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 $s = 1, 2, \ldots, d\}$

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

$$\le 2^d |A|$$

Generalised Arithmetic Progression

2. Bounds on $A+B$

L 2.1

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

Proof

Result is not affected by replacing

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

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

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

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

□

Exercise: $A, B \subseteq G$

$|A+B| \leq |A| \Rightarrow$ $A \subseteq$ Union of 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

(1) 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: $A' = A \cap B$, $B' = A \cup B$

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

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

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

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

$\Rightarrow \Rightarrow A + x \subseteq B$. y $(A + x) \cap B \neq \emptyset$ or $x \in B - A$

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

$B + A - A \subseteq B$

$B_A + A_B - A = B$

$\Rightarrow$ (by Exercise 3)

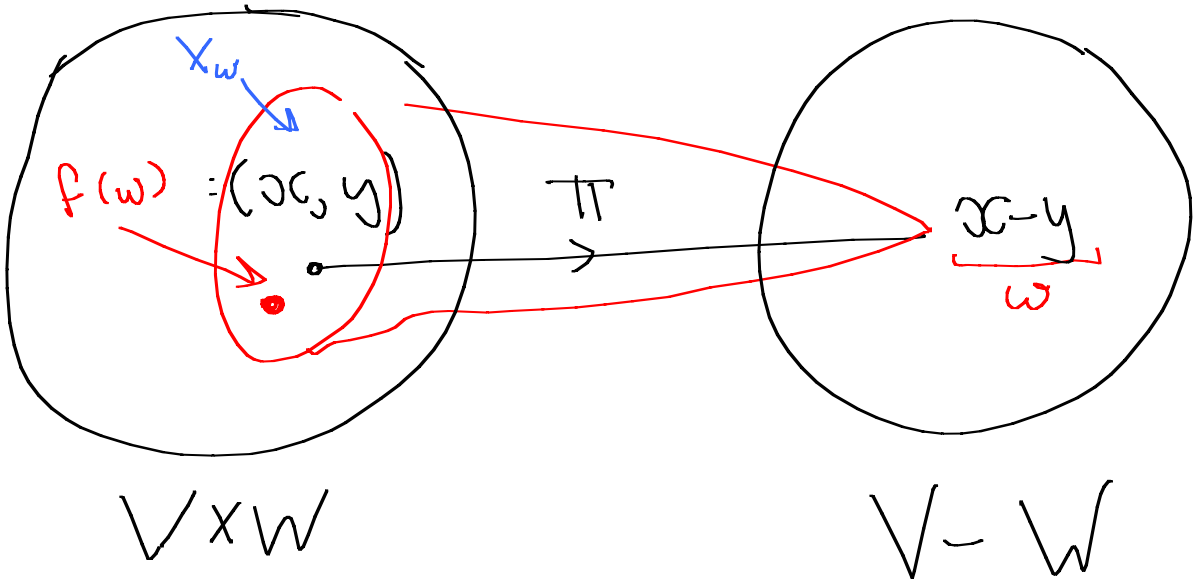
B is a coset of $\mathbb{Z}_p$

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

L 3.1 Ruzsa

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

Proof



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

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

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

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

(iii) $(f(w_1) + U^\Delta) \cap (f(w_2) + U^\Delta) = \emptyset$ $\quad w_1 \neq w_2$

$x \in$

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

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

□

So if

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

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

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

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

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

Plünecke's Theorem!

Plünnecke's Theorem

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

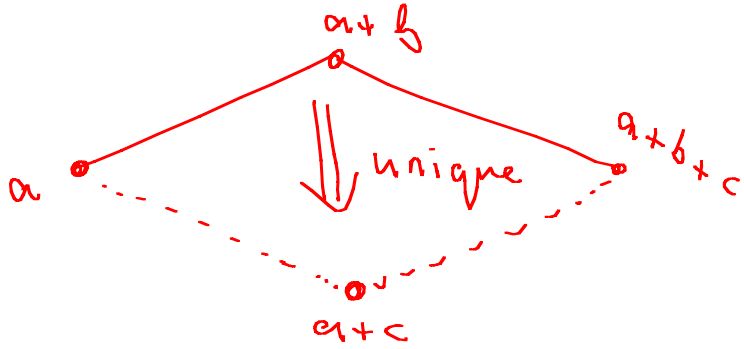
Then

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

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

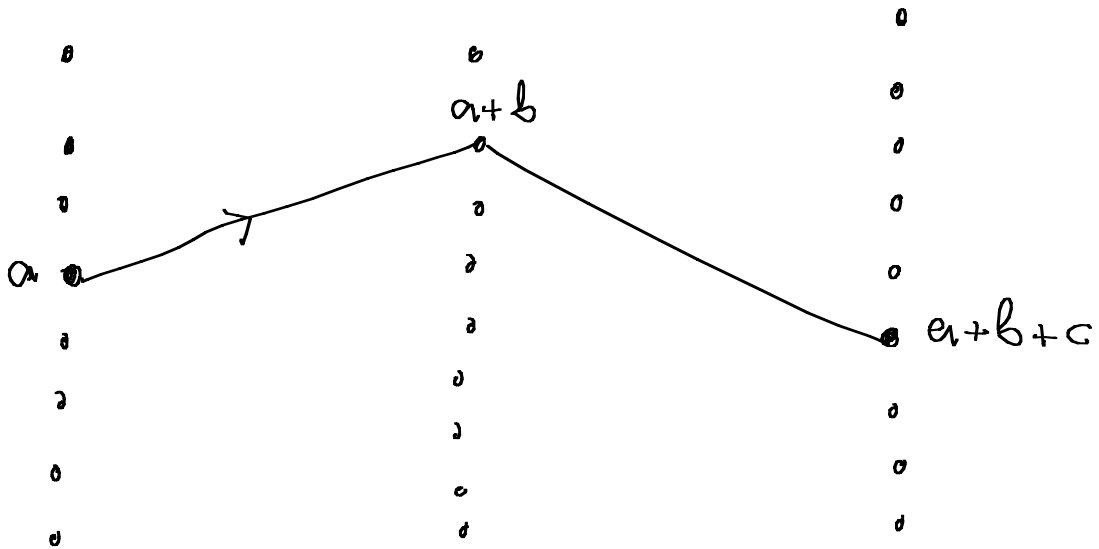
Commuting Graph :

Key Property :

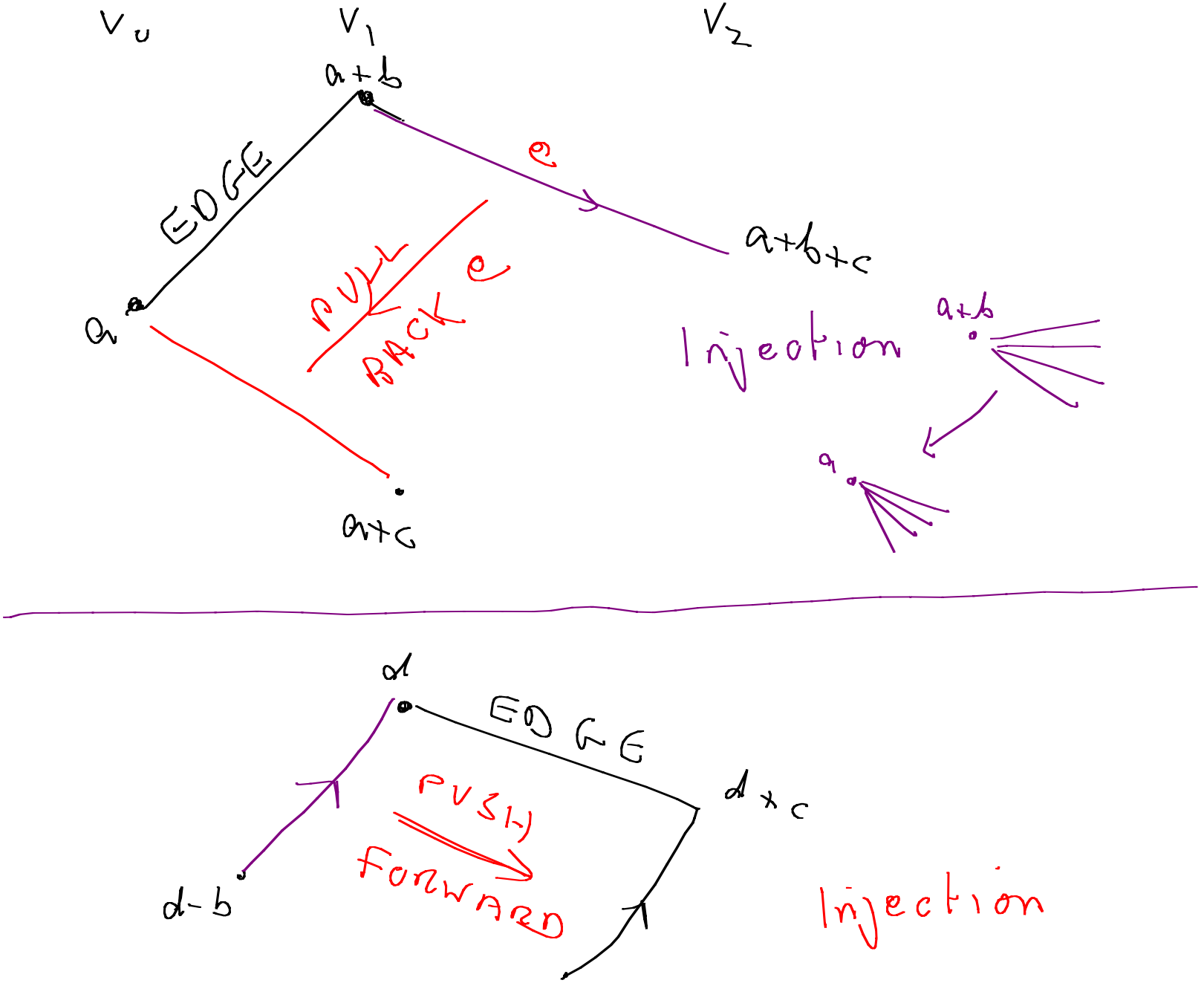


$\Gamma(A, B)$ graph

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



$E_{0 \to 1}$ $\quad E_{1 \to 2}$


V_0
V_1
V_2
a+b
EDGE
e
a
a+b+c
PULL
BACK e
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

V_0 ↓ $V_0 \times \{0\}$

V_1 ↓ $V_1 \times \{1\}$

V_2 ↓ $V_2 \times \{2\}$

Disjoint from picture, we use picture.

Theorem now says:

Let Γ be a commuting graph.

such that $|V_1| < K|V_0|$

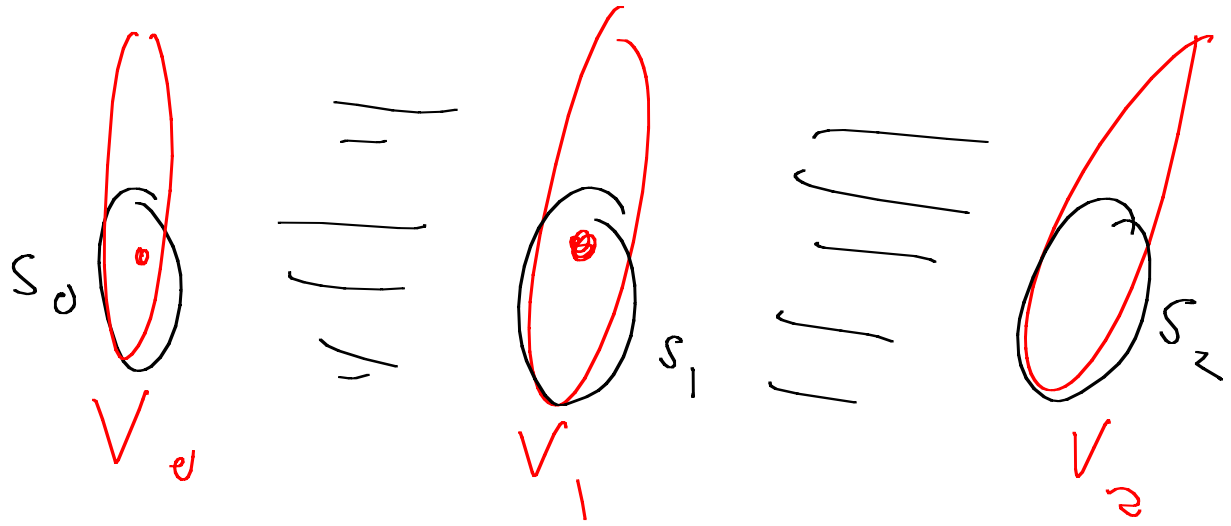
then $\exists\ A' \subseteq V_0$ such that

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

Assume first that $K \geq 1$

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

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 $W_2 \subseteq V_2$

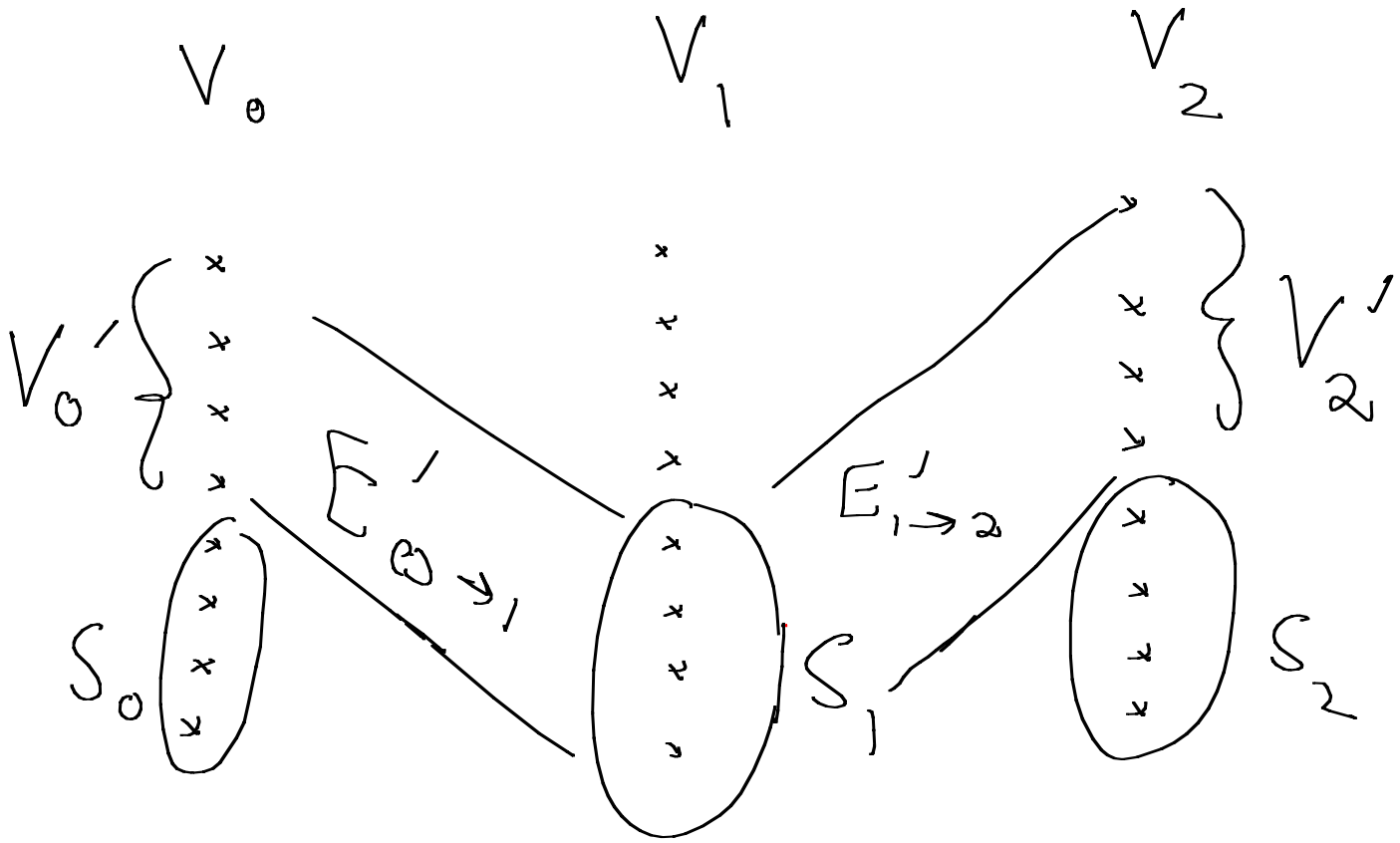
such that $S_0 \cup W_0 \cup W_2$

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

$V_0' \longrightarrow V_2'$

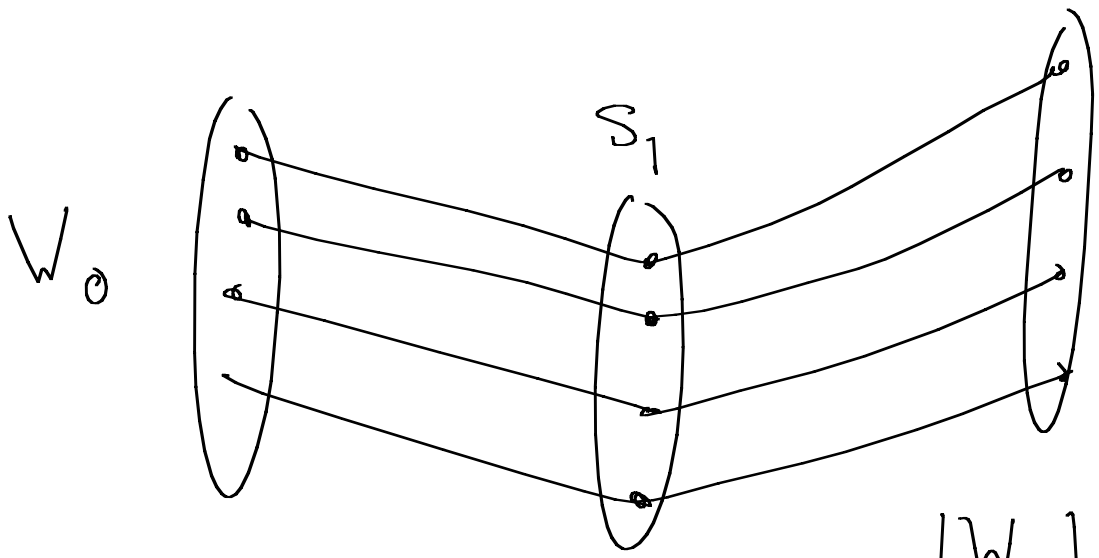
Edges $E'_{0\to 1} \cup E'_{1\to 2}$

(a) S_1 disconnects V_0 from V_2 in Γ'

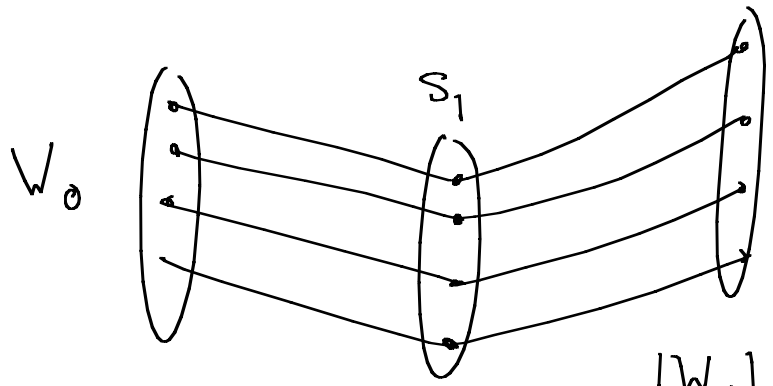
(b) $|S_1| = \text{MINCUT}(V_0', V_2'; \Gamma')$

[otherwise we can reduce size of S]

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



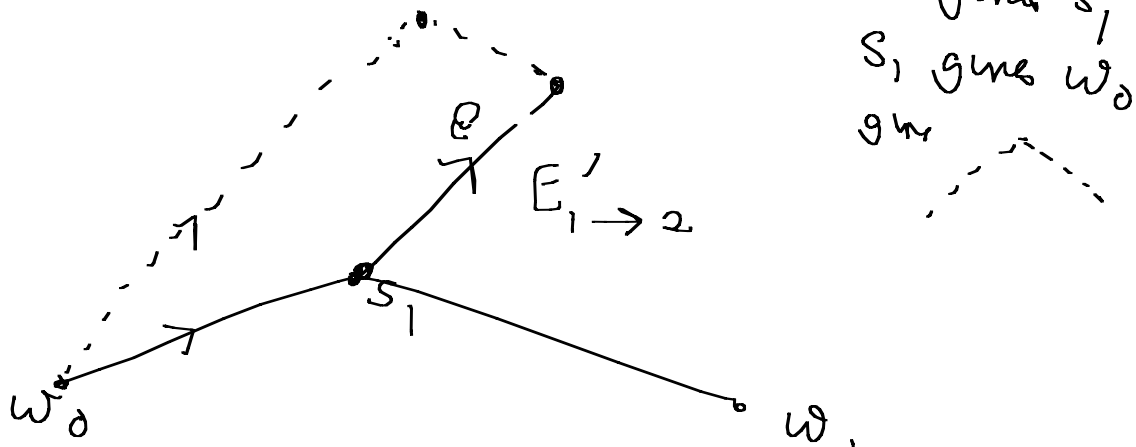
$|W_0| = |S_1| = |W_1|$



$|W_0| = |S_1| \geq |W_1|$

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

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 $W_0 \rightleftarrows$

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

Similarly

Define injection $E'_{0\to 1}$ to W_2

$$|W_2| \le |E'_{1\to 2}| \le |W_0| \le$$

$$|E'_{0,1}| \le |W_2|$$

Therefore $|E'_{0\to 1}| = |W_0|$

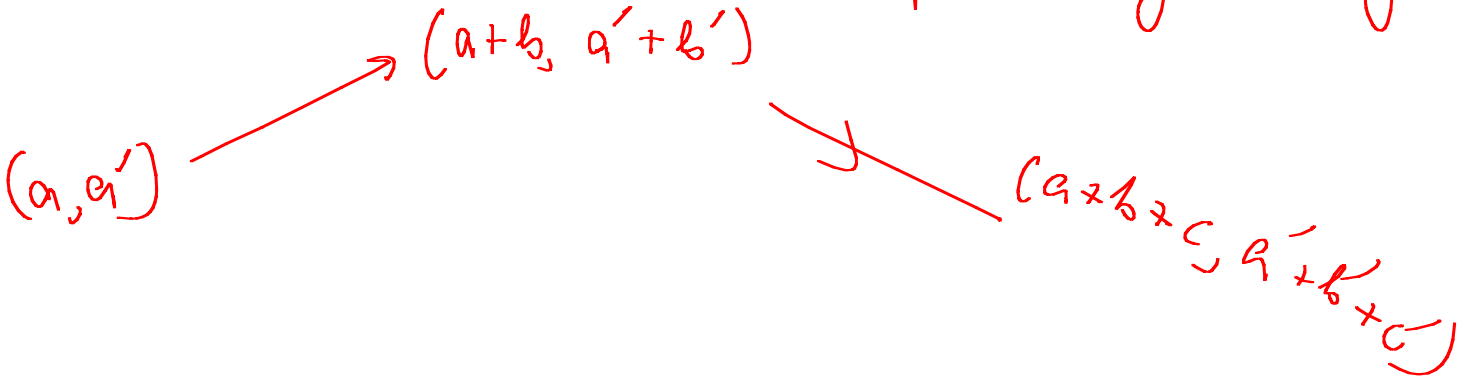
$\Gamma, \hat{\Gamma}$ two commuting graphs on $G, \hat{G}$.

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

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

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

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



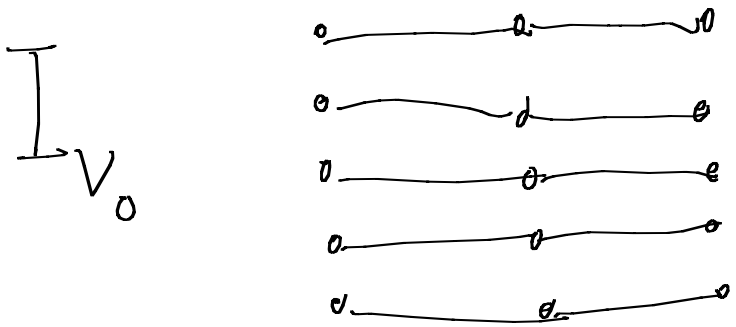
$$D(\Gamma) = \inf_{\substack{A' \subseteq V_0 \\ A' \neq \emptyset}} \frac{|\Gamma^2(A')|}{|A'|}$$

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

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

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

(11)

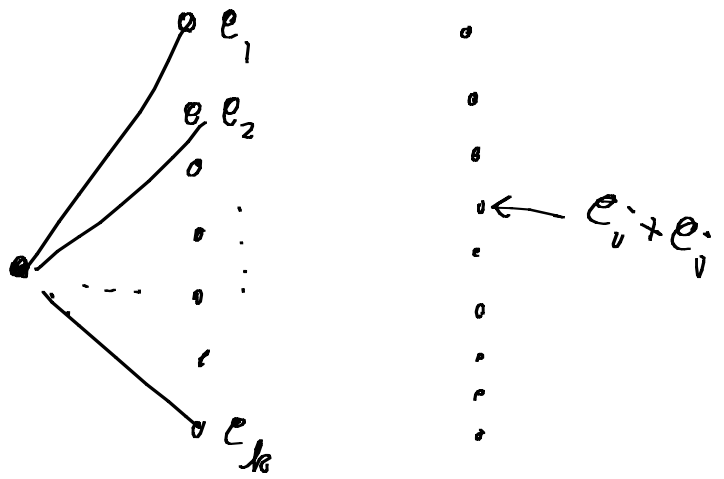


$$\left(\Gamma \times \widehat{\Gamma}\right)^2 (\Omega) = \left(\Gamma \times I_{\widehat{V}_2}\right)^2 \left(I_{V_0} \times \widehat{\Gamma}\right)^2 (\Omega)$$

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

$$|\sim| \leq d\,\widehat{d}\;\; |\Omega|$$

Γ_k :



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

$$D(H_{k_2}) = \frac{k(k-1)}{2}$$

$H_{k_2}^{+}$: reverse

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

End of proof

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

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

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

$$D(\Gamma \times H_k^+) < 1$$

Why

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

$V_1 \times \{k\}$

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

by $K<1$ case

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

Remark (10)

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

$\frac{V_1}{V_0}$ 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 $|A'+B+B| \leq \frac{2K^2}{\delta}|A|$.

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.

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

$$\vdots$$

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

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

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

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

$$\leq \sum_{J=0}^{k-1} \frac{K^2 |A|^2}{|A_J|^2} |A'_J|$$

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

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

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

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

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

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

$A' = A$ is not always possible

Example from Ruzsa.

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

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

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

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

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

$A = A_0 \cup A_1$

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

Iterated Plünnecke

$A, B \subseteq G$ and $|A+B| \leq K|A|$. Then for $t = 1, 2, \ldots$

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

Should be K^t

Proof

(1) $t = 2^0$. $\exists A_2 \subseteq A : |A_2 + B + B| \leq K^2 |A_2|$

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

$\vdots$

(1)

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

t_1

any $b \in B$

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

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

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

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

$2t$ should be t.

Corr. 8.2

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

Proof:

(I) $|mB-mB| \overset{L3.1}{\le} \underbrace{|A_{m+mB}|^2}_{U_m \to |A_m|} \overset{L3.1}{\le} K^{4m}|A|$.

(II) Suppose $m \le n$

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

Covering one set by another

L 9.1 (Ruzsa)

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

Proof

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

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

(i) $|\mathcal{F}| \le \dfrac{|A+B|}{|A|}$

$X = \{b : U_b \in \mathcal{F}\}$

(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

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

(ii) $\forall b \in B$, $\exists \ge \frac{|A|}{2}$ 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) $|X^*| \le \mathrm{Bin}\left[N|Y|, \frac{r}{N|Y|}\right]$

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

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

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

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

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

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

$|X| \le 2r$

$b \in X + A$.

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)

$P_1(v \in S) = p$

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

$E(cr(H)) = t p^4$.

So $t p^4 \geq \geq mp^2 - 3np$

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

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

to maximize RHS

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

□

Point Line Incidences [Szemerédi, Trotter]

Someone else's proof?: Solymosi?

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

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

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

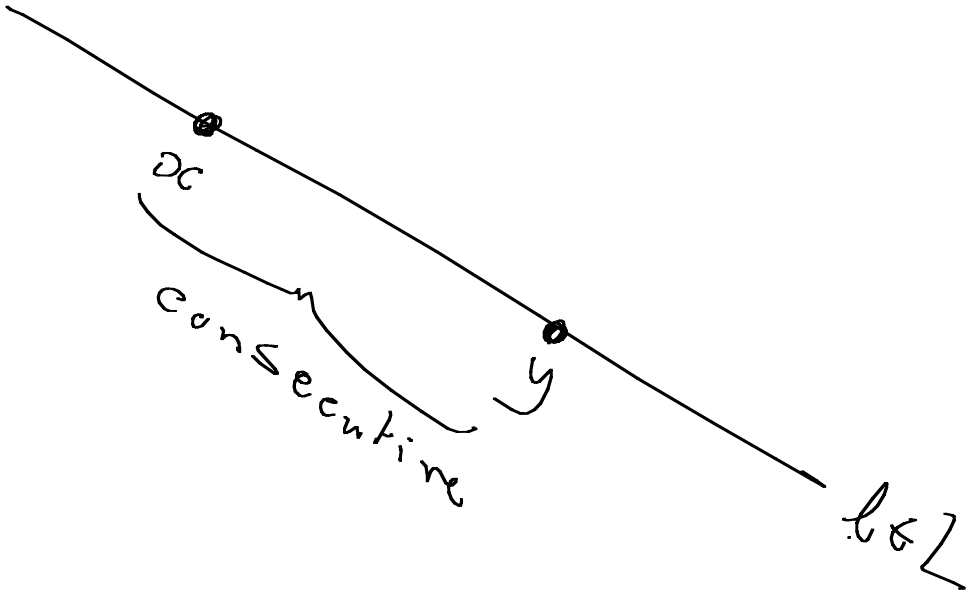
$|I| \leq 4 (m^{2/3} n^{2/3} + m + n \}$

Proof

$G = (P, E)$

n vertices

$|E| - n$ edges



$$cr(G) \leq \binom{n}{2}$$

(I) $|E| - n < 4n$ or (II) $\binom{n}{2} \geq cr(G) \geq \frac{(|E| - n)^3}{64n^2}$

In both cases

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

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

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

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

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

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

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

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

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

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

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

Each $\ell \in L$ 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) $X \leq |B|^2 |C|^2 \Rightarrow X \leq |B|^{2/3} |C|^{2/3} X^{2/3}$

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

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

$X \geq |A|^2$

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

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