CS215: Discrete Math (H)
2024 Fall Semester Written Assignment # 2
Due: Oct. 28th, 2024, 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.

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

(b) $(A \cap B \cap C) \subseteq (A \cup B)$

(c) $\overline{(A - B)} \cap (B - A) = B$

Solution:

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

(b) True. $A \cap B \cap C \subseteq A \cap B \subseteq A \cup B$.

(c) False. Let $A = B = \{1\}$. Then, $\overline{A - B} \cap (B - A) = U \cap \emptyset \neq B = \{1\}$.

$\square$

Q.2 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.3 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.

(a) Determine whether the symmetric difference is associative; that is, if A, B and C are sets, does it follow that $A \oplus (B \oplus C) = (A \oplus B) \oplus C$?

(b) Suppose that A, B and C are sets such that $A \oplus C = B \oplus C$. Must it be the case that $A = B$?

Solution:

(a) Using membership table, one can show that each side consists of the elements that are in an odd number of the sets A, B and C. Thus, it follows.

(b) Yes. We prove that for every element $x \in A$, we have $x \in B$ and vice versa.

First, for elements $x \in A$ and $x \notin C$, since $A \oplus C = B \oplus C$, we know that $x \in A \oplus C$ and thus $x \in B \oplus C$. Since $x \notin C$, we must have $x \in B$. For elements $x \in A$ and $x \in C$, we have $x \notin A \oplus C$. Thus, $x \notin B \oplus C$. Since $x \in C$, we must have $x \in B$.

The proof of the other way around is similar.

□

Q.4 For each set defined below, determine whether the set is *countable* or *uncountable*. Explain your answers. Recall that $\mathbb{N}$ is the set of natural numbers and $\mathbb{R}$ denotes the set of real numbers.

(a) The set of all subsets of students in CS201

(b) $\{(a, b)|a,\ b \in \mathbb{N}\}$

(c) $\{(a, b)|a \in \mathbb{N},\ b \in \mathbb{R}\}$

Solution:

(a) Countable. The number of students in CS201 is finite, so the size of its power set is also finite. All finite sets are countable.

(b) Countable. The set is the same as $\mathbb{N} \times \mathbb{N}$. We now show a bijections between $\mathbb{Z}^+$ and the set:

$$(0, 0), (0, 1), (1, 0), (1, 1), (1, 2), \ldots.$$

(c) Uncountable. Since $\mathbb{R}$ is uncountable, any sequence that includes an element from $\mathbb{R}$ must also be uncountable.

□

Q.5 Give an example of two uncountable sets A and B such that the difference $A - B$ is

(a) finite,

(b) countably infinite,

(c) uncountable.

Solution: In each case, let A be the set of real numbers.

(a) Let B be the set of real numbers as well, then $A - B = \emptyset$, which is finite.

(b) Let B be the set of real numbers that are not positive integers, then $A - B = \mathbf{Z}^+$, which is countably infinite.

(c) Let B be the set of positive real numbers. Then $A - B$ is the set of negative real numbers, which is uncountable.

$\square$

Q.6 Prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ if and only if $A \subseteq B$.
Solution: For the "if" part, given $A \subseteq B$, we want to show that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, i.e., if $C \subseteq A$, then $C \subseteq B$. Since $A \subseteq B$, $A \subseteq C$ directly follows.

For the "only if" part, given that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, we want to show that $A \subseteq B$. Suppose that $a \in A$. Then $\{a\} \in \mathcal{P}(A)$. Since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, it follows that $\{a\} \in \mathcal{P}(B)$, which means that $\{a\} \subseteq B$. This implies that $a \in B$, and completes the proof.

$\square$

Q.7 For each set A, the *identity function* $1_A : A \to A$ is defined by $1_A(x) = x$ for all x in A. Let $f : A \to B$ and $g : B \to A$ be the functions such that $g \circ f = 1_A$. Show that f is one-to-one and g is onto.
Solution: First, let's show that f is one-to-one. Let x, y be two elements of A such that $f(x) = f(y)$. Then $x = 1_A(x) = g(f(x)) = 1_A(y) = y$.

Next, let's show that g is onto. Let x be any element of A. Then $f(x)$ is an element of B such that $g(f(x)) = 1_A(x) = x$, this means for any element in A, $f(x)$ is its preimage in the set B.

$\square$

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).

$\square$

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 Find a formula for $\sum_{k=0}^{m}\lfloor\sqrt{k}\rfloor$, when m is a positive integer.
Solution:

By the definition of the floor function, there are $2n+1$ n's in the summation. Let $n = \lfloor\sqrt{m}\rfloor - 1$. Then

$$\begin{aligned}
&\sum_{k=0}^{m}\lfloor\sqrt{k}\rfloor \\
&= \sum_{i=1}^{n}(2i^2+i) + (n+1)(m-(n+1)^2+1) \\
&= 2\sum_{i=1}^{n} i^2 + \sum_{i=1}^{n} i + (n+1)(m-(n+1)^2+1) \\
&= \frac{n(n+1)(2n+1)}{3} + \frac{n(n+1)}{2} + (n+1)(m-(n+1)^2+1)
\end{aligned}$$

□

Q.12 Show that if A, B, C and D are sets with $|A| = |B|$ and $|C| = |D|$, then $|A \times C| = |B \times D|$.
Solution: We are given bijections f from A to B and g from C to D. Then the function from $A\times C$ to $B\times D$ that sends (a, c) to $(f(a), g(c))$ is a bijection. Thus, we have $|A \times C| = |B \times D|$.

□

Q.13 Show that if A and B are sets with the same cardinality, then $|A| \leq |B|$ and $|B| \leq |A|$.
Solution: If A and B have the same cardinality, then we have a one-to-one correspondence $f : A \to B$. The function f meets the requirement of the definition that $|A| \leq |B|$, and f^{-1} meets the requirement of the definition that $|B| \leq |A|$.

□

Q.14 Suppose that A is a countable set. Show that the set B is also countable if there is an onto function from A to B.

Solution: If $A = \emptyset$, then the only way for the conditions to be met are that $B = \emptyset$ as well, and we are done. So assume that A is nonempty. Let f be the given onto function from A to B, and let $g : \mathbf{Z}^+ \to A$ be an onto function that establishes the countability of A. If A is finite rather than countably infinite, say of cardinality of k, then the function g can be simply defined so that $g(1), g(2), \ldots, g(k)$ will list the elements of A, and $g(n) = g(1)$ for $n > k$. We need to find an onto function from $\mathbf{Z}^+$ to B. The function $f \circ g$ does the trick, because the composition of two onto functions is onto.

□

Q.15 Show that the set $\mathbf{Z}^+ \times \mathbf{Z}^+$ is countable by showing that the polynomial function $f : \mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}^+$ with $f(m, n) = (m + n - 2)(m + n - 1)/2 + m$ is one-to-one and onto.
Solution: It is clear from the formula that the range of values the function takes on for a fixed value of $m+n$, say $m+n = x$, is $(x-2)(x-1)/2+1$ through $(x-2)(x-1)/2+(x-1)$, because m can assume the values $1, 2, 3, \ldots, (x-1)$ under these conditions, and the first term in the formula is a fixed positive integer when $m+n$ is fixed. To show that this function is one-to-one and onto, we merely need to show that the range of values for $x + 1$ picks up precisely where the range of values for x left off, i.e., that $f(x - 1, 1) + 1 = f(1, x)$. We have $f(x - 1, 1) + 1 = (x - 2)(x - 1)/2 + (x - 1) + 1 = (x^2 - x + 2)/2 = (x - 1)x/2 + 1 = f(1, x)$.

□

Q.16 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.

□

Q.17 Suppose that $f(x), g(x)$ and $h(x)$ are functions such that $f(x)$ is $\Theta(g(x))$ and $g(x)$ is $\Theta(h(x))$. Show that $f(x)$ is $\Theta(h(x))$.

Solution: The definition of "$f(x)$ is $\Theta(g(x))$" is that $f(x)$ if both $O(g(x))$ and $\Omega(g(x))$. This means that there are positive constants C_1, k_1, C_2, and k_2 such that $|f(x)| \le C_2|g(x)|$ for all $x > k_2$ and $|f(x) \ge C_1|g(x)|$ for all $x > k_1$. Similarly, we have that there are positive constants C_1', k_1', C_2', and k_2' such that $|g(x)| \le C_2'|h(x)|$ for all $x > k_2'$ and $|g(x)| \ge C_1'|h(x)|$ for all $x > k_1'$. We can combine these inequalities to obtain $|f(x)| \le C_2C_2'|h(x)|$ for all $x > \max(k_2, k_2')$ and $|f(x)| \ge C_1C_1'|h(x)|$ for all $x > \max(k_1, k_1')$. This means that $f(x)$ is $\Theta(h(x))$.

□

Q.18 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 $g(x) = x^2$.

□

Q.19 Show that if $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, where $a_0, a_1, \ldots, a_{n-1}$, and a_n are real numbers and $a_n \ne 0$, then $f(x)$ is $\Theta(x^n)$.
Solution:

We need to show inequalities in both ways. First, we show that $|f(x)| \le Cx^n$ for all $x \ge 1$ in the following. Noting that $x^i \le x^n$ 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 $C = (n+1)M$:

$$\begin{aligned}
|f(x)| &= |a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0| \\
&\le |a_n|x^n + |a_{n-1}|x^{n-1} + \cdots + |a_1|x + |a_0| \\
&\le |a_n|x^n + |a_{n-1}|x^n + \cdots + |a_1|x^n + |a_0|x^n \\
&\le Mx^n + Mx^n + \cdots + Mx^n \\
&= Cx^n.
\end{aligned}$$

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 $x > k$,

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

□

Q.20 Prove that for any $a > 1$, $\Theta(\log_a n) = \Theta(\log_2 n)$.
Solution: We must show that there exist constants C_1, C_2 and n_0 such that $\log_a n \leq C_1 \log_2 n$ and $\log_2 n \leq C_2 \log_a n$ for all $n \geq n_0$. By the change of bases formula we have

$$\log_a n = \frac{\log_2 n}{\log_2 a}.$$

Now, let $C_1 = \frac{1}{\log_2 a}$, $C_2 = \log_2 a$, and $n_0 = 1$.

□

Q.21 The conventional algorithm for evaluating a polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ at $x = c$ can be expressed in pseudocode by where the final value

Algorithm 1 polynomial ($c, a_0, a_1, \ldots, a_n$: real numbers)

```
power := 1
y := a_0
for i := 1 to n do
    power := power * c
    y := y + a_i * power
end for
return y {y = a_n c^n + a_{n-1} c^{n-1} + ... + a_1 c + a_0}
```

of y is the value of the polynomial at $x = c$. Exactly how many multiplications and additions are used to evaluate a polynomial of degree n at $x = c$? (Do not count additions used to increment the loop variable).
Solution: $2n$ multiplications and n additions.

□

Q.22 There is a more efficient algorithm (in terms of the number of multiplications and additions used) for evaluating polynomials than the conventional algorithm described in the previous exercise. It is called **Horner's method**. This pseudocode shows how to use this method to find the value of $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ at $x = c$.

Algorithm 2 Horner ($c, a_0, a_1, \ldots, a_n$: real numbers)

```
y := a_n
for i := 1 to n do
    y := y * c + a_{n-i}
end for
return y {y = a_n c^n + a_{n-1} c^{n-1} + ··· + a_1 c + a_0}
```

Exactly how many multiplications and additions are used by this algorithm to evaluate a polynomial of degree n at $x = c$? (Do not count additions used to increment the loop variable.)

Solution:

n multiplications and n additions.

□

Q.23

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

(2) Order the following function by asymptotic growth rates. That is, list them as $f_1(n), f_2(n), \ldots, f_9(n)$, such that $f_i(n) = O(f_{i+1}(n))$ for all i. You don't have to explain your answer.

n^2, $\log n$, $n \log n$, $n^{\log n}$, $(\log n)^n$, $(\log n)^{\log n}$, $(\log\log n)^{\log n}$, $(\log n)^{\log\log n}$, $3^{n/2}$.

Solution:

(1) Let $n = 2^{2^k}$, then we need to show:

$$(\log 2^{2^k})^{\log\log 2^{2^k}} = O(2^{2^k} \log(2^{2^k})).$$

We then have $(2^k)^k = O(2^{2^k} 2^k)$, and further $2^{2k} = O(2^{2^k + k})$, which is obviously true since $2^{2k} \le 2^{2^k + k}$ for all $k \ge 0$.

(2)

$$\log n,\ (\log n)^{\log\log n},\ n\log n,\ n^2,\ (\log\log n)^{\log n},\ (\log n)^{\log n},\ n^{\log n},\ 3^{n/2},\ (\log n)^n.$$

□

Q.24 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.

□