$NP \subseteq \text{LENP} \iff \exists \text{ poly-time verifier } V$ s.t. $x \in L \implies \exists y, \|y\| \leq \text{poly}(|x|) \text{ st. } V(x, y) \text{ accept}$

$x \notin L \implies \forall y, \textit{V}(x, y) \text{ reject}.$

Claim: $L = 3\text{-COLOR} \iff x = G \text{ and } y = 3\text{-coloring of } G$

Only valid claims have proofs.

For invalid claims, ($x \notin L$), every proof will be rejected.

Requires reading pt. in entirety.

Lazy grader/TAs dream: Can you get by with good confidence by just "spot-checking" $y$?

Goal: Develop robust proof system/proof writing system s.t. for false claims, there are bugs in the proof everywhere.
PCP Theorem: If \( \exists \text{ finite } q \text{ (integer)} \) s.t. a polytime randomized verifier \( V \):
- If \( x \in L \), \( \exists y, |y| \leq \text{poly} \left( |x| \right) \) s.t. \( V(x, y) \) accepts with prob. 1 (Certainly)
- If \( x \notin L \), \( \forall y, |y| \leq \text{poly} \left( |x| \right) \), \( V(x, y) \) rejects with prob. \( \geq 1/3 \)

Furthermore, \( V \) only probes/reads \( q \) locations of the proof \( f \).

\( f \) (randomly chosen)

\[ (P\!P) \quad V \quad (P\!P) \]

\( 2L \!\in \! L \!\in \! \Sigma \!) \]

\( P\!P = \text{ probabilistically checkable proof} \)

Go from reading full proof to a tiny sample of the pf.

\( q \) is independent of \( |x|, |y| \).

In fact, can take \( q \leq 3 \).
Connection to Approximation

3SAT is NP-complete. So given a satisfiable 3SAT formula, there is likely no polynomial algo to find a satisfying assignment.

How about finding an approximately good satisfying assignment? Say satisfies 99% of the clauses. Also seems hard.

How might one prove such a hardness?

A "gap property" reduction:

\[ \text{CircuitSAT} \leq_p \text{APPROX-3SAT} \]

Circuit \( C \) \( \rightarrow \) formula \( \phi = \text{GapRed}(C) \)

\( C \) satisfiable \( \Rightarrow \) \( \phi \) satisfiable
\( C \) not satisfiable \( \Rightarrow \) \( \phi \) is not 99% satisfiable

(C i.e. no assignment gets even 99% of the clauses satisfied in \( \phi \))

Exercise: Such a reduction implies finding a 99% satisfying assignment to a fully satisfiable formula is also hard.
In the usual reduction, you can just violate one gate of circuit & make it satisfiable.

PCP Theorem $\iff$ Existence of such a gap producing reduction

(\approx\text{approximately satisfyin 2SAT is NP-hard})

Hardness of approximation
Let $L = \text{CircuitSAT}$ and $C \in L$ be a circuit.

**PCP proof:** A purported satisfying assignment $\sigma$ to $\phi = \text{GapRed}(C)$.

**Verifier:**
- Pick a random clause of $\phi$.
- Check that it is true under $\sigma$.

- **Reads 3 bits**
- If $C \not\leq L$, write proper $\sigma$ & $\phi$.
- Verifier will surely accept $\sigma$.
- If $C \leq L$, verifier reject with $\geq 1\%$ probability.
- To reject with $\text{prob} \geq \frac{1}{2}$, just repeat $O(1)$ times.

$(0.99)^t \leq \frac{2}{3}$

3t queries.
Once you have hardness of approx result for 3SAT, can prove further "inapproximability" result is via reductions.

Eq: 3SAT ≤ₚ CLIQUE
  \( \forall \rightarrow \langle G, k \rangle \)

Inspection of the reduction shows:

Maximum Clique size of \( G \)

\[ = \text{Max } \# \text{ clauses of } \phi \text{ that can be satisfied} \]

\( \implies \) Finding a 99\% approx clique is \( \text{NP-hard} \)

\( \Downarrow \) Finding a 1\% approx clique is \( \text{NP-hard} \)