1

(Sipser 9.12) Describe the error in the following "proof" that $P \neq NP$. Assume that $P = NP$, then $SAT \in P$ and so for some $k, SAT \in TIME(n^k)$. Because every language in NP is polynomial time reducible to SAT, you have $NP \subset TIME(n^k)$. By the time hierarchy theorem, $TIME(n^{k+1})$ contains a language that is not in $TIME(n^k)$, which contradicts $P \subset TIME(n^k)$. Therefore $P \neq NP$

> The error in this proof comes in the line that "every language in NP is polynomial time rediculble to SAT, then $NP \subset TIME(n^k)$". While it is true that every language is in NP is polynomial time reducible to SAT, it is not guarenteed that the function f that reduces L to SAT is less than n^k. The correct conclusion to their sentence is $NP \subset TIME(O(f(n)+n^k))$. This then makes their following argument incorrect because we cannot determine if $TIME(O(f(n) + n^k)) \subset TIME(n^{k+1})$ because $f(n)$ is not a constant term for all languages in NP.

2

Prove that $USAT \in P^{SAT}$

3

Prove that an oracle C exists for which $NP^C \neq coNP^C$

> Suppose we have language $L = \{w | \exists x \in C \wedge |x| = |w|\}$
>
> The compliment of this language is $\bar{L} = \{w | \forall x \notin C \vee |x| \neq |w|\}$
>
> Let M_L be a NTM that decides L, we need to prove that M_L halts in polynomial time.
>
> M_L simply guesses a string x with size $|x| = |w|$ and accepts or rejects if oracle accepts or rejects. $M_L \in TIME(n)$ because constructing a guess x is $O(n)$ and the guess itself is constant time. If $w \in L$ then M_L will guess $x \in C$ and accept because C accepts x. If $w \notin L$ then M_L will guess a random x and reject because $x \notin C$.
>
> Therefore $L \in NP^C$ because there exists an oracle NTM that decides it in polynomial time.
>
> Since $L \in NP^C$ then $\bar{L} \in coNP^C$

Now we need to show that $\bar{L}$ cannot be decided in polynomial time by an NTM.

Suppose $\bar{L} \in NP$ then $\exists$ NTM $M_{\bar{L}}$ that decides $\bar{L}$ in polynomial time.

Remember $\bar{L}$ accepts all strings w for which there is no string of equal size in C. However the number of strings of equal size to w is $O(2^n)$ which is the number of queries we would need to make to C in order to accept.

Therefore since $M_{\bar{L}}$ can make up to $O(n^k)$ queries it will not be able to say with certainty whether or not a string w is in the language.

Therefore $\exists C(NP^C \neq coNP^C)$

4

Prove that in an interactive proof, if the verifier is required to be a deterministic, polynomial time algorithm with no access to random bits, then the class of languages this system can decide is equal to NP, even if we allow an arbitrary number of queries to the prover.