Tutorial - 1

(equivalence relation, induction)

IIT Kharagpur

5th January 2023

Question 1

Prove that any equivalence relation R on a set A, partitions A into disjoint equivalence classes

Question 1

Prove that any equivalence relation R on a set A partitions A into disjoint equivalence classes

Hint: Need to prove: $A1 \cup A2 \cup A3 \cup ... = A$ where Ai is an equivalence class

Question 1

Prove that any equivalence relation R on a set A partitions A into disjoint equivalence classes

Hint: Remember the definition of equality of sets

Question 1: Solution

Suppose R is an equivalence relation on any non-empty set A. Denote the equivalence classes as $A1, A2, A3, \ldots$.

First we will show $\mathbf{A1 \cup A2 \cup A3 \cup \ldots \subseteq A}$.

If $x \in A1 \cup A2 \cup A3 \cup \ldots$, then x belongs to at least one equivalence class, Ai by definition of union.

And by the definition of equivalence class, $x \in A$. Thus $A1 \cup A2 \cup A3 \cup \ldots \subseteq A$.

Question 1: Solution

Suppose R is an equivalence relation on any non-empty set A. Denote the equivalence classes as $A1, A2, A3,...$.

Next we show **$A \subseteq A1 \cup A2 \cup A3 \cup ...$.**

If $x \in A$, then xRx since R is reflexive. Thus $x \in [x]$.

$[x]=Ai$, for some i since $[x]$ is an equivalence class of R . So, $A \subseteq A1 \cup A2 \cup A3 \cup ...$ by definition of subset.

And so, $A1 \cup A2 \cup A3 \cup ... = A$, by the definition of equality of sets.

Question 1: Solution

Now, from the Fundamental Theorem on Equivalence Relations for any i,j ,

either **$A_i=A_j$ or $A_i \cap A_j = \varnothing$**

Proof: Let's have $[a] \cap [b] \neq \varnothing$

$\exists x (x \in [a] \wedge x \in [b])$ by definition of empty set & intersection.

xRa and xRb by definition of equivalence classes. Also since xRa, aRx by symmetry.

We have aRx and xRb, so **aRb** by transitivity.

Now, we need to prove if aRb then, [a]=[b]

Question 1: Solution

First we will show $[a] \subseteq [b]$.

Let $x \in [a]$, then xRa by definition of equivalence class. Now we have xRa and aRb,

thus xRb by transitivity (since R is an equivalence relation). Since $xRb, x \in [b]$, by definition of equivalence classes.

We have shown if $x \in [a]$ then $x \in [b]$, thus $[a] \subseteq [b]$, by definition of subset.

Next we will show $[b] \subseteq [a]$.

Let $x \in [b]$, then xRb by definition of equivalence class. Since aRb , we also have bRa, by symmetry.

Now we have xRb and bRa, thus xRa by transitivity. Since $xRa, x \in [a]$, by definition of equivalence classes.

We have shown if $x \in [b]$ then $x \in [a]$, thus $[b] \subseteq [a]$, by definition of subset.

Therefore, **$Ai \cap Aj = \varnothing$ or $Ai = Aj$ is true**

Hence, $\{A1, A2, A3, ...\}$ is mutually disjoint

Question 2

Prove that the relation $a \equiv b \pmod{m}$, is an equivalence relation on the set of integers, where m is a positive integer

Question 2

Prove that the relation $a \equiv b \pmod{m}$, is an equivalence relation on the set of integers, where m is a positive integer

Hint: Remember three properties of equivalence relation

Question 2

Prove that the relation $a \equiv b \pmod{m}$, is an equivalence relation on the set of integers, where m is a positive integer

Hint: If $a \equiv b \pmod{m}$, then $a - b = k \cdot m$

Question 2: Solution

Reflexive: If a is an arbitrary integer, then $a - a = 0 = 0 \cdot m$. Thus $a \equiv a \pmod{m}$.

Symmetric: If $a \equiv b \pmod{m}$, then $a - b = k \cdot m$ for some integer k. Thus, $b - a = (-k) \cdot m$ is also divisible by m, and so $b \equiv a \pmod{m}$.

Transitive: Suppose $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then $a - b = k \cdot m$ and $b - c = l \cdot m$ for some integers k and l. Then $a - c = (a - b) + (b - c) = k \cdot m + l \cdot m = (k + l)m$ is also divisible by m. That is, $a \equiv c \pmod{m}$.

Question 3

What are the equivalence classes for the congruence relation:

1. $a \equiv b \pmod{3}$?
2. $a \equiv b \pmod{5}$?

Question 3

What are the equivalence classes for the congruence relation:

1. $a \equiv b \pmod 3$?
2. $a \equiv b \pmod 5$?

Hint: Think what could be the equivalence classes of each element

Question 3

What are the equivalence classes for the congruence relation:

1. $a \equiv b \pmod{3}$?
2. $a \equiv b \pmod{5}$?

Hint: $[m + r] = [q.m + r]$; q is an integer and $0 \leq r < m$

Question 3: Solution

Let, $a \equiv b \pmod 3$

$[0] = \{.., -3, 0, 3, 6,...\}$

$[1] = \{.., -2, 1, 4, 7,...\}$

$[2] = \{.., -1, 2, 5, 8,...\}$

$[3] = \{.., 0, 3, 6, 9....\}$

$\Rightarrow [0] = [3] = [6] = [3.q + 0]$

$\Rightarrow [1] = [4] = [7] = [3.q + 1]$

$\Rightarrow [2] = [5] = [8] = [3.q + 2]$

=> Equivalence classes can be represented as $[3.q + r]$ where $0 \leq r < 3$

Question 4

A palindrome can be defined as a string that reads the same forward and backward, or by the following definition.

(a) ϵ is a palindrome.

(b) If a is any symbol, then the string a is a palindrome.

(c) If a is any symbol and x is a palindrome, then axa is a palindrome.

(d) Nothing is a palindrome unless it follows from (a) through (c).

Prove by induction that the two definitions are equivalent.

Question 4

A palindrome can be defined as a string that reads the same forward and backward, or by the following definition.

(a) ϵ is a palindrome.

(b) If a is any symbol, then the string a is a palindrome.

(c) If a is any symbol and x is a palindrome, then axa is a palindrome.

(d) Nothing is a palindrome unless it follows from (a) through (c).

Prove by induction that the two definitions are equivalent.

Hint 1-

Consider the mentioned one (*def1)* as in the question and the usual one (*def2)* as two equivalent definitions and try to prove by induction on string length.

Question 4

A palindrome can be defined as a string that reads the same forward and backward, or by the following definition.

(a) ϵ is a palindrome.

(b) If a is any symbol, then the string a is a palindrome.

(c) If a is any symbol and x is a palindrome, then axa is a palindrome.

(d) Nothing is a palindrome unless it follows from (a) through (c).

Prove by induction that the two definitions are equivalent.

Hint 2-

Base cases:

- For ϵ , it is part of *def1* (clause 1) while it trivially satisfies *def2*.
- Similar argument holds for strings of unit length (clause 2 in def1).
- For length 2 palindromes, they satisfy *def1* being of the type aa with $x = \epsilon$ (clause 3). Strings of type aa also satisfy *def2* being the same symbol repeated twice.
- Now let us assume both the definitions to be equivalent up to strings of length n > 2 in Σ^*.

Question 4

Solution:

- Base cases: As per Hint2
- Induction step:

Consider a string σ with $|\sigma| = n + 1$ which is a palindrome as per *def2* that implies $\sigma = \sigma^R$ (applying def2). Hence it must be the case that σ starts and ends with the same symbol.

Hence $\exists \sigma' \in \Sigma^*, a \in \Sigma$ such that $\sigma = a\sigma' a$. Also, $\sigma = \sigma^R \Rightarrow a\sigma' a = (a\sigma' a)^R \Rightarrow a\sigma' a = a{\sigma'}^R a \Rightarrow \sigma' = {\sigma'}^R$

Thus σ' is a palindrome as per def2. Since $|\sigma| = n - 1$ and def1, def2 are equivalent for string length up to n, we have σ' as palindrome also for def1. Now, applying clause 3 of def1, we have $\sigma = a\sigma' a$ as palindrome (as per def1).

Consider a string σ with $|\sigma| = n + 1$ which is a palindrome as per def1. Since $n > 2$, we must have a palindrome x such that $|x| = n - 1$ and $axa = \sigma$ for some symbol a.

x should satisfy def2 and hence $x = x^R$. So, $\sigma^R = (axa)^R = ax^R a = axa = \sigma$. This σ is also palindrome as per def2.

Question 5

Prove that for any strings $u, v \in \Sigma^*$, $(uv)^R = v^R u^R$

Question 5

Prove that for any strings $u, v \in \Sigma^*$, $(uv)^R = v^R u^R$

Hint 1:

Try to prove by induction on $|u|$

Question 5

Prove that for any strings $u, v \in \Sigma^*$, $(uv)^R = v^R u^R$

Hint 2:

Base case:

Let u be an arbitrary string of length 0. $u = \epsilon$ since there is only one such string. Then

$$(uv)^R = (\epsilon v)^R = v^R = v^R \epsilon = v^R \epsilon^R = v^R u^R$$

Question 5

Prove that for any strings $u, v \in \Sigma^*$, $(uv)^R = v^R u^R$

Hint 3:

Induction hypothesis:

$\forall n \geq 0$, for any string u of length n:

For all strings $v \in \Sigma^*$, $(uv)^R = v^R u^R$. Now solve for u.

Question 5

Prove that for any strings $u, v \in \Sigma^*$, $(uv)^R = v^R u^R$

Solution:

Induction steps (after solving Hint 1 and Hint 2) :

Let u be an arbitrary string of length $n > 0$. Assume inductive hypothesis holds for all strings w of length $< n$. Since $|u| = n > 0$ and we have $u = ay$ for some string y with $|y| < n$ and $a \in \Sigma$. Then

$$(uv)^R = ((ay)v)^R = (a(yv))^R = (yv)^R a^R = (v^R y^R) a^R = v^R (ay)^R$$
$$= v^R u^R$$

*This works because while applying the first reversal i.e. (a(yv))^R=(yv)^Ra^R, the first element a is of size 1 and the second element is yv, which is fine as we assume no condition on length of second argument in the induction hypothesis.