Today
- Green Tao Theorem
- Dense Model Theorem.

CS5.413.1
Pseudorandomness
Lecture 25 (2021-11-30)
Instructor: Prahladh Harsha.

Szemeredi's Theorem: (weighted version).
$\forall \delta, \ \forall k \geq 3, \ \exists \ c = c(k,\delta)$

$\forall f: \mathbb{Z}_N \to [0,1]$ satisfying $\mathbb{E} f \geq \delta$.
we have.

$$\mathbb{E}_{x,d}\left[f(x) f(x+d) \ldots f(x+(k-1)d)\right] \geq c - o_{k,\delta}(1)$$

$k=3$: Roth's Theorem

Cor: $\forall \delta, k, \ \exists N_0 \ \forall N \geq N_0$
$\forall A \subseteq [N]$, if $|A| \geq \delta N$, then A contains k-AP.

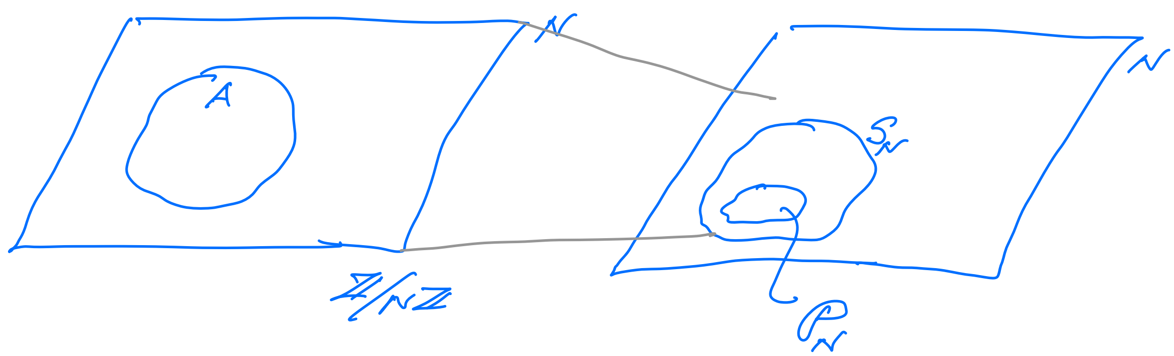
Conjecture (Erdös):
$A \subseteq \mathbb{N}$. satisfying $\sum_{a \in A} \frac{1}{a} \to \infty$
then A contains arbitrarily long AP.

Conj $\Rightarrow$ Primes contain arbitrarily long APs.

Green-Tao: Conj of corollary is in fact true.

For lecture, let us focus on $k=3$.

Proof Outline:



S - almost primes

$$\frac{|A|}{|\mathbb{Z}_N|} \simeq \frac{|P_N|}{|S_N|}$$

S_N is "pseudorandom" (ie, S_N looks like $\mathbb{Z}_N$)

& P_N is "indistinguishable" from A (model dense set).

Corollary (indistinguishability).

$$\frac{\#\{3APs \text{ in } P_N\}}{|S_N|^3} \simeq \frac{\#\{3APs \text{ in } A\}}{N^3}$$

Step 1: Every constant density subset of a pseudorandom set contains 3APs.

Step 2: Primes are a constant density subset of some pseudorandom set.

Step 1: :

1.1: (a) S - "pseudorandom" set

(b) $D \subseteq S$ and $|D| \geq \delta |S|$

$\Downarrow$

(c) $\exists$ a set $A \subseteq \mathbb{Z}_N$ s.t. (i) $|A| \geq \delta N$

D is "indistinguishable" from A

1.2: (a), (b), (c) $\Rightarrow$ D & A contain the same fraction of 3 APs

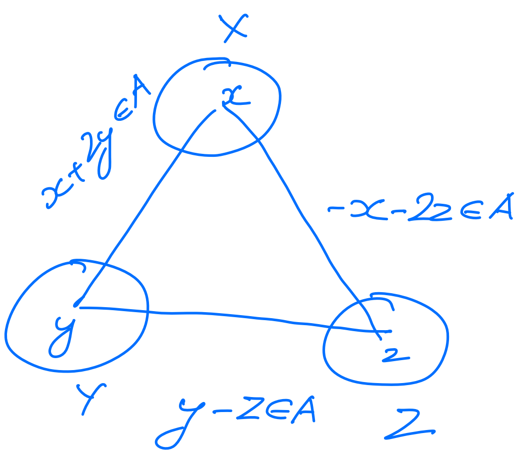
ie, $$\frac{\#\{3APs \text{ in } D\}}{|S|^3} \simeq \frac{\#\{3APs \text{ in } A\}}{N^3}.$$

1.3: There exists a "pseudorandom" set S_N of which the primes.

is a constant density subset.

Pseudorandom & Indistinguishability.

In terms of cut-norm



Recap from last time.

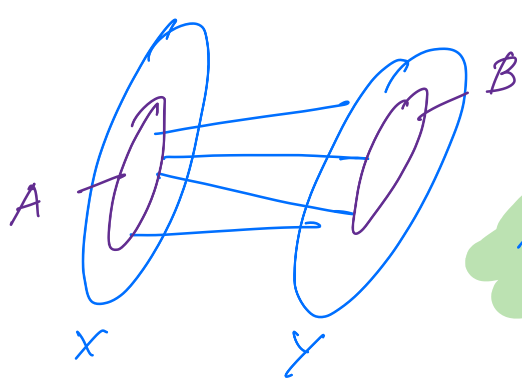
G_A

$A \subseteq [N]$

$x+2y, \quad y-z, \quad -x-2z.$

$-x-y-z \qquad -x-y-z.$

Cut-norm for a bipartite graph.



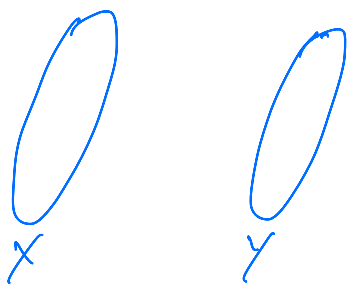
$g: X \times Y \to \mathbb{R}.$

$$\|g\|_\square = \sup_{\substack{A \subseteq X \\ B \subseteq Y}} \left| \mathbb{E}_{\substack{x \in X \\ y \in Y}} \left[g(x,y) 1_A(x) 1_B(y) \right] \right|$$

Not hard to see

$\|g\|_\square$ — norm.

$$\|g\|_\square = \sup_{\substack{a: X \to [0,1] \\ b: Y \to [0,1]}} \left| \mathbb{E}_{x,y}\left[g(x,y)\, a(x)\, b(y) \right] \right|$$



$f: \mathbb{Z}_N \to \mathbb{R}.$

$g_f(x,y) = f(x+y).$

$\|f\|_\square = \|g_f\|_\square$

$$\mathbb{E}_{x,y}\left[f(x+y)\, a(x)\, b(y) \right] = \mathbb{E}_{z}\left[f(z)\, \mathbb{E}_{x}\left[a(x)\, b(z-x) \right] \right]$$
$$= \mathbb{E}_{z}\left[f(z)\, a*b(z) \right]$$
$$= \langle f, a*b \rangle$$

$$\|f\|_\square = \sup_{a,b} \langle f, a*b \rangle$$
$$= \sup_{\substack{\varphi \in \mathrm{Conv}(a*b) \\ a: X \to [0,1] \\ b: Y \to [0,1]}} \langle f, \varphi \rangle$$

<u>Indistinguishability:</u>

$f, f' : \mathbb{Z}_N \to \mathbb{R}$.

$f,$ is ε-indistinguishable from f' if $\|f - f'\|_\square \leq \varepsilon$.

$\nu : \mathbb{Z}_N \to \mathbb{R}$.

measure – $\begin{cases} \nu \geq 0. \\ \mathbb{E}\nu = 1 \end{cases}$

Typically. $S \subseteq [N]$.

$\nu =$ scaled indicator fn.

$= \frac{N}{|S|} 1_S$ (so that $\mathbb{E}\nu = 1$).

ν – like the uniform distribution

$1 : \mathbb{Z}_N \to [0,1]$

$a \mapsto 1$

ν is ε-pseudorandom if $\|\nu - 1\|_\square \leq \varepsilon$.

1.1 (a) S - "pseudorandom" set

(b) $D \subseteq S$ and $|D| \geq \delta |S|$

$\Downarrow$

(c) $\exists$ a set $A \subseteq \mathbb{Z}_N$ s.t. (i) $|A| \geq \delta N$

D is "indistinguishable" from A

Formalize this.

ν — measure corresponding to set S.

$S \subseteq \mathbb{Z}_N \quad \longleftrightarrow \quad \nu : \mathbb{Z}_N \to \mathbb{R}_{\geq 0}$

$D \subseteq S. \quad \longleftrightarrow \quad f : \mathbb{Z}_N \to \mathbb{R}_{\geq 0}.$

$\forall x \quad f(x) \leq \nu(x)$

$|D| \geq \delta |S| \quad \longleftrightarrow \quad \mathbb{E} f \geq \delta$

(Typically, $\nu = \frac{N}{|S|} 1_S$

$f = \nu \cdot 1_D$)

Theorem [Dense Model Theorem [Gowers RTTV]

$\forall \varepsilon, \exists \varepsilon'$ such that $\forall \nu, f$. sat.

(a). $\nu : \mathbb{Z}_N \to \mathbb{R}_{\geq 0}$ is ε'-pseudorandom

$\mathbb{E}\nu = 1$

&

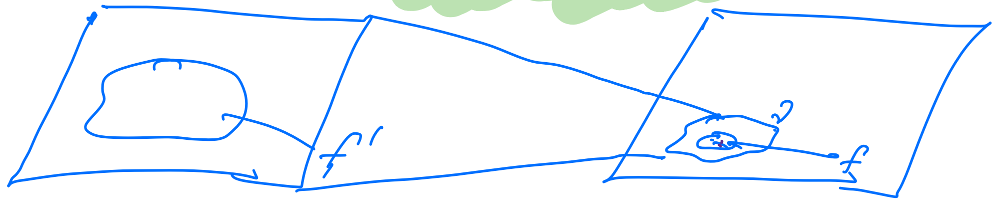
(b). $f : \mathbb{Z}_N \to \mathbb{R}_{\geq 0}$. s.t. $f \leq \nu$

& $\mathbb{E} f = \delta$

then (c) $\exists f' : \mathbb{Z}_N \to [0,1]$ s.t. $f' \leq 1$

6. $\mathbb{E} f' = \mathbb{E} f$

& $\|f - f'\|_\square \leq \varepsilon$.



$$\|f\|_\square = \sup_{\varphi \in \Phi} \langle f, \varphi \rangle$$

Φ is closed under multiplication.

$$\Phi = \mathrm{Conv}\{ \mathbb{1}_A \otimes \mathbb{1}_B \mid A \subseteq X,\ B \subseteq Y \}.$$

Formalize Step 1.2.

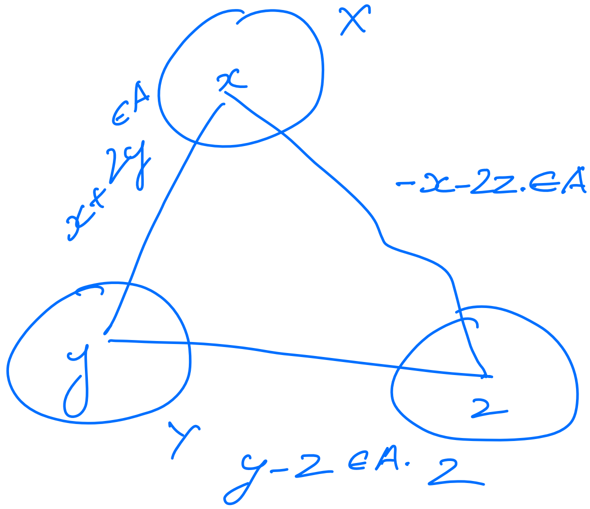
1.2 : (a), (b), (c) $\Rightarrow$ D & A contain the same fraction of 3 APs.

i.e. $\dfrac{\#\{3\text{APs in } D\}}{|S|^3} \cong \dfrac{\#\{3\text{APs in } A\}}{N^3}$.

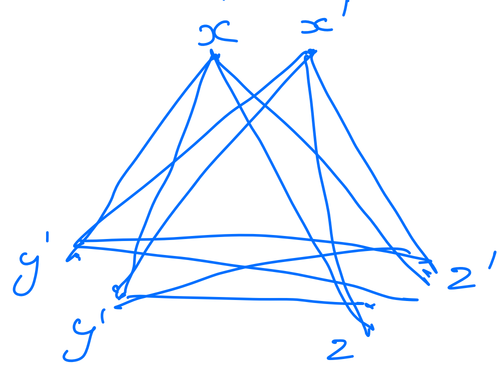
ν - ε-pseudorandom if $\|\nu - \mathbb{1}\|_\square \leq \varepsilon$.

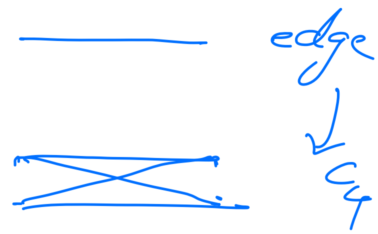
where $\nu \geq 0$; $\mathbb{E}\nu = 1$.

Modify the defn of pseudorandom



$K_{2,2,2}$.





2-blowup of $K_3 = K_{2,2,2}$.

$\nu : \mathbb{Z}_N \to \mathbb{R}_{\geq 0}$, $\mathbb{E}\nu = 1$

satisfies the 3-linear conditions

$$\mathbb{E}_{\substack{x,x'\\y,y'\\z,z'}} \Big[\nu(x+2y)\,\nu(x+2y')\,\nu(x'+2y)\,\nu(x'+2y') \\ \nu(y-z) \cdots \\ \nu(-x-2z) \cdots \Big] = 1 \pm o(1)$$

(for $K_{2,2,2}$ & all subgraphs).

Counting Lemma:

If ν satisfies 3 linear conditions

& $f: \mathbb{Z}_N \to \mathbb{R}_{\geq 0}$; $f \leq \nu$.

& $f': \mathbb{Z}_N \to [0,1]$, $\|f-f'\|_{\square} \leq o(1)$

then.

$$\mathbb{E}[f(x,y)f(y,z)f(z,x) - f'(x,y)f'(y,z)f'(z,x)] = o(1).$$

(Remark: ν satisfies 3 linear cond

$\Downarrow$

ν is $o(1)$-pseudorandom.)

Theorem [Relative Roth Theorem].

Suppose $\nu: \mathbb{Z}_N \to [0,\infty)$ satisfies the 3-linear condition & $f: \mathbb{Z}_N \to [0,\infty)$ s.t. $f \leq \nu$. $\mathbb{E}f = \delta$.

then $\mathbb{E}_{x,d}[f(x)f(x+d)f(x+2d)] \geq c(3,\delta) - o(1)$