CS 70 Discrete Mathematics and Probability Theory
Spring 2019 Ayazifar and Rao

Midterm 2 Solutions

PRINT Your Name: Oski Bear

SIGN Your Name: *OSKI*

Do not turn this page until your instructor tells you to do so.

1. TRUE or FALSE? 2 points each

For each of the questions below, answer TRUE or FALSE. No need to justify answer.

Please fill in the appropriate bubble!

Answer: Note that the answers provide explanations for your understanding, even though no such justification was required

1. If the set of prime numbers that divide x is the same as the set of prime numbers that divide y, then $x = y$.
   Answer: False. Consider p^2 and p.
2. For primes p and q, the function $f(x) = x^{k(p-1)(q-1)+1} \pmod{pq}$ is a bijection for all integers k.
   Answer: True. This is the proof that RSA encryption/decryption returns the original message, which means it is the identity function. The identity is a bijection.
3. Every degree exactly d polynomial over $GF(p)$ can be factored into d polynomials of degree 1, for all d and all primes p.
   Answer: False. This is equivalent to stating that there are d roots. Not all polynomials have d roots as there are more polynomials than there are polynomials with d roots.
4. Let a "probability problem" be a math problem written in LaTeX for which the answer is a probability. There exists a bijection between the set of probability problems and the interval $[0,1]$.
   Answer: False. The set of text written in LaTeX is countable, whereas the set of real numbers is not.
5. Given events A and B in a probability space, the events are independent if and only if $A \cap B$ is empty.
   Answer: False. They are disjoint but definitely not independent: $Pr[A|B] = 0$ where $Pr[A] > 0$, if A is non-empty.
6. Suppose we flip 3 fair coins, let A be the event that all the flips are the same and let B be the event that there are more heads than tails. The events A and B are independent.
   Answer: True. $Pr[A|B] = Pr[A] = 1/4$.
7. A, B and C being pairwise independent implies that A, B and C are mutually independent.
   Answer: False. Consider the events in a two coin experiment where $A = HH, TT, B = \{HT, TH\}$, and $C = \{HH, HT\}$, $Pr[B|A \cap C] = 0 \neq Pr[B]$.

2. Short Answer: RSA. 3 points each.

Write your answer in the simplest form possible. You should use only the variables in the question unless otherwise specified.

1. Given an RSA scheme with public key, (N,e), and the encryptions $E(x) = x'$ and $E(y) = y'$, what is the encryption of xy? (It should be a function of x', y', e, N. You are not given x or y.)
   Answer: $x'y' \pmod N$. $E(xy) = (xy)^e = x^e y^e \pmod N$.
2. What is $[8(7^{-1} \pmod 5)(7) + 6(5^{-1} \pmod 7)(5)] \pmod 5$? (Answer should be in simplest terms.)
   Answer: 3. This is the argument for the correctness of 2-modulus CRT, which amounts to any multiple of 5 evaluates to 0 and $(7^{-1} \pmod 5)7$ evaluates to 1 $\pmod 5$.
3. Let $f(x) = x^7 \pmod{143 = 11 \cdot 13}$, where $f : \{0,1,2,\ldots,142\} \to \{0,1,2,\ldots,142\}$.
   What is the size of the range of f?
   Answer: 143. Valid encryption function, so must be bijective.
4. Let Bob have a public key of $(N,e) = (77,13)$. What is his corresponding private key d?
   Answer: $13^{-1} \pmod{60} = 37$.
5. For a natural number $n \geq 1$, if $a^7 = 3 \pmod n$ and $a^2 = 4 \pmod n$, what is $a^{11} \pmod n$?
   Answer: $48 \pmod p$. $a^{11} = (a^7)(a^2)^2 = 48 \pmod p$. Similar idea is used in repeated squaring.
6. For primes p and q, what is the probability that a random element of $\{0,\ldots,pq-1\}$ is a multiple of p or q?
   Answer: $\frac{p+q-1}{pq}$. The number of multiples of p is q and the number of multiples of q is p, and we double counted 0.

3. Polynomials++: Short Answer. 3 points each.

Write your answer in the simplest form possible. You should use only the variables in the question unless otherwise specified.

1. Consider that $P(x) = 3x^2 + a_1 x + s \pmod 5$ encodes a secret s as $P(0)$; given $P(1) = 3$, $P(2) = 4$, what is the secret?
   Answer: $s = 3 \pmod 5$. We have the equations $3 + a_1(1) + s = 3 \pmod 5$ and the equation $3(2^2) + a_1(2) + s = 4 \pmod 5$. The first implies that $a_1 = -s$, plugging into the second yields $s = 3 \pmod 5$.
2. Given polynomial $P(x)$ of degree d with r_P roots and $E(x)$ of degree k with r_E roots, what is the maximum number of roots that $Q(x) = P(x)E(x)$ can have? (Assume $P(x), E(x)$ are over reals.)
   Answer: $r_P + r_E$. The polynomials can be factored into their roots.
3. Given a polynomial $P(x)$ and 7 ordered pairs $(x_1,r_1),\ldots,(x_7,r_7)$ where $r_i = P(x_i)$ except for at x_1 and x_5. That is, $P(x_1) \neq r_1$ and $P(x_5) \neq r_5$. What is the error locator polynomial in the Berlekamp-Welch algorithm?
   Answer: $(x - x_1)(x - x_5)$.
   In this problem, we will be working with polynomials over $GF(p)$ where p is a prime, unless otherwise specified. Furthermore, when we say we pick a polynomial of degree at most k at random, we pick $P(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ where a_i are chosen uniformly at random from $\{0,\ldots,p-1\}$.
4. Assuming $k < p$, how many degree at most k polynomials are there over $GF(p)$?
   Answer: p^{k+1}. Either specify the polynomial with $k+1$ points or $k+1$coefficients where each is chosen from p possibilities.

5. Given 2 distinct values x_1 and $x_2 \pmod p$, we pick a polynomial $P(x)$ of degree at most 3 at random. What's the probability that $P(x_1) = P(x_2) \pmod p$?

   Answer: $1/p$. There are p^4 polynomials specified by 4 points, a point value assigned to $P(x_1)$ specifies two points, thus one can only pick two more, leaving p^3 total possibilities. Dividing yields the result.

6. Now suppose you have five distinct values x_1, x_2, x_3, x_4, x_5, and $P(x)$ is again a polynomial of degree at most 3 chosen at random. What is the probability that $P(x_1) = P(x_2) = P(x_3) = P(x_4) = P(x_5)$? (Careful.)

   Answer: $1/p^3$. The polynomial must be a constant of which there are p possibilities out of p^4 polynomials as we specified above.

7. How many polynomials of degree at most 5 in $GF(p)$ have **exactly** 5 fixed points? (A fixed point for $P(x)$ is a value a where $P(a) = a$. Assume $p \geq 6$.)

   Answer: $\binom{p}{5} \cdot (p-1)$. Pick the locations of the fixed points, then pick any sixth point to not be a fixed point, then the interpolated polynomial cannot have any other fixed points, else it intersects with $P(x) = x$ at six locations.

8. Let $P(x)$ be a degree exactly 4 polynomial with a leading coefficient of 1 and fixed points at $1, 2, 3$ and 4. What is $P(5)$? (Hint: consider $P(x) - x$.)

   Answer: 29. $P(x) = (x-1)(x-2)(x-3)(x-4) + x$. The product is 0 at $1,2,3,4$ and the addition of x yields the fixed points above. $P(5) = 5 + (4)(3)(2)(1) = 29$.

9. What is the probability that a randomly chosen polynomial modulo a prime p of degree at most d has exactly d distinct roots? (Assume $p > d$.)

   Answer: $\frac{\binom{p}{d}(p-1)}{p^{d+1}}$. Form the polynomial by the location of the d roots, and the leading coefficient.

4. Countability. 5 points each part.

We say a set $A \subseteq \mathbb{Q}$ is *downward closed* if, for each $x \in A$, every rational number smaller than x is also in A. Let $D_{\mathbb{Q}}$ be the set of all downward closed subsets of $\mathbb{Q}$ and let $D^L_{\mathbb{Q}}$ be the set of all downward closed subsets of $\mathbb{Q}$ *that have a largest element*.

For example, the set S of all rationals less than $\sqrt{2}$ is downward closed. It is, however, not in $D^L_{\mathbb{Q}}$ as S does not have a largest element.

1. Prove that $D^L_{\mathbb{Q}}$ is countably infinite. *(Hint: find a bijection $b : D^L_{\mathbb{Q}} \to \mathbb{Q}$)*

   Answer: As suggested in the hint, we find a bijection between $D^L_{\mathbb{Q}}$ and $\mathbb{Q}$ by letting $b(A)$ be the largest element of A. This function is onto since for any $q \in \mathbb{Q}$, the set $\{r \in Q | r \leq q\}$ is in $D^L_{\mathbb{Q}}$ and gets mapped to q by b. To prove it is one-to-one, suppose we have two sets A and B in $D^L_{\mathbb{Q}}$ such that $f(A) = f(B)$. This means that both A and B have the same largest element, q. By the definition of largest, this means that neither A nor B can have any elements larger than q. Since A and B are downward closed, we know that they both contain all elements smaller than q in addition to q itself. Hence, $A = B$, and so b is one-to-one.
   Since we have now found a bijection between $D^L_{\mathbb{Q}}$ and a countably infinite set, we have that $D^L_{\mathbb{Q}}$ is countably infinite.

2. Prove that $D_{\mathbb{Q}}$ is uncountable. *(Hint: find a one-to-one function $f : \mathbb{R} \to D_{\mathbb{Q}}$. You may use without proof the fact that for any $x, y \in \mathbb{R}$ with $x < y$, there exists a $q \in \mathbb{Q}$ such that $x < q < y$.)*

   Answer: Following the hint, we define $f : \mathbb{R} \to D_{\mathbb{Q}}$ by $f(x) = \{r \in \mathbb{Q} | r < x\}$. To show that this function is one-to-one, let $x, y \in \mathbb{R}$ with $x \neq y$ by $f(x) = f(y)$; we can assume WLOG that $x < y$. By the hint, we know that there is some $q \in \mathbb{Q}$ with $x < q < y$. But then we must have that $q \in f(y)$ and

that $q \notin f(x)$. Hence, $f(x) \neq f(y)$, so f is one-to-one.
We have now found an injection from an uncountable set to $D_{\mathbb{Q}}$, and so can conclude that $D_{\mathbb{Q}}$ is uncountable.

5. Computability *I love CS70*. 6 points

The program `Test70(P)` takes in another program `P` as input and determines whether the program `P` returns "I love CS70" on exactly 70 inputs. That is, `Test70(P)` will return true if `P` returns "I love CS70" on 70 different inputs, and does not return it for all other inputs. Otherwise, `Test70(P)` returns False. Show that `Test70(P)` cannot exist.

Answer: We can use `Test70(P)` as a subroutine for `TestHalt(P, x)`

```
def TestHalt(P, x):
  def P'(y):
      P(x)
      if 0 < y <= 70:
          return "I love CS70"
      else:
          loop forever /* Do nothing */
  return Test70(P')
```

6. Counting. 3 points each.

Please state your answer in the simplest form possible. Complicated sums are not necessary for this problem.

1. An outfit consists of a shirt, hat, and skirt where each comes in three colors: blue, gold, and white. How many outfits are there where items are not all the same color? In particular, one can wear a blue shirt, gold hat, and a gold skirt, but one cannot wear all gold clothes.
   Answer: 24. There are 27 total possibilities, but 3 are unwearable.
2. How many permutations of the numbers 1 through n are there?
   Answer: $n!$
3. How many permutations of the numbers 1 through n are there such that 1 comes before 2 and after 3? Assume $n > 3$.
   Answer: $n!/6$. $\binom{n}{3}$ ways to pick positions for 1, 2 and 3, and $(n-3)!$ ways to permute the remaining objects.
   For each permutation σ of 1 through n, let $\sigma(i)$ denote the value at position i. For example, if the permutation is $2,4,1,3$, we have $\sigma(1) = 2$ and $\sigma(2) = 4$.
4. For a fixed $1 \leq k \leq n$, how many permutations σ of 1 through n are there where for all $i < k$, $\sigma(i) < \sigma(k)$? Express your answers in terms of n and k.
   Answer: $n!/k$. $1/k$ of the permutations have $\sigma(k)$ being the largest of the first k elements in $\sigma(\cdot)$.
5. How many permutations of 1 through n are there such that for each i, $\sigma(\sigma(i)) = i$ and $\sigma(i) \neq i$? (For example, the permutation $3,4,1,2$ is such a permutation, since for example $\sigma(\sigma(1)) = \sigma(3) = 1$. You may assume n is even.)
   Answer: $\frac{n!}{2^{n/2}(n/2)!}$. This is the number of ways to swap, so we can pick them out in pairs, which is

$$\binom{n}{2}\binom{n-2}{2}\cdots\binom{2}{2}$$

   But we overcounted since the order in which we pick them doesn't matter. So divide by $(n/2)!$.

7. Combinatorial Proof. 8 points.

Prove the following combinatorial identity using a combinatorial proof:

$$\sum_{k=2}^{n-5} \binom{k}{2}\binom{n-k}{5} = \binom{n+1}{8}$$

(Hint: Consider selecting 8 elements from $\{1,\ldots,n+1\}$.)

Answer: The right hand side counts number of ways to pick 8 elements from $\{1,2,3,...,n+1\}$.

Each term on the left hand side sets the 3-rd **smallest** element to be $k+1$, and picks the remaining elements in the set. There are k numbers **smaller than** $k+1$ left to choose from for the smallest two, and $n-k$ numbers **larger than** $k+1$ left for the other 5.

Summing across all possible choices for the 3-rd smallest element gives us the desired result.

8. Probability (and counting): Short Answer. 3 points each.

1. For the probability space consisting of rolling two six-sided dice, the event A that the dice add up to 3 is $\{(1,2),(2,1)\}$. What is the event that the dice sum to 5?
   Answer: $\{(1,4),(2,3),(3,2),(4,1)\}$. Answer is self explanatory.
2. When rolling two six sided dice, what is the probability that the dice sum to 5?
   Answer: $1/9$. Four possibilities out of 36.
3. Consider rolling a six-sided die 5 times, what is the probability that you see a 2 exactly twice? (An expression here is fine, no need to simplify.)
   Answer: $(\frac{\binom{5}{2}5^3}{6^5})$. $\binom{5}{2}$ places where the 2 appears, and the other three places can only have 5 possibilities.
4. For events A and B, where $Pr[A\cup B] = .6$ and $Pr[A\cap B] = .2$, what is $Pr[A]+Pr[B]$?
   Answer: .8. From inclusion-exclusion, we have $Pr[A]+Pr[B]-Pr[A\cap B] = Pr[A\cup B]$. Substituting in the given values for $Pr[A\cup B]$ and $Pr[A\cap B]$ and solving for $Pr[A]+Pr[B]$ gives us 0.8.
5. For events A and B, where $Pr[A|B] = .4$, $Pr[A|\overline{B}] = .8$, and $Pr[B] = .25$, what is $Pr[A]$?
   Answer: .7. $Pr[A] = Pr[A|B]Pr[B]+Pr[A|\overline{B}]Pr[\overline{B}] = .4(.25)+.8(.75) = .7$.
6. Given that you toss two coins with heads probabilities p and q, what the probability that both are heads? (Assume they are indendependent coins.)
   Answer: pq. They are independent.
7. Consider two coins with heads probability $1/3$ (coin A) and $2/3$ (coin B). If the coins are tossed in random order, and the result is heads and then tails (i.e., the outcome is 'HT'), what is the probability that the coin A was tossed first? Answer as a simplified fraction. (Note that it is going to be less than $1/2$.)
   Answer: 1/5. $Pr[A|HT] = \frac{Pr[A\cap'HT']}{Pr[HT]} = \frac{Pr['HT'|A]Pr[A]}{Pr['HT']} = \frac{1/9}{1/9+4/9} = 1/5$.
8. For an event A with non-zero probability what is $Pr[A]$ if A is independent of itself?
   Answer: 1. The only events that can be independent of themselves have $Pr[A] = 0$ or $Pr[A] = 1$. To be independent, we must have $P[A\cap A] = Pr[A]\times Pr[A]$, we have $Pr[A\cap A] = Pr[A] = x$, where $x = x^2$, which implies that $(x-1)x = 0$ which is only satisfied when $x = 1$ or $x = 0$.

9. You have 5 black cards and 5 red cards. You shuffle thoroughly and draw five of them. What's the probability that the black cards are consecutive and red cards are consecutive? Examples that satisfy the condition are RRRRR, BBRRR, and RRRRB. However, RBRRR and BBBRB do not satisfy the condition. Express your answer as a simplified fraction.

   Answer: $\frac{(2^5-2)2+2}{\binom{10}{5}} = \frac{31}{126}$. Let's order the deck, and there are $\binom{10}{5}$ orderings by enumerating the locations of the R's. We will count how many or these orderings satisfy the condition for the first five cards. If the last five are all the same color, there is one way to fill in the first five. For each of the other 2^5-2 ways to fill in the last five cards, there are two ways to fill in the first five. Then we get the expression in the solution.

10. Jonathan, Jerry, and Bob are deciding which of the four courses, 61A, 61B, 61C, and 70, to enroll in next semester. They want to sign up for the courses such that no course is taken by all three. However, for each pair of people, there should be at least one course that they take together. How many ways can they sign up for the courses, (ignoring pre-requisites)? Note that it is possible for some class to not be taken by any of the three. Answer as a single positive integer. The chart below shows an example enrollment that satisfies the conditions.

	61A	61B	61C	70
Jonathan	Y	N	Y	Y
Jerry	N	Y	N	Y
Bob	Y	Y	N	N

   Answer: 132. There are three cases that are of interest to us. The first case is that each pair signs up for a different class, and then nobody takes the fourth class. There are $4 \cdot 3 \cdot 2$ ways for each pair to sign up for a class. That gives us 24 for this case.

   The second case is that each pair signs up for a different class, and then one person enrolls in the fourth class. There are $4 \cdot 3 \cdot 2$ ways again for each pair to sign up for the class they take together, and then for the last class, there are 3 ways to choose the person that takes that class. That gives us 72 for this case.

   The last case is where that fourth class is taken by two people. We first pick which pair of people will take two classes together, and then pick which two classes they will take together. This gives us $\binom{3}{2} \cdot \binom{4}{2}$. Then, for the two remaining pairs, we decide which classes they will take in $2 \cdot 1$ ways. This case then totals to $3 \cdot 6 \cdot 2 = 36$.

   Adding together these cases gives us $24 + 72 + 36 = 132$.

9. Probability: Quick Argument. 4 points.

1. **[Complementary Independence]**

   Prove—in a succinct, yet clear and convincing fashion—that the following assertion is true:

   > If events A and B are independent, then so are the events A and B^c, where B^c denotes the complement of B.

   Answer: $Pr[A \cap B^c] = Pr[A] - Pr[A \cap B] = Pr[A] - Pr[A]Pr[B] = Pr[A](1 - Pr[B]) = Pr[A]Pr[B^c]$. We used the independence of A and B, $Pr[A \cap B] = Pr[A] \times Pr[B]$, in the second equality.

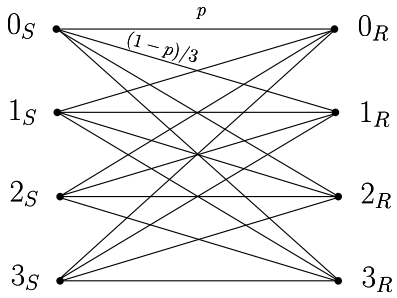
Nothing written below will be considered in evaluating your work. You're limited to the space given above.

10. [Digital Communication Errors]. 3 points each.

In each tick of a system clock, a digital communication transmitter is *equally likely* to transmit only a 0, a 1, a 2, or a 3. That is, we have $P[i_S] = 1/4$ for all i_S.

The communication channel is prone to error, so the number the transmitter sends is not necessarily what arrives at the receiver (shown on the right side of the diagram). With probability p, each number that is sent is received intact (without error), and with probability $1-p$ is corrupted into the other numbers with *equal likelihood*. Specifically, for all $i, j \in \{0,1,2,3\}$, we have

$$Pr[j_R|i_S] = \begin{cases} p & \text{if } i = j \\ \dfrac{(1-p)}{3} & \text{if } i \neq j, \end{cases}$$



where $Pr[j_R|i_S]$ is the conditional probability that the number j is received given that the number i is sent. The figure on the right indicates that source numbers are either transmitted correctly (horizontal lines) with probability p or corrupted (diagonal lines) with probability $(1-p)/3$ for each other number.

1. Determine $Pr[0_R]$, the probability the receiver receives a 0 on any randomly-selected tick of the clock. **Answer:** $1/4$. This is $Pr[0_S \cap 0_R] + Pr[\overline{0_S} \cap 0_R] = Pr[0_R|0_S]Pr[0_S] + Pr[0_R|\overline{0_S}] = (p)(1/4) + \frac{(1-p)}{3}(3/4) = 1/4$. That is probability of recieving a 0, when one was sent is $1/4 \times p$, the probability of recieving a 0, when a non-zero is sent is $3/4 \times \frac{(1-p)}{3}$.
2. Determine $Pr[\varepsilon]$, the probability of an error occuring on any randomly-selected tick of the clock. **Answer:** $(1-p)$. The probability of error is the probability of a cross edge weighted by the start states. Since the cross edges are $(1-p)$ for every starting state, we have this as the probability of error.
3. Determine a reasonably simple expression for $Pr[A_n]$, where A_n denotes the event that there is at least one error in a sequence of n transmissions at n ticks of the clock. **Answer:** $1-(p)^n = 1-(p)^n$. This is the complement of the probability of no errors which is the product of the probability of no error, which is the straight edge.
4. Determine a reasonably simple expression for $Pr[i_S|j_R]$ where $i \neq j$ (in the box).
   Answer: $(1-p)/3$.
   $P(i_S|j_R) = P(j_R|i_S) \times Pr(i_S)/P(j_R) = Pr(j_R|i_S) \times (1/4)/(1/4) = Pr(j_R|i_S)$. Here, we used $Pr(j_R) = 1/4$ due to symmetry. One could sum over the possible inputs, but since they are uniform and the conditional probabilities are uniform, the probability distribution over outputs is uniform.

11. Probability: nihilism, almost. 17 points: 3/3/4/4/3

While eating chicken nuggets at McDonald's, Jonathan challenges Emaan to a game.

Jonathan has a standard 52-card deck, with 26 red cards and 26 black cards. He shuffles the deck and will flip cards one at a time from the top.

Emaan's goal is to call when Jonathan is going to flip over a red card. Before each flip, Emaan can either "pass", meaning Jonathan flips over the next card for Emaan to see, or "bet", meaning Jonathan shows Emaan the next card and if it is red, Emaan wins, and if it is black, he loses. If Emaan never calls "bet", then he loses.

Emaan starts thinking of some strategies, like, he's going to wait until he sees 5 more black cards than red cards, and then once he does, he will call "bet".

1. Let's say Emaan has seen 15 black cards and 10 red cards. If he calls bet, what is the chance he wins the game?

   Answer: $16/27$. There are 16 red cards left out of a total of 27.

2. Let's say Emaan has seen b black cards and r red cards so far, and there are still cards remaining. What is the probability that the *last card* in the deck is red?

   Answer: The probability that the next card is red is $\frac{26-r}{52-b-r}$. This is because of symmetry, so the probability that the next card is red is the same as the probability that the last card is red.

3. Use the previous part to show that no matter what strategy Emaan employs, his chance of winning is always $\frac{1}{2}$.

   Answer: We have now shown that the game is equivalent to "when you say bet, you win if the last card is red". Therefore, there is no action you can take after the game starts to alter the probability that the last card is red.

   To rigorize this argument, let us enumerate all sequences of card flips that will result in a victory for Emaan. For example, if Emaan's strategy is: wait until there are 3 more black cards than red cards, then bet, and if that never happens, then bet on the last card. Then, one possible successful ordering of cards would be BBBR. Adding together the probability of all of these sequences would yield the probability that Emaan wins the game. Now notice that for each of these successful ordering of cards, the probability doesn't change if you swap the bet card with the last card. Going off of our example, the probability of drawing BBBR, is the same as the probability of drawing BBB and having the last card be red. Therefore, adding together the probabilities yields the probability that the last card is going to be red, which is $\frac{1}{2}$. Therefore, no matter what strategy Emaan employs, the probability he wins is always $\frac{1}{2}$.

4. Now let's change the game. Now Emaan's goal is to get the next card to be the same color as the previous card. So, when he calls "bet", he wins if the next card Jonathan shows is the same color as the previous card shown. Therefore, Emaan cannot "bet" on the first turn, he must "pass", since there is no previous card. Prove that Emaan might as well wait until the last two cards before betting. (Note that here Emaan will either bet when two cards are left or when one card is left.)

   Answer: WLOG, let's say the last seen card is black, and there are r red cards and b black cards remaining. If he bets, he loses if the next card is red, with probability $\frac{r}{r+b}$.

   If the last two cards are the same color, Emaan knows to wait one more flip and he will win.

   Otherwise, say Emaan bets at this point, since otherwise he loses for sure.

   On the last two cards, say the third to last card is black, then he loses if the last two cards are red then black. He loses with probability

   $$\frac{r}{r+b} \cdot \frac{b}{r+b-1}.$$

   If the third to last card is red, then a black red ordering is bad for Emaan. Note that this ordering also has the above probability. So, either way Emaan has the same chance of losing.

   The only way in which $\frac{b}{r+b-1} > 1$ is if $b > r+b-1$, or $r = 0$. But if $r = 0$, then the probability of losing is 0 both cases. So Emaan might as well wait until the last two.

5. Given Emaan plays optimally, find the probability Emaan wins.

   Answer: $\frac{38}{51}$. As noted, if the last two cards are same color, Emaan waits one turn, and then bet. Otherwise, coin flip on the upcoming card. Gives us $\frac{25}{51} + \frac{1}{2} \cdot \frac{26}{51}$