Middle East Technical University

Department: Computer Science and Engineering

Year: Fall 2024-2025

Course: Discrete Computational Structures

Student's Solution

Name Surname: Ayşegül ERDEM **Student ID:** 2633196

1 Question 1 - Sets

1.

A	B	C	A⊕B	(A⊕B)⊕C	B⊕C	A⊕(B⊕C)
1	1	1	0	1	0	1
1	1	0	0	0	1	0
1	0	1	1	0	1	0
0	1	1	1	0	0	0
0	0	1	0	1	1	1
0	1	0	1	1	1	1
1	0	0	1	1	0	1
0	0	0	0	0	0	0

M⊕N means that x∈ M or x∈N but not both. For example if x∈M and x∉ N ,then x∈(M⊕N), but if x∈ M and x∈N, then x∉ (M⊕ N).
By using truth table the information above is represented simply by membership cases by assuming there is an x which is a member of a set or not (1 represents membership, 0 represents nonmembership).
In The Fourth Column
To simulate membership of A⊕B , all possible combinations of membership of the sets A or B or C are analyzed. However, since it is about A and B in this case just A and B and A⊕B are simulated.
Case 1 is x∈ A and x∈ B
By the definition of symmetric difference x cannot be an element of A⊕B.
Case 2 is x∈ A and x∉B or x∉ A and x∈ B
By the definition of symmetric difference if x is an element of one of them but not both x can be an element of A⊕B.
Case 3 is x∉A and x∉ B
By the definition of symmetric difference since x is not an element of both sets x is also cannot be an element of A⊕B.
The Fourth column is given to display the definition of symmetric difference and how it is

used in this membership table.
This table is designed to compare (A⊕B)⊕C and A⊕(B⊕C), the aim of comparing these is to understand whether the symmetric difference operation is associative or not. Hence, from the membership values of (A⊕B)⊕C and A⊕(B⊕C) it can be concluded that the symmetric difference operation is associative.

2. Assume g is not a 1-to-1 function from A to B.
It means that there exist some elements in A such that a_1,$a_2 \in$ A and $a_1 \neq a_2$, $g(a_1)$=$g(a_2)$. However, we already knew that $f(x)$ is a 1-to-1 function from B to C which means that for b_1,$b_2 \in$ B if $f(b_1)$= $f(b_2)$, then b_1 is definitely equal to b_2.
From the definition of composition functions since f(x) is a function from B to C and g(x) is a function from A to B fog(x) is a function from A to C. Since we already know that fog (x) is also one to one which can mean that if $f(x_1)$ =$f(x_2)$ for x_1,$x_2 \in$ A , then x_1 is equal to x_2 definitely.
Apply the case for a_1 and a_2, $g(a_1)$=$g(a_2)$
$f(g(a_1))$ is also equal to $f(g(a_2))$ for different parameters a_1 and a_2 because although $a_1 \neq a_2$, $g(a_1)$ is equal to $g(a_2)$ from the assumption above. Then if we assume $g(a_1)$=$g(a_2)$=y_1 and apply this to $fog(a_1)$ and $fog(a_2)$, we can obtain $f(y_1)$ from both of them. Furthermore, even if f(x) is 1-to-1, fog(x) cannot be 1-to-1 because of g(x). There is a contradiction here since we already knew that fog(x) is 1-to-1, but in this case fog(x) is not one to one.
It can be concluded from this contradiction our first assumption was wrong, and g(x) must be 1-to-1.

3. Assume there exist an onto function $f(x)$ which is from S to $P(S)$.
To accurately analyze let's first clarify the concept of an onto function. Assume $g(x)$ is an onto function from A to B. This means that for each element $b \in B$, there exists an element $a \in A$ such that $g(a)$=b. Applying this to our assumption let T be a subset of S which is also an element of $P(S)$. Considering every element in $P(S)$, for each subset of $T \subseteq S$ there should be an element in S such that $s_T \in S$ and $f(s_T)$=T .
Define a new special subset of S such that T=s$\in S$ — s$\notin f(s)$. Let T be a subset that includes all elements of S that are not in $f(s)$. Since T is a subset of S, it is also an element of $P(S)$. Given that f is assumed to be onto, there must be some element $s \in S$ such that $f(s)$=T. Now, if we apply f to this subset T, a contradiction arises. According to our definition of T, if $s \in T$, then $s \notin f(s)$; conversely, if $s \notin S$, then $s \in f(s)$. This contradiction implies that an onto function from a set S to its power set $P(S)$ cannot exist.

4. (a) Since f:$\mathbb{Z}$ x $\mathbb{Z} \rightarrow \mathbb{Z}$ to be onto for every integer z$\in \mathbb{Z}$ there must be an element of (m, n) such that $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$ and $f(m, n)$=z . It simply means that for every integer z, z should be written like $2m$+n=z .If we choose $2m$=$2z$ and n=$(-z)$, $2m$+n = $2z$+$(-z)$ = z . We can simply conclude that f is an onto function because we can obtain every

integer from $2m+n$ equation.

(b) This function represents difference of two squares it can also be represented as $(m-n)$ $(m+n)$. As it can be concluded from this definition the two part of this multiplication must be the same according to their situation about being even or odd which means that if we take m is even and n is even $(m-n)$ and $(m+n)$ should also be even or if we take m is even and n is odd $(m-n)$ and $(m+n)$ should be odd at the same time. It is acceptable for other cases for each case $(m-n)$ and $(m+n)$ must be both odd or both even at the same time. From the information above a counter example can be given which is 2 . Although 2 is in the codomain of f which is an element of $\mathbb{Z}$ it is not reachable for the function f because f can just reach the integers which is a multiplication of two odd integers or two even integers and 0. However, if the result is multiplication of two even integers it means that result is a multiple of 4 which is already greater than 2. In other case if the result is multiple of two odd integers it means that result is also odd. Hence, we cannot reach 2 by using this function, so f is not onto.

(c) Since f:$\mathbb{Z}$ x $\mathbb{Z} \rightarrow \mathbb{Z}$ to be onto for every integer z$\in \mathbb{Z}$ there must be an element of domain (m,n) such that $m \in \mathbb{Z}$ and $n\in \mathbb{Z}$ and $f(m,n)$=z . It simply means that for every integer z, z should be written like $m+n+1$. Let's choose $m=0$ and $n=z-1$ we can simply obtain z from this equation. This means that every $z \in \mathbb{Z}$ is reachable for these function. Therefore f is onto.

(d) The negativity of that function changes according to the values of m and n since they are both absolute values we can accept that if $|n|$ is greater than $|m|$ the result will be negative or if $|m|$ is greater than $|n|$ the result will be positive. From the information above both positive and negative integers can be covered by using this function. For example let's assume m=0, then we can obtain $f(0,n)$=$-|n|$ this gives us $\mathbb{Z}^-$ and if we assume $n=0$, then we can conclude $f(m,0)=|m|$ which gives us $\mathbb{Z}^+$ and finally if we assume $m=0$ and $n=0$ at the same time, we can obtain $f(0,0)$= 0 from this assumption. This assumptions can be concluded that for every integer $z\in \mathbb{Z}$ there exist an element of $\mathbb{Z}$ x $\mathbb{Z}$ such that (m,n) , $f(m,n)$ =z . Hence we could reach all elements of codomain we can conclude that f is onto

(e) This function is not onto because its range cannot cover all the codomain $\mathbb{Z}$. Let's give a counter example which is (-1) . Since $(-1) \in \mathbb{Z}$ there should be an element to be an onto function such that $(m,n) \in \mathbb{Z}$ x $\mathbb{Z}$, and $f(m,n)$ =(-1) . Let's apply the equation of f for (-1) . (m^2-4) should also be equal to (-1) to be onto, but there is not any integer like $m^2=(-3)$. Hence since $(-1) \in \mathbb{Z}$, but is not reachable for the function f , f is not onto.

5. (a) When i increases, the interval of these sets becomes smaller and smaller, this means that each new set is a subset of previous one.
$A_5 \subset A_4 \subset A_3 \subset A_2$
Intersection means that the common subset of these sets. To obtain the $\bigcap_{i=1}^{n}(0-\frac{1}{i}, 5+\frac{1}{i})$ we should just find their smallest interval. In order to do that we should just get i bigger and bigger to make the interval smaller.
Let's check the lower bound. If we increase i repeatedly ,the expression $(0 - \frac{1}{i}\ )$ approaches zero from the negative side but it never actually reaches it. Hence, zero continues to remain within this interval.
If we look at the lower bound similar things happen for it. If we repeatedly increase i the expression $(5 + \frac{1}{i}\ )$ approaches 5 from above but again it never actually reaches. Hence, five is also continues to remain within this interval
As a conclusion, no mater how much we reduce the interval, Even though the two endpoint of this interval are not included, since we cannot reach these values, and we just approaches them, the values will always remain within this range from 0 to 5.

(b) To highlight the information about the expressions in the interval. When i increases, the interval of these sets becomes bigger and bigger. This means that each new set is a subset of next one.
$A_2 \subset A_3 \subset A_4 \subset A_5$
In this case since each set is a subset of next one we should find biggest set to obtain their union.
To obtain $\bigcup_{i=1}^{n}[0+\frac{1}{i}, 5-\frac{1}{i}]$ we should just find the biggest interval. In order to expand the interval we should again get i bigger and bigger repeatedly. We must try to enlarge the upper bound and reduce the lower bound to expand the interval
Raising the upper bound. While we are increasing i the expression $(0+\frac{1}{i})$ is approaching zero from the above but it never reaches it. Therefore, zero cannot be in this interval.
Reducing lower bound. When we want to reduce upper bound similar events with upper bound occur while we are increasing i, the expression of $(5 - \frac{1}{i})$ is approaches 5 from the below, but it cannot never reaches. Therefore, five cannot be in this interval. To conclude, it is not imported that how much we increase i and expand the interval. Although two endpoint of the interval are included since we cannot reach any of them, 0 and 5 cannot be in this interval

2 Question 2 - Algorithms

1. By using the definition of Big-Oh, if we assume $sinx = \mathcal{O}(cosx)$ for some constants C and k for all $x \geq$ k the situation $|sinx| \leq C|cosx|$ can be written. Then from this equation $C \geq |\frac{sinx}{cosx}|$ must be concluded.
   When we take limit of the fraction in order to check whether it has an upper bound or not. Since, $|\frac{sinx}{cosx}|$ is equal to $|tanx|$ when we assume $|cosx| \neq 0$. We can take limit for $|tanx|$ also. $\lim_{x\to\infty} |\frac{sinx}{cosx}| = \lim_{x\to\infty} |tanx| = \infty$
   Since $\lim_{x\to\infty} |tanx|$ does not have an upper bound these limits go to infinity .
   We can conclude from here $|\frac{sinx}{cosx}|$ does not have an upper bound because there is no such number which is greater than infinity.
   Assume $|cosx| = 0$, by using the definition of Big-Oh again from $|sinx| \leq C|cosx| = 0$ we can conclude that $|sinx|$ should be equal or less than 0. however, since it is an absolute value it cannot be negative. Other case is not possible also because for all the x values which makes the $cosx = 0$, $sinx$ cannot be 0.
   Hence there is a contradiction here, and we can conclude from this contradiction $sinx \neq \mathcal{O}(cosx)$.

2. By using the definition of Big-Oh, if $f(x)$ is $\mathcal{O}(x)$ we can conclude there exists C_1 and k_1 such that for all $x \geq k_1$, $|f(x)| \leq C_1|x|$
   $|f(x)| \leq C_1|x| \leq C_1|x^2|$
   We have the knowledge about for all x $-1 \leq cosx \leq 1$ if we add 2 to all sides we can obtain $1 \leq 2 + cosx \leq 3$,and then by multiplying all sides with x^2 we can obtain $x^2 \leq x^2(2 + cosx) \leq 3x^2$
   Since we already mentioned that $|f(x)| \leq C_1|x| \leq C_1|x^2|$ for sufficiently large x, and $x^2 \leq x^2(2 + cosx)$.
   We can get them together as $|f(x)| \leq C_1|x| \leq C_1|x^2(2 + cosx)|$ for sufficiently large C_1.
   This is simply implying that $f(x)$ is $\mathcal{O}(x^2(2 + cosx))$ for constant C_1 and k_1.

3. For x ¿ 1 logarithmic functions grows more slowly than linear functions. It can be expressed like $|xlogx| \leq C\ |x|$ with C =1 and k =1 which are witnesses of this expression. Also, it can be concluded for x ¿ 1 , $|xlogx| \leq C\ |x^2|$. Therefore, for $C = 1$ and $k = 1$ which are the witnesses, $xlogx = \mathcal{O}(x^2)$.
   We can start the assumption which is $x^2 = \mathcal{O}(xlogx)$. Then by the definition of Big-Oh they should be $x^2 \leq C\ (xlogx)$ for all x ¿ 0 .
   We can obtain $\lim_{x\to\infty} |\frac{x^2}{xlogx}| \leq C$.
   Since $|\frac{x^2}{xlogx}|$ is not bounded and it grows unbounded it is not possible define a number C such that $C \geq \infty$. Hence,$x^2 \neq \mathcal{O}(xlogx)$ by the contradiction.

3 Question 3 - Divisibility

1. Assume that $\sqrt{7}$ is a rational number. Then, define two positive integers such that p and q. we can write $\sqrt{7}$ as a fraction of p and g .
   $\sqrt{7} = \frac{p}{q}$ if we take squares of both sides $7 = \frac{p^2}{q^2}$, so we can obtain $7q^2 = p^2$.
   By the Fundamental Theorem of Arithmetic every integer n ¿1 can be written as a unique product of prime numbers. Since we assume p and q are positive integers they should also can be written uniquely as the product of prime numbers. Let's assume $p = 7^m \; a_1^{k_1} \; a_2^{k_2} \; a_3^{k_3} \; ... \; a_n^{k_n}$ and from this equation it can be written that $p^2 = 7^2 m \; a_1^{2k_1} \; a_2^{2k_2} \; a_3^{2k_3} \; ... \; a_n^{2k_n}$, but from the equation above $p^2 = 7 \; q^2$. As it can be observed p^2 has two different products of primes. This is contradicting with the uniqueness of Fundamental Theorem of Arithmetic. Since there is a contradiction here, our assumption was wrong, and $\sqrt{7}$ is not a rational number.

2. If an integer p is the form of $(3k + 2)$, p can also be represented as $p \equiv 2$ (mod 3).
   Let's assume a finite set of prime numbers P of the form $(3k+2)$ such that $P = p_1, p_2, p_3, ...p_k$.
   Let define a new number such that:
   $M = (p_1 \cdot p_2 \cdot p_3 \cdot p_4 ... p_k) + 2$
   Which is not included from the finite set P . Since we obtain M by multiplying all elements in P and adding 2. M also have the same character such that $M = (3k + 2)$. However, we just defined this prime M and it is not an member of P . Hence, if new members can be created for P, P cannot be a finite set. There is a contradiction here. Since $p_n \equiv 2 \pmod 3$, their product will also be the $M \equiv 2 \pmod 3$

3. Assume $r = a$ mod m and $r = b$ mod m at the same time, and assume k and l are the integers such that $a = km + r$ and $b = lm + r$ when $m \geq 2$.
   Let's look at $gcd(a, m)$ by the Euclid's Theorem:
   $gcd(a, m) = gcd($m , a mod m$)$ which is also equal to $gcd($m , r$)$
   $gcd($b , m$)$ by the Euclid's Theorem
   $gcd($b , m$) = gcd($m , b mod m$)$ which is also equal $gcd($m , r$)$
   So $gdc(a, m) = gcd(b, m)$