

Lecture Notes for CT06, 4/10-2006

Peter Sebastian Nordholt

October 27, 2006

In the last lecture we covered relativizable proof techniques. Among other things we showed that since both of the following points are true:

- $\exists A : \mathbf{P}^A = \mathbf{NP}^A$
- $\exists A : \mathbf{P}^A \neq \mathbf{NP}^A$

We can not hope to solve the \mathbf{P} vs. \mathbf{NP} question using relativizable proof techniques.

This lecture we first show a non-relativizable proof of a theorem by Meyer and then go on to start on randomized computation.¹

1 Non-relativizability of Meyer's theorem

Theorem 1.1 (Meyer). $\mathbf{EXP} \subseteq \mathbf{P}/poly \Rightarrow \mathbf{EXP} = \Sigma_2^P$

Proof. Assume $\mathbf{EXP} \subseteq \mathbf{P}/poly$. Let the language $L \in \mathbf{EXP}$ be given. We want to design a two player, polynomial time game s.t. given x Player1 wins the game iff $x \in L$. The game will have only two moves with Player1 moving first. If such a game exists we know by definition of Σ_2^P that $L \in \Sigma_2^P$. Let M be a one-taped turingmachine deciding L in \mathbf{EXP} time. We use the tableau-method to build a tableau of each cell of M 's tape at each timestep of M 's computation. Using this tableau we define the language L_M :

Definition 1.1. $(x, j, t, k) \in L_M \Leftrightarrow$ cell j (of M 's tape) at time t when M computes on input x has a boolean representation where the k 'th bit is 1.

Since $L \in \mathbf{EXP}$ we have that $L_M \in \mathbf{EXP}$ and thus by our initial assumption $L_M \in \mathbf{P}/poly = \mathbf{PSIZE}$.

By (j, t) we will mean the j 'th cell of M 's tape at time t when computing on x . Remember that (j, t) is determined by the three cells $(j - 1, t - 1)$, $(j, t - 1)$ and $(j + 1, t - 1)$. The game on input x then goes as follows:

- Player1 writes down a circuit C for L_M on input of size corresponding to x

¹the second part is covered in slides

- Player2 Tries to point out that this is not a correct circuit, if he does so he is declared the winner. He does this by using C to find a pattern of cells (j, t) , $(j - 1, t - 1)$, $(j, t - 1)$ and $(j + 1, t - 1)$ so that (j, t) is incorrect given the other cells.
- If Player2 fails, a turing machine then checks to see if $C(x, 1, T, *)$ is an accepting state, T being the exact running time of M on x . If it is Player1 is declared to be the winner otherwise Player2 wins.

Now if $x \in L$ Player1 can simply write the correct circuit (which is guaranteed to be possible since $L_M \in \mathbf{PSIZE}$) to win. On the other hand if $x \notin L$, Player1 is forced to write a incorrect circuit C in order to make the turing machine at the end answer yes. Player2 can detect this by simply examining the right cells and thus Player1 has no winning strategy in this case. \square

The next theorem however shows that theorem 1.1 does not relativize:

Theorem 1.2 (Impagliazzo). $\exists A : \mathbf{EXP}^A \subseteq \mathbf{P}^A / poly$ but $\mathbf{EXP}^A \neq \sum_2^{p^A}$

We did not prove this but we noted that the proof we gave for theorem 1.1 would not hold for the relativized version of the theorem since Player2 would not be able to do his check when exponentially long questions were answered by the oracle.