Tao's Lecture notes: Chapter 1

Abelian Group G, usually integers $\mathbb{Z}$ or $\mathbb{Z}_p$ for a large prime p.

Notation:

$A, B \subseteq G$.

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

$$A+A = 2A$$

$$2 \cdot A = \{2a : a \in A\}$$

Typical Question

If

$$|A+A| \leq c|A|$$

where A is "large" and c is "small"

then what can we say about A.

Example

(i) $A = \{a + jr : 1 \le j \le N\} \subseteq \mathbb{Z}$ arithmetic progression

$$|A+A| = 2|A| - 1$$

(ii) $A = \{a + j_1 r_1 + \cdots + j_d r_d : 1 \le j_s \le N_s$ for $s = 1, 2, \ldots, d\}$

Generalised Arithmetic Progression

$$|A+A| = \prod_{j=1}^{d} (2N_j - 1)$$

$$\approx 2^d |A|$$

2. Bounds on $A+B$

L2.1

$$A, B \subseteq \mathbb{Z} \Rightarrow |A+B| \geq |A|+|B|-1$$

Proof

Result is not affected by replacing

$A \longrightarrow A+\{x\}$, $B \longrightarrow B+\{y\}$

Assume $\max A = 0 = \min B$

$$A+B \supseteq A \cup B$$

$$\Rightarrow |A+B| \geq |A \cup B| = |A|+|B|-1.$$

$\square$

Exercise: $A, B \subseteq G$

$|A+B| = |A| \Rightarrow$ $A \subseteq \bigcup$ cosets of finite subgroup H

$B \subseteq$ coset of H.

Thm 2.5

Cauchy-Davenport Inequality

$A, B \subseteq \mathbb{Z}_p \Rightarrow |A+B| \geq \min\{|A|+|B|-1, p\}$

Proof

Suppose $|A|+|B|-1 \geq p$.

By PHP $\quad A \cap (x-B) \neq \emptyset \quad \forall x \in \mathbb{Z}_p$

$\Rightarrow x \in A+B, \quad \forall x \in \mathbb{Z}_p$

$\Rightarrow |A+B| \geq p.$

Proof by contradiction

(ii) Suppose $|A+B| < |A| + |B| - 1 \leq p$

Can assume $|A| \geq 1$ and that $A \cap B \neq \emptyset$

(translate A).

Now assume $|A|$ is as small as possible.

Dyson Transform: $A' = A \cap B$, $B' = A \cup B$

(i) $|A'| + |B'| = |A| + |B|$

(ii) $A' + B' = A' + (A \cup B) \subseteq (A' + B) \cup (A' + A)$

$\subseteq (A+B) \cup (B+A) = A+B$.

So A', B' is a smaller counter-example unless $A \subseteq B$.

Conclusion: If A, B minimal counter-example & $A \cap B \neq \emptyset$ then $A \subseteq B$.

More generally

$$\Rightarrow \quad A + x \subseteq B \quad \forall\, (A+x) \cap B \neq \emptyset$$

or $x \in B - A$

$$\Rightarrow \quad A + B - A \subseteq B$$

$$B + A - A \subseteq B$$

$$\underset{A}{B} + A \underset{B}{-} A = B$$

$\Rightarrow$ (by exercise 3)

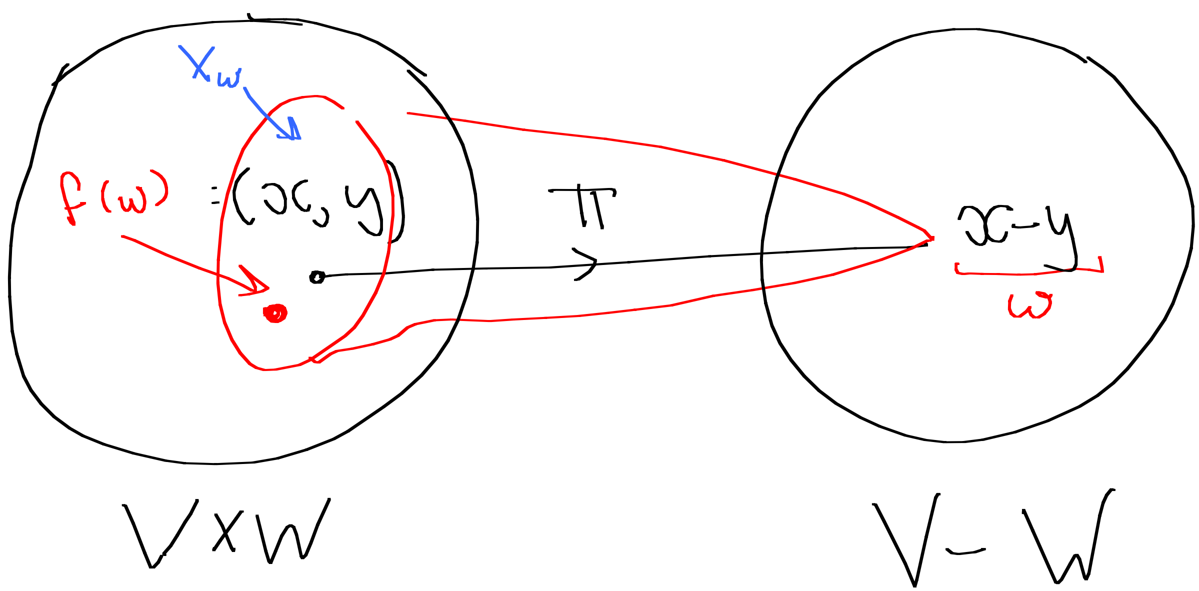
B is a coset of $\mathbb{Z}_p$

$B = \{x\}$ or $\mathbb{Z}_p$

L 3.1 Ruzsa

If $U, V, W \neq \emptyset \subseteq G \Rightarrow |V-W| \leq \dfrac{|U+V|\,|U+W|}{|U|}$

Proof



$$U^{\Delta} = \{ (u,u) : u \in U \}$$

$$(V \times W) + U^{\Delta} \subseteq \underbrace{(U+V) \times (U+W)}$$

(i) $w \in V - W \Rightarrow f(w) + U^{\Delta} \subseteq$

(ii) $|f(w) + U^{\Delta}| = |U|$

(iii) $\underbrace{(f(w_1) + U^{\Delta}) \cap (f(w_2) + U^{\Delta})} = \emptyset$

$w_1 \neq w_2$

$x \in$.

$\pi(x) = \pi(f(w_i))$.

$$|V - W| \cdot |U| \leq |(U+V) \times (U+W)|.$$

$\square$

So if

(i) $|A+B| \leq \alpha A$ and $|A'+B| \leq \alpha' |A'|$

$$|A-A'| \leq \frac{|A+B|\ |A'+B|}{|B|} \leq \frac{\alpha\alpha' |A|\,|A'|}{|B|}$$

(ii) $|A+B| \leq \alpha |A|$, $|A+B'| \leq \alpha' |A|$

$$|B-B'| \leq \frac{|A+B| \cdot |A+B'|}{|A|} \leq \alpha\alpha' |A|$$

? $|A+A'| \leq ?$ $|B+B'| \leq ?$

Plünecke's Theorem!

Plünnecke's Theorem

Suppose $A, B \subseteq G$ and

$|A+B| \leq K|A|$.

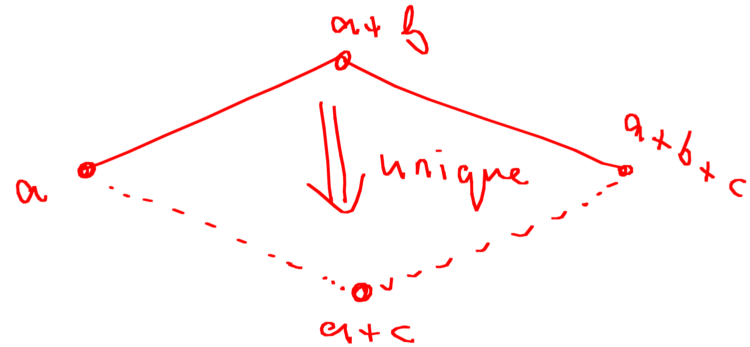
Then

$\exists A' \subseteq A$, $A' \neq \emptyset$ such that

$$|A'+B+B| \leq K^2 |A'|$$

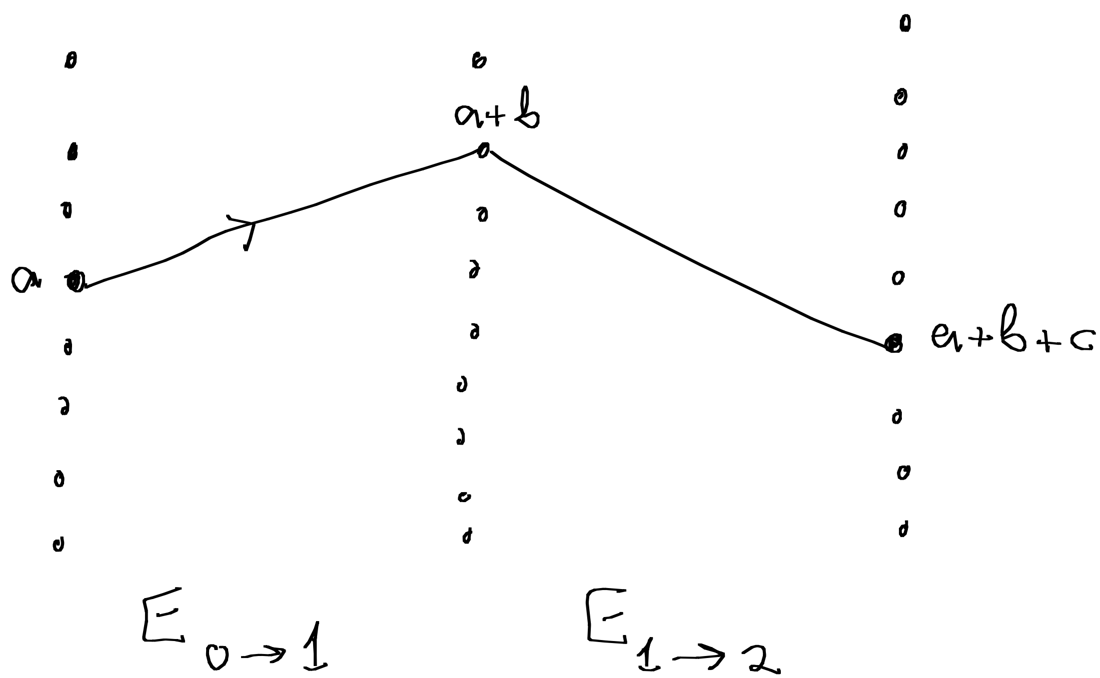
Commuting Graph:

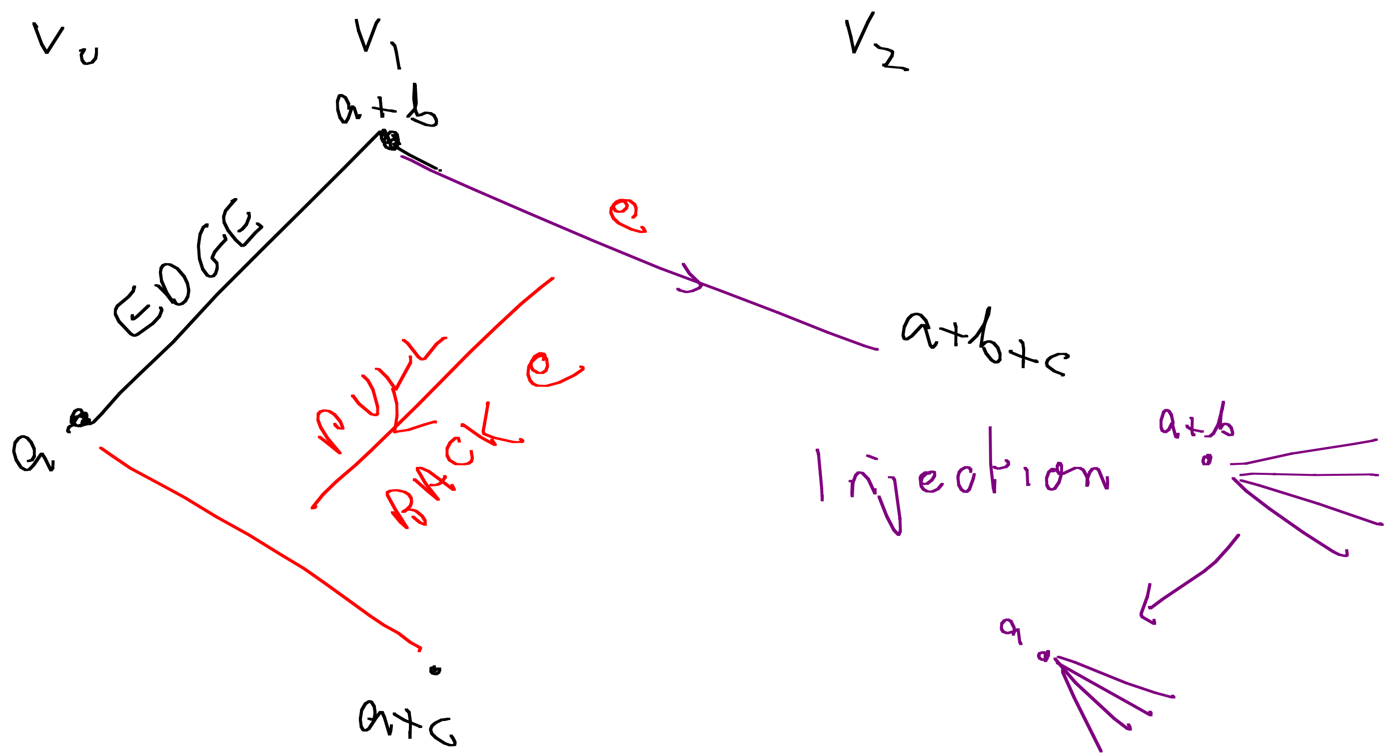
Key Property:

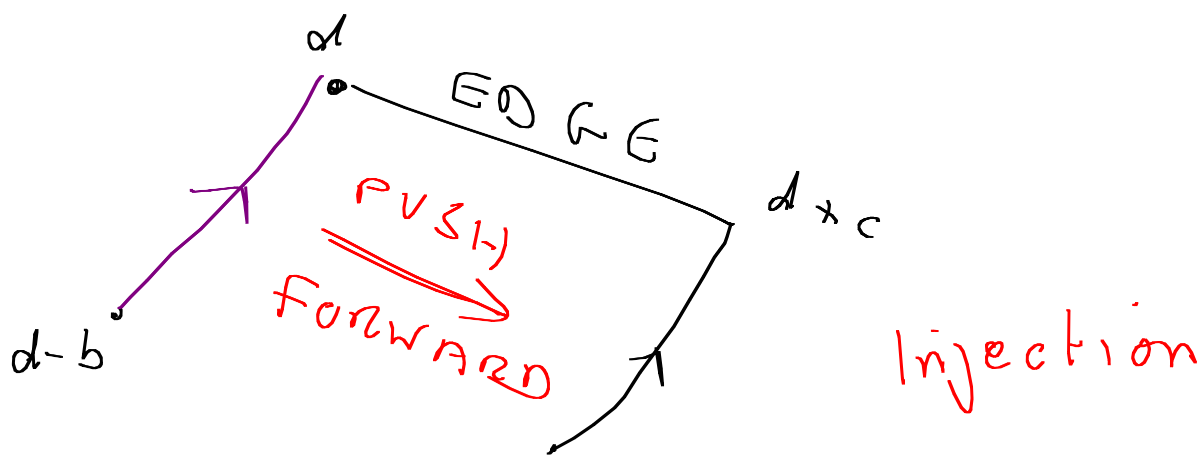


$\Gamma(A,B)$ graph

$V_0 = A$ $\quad V_1 = A+B$ $\quad V_2 = A+B+B$




V0
V1
V2
a+b
EDGE
e
a+b+c
PULL BACK e
a
a+c
Injection
a+b
a


d
EDGE
d+c
PUSH FORWARD
d-b
Injection

Can assume V_0, V_1, V_2 are pairwise disjoint

$$
\begin{array}{ccc}
V_0 & V_1 & V_2 \\
\downarrow & \downarrow & \downarrow \\
V_0 \times \{0\} & V_1 \times \{1\} & V_2 \times \{2\}
\end{array}
$$

Disjoint from picture, we use picture.

Theorem now says:

Let Γ be a commuting graph such that $|V_1| < K|V_0|$

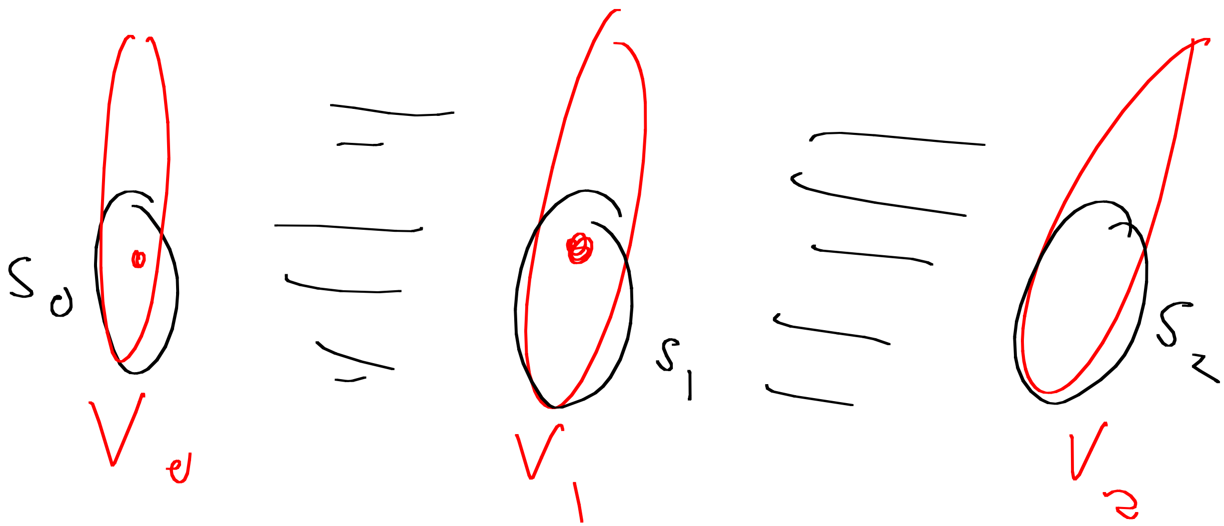
Then $\exists$ $A' \subseteq V_0$ such that

$|\Gamma^2(A)| \leq K^2|A'|$.

Assume first that $k=1$

$$s = \text{MAXFLOW}(V_0 \to V_2 ; \Gamma) \le |V_1| < |V_0|$$

vertex disjoint



Each vertex has capacity 1

By Menger's theorem $\exists\, S = S_0 \cup S_1 \cup S_2$ s.t.

(i) $|S| = s$ & (ii) all $V_0 \to V_2$ paths use S.

Aim to show there exists

$W_0 \subseteq V_0 \setminus S_0$ and $W_2 \subseteq V_2$

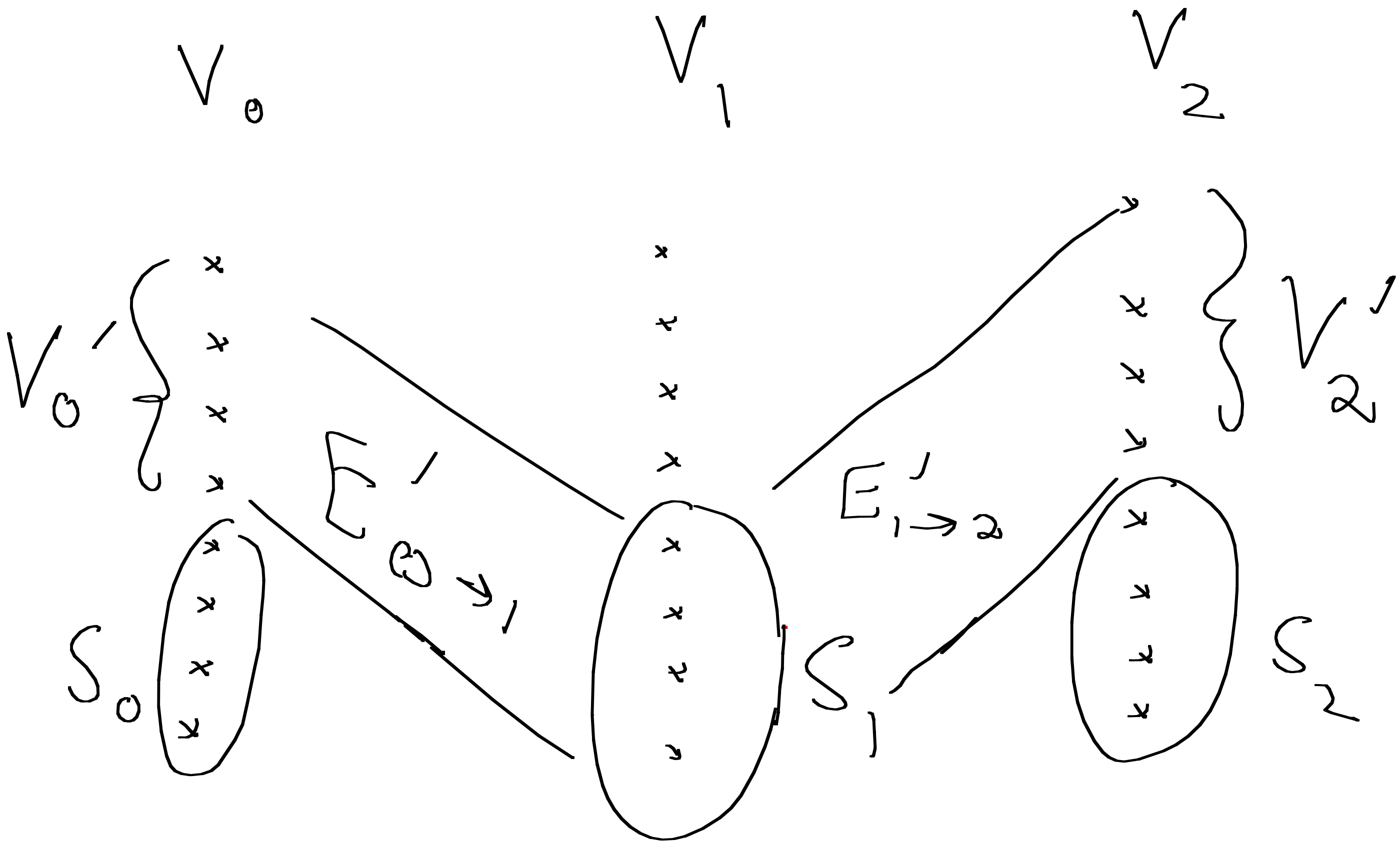
such that $S_0 \cup W_0 \cup W_2$

is minimum "cut".

$A' = V_0 / (S_0 \cup W_0)$.

Then

$$\Gamma^2(A') \subseteq W_2 \ \& \ |W_2| = s - |S_0 \cup W_0| < |A'|$$



Γ' = graph made from edges

$V_0' \longrightarrow V_2'$

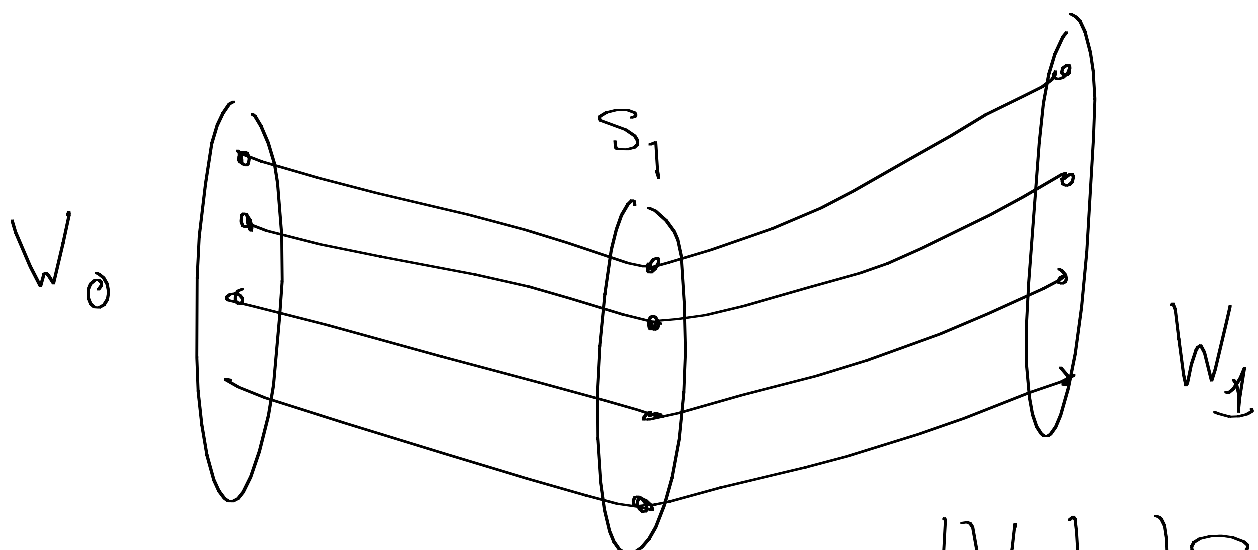
Edges $E'_{0\to 1} \cup E'_{1\to 2}$

(a) S_1 disconnects V_0 from V_2 in Γ'

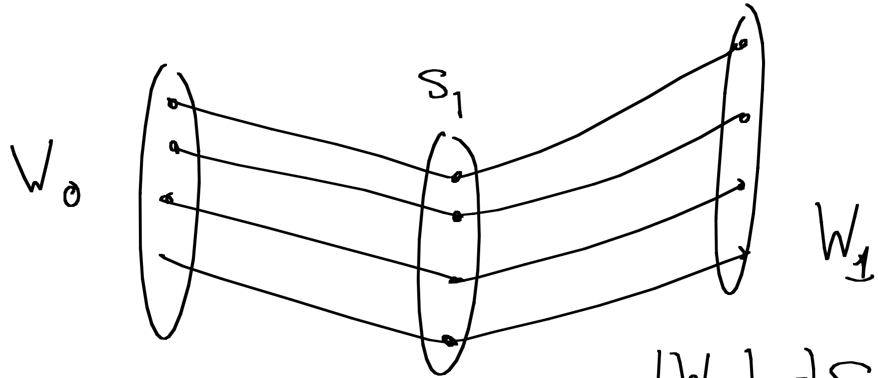
(b) $|S_1| = \text{MINCUT}(V_0', V_2'; \Gamma')$

[otherwise we can reduce size of S]

Hence $\exists$ $|S_1|$ vertex disjoint paths $V_0' \to V_2'$



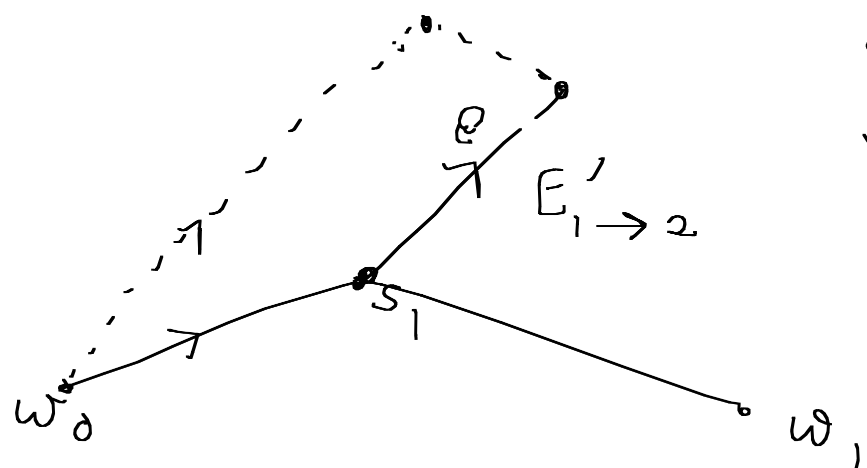
$|W_0| = |S_1| = |W_1|$



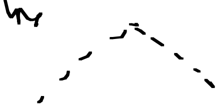
$|W_0| = |S_1| = |W_1|$

Now show $E'_{0 \to 1} = W_0$

and therefore $S_0 \cup W_0 \cup S_2$ is a cut set



e gives s_1
s_1 gives w_0
gives



Define injection: $E'_{1 \to 2}$ to W_0

Define injection: $E'_{1\to 2}$ to $W_0^{\nearrow\rightarrow\searrow}$

Similarly

Define injection $E'_{0\to 1}$ to ${}^{\nearrow\rightarrow\searrow}W_2$

$$\left|{}^{\nearrow\rightarrow\searrow}W_2\right| \le \left|E'_{1\to 2}\right| \le \left|W_0^{\nearrow\rightarrow\searrow}\right| \le$$

$$\left|E'_{0,1}\right| \le \left|{}^{\nearrow\rightarrow\searrow}W_2\right|$$

Therefore $\left|E'_{0\to 1}\right| = \left|W_0^{\nearrow\rightarrow\searrow}\right|$

$\Gamma, \hat{\Gamma}$ two commuting graphs on $G, \hat{G}$.

$\Gamma \times \hat{\Gamma}$ $\quad V_0 \times \hat{V}_0 \quad V_1 \times \hat{V}_1 \quad V_2 \times \hat{V}_2$

$E_{0\to 1} \times \hat{E}_{0\to 1}$

$$((a \to b), (\hat{a} \to \hat{b})) \equiv (a, \hat{a}) \to (b, \hat{b})$$

$\Gamma \times \hat{\Gamma}$ is commuting: treat coordinates independently in diagram.

$$(a, a') \to (a+b,\ a'+b') \to (a+b+c,\ a'+b'+c')$$

$$D(\Gamma) = \inf_{\substack{A' \subseteq V_0 \\ A' \neq \emptyset}} \frac{|\Gamma^2(A')|}{|A'|}$$

$\underline{\text{Prop}}$

$$D(\Gamma \times \hat{\Gamma}) = D(\Gamma) \cdot D(\hat{\Gamma})$$

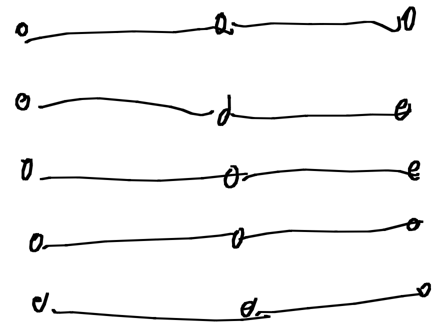
$d \qquad \hat{d}$

(1) $A', \hat{A}'$: $|(\Gamma \times \hat{\Gamma})^2 (A' \times \hat{A}')| = d\hat{d}\, |A'|\,|\hat{A}'|$

$D(\Gamma \times \hat{\Gamma}) \geq d\hat{d}$

(11)

I_{V_0}

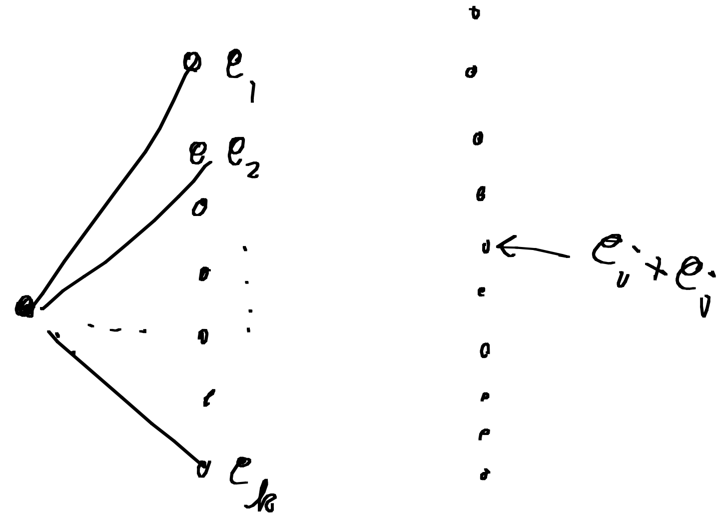


$$(\Gamma \times \hat{\Gamma})^2(\Omega) = (\Gamma \times I_{\hat{V}_2})^2 (I_{V_0} \times \hat{\Gamma})^2(\Omega)$$

$\Omega \subseteq V_0 \times \hat{V}_0$

$$|\sim| \leq d \hat{d} \; |\Omega|$$

Γ_k :

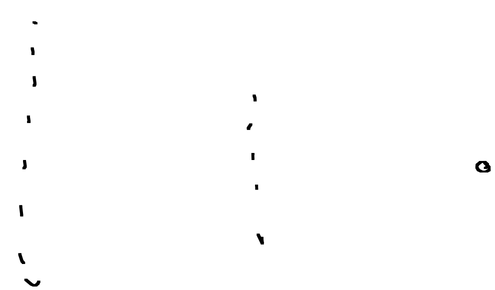


$e_i = [0, 0, \dots 1, \dots, 0] \in \{0,1\}^k$

$D(H_k) = \frac{k(k-1)}{2}$

$H_k^+ =$ renepe

$D(H^+) = \frac{1}{\binom{k}{2}}$



End of proof

$$\frac{|V_1|}{|V_0|} < K. \quad \text{Choose integer } k \in [2K+1, 2K+2]$$

$$\frac{k-1}{2} \in [K, K+\tfrac{1}{2}]$$

$$\text{such } \frac{|V_1|}{|V_0|} \cdot \frac{2}{k-1} < 1$$

$$\rho(\underbrace{\Gamma \times H_k^+}) < 1$$

Why

$$V_0 \times \{\tbinom{k}{2}\}$$

$$V_1 \times \{k\}$$

$$\frac{k|V_1|}{\binom{k}{2}|V_0|} < 1$$

by $K<1$ case

$$D(\Gamma) < \frac{1}{D(H_6^+)} = \frac{k(k-1)}{2} \leq 10K^2$$

Removing (10)

$$D(\Gamma)^M = D(\Gamma \times \Gamma \times \cdots \times \Gamma) \leq 10K^{2M}$$

$$\frac{V_1}{V_0} \text{ ratio} \leq K^m$$

Take M'th roots.

Boosting the size of A':

Let $A, B \subseteq G$ be such that $|A+B| \leq K|A|$ and suppose $0 < \delta < 1$. Then $\exists\, A' \subseteq A$ s.t. $|A'| \geq (1-\delta)|A|$ and such that $|A'+B+B| \leq \frac{2K^3}{\delta}|A|$.

Proof

$A_0 = A$,

$\exists\, A_0' \subseteq A_0 : |A_0' + B + B| \leq \frac{|A_0+B|^2}{|A_0|^2}|A_0'| \leq \frac{K^2|A|^2}{|A_0|^2}|A_0'|$

$A_1 = A_0 \setminus A_0'$: If $|A_1| < \delta|A|$ stop.

$\exists\, A_1' \subseteq A_1 : |A_1' + B + B| \leq \frac{|A_1+B|^2}{|A_1|^2}|A_1'| \leq \frac{K^2|A|^2}{|A_1|^2}|A_1'|$

$$\vdots$$

$$\exists\, A'_{k-1} \subseteq A_{k-1} \;:\; |A'_{k-1} + B + B| \leq \frac{K^2|A|^2}{|A_{k-1}|^2}\, |A'_{k-1}|$$

$$A_k = A_{k-1} \setminus A'_{k-1} \quad \& \quad |A_k| < \delta |A|.$$

$$A' = A \setminus A_k \quad \& \quad |A'| > (1-\delta)|A|,$$

$$|A' + B + B| \leq \sum_{j=0}^{k-1} |A'_j + B + B|$$

$$\leq \sum_{j=0}^{k-1} \frac{K^2 |A|^2}{|A_j|^2} |A'_j|$$

$$= K^2 |A|^2 \sum_{j=0}^{k-1} \frac{|A_j| - |A_{j+1}|}{|A_j|^2}$$

$$\leq K^2 |A|^2 \left[\frac{1}{|A_{k-1}|} + \sum_{j=0}^{k-2} \frac{|A_j| - |A_{j+1}|}{|A_j|^2} \right]$$

$$\leq K^2 |A|^2 \left[\frac{1}{|A_{k-1}|} + \sum_{j=0}^{k-2} \frac{|A_j| - |A_{j+1}|}{|A_j|\,|A_{j+1}|} \right]$$

$$= k^2 |A|^2 \left[\frac{1}{|A_{k-1}|} + \sum_{j=0}^{k-1} \left(\frac{1}{|A_{j+1}|} - \frac{1}{|A_j|} \right) \right]$$

$$\leqslant \frac{2k^2|A|^2}{|A_{k-1}|}$$

$$\leqslant \frac{2k^2|A|}{\delta}.$$

$A' = A$ is not always possible

Example from Ruzsa.

$G = \mathbb{Z}^2$. $\quad B = [n] \times \{0\} \cup \{0\} \times [n]$

$|B| = 2n, \quad |B+B| \approx n^2$

$A_0 = [n] \times [n]$

$A_1 = \{(a_1, a_1), (a_2, a_2), \dots, (a_n, a_n)\}$

where $|a_{j+1} - a_j| \gg n$

$A = A_0 \cup A_1$

$|A| \approx n^2; \quad |A+B| \approx 3n^2; \quad |A+B+B| \approx n^3$

Iterated Plünnecke

$A, B \subseteq G$ and $|A+B| \leq K|A|$. Then

for $t = 1, 2, \ldots$

$\exists A_t \subseteq A$ such that $|A_t + tB| \leq K^{2t} |A_t|$

Should be K^t

~~Proof~~

(1) $t = 2^k$.

$\exists A_2 \subseteq A : |A_2 + B + B| \leq K^2 |A_2|$

$\exists A_4 \subseteq A_2 : |A_4 + (B+B) + (B+B)| \leq K^4 |A_4|$

$\vdots$

(1)

$$2^{k-1} < t < 2^{k}$$

any $b \in B$

t_1

$$|A_{t_1} + tB| = |A_{t_1} + tB + \underbrace{b + b + \cdots + b}_{t_1 - t}|$$

$$\le |A_{t_1} + t_1 B|$$

$$\le K^{t_1} |A_{t_1}|$$

$$\le K^{2t} |A_{t_1}|.$$

$2t$ should be t.

Cor. 8.2

$$|A+B| \leq K|A| \Rightarrow |mB-nB| \leq K^{4\max\{m,n\}}|A|$$

Proof

(i) $$|mB-mB| \overset{L3.1}{\leq} \frac{|A_m+mB|^2}{|A_m|} \leq K^{4m}|A|.$$

$U_m \xrightarrow{L3.1} |A_m|$

(ii) Suppose $m \leq n$

$$|mB-nB| = |\underbrace{b+b+\cdots+b}_{n-m}+mB-nB| \leq |nB-nB| \leq K^{4n}|A|.$$

Covering one set by another

L 9.1 (Ruzsa)

$$\exists X : |X| \leq \frac{|A+B|}{|A|} \text{ and } B \subseteq X + A - A$$

Proof

Let $U_b = b + A$ for $b \in B$

$\mathcal{F}$ = maximal disjoint family of U_b's.

(i) $|\mathcal{F}| \leq \dfrac{|A+B|}{|A|}$ $\quad X = \{b : U_b \in \mathcal{F}\}$

(ii) $b \in B \Rightarrow \exists x \in X$ s.t. $b + A \cap x + A \neq \emptyset$

$\Rightarrow b \in x + A - A$.

Thm 9.2

$A \subseteq G$ and $|A+A| \leq K|A|$, $K = O(1)$.

$|A| = N$.

$\exists |X| = O(\log N)$ such that $B = mA - nA \subseteq X + A$.

Lemma 9.4

$A, B \subseteq G$, $\exists Y$, $|Y| \leq \frac{2|A+B|}{|A|}$ s.t. (I) $B \subseteq Y + A - A$

(II) $\forall b \in B$, $\exists \geq \frac{|A|}{2}$ triples (y, a, a') s.t. $y + a - a' = b$.

Lemma 9.4

$A, B \subseteq G$, $\exists Y$, $|Y| \leq \frac{2|A+B|}{|A|}$ s.t. (i) $B \subseteq Y + A - A$

(ii) $\forall b \in B$, $\exists \geq \frac{|A|}{2}$ triples (y, a, a') s.t. $y + a - a' = b$.

$r = L \log N$, $L \gg |Y| = O(1)$

Choose $X^* \subseteq Y \times A$; $\Pr((y, a') \in X^*) = \frac{r}{N|Y|}$

(i) $|X^*| \equiv \mathrm{Bin}\left[N|Y|, \frac{r}{N|Y|}\right]$

$$\Pr(|X^*| \geq 2r) \leq e^{-r/3}$$

(ii) Fix $b \in B$: $\Pr[\text{No } (y, a') \text{ is chosen}] \leq \left(1 - \frac{r}{N|Y|}\right)^{N/2}$

$\exists a \quad y + a - a' = b$

$\leq e^{-\frac{r}{2|Y|}} \leq N^{-\frac{L}{2|Y|}}$

$\leq \frac{1}{N}$.

$\exists$ choice of X^* s.t. (i) $|X^*| \leq 2r$ & (ii) $\forall b \in B$, $\exists \underbrace{y + a - a' = b}$

$|X| \leq 2r$

$X = \{ x - a' : (x, a') \in X^* \}$

$b \in X + A$.

Lemma 9.4

$A, B \subseteq G$, $\exists Y$, $|Y| \leq \frac{2|A+B|}{|A|}$ s.t. (I) $B \subseteq Y + A - A$

(II) $\forall b \in B$, $\exists \geq \frac{|A|}{2}$ triples (y, a, a') s.t. $y + a - a' = b$.

$Y = \emptyset$

If $\exists y \in B$ s.t. $|(y+A) \cap (Y+A)| < \frac{|A|}{2}$, $Y \to Y + y$

Each addition increases $|Y + A|$ by $|A|/2$.

Final $|Y| \leq \frac{|A+B|}{|A|}$;

$b \in B \Rightarrow |(b+A) \cap (Y+A)| \geq \frac{|A|}{2}$

$b + a' = y + a$

Sum and Product

We show that $\max\{|A+A|, |A\cdot A|\} = \Omega(|A|^{5/4})$.

(a) Crossing Number

For a graph G, $cr(G)$ = min. # edge crossings of any plane drawing of G.

If $G = (V, E)$, $|V| = n$, $|E| = m$ and $m \geq 4n$

then
$$cr(G) \geq \frac{m^3}{64n^2}$$

[Ajtai, Chvatal, Newborn, Szemerédi
Leighton]

(I) $t = cr(G) \geq m - (3n-6) > m - 3n.$

(II) $H = G[S]$ (induced by S)

$P_r(v \in S) = p$

$E(|V(H)|) = np$; $E(|E(H)|) = mp^2$;

$E(cr(H)) = tp^4.$

So $tp^4 \geq \;\; \geq mp^2 - 3np$

$t \geq \frac{m}{p^2} - \frac{3n}{p^3}$

Choose $p = \frac{4n}{m} \leq 1$

to maximise RHS

$t \geq \frac{m^3}{64n^2}.$

$\square$

Point Line Incidences [Szemeredi, Trotter]

Someone elses proof ∵? Solymosi?

Let $P = \{ n \text{ points in plane} \}$

$L = \{ m \text{ lines in plane} \}$

$I = \{ \text{incidences } (x, \ell) : x \in P, \ell \in L, x \in \ell \}$

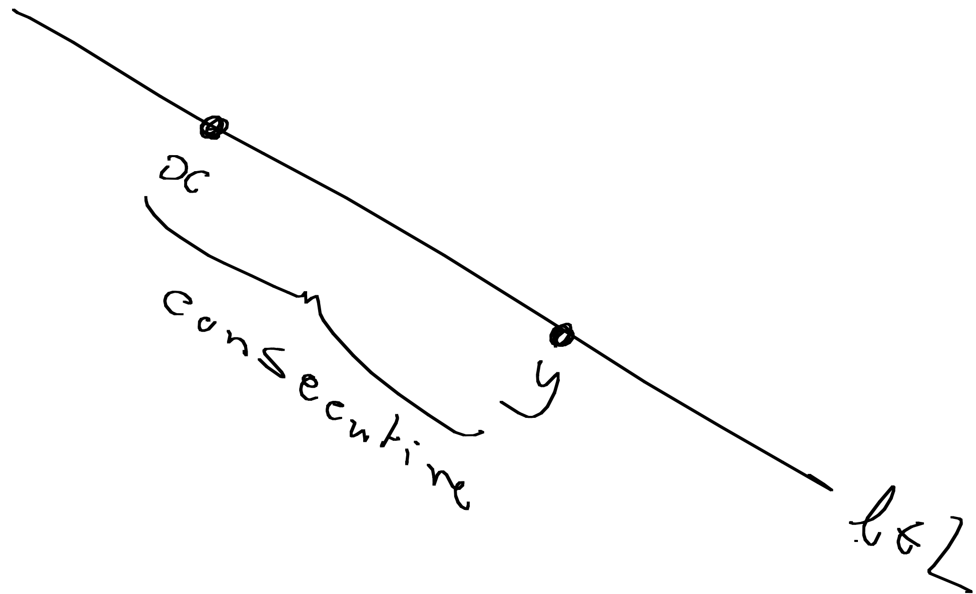
$$|I| < 4 (m^{2/3} n^{2/3} + m + n \}$$

Proof

$G = (P, E)$

P: n vertices

$|I| - m$ edges



$$cr(G) \le \binom{m}{2}$$

(i) $|I| - m < 4n$ or (ii) $\binom{m}{2} \geq cr(G) \geq \dfrac{(|I| - m)^3}{64 n^2}$

In both cases

$$|I| < 4\left(m^{2/3} n^{2/3} + m + n\right)$$

L 1

For any sets $A, B, C \subseteq \mathbb{R}$, $|A| = |B| = |C| = s$

$$|A \cdot B + C| = |\{ab + c\}| = \Omega(s^{3/2}).$$

Proof

$R = A \cdot B + C$; $|R| = r$.

$P = \{(a, t) : a \in A, t \in R\}$

$L = \{y = bx + c : b \in B, c \in C\}$

$|P| = sr$; $|L| = s^2$

$y \in L$ is incident to s points $P : (a, ab + c)$

$$s^3 \leq 4\left(s^{4/3}(sr)^{2/3} + sr + s^2\right).$$

Let A, B, C be finite sets of Reals

$$|A+B| \times |A \cdot C| = \Omega\left(|A|^3 |B| |C|\right)^{1/2}$$

[If $A = B = C$ & $|A| = n$ then $|A+A| \times |A \cdot A| = \Omega(n^{5/2})$.]

Proof

$$P = \{ (a+b, \hat{ac}) \} \qquad |P| = \overbrace{|A+B| \times |A \cdot C|}^{X}$$

$$L = \{ y = c(x-b) \} \qquad |L| = |B| \cdot |C|$$

Each $l \in L$ contains $|A|$ points, $y = ac$, $x = a+b$

$$|A| \cdot |B| \cdot |C| \leq 4\left(|B|^{2/3} |C|^{2/3} X^{2/3} + |B| \cdot |C| + X \right)$$

$$|A| \cdot |B| \cdot |C| \leq 4\left(|B|^{2/3}|C|^{2/3}X^{2/3} + |B|\cdot|C| + X\right)$$

[To show $X = \Omega\left(|A|^{3/2}|B|^{1/2}|C|^{1/2}\right)$]

(I) $|A|$ is small, $X \geq |B|\cdot|C|$

(II) $|A|$ is large, drop $|B|\cdot|C|$ from RHS.

Show

$$|A|\cdot|B|\cdot|C| \leq 3\left(|B|^{2/3}|C|^{2/3}X^{2/3} + X\right).$$

(a) $X \leq |B|^2|C|^2 \Rightarrow X \leq |B|^{2/3}|C|^{2/3}X^{2/3}$

$$|A|\cdot|B|\cdot|C| \leq 6|B|^{2/3}|C|^{2/2}X^{2/3} \quad \checkmark$$

(b) $X \geq |B|^2 |C|^2$

$X \geq |A|^2$

$X \geq |A| |B| |C|$

$X^2 \geq |A|^3 |B| |C|$.

Roth's Theorem

Fix $0 < \delta < 1$. If n is large enough and $A \subseteq [n]$, $|A| = \delta n$ then

A contains x, y, z s.t. x, y, z form a 3-term arithmetic progression

$$y = \frac{1}{2}(x+z).$$

$\delta = \frac{C}{\log\log n}$ works here.

Gowers

Lecture 6

We are now ready to prove the triangle removal lemma.

Theorem 1 (Triangle removal lemma) *For every $\epsilon > 0$ there exists $\delta > 0$ such that, for any graph G on n vertices with at most δn^3 triangles, it may be made triangle-free by removing at most ϵn^2 edges.*

Proof Let $X_1 \cup \cdots \cup X_M$ be an $\frac{\epsilon}{4}$-regular partition of the vertices of G. We remove an edge xy from G if

1. $(x, y) \in X_i \times X_j$, where (X_i, X_j) is not an $\frac{\epsilon}{4}$-regular pair;
2. $(x, y) \in X_i \times X_j$, where $d(X_i, X_j) < \frac{\epsilon}{2}$;
3. $x \in X_i$, where $|X_i| \leq \frac{\epsilon}{4M} n$.

The number of edges removed by condition 1 is at most $\sum_{(i,j)\in I} |X_i||X_j| \leq \frac{\epsilon}{4} n^2$. The number removed by condition 2 is clearly at most $\frac{\epsilon}{2} n^2$. Finally, the number removed by condition 3 is at most $Mn\frac{\epsilon}{4M}n = \frac{\epsilon}{4}n^2$. Overall, we have removed at most ϵn^2 edges.

Now, suppose that some triangle remains in the graph, say xyz, where $x \in X_i$, $y \in X_j$ and $z \in X_k$. Then the pairs (X_i, X_j), (X_j, X_k) and (X_k, X_i) are all $\frac{\epsilon}{4}$-regular with density at least $\frac{\epsilon}{2}$. Therefore, since $|X_i|, |X_j|, |X_k| \geq \frac{\epsilon}{4M} n$, we have, by the counting lemma that the number of triangles is at least

$$\left(1 - \frac{\epsilon}{2}\right)\left(\frac{\epsilon}{4}\right)^3\left(\frac{\epsilon}{4M}\right)^3 n^3.$$

Taking $\delta = \frac{\epsilon^6}{2^{20} M^3}$ yields a contradiction. □

We now use this removal lemma to prove Roth's theorem. We will actually prove the following stronger theorem.

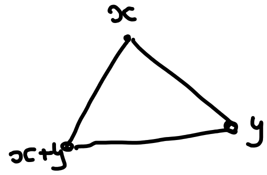
Theorem 2 *Let $\delta > 0$. Then there exists n_0 such that, for $n \geq n_0$, any subset A of $[n]^2$ with at least δn^2 elements must contain a triple of the form $(x, y), (x + d, y), (x, y + d)$ with $d > 0$.*

Proof The set $A + A = \{x + y : x, y \in A\}$ is contained in $[2n]^2$. There must, therefore, be some z which is represented as $x + y$ in at least

$$\frac{(\delta n^2)^2}{(2n)^2} = \frac{\delta^2 n^2}{4}$$

different ways. Pick such a z and let $A' = A \cap (z - A)$ and $\delta' = \frac{\delta^2}{4}$. Then $|A'| \geq \delta' n^2$ and if A' contains a triple of the form $(x, y), (x + d, y), (x, y + d)$ for $d < 0$, then so does $z - A$. Therefore, A will contain such a triple with $d > 0$. We may therefore forget about the constraint that $d > 0$ and simply try to find some non-trivial triple with $d \neq 0$.

Consider the tripartite graph on vertex sets X, Y and Z, where $X = Y = [n]$ and $Z = [2n]$. X will correspond to vertical lines through A, Y to horizontal lines and Z to diagonal lines with constant values of $x + y$. We form a graph G by joining $x \in X$ to $y \in Y$ if and only if $(x, y) \in A$. We also join x and z if $(x, z - x) \in A$ and y and z if $(z - y, y) \in A$.



Degenerate

If there is a triangle xyz in G, then $(x, y), (x, y+(z-x-y)), (x+(z-x-y), y)$ will all be in A and thus we will have the required triple unless $z = x + y$. This means that there are at most $n^2 = \frac{1}{64n}(4n)^3$ triangles in G. By the triangle removal lemma, for n sufficiently large, one may remove $\frac{\delta}{2}n^2$ edges and make the graph triangle-free. But every point in A determines a degenerate triangle. Hence, there are at least δn^2 degenerate triangles, all of which are edge disjoint. We cannot, therefore, remove them all by removing $\frac{\delta}{2}n^2$ edges. This contradiction implies the required result. $\square$

This implies Roth's theorem as follows.

Theorem 3 (Roth) *For all $\delta > 0$ there exists n_0 such that, for $n \geq n_0$, any subset A of $[n]$ with at least δn elements contains an arithmetic progression of length 3.*

Proof Let $B \subset [2n]^2$ be $\{(x, y) : x - y \in A\}$. Then $|B| \geq \delta n^2 = \frac{\delta}{4}(2n)^2$ so we have $(x, y), (x + d, y)$ and $(x, y + d)$ in B. This translates back to tell us that $x - y - d$, $x - y$ and $x - y + d$ are in A, as required. $\square$

To prove Szemerédi's theorem by the same method, one must first generalise the regularity lemma to hypergraphs. This was done by Gowers and, independently, by Nagle, Rödl, Schacht and Skokan. This method also allows you to prove the following more general theorem.

Theorem 4 (Multidimensional Szemerédi) *For any natural number d, any $\delta > 0$ and any subset P of $\mathbb{Z}^d$, there exists an n_0 such that, for any $n \geq n_0$, every subset of $[n]^d$ of density at least δ contains a homothetic copy of P, that is, a set of the form $k.P + \ell$, where $k \in \mathbb{Z}$ and $\ell \in \mathbb{Z}^d$.*

The theorem proved above corresponds to the case where $d = 2$ and $P = \{(0, 0), (1, 0), (0, 1)\}$. Szemerédi's theorem for length k progressions is the case where $d = 1$ and $P = \{0, 1, 2, \ldots, k - 1\}$.

Fourier Analysis

Group G.

$$e : G \times G \longrightarrow S^1 = \{ z \in \mathbb{C} : |z| = 1 \}$$

$G = \mathbb{Z}_N$: $\quad e(x, \xi) = e^{2\pi x \xi i / N}$

Properties :

$$e(x + x', \xi) = e(x, \xi)\, e(x', \xi)$$

$$e(x, \xi + \xi') = e(x, \xi)\, e(x, \xi')$$

Properties: (a) $e(0,\xi) = e(x,0) = 1$

$$e(x,-\xi) = e(-x,\xi) = \overline{e(x,\xi)}$$

(b) $$\frac{1}{|G|} \sum_{x\in G} e(x,\xi)\,\overline{e(x,\xi')} = 1_{\xi=\xi'}$$

Orthonormality

(c) $$\hat{f}(\xi) = \frac{1}{|G|} \sum_{x\in G} f(x)\,\overline{e(x,\xi)}$$

$f : G \to \mathbb{C}$

$$f(x) = \sum_{\xi \in G} \hat{f}(\xi)\, e(x, \xi) \qquad \text{Inversion}$$

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\, \overline{g(x)}$$

Parseval

$$= \sum_{\xi \in G} \hat{f}(\xi)\, \overline{\hat{g}(\xi)}$$

$$\frac{1}{|G|} \sum_{x \in G} |f(x)|^2 = \sum_{\xi \in G} |\hat{f}(\xi)|^2$$

Plancherel

$$f * g(x) = \frac{1}{|G|} \sum_{y \in G} f(y)\, g(x-y)$$ Convolution

$$\widehat{f * g}(\xi) = \hat{f}(\xi)\, \hat{g}(\xi)$$

$$\tilde{f}(x) = \overline{f(-x)}$$ ← Definition

$$\hat{\tilde{f}}(\xi) = \tilde{\hat{f}}(\xi).$$

Roth's Theorem by Fourier Analysis

Fix $0 < \delta < 1$. $A \subseteq [n]$, $|A| = \delta n$

$\Rightarrow \exists$ 3-term arithmetic progression in A.

Easy Case

$\delta \geq .9$. A must contain $x, x+1, x+2$

else $|A| \leq \frac{2}{3} n$.

"Proof by induction on δ"

Assume $|A|$ is odd and that B larger of even elements / odd elements of A.

χ_A, χ_B indicator functions of A, B.

Reduce to $A \subseteq \mathbb{Z}_n$

$$\overset{B}{x} + \overset{B}{y} = 2\overset{A}{z} \mod n \Rightarrow x + y = 2z + kn$$

$k \in \{0 \pm 1\}$

$$\underbrace{x+y}_{\text{even}} = \underbrace{2z}_{\text{even}} + \underbrace{n}_{\text{odd}}$$

parity problem!

$$\Delta = n^2 \sum_{g\in G} \hat{\chi}_B(g)^2 \hat{\chi}_A(-2g)$$

$$= \#(x+y = 2z \mod n,\ x,y\in B,\ z\in A)$$

$$\Delta = \frac{1}{n} \sum_{g\in G} \sum_{\substack{b_1\in B\\ b_2\in B\\ a\in A}} \underbrace{\overline{e(b_1,g)}\ \overline{e(b_2,g)}\ \overline{e(-2a,g)}}_{\exp\{2\pi i(2a-b_1-b_2)g/n\}}$$

Now note

$$\sum_{g\in G} e^{-2\pi i x g/n} = \begin{cases} n & x=0 \\ 0 & x\neq 0 \end{cases}$$

There $|B|$ trivial AP's where $x=y=z$

$$\Delta - |B| = n^2 \sum_{\substack{g\in G\\ g\neq 0}} \hat{X}_B(g)^2\, \hat{X}_A(-2g) + \frac{|A|\cdot|B|^2}{n} - |B|$$

$$\left[\hat{X}_A(0) = \frac{|A|}{n},\quad \hat{X}_B(0) = \frac{|B|}{n}\right]$$

Case 1: $|\hat{\chi}_A(g)| \leq \frac{\delta^2}{4}$, $\forall g \in G, g \neq 0$

$$n^2 \left| \sum_{\substack{g \in G \\ g \neq 0}} \hat{\chi}_B(g)^2 \hat{\chi}_A(-2g) \right| \leq \frac{\delta^2 n^2}{4} \sum_{g \in G} |\hat{\chi}_B(g)|^2$$

$$= \frac{\delta^2 n}{4} \sum_{x \in G} |\chi_B(x)|^2$$

$$= \frac{\delta^2 n |B|}{4} = \frac{|A|^2 |B|}{4n} \leq \frac{|A| |B|^2}{2n}.$$

$$\Delta - |B| \geq \frac{1}{2n} |A| \cdot |B|^2 - |B| > 0.$$

DONE

Case 2: $\exists\, g^* \neq 0$: $|\hat{\chi}_A(g^*)| \geq \delta^2/4$

$$\left| \frac{1}{n} \sum_{x \in G} (\chi_A(x) - \delta) \overline{e(x, g^*)} \right| \geq \delta^2/4$$

Fix $0 < Q < n$: $Q = \sqrt{n}$

Dirichlet theorem [PHP]

$\exists\, b/q$, $q \leq Q$, $(b,q) = 1$: $\left| \frac{g^*}{n} - \frac{b}{q} \right| \leq \frac{1}{qQ}$

Divide $[0, n-1]$ into progressions mod q, each of length $\approx n/q$

Divide each progression into $M = \Theta(\sqrt{n})$ contiguous pieces

Fix an interval I and $x \in I$

$$\overline{e(x, g^*)} = \exp\{-2\pi i x g^*/n\}$$

$$= \exp\left\{-2\pi i x\left(\frac{b}{q} + \frac{\epsilon}{qQ}\right)\right\} \quad |\epsilon| \leq 1$$

$x' \in I \Rightarrow x' = x + rq$, integer r, $|r| \leq \frac{n}{qM}$

$$\frac{\overline{e(x', g^*)}}{\overline{e(x, g^*)}} = \exp\left\{2\pi i\left(br + \frac{\epsilon r}{Q}\right)\right\}$$

$$= \exp\{2\pi i \cdot \epsilon r/Q\}$$

$$= 1 + O\left(\frac{n}{qQM}\right)$$

$$\frac{n\delta^2}{4} \leq \sum_{I} \left| \sum_{x \in I} \left(\chi_A(x) - \delta \right) \overline{e(x, g^*)} \right|$$

$$\leq \sum_{I} \left\{ \left| \sum_{x \in I} \left(\chi_A(x) - \delta \right) \right| + O\left(\frac{n|I|}{qQM} \right) \right\}$$

$$= \sum_{I} \left| \sum_{x \in I} \left(\chi_A(x) - \delta \right) \right| + O\left(\frac{n^2}{qQM} \right)$$

$\parallel$ kill

$Q = \sqrt{n}$, $M = C\sqrt{n}/(q\delta^2)$ C is large

$$\frac{n\delta^2}{8} \leq \sum_{I} \left| \sum_{x \in I} \left(\chi_A(x) - \delta \right) \right|$$

$$\frac{n\delta^2}{8} \leq \sum_{I} \left| \sum_{x \in I} (X_A(x) - \delta) \right|$$

$$\sum_{I} \sum_{x \in I} (X_A(x) - \delta) = 0$$

and so

$$\exists I : \sum_{x \in I} (X_A(x) - \delta) \geq \frac{\delta^2 n}{16 qM} \qquad \# I = \frac{n}{qM}$$

$$\frac{|A \cap I|}{|I|} \geq \delta + \frac{\delta^2}{16}$$

Translate and dilate to $\left[1, \frac{n}{qM}\right]$

$$\delta \longrightarrow \delta\left(1+\frac{\delta}{16}\right)$$

$$n \longrightarrow \frac{n}{qM} = \delta^2 \sqrt{n}/c$$

Iterate $L = D/\delta$ times

Density: $\nearrow$ $\geq \delta\left(1+\frac{\delta}{16}\right)^{D/\delta}$ $\delta \gg \frac{1}{\log\log n}$

Size: $\delta^2 n^{\frac{1}{2^L}}/c \gg 100$

Behrend's Theorem

$\exists A \subseteq [1, N]$, $|A| \geq ne^{-c\sqrt{\log n}}$, A has no 3-term progressions.

Proof

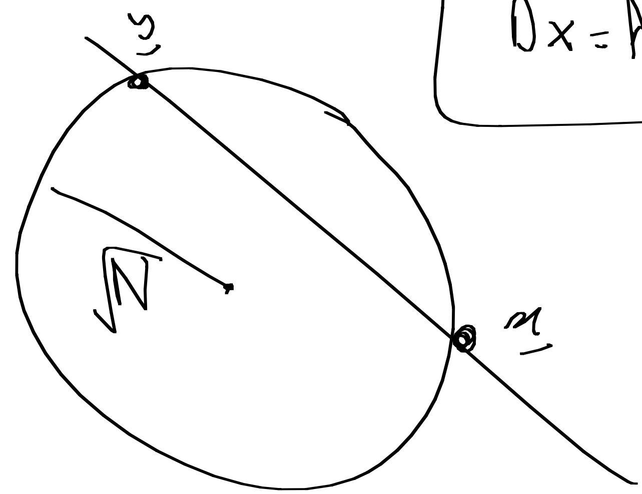
Consider $(x_1, x_2, \ldots x_k) \in [0, d]^k$ integer vectors

$$\sum_{i=0}^{k} x_i^2 \in [0, kd^2]$$

$$\exists N \leq kd^2 : \sum_{i=1}^{k} x_i^2 = N \text{ at least } \frac{(d+1)^k}{kd^2} \text{ times}$$

$$A = \left\{ \sum_{i=1}^{k} x_i (2d+1)^{i-1} : \sum_{i=1}^{k} x_i^2 = N \right\}$$

$\boxed{Dx = N \text{ meets}}$



AP $\Rightarrow$

Check each expression is different.

A NOTE ON ELKIN'S IMPROVEMENT OF BEHREND'S CONSTRUCTION

BEN GREEN AND JULIA WOLF

Abstract. We provide a short proof of a recent result of Elkin in which large subsets of $\{1, \dots, N\}$ free of 3-term progressions are constructed.

To Mel Nathanson

1. Introduction

Write $r_3(N)$ for the cardinality of the largest subset of $\{1, \dots, N\}$ not containing three distinct elements in arithmetic progression. A famous construction of Behrend [1] shows, when analysed carefully, that

$$r_3(N) \gg \frac{1}{\log^{1/4} N} \cdot \frac{N}{2^{2\sqrt{2}\sqrt{\log_2 N}}}.$$

In a recent preprint [2] Elkin was able to improve this 62-year old bound to

$$r_3(N) \gg \log^{1/4} N \cdot \frac{N}{2^{2\sqrt{2}\sqrt{\log_2 N}}}.$$

Our aim in this note is to provide a short proof of Elkin's result. It should be noted that the only advantage of our approach is brevity: it is based on ideas morally close to those of Elkin, and moreover his argument is more constructive than ours.

Throughout the paper $0 < c < 1 < C$ denote absolute constants which may vary from line to line. We write $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$ for the d-dimensional torus.

2. The proof

Let d be an integer to be determined later, and let $\delta \in (0, 1/10)$ be a small parameter (we will have $d \sim C\sqrt{\log N}$ and $\delta \sim \exp(-C\sqrt{\log N})$). Given $\theta, \alpha \in \mathbb{T}^d$, write $\Psi_{\theta,\alpha} : \{1, \dots, N\} \to \mathbb{T}^d$ for the map $n \mapsto \theta n + \alpha (\operatorname{mod} 1)$.

Lemma 2.1. *Suppose that n is an integer. Then $\Psi_{\theta,\alpha}(n)$ is uniformly distributed on $\mathbb{T}^d$ as θ, α vary uniformly and independently over $\mathbb{T}^d$. Moreover, if n and n' are distinct positive integers, then the pair $(\Psi_{\theta,\alpha}(n), \Psi_{\theta,\alpha}(n'))$ is uniformly distributed on $\mathbb{T}^d \times \mathbb{T}^d$ as θ, α vary uniformly and independently over $\mathbb{T}^d$.*

The first author holds a Leverhulme Prize and is grateful to the Leverhulme Trust for their support. This paper was written while the authors were attending the special semester in ergodic theory and additive combinatorics at MSRI.

Proof. Only the second statement requires an argument to be given. Perhaps the easiest proof is via Fourier analysis, noting that

$$\int e^{2\pi i(k\cdot(\theta n+\alpha)+k'\cdot(\theta n'+\alpha))}\, \mathrm{d}\theta\, \mathrm{d}\alpha = 0$$

unless $k + k' = kn + k'n' = 0$. Provided that k and k' are not both zero, this cannot happen for distinct positive integers n, n'. Since the exponentials $e^{2\pi i(kx+k'x')}$ are dense in $L^2(\mathbb{T}^d \times \mathbb{T}^d)$, the result follows. □

Let us identify $\mathbb{T}^d$ with $[0,1)^d$ in the obvious way. For each $r \leqslant \frac{1}{2}\sqrt{d}$, write $S(r)$ for the region

$$\{x \in [0,1/2]^d : r - \delta \leqslant \|x\|_2 \leqslant r\}.$$

Lemma 2.2. *There is some choice of r for which* $\mathrm{vol}(S(r)) \geqslant c\delta 2^{-d}$.

Proof. First note that if $(x_1, \dots, x_d)$ is chosen at random from $[0,1/2]^d$ then, with probability at least c, we have $|\|x\|_2 - \sqrt{d/12}| \leqslant C$. This is a consequence of standard tail estimates for sums of independent identically distributed random variables, of which $\|x\|_2^2 = \sum_{i=1}^d x_i^2$ is an example. The statement of the lemma then immediately follows from the pigeonhole principle. □

Write $S := S(r)$ for the choice of r whose existence is guaranteed by the preceding lemma; thus $\mathrm{vol}(S) \geqslant c\delta 2^{-d}$. Write $\tilde{S}$ for the same set S but considered now as a subset of $[0,1/2]^d \subseteq \mathbb{R}^d$. Since there is no "wraparound", the 3-term progressions in S and $\tilde{S}$ coincide and henceforth we abuse notation, regarding S as a subset of $\mathbb{R}^d$ and dropping the tildes. (To use the additive combinatorics jargon, S and $\tilde{S}$ are *Freiman isomorphic.*) Suppose that (x,y) is a pair for which $x-y, x$ and $x+y$ lie in S. By the parallelogram law

$$2\|x\|_2^2 + 2\|y\|_2^2 = \|x+y\|_2^2 + \|x-y\|_2^2$$

and straightforward algebra we have

$$\|y\|_2 \leqslant \sqrt{r^2 - (r-\delta)^2} \leqslant \sqrt{2\delta r}.$$

It follows from the formula for the volume of a sphere in $\mathbb{R}^d$ that the volume of the set $B \subseteq \mathbb{T}^d \times \mathbb{T}^d$ in which each such pair (x,y) must lie is at most $\mathrm{vol}(S)C^d(\delta/\sqrt{d})^{d/2}$.

The next lemma is an easy observation based on Lemma 2.1.

Lemma 2.3. *Suppose that N is even. Define $A_{\theta,\alpha} := \{n \in [N] : \Psi_{\theta,\alpha}(n) \in S\}$. Then*

$$\mathbb{E}_{\theta,\alpha}|A_{\theta,\alpha}| = N\,\mathrm{vol}(S)$$

whilst the expected number of nontrivial 3-term arithmetic progressions in $A_{\theta,\alpha}$ is

$$\mathbb{E}_{\theta,\alpha}T(A_{\theta,\alpha}) = \frac{1}{4}N(N-5)\,\mathrm{vol}(B).$$

Proof. The first statement is an immediate consequence of the first part of Lemma 2.1. Now each nontrivial 3-term progression is of the form $(n-d, n, n+d)$ with $d \neq 0$. Since N is even there are $N(N-5)/4$ choices for n and d, and each of the consequent progressions lies inside $A_{\theta,\alpha}$ with probability $\mathrm{vol}(B)$ by the second part of Lemma 2.1. $\square$

To finish the argument, we just have to choose parameters so that

$$\frac{1}{3}\,\mathrm{vol}(S) \geqslant \frac{1}{4}(N-5)\,\mathrm{vol}(B). \tag{2.1}$$

Then we shall have

$$\mathbb{E}\Big(\frac{2}{3}|A_{\theta,\alpha}| - T(A_{\theta,\alpha})\Big) \geqslant \frac{1}{3}N\,\mathrm{vol}(S).$$

In particular there is a specific choice of $A := A_{\theta,\alpha}$ for which both $T(A) \leqslant 2|A|/3$ and $|A| \geqslant \frac{1}{2}N\,\mathrm{vol}(S)$. Deleting up to two thirds of the elements of A, we are left with a set of size at least $\frac{1}{6}N\,\mathrm{vol}(S)$ that is free of 3-term arithmetic progressions.

To do this it suffices to have $C^d(\delta/\sqrt{d})^{d/2} \leqslant c/N$, which can certainly be achieved by taking $\delta := c\sqrt{d}N^{-2/d}$. For this choice of parameters we have, by the earlier lower bound on $\mathrm{vol}(S)$, that

$$|A| \geqslant \frac{1}{6}N\,\mathrm{vol}(S) \geqslant c\sqrt{d}2^{-d}N^{1-2/d}.$$

Choosing $d := \lceil\sqrt{2\log_2 N}\rceil$ we recover Elkin's bound. $\square$

3. A question of Graham

The authors did not set out to try and find a simpler proof of Elkin's result. Rather, our concern was with a question of Ron Graham (personal communication to the first-named author, see also [3, 4]). Defining $W(2;3,k)$ to be the smallest N such that any red-blue colouring of $[N]$ contains either a 3-term red progression or a k-term blue progression, Graham asked whether $W(2;3;k) < k^A$ for some absolute constant A or, even more ambitiously, whether $W(2;3,k) \leqslant Ck^2$. Our initial feeling was that the answer was surely no, and that a counterexample might be found by modifying the Behrend example in such a way that its complement does not contain long progressions. Reinterpreting the Behrend construction in the way that we have done here, it seems reasonably clear that it is not possible to provide a negative answer to Graham's question in this way.

4. acknowledgement

The authors are grateful to Tom Sanders for helpful conversations.

References

[1] F. Behrend. *On sets of integers which contain no three terms in arithmetic progression,* Proc. Nat. Acad. Sci., **32**:331–332, 1946

[2] M. Elkin, *An improved construction of progression-free sets,* available at `http://arxiv.org/abs/0801.4310`

[3] R. Graham, *On the growth of a van der Waerden-like function,* Integers, **6**:#A29, 2006

[4] B. Landman, A. Robertson and C. Culver, *Some new exact van der Waerden numbers,* Integers, **5**(2):#A10, 2005

Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WA, England

E-mail address: `b.j.green@dpmms.cam.ac.uk`

Mathematical Sciences Research Institute, 17 Gauss Way, Berkeley, CA 94720, U.S.A.

E-mail address: `julia.wolf@cantab.net`

Freiman's Theorem

$A' \subseteq A$ is a refinement of A if

$$\frac{|A|}{|A'|} = O(1).$$

A' is a small convolution of A

if $A' = X + A$ where $|X| = O(1)$.

Bounded Torsion

Suppose $\exists\, r = O(1)$ such that $rx = 0$, $\forall\, x \in G$.

If $|A+A| = O(1)|A|$ then A is a refinement of a subgroup of G.

Proof

Assume $0 \in A$. [Add if necessary]

(I) $A \subseteq A_0 = A - A$ and $|A_0| = O(1)|A|$. p37 Tao 1

(II) $G_0 = \langle A_0 \rangle$ = subgroup generated by A_0.

$$B = \underbrace{A_0 + A_0 + \cdots + A_0}_{r-1}, \quad |B| \leq O(1)\,|A|$$

$$G_0 \subseteq A_0 + B \subseteq X + A_0 \text{ where } |X| = O(1)$$ p38 cover

$A \subseteq G_0 \subseteq \langle X + A_0 \rangle$ and

$$|\langle X + A_0 \rangle| = O(1)\,|A|.$$

$\square$

Generalised Arithmetic Progression GAP

$$P = \left\{ a + \sum_{i=1}^{d} n_i v_i : \quad 0 \le n_i < N_i \right\}$$

$$= \{ a + n \cdot v : \quad n \in [0, N] \}$$

a = base point

d = dimension = rank

$v_1, \ldots, v_d$ are the basis vectors.

P is proper if $n \cdot v \neq n' \cdot v$
for $n \neq n' \in [0, N]$

Theorem [Freiman]

Suppose G is torsion-free and $|A+A| = O(1)|A|$. Then, A is a refinement of a small convolution of a proper GAP of $O(1)$ rank.

Steps of proof

(A) Reduce to showing that $2A-2A$ contains a large proper GAP.

(B) Replace G by a cyclic group H of order not much more than A.

reduce to showing that if $H \supseteq A$, $|H| = O(1)|A|$ then $2A-2A$ contains a large proper GAP

A) Assume $0 \in A$.

Suppose $P \subseteq 2A - 2A$ and $|P| = \Theta(|A|)$

$$|A+P| \leq |P + \underbrace{2A-2A}_{\supseteq A}| \leq |4A-4A| = O(|A|).$$

Ruzsa:

$$A \subseteq X + P - P \quad \text{where } |X| \leq \frac{|A+P|}{|P|} = O(1)$$

$$P - P = \left\{ \sum_{i=1}^{d} (n_i - n_i') v_i \right\}$$

$$= \left\{ \sum_{i=1}^{d} m_i v_i : |m_i| \leq N_i \right\}$$

$$= \left\{ -\sum N_i v_i + \sum_{i=1}^{d} (m_i + N_i) v_i : 0 \leq m_i + N_i \leq 2N_i \right\}$$

Freiman Homomorphism of order k (FH_k):

$A \subseteq G$, $B \subseteq G'$

$\phi : A \to B$ s.t.

$$\phi(x_1) + \cdots + \phi(x_k) = \phi(y_1) + \cdots + \phi(y_k)$$

whenever

$$x_1 + \cdots + x_k = y_1 + \cdots + y_k$$

Nb: $FH_k \to FH_l$, $l < k$

$$\phi(x_1) + \cdots + \phi(x_l) + \phi(a) + \cdots + \phi(a) = \phi(y_1) + \cdots + \phi(y_l) + \phi(a) + \cdots + \phi(a)$$

Suppose ϕ is FH_2 and P is a GAP. Then

(i) $\phi(P)$ is a GAP and (ii) $\phi(P)$ is proper if P is proper and ϕ is injective

Proof

(i) Can assume $\phi(0) = 0$. $\psi(x) = \phi(x) - \phi(0)$

$$x_1 + x_2 = y_1 + y_2$$
$$\downarrow$$
$$\phi(x_1) + \phi(x_2) = \phi(y_1) + \phi(y_2)$$
$$\downarrow$$
$$\psi(x_1) + \psi(x_2) = \psi(y_1) + \psi(y_2)$$

and $\phi(P) = \psi(P) + \phi(0)$

(ii) $$\phi(a + n_1 v_1 + \dots + n_d v_d) + \phi(0) \overset{FH_2}{=} \phi(a + n_1 v_1 + \dots + (n_d - 1) v_d) + \phi(v_d)$$

$$\overset{\text{Induction}}{=} \phi(0) + n_1 \phi(v_1) + \dots n_d \phi(v_d)$$

G is torsion free, $A \leq G$, $|A| < \infty \Rightarrow$

$\exists$ FH$_k$ $\phi : A \to \mathbb{Z}$

<u>Proof</u>

(i) Embed G in $\underbrace{G \otimes_{\mathbb{Z}} \overset{\text{rationals}}{\mathbb{Q}}}_{\Gamma}$

F = Free abelian group on $G \times \mathbb{Q}$

K = subgroup of F generated by $(a+a', b) - (a,b) - (a',b)$

$(a, b+b') - (a,b) - (a,b')$

$(na, b) - (a, nb)$

F/K

$G \cong G \times \{1\}$

(ii) Assume $0 \in A \subseteq \Gamma$ = vector space over $\mathbb{Q}$

(iii) span(A) = vector space of dimension $n < \infty$

$\subseteq \mathbb{Z}^n$

$$\phi : \mathbb{Z}^n \to \mathbb{Z} \qquad \phi(a_1, a_2, \ldots a_n) = a_1 + a_2 M + \cdots + a_n M^{n-1}$$

$(a_1, \ldots, a_n) \in A$ $\quad M \geq 1$ $\quad M = M(A, k)$

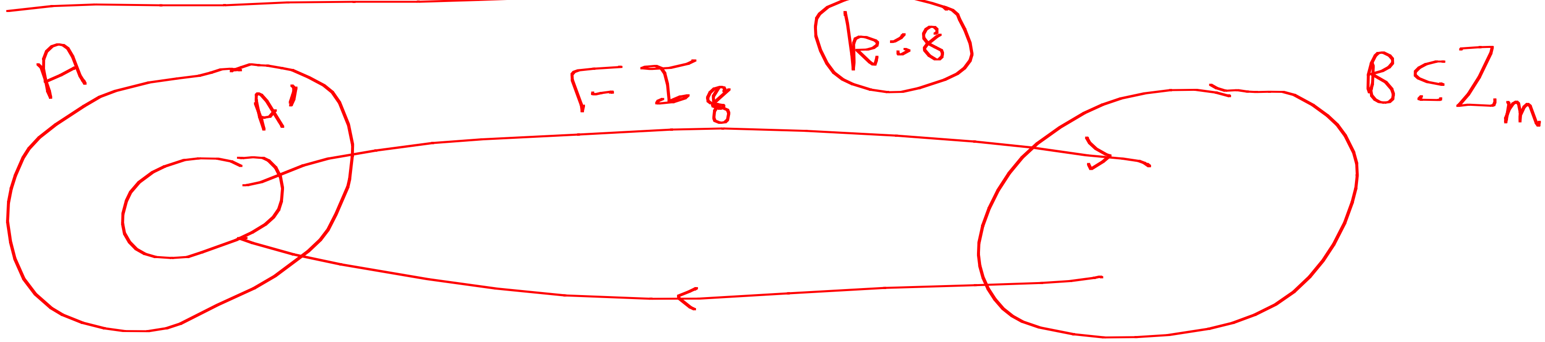
Proposition

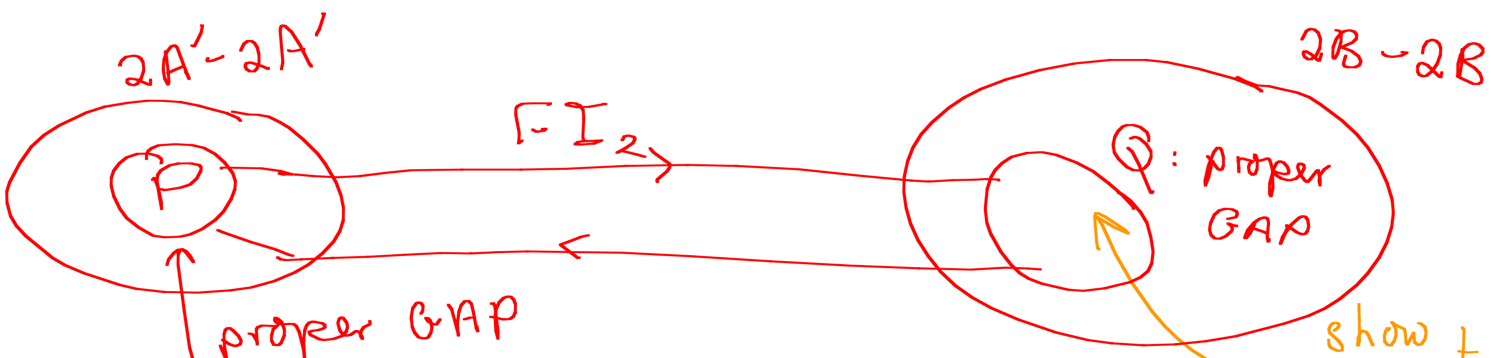
$A \subseteq \mathbb{Z}$ with $|A+A| = Cn$.
$|A| = n$

Assume $m \geq C^{2k} n$ and $k \geq 2$ is integer.

$\exists\ A' \subseteq A$ of size $\geq n/k$ which is k-isomorphic to a subset of $\mathbb{Z}_m$.

Proof later:





p prime, $p \gg n$ s.t. ψ_1 is 1-1 on A

$$\mathbb{Z} \xrightarrow[\text{Red. mod } p]{\psi_1} \mathbb{Z}_p \xrightarrow[\times q]{\psi_2(q)} \mathbb{Z}_p \xrightarrow[\text{embed}]{\psi_3} \mathbb{Z} \xrightarrow[\text{Red mod } m]{\psi_4} \mathbb{Z}_m$$

q to be chosen

$\psi_1, \psi_2, \psi_4 \in FH_\infty$

$\psi_3 \in FH_k$ when restricted to $I_j = \left(\frac{j-1}{k} p, \frac{j}{k} p\right)$

Check: $\psi_3(x_1) + \psi_3(x_2) + \dots + \psi_3(x_k) = \psi_3(y_1) + \psi_3(y_2) + \dots + \psi_3(y_k)$

whenever $x_1 + x_2 + \dots + x_k = y_1 + y_2 + \dots + y_k$

[sum in $[(j-1)p, jp]$ as integers

$$S_j = \{ a \in A : \psi_2(\psi_1(a)) \in I_j \}$$

Choose $j = j(q)$ such that $|S_j| \geq \frac{n}{k}$

$\psi = \psi_1 \circ \psi_2 \circ \psi_3 \circ \psi_4$ is FH_k when restricted to

$S_{\bar{v}(q)}$.

Claim: $\exists q$: ψ is invertible

Suffice to show that

$$\left\{ \begin{array}{l} \psi(x_1) + \cdots + \psi(x_k) = \psi(y_1) + \cdots + \psi(y_k) \\ \Rightarrow \quad x_1 + \cdots + x_k = y_1 + \cdots + y_k . \end{array} \right.$$

Condition fails if

$\exists \; s = x_1 + \cdots + x_k - (y_1 + \cdots + y_k) \neq 0$

s.t. $\quad q s \pmod p = 0 \pmod m$

$$\psi(x) = (qx \bmod p) \bmod m$$

Condition fails if

$\exists\ s = x_1 + \cdots + x_k - (y_1 + \cdots + y_k) \neq 0$ $(*)$

s.t. $\quad q s \pmod p = 0 \pmod m$

$\psi(x) = (qx \bmod p) \bmod m$

Choose q at random.

$\Pr[\exists s : (*) \text{ holds}] \leq \frac{|kA - kA|}{m} < 1$

$[m > C^{2k}|A|.]$

$\square$

Recap

N large integer [$N = m$]

$A \subseteq \mathbb{Z}_N$, $|A| = cN$

$|A+A| = K|A|$ $K = O(1)$

Show
$2A - 2A$ contains (proper) bounded rank GAP P where $|P| = \Omega(N)$.

$G = \mathbb{Z}_N$: Fourier analysis

$$\chi_A(x) = 1_{x \in A} \quad \text{where } |A| = c|G|.$$

Planchered: $$\sum_{\xi \in G} |\hat{\chi}_A(\xi)|^2 = \frac{1}{|G|} \sum_{x \in G} |\chi_A(x)|^2 = c \quad (1)$$

But $$|\hat{\chi}_A(\xi)| = \frac{1}{|G|} \left| \sum_{x \in G} \chi_A(x) \overline{e(x,\xi)} \right|$$

$$\leq \frac{1}{|G|} \sum_{x \in G} \chi_A(x)$$

$$= c. \quad (2)$$

So $$\left| \left\{ \xi \in G : |\hat{\chi}_A(\xi)| \geq \epsilon c \right\} \right| \leq \frac{1}{\epsilon^2 c} \cdot \left[\frac{c}{\epsilon^2 c^2} \right]$$

$$\frac{1}{|G|} \sum_{x \in G} \Big| \underbrace{\chi_A * \chi_A(x)}_{} \Big| = \frac{1}{|G|^2} \sum_{x} \sum_{\substack{y \\ x'}} \chi_A(y)\, \chi_A \overbrace{(x-y)}^{x'}$$

\# non-zeros is at most

$|A + A| \leq cK\, |G|$

$$= \left(\frac{1}{|G|} \sum_{z \in G} \chi_A(z) \right)^2$$

$$= c^2$$

So, by Cauchy-Schwartz

$$\sum_{x \in G} |\chi_A * \chi_A(x)|^2 \geq \frac{1}{cK|G|} \left(c^2 |G| \right)^2$$

$$= \frac{c^3}{K} |G|.$$

$$a_1^2 + a_2^2 + \cdots + a_m^2 \geq \frac{1}{m} (a_1 + \cdots + a_m)^2$$

But

$$\frac{1}{|G|}\sum_{x\in G}|\chi_A*\chi_A(x)|^2=\sum_{\xi\in G}|\widehat{\chi_A*\chi_A}(\xi)|^2$$

$$=\sum_{\xi\in G}|\widehat{\chi}_A(\xi)|^4.$$

So

$$\sum_{\xi\in G}|\widehat{\chi}_A(\xi)|^4\geq\frac{c^3}{|\alpha}$$

$$\widehat{f*g}(\xi)=\widehat{f}(\xi)\widehat{g}(\xi)$$

Now (1) & (2) on p16 imply

$$\sum_{\xi \in G} |\hat{\chi}_A(\xi)|^4 \le c^2 \underbrace{\sum_{\xi \in G} |\hat{\chi}_A(\xi)|^2} = c^3 \qquad (3)$$

Similarly

$$\sum_{\xi \in G : |\hat{\chi}_A(\xi)| \le \epsilon c} |\hat{\chi}_A(\xi)|^4 \le \epsilon^2 c^2 \qquad = \epsilon^2 c^3 \qquad (4)$$

Choose $\epsilon = \frac{1}{2\sqrt{K}}$: $\Lambda = \left\{ \xi : |\hat{\chi}_A(\xi)| \ge \overset{(\epsilon c)}{\frac{c}{2\sqrt{K}}} \right\}$

$$\sum_{\xi \in \Lambda} |\hat{\chi}_A(\xi)|^4 \ge \sum_G - \frac{c^3}{4K} \ge \frac{3}{4} \sum_{\xi \in G} |\hat{\chi}_A(\xi)|^4 .$$

$|\Lambda| \le c^3 / \left(c / 2\sqrt{K} \right)^4 = O(1).$

$\tilde{g}(x) = \overline{g(-x)}$

Now let

$$f = \chi_A * \chi_A * \tilde{\chi}_A * \tilde{\chi}_A$$

This is supported on $2A - 2A$ and

$$\hat{f}(\xi) = |\hat{\chi}_A(\xi)|^4$$

$\hat{\tilde{g}} = \overline{\hat{g}}$

By Fourier inversion

$$f(x) = \sum_{\xi \in G} |\hat{\chi}_A(\xi)|^4 e(x, \xi)$$

$$\hat{f}(\xi) = \hat{\chi}_A(\xi)\, \hat{\chi}_A(\xi) \cdot \overline{\hat{\chi}_A}(\xi) \cdot \overline{\hat{\chi}_A}(\xi)$$

It suffices to find large (proper) GAP $P \subseteq \{x : f(x) \neq 0\}$

Now let

$$X = \{ x \in G : |e(x,\xi) - 1| < \tfrac{1}{4},\ \forall \xi \in \Lambda \}$$

Then

$$x \in X \Rightarrow \mathrm{Re} \sum_{\xi \in \Lambda} |\hat{X}_A(\xi)|^4 e(x,\xi) \geq \frac{3}{4} \sum_{\xi \in \Lambda} |\hat{X}_A(\xi)|^4$$

$$\Big[\mathrm{Re}(\underset{\mathbb{R}}{\alpha} \underset{\mathbb{C}}{z}) = \alpha \,\mathrm{Re}\, z \Big]$$

and so, $x \in X$

$$\Big| \sum_{\xi \in \Lambda} |\hat{X}_A(\xi)|^4 e(x,\xi) \Big| \geq \frac{3}{4} \sum_{\xi \in \Lambda} |\hat{X}_A(\xi)|^4 .$$

But:

$$\sum_{\xi \in \Lambda} |\hat{\chi}_A(\xi)|^4 \geq \frac{3}{4} \sum_{\xi \in G} |\hat{\chi}_A(\xi)|^4$$

implies

$$\left| \sum_{\xi \in G \setminus \Lambda} |\hat{\chi}_A(\xi)|^4 \, e(x,\xi) \right| \leq \sum_{\xi \in G \setminus \Lambda} |\hat{\chi}_A(\xi)|^4$$

$$\leq \frac{1}{4} \cdot \frac{4}{3} \cdot \sum_{\xi \in \Lambda} |\hat{\chi}_A(\xi)|^4 .$$

Thus, by Fourier inversion $\left(\hat{f}(\xi) = |\hat{\chi}_A(\xi)|^4 \right)$

$$f(x) \neq 0, \quad \forall x \in X \quad \left(\frac{1}{3} < \frac{3}{4} \right)$$

We now show $|X| = \Omega(N)$

$X \supseteq$ GAP of $O(1)$-dimension

For $e(x,\xi) = e^{2\pi i x\xi/N}$

$$X = \left\{ x \in G : \left\| \frac{x\xi}{N} \right\| < \delta, \ \forall \xi \in \Lambda \right\}$$

where $\delta = \delta(1/4)$ and $\|\xi\|$ = distance to nearest integer

{We can make δ smaller at the expense of reducing $|X|$}

$$\left[X = \left\{ x \in G : |e(x,\xi) - 1| < \tfrac{1}{4}, \ \forall \xi \in \Lambda \right\} \right]$$

Suppose now that

$$\Lambda = \{\xi_1, \xi_2, \dots \xi_k\} \qquad k = O(1).$$

$$T^k = \mathbb{R}^k / \mathbb{Z}^k$$

$$\underline{\omega} = \left(\frac{\xi_1}{N}, \frac{\xi_2}{N}, \dots, \frac{\xi_k}{N}\right) + \mathbb{Z}^k$$

$N\omega = 0$ and $a\underline{\omega} = 0 \Rightarrow N \mid a$ (N prime

$$X' = \{x \in \mathbb{Z}_N : x\underline{\omega} \in B(0, \eta = \tfrac{\delta}{\sqrt{k}})\} \subseteq X$$

$$\left[x \in X \Rightarrow |x\underline{\omega}| \leq \left|\left(\frac{\delta}{\sqrt{k}}, \frac{\delta}{\sqrt{k}}, \dots, \frac{\delta}{\sqrt{k}}\right)\right| = \delta\right]$$

$B(0,\eta)$ is a subset of T^k. $|y|^2 = \|y_1\|^2 + \|y_2\|^2 + \dots + \|y_k\|^2$

We show $X' \supseteq$ large GAP

$|X'| = \Omega(N)$.

(i) $T^k \le \left(\frac{c'}{\eta}\right)^k$ "balls" of radius $\eta/2$ $\qquad \eta = \frac{\delta}{\sqrt{k}}$

(ii) One ball $B(x_0, \eta/2) \supseteq \left(\frac{\eta}{c'}\right)^k N$ multiples of ω.

(iii) $B(x_0, \eta/2) - B(x_0, \eta/2) = \underbrace{B(0, \eta)}_{X'} \supseteq \left(\frac{\eta}{c'}\right)^k N$ multiples

So $|X'| \geqslant \left(\frac{\eta}{c'}\right)^k N$

Now define

$$\text{span } X'_{\omega} \begin{cases} v_1 \underline{\omega} = \text{shortest vector in } X'_{\underline{\omega}} & [\text{closest to } \underline{0}] \\ v_2 \underline{\omega} = \text{shortest vector in } X'_{\underline{\omega}}, \text{ independent of } v_1 \underline{\omega} \\ \vdots \\ v_\ell \underline{\omega} = \text{shortest vector in } X'_{\underline{\omega}}, \text{ independent of } v_1 \underline{\omega}, \dots v_{\ell-1} \underline{\omega} \end{cases}$$

$$r_j = |v_j \underline{\omega}|, \quad 0 \leq r_1 \leq r_2 \leq \dots \leq r_\ell \leq \delta$$

$$V_j = \text{span}\{v_1 \underline{\omega}, \dots v_j \underline{\omega}\}$$

$\Pi_j \equiv$ orthogonal projection onto V_j

$$B = \left\{ x \in V_\ell : \left| \Pi_{j+1} x - \Pi_j x \right| < \frac{r_j}{2k},\ \forall\, 0 \le j < \ell \right\}$$

$$\subseteq B(0, \delta/2) \quad \text{— triangle inequality}$$

B contains no non-zero of $\underline{\omega}$.

Suppose $a\underline{\omega} \in V_j \setminus V_{j-1}$ is independent of $v_1 \underline{\omega}, \ldots, v_{j-1}\underline{\omega}$.

$$|a\underline{\omega}| = |\Pi_j a\omega| < \frac{r_1}{2k} + \frac{r_2}{2k} + \cdots + \frac{r_j}{2k} < r_j \text{ — contradiction}$$

Thus sets $x\underline{\omega} + \frac{B}{2} \subseteq B(0, 2\delta)$ are disjoint as x ranges over X'.

$$\left[\left(x_1 \underline{w} + \frac{B}{2}\right) \cap \left(x_2 \underline{w} + \frac{B}{2}\right) \neq \emptyset \Rightarrow (x_1 - x_2)\,\underline{w} \in \frac{B}{2} - \frac{B}{2} = B \right]$$

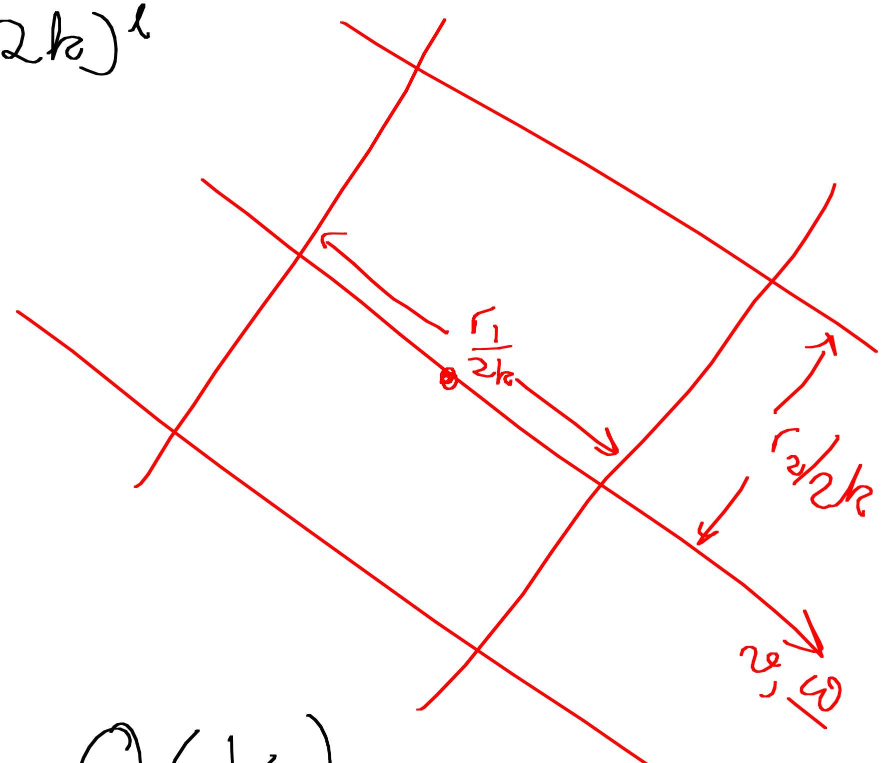
So

$$\mathrm{Vol}(B/2) \leq \frac{\overset{\ell\text{-dim. volume}}{\mathrm{Vol}(B(0,2\delta)) \cap V_\ell)}}{|X'|}$$

$$= O(1/N).$$

But:

$$\mathrm{Vol}(B) \geq \frac{r_1 r_2 \cdots r_\ell}{(2k)^\ell}$$



Hence $r_1 r_2 \cdots r_\ell = O(1/N)$

Now let

$$N_j = \left\lceil \frac{\eta}{k r_j} \right\rceil$$

$\left|\sum N_j v_j \underline{\omega}\right|$

$\leq \sum N_j |v_j \underline{\omega}|$

$\leq \sum N_j \cdot r_j \leq \eta$ ish

$$N_1 N_2 \cdots N_\ell = \Omega(N)$$

Now let

$$P = \left\{ \sum_{j=1}^{\ell} n_j v_j \;:\; 0 \leq n_j \leq N_j \right\}$$

(i) $|P| = \Omega(N)$

(ii) $P\underline{\omega} \subseteq B(0, \eta) \Rightarrow P \subseteq X'$

(iii) P is proper: $p_1 \underline{\omega} = p_2 \underline{\omega} \Rightarrow p_1 = p_2$

Removing convolution from Freiman's Theorem

$A \subseteq X + P$, $|X| = O(1)$ & P is a GAP

$X + P \subseteq Q$ another GAP of bounded dimension.

Theorem

$P \supseteq$ GAP of rank r

$\Rightarrow P \subseteq Q$ = proper GAP of rank r, $\frac{|Q|}{|P|} = O(1)$.

Singularity of random ± 1 matrices

We prove the following result of Kahn, Komlós, Szemerédi:

Let M_n be $n \times n$ ± 1 matrix where

$$\Pr(M_n(i,j) = 1) = 1/2 \quad \forall i,j. \text{ (independently)}$$

Then $\exists$ constant $c < 1$ such that

$$\Pr(M_n \text{ is singular}) \le c^n.$$

Tao, Vu reduced c to $3/4$

$c = \frac{1}{2} + o(1)$ is best possible.

$$M_n = [X_1, X_2, \ldots, X_n]$$

columns

<u>Proposition</u>

Let Ω_1 be the set of $v \in \mathbb{Z}^n$ with at least $3n/\log_2 n$ zero coordinates. Then

$$\Pr(\underbrace{\exists\, v \in \Omega_1 : M_n v = 0}_{\mathcal{E}}) \le (1+o(1))\, n^2 2^{-n}$$

<u>Proof</u>

$$\Pr(\mathcal{E}) = \sum_{2 \le k \le n - 3n/\log_2 n} \Pr(\mathcal{E}_k \setminus \mathcal{E}_{k-1}) \quad \text{where}$$

$$= \{\exists\, v = (a_1, \ldots, a_n) : k \text{ of } a_i \text{ are non-zero},\ a_1X_1 + \cdots + a_nX_n = 0\}$$

$$\Pr(\mathcal{E}_2) \le \mathbb{E}[\#\text{pairs } X_i = \pm X_j] \le n^2 2^{-n}.$$

Assume $k \geq 3$.

$$\Pr(\mathcal{E}_k \setminus \mathcal{E}_{k-1}) \le \binom{n}{k} \Pr(\underbrace{\mathcal{F}_k}_{\left\{\substack{\exists\ a_1X_1+\cdots+a_kX_k=0 \\ a_1,\dots,a_k \neq 0}\right\}} \setminus \mathcal{E}_{k-1})$$

$\mathcal{F}_k \setminus \mathcal{E}_{k-1} \Rightarrow$ matrix $A_k = [X_1, X_2, \dots, X_k]$

has rank $k-1$.

Hence $\exists$ $k-1$ rows R of A_k that "determine"

$a_1, \dots, a_k$ (up to scaling).

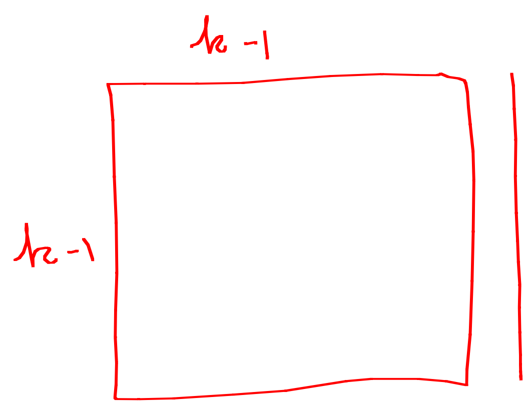
$$\Pr(\mathcal{E}_k / \mathcal{E}_{k-1})$$

$$\sum_{M_n(R,C)}$$

$$\le \sum_{C} \sum_{R} \Pr(\mathcal{F}_k \setminus \mathcal{E}_{k-1} \mid M_n(R,C)) \Pr(M_n(R,C))$$

k cols   k-1 rows

remaining n-k+1 rows here to behave.



$a_1, \ldots, a_k$ fixed up to scaling

$$\le \binom{n}{k}\binom{n}{k-1} \rho^{n-k+1} \overbrace{\sum_{M_n(\square)} \Pr(M_n(\square))}^{1}$$

where ρ is an upper bound on $\Pr[a_1 Z_1 + \cdots + a_k Z_k = 0]$ for $a_1, \ldots, a_k \in \mathbb{Z} \setminus \{0\}$, $Z_i = \pm 1$ independently.

We argue later that

$$p \leq \binom{k}{\lfloor k/2 \rfloor} 2^{-k} \leq \frac{1}{\sqrt{k}} \qquad (*)$$

Thus

$$\sum_{3 \leq k \leq n - 3n/\log_2 n} \Pr(\mathcal{E}_k \setminus \mathcal{E}_{k-1}) \leq \sum_{3 \leq k \leq \cdots} \binom{n}{k}\binom{n}{k-1}\left(\frac{1}{\sqrt{k}}\right)^{n-k+1}$$

(i) $k \leq \epsilon n$: $\binom{n}{k}\binom{n}{k-1}\left(\frac{1}{\sqrt{k}}\right)^{n-k+1} \leq e^{O(\epsilon \ln 1/\epsilon \; n)} \cdot \left(\frac{1}{\sqrt{3}}\right)^{(1-\epsilon)n}$

(ii) $\epsilon n < k \leq n - \frac{3n}{\log_2 n}$: $\binom{n}{k}\binom{n}{k-1}\left(\frac{1}{\sqrt{k}}\right)^{n-k+1}$

$$\leq 2^n \times 2^n \times \left(\frac{1}{\sqrt{\epsilon n}}\right)^{3n/\log_2 n} \longleftarrow \text{take logs}$$

Proof of ⊛ : Littlewood-Offord Problem.

$$\mathcal{A} \subseteq 2^{[n]} \ \& \ A, B \subseteq \mathcal{A} \ni A \not\subseteq B$$

then $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Erdös: Suppose $a_1, a_2, \ldots, a_n \in \mathbb{R}$, with $|a_i| \geq 1$.

Let I be any open interval of width 2.

$$\left|\left\{ (z_1, z_2, \ldots, z_n) \in \{-1, 1\}^n : a_1 z_1 + \cdots + a_n z_n \in I \right\}\right| \leq \binom{n}{\lfloor \frac{1}{2} n \rfloor}.$$

We can assume w.l.o.g. that $a_1, \ldots, a_n \geq 1$ $[a_i \to -a_i$ is ok$]$

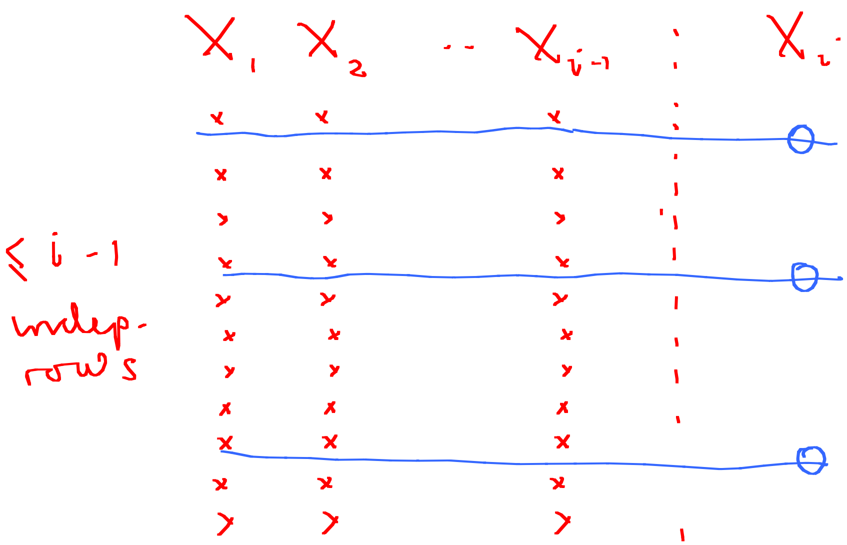
$\mathcal{A} = \{ A : Z_A = \sum_{i \in A} a_i - \sum_{i \notin A} a_i \in I \}$ is a Sperner family

$(A \subsetneq B \Rightarrow Z_B \geq Z_A + 2 \})$.

Proposition

$$\Pr\left(X_i \in \operatorname{span}(X_1, X_2, \ldots, X_{i-1})\right) \leq \min\left\{2^{i-n-1}, O(1/\sqrt{n})\right\}$$

Proof



condition on rows and values of $X_1, \ldots, X_i$ in these $i-1$ rows.

Remaining entries of X_i are determined and $\Pr \leq \frac{1}{2}$ that they are chosen.

This gives upper bound of 2^{i-n-1}.

Now assume that $i \geq .9n$.

Choose a hyperplane $H = \{a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0\}$ that contains $X_1, X_2, \ldots, X_i$.

We can assume by Proposition P2 that $\Omega(n)$ of the a_i are non-zero.

But then

$$\Pr(X_i \in H) = O(1/\sqrt{n}).$$

$\square$

Thus for some $c > 0$

$$\Pr(M_n \text{ is singular}) \leq \sum_{i=2}^{n} \min\left\{2^{i-n-1}, \frac{c}{\sqrt{n}}\right\}$$

$$= \sum_{i=2}^{n-\frac{1}{2}\log_2 n} 2^{i-n-1} + \sum_{i=n-\frac{1}{2}\log_2 n}^{n} \frac{c}{\sqrt{n}}$$

$$= O\left(\frac{\log n}{\sqrt{n}}\right).$$

$\square$

We continue with a proof of an exponential upper bound.

Now let

$$\Omega_2 = \{ v \in \mathbb{Z}^n : |v_i| \leq n^C \; \forall i \}$$

Here C is some constant.

<u>Proposition</u>

$$\Pr(\exists\, v \in \Omega_2 : M_n v = 0) \leq \left(\tfrac{1}{2} + o(1)\right)^n.$$

<u>Proof</u>

For $v \in \Omega_2$, let $p(v) = \Pr(X \cdot v = 0)$ when $X \overset{\text{ran}}{\in} \{\pm 1\}^n$

(I) $\Pr(M_n v = 0) = p(v)^n$

(II) $p(v) \leq \frac{1}{2}$: $\Pr(X \cdot v = 0) = \Pr\left(X_1 v_1 = -\sum_{j=2}^{n} X_j v_j\right) \leq \frac{1}{2}$

assuming $v_1 \neq 0$.

Let $S_j = \left|\{ v \in \Omega_2 : 2^{-j-1} \leq p(v) \leq 2^{-j} \}\right|$

$$\Pr(\exists\, v \in \Omega_2 : M_n v = 0) \leq \sum_{j=1}^{n} (2^{-j})^n S_j$$

[Note $p(v) = 0$ or $p(v) \geq \frac{1}{2^n}$ — there are 2^n choices for X]

If $p(v) \geq n^{-1/3}$ then $\binom{k}{\lfloor k/2 \rfloor} 2^{-k} \geq n^{-1/3}$

Littlewood - Offord - Erdős

where $k = |\{ j : v_j \neq 0 \}|$.

Thus $k = O(n^{2/3})$ and $v \in \Omega_1$.

$|\Omega_2| \leq n^{(C+1)n}$ and so $\displaystyle\sum_{2^{-j} \leq n^{-C-2}} (2^{-j})^n S_j \leq 2^{-n}$.

Remains to consider

$$\sum_{n^{-C-2} \leq 2^{-j} \leq n^{-1/3}} (2^{-j})^n S_j .$$

Fix ϵ small.

Fix i and integer $d = d(i, \epsilon)$ such that

$$n^{-\frac{1}{3} - (d-1)\epsilon} > 2^{-i} \geq n^{-\frac{1}{3} - d\epsilon}$$

Now choose k such that

$$k^{d-1} \ll n^{\frac{1}{3} + (d-1)\epsilon} \qquad \text{(a)}$$

$$k^{d} \gg n^{\frac{1}{3} + d\epsilon} \qquad \text{(b)}$$

$$k = n^{\frac{1}{3(d-1/2)} + \epsilon}$$

Proposition

G is torsion free or of odd order.

For any $d \geq 1$ there is a constant δ_d such that the following holds: suppose $k \geq 2$ and $x \in G$ and $v \in G^n$. Then either

(i) $\Pr(x_1 v_1 + x_2 v_2 + \cdots + x_n v_n = x) \leq \delta_d k^{-d}$

$x_v = \pm 1$ random only

or

(ii) $\exists\, P = [-k, k]^{d-1} \cdot (w_1, \ldots, w_{d-1}) \subseteq G$

and $a_j \in [k]$ such that $a_j v_j \in P$ for all but at most k^2 exceptional values.

Furthermore $w_1, \ldots, w_{d-1} \in \{v_1, \ldots, v_n\}$.

It follows from (b) on P13 that condition 1 fails.

Assume condition 2 and estimate S_j.

$$S_j \leq \underset{(2n^c+1)^{d-1}}{\#\text{ choices for } P} \times \underset{\leq \binom{n}{k^2}(2n^c+1)^{k^2}}{\#\text{ choices for exceptional value}}$$

$$\times \underset{(|P|\,n)^{o(n)}}{\text{choices for rest of } v_i}$$

(i) a_j is a factor of some $x \in P$

(ii) Integer N has $\leq N^{o(1)}$ factors

Hence

$$S_j \leq n^{O(k^2)}\, O(1)^n\, k^{(d-j+o(1))n}$$

and then

$$(2^{-j})^n S_j \leq O(1)^n \left[n^{\frac{d-1}{d-\frac{1}{2}}\cdot\frac{1}{3} + (d-1)\epsilon + o(1) - \frac{1}{3} - (d-1)\epsilon} \right]^n$$

$$= O(1)^n\, n^{-n\epsilon/6d-3} \qquad \#j = O(\log n) \qquad \square$$

Proposition

$$\Pr[M_n \text{ is singular}] = 2^{O(n)} \Pr[\dim(X_1,\dots,X_n) = n-1]$$

Proof

$$\Pr[M_n \text{ is singular}] \geq \Pr[\dim(X_1,\dots,X_n) = n-1].$$

On the other hand: if $X_1,\dots,X_n$ are dependent then $\exists\, d$ such that $X_1,\dots,X_d$ are independent and $X_{d+1} \in \operatorname{Span}(X_1,\dots,X_d)$. Denote this event by $\mathcal{E}_d$.

$$\Pr[\dim(X_1,\dots,X_n) = n-1 \mid \mathcal{E}_d] \geq \prod_{j \geq d+1} \left(1 - \min\left\{\frac{1}{2^{n-d+1}}, \frac{c}{\sqrt{n}}\right\}\right)$$

$$= 2^{-O(n)}.$$

[Just modify proof Prop 7. Here one can fix $X_1,\dots,X_{i-1}$ and $i-1$ coordinates of X_i]

So

$$\underbrace{\sum_d \Pr\left(\dim(X_1,\dots,X_n) = n-1 \wedge \mathcal{E}_d\right)}_{\Pr(\dim(X_1,\dots,X_n)=n-1)} \geq 2^{-O(n)} \underbrace{\sum_d \Pr(\mathcal{E}_d)}_{\Pr(M_n \text{ is singular})}$$

Suffices to show that

$$\sum_V \Pr(X_1,\dots,X_n \text{ span } V) \leq (1-\epsilon_1)^n$$

Sum over V: V is spanned by $n-1$ independent vectors in $\{\pm 1\}^n$.

Density of V: $\Pr(X \in V) = \dfrac{|V \cap \{-1,1\}^n|}{2^n}$

Proposition

$$\Omega_\alpha = \{ V : \Pr[X \in V] \leq \alpha \}$$

$$\sum_{V \in \Omega_\alpha} \Pr(\operatorname{span}(X) = V) \leq n\alpha$$

Proof

$$\sum_{V \in \Omega_\alpha} \Pr(\operatorname{span}(X) = V) = \sum_i \sum_{X_{\neq i}} \underbrace{\Pr[X_{\neq i}]}_{\left(\frac{1}{2}\right)^{n(n-1)}} \underbrace{\Pr[X_i \in \overbrace{\operatorname{span}(X_{\neq i})}^{V}]}_{\leq \alpha}$$

$$\leq \alpha \sum_i \Big[\underbrace{\sum_{X_{\neq i}} \Pr[X_{\neq i}]}_{1} \Big] \leq n\alpha$$

$\square$

From Propositions 16 and 18 we can finish by estimating

$$\Pr\left[V = \mathrm{span}(X_1, \ldots, X_n) \text{ is an } (n-1) \text{ dimensional hyperplane and } (1-\epsilon_1)^n \le \Pr[X \in V] \le \frac{C}{\sqrt{n}} \right]$$

Here C is a large enough constant so that if $\Pr[X \in V] \geq \frac{C}{\sqrt{n}}$ then at most $c'n$ coefficients of the equation defining V are non-zero, where $c' < 1$ is constant.

Fix $v = (v_1, v_2, \ldots, v_n)$ and $0 \leq \mu \leq 1$

$$X_v^{(\mu)} = \sum_{i=1}^{n} \eta_i^{(\mu)} v_i \quad \text{where} \quad \eta_i^{(\mu)} = \begin{cases} 0 & \text{Prob } 1-\mu \\ -1 & \text{Prob } \mu/2 \\ +1 & \text{Prob } \mu/2 \end{cases}$$

<u>Proposition</u>

Let G be torsion free or cyclic of odd prime order.

Let $v \in G^n$ and $0 < \mu \leq \mu' \leq 1$ with $\mu \leq 1/4$. Then

$$\Pr[X_v^{(\mu')} = x] = O\left(\sqrt{\frac{\mu}{\mu'}} \Pr(X_v^{(\mu)} = 0)\right) + O\left(\Pr(X_v^{(\mu)} = 0)^{\Omega(\mu'/\mu)}\right)$$

Suppose $0 < \mu \ll 1$ and $Y \in \{0, \pm 1\}^n = (\eta_1^{(\mu)}, \dots, \eta_n^{(\mu)})$.

Taking $\mu' = 1$ in Proposition 20 and μ small enough

$$\Pr[X \in V] = O(\sqrt{\mu}) \Pr(Y \in V). \quad (*)$$

Here $X_v^{(\mu')} = X \cdot v$ and $X_v^{(\mu)} = Y \cdot v$

Also we can assume $\Pr(Y \in V) = O(1/\sqrt{n})$: whp $\Omega(n)$ of the Y_i are non-zero. Apply L.O.

Choose small δ and a density σ such that $(1-\epsilon_1)^n \leq \sigma \leq c/\sqrt{n}$ and let V be such that $\Pr(X \in V) = (1 + O(1/n))\, \sigma$.

Now choose $Y_1, Y_2, \dots Y_{\delta n}$ independently of $X_1, X_2, \dots, X_n$.

$$\circledast \quad \Pr(Y_1, \dots, Y_{\delta n} \in V) \geq \Omega(1/\sqrt{\mu})^{\delta n} \, \sigma^{\delta n}$$

$\circledast$ on p21

But then

$$\Pr[\overset{A}{Y \text{ is a lin. comb. } Y_1, \dots, Y_{i-1}} \mid \overset{B,\ C}{Y_1, \dots, Y_i \in V}]$$

$$\leq \frac{1}{\sigma} \Pr[Y_i \text{ is a lin. comb. } Y_1 \dots Y_{i-1} \mid Y_1 \dots Y_{i-1} \in V]$$

$$P(A|BC) \leq \frac{P(A|B)}{P[C|B]}$$

$P[C]$

$$\leq \frac{1}{\sigma} \cdot \left(\frac{1}{1-\mu}\right)^{n-i+1}$$

— adapt proof of Proposition 7

So

$$\Pr[Y_1 \dots Y_{\delta n} \text{ not lin. dep.} \mid Y_1 \dots Y_{\delta n} \in V] \leq O\left(\frac{(1-\epsilon_1)^n}{(1-\mu)^{n-\delta n}}\right)$$

$$= o(1).$$

So

$$\Pr(Y_1, Y_2, \ldots Y_{\delta n} \text{ are lin. indep. vectors in } V) \geq \Omega\left(\frac{1}{\sqrt{\mu}}\right)^{\delta n} \sigma^{-\delta n}$$

This follows from ⊛ on P22.

Then

$$\Pr[X_1, \ldots, X_n \text{ span } V] \leq O(\sqrt{\mu})^{\delta n} \sigma^{-\delta n} \Pr(E_V) \quad ⊛$$

where

$$E_V = \{X_1, \ldots, X_n \text{ span } V \text{ and } Y_1, \ldots Y_{\delta n} \text{ are lin. indep. in } V\}$$

Use $\Pr(E_V) = \Pr(X_1 \ldots V)\Pr(Y_1 \ldots V)$

If E_V occurs then $\exists$ $n - \delta n$ vectors in $X_1, \dots X_n$ which together with $Y_1, \dots Y_{\delta n}$ span V.

Fixing these vectors fixes V. Thus

$$\sum_{V : P[X \in V] \sim \sigma} P_r[E_V] = \sum_{\substack{|S| = n - \delta n \\ X_i : i \in S \\ Y_1, \dots Y_{\delta n}}} P_r[X_i, i \in S, Y_1, \dots Y_{\delta n}] \; \sigma^{\delta n} \leq \binom{n}{\delta n} \sigma^{\delta n}$$

remaining X_i are in V

So

$$\sum_{V : P[X \in V] \sim \sigma} P_r[X_1, \dots, X_n \text{ span } V] \leq \underbrace{O(\sqrt{\mu})^{\delta n} \binom{n}{\delta n}}$$

use (*) on p 23

Now choose $\delta = \delta(\mu)$ small, and μ small so that $\leq (1 - \epsilon)^n$

$\# \sigma = O(n^2)$ and we are done.

Focus on $\Pr(X_v^{(\mu)} = x)$

$v = (v_1, \dots, v_n)$ and $X_v^{(\mu)} = \sum_{j=1}^{n} \eta_j^{(\mu)} v_j$

$$\eta_j^{(\mu)} = \begin{cases} 0 & 1-\mu \\ -1 & \mu/2 \\ 1 & \mu/2 \end{cases}$$

A is an additive set — finite subset of an additive abelian group G.

For our purposes it suffices to take $G = \mathbb{Z}_N$ for a large prime $N \gg \sum_{i=1}^{n} |v_i|$.

Proposition

Let G be a finite group of odd order and $v \in G^n$. Then

$$\Pr\left(X_v^{(\mu)} = x\right) = \mathbb{E}_{\xi \in G}\left(\cos(2\pi\, \xi * x) \prod_{j=1}^{n} \left(1-\mu+\mu\cos(2\pi\,\xi * v_j)\right)\right) \qquad (*)$$

[$\xi * x : G \times G \to \mathbb{R}\backslash\mathbb{Z}$ which is a non-degenerate homomorphism in each component.]

If $G = \mathbb{Z}_p$ then we would take

$\xi * x = \frac{\xi x}{p}$, fractional part.

[Previously $\xi \cdot x : G \times G \to S^1$. Use $*$ to differentiate]

RHS (⊗ 30) =

$$E_{\xi \in G} \left(e^{2\pi \xi * x i} \prod_{j=1}^{n} \left(1-\mu+\mu \cos(2\pi \xi * x)\right)\right)$$

$$\left[E_{\xi} \left(\sin(2\pi \xi * x) \prod_{j=1}^{n} (1-\mu+\mu \cos(2\pi \xi * x)\right) = 0.\right.$$

$$\frac{1}{|G|} \sum_{\xi} S(\xi) f(\xi) = \frac{1}{|G|} \sum_{\xi} S(-\xi) f(-\xi)$$

$$= -\frac{1}{|G|} \sum_{\xi} S(\xi) f(\xi). \quad \Big]$$

$$1-\mu+\mu\cos(2\pi\xi * v_j) = E_\mu\left(e^{2\pi\xi*(\eta_v^{(\mu)} v_j) i}\right)$$

$$\left[\text{RHS} = 1-\mu+\frac{\mu}{2}\left[\cos(2\pi\xi*v_j)+i\sin(2\pi\xi*v_j)\right]\right.$$

$$\left.+\frac{\mu}{2}\left[\cos(2\pi\xi*v_j) - i\sin(2\pi\xi*v_j)\right]\right]$$

$$\text{RHS}(*30) = E_\xi\left(\exp\left\{-2\pi\xi*x\, i + 2\pi i\xi*\sum_j \eta_v^{(\mu)} v_j\right\}\right)$$

$$= E_\xi E_\mu e^{2\pi i\xi*(X_n^{(\mu)}-x)}$$

$$= E_\mu\left(\frac{1}{|G|}\sum_{\xi\in G} e^{2\pi i\xi*(X_n^{(\mu)}-x)}\right)$$

$$= E_\mu\left(\mathbb{1}_{X_n^{(\mu)}=x}\right)$$

$$= \Pr\left(X_n^{(\mu)}=x\right).$$

Proposition

(i) $0 \leq \mu \leq \frac{1}{2} \Rightarrow E_\mu = 1 - \mu + \mu \cos(2\pi \xi * \vartheta_0) \geq 0$

(ii) Suppose $0 \leq \mu \leq \frac{1}{4}$

Let $\xi * \vartheta_0 = a + f$, $a \in \mathbb{Z}$, $|f| \leq \frac{1}{2}$

$$E_\mu = 1 - \mu + \mu\left(1 - \frac{(2\pi f)^2}{2!} + \frac{(2\pi f)^4}{4!} - \dots\right)$$

$$= 1 - \mu\left(\frac{(2\pi f)^2}{2!} - \frac{(2\pi f)^4}{4!} + \dots\right).$$

$$E_\mu \leq 1 - \mu\left(\frac{(2\pi f)^2}{2!} - \frac{(2\pi f)^4}{4!}\right) \leq 1 - \mu \frac{2\pi^2}{5} f^2 \leq e^{-\frac{2\pi^2 \mu}{5} f^2}$$

$$E_\mu \geq e^{-20\mu f^2}$$

[Mathematics]

Proposition : G is finite of odd order

Let $v \in G^n$.

(I) **Domination**

$0 \leq \mu \leq \mu' \leq 1$ and (a) $\mu' \leq \frac{1}{2}$ or (b) $\mu \leq \mu'/4$

$$\Pr[X_{vw}^{(\mu')} = \alpha] \leq \Pr[X_v^{(\mu)} = 0]$$

$vw = v_1 \cdots v_m w_1 \cdots w_m$

(II) **Duplication**

If $0 \leq \mu \leq 1/2$ then

$$\Pr(X_{vw}^{(\mu)} = \alpha) \leq \Pr[X_{v^k}^{(\mu/k)} = 0] \qquad v^k = vvv\cdots v$$

$\forall k \geq 1$

(III) Holder

If $0 \le \mu \le \frac{1}{2}$ then

$$\Pr\left[X^{(\mu)}_{v w_1 \cdots w_k} = x \right] \le \prod_{i=1}^{k} \Pr\left(X^{(\mu)}_{v w_i^{k}} = 0 \right)^{1/k}$$

Proof

Holder

$$\text{LHS} \le E_{\xi}\Big(\prod_{j=1}^{n} \left(1-\mu+\mu\cos(2\pi\xi * v_j)\right) \times$$

$$\prod_{i=1}^{k} \prod_{\ell} \left(1-\mu+\mu\cos(2\pi\xi * w_{i,\ell})\right)\Big)$$

$\le$ RHS.

We use Holder's inequality which implies $E(Z_1 Z_2 \cdots Z_k) \le \prod_{i=1}^{k} E(Z_i^{k})^{1/k}$.

Here $Z_i := \prod_{j=1}^{n} \left(1-\mu+\mu\cos(2\pi\xi * v_j)\right)^{1/k} \prod_{\ell} \left(1-\mu+\mu\cos(2\pi\xi * w_{i,\ell})\right)$.

Domination

$\mu' \leq \frac{1}{2}$ follows from non-negativity and monotonicity $\searrow$ in μ of $1-\mu+\mu\cos(2\pi i\, \xi * v_j)$

On the other hand, if $\mu \leq \mu'/4$ then we use

$$|\cos(\pi\theta)| \leq \frac{3}{4} + \frac{1}{4}\cos(2\pi\theta)$$

and then

$$|1-\mu' + \mu'\cos(\pi\theta)| \leq \left(1-\frac{\mu'}{4}\right) + \frac{\mu'}{4}\cos(2\pi\theta).$$

So

$$\mathbb{E}_{\xi} \prod_{j=1}^{n} \left(1 - \mu' + \mu' \cos(2\pi \xi * v_j)\right)$$

$$\leq \mathbb{E}_{\xi} \prod_{j=1}^{n} \left(1 - \frac{\mu'}{4} + \frac{\mu'}{4} \cos(4\pi \xi * v_j)\right)$$

$\forall \mu \leq \frac{\mu'}{4}$

$$\leq \mathbb{E}_{\zeta = 2\xi} \prod_{j=1}^{n} \left(1 - \mu + \mu \cos(2\pi \zeta * v_j)\right)$$

[Random choice of 2ξ = random choice of ξ - $|G|$ odd]

Duplication

$$\left(1-\mu+\mu\cos(2\pi\theta)\right) \le \left(1-\frac{\mu}{k}+\frac{\mu}{k}\cos(2\pi\theta)\right)^k$$

immediately implies duplication inequality.

$k\log\left(1-\frac{t}{k}\right) \ge \log(1-t)$ — concavity of log.

Proposition

Let $v \in G^n$ where G is torsion free and such that $v_i \neq 0$ for at least k of the v_i. Then for all $0 < \mu \leq 1$ and $x \in G$ we have

$$\Pr[X_v^{(\mu)} = x] = O\left(\frac{1}{\sqrt{k\mu}}\right)$$

Proof

If $\mu \geq \frac{1}{2}$ then $\Pr[X_v^{(\mu)} = x] \leq \Pr[X_v^{(1/8)} = 0]$.

Domination

If $\mu \leq \frac{1}{2}$ then

$$\Pr\left(X_v^{(\mu)} = x\right) \leq \Pr\left(X_{vv}^{(\mu/2)} = 0\right) \quad \text{Duplication}$$

$$\leq \prod_{i=1}^{k} \Pr\left(X_{vv_i^k}^{(\mu/2)} = 0\right)^{1/k} \quad \text{Holder}$$

$$\leq \Pr\left(X_{v_j^k}^{(\mu/2)} = 0\right) \quad \text{for some } j.$$

Now this is simple random walk.

Proof of Proposition 20

Using domination we can assume that $\mu' \leq \frac{1}{4}$ and $x = 0$.

We can also assume that $\mu'/\mu \gg 1$ –

[if μ is "large" we use dominance and absorb in constants in O]

Can assume that $G = \mathbb{Z}_p$ for large prime p.

$$f(\xi) = \prod_{j=1}^{n} \left(1 - \mu' + \mu' \cos(2\pi\, \xi * v_j)\right) \leq \exp\left\{-\frac{2\pi^2\mu'}{5} \sum_j \|\xi * v_j\|^2\right\}$$

$$g(\xi) = \prod_{j=1}^{n} \left(1 - \mu + \mu \cos(2\pi\, \xi * v_j)\right) \geq \exp\left\{-20\mu \sum_j \|\xi * v_j\|^2\right\}$$

Must show

$$E_{\mathbb{Z}_p}(f) = O\left(\sqrt{\frac{\mu}{\mu'}}\, E_{\mathbb{Z}_p}(g)\right) + O\left(E_{\mathbb{Z}_p}(g)^{\Omega(\mu'/\mu)}\right).$$

Fix $0 < \alpha \leq 1$.

$f(\xi) \geq \alpha$ implies

$$\exp\left\{-\frac{2\pi^2\mu'}{5}\sum_{j=1}^{n}\|\xi * v_j\|^2\right\} \geq \alpha$$

$$\Rightarrow \left(\sum_{j=1}^{n}\|\xi * v_j\|^2\right)^{1/2} \leq \sqrt{\frac{5}{2\pi^2}}\,\frac{\sqrt{\log 1/\alpha}}{\sqrt{\mu'}}$$

Thus if $\xi_1, \xi_2, \dots, \xi_m \in S_\alpha := \{\xi \in \mathbb{Z}_p : f(\xi) \geq \alpha\}$

then

$$\left(\sum_{j=1}^{m} \|(\xi_1 + \dots + \xi_m) * \vartheta_j\|^2 \right) \leq \sqrt{\frac{5}{2\pi^2}}\, m \sqrt{\frac{\log 1/\alpha}{\mu^2}}$$

Triangle inequality:

$$\left(\sum_{j=1}^{n} \|(\xi_1 + \xi_2) * \vartheta_j\|^2 \right)^{\frac{1}{2}} \leq$$

$$\left(\sum_{j=1}^{n} \left(\|\xi_1 * \vartheta_j\| + \|\xi_2 * \vartheta_j\| \right)^2 \right)^{\frac{1}{2}} \leq$$

$$\left(\sum_{j=1}^{n} \|\xi_1 * \vartheta_j\|^2 \right)^{\frac{1}{2}} + \left(\sum_{j=1}^{n} \|\xi_2 * \vartheta_j\|^2 \right)^{\frac{1}{2}}.$$

Now let $m = \lfloor c\sqrt{\mu'/\mu} \rfloor$ for small $c>0$:

$$g(\xi_1+\cdots+\xi_m) \geq \exp\left\{-20\mu \sum_{j=1}^{n} \|(\xi_1+\cdots+\xi_m)*\vartheta_j\|^2\right\}$$

$$\geq \exp\left\{-20\mu \cdot \frac{5}{2\pi^2} \cdot \lfloor c\sqrt{\mu'/\mu} \rfloor^2 (\log 1/\alpha)/\mu'\right\}$$

$$> \alpha$$

if $c < \frac{2\pi^2}{100}$.

Thus

$$m\{\xi \in \mathbb{Z}_p : f(\xi) > \alpha\} \subseteq \{\xi \in \mathbb{Z}_p : g(\xi) > \alpha\}$$

Applying Cauchy-Davenport $|A+B| \geq \min\{|A|+|B|-1, p\}$

we get:

$$\left|\{\xi \in \mathbb{Z}_p : g(\xi) > \alpha\}\right| \geq \min\left\{m\left|\{\xi \in \mathbb{Z}_p : f(\xi) > \alpha\}\right| - (m-1), p\right\}$$

$$\Pr(g(\xi) > \alpha) \geq \min\left\{m \Pr_{\mathbb{Z}_p}(f(\xi) > \alpha) - \frac{m-1}{p}, 1\right\}$$

If $\alpha > E_{\mathbb{Z}_p}(g)$ then $\Pr_{\mathbb{Z}_p}(g(\xi) > \alpha) < 1$

So

$$\Pr(f(\xi) > \alpha) \leq \frac{1}{m} \Pr(g(\xi) > \alpha) + \frac{1}{p}$$

Integrating over such α

$$\mathbb{E}_{\mathbb{Z}_p}\left(f \mathbb{1}_{\{\alpha \geq \mathbb{E}(g)\}}\right) \leq \frac{1}{m}\mathbb{E}(g) + \frac{1}{p}$$
$$= O\left(\sqrt{\frac{\mu}{\mu'}}\, \mathbb{E}(g)\right).$$

On the other hand

$$f(\xi) \leq g(\xi)^{(100/2\pi^2)\mu'/\mu}$$

and so

$$\mathbb{E}\left(f \mathbb{1}_{\{\alpha < \mathbb{E}(g)\}}\right) \leq \mathbb{E}(g)^{\frac{100}{2\pi^2}\cdot\frac{\mu'}{\mu}}$$

$\square$

Proof of Proposition 14

A tuple $(\omega_1, \omega_2, \dots, \omega_r)$ is <u>k-dissociated</u> if the GAP $[-k,k]^r \cdot (\omega_1, \omega_2, \dots, \omega_r)$ is proper.

Algorithm

Step 0 $r = 0$; $(w_1, w_2, \dots, w_r)$ is trivially $\frac{1}{2}k$-dissociated.

Proposition 29 implies

$$\Pr(X_v^{(1)} = x) \le \Pr\left(X^{(1/4d)}_{v^{d-r} w_1^{k^2} \cdots w_r^{k^2}} = 0\right) \quad \circledast$$

($r = 0$; duplication $\le P[X^{1/d}_{v^d} = 0] \le$ dominance)

Step 1

$\nu = \#\, i : (w_1, w_2, \dots, w_r, v_i)$ is $\frac{k}{2}$-dissociated.

If $\nu \le k^2$, halt.

[On termination for all but $\le k^2$ of $v_1, \dots, v_n$, $\exists\, a = a(v_i) \in [1, k]$ such that $a v_j \in [-k, k]^r \cdot (w_1, \dots, w_r)$.

Step 2

Write $v^{d-r} w_1^{k^2} \cdots w_r^{k^2} = v^{d-r-1} a\, w_1^{k^2} \cdots w_r^{k^2} b_1 b_2 \cdots b_{k^2}$

where $b_1, \ldots, b_{k^2}$ are k-dissociated from $w_1, \ldots, w_r$.

Then

$$P_*\left[X^{(1/4d)}_{v^{d-r} w_1^{k^2} \cdots w_r^{k^2}} = 0 \right] \leq \prod_{i=1}^{k^2} \underbrace{P_i\left[X^{(1/4d)}_{v^{d-r-1} w_1^{k^2} \cdots w_r^{k^2} b_i^{k^2}} \right]}_{\text{Choose } b_i \text{ to maximise}}{}^{1/k^2}$$

Return to step 1 with $r \leftarrow r+1$; $w_{r+1} \leftarrow b_i$

We only need to prove that we can choose δ_d such that if $\Pr[X_v^{(1)} = x] > \delta_d k^{-d}$ then we halt before r reaches d.

Suppose that we reach step 1 and we have k-dissocossiated tiple $(w_1, w_2, \dots, w_d)$ such that

$$P[X_v^{(1)} = x] \leq P[X^{(1)(4d)}_{w_1^{k^2} \cdots w_d^{k^2}} = 0]$$

Let

$$\Gamma = \{(m_1, m_2, \ldots, m_d) : m_1 \omega_1 + \cdots + m_d \omega_d = 0\}.$$

Then, by independence,

$$P[X_v^{(1)} = x] \leq \sum_{(m_1, \ldots, m_d) \in \Gamma} \prod_{j=1}^{d} P(X_{k^2}^{(1/4d)} = m_j)$$

Note that

(1) $P[X_{k^2}^{(1/4d)} = m] = P[X_{k^2}^{(1/4d)} = -m]$ and $\searrow$ with m

$= \Theta_d(1/k)$

Thus

$$\Pr\left[X^{(1/4d)}_{1_{k^2}} = m\right] = O_d\left(\frac{1}{k}\sum_{m' \in m + (-k/2,\, k/2)} P\left(X^{(1/4d)}_{1_{k^2}} = m'\right)\right)$$

and then

$$\Pr\left[X^{(1)}_{v} = x\right] \leq O_d\left(k^{-d}\sum_{m_1,\dots,m_d \in \Gamma}\ \sum_{\substack{(m_1',\dots,m_d') \in \\ (m_1,\dots,m_d) + \left(-\frac{k}{2},\frac{k}{2}\right)^d}}\ \prod_{v=1}^{d} P\left[X^{(1/4d)}_{1_{k^2}} = m_v'\right]\right)$$

Now $(w_1,\dots,w_d)$ $\big[k/2\big]$ disassociated $\Rightarrow$ distinct.

But then

$$\Pr\left[X^{(1)}_{V} = x\right] \leq O_d\left(k^{-d}\right) \quad \text{and we}$$

take δ_d larger than hidden constant in .