co-Classes

- For a language L we define the co-problem as $\overline{L} := \{0,1\}^* \setminus L$.

- This gives us co-classes as:
$$\text{coNP} := \{\overline{L} \mid L \in \text{NP}\}.$$

- In other words, for a language L in coNP it is "easy" to verify $x \notin L$, for a string x.

- What is the "hardest" problem in coNP?

Defn: $\text{Taut} := \{\phi \mid \phi$ is a DNF formula & ϕ is a tautology$\}$.

Proposition: Taut is coNP-complete.

Proof:
- Given a DNF ϕ we consider the CNF $\neg\phi$.
- $\neg\phi \in$ SAT iff $\phi \notin$ Taut.

$\Rightarrow$ Taut $\in$ coNP. [& $\overline{\text{Taut}} \in$ NP]

- Let $L \in$ coNP. Thus $\exists$ poly-time TM M s.t. $x \notin L$ iff $\exists u \in \{0,1\}^{|x|^c}$, $M(x,u) = 1$.
- Use Cook-Levin's reduction on M to get a boolean CNF $\phi_x(u)$ s.t.
  $x \in \overline{L}$ iff $\phi_x(u)$ is satisfiable.

$\Rightarrow$ $x \in L$ iff $\phi_x(u)$ is unsatisfiable.

$\Rightarrow$ $x \in L$ iff $\neg\phi_x(u) \in$ Taut.

$\Rightarrow$ $L \leq_p$ Taut.

- Thus, Taut is coNP-complete. □

– Open qn: NP $\neq$ coNP? Equivalently, Taut $\notin$ NP?

▷ If coNP $\subseteq$ NP then an alternative to Hilbert's Nullstellensatz shall exist to study systems!

- Proposition: (i) $P = coP \subseteq NP \cap coNP$.

(ii) $P = NP \Rightarrow NP = coNP$.

(Thus, $NP \neq coNP \Rightarrow P \neq NP$.)

(iii) $NP \cup coNP \subseteq EXP$.

NEXP

- It is the nondeterministic version of EXP:

$$\underline{NEXP} := \bigcup_{c \in \mathbb{N}} Ntime(2^{n^c}).$$

- Easily,

▷ $P \subseteq NP \subseteq EXP \subseteq NEXP$.

Theorem: $P = NP \Rightarrow EXP = NEXP$.

Proof: **Idea:** Padding a language.

- Suppose $P = NP$ & $L \in NEXP$.

- Let M be a 2^{n^c}-time NDTM that

accepts L.

- Consider the <u>padded</u> version of L:

$$L' := \{(x, 0^{2^{|x|^c}}) \mid x \in L\}.$$

- $L' \in NP$. ($\because$ any $x' \in L'$ can now be accepted by the NDTM M in time $poly(|x'|)$.)

- By the hypothesis $L' \in NP = P$.
  Say, $L' \in Dtime(n^d)$.

$\Rightarrow$ For an x, we can decide $x \in L$ in time $O((|x| + 2^{|x|^c})^d)$.

$\Rightarrow$ $L \in EXP$

$\Rightarrow$ $NEXP = EXP$. □

- <u>OPEN</u>: What about the converse?

- Where to place NEXP ?

Defn: $\underline{EEXP} := \bigcup_{c \in \mathbb{N}} Dtime(2^{2^{n^c}})$.

▷ $EXP \subseteq NEXP \subseteq EEXP$.

and so on .....

Gödel's computation qn.

- $\underline{Thms} := \{(\phi, 1^n) \mid \phi$ is a math. statement with a proof of length $\leq n\}$.

- Since it is "easy" to verify a proof:

▷ $Thms \in NP$.

- If $P=NP$ then every math. statement can be "easily" resolved.

No need for mathematicians!