Middle East Technical University Department of Computer Engineering

CENG 223

Discrete Computational Structures

Fall 2019-2020

Take Home Exam 2 - Solutions

Answer 1

a) (i) $A \cap (B \cup C)$

(ii) $(A \cap B) \cup C$

(iii) $(A - B) \cup (A \cap B \cap C)$
Think of $x \in B \to x \in C$ as $x \notin B \vee x \in C$

b) (i) $u \in (A \times B) \times C \to u = (y, c)$ where $y = (a, b), a \in A, b \in B, c \in C$. If u is also in $A \times (B \times C)$ then $y = (a, b) \in A$ and $c \in B \times C$ should be satisfied. Since A, B, and C are arbitrary sets this is not necessarily satisfied, therefore, the equality does not hold.

(ii)

$$\begin{aligned}(x \in (A \cap B) \cap C) &\leftrightarrow ((x \in A \cap B) \wedge (x \in C)) \leftrightarrow ((x \in A) \wedge (x \in B) \wedge (x \in C)) \\ &\leftrightarrow ((x \in A) \wedge (x \in B \cap C)) \leftrightarrow (x \in A \cap (B \cap C))\end{aligned}$$

Since the arrows are two-sided, this shows that $(A \cap B) \cap C \subseteq A \cap (B \cap C)$ and $A \cap (B \cap C) \subseteq (A \cap B) \cap C$.

(iii)

$$\begin{aligned}(A \oplus B) \oplus C &= (A \cup B - A \cap B) \oplus C = (A \cup B - A \cap B) \cup C - (A \cup B - A \cap B) \cap C \\ &= (A \cup B \cup C - A \cap B \cap \bar{C}) - \Big(((A \cap C) \cup (B \cap C)) - A \cap B \cap C\Big) \\ &= A \cup B \cup C - \big((A \cap \bar{B} \cap C) \cup (A \cap B \cap \bar{C}) \cup (\bar{A} \cap B \cap C)\big)\end{aligned}$$

Similarly,

$$\begin{aligned}A \oplus (B \oplus C) &= A \oplus (B \cup C - B \cap C) = A \cup (B \cup C - B \cap C) - A \cap (B \cup C - B \cap C) \\ &= (A \cup B \cup C - B \cap C \cap \bar{A}) - \big((A \cap \bar{B} \cap C) \cup (A \cap B \cap \bar{C})\big) \\ &= A \cup B \cup C - \big((\bar{A} \cap B \cap C) \cup (A \cap \bar{B} \cap C) \cup (A \cap B \cap \bar{C})\big)\end{aligned}$$

Proof of the used rules in-between the lines is left to the reader as an exercise.

Answer 2

a) $f^{-1}(f(A_0)) = \{a \mid f(a) \in f(A_0)\}$. Let $a \in A_0$. Then $a \in f^{-1}(f(A_0))$ meaning that $A_0 \subseteq f^{-1}(f(A_0))$. The equality does not hold only when there is an $x \notin A_0$ such that $f(x) = f(a)$ for some $a \in A_0$. If the function is injective $f(x) = f(a)$ implies $x = a$ which invalidates the possibility of $x \notin A_0$. Hence, the equaliy holds.

b) Let $b \in f(f^{-1}(B_0)) = f(\{a \mid f(a) \in B_0\})$. Then, such b is necessarily in B_0 -follows from the logical predicate part of the set builder notation-.
The equality does not hold only when there exists some $b \in B_0$ that is not in the range of f. Such a b would not be in the set $f(f^{-1}(B_0))$. But if f is surjective, no such b can exist, and the equality holds.

Answer 3

(i) →(ii) Suppose A is countable. Then it is either countably infinite or finite. If it is countably infinite, then there exist a bijection $f : \mathbb{Z}^+ \to A$ by definition, hence a surjection exists. If A is finite, there is a bijection $h : \{1, 2, \ldots, n\} \to A$ for some $n \geq 1$. h defined in this way can be extended to a surjection $f : \mathbb{Z}^+ \to A$ by defining:

$$f(x) = \begin{cases} h(i) & \text{for } 1 \leq i \leq n \\ h(1) & \text{for } i > n \end{cases}$$

(ii) →(iii) Let $f : \mathbb{Z}^+ \to A$ be a surjection. Then we can define a $g : A \to \mathbb{Z}^+$ by the equation

$$g(a) = \text{ smallest element of } f^{-1}(\{a\}).$$

Because f is surjective $f^{-1}(\{a\})$ is nonempty, which assures that g is well-defined.

Such constructed g is injective: if $a \neq a'$, the sets $f^{-1}(\{a\})$ and $f^{-1}(\{a'\})$ are disjoint -since f is a function-, so their smallest elements are different.

(iii)→(i) Let $f : A \to \mathbb{Z}^+$ be an injection. To acquire a bijection from f, it is enough to discard the numbers in $\mathbb{Z}^+$ that are not mapped to. This gives us a bijection of A with a subset of $\mathbb{Z}^+$. Thus, if we prove that every subset of $\mathbb{Z}^+$ is countable, we are done.

Let the range of f be the set $C \subseteq \mathbb{Z}^+$. If C is finite, its countability is obvious. For the case of infinite C, rigor in solutions are not sought since it is a bit cumbersome to prove the countability of an infinite subset of Z. Hence, vague arguments are accepted as solutions.

For the sake of completeness the below Lemma gives a formal proof of this claim.

Lemma. *If C is an infinite subset of $\mathbb{Z}^+$, then C is countably infinite.*

Proof. Define a bijection $h : \mathbb{Z}^+ \to C$. Define $h(1)$ to be the smallest element of C. Such an element exists, since every nonempty subset of $\mathbb{Z}^+$ has a smallest element. Then assuming that $h(1), \ldots, h(n-1)$ are defined, we define $h(n)$ as

$$h(n) = \text{smallest element of } [C - h(\{1, \ldots, n-1\})].$$

The set $C - h(\{1, \ldots, n-1\})$ is nonempty. It would be empty iff $h : \{1, \ldots, n-1\}) \to C$ is surjective, which would mean that C is a finite set - which is not the case. Thus, we have a well-defined $h(n)$.

h **is injective:** Given $m < n$, $h(m) \in h(\{1, \ldots, n-1\})$ whereas $h(n)$ is not an element of that set. Thus, $h(n) \neq h(m)$.

h **is surjective:** Let $c \in C$. Note that $h(\mathbb{Z}^+)$ cannot be contained in the finite set $\{1, \ldots, c\}$, because $h(\mathbb{Z}^+)$ would then be finite. Therefore, there is an n such that $h(n) > c$. Let $m \in \mathbb{Z}^+$ be the smallest integer satisfying $h(m) \geq c$ (m is well-defined because, again, each nonempty subset of $\mathbb{Z}^+$ has a smallest element). Then for all $i < m$, we must have $h(i) < c$. Thus, c is not in $h(\{1, \ldots, m-1\})$. Since $h(m)$ is defined as the set $C - h(\{1, \ldots, m-1\})$, we must have $h(m) \leq c$. The two inequalities together implies that $h(m) = c$. Hence the surjectivity of h. ■

Answer 4

a First notice that, the set we are talking about is a union of countable sets. If we ascribe A_n as the set of all binary strings of length n, it is clear to see that each such set has 2^n elements. Further, since our choice of n is restricted to $\mathbb{Z}^+$, the union is of countably many finite sets. Using the lemma that a countable union of countable sets is countable, we show that this set, $\bigcup_1^n A_n$, itself is countable.

> **Lemma.** *A countable union of countable sets is countable.*
>
> *Proof.* Let $A = \bigcup_1^n A_n$, where each A_n is countable. Due to the countability of each A_n there exists a function $f_n : \mathbb{Z}^+ \to A_n$ (this follows from Q3). Now, defining an indexing function for the set A would suffice to prove. To this end, we construct a $h : \mathbb{Z}^+ \times \mathbb{Z}^+ \to A$ by
>
> $$h(k, m) = f_{g(k)}(m).$$
>
> That is, the first variable of h help us choose the corresponding indexing function of the set A_k, and the second parameter is passed to the parameter of the relevant indexing function. Now, such constructed h is surjective. But since $\mathbb{Z}^+$ and $\mathbb{Z}^+ \times \mathbb{Z}^+$ are in bijective correspondence, we are done. ■

b The set at hand is uncountable by the Cantor's argument of diagonalization. You could also argue about the uncountability of this set by mapping the infinite binary strings to the interval [0, 1] of real numbers, bijectively, and make use of the cardinality of [0, 1], etc. Let us show these more formally.

Lemma. *Let* $X = \{0, 1\}$*. Then the set* $X^{|\mathbb{Z}^+|}$ *is uncountable.*

Proof. Given any function $g : \mathbb{Z}^+ \to X^\omega$, we should show that g is not surjective (ω stands for $|\mathbb{Z}^+|$). Each $g(n)$ is an ω**-tuple**, that is,

$$g(n) = (x_{n1}, x_{n2}, \ldots, x_{nm}, \ldots), \quad x_{ni} \in \{0, 1\}, i \in \mathbb{Z}^+$$

Then define an element $y = (y_1, y_2, \ldots, y_n, \ldots) \in X^\omega$ such that (this is the Cantor part)

$$y_n = \begin{cases} 0 & \text{if } x_{nn} = 1, \\ 1 & \text{if } x_{nn} = 0. \end{cases}$$

Such defined y is not mapped to by g, since by definition it differs from each $x \in X^\omega$. But clearly, $y \in X^\omega$ as well. Hence g is not surjective. ■

Answer 5

a If $\log n!$ is $\Theta(n \log n)$ then $\log n!$ should be $\Omega(n \log n)$ and $O(n \log n)$. Assume $\log n!$ is $\Omega(n \log n)$, then there are witnesses C and k such that for $n \geq k$

$$|\log n!| \geq C |\log n^n|.$$

Since functions are always positive, we have

$$\begin{aligned} logn! \geq C \log n^n \to n! \geq e^C + n^n &\to n\left(n^{n-1} - (n-1)!\right) \leq e^C \\ &\to n \leq e^C, \end{aligned}$$

where in the last step we have used $n^{n-1} - (n-1)! \geq 1$ for $n \geq 1$. Then this means that n, which is an unbounded variable cannot be greater than some constant e^C. Due to this contradiction, $\log n!$ is not $\Theta(n \log n)$.

b For $n = 4$ we have $2^n = 16 < n! = 24$. Using this for $n \geq 4$ we establish that $n!$ grows faster:

$$2^n = 2^4\, 2^{n-4} \leq 4!\, 2^{n-4} \leq 4!\, \frac{n!}{4!} = n!$$

Here, we made use of the fact that 2^{n-4} has $n - 4$ elements, all of which are lesser than those in $\frac{n!}{4!}$, which also has $n - 4$ elements.