Homework 20

Joe Baker, Brett Schreiber, Brian Knotten

March 12, 2018

32

a

First, it must be proven that $IP' \subseteq IP$. Every time the verifier would ask the prover a question, instead, ask it n times. n can be so large, (say, 1000), that the probability gets so high that one of the responses is guaranteed to be true. And thus we have a deterministic prover and $IP' \subseteq IP$

Next, it must be proven that $IP \subseteq IP'$. Any IP protocol is also IP', because the definitions match in every way, except the prover's chance of success. But a deterministic prover's chance of an accurate response $= 1 > 2/3$. Therefore we have $IP \subseteq IP'$ and $IP' = IP$

b

Prove that $IP \subseteq PSPACE$.
Consider that an exponential number of proofs can be searched for in a proof tree using polynomial space by checking one branch at a time. Similarly, for any verifier V in an IP problem, a $PSPACE$ prover can be the prover that considers all possible sequences of messages that the verifier could send. The prover considers one branch of messages at a time using only a polynomial amount of space. So the prover is in $PSPACE$.

c

$IP' \subseteq IP$, because any language in IP' trivially meets the same requirements for completeness and soundness for IP.

$IP \subseteq IP'$, because you can ask for enough advices such that one of the advices causes V to accept x. Again, this uses the probabilistic method as in our other proofs. Thus, $IP' = IP$.

d

To show that $NP \subseteq IP'$, have the prover send the advice that causes the verifier to accept. This works deterministically with probability of accepting correct inputs $1 > 2/3$, and probability of rejecting incorrect inputs 0. So $NP \subseteq IP$.

To show that $IP' \subseteq NP$, ask the prover n times. Again, n can be so large that the probability gets so high that one of the responses is guarunteed to be true. And thus we have a deterministic prover. That is, one of the advices can be used in an NP problem to decide L. Therefore $IP' = NP$.

33

It is trivial to prove that $IP' \subseteq IP$, since given that a prover P in IP' for all $x \in L$, then for each $x \in L$ there exists a prover, specifically, P.

Next it must be proven that $IP \subseteq IP'$. Consider a prover P which is $\bigcup_{i=0}^{n} P_i$ where P_i is a prover for $x \in L$. All these P_i are given from the definition of IP. Therefore $IP' = IP$.

34

First, it must be proved that $BP \cdot NP \subseteq AM$ [2]. Given a language $L \in BP \cdot NP$, let L be the subject to an interactive proof. So the prover and verifier both have access to a given string x, and the prover P has to prove to the verifier V that $x \in L$. Since $L \in BP \cdot NP$, there exists a certain set of advice which can cause a reducer R to successfully reduce x into an instance of 3SAT, x'. The prover has an unlimited amount of time to try different advices and successfully reduce x into x'. Then, the prover can send over the reduction and the verifier can perform it. The prover can then decide the satisfiability of x' and send over the satisfying assignments to the verifier.