**Theorem:** \( NP \subseteq \text{PCPP}[\text{poly},1] \)

Recall that in the previous lecture we defined:

**Def:** The quadratic functions encoding \( Q : \{0,1\}^{n+1} \rightarrow \{0,1\}^{n^2} \) maps \((a_1, a_2) \in \{0,1\}^{n+1}\) into \( H(a \oplus a) \)

where \( a \oplus a \in \{0,1\}^n \) is defined by \((a \oplus a)_i = a_i \cdot a_i^*, \)

and \( a^* \in \{0,1\}^n \) is the vector \((a_1, a_2, \ldots, a_n)\).

* This encoding is self correctable (2 queries)
* It is locally testable (exercise). Namely:

  There is a randomized procedure that, given oracle access to \( w \), makes \( o(1) \) queries and
  1) if \( \text{wQF} \) accepts \( w \) with prob \( 1 \)
  2) if \( d = \text{dist}(w, QF) > c \) rejects \( w \) with prob \( 1 - c \) (for an\( \text{abs. const.} \( c \))

**Proof of Theorem:**

**Step 1:** Recall that zero testing is \( NP \)-complete. Moreover,

**Lemma 1:** Let \( \phi \) be a 3-SAT formula over vars \( X = x_1, \ldots, x_n^3 \). There are \( m \) degree-2 polynomials \( P_1, \ldots, P_m \) over variables \( X \cup Y \cup Z \), \( n^1 \cdot y_1 = n^{o(1)} \), such that

(i) If \((a_1, \ldots, a_m) \in \{0,1\}^{3n} \) satisfies \( \phi \), then \( \exists (b_1, \ldots, b_m) \in \{0,1\}^{3n} \)
such that \( P_i(a \oplus b) = 0 \) for all \( i \).

(ii) If \( \phi \) is unsatisfiable, then for any \( a \) there is no \( b \) s.t. \( P_i(a \oplus b) = 0 \) for all \( i \).
Proof: connect each $x_i \cdot x_j \cdot \bar{x}_k$ to $(1-x_i)(1-x_j)x_k$ etc. whenever a poly contains $x_i x_j$ replace by a new var $y_{ij}$ and add a poly $x_i x_j - y_{ij}$.

$i)$ + $(ii)$ are immediate. 

Step 2:

Note that if $a_1, \ldots, a_m$ does not zero at least one of $P_1 \ldots P_m$ then for a random $\bar{r} = (r_1, \ldots, r_m) \in \{0, 1\}^m$

$$Pr\left[Q_r(a) = \Sigma_i P_i(\bar{a}) = 0 \right] \leq \frac{1}{2}$$

Step 3:

We describe a verifier of proximity for 3SAT.

Ver has explicit input $\Phi$ and implicit input $a_1, \ldots, a_m$.

Ver expects as proof, the quad. function encoding of $(\bar{a}, \bar{b})$

where $b$ is the assignment to aux. vars that together zero all $\{P_i\}$ resulting from the reduction in the lemma.

1) Test that $\Phi$ is a legal QF encoding, if not reject.

2) Compute $P_1 \ldots P_m$. Choose $\bar{r} \in \{0, 1\}^m$ and compute

$$Q_r = \Sigma_i P_i$$

(i.e. compute the coefs of the quad. func.)

Use self-correction to verify that $Q_r(\bar{a}, \bar{b}) = 0$

3) Consistency: Select $i \in \{1, \ldots, n\}$, test that $a_i$ equals the appropriate bit encoded by $\Phi$, using self correction.

i.e. test that $S^\Phi(e_i) = a_i$
Proof of completeness: immed.

Proof of Soundness: If $\bar{a}$ is $\delta$-far from satisfying $\phi$, we prove that $\bar{a}$ rejects w. prob $> \mathcal{N}(\delta)$.

- if $\bar{a}$ is $\delta$-far from a legal $\phi^r$, step 1 rejects w. prob $\mathcal{N}(\delta)$.

otherwise, $\bar{a}$ is $\delta$-close to $\phi_f(a_{b_4})$.

- if $a_{b_4}$ are such that $\exists i: P_i(a_{b_4}) \leq 0$, then w. prob $> \frac{1}{2}$ $Q_f(a_{b_4}) \leq 0$, and with $\mathcal{N}(\delta)$ probability, step 2 rejects. (depending on the self-correction). Otherwise,

- $a_{b_4}$ is s.t. $\forall i P_i(a_{b_4}) = 0$, so $\text{dist}(a,a_i) \geq \delta$. (By lemma)

So w. prob $\mathcal{N}(\delta)$ step 3 rejects.

params:
- randomness - polr.
- queries - $O(1)$
- completeness - 1
- soundness - constant
Expander Graphs

Expander graphs are graphs without "bottlenecks".

Given \( G = (V,E) \), and \( S \subseteq V \), we consider

\[
\delta(S, \bar{S}) = \frac{|\{uv \in E \mid u \in S, v \in \bar{S}\}|}{|S||\bar{S}|}, \text{ relative to } |S|, |\bar{S}|.
\]

Define the edge expansion of \( G \) as

\[
\overline{\delta}(G) = \min_{S, 1 \leq |S| \leq \frac{|V|}{2}} \frac{\delta(S, \bar{S})}{|S|}
\]

\( \overline{\delta}(G) \) is the size of the smallest bottleneck.

A clique is a graph without bottlenecks, but that's easy since it is dense.

A path has a tiny bottleneck.

A sparse graph without (small) bottlenecks is called an "expander".

Definition: A family \( \{G_n\}_{n=1}^{\infty} \) of graphs on \( n \) vertices is \( \varepsilon \)-expanding if \( \overline{\delta}(G_n) \geq \varepsilon \) for all \( n \geq n_0 \).

Theorem: There exist \( d \in \mathbb{N} \) and \( \varepsilon > 0 \) and a family \( \{G_n\}_{n=1}^{\infty} \) of \( d \)-regular graphs that is \( \varepsilon \)-expanding. (in fact, a random \( d \)-regular graph is quite expanding)
The 2nd Largest Eigenvalue

An alternate way to measure expansion, is via the eigenvalue gap. Let \( G = (V, E) \) be a d-regular graph on \( n \) vertices. Let \( A = (a_{ij}) \) be its adjacency matrix. Then \( A \) is symmetric and has \( n \) real eigenvalues

\[ d = \lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_{n-1} \geq -d \]

with eigenvectors \( v_0, \ldots, v_{n-1} \). \( (v_0 = \mathbf{1}) \).

Def: A d-regular graph on \( n \) vertices is an \((n,d,\lambda)\)-expander if
\[ \lambda = \max(1, \lambda_1, 1, \lambda_{n-1}) < d \]
\( \lambda - \lambda \) is called the spectral gap of \( G \).

Thm: \( \frac{\phi(G)}{2d} \leq d - \lambda \leq 2\phi(G) \)

we will only prove (which is easier) since it is suff. for our application.

Thm: There are explicit \( d \geq 3 \) and \( \lambda < d \) and an explicit (finite) family of \((n,d,\lambda)\)-expanders.

Lubotsky - Philips - Sarnak (LPS) construction:
\[ V = \mathbb{Z}_p \times \mathbb{S}_3 \times \text{connected with } x+1, x-1, x^{-1}. \]

Also - A random d-regular graph, has \( \lambda \leq 2\sqrt{d - 1} \) whp.
The Rayleigh Quotient:

**Claim:** For a real symmetric matrix $A$, the following is true:

$$
\lambda_i = \max_{x: \|x\|=1} \langle x, Ax \rangle
$$

where $v_0, \ldots, v_{n-1}$ are eigenvectors of eigenvalues $\lambda_0, \ldots, \lambda_{n-1}$.

**Proof:** Clearly taking $x = v_i/\|v_i\|$ we obtain $\lambda_i$.

Write $x = \sum_{i,j} x_{ij} v_i \cdot v_j$. Then, assuming $\|x\|=1$,

$$
\begin{align*}
    x^T A x &= \sum_{i,j} x_{ij}^2 v_i \cdot v_j A(v_i \cdot v_j) \\
           &= \sum_{i,j} x_{ij}^2 \lambda_j \leq \lambda_j \quad \text{(since } \sum_i x_{ij}^2 = \|x\|^2 = 1) \tag{1}
\end{align*}
$$

Similarly, $\lambda = \max_{x: \|x\|=1} \frac{|x^T A x|}{\|x\|^2}$.

**Lemma:** Let $G_i = (V_i, E_i)$ be an $(n, d_i, \lambda_i)$-expander for $i = 1, 2$.

Define $H = (V, E_1 + E_2)$ by adding the adj matrices

$$
    A = A_1 + A_2 \quad \text{(so } H \text{ is possibly a multigraph)}.
$$

Then $H$ is an $(n, d_1 + d_2, \lambda_1 + \lambda_2)$ expander.

**Proof:** Choose $x$ st. $\lambda = x^T A x$ (and $\|x\|=1$, and $\perp 1$)
Then clearly \( x^T A_1 x = x^T (A_1 + A_2) x = x^T A_1 x + x^T A_2 x \)

\[ \leq \lambda(A_1) + \lambda(A_2) \]

This makes sense: if all the edges of two graphs and one of them had no small bottlenecks then the result must also have this property.

We now prove the connection between “bottlenecks” and \( \lambda \):

**Lemma**: Let \( G \) be an \((n,d,\lambda)\)-expander, then \( d - \lambda \leq 2\Phi(G) \).

**Proof**: Suppose \( S \subseteq V \) is st. \( |S| \leq n/2 \) and \( \phi(S) = \frac{E(S, \overline{S})}{|S|} \).

The idea is to consider the following vector \( x \)

\[ x = \begin{cases} \frac{1}{\sqrt{|S|}} & \text{if } v \in S \\ 0 & \text{if } v \in \overline{S} \end{cases} \]

(for simplicity think that \( |S| = \frac{n}{2} \) and then \( x \) is a normalized \( \pm 1 \) vector def. by \( S \)).

\[ x^T A x = \langle x, Ax \rangle = \sum_{v \in \overline{S}} x_v A_{v\overline{S}} x_{\overline{S}} = 2 \sum_{(s, \overline{s}) \in E} x_s x_{\overline{s}} \]

\[ = 2 \frac{E(S, \overline{S})}{|S|} (1 - (|S| - |S|)^2 + (|S| - |S|)^2) \]

\[ = d|S||\overline{S}|n - n^2 E(S, \overline{S}) \]

Since \( x^T A x \leq \|x\|_2^2 \) we get

\[ d|S||\overline{S}|n - n^2 E(S, \overline{S}) \leq \lambda(n|S||\overline{S}|) \]

\[ d - \lambda \leq \frac{n E(S, \overline{S})}{|S||\overline{S}|} \leq 2 \Phi(G). \]
Expander Mixing Lemma

We said that expanders have no "bottlenecks", and that random graphs are expanders. It turns out that expanders "emulate" random graphs in certain precise ways.

For an expander $G = (V, E)$, and for any subsets $S, T \subseteq V$ the # of edges between $S$ and $T$ is "close" to what it would be in a random graph of the same density:

Lemma (EMC): Let $G$ be an $(n, d, \lambda)$-expander, and let $S, T \subseteq V(G)$.

$$|E(S, T) - d|S||T|| \frac{1}{n} | \leq \lambda \sqrt{|S||T|}$$

in a random $G$: $d|S||T|$ edges from $S$, each hits $T$ w. prob $1/|T|/n$.

Random Walks on Expanders

Any graph naturally gives rise to a Markov chain $X_0, X_1, \ldots, X_t, \ldots$

(whose $X_i$ is a random variable that takes values in $V_i$ and $\text{Pr}(X_i = X_j | X_{i-1}) = \text{Pr}(X_i = X_{i-1})$)

where $X_i$ is the vertex in the $i$-th step of a random walk.

Expanders are graphs on which this chain is "rapidly mixing", i.e. even if the distribution of $X_0$ is not very random, $X_t$ will be "close" to uniformly distributed on $V$ for rather small $t$'s. (i.e. the walk quickly "forgets" its starting point)
In particular, consider the following scenario. Let $B \subseteq V$ be a set of density $\frac{|B|}{|V|} = \beta$. Choosing $t$ vertices independently at random, the probability of them all being in $B$ is $\beta^t$.

What if we choose them by taking $V_1$ at random and then $V_2, V_3, \ldots, V_t$ a random walk from $V_1$? The probability is similar to $\beta^t$, with an error that goes to zero when $\lambda \to 0$.

We prove the following edge variant (which will be needed for proving the PCP theorem):

**Lemma:** Let $G$ be an $(n, d, \lambda)$-expander, and let $F \subseteq E$ with $\frac{|F|}{|E|} = \beta$. and let $(V_0, V_1, \ldots, V_t, V_{t+1})$ be a random walk. (i-th step = $(V_i, V_{i+1})$)

The probability that $(V_t, V_{t+1}) \in F$, conditioned on $(V_0, V_1) \in F$ is at most

$$\frac{|F|}{|E|} + \left(\frac{\lambda}{d}\right)^{t-1}$$

error term decaying exp. with $t$.

**Proof:** Let $A$ be the normalized adjacency matrix of $G$.

Suppose $x \in \mathbb{R}^n$ is a probability vector ($x_i \geq 0$, $\sum x_i = 1$)

Let $U_1, \ldots, U_t$ be a Markov chain defined by the random walk on $G$, and assume $U_1$ is distributed according to $x$. Then the distribution of $U_t$ is given by $y = Ax$ and of $U_t$ by $A^{t-1} x$.
\[
y_v = \sum_u A_{uv} x_v = \frac{1}{d} \sum_u x_v = \sum_v \text{Prob}[U_1 = v] \cdot \text{Prob}[U_2 = u | U_1 = v] \cdot \text{Prob}[U_2 = u].
\]

In the lemma, \((v_0, v)\) is a random edge in \(F\), so \(v_0\) is distributed according to \(x_v = \frac{k}{2F}\) where \(k = \# \text{ of } F \text{ edges touching } v\). (Check: \(\sum x_v = \sum u : \deg u = 1\).)

The probability that the \(t\)-th step is in \(F\) is \(\frac{k}{d}\) where \(k\) is the \# of \(F\)-edges incident on \(v_t\). This is described by \(y_v = x_v \cdot \frac{2F}{d}\).

 Altogether, we are interested in

\[
\langle A^{t-1} x, y \rangle = \sum_v \text{Prob}[V_t = V] \cdot \text{Prob}[(v_t, v_{t+1}) \in F | V_t = V] = \text{Prob}[t\text{-th step of } \tilde{y}].
\]

Now, let's compute. \(\langle A^{t-1} x, y \rangle = \langle A^{t-1} x, x \rangle \cdot \frac{2F}{d}\). If \(u = \frac{1}{n} \cdot \vec{1}\)

We write \(x = x'' + x'\) where \(x'' = \langle x, u \rangle u\) and \(x' = x - x''\).

So (i) \(\langle x', x' \rangle = 0\) and (ii) \(\langle x'' \rangle = \sum x_v = \frac{1}{n}\) so \(\|x''\|^2 = \frac{1}{n}\).

\[
A^{t-1} x = A^{t-1} x'' + A^{t-1} x' = x'' + A^{t-1} x'
\]

\[
\langle A^{t-1} x, x \rangle = \langle x'', x \rangle + \langle A^{t-1} x', x'' + x' \rangle
\]

\[
\leq \frac{1}{n} + \frac{1}{d} A^{t-1} x'' \cdot \frac{1}{n} x'' \leq \frac{1}{n} + \frac{1}{d} A^{t-1} \frac{1}{n} x'' \frac{1}{n} x'' \leq \frac{1}{n} + \frac{1}{d} A^{t-1} \frac{1}{n} x'' \frac{1}{n} x'' \leq \frac{1}{n} + \frac{1}{d} A^{t-1} \frac{1}{n} x'' \frac{1}{n} x''
\]
\( \| x \|_2^2 = \sum \left( x_v \right)^2 \leq \max x_v \cdot \sqrt{\sum x_v} = \max x_v = \frac{d}{2F} \) .

Multiplying by \( \frac{\varepsilon F}{d} \) we get (note that \( |E| = \frac{\varepsilon d}{n} \) so \( \frac{\varepsilon}{d} \cdot \frac{1}{n} = \frac{|E|}{|\mathbb{E}|} \) )

\[
P_{\text{ub}} = \langle A^t x, y \rangle = \frac{|E|}{|\mathbb{E}|} + \left( \frac{\lambda}{d} \right)^{-1}
\]