

# EXPANDERS AND THEIR APPLICATIONS

## References

- Expander Graphs and their Applications by Hoory, Linial and Wigderson
  - Video: An introductory survey on expanders and their applications by Avi Wigderson
  - Pseudorandomness Chapter 4 by Salil Vadhan.
- 

Expander Graphs are very useful objects for both math & CS communities. Some applications in CS:

- Desandomization
- Circuit complexity
- Error correcting codes (Chalk & Talk)
- • Cryptography
- Communication and sorting networks
- Approximate counting
- etc.

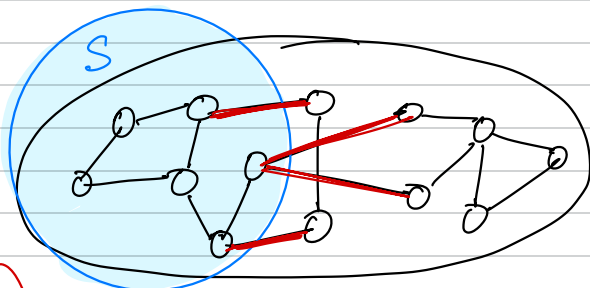
Expander graphs are "sparse" graphs that "behave like" random graphs.

They satisfy following (equivalent) properties:

- ① Combinatorial: no small cuts, high connectivity  
(you cannot separate a set without severing many edges)

② Probabilistic: rapid convergence of random walk

③ Algebraic: small second eigenvalue ( $\lambda_2$ ) of normalized adjacency matrix.



$G = (V, E)$   
 $|V| = n \ ( \rightarrow \infty )$   
 $(d\text{-regular graphs})$   
 $d$ -fixed.

(\* called edge expansion)

← Combinatorial view (high-connectivity)

$$\forall S, |S| < n/2, |E(S, S^c)| > c \cdot |S| \cdot d$$

# edges between  $S$  and  $S^c$

some constant  $c$

Q: What would  $|E(S, S^c)|$  be for random graph?  
 (see that this matches what we expect from an expander)

Probabilistic View (rapid convergence of random walk)

$u_0 \sim p_0$  (any distribution)

$u_0 \rightarrow u_1 \rightarrow u_2 \rightarrow \dots \rightarrow u_t$  ( $t$ -random walk)

$p_t$  converges to  $\pi$  (uniform distribution) in  $O(\log n)$  steps (as fast as possible).

(\* called spectral expansion)

← Algebraic View (small second eigenvalue of  $K$ )

Recall, normalized adjacency matrix  $K$

For  $d$ -regular graphs (recall):

$$K = \frac{1}{d} \cdot A_G, \text{ where } A_G \text{ is adjacency matrix of } G$$

$$A_G(u, v) = \begin{cases} 1 & \text{if } (u, v) \in E \\ 0 & \text{if } (u, v) \notin E. \end{cases}$$

Eigenvalues of  $K$  are (recall)

$$1 = k_0 \geq k_1 \geq \dots \geq k_{n-1} \geq -1$$

$$K(G) = \max_{i \geq 1} |k_i|$$

Recall, for convergence of random walk, we want  $K(G) \leq 1 - \epsilon$  (for  $0 < \epsilon < 1$ )  $\rightarrow$  we saw this.

$\hookrightarrow K(G)$  is called "spectral gap".

$G$  is  $(n, d, \epsilon)$ -graph:  $K(G) \leq \epsilon$ .  $G$  expander if  $\epsilon < 1$ .

Defn: An infinite family  $\{G_i\}$  of  $(n_i, d, \epsilon)$ -graphs is an expander family if  $\forall \epsilon, \epsilon < 1$ .

(spectral expansion)  $\leftrightarrow$  Algebraic Expansion  $\Rightarrow$  Fast Mixing

why?  
(think)

$$\rightarrow K(G) = \max \{ \|SK\|_2 : \|S\|_2 = 1, S \perp \pi \} \rightarrow \textcircled{1}$$

$S$  orthogonal to  $\pi = (\frac{1}{n} \ \frac{1}{n} \ \dots \ \frac{1}{n})$

Theorem (Algebraic Expansion  $\Rightarrow$  Fast Mixing):

For any starting distribution  $S$ , after  $t$  random walk

$$\|SK^t - \pi\|_2 \leq K(G)^t$$

Proof:

$$\|\delta K^t - \pi\|_2 = \|(\delta - \pi) \cdot K^t\|$$

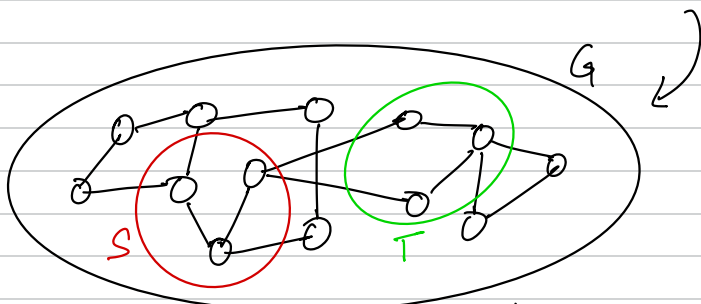
Exercise: show that  $(\delta - \pi) \perp \pi$ .

Then, by repeated use of ① we get

$$\|\delta K^t - \pi\|_2 \leq K(G)^t$$

( $\Rightarrow$  convergence in  $O(\log n)$  steps  $\because$   
 $K(G) \leq \delta$  for  $\delta < 1$  *good enough closeness!*)

Algebraic Expansion  $\Rightarrow$  Combinatorial Expansion  
 (or spectral expansion) (or Edge expansion)



Edge expansion  $\because$  The number of edges between any two large sets  $S$  &  $T$  is what you expect in a random  $d$ -regular graph.

Expander Mixing Lemma: Let  $G$  be a  $d$ -regular graph with spectral gap  $1 - K(G)$ . Then  $\forall$  sets  $S$  &  $T$  of densities  $\alpha = |S|/n$  &  $\beta = |T|/n$ , we have:

$$\left| \frac{E(S, T)}{n \cdot d} - \alpha \beta \right| \leq K(G) \sqrt{\alpha(1-\alpha) \beta(1-\beta)}$$

∴ If you take  $T = S^c \Rightarrow \beta_2 = 1 - \alpha$  then above lemma gives

$$\left| \frac{E(S, S^c)}{n \cdot d} - \alpha(1 - \alpha) \right| \leq K(G) \alpha(1 - \alpha)$$

$$\Rightarrow \frac{E(S, S^c)}{n \cdot d} \geq (1 - K(G)) \cdot \alpha(1 - \alpha) \geq (1 - K(G)) \cdot \frac{\alpha}{2}$$

for  $\alpha = \frac{|S|}{n} < \frac{1}{2}$

(prove this)

$\Rightarrow$  For all  $S$  with  $|S| < \frac{n}{2}$ ,

$$E(S, S^c) \geq \frac{(1 - K(G))}{2} |S| \cdot d.$$

Solution

[Recall that assignment 5, Q5B) asked you to prove this lemma.]

Proof (Sketch):

$\mathbb{1}_S$  &  $\mathbb{1}_T$  be indicators for  $S$  &  $T$ . Then

$$E(S, T) = \mathbb{1}_S^T \cdot A_G \cdot \mathbb{1}_T = \mathbb{1}_S^T \cdot (d \cdot K) \cdot \mathbb{1}_T$$

$$\text{We know } \mathbb{1}_S = \sum_{i=0}^{n-1} \hat{\mathbb{1}}_S(i) \cdot \phi_i \text{ \& } \mathbb{1}_T = \sum_{i=0}^{n-1} \hat{\mathbb{1}}_T(i) \cdot \phi_i$$

(where  $\phi_0, \phi_1, \dots, \phi_{n-1}$  are eigenvectors of  $K$ )

$$\begin{aligned} \frac{E(S, T)}{dn} &= \frac{\mathbb{1}_S^T \cdot K \cdot \mathbb{1}_T}{n} = \frac{1}{n} \sum_{i=0}^{n-1} K_i \hat{\mathbb{1}}_S(i) \cdot \hat{\mathbb{1}}_T(i) \\ &= \alpha \beta_2 + \frac{1}{n} \sum_{i=0}^{n-1} K_i \hat{\mathbb{1}}_S(i) \hat{\mathbb{1}}_T(i) \end{aligned}$$

prove this corresponds to the  $i=0$  term

$$\Rightarrow \left| \frac{E(S, T)}{dn} - \alpha \beta_2 \right| = \left| \frac{1}{n} \sum_{i=0}^{n-1} K_i \hat{\mathbb{1}}_S(i) \hat{\mathbb{1}}_T(i) \right|$$

Now, use Cauchy-Schwartz & complete the proof. (main part is done above).

## EXISTENCE OF EXPANDERS

Theorem [Pinsker '73, Kolmogorov-Barzdin '67]

Most 3-regular graphs are expanders.

[Try to prove this: (probabilistic method)  $\rightarrow$  pick a random 3-regular graph  $G$  and show that  $\Pr[G \text{ is not (edge) expanding}] < 1/2$ ]

Challenge  $\Rightarrow$  finding "Explicit expanders" of small degree.

What does explicit mean?

- Weakly explicit:  $\{G_E = (V_E, E_E)\}$  weakly explicit means the adjacency matrix  $A_{G_E}$  can be constructed in  $\text{poly}(|V_E|)$ -time.
- Strongly explicit:  $A_{G_E}$  can be constructed in  $\text{polylog}(|V_E|)$  time: i.e. given  $i, u \in V_E$ , in  $\text{polylog}(|V_E|)$ -time you can list all  $v \in V_E$  s.t.  $(u, v) \in E_E$ .

Example of a strongly explicit expander family

For prime  $p$ , take  $V = \mathbb{Z}_p$ .

- $\forall x \in \mathbb{Z}_p, (x, (x+1) \bmod p) \in E$
- $\forall x \in \mathbb{Z}_p, x \neq 0, (x, x^{-1}) \in E$
- $(0, 0) \in E$

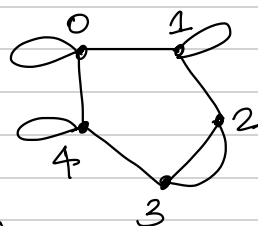
3-regular graph  $G_p$

[Lubotzky-Phillips-Sarnak '86]

For every prime  $p$ ,  $G_p$  is a strongly explicit 3-regular expander ( $K(G_p) < 0.99$ )

No simple direct proof known  
(proof uses stronger [Selberg '65],  
[Bourgain-Gamburd '05])

Example:  $p=5$



But 0.99 is large, so a natural question:

How small can  $K(G)$  be?

Amplification:  $G$  is  $(n, d, \epsilon)$ -graph ( $\epsilon < 1$ )  
then  $G^k$  is  $(n, d^k, \epsilon^k)$ -graph.

(take  $k$ -th  
power of  
Adjacency matrix)

↓  
Exercise: show this  
(this is specific for  
 $d$ -regular graphs)

∴ can shrink  $K(G)$  at the cost of increasing degree.

Theorem (lower bound on  $K(G)$ ) [Alon-Boppana]:

An infinite family  $\{G_p\}$  of  $(n_p, d)$ -graphs must have  $K(G) \geq (2\sqrt{d-1})/d \approx 1/\sqrt{d}$ .

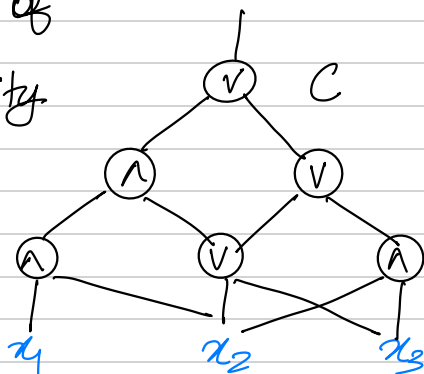
↑  
this is a tight bound [LPS '85]  
graphs meeting this bound  
called Ramanujan graphs!

# EXAMPLE APPLICATION: FAULT-TOLERANT COMPUTATION [von Neumann]

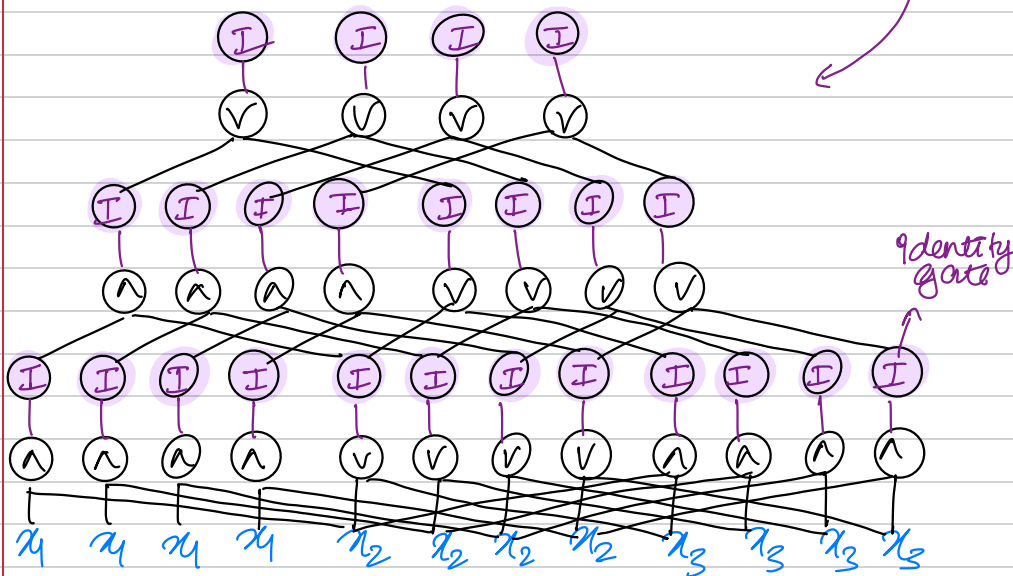
(Can you build reliable circuits from unreliable components?)

Given: a circuit  $C$  for  $f$  of size  $s$  such that every gate fails with probability  $p < \frac{1}{10}$ .

Can you construct  $C'$  for  $C'(x) = f(x)$  w.h.p. & with small size  $S$ ?



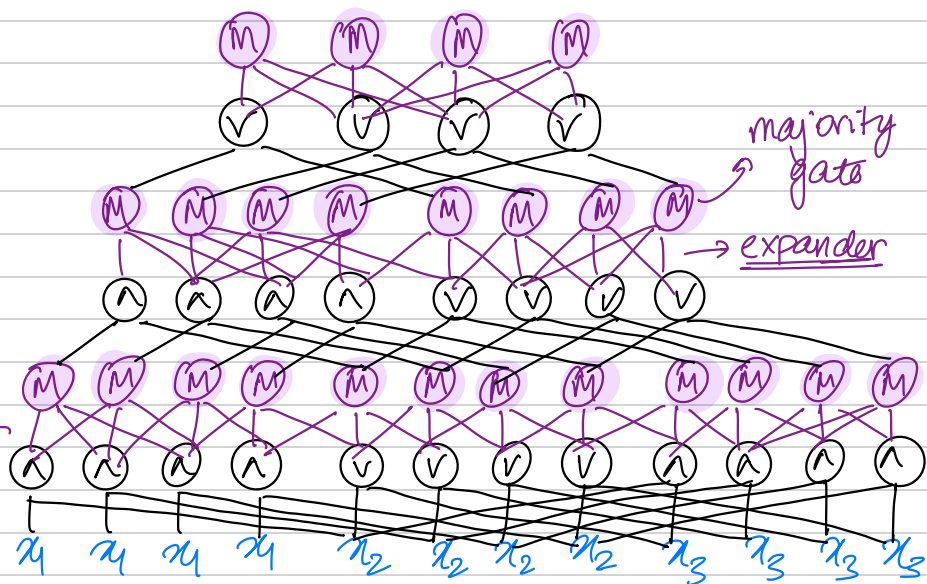
Initial idea: just replicate gates!



Take  $k \approx \log s$  copies of each gate. Hope is that this block of  $k$  copies will try to "propagate" correct values of computation.

$\therefore$  We do not want errors to increase and accumulate across levels!

Use expanders! [von Neumann Dobrushin-Ortyukov, Pippenger]



Idea: Majority gates connected using expanders of size  $O(\log s)$

Why does this help?

(Intuitive Discussion)

Expander Mixing Lemma (stated differently):  
If  $S, T \subseteq V$ ,

$$|\Pr_{u,v} [u \in S, v \in T] - \text{rel}(S) \text{rel}(T)| < \epsilon$$

(Take  $G$  to be  $(n, d, s)$ -graph)

## Corollary of Expander mixing

(I) Every set  $S$  of size  $|S| < \frac{8n}{2}$  contains at most  $\frac{8n}{2}$  vertices with  $> 2\delta d$  neighbors in  $S$ .

$\Rightarrow$  (II) Infection process: Say at every step some adversary picks  $I_0, I_1, \dots, I_t$  such that  $\text{val}(I_k) \leq \delta/4$ . ("infected" vertex sets at each stage)

Let  $I_0 = S_0, S_1, S_2, \dots, S_t$  be defined as:  
 $\forall i > 0, v \in S_{i+1}$  iff majority of its neighbors in  $S_i$ .

Let  $I_0 = R_0, R_1, R_2, \dots, R_t$  be defined as  
 $R_i = S_i \cup I_i \quad \forall i$

Then (I)  $\Rightarrow$  •  $S_t = \emptyset$  for  $t > \log n$   
•  $\text{val}(R_t) \leq \delta/2 \quad \forall t$

## Coming back to the modified circuit $C'$

What (II) says that fraction of values in every block that is not the correct value of the computation is some small constant fraction! (so you can go across every layer without blowing up the errors too much.

& the blow-up in size only by  $O(\log s)$

There are many more applications  $\rightarrow$  error-correction we will see in Chalk and talk.  
If interested  $\rightarrow$  see Avi's talk (reference on Pg 1) for many more applications.