

Due Dec 3

COURSE WEBSITE: "http://www.cs.umd.edu/gasarch/652/652.html"

1. (10 points) What is your name? If you were a movie star, what would be your stage name? When is the final? Where is the final?
2. Recall that AM was defined with PUBLIC COINS. What if the coins are private? We define AM^{priv} which involves private coins. We first describe it informally and then formally. Informally: On input x , Arthur flips coins to get a random string r and then *computes a function* $f(x, r)$, sends Merlin $f(x, r)$, and Merlin has to respond. Note that Merlin does not know r , just $f(x, r)$. f is many-to-one so Merlin really cannot deduce r even if he is all powerful.

We can now define AM^{priv} rigorously.

A set A is in AM^{priv} if there exists $V \in P$, an function f in P , and a polynomial p such that, for all x of length n ,

$$x \in A \Rightarrow \text{Prob}_{r \in \{0,1\}^{p(n)}}[(\exists^p y)[V(x, y, f(x, r))]] \geq 1 - \frac{1}{2^n}$$

$$x \notin A \Rightarrow \text{Prob}_{r \in \{0,1\}^{p(n)}}[(\exists^p y)[V(x, y, f(x, r))]] \leq \frac{1}{2^n}$$

(As usual the error probabilities can be reduced.)

(NOTE: What I call AM^{priv} is usually called $IP[2]$ in the literature.)

- (a) (30 points) Show that $AM = AM^{\text{priv}}$.

(HINT: Do not try to look this one up in the literature. The relevant paper proves something much more general and is unneeded here.)

- (b) (30 points) Informally, AMA^{priv} means that Arthur sends, then Merlin sends, Arthur flips coins to verify. Define this rigorously.

(HINT: Do not try to look this one up in the literature. Nobody defines this term, though they do use it.)

- (c) (30 points) Show that $AMA^{\text{priv}} = AM^{\text{priv}}$.