RELATIONS

a relation between A and B is a subset of the cartesian product $A \times B$ $(R / \rho / r)$

$R \subseteq A \times B$

$(x, y) \in R \rightarrow {}_xR_y \quad / \quad {}_x\rho_y$

$(x, y) \notin R \rightarrow {}_x(\sim R)_y$ (x is NOT related to y in R)

ex $R = \{(x, y) \in I \times I : x > y\}$ $\quad 7 R 5$

ex $R = \{(x, y) \in N \times N : x = 3y\}$ $\quad 15 R 5, \; 18 R 6, \; 27 R 9$

INVERSE RELATION

$R^{-1} = \{(y, x) : y \in B, \; x \in A, \; (x, y) \in R\}$

$(x, y) \in R \iff (y, x) \in R^{-1}$

ex $A = \{1, 2\} \quad B = \{2, 3\}$
$R = \{(1, 2), (2, 3)\}$

$R^{-1} = \{(2, 1), (3, 2)\}$

th if R be a relation from A to B, then the domain of R is the range of R^{-1} and the range of R is the domain of R^{-1}.

th if R be a relation from A → B, then $(R^{-1})^{-1} = R$

REFLEXIVE RELATION

$R \subseteq A \times A$ and $(a,a) \in R \ \forall \ a \in A$ (for all)

aRa holds for all $a \in A$

ex $R = \{(a,a), (a,c), (b,b), (c,c), (d,d)\}$ (reflexive).
$A = \{a, b, c, d\}$

ex $A = \{a, b, c, d\}$
$S = \{(a,a), (a,c), (b,c), (b,d), (c,d)\}$
not reflexive as $(b,b), (c,c), (d,d) \notin S$

SYMMETRIC RELATION

$R \subseteq A \times A$ and $(a,b) \in R \Rightarrow (b,a) \in R \ \forall \ a,b \in A$

$aRb \Rightarrow bRa$ for every $a,b \in A$

ex $R = \{(x,y) \in N \times N : x$ is a divisor of $y\}$ (not symmetric)

ex $R = \{(x,y) \in N \times N : x+y = 5\}$ (symmetric)

th for a symmetric relation,
$R^{-1} = R$

RTP (i) $R \subseteq R^{-1}$ (ii) $R^{-1} \subseteq R$

(i) $(x, y) \in R$ let
$\Rightarrow (y, x) \in R$ as R is symmetric
$\Rightarrow (x, y) \in R^{-1}$ by definition
thus, $R \subseteq R^{-1}$

(ii) $(x, y) \in R^{-1}$ let
$\Rightarrow (y, x) \in (R^{-1})^{-1} = R$ by definition
$\Rightarrow (x, y) \in R$ as R is symmetric
thus, $R^{-1} \subseteq R$

ANTI SYMMETRIC RELATION

$R \subseteq A \times A$ and aRb and $bRa \Rightarrow a = b \quad \forall a, b \in A$

ex $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x \leq y\}$ (anti symmetric)

xRy and yRx
$\Rightarrow x \leq y \quad y \leq x$
$\Rightarrow x = y$

TRANSITIVE RELATION

$R \subseteq A \times A$ and $aRb, bRc \Rightarrow aRc \quad \forall a,b,c \in A$

ex $R = \{(x,y) \in \mathbb{N} \times \mathbb{N} : x < y\}$ (transitive)

xRy and yRz
$\Rightarrow x < y \quad y < z$
$\Rightarrow x < z$

EQUIVALENCE RELATION

$R \subseteq A \times A$ and R is reflexive, symmetric, transitive

aRa $\quad aRb \Rightarrow bRa$ $\quad aRb, bRc \Rightarrow aRc$

ex a relation ρ is defined on the set $\mathbb{Z}$ (set of all integers) by $a \rho b$ iff $(2a+3b)$ is divisible by 5. prove or disprove: ρ is an equivalence relation.

(i) reflexive $a \rho a \; \forall \; a \in \mathbb{Z}$

$(2a+3a) = 5a$ is divisible by 5.
$\therefore (a,a) \in \rho \quad \forall a \in \mathbb{Z}$ (reflexive).

(ii) symmetric $a \rho b \Rightarrow b \rho a \quad \forall a, b \in \mathbb{Z}$

$2a + 3b = 5n$

$$2a = 5n - 3b$$

$$a = \frac{5n-3b}{2}$$

$$3a + 2b = 3\left(\frac{5n-3b}{2}\right) + 2b$$

$$= \frac{15n-9b}{2} + 2b$$

$$= \frac{15n-5b}{2}$$

Since $3a + 2b \in \mathbb{Z}$

$\Rightarrow \frac{15n-5b}{2} \in \mathbb{Z}$

$\Rightarrow 15n + 5b \; 5\left(\frac{3n-b}{2}\right)$ is divisible by 5.

$\therefore (a,b) \in R \Rightarrow (b,a) \in R \quad \forall a,b \in \mathbb{Z}$

(iii) transitive $aRb, bRc \Rightarrow aRc$

$3a + 2b = 5n \quad \Rightarrow a = \frac{5n-3b}{2}$

$3b + 2c = 5m \quad \Rightarrow c = \frac{5m-3b}{2}$

$$3a + 2c = 3 \times \frac{5n - 2b}{3} + 2 \times \frac{5m - 3b}{2}$$

$$= 5n - 2b + 5m - 3b$$

$$= 5n + 5m - 5b \quad \text{is divisible by 5.}$$

$\therefore (a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R \quad \forall a, b, c \in \mathbb{Z}$

alternative solution (pdf):

claim1: let $a \in \mathbb{Z}$

then $2a + 3a = 5a$ (divisible by 5)

hence aRa holds $\forall a \in \mathbb{Z}$

$\Rightarrow \rho$ is reflexive.

claim2:

lemma: if $a (\neq 0)$ divides b $(a|b)$, $a, b \in \mathbb{Z}$

then $\exists\ x \in \mathbb{Z}$ such that $b = ax$

($\exists$: there exists)

lemma: if p be prime and $a, b \in \mathbb{Z}$ then $p|a$ or $p|b$.

let $a, b \in \mathbb{Z}$

assume that aRb holds.

then, $(2a + 3b)$ is divisible by 5.

by euclid's division algorithm, we have

$2a + 3b = 5k_1$ for some $k_1 \in \mathbb{Z}$

$\Rightarrow 2(2a + 3b) = 10k_1$

$\Rightarrow 4a + 6b = 10k_1$

$\Rightarrow 3(2b + 3a) - 5a = 10k_1$

$\Rightarrow 3(2b + 3a) = 5(a + 2k_1) = 5k_2$, say $k_2 \in \mathbb{Z}$

$5 \mid 3(2b + 3a) \Rightarrow 5 \mid (2b + 3a)$

$\Rightarrow b f a$ holds. f is symmetric.

Claim 3: Let $a f b$ and $b f c$ hold. for every $a, b, c \in \mathbb{Z}$

then, $(2a + 3b)$ is divisible by 5

$\Rightarrow 2a + 3b = 5l_1$ for some $l_1 \in \mathbb{Z}$

$(2b + 3c)$ is divisible by 5

$\Rightarrow 2b + 3c = 5l_2$ for some $l_2 \in \mathbb{Z}$

Now, $2(2a + 3b) - 3(2b + 3c) = 10l_1 - 15l_2$

$\Rightarrow 4a - 9c = 10l_1 - 15l_2$

$\Rightarrow 2(2a + 3c) = 10l_1 - 15l_2 + 15c$

$= 5(2l_1 - 3l_2 + 3c) = 5l_3$ say

$\Rightarrow 5 \mid 2(2a + 3c) \Rightarrow 5 \mid (2a + 3c)$

$\Rightarrow a f c$ holds. f is transitive.

Since f is reflexive, symmetric and transitive, so f is an equivalence relation.

PARTIAL ORDER RELATION

$R \subseteq A \times A$ and R is reflexive, antisymmetric, transitive

aRa $\quad aRb, bRa \Rightarrow a=b$ $\quad aRb, bRc \Rightarrow aR$

ex a relation R is defined on the set $\mathbb{N}$ by aRb iff a divides b.

$R = \{(a,b) \in \mathbb{N} \times \mathbb{N} : a|b\}$

prove or disprove: R is a partial order relation.

(i) $aRa \quad \forall a \in \mathbb{N}$

$a|a \Rightarrow aRa$ holds. R is reflexive.

(ii) $aRb, bRa \Rightarrow a=b \quad a,b \in \mathbb{N}$

$a|b$ and $b|a \Rightarrow a=b$. R is anti-symmetric.

(iii) $aRb, bRc \Rightarrow aRc$

$a|b, b|c \Rightarrow a|c$, R is transitive.

∴ R is a partial order relation.

ex $R \subseteq \mathbb{Z} \times \mathbb{Z}^+$ $(a,b) R (c,d)$ iff $ad = bc \quad \forall a,b,c,d \in \mathbb{Z}$

prove or disprove: R is a partial-order relation.

(i) ~~$aRa, \forall a \in a$~~ $(a,b) R (a,b) \quad \forall a,b \in \mathbb{Z}$

$\frac{a}{b} = \frac{a}{b} \Rightarrow (a,b) R (a,b)$ holds. R is ~~sym~~ reflexive.

(ii) $(a,b)\,R\,(c,d)$, $(c,d)\,R\,(a,b) \Rightarrow (a,b) = (c,d)$

$\frac{a}{b} = \frac{c}{d}$, $\frac{c}{d} = \frac{a}{b}$?? what.

R is anti-symmetric.

(iii) $(a,b)\,R\,(c,a)$, $(c,d)\,R\,(e,b) \Rightarrow (a,b)\,R\,(e,f)$

$\frac{a}{b} = \frac{c}{d}$ $\frac{c}{a} = \frac{e}{b} \Rightarrow \frac{a}{b} = \frac{e}{b}$

R is transitive.

∴ R is a partial order relation.

PARTIAL ORDER SET (POSET)

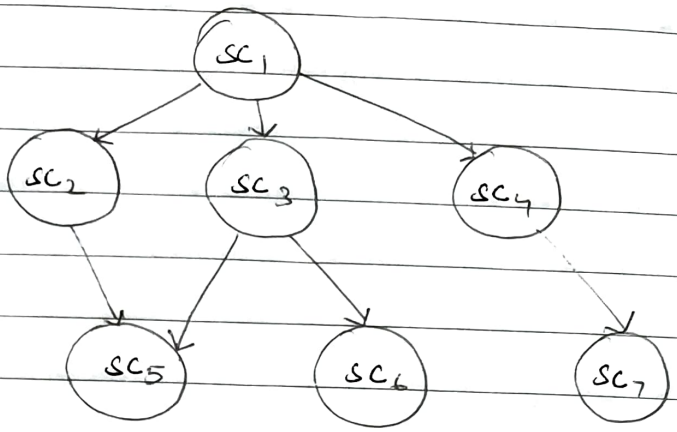
a non-empty set in which partial order relation is defined.

A PRACTICAL APPLICATION OF POSET:
HIERARCHICAL ACCESS CONTROL

User hierarchy consists of n disjoint security classes $SC_1, SC_2, \ldots SC_n$.
$SC = \{SC_1, SC_2, \ldots SC_n\}$

a relation $\geq$ is defined on SC (security clearance)
$\geq$ is a partial order relation on poset SC.

an encrypted message is only decrypted by the sender class as well as all its predecessor security classes.



a trusted central authority (CA) distributes keys to each security class in the hierarchy such that any predecessor can easily derive its successor's secret key.

EQUIVALENCE CLASSES

A = set , R = equivalence relation

$a \in A \quad x \in A$

$x \in A$ such that $x R a \subseteq A$

called equivalence class of a in A wrt R.

$\therefore A_a \;/\; [a] \;/\; d(a) \;/\; \bar{a}$

$= \{ x \mid_x R_a , x \in A \}$

set of inputs that results in a.

$a \in [a]$

$b \in [a] \Rightarrow [b] = [a]$

$[a] = [b] \Leftrightarrow (a, b) \in R$

$[a] = [b] \;/\; [a] \cap [b] = \phi$

ex Let A be the set of triangles in a plane. Let R be a relation in A defined by "x is similar to y", where $x, y \in A$. Verify whether R is an equivalence relation if so, find the equivalence classes.

(i) reflexive ✓ (ii) symmetric ✓ (iii) transitive ✓.
R is an equivalence relation.

$R = \{(x,y) \mid x, y \in A,\ x \text{ is similar to } y\}$

let $a \in A$ be an arbitrary Δ in the plane.

$[a] = \{x \mid x \in A \text{ and } xRa\}$
$= \{x \mid x \in A \text{ and } x \text{ is similar to } a\}$
is an equivalence class of $a \in A$.

ex $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : (x-y) \text{ is divisible by } m\}$

$R = \{(x,y) \mid x, y \in \mathbb{Z},\ m \mid (x-y)\}$

Verify whether R is an equivalence relation.
if so, equivalence classes.

(i) reflexive ✓ (ii) symmetric ✓ (iii) transitive ✓
R is an equivalence relation.

$[a] = \{x \mid x \in \mathbb{Z},\ (x-a) \text{ is divisible by } m\}$

PARTITIONS

collection of non-empty disjoint subsets of set S whose union is S.

if $A_1, A_2, \ldots A_n$ = nonempty subsets of S
then partition of S $P = \{A_1, A_2, \ldots A_n\}$, if

① $A_1 \cup A_2 \cup A \ldots A_n = S$

② $A_i \cap A_j = \phi$ or $A_i = A_j \ \forall \ i = 1 \ldots n$

ex $S = \{1, 2, 3, \ldots 22\}$
$A = \{1, 4, 7, \ldots 22\}$
$B = \{2, 5, 8, \ldots 20\}$
$C = \{3, 6, 9, \ldots 21\}$

$A \cup B \cup C = S$
$A \cap B = A \cap C = B \cap C = \phi$

$\therefore P = \{A, B, C\}$ forms a partition of S.

FUNDAMENTAL THEORM ON EQUIVALENCE RELATIONS

th an equivalence relation R in a non-empty set A partitions A, and conversely, a partition of A defines an equivalence relation.

COMPATIBILITY RELATION

relation that is both reflexive & symmetric.

aRa $\quad aRb \Rightarrow bRa$

ex: Let A be a set of people

$R = \{(a, b) \mid a, b \in A,\ a \text{ is a friend of } b\}$

(i) reflexive ✓ (ii) symmetric ✓

R is a compatibility relation.

all equivalence relations are compatibility relations.

R, S = compatibility relations on set A

$R \cap S$ = compatibility relation

$R \cup S$ = may or may not be compatibility relation.

CLOSURE OF RELATIONS

relation R' is a reflexive closure of R iff,

(a) R' is reflexive

(b) $R \subseteq R'$

(c) if $R \subseteq R''$ and R'' is reflexive

then $R' \subseteq R''$

i.e., R' is the smallest relation that satisfies (a) and (b)

denoted by $r(R)$

ex: $A = \{a, b, c\}$

$R = \{(a, b), (b, a), (b, b), (c, b)\}$

compute reflexive closure $r(R)$ of R.

R is not reflexive since, $(a,a), (c,c) \notin R$

$R' = R \cup \{(a,a), (c,c)\}$

$= \{(a,a), (a,b), (b,a), (b,b), (c,b), (c,c)\}$

R' is reflexive & $R \subseteq R'$.

furthermore, any other relation R'' containing R must also contain (a,a) and (c,c); otherwise it will not be reflexive.

& $R' \subseteq R''$.

as R' contains R, and R' is reflexive, and is contained in every reflexive relation that contains R, so R' is the smallest relation that satisfies (a) and (b).

hence, $r(R) = R'$.

SYMMETRIC CLOSURE

a relation R' is the symmetric closure of relation R iff:

(a) R' is symmetric

(b) $R \subseteq R'$

(c) for any relation R'', if $R \subseteq R''$ and R'' is symmetric, then $R' \subseteq R''$, i.e., R' is the smallest relation that satisfies conditions (a) and (b).

denoted by $s(R)$.

ex $A = \{a, b, c\}$

$R = \{(a,a), (a,b), (c,c), (b,c), (b,a), (a,c)\}$

R is not symmetric. since $(c,b), (c,a) \notin R$

$R' = R \cup \{(c,b), (c,a)\}$

$= \{(a,a), (a,b), (a,c), (b,a), (b,c), (c,a), (c,b), (c,c)\}$

Clearly R' is symmetric and $R \subseteq R'$

furthermore any other relation R'' containing R must also contain $(c,b), (c,a)$ otherwise it will not be symmetric. so $R' \subseteq R''$. so, R' is the smallest relation satisfying conditions (a) and (b).

hence, $s(R) = R'$.

TRANSITIVE CLOSURE

a relation R' is the transitive closure of relation R iff:

(a) R' is transitive

(b) $R \subseteq R'$

(c) for any relation R'', if $R \subseteq R''$ and R'' is transitive, then $R' \subseteq R''$, i.e., R' is the smallest relation that satisfies the conditions (a) and (b)

denoted by $t(R)$

ex let R be the (<) relation on $\mathbb{Z}$. compute $t(R)$.

the transitive closure of the less than (<) relation on $\mathbb{Z}$ is the less than (<) relation itself.

$R^t = R \cup \{(a,b) \in R^t \wedge (b,c) \in R^t \Rightarrow (a,c) \in R^t\}$

ex $A = \{1, 2, 3\}$

$R = \{(1,1), (1,2), (1,3), (2,3), (3,1)\}$ R^t?

R is not transitive, since $(3,2), (3,3) \notin R$

$R' = R \cup \{(3,2), (3,3)\}$

$= \{(1,1), (1,2), (1,3), (2,3), (3,1), (3,2), (3,3)\}$

but it is not transitive yet. it still need $(2,1)$, $(2,2)$

$\therefore R' = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}$.

$R^t = t(R) =$ ↑