Mandatory Excercise 3

Computationally hard problems

September 21, 2015

Troels Thomsen `152165`

Solution discussed with Rasmus Haarslev `152175`

1 Excercise 3.1

1.1 Proof $RP_{1/\pi} = RP$

We consider it trivially true that an algorithm which can solve problems of class RP, can also solve problems of class $RP_{1/\pi}$. In order to prove the equality between these two classes, we must prove the inverse relationship.

To do this we consider a randomized algorithm A bounded by a polynomial p, which solves problems of class $RP_{1/\pi}$.

If we repeat the algorithm A x number of times on the same input, we will eventually reach a probability of $\frac{1}{2}$ or greater, enabling algorithm A to solve problems in RP after x tries. This turns out to be $x \geq 2$ times, since

$$\sum_{n-1}^{x} \frac{1}{\pi} \geq \frac{1}{2}$$

solves to $x \geq \frac{\pi}{2}$.

Thus if we run A twice we can solve problems of class RP, with A bounded by a polynomial of size $2p$. But since $O(2p) = O(p)$, A is actually still bounded by p, and thus A can also solve problems of class RP.

Thus if an algorithm which can solve problems of class $RP_{1/\pi}$ can also solve problems of class RP within the same bounds, the problems in $RP_{1/\pi}$ and RP must be of the same complexity rendering $RP_{1/\pi} = RP$.

1.2 Proof $RP \subseteq BPP$

In order to proof our assumption that $RP \subseteq BPP$, we consider a randomized algorithm A bounded by some polynomial p, which can solve problems of class RP.

Since A can solve problems of class RP, we can we repeat the algorithm A some number $x > 1$ times on the same problem, and find a true answer with a higher probability than $\frac{1}{2}$. We consider the new probability for finding the true answer to our problem to be $\frac{1}{2} + \epsilon$, where ϵ is some constant > 0. We consider it trivial that A can also find the true answer no to a problem with a probability of $\frac{1}{5} + \epsilon$ or higher, since A is able to solve RP problems.

By repeating A we increase the running time from p to $x \times p$. Since $O(x \times p) = O(p)$ we notice that our algorithm A in this case is in fact still a p-bounded algorithm.

Since ϵ is not bounded by the input, but rather by the number of times our algorithm is run, we can state that A repeated x times is in fact a randomized p-bounded algorithm able to solve problems of class BPP. If A can solve problems of both class RP and BPP then it must be true that $RP \subseteq BPP$.