Class Exercises: 2019-09-17

1. **(Roster and Set-Builder Notations)** Here are some sets described in set-builder notation. Describe each of them in roster notation. Note: $\mathbb{Z}$ denotes the set of all integers.

   1.1. $\{k \in \mathbb{Z} : 10 \le k \le 99 \text{ and the sum of the digits of } k \text{ is } 9\}$

   1.2. $\left\{x \in \mathbb{Z} : 0 \le x \le 10 \text{ and } \dfrac{x}{2} \notin \mathbb{Z}\right\}$

   1.3. $\{S : S \subseteq \{a, b, c\}\}$

   1.4. $\{S : S \subseteq \{a, b, c, d\} \text{ and } |S| \text{ is even}\}$

2. **(Basic Operations on Sets)** Let $A = \{1, 2, 3, 4, 5, 6\}, B = \{2, 4, 6, 8, 10\}$ and $C = \{0, 1, 5, 6, 9\}$. In the following subproblems, you must show your steps for those cases where the statement asks you to "verify" an equation. For the rest, you do not need to show any steps.

   2.1. What is $A \cup B$? What is $(A \cup B) \cup C$?

   2.2. What is $B \cup C$? What is $A \cup (B \cup C)$?

   2.3. What is $A \cap B \cap C$?

   2.4. Verify by direct computation that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

   2.5. What is $A - B$? What is $B - C$?

   2.6. What is $(A - B) - C$? What is $A - (B - C)$?

   2.7. Verify by direct computation that $(A - B) - C = A - (B \cup C)$.

   2.8. Verify by direct computation that $A - (B - C) = (A - B) \cup (A \cap B \cap C)$.

3. **(Further Set Operations and Thinking)** For each of the following equations involving arbitrary sets A, B, C, and D, state whether or not it always holds. Further ...

   - If you say *no*, justify your answer by giving a specific counterexample.
   - If you say *yes*, justify your answer by writing out your reasoning in English sentences peppered with some math. Explain this reasoning to your group's Discrete Math Ninja. (This kind of justification is called a *mathematical proof*. This entire course is about learning to write *good* mathematical proofs.)

   3.1. $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$.

   3.2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

   3.3. $(A - C) \cap (C - B) = \varnothing$.

CS 30
Fall 2019
Discrete Mathematics

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

Class Exercises: 2019-09-19

1. **(Proving Set Equality)** Let A, B, and C be arbitrary sets. Prove each of the following statements.

   I want each group to write down at least one of these proofs in full English sentences. Ninjas, please ensure that your group does this (and give them plenty of help if needed).

   1.1. $A \times (B - C) = A \times B - A \times C$. ◁ *Operator precedence: "×" has higher precedence than "−".*

   1.2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. ◁ *We need parentheses because "∪" and "∩" have equal precedence.*

2. **(Symmetric and transitive relations)** A relation R with the property that

   $$\text{whenever } (a,b) \in R, \text{ we also have } (b,a) \in R$$

   is called a *symmetric relation*. A relation S with the property that

   $$\text{whenever } (a,b) \in R \text{ and } (b,c) \in R, \text{ we also have } (a,c) \in R$$

   is called a *transitive relation*. For each of the following relations, state whether or not it is (a) symmetric; (b) transitive. Whenever your answer is "no", explain why. This means that if, for instance, you say that a relation R is not symmetric, you must exhibit a pair (a,b) such that $(a,b) \in R$ but $(b,a) \notin R$.

   2.1. The relation "divides", on $\mathbb{N}$ ("m divides n" means "n/m is an integer").

   2.2. The relation "is disjoint from", on $\mathscr{P}(\mathbb{Z})$.

   2.3. The relation "is no larger than", on $\mathscr{P}(\mathbb{Z})$. We say that A is no larger than B when one of the following holds:
   - A and B are both finite sets, and $|A| \le |B|$.
   - A is a finite set and B is an infinite set.
   - A and B are both infinite sets.

3. **(Understanding functions)** Let $S = \{$"RED", "BLUE", "GREEN", "YELLOW", "ORANGE", "BLACK"$\}$ and $T = \{1,2,3,4,5,6\}$. Consider the function $\text{len}\colon S \to T$ given by $\text{len}(s)$ = the length of the string s (as in the Python programming language).

   3.1. Describe the "len" function pictorially, using arrows, as done in class.

   3.2. Reverse the directions of all the arrows in your picture. Does this new picture represent another function $g\colon T \to S$? If not, why not?

CS 30
Fall 2019
Discrete Mathematics

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

Class Exercises: 2019-09-24

1. Let $f : B \to C$ and $g : A \to B$ be two bijections, where A, B, and C are arbitrary nonempty sets.

   1.1. Prove that $f \circ g$ is a bijection.

   1.2. Recall that every bijection has an inverse function. Prove that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

2. Define the function $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(m) = \begin{cases} (m+1)/2\,, & \text{if } m \text{ is odd,} \\ -m/2\,, & \text{if } m \text{ is even.} \end{cases}$$

   First, convince yourself that the infinite lists $(f(0), f(1), f(2), \ldots)$ and $(0, 1, -1, 2, -2, 3, -3, \ldots)$ are identical.

   Now, prove that f is a bijection. Instead of using the definition of bijection, give an algebraic formula for a function $g : \mathbb{Z} \to \mathbb{N}$ such that $f \circ g = \mathrm{id}_{\mathbb{Z}}$ and $g \circ f = \mathrm{id}_{\mathbb{N}}$. Why does this prove that f is a bijection?

3. Prove that $\mathbb{N} \times \mathbb{N}$ is countable.

   Method 1: You can directly use the definition of a countably infinite set, i.e., give a bijection $h : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$

   Method 2: Alternatively, you can construct an injection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and invoke the following result.

   "If there exists an injection $f : A \to \mathbb{N}$, then A is countable."

CS 30
Fall 2019
Discrete Mathematics

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

Class Exercises: 2019-09-26

1. Consider the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by $f(a,b) = 2^a 3^b$. Prove that f is injective using just simple algebra and observations about odd and even numbers, without using the powerful Unique Factorization Theorem (UFT). You'll need the following facts:

   - The product of an even integer and an arbitrary integer is even.
   - The product of two odd integers is odd.

   Suppose that we have arbitrary $a, b, c, d \in \mathbb{N}$ such that

   $$2^a 3^b = 2^c 3^d \,. \tag{1}$$

   1.1. Consider the case when $b = d$. Prove that $(a,c) = (b,d)$.

   1.2. Now consider the case when $b \neq d$. Say $b < d$. Rewrite Eq. (1) in the form $2^p = 3^q$ with $q \in \mathbb{N}$.

   1.3. Based on the facts noted above, conclude that 3^q is odd.

   1.4. Based on the facts noted above and the previous part, conclude that $p = 0$.

   1.5. Based on all of the above, conclude that $(a,c) = (b,d)$.

   1.6. Wrap up the proof that f is injective.

2. Problem Set 3 asks you to prove the following fact:

   - If A and B are countable sets, then $A \times B$ is countable.

   Using the above fact, prove that $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is countable.

3. Given a character set S (sometimes called an *alphabet*), we can consider *strings* formed from the characters in S. Formally:

   - An *alphabet* is a nonempty finite set.
   - Having chosen an alphabet S, each of its elements is called a character.
   - A string is a finite-length sequence of zero or more characters.
   - The set of all such strings (over the alphabet S) is denoted S^*.

   3.1. Prove that S^* is countable.
   Hint: Come up with a systematic scheme for listing all the strings in S^*.

   3.2. Argue that the set of all conceivable Python programs is countable.

Class Exercises: 2019-10-01

1. Let $d \in \mathbb{N}^+$ and $a, b, x, y \in \mathbb{Z}$ be such that

$$\begin{aligned} a &\equiv b \pmod{d}, \\ x &\equiv y \pmod{d}. \end{aligned}$$

Using the definition of congruence, prove that

$$\begin{aligned} a + x &\equiv b + y \pmod{d}, \\ ax &\equiv by \pmod{d}. \end{aligned}$$

2. Compute $2^{2019} \bmod 17$. Do not use a calculator. In fact, think of a way to compute this entirely in your head.

3. Prove that a perfect square cannot end in the digit 7 when written out in decimal representation.
Hint: For what value of d would arithmetic modulo d help you reason about the last digit of an integer?

4. Prove that the product of any three consecutive integers must be divisible by 6.
Write a careful proof using only the facts established in the course up to this point. Don't jump to conclusions.

Class Exercises: 2019-10-03

Have a copy of the lecture notes on modular arithmetic available as you work on these problems.

1. Using Euclid's GCD algorithm, compute the gcd of 276 and 437, showing your work at each step.

2. An "integer linear combination (IntLC) of a and b" is defined to be an expression of the form $ka + \ell b$, where k and ℓ are integers. For each of the following statements, indicate "true" or "false." If true, provide a concise proof. If false, provide a specific counterexample.

   For all $a, b, c, n \in \mathbb{N}^+$,

   2.1. $\gcd(a, b) \neq 1 \wedge \gcd(b, c) \neq 1 \implies \gcd(a, c) \neq 1$.

   2.2. $\gcd(ab, ac) = a \cdot \gcd(b, c)$.

   2.3. $\gcd(1 + a, 1 + b) = 1 + \gcd(a, b)$.

   2.4. if an IntLC of a and b equals 1, then so does some IntLC of a and b^2.

3. Using the Inverse Existence Theorem (see the lecture notes), prove the following. If p is a prime, $b \in \mathbb{Z}_p$, and $b \neq 0$, then

   3.1. b has an inverse modulo p;

   3.2. the function $f_b : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $f_b(x) = bx \bmod p$ is a bijection.

Class Exercises: 2019-10-08

1. Consider arithmetic modulo 30, in the domain $\mathbb{Z}_{30}$. For each of the following numbers, find

   1.1. its inverse modulo 30;

   1.2. the smallest positive power of the number that is congruent to 1 modulo 30.

$$1,\ 10,\ 13,\ 19,\ 27,\ 29\,.$$

   Some of your answers might be "does not exist." You may use a calculator and/or the Python 'egcd' function from class.

Recall some notation from the lecture notes:

$$\mathbb{Z}_m^* := \{a \in \mathbb{Z} : 0 \le a < m \text{ and } \gcd(a,m) = 1\}\,; \quad \phi(m) = |\mathbb{Z}_m^*|\,.$$

Let's introduce an important piece of mathematical vocabulary. Consider a set S and an operation "op" on elements on S. We say that S is closed under "op" if the result of applying "op" to elements of S always produces an element of S. The concept is best understood through concrete examples.

- The set $\mathbb{N}$ is closed under the *addition* operation, because if $x, y \in \mathbb{N}$, then $x + y \in \mathbb{N}$.
- Similarly, $\mathbb{N}$ is closed under *multiplication*.
- However, $\mathbb{N}$ is not closed under *subtraction*, because there do exist $x, y \in \mathbb{N}$ such that $x - y \notin \mathbb{N}$.
- On the other hand, the larger set $\mathbb{Z}$ is indeed closed under subtraction.

2. Prove that $\mathbb{Z}_m^*$ is closed under multiplication modulo m, for all $m \in \mathbb{N}^+$.

3. Let p and q be two distinct primes. Prove that $\phi(pq) = (p-1)(q-1)$.

4. Suppose that p and q are distinct primes and $n \in \mathbb{Z}$ is such that $p \mid n$ and $q \mid n$. Prove that $pq \mid n$.
   Hint: Use the GCD Linear Combination Theorem and write $n = n(kp + \ell q)$.

Class Exercises: 2019-10-10

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

1. Dr. Speedy proposes a cryptosystem that would work faster than RSA by working modulo a large *prime*.

   - Bob chooses a public key of the form (P, e), where P is a very large (say 300-digit) prime.
   - When Alice wants to send a message $M \in \mathbb{Z}_P$ to Bob, she will send $C := M^e \pmod{P}$.
   - Bob has a secret key d such that $ed \equiv 1 \pmod{P-1}$; using it, he decrypts $M' := C^d \pmod{P}$.

   1.1. Show that Dr. Speedy's cryptosystem is sane, in the sense that $M' = M$ always.

   1.2. Why aren't we all using Dr. Speedy's cryptosystem instead of RSA, which is more complicated?

2. The security of RSA would be compromised if you could find an algorithm $\mathscr{A}$ to quickly compute $\phi(N)$, given N. We believe that factoring is hard, but why should computing ϕ be hard?

   Prove that if computing ϕ were easy—i.e., algorithm $\mathscr{A}$ exists—then $\mathscr{A}$ can be used to quickly factor the RSA modulus N. You'll need to use the fact that N is the product of *exactly two* primes.

3. In class (see the slides), we used a clever method to compute $a^{42} \bmod n$, based on the decomposition $42 = 32 + 8 + 2$.

   3.1. Find a connection between the above decomposition and the binary representation of 42.

   3.2. Explain how you would compute $a^{83} \bmod n$ along similar lines.

CS 30
Fall 2019
Discrete Mathematics

Class Exercises: 2019-10-15

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

These exercises are about basic counting. Some of them will continue the devlopment of ideas and methods we touched upon in the lecture. Do good work on them, understand them well, and seek help from your Ninja as needed.

Here are some important counting principles for *finite* sets.

- *Sum Principle.* If A and B are disjoint (i.e., $A \cap B = \varnothing$), then $|A \cup B| = |A| + |B|$.
- *Extended Sum Principle.* If $A_1, \ldots, A_k$ are pairwise disjoint, then $|A_1 \cup \cdots \cup A_k| = |A_1| + \cdots + |A_k|$.
- *Generalized Sum Principle.* For all sets A and B, $|A \cup B| = |A| + |B| - |A \cap B|$.
- *Product Principle.* For all sets A and B, $|A \times B| = |A| \cdot |B|$.
- *Extended Product Principle.* For all sets $A_1, A_2, \ldots, A_k$, $|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \cdot |A_2| \cdots |A_k|$.
- *Generalized Product Principle.* If we have to make a sequence of k choices and
  - there are n_1 ways to make the first choice,
  - for each first choice, there are n_2 ways to make the second choice,
  - for each of the first two choices, there are n_3 ways to make the third choice,
  - $\cdots$
  - for each of the first $k-1$ choices, there are n_k ways to make the kth choice,

  then the overall number of ways to make the entire sequence of choices is $n_1 n_2 \cdots n_k$.
- *Bijection Principle.* If there exists a bijection $f : A \to B$, then $|A| = |B|$.
- *Division Principle.* If there exists an r-to-1 correspondence $f : A \to B$, then $|B| = |A|/r$.

1. Solve each of the following counting problems. In each case, name the counting principle(s) you used.

   1.1. An office building contains 27 floors and has 37 offices on each floor. How many offices are in the building?

   1.2. Alice picks a card out of a standard 52-card deck. Then Bob picks a card from the ones that remain. Overall, how many different outcomes can there be?

   1.3. How many of the integers between 1 and 1000 (inclusive) are multiples of either 3 or 5?

2. Solve each of the following counting problems. In each case, name the counting principle(s) you used. You may need to further extend one of the given counting principles. Get help from your Ninja as needed.

   2.1. Each user on a certain computer system has a password, which is six to eight characters long, where each character is a letter (either uppercase or lowercase) or a digit. Each password must contain at least one digit. How many possible passwords are there?

   2.2. The password rules in the above system have been modified. Now each password must contain at least one uppercase letter, at least one lowercase letter, and at least one digit. How many possible passwords are there now?

3. This part is warm-up. A *permutation* of a sequence is another sequence obtained by rearranging its terms. For instance, the three-term sequence (apple, pear, mango) has six permutations, shown below.

(apple, mango, pear) (apple, pear, mango) (mango, apple, pear)
(mango, pear, apple) (pear, apple, mango) (pear, mango, apple)

Notice that a sequence is considered to be a permutation of itself.

3.1. How many permutations does the four-term sequence $(1,3,8,9)$ have?

3.2. Generalize! How many permutations does an n-term sequence have, assuming the terms are all distinct?

Now for the real problem. Suppose $|S| = n$. We're going to work out the number of k-element subsets of S. Define

$$\mathscr{T} = \{\, (a_1, a_2, \ldots, a_k) \in S^k :\; a_i \neq a_j \text{ whenever } i \neq j \,\}\,;$$
$$\mathscr{U} = \{\, A \subseteq S :\; |A| = k \,\}\,.$$

Study these definitions carefully!

3.3. To solidify your understanding, redefine $\mathscr{T}$ in words like this: "$\mathscr{T}$ is the set of all k-tuples such that..."

3.4. Determine $|\mathscr{T}|$ using the extended product principle.

3.5. Define the function $\textsc{MakeSet} : \mathscr{T} \to \mathscr{U}$ by

$$\textsc{MakeSet}(a_1, a_2, \ldots, a_k) = \{a_1, a_2, \ldots, a_k\}\,.$$

For what value of r is $\textsc{MakeSet}$ an r-to-1 correspondence?

3.6. Apply the division principle to determine $|\mathscr{U}|$.

4. Suppose that 13 people on a softball team show up for a game.

4.1. How many ways are there to choose 10 players to take the field?

4.2. How many ways are there to assign the 10 positions by selecting from the players who showed up?

4.3. Of the 13 who showed up, 11 are students and the other 2 are professors. How many ways are there to choose 10 players to take the field if at least one of these players must be a professor?

Class Exercises: 2019-10-17

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

For today's exercises, please write out a detailed proof for the first problem, following the proof-by-induction template I've shown you. For the next two problems, if you don't have enough time, skip the template and just show your pod's Ninja the "meat" of your proof.

1. Using mathematical induction, prove that $\forall\, n \in \mathbb{N}$: $\displaystyle\sum_{i=1}^{n}(2i-1) = n^2$.

2. Using mathematical induction, prove that the following identity holds for all $n \in \mathbb{N}$ and all $x \in \mathbb{R} - \{1\}$:

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1}-1}{x-1}\,,$$

   Careful: the identity has two variables; your first step should be to write an appropriate one-variable predicate.

3. Using mathematical induction, prove that every positive integer n can be written as a sum of one or more *distinct* powers of 2. For example, $42 = 2^5 + 2^3 + 2^1$ and $77 = 2^6 + 2^3 + 2^2 + 2^0$.

   Hint: You might want to consider using strong induction.

4. *[Optional problem, if you've finished the first three.]*

   Recall that the basic sum principle applies to *exactly two* disjoint sets whereas the extended sum principle applies to $n \geq 2$ pairwise disjoint sets.

   Use mathematical induction to prove that the extended sum principle follows from the basic sum principle.

CS 30
Fall 2019
Discrete Mathematics

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

Class Exercises: 2019-10-22

1. We'll now study the fourth (and most complicated) case of the four-fold formulas. For starters, let's consider special cases.

   You are in a candy store. There are six (6) kinds of candy on offer and the store has plenty of pieces of each kind in stock. You love all six kinds on offer. You just want to take home as much candy as your parent will allow!

   1.1. You have been allowed to pick two (2) pieces of candy to take home. The two pieces may be of the same kind or of different kinds. In how many different ways can you make your picks?

   1.2. Suppose, instead, that you have been allowed to pick three (3) pieces. How does the answer change?
   The new answer is $\binom{6}{1} + 2\binom{6}{2} + \binom{6}{3}$. How did I get this?

2. It's your lucky day: you have been allowed to pick 15 pieces of candy from the above candy store! In how many ways can you make your choice now?

   It's going to be tedious to generalize the expressions you wrote in the previous problem, so you try another idea. Visualize a row of 15 books laid out on a bookshelf, to represent the 15 pieces of candy you'll pick. Now you want to assign a kind of candy to each book: remember that there are 6 kinds of candy in the store. To do so, visualize 5 separators placed on the same bookshelf, dividing up the row of books into 6 sections. The number of books in the jth section will correspond to the number of pieces of the jth kind of candy you'll pick.

   2.1. Draw a picture showing two different bookshelf layouts with the 15 books and 5 separators. For each of the layouts, write down the candy choices they indicate.

   2.2. In how many ways can you lay out 15 books and 5 separators on a bookshelf? The books are to be treated as indistinguishable from one another and so are the separators.

   2.3. Generalize! Suppose the candy store had n kinds of candy on offer and you are allowed to take home t pieces (repetitions allowed, as usual). How many books and how many separators should you use to represent your possible picks? Based on this, what is the number of ways to pick t pieces of candy from a store than offers n kinds of candy?

3. Give combinatorial proofs of the following identities.

   3.1. For all $n \in \mathbb{N}^+$: $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$.

   3.2. For all $k, n \in \mathbb{N}^+$ with $k \le n$: $\displaystyle k\binom{n}{k} = n\binom{n-1}{k-1}$.
   Hint: Consider choosing a k-person committee and then a chairperson of that committee.

CS 30
Fall 2019
Discrete Mathematics

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

Class Exercises: 2019-10-24

1. Work out each of the following probabilities *systematically*, using the Four-Step Method. No need to get final numerical answers unless you have a calculator handy.

1.1. First one digit is chosen uniformly at random from $\{1, 2, 3, 4, 5\}$ and is removed from the set; then a second digit is chosen uniformly at random from the remaining digits. What's the probability that an odd digit is picked the second time?

1.2. You are dealt a poker hand of 5 cards drawn at random from a well-shuffled standard deck of 52 cards. The hand is called a *full house* if it has three cards of one rank and two of another rank (e.g., three kings and two 7s). What is the probability that your hand is a full house?

1.3. A fair coin is flipped n times. What's the probability that all the heads occur at the end of the sequence? If no heads occur, then the statement "all the heads are at the end of the sequence" is vacuously true.

2. Work out each of the following probabilities. It's okay to shortcut, but if you get confused, do use the Four-Step Method. No need to get final numerical answers unless you have a calculator handy.

2.1. A standard bag of Scrabble tiles has 100 tiles, exactly two (2) of which are *blank tiles*. Blanks are valuable assets in the game, since they can be turned into whatever letter you want.

You have just begun a game of Scrabble, drawing your first rack of seven (7) tiles from a full bag. Waht is the probability that your rack contains a blank?

2.2. How does the answer to the above question change if your opponent is to make the first move, so your opponent picks seven random tiles first and *then* you get to pick seven from the 93 remaining tiles?

3. A card C is drawn uniformly at random from a standard 52-card deck. This is naturally modeled using the sample space $\mathscr{S} = \{\clubsuit 2, \diamondsuit 2, \heartsuit 2, \spadesuit 2, \clubsuit 3, \diamondsuit 3, \heartsuit 3, \spadesuit 3, \ldots, \spadesuit \mathrm{A}\}$ and the function Pr that sets $\Pr[x] = 1/52$ for each $x \in \mathscr{S}$.

3.1. Suppose you are *told* that C is a black card. Without changing the sample space $\mathscr{S}$, how should you modify the probability function to model this new reality?

3.2. Suppose, instead, that you are told that C has a prime number on it (you are not told anything about the color). Again, sticking with the same sample space $\mathscr{S}$, what probability function should you use to model this new reality?

3.3. Continue to assume that you are told that C has a prime number on it. Under this *condition*, based on your modified probability function, work out the probability of each of the following events.

i. The event that C is a red card.
ii. The event that C has the number 2 on it.
iii. The event that C has the number 6 on it.
iv. The event that C either has a 5 or a 6 on it.

Class Exercises: 2019-10-29

1. Two fair dice are rolled in another room, out of your sight. If the sum of the two dice values is seven, you *win*. Your friend is in the other room and can observe the dice.

   1.1. Your friend calls out that one of the dice came up six. Given this information, what is the probability that you won?

   1.2. Suppose, instead, that your friend tells you that you won. In this case, what is the probability that one of the dice came up five?

2. Sally Smart just graduated from high school. She was accepted to three reputable colleges.

   - With probability 4/12, she attends Brown.
   - With probability 5/12, she attends Dartmouth.
   - With probability 3/12, she attends Little Hoop Community College.

   Sally is either happy or unhappy in college.

   - If she attends Brown, she is happy with probability 4/12.
   - If she attends Dartmouth, she is happy with probability 7/12.
   - If she attends Little Hoop, she is happy with probability 11/12.

   2.1. What is the probability that Sally is happy in college?

   2.2. What is the probability that Sally attends Brown, given that she is happy in college?

   2.3. Show that the events "Sally attends Brown" and "Sally is happy" **are not** independent.

   2.4. Show that the events "Sally attends Dartmouth" and "Sally is happy" **are** independent.

3. The Chain Rule for probability says that if $A_1, A_2, \ldots, A_n$ are events in a probability space $(\mathscr{S}, \Pr)$, then

$$\begin{aligned}\Pr[A_1 \cap A_2 \cap \cdots \cap A_n] &= \Pr[A_1] \cdot \Pr[A_2 \mid A_1] \cdot \Pr[A_3 \mid A_1 \cap A_2] \cdot \cdots \cdot \Pr[A_n \mid A_1 \cap A_2 \cap \cdots \cap A_{n-1}] \\ &= \Pr[A_1] \cdot \Pr[A_2 \mid A_1] \cdot \Pr[A_3 \mid A_1, A_2] \cdot \cdots \cdot \Pr[A_n \mid A_1, A_2, \ldots, A_{n-1}] \\ &= \prod_{j=1}^{n} \Pr[A_j \mid A_1, A_2, \ldots, A_{j-1}] .\end{aligned}$$

   3.1. Prove this rule, i.e., prove the first equation. (The other two lines are just rewritings.)
   Hint: Don't use induction. Start with the right-hand side.

   3.2. Use this rule to answer the following question. Suppose n passengers board a flight that has n seats and they each take a seat at random, ignoring their assigned seating. The passengers board one by one. What is the probability that passengers 1 through k (inclusive) all end up in their assigned seats?

Bonus question: What do #2.3 and #2.4 teach you about independence of events?

CS 30
Fall 2019
Discrete Mathematics

Class Exercises: 2019-10-31

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

1. Let $n \geq 2$ be an integer. We choose a random integer $X \in \mathbb{Z}_n$ uniformly. Let $Y = \gcd(X, n)$. Determine $\mathrm{Ex}[Y]$ in each of the following cases.

   1.1. $n = 7$.

   1.2. $n = 9$.

   1.3. $n = p^2$, where p is a prime.

2. We roll two fair dice, a *red* die and a *blue* die, and they show numbers X and Y, respectively (these are therefore random variables). Let $W = X + Y$.

   2.1. Compute $\mathrm{Ex}[X^2 \mid X \text{ is a perfect square}]$.

   2.2. Show that $\mathrm{Ex}[WX] \neq \mathrm{Ex}[W]\,\mathrm{Ex}[X]$.

3. We roll 24 fair dice, and they show numbers $X_1, \ldots, X_{24}$.

   3.1. How many sixes do we expect to see? In other words, compute $\mathrm{Ex}\big[|\{j : X_j = 6\}|\big]$.

   3.2. Even though each die is fair, they have been connected together by very thin weightless threads and this causes $X_1, \ldots, X_{24}$ to be correlated in some unknown way. (For example, it may be that whenever X_1 is even, X_2 is more likely to be even than odd; or that whenever X_8 is a prime number, X_{20} is sure to be prime; or both of the above.) How does this affect your answer above?

4. The below problems have special significance in Computer Science. They model the process of inserting keys into a hash table.

   4.1. Two people that have the same birthday are said to form a *calendrical bond*. Assuming that the n students in a class have birthdays distributed uniformly among the d days in a year, and birthdays are mutually independent, what is the expected number of calendrical bonds among students in the class? Derive a formula in terms of n and d, then apply it to our CS30 class, using $n = 57$ and $d = 365$.

   Hint: The random variable of interest here is a sum of $\binom{n}{2}$ indicator RVs.

   4.2. There are n bins, initially all empty. Then n balls are thrown randomly (uniformly) and independently into the bins: "uniformly" means that each ball is equally likely to go into each of the bins. What is the expected number of bins that remain empty after this process?

   Hint: Again use a sum of appropriate indicator RVs.