Pseudorandomness : Lecture 11

Instructor: Ramprasad Saptharishi
2021-09-28

Recap:

- Spectral expanders $\quad (N, D, \lambda)$- expanders.
  - G - deg D, λ-spectral expanders
  - $\lambda(G) = \max\limits_{x \perp \pi} \dfrac{\|xM\|}{\|x\|}$ $\qquad M^T = M$.
  - Spectral gap: $1 - \lambda(G)$.
- Spectral expanders $\Rightarrow$ vertex expanders.
- Random walks:

  p - prob dist. $\qquad p = p^{\parallel} + p^{\perp}$ $\qquad$ along π $\quad \perp \pi$

  $$= \pi + p^{\perp}$$

  $$(\pi + p^{\perp}) M = \pi M + p^{\perp} M$$
  $$= \pi + (\text{error term})$$

  λ factor smaller than p

  $$\begin{bmatrix} -\pi- \\ \vdots \\ -\pi- \end{bmatrix}$$

  $$M = (1-\lambda) J + \lambda . E \quad , \text{ where } \|E\| \leq 1.$$

- $\{ G_{N_i} = (N_i, D, \lambda) \text{ exp.} \}_{i=1 \ldots \infty}$

  Mildly explicit: Generate adj matrix in poly(N) time.

  Super explicit: Get i^{th} neighbour of vertex u in poly$(\log N, \log D)$.

- Applications to error reduction with "few" random bits.

Are there explicit expander families?

▷ Margulis' construction:

$V = \mathbb{Z}_N \times \mathbb{Z}_N$. Spectral gap > const. > 0

Neighbours of (a,b):

$$\{(a\pm1, b), (a, b\pm1), (a, b\pm a), (-b, a), (b, -a), (a,b)\}.$$

▷ p-cycle with inverses. (Selberg graphs)

$V = \mathbb{Z}_p$.

Neighbours of $x = \{x+1, x-1, x^{-1}\}$. $0^{-1} = 0$

Thm: There is an $\varepsilon > 0$ s.t. this is a $(p, 3, 1-\varepsilon)$-expander for any prime p.

What is the best we can hope for?

What do random graphs give? $\lambda(G) \leq \frac{2\sqrt{D-1}}{D} + o_n(1)$

For any D-reg family, $\lambda(G) \geq \frac{2\sqrt{D-1}}{D} - o_n(1)$

LPS : $\lambda(G) \leq \frac{2\sqrt{D-1}}{D}$ "Ramanujan graphs"

Can we build good expanders by making a "bad" expander better?

Operations on graphs:

Say G is an (N, D)-graph.

$\Gamma(u, i)$ = the i^{th} neighbour of u.

$= v$ $\qquad\qquad$ $Rot_G(u,i) = (v, j)$

$\Gamma(v, j) = u$

▷ Suppose G is an (N, D, λ)-expander.

G^2: $V = [N]$

For every length 2 path $u \sim v \sim w$ in G, add a edge between u & w in G^2.

$Rot_G(u,i) = (v,j)$
Then $\Gamma_{G^2}(u, (i,j)) = u$

Degree? D^2.

$$\Gamma_{G^2}(u, (i,j)) = \Gamma_G(\Gamma_G(u,i), j)$$

What is the random walk matrix? $\qquad M_G^2$

And what is $\lambda(G^2)$?

$$\lambda(G^2) = \max_{x \perp \pi} \frac{\|xMM\|}{\|x\|} = \lambda \cdot \max_{x \perp \pi} \frac{\|xM\|}{\|x\|} = \lambda^2.$$

"Graph powering" $\qquad\qquad G^{10}$

Pro: Brings down λ.

Con: Doesn't increase N.

Increases D.

▷ $G_1 = (N_1, D_1, \lambda_1)$ expander

$G_2 = (N_2, D_2, \lambda_2)$ expander.

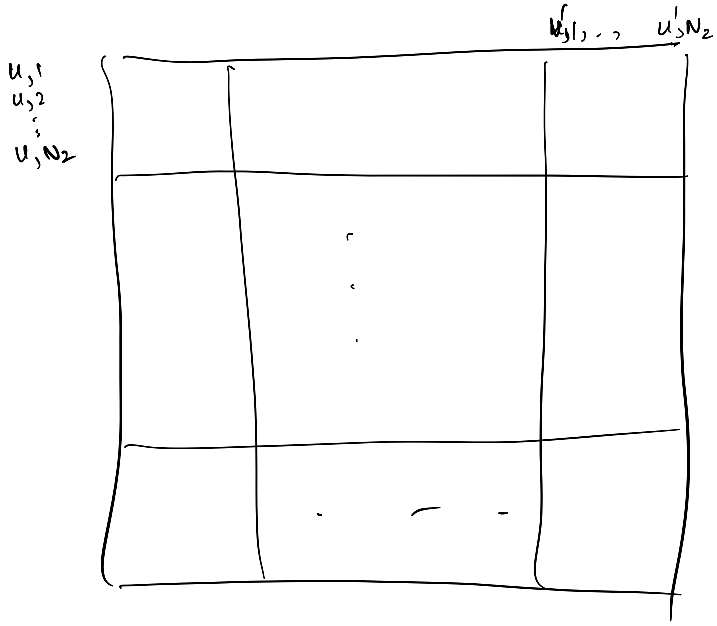
$G_1 \otimes G_2$: Graph on $[N_1] \times [N_2]$

(u_1, v_1) conn to (u_2, v_2) if

$(u_1\ u_2) \in G_1$ & $(v_1\ v_2) \in G_2$.

What is the degree? $D_1 D_2$ $\quad \{(i,j) : i \in [D_1],\ j \in [D_2]\}$

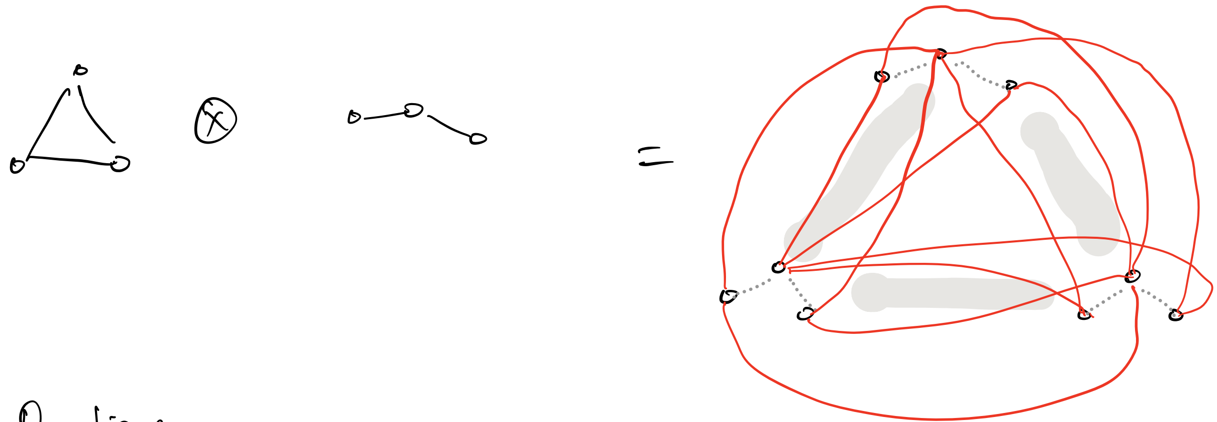
What about eigenvalues? What is the adjacency matrix?



$A_G \otimes A_H$

replace every entry $(A_G)_{ij}$ by $(A_G)_{ij} \cdot A_H$

"Tensoring" = "Take steps in parallel"!



Question:

$(u \otimes v)\, A_1 \otimes A_2 = uA_1 \otimes vA_2 \longrightarrow$ Check this!

$= \alpha\beta\, u \otimes v$

If u is an eigenvector of A_1 with e.val α

v " " " " A_2 " " β,

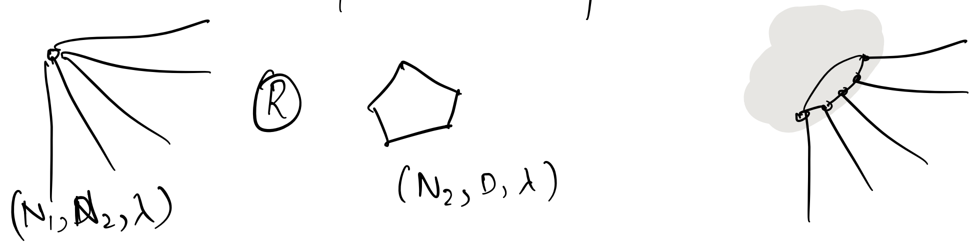
$u \otimes v$ " " " " $A_1 \otimes A_2$ " " $\alpha\beta$

$G_1 \otimes G_2$:

# vertices	$N_1 N_2$	:)
λ	$\max(\lambda(G_1), \lambda(G_2))$	:|
Deg	$D_1 D_2$	:(

How do we reduce degree without losing too much in λ?

Candidate : Replacement product.



$G_1 \circledR G_2$ — $N_1 N_2$ vertices.

Degree $D_2 + 1$. B-)

λ ?? Slightly painful to analyse.

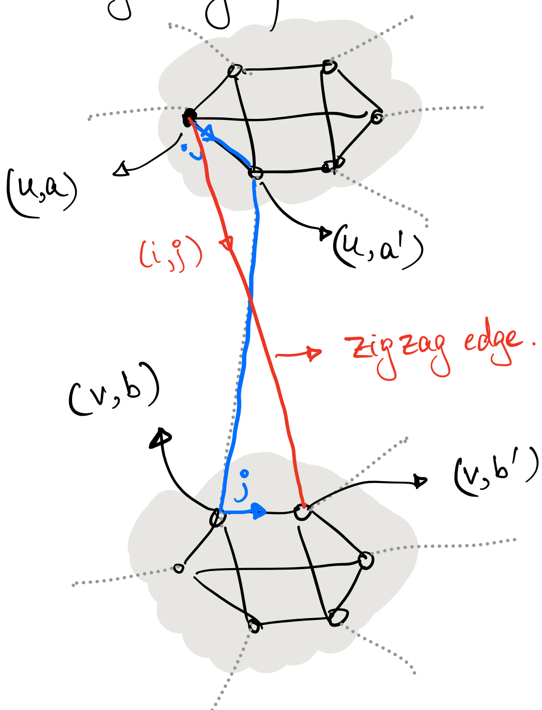
Too tied to the cloud...

Can we come up with a graph product $G_1 ⓩ G_2$ that has a better balance between inter-cloud & intra-cloud mixing?

Zig-zag product: (N, D, λ_1) (D, d, λ_2)

$G_1 ⓩ G_2$.

- Graph on ND vertices
- Deg d^2.



$\Gamma_{G ⓩ H}((u,a), (i,j))$:

$\Gamma_H(a, i) = a'$

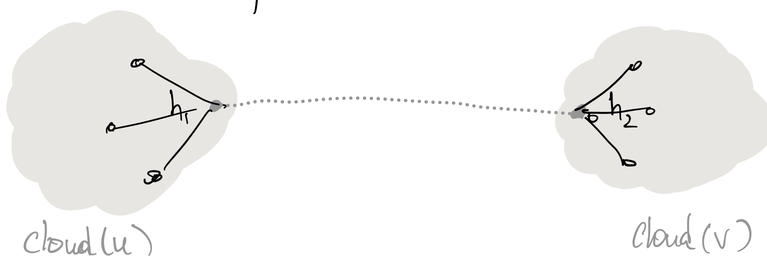
$Rot_G(u, a') = (v, b)$

$\Gamma_H(b, j) = b'$

$\therefore \Gamma_{G ⓩ H}((u,a),(i,j)) = (v, b')$

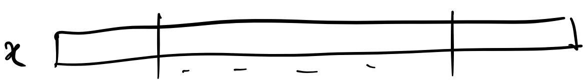
Qn: If H is the complete graph on D vertices with self-loops, what is $G \textcircled{z} H$? $G \otimes H$

Alternate view point:

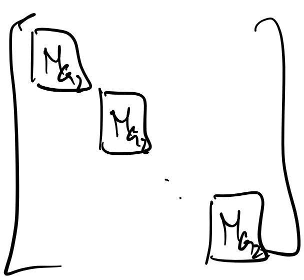


Put a complete bipartite graph between $\Gamma_H(h_1)$ & $\Gamma_H(h_2)$.

Analysing the eigenvalue bound for zig-zag: $G \textcircled{z} H$.



$x \perp \pi \Rightarrow \sum x_{u,a} = 0$



Step 1: Walk within the cloud.
$I \otimes M_H$

Step 2: Take the intercloud edge.
Rot_G.

Step 3: $I \otimes M_H$

$$M = (I \otimes H) \cdot Rot_G \cdot (I \otimes H)$$

$$H = (1-\lambda_2) \cdot J + \lambda_2 \cdot E$$

$$= \underbrace{I \otimes J \cdot Rot_G \cdot I \otimes J}_{\text{zigzag of } G \text{ with the complete graph (with) self loops}} \cdot (1-\lambda_2)^2.$$

$$+ (1-\lambda_2)\cdot\lambda_2\cdot\left(I\otimes J\cdot \mathrm{Rot}_G\cdot I\otimes E\right)$$
$$+ (1-\lambda_2)\cdot\lambda_2\left(I\otimes E\cdot \mathrm{Rot}_G\cdot I\otimes J\right)$$
$$+ \lambda_2^2\cdot (I\otimes E)\cdot \mathrm{Rot}_G\cdot (I\otimes E)$$

spectral norm ≤ 1

$$= G\otimes K_D^*\cdot(1-\lambda_2)^2 + (1-\lambda_2)\lambda_2\cdot E_1 + (1-\lambda_2)\lambda_2\cdot E_2 + \lambda_2^2\cdot E_3$$

spectral norm 1.

$$\therefore \underset{\|x\|=1}{x\perp\pi} \Rightarrow \|xM\| \leq \lambda_1\cdot(1-\lambda_2)^2 + 2\lambda_2(1-\lambda_2)+\lambda_2^2 = 1-(1-\lambda_1)(1-\lambda_2)^2.$$

Thm: [Reingold-Vadhan-Wigderson] G: (N, D, λ_1)-exp and H: (D, d, λ_2)-exp, then $G ⓩ H$ is an (ND, d^2, λ) expander where $1-\lambda = \gamma_1\gamma_2^2$

Constructing an expander family:

H - $(D^4, D, 1/8)$-expander. $\quad G_1 = H^2$

$$G_t = G_{t-1}^2 ⓩ H.$$

Claim: G_t is a $(D^{4t}, D^2, 1/2)$-expander for all $t\geq 1$.

How long does it take to compute $\Gamma_{G_t}(u, i)$?

$$\mathrm{Time}(t) = 2\,\mathrm{Time}(t-1) + O(1)$$
$$= 2^{O(t)} \quad \ldots \text{ damn it! too slow.}$$

Attempt 2: $H = (D^8, D, 1/8)$ base graph.

$$G_1 = H^2$$

$$G_2 = \left[G_{\frac{t}{2}} \otimes G_{\frac{t}{2}}\right]^2 ⓩ H$$

Claim: G_t is a $(D^{8t}, D^2, 1/2)$-expander.

How much time for $\Gamma_{G_t}(u, i)$?

$$\text{Time}(t) = 4\,\text{Time}(t/2) + O(1)$$
$$= \text{poly}(t).$$

Woohoo!

This is a strongly explicit family

... t needs to be a power of 2 ... too sparse a family.

Fix:

$$G_1 = H^2$$
$$G_t = \left(G_{\lceil \frac{t}{2} \rceil} \otimes G_{\lfloor \frac{t}{2} \rfloor}\right)^2 ⓩ H.$$

Same guarantee.

Further, for every M, there is a graph in the above family with # vertices M' with

$$M \le M' \le M \cdot |H|.$$

.. and now we are done.