cs579: Computational Complexity Assigned: *Mon., Mar. 5, 2018*

Problem Set #4

Prof. Michael A. Forbes Due: *Mon., Mar. 26, 2018 (3:30pm)*

1. Let $\ell : \{0,1\}^\star \to \mathbb{N}$ be a *length* function, meaning that $\ell(x)$ is computable in $\mathsf{poly}(|x|)$ time and $\ell(x) \leq \mathsf{poly}(|x|)$. A function $f : \{0,1\}^\star \to \{0,1\}^\star$ is *downward self-reducible* with respect to ℓ if

   - If $\ell(x) = 0$ then $f(x)$ is computable in $\mathsf{poly}(|x|)$ time.
   - In general, x can be computed in $\mathsf{poly}(|x|)$ time given oracle access to f on inputs $\{y : \ell(y) < \ell(x)\}$.

   Prove that

   (a) Prove that SAT is downward self-reducible with respect to $\ell(\varphi)$ being the number of variables in φ.

   (b) Show that computing the number of perfect matchings of a graph is downward self-reducible with respect to some natural length function.

   (c) (Arora-Barak Problem 8.9) Any downward self-reducible function is computable in $\mathsf{poly}(|x|)$ space (ie, PSPACE when f is a language).

2. Let $\mathbb{F}_2 = \{0,1\}$ be the field of two elements. A matrix $A \in \mathbb{F}_2^{k \times n}$ is *Toeplitz* if it is constant on diagonals, that is, $A_{i+1,j+1} = A_{i,j}$ for all $0 \leq i < k$ and $0 \leq j < n$. Let $\mathrm{Toep}(\mathbb{F}_2^{k \times n})$ be the set of all such Toeplitz matrices. Define the hash function $h : \mathbb{F}_2^n \times (\mathrm{Toep}(\mathbb{F}_2^{k \times n}) \times \mathbb{F}^k) \to \mathbb{F}_2^k$ by $h(x,(A,b)) = Ax + b$. Show that h is a pairwise independent hash family. That is, when A and b are chosen uniformly at random, for any $x \neq y \in \mathbb{F}_2^n$ and $c, d \in \mathbb{F}_2^k$,

$$\Pr_{\mathsf{A} \in \mathrm{Toep}(\mathbb{F}_2^{k \times n}), \mathsf{b} \in \mathbb{F}_2^k} [h(x,(\mathsf{A},\mathsf{b})) = c \wedge h(y,(\mathsf{A},\mathsf{b})) = d] = \frac{1}{2^{2k}} .$$

3. A language $L \subseteq \{0,1\}^\star$ is in AM if there is a $\mathsf{poly}(|x|)$-time machine $M(x,y,z)$ such that for $x \in L$

$$\Pr_{y \in \{0,1\}^{p(|x|)}} [\exists z \in \{0,1\}^{q(|x|)} M(x,y,z) = 1] \geq \frac{2}{3}$$

   for some polynomials $p(|x|)$ and $q(|x|)$. For $x \notin L$, this probability is at most $\frac{1}{3}$. A language $L \subseteq \{0,1\}^\star$ is in MA if for $x \in L$

$$\exists y \in \{0,1\}^{p(|x|)} \Pr_{z \in \{0,1\}^{q(|x|)}} [M(x,y,z) = 1] \geq \frac{2}{3}$$

   while for $x \notin L$ this probability is at most $\frac{1}{3}$ for *all* y.

   Show that $\mathsf{MA} \subseteq \mathsf{AM}$.

4. Say that a language $L \subseteq \{0,1\}^\star$ is in AM_δ if there is a $\mathsf{poly}(|x|)$-time machine $M(x,y,z)$ such that for $x \in L$

$$\Pr_{y \in \{0,1\}^{p(|x|)}}[\exists z \in \{0,1\}^{q(|x|)} M(x,y,z) = 1] \geq \frac{1}{2} + \delta$$

for some polynomials $p(|x|)$ and $q(|x|)$. For $x \notin L$, this probability is at most $\frac{1}{2} - \delta$. Thus, $\mathsf{AM}_{\frac{1}{6}}$ is the usual definition of AM.

Show that $\mathsf{AM}_{\frac{1}{\mathsf{poly}(n)}} = \mathsf{AM}_{\frac{1}{2} - \frac{1}{2^{\mathsf{poly}(n)}}}$.

Some hints.

4. Repeat the AM protocol in parallel k times. Note that the prover *can* respond in a way which depends on *all* k challenges. However, argue that an *optimal* prover can respond to each challenge individually. Then use a standard error-reduction argument.