Student Information

Full Name : Alperen OVAK
Id Number : 2580801

Answer 1

(a)

Base Case ($m = 3$):

Assume $\mathbf{x_1}, \mathbf{x_2}, \mathbf{x_3}$ are three arbitrary points in the convex set $\mathcal{C}$. We want to show that any linear combination of these three points is also in $\mathcal{C}$.

Consider $\mathbf{x_1}, \mathbf{x_2}, \mathbf{x_3}$ and $\lambda_1, \lambda_2, \lambda_3$ such that $\mathbf{x_1} \geq 0$, $\mathbf{x_2} \geq 0$, $\mathbf{x_3} \geq 0$, $\lambda_1 \geq 0$, $\lambda_2 \geq 0$, $\lambda_3 \geq 0$, and $\mathbf{x_1} + \mathbf{x_2} + \mathbf{x_3} = 1$, $\lambda_1 + \lambda_2 + \lambda_3 = 1$. Now, consider the linear combination

$$\lambda_1\mathbf{x_1} + \lambda_2\mathbf{x_2} + \lambda_3\mathbf{x_3}.$$

Since $\lambda_1\mathbf{x_1} + (1-\lambda_1)\mathbf{x_2}$ is in $\mathcal{C}$ (as given in the premise), we can use the same reasoning for the pair $(\lambda_1\mathbf{x_1}+(1-\lambda_1)\mathbf{x_2})$ and $\mathbf{x_3}$. Therefore, the linear combination $\lambda_3(\lambda_1\mathbf{x_1}+(1-\lambda_1)\mathbf{x_2})+(1-\lambda_3)\mathbf{x_3}$ is also in $\mathcal{C}$.

Now, let's express this in terms of λ_i's:

$$\begin{aligned}
&\lambda_3(\lambda_1\mathbf{x_1} + (1-\lambda_1)\mathbf{x_2}) + (1-\lambda_3)\mathbf{x_3} \\
&= \lambda_3\lambda_1\mathbf{x_1} + \lambda_3(1-\lambda_1)\mathbf{x_2} + (1-\lambda_3)\mathbf{x_3}
\end{aligned}$$

Now, observe that $\lambda_3\lambda_1 + \lambda_3(1-\lambda_1) + (1-\lambda_3) = 1$, which satisfies $\sum_{i=1}^{3} \lambda_i = 1$.

Therefore, the base case $m = 3$ holds.

Inductive Step:

Assume that the statement holds for $m = k$, where k is some positive integer greater than 3. That is, for any set of k points $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}$ in $\mathcal{C}$ and coefficients $\lambda_1, \lambda_2, \ldots, \lambda_k$ satisfying $\mathbf{x_i} \geq 0$, $\lambda_i \geq 0$, and $\sum_{i=1}^{k} \lambda_i = 1$, the linear combination $\sum_{i=1}^{k} \lambda_i\mathbf{x_i}$ is in $\mathcal{C}$.

Now, we want to prove the statement for $m = k+1$. Consider $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}, \mathbf{x_{k+1}}$ as $k+1$ points in $\mathcal{C}$ and coefficients $\lambda_1, \lambda_2, \ldots, \lambda_k, \lambda_{k+1}$ such that $\mathbf{x_i} \geq 0$, $\lambda_i \geq 0$, and $\sum_{i=1}^{k+1} \lambda_i = 1$.

By the inductive assumption, the linear combination $\sum_{i=1}^{k} \lambda_i\mathbf{x_i}$ is in $\mathcal{C}$. Now, consider the convex combination of this result with $\mathbf{x_{k+1}}$ using the coefficients λ_{k+1}:

$$\lambda_{k+1}\left(\sum_{i=1}^{k} \lambda_i\mathbf{x_i}\right) + (\lambda_{k+1} - 1)\mathbf{x_{k+1}}.$$

Since $\mathcal{C}$ is convex, this convex combination is also in $\mathcal{C}$.

Therefore, by mathematical induction, the statement holds for all $m > 3$.

This completes the proof.

(b) counterexample to illustrate that the composition of convex functions is not always convex:

Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = x^2$, which is a convex function.

Let $g : \mathbb{R} \to \mathbb{R}$ be defined as $g(x) = x^2 - 1$, which is also convex.

Then we have $h = f \circ g$, where $h(x) = f(g(x))$ be defined as $h(x) = x^4 - 2x^2 + 1$.

Let's choose two points $\mathbf{x}_1 = -1$ and $\mathbf{x}_2 = 1$, and $\mathbf{t} = 0.3$ in the range $[0, 1]$.

$$h(0.3(-1) + (0.7)1) = h(0.4) = 0.7056$$
$$0.3h(-1) + (0.7)h(1) = 0$$
$$0.7056 > 0$$

Therefore $h(x) = x^4 - 2x^2 + 1$ is not convex, so we cannot say $f \circ g$ is convex if g and f are convex functions.

(c) Implication 1:
Assume $f()$ is a convex function. We should show that S is a convex set, and $g(t) = f(x + tv)$ is convex for all t such that $x + tv \in S$.

1. **Convexity of S:** Since $f()$ is defined on S, and $f()$ is convex, it implies that S must be a convex set. This is because the domain of a convex function is always convex.

2. **Convexity of $g(t) = f(x + tv)$:** Let $y_1 = x + t_1 v$ and $y_2 = x + t_2 v$ be two points in S where t_1, t_2 are such that $x + t_1 v, x + t_2 v \in S$.
Now, consider $z = \lambda y_1 + (1 - \lambda) y_2$, where λ is a convex combination coefficient $(0 \le \lambda \le 1)$.
$z = \lambda(x + t_1 v) + (1 - \lambda)(x + t_2 v)$ and $z = x + (\lambda t_1 + (1 - \lambda)t_2)v$.
Since S is convex, $x + (\lambda t_1 + (1 - \lambda)t_2)v \in S$, and by the convexity of $f()$, $g(t) = f(x + tv)$ is convex.

Therefore, the first implication holds.

Implication 2:
Assume S is a convex set, and $g(t) = f(x + tv)$ is convex for all t such that $x + tv \in S$. We want to show that $f()$ is a convex function.

To show that $f()$ is convex, we need to consider two arbitrary points x_1, x_2 in the domain of $f()$ and show that $f(\lambda x_1 + (1 - \lambda)x_2) \le \lambda f(x_1) + (1 - \lambda) f(x_2)$ for all λ in $[0, 1]$.

Consider x_1, x_2 in the domain of $f()$. Let λ be a convex combination coefficient $(0 \le \lambda \le 1)$. Now, consider $z = \lambda x_1 + (1 - \lambda)x_2$. Since S is convex, z is also in S. Therefore, we can use the convexity of $g(t) = f(x + tv)$ for t such that $x + tv = z$.

$$g(t) = f(x + tv) = f(\lambda x_1 + (1 - \lambda)x_2)$$

By the convexity of $g(t)$:

$$f(\lambda x_1 + (1-\lambda)x_2) \leq \lambda f(x_1) + (1-\lambda) f(x_2)$$

Therefore, the second implication holds.

Since both implications hold, we can conclude that a function $f()$ is convex if and only if S is a convex set, and the function $g(t) = f(x + tv)$ is convex for all t such that $x + tv \in S$.

Answer 2

(a)

(i) if X is uncountable The set of all $U \subseteq X$ is not a σ-algebra on X

Let's show a counterexample:

Let $X = \mathbb{R}$ and $U_1 = \mathbb{R} - \{1\}$.

Since $X - U_1 = \{1\}$ satisfies the condition U_1 must be in this set where $U \subseteq X$.

If this set is denoted by Σ, then from property (2) $X - U_1 = U_2$ must be in this set.

However, since $X - U_2 = \mathbb{R} - \{1\}$, which is infinite, U_2 cannot be in this set. This leads to a contradiction.

Therefore, if X is an uncountable infinite set, the set of all $U \subseteq X$ such that $X - U$ is either finite or is $\emptyset$ is **not** a σ-algebra on X.

(ii) if X is countable infinite The set of all $U \subseteq X$ is not a σ-algebra on X

Let's show a counterexample:

Let $X = \mathbb{Z}$ and $U_1 = \mathbb{Z} - \{1\}$.

Since $X - U_1 = \{1\}$ satisfies the condition U_1 must be in this set where $U \subseteq X$.

If this set is denoted by Σ, then from property (2) $X - U_1 = U_2$ must be in this set.

However, since $X - U_2 = \mathbb{Z} - \{1\}$, which is infinite, U_2 cannot be in this set. This leads to a contradiction.

Therefore, if X is an countable infinite set, the set of all $U \subseteq X$ such that $X - U$ is either finite or is $\emptyset$ is **not** a σ-algebra on X.

(iii) if X is finite

The set in question must contain the empty set $\emptyset$. This property is satisfied because $X - X = \emptyset$, and $\emptyset$ itself is also part of the set.

Since every U is finite where all $U \subseteq X$, $X - U$ is also finite and this satisfies the condiciton.

Therefore, if this set is denoted by Σ, then $X - U$ must be in this set.

Since $X - (X - U) = U$ is finite, this satisfies the condiciton.

Since each U where $U \subseteq X$ satisfies the condiciton, the set of all $U \subseteq X$ is $P(X)$.

Since $\Sigma \subseteq P(X)$, Therefore, if X is an uncountable infinite set, the set of all $U \subseteq X$ such that $X - U$ is either finite or is $\emptyset$ is a σ-algebra on X.

(b)

(i) if X is uncountable The set of all $U \subseteq X$ is not a σ-algebra on X

Let's show a counterexample:

Let $X = \mathbb{R}$ and $U_1 = \mathbb{R} - \{1\}$.

Since $X - U_1 = \{1\}$ satisfies the condition U_1 must be in this set where $U \subseteq X$.

If this set is denoted by Σ, then from property (2) $X - U_1 = U_2$ must be in this set.

However, since $X - U_2 = \mathbb{R} - \{1\}$, which is uncountable, U_2 cannot be in this set. This leads to a contradiction.

Therefore, if X is an uncountable infinite set, the set of all $U \subseteq X$ such that $X - U$ is either finite or is $\emptyset$ is **not** a σ-algebra on X.

(ii) if X is countable infinite

The set in question must contain X. This property is satisfied because $X - \emptyset = X$, and X itself is also part of the set.

Since every U is countable where $U \subseteq X$, $X - U$ is also uncountable and this satisfies the condiciton.

Therefore, if this set is denoted by Σ, then $X - U$ must be in this set.

Since $X - (X - U) = U$ is countable, this satisfies the condiciton.

Since each U where $U \subseteq X$ satisfies the condiciton, the set of all $U \subseteq X$ is $P(X)$.

Since $\Sigma \subseteq P(X)$, Therefore, if X is an countable infinite set, the set of all $U \subseteq X$ such that $X - U$ is either countable or is all of X is a σ-algebra on X.

(iii) if X is finite X is in Σ:
Since $X - X = \emptyset$ (the empty set) is finite, X is in Σ.
Σ is closed under complementation:
If U is in Σ, then $X - U$ is finite or all of X. The complement of U is $X - U$. If $X - U$ is finite, then U is in Σ. If $X - U$ is all of X, then U is also in Σ. Therefore, Σ is closed under complementation.
Σ is closed under finite unions:
Let $A_1, A_2, \ldots$ be sets in Σ. This means that for each A_i, $X - A_i$ is either finite or all of X.
Consider the union $A = A_1 \cup A_2 \cup \ldots$. The complement of A is

$$X - A = (X - A_1) \cap (X - A_2) \cap \ldots.$$

If for each i, $X - A_i$ is finite, then $X - A$ is also finite (finite union of finite sets is finite). If for each i, $X - A_i$ is all of X, then $X - A$ is also all of X.
Therefore, Σ is closed under finite unions.
Since the set Σ satisfies all three properties, it is a σ-algebra on the finite set X.

(c)

(i) if X is uncountable The set of all $U \subseteq X$ is not a σ-algebra on X

Let's show a counterexample:

Let $X = \mathbb{R}$ and $U_1 = \{1\}$.

Since $X - U_1 = \mathbb{R} - \{1\}$ satisfies the condition. U_1 must be in this set where $U \subseteq X$.

If this set is denoted by Σ, then from property (2) $X - U_1 = U_2$ must be in this set.

However, since $X - U_2 = \{1\}$, which is finite, U_2 cannot be in this set. This leads to a contradiction.

Therefore, if X is an uncountable infinite set, the set of all $U \subseteq X$ such that $X - U$ is infinite or $\emptyset$ or X is **not** a σ-algebra on X.

(ii) if X is countable infinite The set of all $U \subseteq X$ is not a σ-algebra on X

Let's show a counterexample:

Let $X = \mathbb{Z}$ and $U_1 = \{1\}$.

Since $X - U_1 = \mathbb{Z} - \{1\}$ satisfies the condition. U_1 must be in this set where $U \subseteq X$.

If this set is denoted by Σ, then from property (2) $X - U_1 = U_2$ must be in this set.

However, since $X - U_2 = \{1\}$, which is finite, U_2 cannot be in this set. This leads to a contradiction.

Therefore, if X is an countable infinite set, the set of all $U \subseteq X$ such that $X - U$ is infinite or $\emptyset$ or X is **not** a σ-algebra on X.

(iii) if X is finite

1. X is in Σ:

In this case, X itself is in the set because $X - X = \emptyset$ is in the set. So, the first property is satisfied.

2. Σ is closed under complementation:

If A is in Σ, then $X - A$ is infinite or $\emptyset$ or X. Let's consider each case:

- If A is finite where $A \neq X$ and $A \neq \emptyset$, then $X - A$ is also finite, which is not in the set.
- If A is $\emptyset$, then $X - A$ is X, which is in the set.
- If A is X, then $X - A$ is $\emptyset$, which is in the set.

So, the set is closed under complementation.

3. Σ is closed under countable unions:

Let $A_1, A_2, \ldots$ be sets in Σ. We want to show that their union,

$$A = A_1 \cup A_2 \cup \ldots,$$

is also in Σ.

- Since we have only two elements in this set, which is $\emptyset$ and X, then $A = X \cup \emptyset = X$ is also in the set.

Since all three properties are satisfied, the given set is a σ-algebra on the finite set X.

Answer 3

(a) **Suppose** $ax \equiv b \pmod{p}$ **has a solution.**
This implies that there exists an integer x such that $ax - b = p \cdot q$ for some integer q.
Take $d = \gcd(a, p)$. We have:

$$a = a \cdot t + p \cdot r$$

where t and r are integers.
Since $d = \gcd(a, p)$, it follows that d divides both a and p. Therefore, we can express a and n as:

$$a = d \cdot q_1 \quad \text{where} \quad q_1 \in \mathbb{Z}$$

$$p = d \cdot q_2 \quad \text{where} \quad q_2 \in \mathbb{Z}$$

Lastly, from the earlier expression $ax - b = p \cdot q$, we can substitute a and n using the above expressions:

$$b = a \cdot x - p \cdot q = (d \cdot q_1) \cdot x - (d \cdot q_2) \cdot q = d \cdot (q_1 \cdot x - q_2 \cdot q)$$

Let $c = q_1 \cdot x - q_2 \cdot q$, then $b = d \cdot c$.
Thus, $d = \gcd(a, p)$ divides b, indicating that if there is a solution to $ax \equiv b \pmod{n}$, then $d = \gcd(a, p)$ divides b.

Suppose $d = \gcd(a, p)$ **and** $d \mid b$**.**
Then we have

$$\begin{cases} d = a \cdot t + p \cdot r, \quad t, r \in \mathbb{Z} \\ d \mid b \end{cases}$$

From these equations, it follows that

$$b = d \cdot c = (a \cdot t + p \cdot r) \cdot c = atc + prc \implies b - a \cdot (tc) = p \cdot (rc) \implies a \cdot (tc) = b \pmod{p}$$

This implies that $ax \equiv b \pmod{p}$ has a solution, where $x = t \cdot c$.

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

(b) To prove that the pair of congruences has a solution for x under the given conditions, we will use Bézout's identity.

Let $d = \gcd(p_1, p_2) = 1$ (since $\gcd(p_1, p_2) = 1$).

By Bézout's identity, there exist integers s and t such that $sp_1 + tp_2 = 1$.

Now, consider the system of congruences:

1. $a_1 x \equiv b_1 \pmod{p_1}$
2. $a_2 x \equiv b_2 \pmod{p_2}$

We want to find a solution x that satisfies both congruences.

Let's define $x_0 = t \cdot p_2$ (Note that x_0 is a solution to the second congruence since $a_2 x_0 = a_2(t \cdot p_2) \equiv b_2 \pmod{p_2}$).

Now, let's consider the first congruence with this value of x_0:

$$a_1 x_0 = a_1(t \cdot p_2) \equiv b_1 \pmod{p_1}$$

Since $sp_1 + tp_2 = 1$, we can multiply the entire congruence by s (which is congruent to 1 modulo p_1):

$$a_1(t \cdot p_2) \cdot s \equiv b_1 \cdot s \pmod{p_1}$$

This simplifies to:

$$a_1(t \cdot p_2 \cdot s) \equiv b_1 \cdot s \pmod{p_1}$$

Since $t \cdot p_2 \cdot s$ is congruent to 1 modulo p_1, we have:

$$a_1 \cdot 1 \equiv b_1 \cdot s \pmod{p_1}$$

This implies that $a_1 \equiv b_1 \cdot s \pmod{p_1}$. Since s is an integer, $b_1 \cdot s$ is divisible by $\gcd(a_1, p_1)$.

Therefore, $a_1 \equiv b_1 \cdot s \pmod{p_1}$ implies that $a_1 x_0 \equiv b_1 \pmod{p_1}$, and x_0 is a solution to the first congruence as well.

So, $x = x_0$ is a solution to the pair of congruences.

(c) **Given:** We consider the system of congruences:

$$a_j x \equiv b_j \pmod{p_j}$$

where $(a_j, p_j) = 1$ for all j.

Claim (1): There always exists a solution for

$$a_j x \equiv b_j \pmod{p_j}$$

regardless of the choice of b_j.

Proof: Let C_j be a solution for $a_j x \equiv b_j \pmod{p_j}$ for $j = 1, 2, ..., k$. Since $(a_j, p_j) = 1$, we have $[p_1, p_2, ..., p_k] = \Pi$, where Π is the product of all p_j since they are coprime. Consider m_j such that $m_j \Pi \equiv 1 \pmod{p_j}$ [Equation (2)]. This gives a unique solution $x \equiv m'_j \pmod{p_j}$.

Considering

$$x_0 = c_1 m_1 m_1' + c_2 m_2 m_2' + ... + c_k m_k m_k',$$

where c_j is a chosen solution for $a_j x \equiv b_j \pmod{p_j}$ [Equation (1)], we can show that x_0 is a common solution to the system.

For $i \neq j$, p_i divides $m_j = p_1 p_2 ... p_k p_j$. Therefore,

$$a_j x_0 \equiv \sum_{i=1}^{k} a_i c_i m_i m_i' \equiv a_j c_j m_j m_j' \equiv a_j c_j \pmod{p_j}$$

Since $m_j m_j' \equiv 1 \pmod{p_j}$, we have $a_j x_0 \equiv a_j c_j \equiv b_j \pmod{p_j}$. Thus, x_0 is a common solution for $j = 1, 2, ..., k$.

Claim (2): If x is another solution to the system of congruences, then

$$x \equiv x_0 \pmod{[p_1, p_2, ..., p_k]}$$

.

Proof: Let x be another solution. This implies

$$x_0 \equiv c_j \equiv x \pmod{p_j}$$

for all $j = 1, 2, ..., k$. Thus, $x_0 - x$ is a common multiple of $p_1, p_2, ..., p_k$, and hence a multiple of $[p_1, p_2, ..., p_k] = \Pi$. Therefore,

$$x \equiv x_0 \pmod{[\Pi]}$$

.

Answer 4

(a) Let's denote this set by X^ω. Then we will show that a function $g : \mathbb{Z}^+ \to X^\omega$ cannot be surjective to prove the uncountability of this set.

Let's denote this set by X^ω. We will show that a function $g : \mathbb{Z}^+ \to X^\omega$ cannot be surjective to prove the uncountability of this set.

For a function g defined as $g(n) = (x_{n1}, x_{n2}, \ldots, x_{nn}, \ldots)$ where each x_{ij} belongs to the set $X = \{a, b, \ldots, z\}$, consider the element $y = (y_1, y_2, \ldots) \in X^\omega$ given by:

$$y_n = \begin{cases} a & \text{if } x_{nn} \neq a \\ b & \text{if } x_{nn} = a \end{cases}$$

In other words, y is constructed such that it differs from each $g(n)$ by at least one coordinate. This means that y is not mapped to by g, and therefore, g cannot be surjective.

This argument generalizes to any countable product of a set X with $|X| > 1$. If X has $|X| = k$ elements, then there are $k^{\mathbb{N}}$ distinct sequences in the countable product X^ω, making it uncountable.

(b) Let $Y = \bigcup_{i \in \mathbb{N}} Y_i$.
The sets Y_i are infinitely countable; therefore, there exist surjective functions $f_i : \mathbb{N} \to Y_i$.
By Cantor's first diagonal argument, it is known that $\mathbb{N} \times \mathbb{N}$ is countable.
So let's define:

$$F : \mathbb{N} \times \mathbb{N} \to Y$$

$$(i, x) \mapsto f_i(x)$$

Per the definition of the union, this mapping is surjective.
So, Y is indeed countable.