CS174 **Midterm 2** **Spring 2000**
J. Canny **April 6**

This is a closed-book exam with 4 questions. You are allowed to use the 4 sides of notes that you brought with you. The marks for each question are shown in parentheses, and the total is 80 points. Make sure you allocate enough time to attempt all the questions. Write all your answers in this booklet. Good Luck!

NAME____

SID Number____

1. (20 points) Give brief answers to the following:

   (a) (4 points) Consider the randomized routing algorithm from class on $N = 2^n$ processors. What is the *expected* number of steps to route a packet to a random destination by bit fixing? Ignore collisions in your answer.

   (b) (4 points) Suppose we choose an r uniformly at random from $\{1, \ldots, n\}$. Give a bound on the probability that two degree d polynomials P and Q satisfy $P(r) = Q(r)$.

   (c) (4 points) What is the expected depth of a data-punctuated token tree on a string of length N characters? Include the constant factor in your answer.

   (d) (4 points) In the Byzantine agreement algorithm from class, what is the probability that bad processors cannot foil the threshold on a given round?

   (e) (4 points) In a graph G with n vertices whose minimum cut has k edges in it, give a lower bound on the number of edges of G.

2. (20 points) Let $P(x, y)$ and $Q(x, y)$ be polynomials of total degree d. Suppose you are given an algorithm A which multiplies P and Q to produce a product $R(s, t)$ of degree $2d$.

   (a) (10 points) Give a program checker for A.

   (b) (6 points) What is the time complexity of your checker? Assume that evaluation of a degree d polynomial in two variables takes $O(d^2)$ time.

   (c) (4 points) What is the probability of failure for your algorithm?

3. (20 points) The code for Byzantine agreement is shown below:

```
L = (5/8)n+1     H = (3/4)n+1     G = (7/8)n

1. vote = bi
2. For each round, do
   3. Broadcast vote.
   4. Receive votes from other processors.
   5. maj <-- majority vote received including own vote.
   6. tally <-- number of occurences of maj among votes received.
   7. If coin = HEADS then threshold <-- L
      else threshold <-- H
   8. If tally >= threshold then vote <-- maj
      else vote <-- 0
   9. If tally >= G then set di to maj permanently
```

Suppose that the global coin toss is not fair, but has $\Pr[HEAD] = p$.

(a) (5 points) What is the expected number of rounds until the threshold is not foiled? i.e. until all good processors vote the same.

(b) (15 points) If bad processors could predict the coin toss outcome, can they prevent the algorithm from halting? Explain why or why not.

4. (20 points) Boruvka's algorithm for computing minimum spanning trees of a graph G with n vertices and m edges does the following:

```
Algorithm Boruvka(G)
For each v in V do
  Let e be the minimum weight edge that is incident on v.
  T <-- T + {e}
G' <-- G with all edges in T contracted.
T' <-- recursively compute the minimum spanning tree of G'.
Return T + T'.
```

   (a) (10 points) Suppose we randomly remove edges with probability $1/2$ before running the algorithm. That is, we apply Boruvka to the graph $G(p)$ with $p = 1/2$ to give a spanning tree T_p. If the minimum spanning tree of G is T, what is the expected number of edges of T that also appear in T_p?

   (b) (10 points) What is the time complexity of Boruvka when the $G(p)$ sampling is performed on every recursion? That is, assume Boruvka begins with a step that samples the edges of the input graph.