- Expander Graph

Def (Spectral expander)

G be (n, d, λ)-expander, if

- G n vertices, d-regular
- $\max\{\lambda_2(A_G), |\lambda_n(A_G)|\} \leq \lambda d$.

Recall $d = \lambda_1, \ldots, \lambda_n \geq -d$

Def (Combinatorial expander)

G, n vertices, d-regular

(n, d, ρ)-edge expander if

$$\forall\ S \subseteq V,\quad |S| \leq \frac{n}{2},$$

$$\frac{E(S, \bar{S})}{d|S|} \geq 1 - \rho.$$

Thm (i) (n, d, λ)-expander $\Rightarrow$

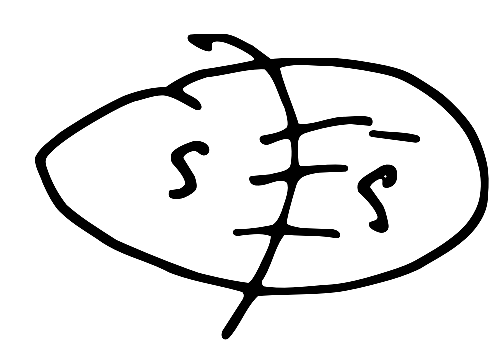
$(n, d, \frac{1+\lambda}{2})$-edge expander

(ii) (n, d, ρ)-edge expander

$\Rightarrow$ $(n, d, \lambda(\rho))$-expander ☆

(See [Arora-Barak] Chapter 21, a beautiful proof)

Pf. "$\Rightarrow$" $\forall |S| \le \frac{n}{2}$.



$$\frac{|E(S,\bar{S})|}{d|S|} = \frac{ds - E(S,S)}{ds} = 1 - \frac{E(S,S)}{ds}$$

$$E(S,S) = 1_S^t A_G \cdot 1_S \qquad \mu := \left(\frac{1}{\sqrt{n}}, \dots \frac{1}{\sqrt{n}}\right)$$

$$= \left(\frac{s}{\sqrt{n}}\mu + \sqrt{\frac{s(n-s)}{n}}\mu'\right) A_G \left(\frac{s}{\sqrt{n}}\mu + \sqrt{\frac{s(n-s)}{n}}\mu'\right)$$

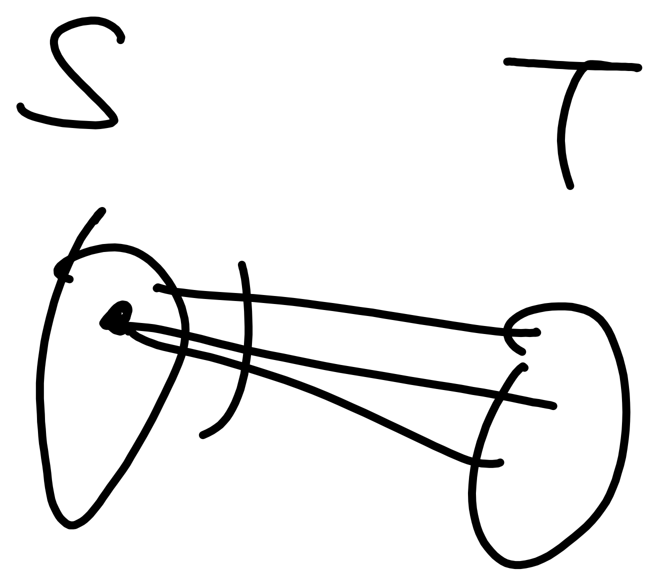
$$\le \frac{ds^2}{n} + \frac{s(n-s)}{n}\lambda d$$

$$\le ds\left(\frac{s}{n} + \frac{n-s}{n}\lambda\right) \le ds\left(\frac{1}{2} + \frac{\lambda}{2}\right)$$

■

Expander Mixing Lemma $\quad \forall S,T \subseteq V$

$$\left| E(S,T) - \frac{d|S|\cdot|T|}{n} \right| \le \lambda d \sqrt{|S||T|}$$



on average, for $|S| \ge |T|$

$$\frac{E(S,T)}{|S|} \approx d\cdot\frac{|T|}{n} \pm \lambda d \sqrt{\frac{|T|}{|S|}}$$

Expander Hitting Property — "Indepence"

G (n,d,λ)-expander.

Consider $B \subseteq V$, $\quad p = \frac{|B|}{|V|}$.

Take $v_0 \in V$ u.a.r.,

$v_0 - v_1 - v_2 - \cdots - v_t$ random walk based on A_G/d.

Then: $$\Pr\left[\bigvee_{i=0}^{t} v_i \in B\right] \le p(p+\lambda)^t.$$

Pf: Let $P = \begin{pmatrix} 0 & & \\ & 1 & \\ & & 0 \end{pmatrix} \in \mathbb{R}^{V \times V}$

$P(u,u) = 1$ if $u \in B$

$u = \left(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n}\right)^\perp$.

$$w = P A_{a/d} \cdots A_{a/d} P A_{a/d} P u = (P A_{a/d} P)^t \cdot P u$$

$$\Pr\left[\bigvee_{i=0}^{t} v_i \in B\right] = \sum_{v \in V} w_v$$

$$\leq \sqrt{\sum_{v \in B} w_v^2} \cdot \sqrt{pn} \quad \text{(Cauchy-Schwarz)}$$

$$= \|(P A_{a/d} P)^t P u\| \cdot \sqrt{pn}$$

$$\leq \|P A_{a/d} P\|^t \cdot \underbrace{\|Pu\|}_{=\sqrt{pn}} \cdot \sqrt{pn}$$

$$\|P A_a P\| = \max_{\|v\|=1} v^\perp P A_a \underset{\sim}{Pv}$$

Decompose $Pv = \sqrt{\alpha}\,\mu + \sqrt{1-\alpha}\,\mu'$; $\mu = \left(\frac{1}{\sqrt{n}}, \dots, \frac{1}{\sqrt{n}}\right)^\perp$

$$\leq \alpha d + \lambda(1-\alpha) d$$

$\sqrt{\alpha} = \langle Pv, \mu \rangle = \langle v, P\mu \rangle \leq \|v\| \, \underset{\leq p}{\|P\mu\|}$

$$\leq (p + \lambda) d.$$

Remark: (i) $B_0, B_1, \ldots, B_t$ instead of $B\ B\ B\ B \ldots$

(ii) $\Pr\left[\bigvee_{i=0}^{t} v_i \in B\right] \geq p\,(p - O(\lambda))^t$

[Alon-Feige-Wigderson-Zuckerman 95]

Thm ~~Expander~~ Chernoff Bound (Gillman 98)

$v_0, v_1, \ldots, v_t$ $\underbrace{\text{i.i.d, u.a.r.} \in V}$

v_i u.a.r.

$v_i \cdots v_t$ expander walk

$$X_i := \begin{cases} 1 & v_i \in B, \\ 0 & \text{o/w} \end{cases}$$

$$\Pr\left[\left|\frac{1}{t+1}\sum X_i - p\right| > \varepsilon + \lambda\right] \leq \exp(-\Omega(\varepsilon^2 t))$$

Application 1. Error reduction.

$\mathcal{A}$ one-sided error randomized alg. using r bit

$x \in f^{-1}(0)$, $\mathcal{A}(x) = 0$

$x \in f^{-1}(1)$, $\mathcal{A}(x) = 1$ w.p. $1/2$.

- Repeat $\mathcal{A}$ t times

  using ~~fresh random bits~~, expander graph $(2^r, d, \lambda)$

  output 1 if in any run $\mathcal{A}(x)=1$

  0 o/w

$\mathcal{A}^t$ one-sided error, error prob. $\le \cancel{2^{-t}}$. $\exp(-\Omega(t))$.

uses $\cancel{t \cdot r}$ rand. bits.

$r + (t-1)\log d = r + O(t)$.

Application 2 coding theory

Def Error correcting codes (ecc)

$$C : \{0,1\}^m \to \{0,1\}^n .$$

e.g. repetition code

$0 \mapsto 000$

$1 \mapsto 111$

Hamming code $(4,7)$

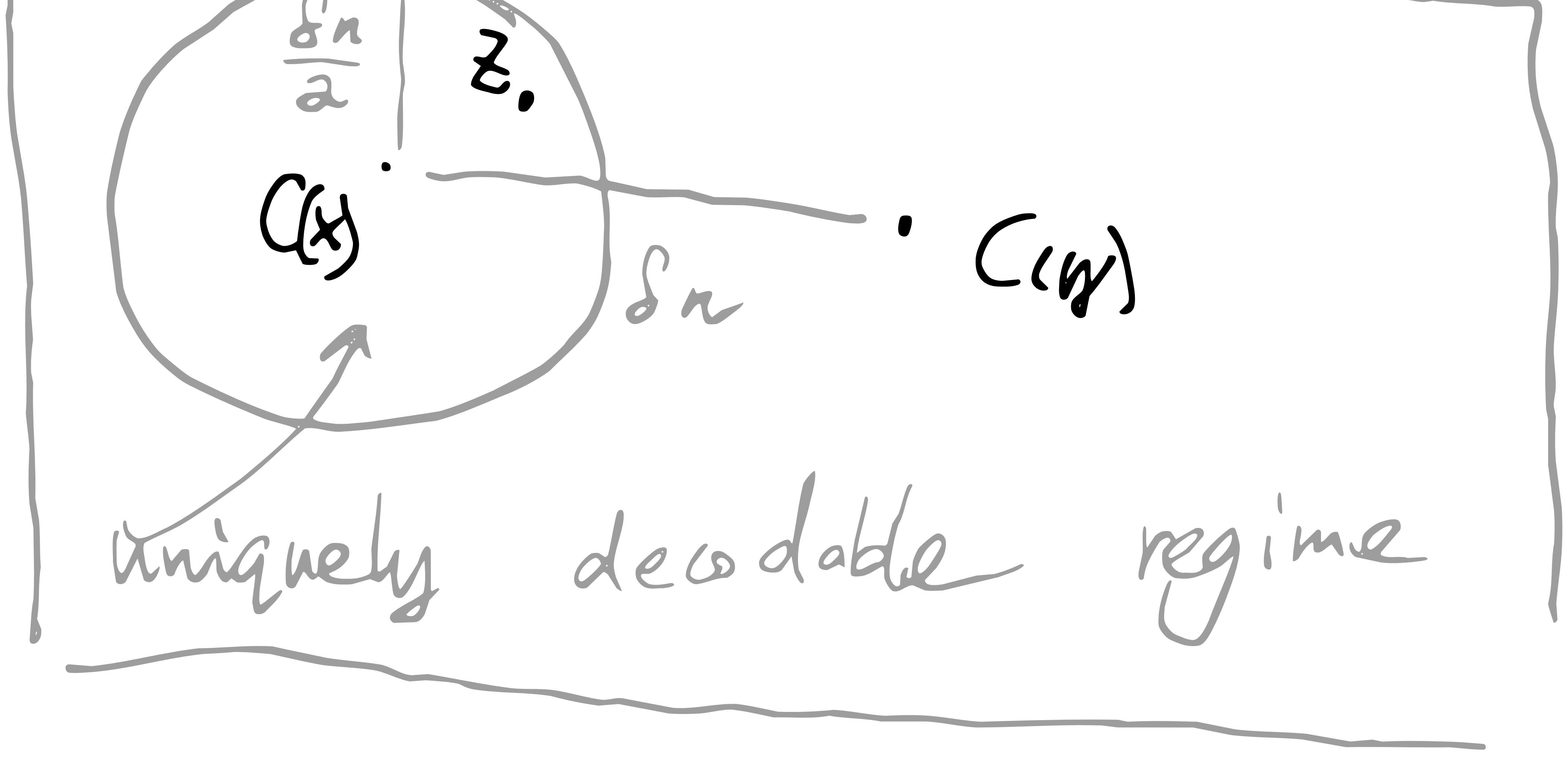
(x_1, x_2, x_3, x_4)

$\mapsto (x_1, x_2, x_3, x_4, x_1 \oplus x_2 \oplus x_4, x_1 \oplus x_3 \oplus x_4, x_2 \oplus x_3 \oplus x_4)$

rate : $\dfrac{m}{n}$,

distance (relative) δ : $\displaystyle \min_{x \neq y \in \{0,1\}^m} \frac{\Delta(C(x), C(y))}{n}$

Δ : Hamming distance



Linear codes

We don't worry about messages. In the end, $C : \{0,1\}^m \to \{0,1\}^n$ corresponds to some linear algebra problem.

$$C \underset{\text{subspace}}{\subset} \{0,1\}^n$$

If $X \in C$, $Y \in C$, then $X + Y \in C$. (Bool operation)

Given <u>parity checking matrix</u> $P \in \{0,1\}^{k \times n}$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \\ & & 1 \end{pmatrix}$$

Repetition

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ & & & & \ddots & & & \end{pmatrix}$$

Hamming

$$C = \ker P := \{X : PX = 0\}.$$

<u>rate</u>: $\dfrac{\dim C}{n} \geq 1 - k/n$

<u>dist</u>: $\min\limits_{\substack{X \in \ker P \\ X \neq 0}} \dfrac{|X|}{n} = \min\limits_{\substack{X, Y \in \ker P \\ X \neq Y}} \dfrac{|X+Y|}{n}$

- Expander codes

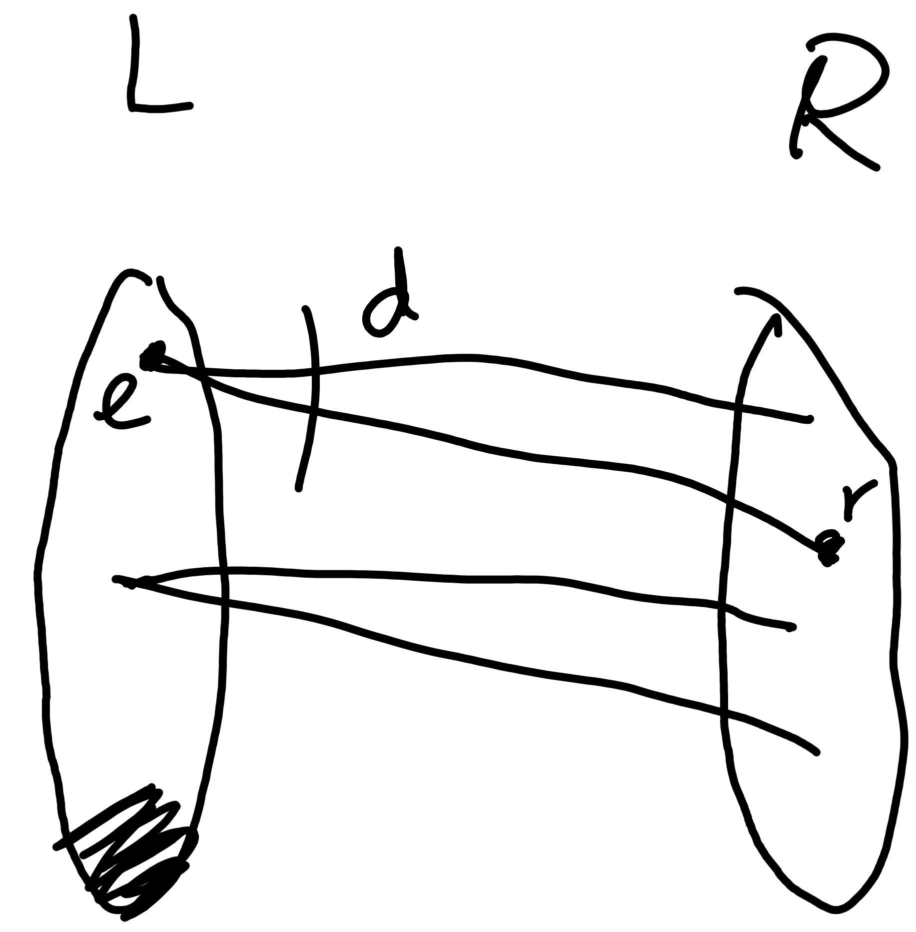
Def: Bipartite expander graph $G = (L \cup R, E)$

(n, k, d, α, ρ)-left expander, if

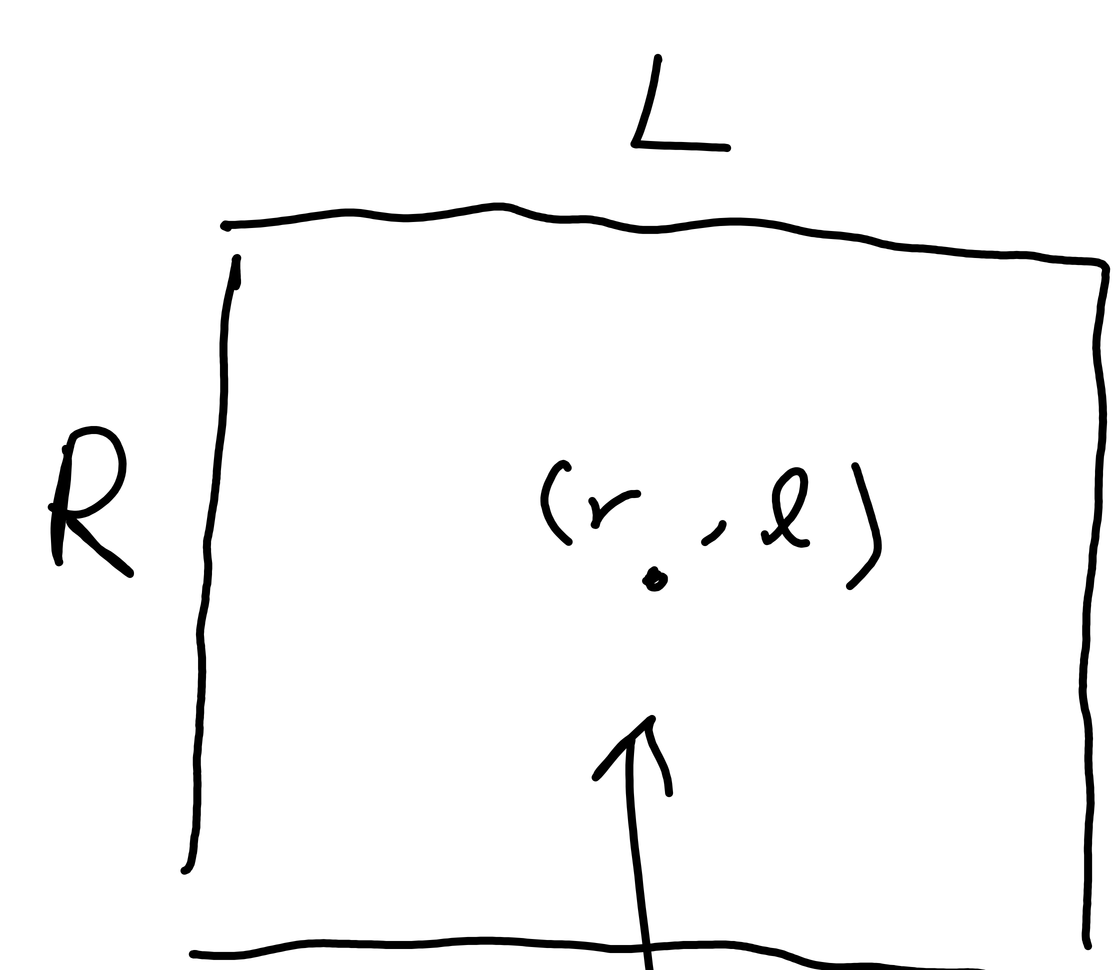
- left d-regular, $|L| = n$, $|R| = k$
- left (α, ρ)-expansion, i.e.,

$S \subseteq L$, $|S| \le \alpha n$, then

$N(S) \ge (1-\rho)\, d|S|$.



$\Rightarrow$



1 if $(l, r) \in E$

M_G

Thm: Suppose G is

$(n, k, d, \alpha, 0.2)$ - bipartite expander. $\quad \rho \leq 0.5 - o(1)$

Then $C := \ker M_G$ is st.

$\text{rate}(C) \geq 1 - \frac{k}{n}$,

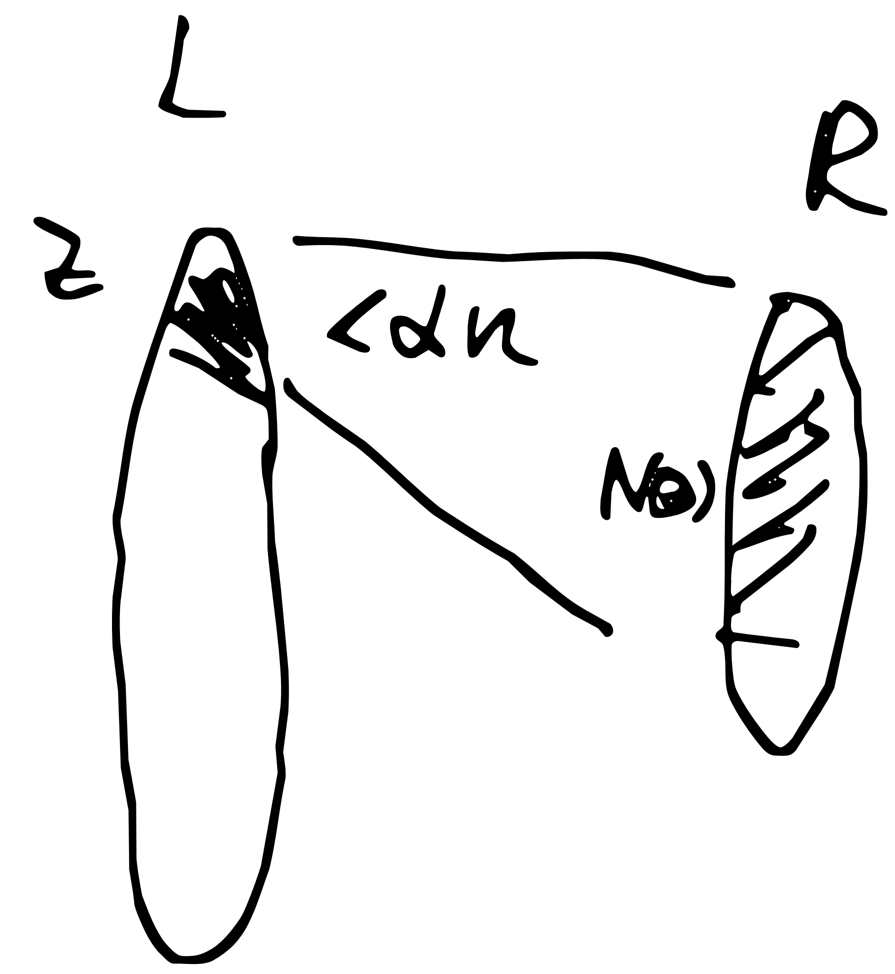
$\text{distance}(C) > \alpha$.

Pf: • rate ✓

• $\text{distance}(C) > \alpha$

$\Leftarrow \forall z \in \ker M_G \setminus \{0^n\}, \ |z| > \alpha n$.

$\Leftarrow \forall |z| \leq \alpha n, \ z \neq 0^n, \ M_G \cdot z \neq 0$.



▲ $N(z) \geq 0.8\, d\, |z|$

▲ If $M_G \cdot z = 0$, each $r \in N(z)$
$|N(r) \cap z|$ even

$\Rightarrow E(z, N(z)) \geq N(z) \cdot 2$
$= 1.6\, d|z|$ ∎

<u>Decode</u> (Sipser–Spielman 98)

Let z be received word.
while $\exists\, u \in L$, s.t. $\text{unsat}(N(u)) > \frac{d}{2}$,
flip $z(u)$. $(0 \to 1,\ 1 \to 0)$

$\boxed{\text{Thm: If } \Delta(z, X) < \frac{\alpha}{2} n, \text{ for some } X \in C \text{. Then Decode}(z) = X.}$

Pf: For any z, let $U \subseteq R$ be unsat ...

① As long as $0 < \Delta(z, X) < \alpha n$,
exist $u \in L$, s.t. $|N(u) \cap U| > \frac{d}{2}$.

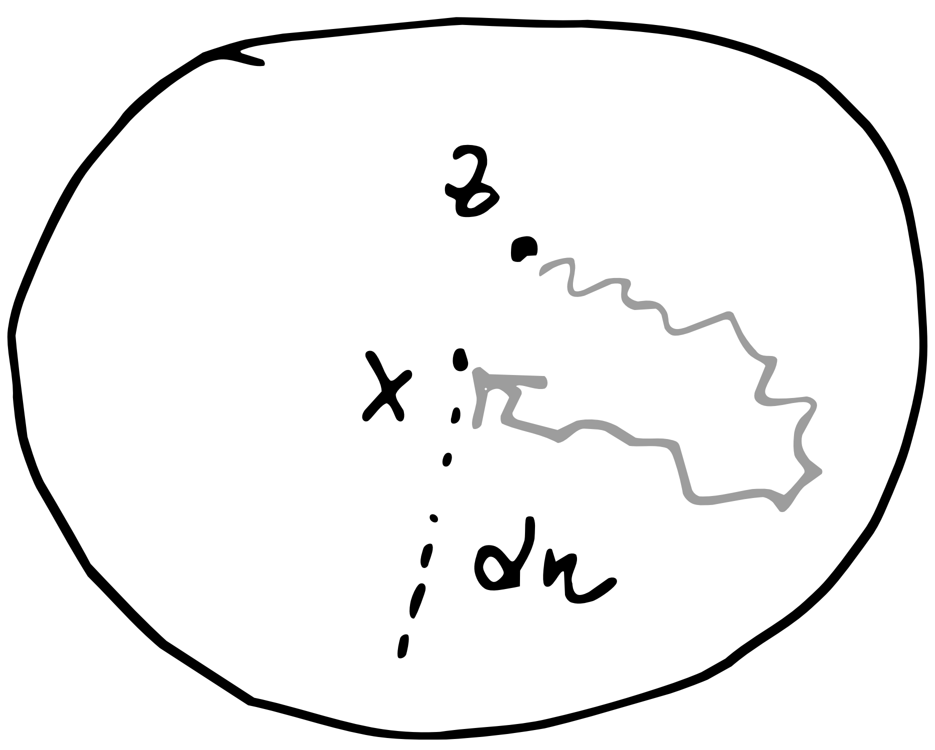
$N(Y) \geq 0.8\, d|Y|$, $Y = z + X$

$$\Rightarrow \Big| \underbrace{\{ r \in N(Y) : |N(r) \cap Y| = 1 \}}_{\subseteq U} \Big| \geq 0.6 d |Y|$$

If ① not true, $|U| \leq |Y| \cdot d/2 < 0.6 d |Y|$,
a contradiction!

② If in the beginning $\Delta(z_0, x) < \frac{\alpha}{2} n$.

in Decode, $\Delta(z_t, x) < \alpha n$ always.



<u>Suppose</u> at some point

$\Delta(z_t, x) = \alpha n$.

Let $Y_t = z_t \Delta X$

Then, $|U_t| \geq 0.6\, d \alpha n$.

However $U_0 \leq d\,|Y_0| < \frac{d \alpha n}{2} < |U_t|$,

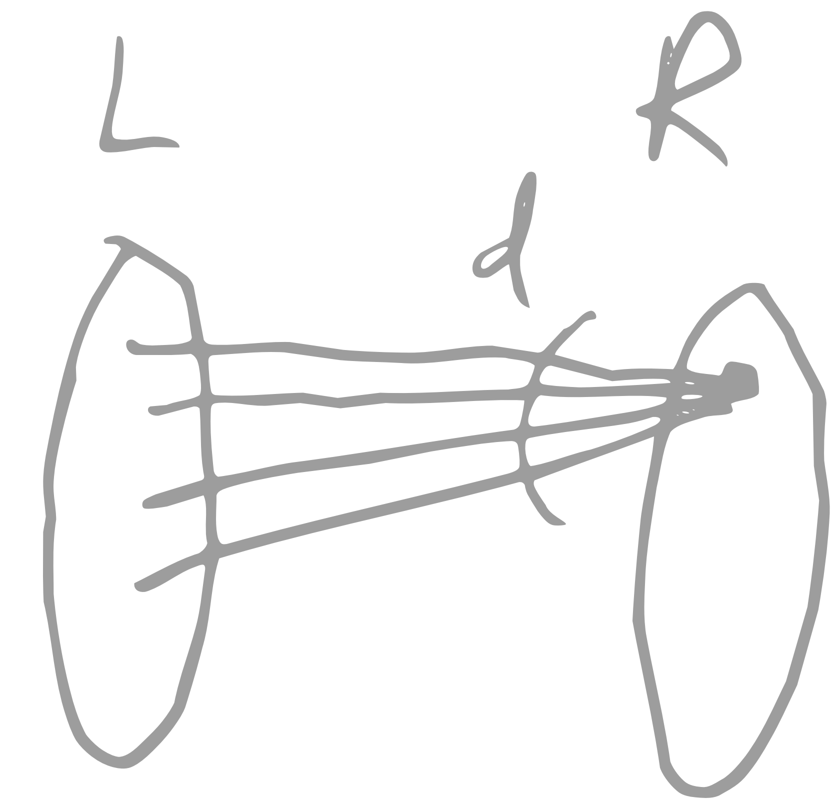
a contradiction!

$\boxtimes$

- Tanner Code

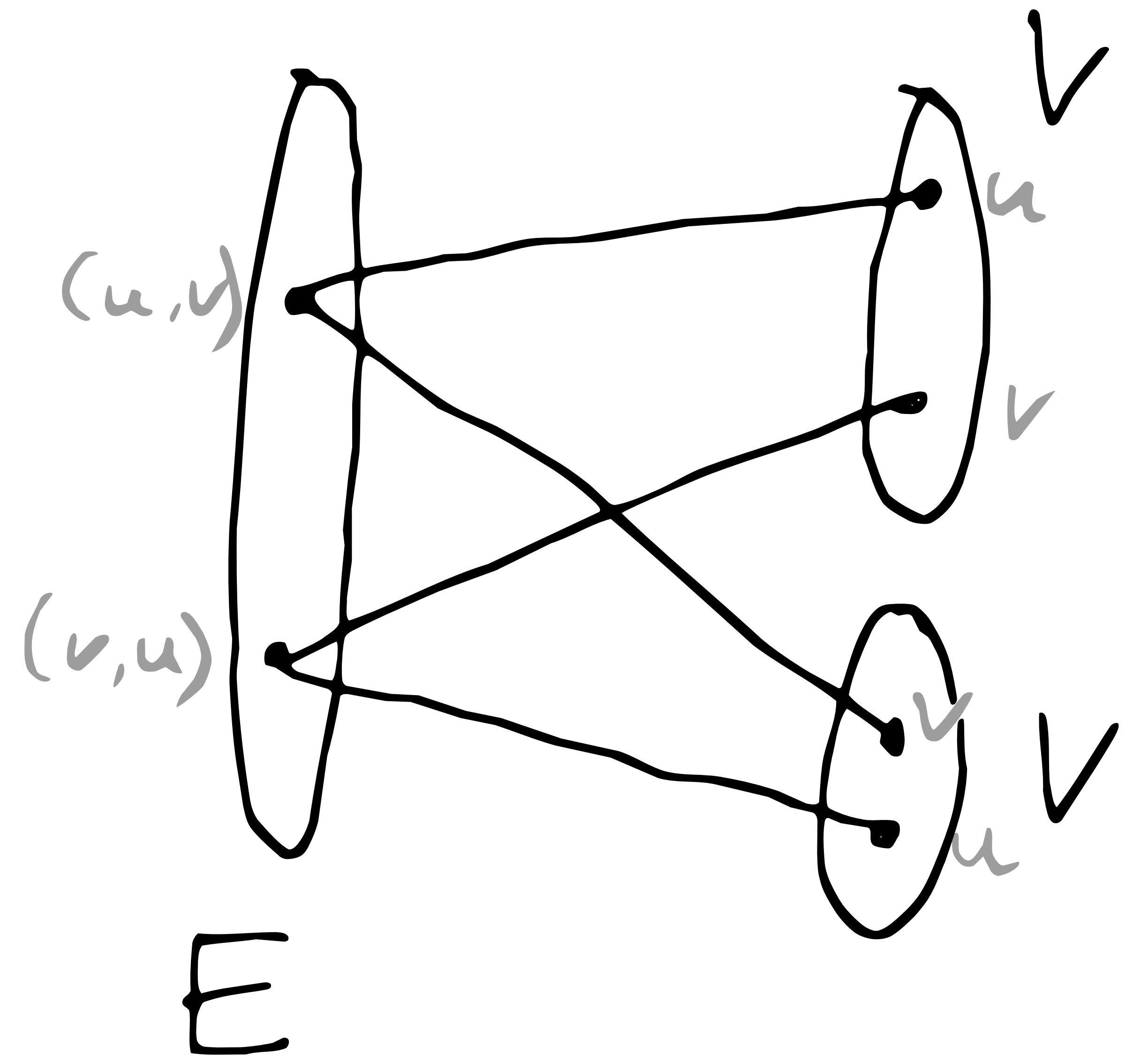
$T(G, C_0)$, where $G = (L \cup R, E)$ is right d-regular. C_0 is a linear code $\subseteq \{0,1\}^d$.

$X \in T(G, C_0)$, if $\forall\, r \in R$, $X|_{N(r)} \in C_0$.



- where is G from?

$H = (V, E)$ be (n, d, λ)-expander



$L = E$

$R = V_0 \sqcup V_1$

Thm Suppose C_0 (ρ, δ)-code. H is (n, d, λ).

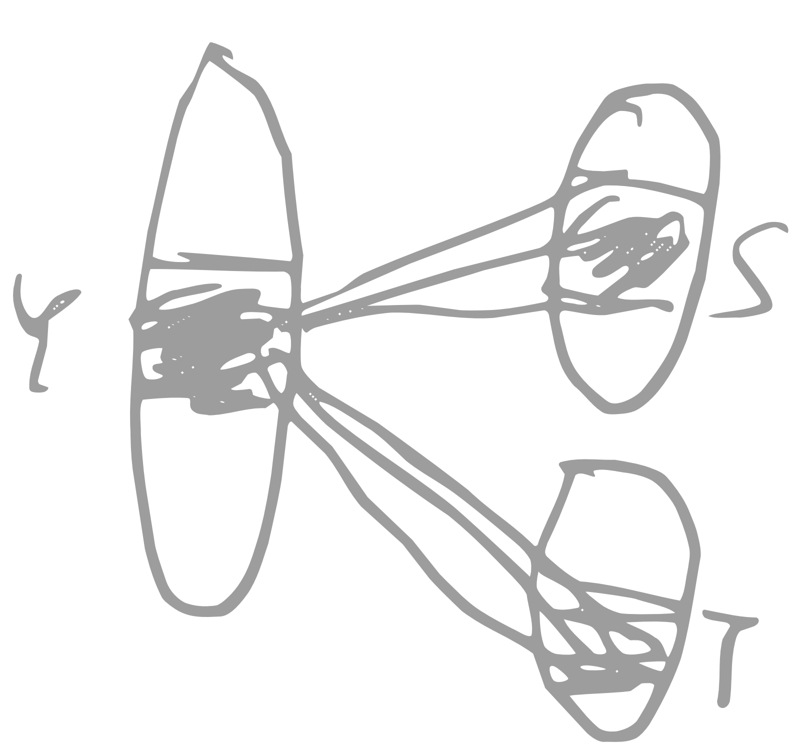
rate ↑ dist ↑

then $T(G_H, C_0)$ is $(2\rho - 1, \delta(\delta - \lambda))$

Pf: ▶ rate $\geq 1 - \underbrace{2n}_{\text{vertices in } R} \underbrace{(d - \dim C_0)}_{\text{each vertex induce \# constraints}} / dn$

$= 2\rho - 1$

▶ distance $Y \subseteq E$, $Y \in T(G_H, C_0)$



By C_0, $\forall u \in N(Y)$

$|N(u) \cap Y| \geq \delta d$. (1)

"Average degree large"

But, by expander mixing lemma. $(|S| \geq |T|)$

$$|E(S, T)| \leq \frac{d}{n}|S||T| + \lambda d \sqrt{|S||T|} \quad (2)$$

"Average degree small if T small,

implied by Y small"

From (1)

$$|Y| \geq \frac{1}{2}\left(|S|\delta d + |T|\delta d\right) \geq \sqrt{|S||T|}\cdot\delta d,$$

From (2)

$$\frac{d}{n}|S||T| + \lambda d\sqrt{|S||T|} \geq \sqrt{|S||T|}\,\delta d$$

$$\iff \quad \sqrt{|S||T|} \geq n(\delta-\lambda)$$

$$\implies |Y| \geq \delta(\delta-\lambda)\,dn.$$

<u>Decode</u> : Given $z \in \{0,1\}^E$,

Repeat for $O(\log n)$ times

- For $u \in V_0$, (Up-correction)
  decode $z|_{N(u)}$ based on C_0
- For $v \in V_1$, (Down-Correction)
  decode $z|_{N(v)}$ based on C_0

Thm (Zémor 01) For $\lambda < 0.1\delta$,

$\Delta(z, x) \le \delta^2/4$, for $x \in T(G_H, C_0)$.

~ We can show 6

Then, $\mathrm{Decode}(z) = x$

Pf $z = z_0' \xrightarrow{\text{up}} z_1 \xrightarrow{\text{Down}} z_1' \xrightarrow{\text{up}} z_2 \xrightarrow{\text{Down}} z_2' \to \cdots$

Define $U_i = \{ u \in V_0 :$

$$\underbrace{\Delta\left(z_{i-1}'|_{N(u)}, x|_{N(u)}\right) \ge \frac{\delta}{2} d}_{\substack{\text{Thus after UP-correction} \\ z_i|_{N(u)} \ne x|_{N(u)}}} \}.$$

$D_i = \{ v \in V_1 :$

$$\Delta\left(z_i|_{N(v)}, x|_{N(v)}\right) \ge \frac{\delta}{2} d \}.$$

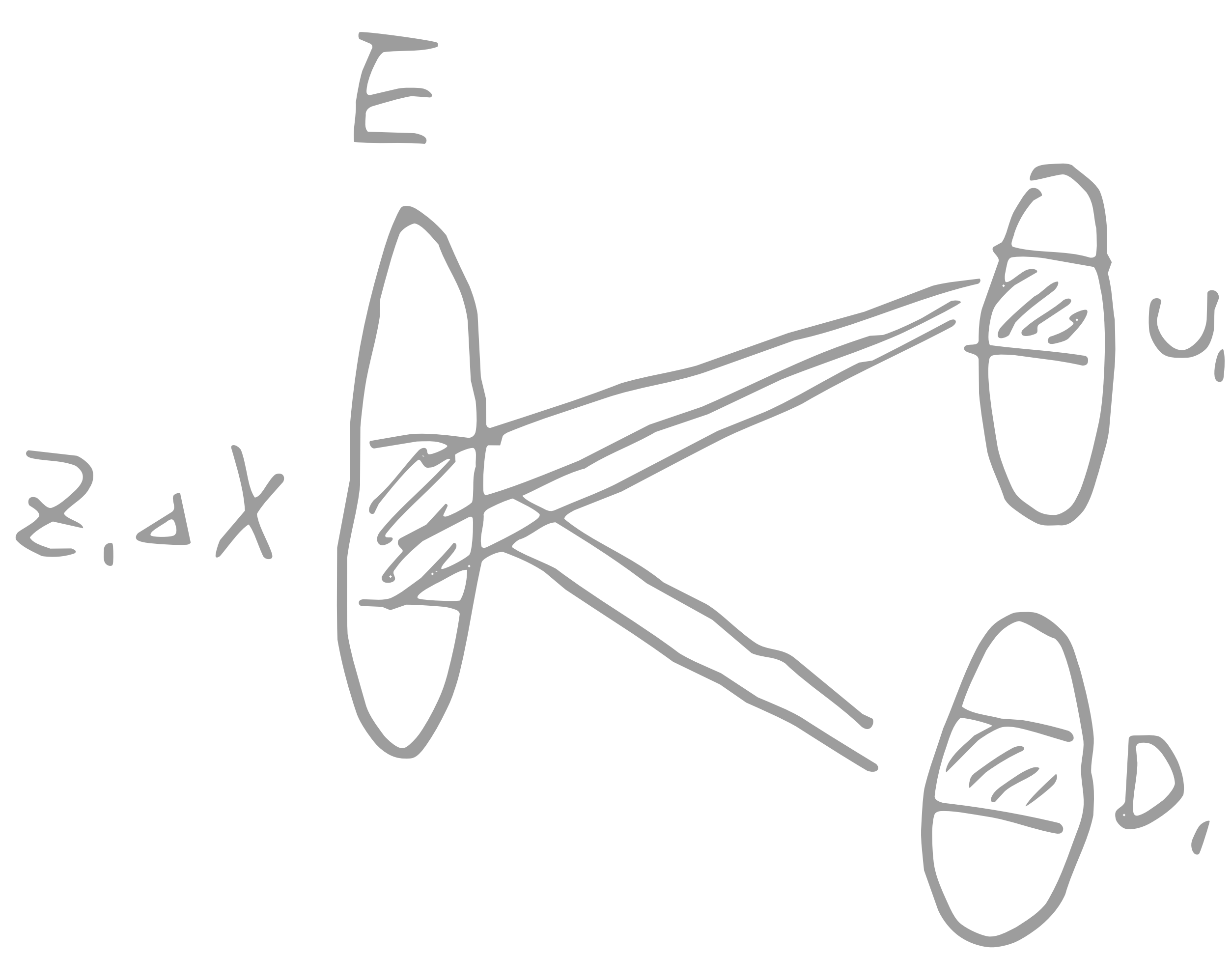
Idea: Show for some $\epsilon > 0$, $\forall i$

(i) $|D_i| \le (1-\epsilon)|U_i|$,

(ii) $|U_i| \le (1-\epsilon)|D_{i-1}|$.

Suppose error $\le \delta^2/6 \cdot dn$

$$|U_1| \le \frac{\text{error}}{\delta/2\, d} \le \delta/3\, n.$$



Note:

- $Z_1 \Delta X \subseteq N(U_1)$

$\Rightarrow D_1 \subseteq N(Z_1 \Delta X)$

① By definition, $N(D_1) \geq |D_1| \cdot \frac{\delta}{2} d$

Avg deg large

② By E.M.L.

$$\frac{|E(D_1, S_1)|}{|D_1|} \leq |D_1| \cdot \left(\frac{|S_1|}{n} + \lambda \sqrt{\frac{|S_1|}{|D_1|}} \right) d$$

$$\frac{|S_1|}{n} + \lambda \sqrt{\frac{|S|}{|D_1|}} \geq \frac{\delta}{2}$$

$$\Rightarrow \frac{|S_1|}{|D_1|} \geq \left(\frac{\delta}{2} - \frac{\delta}{3} \right)^2 \lambda^{-2}$$

$$= \left(\frac{\delta}{6\lambda} \right)^2 \geq \left(\frac{5}{3} \right)^2$$

as long as $\lambda \leq 0.1\, \delta$.

∎

- Construction of expander

Limitation

$\boxed{\begin{array}{l} \underline{\text{Thm}}: \text{For any } d\text{-regular } G, \\ \lambda(G) := \max\{\lambda_2(A_G), |\lambda_n(A_G)|\} \\ \geq \Omega(\sqrt{d}). \end{array}}$

Pf "Trace method"

$$\lambda_i(A_G^t) = \lambda_i(A_G)^t$$

$$\operatorname{tr}(A_G^t) = \sum_{i=1}^{n} \lambda_i(A_G^t) = \sum \lambda_i(A_G)^t$$

$$\leq d^t + (n-1)\lambda(G)^t \qquad (1)$$

$\operatorname{tr}(A_G^t) \geq n \cdot d^{t/2}$ by counting paths.

$\therefore$ Set $t=2$, $\lambda(G) \geq \sqrt{d} \cdot \sqrt{\frac{n-d}{n-1}}$. ∎

Thm (Alon-Boppana). For every (n,d) graph G

$$\lambda(G) \geq 2\sqrt{d-1} - o(1).$$

1. Existance of expander graph (family, for infinitely many n)

Answer: almost all (n,d) graphs!

Thm (Friedman 03) For any $\epsilon > 0$,

$$\Pr_{G \sim (n,d)\text{-graph}}[\lambda(G) \leq 2\sqrt{d-1} + \epsilon] = 1 - o_n(1).$$

2. Explicit expander graph

Thm (Margulis 73, Gabber-Galil 81)
8-regular graph G, $V = \mathbb{Z}_n \times \mathbb{Z}_n$.

$$(x,y) \sim (x \pm 2y, y), \ (x, y \pm 2x)$$
$$(x \pm (2y+1), y), \ (x, y \pm (2x+1)).$$

$\lambda(G) < 1$.

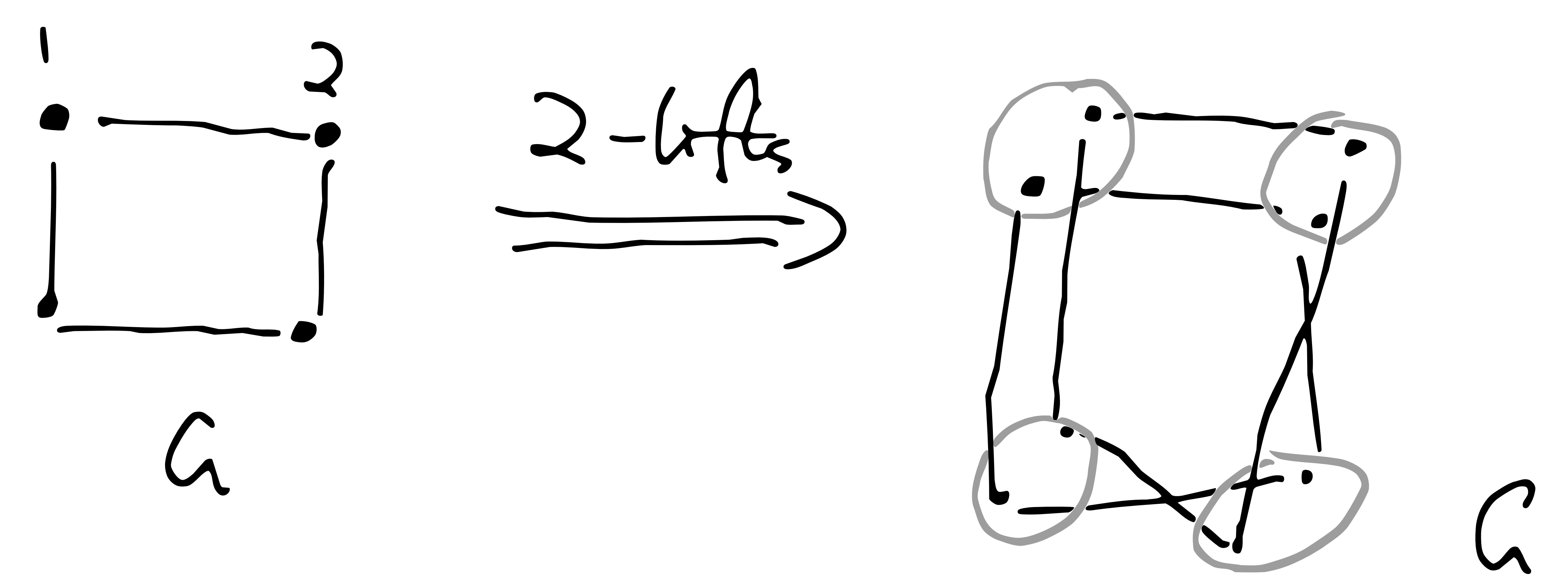
Thm (LPS 88) For every prime p, every positive $k \in \mathbb{Z}$

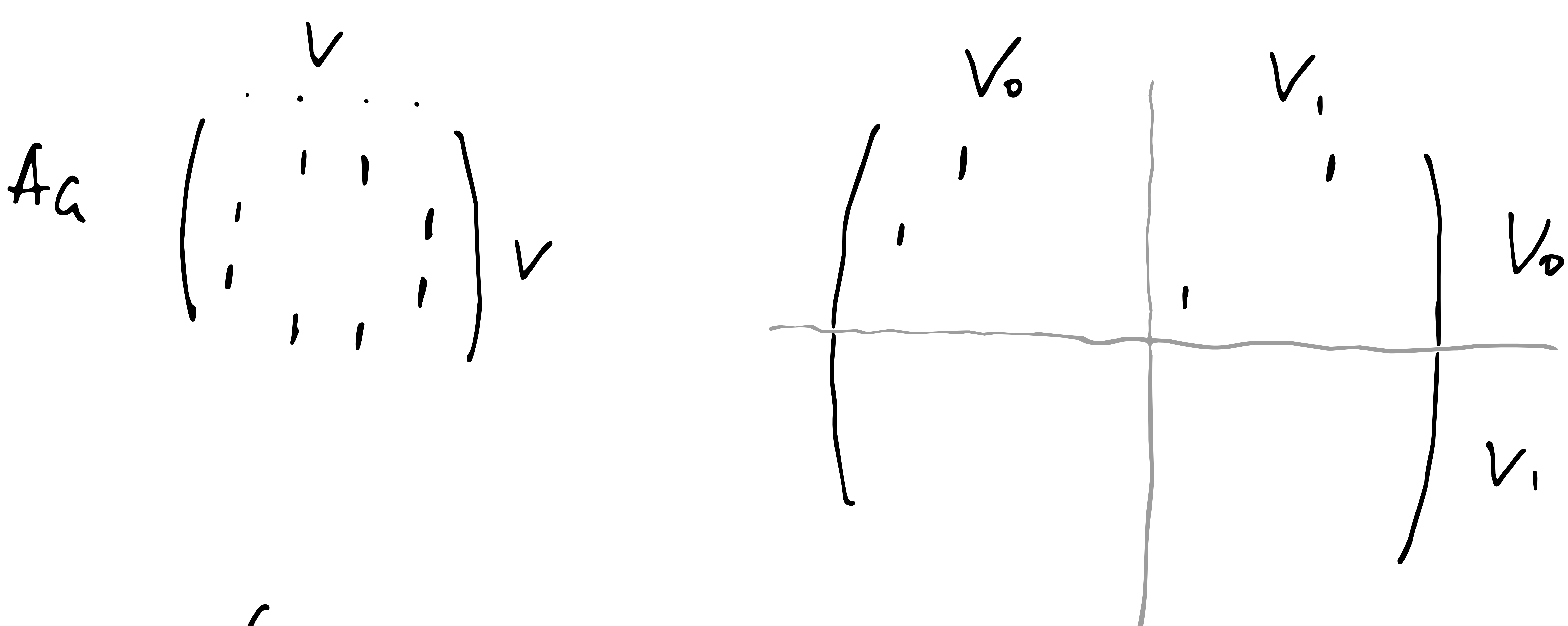
$\exists$ family of (n,d)-graph G, $d = p^k + 1$.

$$\lambda(G) = 2\sqrt{d-1}.$$

3. Combinatorial construction

- Lifts





$$A_{G'} = \begin{pmatrix} B & C \\ C & B \end{pmatrix}, \text{ s.t. } \quad B + C = A_G$$

Signed A_G, $\tilde{A}$ symmetric, s.t.

$$\tilde{A}(i,j) = \begin{cases} \pm 1 & \text{u.a.r.} \quad (i,j) \in G, \\ 0 & \text{o/w}. \end{cases}$$

$$B = \frac{A_G + \tilde{A}}{2}, \quad C = \frac{A_G - \tilde{A}}{2}.$$

Claim: $\lambda_i(A_G)$, $\lambda_i(\tilde{A})$ forms the spectrum of $A_{G'}$.

Pf: ① Let v, λ be s.t. $A_G \cdot v = \lambda v$

$$\begin{pmatrix} B & C \\ C & B \end{pmatrix} \begin{pmatrix} v \\ v \end{pmatrix} = \lambda \begin{pmatrix} v \\ v \end{pmatrix}.$$

② Let v, λ be s.t $\tilde{A} v = \lambda v$

$$\begin{pmatrix} B & C \\ C & B \end{pmatrix} \begin{pmatrix} v \\ -v \end{pmatrix} = \begin{pmatrix} (B-C)v \\ -(B-C)v \end{pmatrix} = \lambda \begin{pmatrix} v \\ -v \end{pmatrix}. \quad \blacksquare$$

$\underline{\underline{\text{Thm}}}$ (Marcus-Spielman-Srivastava 15)

For any (n,d)-graph G, exists $\tilde{A}$, s.t.

$$\lambda_1(\tilde{A}) \leq 2\sqrt{d-1}.$$

$|\lambda_i(\tilde{A})| \leq O(\sqrt{d \log^2 d})$ (Bilu-Linial 06)

$O(d^{3/4})$ (Friedman 03, k lifts w.h.p)

- Zig-Zag Product [Reingold-Vadhan-Wigderson 02]

$\underline{\underline{\text{Def}}}$: G : (n,m,α)-expander (V_G, E_G)

H : (m,d,β)-expander (V_H, E_H)

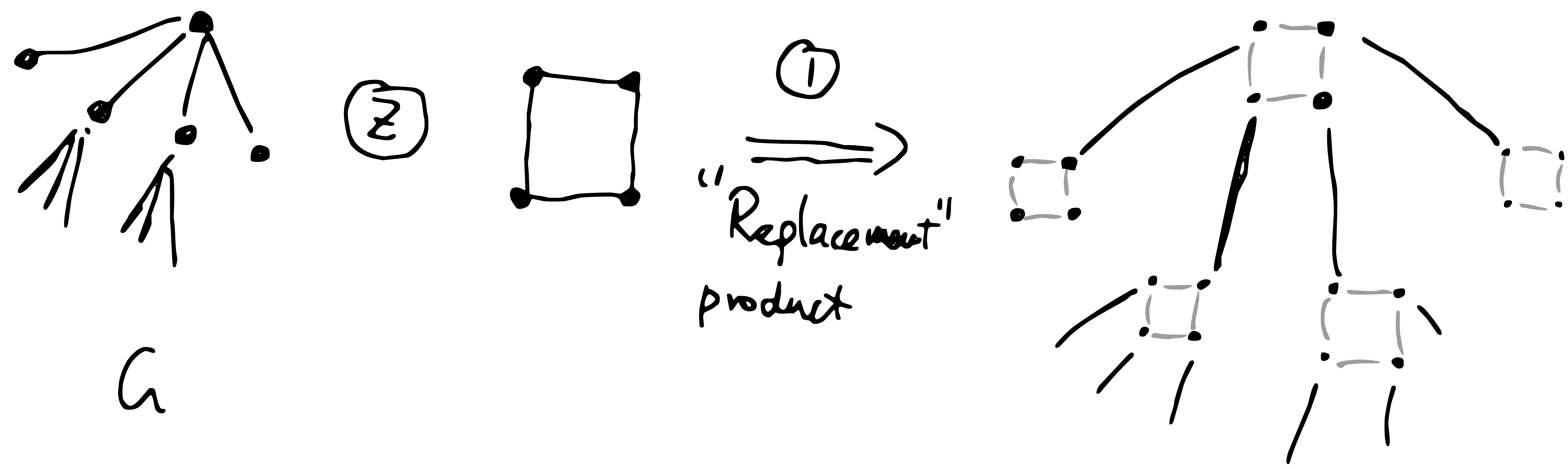
$G \circledz H$ is

$$V = V_G \times V_H$$

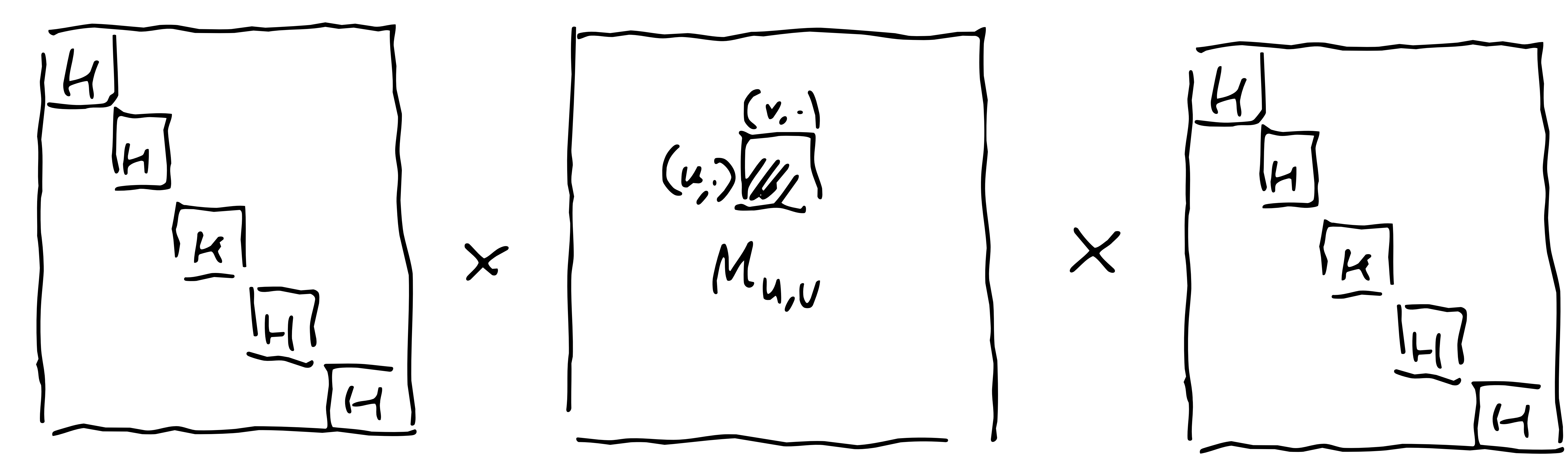
E see picture

$\underline{\text{Then}}$, $\lambda \leq \max\{\alpha+\beta, \beta+\beta^2\}$

see analysis



$A_{G ⓩ H} =$



① a walk in H
$W_H = I \otimes H$

② a walk in G
W_G

③
W_H

$$M_{u,v} = \boxed{\;\cdot\;(i,j)\;}$$

$(i,j) = 1$ if
$(u,v) \in G$
u is v's j^{th} neighbor
v is u's i^{th} neighbor

For any $v \in \mathbb{R}^{mn}$, $\|v\|=1$, $\sum v_i = 0$

$$v = \Big(\overset{1,2,\dots m}{\underbrace{\boxed{v_{u,1} \cdots v_{u,m}}}_{u}}, \underbrace{\boxed{\qquad}}_{v}, \;\dots\; \boxed{\qquad}\Big)^{\perp}$$

$\mu = \left(\frac{1}{\sqrt{m}}, \dots, \frac{1}{\sqrt{m}}\right)^{\perp}$, $a_u = \langle (v_{u,1} \dots v_{u,m}), \mu \rangle$

$$\tilde{v} = \Big(a_u \boxed{\tfrac{1}{\sqrt{m}}, \cdots \tfrac{1}{\sqrt{m}}}, a_v \boxed{\tfrac{1}{\sqrt{m}} \cdots}, \;\dots\; \Big)^{\perp} \Big/ \|\tilde{v}\|$$

$$\boxed{\underline{\text{Claim}}: \sum a_u^2 \le 1, \quad \sum a_u = 0}$$ $\leftarrow$ Why?

Decomposition

$$v = \sqrt{\gamma}\,\tilde{v} + \sqrt{1-\gamma}\,\hat{v}, \quad \gamma = \sum a_u^2,$$

$$\hat{v} \perp \tilde{v}, \quad \|\hat{v}\| \le 1$$

$$W_H \cdot v = d\,\tilde{v} + \sqrt{1-\gamma} \cdot \beta' d\,\bar{v},$$

(By H expansion) $\bar{v} \perp \tilde{v}$, $\|\bar{v}\| \le 1$, $\beta' \le \beta$

$$\lambda(G) = \max_{\|v\|=1} |v^t W_H W_G W_H v|$$

$$= d^2 \left|\left\langle \left(\sqrt{\gamma}\,\tilde{v} + \beta' \sqrt{1-\gamma}\,\bar{v}\right), \underline{\underline{W_G}} \left(\sqrt{\gamma}\,\tilde{v} + \beta' \sqrt{1-\gamma}\right)\bar{v}\right\rangle\right|$$

Permutation matrix

$$\leq d^2 \Big(\gamma\, |\langle \tilde{v}, W_G \tilde{v}\rangle| + 2\beta' \sqrt{\gamma(1-\gamma)}\, |\langle \tilde{v}, W_G \bar{v}\rangle|$$

$$+ \beta'^2 (1-\gamma) \underbrace{|\langle \bar{v}, W_G \bar{v}\rangle|}_{\leq \|\bar{v}\|\,\|\bar{v}\| \leq 1} \Big)$$

Think why!

$$\leq d^2 \left(\frac{a^\perp A_G a}{m} + 2\beta\sqrt{\gamma(1-\gamma)} + \beta^2(1-\gamma) \right)$$

$$\leq d^2 \Big(\underbrace{\gamma \cdot \alpha + 2\beta\sqrt{\gamma(1-\gamma)} + \beta^2(1-\gamma)} \Big)$$

$$\leq \alpha\gamma + \beta + \beta^2(1-\gamma)$$

$$\leq \max\{\alpha+\beta,\ \beta+\beta^2\}$$

$\blacksquare$

Suppose,

G_0 (n, d^2, α)-expander

H (d^4, d, β)-expander

"$\alpha \geq \beta + \alpha^2$"

Construct

$$G_1 := \underbrace{G_0^2}_{(n, d^4, \alpha^2)} ⓩ H, \ldots$$

$$G_2 := G_1^2 ⓩ H, \ldots$$

G_0 — G_1 — G_2 — ....

(n, d^2, α)-expander (nd^4, d^2, α)-expander (nd^8, d^2, α)-expander

Thus, a family of expander graphs.