Last lecture:

1. Repeat probabilistic algorithm to drive down error probability exponentially
   Use highly dependent random samples to get qualitatively similar error reduction while saving log on randomness

   How? Take a walk on an expander

2. Started building explicit expander
   Build recursively using three different graph products

   A. Matrix product
      \[ n = n' \]
      \[ G \circ G' \text{ graph with normalized adjacency matrix } \hat{A}_{G \circ G'} = \frac{A_G}{\sqrt{d}} \cdot \frac{A_{G'}}{\sqrt{d'}} \]
      # vertices: \( n \)
      degree: \( dd' \)
      expansion: improves

   B. Tensor product
      \[ G \otimes G' \text{ graph with normalized adjacency matrix } \hat{A}_{G \otimes G'} = \frac{A_G}{\sqrt{d}} \otimes \frac{A_{G'}}{\sqrt{d'}} \]
      \[
      \begin{pmatrix}
      a_{11} \hat{A}_G & a_{12} \hat{A}_G & \cdots & a_{1n} \hat{A}_G \\
      a_{21} \hat{A}_G & a_{22} \hat{A}_G & \cdots & a_{2n} \hat{A}_G \\
      \vdots & \vdots & \ddots & \vdots \\
      a_{n1} \hat{A}_G & a_{n2} \hat{A}_G & \cdots & a_{nn} \hat{A}_G \\
      \end{pmatrix}
      \]
(Tensor product continued)

- # vertices \( n \) increases
- degree \( d \) increases
- expansion doesn't get worse

(Replacement product)
- \( d' = n' \) (degree in \( G = \# \text{vertices in } G' \))
- \( d' \) constant (our design choice, definition)

*** To be described today ***

- # vertices \( n n' = n d \)
- degree \( 2 d' \) constant
- expansion doesn't get too much worse

Game plan

- Build sequence of expanders as follows

  (i) Let \( G(1) = \) excellent constant-size expander (if nothing else, can find using brute force)

    for \( i = 1, 2, 3, \ldots \)

  (ii) \( G(i) = G(i) \otimes G(i) \) \( [\text{increase size}] \)

  (iii) \( G(2) = \underbrace{G(1) \otimes G(1) \otimes \cdots \otimes G(1)}_{\text{suitably many times}} \) \( [\text{improve exp degree}] \)

(iv) \( G(i+1) = G(2) \otimes H \) \( [\text{decrease degree} \text{ still good expansion}] \)

   another constant-size excellent expander
Last time we proved

**Lemma 1**

If $G$ is an $(n,d,\lambda)$-spectral expander, then $G^2$ is an $(n,d^2,\lambda^2)$-spectral expander.

**Lemma 2**

If $G$ is a $(n,d,\lambda)$-spectral expander and $G'$ is a $(n,d',\lambda')$-spectral expander, then $G \otimes G'$ is a $(nn',dd',\max(\lambda,\lambda'))$-spectral expander.

We also introduced graph representation rotation map $\hat{G} : [n] \times [d] \to [n] \times [d]$.

Number neighbours of each vertex $1,2,\ldots,d$

$\hat{G}(u,i) = (v,j)$ if

(a) $v$ is a $j$th neighbour of $u$

(b) $u$ is a $j$th neighbour of $v$

$\hat{G}(\hat{G}(u,i)) = (u,i)$

$\hat{G}$ is a permutation on $[n] \times [d]$

We saw that $\hat{G}^2$ and $\hat{G} \otimes \hat{G'}$ are easy to compute from $\hat{G}$, $\hat{G'}$.

Why this representation? Convenient to describe replacement product, which we will do next.
Replacement product \( G \odot G' \) has:
- \# vertices \( nD \)
- degree \( 2d \)
- spectral expansion to be determined

1) For every vertex \( u \) of \( G \), make copy of \( G' \) (including vertices and edges)

2) If \( \hat{G}(u, i) = (v, j) \), make \( d \) parallel edges between \( i \)th vertex in \( u \)-copy of \( G' \) and \( j \)th vertex in \( v \)-copy of \( G' \)

[Some versions do only have single edge in 2]

With \( d \) parallel edges, yet that random step stays in same cluster with prob \( \frac{1}{2} \) moves to neighboring cluster with prob \( \frac{1}{2} \)

Rotation map for \( G \odot G' \):
- \( nD \) vertices: index by \( (u, v) \in [n] \times [D] \)
- \( 2d \) edges: index by \( (i, v') \in [D] \times \{0,1\} \)

\( b = 0 \) stage inside cluster (treat \( v \) as vertex of \( G' \))
\[ G \odot G' \left( (u, v), (i, 0) \right) = (u, \hat{G'}(v, i), 0) \]

\( b = 1 \) move to neighboring cluster (treat \( v \) as edge label of \( G' \))
\[ G \odot G' \left( (u, v, i), 1 \right) = (\hat{G}(u, v), i, 1) \]
\( G \) and \( G' \) with the following mappings:

- \( (u, 1) = (v, 3) \)
- \( (u, 2) = (w, 2) \)
- \( (u, 3) = (z, 1) \)
- \( (v, 1) = (w, 3) \)
- \( (v, 2) = (z, 2) \)
- \( (v, 3) = (u, 1) \)
- \( (w, 1) = (z, 3) \)
- \( (w, 2) = (u, 2) \)
- \( (w, 3) = (v, 1) \)
- \( (z, 1) = (u, 3) \)
- \( (z, 2) = (v, 2) \)
- \( (z, 3) = (w, 3) \)
Random-walk matrix normalized adjacency matrix
Again index vertices \((u, i) \in [n] \times [d]\)

0-edges inside same cluster described by
\[
I_n \otimes \hat{A}_G = \begin{pmatrix}
\hat{A}_G & 0 & \cdots & 0 \\
0 & \hat{A}_G & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \hat{A}_G
\end{pmatrix}
\]

1-edges described by \(\hat{G}\) written as permutation matrix
\[
\hat{A}((u, i), (v, j)) = \begin{cases} 
1 & \text{if } \hat{G}(u, i) = (v, j) \\
0 & \text{otherwise}
\end{cases}
\]

Why is this matrix even symmetric?
Because \(\hat{G}(u, i) = (v, j)\) iff \(\hat{G}(v, j) = (u, i)\)
by def of rotation map.

Adding these matrices and scaling by \(\frac{1}{2}\) to normalize, we get
\[
\hat{A}_G \otimes \hat{G}_1 = \frac{1}{2} \hat{A} + \frac{1}{2} (I_n \otimes \hat{A}_G) \quad (\dagger)
\]

We will do replacement product with fixed graph \(H\) having fixed degree \(d\)
⇒ bring degree down to constant again

What happens to expansion?
Lemma 3
If \( G \) is a \((n, D, 1-\epsilon)\)-spectral expander and \( H \) is a \((D, d, 1-\delta)\)-spectral expander, then \( G \otimes H \) is a \((n^2, 2Dd, 1 - \frac{\epsilon\delta^2}{2g})\)-spectral expander.

Intuition
- \( G \) is a good expander, but degree \( D \) is too high.
- \( k \)-step random walk on \( G \) requires \( O(k \log D) \) random bits.
- Want to use less randomness.
- Randomness reduction using expander walk on \( G' \):
  - \( G' \) has \( D \) vertices – needed domain for edge labels.
  - Degree \( \ll D \) – much less randomness.
  - At each step of walk, flip fair coin
    - With 50% prob take random step on \( G' \).
    - With 50% prob use random label from \( G' \) to pick edge in \( G \).

Definition: The **spectral norm** of an \( n \times n \) matrix \( A \) is \( \max \|Av\|_2 \) for \( v \in \mathbb{R}^n \), \( \|v\|_2 = 1 \).

For our random-walk matrices, the norm is just the absolute value of the largest eigenvalue, i.e., 1.

In addition, \( \|AB\| \leq \|A\| \|B\| \).
LEMMA 5

Let \( G(n,d,\lambda) \)-spectral expander with random-walk matrix \( A = \tilde{A}_G \).

Let \( J \) be the all-ones matrix and let

\[
\frac{1}{n} \tilde{A}_G \quad \text{be the random-walk matrix of the } n \text{-clique}
\]

with self-loops added. Then

\[
A = (1 - \lambda) \frac{1}{n} J + \lambda C
\]

for some \( C \) such that \( \|C\| \leq 1 \).

Proof

Define \( C = \frac{1}{\lambda} \left( A - (1 - \lambda) \frac{1}{n} J \right) \).

Need to prove \( \|Cv\|_2 \leq \|v\|_2 \quad \forall v \in \mathbb{R}^n \).

Decompose \( v = u + w \) \quad \text{with} \quad u = x \cdot 1 \quad \text{for some } x \in \mathbb{R}

\[ w \perp 1 \]

where

\[
Cu = \frac{1}{\lambda} \left( u - (1 - \lambda)u \right) = u
\]

Let \( w^i = Aw \).

Then

\[
\|w^i\|_2 \leq \lambda \|w\|_2
\]

and since \( A \) maps \( 1^T \) into itself we have

\[
w^i \perp 1
\]

Also \( Jw = 0 \) since \( \sum_i w_i = 0 \).
Hence

\[
Cw = \frac{1}{\lambda} \left( A - (1-\lambda) \frac{1}{n} J \right) w
\]

\[
= \frac{1}{\lambda} w' \quad \text{(3)}
\]

Since \( u \perp w' \), we get

\[
\| C w \|_2^2 = \| u + \frac{1}{\lambda} w' \|_2^2 \quad \text{[by (1) & (3)]}
\]

\[
= \| u \|_2^2 + \| \frac{1}{\lambda} w' \|_2^2 \quad \text{[by Pythagoras]}
\]

\[
\leq \| u \|_2^2 + \| w' \|_2^2 \quad \text{[by (3)]}
\]

\[
\leq \| v \|_2^2
\]

and it follows that \( \| C \| \leq 1 \) \( \square \)

Proof of Lem 3

If we want to prove \( k^2 \leq 1 - x \), then sufficient to prove \( k^3 \leq 1 - 3x \)

since \( 1 - 3x \leq (1 - x)^3 \)

So we show \( \lambda (G \otimes H)^3 \leq 1 - \frac{\varepsilon \delta^2}{8} \)

By Lem 1 \( \lambda (G \otimes H)^3 = \lambda \left( (G \otimes H)^3 \right) \)

Let \( \hat{H} \) random-walk matrix of corresponding to \( H \)

Let \( C \) random-walk matrix of \( (G \otimes H)^3 \)
Then by \((1)\) we have
\[
C = \left( \frac{1}{2} \hat{A}^3 + \frac{1}{2} (I_n \otimes B) \right)^3
\]
If we expand this out, we get 8 terms like
\[
\frac{1}{8} \hat{A}^3
\]
\[
\frac{1}{8} \hat{A}^2 (I_n \otimes B)
\]
Hence, all of these are random matrices and thus have norm \(\leq 1\).

Summing up, we can write
\[
C = \frac{7}{8} C' + \frac{1}{8} (I_n \otimes B)^A (I_n \otimes B) \quad (\times)
\]
for \(\|C'\| \leq 1\). Want to prove that second term shrinks vectors \(v, v \perp 1\), by some norm ratio factor.

Now use that by Lem 5
\[
B = (1 - \delta) B' + \frac{\delta}{D} J_D \quad (**)
\]
for \(\|B'\| \leq 1\). Then plugging \((**)\) into 2nd term of \((\times)\):
\[
\frac{1}{8} (I_n \otimes B)^A (I_n \otimes B) = \frac{1}{8} (I_n \otimes (1 - \delta) B' + \frac{\delta}{D} J_D)^A \left( I_n \otimes \left( (1 - \delta) B' + \frac{\delta}{D} J_D \right) \right) \quad (\dagger)
\]
We need that if $\|B\|_1 \leq 1$ then $\|\text{In } \otimes B\|_1 \leq 1$. Gathering terms again, we get that (4) can be written

$$\frac{1}{8} \frac{\sigma^2}{\delta^2} (\text{In } \otimes \frac{1}{D}) \hat{A} (\text{In } \otimes \frac{1}{D}) + \frac{1}{8} (1 - \sigma^2) C'' (\#)$$

for $\|C''\|_2 \leq 1$.

Combining (\#) and (\#\#) we get

$$C = \left(1 - \frac{\sigma^2}{8}\right) C'' + \frac{\sigma^2}{8} (\text{In } \otimes \frac{1}{D}) \hat{A} (\text{In } \otimes \frac{1}{D}) (\#\#)$$

for $\|C''\|_2 \leq 1$.

We claim

Claim A: $\lambda (\text{In } \otimes \frac{1}{D}) \hat{A} (\text{In } \otimes \frac{1}{D}) \leq 1 - \epsilon$

By Claim A and the triangle inequality, we get that for any $v, v' \neq 1$, $\|Cv\|_2$ shrinks compared to $\|v\|_2$ by factor

$$\left(1 - \frac{\sigma^2}{8}\right) 1 + \frac{\sigma^2}{8} (1 - \epsilon) = 1 - \frac{\sigma^2 \epsilon}{8}$$

which is exactly what we wanted to show.
Theorem A in turn follows from

\[(I_n \otimes \frac{1}{D} J_D)^\hat{A} (I_n \otimes \frac{1}{D} J_D) = A \otimes J_D\]

Proof of Claim B

Both sides describe random walks on graphs on nD vertices. Want to prove that graphs are the same. Look first at LHS.

Here we take one step from \(u,i\) by

1) Pick random \(k \in [D]\) and move to \((u,k)\),
   (because \((u,i)\) has edges precisely to all other \((u,j)\) including \(j = k\))

2) Move from \((u,k)\) to \(G(u,k) = (v,j')\)

3) Pick random \(j' \in [D]\) and move to \((v,j')\)

On RHS, the random walk takes one step from \((u,i)\) by

1) Pick \(j' \in [D]\) randomly.

2) Pick \(v\) as random neighbour in \(G\) and go to \((v,j')\)

This is the same walk, so graphs are equal. Claim B follows.
Perhaps another, more formal, way of looking at RHS in Claim B.

Let \( e_u \in \mathbb{R}^n \) indicator vector for \( u \)
\( e_i \in \mathbb{R}^D \) indicator vector for \( i \).

Want to see where we can go from \((u, i)\)
This is described by

\[
\left( A \otimes \frac{1}{D} J_D \right) \left( e_u \otimes e_i \right) = \left( A e_u \right) \otimes \left( \frac{1}{D} J_D e_i \right)
\]

which is choosing a neighbour of \( u \) in \( G \) plus a completely random \( j \in [D] \).

---

Claim A

Proof of

We want to bound \( \lambda \left( A \otimes \frac{1}{D} J_D \right) \)
which is \( \max \left( \lambda (A), \lambda \left( \frac{1}{D} J_D \right) \right) \)

But \( \lambda (J_D) = 0 \)

Suppose \( v \cdot 1 = 1 \), i.e. \( \sum_i v_i = 0 \)

Then \( (J_D v)_i \) just sums up coordinates and \( (J_D v)_i = 0 \quad \forall i \in [D] \)

Hence \( \lambda (J_D) = \max_{v \perp 1} \left| \frac{v^T J_D v}{v^T v} \right| = \left| \frac{v^T 0}{v^T v} \right| = 0 \)

and so \( \lambda (A \otimes \frac{1}{D} J_D) = \lambda (A) \leq 1 - \varepsilon \) by assumption.
Putting the pieces together

Now we can (semi-) describe a strongly explicit expander-graph construction and prove its properties.

**THEOREM 6**

There exist constants $c_0 \in \mathbb{N}^+$, $\lambda < 1$ such that a strongly explicit family of degree-$c_0$ graphs with spectral expansion $\lambda$ exist.

**Remark 7**

Once we have this, we get expansion for any $\lambda$ (but then $c_0$ depends on $\lambda$).

Just use matrix product.

We will actually prove something slightly weaker, namely that there is a $c_0 \in \mathbb{N}^+$ such that for every $c_0 \leq k \in \mathbb{N}^+$ we can find a strongly explicit expander on $c_0^k$ vertices. This can then be improved to yield Theorem 6, but we might not have the energy to do that.

We prove Theorem 6 by finding 3 base case expanders with good enough spectral expansion and then following our game plan.
Let $D = (2d)^{100}$ for $d$ chosen large enough. Find by brute force:

- $H(D, d, 0, 0.01)$ - spectral expander
- $G_1(D, 2d, 1/2)$ - spectral expander
- $G_2(D^2, 2d, 1/2)$ - spectral expander

For $G_k > 2$, let

$$G_k = \left( \frac{G_{1 \times k - 1}}{2} \right) \otimes \left( \frac{G_{2k - 1}}{2} \right)^{50} \oplus H$$

**Lemma 8**

For every $k \leq N^+$, $G_k$ is a

$$((2d)^{100k}, 2d, 1 - \frac{1}{50})$$ - spectral expander.

Furthermore, there is a poly$(k)$-time algorithm that given $k$, $i$, $j$ finds the $j$th neighbour of $i$ in $G_k$.

**Proof**

The algorithm can be reconstructed from our discussions how to compute rotation maps for our different graph products plus using recursion. We skip the details.

Let us verify the parameters of $G_k$.

Base cases $G_1$ and $G_2$ are clearly OK.
$\text{Elves}$ $v_k = |V(G_k)|$

\[v_k = \frac{n_k(k-1)}{2} \cdot \binom{k}{2}^{k-1} \cdot 2d^{(2d)^{100}} = \left[ \text{Induction hypothesis} \right] \]

\[= \left(2d\right)^{100} \frac{(k-1)}{2} \cdot \left(2d\right)^{100} \binom{k}{2}^{(k-1)/2} \cdot \left(2d\right)^{100}
\]

\[= \left(2d\right)^{100} \frac{(k-1)}{2} + \left[ \frac{k-1}{2} \right] = k-1\]

\[= \left(2d\right)^{100} (k-1) + 100 = \left(2d\right)^{100k}\]

$G_k$ $k' < k$ have degree $2d$

$G_{\frac{k-1}{2}} \otimes G_{\frac{k-1}{2}}$ has degree $\left(2d\right)^2$

Taking matrix product $50$ times yields degree $\left((2d)^2\right)^{50} = \left(2d\right)^{100}$

This is $\frac{1}{2} |V(H)|$

Taking replacement product brings degree down to $2d$ again
\[ \lambda(G_{k+1}) \leq 1 - \frac{1}{50} \text{ by induction hypothesis} \]

\[ \lambda \left( \frac{G_{k+1}}{2} \right) \leq 1 - \frac{1}{50} \text{ by Lem 2} \]

\[ \lambda \left( \left( \frac{G_{k+1}}{2} \right) \times G_{\frac{d-k+1}{2}} \right) \leq (1 - \frac{1}{50})^{50} \text{ by Lem 1} \]

Use \( 1 + x \leq e^x \) to derive

\[ (1 - \frac{1}{50})^{50} \leq \frac{1}{e} < \frac{1}{2} \]

By Lem 3 we have

\[ \lambda(G_k) \leq 1 - \left( \frac{1}{2} \right)^{\frac{400}{99/100}} \]

\[ 1 - \left( \frac{1}{2} \right) \left( \frac{99}{100} \right)^2 \]

\[ \leq 1 - \frac{1}{50} \]

which proves Lem 8.

To get Thm 6, show that \((n, d, \lambda)-\)expander can be transformed into \((n', cd, \lambda')\)-expander for any \( n/c \leq n' \leq n \), \( \lambda' = \lambda'(\lambda, d) \) by joining together sets of at most \( c \) vertices into "mega-vertices."
Final remarks

Quantitative bounds in Theorem 6 pretty bad:
- Relative degree - expansive
- Running time

Partly because of simplified exposition.
Further optimizations possible.
But even then this construction is not best known.

However:
- Analysis completely elementary
- This particular construction has found several applications elsewhere in TCS
  (which we won't have time/energy to study during this course)