CSCE 222
Discrete Structures for Computing

Relations

Dr. Hyunyoung Lee

Based on slides by Andreas Klappenecker
Suppose we have three rabbits called Albert, Bertram, and Chris that have distinct heights.

Let us write \((a,b)\) if \(a\) is taller than \(b\).

Obviously, we cannot have both \((Albert, Bertram)\) and \((Bertram, Albert)\), so not all pairs of rabbit names will occur.

Suppose: Albert is taller than Bertram, and Bertram is taller than Chris.

Then the set of “taller than” relations is:

\[\{(Albert, Bertram), (Bertram, Chris), (Albert, Chris)\}\]
Let
\[ A = \{ \text{Albert, Bertram, Chris} \} \]
be the set of rabbits.

Then the "taller than" relations is a subset of the cartesian product \( A \times A \), namely \( \{ (\text{Albert, Bertram}), (\text{Bertram, Chris}), (\text{Albert, Chris}) \} \subseteq A \times A \).
Binary Relations

Let $A$ and $B$ be sets.

A binary relation from $A$ to $B$ is a subset of $A \times B$.

A relation on a set $A$ is a subset of $A \times A$. 
Examples

Let us consider the following relations on the set of integers:

\[ A = \{ (a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a \leq b \} \]

\[ B = \{ (a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a > b \} \]

\[ C = \{ (a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a = b \text{ or } a = -b \} \]
Let $R$ be a relation from $A$ to $B$. In other words, $R$ contains pairs $(a, b)$ with $a$ in $A$ and $b$ in $B$.

If $(a, b)$ in $R$, then we say that $a$ is related to $b$ by $R$.

It is customary to use infix notation for relations. Thus, we write $a \, R \, b$ to express that $a$ is related to $b$ by $R$. In other words, $a \, R \, b$ iff $(a, b)$ in $R$. 
Example

Let $A$ be the set of city names of the USA. Let $B$ be the set of states. Define the relation $C$

$$C = \{ (a,b) \in A \times B \mid a \text{ is a city of } b \}$$

Then

(College Station, Texas)

(Austin, Texas)

(San Francisco, California)

all belong to the relation $C$. 
The concept of a relation generalizes the concept of a function. A function $f$ relates the argument $x$ with its function value $f(x)$. The difference is that a relation can relate an element $x$ with more than one value.

For example, consider the relation

$$A = \{ (a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a \leq b \}.$$
Plan

We are going to study relations as mathematical objects. This allows us to abstract from well-known relations such as $\leq$, $=$, “is taller than”, “likes the same sport as”.

We identify some basic properties of relations. Then we study relations generalizing the equality relation (so-called equivalence relations), and relations generalizing $\leq$ (so-called partial order relations).
Basic Properties of Relations
Reflexivity

We call a relation $R$ on a set $A$ reflexive if and only if $(a,a) \in R$ holds for all $a$ in ${A}$.

Example: The equality relation $=$ on the set of integers is reflexive, since $a=a$ holds for all integers $a$.

The less than relation $<$ on the set of integers is not reflexive, since $1<1$ does not hold.
X1 Let $\mid$ denote the divides relation on the set of positive integers, so $2 \mid 4$ means that there exists an integer $x$ such that $2x = 4$. Is the relation $\mid$ reflexive?

X2 Let $S$ be the set of students in this class. Consider the relation $R = “wears the same color shirt as.”$ Is the relation $R$ reflexive?
We call a relation \( R \) on a set \( A \) **symmetric** if and only if \((a,b) \in R\) implies that \((b,a) \in R\) holds.

Example: The equality relation \( = \) on the set of integers is symmetric, since \( a=b \) implies that \( b=a \).

The less than relation \( < \) on the set of integers is not symmetric, since \( 1<2 \) but \( 2<1 \) does not hold.
X1 Let $|$ denote the divides relation on the set of positive integers, so $2 \mid 4$ means that there exists an integer $x$ such that $2x=4$. Is the relation $|$ symmetric?

X2 Let $S$ be the set of students in this class. Consider the relation $R = \text{“wears the same color shirt as”}$. Is the relation $R$ symmetric?
We call a relation $R$ on a set $A$ **antisymmetric** if and only if $(a,b) \in R$ and $(b,a) \in R$ imply that $a=b$.

Formally: $\forall a \forall b ((a,b) \in R \land (b,a) \in R) \rightarrow a=b$.

Example: The equality relation $=$ on the set of integers is antisymmetric, since $a=b$ and $b=a$ implies that $a=a$.

The less than relation $<$ on the set of integers is antisymmetric. Why?
X1 Let $\mid$ denote the divides relation on the set of positive integers, so $2 \mid 4$ means that there exists an integer $x$ such that $2x = 4$. Is the relation $\mid$ antisymmetric?

X2 Let $S$ be the set of students in this class. Consider the relation $R = \text{“wears the same color shirt as”}$. Is the relation $R$ antisymmetric?
The meaning of antisymmetry is not opposite to the meaning of symmetry! In fact, we have already seen that the equality relation = on the set of integers is both symmetric and antisymmetric.

You should very carefully study the meaning of these terms.
We call a relation $R$ on a set $A$ \textit{transitive} if and only if $(a,b) \in R$ and $(b,c) \in R$ imply that $(a,c) \in R$.

Example: The equality relation $=$ on the set of integers is transitive, since $a=b$ and $b=c$ implies that $a=c$.

The less than relation $<$ on the set of integers is transitive, since $a<b$ and $b<c$ imply that $a<c$. 
Test Yourself...

X1 Let $|$ denote the divides relation on the set of positive integers, so $2 \mid 4$ means that there exists an integer $x$ such that $2x = 4$. Is the relation $|$ transitive?

X2 Let $S$ be the set of students in this class. Consider the relation $R =$ “wears the same color shirt as. Is the relation $R$ transitive?
Equivalence Relations
A relation $R$ on a set $A$ is called an equivalence relation if and only if $R$ is reflexive, symmetric, and transitive.

- Reflexive: For all $a$ in $A$, we have $(a,a)$ in $R$.
- Symmetric: $(a,b)$ in $R$ implies that $(b,a)$ in $R$.
- Transitive: $(a,b)$ in $R$ and $(b,c)$ in $R$ implies that $(a,c)$ in $R$. 
Example: Equality

The equality relation $=\ $on the set of integers is an equivalence relation.

Indeed,

the relation $=\ $is reflexive, since $a=a$ holds for all integers $a$.

the relation $=\ $is symmetric, since $a=b$ and $b=a$ implies that $a=a$.

the relation $=\ $is transitive, since $a=b$ and $b=c$ implies that $a=c$. 

22
Example: String Length

Let \( A \) be the set of strings of English letters. Let \( R \) be the relation on \( A \) given by \( a \sim b \) iff the strings \( a \) and \( b \) have the same length.

For every string \( s \) in \( A \), we have \( s \sim s \), since \( s \) has the same length as itself. Thus, \( R \) is reflexive.

For all strings \( a \) and \( b \), if \( a \sim b \), then \( a \) and \( b \) have the same length, so \( b \sim a \) holds as well. Therefore, \( R \) is symmetric.

For all strings \( a, b, c \), if \( a \sim b \) and \( b \sim c \), then the strings \( a \) and \( b \) have the same length, and the string \( b \) and \( c \) have the same length, so \( a \sim c \). Thus, \( R \) is transitive.
Example: Congruence mod m

Let m be a positive integer. For integers a and b, we write

\[ a \equiv b \pmod{m} \]

if and only if m divides \( a-b \).

For all \( a \) in \( \mathbb{Z} \), we have \( m \mid (a-a) \), since \( m \cdot 0 = 0 = a-a \). Thus, \( a \equiv a \pmod{m} \) holds for all integers \( a \). Thus, the relation is reflexive.

For \( a, b \) in \( \mathbb{Z} \), if \( a \equiv b \pmod{m} \), then this means that there exists an integer \( k \) such that \( m k = a-b \). Thus, \( m(-k) = b-a \), which implies \( b \equiv a \pmod{m} \). Thus, the relation is symmetric.
Example: Congruence mod m

If \( a \equiv b \pmod{m} \) and \( b \equiv c \pmod{m} \) holds, then this means that there exist integers \( k \) and \( l \) such that

\[ mk = a-b \quad \text{and} \quad ml = b-c \]

Hence, \( m(k+l) = a-b + b-c = a-c \)

This shows that \( a \equiv c \pmod{m} \) holds.

Therefore, the relation is \textbf{transitive}.

We can conclude that \( a \equiv b \pmod{m} \) is an equivalence relation.
Equivalence Classes

Let $R$ be an equivalence relation on a set $A$. For an element $a$ in $A$, the set of elements
$$[a]_R = \{ b \in A \mid a R b \}$$
is called the equivalence class of $a$. 
Let us consider the equivalence relation $a \equiv b \pmod{4}$ on the set of integers. Thus, two integers $a$ and $b$ are related whenever their difference is a multiple of 4. Thus, the equivalence classes are:

$[0] = \{ ..., -8, -4, 0, 4, 8, ... \}$

$[1] = \{ ..., -7, -3, 1, 5, 9, ... \}$

$[2] = \{ ..., -6, -2, 2, 6, ... \}$

$[3] = \{ ..., -5, -1, 3, 7, ... \}$

Theorem

Let $R$ be an equivalence relation on a set $A$. Then the following statements are equivalent:

a) $a \sim b$

b) $[a] = [b]$

c) $[a] \cap [b] \neq \emptyset$
Proof

Suppose that $aRb$ holds. We are going to show that $[a] \subseteq [b]$ holds. Let $c \in [a]$. This means that $aRc$ holds. Since $R$ is symmetric, $aRb$ implies that $bRa$. By transitivity, $bRa$ and $aRc$ imply that $bRc$ holds. Hence, $c \in [b]$. Therefore, we have shown that $[a] \subseteq [b]$. The proof that $[b] \subseteq [a]$ is similar. Hence, we have shown that statement a) implies statement b).

We will show now that b) implies c). Since $a \in [a]$, we know that the equivalence class of $a$ is not empty. As $[a] = [b] \neq \emptyset$, we have $[a] \cap [b] \neq \emptyset$. 

29
Proof (continued)

We will show now that c) implies a).

Suppose that \([a] \cap [b] \neq \emptyset\). Thus, there exists an element \(c\) such that \(aRc\) and \(bRc\). By symmetry, we get \(cRb\). It follows by transitivity that \(aRb\) holds. \(\Box\)
Partial Order Relations
Partial Orders

A relation $R$ on a set $A$ is called a **partial order** if and only if it is reflexive, antisymmetric, and transitive.

A set $A$ with a partial order is called a partially ordered set (poset).
The “less than or equal to” relation ≤ on the set of integers is a partial order relation.

Indeed, since a ≤ a holds for all integers a, the relation ≤ is reflexive.

Since a ≤ b and b ≤ a implies that a = b, the relation is antisymmetric.

Since a ≤ b and b ≤ c implies that a ≤ c, the relation is transitive.
The divides relation $|$ on the set of positive integers is a partial order relation.

Indeed, since $a | a$ for all positive integers $a$, the relation $|$ is reflexive.

If $a | b$ and $b | a$, then there exist integers $k$ and $l$ such that $a k = b$ and $b l = a$. Therefore, $a k l = a$, so $k l = 1$. This means that either $k = l = 1$ or $k = l = -1$. Since $a$ and $b$ are positive integers, we cannot have $a(-1) = b$. Therefore, we must have $k = l = 1$, which means that $a = b$. Thus, $|$ is an antisymmetric relation.

The relation $|$ is transitive, since $a | b$ and $b | c$ means that there exist integers $k$ and $l$ such that $ak = b$ and $bl = c$, so $a(kl) = c$, which implies that $a | c$. 

Example 2
Test Yourself ...

X1 Is the less than relation $<$ on the set of integers a partial order relation?

X2 Let $S$ be a set. Is the subset relation $\subseteq$ on the set $P(S)$ a partial order relation?
Comparable Elements

A partial order on a set $S$ is often denoted by symbols resembling the notation commonly used for “less than or equal to”, namely $\leq$ or $\subseteq$ or $\preceq$.

Let $(S, \preceq)$ be a partially ordered set. For two elements $a$ and $b$ of $S$, we do not necessarily have that one of the relations $a \preceq b$ or $b \preceq a$ holds. If one of them holds, then we call $a$ and $b$ comparable elements of $S$, otherwise $a$ and $b$ are incomparable.
Total Orders

A partially ordered set \((S, \leq)\) in which any two elements are comparable is called a total order.

A totally ordered set is also called a chain.

For example, consider the set of positive integers \(\mathbb{N}\) with \(\leq\). Any two positive integers are comparable with \(\leq\). It can form a chain such that \(1 \leq 2 \leq 3 \leq 4 \leq \ldots\)
Lexicographic Ordering

Suppose that we have two partially ordered sets:

\((A, \preceq_1)\) and \((B, \preceq_2)\).

We can construct a partial order on \(A \times B\) by defining

\[(a_1, b_1) \preceq (a_2, b_2)\]

if and only if \((a_1 = a_2 \text{ and } b_1 \preceq_2 b_2)\) or \((a_1 <_1 a_2)\) holds.

We call the relation \(\preceq\) the **lexicographic order** on the cartesian product \(A \times B\).
Example

Let \( \mathbb{Z} \) be the set of integers, totally ordered with the “less than or equal to” relation \( \leq \).

In the lexicographic order \( \precsim \) on \( \mathbb{Z} \times \mathbb{Z} \), we have

\[
(3,4) \precsim (4,2) \\
(3,7) \precsim (3,8)
\]
A set \((S, \preceq)\) is a well-ordered set if and only if

a) \(\preceq\) is a total order on \(S\) and

b) every nonempty subset \(A\) has a least element.

An element \(a\) in \(A\) is called a least element if and only if \(a \preceq b\) holds for all \(b\) in \(A\).
Let $N$ be the set of positive integers with $\leq$.

Then $N \times N$ with the lexicographic order is a well-ordered set.
Test Yourself...

X1 Is the set \((\mathbb{Z}, \leq)\) a well-ordered set?

X2 Is the set of negative integers with \(\leq\) a well-ordered set?

X3 Is the set of positive real numbers with \(\leq\) a well-ordered set?

A set \((S, \leq)\) is a well-ordered set if and only if
a) \(\leq\) is a total order on \(S\) and
b) every nonempty subset \(A\) has a least element.
Principle of Well-Ordered Induction

Let \((S, \preceq)\) be a well-ordered set. Let \(P: S \rightarrow \{t,f\}\) be a predicate on \(S\).

Then \(P(x)\) is true for all \(x\) in \(S\) if and only if the inductive step holds:

**Inductive Step:** For every \(y\) in \(S\), if \(P(x)\) is true for all \(x\) in \(S\) with \(x \prec y\), then \(P(y)\) is true.

[Did we forget the base step?]
Proof (1)

(⇒) If $P(x)$ is true for all $x$ in $S$, then the Inductive Step evidently holds.

(⇐) Let us assume that the Inductive Step holds. We will use proof by contradiction to show that $P(x)$ is true for all $x$ in $S$. 
Seeking a contradiction, let us assume that $P(x)$ is not true for all $x$ in $S$. In other words, there exists an element $x'$ in $S$ such that $P(x')$ is false. Therefore, the set

$$C = \{ x' \in S \mid P(x') \text{ is false} \}$$

is not empty. Since $S$ is well-ordered, the set $C$ has a least element $a$. However, we know that $P(x)$ is true for all $x < a$. By the inductive step $P(a)$ is true, contradicting the fact that $a \in C$. 
Ackermann Function

\[
A(m, n) = \begin{cases} 
  n + 1 & \text{if } m = 0, \\
  A(m - 1, 1) & \text{if } m > 0 \text{ and } n = 0, \\
  A(m - 1, A(m, n - 1)) & \text{if } m > 0 \text{ and } n > 0
\end{cases}
\]

Let \( S \) be the set of all pairs of nonnegative integers order with the lexicographic order.
Let \( P(m,n) \) be the property that the Ackermann function called with arguments \( m \) and \( n \) will terminate.
Suppose that \( P(a,b) \) holds for all \( (a,b) \prec (m,n) \). If \( m=0 \), then \( P(m,n) \) is true. If \( m>0 \), then \( A(m,n) \) is defined in terms of functions \( A(a,b) \) with \( (a,b) \prec (m,n) \), so in terms of terminating functions. Therefore, \( P(m,n) \) is true for \( m>0 \) as well. By the principle of well-ordered induction, \( A(m,n) \) terminates for all pairs of nonnegative integers \( (m,n) \).
Maximal and Minimal Elements

Let \((S, \leq)\) be a partially ordered set.

An element \(m\) in \(S\) is called **maximal** iff there does not exist any element \(b\) in \(S\) such that \(m < b\).

An element \(m\) in \(S\) is called **minimal** iff there does not exist any element \(b\) in \(S\) such that \(b < m\).
Example

Determine the maximal elements of the set 
\{2,4,5,10,12,20,25\},
partially ordered by the divisibility relation.
The elements 12, 20, and 25 are the maximal elements.

Determine the minimal elements of the set 
\{2,4,5,10,12,20,25\}
The elements 2 and 5 are the minimal elements.
Least and Greatest Element

Let \((S, \leq)\) be a partially ordered set.

An element \(a\) in \(S\) is called the least element iff \(a \leq b\) holds for all \(b\) in \(S\).

[A least element does not need to exist. If it does, then it is uniquely determined.]

An element \(z\) in \(S\) is called the greatest element iff \(b \leq z\) holds for all \(b\) in \(S\).

[A greatest element does not need to exist. If it does, then it is uniquely determined.]
Test Yourself...

X1 Determine the least and greatest element of the set of positive integers partially ordered by divisibility.

X2 Let $S$ be a nonempty set. Partially order the power set $P(S)$ by inclusion. Determine the least and greatest elements of $P(S)$.
Let \((S, \leq)\) be a finite partially ordered set.

Suppose that \(a\) and \(b\) are distinct elements of \(S\) such that \(a \leq b\). We say that \(b\) covers \(a\) if and only if there does not exist an element \(c\) in \(S\) such that \(a < c < b\).

The Hasse diagram of \((S, \leq)\) is a diagram in which an element \(b\) of \(S\) is written above \(a\) and connected by a line if and only if \(b\) covers \(a\).
Examples

Consider \{2,4,5,10,12,20,25\} with divisibility condition.

The Hasse diagram is given by

![Hasse diagram](image)

The Hasse diagram is more economical than representing the partial order relation by a directed graph (with an edge from \(a\) to \(b\) whenever \(a \leq b\)). Self-loops and transitively implied relations are omitted.
Lattices
Upper and Lower Bounds

Let \((S, \leq)\) be a partially ordered set.

Let \(A\) be a subset of \(S\).

An element \(u\) of \(S\) is called an upper bound of \(A\) if and only if \(a \leq u\) holds for all \(a\) in \(A\).

An element \(l\) of \(S\) is called a lower bound of \(A\) if and only if \(l \leq a\) holds for all \(a\) in \(A\).
Example

Let \{2,4,5,10,12,20,25\} with divisibility condition.

The Hasse diagram is given by

The subset \( A = \{4,10\} \) has 20 as an upper bound, and 2 as a lower bound.

The subset \( A = \{12\} \) has 12 as an upper bound, and 2, 4 and 12 as lower bounds.
Let \((S, \leq)\) be a partially ordered set, and \(A\) a subset of \(S\). An element \(u\) of \(S\) is called a **least upper bound** of \(A\) if it is an upper bound that is less than any other upper bound of \(A\).

[Unlike upper bounds, the least upper bound is uniquely determined if it exists]
Greatest Lower Bounds

Let \((S, \leq)\) be a partially ordered set, and \(A\) a subset of \(S\). An element \(l\) of \(S\) is called a greatest lower bound of \(A\) if it is a lower bound that is greater than any other lower bound of \(A\).

A greatest lower bound is uniquely determined if it exists.
Example

Consider the poset \((S=\{2, 4, 6, 9, 12, 18, 27, 36, 48, 60, 72\}, \mid )\).

Draw the Hasse diagram:

What are the upper bounds of the subset \(A=\{2, 9\}\)?

What are the lower bounds of the subset \(B=\{60, 72\}\)?
A partially ordered set in which every pair has both a least upper bound and a greatest lower bound is called a lattice.
Consider the set \((N,|)\) of positive integers that is partially ordered with respect to the divisibility relation.

Let \(a\) and \(b\) be two distinct positive integers. Then the least upper bound of \(\{a,b\}\) is the least common multiple of \(a\) and \(b\). The greatest lower bound is the greatest common divisor of \(\{a,b\}\). Therefore, \((N,|)\) is a lattice.
The flow of information from one person (or one computer program) to another might be restricted via security clearances.

For example, multilevel security policy is often used in government and military systems. Each piece of information is assigned to a security class. Each security class is represented by a pair \((A,C)\), where \(A\) is an authority level, and \(C\) is a category.

**Authority levels:** \{unclassified, confidential, secret, top secret\}

**Categories:** \{medical, financial, criminal\}
We can order the security classes by specifying
\[(A_1, C_1) \leq (A_2, C_2) \text{ if and only if } A_1 \leq A_2 \text{ and } C_1 \subseteq C_2.\]

For example, information can flow from
\[(\text{confidential, \{financial\}}) \text{ to } (\text{secret, \{financial, criminal\}})\]

but not from
\[(\text{confidential, \{financial, medical\}}) \text{ to } (\text{top secret, \{financial\}}).\]

The set of all security classes with this ordering forms a lattice.
Lattice Model of Information Flow

\[ A = \{ \text{unclassified, confidential, secret, top secret} \} \]

\[ C = \{ \text{medical, financial, criminal} \} \]

\((A_1, C_1) \leq (A_2, C_2)\) if and only if \(A_1 \leq A_2\) and \(C_1 \subseteq C_2\)

To show \((A \times C, \leq)\) is a lattice,

1. Show that this is a poset — reflexive, antisymmetric, and transitive.

2. Show that every pair has a least upper bound and a greatest lower bound.
(A_1, C_1) \leq (A_2, C_2) if and only if A_1 \leq A_2 and C_1 \subseteq C_2

1. Show that this is a poset

(i) reflexive: (A_1, C_1) \leq (A_1, C_1) because A_1 \leq A_1 and C_1 \subseteq C_1

(ii) antisymmetric: (A_1, C_1) \leq (A_2, C_2) and (A_2, C_2) \leq (A_1, C_1) implies that (A_1, C_1) = (A_2, C_2)

(iii) transitive: (A_1, C_1) \leq (A_2, C_2) and (A_2, C_2) \leq (A_3, C_3) if and only if A_1 \leq A_2 \leq A_3 and C_1 \subseteq C_2 \subseteq C_3, which yields that A_1 \leq A_3 and C_1 \subseteq C_3 and thus (A_1, C_1) \leq (A_3, C_3)
(A_1, C_1) \leq (A_2, C_2) \text{ if and only if } A_1 \leq A_2 \text{ and } C_1 \subseteq C_2

2a. Show that every pair has a least upper bound.

B=\{(A_1, C_1), (A_2, C_2)\}

(A,C) \text{ is an upper bound of } B \text{ iff (both } A_1 \text{ and } A_2) \leq A \text{ and (both } C_1 \text{ and } C_2) \subseteq C

(both } A_1 \text{ and } A_2) \leq \max(A_1, A_2) \leq A \text{ and (both } C_1 \text{ and } C_2) \subseteq (\text{union of } C_1 \text{ and } C_2) \subseteq C
Lattice Model of Information Flow

\[(A_1, C_1) \leq (A_2, C_2) \text{ if and only if } A_1 \leq A_2 \text{ and } C_1 \subseteq C_2\]

2b. Show that every pair has a greatest lower bound.

\[B=\{(A_1, C_1), (A_2, C_2)\}\]

\[(A,C)\text{ is a lower bound of } B \text{ iff } A \leq \text{(both } A_1 \text{ and } A_2) \text{ and } C \subseteq \text{(both } C_1 \text{ and } C_2)\]

\[A \leq \min(A_1, A_2) \leq \text{(both } A_1 \text{ and } A_2) \text{ and } C \subseteq \text{(intersection of } C_1 \text{ and } C_2) \subseteq \text{(both } C_1 \text{ and } C_2)\]