

CS174
J. Canny

Midterm 2

Spring 98
April 7

This is a closed-book exam with 4 questions. The marks for each question are shown in parentheses, and the total is 60 points. Make sure you allocate enough time to attempt all the questions. You are allowed to use the formula sheet that will be handed out with the exam. No other notes are allowed. Calculators are OK. Write all your answers in this booklet. Good Luck!

NAME _____

SID Number _____

1. (20 points) Count the number of permutations (with repeats) of length k of the 5 characters a, b, c, d, e , if:
- (a) There are exactly two occurrences of the substring “ab”?
 - (b) There are exactly two occurrences of the substring “aa”? Note that the substring “aaa” counts as two occurrences.

-
2. (15 points) A program P is supposed to compute the inverse of an $n \times n$ input matrix A . Describe the steps of a probabilistic program checker that would run to check that the output is correct. You should analyze its running time.

3. (10 points) Suppose you have a self-aligning fingerprint tree for a string S and self-aligning fingerprint tree for T . Both S and T have at most n characters. Briefly describe how you would *efficiently* compute the fingerprint tree for the concatenation $S+T$. What is the running time and how many new nodes did you need to create (as big-O bounds)?

4. (15 points) For the Byzantine general agreement protocol:

(a) Do all the good processors reach agreement in the same round? If not, how many steps does it take? Explain briefly.

(b) Suggest a modification to the Byzantine agreement program (the pseudo-code is given on the next page) so that all the processors halt after complete (good-processor) agreement is reached.

Algorithm ByzGen:

Input: A value b_i .

Output: A decision d_i .

- (a) $vote = b_i$.
- (b) For each Round, do:
 - i. Broadcast $vote$.
 - ii. Receive votes from all other processors.
 - iii. $maj \leftarrow$ majority value (0 or 1) among votes received including own vote.
 - iv. $tally \leftarrow$ number of occurrences of maj among votes received.
 - v. If $coin = HEADS$ then $threshold \leftarrow L$.
else $threshold \leftarrow H$.
 - vi. If $tally \geq threshold$ then $vote \leftarrow maj$.
else $vote \leftarrow 0$.
 - vii. If $tally \geq G$ then set d_i to maj permanently.