SID:

1. Short Questions: 3/3/5/5 Provide a clear and concise justification of your answer.

In this problem, you flip a coin that is such that $Pr[H] = p$. For questions 1-2-3(a), express the answers in terms of p. For questions 3(b) and 4, we are looking for answers such as $2\%, 4\%$, or the like.

1. If you flip the coin three times, what is the probability that the number X of heads exceeds the number of tails? (Express in terms of p.)

   Answer: We know that X is $B(3,p)$. Thus, $Pr[X = 2 \text{ or } 3] = 3p^2q + p^3 = 3p^2 - 2p^3$.

2. How many times do you have to flip the coin, on average, until you see the fifth 'heads'. (The fifth head counts as a flip, of course. Express in terms of p.)

   Answer: The average number of flips until each H is $1/p$, so we need $5/p$ flips, on average.

3. Assume $p < 0.5$. (a) Use Chebyshev's inequality to get an upper bound on the probability that when you flip the coin 100 times the number of heads exceeds the number of tails. (Again, express in terms of p.) (b) Find the value when $p = 0.4$. (Evaluate to a numeric value.)

   Answer: (a) Let X be the number of heads. Then,

$$\begin{aligned} Pr[X > 50] &= Pr[X > 100p + (50 - 100p)] \leq Pr[|X - 100p| > (50 - 100p)] \\ &\leq \frac{var(X)}{(50-100p)^2} = \frac{100pq}{2500(1-2p)^2} = \frac{pq}{25(1-2p)^2}. \end{aligned}$$

   (b) For $p = 0.4$, the value is $\frac{0.24}{25(0.2)^2} = 0.24 = 24\%$.

4. Assume $p = 0.4$. Use the CLT to get an estimate of the probability that when you flip the coin 100 times the number of heads exceeds the number of tails. (Use the fact that $\sqrt{0.4 \times 0.6} \approx 0.5$ and evaluate to a numeric value.)

   Answer: Let X be the number of heads. Then $(X - 100p)/(10\sqrt{pq}) \approx \mathcal{N}(0,1)$. Hence,

$$Pr[X > 50] = Pr[\frac{X - 100p}{10\sqrt{pq}} > a := \frac{50 - 100p}{10\sqrt{pq}}].$$

   Now, $a = \frac{5-10p}{\sqrt{pq}} \approx 2$. Thus,

$$Pr[X > 50] \approx Pr[\mathcal{N}(0,1) > 2] \approx 2.5\%.$$

2. Short Questions: 3/3/3/3/3 Provide a clear and concise justification of your answer.

When asked for justification for true/false. If true, prove or justify. If false, give a counterexample.

1. True or False (and justification): Let X, Y, Z be three random variables defined on the same probability space. If $cov(X,Y) \geq 0$ and $cov(Y,Z) \geq 0$, then it must be that $cov(X,Z) \geq 0$.

   Answer: False. Let U, Y be i.i.d. and equally likely to take the values $\{-1, 1\}$. Let also $X = Y - 2U$ and $Z = Y + 2U$. Then $cov(X,Y) = 1, cov(Y,Z) = 1, cov(X,Z) = -3$.

2. True or False (and justification): Say that you roll a six sided die 100 times and the total number of dots you get is 350. Given that information, the expected number of dots on the next roll is 3.5.

   Answer: False: There is not enough information to answer this question. For instance, if you know that the die is loaded in a way that the expected number of dots is 4, then the expected number of dots on the next roll is 4, independently of what happened previously.

3. True or False (and justification): Let X, Y be two random variables such that $E[Y|X] = 2+3X$. Then $L[Y|X] = 2+3X$.

   Answer: True. Since $2+3X$ is the function of X that minimizes the mean squared estimation error, it must be that there is no other linear function of X with a smaller mean squared estimation error.

4. True or False (and justification): Let X, Y be two random variables such that $E[Y|X] = 2+3X$. Then it must be that $E[Y^2|X] = 4+12X+9X^2$.

   Answer: False. For instance, assume that Y takes only the values 0 and 1. Then $Y^2 = Y$ and $E[Y^2|X] = E[Y|X] = 2+3X$.

5. True or False (and justification): Consider an irreducible Markov chain $\{X_n, n \geq 0\}$ on $\{1,2,\ldots,17\}$ with a uniform invariant distribution and assume that $P(1,1) = 0.2$. Is it true that $P[X_n \leq 5]$ as $n \to \infty$ converges to $\frac{5}{17}$.

   Answer: True. Since $P(1,1) > 0$, we know that the Markov chain is aperiodic. Hence, $Pr[X_n = i] \to \pi(i) = 1/17$ since the invariant distribution is uniform. Consequently, $P[X_n \leq 5] = \sum_i i \leq 5 Pr[X_n = i] \to 5/17$.

3. Longer Questions: 8/8/8/7/6/6/6 Provide a clear and concise justification of your answer.

1. (Short Answers - No justification required.) The left-hand side of Figure 2 shows the six equally likely values of the random pair (X,Y). For questions $A-D$, specify the functions.

   [A]. $L[Y|X] =$
   [B]. $E[X|Y] =$
   [C]. $L[X|Y] =$
   [D]. $E[Y|X] =$

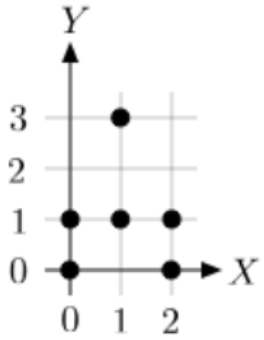

Figure 1: (X,Y) in Question 3.1

   Answer:
   [A]. $L[Y|X] = E[Y] = 1$ since $cov(X,Y) = 0$. Indeed, $E[XY] = (1+3+2)/6 = 1, E[X] = E[Y] = 1$.
   [B]. $E[X|Y] = 1$, by inspection.
   [C]. $L[X|Y] = 1$, in view of [B].
   [D]. $E[Y|X=0] = 0.5, E[Y|X=1] = 2, E[Y|X=2] = 0.5$.

2. (Multiple Choice - No justification - Indicate which statements are correct by checking the corresponding boxes). The right-hand part of Figure 2 shows the state transition diagram of a Markov chain.

   [ ] A. This Markov chain is irreducible and aperiodic.

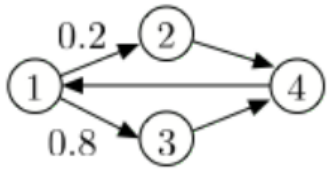

Figure 2: Markov Chain in Question 3.2

[ ] B. This Markov chain is irreducible and periodic.
[ ] C. $\pi = [0.25, 0.25, 0.25, 0.25]$ is invariant for the Markov chain.
[ ] D. $\pi = [1/3, 1/15, 4/15, 1/3]$ is invariant for the Markov chain.
[ ] E. If $\pi_0 = [1,0,0,0]$, then π_n converges as $n \to \infty$.
[ ] F. If $\pi_0 = [1,0,0,0]$, then π_n does not converge as $n \to \infty$.
[ ] G. If $\pi_0 = [1,0,0,0]$, then $(1/n)\sum_{m=0}^{n-1} 1\{X_m = 1\}$ does not converge as $n \to \infty$.
[ ] H. If $\pi_0 = [1,0,0,0]$, then $(1/n)\sum_{m=0}^{n-1} 1\{X_m = 1\}$ converges as $n \to \infty$.

Answer: Correct statements: B, D, F, H. To see D, note that $\pi(1) = \pi(4)$, $\pi(3) = 0.8\pi(1)$ and $\pi(2) = 0.2\pi(1)$.

3. You flip a fair coin. What is the average number of tails (not flips!) until you get (tails, heads, heads) in a row (i.e., THH)?

   Note: You will get 75% of the credit if you write correctly the relevant first step equations and an additional 25% if you can solve them.

   Answer:

   We draw the state transition diagram with states S, T, H, TH, E, with the obvious meaning. We then write the first step equations for the average number of tails $\gamma(i)$ from state i until state E and we count the tails just after we get them, i.e., when we flip the coin after getting tails. One has

$$\begin{aligned}
\gamma(S) &= 0 + 0.5\gamma(H) + 0.5\gamma(T) \\
\gamma(T) &= 1 + 0.5\gamma(TH) + 0.5\gamma(T) \\
\gamma(TH) &= 0.5\gamma(T) \\
\gamma(H) &= 0 + 0.5\gamma(H) + 0.5\gamma(T).
\end{aligned}$$

   To solve, we substitute the third equation into the second and we get

$$\gamma(T) = 1 + 0.25\gamma(T) + 0.5\gamma(T),$$

   which gives $\gamma(T) = 4$. The last equation then gives

$$\gamma(H) = 0.5\gamma(H) + 2,$$

   so that $\gamma(H) = 4$. Finally, the first equation gives $\gamma(S) = 4$.

4. Consider a population of N healthy people. Every week, a healthy person gets sick with probability $\alpha \in (0,1)$ and a sick person gets healthy with probability $\beta \in (0,1)$. For $n \geq 1$, let X_n be the number of sick people at the start of week n.

   (a) Find $E[X_{n+1}|X_n]$.

   (b) Find $E[X_n]$ for $n \geq 1$.

(c) As $n \to \infty$, what does $Pr[X_n = m]$ converge to?

Answer:

(a) One sees that $E[X_{n+1}|X_n = m] = m(1-\beta) + (N-m)\alpha = N\alpha + m(1-\alpha-\beta)$.

(b) Thus, $E[X_{n+1}|X_n] = a + \rho X_n$ where $a = N\alpha$ and $\rho = 1-\alpha-\beta$, so that $E[X_{n+1}] = a + \rho E[X_n]$. Hence,

$$\begin{aligned} E[X_1] &= 0; \\ E[X_2] &= a; \\ E[X_3] &= a + \rho a; \\ E[X_4] &= a + \rho(a + \rho a) = a(1 + \rho + \rho^2); \\ E[X_n] &= a(1 + \rho + \cdots + \rho^{n-2}) = a\frac{1-\rho^{n-1}}{1-\rho}. \end{aligned}$$

(c) Consider one particular person. Observer that her health behaves like a Markov chain on $\{H, S\}$ where H means healthy and S sick. That Markov chain is such that $P(H,S) = \alpha$ and $P(S,H) = \beta$. It is irreducible and aperiodic and its distribution converges to $[1-\gamma, \gamma]$ where $\gamma = \alpha/(\alpha+\beta)$. Also, the states of the different people are independent. Hence, for n large, $X_n \approx B(N, \gamma)$.

5. You play a game of darts with a friend. You are better than he is and the distances of your darts to the center of the target are i.i.d. $U[0,1]$ whereas his are i.i.d. $U[0,2]$. To make the game fair, you agree that you will throw one dart and he will throw two darts. The dart closest to the center wins the game. What is the probability that you will win? *Note:* The distances ***from the center of the board*** are uniform..

   Answer:

   Let X be the distance of your closest dart to the center and Y that of the closest of your friend's darts. Then, for $x \in [0,1]$ and $y \in [0,2]$,

   $$Pr[X > x] = (1-x) \text{ and } Pr[Y > y] = (1-y/2)^2.$$

   Hence,

   $$f_X(x) = -\frac{d}{dx}(1-x) = 1, x \in [0,1].$$

   Also,

   $$Pr[Y > X | X = x] = (1-x/2)^2.$$

   Thus,

   $$\begin{aligned} Pr[Y > X] &= E[(1-X/2)^2] = E[(1 - X + X^2/4] \\ &= 1 - 1/2 + 1/12 = 7/12 \end{aligned}$$

   Since, $E(X) = 1/2$ and $E[X^2] = \int_0^1 x^2 dx = \frac{1}{3}$.

6. There are two indistinguishable bags. Bag A contains 60 red marbles and 40 blue marbles. Bag B contains 40 red marbles and 60 blue marbles. One chooses one of the two bags at random, so that each bag has probability 0.5 of being selected. One then removes 3 marbles from the selected bag, without replacement.

   (a) Assume that all the three marbles were red. What is the probability that the selected bag is A? *Note: We don't want you to evaluate numerically the expression.*

   (b) Assume that r of the 3 marbles were red and b were blue and let p be the conditional probability that the selected bag is A given that information. What is the probability that if you pick one more ball

from the same bag it will be red? *Note: The expression will contain* (p,r,b) *and we do not want you to express* p *as a function of* r *and* b.

Answer:

(a) Here, intuition suggests that it is much more likely that we picked bag A. We can show this by using Bayes' rule. Let R be the event that the three marbles are red. Then,

$$\begin{aligned} Pr[A] &= Pr[B] = 1/2 \\ Pr[R|A] &= \frac{60}{100} \times \frac{59}{99} \times \frac{58}{98} \\ Pr[R|B] &= \frac{40}{100} \times \frac{39}{99} \times \frac{38}{98}. \end{aligned}$$

Bayes' rule then says that

$$\begin{aligned} Pr[A|R] &= \frac{Pr[A]Pr[R|A]}{Pr[A]Pr[R|A] + Pr[B]Pr[R|B]} \\ &= \frac{60 \times 59 \times 58}{60 \times 59 \times 58 + 40 \times 39 \times 38} \end{aligned}$$

We used a calculator and we found that this probability is approximately 0.776.

(b) If we pick from bag A, the probability that the fourth ball is red is $(60-r)/97$. If we pick from bag B, it is $(40-r)/97$. Hence, the desired probability is

$$p \times \frac{60-r}{97} + (1-p) \times \frac{40-r}{97}.$$

7. We throw n balls in m bins where $n > 0$ and $m \geq 2$. Each ball is equally likely to drop into any one of the bins, independently of other balls. Let X and Y be the number of balls that fall into bins 1 and 2, respectively.

   (a) Calculate $E[Y|X]$.

   (b) Calculate $L[Y|X]$.

   (c) Write the first step equations to calculate the expected number of balls one has to throw until one bin contains 2 balls. (*Hint:* What is the Markov chain that you consider? Do not solve the equations.)

   Answer:

   (a) We claim that $E[Y|X=x] = (n-x)/(m-1)$. Indeed, if x balls fall in bin 1, then we know that the $m-x$ other balls are equally likely to fall into any one of the other $m-1$ bins.

   (b) Since $E[Y|X]$ is linear, it must be equal to $L[Y|X]$.

   (c) Let $X_0 = S$. Then, for $n \geq 1$, let X_n be the number of bins that contain exactly one ball after throwing n balls if no bin has already more than one ball; let also $X_n = E$ if one bin has already more than one ball. Then,

$$\begin{aligned} &X_1 = 1; \\ &Pr[X_{n+1} = X_n + 1 | X_n = k] = (m-k)/m, \text{ for } 1 \leq k \leq m; \\ &Pr[X_{n+1} = E | X_n = k] = k/m, \text{ for } 1 \leq k \leq m. \end{aligned}$$

   Finally, define $\beta(i)$ to be the average time until the Markov chain reaches the state E starting from state $i \in \{S, 1, 2, \ldots, m\}$. The first step equations are

$$\begin{aligned} &\beta(S) = 1 + \beta(1); \\ &\beta(k) = 1 + ((m-k)/m)\beta(k+1) + (k/m) \times 0, 1 \leq k < m; \\ &\beta(m) = 1. \end{aligned}$$

4. True/False (All 1 point)

1. $(Q \implies P) \equiv (\neg(Q \wedge \neg P))$
   Answer: True. $Q \implies P \equiv (\neg Q \vee P) \equiv \neg\neg(\neg Q \vee P) \equiv \neg(Q \wedge \neg P)$
   First equivalence from implication as conjuction. The second from negation of negation. Third from DeMorgan's law.
2. $(((\forall x)P(x)) \implies ((\forall y)Q(y))) \equiv (((\exists y)\neg Q(y)) \implies (\neg(\forall x)P(x)))$
   Answer: True. $((\forall x)P(x) \implies (\forall y)Q(y)) \equiv (\neg(\forall y)Q(y)) \implies (\neg(\forall x)P(x)) \equiv ((\exists y)\neg Q(y)) \implies (\neg(\forall x)P(x))$
   First equivalence from contrapositive. The second from DeMorgan's on one side.
3. $(R \wedge \neg R) \implies P$
   Answer: True.
   $R \wedge \neg R)$ is false, which implies every statement.
4. The problem of computing whether P and Q have the same behavior (that is, outputs the same thing as $P(x)$ for all x and loops on x when $P(x)$ does not halt), is decidable/undecidable. (Please answer either decidable or undecidable.)
   Answer: Undecidable. We know the halting problem is undecidable, but to decide the halting problem on P on x, we can write a program, P', that ignores its input and runs P on x.
   Then we check whether P' has the same behavior as a program that loops forever.
5. The problem of computing whether P and Q have the same behavior on all inputs of length at most $|P|$ is decidable/undecidable? (Please answer either decidable or undecidable.)
   Answer: Undecidable. The reduction above works, as even with zero length inputs the program P''s behavior solves the halting problem.
6. The problem of computing whether P and Q have the same behavior on all inputs of length $|P|$ and where the space used by $|P|$ is at most $|P|^2$ is decidable/undecidable? (Please answer either decidable or undecidable.)
   Answer: Decidable. You can simulate P and Q on all inputs of length $|P|$ and if a state repeats during the simulation you know a program runs forever as the state is finite, and thus a repitition must happen in $2^{|P|^2}$ time.

5. What number (or expression)? 1/1/2/2/2/2/2/2/2/2)

1. The number of binary strings of length n.
   Answer: 2^n
2. The number of binary strings of length n (where n is even) with a run of at least $n/2$ zeros.
   Answer: $2^{n/2} + (\frac{n}{2} - 1)2^{n/2-1}$
   The first term counts the number of strings that start with a string of $n/2$ ones. The rest count the number of strings with a 0 followed by $n/2$ for each of $\frac{n}{2} - 1$ starting positions.
3. The number of ways to split n dollars among k people where at most one gets zero dollars.
   Answer: $k\binom{n-(k-1)+(k-2)}{(k-2)} + \binom{n-(k-1)+(k-1)}{k-1} = k\binom{n-1}{k-2} + \binom{n-1}{k-1}$.
   We first count the ways where exactly one gets zero; there are k choices for the person who may get zero, then we distribute the dollars to the $k-1$ remaining people so that each gets at least one. Then we add the ways for all to get at least one.

4. An n packet message was sent through a channel by sending m points on a degree $n-1$ polynomial. If k packets were lost, what is the maximum number of the remaining $m-k$ packets that could be corrupted so that the original message can still be recovered.

   Answer: $m-k >= n+2e$ thus e can be at most $\frac{m-n-k}{2}$

5. How many degree d polynomials, $P(x)$, modulo p are there with exactly d solutions to $P(x) = 5 \pmod{p}$? (You may assume that p is prime and at least 5 and that $d < p$.)

   Answer: There are $\binom{p}{d}(p-1)$ polynomials where we choose d zeros (counting distinct roots and scaling.) Then adding five to each produces a polynomial that has d positions that equal 5.

6. What is $2^{53} \pmod{15}$?

   Answer: $2 \pmod{15}$

   $2^{48} = 1 \pmod{15}$ and $2^5 = 32 = 2 \pmod{15}$

7. What is the maximum degree of an undirected graph whose vertices are $\{0,\ldots,p-1\}$ edges $\{(i, i+1 \pmod{p}) : i \in \{0,\ldots,p-1\}\}$? (You can assume p is prime.)

   Answer: 2.

   $i+1$ is a bijection. Thus, each vertex is incident to two edges, one from below, and one to above.

8. What is the maximum degree of an undirected graph, $G(a,p)$, whose vertices are $\{0,\ldots,p^2-1\}$, and edges $\{(i, ai \pmod{p^2}) : i \in \{0,\ldots,p^2-1\}\}$? Assume $a \neq 0 \pmod{p^2}$. (Give an expression that possibly depends on a and p and properties thereof. Again, p is prime, but a may not be, so your formula may have cases.)

   Answer: If a is a multiple of p all the multiples of p are incident to 0. Thus, the maximum degree in that case is $p+1$, since there are p vertices that are multiples of p (including 0) and 0 has a self loop, which gives an additional 1.

   Otherwise, if $gcd(a,p^2) = 1$, the function has an inverse and the maximum degree is 2, except for the vertex 0, which has a self loop, in which case the degree is 2.

9. Given a connected planar graph with f faces, if one adds an edge and it remains planar, what is the number of faces in the resulting planar graph? (An expression perhaps involving f.)

   Answer: $f+1$

   By Euler's formula.

10. Let S be the set of all planar bipartite graphs with v vertices. What is the maximum number of edges a graph in S can have? Express it in terms of v.

    Answer: $2v-4 \geq e$.

    The number of edge-face incidences is at most $2e$ and at least $4f$ since each cycle and therefore face is of length at least 4.

    Thus, we have $2e \geq 4f$,

    We have $v+f = e+2$, or $v+e/2 \geq v+f = e+2$. Thus, $v+e/2 \geq e+2$, which means that $2v-4 \geq e$.

6. Proofs and Algorithm (4 points each.)

1. Prove that for all primes p that if $p \not| x^2$ then $p \not| x$.

   Answer: Contrapositive. If $p|x$, then $x = ap$ and $x^2 = a^2p^2$ and $p|x^2$.

   Note that the primality does not matter.

2. Consider two degree d polynomials $P(x)$ and $Q(y)$ modulo p, and the two-variable polynomial $f(x,y) = P(x)Q(y)$. (***You may assume that you can efficiently recover a degree*** d ***polynomial from*** $d+1$ ***points or anything else we proved about polynomials in this class.***)

   Say you are given the value of $f(x,y)$ on $(1,1),\ldots,(2d+1,2d+1)$ and on $(1,1),\ldots,(1,d+1)$, give a method to reconstruct $Q(y)$ and $P(x)$. You may assume that the leading coefficients of $Q(y)$ and $P(x)$ are 1.

   Answer: Use the points $(1,1),\ldots,(1,d+1)$ to reconstruct $P(1)Q(x)$, and divide the polynomial to get the leading coefficient of $Q(x)$ to be 1 and produce $Q(x)$.

   Use the points $(1,1),\ldots,(2d+1,2d+1)$ to reconstruct the degree $2d$ polynomial $Z(x) = P(x)Q(x)$, then divide $Z(x)$ by $Q(x)$ to recover $P(x)$.

3. Given a set of k triples from a set of vertices $\{1,\ldots,n\}$ (e.g., $(2,4,10)$ is a triple when $n \geq 10$) where each $i \in \{1,\ldots,n\}$ is in at most d triples, describe an algorithm that uses at most $3d-2$ colors to legally color the triples so that no two triples that contain the same vertex have a common color.

   (Note: two $(2,4,6)$ and $(2,8,10)$ both contain vertex 2 and thus cannot have the same color. We are looking for a two line algorithm including justification. A line or two more is ok.)

   Answer:

   Remove a triple, color the remaining triples using $3d-2$ colors, the neighboring vertices are now each incident to $d-1$ other triples thus use together at most $3(d-1)$ colors leaving one available to color this triple.

4. Prove that a number is divisible by 3 if and only if the sum of its digits is divisible by 3. (Hint: One way to prove this is to strengthen an inductive statement into a statement about the value of a number modulo 3.)

   Answer:

   We prove that the stronger statement that sum of the digits is equal modulo 3 to the number x.

   By induction. If the number of digits is 1, it is trivial.

   Induction Hypothesis: True for n digit numbers.

   Consider a number $x = 10y + a$ where y is an n digit number. We take this expression modulo 3 and obtain $x = y + a = \sum_i y_i + a \pmod 3$, where y_i is the ith digit of y. We used the fact that $10 = 1 \pmod 3$ in the first equality and the induction step in the second. The final expression yields the statement.