CS201H: Discrete Math for Computer Science
2021 Fall Semester   Written Assignment # 2
Due: Oct. 27th, 2021, 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) $(A \subseteq B) \rightarrow (|A \cup B| \geq 2|A|)$

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

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

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

□

Q.2 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.3 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.4 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 $\{a\} \in \mathcal{P}(A)$, so $\{a\} \in \mathcal{P}(A)$. 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.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.

(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.

$\square$

Q.6 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.7 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.8 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 $3n+2$.

$\square$

Q.9 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.10 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

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

$\square$

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 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 $|A \times C| = |B \times D|$.

$\square$

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 $|B| \leq |A|$.

$\square$

Q.14 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 $|A| \leq |C|$.

$\square$

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 $f(x - 1, 1) + 1 = (x - 2)(x - 1)/2 + (x - 1) + 1 = (x^2 - x + 2)/2 = (x - 1)x/2 + 1 = f(1, x)$.

$\square$

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.

$\square$

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 $|f(x)| \leq C_2|g(x)|$ for all $x > k_2$ and $|f(x) \geq C_1|g(x)|$ for all $x > k_1$. Similarly, we have that there are positive constants C_1', k_1', C_2', and k_2' such that $|g(x)| \leq C_2'|h(x)|$ for all $x > k_2'$ and $|g(x)| \geq C_1'|h(x)|$ for all $x > k_1'$. We can combine these inequalities to obtain $|f(x)| \leq C_2 C_2'|h(x)|$ for all $x > \max(k_2, k_2')$ and $|f(x)| \geq C_1 C_1'|h(x)|$ 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 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, 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 $x > k$,

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

□

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 $n^n \geq 1 \cdot 2 \cdot \cdots \cdot n = n!$, 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 $i = 0, 1, \ldots, n-1$. Thus, $(n!)^2 = (n \cdot 1)((n-1) \cdot 2)((n-2) \cdot 3) \cdots (2 \cdot (n-1))(1 \cdot n) \geq n^n$. Therefore, $2 \log n! \geq n \log n$.

□

Q.21

(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 $S \neq 0$ **do**
  $count := count + 1$
  $S := S \wedge (S - 1)$
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.22

(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.

$\square$

Q.23 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 $g(n) = n^{2\lceil n/2\rceil}$.

$\square$