Computer Science 70: Discrete Mathematics

Final Review

(1) (True or False) Answer the following true-or-false questions and provide a justification for your answer
- If the implication $P \implies Q$ is true, then $Q \implies P$ is also true.
- $\forall w \in \mathbb{Z}, \exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, \exists z \in \mathbb{Z} : w + x = y + z$.
- $\exists x \in \mathbb{N}, \forall p \in \mathbb{Z} : p > 5 \implies x^2 \equiv 1 \pmod{p}$.
- If m is any natural number satisfying $m \equiv 1 \pmod{2}$, then the equation $2048x \equiv 1 \pmod{m}$ is guaranteed to have a solution for x.
- If p is prime, then $x^{p-1} \equiv 1 \pmod{p}$ for all $x \in \mathbb{N}$.
- If $p \in \mathbb{N}$ is such that $x^{p-1} \equiv 1 \pmod{p}$ for every $x \in \mathbb{N}$, $\gcd(x, p) = 1$, then p is prime.
- For arbitrary sets S and T, $|S \cup T| = |S| + |T|$.

(2) (Satisfiability) For each of the following Boolean expressions, decide if it is (i) valid (ii) satisfiable (iii) unsatisfiable.
- $[(P \implies Q) \wedge (Q \implies R)] \implies (P \implies R)$
- $\neg(P \implies Q) \ \wedge \ \neg(Q \implies P)$
- $((P \wedge Q) \vee R) \implies P)$
- $((P \wedge (Q \vee R)) \implies \neg P)$

(3) (Logic and proofs)
- Can you define *open sentences* (i.e., sentences whose truth value depends on some variable x) $P(x)$ and $Q(x)$ and a universe U so that

  $(\forall x \in U)(P(x) \Rightarrow Q(x))$ is false, and
  $(\forall x \in U)(Q(x) \Rightarrow P(x))$ is false?

  If yes, give an example. If no, explain why not.
- Can you define *propositions* (i.e., sentences with a fixed truth value) P and Q so that

  $P \Rightarrow Q$ is false, and
  $Q \Rightarrow P$ is false?

  If yes, give an example. If no, explain why not.
- Can you define *open sentences* (that is, sentences whose truth value depends on some variable x) $P(x)$ and $Q(x)$ and a universe U so that

  $(\forall x \in U)(P(x) \Rightarrow Q(x))$ is false, and
  $(\forall x \in U)(Q(x) \Rightarrow P(x))$ is false?

  If yes, give an example. If no, explain why not.

(4) (Modular Arithmetic)
- Use the extended GCD algorithm to find the inverse of 5 modulo 36. Show all your work. Use this result to solve the equation $5x + 19 \equiv 35 \pmod{36}$.

- What is $70^{2003} \pmod{11}$? Simplify your answer to an integer between 0 and 10.
- What is $70^{2003} \pmod{77}$? Simplify your answer to an integer between 0 and 76.

(5) (Lagrange Interpolation)
- Find the polynomial f of least degree (over the real numbers $\mathbb{R}$) such that $f(0) = 2$, $f(1) = 6$, and $f(3) = 20$.
- Prove that no polynomial of degree less than the degree of f can satisfy the same conditions.
- Find another polynomial g that satisfies the same conditions.

(6) (Basic probability) Each of the 50 states has two senators. A committee of 20 senators is chosen uniformly at random from among all 100 senators. Answer the following questions and justify your answers carefully:
- What is the sample space and what is the probability of each sample point?
- Let CC be the event that the committee includes both of the senators from California. What is the probability of CC?
- Let W be the event that the committee contains at least one senator from Wyoming. What is the conditional probability of CC given W?
- Are CC and W independent events?
- What is the probability that at least one state has two members on the committee?

(7) Suppose the events A and B are independent and the events B and C are independent. Are the events A and C necessarily independent? Prove or give a counterexample.

(8) A candy bar of total length L is made up of a linear sequence of n equal-length blocks. Assume that n is odd. Suppose you cut the bar at one of the $L-1$ boundaries between two blocks chosen uniformly at random. Let the r.v. X be the length of the *longer* of the two resulting pieces.
  (a) Compute $\mathbf{E}(X)$ in the case $n = 5$.
  (b) Compute $\mathbf{E}(X)$ as a function of n. Check your answer against the value you obtained in part (a).
  (c) Compute the variance $\mathbf{Var}(X)$ as a function of n. [Hint: You may use the fact that the sum of the squares of the first m positive integers is $\sum_{i=1}^{m} i^2 = \frac{1}{6}m(m+1)(2m+1)$.]
  (d) Use Chebyshev's inequality together with parts (b) and (c) to derive an upper bound on the probability that the longer piece has length at least $\frac{7L}{8}$.

(9) n people take part in a lottery, in which there are a total of $2n$ tickets, n of which are winning tickets and the remaining n losing tickets. Each person buys one ticket, which is drawn uniformly at random

from all those remaining. Let the random variable X denote the number of people who win a prize. Answer the following questions.

(a) What is the sample space, and how many sample points does it contain?

(b) In the special case $n = 2$, write down the distribution of the r.v. X, and compute its expectation $\mathbf{E}(X)$ and its variance $\mathbf{Var}(X)$.

(c) Give a simple but rigorous argument to show that, for any value of n, the expectation $\mathbf{E}(X)$ is exactly $\frac{n}{2}$. [Hint: Write $X = \sum_{i=1}^{n} X_i$, for simpler r.v.'s X_i.]

(d) Consider any two particular people. What is the probability that both of these people buy a winning ticket, as a function of n? Justify your answer carefully.

(e) Now compute the variance $\mathbf{Var}(X)$, as a function of n. [Hint: Use the same representation $X = \sum_{i=1}^{n} X_i$; use part (d) to compute $\mathbf{E}(X_i X_j)$ for $i \neq j$. Check your answer for $n = 2$ against the value you computed in part (b).]

(f) Now suppose that $n = 100$. Use Chebyshev's inequality to compute an upper bound on the probability that 60 or more people win a prize.

(10) Suppose you are given a bag containing n unbiased coins. You are told that $n-1$ of these are normal coins, with heads on one side and tails on the other; however, the remaining coin has heads on both its sides.

(a) Suppose you reach into the bag, pick out a coin uniformly at random, flip it and get a head. What is the (conditional) probability that this coin you chose is the fake (i.e., double-headed) coin?

(b) Suppose you flip the coin k times after picking it (instead of just once) and see k heads. What is now the conditional probability that you picked the fake coin?

(c) Suppose you wanted to decide whether the chosen coin was fake by flipping it k times; the decision procedure returns FAKE if all k flips come up heads, otherwise it returns NORMAL. What is the (unconditional) probability that this procedure makes an error?

(11) Recall that a set E is said to be *finite* if there is a bijection $f : E \to \{1, 2, \ldots, n\}$. A set is *infinite* if it is not finite. Prove that a set F is infinite if and only if there is a bijection from F to some proper subset F' of F.