Alin Tomescu, *6.840 Theory of Computation (Fall 2013)*, taught by Prof. Michael Sipser

Oracles

Notation: M^B denotes the oracle TM M with oracle access to problem B (constant time solver for B)

Notation: $P^B = \{A \mid A \text{ is poly} - \text{time decidable with an oracle for } B\}$

Theorems

$\exists A, B$ such that $P^A = NP^A$ and $P^B \neq NP^B$ (contradictory relativizations)

Part I: Prove that $P^A = NP^A$ for $A = TQBF$

$NP^{TQBF} \subseteq NPSPACE^{TQBF}$ because $NP \subseteq NPSPACE$, and $TQBF \in NPSPACE$

Also, $NPSPACE^{TQBF} \subseteq NPSPACE$ because a TQBF oracle is useless in NPSPACE, where you can just solve the problem. So, $NP^{TQBF} \subseteq NPSPACE$.

Savitch's theorem tells us that $NPSPACE = PSPACE$, and with a $TQBF$ oracle in P we can solve any PSPACE problem so $NPSPACE = PSPACE \subseteq P^{TQBF} \subseteq NP^{TQBF}$

Thus, we have $NP^{TQBF} \subseteq NPSPACE \subseteq P^{TQBF} \subseteq NP^{TQBF} \Rightarrow P^{TQBF} = NP^{TQBF}$

Part II: Prove that $P^B \neq NP^B$ for $A = \emptyset$, because an "empty" oracle will not give much power to P, assuming $P \neq NP$ (I think more complicated proof for $P = NP$ can be found in textbook).

$NP \subseteq P^{SAT}, coNP \subseteq P^{SAT}$

Note that now you can just flip the answer to the SAT oracle so in effect you also have an $UNSAT$ oracle, thus $coNP \subseteq P^{SAT} = P^{UNSAT}$

$NP \subseteq P^{NP}$

Not sure of the notation P^{NP}, but if it means "P with oracle access to all languages in NP" or "with oracle access to an NP-complete language", then it's obvious that $NP \subseteq P^{NP}$, since $\forall A \in NP$ we can use the NP-complete oracle to solve it in P.

Open problems

$$NP \neq NP^{NP} \text{ (believed)}$$

$$coNP \neq NP^{NP} \text{ (believed)}$$

$P^{SAT} \subseteq NP \cup coNP$ is unknown because it would imply $NP = coNP$, since $NP \cup coNP \subseteq P^{SAT}$

Is NP^{SAT} closed under complement?

Is $P^{SAT} = NP^{SAT}$?