Lecture Overview

Relations

Operations on Relations

Equivalence Relations and Partitions

Partial Orders

Relations

Relationship between elements of sets

Binary relation *from* a set A to a set B is
$R \subseteq A \times B$.
Or, $a \sim_R b$ or aRb instead of $(a,b) \in R$

A binary relation *on* a set A is a subset $R \subseteq A^2$
A relation from A to A.

The relation "is taking a class" as a subset of $\{students\ at\ MIT\} \times \{classes\ at\ MIT\}$.
A relation from students to classes

Properties of Relations

reflexive — if for every $a \in A$, $a \sim_R a$.
"is living in the same room"
$\{students\ at\ MIT\} \times \{students\ at\ MIT\}$

irreflexive — if for every $a \in A$, $a \not\sim_R a$.
"parent", on the set {people}

transitive — if for every $a, b, c \in A$,
$a \sim_R b$ and $b \sim_R c$ implies $a \sim_R c$.
"can drive from first to second city"

symmetric —
if for every $a, b \in A$, $a \sim_R b$ implies $b \sim_R a$.
"is living in the same room"

antisymmetric — if for every $a, b \in A$,
$a \sim_R b$ and $b \sim_R a$ implies $a = b$.
$A = \mathbb{N}$ and $a \sim_R b$ iff $a \leq b$.

asymmetric — if for every $a, b \in A$,
$a \sim_R b$ implies $\neg(b \sim_R a)$.
$A = \mathbb{N}$ and $a \sim_R b$ iff $a < b$.

Properties of Relations, Ex.

Relation on computers,
"are connected (directly) by wire"
symmetric but not transitive

$A = \Re^2$ and define $a \sim_R b$ iff $d(a,b) = 1$.
is only symmetric.

"likes"
not symmetric, not antisymmetric, not transitive, not (even) reflexive, not irreflexive, not asymmetric.

Representation

Lists, Matrices, Graphs

List all pairs

Relation from
$A = \{0, 1, 2, 3\}$ to $\{a, b, c\}$
to be the list:
$\{(0, a), (0, c), (1, c), (2, b), (1, a)\}$.

Reflexivity — contains all pairs (a, a)
Symmetry — contains (a, b) then (b, a)
Transitivity — contains (a, b) and (b, c) then also (a, c).

Boolean matrices

Used for finite sets A, B
Rows for elements of A, columns for B.
1 in position if the pair is in the relation,
0 otherwise.

The relation $\{(0, a), (0, c), (1, c), (2, b), (1, a)\}$. from $\{0, 1, 2, 3\}$ to $\{a, b, c\}$ is represented by the matrix

	a	b	c
0	1	0	1
1	1	0	1
2	0	1	0
3	0	0	0

Boolean matrices, Cont.

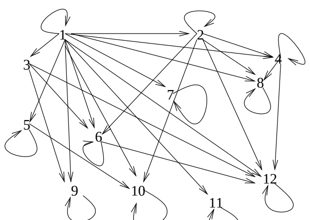
The divisibility relation over $\{1, 2, \ldots, 12\}$

	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	1	0	1	0	1	0	1	0	1	0	1
3	0	0	1	0	0	1	0	0	1	0	0	1
4	0	0	0	1	0	0	0	1	0	0	0	1
5	0	0	0	0	1	0	0	0	0	1	0	0
6	0	0	0	0	0	1	0	0	0	0	0	1
7	0	0	0	0	0	0	1	0	0	0	0	0
8	0	0	0	0	0	0	0	1	0	0	0	0
9	0	0	0	0	0	0	0	0	1	0	0	0
10	0	0	0	0	0	0	0	0	0	1	0	0
11	0	0	0	0	0	0	0	0	0	0	1	0
12	0	0	0	0	0	0	0	0	0	0	0	1

Reflexivity — major diagonal is all 1
Symmetry — matrix symmetric around the major diagonal

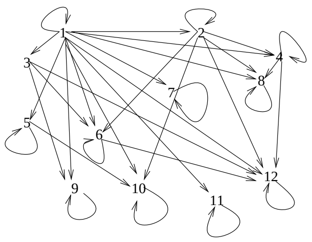
Directed graphs – Digraphs

Used for relations where $A = B$
in this case a dot represents an element in A and an arrow for every relation.



Reflexivity: All nodes have self-loops.
Symmetry: all edges are bidirectional.
Transitivity: Short-circuits, for any sequence of consecutive arrows, there is a single arrow from the first to the last node.

Paths in Directed graphs — L5—P. 9



A *path* in a relation R is a sequence $a_0, \ldots, a_k$ with $k \geq 0$ such that $(a_i, a_{i+1}) \in R$ for every $i < k$. We call k the *length* of the path.

Operations on Relations, Inverse — L5—P. 10

If R is a relation on $A \times B$, then R^{-1} is a relation on $B \times A$ given by $R^{-1} = \{(b, a) \mid (a, b) \in R\}$. It's just the relation "turned backwards."

Inverse of "parent-of" is "child-of."

Composition of Relations — L5—P. 11

The *composition* of relations $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$ is the relation $R_2 \circ R_1 = \{(a, c) \mid (\exists b)((a, b) \in R_1) \wedge ((b, c) \in R_2)\}$.

Examples:
Composition of parent-of relation with itself gives grandparent-of.

Composition of relations is equivalent to matrix multiplication, with $+$ replaced by $\vee$ (Boolean or) and $*$ replaced by $\wedge$.

Ex:
Let R_1 be relation (student in-class class-number):

	a	b	c
s_0	1	0	1
s_1	1	0	1
s_2	0	1	0
s_3	0	0	0

Let R_2 be relation (class-number in-class-rooms class-room) from $\{a, b, c\}$ to $\{d, e, f\}$ given by:

	d	e	f
a	1	1	1
b	0	1	0
c	0	0	1

Then $R_2 \circ R_1 = \{(s_0, d), \ldots\}$, (student in-class-rooms class-room) that is,

	d	e	f
s_0	1	1	1
s_1	1	1	1
s_2	0	1	0
s_3	0	0	0

Relational composition is associative. Just like matrix multiplication.

	a	b	c
s_0	1	0	1
s_1	1	0	1
s_2	0	1	0
s_3	0	0	0

Multiply by:

	d	e	f
a	1	1	1
b	0	1	0
c	0	0	1

Composition of Relations R^k L5–P. 14

Useful Lemma: $\forall k \geq 1$ $R^k =$
$\{(a,b) \mid$ there is a length k path from a to b in $R\}$

"Proof" by example, consider the relation R, (a,b), (b,d), (d,e) or:

	a	b	c	d	e
a	0	1	0	0	0
b	0	0	0	1	0
c	0	0	0	0	0
d	0	0	0	0	1
e	0	0	0	0	0

Or, $a \to b \to d \to e$ and an additional node c

So, R^2 (according to the relation composition definition) will be
(Note that matrix multiplication gives
1st line and 4th column results in 1
2nd line and 5th column results in 1)

	a	b	c	d	e
a	0	0	0	1	0
b	0	0	0	0	1
c	0	0	0	0	0
d	0	0	0	0	0
e	0	0	0	0	0

Proof: induction on k
Base case: $k = 1$ then we have R
Step: assume for R^k and prove for R^{k+1}.
If there is a path $a_0, \ldots, a_{k+1}$ in R then there is a path $a_0, \ldots, a_k$ in R and
a tuple (a_k, a_{k+1}) in R.
By induction $(a_0, a_k) \in R^k$.
By definition of composition of $R^k \circ R$ $(a_0, a_{k+1}) \in R^{k+1}$.
Still to show that if $(a,b) \in R^{k+1}$ then a path $a_0, \ldots, a_{k+1}$ exists in R...

Closure of Relation
Reflexive Closure L5–P. 16

The *reflexive closure* of R is
$S = R \cup \{(a,a) \mid a \in A\}$

	a	b	c	d	e
a	0	1	1	0	0
b	0	0	0	1	0
c	0	0	0	0	0
d	0	0	0	0	1
e	0	0	0	0	0

is changed to:

	a	b	c	d	e
a	1	1	1	0	0
b	0	1	0	1	0
c	0	0	1	0	0
d	0	0	0	1	1
e	0	0	0	0	1

Closure of Relation
Symmetric Closure

The *symmetric closure* of R is $S = R \cup R^{-1}$.

	a	b	c	d	e
a	0	1	1	0	0
b	0	0	0	1	0
c	0	0	0	0	0
d	0	0	0	0	1
e	0	0	0	0	0

Is changed to:

	a	b	c	d	e
a	0	1	1	0	0
b	1	0	0	1	0
c	1	0	0	0	0
d	0	1	0	0	1
e	0	0	0	1	0

Closure of Relation
Transitive Closure

The *transitive closure* of a relation R is that set:
$S = \{(a, b) \mid \text{there is a path from } a \text{ to } b \text{ in } R\}$.

	a	b	c	d	e
a	0	1	0	0	0
b	0	0	0	1	0
c	0	0	0	0	0
d	0	0	0	0	1
e	0	0	0	0	0

Or,
$a \to b \to d \to e$ and an additional node c

Is changed to:

	a	b	c	d	e
a	0	1	0	1	1
b	0	0	0	1	1
c	0	0	0	0	0
d	0	0	0	0	1
e	0	0	0	0	0

Closure of Relation, Cont.

Definition: The *closure* of relation R with respect to property P is the relation S that
(i) contains R,
(ii) has property P, and
(iii) is contained in *any* relation satisfying (i) and (ii).
That is, S is the "smallest" relation satisfying (i) and (ii). So we need to show:

Lemma: The *reflexive closure* of R is
$S = R \cup \{(a, a) \mid a \in A\}$

Lemma: The *symmetric closure* of R is $S = R \cup R^{-1}$.

Lemma: The *transitive closure* of a relation R is that set:
$S = \{(a, b) \mid \text{there is a path from } a \text{ to } b \text{ in } R\}$.

We may show that *any* relation satisfying (i) and (ii) will have at least the ones in our choice of closure matrix.

Computing Transitive Closure

Recall R^i, $i \geq 1$ implies there is a path of length i.

Transitive closure of R is $R \cup R^2 \cup R^3 \cdots$.

We only need the first n elements —

if there is a path from A to B, there is a path of length at most n from A to B.

Computing Transitive Closure, Cont.

Consider the shortest path from a to b (well ordering).
Suppose $k > n$ then some element of A appears twice in the path
(cut the loop) and contradict shortest property.

So we don't need infinitely many terms.
It is enough to take paths of length n, namely $R^1 \cup R^2 \cdots \cup R^n$.
In fact we may stop earlier.

Equivalence relations and partitions

Definition: An *equivalence relation* is a relation that is reflexive, symmetric and transitive.

"roommates", "married to", "on same Ethernet hub"

A *partition* of a set A is a collection of subsets $\{A_1, \cdots, A_k\}$ such that any two of them are disjoint (for any $i \neq j$, $A_i \cap A_j = \emptyset$) and such that their union is A.

That is, every element of A is in exactly one subset.

Fix an equivalence relation R on A.
For an element $a \in A$, let [a] denote the set $\{b \in A | a \sim_R b\}$.
We call this set the *equivalence class of* a *under R*. We call a a *representative* of [a].

Equivalence relations and partitions, Cont.

Lemma: The sets $[a]$ for $a \in A$ constitute a partition of A. That is, for every $a, b \in A$, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

$[a] \neq [b]$
Let $c \in [b] - [a]$ (or $c \in [a] - [b]$)
$[a] \cap [b] \neq \emptyset$
Let $d \in [a] \cap [b]$
We aim for a contradiction showing that $c \in [a]$
$a \sim_R d$, $d \sim_R b$, $b \sim_R c$
$d \sim_R c$
$a \sim_R d$ and $d \sim_R c$
$a \sim_R c$

Partitions, Integers modulo m

integers (positive, negative and 0)

Definition: If a and b are integers, then $a = b(mod\ m)$ if $m|(a-b)$.
or $a = b + km$ for some integer k.

Theorem:
Equality modulo m is an equivalence relation

Proof
reflexive: $m|(a-a) = 0$, so $a = a\ (mod\ m)$
symmetric: $a = b + km$ then $b = a + (-k)m$
transitive: $a = b + k_1 m$, $b = c + k_2 m$, so $a = c + k_2 m + k_1 m$

Fast Exponentiation

Lemma: If $a = x \pmod{m}$ and $b = y \pmod{m}$ then $(a+b) = (x+y) \pmod{m}$.
Proof: $m \mid (a-x)$ and $m \mid (b-y)$ so $m \mid ((a-x)+(b-y)) = (a+b)-(x+y)$,

The same fact can be proven for multiplication.

Lemma: If $a = x \pmod{m}$ and $b = y \pmod{m}$ then $(a \times b) = (x \times y) \pmod{m}$.

To compute mod b of x^a we may compute x^2 replace it with $y = x^2 (\text{mod } b)$. Then repeat the same, compute y^2 replace with $z = y^2(\text{ mod } b)$. Be careful, when a is odd...

Partial Orders

A type of binary relation (two elements).

A binary relation $R \subseteq A \times A$ is a **partial order** if it is reflexive, transitive, and antisymmetric.

reflexive: aRa
transitive: $aRb \wedge bRc \Rightarrow aRc$
antisymmetric: $aRb \wedge bRa \Rightarrow a = b$.
i.e., $\forall a \neq b, aRb \Rightarrow \neg bRa$.
Means NEVER symmetric!

Ordering relation (a before b then b cannot be before a).

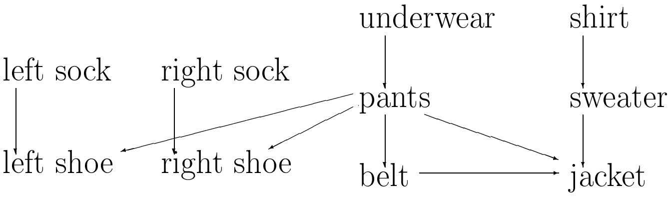
Definition: a set A together with a partial order $\preceq$ is called a **poset** $(A, \preceq)$.

Partial Orders

Examples of posets:
$A = N, R = \leq$, reflexive, transitive, antisymmetric
$A = N, R = \geq$, same.
$A = N, R = <$, NOT because not reflexive
$A = N, R = |$ (divides), easy to check reflexive, transitive, antisymmetric

Directed Acyclic Graph, DAG L5—P. 29

Task graph, A is a set of tasks.
aRb means "b cannot be done until a is finished".



We need to find the reflexive and transitive closure in order to have a partial order (resulting in "must be done before").

No cycles! no path that ends where it started. otherwise we cannot get dressed.

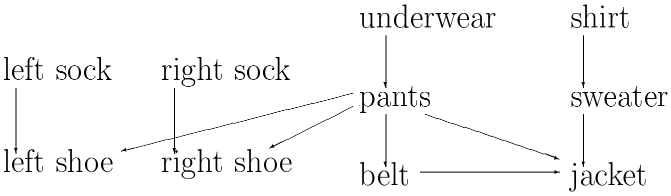
directed acyclic graph — directed graph with no cycles.

The transitive reflexive closure of a DAG is a partial order.

Hasse Diagrams L5—P. 30

Hasse diagram for a poset $(A, \preceq)$ is a graph:
- whose vertices are the elements of A,
- whose edges (arrows) represent pairs (a, b), where $a \preceq b$ but $a \neq b$,
- that contains no "transitive edges",
- for which all pairs in $\preceq$ are obtainable by transitivity from edges in the diagram.

(we need to remove the pants $\rightarrow$ jacket arrow).



Partial vs. Total Orders L5—P. 31

a and b are **incomparable** if neither $a \preceq b$ nor $b \preceq a$.

the shoes in our example

a and b are **comparable** if $a \preceq b$ or $b \preceq a$

A poset $(S, \preceq)$ is **totally ordered** if $(\forall a, b \in S)[a \preceq b \vee b \preceq a]$.

Examples:
$S = N, \preceq = \leq$
$S = N, \preceq = |$, NOT because neither $3|5$ nor $5|3$
$S = P(N), \preceq = \subseteq$, NOT because neither $\{3\} \subseteq \{5\}$ nor $\{5\} \subseteq \{3\}$
Lexicographic order on pairs of natural numbers, defined by:
$(a_1, a_2) \preceq (b_1, b_2)$ if and only if either $a_1 < b_1$, or else $a_1 = b_1$ and $a_2 \leq b_2$.

The Hasse diagram of a total order looks like a line.

Topological Sorting L5—P. 32

Definition: A **topological sort** of a finite poset $(A, \preceq)$ is a total ordering of all the elements of A, $a_1, a_2, \cdots, a_n$
in such a way that $\forall i < j$, either $a_i \prec a_j$ or a_i and a_j are incomparable in $(A, \preceq)$ (equivalently, it is not the case that $a_j \prec a_i$).

Lemma: Every *finite* poset $(A, \preceq)$ has a minimal element.

By induction on the number of elements.
$n = 1$ is clear.
Suppose it is true for all size-n posets.
Remove an element a from the $n + 1$ poset.
We still have a poset, use induction hypothesis to have the minimal element b.
If $a \not\preceq b$ then b is a minimal element of the poset.
Otherwise, a is the minimal element of the poset: assume that there is $c \preceq a$ then we have $c \preceq b$ which contradicts the choice of b.