

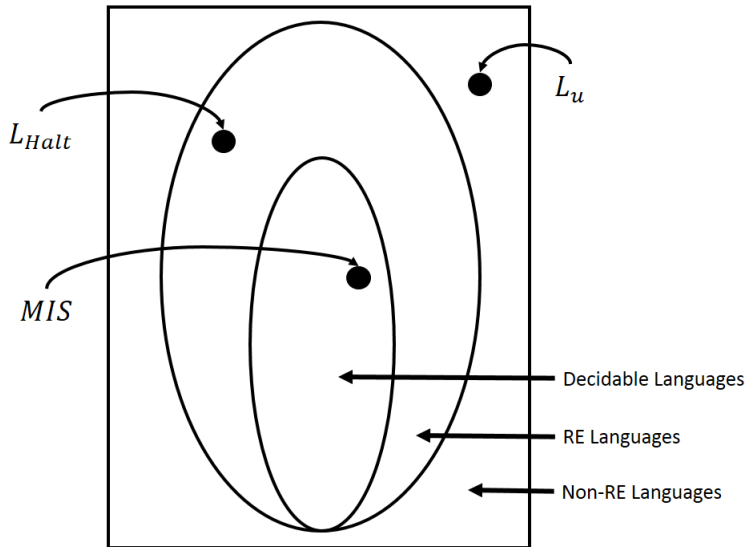
CSL853: Complexity Theory

Ragesh Jaiswal, CSE, IIT Delhi

Complexity Diagram

Complexity Diagram

Our current view of complexity classes



Reduction and NP-completeness

NP-hard and NP-complete

Theorem (Cook-Levin Theorem)

Let SAT be the language of all satisfiable Boolean formulae, then SAT is NP-complete.

Reduction and NP-completeness

NP-hard and NP-complete

Theorem

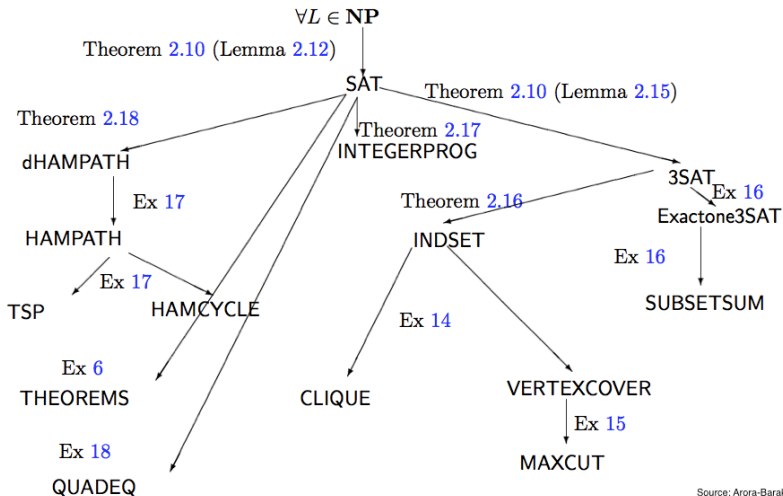
Let $3\text{-SAT} = \{\langle \psi \rangle : \text{s.t. } \psi \text{ is a Boolean formula in 3-CNF form and } \psi \text{ is satisfiable}\}$.
Then 3-SAT is NP-complete.

Theorem

Let $\text{INDSET} = \{\langle G, k \rangle : G \text{ has independent set of size } k\}$. Then INDSET is NP-complete.

Reduction and NP-completeness

NP-hard and NP-complete



Source: Arora-Barak

Search Vs. Decision

- Downward-self reducible: A problem is said to be *downward-self reducible* if the problem instances on inputs of length n can be solved using an algorithm that solves problems instances with input length smaller than n .

Theorem

SAT is downward-self reducible.

Search Vs Decision

- Downward-self reducible: A problem is said to be *downward-self reducible* if the problem instances on inputs of length n can be solved using an algorithm that solves problems instances with input length smaller than n .

Theorem

SAT is downward-self reducible.

Theorem

Suppose that $P = NP$. Then for every NP language L and a verifier TM M for L , there is a polynomial-time TM B that on input $x \in L$, outputs a certificate for x (with respect to the language L and TM M).

co-NP

- If $L \subseteq \{0, 1\}^*$ is a language, then we denote by $\bar{L}$ the *complement* of L . That is, $\bar{L} = \{0, 1\}^* \setminus L$.

Definition (co-NP)

$\text{co-NP} = \{L : \bar{L} \in \text{NP}\}.$

- Is co-NP complement of the class NP?
- Let $\overline{\text{SAT}} = \{\psi : \psi \text{ is not satisfiable}\}$. Let M be an NDTM that decides SAT by non-deterministically guessing the satisfying assignment and then checking. Let $\bar{M}$ denotes the TM M with its output flipped. Then $\bar{M}$ decides $\overline{\text{SAT}}$?
- Is there a language L such that $L \in \text{NP}$ and $L \in \text{co-NP}$?
- Show that: If $\text{NP} \neq \text{co-NP}$, then $\text{P} \neq \text{NP}$.

Definition (co-NP)

co-NP = $\{L : \bar{L} \in \text{NP}\}$.

Definition (co-NP, alternate definition)

For every $L \subseteq \{0,1\}^*$, we say that $L \in \text{co-NP}$ if there exists a polynomial $p : \mathbb{N} \rightarrow \mathbb{N}$ and a polynomial-time TM M such that for every $x \in \{0,1\}^*$,

$$x \in L \leftrightarrow \forall u \in \{0,1\}^{p(|x|)} \text{ s.t. } M(x, u) = 1.$$

Theorem

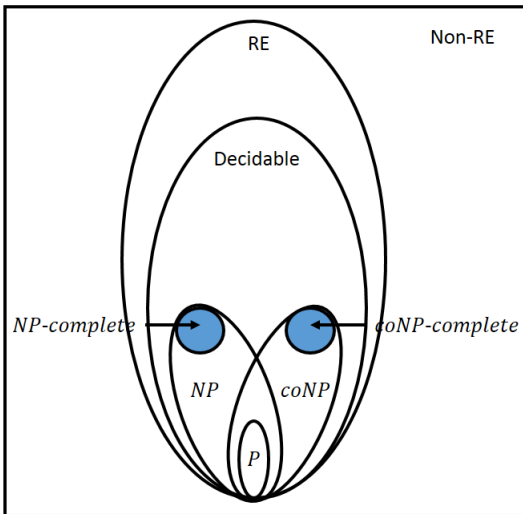
The following language is co-NP-complete:

$$\text{TAUTOLOGY} = \{\psi : \psi \text{ is a tautology}\}.$$

The Complexity Diagram

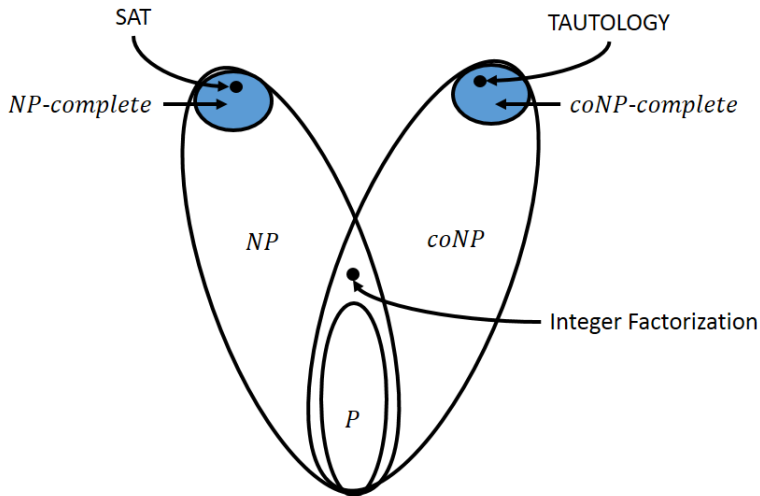
Complexity Diagram

Our current view of complexity classes



Complexity Diagram

Our current view of complexity classes



End