Middle East Technical University

Department: Computer Science and Engineering

Year: Fall 2024-2025

Course: Discrete Computational Structures

Student's Solution

Name Surname: <Muhammed Ömer> **Student ID:** <2683142>

1 Question 1 - Sets

$x \in A$	$x \in B$	$x \in C$	$x \in (A \oplus B) \oplus C$	$x \in A \oplus (B \oplus C)$	$(A \oplus B) \oplus C \iff A \oplus (B \oplus C)$
0	0	0	0	0	1
0	0	1	1	1	1
0	1	0	1	1	1
0	1	1	0	0	1
1	0	0	1	1	1
1	0	1	0	0	1
1	1	0	0	0	1
1	1	1	1	1	1

1. **Explanations:**

- **Column 1 ($x \in A$):** This column indicates whether element x belongs to set A.
- **Column 2 ($x \in B$):** This column indicates whether element x belongs to set B.
- **Column 3 ($x \in C$):** This column indicates whether element x belongs to set C.
- **Column 4 ($x \in (A \oplus B) \oplus C$):** This column represents the symmetric difference of $(A \oplus B)$ with C. Here, $x \in (A \oplus B) \oplus C$ if either $x \in (A \oplus B)$ and $x \notin C$, or $x \notin (A \oplus B)$ and $x \in C$.
- **Column 5 ($x \in A \oplus (B \oplus C)$):** This column represents the symmetric difference of A with $(B \oplus C)$. In other words, $x \in A \oplus (B \oplus C)$ if either $x \in A$ and $x \notin (B \oplus C)$, or $x \notin A$ and $x \in (B \oplus C)$.
- **Column 6 ($(A \oplus B) \oplus C \iff A \oplus (B \oplus C)$):** This column compares the values in Columns 4 and 5. If both columns have the same value, it records 1 (true); otherwise, it records 0 (false).

Conclusion:

Since the final column (Column 6) contains a value of 1 for each row, we can see that $(A \oplus B) \oplus C$ is equal to $A \oplus (B \oplus C)$ in all cases. This confirms that the symmetric difference operation is associative.

2. - $f : B \to C$ is one-to-one.
   - $f \circ g : A \to C$ is one-to-one.

     Assume that g is not one-to-one.

     This means there exist distinct elements $a_1, a_2 \in A$ such that $a_1 \neq a_2$ but $g(a_1) = g(a_2) = b$ for some $b \in B$.

     Consider the images of a_1 and a_2 under $f \circ g$:

     $$(f \circ g)(a_1) = f(g(a_1)) = f(b)$$

     and

     $$(f \circ g)(a_2) = f(g(a_2)) = f(b).$$

     Since $g(a_1) = g(a_2) = b$, it follows that $(f \circ g)(a_1) = (f \circ g)(a_2)$.
   - Given that $f \circ g$ is one-to-one (injective), we know that if $(f \circ g)(a_1) = (f \circ g)(a_2)$, then it must be that $a_1 = a_2$. However, this contradicts our assumption that $a_1 \neq a_2$.
   - **Conclusion:** Therefore, our initial assumption that g is not one-to-one must be false. So, g must be one-to-one.

3. Assume that there exists a function $f : S \to P(S)$ that is onto. This means that for every subset $A \subseteq S$, there is some $s \in S$ such that $f(s) = A$.

   Definition:

   $$T = \{s \in S \mid s \notin f(s)\}.$$

- Assume that there is an element $s_T \in S$ such that $f(s_T) = T$. Then, we examine whether $s_T \in T$ or $s_T \notin T$ could hold:
  - If $s_T \in T$. By the definition of T, if $s_T \in T$, then $s_T \notin f(s_T)$. But since $f(s_T) = T$, this implies $s_T \notin T$. This is a contradiction.
  - If $s_T \notin T$. Then, by the definition of T, $s_T \notin T$ implies $s_T \in f(s_T)$. But since $f(s_T) = T$, this implies $s_T \in T$. This is again a contradiction.
- **Conclusion:** In both cases, we reach a contradiction. Therefore, our assumption that there exists an element $s_T \in S$ such that $f(s_T) = T$ must be false. Consequently, no such function f can be onto.

4. **a)**

Given any $y \in \mathbb{Z}$, we need to find integers m and n such that:

$$f(m, n) = 2m + n = y$$

For example, if we choose $m = 0$, then:

$$f(0, n) = 2 \cdot 0 + n = n$$

Since $n \in \mathbb{Z}$, the image of the function is all integers $\mathbb{Z}$. So, the function is **onto**.

b)

$$f(m, n) = m^2 - n^2 = y$$

Rewriting the expression:

$$f(m, n) = (m - n)(m + n) = y$$

For any $y \in \mathbb{Z}$, it's not always possible to factorize y into two integer factors. For example, for $y = 2 or y = 4$, they cannot be written as the product of two integers of the form $(m - n)(m + n)$.

for $y = 2$ the equation becomes:

$$(m - n)(m + n) = 2$$

The possible factorizations of 2 are 2×1 and $(-2) \times (-1)$, but these forms cannot be obtained by $m - n$ and $m + n$ for $m \in \mathbb{Z}$, $n \in \mathbb{Z}$.

Thus, the function is **not onto**.

c)

For any $y \in \mathbb{Z}$, we need to find m and n such that:

$$f(m, n) = m + n + 1 = y$$

For example, choose $m = -1$, then:

$$f(m, n) = n$$

Since we can obtain all $\mathbb{Z}$, the function is **onto**.

d)

For any $y \in \mathbb{Z}$, we need to find m and n such that:

$$f(m, n) = |m| - |n| = y$$

- If $y > 0$, we can set $m = y$ and $n = 0$ to get $f(m, n) = |y| - 0 = y$.
- If $y = 0$, we can set $m = 0$ and $n = 0$ to get $f(0, 0) = 0$.
- If $y < 0$, we can set $m = 0$ and $n = -y$ to get $f(0, -y) = |0| - |-y| = 0 - y = y$.

So, for any $y \in \mathbb{Z}$, we can find integers m and n such that $f(m, n) = y$. Therefore, the function is **onto**.

e)

For any $y \in \mathbb{Z}$, we need to find m such that:

$$f(m,n) = m^2 - 4 = y$$

Rewrite:

$$(m+2)(m-2) = y$$

For $y = 6$, it cannot be represented like $(m+2)(m-2)$. So, the function is **not onto**.

5. (a) For 2 for i, we have $\left(-\frac{1}{2}, \frac{11}{2}\right)$, and we are approaching to infinity.
   Let assume that 0 and 5 are not included at index $c \in \mathbb{Z}$. This means that $1/i$ in $\left(0 - \frac{1}{i}, 5 + \frac{1}{i}\right)$, equal to 0. But for c, $1/c$ cannot be 0. There is a contradiction. Then we say that 0 and 5 are in our intersection interval.

   (b) For 2 for i, we have $\left[\frac{1}{2}, \frac{9}{2}\right]$, and we are approaching to infinity.
   Let assume that 0 and 5 are included at index $c \in \mathbb{Z}$. This means that $1/i$ in $\left[0 + \frac{1}{i}, 5 - \frac{1}{i}\right]$, equal to 0. But for c, $1/c$ cannot be 0. There is a contradiction. Then we say that 0 and 5 are not in our union interval.

2 Question 2 - Algorithms

1. No, whatever values we choose for $k \in \mathbb{R}$, there exists x such that:

$$\forall k \in \mathbb{R}, \exists x \in \mathbb{R} \text{ such that } \sin(x) \geq k\cos(x)$$

Since $\sin(x)$ and $\cos(x)$ are periodic functions, for example, if $k \in (0, \infty)$ and $x = \frac{\pi}{2}$, $\sin(x) \geq k\cos(x)$. They dominate each other as x goes to infinity.

2. Given that $f(x) = O(x)$, there exist constants $c_1 > 0$, $k_1 > 0$ and $x \geq k_1$ such that:
$|f(x)| \leq c_1|x|$.
For: $a_2 > 0$, $m_2 > 0$, $x \geq m_2$, then:
$|f(x)| \leq a_2|x|^2(2 + \cos x)$.
$\cos x$ in the range $[-1, 1]$, so, $2 + \cos x$ is in $[1, 3]$. So, for $x \geq 0$;
$x^2 \leq x^2(2 + \cos x) \leq 3x^2$.
We know $|f(x)| \leq c_1|x|$ and $x^2 \leq x^2(2 + \cos x)$, it can be rewritten as:
$|f(x)| \leq c_1|x| \leq c_1 \cdot \frac{1}{x} \cdot |x|^2(2 + \cos x)$, then:
$|f(x)| \leq c_2|x|^2(2 + \cos x)$ can be obtained as $c_2 = c_1/x$ and $k_2 = k_1$.

So, $f(x) = O(x^2(2 + \cos x))$.

3. We need to find a constant $C > 0$ such that for sufficiently large x:

$$x \log x \leq C \cdot x^2.$$

Since x^2 grows faster than $x \log x$ as x increases, we know that there exists a constant C such that:

$$x \log x \leq C \cdot x^2$$

for large enough values of x. This confirms that $x \log x \in O(x^2)$.

Assume $x^2 \in O(x \log x)$. This would mean there exists a constant $C > 0$ such that for sufficiently large x:

$$x^2 \leq C \cdot x \log x.$$

Dividing both sides by x (for $x > 0$) gives:

$$x \leq C \cdot \log x.$$

Now, we can see that the term x grows much faster than $\log x$, which means that for large values of x, x will eventually exceed any constant multiple of $\log x$. No matter how large we choose C, there will always be a point beyond which $x > C \cdot \log x$. This is a contradiction.

Conclusion:

$x \log x \in O(x^2)$, but $x^2 \notin O(x \log x)$.

3 Question 3 - Divisibility

1. Assume that $\sqrt{7}$ is rational.

   By definition of rational numbers: $\sqrt{7} = \frac{p}{q}$ where $p, q \in \mathbb{Z}$, $q \neq 0$, $\gcd(p, q) = 1$.

   $$\sqrt{7} = \frac{p}{q} \Rightarrow 7 = \frac{p^2}{q^2} \Rightarrow 7q^2 = p^2$$

   So, $7|p^2$ and we can say that:

   $$p = 7a \Rightarrow 7q^2 = (7a)^2 \Rightarrow 7q^2 = 49a^2 \Rightarrow q^2 = 7a^2$$

   Similarly, $7|q^2 \Rightarrow 7|q$.

   However, there is a contradiction. We said that $\gcd(p, q) = 1$, but p and q can both divided by 7. So, assumption is false. Then, $\sqrt{7}$ is not rational number.

2. Assume that finitely many such primes exist. Let $P = \{q_1, q_2, q_3, ..., q_n\}$ be the set of all primes of form $3k + 2$.

   Consider:

   $$S = 3q_1q_2q_3...q_n - 1$$

   Note that S has form $3k + 2$ because:

   $$S = 3(q_1q_2q_3...q_m) - 1 = 3k + 2$$

   Consider:

   $$\forall i \in \{1, 2, \ldots, n\},\ \frac{S}{P_i}\ \textit{ is a natural number? No, everytime it has remaining}$$

   Since number S is form of $3k + 2$ and it cannot be divided by all these primes, S has another prime factor that is form of $3k + 2$. So, there is a contradiction. Then, we can say that the set of primes of the form $3k + 2$ are not finite.

3. By $a \equiv b \pmod{m}$, we know that:

   $$a = b + k \cdot m.$$

   Thus, we can substitute $a = b + k \cdot m$:

   $$\gcd(a, m) = \gcd(b + k \cdot m, m)$$

   By the Euclidean Algorithm:

   $$\gcd(b + k \cdot m, m) = \gcd(b, m)$$
   $$= \gcd(m, b) = \gcd(b, m)$$

   Therefore, by the Euclidean Algorithm we can say that:

   $$\gcd(a, m) = \gcd(b, m)$$