

## Student Information

Full Name : Mert Kaan YILMAZ

Id Number : 2381093

### Answer 1

- (a) (i)  $\mathcal{T}_1$  is a topology. Since the entire space and the empty set are both open ( $A, \emptyset \in \mathcal{T}_1$ ), and there are no other elements other than those, we can say that  $\mathcal{T}_1$  is a topology.
- (ii)  $\mathcal{T}_2$  is not a topology, because "the union of any number of open sets is open" property does not hold for  $\mathcal{T}_2$ . For example,  $\{a\} \cup \{b\} = \{a, b\} \notin \mathcal{T}_2$ . Therefore, we can say  $\mathcal{T}_2$  is not a topology.
- (iii)  $\mathcal{T}_3$  is a topology.  $\emptyset$  and  $A$  are in the  $\mathcal{T}_3$ . The union of the elements of any subset of  $\mathcal{T}_3$  is in  $\mathcal{T}_3$ . Also the intersection of the elements of any subset of  $\mathcal{T}_3$  is in  $\mathcal{T}_3$ . Therefore, we can say that  $\mathcal{T}_3$  is a topology.
- (iv)  $\mathcal{T}_4$  is not a topology.  $\emptyset$  and  $A$  are in the  $\mathcal{T}_3$ , but we cannot say the union of any collection of sets in  $\mathcal{T}_4$  is also in  $\mathcal{T}_4$ . For example,  $\{a, c\} \cup \{b\} \notin \mathcal{T}_4$ , so  $\mathcal{T}_4$  is not a topology.
- (b) (i)
- (ii)
- (iii)

### Answer 2

- (a) Yes,  $f$  is injective. Let's pick random different points from,  $A \times (0,1]$  such that  $(a_1, b_1)$  and  $(a_2, b_2)$ . Assume  $f(a_1, b_1) = f(a_2, b_2)$ , so this means  $a_1 + b_1 = a_2 + b_2$ . This can be written as  $a_1 - a_2 = b_2 - b_1$ . Since the least possible difference for  $a_1 - a_2$  is 1, this equation does not hold, because  $|b_2 - b_1| < 1$  for all values of  $b_1$  and  $b_2$  in  $(0,1)$ .
- (b) No,  $f$  is not surjective. Note  $a + b \in [0, \infty)$ , and  $f(a, b) \neq 0 \forall (a, b) \in A \times (0,1)$ . If it was, then  $f(a, b) = 0 \rightarrow a + b = 0 \rightarrow a = -b$ . So  $a$  and  $b$  both should be zero, or  $b$  should be equal to  $-a$ , but  $(0,0) \notin A \times (0,1)$  and there are no  $a$  such that  $-a \in (0,1)$ . Therefore  $f$  is not surjective.
- (c) By Cantor-Schroder-Bernstein theorem, if  $A$  and  $B$  are sets with  $|A| \leq |B|$  and  $|B| \leq |A|$ , then  $|A| = |B|$ . Namely if we can show there are 1-to-1 functions  $f$  from  $A$  to  $B$  and  $B$  to  $A$ , cardinalities of  $A$  and  $B$  are same, because there is one-to-one correspondence. Since we have defined  $f$  function that is injective and given  $g$  function which is also injective, we have bijection between  $A \times (0,1)$  and  $[0, \infty)$ . Therefore, we can say that  $A \times (0,1)$  and  $[0, \infty)$  have the same cardinality.

### Answer 3

- (a) Since the domain of function is finite, and co-domain is countable; we can list all the function elements like,  $\{(0,1),(1,1),(0,2),(1,2),(0,3),(1,3),\dots\}$ , we can say that this set of function is countable.
- (b) In this function set, our domain is finite and co-domain is countable, so we can list all the function set as  $\{(0,1),(1,1),(2,1),\dots,(n,1),(0,2),(1,2),\dots,(n,2),(0,3),\dots\}$ , this function set is countable.
- (c) We count the elements of  $\mathbb{Z}^+$  like  $\mathbb{Z}^+ = \{1, -1, 2, -2, 3, -3, \dots\}$   
 Since, we can define a bijective function such that  $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+ : f(x) = x \forall x \in \mathbb{Z}^+$   
 we can say that the set C of all functions  $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  is countable.
- (d) Let's assume there are countable infinite functions from  $\mathbb{N} \rightarrow \{0,1\}$ . Functions that are defined can be written as  $f_1 : 00010101\dots$ ,  $f_2 : 110101010\dots$ ,  $f_3 : 01010111101\dots$ , ...  
 If we pick  $n^{th}$  element of  $n^{th}$  function for different n values, and construct a function, which is not in this countable infinite list, we prove by contradiction, the set D is uncountably infinite.
- (e)

### Answer 4

- (a) We start by showing that  $\log(n!)$  is  $O(n^n)$ . Then we should show that  $|\log(n!)| \leq C|\log(n^n)|$  and in the end,  $n! \leq Cn^n$  for some C and all  $n \geq k$ ;  $k, C \in \mathbb{Z}^+$ . If we choose  $k=C=1$ , we will have

$$\begin{aligned} \log(n!) &= \log(n \cdot (n-1) \dots 2 \cdot 1) \\ &= \log(1) + \log(2) + \dots + \log(n) \leq \log(n) + \log(n) + \dots + \log(n) = n \cdot \log(n) = \log(n^n) \end{aligned}$$

Therefore,  $n! < n^n$  and  $n!$  is  $O(n^n)$ .

Now we will show that  $\log(n!)$  is  $\Omega(n^n)$ . If we can show  $C|\log(n^n)| \leq |\log(n!)|$  for some C and all  $n \geq k$ ;  $C \in \mathbb{Z}^+$ . We choose  $C=k=1$ .

$$\begin{aligned} \log(n!) &= \log(1) + \log(2) + \dots + \log(n/2) + \dots + \log(n) \geq \log(n/2) + \dots + \log(n) = n/2 \cdot \log(n) \\ \log(n!) &\geq \log(n^{n/2}). \end{aligned}$$

When take exponent 10 of both sides, we can write this as,  
 $n! \geq (n/2)^{n/2}$  so,  $n!$  is  $\Omega(n^n)$

Since  $n!$  is  $O(n^n)$  and  $n!$  is  $\Omega(n^{n/2})$  We can say that  $n!$  is  $\Theta(n^n)$ .

- (b) If we can show that  $(n+a)^b$  is  $O(n^b)$  and  $(n+a)^b$  is  $\Omega(n^b)$ , then we can say  $(n+a)^b$  is  $\Theta(n^b)$ .

$$\begin{aligned} \text{for } n \geq |a| \quad (n+a)^b &\leq (2n)^b = 2^b n^b = Cn^b \\ \text{Therefore, for } C = 2^b, &\text{ we can say } (n+a)^b \text{ is } O(n^b) \end{aligned}$$

$$\begin{aligned} \text{for } n \geq |a| \quad (n+a)^b &\geq (n/2)^b = 2^{-b} n^b = Cn^b \\ \text{Therefore, for } C = 2^{-b}, &\text{ we can say } (n+a)^b \text{ is } \Omega(n^b) \end{aligned}$$

From these results, we concluded  $(n+a)^b$  is  $\Theta(n^b)$ .

## Answer 5

- (a) Let  $x = y \cdot q + r$ , and  $r = x \pmod{y}$ . We know that  $a^b - 1 = (a - 1) \cdot (a^{b-1} + a^{b-2} + \dots + 1)$ ,  $\forall k \geq 1$ . Namely,  $(a - 1) | (a^b - 1)$ .

If we choose  $2^y$  as "a" value, we get  $(2^y - 1) | (2^{y \cdot q} - 1)$ .

Therefore,

$$(2^x - 1) \pmod{(2^y - 1)} = 2^r - 1 = 2^{x \pmod{y}} - 1$$

- (b) For the Bézout's theorem, if a and b are positive integers, then there exist integers s and t such that  $\gcd(a, b) = sa + tb$

Let  $\gcd(2^m - 1, 2^n - 1) = k \mid 1$ , then,

$$2^{m-1} \equiv 0 \pmod{k} \text{ and } 2^{n-1} \equiv 0 \pmod{k}$$

$$2^m \equiv 1 \pmod{k} \text{ and } 2^n \equiv 1 \pmod{k}$$

and thus,

$$2^{ms+nt} \equiv 1 \pmod{k} \quad \forall s, t \in \mathbb{Z}$$

As we mentioned above,  $ms+nt = \gcd(m, n)$

$$2^{ms+nt} \equiv 1 \pmod{k} = 2^{\gcd(m, n)} - 1 \equiv 0 \pmod{k}$$

Therefore,

$$\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m, n)} - 1$$