CS 579: Computational Complexity. Lecture 17

PCP and Hardness of Approximation

Alexandra Kolla
Today

- Define PCPs, state PCP Theorem.
- Motivation, approximation algorithms.
- PCP and MAX-3SAT.
- Max Clique.
**Definition (PCP).** Given functions \( r(n), q(n) \), we say that \( L \in \text{PCP}(r(n), q(n)) \) is there is a polynomial time probabilistic verifier \( V \), which is given \( x \), oracle access to a proof \( \pi \), uses \( r(|x|) \) random bits, reads \( q(|x|) \) bits of \( \pi \) and such that:

\[
\begin{align*}
\circ & \ x \in L \implies \exists \pi \Pr[V^\pi(x) = 1] = 1 \\
\circ & \ x \notin L \implies \forall \pi \Pr[V^\pi(x) = 1] \leq \frac{1}{2}
\end{align*}
\]
Discussion of PCPs as “new way to see proofs”.
Non-adaptive queries.
Arbitrary constant soundness.

\[ PCP(r(n), q(n)) \subseteq NTIME(2^{O(r(n))}q(n)). \]
\[ PCP(O(\log n), O(1)) \subseteq NP. \]
PCP Theorem

\[ NP = PCP(O(\log n), O(1)) \]
Approximation of NP-hard problems

- Can’t solve NP-hard problems efficiently, what about approximating them?
- Some times it’s just as good.
- E.g. approximation of MAX-3SAT: For every 3CNF formula $\varphi$, the value of $\varphi$, denoted $\text{val}(\varphi)$, is the maximum fraction of clauses that can be satisfied by any assignment to the variables. In particular, $\text{val}(\varphi)=1$ if the formula is satisfiable.
- For every $\rho \leq 1$, the algorithm $A$ is a $\rho$-approximation algorithm for MAX-3SAT if for every CNF formula $\varphi$ with $m$ clauses, it outputs an assignment that satisfies at least $\rho \text{val}(\varphi)m$ clauses.
PCP and MAX-3SAT

- **Definition (MAX-3SAT).** Given a 3CNF formula \( \varphi \) (at most 3 variables per clause), find an assignment that satisfies the largest number of clauses.

- Generalizes 3SAT so NP-hard.
- Easy to approximate within factor of 2. (proof)
- Possible to do better (Karloff-Zwick) gives 7/8.
PCP and MAX-3SAT

- Some problems admit ptime algorithms with approximation ratio $\geq (1 - \epsilon)$, $\forall \epsilon$.
- The PCP Theorem implies this is not the case for MAX-3SAT.

Theorem. The PCP theorem implies that there is an $\epsilon > 0$ such that $(1 - \epsilon)$-approximation of MAX-3SAT is NP-hard.
PCP and MAX-3SAT

**Theorem.** If there is a reduction like above, for some problem $L \in NP$, then $L \in PCP(O(\log n), O(1))$, i.e. the PCP theorem holds for that problem.
PCP and MAX-3SAT

- **Tighter result (Hastad).** There is a PCP verifier for NP that uses $O(\log n)$ bits of randomness which, based on $R$, choses 3 positions $i_1, i_2, i_3$ and a bit $b$ and accepts iff $\pi(i_1) \oplus \pi(i_2) \oplus \pi(i_3) = b$. The verifier satisfies
  - $x \in L \Rightarrow \exists \pi Pr [V^\pi(x) = 1] \geq 1 - \epsilon$
  - $x \notin L \Rightarrow \forall \pi Pr [V^\pi(x) = 1] \leq \frac{1}{2} + \epsilon$
PCP and MAX-3SAT

- Implies $7/8 + \epsilon$ hardness of approximation for MAX-3SAT
Max Clique

- **Definition.** Given an undirected graph $G(V,E)$, find the largest $C \subseteq V$ such that $\forall u, v \in C, (u, v) \in E$. When convenient, we use the complementary graph equivalent “Max Independent Set” which is the largest $I \subseteq V$ such that $\forall u, v \in C, (u, v) \notin E$. 
Max Clique

- NP-hard, ask for approximations. \( \frac{\log n}{n} \) approx, simple.
- Best known \( \frac{(\log n)^2}{n} \)
- From PCP theorem we get that we cannot approximate Max Clique within any constant (proof).
Max Clique

- Hastad showed that if $NP \neq ZPP$, we cannot approximate Max-IS better than $\frac{1}{n^{1-\epsilon}}$, $\forall \epsilon > 0$. 