CS215: Discrete Math (H)
2025 Fall Semester Written Assignment # 2
Due: Oct. 27th, 2025, please submit at the beginning of class

Q.1 Suppose that A, B and C are three finite sets. For each of the following, determine whether or not it is true. Explain your answers.

(1) $(A - B = A) \to (B \subseteq A)$

(2) $(A - B = \emptyset) \to (A \cap B = B \cap A)$

(3) $(A \subseteq B) \to (|A \cup B| \geq 2|A|)$

Solution:

(1) False. As an counterexample, let $A = \{1\}$, and $B = \{2\}$. Then $A - B = A$, but B is not a subset of A.

(2) True. $A \cap B = B \cap A$ is always true. This is a trivial proof.

(3) False. Let $A = B = \{1\}$. Then, $A \subseteq B$ is true, but $|A \cup B| = 1 < 2 = 2|A|$, which is false.

$\square$

Q.2 Let's formulate the "Barber's paradox" in the language of predicate logic. In English, the paradox may be stated as:

"The barber of the village Seville shaves those residents of Seville who do not shave themselves."

Assume that S is the set of all residents of Seville, which includes the barber. We have the following predicates over elements of the set S:

- $Shaves(x, y)$: true if x shaves y, false otherwise.
- $Barber(x)$: true if x is the barber of Seville (you may assume that Seville has just one barber), false otherwise.

Rewrite the statement of the paradox using only these two predicates, along with the notation of mathematical logic. Please also state the reason why the paradox occurs in the logical statement.

Solution: We first rephrase the paradox in a more logic-friendly form:

"The barber of Seville shaves every resident of Seville if and only if the latter does not shave himself."

This seems easier to translate. Here is a first attempt:

$$\forall x \in S \ (Shaves(\text{Barber-of-Seville}, x) \leftrightarrow \neg Shaves(x, x))$$

But what is this mysterious "Barber-of-Seville" object? We have no constants like this given to us. So we must think of a clever way to introduce the barber. We rephrase the statement again:

"There is a barber of Seville, and he shaves every resident of Seville if and only if the latter does not shave himself."

This can be translated as:

$$\exists y \in S \ Barber(y) \wedge (\forall x \in S \ (Shaves(x, y) \leftrightarrow \neg Shaves(x, x)))$$

The paradox occurs, of course, because we allow $x = y$, in which case we have $Shaves(y, y) \leftrightarrow \neg Shaves(y, y)$, which is apparently false, so the condition on y can never be satisfied and this contradicts the existence of such a y. Note that the $Barber(y)$ term is actually completely unnecessary for the paradox itself.

□

Q.3 Prove or disprove the following.

(1) For any three sets A, B, C, $C - (A \cap B) = (C - A) \cap (C - B)$.

(2) For any two sets A, B, $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$, where $\mathcal{P}(A)$ denotes the power set of the set A.

(3) For any two sets A, B, $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$, where $\mathcal{P}(A)$ denotes the power set of the set A.

(4) For a function $f : X \to Y$, $f(A \cap B) = f(A) \cap f(B)$, for any two sets $A, B \subseteq X$.

Solution:

(1) The statement is false. A counterexample is: $A = \{1\}$, $B = \{2\}$, $C = \{1, 2\}$. Then $C - (A \cap B) = \{1, 2\}$ but $(C - A) \cap (C - B) = \emptyset$.

(2) The statement is true. We first prove that $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$. Take any subset $X \subseteq A \cap B$, then by definition of power set, $X \in \mathcal{P}(A \cap B)$. Also, $X \subseteq A$ and $X \subseteq B$, it follows that $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$. Then we have $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$. On the other hand, for $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$, we have $X \subseteq A$ and $X \subseteq B$. This means that $X \subseteq A \cap B$. Thus, $X \in \mathcal{P}(A \cap B)$. The other part $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$ is proved.

(3) The statement is false. A counterexample is: $A = \{1\}$, $B = \{2\}$. Then $\mathcal{P}(A) = \{\emptyset, \{1\}\}$, $\mathcal{P}(B) = \{\emptyset, \{2\}\}$, $\mathcal{P}(A) \cup \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}\}$. However, $\mathcal{P}(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

(4) The statement is false. A counterexample is: $f(n) = n^2$. Consider $A = \{1\}$ and $B = \{-1\}$. Then $f(A) = \{1\}$ and $f(B) = \{1\}$. Thus, $f(A) \cap f(B) = \{1\}$. However, $A \cap B = \emptyset$ and hence $f(A \cap B) = \emptyset$.

$\square$

Q.4 Give an example of two uncountable sets A and B such that the intersection $A \cap B$ is

(a) finite,

(b) countably infinite,

(c) uncountable.

Solution:

(a) $A = \{x \in \mathbb{R} | x \geq 0\}$, $B = \{x \in \mathbb{R} | x \leq 0\}$

(b) $A = \{x \in \mathbb{R} | 0 < x < 1\} \cup \mathbb{N}$, $B = \{x \in \mathbb{R} | 1 < x < 2\} \cup \mathbb{N}$

(c) $A = \{X \in \mathbb{R} | 0 < x < 1\}$, $B = \{x \in \mathbb{R} | 0 < x < 2\}$.

$\square$

Q.5 The *symmetric difference* of A and B, denoted by $A \oplus B$, is the set containing those elements in either A or B, but not in both A and B. Give an example of two uncountable sets A and B such that the intersection $A \oplus B$ is

(a) finite,

(b) countably infinite,

(c) uncountable.

Solution:

(a) $A = \{x \in \mathbb{R} | 1 \leq x < 2\}$, $B = \{x \in \mathbb{R} | 1 < x \leq 2\}$. Then $A \oplus B = \{1, 2\}$.

(b) $A = \{x \in \mathbb{R} | 1 < x < 2\} \cup \mathbb{N}$, $B = \{x \in \mathbb{R} | 1 < x < 2\} \cup \{0\}$. Then $A \oplus B = \mathbb{Z}^+$.

(c) $A = \{x \in \mathbb{R} | 0 < x \leq 1\}$, $B = \{x \in \mathbb{R} | 0 < x < 2\}$. Then $A \oplus B = \{x \in \mathbb{R} | 1 < x < 2\}$.

$\square$

Q.6 Show that if $A \subseteq C$ and $B \subseteq D$, then $A \times B \subseteq C \times D$.
Solution: We need to show that every element of $A \times B$ is also an element of $C \times D$. By definition, a typical element of $A \times B$ is a pair (a, b) where $a \in A$ and $b \in B$. Because $A \subseteq C$, we know that $a \in C$; similarly, $b \in D$. Therefore, we have $(a, b) \in C \times D$.

$\square$

Q.7 Suppose that f is an invertible function from Y to Z and g is an invertible function from X to Y. Show that the inverse of the composition $f \circ g$ is given by $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
Solution: This follows directly from the definition. We want to show that

$$\begin{array}{l} ((f \circ g) \circ (g^{-1} \circ f^{-1}))(z) \\ \quad = \quad (f \circ g)((g^{-1} \circ f^{-1})(z)) \\ \quad = \quad (f \circ g)(g^{-1}(f^{-1}(z))) \\ \quad = \quad f(g(g^{-1}(f^{-1}(z)))) \\ \quad = \quad f(f^{-1}(z)) \\ \quad = \quad z. \end{array}$$

The second equality is similar.

□

Q.8 Suppose that two functions $g : A \to B$ and $f : B \to C$ and $f \circ g$ denotes the *composition* function.

(a) If $f \circ g$ is one-to-one and g is one-to-one, must f be one-to-one? Explain your answer.

(b) If $f \circ g$ is one-to-one and f is one-to-one, must g be one-to-one? Explain your answer.

(c) If $f \circ g$ is one-to-one, must g be one-to-one? Explain your answer.

(d) If $f \circ g$ is onto, must f be onto? Explain your answer.

(e) If $f \circ g$ is onto, must g be onto? Explain your answer.

Solution:

(a) No. We prove this by giving a counterexample. Let $A = \{1, 2\}$, $B = \{a, b, c\}$, and $C = A$. Define the function g by $g(1) = a$ and $g(2) = b$, and define the function f by $f(a) = 1$, and $f(b) = f(c) = 2$. Then it is easily verified that $f \circ g$ is one-to-one and g is one-to-one. But f is not one-to-one.

(b) Yes. For any two elements $x, y \in A$ with $x \neq y$, assume to the contrary that $g(x) = g(y)$. On one hand, since $f \circ g$ is one-to-one, we have $f \circ g(x) \neq f \circ g(y)$. One the other hand, $f \circ g(x) = f(g(x)) = f(g(y)) = f \circ g(y)$. This leads to a contradiction. Thus, $g(x) \neq g(y)$, which means that g must be one-to-one.

(c) Yes. Similar to (b), the condition that f is one-to-one is in fact not used.

(d) Yes. Since $f \circ g$ is onto, we know that $f \circ g(A) = C$, which means that $f(g(A)) = C$. Note that $g(A)$ is a subset of B, thus, $f(B)$ must also be C. This means that f is also onto.

(e) No. A counterexample is the same as that in (a).

□

Q.9 Derive the formula for $\sum_{k=1}^{n} k^2$.
Solution: First we note that $k^3-(k-1)^3 = 3k^2-3k+1$. Then we sum this equation for all values of k from 1 to n. On the left, because of telescoping, we have just n^3; on the right we have

$$3\sum_{k=1}^{n} k^2 - 3\sum_{k=1}^{n} k + \sum_{k=1}^{n} 1 = 3\sum_{k=1}^{n} k^2 - \frac{3n(n+1)}{2} + n.$$

Equating the two sides and solving for $\sum_{k=1}^{n} k^2$, we obtain

$$\begin{aligned}
\sum_{k=1}^{n} k^2 &= \frac{1}{3}\left(n^3 + \frac{3n(n+1)}{2} - n\right) \\
&= \frac{n}{3}\left(\frac{2n^2+3n+3-2}{2}\right) \\
&= \frac{n}{3}\left(\frac{2n^2+3n+1}{2}\right) \\
&= \frac{n(n+1)(2n+1)}{6}
\end{aligned}$$

$\square$

Q.10 Derive the formula for $\sum_{k=1}^{n} k^3$.
Solution: Again, we use "telescoping" to derive this formula. Since $k^4 - (k-1)^4 = k^4 - (k^4 - 4k^3 + 6k^2 - 4k + 1) = 4k^3 - 6k^2 + 4k - 1$, we have

$$\begin{aligned}
\sum_{k=1}^{n} [k^4 - (k-1)^4] &= 4\sum_{k=1}^{n} k^3 - 6\sum_{k=1}^{n} k^2 + 4\sum_{k=1}^{n} k - \sum_{k=1}^{n} 1 \\
&= 4\sum_{k=1}^{n} k^3 - 6n(n+1)(2n+1)/6 + 4n(n+1)/2 - n \\
&= 4\sum_{k=1}^{n} k^3 - n(n+1)(2n+1) + 2n(n+1) - n \\
&= n^4.
\end{aligned}$$

Thus, it then follows that

$$\begin{aligned}
4\sum_{k=1}^{n} k^3 &= n^4 + n(n+1)(2n+1) - 2n(n+1) + n \\
&= n^2(n+1)^2.
\end{aligned}$$

Then we get the formula $\sum_{k=1}^{n} k^3 = n^2(n+1)^2/4$.

$\square$

Q.11 Show that a subset of a countable set is also countable.
Solution: If a set A is countable, then we can list its elements, $a_1, a_2, a_3, \ldots, a_n, \ldots$ (possibly ending after a finite number of terms). Every subset of A consists of some (or none or all) of the items in this sequence, and we can list them in the same order in which they appear in the sequence. This gives us a sequence (again, infinite or finite) listing all the elements of the subset. Thus the subset is also countable.

$\square$

Q.12 Assume that $|S|$ denotes the cardinality of the set S. Show that if $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$.
Solution:

By definition, we have one-to-one and onto functions $f : A \to B$ and $g : B \to C$. Then $g \circ f$ is a one-to-one and onto function from A to C, so we have $|A| = |C|$.

$\square$

Q.13 If A is an uncountable set and B is a countable set, must $A - B$ be uncountable?
Solution: Since $A = (A-B) \cup (A \cap B)$, if $A-B$ is countable, the elements of A can be listed in a sequence by alternating elements of $A - B$ and elements of $A \cap B$. This contradicts the uncountability of A.

$\square$

Q.14 By the Schröder-Bernstein theorem, prove that $(0, 1)$ and $[0, 1]$ have the same cardinality.
Solution: By the Schröder-Bernstein theorem, it suffices to find one-to-one functions $f : (0, 1) \to [0, 1]$ and $g : [0, 1] \to (0, 1)$. Let $f(x) = x$ and $g(x) = (x + 1)/3$. It is then straightforward to prove that f and g are both one-to-one.

$\square$

Q.15 If $f_1(x)$ and $f_1(x)$ are functions from the set of positive integers to the set of positive real numbers and $f_1(x)$ and $f_2(x)$ are both $\Theta(g(x))$, is $(f_1 - f_2)(x)$ also $\Theta(g(x))$? Either prove that it is or give a counter example.
Solution: This is false. Let $f_1 = 2x^2 + 3x$, $f_2 = 2x^2 + 2x$ and $g(x) = x^2$.

$\square$

Q.16 Show that if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, a_1, \ldots, a_{n-1}$, and a_n are real numbers and $a_n \neq 0$, then $f(x)$ is $\Theta(x^n)$.
Solution:

We need to show inequalities in both ways. First, we show that $|f(x)| \leq Cx^n$ for all $x \geq 1$ in the following. Noting that $x^i \leq x^n$ for such values of x whenever $i < n$. We have the following inequalities, where M is the largest of the absolute values of the coefficients and $C = (n+1)M$:

$$\begin{aligned}
|f(x)| &= |a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0| \\
&\leq |a_n|x^n + |a_{n-1}|x^{n-1} + \cdots + |a_1|x + |a_0| \\
&\leq |a_n|x^n + |a_{n-1}|x^n + \cdots + |a_1|x^n + |a_0|x^n \\
&\leq Mx^n + Mx^n + \cdots + Mx^n \\
&= Cx^n.
\end{aligned}$$

For the other direction, let k be chosen larger than 1 and larger than $2nm/|a_n|$, where m is the largest of the absolute values of the a_i's for $i < n$. Then each a_{n-i}/x^i will be smaller than $|a_n|/2n$ in absolute value for all $x > k$. Now we have for all $x > k$,

$$\begin{aligned}
|f(x)| &= |a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0| \\
&= x^n \left| a_n + \frac{a_{n-1}}{x} + \cdots + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n} \right| \\
&\geq x^n |a_n/2|.
\end{aligned}$$

$\square$

Q.17 Prove that $n \log n = \Theta(\log n!)$ for all positive integers n.

Solution: We first prove that $n \log n = \Omega(\log n!)$. Since $n^n \geq 1 \cdot 2 \cdot \dots \cdot n = n!$, we have $n \log n \geq \log n!$ for all positive integers n.

We now prove that $n \log n = O(\log n!)$. It is easy to check that $(n-i)(i+1) \geq n$ for $i = 0, 1, \dots, n-1$. Thus, $(n!)^2 = (n \cdot 1)((n-1) \cdot 2)((n-2) \cdot 3) \cdots (2 \cdot (n-1))(1 \cdot n) \geq n^n$. Therefore, $2 \log n! \geq n \log n$.

$\square$

Q.18

(a) Show that this algorithm determines the number of 1 bits in the bit string S:

Algorithm 1 bit count (S: bit string)

```
count := 0
while S ≠ 0 do
    count := count + 1
    S := S ∧ (S − 1)
end while
return count {count is the number of 1's in S}
```

Here $S - 1$ is the bit string obtained by changing the rightmost 1 bit of S to a 0 and all the 0 bits to the right of this to 1's. [Recall that $S \wedge (S-1)$ is the bitwise AND of S and $S-1$.]

(b) How many bitwise AND operations are needed to find the number of 1 bits in a string S using the algorithm in part a)?

Solution:

(a) By the way that $S - 1$ is defined, it is clear that $S \wedge (S-1)$ is the same as S except that the rightmost 1 bit has been changed to a 0. Thus, we add 1 to *count* for every one bit (since we stop as soon as $S = 0$, i.e., as soon as S consists of just 0 bits.)

(b) Obviously, the number of bitwise AND operations is equal to the final value of *count*, i.e., the number of one bits in S.

$\square$

Q.19

(1) Show that $(\sqrt{2})^{\log n} = O(\sqrt{n})$, where the base of the logarithm is 2.

(2) Arrange the functions

$$n^n,\ (\log n)^2,\ n^{1.0001},\ (1.0001)^n,\ 2^{\sqrt{\log_2 n}},\ n(\log n)^{1001}$$

in a list such that each function is big-O of the next function.

Solution:

(1) We have

$$(\sqrt{2})^{\log n} = 2^{\log n \frac{1}{2}} = n^{\frac{1}{2}} = \sqrt{n}.$$

Thus, it is clear that $(\sqrt{2})^{\log n} = O(\sqrt{n})$.

(2) $(\log n)^2$, $2^{\sqrt{\log_2 n}}$, $n(\log n)^{1001}$, $n^{1.0001}$, $(1.0001)^n$, n^n.

□

Q.20 Give an example of two increasing functions $f(n)$ and $g(n)$ from the set of positive integers to the set of positive integers such that neither $f(n)$ is $O(g(n))$ nor $g(n)$ is $O(f(n))$.

Solution: For example, $f(n) = n^{2\lfloor n/2 \rfloor + 1}$, and $g(n) = n^{2\lceil n/2 \rceil}$.

□

Q.21 Aliens from another world come to the Earth and tell us that the *3SAT* problem is *solvable* in $O(n^8)$ time. Which of the following statements follow as a consequence?

A. All NP-Complete problems are solvable in polynomial time.

B. All NP-Complete problems are solvable in $O(n^8)$ time.

C. All problems in NP, even those that are not NP-Complete, are solvable in polynomial time.

D. No NP-Complete problem can be solved *faster* than in $O(n^8)$ in the worst case.

E. P = NP.

Solution: A. C. E.

$\square$

Q.22 Compare the following pairs of functions in terms of order of growth. In each of the following, determine if $f(n) = O(g(n))$, $f(n) = \Omega(g(n))$, $f(n) = \Theta(g(n))$. There is **no need** to explain your answers.

	$f(n)$	$g(n)$	
(1)	$(\log_2 n)^a$	n^b	here $a, b > 0$
(2)	$2^{n \log_2 n}$	$10n!$	
(3)	$\sqrt{n}$	$(\log_2 n)^5$	
(4)	$\frac{n^2}{\log_2 n}$	$(n \log_2 n)^4$	
(5)	$\log_2 n$	$\log_2(66n)$	
(6)	$1000(\log_2 n)^{0.9999}$	$(\log_2 n)^{1.001}$	
(7)	n^2	$n(\log_2 n)^{15}$	

Solution:

(1) $f(n) = O(g(n))$

(2) $f(n) = \Omega(g(n))$

(3) $f(n) = \Omega(g(n))$

(4) $f(n) = O(g(n))$

(5) $f(n) = \Theta(g(n))$

(6) $f(n) = O(g(n))$

(7) $f(n) = \Omega(g(n))$

$\square$