Discrete Mathematics and Algorithms (CSE611)

Dr. Ashok Kumar Das

Assistant Professor
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad
Gachibowli 500 032, Hyderabad, India

E-mail: *ashok.das@iiit.ac.in*
Homepage: http://www.iiit.ac.in/people/faculty/ashokkdas
Personal Homepage: https://sites.google.com/site/iitkgpakdas/

August 6, 2012

RELATIONS

Definition

- A relation between two sets A and B is a subset of the cartesian product $A \times B$ and is defined by R (or ρ or r).
  $R \subseteq A \times B$.
- We write ${}_xR_y$ or ${}_x\rho_y$ if and only if (iff) $(x, y) \in R$ (or ρ).
- We also write ${}_x(\sim R)_y$ when x is NOT related to y in R.

Examples

- **Example.** Consider the relation $R = \{(x, y) \in I \times I : x > y\}$, where I is the set of all integers.
  Clearly, $R \subseteq I \times I$ and R is a relation in I.
  We write ${}_7R_5$ as $(7, 5) \in I \times I$ and $7 > 5$.
- **Example.** Consider the relation $R = \{(x, y) \in N \times N : x = 3y\}$, where N is the set of natural numbers.
  Clearly, $R \subseteq N \times N$ and R is a relation on the set N.
  We write ${}_{15}R_5$, ${}_{18}R_6$, and ${}_{27}R_9$.

Inverse Relation

- If R be the relation from A to B, then the inverse relation of R is the relation from B to A and is denoted and defined by
  $R^{-1} = \{(y, x) : y \in B, x \in A, (x, y) \in R\}$.
  $\Longrightarrow (x, y) \in R \Leftrightarrow (y, x) \in R^{-1}$
- **Example.** If $A = \{1, 2\}$, $B = \{2, 3\}$ and R be the relation from A to B, $R = \{(1, 2), (2, 3)\}$, then $R^{-1} = \{(2, 1), (3, 2)\}$.

Theorem

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}.

Theorem

If R be a relation from A to B, then $(R^{-1})^{-1} = R$.

Reflexive relation

- Let A be a set and R the relation defined in it (i.e., $R \subseteq A \times A$). R is said to be *reflexive*, if $(a, a) \in R, \forall a \in A$
  $\implies {}_aR_a$ holds for every $a \in A$.
- **Example.** Consider the relation
  $R = \{(a, a), (a, c), (b, b), (c, c), (d, d)\}$ in the set $A = \{a, b, c, d)\}$.
  Then R is reflexive, since $(x, x) \in R, \forall x \in A$, that is, ${}_xR_x$ holds for every $x \in A$.
- **Example.** Consider the relation
  $S = \{(a, a), (a, c), (b, c), (b, d), (c, d)\}$ in the set $A = \{a, b, c, d)\}$.
  Verfify whether S is reflexive.

Symmetric relation

- Let A be a set and R the relation defined in it (i.e., $R \subseteq A \times A$). R is said to be *symmetric*, if $(a, b) \in R \Rightarrow (b, a) \in R, \forall a, b \in A$
  In other words, ${}_aR_b \Rightarrow {}_bR_a$ for every $a, b \in A$.
- **Example.** Let N be the set of natural numbers and R the relation defined in it such that ${}_xR_y$ if x is a divisor of y (that is, $x|y$), $x, y \in N$.
  Then R is NOT symmetric, since ${}_xR_y \not\Rightarrow {}_yR_x, \forall x, y \in N$.
  For example, ${}_3R_9 \not\Rightarrow {}_9 R_3$.
- **Example.** Consider the relation S in the set of natural numbers N as $R = \{(x, y) \in N \times N : x + y = 5\}$. Verfify whether S is symmetric.

Theorem

For a symmetric relation R, $R^{-1} = R$.

Proof.

Required to prove (RTP) (i) $R \subseteq R^{-1}$, and (ii) $R^{-1} \subseteq R$.
(i) Let $(x, y) \in R$.
Then $(x, y) \in R \Rightarrow (y, x) \in R$, since R is symmetric
$\Rightarrow (x, y) \in R^{-1}$, by definition of R^{-1}
Thus, $R \subseteq R^{-1}$.
(ii) Let $(x, y) \in R^{-1}$.
Then $(y, x) \in (R^{-1})^{-1} = R$, by definition of R^{-1}
$\Rightarrow (x, y) \in R$, since R is symmetric
Thus, $R^{-1} \subseteq R$.

$\square$

Anti-symmetric relation

- Let A be a set and R the relation defined in it (i.e., $R \subseteq A \times A$). R is said to be *anti-symmetric*, if ${}_aR_b$ and ${}_bR_a \Rightarrow a = b$, for every $a, b \in A$.
- **Example.** Let A be the set of real numbers and R the relation defined in it such that ${}_xR_y$ if $x \leq y$, that is, $R = \{(x, y) \in A \times A : x \leq y\}$.
  Then R is anti-symmetric, since
  ${}_xR_y$ and ${}_yR_x$
  $\Rightarrow x \leq y$ and $y \leq x$
  $\Rightarrow x = y$.

Transitive relation

- Let A be a set and R the relation defined in it (i.e., $R \subseteq A \times A$). R is said to be *transitive*, if ${}_aR_b$ and ${}_bR_c \Rightarrow {}_aR_c$, $\forall a, b, c \in A$.
- **Example.** Let N be the set of natural numbers and R the relation defined in it such that ${}_xR_y$ if $x < y$, that is,
  $R = \{(x, y) \in N \times N : x < y\}$.
  Then R is transitive, since
  ${}_xR_y$ and ${}_yR_z$
  $\Rightarrow x < y$ and $y < z$
  $\Rightarrow x < z$
  $\Rightarrow {}_xR_z$.

Equivalence relation

- Let A be a set and R the relation defined in it (i.e., $R \subseteq A \times A$). R is said to be an *equivalence* relation, if and only if
  1. R is reflexive, that is, ${}_aR_a$ holds, for every $a \in A$.
  2. R is symmetric, that is, ${}_aR_b \Rightarrow {}_bR_a$, $\forall a, b \in A$.
  3. R is transitive, that is, ${}_aR_b$ and ${}_bR_c \Rightarrow {}_aR_c$, $\forall a, b, c \in A$.

Problem: A relation ρ is defined on the set Z (set of all integers) by ${}_a\rho_b$ if and only if $(2a + 3b)$ is divisible by 5. Prove or disprove: ρ is an equivalence relation.

- Claim 1: Let $a \in Z$. Then, $2a + 3a = 5a$ is divisible by 5.
  Hence, ${}_a\rho_a$ holds, $\forall a \in Z$.
  $\Rightarrow \rho$ is ***reflexive***.
- Claim 2: **Lemma:** If $a(\neq 0)$ divides b (i.e., $a|b$), $a, b \in Z$ being integers, then $\exists\ x \in Z$ such that $b = ax$.
  Lemma: If p be prime and a, b are integers such that $p|ab$, then either $p|a$ or $p|b$.

Problem (Continued...)

- Let $a, b \in Z$. Assume that ${}_a\rho_b$ holds. Then, $(2a + 3b)$ is divisible by 5. By the Euclid's division algorithm, we have,
  $2a + 3b = 5k_1$, for some integer $k_1 \in Z$.
  $\Rightarrow 2(2a + 3b) = 10k_1$
  $\Rightarrow 4a + 6b = 10k_1$
  $\Rightarrow 3(2b + 3a) - 5a = 10k_1$
  $\Rightarrow 3(2b + 3a) = 5(a + 2k_1) = 5k_2$, say, where $k_2 = (a + 2k_1)$ is an integer
  If p is prime and $p|ab$, then either $p|a$ or $p|b$. Thus, $5|(2b + 3a) \Rightarrow {}_b\rho_a$ holds. Hence, ρ is ***symmetric***.

Problem (Continued...)

- Claim 3: Let ${}_a\rho_b$ and ${}_b\rho_c$ hold, for every $a, b, c \in Z$. Then $(2a + 3b)$ is divisible by 5
  $\Rightarrow 2a + 3b = 5l_1$, for some $l_1 \in Z$, and
  $(2b + 3c)$ is divisible by 5
  $\Rightarrow 2b + 3c = 5l_2$, for some $l_2 \in Z$.
  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,
  where $l_3 = 2l_1 - 3l_2 + 3c \in Z$
  $\Rightarrow 5|(2a + 3c)$
  $\Rightarrow_a \rho_c$ holds and ρ is also ***transitive***.
  Since ρ is reflexive, symmetric and transitive, so ρ is an equivalence relation.

Partial-order relation

- Let S be a non-empty set and R the relation defined in it (i.e., $R \subseteq S \times S$). R is said to be an *partial-order* relation, if and only if it satisfies the following three conditions:
  1. R is reflexive, that is, ${}_aR_a$ holds, for every $a \in S$.
  2. R is anti-symmetric, that is, ${}_aR_b$ and ${}_bR_a \Rightarrow a = b, \forall a, b \in S$.
  3. R is transitive, that is, ${}_aR_b$ and ${}_bR_c \Rightarrow {}_aR_c, \forall a, b, c \in S$.

Problem: A relation R is defined on the set N (set of natural numbers) by ${}_aR_b$ if and only if a divides b, that is, $R = \{(a, b) \in N \times N : a|b\}$. Prove or disprove: R is a partial-order relation.

- Claim 1: Verify whether R is ***reflexive***. (Yes/No)
- Claim 2: Verify whether R is ***anti-symmetric***. (Yes/No)
- Claim 3: Verify whether R is ***transitive***. (Yes/No)

Problem: Z be the set of all integers. Define a relation R on the set $Z \times Z$ by $_{(a,b)}R_{(c,d)}$ if and only if $ad = bc$, $\forall a, b, c, d \in Z$. Prove or disprove: R is a partial-order relation.

- Claim 1: Verify whether R is ***reflexive***. (Yes/No)
- Claim 2: Verify whether R is ***anti-symmetric***. (Yes/No)
- Claim 3: Verify whether R is ***transitive***. (Yes/No)

Partial-Order Set (POSET)

- A non-empty set in which the partial-order relation is defined, is called the partial-order set (poset/POSET).
- Example: In the above example, the set N is POSET under which partial-order relation R is defined.

A Practical Application of POSET: Hierarchical Access Control

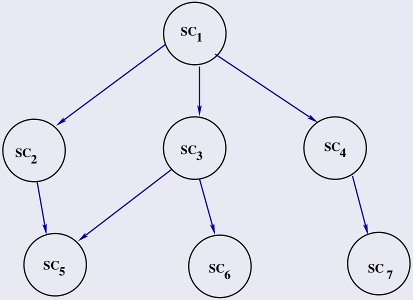
- Hierarchical access control is an important research area in computer science, which has numerous applications including schools, military, governments, corporations, database management systems, computer network systems, e-medicine systems, etc.
- In a hierarchical access control, a user of higher security level class has the ability to access information items (such as message, data, files, etc.) of other users of lower security classes.
- A user hierarchy consists of a number n of disjoint security classes, say, SC_1, SC_2, ..., SC_n. Let this set be $SC = \{SC_1, SC_2, \ldots, SC_n\}$.
- A binary partially ordered relation $\geq$ is defined in SC as $SC_i \geq SC_j$, which means that SC_i has a security clearance higher than or equal to SC_j.

A Practical Application of POSET: Hierarchical Access Control (Continued...)

- In addition the relation $\geq$ satisfies the following properties:
  - (a) [Reflexive property] $SC_i \geq SC_i$, $\forall SC_i \in SC$.
  - (b) [Anti-symmetric property] If $SC_i, SC_j \in SC$ such that $SC_i \geq SC_j$ and $SC_j \geq SC_i$, then $SC_i = SC_j$.
  - (c) [Transitive property] If $SC_i, SC_j, SC_k \in SC$ such that $SC_i \geq SC_j$ and $SC_j \geq SC_k$, then $SC_i \geq SC_k$.
- If $SC_i \geq SC_j$, we call SC_i as the predecessor of SC_j and SC_j as the successor of SC_i. If $SC_i \geq SC_k \geq SC_j$, then SC_k is an intermediate security class. In this case SC_k is the predecessor of SC_j and SC_i is the predecessor of SC_k.
- In a user hierarchy, the encrypted message by a successor security class is only decrypted by that successor class as well as its all predecessor security classes in that hierarchy.

A Practical Application of POSET: Hierarchical Access Control (Continued...)

- Consider a simple example of a poset in a user hierarchy in Fig. 1. In this figure, we have the following relationships: $SC_2 \leq SC_1$, $SC_3 \leq SC_1$, $SC_4 \leq SC_1$, $SC_5 \leq SC_1$, $SC_6 \leq SC_1$, $SC_7 \leq SC_1$; $SC_5 \leq SC_2$; $SC_5 \leq SC_3$, $SC_6 \leq SC_3$; $SC_7 \leq SC_4$.



A Practical Application of POSET: Hierarchical Access Control (Continued...)

- In a hierarchical access control, a trusted central authority (CA) distributes keys to each security class in the hierarchy such that any predecessor of a successor class can easily derive its successor's secret key.
- Using that derived secret key, the predecessor class can decrypt the information encrypted by its successor.
- However, the reverse is not true in such access control, that is, no successor class of any predecessor will be able to derive the secret keys of its predecessors.

Equivalence classes

- Let A be a non-empty set and R be an equivalence relation defined in A.
- Let $a \in A$ be an arbitrary element. Then the elements $x \in A$ which satisfy ${}_xR_a$ form a subset of A which is called the *equivalence class* of a in A with respect to (w.r.to) R.
- Thus, A_a or $[a]$ or $cl(a)$ or $\bar{a}$
  $= \{x | {}_xR_a, x \in A\}$
  is called the equivalence class of a in A w.r.to R.

Important properties of equivalence classes

- Let A be a non-empty set and R be an equivalence relation defined in A.
- Let $a \in A$ and $b \in A$ be two arbitrary elements. Then,
  1. $a \in [a]$;
  2. $b \in [a] \Rightarrow [b] = [a]$;
  3. $[a] = [b] \Leftrightarrow (a, b) \in R$;
  4. either $[a] = [b]$ or $[a] \cap [b] = \emptyset$, that is, either two equivalence classes are identical or disjoint.

Problem(Equivalence classes): 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.

- **Part 1.** *Claim:* R is an equivalence relation.
- **Part 2.** Here $R = \{(x, y) | x, y \in A, x \text{ is similar to } y\}$.
  Let $a \in A$ be an arbitrary triangle in the plane.
  Then,

$$\begin{aligned} [a] &= \{x | x \in A \text{ and } {}_x R_a\} \\ &= \{x | x \in A, x \text{ is similar to } a\} \end{aligned}$$

is an equivalence class of $a \in A$.

Problem(Equivalence classes): Let Z be the set of integers. Let R be a relation in Z defined by the open sentence "$(x - y)$ is divisible by m", where $x, y \in Z$. Verify whether R is an equivalence relation. If so, find the equivalence classes.

- **Part 1.** *Claim:* R is an equivalence relation.
- **Part 2.** Equivalnce classes.

Partitions

- Let S be a non-empty set. Then a *partition* of S is a collection of non-empty disjoint sub-sets of S whose union is S.
- In other words, if $A_1, A_2, \ldots, A_n$ be the non-empty sub-sets of S, then the set $\mathcal{P} = \{A_1, A_2, \ldots, A_n\}$ is said to be a partition of S, if
  1. $A_1 \cup A_2 \cup \ldots \cup A_n = S$,
  2. either $A_i = A_j$ or $A_i \cap A_j = \emptyset$, for all $i, j = 1, 2, \ldots, n$.

Example (Partitions)

- Consider a set $S = \{1, 2, 3, \ldots, 22\}$. Now consider three subsets A, B and C of S as follows:
  $A = \{1, 4, 7, \ldots, 22\}$,
  $B = \{2, 5, 8, \ldots, 20\}$,
  $C = \{3, 6, 9, \ldots, 21\}$.
  See that
  1. $A \cup B \cup C = S$, and
  2. $A \cap B = B \cap C = C \cap A = \emptyset$.

  Hence, the set $(P) = \{A, B, C\}$ forms a partition of S.

Relationship between Partitions and Equivalence relations

Theorem (Fundamental Theorem on Equivalence Relations)

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

Compatible Relation

Definition (Compatibility Relation)

Let R be a relation in a non-empty set A (i.e., $R \subseteq A \times A$). Then, R is said to be a *compatibility relation* if it is both reflexive and symmetric.

- **Problem:** Let A be a set of people, and R a binary relationon A such that $(a, b) \in R$ if a is a friend of b.
  - ***Solution:*** (i) R is reflexive, since a is always a friend of $a \in A$ (i.e., himself/herself), that is, ${}_aR_a$ holds, $\forall a \in A$.
    (ii) R is symmetric, since, if a is a friend of b, then obviously b is also a friend of a, that is,
    if ${}_aR_b$ holds, then ${}_bR_a$ also holds, $\forall a, b \in A$.

  Hence, R is a compatibility relation.

Compatible Relation (Continued...)

- **Important Observations**
  - All equivalence relations are compatibility relations.
  - Let R and S be two compatibility relations on a set A. Then $R \cap S$ is a compatibility relation, but $R \cup S$ may or may not be a compatibility relation.

Closure of Relations

Definition (Reflexive Closure)

A relation R' is the reflexive closure of a relation R if and only if
(a) R' is reflexive,
(b) $R \subseteq R'$,
(c) For any relation R'', if $R \subseteq R''$ and R'' is reflexive, then $R' \subseteq R''$,
i.e., R' is the smallest relation that satisfies the conditions (a) and (b).

The reflexive closure of a relation R is denoted by $r(R)$.

Problem (Closure of Relations): Given the relation $R = \{(a,b),(b,a),(b,b),(c,b)\}$ on the set $A = \{a,b,c\}$. Compute the reflexive closure $r(R)$ of R.

- It is clear that R is not reflexive, since $(a,a) \notin R$ and $(c,c) \notin R$.
- Consider a relation R' which contains R as well as the tuples (a,a) and (c,c), that is,

$$\begin{aligned} R' &= R \cup \{(a,a),(c,c)\} \\ &= \{(a,a),(a,b),(b,a),(b,b),(c,b),(c,c)\} \end{aligned}$$

  Then, clearly R' is reflexive and $R \subseteq R'$.
- Furthermore, any other relation, say R'', containing R must also contain (a,a) and (c,c); otherwise it will not be reflexive. So, $R' \subseteq R''$. As R' contains R, and R' is reflexive, and is contained in every reflexive relation that contains R, so R' is the smallest relation satisfies conditions (a) and (b). Hence, $r(R) = R'$.

Closure of Relations (Continued...)

Definition (Symmteric Closure)

A relation R' is the symmetric closure of a relation R if and only if
(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 the conditions (a) and (b).

The symmetric closure of a relation R is denoted by $s(R)$.

Problem (Closure of Relations): Given the relation $R = \{(a,a),(a,b),(c,c),(b,c),(b,a),(a,c)\}$ on the set $A = \{a,b,c\}$. Compute the symmetric closure $s(R)$ of R.

- It is clear that R is not symmetric.
- To be symmetric, R needs the pairs (c,b) and $c,a)$. Consider a relation R' which contains R as well as the tuples (c,b) and $c,a)$, that is,

$$\begin{aligned} R' &= R \cup \{(c,b),(c,a)\} \\ &= \{(a,a),(a,b),(c,c),(b,c),(b,a),(a,c),(c,b),(c,a)\} \end{aligned}$$

  Then, clearly R' is symmetric and $R \subseteq R'$.
- Furthermore, any other relation, say R'', containing R must also contain (c,b) and (c,a); otherwise it will not be symmetric. So, $R' \subseteq R''$. So, R' is the smallest relation satisfies conditions (a) and (b). Hence, $s(R) = R'$.

Closure of Relations

Definition (Transitive Closure)

A relation R' is the transitive closure of a relation R if and only if
(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).

The transitive closure of a relation R is denoted by $t(R)$ or R^t.

Problem (Closure of Relations): Let R be the less than ($<$) relation on the set Z of integers. Compute the transitive closure $t(R)$ of R.

- The transitive closure of the less than ($<$) relation on Z is the less than ($<$) relation itself.

How to find Transitive Closure of a given Relation R ?

- We need to add the minimum number of tuples to R giving us R^t such that if $(a, b) \in R^t$ and $(b, c) \in R^t$, then $(a, c) \in R^t$.
- Thus, $R^t = R \cup \{(a, b) \in R^t \wedge (b, c) \in R^t \Rightarrow (a, c) \in R^t\}$.

Problem (Closure of Relations): Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (1, 2), (1, 3), (2, 3), (3, 1)\}$ be a relation on A. Compute the transitive closure R^t of R.

Solution

- Clearly, R is not transitive. For example, $(2,3) \in R \wedge (3,1) \in R \not\Rightarrow (2,1) \in R$.
- Add the following mininum number of tuples in R to construct R' such that $R \subseteq R'$ and R' is symmetric:

$$\begin{aligned}
(2,3) \in R \wedge (3,1) \in R &\Rightarrow (2,1) \in R^t \\
(3,1) \in R \wedge (1,2) \in R &\Rightarrow (3,2) \in R^t \\
(3,1) \in R \wedge (1,3) \in R &\Rightarrow (3,3) \in R^t \\
(2,1) \in R^t \wedge (1,2) \in R &\Rightarrow (2,2) \in R^t
\end{aligned}$$

- Thus, $R^t = t(R) = R' = R \cup \{(2,1),(2,2),(3,2),(3,3)\}$.

End of this lecture