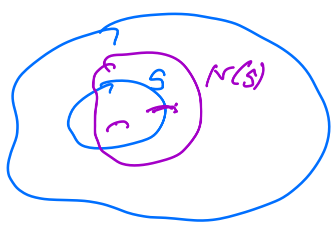
Today
- Vertex Expansion
  - Random graphs
  - KPS Generator
- Spectral Expansion

CSS.413.1
Pseudorandomness
Lecture 07 (2021-9-14)
Instructor: Prahladh Harsha.

Recall from last time

Vertex Expansion: $G=(V,E)$ on N vertices (D-regular) is called a (K,A)-vertex expander for some $1 \le K \le N$, $A > 1$ if $\forall S \subseteq V$, $|S| < K \Rightarrow |N(S)| > A|S|$.



$N(S) = \{v \in V \mid \exists u \in S, \{u,v\} \in E\}$.

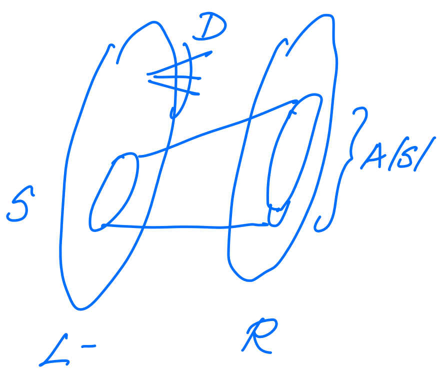
Q1: Do such graphs exist?

Random graph (picked uniformly from the set of D-regular graph of N vertices) is "expanding"

<u>Thm</u>: $\forall D \ge 3$, $\exists \alpha$ $\forall N$, a random D-regular graph on N vertices is

$(\alpha N, D-1.01)$ - vertex expander, with high probability.

Prove a (weaker) bipartite version of above theorem.



$|L| = |R| = N$

$G = (L, R, E)$ is a (K, A) - left expander if

$\forall S \subseteq L$

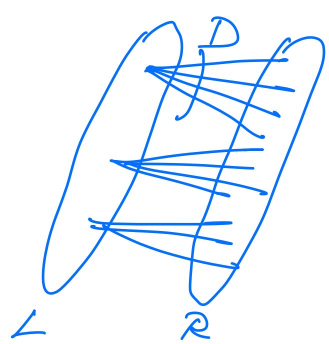
$|S| < K \Rightarrow |N(S)| > A|S|$

Theorem: $\forall D, \exists \alpha, \forall N$ a graph sampled from $Bip(N,D)$ is an $(\alpha N, D-2)$ - left expander with probability at least $1/2$.

$\underline{Bip(N,D)}$:

$|L| = |R| = N$.

(D-left regular).



For each $v \in L$ pick D vertices in R uniformly at random (w/ repetition) & assign them as nbrs of D

Pf: Let $K \leq \alpha N$

$$P_k = \Pr_{G \leftarrow Bp(N,D)} \left[\exists S \subseteq L,\ |S| = k,\ |N(S)| < (D-2)k \right]$$

$$P_k(S) = \Pr_{G \leftarrow Bp(N,D)} \left[|N(S)| < (D-2)k \right]$$

where $S \in \binom{L}{k}$

$$P_k \leq \sum_{S \in \binom{L}{k}} P_k(S)$$

Event: $|N(S)| < (D-2)k$

Nbrs of S
$= v_1, \ldots \quad v_{kD}$
(picked uniformly at random from R).

$$\Pr[i^{th} \text{ vertex is a repeat}] \leq \frac{i-1}{N}$$

$$\leq \frac{kD}{N}$$

$P_k(S)$

$$\Pr[|N(S)| < (D-2)k] = \Pr[\text{There are at least } 2k \text{ repeats}]$$

$$\leq \binom{kD}{2k} \left(\frac{kD}{N}\right)^{2k}$$

$$P_k \leq \sum_{S \in \binom{L}{k}} P_k(S) = \binom{N}{k} \binom{kD}{2k} \left(\frac{kD}{N}\right)^{2k}$$

$$\leq \left(\frac{Ne}{k}\right)^{k} \left(\frac{\cancel{k}De}{2\cancel{k}}\right)^{2k} \left(\frac{kD}{N}\right)^{2k} \quad \left(\binom{n}{r} \leq \left(\frac{ne}{r}\right)^{r} \right)$$

$$= \left(\frac{Ne^3k^2D^4}{4k\ \ N^2}\right)^{k}$$

$$= \left(\frac{e^3kD^4}{4N}\right)^{k} \qquad k \leq \alpha N$$

$$= \left(\frac{e^3\alpha D^4}{4}\right)^{k} \qquad \left(\text{Set } \alpha = \frac{1}{e^3D^4}\right.$$

$$\leq \left(\frac{1}{4}\right)^{k}$$

$\Pr_G$ [G is not a $(\alpha N, D-2)$-left expander]

$$\leq P_1 + P_2 + \dots + P_{\alpha N}$$

$$\leq \left(\frac{1}{4}\right)^{1} + \left(\frac{1}{4}\right)^{2} + \dots \left(\frac{1}{4}\right)^{\alpha N}$$

$$< \frac{1}{2}.$$

G is a $(\alpha N, D-2)$-left expander w/ prob $\geq 1/2$. $\boxtimes$

Can we construct such graphs explicitly?

Explicit Construction: Fix D, construct a family of

$(\alpha N, A)$ expanders $\{G_N\}_{N=1}^{\infty}$

where $|V(G_N)| = N$.

Explicit Construction: Given N, outputs G_N in time $poly(N)$

Super-explicit Construction: Given N, and $v \in [N]$ & $i \in [D]$, output the i-th neighbour of v in G_N in $poly(\log N, \log D)$

Q2: Are expanders useful?

Application: Reducing Randomness (if super-explicit construction of expanders exist).

RP: $L \in RP$

if $\exists$ a rand polytime alg A s.t

$$x \in L \Rightarrow \Pr_r [A(x,r) = acc] \geq 1/2$$

$$x \notin L \Rightarrow \Pr_r [A(x,r) = acc] = 0.$$

Error Reduction:

k independent repetitions

Reduce error from $\frac{1}{2}$ to 2^{-k}

by choosing k and x_i's

random coins $= k \cdot m$

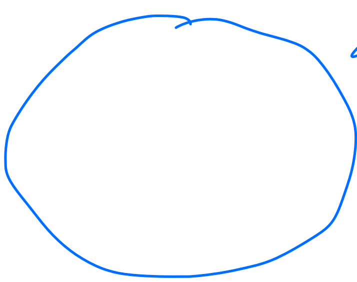
repetitions $= k$.

Reduce error from $\frac{1}{2}$ to δ

random coins $= m \cdot \log\left(\frac{1}{\delta}\right)$

repetitions $= \log\left(\frac{1}{\delta}\right)$.

$\rightarrow$ Use expanders to reduce # random coins.



$\{0,1\}^m = N$

- space of random coins

Suppose we have a $\left(\frac{N}{2}, A\right)$-expander which is D-regular for some constant $D \geq 3$ & $A > 1$

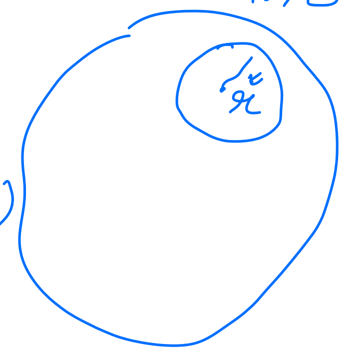
(super explicit construction)

$A^{(t)}$: On input $x \in \{0,1\}^n$

(Run A on $Ball(r,t)$ for a random r)

- Pick $r \in_U \{0,1\}^m$
- "Let G_N $(N = 2^m)$" super-explicitly construction
- Think r - vertex in G_N

r-vertex in G



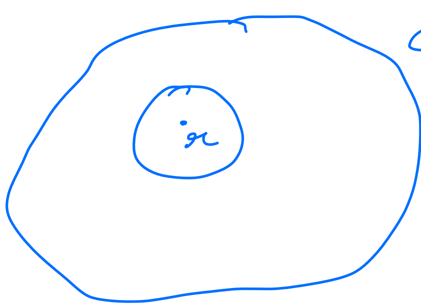
polytime because of super-explicit construction

- [Let $r_1 \ldots r_k$ be the set of all vertices within distance t of r]

ie, $\{r_1 \ldots r_k\} = Ball(r,t)$
$= \{r' \in V(G_N) \mid d(r,r') \le t\}$

- Run A on $(x,r_1) \ldots (x,r_k)$ & accept if any one acc & rej otherwise.

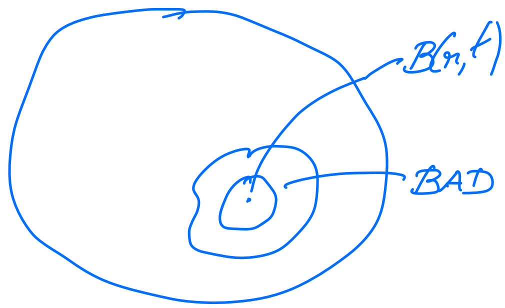
$G = \{0,1\}^m$



\# random coins $= m$

\# repetitions $= D^t$
($t = O(\log n)$ if $A^{(t)}$-runs in poly time)

$\Pr[A^{(t)} \text{ errs}]$??



Fix $x \in L$.

$$BAD_x = \{r \in \{0,1\}^m \,/\, A(x,r) = rej\}$$

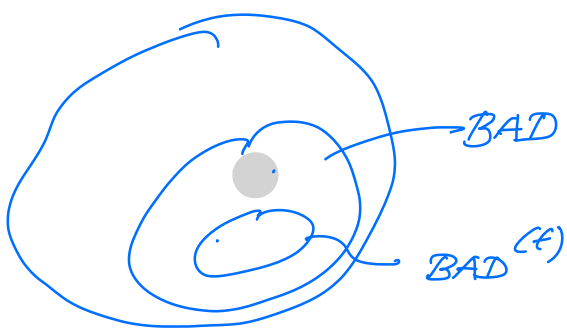
$$\frac{|BAD_x|}{2^m} < \frac{1}{2}.$$

error $\Pr_r[A^{(t)}(x,r) \neq acc] = \Pr_r[B(r,t) \subseteq BAD_x]$

$$BAD_x^{(t)} = \{r \,/\, B(r,t) \subseteq BAD_x\}$$

$$\text{error} = \frac{|BAD_x^{(t)}|}{2^m}$$

Fix x



$Ball(BAD_x^{(t)}, t) \subseteq BAD_x$

$$|BAD_x| \geq |Ball(BAD_x^{(t)}, t)| \geq A^t \cdot |BAD_x^{(t)}|$$

$$|BAD_x^{(t)}| \leq \frac{|BAD|}{A^t}$$

$$\text{error} = \frac{|BAD_x^{(t)}|}{2^m} \leq \frac{|BAD|}{2^m A^t} \leq \frac{1}{2 \cdot A^t} \leq 1/A^t$$

Error has dropped from $1/2$ to $\frac{1}{A^t} = \delta$

(Setting $t = \frac{\log(1/\delta)}{\log A}$)

[Karp Pippenger Sipser]

Thm: $G = (V, E)$ - D-regular graph on N vertices & $(\frac{N}{2}, A)$-expander for some $A > 1$, then $\forall B \subseteq V$, $|B| < N/2$,

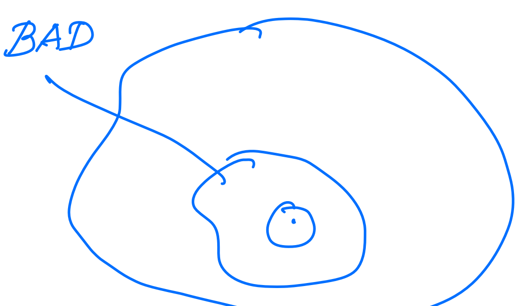
$$\Pr_x [B(x,t) \subseteq B] \leq \frac{1}{A^t}.$$

Error reduction $(1/2 \to \delta)$.

$\#$ random coins $= m$

$\#$ repetitions $= D^t = \text{poly}(\frac{1}{\delta})$

(since D, A are constants, $\delta = \frac{1}{A^t}$)



$G = (V, E)$

(K, A)-expander

Next time: Spectral Expansion