We had: $\{I_i\}$ design with (ℓ, n, d), $m = 2^{d/10}$, f 2^{2d} avg-hard

then $G(U_\ell)$ $(2^{2d}/10, 1/10)$-pseudorandom.

Let us give values. ℓ, $S = h_{avg}(f)$ given.

pick n largest st $\ell > \frac{100 n^2}{\log S(n)}$. $\Rightarrow n \geq \sqrt{\ell \log S(n)/200}$

$d = \log S(n)/10$.

output first $S(n)^{1/40}$ bits of NW generator.

obs map ℓ bits into $S(n)^{1/40}$, so $S'(\ell) = S(n)^{1/40} = S(\sqrt{\ })^{1/40}$.

//

Pseudorandom Objects.

Expander graphs: graphs with excellent connectivity.
Almost as good as K_{nn}, but small degree.
Two ways of measuring: algebraic / combinatorial.
We'll work with d-regular graphs, undirected.

Combinatorial Expansion.

G well-connected if every set of vertices hard to disconnect,
i.e. many edges go from S to $\bar{S} = V \setminus S$.
If deg $G = d$, best can hope for is $|E(S, \bar{S})| = d \cdot |S|$.
Edge expansion measures how far we are:

$$h_S = \frac{|E(S,\bar{S})|}{d \cdot |S|} \qquad h_G = \min_{\substack{S \subseteq V \\ |S| \leq n/2}} h_S.$$

Can also measure vertex expansion: $\frac{|N(S)|}{d \cdot |S|}$.

Algebraic Expansion.

G well-connected if a random walk converges quickly
to uniform. Represent with linear algebra:
If start at v, then in one step we are in each
neighbour of v w. pr. $1/d$.
Obs equiv to $\left(\frac{1}{d} A\right) \cdot \mathbb{1}_v$ — 1 in row of v, 0 elsewhere; adj. matrix.

A distribution over vertices is simply a vector of probabilities.
One step of random walk is then mult. by (A/d).
From now on redefine $A = A/d$.

Play w. eigenvalues of A.

$A \cdot \mathbb{1} = \mathbb{1} \Rightarrow \mathbb{1}$ eigenv. of eigenvalue 1.
(and this is largest: $\lambda_1 = \max_x \frac{x^T A x}{x^T x}$.

What about 2nd? → (in absolute value)
If G disconnected, then 1_S is also evec w eval 1
If G bipartite, then $A 1_S = c 1_{\bar{S}} \rightsquigarrow c_1 1_S + c_2 1_{\bar{S}}$
evec w. eval -1.
Other dir. also true: if $\lambda = |\lambda_2| = 1$ then G bipartite or
disconnected.

In fact spectral expansion $= 1 - \lambda$ measures how connected
graph is.
Can also compute λ as $\max_{x \perp \mathbb{1}} \frac{x^T A x}{x^T x}$. (Rayleigh).

prop $\|v\|_1 = 1 \Rightarrow \| A^k v - \mathbb{1}/n \| \leq \lambda^k$

proof: write $v = \alpha \cdot \mathbb{1} + w$, $w \perp \mathbb{1}$.

obs $1 = \|v\|_1 = \langle v, \mathbb{1} \rangle = \alpha \langle \mathbb{1}, \mathbb{1} \rangle + \langle w, \mathbb{1} \rangle = \alpha \cdot n$

obs $Av = \alpha \mathbb{1} + Aw \Rightarrow A^k v = \alpha \mathbb{1} + A^k w$

$\Rightarrow \|A^k_v - \mathbb{1}/n\| = \|A^k w\| \leq \lambda^k w$
↑ Rayleigh.

cf $A = J$, where $J_{ij} = 1/n$, matrix of $K_{n,n}$. then $Jv = \mathbb{1}/n$. $\forall v$.
lemma $A = (1-\lambda) J + \lambda C$, $\|C\| \leq 1$
proof: $C = \frac{1}{\lambda} \cdot (A - (1-\lambda) \cdot J)$.

th. Spectral & combinatorial expansion equivalent.
th (formal) 1. $h(G) \geq \frac{1-\lambda}{2}$
2. $\lambda(G) \leq 1 - \min\left(\frac{2}{d}, \frac{h^2}{2}\right)$

* 2 is assuming G has (all) self-loops,
i.e. A is $A + I$.

prop If G random graph $\Rightarrow h(G) = \varepsilon d$.
th Explicit graphs with $\lambda \leq 1 - \varepsilon$ exist.
↳ $\exists$ algo st given v, outputs $N(v)$ in poly time.

Error Reduction with little randomness.

Recall can reduce BPP error by repeating algo k times
(and using $m \cdot k$ coins).
th: $m + O(k)$ coins enough.

proof: Let G graph on 2^m vertices, deg. d, $\lambda < 9/10$

Let $v_1 \dots v_k$ seq. obtained by picking v_1 at random,
and v_i a neighbour of v_{i-1}. at random.

Run algo k times with random string v_i.
Output majority answer.

We'll show RP case ($x \in L \Rightarrow M = 1$ w. pr $\geq 2/3$
$x \notin L \Rightarrow \qquad = 0$).

claim. G (n, d, λ)-expander. $U \subseteq V$, $\beta = |U|/|V|$.
then $\Pr[\{v_1 \dots v_k\} \subseteq U] \leq ((1-\lambda) \cdot \sqrt{\beta} + \lambda)^{k-1}$.

obs th follows: we have $\lambda < 9/10$, $\beta = 1/3$.
(U is set of bad coins).

proof of claim.
let $B_i =$ "$v_i \in U$". let $p_i = \Pr[\bigcap^i B_j]$.
let $D_i =$ distr. of v_i conditioned on $B_1 \dots B_i$
let $B = \mathrm{diag}(\mathbb{1}_U)$.
can write $D_1 = \frac{1}{p_1} \cdot B \mathbb{1}/n$, $D_2 = \frac{1}{p_2} \cdot B \cdot A \cdot B \mathbb{1}/n$, etc.

$\|D_k\|_1 = 1 \Rightarrow p_k = \|(BA)^{k-1} B \mathbb{1}/n\|_1 \leq \sqrt{n} \cdot \| \sim \|_2$.

claim. $\| \sim \|_2 \leq ((1-\lambda) \cdot \sqrt{\beta} + \lambda)^{k-1} / \sqrt{n}$.

proof: write $A = (1-\lambda) J + \lambda C$.

$\|BA\| \leq (1-\lambda) \|BJ\| + \lambda \|BC\|$

$\|BJ\| = \max_{\|v\|=1} \|BJv\|$. $Jv = \mathbb{1}/n \Rightarrow \|BJ\| = \|B \mathbb{1}/n\| = \sqrt{\beta}$

$\|BC\| \leq \|B\| \|C\| \leq 1$.

$\|(BA)^{k-1} B \mathbb{1}/n\|_2 \leq ((1-\lambda)\sqrt{\beta} + \lambda)^{1-k} \cdot \frac{\sqrt{n}}{n}$.