CSci 4554 Assignment 4

Due Friday, February 22nd in class

Problem 1 (20 points). Consider a procedure of recognizing whether a given integer p appears among the first $k = \log_2 p$ numbers generated by a pseudo-random number generator with an unknown seed $x \in_U [1, m]$, where m is a known constant. The function used by the generator is deterministic and runs in time polynomial in k. The recognition procedure works by generating a random seed and testing whether p is among the first k numbers generated starting at this seed.

Question 1 (5 points). Give a step-by-step algorithm for recognizing p using the procedure given above.

Question 2 (8 points). Let R_k denote the set of numbers that are generated in at most k steps by the pseudo-random number generator with any seed x, as described above. Let single-quoted string denote the result of the recognition algorithm in question 1. Compute the probabilities $\epsilon = \text{Prob}['p \in R'_k \mid p \in R_k]$ and $\delta = \text{Prob}['p \in R'_k \mid p \notin R_k]$. Show all your work.

Question 3 (2 points). Is the algorithm Monte Carlo, Las Vegas, or Atlantic City? Please explain using your answer to question 2.

Question 4 (5 points). Prove that the algorithm is in *PP* (Probabilistic Polynomial) class. Would is still be in *PP* if we change k to be equal to p? Please explain your answer.

Problem 2 (15 points). Suppose that in the Quantum Key Distribution algorithm (as given in the book) Alice and Bob use the rectilinear polarizer (and, consequently, observer) $\frac{1}{3}$ of the time, and diagonal polarizer (observer) $\frac{2}{3}$ of the time. This is known to Eve. How does this affect the completeness and soundness probabilities (ϵ and δ)? Show all your work.

Will the modified algorithm still be in the *BPP* class? Please explain your answer using the computed probabilities.

Problem 3 (15 points). Consider the following two generators for a random bit:

- E_1 generates a uniformly distributed 100-bit integer n and a uniformly distributed integer i between 1 and a 100. It then returns the i-th bit of n. Assume that both n and i are truly uniformly distributed in their ranges.
- E_2 uses a physical random bit generator that is guaranteed to have a uniform distribution of 0s and 1s.

Consider the following distinguisher D for the above series of zeros and ones:

- As a preprocessing step it runs E_1 a large number of times and then E_2 a large number of times and records the resulting frequencies of numbers of zeros and ones in each group. Assume that this step happens instantly (maybe the algorithm just looks up prerecorded frequencies).
- It computes the total numbers of zeros and ones in the actual series. If they are closer to one of the recordings then the output is that generator. If they are in-between the two recordings or the two recordings are exactly the same then the algorithm outputs E_1 or E_2 with the $\frac{1}{2}$ probability.

Prove that the distinguisher has no advantage, i.e. $Adv(D) = 0$. Also prove that it is a polynomial distinguisher (not counting the preprocessing step).