0.1 Motivation

Before introducing proof systems and discussing their complexity, we must clarify the underlying motivation. Let's consider two common complexity class NP and coNP. Because all deterministic time complexity classes, i.e. P, are closed under complementation, one possible way to prove P $\neq$ NP is by proving NP is not closed under complementation, which means starting with NP $\neq$ coNP. We already know that TAUT is coNP-complete. Naturally, we have:

Theorem 0.1. NP *is closed under complementation if and only if* TAUT *is in* NP.

The question of whether TAUT is in NP is equivalent to whether there is a propositional proof system in which every tautology has a short proof. In other words, we can view a proof system as a verifier. If the proposition is tautology, there exists a proof such that all steps in it stay consistent with the proof system which means pass the verification. If both proof system and proof are properly defined, we can believe that searching adequate proof can be simulated in NTM and such proof can be verified in polynomial time TM.

Definition 0.1. *If $L \subseteq \Sigma^*$, a proof system for L is a function $f : \Sigma_1^* \to L$ for some alphabet Σ_1 and f such that f is a surjective function. We say that the proof system is polynomially bounded iff there is a polynomial $p(n)$ such that for all $y \in L$ there is $x \in \Sigma_1^*$ such that $y = f(x)$ and $|x| \leq p(|y|)$.*

Because computing function $f(x)$ actually only requires verifying whether each step in the proof x conforms to the rules of reasoning and the size of rules is finite, we can compute $f(x)$ in $O(|x|)$. Therefore, we should focus on $|x|$. [**TBD:** A natural question is why we need different proof system. I think it's hard to proof any kind of problem using only one proof system. Can I take an example? But some proof system may have stronger power than others, does it mean if we have to restrict what system we use the proof complexity cannot perferctly capture the difficulty?] Additionally, a set L is in NP if L has a polynomially bounded proof system where proof system could be any possible one because any bounded proof system can be simulated by a NTM, and the computation steps on NTM to decide a language L is in NP forms a proof! Then we can answer whether TAUT is in NP by giving a polynomially bounded proof system.

Theorem 0.2. *A set L is in* NP *iff $L = \emptyset$ or L has a polynomially bounded proof system.*

[**TBD:** Why there is a case $L = \emptyset$?] [**ToLearn:** Recursive function theory: recursively enumerate set]

0.2 Concrete Definitioin