Undergraduate Complexity Theory
Lecture 15: coNP

Marcythm

July 18, 2022

1 Lecture Notes

idea: NP: efficiently certifying $x \in L$, coNP: efficiently certifying $x \notin L$. Recall UNSAT in hw5.

Definition 1.1. $\mathsf{coNP} = \{L : \overline{L} \in \mathsf{NP}\}$.

Remark 1.2. $\mathsf{coNP} \neq \overline{NP}$.

Theorem 1.3. $\mathsf{SAT} \in \mathsf{P} \implies \mathsf{UNSAT} \in \mathsf{P}$.

Theorem 1.4. $A \leq_m^{\mathsf{P}} B \iff \overline{A} \leq_m^{\mathsf{P}} \overline{B}$.

Theorem 1.5. P *is closed under complement.*

Theorem 1.6. $\mathsf{P} \subseteq \mathsf{coNP}$.

Theorem 1.7. $\mathsf{P} = \mathsf{NP} \implies \mathsf{P} = \mathsf{coNP}$.

Corollary 1.8. $\mathsf{P} = \mathsf{NP} \implies \mathsf{coNP} = \mathsf{NP}$.

Corollary 1.9. $\mathsf{coNP} \neq \mathsf{NP} \implies \mathsf{P} \neq \mathsf{NP}$.

Theorem 1.10. UNSAT *is* coNP*-complete.*

Proof. $\forall A \in \mathsf{coNP} : \overline{A} \in \mathsf{NP} \implies A \leq_m^{\mathsf{P}} \overline{A} \leq_m^{\mathsf{P}} \mathsf{SAT} \leq_m^{\mathsf{P}} \mathsf{UNSAT}$. $\square$

Definition 1.11. $\mathsf{TAUTOLOGY} = \{\langle \phi \rangle :$ every truth assignment makes ϕ true$\}$.

$\mathsf{TAUTOLOGY} \in \mathsf{NP}$? $\mathsf{TAUTOLOGY} \in \mathsf{coNP}$? $\overline{\mathsf{TAUTOLOGY}} \in \mathsf{NP} \implies \mathsf{TAUTOLOGY} \in \mathsf{coNP}$.
$\mathsf{PRIME} \in \mathsf{coNP}$.
review:

1. $L \in \mathsf{NP}$: $\forall x \in L$, $\exists$ succinct efficiently checkable proof of $x \in L$.
2. $L \in \mathsf{coNP}$: $\forall x \notin L$, $\exists$ succinct efficiently checkable proof of $x \notin L$.
3. $L \in \mathsf{NP} \cap \mathsf{coNP}$: ..., has "good characterization". e.g.
   (a) $\mathsf{PERFECT\text{-}MATCHING}$, obviously in NP. Suppose the graph $G = (L, R, E)$, the Hall's Theorem: $\forall S \subseteq L : |N(S)| \geq |S|$ implies G has PM, which is the converse of the intuition: $\exists S \subseteq L : |N(S)| < |S|$ implies G has no PM. Then also $\mathsf{PERFECT\text{-}MATCHING} \in \mathsf{coNP}$. Actually, $\mathsf{PERFECT\text{-}MATCHING} \in \mathsf{P}$.
   (b) A similar question: $\mathsf{LinearProgramming} \in \mathsf{NP} \cap \mathsf{coNP}$, whether it's in P? unknown til now.
   (c) $\mathsf{PRIMES} \in \mathsf{NP}$ is shown in 1975 by Pratt, thus it's also in $\mathsf{NP} \cap \mathsf{coNP}$. It's proven in P.
   (d) $\mathsf{FACTOR} \in \mathsf{NP} \cap \mathsf{coNP}$, here $\mathsf{FACTOR} = \{\langle X, A, B \rangle : X$ has a prime factor between A and $B\}$.

Theorem 1.12. *B is prime iff* $\exists A \in [1, B)$ *s.t.* $A, A^2, A^3, \ldots, A^{B-2} \neq 1 \pmod B$.