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:

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

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. $\forall x(C(x) \rightarrow P(x))$ 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. $(p \wedge t) \rightarrow (r \vee s)$	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. $u \rightarrow p$	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. $(u \wedge t) \rightarrow r$	Logical equivalence of (10)
12. $q \rightarrow (u \wedge t)$	Premise
13. $q \rightarrow r$	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 $(p \to q) \to q$, then we can use a truth table to see the truth values.

p	q	$p \to q$	$(p \to q) \to q$
T	T	T	T
T	F	F	T
F	T	T	T
F	F	T	F

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

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 $p \to q$ 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 $(p \to q)$ 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:

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

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 $g(x)>g(y)\stackrel{\text{def}}{=}\frac{1}{f(x)}<\frac{1}{f(y)}$ 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

$$\begin{aligned}\sum_{i=1}^{n} \frac{1}{i(i+1)} &= \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1}\right) \\ &= \frac{1}{1} - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{n} - \frac{1}{n+1} \\ &= 1 - \frac{1}{n+1}\end{aligned}$$

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 $f(x) = O(g(x))$.

First, I tested $c = 2$ and $k = 2$. Testing the definition for $n = 3$, I got $f(2.5) \leq c(g(2.5)) \rightarrow 25 \leq 54$. 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 $f(4) \leq c(g(4)) \rightarrow 33 \leq 162$. 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:

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

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

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 3×9, 9×4, and 4×2, respectively:

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

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

The above calculations show that `A(BC)` is more efficient than `(AB)C` while maintaining the resulting 3×2 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 $(20\text{CBA})_{16}$ and $(\text{A01})_{16}$ are shown below.

$$\begin{array}{rr} & {\scriptstyle 1} \\ & 20\text{CBA}_{16} \\ + & \text{A01}_{16} \\ \hline & 216\text{BB}_{16} \end{array}$$

$$\begin{array}{rr} & {\scriptstyle 7\ 7\ 6} \\ & 20\text{CBA}_{16} \\ \times & \text{A01}_{16} \\ \hline & 20\text{CBA}_{16} \\ & 0 \\ + & 147\text{F}4400_{16} \\ \hline & 148150\text{BA}_{16} \end{array}$$

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

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 $p_1p_2 \cdots p_n + 1$ is prime for every n where $p_1p_2 \cdots p_n$ are the n smallest prime numbers, we can test random numbers of the first few prime numbers.

$$
\begin{aligned}
n = 1 &: 2 + 1 = 3 \text{ prime} \\
2 &: 2 \times 3 + 1 = 7 \text{ prime} \\
3 &: 2 \times 3 \times 5 + 1 = 31 \text{ prime} \\
4 &: 2 \times 3 \times 5 \times 7 + 1 = 211 \text{ prime} \\
5 &: 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311 \text{ prime} \\
6 &: 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509 \text{ NOT prime}
\end{aligned}
$$

Because the statement fails for the 6 smallest prime numbers, we can say that $p_1p_2 \cdots p_n + 1$ is not prime for every n.

Question 2

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

$$
\begin{aligned}
89 &= 2 \times 34 + 21 \\
34 &= 1 \times 21 + 13 \\
21 &= 1 \times 13 + 8 \\
13 &= 1 \times 8 + 5 \\
8 &= 1 \times 5 + 3 \\
5 &= 1 \times 3 + 2 \\
3 &= 1 \times 2 + \boxed{\mathbf{1}}
\end{aligned}
$$

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

$$
\begin{aligned}
1 &= 3 - (5 - 3) \\
&= 2 \times 3 - 5 \\
&= 2 \times (8 - 5) - 5 \\
&= 2 \times 8 - 3 \times 5 \\
&= 2 \times 8 - 3 \times (13 - 8) \\
&= 5 \times 8 - 3 \times 13 \\
&= 5 \times (21 - 13) - 3 \times 13 \\
&= 5 \times 21 - 8 \times 13 \\
&= 5 \times 21 - 8(34 - 21) \\
&= 13 \times 21 - 8 \times 34 \\
&= 13 \times (89 - 2 \times 34) - 8 \times 34 \\
&= 13 \times 89 - 26 \times 34 - 8 \times 34 \\
&= 13 \times 89 - \boxed{\mathbf{34}} \times 34
\end{aligned}
$$

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.

$$
\begin{aligned}
34x &\equiv 77 (\mathrm{mod}\, 89) \\
1870x &= 55 \times 77 (\mathrm{mod}\, 89) \\
x &\equiv 4235 \equiv 47 \times 89 + 52 \equiv \boxed{\mathbf{52}} (\mathrm{mod}\, 89)
\end{aligned}
$$

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:

$$
\begin{aligned}
2 \times 6 = 12 = 1 \times 11 + 1 &\equiv 1 (\mathrm{mod}\, 11) \\
3 \times 4 = 12 = 1 \times 11 + 1 &\equiv 1 (\mathrm{mod}\, 11) \\
5 \times 9 = 45 = 4 \times 11 + 1 &\equiv 1 (\mathrm{mod}\, 11) \\
7 \times 8 = 56 = 5 \times 11 + 1 &\equiv 1 (\mathrm{mod}\, 11)
\end{aligned}
$$

Question 5

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

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

Therefore, we can solve $23^{1002} \bmod 41$ by:

$$\begin{aligned}
23^{1002} (\mathrm{mod}\, 41) &= (23^{40})^{23} \times 23^2 (\mathrm{mod}\, 41) \\
&= 1^{23} \times 23^2 (\mathrm{mod}\, 41) \\
&= 23^2 (\mathrm{mod}\, 41) \\
&= 529 (\mathrm{mod}\, 41) \\
529 &= 12 \times 41 + 37 \\
529 (\mathrm{mod}\, 41) &= \boxed{\mathbf{37}}
\end{aligned}$$