# CS220 Discrete Math - Homework #1

Brendan Nguyen - brendan.nguyen001@umb.edu

February 3, 2022

## Question 1

The expanded form of the given compound composition is:

$$\bigwedge_{i=1}^{n-1} \bigwedge_{j=i+1}^{n} (\neg p_i \vee \neg p_j) = (\neg p_1 \vee \neg p_2) \wedge (\neg p_1 \vee \neg p_3) \wedge (\neg p_1 \vee \neg p_4)$$

$$\wedge \ldots \wedge (\neg p_1 \vee \neg p_n) \wedge (\neg p_2 \vee \neg p_3) \wedge \ldots \wedge (\neg p_2 \vee \neg p_n)$$

$$\wedge \ldots \wedge (\neg p_{n-1} \vee \neg p_n)$$

Using what we know:

1. DeMorgan's Law: $(\neg p_i \vee \neg p_j) = \neg(p_i \wedge p_j)$

2. The above should be `true` for all $i$ and $j$

Statement 2 implies that $(p_i \wedge p_j)$ should be `false` for all $i$ and $j$, which can only be fulfilled for at most 1 $p$ that is `true`. The case of at most 1 $p$ that is `true` results in $(\neg p_i \vee \neg p_j)$ is always `true`.

## Question 2

The truth table is as follows:

| $p$ | $q$ | $r$ | $p \wedge q$ | $\neg r$ | $(p \wedge q) \vee \neg r$ |
|---|---|---|---|---|---|
| T | T | T | T | F | T |
| T | T | F | T | T | T |
| T | F | T | F | F | F |
| T | F | F | F | T | T |
| F | T | T | F | F | F |
| F | T | F | F | T | T |
| F | F | T | F | F | F |
| F | F | F | F | T | T |

Table 1: Expanded truth table for $(p \wedge q) \vee \neg r$

## Question 3

The statement, "This statement is false," is not a proposition because it cannot have a truth value. If the statement was `true`, then it would assert that it's `false`, which is a contradiction. Similarly, if the statement was `false`, it would assert that it's `true`, another contradiction.

# Question 4

Testing the truth values of $p$ and $q$ for the compound proposition, you get:

| $p$ | $q$ | $\neg p$ | $p \to q$ | $\neg p \wedge (p \to q)$ | $\neg q$ | $(\neg p \wedge (p \to q)) \to \neg q$ |
|---|---|---|---|---|---|---|
| F | F | T | T | T | T | T |
| F | T | T | T | T | F | F |
| T | F | F | F | F | T | T |
| T | T | F | T | F | F | T |

Table 2: Expanded truth table for $(\neg p \wedge (p \to q)) \to \neg q$

By definition of a tautology, the compound proposition $(\neg p \wedge (p \to q)) \to \neg q$ is not a tautology because not all truth values are `true` for all $p$ and $q$.

# Question 5

The simplest way to evaluate the logical equivalence of the compound propositions $(p \to q) \vee (p \to r)$ and $p \to (q \vee r)$ is to compare their truth tables.

| $p$ | $q$ | $r$ | $p \to q$ | $p \to r$ | $(p \to q) \vee (p \to r)$ | $q \vee r$ | $p \to (q \vee r)$ |
|---|---|---|---|---|---|---|---|
| T | T | T | T | T | T | T | T |
| T | T | F | T | F | T | T | T |
| T | F | T | F | T | T | T | T |
| T | F | F | F | F | F | F | F |
| F | T | T | T | T | T | T | T |
| F | T | F | T | T | T | T | T |
| F | F | T | T | T | T | T | T |
| F | F | F | T | T | T | T | T |

Table 3: Expanded truth tables for $(p \to q) \vee (p \to r)$ and $p \to (q \vee (p \to r))$

Comparing the 2 truth tables shown in Table 3, you can see that for all $p$, $q$, and $r$, the truth values of the compound propositions are equivalent.

# CS220 Discrete Math - Homework #2

Brendan Nguyen - `brendan.nguyen001@umb.edu`

February 10, 2022

## Question 1

(a) For the domain of $x$ being all students in CS220

   i. $\forall x(P(x))$ represents the statement, "Everyone in CS220 has a cellphone."

   ii. $\exists x(Q(x))$ represents the statement, "Somebody in CS220 can solve quadratic equations."

   iii. $\exists x(\neg R(x))$ represents the statement, "Somebody in CS 220 does not want to be rich."

(b) For the domain of $x$ being all students and that $C(x)$ is a predicate for "$x$ is in CS220"

   i. $\forall x(C(x) \to P(x))$ represents the statement, "Everyone in CS220 has a cellphone."

   ii. $\exists x(C(x) \wedge Q(x))$ represents the statement, "Somebody in CS220 can solve quadratic equations."

   iii. $\exists x(C(x) \wedge \neg R(x))$ represents the statement, "Somebody in CS 220 does not want to be rich."

## Question 2

The argument with the given premises and the conclusion $r$ is valid as shown below:

| Step | Reason |
|---|---|
| 1. $(p \wedge t) \to (r \vee s)$ | Premise |
| 2. $\neg p \vee \neg t \vee r \vee s$ | Logical equivalence of (1) |
| 3. $s \vee (\neg p \vee \neg t \vee r)$ | Commutative and Associative laws on (2) |
| 4. $\neg s$ | Premise |
| 5. $\neg p \vee \neg t \vee r$ | Disjunctive syllogism on (3) and (4) |
| 6. $u \to p$ | Premise |
| 7. $\neg u \vee p$ | Logical equivalence of (6) |
| 8. $p \vee \neg u$ | Commutative law on (7) |
| 9. $\neg u \vee \neg t \vee r$ | Resolution rule on (5) and (7) |
| 10. $\neg(u \wedge t) \vee r$ | DeMorgan's Law on (9) |
| 11. $(u \wedge t) \to r$ | Logical equivalence of (10) |
| 12. $q \to (u \wedge t)$ | Premise |
| 13. $q \to r$ | Hypothetical syllogism on (12) and (11) |
| 14. $q$ | Premise |
| 15. $r$ | Modus ponens on (14) and (13) |

# Question 3

Let the conditional statement $S$ be $(p \rightarrow q) \rightarrow q$, then we can use a truth table to see the truth values.

| $p$ | $q$ | $p \rightarrow q$ | $(p \rightarrow q) \rightarrow q$ |
|---|---|---|---|
| T | T | T | T |
| T | F | F | T |
| F | T | T | T |
| F | F | T | F |

Table 1: Truth table for $(p \rightarrow q) \rightarrow q$

In the statement above, $p$ represents the statement, "$S$ is true," and $q$ represents the statement, "Unicorns live." If $S$ is a proposition (in other words $p \rightarrow q$ is true), then $q$ is true, meaning that "Unicorns live." If $S$ is not a proposition, then it has both true and false values. We know that if $S$ is true, then $p$ is true. Both true and false for $q$ still results in true for $S$. If $S$ is false, then $(p \rightarrow q)$ is true, $p$ and $q$ are both false. Due to the fact that we can't determine the truth value of $S$, we can determine that $S$ is not a proposition by the definition that a statement can have a true or false value but not both.

# Question 4

The statement, "No one has more than two grandmothers," can be rewritten as, "There does not exists three different people that are grandmothers of the same person". We can translate this statement into a predicate as shown below:

$$\forall x \left[ \neg \exists w \exists y \exists z [G(w, x) \wedge G(y, x) \wedge G(z, x) \wedge (w \neq y \neq z)] \right]$$

where $x$ is a person and $w$, $y$, and $z$ are grandmothers of person $x$.

# Question 5

Because $A$ is a nonempty set, you can say that $a \in A$. In order to prove if $B = C$, we denote a variable $x$ such that $x \in B$. Then by set product, we can say that $\langle a, x \rangle \in A \times B$. Using the original problem statement, $A \times B = A \times C$, we can then state that $\langle a, x \rangle \in A \times C$ and $x \in C$ using set product again. Therefore, $B$ is included in $C$. Now, since $A$ is a subset of $B$ because every element of $A$ is also an element of $B$, we can say that $B$ is a subset of $C$ and $C$ is a subset of $B$. Therefore, by this definition, we can state that $B = C$ since $B \subseteq C$ and $C \subseteq B$.

# CS220 Discrete Math - Homework #3

Brendan Nguyen - brendan.nguyen001@umb.edu

February 17, 2022

## Question 1

$A$, $B$, and $C$ are sets.

$$
\begin{aligned}
(A - C) - (B - C) &= (A \cap C^c) \cap (B \cap C^c)^c \\
&= (A \cap C^c) \cap (B^c \cup C) \\
&= ((A \cap C^c) \cap B^c) \cup ((A \cap C^c) \cap C) \\
&= ((A \cap B^c) \cap C^c) \cup (A \cap (C^c \cap C)) \\
&= ((A \cap B^c) \cap C^c) \cup (A \cap \varnothing) \\
&= ((A - B) - C) \cup \varnothing \\
&= (A - B) - C
\end{aligned}
$$

## Question 2

By definition, $f(x)$ is strictly increasing if:

$$\forall x \forall y (x < y \rightarrow f(x) < f(y))$$

Dividing the inequality $f(x) < f(y)$ by the inequality $f(x)f(y) > 0$ results in:

$$\frac{1}{f(y)} < \frac{1}{f(x)}$$

The above inequality is equal to $g(y) < g(x)$, therefore:

$$\forall x \forall y (x < y \rightarrow g(x) > g(y))$$

Conversely, we can prove the inverse by testing $g(x) = \frac{1}{f(x)}$ which is strictly decreasing:

$$\forall x \forall y (x < y \rightarrow g(x) > g(y))$$

Using $g(x) > g(y) \overset{\text{def}}{=} \frac{1}{f(x)} < \frac{1}{f(y)}$ that we proved previously, we get:

$$\forall x \forall y (x < y \rightarrow f(x) < f(y))$$

Meaning that $f(x)$ is strictly increasing.

## Question 3

(a) $A_n = 1.09 \cdot A_{n-1}$ denotes the recurrence relation for the amount in the account at the end of $n$ years.

(b) $A_n = 1000 \cdot 1.09^n$ denotes the explicit formula for the amount in the account at the end of $n$ years.

(c) $A_{100} = 1000 \cdot 1.09^{100} = \$5,529,040.79$ is the amount of money in the account after 100 years.

## Question 4

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \sum_{k=1}^{n} \left( \frac{1}{k} - \frac{1}{k+1} \right)$$

$$= \frac{1}{1} - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{n} - \frac{1}{n+1}$$

$$= 1 - \frac{1}{n+1}$$

## Question 5

To show that the set of functions $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is uncountable, we can use the fact that the set of all subsets of $\mathbb{N}$, $F(\mathbb{N})$, is uncountable. We see that the set of functions from $\mathbb{N}$ to $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ contains the set $\{0, 1\}^{\mathbb{N}}$ of functions from $\mathbb{N}$ to $\{0, 1\}$ using injection. Therefore, you can say that there is a bijection between $F(\mathbb{N})$ and $\{0, 1\}^{\mathbb{N}}$. In conclusion, since the set $\{0, 1\}^{\mathbb{N}}$ is uncountable and the set is a subset in the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, then we can say that the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is also uncountable.

# CS220 Discrete Math - Homework #4

Brendan Nguyen - `brendan.nguyen001@umb.edu`

February 24, 2022

## Question 1

The definition of big-O notation tells you that have you to find the witnesses $c$ and $k$ such that $f(x) \leq c(g(x))$ when $f(x) = \mathrm{O}(g(x))$.

First, I tested $c = 2$ and $k = 2$. Testing the definition for $n = 3$, I got $f(2.5) \leq c(g(2.5)) \to 25 \leq 54$. Although this pair seemed to work, when testing values approaching $n = 2$, I found that $n = 2.1$ fails the inequality ($f(2.1) = 21.287$ and $2(g(2.1)) = 20.090$).

Afterwards, I tested $c = 2$ and $k = 3$. Plugging in $n = 4$, I got $f(4) \leq c(g(4)) \to 33 \leq 162$. Testing values approaching $n = 3$ shows us that the **witnesses** $c = 2$ and $k = 3$ are valid as no decimals fail the inequality.

## Question 2

According to the definition of big-O notation, we can say that:

$$1^k + 2^k + \cdots + n^k < n^k + n^k + \cdots + n^k = n \cdot n^k = n^{k+1}$$

Since the sum $(n^k + n^k + \cdots + n^k)$ is greater than the sum $(1^k + 2^k + \cdots + n^k)$ and is clearly $\mathrm{O}(n^{k+1})$ since the sum is exactly $n^{k+1}$. Therefore the smaller sum of $(1^k + 2^k + \cdots + n^k)$ is also $\mathrm{O}(n^{k+1})$.

## Question 3

There are some statements that we can say about the big-O estimates involved in the problem:

1. Logarithmic functions grow slower than all positive powers of $n$ (i.e. $\sqrt{n}$, $n$, $n^2$, $n^3$, etc.)

2. Exponential functions grow faster than polynomial functions

3. Factorials grow faster than exponential functions

With these statements in mind, we can order the given functions as such:

$$(\log n)^3, \sqrt{n}\log n, n^{99} + n^{98}, n^{100}, (1.5)^n, 10^n, (n!)^2$$

We use Statement 1 to say that $(\log n)^3$ is the slowest growing function. The next three can be placed in order of power of $n$ due to Statement 2 ($\frac{1}{2}$, 99, and 100, respectively). Statement 2 also puts the two exponential functions afterwards in order of base. Finally, the statement $(n!)^2$ is the fastest growing function due to Statement 3.

## Question 4

The C code block from page 50 and Exercise 2-9 of the C Programming Language by Kernighan and Ritchie, the second edition.

```
int bitCount(unsigned x) {
    int count;

    for (count = 0; x != 0; x &= (x - 1))
        count++;
    return count;
}
```

(a) The best way to show that the above function returns the number of 1 bits in the unsigned integer x is to use an example of the computation of unsigned int x = 7.

The first iteration of the loop would compare x = 7 and x = 6.

$$\begin{array}{r} 0111 \\ \&\ 0110 \\ \hline 0110 \end{array}$$

The second iteration has a count = 1 with x = 6 and it would compare x = 6 and x = 5.

$$\begin{array}{r} 0110 \\ \&\ 0101 \\ \hline 0100 \end{array}$$

The third iteration has a count = 2 with x = 4 and it would compare x = 4 and x = 3.

$$\begin{array}{r} 0100 \\ \&\ 0011 \\ \hline 0000 \end{array}$$

Now the count = 3 and x = 0 so the loop would end. The count now equals the number of 1 bits in the unsigned integer 7 (0111).

(b) The number of iterations equals the number of count which equals the number of 1 bits in the unsigned integer x.

## Question 5

We can find which method is more efficient by analyzing the matrix multiplication operations for each method. In the case of (AB)C, you calculate the number of operations in AB and add it to the operations of multiplying C and the resulting matrix of AB. Similarly for A(BC), you calculate the number of operations in BC and add it to the operations of multiplying A and the resulting matrix of BC.

For the matrices $A$, $B$, and $C$ with dimensions $3 \times 9$, $9 \times 4$, and $4 \times 2$, respectively:

$$\texttt{(AB)C} = (3 \cdot 9 \cdot 4) + (3 \cdot 4 \cdot 2) = 132 \text{ integer multiplications}$$

$$\texttt{A(BC)} = (9 \cdot 4 \cdot 2) + (3 \cdot 9 \cdot 2) = 126 \text{ integer multiplications}$$

The above calculations show that $\texttt{A(BC)}$ is more efficient than $\texttt{(AB)C}$ while maintaining the resulting $3 \times 2$ matrix.

# CS220 Discrete Math - Homework #5

Brendan Nguyen - brendan.nguyen001@umb.edu

March 3, 2022

## Question 1

The addition and multiplication tables for $Z_7$ are shown below. To fill the tables, we use the defined operations for addition and multiplication modulo $m$, $a +_m b = (a+b) \bmod m$ and $a \cdot_m b = (a \cdot b) \bmod m$ respectively.

| $+_7$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

| $\cdot_7$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

Examples of above calculations where $m = 7$:

$a = 5, b = 6 : (5 + 6) \bmod 7 = 11 \bmod 7 = 4$

$a = 6, b = 4 : (6 \cdot 4) \bmod 7 = 24 \bmod 7 = 24 \bmod 21 = 3$

## Question 2

The sum and product of $(20CBA)_{16}$ and $(A01)_{16}$ are shown below.

$$
\begin{array}{r}
1 \phantom{00000} \\
2\,0\,C\,B\,A_{16} \\
+ \quad A\,0\,1_{16} \\
\hline
2\,1\,6\,B\,B_{16}
\end{array}
$$

$$
\begin{array}{r}
7\;7\;6 \phantom{0000} \\
2\,0\,C\,B\,A_{16} \\
\times \quad A\,0\,1_{16} \\
\hline
2\,0\,C\,B\,A_{16} \\
0 \\
+\,1\,4\,7\,F\,4\,4\,0\,0_{16} \\
\hline
1\,4\,8\,1\,5\,0\,B\,A_{16}
\end{array}
$$

The corresponding binary values can be used to double check the above. The sum $(216BB)_{16}$ gets the correct binary value of $(136{,}891)_{10}$ (or $134{,}330 + 2{,}561$). The product $(148150BA)_{16}$ gets the correct binary value of $(344{,}019{,}130)_{10}$ (or $134{,}330 \cdot 2{,}561$).

# Question 3

Just to establish a preconceived definition of a factorial. The given factorial $100! = 100 \times 99 \times 98 \times 97 \times \cdots \times 3 \times 2 \times 1$. In order to count the number of trailing zeros that exist in the result of $100!$, we should find situations (meaning combinations of factors) that could result in an additional trailing zero. We can infer that a trailing zero will be formed by multiplying a multiple of $5$ and a multiple of $2$ together.

First, we can count the multiples of $5$. These consist of $5, 10, 15, 20, 25, \ldots, 95, 100$, 20 multiples of $5$. However, the four multiples of 25 $(25, 50, 75, 100)$ need to be counted twice since $25 = 5^2$ (meaning each multiple of $25$ is essentially 2 multiples of $5$). The final count of multiples of $5$ is 24.

Next, we can count the multiples of $2$. Getting the initial set of multiples of $2$, we get a total of 50 multiples. As we did before, we also need to take into account multiples of $4$, $8$, etc. We can reasonably infer that the total multiples of $2$ will far exceed the initial 50.

Finally, because we have only 24 multiples of $5$ and far more multiples of $2$, we can say that there will only be 24 trailing zeros in $100!$ because we can only have that number of unique pairs of multiples of $5$ and $2$.

# Question 4

Listing the factors of 6 and 28 (not including the numbers themselves) and adding them together will show that they are perfect.

6: $1 + 2 + 3 = \mathbf{6}$

28: $1 + 2 + 4 + 7 + 14 = \mathbf{28}$

# Question 5

We know that $a$ is congruent to $b \bmod m$ if $m$ divides $a - b$. We also know that $a$ divides $b$ is there's an integer $x$ that satisfies $b = ax$. We can combine these two factors to say that there is an integer $x$ such that $a - b = mx$ or $a = mx + b$. Next, we can define constants that will help us find the gcds: $A = \gcd(a, m)$ and $B = \gcd(b, m)$. Listing the gcds of two integers gets us: $A|a$, $A|m$, $B|b$, and $B|m$.

Since $a = mx + b$, $A|a$ and $A|m$ implies $A|b$. Similarly, $B|b$ and $B|m$ implies $B|a$. Then we can state that if an integer divides two integers, then the integer also divides their gcd.

$$A| \gcd(b, m)$$
$$B| \gcd(a, m)$$

Since $A = \gcd(a, m)$ and $B = \gcd(b, m)$, we can substitute into the two statements above which results in: $A|B$ and $B|A$. If $A|B$ and $B|A$ is true, then you can imply that $A = B$ and therefore, $\gcd(a, m) = \gcd(b, m)$.

# CS220 Discrete Math - Homework #6

Brendan Nguyen - `brendan.nguyen001@umb.edu`

March 10, 2022

## Question 1

In order to prove or disprove that $p_1 p_2 \cdots p_n + 1$ is prime for every $n$ where $p_1 p_2 \cdots p_n$ are the $n$ smallest prime numbers, we can test random numbers of the first few prime numbers.

$n = 1 \rightarrow 2 + 1 = 3$ prime

$\quad 2 \rightarrow 2 \cdot 3 + 1 = 7$ prime

$\quad 3 \rightarrow 2 \cdot 3 \cdot 5 + 1 = 31$ prime

$\quad 4 \rightarrow 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ prime

$\quad 5 \rightarrow 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ prime

$\quad 6 \rightarrow 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ NOT prime

Because the statement fails for the 6 smallest prime numbers, we can say that $p_1 p_2 \cdots p_n + 1$ is not prime for every $n$.

## Question 2

First, we need to find $\gcd(34, 89)$ using the Euclidean algorithm.

$$89 = 2 \cdot 34 + 21$$
$$34 = 1 \cdot 21 + 13$$
$$21 = 1 \cdot 13 + 8$$
$$13 = 1 \cdot 8 + 5$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + \boxed{1}$$

Then we use Bézout's theorem to find the linear combination. We will work backwards from the previous operations.

$$1 = 3 - (5 - 3)$$
$$= 2 \cdot 3 - 5$$
$$= 2 \cdot (8 - 5) - 5$$
$$= 2 \cdot 8 - 3 \cdot 5$$
$$= 2 \cdot 8 - 3 \cdot (13 - 8)$$
$$= 5 \cdot 8 - 3 \cdot 13$$
$$= 5 \cdot (21 - 13) - 3 \cdot 13$$
$$= 5 \cdot 21 - 8 \cdot 13$$
$$= 5 \cdot 21 - 8(34 - 21)$$
$$= 13 \cdot 21 - 8 \cdot 34$$
$$= 13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34$$
$$= 13 \cdot 89 - 26 \cdot 34 - 8 \cdot 34$$
$$= 13 \cdot 89 - \boxed{34} \cdot 34$$

The inverse of 34 modulo 89 is **-34** or **55**.

## Question 3

Using $a$ that we found previously, we can solve the given linear congruence.

$$34x \equiv 77 \ (\mathrm{mod} \ 89)$$
$$1870x = 55 \cdot 77 \ (\mathrm{mod} \ 89)$$
$$x \equiv 4235 \equiv 47 \cdot 89 + 52 \equiv \boxed{52} \ (\mathrm{mod} \ 89)$$

## Question 4

The pairs of positive integers that are less than 11 (that don't include 1 or 10) such that each pair are inverses of each other modulo 11 are shown below:

$$2 \cdot 6 = 12 = 1 \cdot 11 + 1 \equiv 1 \ (\mathrm{mod} \ 11)$$
$$3 \cdot 4 = 12 = 1 \cdot 11 + 1 \equiv 1 \ (\mathrm{mod} \ 11)$$
$$5 \cdot 9 = 45 = 4 \cdot 11 + 1 \equiv 1 \ (\mathrm{mod} \ 11)$$
$$7 \cdot 8 = 56 = 5 \cdot 11 + 1 \equiv 1 \ (\mathrm{mod} \ 11)$$

# Question 5

Fermat's Little Theorem states that, if a number $p$ is prime and another number $a$ is not divisible by $p$, then

$$a^{(p-1)} = 1 \ (\text{mod } p)$$

Therefore, we can solve $23^{1002} \ (\text{mod } 41)$ by:

$$23^{1002} \ (\text{mod } 41) = (23^{40})^{23} \cdot 23^2 \ (\text{mod } 41)$$
$$= 1^{23} \cdot 23^2 \ (\text{mod } 41)$$
$$= 23^2 \ (\text{mod } 41)$$
$$= 529 \ (\text{mod } 41)$$
$$529 = 12 \cdot 41 + 37$$
$$529 \ (\text{mod } 41) = \boxed{37}$$

# CS220 Discrete Math - Homework #7

Brendan Nguyen - `brendan.nguyen001@umb.edu`

March 24, 2022

## Question 1

We will use induction to prove that 6 divides $n^3 - n$ for every nonnegative integer $n$. We can first define a temporary function $F(n)$ that is defined by the statement "6 divides $n^3 - n$".

**Basis step:** $n = 0$
$0^3 - 0 = 0$ & 6 divides $0 \therefore F(n)$ is true when $n = 0$

**Inductive step:** $F(n) \rightarrow F(n+1)$
We can assume that $F(n)$ is true for some positive integer $n$. We can calculate $F(n+1)$ as shown below:

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1$$
$$= (n^3 - n) + (3n^2 + 3n)$$
$$= (n^3 - n) + 3n(n+1)$$

Next, we can use features of numbers to help with our proof. We know that exactly one of any two consecutive integers will be even. Therefore, we can say that 2 divides $n(n+1)$ and $3n(n+1)$. We can also say that both 3 and 6 divide $3n(n+1)$.

By inductive hypothesis, we know that 6 divides $n^3 - n$. The previous two statements allow us to state that 6 divides $(n^3 - n) + 3n(n+1)$. Since $(n^3 - n) + 3n(n+1) = (n+1)^3 - (n+1)$, we can state that 6 also divides $(n+1)^3 - (n+1)$, in order words 6 divides $F(n+1)$.

With everything in mind, we can say that $F(n) \rightarrow F(n+1)$.

## Question 2

We can mathematical induction to prove that $AB^n = B^n A$ for all nonnegative integer $n$ given that $AB = BA$.

Firstly, we can denote a function $F(n)$ that is defined by the given statement above. Then we can prove that the function is true for $n = 1$.

$$AB^1 = AB$$
$$B^1 A = BA$$

The statements above signify each side of the inequality. Because both sides are equal to each other, we can say that $F(n)$ is true for $n = 1$. Next, we assume that $F(x)$ is true and then prove that $F(n+1)$ is true. In other words, if $AB = BA$, then $AB^x = B^x A$. By proving if $F(x+1)$ is true, we will find out if $AB^{x+1} = B^{x+1} A$ given that $AB = BA$.

$$AB^{x+1} = A \cdot (B^x B)$$
$$= (AB^x) \cdot B$$
$$= (B^x \cdot A)B$$
$$= B^x(AB)$$
$$= B^x(BA)$$
$$= (B^x B)A$$
$$= B^{x+1}A$$

Similar to before, we can say that $F(x+1)$ is true when $F(x)$ is true. Finally, by mathematical induction, we can say that $F(n)$ is true for all nonnegative integers $n$.

## Question 3

The main issue with this induction proof is the basis step. By claiming that, "$a^0 = 1$ is true by the definition of $a^0$," they are making an incorrect assumption. In order for the inductive step to work correctly, the denominator used must be one.

$$a^{k+1} = \frac{a^k \cdot a^k}{a^{k-1}}$$

The denominator hints that you must have $k \geq 1$ but we need to start the induction at $k = 0$. However, when we start at $k = 0$, then we get

$$a^1 = \frac{a^0 \cdot a^0}{a^{-1}}$$

But, we don't know for certain that $a^{-1} = 1$.

## Question 4

The set of all bit strings that are palindromes can be defined as:

- The empty string and the bit strings $0$ and $1$ are in the set
- If a string $s$ is in the set, then $0s0$ and $1s1$
- A string $s$ is in the set if it can be constructed using the two previously stated rules

## Question 5

We can use the given equality $a^{2^{n+1}} = (a^{2^n})^2$ to write the recursive algorithm below:

```
function pow(x : a real number, n : a positive integer) {
    if (n = 1) {
        return $x^2$
    }
    else {
        return pow(x, n - 1)$^2$
    }
}
```

# CS220 Discrete Math - Homework #8

Brendan Nguyen - brendan.nguyen001@umb.edu

April 7, 2022

## Question 1

First, we consider the properties of the compound proposition of $n$ variables. Each variable in the proposition has 2 options, `true` or `false`. Therefore, we can use the product rule to say that the amount of options for row will equal two times itself for the number of variables in the proposition $n$, which is $2^n$.

Then, we need to consider that each row will also have 2 options, `true` or `false`. Applying the product rule again, we see that the amount of options for truth tables will equal two times itself $2^n$ times, which is $2^{2^n}$.

## Question 2

There are 5 different congruence options for $a$ and 5 different congruence options for $b$. This means that there are 25 classes for the congruence of the pair $(a, b)$. Then, we can use pigeonhole principle to state that:

$$\left\lceil \frac{n}{25} \right\rceil = 2$$

Therefore, we can say that $\boxed{26}$ will guarantee that we have a repeating classes for the congruence of the pair $(a, b)$.

## Question 3

We can use the pigeonhole principle to prove or disprove the statement: "Let $n_1, n_2, \ldots, n_t$ be positive integers. If $n_1 + n_2 + \cdots + n_t - t + 1$ objects are placed into $t$ boxes, then for some $i$, $i = 1, 2, \ldots, t$, the $i$-th box contains at least $n_i$ objects."

First we can test it by saying that if this hypothesis is not true, then:

$$\text{box 1 contains } \leq n_1 - 1 \text{ objects}$$
$$\text{box 2 contains } \leq n_2 - 1 \text{ objects}$$
$$\vdots \qquad\qquad \vdots$$
$$\text{box } t \text{ contains } \leq n_t - 1 \text{ objects}$$

Using the equations above, we can say that all the boxes would contain $\leq (n_1 + n_2 + \cdots + n_t) - t$ objects, which would contradict the original hypothesis.

## Question 4

Given the letters ABCDEFGH,

(a) The set of permutations of the letters ABCDEFGH that contain the string ED is the same as the set of permutations of the 7-element set {A, B, C, ED, F, G, H}. Therefore, there are 7!, or 5040, permutations.

(b) Similarly, the set of permutations that contain CDE is the set of permutations of the 6-element set {A, B, CDE, F, G, H}. Therefore, there are 6!, or 720, permutations.

(c) The set of permutations that contains the strings BA and FGH is the set of permutations of the 5-element set {BA, C, D, E, FGH}. Therefore, there are 5!, or 120, permutations.

(d) The set of permutations that contains the strings AB, DE, and GH is the set of permutations of the 5-element set {AB, C, DE, F, GH}. Therefore, there are also 5!, or 120, permutations of this set.

(e) The only way this is possible is if you have a set that contains CABED. This set of permutations would have elements with {CABED, F, G, H}. Therefore, there are 4!, or 24, permutations.

(f) It is impossible for a set of permutations to contain both BCA and ABF.

## Question 5

The combinations that would satisfy the condition that there must be more women than men in the six person committee is as follows: 4 women and 2 men, 5 women and 1 man, or 6 women.

$$\binom{15}{4} \cdot \binom{10}{2} = \frac{15!}{4! \cdot 11!} \cdot \frac{10!}{2! \cdot 8!} = 1365 \cdot 45 = 61425$$

$$\binom{15}{5} \cdot \binom{10}{1} = \frac{15!}{5! \cdot 10!} \cdot \frac{10!}{1! \cdot 9!} = 3003 \cdot 10 = 30030$$

$$\binom{15}{6} = \frac{15!}{6! \cdot 9!} = 5005$$

$$\binom{15}{4} \cdot \binom{10}{2} + \binom{15}{5} \cdot \binom{10}{1} + \binom{15}{6} = 61425 + 30030 + 5005 = \boxed{96460}$$

# CS220 Discrete Math - Homework #9

Brendan Nguyen - `brendan.nguyen001@umb.edu`

April 14, 2022

## Question 1

The coefficients of $x^7$ and $x^8$ for the expansion of $(x + \frac{1}{x})^{15}$ can be found using the binomial theorem. The theorem states that given that $x$, $y$ are variables and $n$ is a nonnegative integer:

$$(x + y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} xy^{n-1} + \binom{n}{n} y^n$$

In the case of $(x + \frac{1}{x})^{15}$, our variables $x$, $y$, and $n$ are $x$, $\frac{1}{x}$, and 15 respectively as seen below:

$$\left(x + \frac{1}{x}\right)^{15} = \binom{15}{0} x^{15} + \binom{15}{1} x^{14} \left(\frac{1}{x}\right) + \binom{15}{2} x^{13} \left(\frac{1}{x}\right)^2 + \cdots + \binom{15}{14} x \left(\frac{1}{x}\right)^{14} + \binom{15}{15} \left(\frac{1}{x}\right)^{15}$$

From this rule, we can simplify each term of the expansion of $(x + \frac{1}{x})^{15}$ since $y$ is a power of $x$. Therefore, we find that the exponents of $x$ for the 16 terms of the expansion are as follows: 15, 13, 11, 9, 7, 5, 3, 1, -1, -3, -5, -7, -9, -11, -13, -15. As we can see, the expansion doesn't contain any powers of $x$ of even multiplicity so there is **no** coefficient for $x^8$. Looking at the previously compiled list of exponents, we see that the $x^7$ appears as the fifth term of the expansion and its coefficient is:

$$\binom{15}{4} = \frac{15!}{4!(15-4)!} = \frac{15!}{4! \cdot 11!} = 1365$$

## Question 2

Using a combinatorial argument, we will assume that there are two groups A and B, each of which has $n$ members in them. If we select 2 members in total, we can select either:

- One from each group: $\binom{n}{1} \cdot \binom{n}{1}$
- Two from either group: $\binom{n}{2} + \binom{n}{2}$

Therefore, we can say that:

$$\binom{2n}{2} = \binom{n}{1} \cdot \binom{n}{1} + \binom{n}{2} + \binom{n}{2}$$

$$= n \cdot n + 2\binom{n}{2}$$

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

# Question 3

If a standard deck of 52 cards is a dealt to four players, each player will get 13, or $\frac{52}{4}$, cards. Then we can use the theorem for the number of permutations with distinguishable objects which allow us to compute the number of permutations of $n$ objects in $k$ different categories given by:

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

In this example, we know that $n = 52$, $k = 4$, and $n_1, n_2, n_3, n_4 = 13$. Applying these values to the previously mentioned theorem, we get:

$$\frac{52!}{13! \cdot 13! \cdot 13! \cdot 13!} = \frac{52!}{(13!)^4} \approx 5.4 \cdot 10^{28} \text{ permutations}$$

# Question 4

We know that 7 books will not be selected (since we are choosing 5 books out of 12 total). We then create a model that represents the order of selected book using the bars and stars analogy that is hinted in the problem statement. This model would be:

$$\_ \star \_ \star \_ \star \_ \star \_ \star \_ \star \_$$

The above model suggests that we have 8 total options to place a book (as denoted by the \_) around the 7 books that won't be selected already in place (as denoted $\star$). Out of those 8 possible options, we need to place five (as denoted by $||$ below) as the above model guarantees that the none of the placed books will be adjacent to another one. One example is:

$$|| \star || \star || \star \_ \star || \star \_ \star \_ \star ||$$

The total possible combinations is:

$$\binom{8}{5} = \frac{8!}{5!(8-5)!} = \frac{8!}{5! \cdot 3!} = 56 \text{ ways}$$

Another solution to this problem is adjusting our bars and stars model. In this model, we have 5 bars and 7 stars. Then, we first place 1 star between a pair of bars, which uses 4 stars. That means that we are left with 3 stars with places left $-$ before the first bar, between 4 pairs of bars, and after that last bar. Therefore, the number of ways using this model is:

$$\binom{6+3-1}{3} = \binom{8}{3} = \frac{8!}{3!(8-3)!} = \frac{8!}{3! \cdot 5!} = 56 \text{ ways}$$

# Question 5

(a) In order to find the number of ways to place 5 distinguishable balls into 7 distinguishable boxes, we have to find the number of permutations since order matters, which is given by:

$$_nP_k = \frac{n!}{(n-k)!}$$

For our problem, $n$ is the number of distinguishable boxes, 7, and $k$ is the number of distinguishable balls, 5.

$$_7P_5 = \frac{7!}{(7-5)!} = \frac{7!}{2!} = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 2520 \text{ permutations}$$

(b) In order to find the number of ways to place 5 indistinguishable balls into 7 distinguishable boxes, we have to find the number of combinations since order doesn't matter, which is given by:

$$_nC_k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

As with the previous part, $n$ is the number of distinguishable boxes, 7, but $k$ is the number of indistinguishable balls, 5.

$$\binom{7}{5} = \frac{7!}{5!(7-5)!} = \frac{7!}{5! \cdot 2!} = 21 \text{ combinations}$$

# CS220 Discrete Math - Homework #10

Brendan Nguyen - brendan.nguyen001@umb.edu

April 21, 2022

## Question 1

To get the probability that a five-card poker hand contains a royal flush (a 10, jack, queen, king, and ace of the same suit), we first consider the amount of total possible five-card poker hands which is:

$$\binom{52}{5} = \frac{52!}{5!(52-5)!} = \frac{52!}{5! \cdot 47!} = 2,598,960 \text{ different poker hands}$$

There are only four possible poker hands that would contain a royal flush, one of each suit. This means that the probability is:

$$P(\text{royal flush hand}) = \frac{4}{\binom{52}{5}} = \frac{4}{2,598,960} \approx 1.539 \cdot 10^{-6} \equiv 0.00154\%$$

## Question 2

For the Monty Hall puzzle presented in the problem, we consider four doors. You have a $\frac{1}{4}$, or 25%, chance of selecting the right door without changing doors.

If we were to change doors, we would have to consider the remaining probability, $\frac{3}{4}$ or 75%. However, we also have to consider the fact that the host also uncovers one of the other losing doors before you change doors, meaning that the remaining $\frac{3}{4}$ is split between the two remaining doors. In mathematical form, we can represent this by denoting $D_1, D_2, D_3, D_4$ as the doors in the puzzle. We can imagine that we chose $D_1$ as an incorrect door and any one of the others doors is revealed to be an incorrect door as well.

$$P(\text{right door after changing}) = \frac{P(D_2) + P(D_3) + P(D_4)}{2} = \frac{\frac{1}{4} + \frac{1}{4} + \frac{1}{4}}{2} = \frac{\frac{3}{4}}{2} = \frac{3}{8} = 37.5\%$$

## Question 3

There are 6, or $_3P_3$, total permutations for the set $\{1,2,3\}$.

(a) There are three possible events where 1 precedes 3: $\{1,2,3\}$, $\{1,3,2\}$, and $\{2,1,3\}$. Therefore, the probability that the randomly selected permutation contains a set where 1 precedes 3 is $\frac{1}{2}$, or 50%.

(b) There are only two possible events where 3 precedes both 1 and 2: $\{3,1,2\}$ and $\{3,2,1\}$. Therefore, the probability that the randomly selected permutation contains a set where 3 precedes both 1 and 2 is $\frac{1}{3}$, or 33%.

# Question 4

There are 26!, or about $4.03 \cdot 10^{26}$, total permutations of the 26 lowercase letters.

(a) To find the probability that the randomly set of lowercase letters contains the first 13 letters in order, we only need to consider the amount of permutations of the last 13 letters because our condition will be equally likely in each of these permutations. Therefore, the probability is:

$$P(\text{first 13 in order}) = \frac{_{13}P_{13}}{26!} = \frac{13!}{26!} = \frac{1}{13!} = 1.606 \cdot 10^{-10}$$

(b) To find the probability that the randomly set of lowercase letters contains a and z next to each other, we can simplify what we are permuting on. In other words, we can think of the set as permuting 25 objects, the letters b through y and "az". In combination with the 2 permutations of "az", we then find that there are 25! permutations of the 25 objects set described previously. Thus the probability is:

$$P(\text{a and z are adjacent}) = \frac{2 \cdot 25!}{26!} = \frac{1}{13} \approx 0.077 \equiv 7.7\%$$

(c) The probability that the randomly permuted set doesn't contain a and z adjacent to one another is just to opposite of the answer in part (c):

$$P(\text{a and z are not adjacent}) = 1 - P(\text{a and z are adjacent}) = 1 - \frac{1}{13} = \frac{12}{13} \approx 0.923 \equiv 92.3\%$$

# Question 5

We know that events $E$ and $F$ are independent if and only if $p(E \cap F) = p(E)p(F)$ from the class notes. We can list all of the possible bit strings of length three.

| | | |
|---|---|---|
| 000 | 011 | 110 |
| 001 | 100 | 111 |
| 010 | 101 | |

From the list above, we can see that half of the bit strings have an odd number of 1's ($\{001, 010, 100, 111\}$) and half of them starts with 1 ($\{100, 101, 110, 111\}$). Therefore, $p(E) = \frac{1}{2}$ and $p(F) = \frac{1}{2}$. In addition, we can observe that two of the bit strings listed previously fits the criteria of when events $E$ and $F$ occur at the same time ($E \cap F : \{100, 111\}$). Therefore, $p(E \cap F) = \frac{1}{4}$. Finally, we can see if the conditions for independent events is true in this situation. We observe that:

$$p(E)p(F) = \left(\frac{1}{2}\right)\left(\frac{1}{2}\right) = \frac{1}{4} = p(E \cap F)$$

Therefore, $E$ and $F$ are independent.

# CS220 Discrete Math - Homework #11

Brendan Nguyen - brendan.nguyen001@umb.edu

April 28, 2022

## Question 1

Given that $p(E) = \frac{2}{3}$, $p(F) = \frac{3}{4}$, and $p(F|E) = \frac{5}{8}$, we can solve for $p(E|F)$ by calculating the union of $E$ and $F$.

$$p(F|E) = \frac{p(E \cap F)}{p(E)}$$

$$p(E \cap F) = p(F|E)p(E)$$

$$= \left(\frac{5}{8}\right)\left(\frac{2}{3}\right)$$

$$= \frac{5}{12} \approx 0.417$$

Finally, all we have to do is solve for $p(E|F)$ similarly to how to solved the above.

$$p(E|F) = \frac{p(E \cap F)}{p(F)}$$

$$= \left(\frac{5}{12}\right)\left(\frac{4}{3}\right)$$

$$= \frac{5}{9} \approx 0.556$$

## Question 2

Given that $E$, $F_1$, $F_2$, and $F_3$ are events from a sample space $S$ and that $F_1$, $F_2$, and $F_3$ are pairwise disjoint with their union $S$, we can use the Generalized Bayes' Theorem to find $p(F_2|E)$. The theorem is given by:

$$p(F_j|E) = \frac{p(E|F_j)p(F_j)}{\sum_{i=1}^{n} p(E|F_i)p(F_i)}$$

Applying this to our problem, we get:

$$p(F_2|E) = \frac{p(E|F_2)p(F_2)}{p(E|F_1)p(F_1) + p(E|F_2)p(F_2) + p(E|F_3)p(F_3)}$$

Finally, we just need to insert all of the values of the equation. We know that: $p(E|F_1) = \frac{2}{7}$, $p(E|F_2) = \frac{3}{8}$, $p(E|F_3) = \frac{1}{2}$, $p(F_1) = \frac{1}{6}$, $p(F_2) = \frac{1}{2}$, and $p(F_3) = \frac{1}{3}$. So, $p(F_2|E)$ is:

$$p(F_2|E) = \frac{p(E|F_2)p(F_2)}{p(E|F_1)p(F_1) + p(E|F_2)p(F_2) + p(E|F_3)p(F_3)}$$

$$= \frac{\left(\frac{3}{8}\right)\left(\frac{1}{2}\right)}{\left(\frac{2}{7}\right)\left(\frac{1}{6}\right) + \left(\frac{3}{8}\right)\left(\frac{1}{2}\right) + \left(\frac{1}{2}\right)\left(\frac{1}{3}\right)}$$

$$= \frac{\frac{3}{16}}{\frac{1}{21} + \frac{3}{16} + \frac{1}{6}}$$

$$= \frac{\frac{3}{16}}{\frac{45}{112}} = \left(\frac{3}{16}\right)\left(\frac{112}{45}\right)$$

$$= \frac{7}{15} \approx 0.467$$

## Question 3

In order to compute the expected value of a $1 lottery ticket, you need to compute a number of two elements: the probability of winning and the probability of losing. First, we know that there are $\binom{50}{6}$, or 15,890,700, possible tickets. Therefore:

$$P(\text{winning}) = \frac{1}{15,890,700} \approx 6.29 \cdot 10^{-8}$$

From this, we also know that the probability of losing is $1 - P(\text{winning})$, or 99%. A person with a winning ticket would have a net gain of $9,999,999 but a person with a losing ticket would have a net loss of $1. Therefore, the expected value $E(t)$ for an imaginary function $f(t)$ which relates ticket to winnings can be calculated as:

$$E(t) = f(\text{winning})P(\text{winning}) + f(\text{losing})P(\text{losing})$$

$$= 9,999,999 \cdot P(\text{winning}) - 1 \cdot P(\text{losing})$$

$$= \frac{9,999,999}{\binom{50}{6}} - \left(1 - \frac{1}{\binom{50}{6}}\right)$$

$$= \frac{10,000,000}{\binom{50}{6}} - 1$$

$$= \frac{10,000,000}{15,890,700} - 1$$

$$= 0.629 - 1$$

$$\approx -0.371$$

Our expected value of -0.371 means that a person loses 37 cents on average every time you pay the $1 price for a lottery ticket.

The wording of the question can also be understood as the expected value of the ticket given that you have already bought the ticket. This changes the expected value to not include the value of a losing

ticket (which would be $0). Therefore, the expected value just be:

$$E(t) = f(\text{winning})P(\text{winning})$$
$$= \frac{10,000,000}{\binom{50}{6}}$$
$$\approx 0.629$$

This expected value of 0.629 means that a ticket buyer is expected to win 63 cents on average for every ticket.

## Question 4

To find the variance of the number of times a 6 appears when a fair die is rolled 10 times, we can use the variance for a binomial distribution which is given by:

$$\sigma^2 = np(1-p)$$

Where $n$ is the number of trials and $p$ is the probability of getting a success in a fair trial. In this situation, we have 10 trials with the probability of rolling a 6, the successful result, being $\frac{1}{6}$. Therefore, the variance is:

$$\sigma^2 = npq = np(1-p) = (10)\left(\frac{1}{6}\right)\left(1-\frac{1}{6}\right) = (10)\left(\frac{1}{6}\right)\left(\frac{5}{6}\right) = \frac{25}{18} \approx 1.39$$

## Question 5

Chebyshev's Inequality tells us that:

$$p(|X(s) - E(X)| \geq r) \leq \frac{V(X)}{r^2}$$

In our problem, we will be finding the upper bound on the probability that the deviation of the coin flip is greater than $\sqrt{n}$. We can treat this problem as a Bernoulli experiment where the probability of success (getting a tail) is $\frac{2}{5}$, or 0.4.

By Theorem 4.2, the expected value for mutually independent Bernoulli trials is $np$, which is $E(X) = n \cdot \frac{2}{5} = \frac{2n}{5}$ in this case. Similarly, the variance of mutually independent Bernoulli trials is $np(1-p)$, or $V(X) = n \cdot \frac{3}{5} \cdot \frac{2}{5} = \frac{6n}{25}$. Finally, we can plug in all these values in addition to $r = \sqrt{n}$:

$$p\left(\left|X(s) - \frac{2n}{5}\right| \geq \sqrt{n}\right) \leq \frac{\frac{6n}{25}}{(\sqrt{n})^2} = \frac{6}{25} = 0.24$$

# CS220 Discrete Math - Homework #12

Brendan Nguyen - `brendan.nguyen001@umb.edu`

May 5, 2022

## Question 1

The matrix representing $R^2$ can be found by multiplying the matrix that represents $R$ by itself.

$$M_{R^2} = M_R \circ M_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

## Question 2

For these problems, we will be finding $R$, which is the smallest relation that contains the given relation $\{(1,2),(1,4),(3,3),(4,1)\}$.

(a) In order for $R$ to be **reflexive**, we know that $(1,1)$, $(2,2)$, $(3,3)$, and $(4,4)$ must be in the relation.

In order for $R$ to be **transitive**, we can see a number of things about the given relation. First, since $(1,4)$ and $(4,1)$ are in the set, 1 relates to itself (in other words, $(1,1)$ must be in the relation. Similarly, $(4,4)$ must be in the set because $(4,1)$ and $(1,4)$ are in the given relation. Finally, $(4,2)$ must also be in the relation because $(4,1)$ and $(1,2)$ are in the given relation.

Therefore, the smallest relation that is reflexive and transitive is:

$$R: \{(1,1),(2,2),(3,3),(4,4),(1,2),(4,1),(1,4),(4,2)\}.$$

(b) In order for $R$ to be **symmetric**, we know that $(2,1)$ must be in the relation because $(1,2)$ is in the relation as well. In addition, $(4,1)$ must be in the relation because $(1,4)$ is in the relation.

Our analysis of the **transitive** properties of the relation will be similar to the previous question. $(1,1)$ must be in the relation because $(1,2)$ and $(2,1)$ are in the relation. Similarly, $(4,4)$ exists because $(4,1)$ and $(1,4)$ are in the relation. Because $(2,1)$ and $(1,4)$ are in the relation, $(2,4)$ must also exist in this relation. Similarly, $(4,2)$ exists since $(4,1)$ and $(1,2)$ exists in the relation. Finally, $(2,2)$ must exist because $(2,4)$ and $(4,2)$ exist.

Therefore, the smallest relation that is symmetric and transitive is:

$$R: \{(1,1),(2,2),(3,3),(4,4),(1,2),(1,4),(2,1),(2,4),(4,1),(4,2)\}$$

(c) We can use the same **reflexive** reasoning as in part (a) to say that $(1,1)$, $(2,2)$, $(3,3)$, and $(4,4)$ are in $R$.

For $R$ to be **symmetric**, $(2,1)$ must be in $R$ because $(1,2)$ is in the relation. Also, $(4,1)$ must be in $R$ because $(1,4)$ is in the relation.

For $R$ to be **transitive**, $(4,2)$ and $(2,4)$ are in the relation. This is due to $(4,1)$ and $(1,2)$, and $(2,1)$ and $(1,4)$ are in the relation, respectively.

Therefore, the smallest relation that is reflexive, symmetric, and transitive is:

$$R : \{(1,1), (2,2), (3,3), (4,4), (1,2), (1,4), (2,1), (2,4), (4,1), (4,2)\}$$

## Question 3

To show that $R$ is an equivalence relation, we must show that $R$ is reflexive, symmetric, and transitive.

We can say that $R$ is **reflexive** because $((a,b),(a,b)) \in R$ since $ab = ba$.

If $ad = bc$, then $cb = da$ and $((c,d),(a,b)) \in R$, meaning that $R$ is **symmetric**.

We then denote $(e,f)$ as another ordered pair in the relation. If they were to follow the previously stated rule, then $((a,b),(c,d)) \in R$ and $((c,d),(e,f)) \in R$ which means that $ad = bc$ and $cf = de$. Multiplying this system of equations together results in $acdf = bcde$. Simplifying this equation results in $af = be$. Therefore $((a,b),(e,f)) \in R$ meaning that $R$ is also **transitive**.

With all of this in mind, we can say that $R$ is an equivalence relation because it is reflexive, symmetric, and transitive.

## Question 4

For each of the matrices, they are transitive if all of the diagonals are all 1s. To check for symmetry, we will turn the rows of the matrix into columns and check if the matrix is still the same. To check if it is transitive, the matrix representing $R^2$ should be the same as the matrix that represents $R$ (in other words, $M_R \circ M_R = M_R$).

(a) This relation is **reflexive** because all of its diagonals are 1's. The matrix to check for symmetry is:

$$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Because this matrix is not the same as the original matrix, we can say that $R$ is **not symmetric**. Because the matrix is not symmetric, we can say that the matrix is not a equivalence relation without checking for transitivity.

(b) This relation is **reflexive** because all of its diagonals are 1's. The matrix to check for symmetry is:

$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

This matrix is the same as the original matrix so we can say that it is **symmetric**. To check for

transitivity, we have the following:

$$M_{R^2} = M_R \circ M_R = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

Because $M_{R^2}$ is the same matrix as $M_R$, we can say that $M_R$ is a **transitive** matrix. Therefore, the matrix that represents $R$ represents an equivalence relation because it's reflexive, symmetric, and transitive.

(c) This relation is **reflexive** because all of its diagonals are 1's. The matrix to check for symmetry is:

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

This matrix is the same as the original matrix so we can say that it is **symmetric**. To check for transitivity, we have the following:

$$M_{R^2} = M_R \circ M_R = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Because $M_{R^2}$ is the same matrix as $M_R$, we can say that $M_R$ is a **transitive** matrix. Therefore, the matrix that represents $R$ represents an equivalence relation because it's reflexive, symmetric, and transitive.

## Question 5

We know that a relation is a partial ordering if it is reflexive, antisymmetric, and transitive. We will test this for each of the relations $M_R$ below.

(a) $R$ is **reflexive** because the matrix only contains 1's in the diagonal.

$R$ is also **antisymmetric** because $m_{ij} = m_{ij} = 1$ is only true when $i = j$.

We can use $M_{R^2} = M_R \circ M_R = M_R$ to check for transitivity.

$$M_{R^2} = M_R \circ M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Because $M_{R^2} \neq M_R$, $R$ is **not transitive**.

Therefore, $R$ is not a partial ordering because it is not transitive.

(b) $R$ is **reflexive** because the matrix only contains 1's in the diagonal.

$R$ is also **antisymmetric** because $m_{ij} = m_{ij} = 1$ is only true when $i = j$.

We can use $M_{R^2} = M_R \circ M_R = M_R$ to check for transitivity.

$$M_{R^2} = M_R \circ M_R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

We can see that $M_{R^2} = M_R$ meaning that $R$ is **transitive**.

Therefore, $R$ is a partial ordering because it is reflexive, antisymmetric, and transitive.

(c) $R$ is **reflexive** because the matrix only contains 1's in the diagonal.

$R$ is also **antisymmetric** because $m_{ij} = m_{ij} = 1$ is only true when $i = j$.

We can use $M_{R^2} = M_R \circ M_R = M_R$ to check for transitivity.

$$M_{R^2} = M_R \circ M_R = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Because $M_{R^2} \neq M_R$, $R$ is **not transitive**.

Therefore, $R$ is not a partial ordering because it is not transitive.