15-252 LECTURE #9, 3/19/2020
PCP and HARDNESS OF APPROXIMATION

NP: $L \in NP$ $\exists$ det. poly time verifier V
s.t. $x \in L \Rightarrow \exists y, |y| \le poly(|x|)$ s.t. $V(x,y)$ accept
$x \notin L \Rightarrow \forall y, V(x,y)$ reject.

$\{x \in L\}$ Claim

y (proof/certificate)

$L = 3COLOR$. $x = G$ $y =$ 3-coloring of G

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

Requires reading pf. in entirety.
Lazy grader/TAs dream: Can you get by with good confidence by just "spotchecking" y?

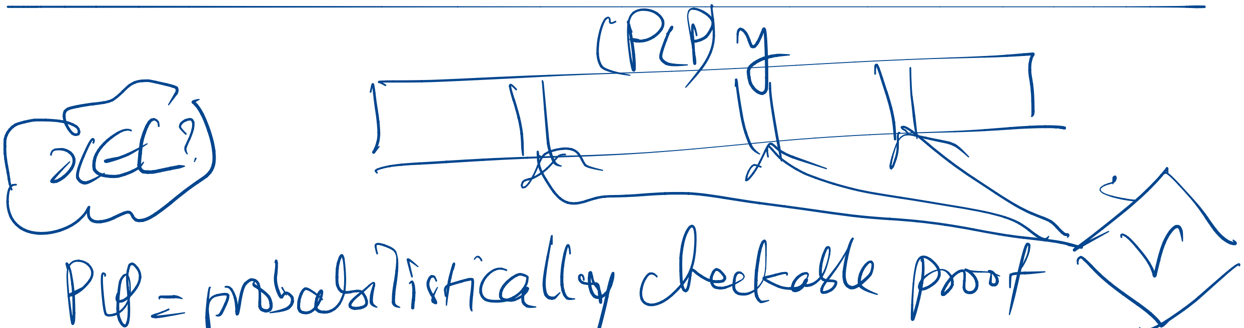
Goal: Develop robust proof system/proof writing format s.t. for false claims, there are bugs in the proof everywhere.

PCP Theorem ∃ finite q (integer) s.t. following holds:

$\forall L \in NP$, ∃ a polytime randomized verifier V:

- If $x \in L$, $\exists y$, $|y| \le poly(|x|)$ s.t. $V(x,y)$ accepts with prob. 1 (certainty)
- If $x \notin L$, $\forall y$, $|y| \le poly(|x|)$, $V(x,y)$ rejects with prob $\ge 1/3$

Furthermore, V only probes/reads q locations of the proof y.
(randomly chosen)



PCP = probabilistically checkable proof

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

q is independent of $|x|, |y|$

In fact, can take $\boxed{q = 3}$

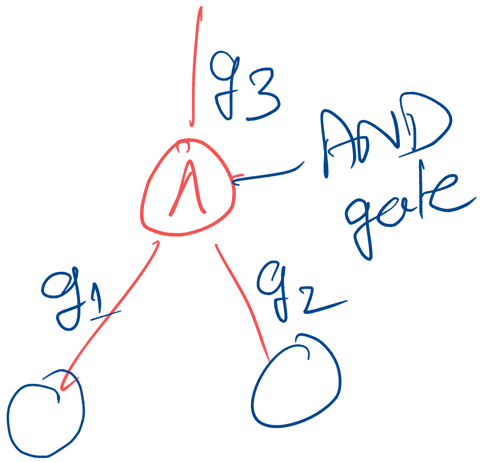
Connection to Approximation

3SAT is NP-complete
So given a satisfiable 3SAT formula,
there is likely no polytime 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 producing" reduction:
CIRCUITSAT $\leq_p$ APPROX-3SAT
Circuit $C \longmapsto$ formula $\phi = \mathrm{GapRed}(C)$
C satisfiable $\Longrightarrow$ ϕ satisfiable
C not satisfiable $\Longrightarrow$ ϕ is not 99% satisfiable

(ie no assignment gets even 99% of the clauses satisfied in ϕ)

Exercise: Such a reduction implies finding a 99% satisfying assignment to a fully satisfiable formula is also hard.



$$g_3 = g_1 \wedge g_2$$

$$(\bar{g}_1 \vee \bar{g}_2 \vee g_3) \wedge$$
$$(\bar{g}_1 \vee g_2 \vee \bar{g}_3) \wedge$$
$$(g_1 \vee \bar{g}_2 \vee \bar{g}_3) \wedge$$
$$(g_1 \vee g_2 \vee \bar{g}_3)$$

In the usual reduction, you can just violate one gate of circuit & make it satisfiable

---

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

if & only if

($\approx$ approximately satisfying 3SAT is NP-hard)

PCP Thm $\Longleftarrow$ Hardness of approximation

$\Longrightarrow$

$L = \text{CIRCUITSAT}$ $\quad C \mapsto \phi = \text{GapRed}(C)$

$C \in L$ $\quad$ 3SAT formula

circuit

<u>PCP proof</u>: A purported satisfying assignment σ to $\phi := \text{GapRed}(C)$

<u>Verifier</u>:

- Pick a random clause of ϕ
- Check that it is true under σ

- Reads 3 bits ✓
- If $C \in L$, write proper σ & Verifier will surely accept ✓
- If $C \notin L$, Verifier reject with $\geq 1\%$ probability.

To reject with prob $\geq 1/3$, just repeat $O(1)$ <u>times</u>

$$(0.99)^t \leq 2/3$$

3t queries

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

Eg: $3SAT \leq_p CLIQUE$

$\varphi \longmapsto \langle G, k \rangle$

Inspection of the reduction shows:

Maximum Clique size of G

= Max # clauses of φ that can be satisfied

$\Rightarrow$ Finding a 99% approx clique is NP-hard

Amplify $\Rightarrow$ Finding a 1% approx clique is NP-hard