CS 466/666 Fall 2018 due Tuesday October 30, 5 PM
A. Lubiw

ASSIGNMENT 4

DO NOT COPY. ACKNOWLEDGE YOUR SOURCES.

1. [10 marks] Prove that RP $\cap$ co-RP $\subseteq$ ZPP. See Lecture 8 notes for definitions of these classes. Recall that I gave the idea of this proof in class: assume you have an RP algorithm A and a co-RP algorithm A'. By running these (repeatedly) build a ZPP algorithm. Include probability details in your solution.

2. [10 marks] Two multisets of numbers are equal if they contain the same numbers with the same multiplicities, e.g., $\{1, 2, 1\}$ and $\{2, 1, 1\}$ are equal, but $\{1, 2, 2\}$ is not. We can test if two multisets of size n are equal by sorting in $O(n \log n)$ or by hashing, but here is another method.

   For a multiset $S = \{e_1, e_2, \ldots, e_n\}$ define $P(S) = (x - e_1)(x - e_2) \cdots (x - e_n)$, a polynomial in one variable x.

   (a) [3 marks] For multisets S_1 and S_2 prove that $S_1 = S_2$ iff $P(S_1) \equiv P(S_2)$. (You may quote results from linear algebra without proof.)

   (b) [7 marks] Based on this, and on the Schwartz-Zippel result from class, suggest a randomized Monte Carlo algorithm to test if $S_1 = S_2$. Your algorithm should have error probability at most $1/2$. Be clear about the range of your random numbers. On which side are the one-sided errors? Analyze the run-time of your algorithm, assuming arithmetic operations take constant time.

   For practicality, your computations should be done modulo a small prime, but you do not need to analyze how large a prime is needed.