Homework 2

Out: *March 12* Due: *March 27*

You are encouraged to collaborate with your classmates, but be sure to list your collaborators with your answers and write your final solutions on your own. (Note that no credit is lost due to collaboration.) Remember: False proofs cause brain damage. Do not ever attempt to write down a proof that you are unsure about. It is better to write down your thoughts, and point out where you are stuck. Please be concise in your answers. If you suspect a problem is open, just say so and give reasons for your suspicion.

§1 Show that for each $k > 0$ there is a language in **PH** that is not decidable by circuits of size n^k.

§2 Show that computing the permanent of an integer matrix is in $FP^{\#P}$.

§3 Show that $\mathbf{AM}[2] \subset \mathbf{NP}/\text{poly}$. Show that if $\overline{SAT} \in \mathbf{NP}/\text{poly}$, then the polynomial hierarchy collapses to Σ_3^p. Note that this means **coAM** cannot contain **NP**-hard problems unless the hierarchy collapses.

§4 Give an example of an **AM** protocol for which the obvious method of converting it to a 2-round protocol provably fails to be sound: By the obvious method, we mean the one discussed in class: Concatenate all the (random) Verifier messages into the first message; and concatenate all the prover responses in the second message.

§5 Prove a version of the **AM** collapse theorem: Show that for all constants k, we have $\mathbf{AM}[2k+2] \subset \mathbf{AM}[2k]$. (This problem is mildly tricky; give yourself enough time to think about it.)