Due: November 17th, 2017
Date: November 7, 2017

Assignment 5

You must submit it electronically to ELMS. This is a group assignment. Every group only needs to submit one solution. Group members get the same credit for the group submission.

This assignment is 7% in your total points. For the simplicity of the grading, the total points for the assignment is 70.

Problem 1 [20 pts]. Let $k \leq n$. Prove that the following family $\mathcal{H}_{n,k}$ is a collection of pairwise independent functions from $\{0,1\}^n$ to $\{0,1\}^k$: identify $\{0,1\}$ with the field of $GF(2)$. For every $k \times n$ matrix A with entries in GF(2), and $\mathbf{b} \in GF(2)^k$, $\mathcal{H}_{n,k}$ contains the function $h_{A,\mathbf{b}} : GF(2)^n \to GF(2)^k$ defined as $h_{A,\mathbf{b}}(x) = Ax + \mathbf{b}$.

Problem 2 [20 pts]. Prove that these exists an AM protocol such that: given any set $S \subseteq \{0,1\}^n$ either $|S| \geq K$ or $|S| \leq K/8$ for some $K = 2^k$ and $k \leq n$, that AM protocol can tell which case it is with perfect completeness and constant soundness. (In the lecture, we talked about an AM protocol with only constant (but not perfect) completeness.)

Problem 3 [30 pts]. Consider the follow (true) TQBF statement

$$\phi : \forall x_1 \exists x_2 : (x_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee x_2)$$

- (1) [10 pts] Write out the arithmetization Φ of ϕ, and prove that

$$\prod_{x_1 \in \{0,1\}} R_{x_1} \coprod_{x_2 \in \{0,1\}} R_{x_1} R_{x_2} \Phi(x_1, x_2) = 1 \mod 11,$$

  where R_x denotes the "degree reduction" operation applied to variable x (i.e., $x^k = x$ for any $k > 0$ defined in Katz's lecture 19).

- (2) [20 pts] Explicitly write out the entire interactive proof for the statement above, following exactly the template given in class. Work modulo q = 11, and assume that in the first iteration the verifier chooses "random value" 1, then "random value" 2, "random value" 3, and so on. (These choices of the random numbers are just for the convenience of grading. In a real execution of the protocol, the verifier would of course need to choose the random values at random, and we would have to take q larger than 11.)
