integers

$A \subset \mathbb{Z}$ 'the' set of integers

solve $f(x, y, z, w, \dots) = 0$ with $x, y, z, w, \dots \in A$

$A \subset \mathbb{Z}$ 'the' set of integers

solve $f(x, y, z, w, \dots) = 0$ with $x, y, z, w, \dots \in A$

$x + y = z + w$ (add. quad.)

$A \subset \mathbb{Z}$ 'the' set of integers

solve $f(x, y, z, w, \dots) = 0$ with $x, y, z, w, \dots \in A$

$x + y = z + w$ (add. quad.)

$x + y = 2z$ (3ap)

$A \subset \mathbb{Z}$ 'the' set of integers

solve $f(x, y, z, w, \dots) = 0$ with $x, y, z, w, \dots \in A$

$x + y = z + w$ (add. quad.)

$x + y = 2z$ (3ap)

aim: show finding solutions is 'equally' difficult

$A \subset \mathbb{Z}$ 'the' set of integers

solve $f(x, y, z, w, \dots) = 0$ with $x, y, z, w, \dots \in A$

$$x + y = z + w \text{ (add. quad.)}$$

$$x + y = 2z \text{ (3ap)}$$

aim: show finding solutions is 'equally' difficult

(inequivalent: $x + y = z, x - y = 7$)

$$Q(A) := |\{(x,y,z,w) \in A^4 : x+y=z+w\}|$$

and

$$T(A) := |\{(x,y,z) \in A^3 : x+y=2z\}|$$

$$Q(A) := |\{(x,y,z,w) \in A^4 : x + y = z + w\}|$$

and

$$T(A) := |\{(x,y,z) \in A^3 : x + y = 2z\}|$$

then

$$Q(A) \leq |A|^3 \text{ and } T(A) \leq |A|^2$$

$$Q(A) := |\{(x, y, z, w) \in A^4 : x + y = z + w\}|$$

and

$$T(A) := |\{(x, y, z) \in A^3 : x + y = 2z\}|$$

then

$$Q(A) \leq |A|^3 \text{ and } T(A) \leq |A|^2$$

$$\text{think } |A| \to \infty$$

$$Q(A) := |\{(x,y,z,w) \in A^4 : x+y = z+w\}|$$

and

$$T(A) := |\{(x,y,z) \in A^3 : x+y = 2z\}|$$

then

$$Q(A) \leq |A|^3 \text{ and } T(A) \leq |A|^2$$

think $|A| \to \infty$

'many' means positive proportion of max

easy fact: 'many 3aps $\Rightarrow$ many add. quads.'

easy fact: ‘many 3aps $\Rightarrow$ many add. quads.’

$$T(A) = \sum_{z} 1_{2\cdot A}(z) \sum_{x+y=z} 1_A(x)1_A(y)$$

easy fact: 'many 3aps ⇒ many add. quads.'

$$\begin{aligned} T(A) &= \sum_z 1_{2\cdot A}(z) \sum_{x+y=z} 1_A(x)1_A(y) \\ &\leq |2\cdot A|^{1/2}\left(\sum_z\left(\sum_{x+y=z} 1_A(x)1_A(y)\right)^2\right)^{1/2} = (|A|Q(A))^{1/2} \end{aligned}$$

easy fact: 'many 3aps ⇒ many add. quads.'

$$
\begin{aligned}
T(A) &= \sum_z 1_{2\cdot A}(z) \sum_{x+y=z} 1_A(x)1_A(y) \\
&\leq |2\cdot A|^{1/2}\left(\sum_z\left(\sum_{x+y=z} 1_A(x)1_A(y)\right)^2\right)^{1/2} = (|A|Q(A))^{1/2}
\end{aligned}
$$

so

$$T(A) \geq \delta|A|^2 \Rightarrow Q(A) \geq \delta^2|A|^3.$$

not polynomially equivalent (Behrend):

$$Q(A) \geq \delta|A|^3 \not\Rightarrow T(A) \geq \delta^{O(1)}|A|^2.$$

not polynomially equivalent (Behrend):

$$Q(A) \geq \delta|A|^3 \not\Rightarrow T(A) \geq \delta^{O(1)}|A|^2.$$

maybe

$$Q(A) \geq \delta|A|^3 \Rightarrow T(A) \geq \exp(-O(\log^2 \delta^{-1}))|A|^2?$$

not polynomially equivalent (Behrend):

$$Q(A) \geq \delta|A|^3 \not\Rightarrow T(A) \geq \delta^{O(1)}|A|^2.$$

maybe

$$Q(A) \geq \delta|A|^3 \Rightarrow T(A) \geq \exp(-O(\log^2 \delta^{-1}))|A|^2?$$

hard fact: (Freĭman, Heath-Brown, Ruzsa, Szemerédi)

$$Q(A) \geq \delta|A|^3 \Rightarrow T(A) \geq \exp(-\delta^{-O(1)})|A|^2$$

Arguments

generalisation: $\mathbb{Z} \mapsto$ (Abelian) group

Arguments

generalisation: $\mathbb{Z} \mapsto$ (Abelian) group, 'approximate' group

Arguments

generalisation: $\mathbb{Z} \mapsto$ (Abelian) group, 'approximate' group

$\mathbb{Z} \mapsto \mathbb{F}_3^n$: Bateman-Katz!

Arguments

generalisation: $\mathbb{Z} \mapsto$ (Abelian) group, 'approximate' group

$\mathbb{Z} \mapsto \mathbb{F}_3^n$: Bateman-Katz!

B approximate group $\to$ T_B and Q_B

Arguments

generalisation: $\mathbb{Z} \mapsto$ (Abelian) group, 'approximate' group

$\mathbb{Z} \mapsto \mathbb{F}_3^n$: Bateman-Katz!

B approximate group $\rightarrow$ T_B and Q_B

plan: find an 'approximate' group B so that Q_B and T_B (strongly) polynomially equivalent

Arguments

generalisation: $\mathbb{Z} \mapsto$ (Abelian) group, 'approximate' group

$\mathbb{Z} \mapsto \mathbb{F}_3^n$: Bateman-Katz!

B approximate group $\to$ T_B and Q_B

plan: find an 'approximate' group B so that Q_B and T_B (strongly) polynomially equivalent

($A' := A \cap B$ is large and has $Q_B(A')|A'| \approx T_B(A')^2$)

Arguments

generalisation: $\mathbb{Z} \mapsto$ (Abelian) group, 'approximate' group

$\mathbb{Z} \mapsto \mathbb{F}_3^n$: Bateman-Katz!

B approximate group $\rightarrow T_B$ and Q_B

plan: find an 'approximate' group B so that Q_B and T_B (strongly) polynomially equivalent

($A' := A \cap B$ is large and has $Q_B(A')|A'| \approx T_B(A')^2$)

Bourgain

fact: (Peng, Rödl, Rucinski, Gowers) making Q and T strongly polynomially equivalent *can* be exponentially expensive.

fact: (Peng, Rödl, Rucinski, Gowers) making Q and T strongly polynomially equivalent *can* be exponentially expensive.

good aim

$$Q(A) \geq \delta|A|^3 \Rightarrow T(A) \geq \exp(-\delta^{o(1)})|A|^2?$$

fact: (Peng, Rödl, Rucinski, Gowers) making Q and T strongly polynomially equivalent *can* be exponentially expensive.

good aim

$$Q(A) \geq \delta|A|^3 \Rightarrow T(A) \geq \exp(-\delta^{o(1)})|A|^2?$$

so ~~precise direct counting~~
Bloom, Henriot, Schoen, Shkredov