1 Implication

Note 0
Note 1

Which of the following implications are always true, regardless of P? Give a counterexample for each false assertion (i.e. come up with a statement $P(x,y)$ that would make the implication false).

(a) $\forall x \forall y P(x,y) \implies \forall y \forall x P(x,y)$.

(b) $\forall x \exists y P(x,y) \implies \exists y \forall x P(x,y)$.

(c) $\exists x \forall y P(x,y) \implies \forall y \exists x P(x,y)$.

2 Pebbles

Note 2

Suppose you have a rectangular 2D array of pebbles, where each pebble is either red or blue. Suppose that for every way of choosing one pebble from each column, there exists a red pebble among the chosen ones.

Prove that there must exist an all-red column.

3 Fibonacci for Home

Note 3

Recall, the Fibonacci numbers, defined recursively as $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-2} + F_{n-1}$.

Prove that every third Fibonacci number (starting from F_3) is even. For example, $F_3 = 2$ is even and $F_6 = 8$ is even.

4 Stable Matching III

Note 4

(a) True or False?

(i) If a candidate accidentally rejects a job they prefer on a given day, then the algorithm still always ends with a matching.

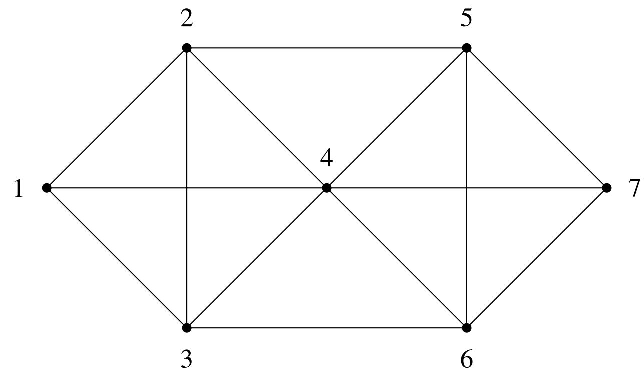
(ii) The Propose-and-Reject Algorithm never produces a candidate-optimal matching.

(iii) If the same job is last on the preference list of every candidate, the job must end up with its least preferred candidate in any possible stable matching.

(b) As you've seen from lecture, the jobs-proposing Propose-and-Reject Algorithm produces an employer-optimal stable matching. Let's see if the candidates have any way of improving their standing. Suppose exactly one of the candidates has the power to arbitrarily reject one proposal, regardless of which job they have on their string (if any). Construct an example that illustrates the following: for any $n \geq 2$, there exists a stable matching instance for which using this power helps **every** candidate, i.e. every candidate gets a better job than they would have gotten under the jobs-proposing Propose-and-Reject Algorithm.

5 Eulerian Tour and Eulerian Walk

Note 5



(a) Is there an Eulerian tour in the graph above? If no, give justification. If yes, provide an example.

(b) Is there an Eulerian walk in the graph above? An Eulerian walk is a walk that uses each edge exactly once. If no, give justification. If yes, provide an example.

(c) What is the condition that there is an Eulerian walk in an undirected graph? Briefly justify your answer.

6 Hypercubes

Note 5

The vertex set of the n-dimensional hypercube $G = (V,E)$ is given by $V = \{0,1\}^n$ (recall that $\{0,1\}^n$ denotes the set of all n-bit strings). There is an edge between two vertices x and y if and only if x and y differ in exactly one bit position.

(a) Draw 1-, 2-, and 3-dimensional hypercubes and label the vertices using the corresponding bit strings.

(b) Show that the edges of an n-dimensional hypercube can be colored using n colors so that no pair of edges sharing a common vertex have the same color.

(c) Show that for any $n \geq 1$, the n-dimensional hypercube is bipartite.

7 Fibonacci GCD

Note 6

(a) Prove that, for positive integers x and y, if $x \geq y$, then $\gcd(x,y) = \gcd(y,x-y)$.

(b) The Fibonacci sequence is given by $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. Prove that, for all $n \geq 1$, $\gcd(F_n, F_{n-1}) = 1$.

8 Baby Fermat

Note 6

Assume that a does have a multiplicative inverse mod m. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the infinite sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions.

(**Hint:** Consider the Pigeonhole Principle.)

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what is the value of $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

9 RSA Gone Wrong?

Note 7

Alice wants to send a message to Bob using RSA. Unfortunately for them, there is an eavesdropper Eve, and Eve has evolved. **cue dramatic music**

(a) Suppose that Eve has a magical eye that can see the prime factors of any number, no matter how large or small. Can Eve obtain Alice's original message? If so, how?

(b) Suppose that Eve acquires the modular n^{th}-root-inator, which allows her to find the n^{th} root of any number in modular arithmetic. Precisely, when given n and $a^n \pmod{p}$, Eve can use the modular n^{th}-root-inator to obtain a. Can Eve obtain Alice's original message? If so, how?

Alice and Bob decide to modify their RSA scheme, but they forgot to consider whether their scheme remains both correct and secure!

(c) Suppose Alice and Bob continue to use large primes p, q, but they choose to use $e = 2$. Is their scheme correct (they can encrypt and decrypt to recover the original message)? If so, is it secure (Eve cannot obtain the original message)?

(d) Suppose Alice wants to send a Bob her 3-digit code on the back of her credit card, with the standard RSA scheme. (All codes on the back of credit cards are 3 digits.) Is their scheme correct? If so, is it secure?

10 Secrets in the United Nations

Note 8

A vault in the United Nations can be opened with a secret combination $s \in \mathbb{Z}$. In only two situations should this vault be opened: (i) all 193 member countries must agree, or (ii) at least 55 countries, plus the U.N. Secretary-General, must agree.

(a) Propose a scheme that gives private information to the Secretary-General and all 193 member countries so that the secret combination s can only be recovered under either one of the two specified conditions.

(b) The General Assembly of the UN decides to add an extra level of security: each of the 193 member countries has a delegation of 12 representatives, all of whom must agree in order for that country to help open the vault. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary-General and to each representative of each country.

11 Berlekamp-Welch Algorithm with Fewer Errors

Note 9

In class we derived how the Berlekamp-Welch algorithm can be used to correct k general errors, given $n+2k$ points transmitted. In real life, it is usually difficult to determine the precise number of errors that will occur. What if we have less than k errors? This is a follow up to the exercise posed in the notes.

Suppose Alice wants to send 1 message to Bob, $m_1 = 4$, and guard against 1 general error. She encodes the message with the polynomial $P(x) = 4$, then sends the codeword $P(1), P(2), P(3) = (4,4,4)$ to Bob.

(a) Suppose Bob receives $(5,4,4)$. Without performing Berlekamp-Welch explicitly, help Bob find $E(x)$ and $Q(x)$, using only the information Bob (the recipient) knows.

(b) Now, suppose there were no general errors, and Bob receives $(4,4,4)$. Show that the $Q(x)$ and $E(x)$ that you found in part (a) still satisfies $Q(i) = r_i E(i)$ for all $i = 1,2,3$.

(c) Verify that $E(x) = x-2$, $Q(x) = 4x-8$ also satisfies $Q(i) = r_i E(i)$ for all $i = 1,2,3$.

(d) Suppose Bob tries to decode his received packets $(4,4,4)$. From what you showed in parts (b)–(c), what will happen when Bob tries to solve for the unknown coefficients of $Q(x)$ and $E(x)$?

(e) Prove that in general, no matter what solution of $Q(x)$ and $E(x)$ Bob obtains, the recovered $P(x)$ will always be the same.

12 Counting Produce

Note 10

(a) Let d and y be fixed positive integers. How many solutions does $x_0 + x_1 + \cdots + x_d = y$ have, if each x_i must be a non-negative integer?

(b) Let d and y be fixed positive integers. How many solutions does $x_0 + x_1 + \cdots + x_d = y$ have, if each x_i must be a positive integer?

Armed with the above knowledge, you visit Berkeley Bowl. Suppose you want to buy f fruits. Count how many ways you can do this, assuming:

(c) There are peaches and apples at the market.

(d) There are peaches, apples, oranges, and pears at the market.

(e) There are t types of fruits at the market, and you want to end up with at least two different types of fruit.

13 CS70: The Musical

Note 10

Edward, one of the previous head TA's, has been hard at work on his latest project, *CS70: The Musical*. It's now time for him to select a cast, crew, and directing team to help him make his dream a reality.

(a) First, Edward would like to select directors for his musical. He has received applications from $2n$ directors. Use this to provide a combinatorial argument that proves the following identity:

$$\binom{2n}{2} = 2\binom{n}{2} + n^2.$$

(b) Edward would now like to select a crew out of n people. Use this to provide a combinatorial argument that proves the following identity: (this is called Pascal's Identity)

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

(c) There are n actors lined up outside of Edward's office, and they would like a role in the musical (including a lead role). However, he is unsure of how many individuals he would like to cast. Use this to provide a combinatorial argument that proves the following identity:

$$\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$$

(d) Generalizing the previous part, provide a combinatorial argument that proves the following identity:

$$\sum_{k=j}^{n} \binom{n}{k}\binom{k}{j} = 2^{n-j}\binom{n}{j}.$$

14 Counting Cartesian Products

Note 11

For two sets A and B, define the cartesian product as $A \times B = \{(a,b) : a \in A, b \in B\}$.

(a) Given two countable sets A and B, prove that $A \times B$ is countable.

(b) Given a finite number of countable sets $A_1, A_2, \ldots, A_n$, prove that

$$A_1 \times A_2 \times \cdots \times A_n$$

is countable.

(c) Consider a countably infinite number of finite sets: $B_1, B_2, \ldots$ for which each set has at least 2 elements. Prove that $B_1 \times B_2 \times \cdots$ is uncountable.

15 N-Bit

Note 12

Let N-Bit be a program that takes in a program P and an input x and outputs "true" if the program ever directly assigns a variable to an n-bit number and "false" otherwise. Can N-Bit exist? If so, describe the procedure, and if not, prove that it cannot exist. (Hint: model off of the proof that TestHalt cannot exist)

16 Intransitive Dice

Note 13

You're playing a game with your friend Bob, who has a set of three dice. You'll each choose a different die, roll it, and whoever had the higher result wins. The dice have sides as follows:

- Die A has sides 2, 2, 4, 4, 9, and 9.
- Die B has sides 1, 1, 6, 6, 8, and 8.
- Die C has sides 3, 3, 5, 5, 7, and 7.

(a) Suppose you have chosen die A and Bob has chosen die B. What is the probability that you win? *Hint: It may be easier to work with a sample space smaller than* 6×6.

(b) Suppose you have chosen die B and Bob has chosen die C. What is the probability that you win?

(c) Suppose you have chosen die C and Bob has chosen die A. What is the probability that you win?

(d) Bob offers to let you choose your die first so that you can choose the best one. Is this an offer your should accept? Why or why not?

17 Pairwise Independence

Note 14

Recall that the events A_1, A_2, and A_3 are *pairwise independent* if for all $i \neq j$, A_i is independent of A_j. However, pairwise independence is a weaker statement than *mutual independence*, which requires the additional condition that $\mathbb{P}[A_1 \cap A_2 \cap A_3] = \mathbb{P}[A_1]\,\mathbb{P}[A_2]\,\mathbb{P}[A_3]$.

Suppose you roll two fair six-sided dice. Let A_1 be the event that the first die lands on 1, let A_2 be the event that the second die lands on 6, and let A_3 be the event that the two dice sum to 7.

(a) Compute $\mathbb{P}[A_1]$, $\mathbb{P}[A_2]$, and $\mathbb{P}[A_3]$.

(b) Are A_1 and A_2 independent?

(c) Are A_2 and A_3 independent?

(d) Are A_1, A_2, and A_3 pairwise independent?

(e) Are A_1, A_2, and A_3 mutually independent?

18 Aces

Note 14

Consider a standard 52-card deck of cards, which has 4 suits (hearts, diamonds, clubs, and spades) with 13 cards in each suit. Each suit has one ace. Hearts and diamonds are red, while clubs and spades are black.

(a) Find the probability of getting an ace or a red card, when drawing a single card.

(b) Find the probability of getting an ace or a spade, but not both, when drawing a single card.

(c) Find the probability of getting the ace of diamonds when drawing a 5 card hand.

(d) Find the probability of getting exactly 2 aces when drawing a 5 card hand.

(e) Find the probability of getting at least 1 ace when drawing a 5 card hand.

(f) Find the probability of getting at least 1 ace or at least 1 heart when drawing a 5 card hand.

19 Planetary Party

Note 15

For this question, you may use a calculator.

(a) Suppose we are at party on a planet where every year is 2849 days. If 30 people attend this party, what is the exact probability that at least two people will share the same birthday? You may leave your answer as an unevaluated expression.

(b) From lecture, we know that given n bins and m balls, $\mathbb{P}[\text{no collision}] \approx \exp(-m^2/(2n))$. Using this, give an approximation for the probability in part (a).

(c) Using the approximation in part (b), what is the approximate minimum number of people that need to attend this party to ensure that the probability that any two people share a birthday is at least 0.5?

(d) Now suppose that 70 people attend this party. What the is probability that none of these 70 individuals have the same birthday? You can use the approximation you used in the previous parts.

20 Linearity

Note 16

Solve each of the following problems using linearity of expectation. Explain your methods clearly.

(a) In an arcade, you play game A 10 times and game B 20 times. Each time you play game A, you win with probability $1/3$ (independently of the other times), and if you win you get 3 tickets (redeemable for prizes), and if you lose you get 0 tickets. Game B is similar, but you win with probability $1/5$, and if you win you get 4 tickets. What is the expected total number of tickets you receive?

(b) A monkey types at a 26-letter keyboard with one key corresponding to each of the lower-case English letters. Each keystroke is chosen independently and uniformly at random from the 26 possibilities. If the monkey types 1 million letters, what is the expected number of times the sequence "book" appears? (*Hint*: Consider where the sequence "book" can appear in the string.)

21 Number Game

Note 17

Sinho and Vrettos are playing a game where they each choose an integer uniformly at random from $[0,100]$, then whoever has the larger number wins (in the event of a tie, they replay). However, Vrettos doesn't like losing, so he's rigged his random number generator such that it instead picks randomly from the integers between Sinho's number and 100. Let S be Sinho's number and V be Vrettos' number.

(a) What is $\mathbb{E}[S]$?

(b) What is $\mathbb{E}[V \mid S = s]$, where s is any constant such that $0 \leq s \leq 100$?

(c) What is $\mathbb{E}[V]$?

22 Working with the Law of Large Numbers

Note 19

(a) A fair coin is tossed multiple times and you win a prize if there are more than 60% heads. Which number of tosses would you prefer: 10 tosses or 100 tosses? Explain.

(b) A fair coin is tossed multiple times and you win a prize if there are more than 40% heads. Which number of tosses would you prefer: 10 tosses or 100 tosses? Explain.

(c) A fair coin is tossed multiple times and you win a prize if there are between 40% and 60% heads. Which number of tosses would you prefer: 10 tosses or 100 tosses? Explain.

(d) A fair coin is tossed multiple times and you win a prize if there are exactly 50% heads. Which number of tosses would you prefer: 10 tosses or 100 tosses? Explain.

23 Shuttles and Taxis at Airport

Note 18

In front of terminal 3 at San Francisco Airport is a pickup area where shuttles and taxis arrive according to a Poisson distribution. The shuttles arrive at a rate $\lambda_1 = 1/20$ (i.e. 1 shuttle per 20 minutes) and the taxis arrive at a rate $\lambda_2 = 1/10$ (i.e. 1 taxi per 10 minutes) starting at 00:00. The shuttles and the taxis arrive independently.

(a) Write in terms of a Poisson distribution, the distribution of taxis between 00:00 and 00:01:

(b) What is the distribution of the following:

  (i) The number of taxis that arrive between times 00:00 and 00:20?

  (ii) The number of shuttles that arrive between times 00:00 and 00:20?

  (iii) The total number of vehicles (shuttles and taxis) that arrive between times 00:00 and 00:20?

(c) What is the probability that exactly 1 shuttle and 3 taxis arrive between times 00:00 and 00:20?

(d) Given that exactly 1 pickup vehicle arrived between times 00:00 and 00:20, what is the conditional probability that this vehicle was a taxi?

(e) Suppose you reach the pickup area at 00:20. You learn that you missed 3 taxis and 1 shuttle in those 20 minutes. What is the probability that you need to wait for more than 10 mins until either a shuttle or a taxi arrives?

24 Continuous Joint Densities

Note 20

The joint probability density function of two random variables X and Y is given by $f(x,y) = Cxy$ for $0 \le x \le 1, 0 \le y \le 2$, and 0 otherwise, where C is a constant.

(a) Find the value of C that ensures that $f(x,y)$ is indeed a probability density function.

(b) Find $f_X(x)$, the marginal density function of X.

(c) Calculate $\mathbb{E}[XY]$.

25 Erasures, Bounds, and Probabilities

Note 19
Note 20

Alice is sending 1000 bits to Bob. The probability that a bit gets erased is p, and the erasure of each bit is independent of the others.

Alice is using a scheme that can tolerate up to one-fifth of the bits being erased. That is, as long as Bob receives at least 801 of the 1000 bits correctly, he can decode Alice's message.

In other words, Bob becomes unable to decode Alice's message only if 200 or more bits are erased. We call this a "communication breakdown", and we want the probability of a communication breakdown to be at most 10^{-6}.

For this question, you may use a calculator.

(a) Use Chebyshev's inequality to upper bound p such that the probability of a communications breakdown is at most 10^{-6}.

(b) As the CLT would suggest, approximate the fraction of erasures by a Gaussian random variable (with suitable mean and variance). Use this to find an approximate bound for p such that the probability of a communications breakdown is at most 10^{-6}.

You may use that $\Phi^{-1}(1-10^{-6}) \approx 4.753$.

26 Skipping Stones

Note 21

We consider a simple Markov chain model for skipping stones on a river, but with a twist: instead of trying to make the stone travel as far as possible, you want the stone to hit a target. Let the set of states be $\mathscr{X} = \{1,2,3,4,5\}$. State 3 represents the target, while states 4 and 5 indicate that you have overshot your target (and thus end in failure). Assume that from states 1 and 2, the stone is equally likely to skip forward one, two, or three steps forward. If the stone starts from state 1, compute the probability of reaching our target before overshooting, i.e. the probability of $\{3\}$ before $\{4,5\}$.

27 Can it be a Markov Chain?

Note 21

(a) A fly flies in a straight line in unit-length increments. Each second it moves to the left with probability 0.3, right with probability 0.3, and stays put with probability 0.4. There are two spiders at positions 1 and m and if the fly lands in either of those positions it is captured.

Given that the fly starts at state i, where $1 < i < m$, model this process as a Markov Chain. (Don't forget to specify the initial distribution!)

(b) Take the same scenario as in the previous part with $m = 4$. Let $Y_n = 0$ if at time n the fly is in position 1 or 2 and let $Y_n = 1$ if at time n the fly is in position 3 or 4.

Provide the state space for Y_n. Is the process Y_n a Markov chain?