CS174 **Practice Final Exam** **Spring 99**
J. Canny **May 4**

This is a closed-book exam with 6 questions. The marks for each question are shown in parentheses, and the total is 120 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!

1. Recall that in the stable marriage algorithm, males and females have preference lists, and each male proposes to his most-preferred female who has not rejected him yet. Each female accepts unless she is married to a more-preferred partner. Let n be the number of people. Assume the rank lists are random permutations of $(1, \ldots, n)$.

   (a) What is the expected number of proposals that a male makes? (note that this is the same as the expected number of proposals that each female receives)

   (b) What is the expected rank of each males final wife?

   (c) What is the expected rank of each females final husband?

   HINT: Think about the coupon collector's problem.

2. Give Markov, Chebyshev and Chernoff bounds for the following problem:

   What is the probability of more than 30 heads in 40 tosses of a fair coin?

3. The code for a choice coordination algorithm is shown below. The goal of the algorithm is to write the symbol $\surd$ into exactly one of the registers. Random bits are used in the algorithm, and suppose that p is the probability that a random bit is 1 at any step, and $1 - p$ is the probability that a random bit is 0. What is the expected running time of the algorithm as a function of p?

   There are two registers C_0 and C_1, and two processors P_0 and P_1. The registers are assumed to be initialized to zero. Each processor has a local variable B_i, which is also zero initially.

   Here is pseudo-code for the algorithm:

   Input: Registers C_0 and C_1 initially zero

   Output: Exactly one of the registers has the value $\surd$

   (a) P_i is scanning register C_i.

   (b) Read the current register and get a bit R_i.

   (c) Select a case:

      i. $R_i = \surd$: halt

      ii. $R_i = 0$, $B_i = 1$: Write $\surd$ into the current register and halt

      iii. Otherwise: pick a random bit for B_i and write it into the current register.

(d) P_i exchanges its current register with P_{1-i} and we go to step (a).

4. Suppose n is a power of two, $n = 2^k$,

   (a) What is $\phi(n)$?

   (b) What are the possible orders of elements a in the multiplicative subgroup $(\mathbb{Z}_n^*, *)$?

   (c) If the order of a is m, what is the order of any odd power of a?

   (d) Let H_m be the subset of $\mathbb{Z}_n^*$ consisting of elements whose order is less than or equal to m (which you can assume is a power of two). Show that H_m is a multiplicative subgroup.

5. Recall that RSA encryption of a message M involves computing $F(M) = M^e (\bmod\ n)$ where e is the (public) encryption key.

   (a) Can a doubly-encrypted message (that is $f(f(M))$) be decrypted by two decryption steps?

   (b) Can the owner of an RSA key d perform an RSA signature of a message $f(M)$ that has been encrypted using their own public key e? Why?

   (c) In general, it is hard to find a factorization of a large integer n which has two factors. Suppose $p > n$ is a prime. How hard is it to find a, b such that $ab = n (\bmod\ p)$? Explain briefly

6. Consider the problem of dealing five cards from a pack of 52 in a perfectly fair way. Suppose the dealer shuffles the deck, and then bit commits each card. The recipient picks five cards at random, and asks the dealer to reveal them.

   (a) What additional steps should the recipient take to make sure that the dealer isnt cheating (e.g. by putting lots of extra twos and threes in the deck)? Think of zero-knowledge proofs.

   (b) Suppose we change the scheme so that the recipient chooses a random number k first and gives it to the dealer. The dealer shuffles and bit commits the cards. How can the *dealer* choose the five cards in such a way that the recipient is convinced that the dealer is not cheating ? (remember how secure hash functions work)