CS215: Discrete Math (H)

2023 Fall Semester Written Assignment # 2

Due: Oct. 30th, 2023, 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)
$$(A \cap B \neq \emptyset) \rightarrow ((A - B) \subset A)$$

(b)
$$(A - B = \emptyset) \rightarrow (A \cap B = B \cap A)$$

(c)
$$(A \subseteq B) \rightarrow (|A \cup B| > 2|A|)$$

Solution:

- (a) True. $A \cap B \neq \emptyset$ means that an element of the intersection will not be in A B. So, a nonempty intersection means A B is missing at least one element of A.
- (b) True. $A \cap B = B \cap A$ is always true. This is a trivial proof.
- (c) False. Let $A = B = \{1\}$. Then, $A \subseteq B$ is true, but $|A \cup B| = 1 < 2 = 2|A|$, which is false.

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.

1

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:

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

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:

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

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 In addition to union (\cup), intersection (\cap), difference (-), and power set ($\mathcal{P}(S)$), let's now add two more operations to our dealings with sets:

• Pairwise addition: $A \oplus B := \{a+b \mid a \in A, b \in B\}$ (This is also called the *Minkowski addition* of sets A and B.)

• Pairwise multiplication: $A \otimes B := \{a \times b \mid a \in A, b \in B\}.$

For example, if A is $\{1,2\}$ and B is $\{10,100\}$, then $A \oplus B = \{11,12,101,102\}$ and $A \otimes B = \{10,20,100,200\}$. Answer the following questions, and explain your answers.

- (1) Briefly describe the following sets, where \mathbb{N} denotes the set of natural numbers, and $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$:
 - (a) $\mathbb{N} \oplus \emptyset$
 - (b) $\mathbb{N} \oplus \mathbb{N}$
 - (c) $\mathbb{N}^+ \oplus \mathbb{N}^+$
 - (d) $\mathbb{N}^+ \otimes \mathbb{N}^+$
- (2) If E denotes the set of all positive even numbers, how to represent the set of all positive multiples of 4 in terms of E and the set operations above? And, how to represent the set of all positive multiples of 8?
- (3) Let $S := \{n^2 : n \in \mathbb{N}^+\}$. A Pythagorean triple consists of three positive integers x, y and z such that $x^2 + y^2 = z^2$. Construct the set of all possible z^2 such that z is the last element of a Pythagorean triple using only the set S and the set operations we have so far.

- (1) (a) \emptyset
 - (b) \mathbb{N} . The sum of any two natural numbers is a natural number. Thus, $\mathbb{N} \oplus \mathbb{N} \subseteq \mathbb{N}$, and since $0 \in \mathbb{N}$, $\mathbb{N} = \mathbb{N} \oplus \{0\} \subseteq \mathbb{N} \oplus \mathbb{N}$. We have $\mathbb{N} \oplus \mathbb{N} = \mathbb{N}$.
 - (c) $\mathbb{N}^+ \setminus \{1\}$. The sum of two positive integers is an integer ≥ 2 , and every integer $n \geq 2$ can be written as (n-1)+1, where we note that n-1 and 1 are both positive integers.
 - (d) \mathbb{N}^+ . Exactly the same argument as the second part, replacing \mathbb{N} with \mathbb{N}^+ , \oplus with \otimes and 0 with 1.
- (2) Let F be the set of positive multiples of 4. We claim that $F = E \otimes E$. Every positive even number can be written as 2k for some $k \in \mathbb{N}^+$, so $E \otimes E$ consists of elements of the general form $2j \times 2k = 4jk$, for $j, k \in \mathbb{N}^+$. In other words, every element of $E \otimes E$ is a multiple of 4. So $E \otimes E \subseteq F$. Also, every multiple of 4 is of the form $4k = 2 \times 2k$, for $k \in \mathbb{N}^+$, so $F \subseteq \{2\} \otimes E \subseteq E \otimes E$. This proves the claim.

A similar argument may show that T, the set of positive multiples of 8, is $E \otimes E \otimes E$.

(3) Observe that the set of all possible numbers of the form $x^2 + y^2$, where x and y are positive integers, is $S \oplus S$. If such a number is also the square of a positive integer z, it must be in $(S \oplus S) \cap S$, which is the required set.

Q.4 Let A, B and C be sets. Prove the following using set identities.

(1)
$$(B-A) \cup (C-A) = (B \cup C) - A$$

(2)
$$(A \cap B) \cap \overline{(B \cap C)} \cap (A \cap C) = \emptyset$$

Solution:

(1) We have

$$(B-A) \cup (C-A) = (B \cap \overline{A}) \cup (C \cap \overline{A})$$
 by definition
= $\overline{A} \cap (B \cup C)$ ditributive law
= $(B \cup C) - A$ by definition

(2) We have

$$(A \cap B) \cap \overline{(B \cap C)} \cap (A \cap C)$$

$$= (A \cap B) \cap (A \cap C) \cap \overline{(B \cap C)} \quad \text{commutative law}$$

$$= (A \cap B \cap C) \cap \overline{(B \cap C)} \quad \text{associative law}$$

$$= (A \cap B \cap C) \cap \overline{(B} \cup \overline{C}) \quad \text{De Morgan}$$

$$= ((A \cap B \cap C) \cap \overline{B}) \cup ((A \cap B \cap C) \cap \overline{C}) \quad \text{distributive law}$$

$$= \emptyset \cup \emptyset \quad \text{Complement}$$

$$= \emptyset.$$

- Q.5 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)
$$A = \{x \in \mathbb{R} | x \ge 0\}, B = \{x \in \mathbb{R} | x \le 0\}$$

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

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

Q.6 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)
$$A = \{x \in \mathbb{R} | 1 \le x < 2\}, B = \{x \in \mathbb{R} | 1 < x \le 2\}.$$
 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)
$$A = \{x \in \mathbb{R} | 0 < x \le 1\}, B = \{x \in \mathbb{R} | 0 < x < 2\}.$$
 Then $A \oplus B = \{x \in \mathbb{R} | 1 < x < 2\}.$

Q.7 For each of the following mappings, indicate what type of function they are (if any). Use the following options to describe them, and explain your answers.

- i. Not a function.
- ii. A function which is neither one-to-one nor onto.
- iii. A function which is onto but not one-to-one.
- iv. A function which is one-to-one but not onto.
- v. A function which is both one-to-one and onto.

- (a) The mapping f from \mathbb{Z} to \mathbb{Z} defined by f(x) = |2x|.
- (b) The mapping f from $\{1,3\}$ to $\{2,4\}$ defined by f(x)=2x.
- (c) The mapping f from \mathbb{R} to \mathbb{R} defined by f(x) = 8 2x.
- (d) The mapping f from \mathbb{R} to \mathbb{Z} defined by $f(x) = \lfloor x+1 \rfloor$.
- (e) The mapping f from \mathbb{R}^+ to \mathbb{R}^+ defined by f(x) = x 1.
- (f) The mapping f from \mathbb{Z}^+ to \mathbb{Z}^+ defined by f(x) = x + 1.

- (a) ii.
- (b) i.
- (c) v.
- (d) iii.
- (e) i.
- (f) iv.

Q.8 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.

Q.9 Suppose that two functions $g:A\to B$ and $f:B\to C$ and $f\circ g$ denotes the *composition* function.

6

- (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.

- (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.10 Let x be a real number. Show that $\lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor$. Solution:

Certainly every real number x lies in an interval [n, n+1) for some integer n; indeed $n = \lfloor x \rfloor$.

- if $x \in [n, n + \frac{1}{3})$, then 3x lies in the interval [3n, 3n + 1), so $\lfloor 3x \rfloor = 3n$. Moreover in this case $x + \frac{1}{3}$ is still less than n + 1, and $x + \frac{2}{3}$ is still less than n + 1. So, $\lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor = n + n + n = 3n$ as well.
- if $x \in [n + \frac{1}{3}, n + \frac{2}{3})$, then $3x \in [3n + 1, 3n + 2)$, so $\lfloor 3x \rfloor = 3n + 1$. Moreover in this case $x + \frac{1}{3}$ is in $[n + \frac{2}{3}, n + 1)$, and $x + \frac{2}{3}$ is in $[n + 1, n + \frac{4}{3})$, so $\lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor = n + n + (n + 1) = 3n + 1$ as well.

• if $x \in [n + \frac{2}{3}, n + 1)$, similar and both sides equal 3n + 2.

Q.11 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

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

$$= \frac{n}{3} \left(\frac{2n^{2} + 3n + 3 - 2}{2} \right)$$

$$= \frac{n}{3} \left(\frac{2n^{2} + 3n + 1}{2} \right)$$

$$= \frac{n(n+1)(2n+1)}{6}$$

Q.12 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

$$\sum_{k=1}^{n} [k^4 - (k-1)^4] = 4 \sum_{k=1}^{n} k^3 - 6 \sum_{k=1}^{n} k^2 + 4 \sum_{k=1}^{n} k - \sum_{k=1}^{n} 1$$

$$= 4 \sum_{k=1}^{n} k^3 - 6n(n+1)(2n+1)/6 + 4n(n+1)/2 - n$$

$$= 4 \sum_{k=1}^{n} k^3 - n(n+1)(2n+1) + 2n(n+1) - n$$

$$= n^4.$$

Thus, it then follows that

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

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

Q.13 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 $n=|\sqrt{m}|-1$. Then

$$\sum_{k=0}^{m} \lfloor \sqrt{k} \rfloor$$

$$= \sum_{i=1}^{n} (2i^{2} + i) + (n+1)(m - (n+1)^{2} + 1)$$

$$= 2\sum_{i=1}^{n} i^{2} + \sum_{i=1}^{n} i + (n+1)(m - (n+1)^{2} + 1)$$

$$= \frac{n(n+1)(2n+1)}{3} + \frac{n(n+1)}{2} + (n+1)(m - (n+1)^{2} + 1)$$

Q.14 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.

Q.15 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|.

Q.16 Show that if A, B and C are sets such that $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$.

Solution: By the definition of $|A| \leq |B|$, there is a one-to-one function f from A to B. Similarly, there is a one-to-one function g from B to C. Let x and y be distinct elements of A. Because g is one-to-one, g(x) and g(y) are distinct elements of B. Because f is one-to-one, $f(g(x)) = (f \circ g)(x)$ and $f(g(y)) = (f \circ g)(y)$ are distinct elements of C. Hence, $f \circ g$ is one-to-one from A to C. It then follows that $|A| \leq |C|$.

Q.17 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.

Q.18 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.19 Show that if $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, where a_0, a_1, \dots, 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 $|f(x)| \le Cx^n$ 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:

$$|f(x)| = |a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0|$$

$$\leq |a_n| x^n + |a_{n-1}| x^{n-1} + \dots + |a_1| x + |a_0|$$

$$\leq |a_n| x^n + |a_{n-1}| x^n + \dots + |a_1| x^n + |a_0| x^n$$

$$\leq M x^n + M x^n + \dots + M x^n$$

$$= C x^n.$$

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,

$$|f(x)| = |a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0|$$

$$= x^n \left| a_n + \frac{a_{n-1}}{x} + \dots + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n} \right|$$

$$\geq x^n |a_n/2|.$$

Q.20 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 $n^n \ge 1 \cdot 2 \cdot \dots \cdot n = n!$, we have $n \log n \ge \log n!$ for all positive integers n.

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

Q.21

- (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.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.

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

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

Q.23 Suppose that $T_1(n) = O(f(n))$ and $T_2(n) = O(f(n))$. Determine whether each of the following is true or false. Justify your answers.

(1)
$$T_1(n) + T_2(n) = O(f(n))$$

(2)
$$\frac{T_1(n)}{T_2(n)} = O(1)$$

(3)
$$T_1(n) = O(T_2(n))$$

Solution:

- (1) True. Since $T_1(n) = O(f(n))$ and $T_2(n) = O(f(n))$, it follows from the definition that there exist constants $c_1, c_2 > 0$ and positive integers n_1, n_2 such that $T_1(n) \leq c_1 f(n)$ for $n \geq n_1$ and $T_2(n) \leq c_2 f(n)$ for $n \geq n_2$. This implies that, $T_1(n) + T_2(n) \leq (c_1 + c_2) f(n)$ for $n \geq \max(n_1, n_2)$. Thus, $T_1(n) + T_2(n) = O(f(n))$.
- (2) False. For a counterexample to the claim, let $T_1(n) = n^2$, $T_2(n) = n$, $f(n) = n^2$. Then $T_1(n) = O(f(n))$ and $T_2(n) = O(f(n))$ but $\frac{T_1(n)}{T_2(n)} = n \neq O(1)$.
- (3) False. We can use the same counterexample as in (2). Note that $T_1(n) \neq O(T_2(n))$.

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.