Review Problems

Logic and Induction

1. True/False

In this question, let P and Q be predicates and $n \in \mathbb{Z}^+$. Which of the following statements are true for all P and Q and which may be false?

Do not guess: incorrect answers may receive negative credit.

(a) $P(1) \wedge Q(2) \wedge [\forall n.\ P(n) \Rightarrow P(n+2)] \wedge [\forall n.\ Q(n) \Rightarrow Q(n+2)] \implies \forall n.\ \neg P(n) \Rightarrow Q(n)$

(b) $P(1) \wedge Q(2) \wedge [\forall n.\ P(n) \Rightarrow P(n+2)] \wedge [\forall n.\ Q(n) \Rightarrow Q(n+2)] \implies \neg[\exists n.\ \neg P(n) \wedge \neg Q(n+1)]$

(c) $P(1) \wedge Q(2) \wedge [\forall n.\ P(n) \Rightarrow P(n+1)] \wedge [\forall n.\ Q(n) \Rightarrow Q(n+2)] \implies \forall n.\ P(n) \Rightarrow Q(n)$

(d) $P(1) \wedge Q(2) \wedge [\forall n.\ P(n) \Rightarrow Q(n+1)] \wedge [\forall n.\ Q(n+1) \Rightarrow P(n)] \implies \forall n.\ P(n) \Rightarrow Q(n)$

2. Proofs

(a) For all $n \geq 1$, prove that

$$\sum_{k=0}^{n} 2 \cdot 3^k \ = \ 3^{n+1} - 1.$$

(b) Guess and prove a formula for

$$1 - 2 + 3 - 4 + \cdots + (-1)^{n-1} n.$$

You may give different formulas for the cases when n is odd and when it is even. Note that $(-1)^{n-1}$ is just 1 if n is odd and -1 if n is even.

(c) Use induction to prove the following for all $n \geq 1$:

The number of ways to pick two items out of a given set of n items is $n(n-1)/2$.

(d) Prove by induction that $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$.

Stable Marriage

3. TMA Algorithm

(a) Consider the set of men $\mathcal{M} = \{m_1, m_2, m_3\}$ with the following preferences on the set of women:

- $P_{m_1} = \{1, 2, 3\}$;
- $P_{m_2} = \{1, 3, 2\}$;
- $P_{m_3} = \{3, 1, 2\}$,

and the set of women $\mathcal{W} = \{w_1, w_2, w_3\}$ with the following set of preferences on the set of men:

- $P_{w_1} = \{3, 1, 2\}$;
- $P_{w_2} = \{3, 2, 1\}$;
- $P_{w_3} = \{2, 3, 1\}$.

Run the traditional marriage algorithm on this example. How many times does the main loop run until reaching a stable matching in this case?

(b) Suppose the traditional marriage algorithm is run to produce a man-optimal stable pairing. Suppose then that one of the men moves one of the women *to whom he never proposed* up higher in his preference list (but all other preference lists remain unchanged). Then must the pairing remain stable?

(c) If man M does not propose to woman W in the traditional marriage algorithm, then can there be a stable pairing in which M is matched with W?

Modular Arithmetic

4. Prime Triplets
Three numbers $p, p+2, p+4$ are a *prime triplet* if they are all primes. For example 3,5,7 are a prime triplet. Prove that there is no other prime triplet. [*Hint*: consider an argument modulo 3.]

5. RSA

(a) If $p = 7$, $q = 13$ and $e = 5$ then what is the private key according to the RSA algorithm?

(b) If Alice wants to send the message $m = 23$, what is the encrypted message?

6. Secret Sharing
The 4 GSIs and 8 readers for CS70 wanted to share a secret. The secret s, which is a number between 0 and 6, is split among them as below. Note that **all operations and values are modulo 7.**

- The number s is split into two parts s_1 and s_2 such that $s \equiv s_1 + s_2$.
- A degree 1 polynomial P_1 and a degree 2 polynomial P_2 are constructed such that $P_1(0) \equiv s_1$ and $P_2(0) \equiv s_2$.
- The 4 GSIs are given the values $P_1(1), P_1(2), P_1(3), P_1(4)$, and the readers are given the values $P_2(1), P_2(2), P_2(3), P_2(4), P_2(5), P_2(6), P_2(8), P_2(9)$.

(a) Prove that the secret can be recovered only when at least 2 GSIs and at least 3 readers are present.

(b) If 2 GSIs and 3 readers are present, is it always possible to recover the secret?

(c) Suppose that 2 GSIs meet and exchange the information that $P_1(1) \equiv 5$ and $P_1(2) \equiv 0$. Also, 3 readers exchange the information that $P_2(2) \equiv 0$, $P_2(3) \equiv 2$, and $P_2(5) \equiv 4$. Using this information, find the secret.

7. Erasure Codes
A communication channel accepts only messages of length m packets. When a length-m message is transmitted, up to k of the packets will be lost by the channel.

(a) Suppose you want to send a message on this channel. What is the maximum number of message packets you can send in one shot (excluding redundant packets) so that the message can be reliably recovered by the receiver? Explain your answer.

(b) Assume now that $m = 5$ and $k = 2$, and suppose you want to send a message consisting of the six digits $(0, 1, 2, 1, 2, 0)$. Describe a scheme to reliably send this message. You should give all the details related to your scheme, but you do not need to explain how the received message is decoded.

(c) Now suppose you are told that, working over $GF(5)$, the recipient receives the packets $(3, 2, -, 1, -)$. What is the original message intended by the sender?
Updated 12/13/10.

Counting and Basic Probability

8. A Tale of Two Proofs

(a) Prove algebraically that
$$\binom{n}{r} \cdot \binom{r}{k} = \binom{n}{k} \cdot \binom{n-k}{r-k}.$$

(b) Give a combinatorial proof for the above identity.

9. ID DQD
A UC Berkeley SID number has 8 digits. Every digit can be any number from $0 - 9$. How many ways are there to have:

(a) An SID where no number repeats.
(b) An SID where every digit is bigger than the previous digit.
(c) An SID that is divisible by 3.
(d) An SID where at least 1 number repeats.
(e) An SID where exactly 1 number repeats exactly once.

10. Keeping Count

(a) Suppose we roll n dice and are only interested in how many dice came up with each number. How many different outcomes are possible?

(b) A certain department offers 8 lower level courses $L_1, L_2, \cdots, L_8$ and 10 higher level courses $H_1, H_2, \cdots, H_{10}$. A valid curriculum consists of 4 lower level courses and 3 higher level courses.

(i) How many valid curricula are possible?

(ii) Suppose that L_1 is a prerequisite for $H_1, \cdots, H_5$ (i.e. any curriculum that includes one of $H_1, \cdots, H_5$ must also include L_1) and L_2 and L_3 are prerequisites for $H_6, \cdots, H_{10}$. Now how many valid curricula are there?

(c) The weather on any given day can be sunny, cloudy, rainy, or snowy. Assume four sequential seasons (fall, winter, spring, summer), that a snowy day can happen only during the winter, that a rainy day cannot happen in the summer, and that each season has 90 days. What is the number of all possible distinct 360-day weather sequences (consecutive days)?

11. Flipping a Coin

We flip a biased coin with probability p of getting heads until one of the following events occur:

- we get heads;
- we flipped the coin three times.

(a) Describe the probability space and the probabilities for each point in the space.
(b) What is the probability that we are still playing in the third round?
(c) Are the events "heads on the second round" and "heads on the third round" disjoint? independent?
(d) Given that we flipped more than once and that we did end up with heads, what is the probability that we got heads on the second flip? Again, conditioned on the above, what is the probability that we got heads in the third flip?

12. Conditional Independence

Prove that if A and B are independent conditional on C, then $\Pr[A|B, C] = \Pr[A|C]$.

Distribution, Expectation, and Variance

13. Love is Random

Consider an instance of the stable marriage problem with n men and n women. Suppose each individual's preference list is randomly ordered with uniform probability and that the traditional marriage algorithm is used to produce a matching.

(a) What is the distribution of the number of men that woman 1 will reject in the first round?

(b) How many total rejections do you expect to occur in the first round? [You may assume that $\left(1 - \frac{1}{n}\right)^n \approx \frac{1}{e}$.]

14. CS70 Ruined My Life

You are constantly pondering CS70 problems, and as a result, you become very absent-minded. Suppose there are 52 weeks in a calendar year, and on each week, you have a $\frac{1}{6}$ chance of losing your cell phone, independently of all other weeks. Every time you lose your phone, you purchase a new one that you start using the following week.

(a) Upon buying a new phone, how many weeks do you expect to go before you lose it? What is the variance in the number of weeks you expect to have your phone?

(b) How many phones do you expect to own during the course of a calendar year, including the one you started out with? What is the variance?

(c) Suppose you enter the 29th week of the year (meaning 28 weeks have passed) having already lost your phone 6 times. How many phones do you expect to go through during the year? What is the variance?

(d) Are the following events independent:

A: you lose your phone at least 8 times during the course of the year
B: you lose your phone exactly 10 times over the course of the year

What about the following events:

A: you lose your phone sometime in February
B: you lose your phone sometime in April

15. Basketball: A Game of Chance?

(a) The Cal Men's Basketball Team is on a shooting slump; their five starters make each of their baskets with probability $\frac{1}{5}$, where each shot is independent from the rest. However, they do have incredibly good teamwork, so they all take the same number of shots per game - 10 shots each. Use Chebyshev's inequality to find an upper bound on the probability that they make at least 40 baskets.

(b) Now, it turns out that there is actually a star player on the Cal Basketball Team who makes each of his baskets with probability $\frac{4}{5}$ and attempts 30 shots a game. The other players still only take 10 shots each. What is the new upper bound on the probability that they make at least 40 baskets.

16. Exam Scores

Suppose that a student has learned a fraction p of the material in class and that a final exam consists of n randomly and independently chosen questions from the covered material. Assume that the student gets a problem correct if he learned the material for the problem.

(a) Provide an expression for the exact probability that the student gets more than half the questions correct.

(b) Suppose $p = 0.8$. How many questions should the exam contain so that the student gets at least 70% of the questions right with probability at least 0.75?

Inference

17. Cheating the Villain... and Death

James Bond challenges Blofeld to a game of craps. Blofeld, having tangled with Bond many times, suspects that Bond is using a loaded die. Suppose he initially believes with probability 2/3 that Bond is cheating with a die that has probability 1/2 of coming up 1 and 1/10 for each of the remaining values.

(a) What is the (unconditional) probability that the first roll of the suspect die will be 1?

(b) Suppose the die comes up 2 on the first roll. What is the new probability that the die is loaded?

a	$\Pr[X \geq a]$	a	$\Pr[X \geq a]$	a	$\Pr[X \geq a]$
0.0	0.50	0.7	0.24	1.4	0.081
0.1	0.46	0.8	0.21	1.5	0.067
0.2	0.42	0.9	0.18	1.6	0.055
0.3	0.38	1.0	0.16	1.7	0.045
0.4	0.34	1.1	0.14	1.8	0.036
0.5	0.31	1.2	0.12	1.9	0.029
0.6	0.27	1.3	0.097	2.0	0.023

Table 1: Probabilities for a standard normal distribution X.

Continuous Probability

18. Throwing Darts

Consider a dartboard of radius $r \in \mathbb{N}$ that is divided by concentric circles at radii $i = 1, 2, \cdots, r-1$.

(a) Suppose a player throws a dart that strikes any position on the board with uniform probability. Assuming that the dart hits the board, what is the probability that the player hits the ith section from the center, between the $(i-1)$th and ith circles?

(b) Now suppose that the player throws a dart such that the distance from the center is exponentially distributed with parameter λ. What is the probability that the player hits the ith section? [Note that the player may miss the board.]

19. Probabilistic Test Taking

Consider a final exam that consists of 9 questions. Suppose the amount of time it takes a particular student to answer each question is mutually independent and approximately normally distributed with a mean of 8 minutes and a standard deviation of 5 minutes.

(a) What is the expected amount of time it will take for the student to complete the exam?

(b) What is the probability that the student will finish the exam in 1 hour?
(Hint: For any two normally distributed random variables $X_1 \sim N(\mu_1, \sigma_1^2)$ and $X_2 \sim N(\mu_2, \sigma_2^2)$, the sum $Y = X_1 + X_2$ has distribution $Y \sim N(\mu_1 + \mu_2, \sigma_1^2 + \sigma_2^2)$.)

20. Polling Your Constituency

Suppose the whole population of California has 60% Democrats, 40% Republicans, and no other parties. You choose 1000 people independently and uniformly at random from the Californian population, and for each person, you record whether s/he is a Democrat or a Republican. Let S denote the number of Democrats among the 1000 people.

(a) Specify the probability density function that you would use to model the distribution of S.

(b) What is the probability that you chose more than 625 Democrats?

Cardinality

21. Infinity$^{\text{Infinity}}$

Consider an infinite sequence of disjoint sets $S_1, S_2, \cdots$, where each S_i is countably infinite. Prove that the union $S = \bigcup_{i=1}^{\infty} S_i$ is countable.