University of Maryland
CMSC652 — Complexity Theory
Professor Jonathan Katz

Homework 4

Due at the *beginning* of class on Nov. 16

I suggest to use LaTeXwhen typing up your solutions.

1. Prove Claim 3 in the notes for lecture 12. Prove also that $\mathcal{ZPP} = \mathcal{RP} \cap \mathsf{co}\mathcal{RP}$.
2. Arora-Barak, Exercise 7.10.
3. Arora-Barak, Exercise 8.1(d).
4. Arora-Barak, Exercise 8.4.
5. Consider the follow (true) TQBF statement ϕ: $\forall x_1 \exists x_2 : (x_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee x_2)$.
   (a) Write out the arithmetization Φ for ϕ, and prove that
   $$\prod_{x_1 \in \{0,1\}} R_{x_1} \coprod_{x_2 \in \{0,1\}} R_{x_1} R_{x_2} \Phi(x_1, x_2) = 1 \bmod 11.$$
   (b) 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, . . . , etc. (This is only to make it easier for the TA to grade — 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.)