

CENG 223

Discrete Computational Structures

Fall 2023 - Take Home Exam 2

Sets and Functions

Due date: 17 November 2023, Friday, 23:59 (No Late Allowed!)

1 Specifications

1. Your work must be preferably written in a single L^AT_EX file which must be compilable in *inexs*.
2. Your work must be of your own. This is an individual homework, no collaboration is allowed.
3. Your work must obey, of course, **zero tolerance policy for cheating**. People involved in cheating will be punished according to the university regulations.
4. Your work must be submitted before the deadline. There is **no late submission policy**.
5. Your work must be submitted as specified in the section 4, otherwise there is a penalty of 10 points.
6. You may ask your questions by posting in the forum or by sending an email to “adhd@ceng.metu.edu.tr”.

2 Questions

For the following questions below, either prove the statement to be true, or disprove by contrapositive.

Question 1

convex function is a real-valued function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ if the line segment between any two distinct points on the graph of the function lies above the graph between the two points. (see figure 1)

$$\forall x_1, x_2 \in \mathbb{R}^n, t \in [0, 1] \quad f(tx_1 + (1-t)x_2) \leq tf(x_1) + (1-t)f(x_2)$$

convex set is, similarly, a real subset $\mathcal{X} \subseteq \mathbb{R}^n$ if and only if given two points in the subset, the whole line segment that joins them is also in the subset.

$$\forall x_1, x_2 \in \mathcal{X}, t \in [0, 1] \quad tx_1 + (1-t)x_2 \in \mathcal{X}$$

fun fact: a real-valued function is convex function if and only if its epigraph (the set of points on or above the graph of the function) is a convex set.

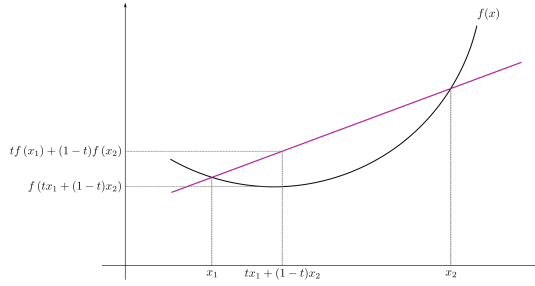


Figure 1: A convex function illustration

- a) Assume that the set $C \subseteq \mathbb{R}^n$ is a convex set. For a fixed $m > 3$ (pick 4 or 5), any linear combination of m points in the set C is also in the set C . In other words, $\sum_{i=1}^m \lambda_i x_i \in C$, where $x_i \in C$ and $\lambda_i \in \mathbb{R}$, $i = 1, \dots, m$ satisfying $\lambda_i \geq 0$ and $\sum_{i=1}^m \lambda_i = 1$
- b) Assume that the functions f and g are convex functions. Then, the function $f \circ g$ is a convex function as well.
- c) A function $f(\cdot) : S \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$ is a convex function if and only if S is convex set and the function $g(t) = f(x + tv)$ is a convex function for all $t \in \mathbb{R}$ such that $x + tv \in S$.

Question 2

σ -algebra is a subset $\Sigma \subseteq P(X)$ if and only if Σ satisfies the following three properties, where X is some set and $P(X)$ represent its power set:

- X is in Σ .
- Σ is closed under complementation: If A is in Σ , then so is its complement $X - A$.
- Σ is closed under countable unions: If A_1, A_2, \dots are in Σ , then so is $A = A_1 \cup A_2 \cup \dots$.

fun fact: elements of the **σ -algebra** are called **measurable sets**. An ordered pair (X, Σ) , where X is a set and Σ is a σ -algebra over X , is called a **measurable space**. check probability space for dig into more.

Let X be a set. Show for each of the following sets whether they are a σ -algebra on X or not.

- a) the set of all $U \subseteq X$ such that $X - U$ is either finite or is \emptyset .
- b) the set of all $U \subseteq X$ such that $X - U$ is either countable or is all of X .
- c) the set of all $U \subseteq X$ such that $X - U$ is infinite or \emptyset or X .

Question 3

Let define a congruence, for any $a, b, x \in \mathbb{Z}$ and $p \in \mathbb{N}_0/\{0\}$

$$ax \equiv b \pmod{p} \Leftrightarrow ax = b + kp \quad \exists k \in \mathbb{Z}$$

A solution for x exists if and only if $x \equiv c \pmod{q}$ for some $c \in \mathbb{Z}$ and some $q \in \mathbb{N}_0/\{0\}$.

- a) the congruence $ax \equiv b \pmod{p}$ has a solution for x if and only if $\gcd(a, p) \mid b$.

hint: Bezout's identity.

- b) the pair of congruences

$$a_1x \equiv b_1 \pmod{p_1} \quad a_2x \equiv b_2 \pmod{p_2}$$

has a solution for x if $\gcd(p_1, p_2) = 1$, $\gcd(a_1, p_1) \mid b_1$, and $\gcd(a_2, p_2) \mid b_2$.

hint: Euclid's or Bezout's identity.

- c) the system of congruences

$$a_1x \equiv b_1 \pmod{p_1} \quad a_2x \equiv b_2 \pmod{p_2} \quad \dots \quad a_kx \equiv b_k \pmod{p_k}$$

has a solution for x of the form $x \equiv c \pmod{\Pi}$, where $\Pi = p_1p_2 \dots p_k$ and $\gcd(p_1, \dots, p_k) = 1$ and $\gcd(a_i, p_i) \mid b_i$ for some $c \in \mathbb{Z}$ and $i = \{1, \dots, k\}$.

hint: Chinese Remainder Theorem :D.

Question 4

- a) Let X denote the letters of the Turkish alphabet, *i.e.* $X = \{a, b, \dots, z\}$ and $|X| = 29$. Show whether $\prod_{i \in \mathbb{Z}^+} X$ is countable or not. The product symbol stands for Cartesian products of the set X with itself.
- b) Let $\{Y_i\}_{i \in \mathbb{Z}^+}$ be a family of sets each of which is countably infinite. Show whether the set $\bigcup_{i \in \mathbb{Z}^+} Y_i$ is countable or not.

Note: Your proof should take all cases in to consideration. For example, assuming $Y_i = \mathbb{Z}$ for all i and showing that the final set is countable is not a valid proof.

Note 2: For this question (both **a**) and **b**)), you can use the following without proving them: *i*) a set A is countable if and only if there exists some $f : \mathbb{Z} \rightarrow A$ that is surjective, *ii*) the set of positive integers \mathbb{Z}^+ , \mathbb{Z} and $\mathbb{Z} \times \mathbb{Z}$ have the same cardinality.

3 Ungraded Questions

Question 5

A **group** (S, \oplus) is a set S with a binary operation \oplus satisfying following four properties,

- **closure:** $\forall a, b \in S$ we have $a \oplus b \in S$
- **associativity:** $\forall a, b, c \in S$ we have $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
- **identity:** $\exists e \in S, \forall a \in S$ we have $a \oplus e = e \oplus a = a$
- **inverse:** $\forall a \in S, \exists a^{-1} \in S$ we have $a \oplus a^{-1} = a^{-1} \oplus a = e$

Let $[b]_p = \{z \in \mathbb{Z} : z \equiv b \pmod{p}\}$ denote the set of all integers congruent to b and $\mathbb{Z}_p = \{[0]_p, \dots, [p-1]_p\}$ denote the set of all integers congruents of the congruence $(\text{mod } p)$. Loosely, we can simply write it as $\{0, \dots, p-1\}$.

For questions below imagine a binary operation \oplus such that $[a]_p \oplus [b]_p = [a + b]_p$;

- a) The set $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$ forms a group under addition \oplus .

- b) The set $\mathbb{Z}_{2 \times 3} = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ forms a group under addition \oplus .
- c) The function $f_b(x) : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6 := b + x \pmod{6}$ is a bijection, more strongly a permutation.
- d) Let $[n] = \{1, \dots, n\}$ and $f_n(\cdot) : [n] \rightarrow [n]$ is a permutation of n elements. Let's denote \mathbb{S}_n to be the set of all permutations of n elements, i.e. cyclic set of order n . Then, using this definition:
The set \mathbb{S}_6 forms a group under function composition \circ .
- e) The group (\mathbb{Z}_6, \oplus) in the part (b)) forms an isomorphism to a subset of the set \mathbb{S}_6 in the part (d)) under function composition \circ , i.e. $\exists S_6 \subseteq \mathbb{S}_6$ such that $(\mathbb{Z}_6, \oplus) \cong (S_6, \circ)$. **hint:** use part (c)).
- f) The group $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ and $(\mathbb{Z}_6, +)$ forms an isomorphism under the bijection $f : \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_6$ where $f(a, b) \rightarrow (3a + 4b) \pmod{6}$.
- g) Consider whether the bijection in part (f)) is unique or not. Try to relate it with Chinese Remainder Theorem.
hint: under which conditions is this function a bijection?

4 Submission

Please submit a single and readable PDF file named **hw2_1234567.pdf** to ODTUClass, where 1234567 is a place holder for your student number. Please note that, in case of integrity or similarity investigation, we reserve our right to demand you to submit your corresponding TEX file **hw2_1234567.tex** as well.

Glossary

set is a degenerate mathematical structure for a collection of different things, e.g. numbers, or objects.

binary relation is associates elements of one set X , called the domain, with elements of another set, called the codomain Y . If $X = Y$, then it is called homogeneous or endorelation. Common types of endorelation includes orders, graphs, equivalences.

partial order is a binary relation on a set P , if and only if it is *reflexive*, *anti-symmetric*, and *transitive*. That is, for all a, b , and $c \in P = X = Y$,

- reflexivity, aRa
- anti-symmetry, $aRb \wedge bRa \Rightarrow a = b$
- transitivity, $aRb \wedge bRc \Rightarrow aRc$

total order is a partial order in which any two elements are comparable. That is, for a binary relation R satisfying partial ordering properties, it also satisfies the following

- connectedness, $\forall a, b \in P, aRb \vee bRa$

congruence is a binary relation \sim on a set P if and only if it is *reflexive*, *symmetric*, and *transitive*. That is, for all a, b , and $c \in P = X = Y$,

- reflexivity, $a \sim a$.
- symmetry, $a \sim b \Leftrightarrow b \sim a$.
- transitivity, $a \sim b \wedge b \sim c \Rightarrow a \sim c$

function is a binary relation f that satisfies *functional* or *right-unique* property. That is for all $a, \in X$, and $b, c \in Y$,

- right-unique, $afb \wedge afc \Rightarrow b = c$

therefore it can also be denoted as $f(x) = y$, i.e, a mapping $f(\cdot) : X \rightarrow Y$ from a set X to another set Y .

injection is an one-to-one function; i.e, a mapping preserving distinctness.

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2, \text{ where } x_1, x_2 \in X, f(\cdot) : X \rightarrow Y$$

surjection is an onto function; i.e., reaches every point in the codomain. More simply, for every $y \in Y$, there exists an $x \in X$, such that $f(x) = y$.

bijection is an one-to-one and onto function; i.e, injection and surjection.

permutation is a bijection from a set S to itself, $f(\cdot) : S \rightarrow S$.

group is a non-empty set G with a binary operator \oplus , say (G, \oplus) , .e.g integers with addition operator.

- **closure:** $\forall a, b \in S$ we have $a \oplus b \in S$
- **associativity:** $\forall a, b, c \in S$ we have $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
- **identity:** $\exists e \in S, \forall a \in S$ we have $a \oplus e = e \oplus a = a$
- **inverse:** $\forall a \in S, \exists a^{-1} \in S$ we have $a \oplus a^{-1} = a^{-1} \oplus a = e$

morphism is a mapping that preserves group structure. That is, given two groups (G, \oplus) and (H, \otimes) , and a morphism $f : G \rightarrow H$,

$$f(g_1 \oplus g_2) = f(g_1) \otimes f(g_2), \text{ where } g_1, g_2 \in G$$

More simply, let $g_3 = g_1 \oplus g_2$ and $h_3 = h_1 \otimes h_2$. Let $f(\cdot) : G \rightarrow H$ be a function such that $h_1 = f(g_1)$ and $h_2 = f(g_2)$. f is a morphism if and only if $h_3 = f(g_3)$.

monomorphism is an injection (or, one-to-one) morphism.

epimorphism is a surjection (or, onto) morphism.

isomorphism is a bijection morphism; i.e., injection and surjection. Its inverse is also a morphism. ¹

endomorphism is a morphism from a group (G, \oplus) to itself; i.e, $f(\cdot) : G \rightarrow G$. ²

automorphism is a bijection endomorphism and hence an isomorphism from a group (G, \oplus) to itself.

³

¹In this case, the groups (G, \oplus) and (H, \otimes) are called isomorphic.

²In this case, f is called an endomorphism of G .

³In this case, f is called an automorphism of G , i.e. $f \in \text{Aut}(G)$