Proof strategies

Constructing proofs is a learned skill. There is no mechanical method to tell you which proof method to use. But with practice, it will become easier to see your way. Here is how you might approach it:

- Write down an accurate statement of what you are trying to prove.
- Does forward reasoning work? Can you write a direct proof?
- Does the contrapositive give a better starting point?

- Backward reasoning: If you can't prove statement p, can you find a statement q so that you can prove q and $q \Longrightarrow p$?

- Would it help to break down the proof into cases? What are the relevant cases?

- Can you adapt a proof you have already seen?

- Proof/Disproof: Conjecture and proof.

- Proof/Disproof: Conjecture and counter-examples.

Example: Prove that the square of any integer has the form $4k$ or $4k+1$ for some integer k.

Proof. Suppose n is an integer. By the division algorithm, n can be written in one of the forms

$$4q \text{ or } 4q+1 \text{ or } 4q+2 \text{ or } 4q+3$$

for some integer q.

Case 1 ($n = 4q$): Since $n = 4q$
$n^2 = (4q)^2 = 16q^2 = 4(4q^2)$.
Let $k = 4q^2$. Then $n^2 = 4k$.

Case 2 ($n = 4q+1$): Since $n = 4q+1$
$n^2 = (4q+1)^2 = 16q^2 + 8q + 1 = 4(4q^2 + 2q) + 1$.
Let $k = 4q^2 + 2q$. Then $n = 4k + 1$.

Case 3 $(n = 4q + 2)$: Since $n = 4q + 2$
$n^2 = (4q + 2)^2 = 16q^2 + 16q + 4 = 4(4q^2 + 4q + 1)$.
Let $k = 4q^2 + 4q + 1$. Then $n = 4k$.

Case 4 $(n = 4q + 3)$: Since $n = 4q + 3$
$n^2 = (4q + 3)^2 = 16q^2 + 24q + 9 = 4(4q^2 + 6q + 2) + 1$.
Let $k = 4q^2 + 6q + 2$. Then $n = 4k + 1$.

In each case, we have shown that there is an integer k such that $n = 4k$ or $n = 4k + 1$ as desired.

Theorem: *There is no integer $n > 3$ such that n,$n+2$ and $n+4$ are all prime numbers.*

Proof (by contradiction). Assume n, $n+2$ and $n+4$ are primes > 3. If n is prime and $n > 3$ then $n \bmod 3 = 1$ or $n \bmod 3 = 2$.

If $n \bmod 3 = 1$ then $(n+2) \bmod 3 = 0$ and $n+2 > 3$ is not a prime, a contradiction.

If $n \bmod 3 = 2$ then $(n+4) \bmod 3 = 0$ and $n+4 > 3$ is not a prime, a contradiction.

Theorem
There are infinitely many primes.

Assume that there are only finitely many primes, i.e. there is an integer n such that the prime numbers are the set $\{p_1, p_2, p_3, \ldots, p_n\}$

Assume without loss of generality that p_n is the largest among them.

$\Longrightarrow$ If m is an integer and $m > p_n$ then m must be a composite number.

$\Longrightarrow$ If m is an integer and $m > p_n$ then there exists i, $1 \leq i \leq n$ such that p_i divides m.

Consider the integer $(p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n) + 1$

$(p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n) + 1$ is greater that p_n, so it should be divisible by at least one of the primes.

However, none of p_i, $1 \leq i \leq n$ divides it, since $(p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n) + 1 \bmod p_i = 1$.
A contradiction.

Thus, the assumption of having finitely many primes is false.

Conclusion: There are infinitely many prime numbers. (Book 9 of Euclid)

Proof by Mathematical Induction

Mathematical induction is a proof technique that is used to prove a property of a set of positive integers.

General example:

$P(n)$ is true for all integers $n \geq c$.

Specific examples:

Show that $2^n > n^2$ for all integers $n > 4$.

Show that $1 + 2 + 3 + \cdots + n = n(n + 1)/2$
for all integers $n \geq 1$

Mathematical induction has great applicability in computer science and can be used to prove:

- Properties of strings (induction on the lengths of strings).
- Correctness of computer programs (induction on the number of steps in a program, number of iterations of a loop).
- Theorems about graphs and trees.
- Theorems about the complexity of algorithms.

To show that

$P(n)$ is true for all integers $n \geq c$,

we do the following steps

1. Basis step Show that $P(c)$ is true (where c is the smallest element).

2. Inductive step Show that $P(n) \rightarrow P(n+1)$. is true for all $n \geq c$, i.e.
   show that $P(n) \Longrightarrow P(n+1)$. (Assume $P(n)$ is true and show that $P(n+1)$ is true.)

A proof by mathematical induction **follows a fixed pattern**.

Theorem: *For any positive integer n, when $a \neq 1$,*
$1 + a + a^2 + a^3 + \ldots + a^n = \frac{a^{n+1}-1}{a-1}$.

Proof.

Basis Step: $n = 1$

lhs: $1 + a$

rhs: $\frac{a^2-1}{a-1} = \frac{(a-1)(a+1)}{a-1} = a + 1$

So it is true for $n = 1$.

Inductive Step:

Assume that for some integer n,
$1 + a + a^2 + a^3 + \ldots + a^n = \frac{a^{n+1}-1}{a-1}$

We have to show that
$1 + a + a^2 + a^3 + \ldots + a^n + a^{n+1} = \frac{a^{n+2}-1}{a-1}$

$1 + a + a^2 + a^3 + \ldots + a^n + a^{n+1}$
$= \frac{a^{n+1}-1}{a-1} + a^{n+1}$
$= \frac{a^{n+1}-1+a \cdot a^{n+1}-a^{n+1}}{a-1}$
$= \frac{a^{n+2}-1}{a-1}$

Thus, the formula is valid for $n+1$. By mathematical induction, the formula is valid for every integer $n \geq 1$.

Theorem: *6 divides* $n^3 - n$ *for any integer* $n \geq 1$.

Proof.

Basis Step: $n = 1$

For $n = 1$, $n^3 - n = 1 - 1 = 0$ and $6|0$

Inductive Step:

Assume that for some integer n,

6 divides $n^3 - n$, i.e. $n^3 - n = 6i$ for some integer i.

We have to show that

6 divides $(n+1)^3 - (n+1)$.

$(n+1)^3 - (n+1)$
$= n^3 + 3n^2 + 3n + 1 - n - 1$
$= (n^3 - n) + 3(n^2 + n)$
$= (n^3 - n) + 3 \cdot n \cdot (n+1)$

Now, $(n^3 - n)$ is divisible by 6, and
$3 \cdot n \cdot (n+1)$ is divisible by 3 and also by 2, since one of n, $n+1$ must be even.
If $6|a$ and $6|b$ then $6|(a+b)$.
Thus $6|((n+1)^3 - (n+1))$.

Problem: *Show that* $2^n > n^2$ *for any integer* $n > 4$.

Proof.
<u>Basis Step</u>: $n = 5$
$2^5 = 32 > 25 = 5^2$

<u>Inductive Step</u>: Assume that $2^n > n^2$ for some integer n.
We have to show that $2^{n+1} > (n+1)^2$

$(n+1)^2 = n^2 + 2n + 1$
$< n^2 + 2n + n$
$= n^2 + 3n$
$< n^2 + n \cdot n$
$= n^2 + n^2$
$< 2^n + 2^n$
$= 2^{n+1}$
Thus, the inequality is valid for $n + 1$.

Problem: *Show that for any integer* $n > 1$

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n}$$

Proof.

Basis Step: $n = 2$

$1 + \frac{1}{4} = \frac{5}{4} < \frac{6}{4} = 2 - \frac{1}{2}$

Inductive Step:

Assume that for some n,

$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n}$

We have to show that

$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} < 2 - \frac{1}{n+1}$

$lhs = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} <$

$2 - \frac{1}{n} + \frac{1}{(n+1)^2} = \frac{2n(n+1)^2 - (n+1)^2 + n}{n(n+1)^2}$

$= \frac{2n^3 + 4n^2 + 2n - n^2 - 2n - 1 + n}{n(n+1)^2} = \frac{2n^3 + 3n^2 + n - 1}{n(n+1)^2}$

The right-hand side of the inequality is

$2 - \frac{1}{n+1} = \frac{2n+2-1}{n+1} = \frac{2n^2+n}{n(n+1)}$

$= \frac{2n^3 + 3n^2 + n}{n(n+1)^2}$

Thus,
$lhs < \frac{2n^3+3n^2+n-1}{n(n+1)^2} < \frac{2n^3+3n^2+n}{n(n+1)^2} = 2 - \frac{1}{n+1}$

Therefore the inequality is valid for $n + 1$.

We are to show
$P(n)$ is true for any integer $n \geq c$.

In some cases, we cannot prove the validity of $P(n+1)$ from the validity of $P(n)$. But we could prove the validity of $P(n+1)$ from the validity of $P(n) \wedge P(n-1) \wedge P(n-2) \wedge \cdots \wedge P(c)$.

We need to use a

generalized form of induction

Strong Mathematical Induction

(also called generalized induction)

1. Basis step: Show that $P(c)$ is true (where c is the smallest element).

2. Inductive step: Show that $P(c) \wedge P(c+1) \wedge \cdots \wedge P(n) \Longrightarrow P(n+1)$ if $n \geq c$.

   Assume $P(c) \wedge P(c+1) \wedge P(c+2) \wedge \cdots \wedge P(n)$ is true and show that $P(n+1)$ is true.

Example: Show that for every integer $n \geq 2$,
n is a prime or a product of primes.

Basis step: $n = 2$ is a prime.
Inductive step: Assume that for some integer n, every integer i, $2 \leq i \leq n$ is either a prime or $i = p_1 \cdot p_2 \cdots p_{m_i}$ where p_k is a prime for $1 \leq k \leq m_i$.

Consider $n + 1$. If $n + 1$ is a prime than we are done.
If $n + 1$ is not a prime than $n + 1 = a \cdot b$ where $2 \leq a \leq n$ and $2 \leq b \leq n$.

By the hypothesis, either a is a prime or $a = p_1 \cdot p_2 \cdots p_{m_a}$
and either b is a prime or $b = q_1 \cdot q_2 \cdots q_{m_b}$
where all $p_1, p_2, \ldots$ and $q_1, q_2, \ldots$ are primes.

Since $n + 1 = a \cdot b$, in all cases, $n + 1$ is a product of primes.

Theorem: Show that the number of subsets of an n-element set is 2^n.

Proof:

Basis: The statement is true for $n = 0$, since the empty set (the only set with 0 elements) has exactly $2^0 = 1$ subset, namely, itself.

Inductive step: Assume that every set with n elements has exactly 2^n subsets. Let T be a set with $n + 1$ elements. Then it is possible to write $T = S \cup \{a\}$ where $a \in T$ and $a \notin S$.

For each subset X of S there are exactly two subsets of T: X itself, and $X \cup \{a\}$. These constitute all the subsets of T and are all distinct. Since there are 2^n subsets of S, there are $2(2^n) = 2^{n+1}$ subsets of T. This finishes the proof.

Recursive Definitions

Sometimes it is not easy to find a direct definition of a function $f(n)$, i.e., to give an explicit formula for $f(n)$.

However, it may be possible to define $f(n)$ by:

(1) giving an explicit definition of $f(n)$ for small values of n, and
(2) for any other value of n, specifying $f(n)$ in terms of some $f(m)$ for m smaller than n.

A definition in the style of (1) and (2) is called a **recursive definition**.

Example: The rabbit problem

Rabbits follow the following law of breeding:

Every pair of rabbits at least two months old will produce one pair of rabbits as offspring every month.

Question: If we start with a pair of newly born rabbits, how many pairs of rabbits will we have after n months?

Find a function $f(n)$ that gives the number of pairs of rabbits that we will have after n months.

Rules:

$f(0) = 0$
$f(1) = 1$

For $n > 2$

Every pair that is alive in month $n - 1$ is still there in month n.

Every pair that is alive in the month $n-2$ will produce one more pair for the month n, $n \geq 2$.

$f(n) = f(n-1) + f(n-2)$ for $n \geq 2$

$f(0) = 0,\ f(1) = 1$
$f(n) = f(n-1) + f(n-2)$ for $n \geq 2$

is an example of a recursive definition of a function $f(n)$.

The sequence of numbers generated by the function f

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$

is called the *Fibonacci sequence*.

It represents population growth in many situations.

A *recursive definition* is also called an *inductive definition*.

Any function can be defined using recursion:

Examples:

$fac(n) = n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1) \cdot n$

Recursive definition of $fac(n)$:
$fac(0) = 1$
$fac(n) = n \cdot fac(n-1)$ for $n \geq 1$

$add(m, n) = m + n$

Recursive definition of $add(m, n)$:
$add(m, 0) = m$
$add(m, n) = 1 + add(m, n-1)$ for $n \geq 1$

Sets can be defined recursively.

The set of all correctly written logical formulae called *well-formed formulae (wff)* can be defined as follows:

(1) **F**, **T**, and simple logical variables like p, q, r, etc. are well-formed formulae.

(2) If a and b are well-formed formulae then $(\neg a)$, $(a \vee b)$, $(a \wedge b)$, $(a \rightarrow b)$, $(a \leftrightarrow b)$ are well-formed formulae.

This formulation can be used to

(1) construct well-formed formulae,

(2) check the correctness of a given formula.

We will use recursive definitions on several occasions.

Recursive functions and recursive definitions of objects are important in software development.

Recursion is used to write software components that are

- concise,
- easy to verify.

Induction is generally a good proof technique to prove the correctness of recursive functions, formulae etc.

Problem: Suppose $b_1, b_2, \ldots$ is a sequence defined as follows:

$$b_1 = 4, b_2 = 12$$

$$b_k = b_{k-1} + b_{k-2} \text{ for all integers } k \geq 3$$

Prove that $4|b_n$ for all integers $n \geq 1$.

Proof.

Basis step: $4|4$ and $4|12$, so $4|b_1$ and $4|b_2$.

Inductive step: Suppose $4|b_i$ for all i such that $1 \leq i < n$ where $n > 2$. We want to show that $4|b_n$.

By the inductive hypothesis, $4|b_{n-1}$ and $4|b_{n-2}$
$\implies 4|(b_{n-1} + b_{n-2})$
$\implies 4|b_n$ since $b_n = b_{n-1} + b_{n-2}$.

By mathematical induction, $4|b_n$ for all positive integers n.

Example: Prove that $\forall n \in Z^+$, $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$ (where f_i is the i^{th} Fibonacci number).

Proof. We will prove the result by induction on n.
Basis: $n = 1$. Then LHS $= f_2 f_0 - f_1^2 = 0 - 1 = (-1)^1 =$ RHS
Inductive step: Assume that for some $n \in Z^+$
$f_{n+1}f_{n-1} - f_n^2 = (-1)^n$.
We have to prove that $f_{n+2}f_n - f_{n+1}^2 = (-1)^{n+1}$.

$$\begin{aligned}
&f_{n+2}f_n - f_{n+1}^2\\
&= (f_{n+1} + f_n)f_n - f_{n+1}(f_n + f_{n-1})\\
&= f_{n+1}f_n + f_n^2 - f_{n+1}f_n - f_{n+1}f_{n-1}\\
&= -(f_{n+1}f_{n-1} - f_n^2)\\
&= -1(-1)^n = -1^{n+1}
\end{aligned}$$

The result is proved by mathematical induction.

Relations

A function

$$f: \ A \rightarrow B$$

assigns to
each element of A **one** element of B.

This definition restricts what a function can express. For example, it cannot express an assignment in which:

(1) an element of A is not assigned any element of B,

(2) an element of A is assigned more than one element of B.

Example:

We have a student database where we want to store, for every student, the courses the student is taking this term.

This assignment **Registered** cannot be a function from the set of students to the set of courses since:

(1) some students are not taking any courses this term.

(2) some students are taking more than one course this term.

This type of assignment occurs often in computer applications.

Thus, we need something that generalizes the concept of a function.

A function

$$f: \; A \to B$$

can be seen as a set of ordered pairs

$$\{(x, f(x)) \,|\, x \in A \text{ and } f(x) \in B\}$$

Thus, a function is a subset of $A \times B$, however not every subset of $A \times B$ is a function.

We define a binary **relation** from A to B as a generalization of a function.

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

If R is a relation from A to B then for a pair (a, b) in the relation R we write

$(a, b) \in R$ or $a\ R\ b$

(read it as: a is related to b by relation R)

If $A = B$ we say that R is a relation **on** A.

Example 1

S ... the set of students at Concordia.

C ... the set of courses at Concordia

Let $Registered$ be the relation containing all pairs (s, c) such that the student s is registered in the course c this term.

$Registered$ consists of pairs like

$(Smith, comp238)$
$(Smith, math244)$
$(Tremblay, comp238)$
$(Tremblay, comp228)$
$(Nguyen, elec232)$
....

Example 2: Let A be the set of countries in the world, and let *is-neighbor-of* be the relation defined as:

a *is-neighbor-of* b whenever the countries a and b share a common border.

The following pairs are members of the relation *is-neighbor-of*:

(USA, Mexico) $\in$ *is-neighbor-of*
(France, Germany) $\in$ *is-neighbor-of*
(Russia, China) $\in$ *is-neighbor-of*
(Iran, Turkey) $\in$ *is-neighbor-of*
(Argentina, Uruguay) $\in$ *is-neighbor-of*

Some relations that you already know

L and G are relations on real numbers.

$L = \{(a, b) \mid a < b\}$

$2 < 3.4$, so $(2, 3.4) \in L$
$2 < 13$, so $(2, 13) \in L$
$2 < 209$ so $(2, 209) \in L$
$5 < 6$ so $(5, 6) \in L$

$13 \not< 2$ so $(13, 2) \notin L$

$G = \{(a, b) \mid a > b\}$

$5 > 2$ so $(5, 2) \in G$
$5 > -2$ so $(5, -2) \in G$
$5 \not> 20$ so $(5, 20) \notin G$

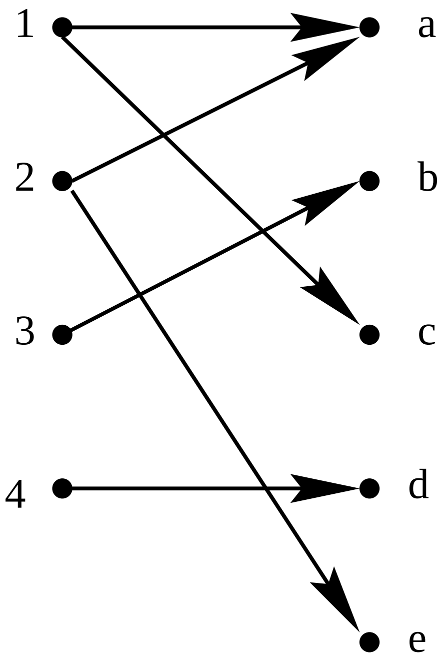
Graph of a relation

Let R be a relation from $A = \{1, 2, 3, 4\}$ to set $B = \{a, b, c, d, e\}$ consisting of the following pairs:

$R = \{(1, a), (1, c), (2, a), (2, e), (3, b), (4, d)\}$

If A and B are finite, we can represent the relation R by a graph or a table.

R:



	a	b	c	d	e
1	×		×		
2	×				×
3		×			
4				×	

Representing Relations using Graphs

A relation R **on** a set A is represented by a graph that has

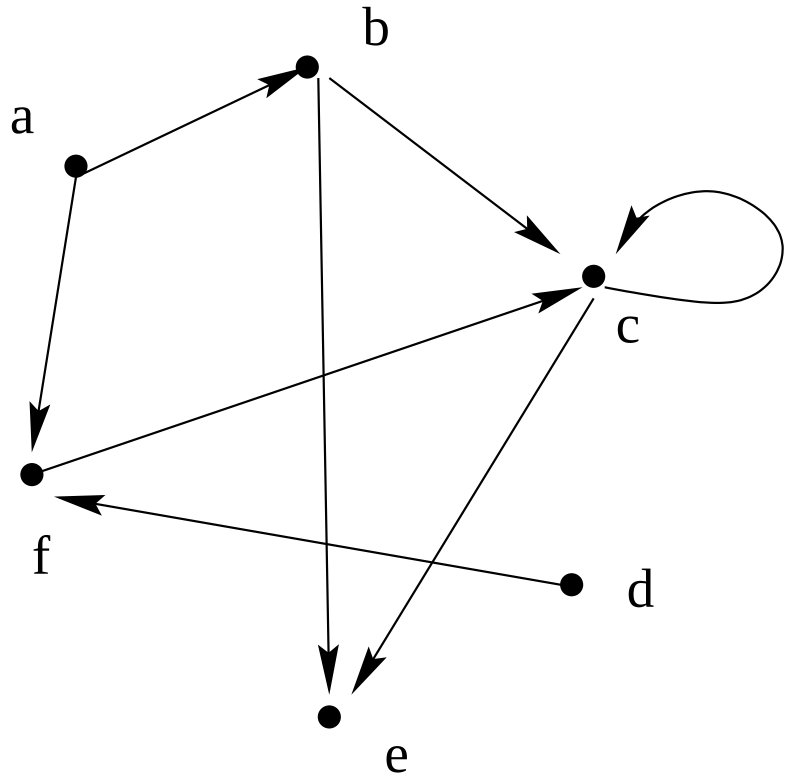
- one point (*node*) for each element of A and

- an arc (*edge/link*) from node a to node b whenever $(a, b) \in R$.

Example

$A = \{a, b, c, d, e, f\}$

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



Representing Relations using Matrices

A relation R from a finite set A to a finite set B can be represented by a matrix.

If $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ we can represent R by an $m \times n$ matrix.

$\boldsymbol{M}_R = [m_{i,j}]$

such that $m_{i,j} = \begin{cases} 1 & \text{if } (a_i, b_j) \text{ is in } R \\ 0 & \text{if } (a_i, b_j) \text{ is not in } R \end{cases}$

Example: For the relation R from A to B where $A = \{a, b, c, d\}$ and $B = \{1, 2, 3, 4, 5, 6\}$.
$R = \{(a, 2), (a, 6), (b, 5), (b, 3), (c, 3), (c, 5), (d, 6)\}$

$$\boldsymbol{M}_R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Properties of Relations on a Set

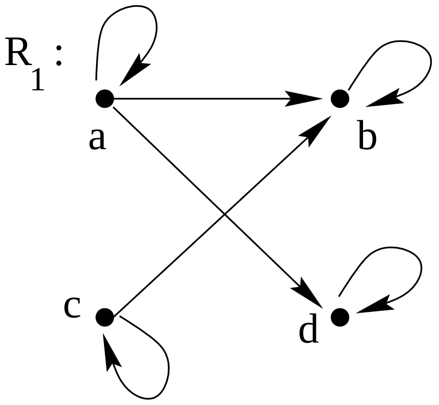
Let R be a relation on a set A.

Definition
A relation is **reflexive** if every element of A is related to itself.

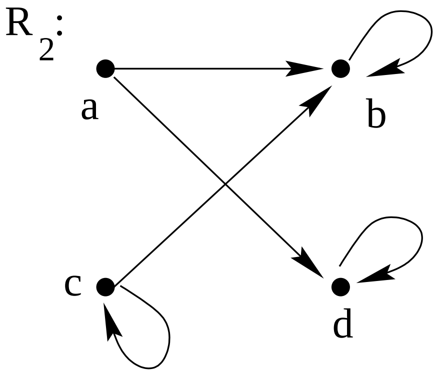
$$\forall a\ [(a,a) \in R]$$

$\leq$ is a reflexive relation on Z since $a \leq a$ for every $a \in Z$.

is-a-parent-of is not a reflexive relation.



a reflexive relation



not a reflexive relation

If R is a reflexive relation then its matrix representation M_R must contain 1 all along the main diagonal.

$$\boldsymbol{M}_R = \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & . & & & & \\ & & & . & & & \\ & & & & . & & \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix}$$

Entries outside the main diagonal are 0 or 1.

Definition

A relation is **symmetric** if $(b, a) \in R$ whenever $(a, b) \in R$

$$\forall a\, \forall b\, [((a, b) \in R) \leftrightarrow ((b, a) \in R)]$$

---

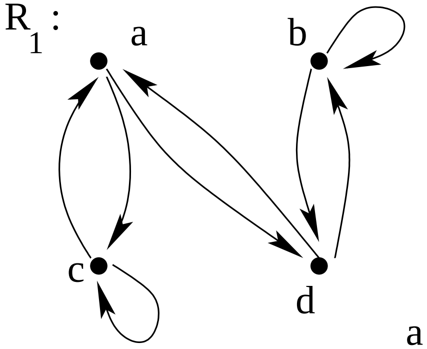
is-a-sibling-of is a symmetric relation.

is-a-parent-of is not a symmetric relation.

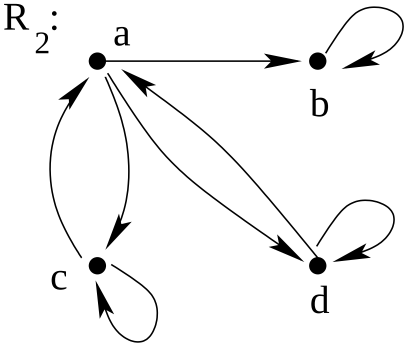
$=$ is a symmetric relation on integers.

$\leq$ is not a symmetric relation on the set of reals.

Graph Representation:



a symmetric relation



not a symmetric relation

If R is a symmetric relation then its matrix representation M_R is a symmetric matrix.

A matrix is symmetric if for any i,
row i of the matrix is the same as column i .

Example of a symmetric matrix:

$$\boldsymbol{M}_R = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Definition

A relation is **antisymmetric** when

$(b, a) \in R$ and $a \neq b$ implies that $(a, b) \notin R$

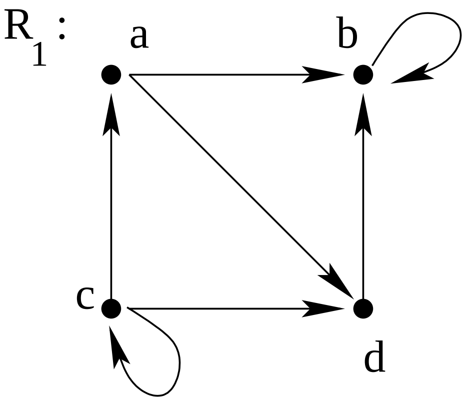
$$\forall a\, \forall b\, [(((a, b) \in R) \wedge (a \neq b)) \rightarrow ((b, a) \notin R)]$$

---

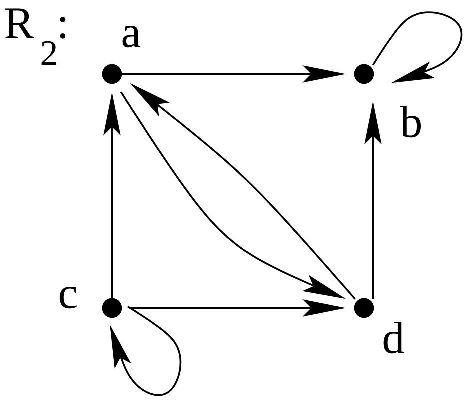
is-a-parent-of is an antisymmetric relation.

is-a-sibling-of is not antisymmetric.

$\leq$ on integers is an antisymmetric relation.



an antisymmetric relation



not an antisymmetric relation

(not a symmetric relation)

If R is an antisymmetric relation then its matrix representation M_R satisfies the following:

If $i \neq j$ and $M_R[i,j] = 1$ then $M_R[j,i] = 0$.

Example of a matrix of an antisymmetric relation:

$$\boldsymbol{M}_R = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

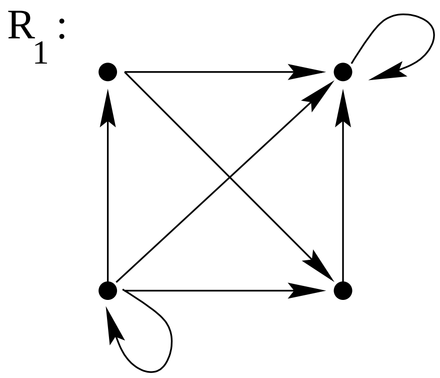
Definition

A relation is **transitive** if $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$.

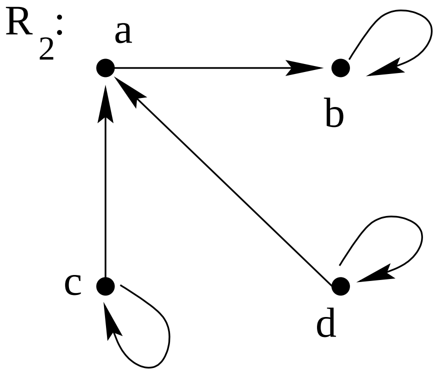
$$\forall a\, \forall b\, \forall c\, [((a, b) \in R \wedge (b, c) \in R) \rightarrow ((a, c) \in R)]$$

---

is-an-ancestor-of is transitive.
is-a-parent-of is not a transitive relation.
$\leq$ is a transitive relation on integers.
The divisibility D relation on N, where
$(a, b) \in D$ if $a|b$, is transitive.



a transitive relation



not a transitive relation

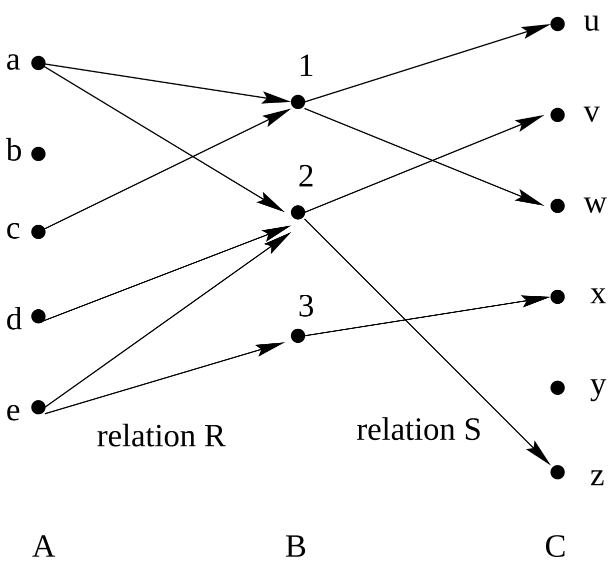
There is no simple way of determining whether a relation is transitive from its matrix or graph representation.

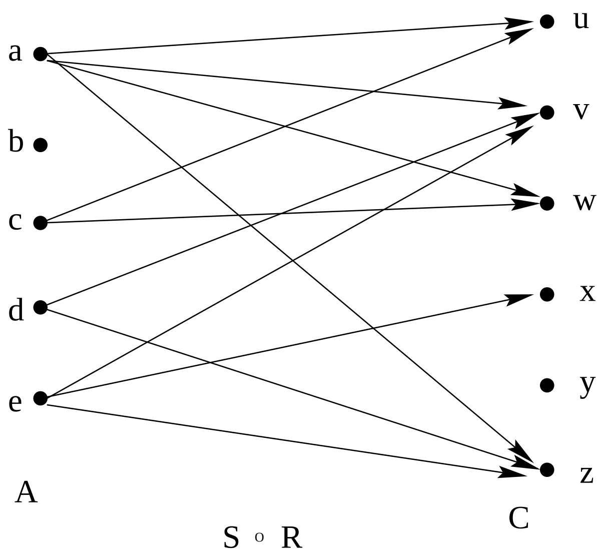
Combining relations

Relations from A to B are subsets of $A \times B$.

Thus, any two relations R_1, R_2 from A to B are sets and they can be combined using set operations, such as union, intersection, and difference.
Just as we defined composition of functions, we can define composition of relations:

Definition
Let R be a relation from A to B and S be a relation from B to C. The **composite** $S \circ R$ of R and S is the relation from A to C consisting of $\{(a, c) \,:\, (a \in A), (c \in C)\}$ for which there exists an element $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S\}$.
Note that $S \circ R$ means first R then S.


a
b
c
d
e
1
2
3
u
v
w
x
y
z
relation R
relation S
A
B
C


a
b
c
d
e
u
v
w
x
y
z
A
C
S ∘ R

Notice that, in general, the composition of relations is not commutative.

Relation $S \circ R$ may exist and $R \circ S$ does not need to exist, or they can be different.

Example:
Reg is a relation from the set of students to the set of courses, $Exam\_dates$ is a relation from the set of courses to the set of exam dates.

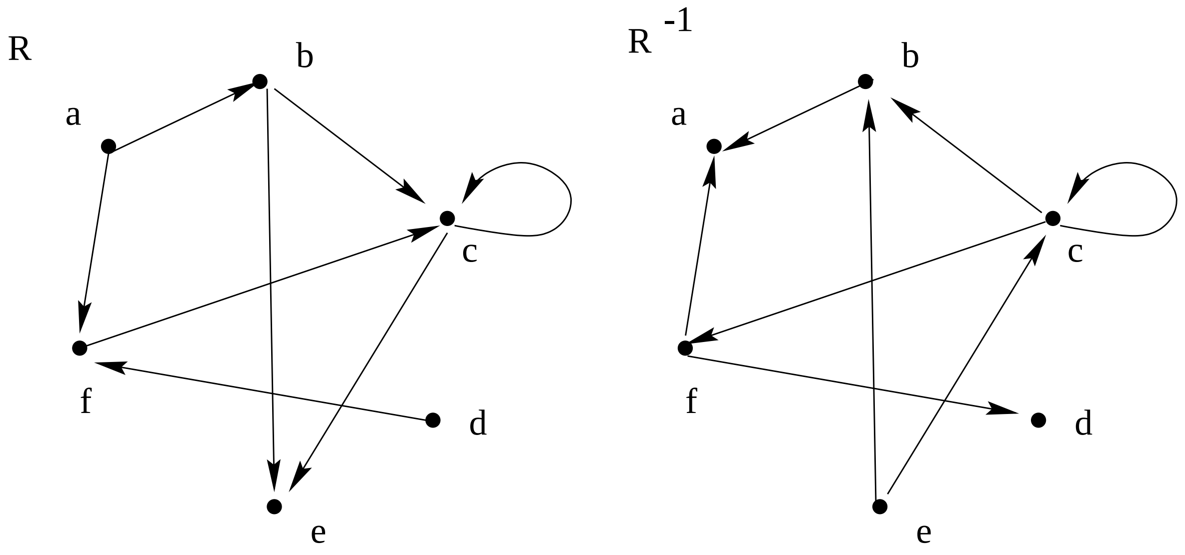
$Exam\_dates \circ Reg$ exists and relates each student to his/her exam dates.

$Reg \circ Exam\_dates$ does not exist.

Inverse of a relation

Define the **inverse** of R to be $R^{-1} = \{(b, a) \mid (a, b) \in R\}$.

Example



$M_{R^{-1}}$ is obtained from M_R by the transposition $M_{R^{-1}} = (M_R)^t$

Relation operations using matrices

$$M_{R\cup S} = M_R \vee M_S$$

$$M_{R\cap S} = M_R \wedge M_S$$

where

$1 \vee 1 = 1$ and $1 \vee 0 = 0 \vee 1 = 1$, $0 \vee 0 = 0$

and

$1 \wedge 1 = 1$ and $1 \wedge 0 = 0 \wedge 1 = 0 \vee 0 = 0$

$$M_{S \circ R} = M_R \odot M_S$$

where $\odot$ represents a 'boolean' product of the two matrices, which can be obtained by finding the ordinary product of matrices and replacing any nonzero entry by 1.
(Also called the **skeleton** of the matrix).

$$\boldsymbol{M}_R = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$\boldsymbol{M}_S = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$\boldsymbol{M}_{S\circ R} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

For a relation R from A to A, we define R^2 to be $R \circ R$, and R^3 to be $R \circ R \circ R$ and so on.

R^n can be defined recursively as follows:

$$R^1 = R$$

$$R^n = R^{n-1} \circ R \text{ for } n > 1$$

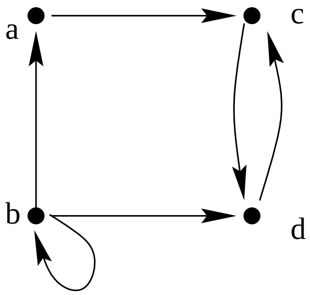
$a\ R^n\ b$ iff in the graph of R there is a possibility to go from a to b by a sequence of n arcs.

(We say that there is a **path** of length n from a to b in R). xs

Theorem

A relation R is transitive if and only if $R^n \subseteq R$ for all $n \geq 1$.

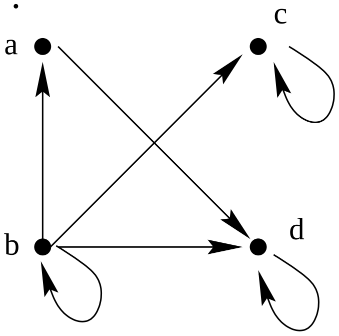
R :



M_R :

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

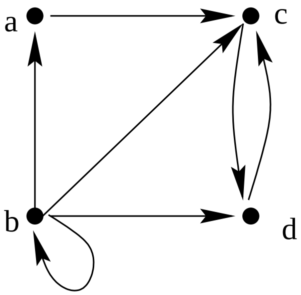
$R^2 = R \circ R$:



M_{R^2} :

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$R^3 = R \circ R \circ R$:



M_{R^3} :

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Closures of Relations

Let R be a relation **on** a set A.

R may or may not be reflexive, but we may need to obtain a relation Q that

- contains R,
- is reflexive,
- is the smallest relation that contains R and is reflexive.

Q is called the **reflexive closure** of R.

Let R be a relation **on** a set A.

The **reflexive closure** of R is the smallest relation that contains R and is reflexive.

The **symmetric closure** of R is the smallest relation that contains R and is symmetric.

The **transitive closure** of R is the smallest relation that contains R and is transitive.

Reflexive closure

Add to R all pairs relating an element to itself.
Define the diagonal relation on A as $\Delta = \{(a,a) \mid a \in A\}$

The reflexive closure of R is equal to $R \cup \Delta$

$$M_{R \cup \Delta} = M_R \vee \left[\begin{array}{ccccc} 1 & 0 & .. & & 0 \\ 0 & 1 & 0 & .. & 0 \\ 0 & 0 & 1 & 0.. & 0 \\ .... & & & & \\ 0 & 0 & .. & 0 & 1 \end{array} \right]$$

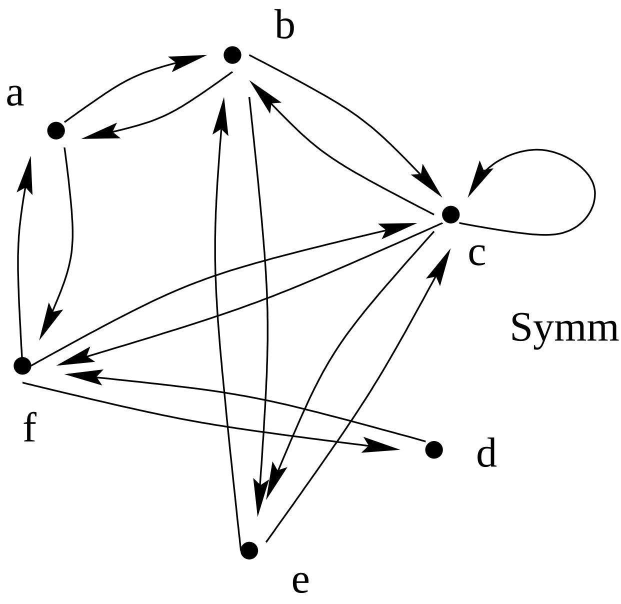
i.e., to get the matrix representation of the reflexive closure of R, take M_R and make all diagonal entries equal to 1. All other entries are unchanged.

Symmetric closure

To obtain the symmetric closure of R, for every pair $(a, b) \in R$, add the pair (b, a).

We can use the inverse of R to obtain the symmetric closure. The symmetric closure of R is equal to

$$R \cup R^{-1}$$



Symmetric closure of R

The matrix of the symmetric closure of R is equal to

$$M_R \vee (M_R)^t$$

The **connectivity relation** R^* of R consists of all pairs (a, b) such that there is a path from a to b in R.

$$R^* = R \cup R^2 \cup R^3 \cdots = \bigcup_{i=1}^{\infty} R^i$$

Example Let P be the relation where $a\ P\ \ b$ if a is a parent of b.

We define P^* in the following way:
$a\, P^*\, b$ if a is an ancestor of b.

Finding the transitive closure of a relation:

Theorem The **transitive closure** of R is equal to R^*.

Theorem

If R is a relation on a finite set A of cardinality n then

$$R^* = R \cup R^2 \cup R^3 \cup \cdots \cup R^n = \bigcup_{i=1}^{n} R^n$$

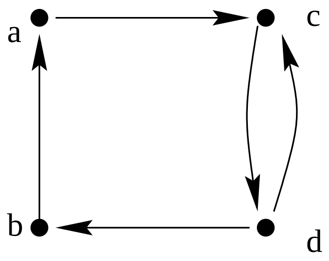
<u>Proof</u>

Consider the connectivity relation R^*.

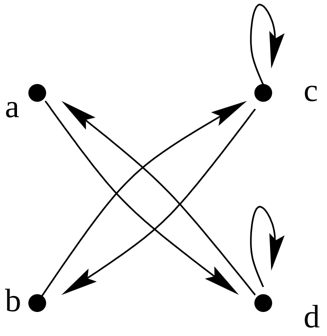
In a graph representation of R, if we can reach point b from point a, we can reach it by a path of length at most n:

Take the shortest path from a to b in the graph of R. If the path contains i arcs, $i \leq n$ then the pair (a, b) is in R^i and thus also in R^*. If the path contains j arcs, $j > n$ then the path must pass through some point twice and it is not the shortest path.

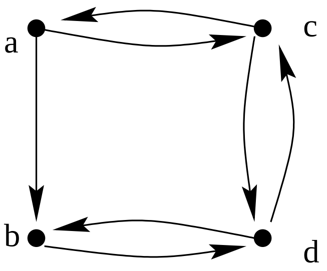
R_1:



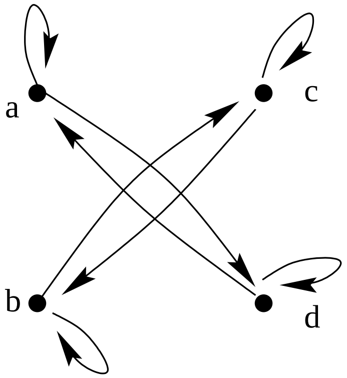
R_1^2:



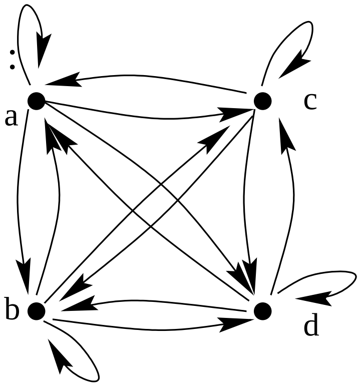
R_1^3:

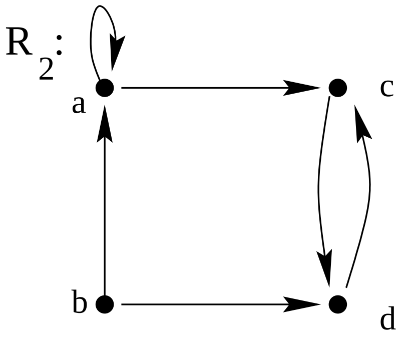


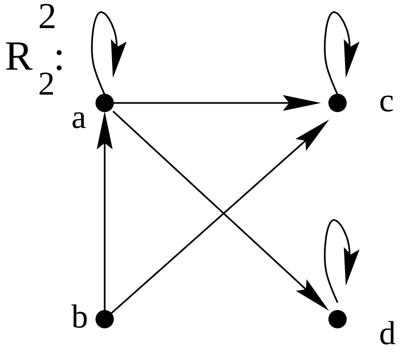
R_1^4:

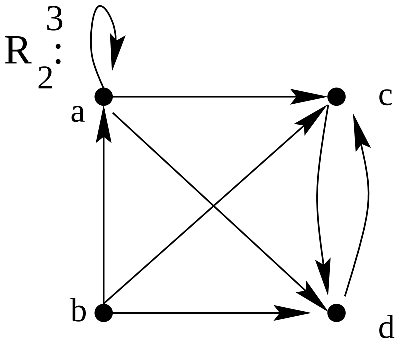


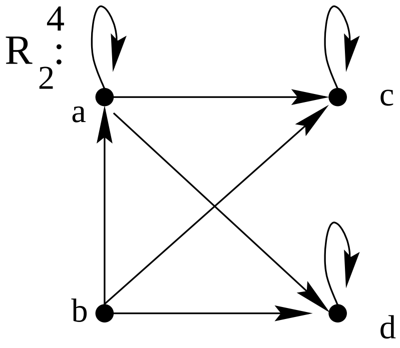
R_1^* :

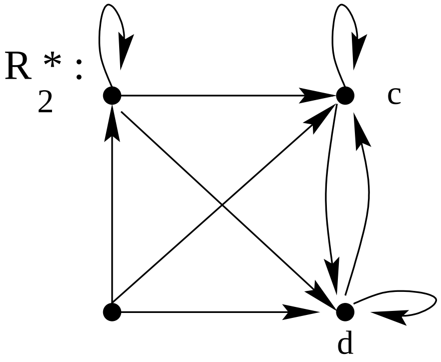



R_2:
a
c
b
d


R_2^2:
a
c
b
d


R_2^3:
a
c
b
d


R_2^4:
a
c
b
d


R_2^*:
c
d

Equivalence relation

Definition A relation on a set A is an **equivalence relation** if it is reflexive, symmetric and transitive.

Example 1 Let S be a relation on people such that
$a\,S\,b$ if a and b have the same parents.

Example 2 Let M be a relation on integers such that
$(i, j) \in M$ if $i \equiv j (\text{mod } 5)$

$(0, 0) \in M$, $(0, 5) \in M$, $(5, 0) \in M$, $(0, 10) \in M$
$(1, 1) \in M$, $(1, 6) \in M$, $(6, 1) \in M$, $(1, 11) \in M$
$(2, 2) \in M$, $(2, 7) \in M$, $(7, 2) \in M$, $(2, 12) \in M$
$(3, 3) \in M$, $(3, 8) \in M$, $(8, 3) \in M$, $(3, 13) \in M$
$(4, 4) \in M$, $(4, 9) \in M$, $(9, 4) \in M$, $(4, 14) \in M$

$a, b \in \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\} \Longrightarrow aMb$

Similarly:

$a, b \in \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\} \Longrightarrow aMb$

$a, b \in \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\} \Longrightarrow aMb$

$a, b \in \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\} \Longrightarrow aMb$

$a, b \in \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\} \Longrightarrow aMb$

where $i \, M \, j$ if $i \equiv j \pmod 5$

Equivalence Classes

Definition
Let R be an equivalence relation on a set A. For any a in A, the set of all elements related to a by R is called the **equivalence class** of a.

We denote the equivalence class of a by $[a]_R$

$[a]_R = \{b \mid (a, b) \in R\}$,
the set of all elements related to a by R.

A **representative** of an equivalence class is any element a in that class.

Example:

$[0]_M = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}$
$[1]_M = \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\}$
$[2]_M = \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}$
$[3]_M = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$
$[4]_M = \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}$

$[0]_M = [5]_M = [-10]_M,\ [0]_M \cap [1]_M = \varnothing$

Theorem Let R be an equivalence relation. The following statements have the same truth values:

1. $a\,R\,b$
2. $[a]_R = [b]_R$
3. $[a]_R \cap [b]_R \neq \varnothing$

So any two classes of an equivalence relation are either the **same** or **disjoint**.

Theorem Let R be an equivalence relation on set A. The distinct equivalence classes of R form a partition of A.
Conversely, given a partition $A_1, A_2, \ldots, A_n$ of A, there is an equivalence relation R that has $A_1, A_2, \ldots, A_n$ as its equivalence classes.

Partial Orderings

A generalization of the relation $\leq$ on numbers.

Recall that $\leq$ is a reflexive, antisymmetric and transitive relation.

Definition
A relation on a set A is a **partial ordering** if it is reflexive, antisymmetric and transitive.

Example 1
The operation $\subseteq$ is a partial ordering on a set of subsets.

Definition
The pair (A, R) is called a **partially ordered set** or **poset** when A is a set and R is a partial ordering on A.

In a poset (A, R), if $(a, b) \in R$ we write

$$a \preceq b \text{ (or } b \succeq a)$$

We say a is "less than or equal to" b even if A is not a set of numbers.

If $a \preceq b$ or $b \preceq a$ then a and b are **comparable**.

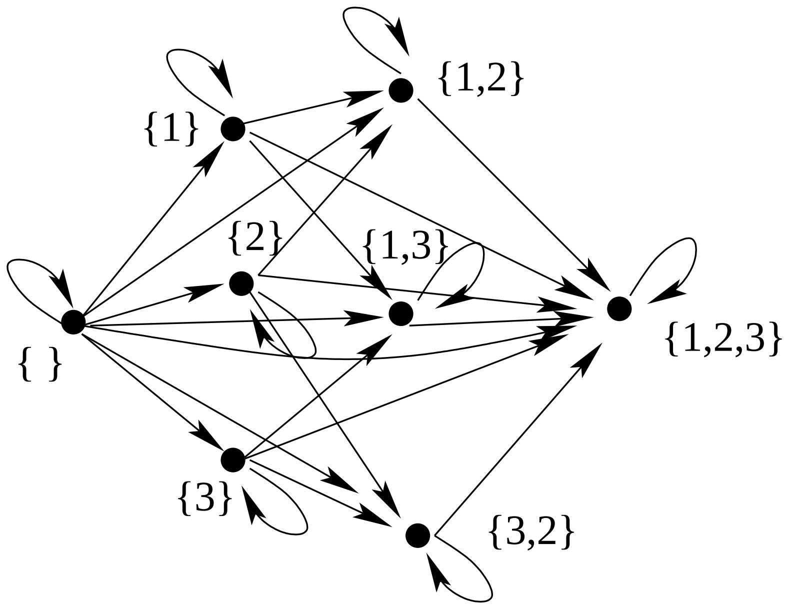
In a poset, there might be elements a and b such that $a \not\preceq b$ and $b \not\preceq a$.
We call such elements **incomparable**.

Definition
Let $(A, \preceq)$ be a poset. If every pair of elements in A is comparable then A is called a **totally ordered set** and $\preceq$ is called a **total order**.

If $a \preceq b$ and $a \neq b$ then we write $a \prec b$.

The usual graph representation of a poset is crowded with arcs:

Example:
Set $A = \{1, 2, 3\}$ and the poset $(P(A), \subseteq)$

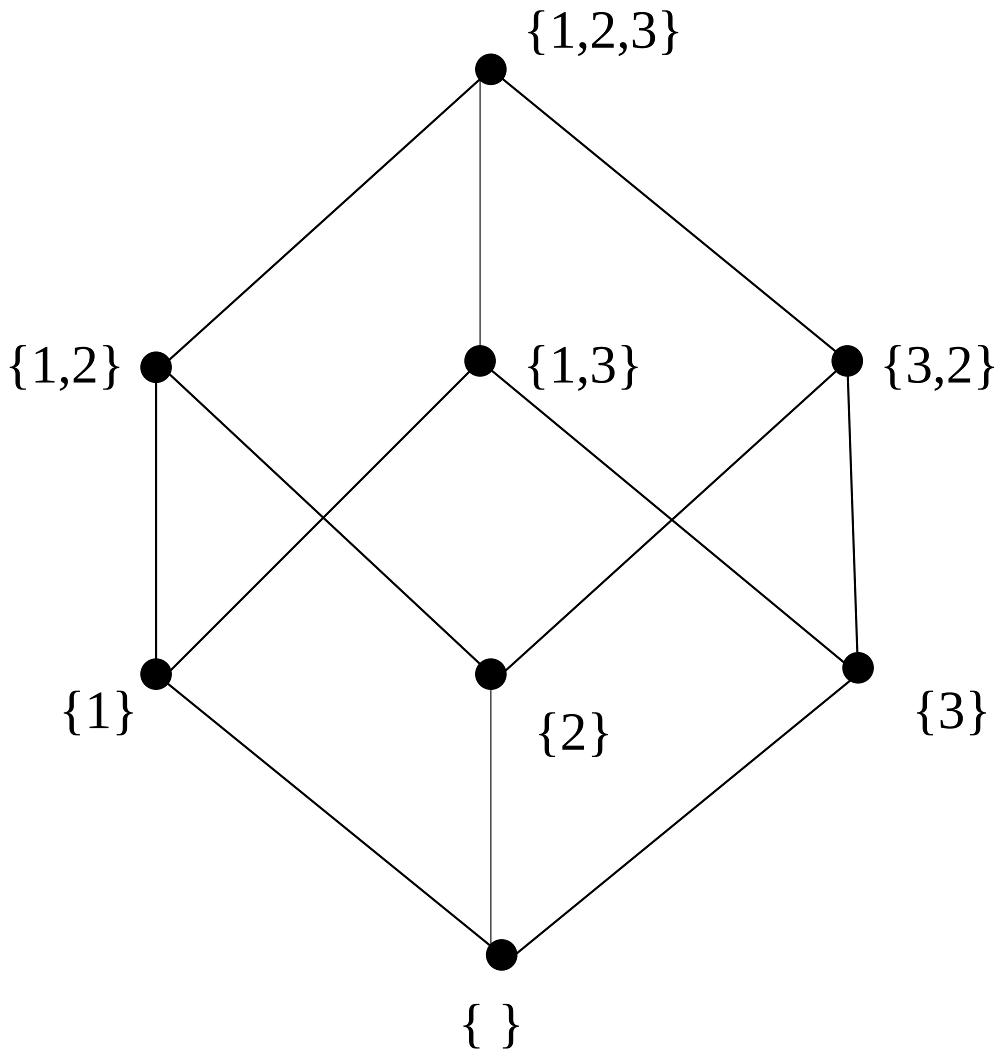


Hasse diagram for posets:
Obtained from the graph representation by:

Removing all arcs due to reflexivity,

Removing all arcs due to transitivity,

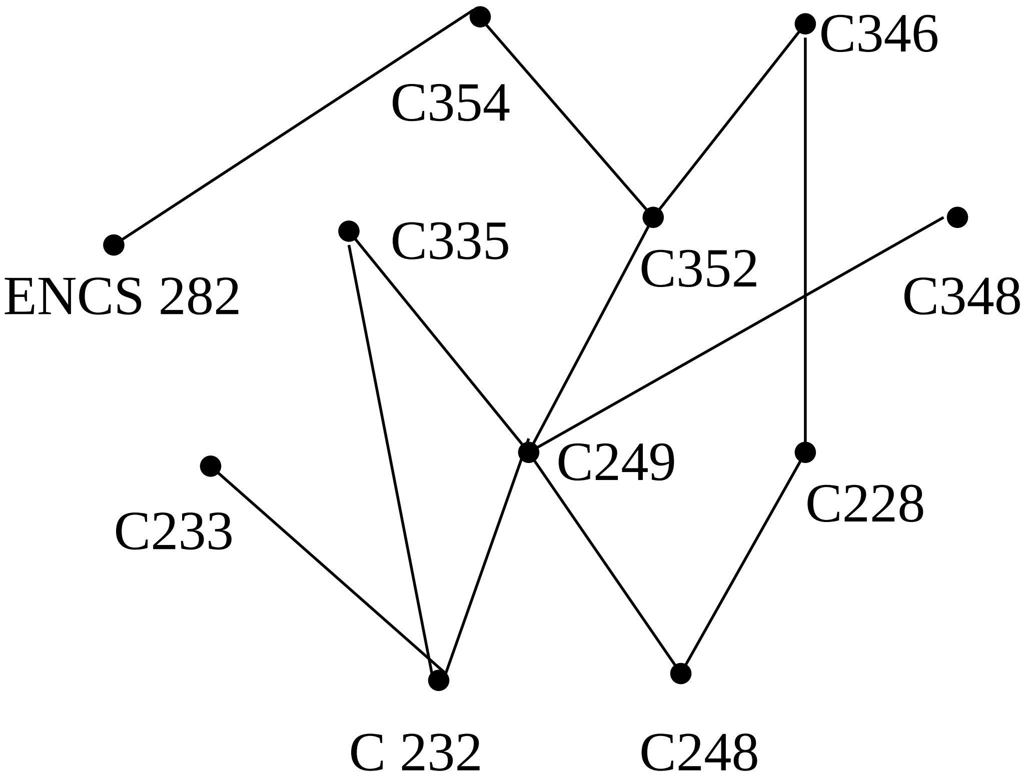
Positioning all elements so that if $a \prec b$ then b is above a.


{1,2,3}
{1,2}
{1,3}
{3,2}
{1}
{2}
{3}
{ }

A Hasse diagram is the usual representation of partial orders.

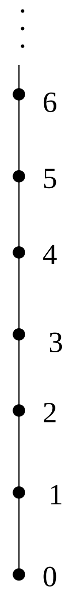
Example

The Hasse diagram of course prerequisites.



If R is a total order then in the Hasse diagram of R all elements of R are aligned on a line.

$\leq$ on natural numbers is a total order.



Lexicographic Order

A method to extend a partial order from a set A of elements to strings constructed from elements in A. Also called *dictionary order*.

Example We have a partial or total ordering on letters:
$a \preceq b \preceq c \preceq d \preceq e \cdots \preceq y \preceq z$

We want to extend it to words made from letters to get the ordering as in dictionaries.

$ace \preceq bank \preceq book \preceq zebra$

First, we show how to extend partial orders of sets A and B to obtain an ordering of $A \times B$.

Let $(A, \preceq_1)$ and $(B, \preceq_2)$ be two partially ordered sets. The **lexicographic ordering** on $A \times B$ is defined as follows:

$(a_1, b_1) \prec (a_2, b_2)$ if either $a_1 \prec_1 a_2$
or $a_1 = a_2$ and $b_1 \prec_2 b_2$

Lexicographic ordering for strings on a poset $(A, \preceq)$

$u = a_1 a_2 a_3 \cdots a_m$ and $v = b_1 b_2 b_3 \cdots b_n$

$u \prec v$ if either $a_1 \prec b_1$
or $a_1 = b_1$ and $a_2 \prec b_2$
or $a_1 a_2 = b_1 b_2$, and $a_3 \prec b_3$
.....
or $a_1 a_2 \cdots a_m = b_1 b_2 \cdots b_m$
and $m < n$

Let $(A, \preceq)$ be a poset.

An element $a \in A$ is **minimal** if there is no element $b \in A$ such that $b \prec a$.

An element $a \in A$ is **maximal** if there is no element $b \in A$ such that $a \prec b$.

An element $a \in A$ is the **greatest element** if $b \preceq a$ for all b in A.

An element $a \in A$ is the **smallest element** if $a \preceq b$ for all b in A.

An element $a \in A$ is an **upper bound** of set $B \subseteq A$ if $b \preceq a$ for all $b \in B$.

An element $a \in A$ of a poset is a **lower bound** of set $B \subseteq A$ if $a \preceq b$ for all $b \in B$.

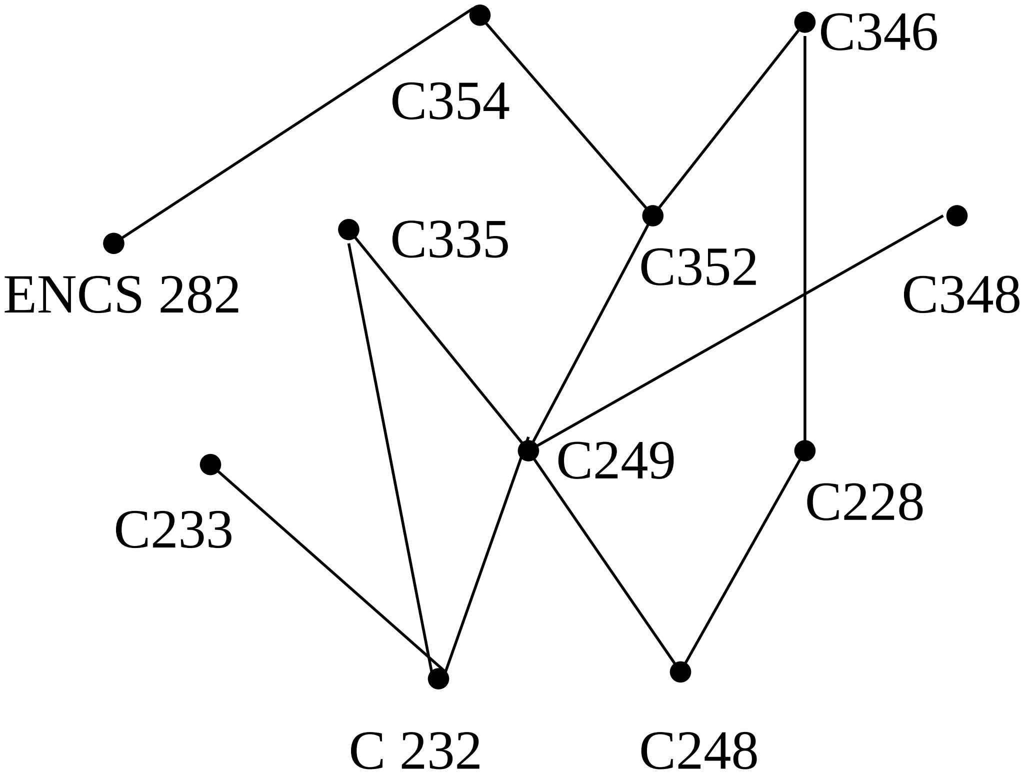
An element $a \in A$ of a poset is the **least upper bound** of set $B \subseteq A$ if $a \preceq$ all other upper bounds of B.

An element $a \in A$ of a poset is the **greatest lower bound** of set $B \subseteq A$ if $a \succeq$ all other lower bounds of B.

Some posets don't have any minimal element, some can have more than one.

Some posets don't have any maximal element, some can have more than one.

Example: In the Hasse diagram of COMP core courses, what are the minimal and maximal elements? Upper bounds of $\{C228, C248\}$? Lower bounds of $\{C335, C352\}$? Least upper bound of $\{C232, C249\}$?



Review

Logic

Important concepts:

proposition
tautology
contradiction
contingency

basic **logical operations** $\vee, \wedge, \neg, \rightarrow, \leftrightarrow$

Logical equivalences

Important concepts:

logical equivalences and implications.

basic **logical equivalences**,
translation of $\rightarrow, \leftrightarrow$ using other logical operations.

rules of inference

how to **construct** a **truth table**.
how to **use** logical equivalences.
how to **reason** with rules of inference.

Quantifiers

Important concepts:

propositional function, or a **predicate**
universal quantifier, existential quantifier

interaction of logical operations and quantifiers.

how to **translate**
a quantified expression into an English sentence,

an English sentence into a quantified expression,

how to reason with rules of inference for quantified statements.

Methods of Proofs

Important concepts:

theorem, axiom, definition, conjecture, counterexample.

direct proof,
indirect proof,
proof by contradiction,
proof by cases,
proof by induction,

how to write a simple proof.

Sets

Important concepts:

$\in, \subseteq, \subset, =,$

basic set operations
$A \cap B, A \cup B, \overline{A}, A - B,$ power set, $A \times B, etc.,$

basic **set identities**,

Venn diagrams,

proving set identities and set inclusions,

relationship between sets and logic.

Functions

Important concepts:

function, domain, codomain, range,

when a function is:
one-to-one, onto, bijection,

inverse function, composition of functions,

floor and ceiling functions.

Integers and Division

Important concepts:

$a|b$

quotient remainder theorem/division algorithm,

prime numbers, factors, composite numbers, GCD, LCM,

prime factorizations.

Euclidean algorithm to find GCD

Binary Relations

Important concepts:

binary relations from A to B, on A,

when a relation is reflexive, symmetric, antisymmetric, transitive,

operations on relations: $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_1 \circ R_2$, R^i, R^t,

transitive closure,

equivalence relations, partial orders, total orders,

Hasse diagram.

Final exam covers all the topics in the course.

Hints:

- Read each question carefully.
- Start with questions that are easy for you.
- If you get bogged down in a problem, go to a different question, come back to it later.
- Check your answers for logical consistency.