Computer Science 468/568
Homework #8, due in class Thursday, April 12, 2018.

1. (10 points) Please list any persons (including course staff) you talked with about this assignment and cite any resources (other than the textbook) you consulted in connection with this assignment (with enough information that another person could find the materials you cite).

2. (30 points) This is an alternate construction of a pairwise independent family of hash functions $H_{n,k}$ mapping $\{0,1\}^n$ to $\{0,1\}^k$. Let F be the field $\{0,1\}$, where addition is modulo 2. Then we can consider a string $x \in \{0,1\}^n$ as a vector of dimension n over F. The functions in $H_{n,k}$ are specified by choosing a matrix A of dimension $k \times n$ and a vector b of dimension k over F. Then, for any vector x of dimension n over F,

$$h_{A,b}(x) = Ax + b.$$

   Prove that for any distinct vectors x, x' of dimension n over F and any vectors y, y' of dimension k over F, if we choose $h_{A,b}$ uniformly at random,

$$\Pr[(h_{A,b}(x) = y) \wedge (h_{A,b}(x') = y')] = 2^{-2k}.$$

   Also show that this construction wouldn't work if we left out the vector b.

3. (30 points) For this problem and the next, we consider a language $L \in \mathbf{MA}$ such that $p(n)$ is a polynomial and M is a deterministic polynomial time Turing machine such that

$$\text{if } x \in L \text{ then } \exists y \in \{0,1\}^{p(|x|)} \Pr[M(x,y,r) = 1] \geq 2/3$$
$$\text{if } x \notin L \text{ then } \forall y \in \{0,1\}^{p(|x|)} \Pr[M(x,y,r) = 1] \leq 1/3,$$

   where in each case the probability is for r chosen uniformly at random from $\{0,1\}^{p(|x|)}$. This corresponds to a two-round interactive protocol where Merlin (the prover) sends the first message y, then Arthur (the verifier) chooses a string r at random and uses $M(x,y,r)$ to decide whether to accept or not.

   Prove that $L \in PSPACE$ by giving and analyzing a polynomial space algorithm to decide L.

4. (30 points) (We use the L, p and M defined in the previous problem.) Consider the following protocol with input $x \in \{0,1\}^*$.

V chooses $r_1, r_2, \ldots, r_m$ uniformly and independently at random from $\{0,1\}^{p(|x|)}$ and sends them to P.

P chooses some $y \in \{0,1\}^{p(|x|)}$ and sends it to V.

V computes $M(x, y, r_i)$ for $i = 1, 2, \ldots, m$ and outputs 1 if at least $m/2$ of the results are 1, else outputs 0.

Prove that there exists a polynomial $q(n)$ such that if m is set to $q(|x|)$ in the above protocol, then the resulting V shows that $L \in \mathbf{AM}$. (Then we can conclude that $\mathbf{MA} \subseteq \mathbf{AM}$.)

5. (10 points) This problem is required of students enrolled in CPSC 568, but not of students enrolled in CPSC 468.

   Write a brief (at most one paragraph) progress report for your final paper. Recall that a complete preliminary draft is due April 19 in class.