22C:131 Homework 3

Due: Monday, 5/8

Notes: (a) Solve all 4 problems listed below. The problem numbers refer to problems in the second edition of Sipser. (b) It is possible that solutions to some of these problems are available to you via other theory of computation books or on-line lecture notes, etc. If you use any such sources, please acknowledge these in your homework. You will benefit most from the homework, if you sincerely attempt each problem on your own first, before seeking other sources. (c) It is okay to discuss these problems with your classmates. Just make sure that you take no written material away from these discussions.

1. Consider the following randomized algorithm for PATH. The algorithm consists of repeatedly executing the following two steps:

   (a) Starting at s, simulate a random walk of $n-1$ steps. Each step consists of choosing an edge leaving the current vertex uniformly at random. If t is reached, output YES and stop. If the walk reaches a vertex with no outgoing edge, or a vertex other than t after $n-1$ steps, return to s.

   (b) Flip $\log n^n$ unbiased coins. If they all come up HEADS, halt and output NO.

   Answer the following questions about this algorithm.

   (i) Can the algorithm be implemented in $O(\log n)$ space? Describe how.

   (ii) Suppose the digraph has an st-path. What is the best lower bound you can show on the probability that the algorithm will output YES? Show how you obtained this lower bound.

   (iii) Do the results obtained in (i)-(ii) show that $PATH \in RL$? Explain why or why not.

   (iv) Even before you saw this algorithm, based on results already proved in class, you could have deduced that there is a randomized $O(\log n)$-space algorithm for PATH that rejects $(G, s, t) \notin PATH$ with probability 1 and accepts $(G, s, t) \in PATH$ with probability $\geq 1/2$. Explain how you could have reached this conclusion based on results proved in class.

2. 9.13

3. 9.14

4. You will have to write a little program for this. For the Carmichael number 1729, according to the theorem that shows $PRIMES \in BPP$, there are at least 864 witnesses (these are all Step (6) witnesses for compositeness). Report the exact number of witness for 1729. For the smallest witness a, report a non-trivial square root of 1 modulo 1729.