CENG 223

Discrete Computational Structures

Fall 2023 - Take Home Exam 2 Solutions

Sets and Functions

Question 1 - Answer

a) Assume that the set C $\in \mathbb{R}^n$ is a convex set. For arbitrary m, show that

$$\sum_{i=1}^{m} \lambda_i x_i = C$$

where $x_i \in C$ and $\lambda_i \in \mathbb{R}$, $i = 1, 2, \ldots, m$ satisfying $\lambda_i \geq 0$ and $\sum\limits_{i=1}^{m} \lambda_i = 1$.

By definition of set convexity, $\forall x_1, x_2 \in C$, $\lambda \in [0, 1]$, $\lambda x_1 + (1 - \lambda)x_2 \in C$.

Then we can prove by induction. Let, $p(n) = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$ where $i = 1, \ldots, n$; $\lambda_i \in [0, 1]$ and $x_i \in C$ satisfying $\sum\limits_{i=1}^{n} \lambda_i = 1$.

Since $p(1) = x_1 \in C$ is trivial and $p(2) = \lambda_1 x_1 + \lambda_2 x_2 = \lambda_1 x_1 + (1 - \lambda_1)x_2 \in C$ by set convexity, let's assume that $p(k) \in C$ where $i = 1, \ldots, k$; $\lambda_i \in [0, 1]$ and $x_i \in C$ satisfying $\sum\limits_{i=1}^{k} \lambda_i = 1$.

Since $p(k) \in C$, we can pick an element $x_{k+1} \in C$ and state $(1 - \alpha)p(k) + \alpha x_{k+1} \in C$, by set convexity. Let's expand the statement below,

$$(1 - \alpha)(\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_k x_k) + \alpha x_{k+1} = (1 - \alpha)\sum_{i=1}^{k} \lambda_i x_i + \alpha x_{k+1} \in C$$

Let's rewrite $\alpha = \lambda^*_{k+1}$ such that $\lambda_i = \lambda^*_i/(1 - \alpha) = \lambda^*_i/(1 - \lambda^*_{k+1})$ satisfying $\sum\limits_{i=1}^{k+1} \lambda^*_i = \sum\limits_{i=1}^{k}(1 - \lambda^*_{k+1})\lambda_i + \lambda^*_{k+1} = (1 - \lambda^*_{k+1}) + \lambda^*_{k+1} = 1$ where $i = 1, \ldots, k$ and $\alpha = \lambda^*_{k+1} \in (0, 1)$. Therefore the statement is also equal to,

$$(1 - \lambda^*_{k+1})\sum_{i=1}^{k} \frac{\lambda^*_i}{(1 - \lambda^*_{k+1})} x_i + \lambda^*_{k+1} x_{k+1} = \sum_{i=1}^{k} \lambda^*_i x_i + \lambda^*_{k+1} x_{k+1} = p(k + 1) \in C$$

Since λ values for $p(k)$ are arbitrary satisfying just $\lambda_i \in [0, 1]$ and $\sum\limits_{i=1}^{k} \lambda_i = 1$, for $p(k + 1)$ we can consider that λ^*_i values from $p(k)$ are λ_i values from $p(k + 1)$.

Therefore, by induction, the statement is true for any arbitrary m by $p(2) \Rightarrow \cdots \Rightarrow p(k) \Rightarrow p(k + 1) \Rightarrow \cdots \Rightarrow p(m)$.

b) No, counterexample is any non-increasing convex $f : \mathbb{R} \to \mathbb{R}$ and any convex $g : \mathbb{R} \to \mathbb{R}$ functions. For example, The composition of $f(x) = -x$ and $g(x) = x^2$ is $f \circ g(x) = -x^2$ is not a convex function.

The convexity of $f(x)$ is entailed by the following equality

$$\begin{aligned} \forall x_1, x_2 \in \mathbb{R}, \lambda \in [0,1] \quad : \quad f(\lambda x_1 + (1-\lambda)x_2) &= -(\lambda x_1 + (1-\lambda)x_2) \\ &= \lambda(-x_1) + (1-\lambda)(-x_2) = \lambda f(x_1) + (1-\lambda) f(x_2) \\ &\therefore f(\lambda x_1 + (1-\lambda)x_2) \leq (\lambda f(x_1) + (1-\lambda) f(x_2)) \end{aligned}$$

Similarly, The convexity of $g(x)$ is entailed by the left hand side from the right hand side of the convexity inequality

$$\begin{aligned} \forall x_1, x_2 \in \mathbb{R}, \lambda \in [0,1] \quad : \quad & g(\lambda x_1 + (1-\lambda)x_2) - (\lambda g(x_1) + (1-\lambda) g(x_2)) \\ &= (\lambda x_1 + (1-\lambda)x_2)^2 - (\lambda x_1^2 + (1-\lambda x_2^2)) \\ &= \lambda^2 x_1^2 + 2\lambda(1-\lambda)x_1x_2 + (1-\lambda)^2 x_2^2 - \lambda x_1^2 - (1-\lambda)x_2^2 \\ &= (\lambda^2 - \lambda)x_1^2 + 2\lambda(1-\lambda)x_1x_2 + ((1-\lambda)^2 - (1-\lambda))x_2^2 \\ &= (\lambda^2 - \lambda)x_1^2 - 2(\lambda^2 - \lambda)x_1x_2 + (\lambda^2 - \lambda)x_2^2 \\ &= (\lambda^2 - \lambda)(x_1 - x_2)^2 \leq 0 \\ &\therefore g(\lambda x_1 + (1-\lambda)x_2) \leq (\lambda g(x_1) + (1-\lambda) g(x_2)) \end{aligned}$$

However, let $x_1 = 1$, $x_2 = -1$, $\lambda = 0.5$. Then we have the followings

- $h(\lambda x_1 + (1-\lambda)x_2) = h(0.5 - 0.5) = h(0) = 0$
- $\lambda h(x_1) + (1-\lambda)h(x_2) = 0.5h(1) + 0.5h(-1) = -0.5 - 0.5 = -1.$

Thus, $h(\lambda x_1 + (1-\lambda)x_2) = 0 \nleq -1 = \lambda h(x_1) + (1-\lambda)h(x_2)$. Therefore, we have a witness stating that $h(x)$ is not convex.

c) ($\Rightarrow$) Assume that f(x) is convex, then by definition of convexity, S is convex too.

$$\begin{gathered} \forall y, z \in \text{dom(g)} \quad x + yv, x + zv \in S \\ \forall t \in [0,1] \quad t(x+yv) + (1-t)(x+zv) = x + (ty + (1-t)z)v \in S \quad \text{(by convexity of S)} \end{gathered}$$

$\implies ty + (1-t)z \in \text{dom(g)} \implies$ dom(g) is convex. Lastly,

$$\begin{aligned} g(ty + (1-t)z) &= f(x + (ty + (1-t)z)v) \\ &= f(t(x+yv) + (1-t)(x+zv)) \\ &\leq tf(x+yv) + (1-t)f(x+zv) \\ &= tg(y) + (1-t)g(z) \end{aligned}$$

$\implies$ g(x) is convex.

($\Leftarrow$) Assume that f is not conxex and S is convex. Then,

$$\exists x, y \in S, \exists t \in [0,1] \quad f(ty + (1-t)x) > tf(y) + (1-t)f(x)$$

Put $v = y - x$,

$$\begin{aligned} g(t) &= f(x + t(y-x)) \\ &= f(ty + (1-t)x) \\ &> tf(y) + (1-t)f(x) \\ &= tg(1) + (1-t)g(0) \end{aligned}$$

$\implies$ g(x) is not convex.

Question 2 - Answer

Considering the subsets of X under mild assumptions and their consequential propositions,

a) $\Sigma = \{ \ U \subseteq X : U^c$ is either finite or empty set $\} = \{ \ U \subseteq X : U^c$ is finite $\} \cup \{ \ X \ \}$.

(*) $X \in \Sigma$ is trivially satisfied for every choice of X.

(*) Assume X is finite or empty, i.e. bijective to $\mathbb{Z}_n$. Every subset $U^c \subseteq X$ has a finite or empty complementary set $(U^c)^c = U$ by Proposition 1 and Lemma 1. Thus, $\forall U^c \subseteq X.(x \in \Sigma) \Rightarrow (\Sigma = P(X))$. Therefore, Σ is a σ-algebra by Corrolary 2.

(*) Assume X is countably infinite, i.e. bijective to $\mathbb{Z}^+$. Every finite subsets $U^c \subseteq X$, has an countably infinite complement $(U^c)^c = U \in \Sigma$, by Proposition 3. Therefore, Σ includes only countably infinite subsets U whose complement U^c is a finite set.
However, Σ is **not** a σ-algebra, considering such a countably infinite set $U \subseteq X$, whose complement U^c is a finite set U^c as we assumed. Thus $U \in \Sigma$ but $U^c \notin \Sigma$ since $(U^c)^c = U$ is not finite.

(*) Assume X is uncountable, i.e. not bijective to $\mathbb{Z}$. Every finite subsets $U^c \subseteq X$ has an uncountable complementary subset $(U^c)^c = U$ by Proposition 4. However, considering such an uncountable subset $U \subseteq X$, whose complement U^c is a finite set U^c as we assumed. Thus $U \in \Sigma$ but $U^c \notin \Sigma$ since $(U^c)^c = U$ is not finite. Therefore, Σ is **not** a σ-algebra.

b) $\Sigma = \{ \ U \subseteq X : U^c$ is either countable or X $\} = \{ \ U \subseteq X : U^c$ is countable $\} \cup \{ \ \emptyset \ \}$.

(*) $X \in \Sigma$ since $X^c = \emptyset$ is countable. [1]

(*) Assume X is finite, i.e. bijective to $\mathbb{Z}_n$. Every subset $U \subseteq X$ has a countable complementary set U^c by Proposition 1 and Lemma 1. Thus, $\forall U^c \subseteq X.(x \in \Sigma) \Rightarrow (\Sigma = P(X))$. Therefore, Σ is a σ-algebra by Corrolary 2.

(*) Assume X is countably infinite, i.e. bijective to $\mathbb{Z}^+$. Every subset $U \subseteq X$ has a countable complementary set U^c by Propositions 2 and 3.
Thus, $\forall U^c \subseteq X.(x \in \Sigma) \Rightarrow (\Sigma = P(X))$. Therefore, Σ is a σ-algebra by Corrolary 2.

(*) Assume X is uncountable, i.e. not bijective to $\mathbb{Z}$. Every countable subset $U^c \subseteq X$ has an uncountable complementary set $(U^c)^c = U$ by Proposition 4. However, considering an uncountable subset $U \subseteq X$, whose complement U^c is countable U^c as we assumed. Thus $U \in \Sigma$ but $U^c \notin \Sigma$ since $(U^c)^c = U$ is countable. Therefore, Σ is **not** a σ-algebra.

c) $\Sigma = \{ \ U \subseteq X : U^c$ is uncountable or $\emptyset$ or X $\} = \{ \ U \subseteq X : U^c$ is uncountable $\} \cup \{ \ \emptyset, X \ \}$.

(*) $X \in \Sigma$ and $\emptyset \in \Sigma$ by definition.

(*) Assume X is finite, i.e. bijective to $\mathbb{Z}_n$. Since every subset U and the related complement U^c is finite, there is no uncountable subset of X, thus $\{ \ U \subseteq X : U^c$ is uncountable $\} = \emptyset$ and $\Sigma = \{ \ \emptyset, X \ \}$. Therefore, Σ is a trivial σ-algebra by Corrollary 1.

[1] However, stating that Σ is not a sigma algebra (unless $X = \emptyset$) because $\emptyset$ is not countably infinite is acceptable.

(*) Assume X is countably infinite, i.e. bijective to $\mathbb{Z}^+$. Since every subset $U^c \subseteq X$ is countable, $\Sigma = \{\ \emptyset,\ X\ \}$, by Proposition 2. Therefore, Σ is a trivial σ-algebra by Corrollary 1.

(*) Assume X is uncountable, i.e. not bijective to $\mathbb{Z}$. Every countable subsets $U^c \subseteq X$, has an uncountable complement $(U^c)^c = U \in \Sigma$, by Proposition 4. However, Σ is **not** a σ-algebra, considering such an uncountable subset $U \subseteq X$, whose complement U^c is a countable set as we assumed. Thus $U \in \Sigma$ but $U^c \notin \Sigma$ since $(U^c)^c = U$ is not uncountable.

Question 3 - Answer

a) ($\Rightarrow$) Assume $ax \equiv b$ (mod p) has a solution. Then,

$$ax - b = pq, \exists q \in \mathbb{Z} \tag{1}$$

Take $d = \gcd(a, p)$ We have, by Bezout's Identity,

$$d = at + pr, \quad \exists t, r \in \mathbb{Z} \tag{2}$$

$$\begin{aligned}
\text{Since } d = \gcd(a,p) &\implies d|a \wedge d|p \\
&\implies a = dq_1 \wedge p = dq_2, \quad \exists q_1, q_2 \in \mathbb{Z} \\
\text{from (1) we have} \quad b &= ax - pq = (dq_1)x - (dq_2)q \\
&= d(q_1 x - q_2 q) = dc, \exists c \in \mathbb{Z} \implies d|b
\end{aligned}$$

($\Leftarrow$) Assume $d = \gcd(a, p)$ and $d|b$. Then we have again Bezout's Identity (2).

$$\begin{aligned}
b = dc = (at + pr)c &= atc + nrc \\
\implies b - a(tc) &= p(rc) \\
\implies a(tc) &\equiv b \text{ (mod } p) \\
\implies ax &\equiv b \text{ (mod } p) \text{ has a solution when } x = tc
\end{aligned}$$

b) The method to find a solution for the pair of two congruences below will take the following approach: first, write $x = b_1 + kp_1$. Plug that in to the second equation to obtain $kn_1 \equiv b_2 - b_1$ (mod p_2).

$$\begin{aligned}
x &\equiv b_1 \text{ (mod } p_1) \\
x &\equiv b_2 \text{ (mod } p_2)
\end{aligned}$$

If p_1 and p_2 share factors, then we may not be able to solve this equivalence, by the assumption in part (a). Hence, we can demand that p_1 and p_2 are relatively prime, and this should solve that problem

c) For each i with $1 \leq i \leq k$, put $m_i = \frac{\Pi}{p_i}$. Notice that since the moduli are relatively prime, and m_i is the product of all the moduli other than ni, we have that $p_i \perp m_i$, and hence $m_i i$ has a multiplicative inverse modulo p_i, say y_i. Moreover, note that m_i is a multiple of n_j for all $j \neq i$

Put $x = y_1 b_1 m_1 + y_2 b_2 m_2 + \cdots + y_k b_k m_k$.

Notice that for each i with $1 \leq i \leq k$, we obtain

$$\begin{aligned}
x &\equiv y_1 b_1 m_1 + y_2 b_2 m_2 + \cdots + y_k b_k m_k (\text{mod } p_i) \quad \text{(Since we put x it so)} \\
&\equiv y_i b_i m_i (\text{mod } p_i) \quad (\text{since each } m_j \text{ with } j \neq i \text{ is a multiple of } p_i) \\
&\equiv b_i (\text{mod } p_i) \quad (\text{since } y_i \text{ is an inverse to } m_i \text{ modulo } p_i).
\end{aligned}$$

Therefore, we have that $x \equiv b_i \pmod{p_i}$ for all $1 \leq i \leq k$. Finally, we wish to show uniqueness of the solution (mod Π). Suppose that x and y both solve the congruences. Then we have that for each i, p_i is a divisor of $x - y$. Since the p_i are relatively prime, this means that Π is a divisor of $x - y$, and hence $x - y$ are congruent modulo Π.

Question 4 - Answer

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.

For a such defined function g, we have $g(p) = (x_{n1}, x_{n2}, \ldots, x_{nn}, \ldots)$ where each x_{ij} are either 0 or 1. Then we consider $y = (y_1, y_2, \ldots) \in X^\omega$ given by

$$y_n = \begin{cases} 0 & \text{if } x_{nn} = 1 \\ 1 & \text{if } x_{nn} = 0\,. \end{cases}$$

Such defined y is not mapped to by g: it differs from each $g(p)$ by at least one coordinate. Hence g cannot be surjective. Hence, the uncountability of X^ω.

b) The question basically asks whether the countable union of countable sets is countable. By being countable, each Y_i admits a surjective function $f_i : \mathbb{Z}^+ \to Y_i$. Then we can define a function $g : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \bigcup_{i \in \mathbb{Z}^+} Y_i$ such that $g(i,j) = f_i(j)$. With this, we have defined a surjective function from $\mathbb{Z}^+ \times \mathbb{Z}^+$ which has the same cardinality with $\mathbb{Z}$ (no need to prove this, as stated in the note). Thus, the given set is countable.

Extra Proofs

Definition 1. *The subset of the domain of the mapping f to A is $Sub(f|A) = \{x \in dom(f) : f(x) \in A\}$.*

Definition 2. *The graph of a mapping $f : A \to B$ is $G(f) = \{(x, y) \in A \times B : f(x) = y\}$.*

Proposition 1. *Let X be a finite or empty set. Every subset $U \subseteq X$ is either a finite or an empty set.*

Proof. (see also finite-measure) Since X is a finite or an empty set, there is a bijection $f_X : \mathbb{Z}_n \to X$ (or an injection $g : X \to \mathbb{Z}_n$). The restriction of the g's domain to U, $g|U$: $\mathbb{Z}_n \to U$, defined by $g|U(u) = g(u)$ for every $u \in U$, is an injection since if $u_1, u_2 \in U$, then $g|U(u_1) = g|U(u_2) \Rightarrow g(u_1) = g(u_2) \Rightarrow u_1 = u_2$.

Lastly, setting the co-domain of $g|U$ into $Sub(g|U)$ defines a bijection $f_U : Sub(f_X|U) \to U$ by definition 1. Since $Sub(f_X|U) \subseteq \mathbb{Z}_n \subset \mathbb{Z}^+$, by definition, an arbitrary subset $U \subseteq X$ is finite.

□

Lemma 1. *Let X be a finite or empty set. The complementary sets of any subset $U^c = X - U \subseteq X$, entailed by proposition 1.*

Proposition 2. *Let X be a countably infinite set. Every subset $U \subseteq X$ is countable.*

Proof. Let X be a countably infinite set. Then, there exists a bijection $f : X \to \mathbb{Z}$. Assume there exists an uncountable subset $U \subseteq X$. Thus, there exists no bijection from U to any subset of $\mathbb{Z}$, i.e. $g : U \to \mathbb{Z}_n$ cannot be bijective. However, considering $f|U : U \to \mathbb{Z}$, where $f|U(x) = f(x)$ for every $x \in U$, is an injection since f is a bijection. Moreover, setting the co-domain of $f|U$ into $Sub(f|U)$ defines a bijection $h : U \to Sub(f|U)$. Therefore, this is a contradiction.

$\square$

Proposition 3. *Let X be a countably infinite set. Every finite subset U, has a countably infinite complementary set $U^c = X - U$.*

Proof. Considering the proof for Proposition 2, Assume $U \subseteq X$ is a finite set and its complement U^c isn't countably infinite, i.e. finite. Therefore, there are two bijections $f : U \to \mathbb{Z}_n$ and $g : U^c \to \mathbb{Z}_m$ as a logical consequence of their finiteness. We can define a bijection $h : U \cup U^c \to \mathbb{Z}_{m+n}$, where

$$h(x) = \begin{cases} f(x) & \text{if } x \in U \\ g(x) + n & \text{if } x \notin U. \end{cases}$$

Therefore, $h : X \to \mathbb{Z}_{m+n}$ implies that X is a finite set, which is a contradiction. $\square$

Proposition 4. *Let X be a continuum. Every finite or countable subset $U \in X$ has an uncountable complement $U^c = X - U$.*

Proof. Let X be a continuum. Assume that there exists a finite set $U \subseteq X$, whose the complement U^c isn't uncountable, i.e. U^c is countable. Therefore, there exists a bijection $f : U \to \mathbb{Z}_n$ and $g : U^c \to \mathbb{Z}^+$. Thus, we can construct a bijection $h : U \cup U^c \to \mathbb{Z}^+$, where

$$h(x) = \begin{cases} f(x) & \text{if } x \in U \\ g(x) + n & \text{if } x \notin U = x \in U^c. \end{cases}$$

Since, $h : X \to \mathbb{Z}^+$ is a bijection, X is countable, which is a contradiction. Therefore there exists no finite set $U \subseteq X$, whose subset U^c is countable.

$\square$

Proposition 5. *Let $P(X)$ be the power set of X. Then $\forall U_i \in P(X) : n = 1, 2, \dots : \bigcup_{n \in \mathbb{Z}^+} U_n \in P(X)$.*

Proof. Let $\{U_n\}_{n \in \mathbb{Z}^+}$ be a countable infinite sequence of sets in $P(X)$.

Consider an element of the union of all the sets in this $\{U_n\}_{n \in \mathbb{Z}^+}$:

$$x \bigcup_{n \in \mathbb{N}} U_n$$

By definition of union, $\exists n \in \mathbb{N} : x \in U_n$.

But $U_n \in P(X)$ and so by definition $U_n \subseteq X$. By definition of subset, it follows that $x \in X$.

Hence, again by definition of subset:

$$\bigcup_{n \in \mathbb{N}} U_n \subseteq X$$

Finally, by definition of power set:

$$\bigcup_{n \in \mathbb{N}} U_n \in P(X)$$

.

Thus, The power set is closed under countable unions. $\square$

Corollary 1. *The set $\Sigma = \{ \emptyset, X \}$ is (minimal or* ***trivial****)* σ*-**algebra**. see separable sigma-algebras.*

Proof. We have the following properties satisfied:

- $X \in \Sigma$ by definition.
- $X^c = \emptyset \in \Sigma$ and $\emptyset^c = X \in \Sigma$ by definition.
- $\emptyset \cup \emptyset = \emptyset$ and $\emptyset \cup X = X \cup \emptyset = X \cup X = X$ by idempotemcy and commutativity of union. Thus, $\forall U_i = X, \emptyset : \bigcup_{i \in \mathbb{Z}^+} U_i \in \Sigma$

So, by definition, $\{ \emptyset, X \}$ is a σ-algebra. $\square$

Corollary 2. *The power set of X is a σ-algebra is (****discrete****)* σ*-**algebra**.*

Proof. see power-set sigma-algebras.

We have the following properties satisfied:

- $X \in P(X) = \Sigma$ by definition of power set.
- $\forall U \subseteq X : U^c = X - U \subseteq X$, implies $U^c \in P(X) = \Sigma$ by definition of power set.
- $\forall U_n \in P(X) : n = 1, 2, \dots : \bigcup\limits_{n \in \mathbb{N}} U_n \in P(X)$ by Proposition 5.

So, by definition, $P(X)$ is a σ-algebra. $\square$