# Homework 20

Austin Frownfelter Matthew Bialecki

February 12, 2018

## 1 Problem 32

### 1.1 Part a

Prove IP' = IP

Let L be an arbitrary language in IP'.
$\exists$ BPP verifier
$\exists$ probabilistic prover
The prover-verifier protocol is run, with the end result having the verifier accepting or rejecting if the prover's strategy is correct or not. Instead of halting here, run the protocol a polynomial number of times and output the majority (i.e. boost the result to near-certainty).
This runs in a polynomial number of steps, thus it runs in polynomial time.
Therefore, L $\in$ IP.

This is true for all languages in IP', therefore IP' = IP.

### 1.2 Part b

Prove IP $\subseteq$ PSPACE.

The Prover may use unbounded computational power to prove the string is in the language. However, there exists some optimal prover for a given verifier V, which we can find in polynomial space.

To find the optimal prover, recursively iterate over all possible communications between the prover and the verifier. We will use the best P such that V will accept iff P can prove x is in the language.

To recursively iterate over all communications, do a depth-first search to find the best path that yields an accept result. Since by definition of IP, there are a polynomial number of questions from the verifier, there is a polynomial depth to this tree. The size of the resulting path would be polynomial, since the path itself would have values on the order of exponential.

As a result, the prover can be polynomial size, therefore IP $\subseteq$ PSPACE.

### 1.3 Part c

Prove IP' = IP

Let L be an arbitrary language in IP'. The probability a TM that decides L accepts if x∈L = 1, which is greater than $\frac{2}{3}$. Thus, L $\in$ IP.

Let L be an arbitrary language in IP. Boost the TM that decides L to drive the probability it is correct if x∈L to 1-$\frac{1}{4^n}$. Then, use the strategy from the proof that BPP $\in \Sigma_2^p$ to marry k results from that TM. There must exist some sequence of weddings such that the result will always be correct if x∈L.

Thus, L $\in$ IP'. Therefore, IP' = IP.

### 1.4 Part d

Prove IP' = IP

Let L be an arbitrary language in NP. The probability a TM that decides L is correct is 1, which is greater than the probabilities of IP'. Therefore, L $\in$ IP'.

Let L be an arbitrary language in IP'. Boost the TM that decides L to drive the probability it is correct when x $\in$ L from $\frac{2}{3}$ to $1 - \frac{1}{4^n}$. Do the marriage strategy like in Part c, to make certain the result is correct.

Thus, L $\in$ NP. Therefore, IP' = NP.

## 2 Problem 33

If for every x $\in$ L there exists a prover, then we can find that prover when that x occurs. We can construct a prover P which includes all of those provers, which will satisfy all strings x $\in$ L.

## 3 Problem 34

Prove AM = BP.NP

Prove AM $\subseteq$ BP.NP

The AM protocol states V sends random bits to M, which then sends an advice string which V should use to accept or reject. The probability V accepts is $\geq \frac{2}{3}$ if x $\in$ L and $\leq \frac{1}{3}$ if x $\notin$ L.

With these values r, the random question, and x, the input, there exists some function which is the randomized reduction from the language to 3SAT. If x $\in$ L, then the probability the randomized reduction is in 3SAT is $\geq \frac{2}{3}$, otherwise it is $\leq \frac{1}{3}$.

Therefore, AM $\subseteq$ BP.NP.

Prove BP.NP $\subseteq$ AM

There exists some function which constructs a randomized reduction from L to 3SAT. V sends a random message to M, which M then uses to construct a valid randomized reduction from L to 3SAT. If the reduction is actually valid, V accepts with probability $\geq \frac{2}{3}$, otherwise it accepts with probability $\leq \frac{1}{3}$.

Therefore, BP.NP $\subseteq$ AM.

Therefore, AM = BP.NP