# Assignment 5: Computational Complexity

Due date: Tuesday 29 April *before* the class starts.
If you are presenting a project on 29 April, you can submit by Friday 2 May.

1. (15) In class we defined a one-way functions as: $f\colon \{0,1\}^* \to \{0,1\}^*$ is a one-way function iff it is computable in polynomial time and for every probabilistic polynomial time (PPT) algorithm $A$ and sufficiently large $n$ it holds that

$$\Pr_{x \leftarrow \{0,1\}^n}[f(A(y)) = y \mid y = f(x)] < 1/2.$$

   Prove that OWFs exist if and only if the following statement is true:

   - (*) There is an efficient randomized algorithm $G$ that only gets randomness $r$ as its input, runs in time $poly(|r|)$ and outputs $(F, x)$ such that: $y$ is a 3CNF formula and $x$ is a satisfying assignment for $F$ (namely $F(x) = 1$). Also, for any PPT $A$ and sufficiently large $n$ it holds that

$$\Pr_{r \leftarrow \{0,1\}^n}[F(A(y)) = 1 \mid (x, y) = G(r)] < 1/2.$$

     Namely, we can "generate" 3CNF instances *together* with a solution for them such that no efficienet algorithm can solve them with probability better than half when this probability is also over the randomness of generating the 3CNF formula. In particular, no algorithm can solve more than half of the generated instances. This is known as "average-case" hardness.

   Proving "OWF $\Rightarrow$ (*)" has 5 points and proving "(*) $\Rightarrow$ OWF" has 10 points.

2. Problem 11.6 from the book. For this you might read Def 11.4 from the book, but for sake of completeness here I give a self-contained description of this problem in terms of how we defined PCPs in class. Suppose $L$ is a language that has a PCP. Suppose the proof is Boolean; namely, the proof oracle $\pi$ for $x \in L$ is a (perhaps exponentially long) string of zeros and ones, and the verifier can choose to read any bits from $\pi$. Equivalently, considering $\pi$ as an oracle, the answers returned by $\pi$ are Boolean. Assuming the verifier of the PCP is *deterministic* prove the following:

   (a) (5) $L \in NP$. Hint: note that the verifier cannot read more than a polynomial number of the bits of the (possibility exponentially long) proof $\pi$ anyway. What would be a natural "witness" and "verifier" for proving $x \in L$ ?

   (b) (10) If the verifier reads only $O(\log n)$ bits from the proof, then $L \in P$. Hint: how many total possible answers might the verifier receive from the proof oracle?

3. (10) Recall the notion of zero-knowlege proof systems as we defined in class (namely: for any malicious verifier $V^*$ there exists a simulator $S$ running in polynomial time who simulates the "view" of $V^*$ interacting with the honest prover $P$ whenever $x \in L$). Prove that if $L$ has a "one-message" zero-knowledge protocol (in which there is only one message going from prover

to the verifier) then $L \in P$. Hint: try to use the simulator and the soundness properties both to decide $L$ in polynomial time.

(Note: no 2-message protocol could be zero-knowledge unless $L \in P$ but that is a bit harder.)

4. Suppose we define class $IP$ by allowing error on both sides. Namely $L \in IP$ if there is an interactive randomized poly-time verifier $V$ and a (possibly inefficient) prover $P$ such that:

   - If $x \in L$ then $V(x)$ accepts interaction with $P(x)$ with probability $\geq 2/3$.
   - If $x \notin L$ then $V(x)$ rejects interaction with any $P^*(x)$ with probability $\geq 2/3$.

   Our goal in this problem is to show that the errors can be made arbitrary small by repetition.

   Suppose $V^k$ and $P^k$ are a verifier and a prover that run the original protocol $V$ and $P$ $k$ times (with independent randomness) and $V^k$ accepts at the end, if at least $k/2$ of the executions of $V$ accept.

   (a) (5) Completeness: Use Chernoff-Hoeffding bound, as defined in class, to prove that if $x \in L$ then $V^k(x)$ accepts interaction with $P^k(x)$ with probability at least $1 - 2^{-k/100}$.

   (b) (10) Soundness: The following is a generalization of the Chernoff-Heffding bound:

   - Let $Y_1, \ldots, Y_k$ be a sequence of possibly *correlated* Boolean random variables. Suppose for any $1 < i \leq k$ and any Boolean values $y_1, \ldots, y_{i-1}$ it holds that

   $$\Pr[Y_i = 1 \mid Y_1 = y_1, \ldots, Y_{i-1} = y_{i-1}] \leq \rho.$$

   Let $Y = \frac{1}{k} \cdot \sum_i Y_i$ be the average of $Y_i$'s. Then it holds that: $\Pr[Y > \rho + \epsilon] < 2^{-k\epsilon^2}$.

   Now let $P^*$ be an arbitrary prover who interacts with $V^k$ (and might use a correlated strategy for its $k$ interactions with $V^k$, as opposed to $P^k$ who runs $k$ independent executions). Prove that if $x \notin L$ then $V^k$ rejects the interaction with $P^k$ with probability at least $1 - 2^{-k/100}$.

   (c) (5) Explain briefly why we could not use the original form of Chernoff-Hoeffding (in which $Y_i$'s are assumed to be independent) to prove that the soundness error decreases.

5. Extra credit (10): read the definition of classes $AM$ and $MA$ from the manual to assignment 4 and show that $MA \subseteq AM$.