LECTURE NOTES

PROGRAMME – BCA

SEMESTER- II

DISCRETE MATHEMATICS (BCA- 401)

UNIT III

Unit-III (10)

Partial order sets: Definition, Partial order sets, Combination of partial order sets, Hasse diagram. **Lattices:** Definition, Properties of lattices – Bounded, Complemented, Modular and Complete lattice. Boolean Algebra: Introduction, Axioms and Theorems of Boolean algebra ,Algebraic manipulation of Boolean expressions. Simplification of Boolean Functions, Karnaugh maps,

Logic gates, Digital circuits and Boolean algebra.

Partial orders, Lattices, etc.

In our context…

- We aim at computing properties on programs
- How can we represent these properties? Which kind of algebraic features have to be satisfied on these representations?
- Which conditions guarantee that this computation terminates?

Motivating Example (1)

- Consider the renovation of the building of a firm. In this process several tasks are undertaken
  - Remove asbestos
  - Replace windows
  - Paint walls
  - Refinish floors
  - Assign offices
  - Move in office furniture
  - …

Motivating Example (2)

- Clearly, some things had to be done before others could begin
  - Asbestos had to be removed before anything (except assigning offices)
  - Painting walls had to be done before refinishing floors to avoid ruining them, etc.
- On the other hand, several things could be done concurrently:
  - Painting could be done while replacing the windows
  - Assigning offices could be done at anytime before moving in office furniture
- This scenario can be nicely modeled using <u>partial orderings</u>

Partial Orderings: Definitions

- **Definitions**:
  - A relation *R* on a set *S* is called a <u>partial order</u> if it is
    - Reflexive
    - Antisymmetric
    - Transitive
  - A set S together with a partial ordering R is called a <u>partially ordered set</u> (poset, for short) and is denote (*S*,*R*)
- Partial orderings are used to give an order to sets that may not have a natural one
- In our renovation example, we could define an ordering such that (a,b)$\in$*R* if ‘a must be done before b can be done’

Partial Orderings: Notation

- We use the notation:
  - a p b, when $(a,b) \in R$
  - a $\not{p}$ b, when $(a,b) \in R$ and $a \neq b$
- The notation p is not to be mistaken for "less than" (p versus ≤)
- The notation p is used to denote <u>any</u> partial ordering

Comparability: Definition

- **Definition**:
  - The elements a and b of a poset (S, p) are called <u>comparable</u> if either apb or bpa.
  - When for a,b∈S, we have neither apb nor bpa, we say that a,b are <u>incomparable</u>
- Consider again our renovation example
  - Remove Asbestos p a_i for all activities a_i except assign offices
  - Paint walls p Refinish floors
  - Some tasks are incomparable: Replacing windows can be done before, after, or during the assignment of offices

Total orders: Definition

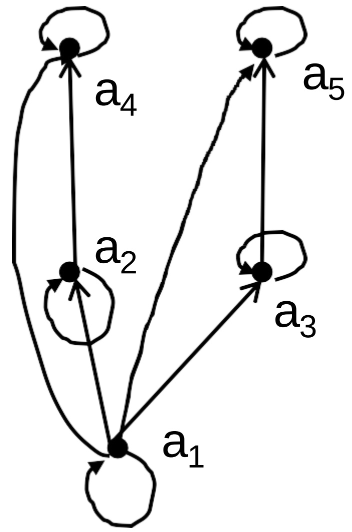
- **Definition**:
  - If (S, p) is a poset and every two elements of S are comparable, S is called a totally ordered set.
  - The relation p is said to be a total order
- Example
  - The relation "less than or equal to" over the set of integers $(Z, \leq)$ since for every $a, b \in Z$, it must be the case that $a \leq b$ or $b \leq a$
  - What happens if we replace $\leq$ with $<$?

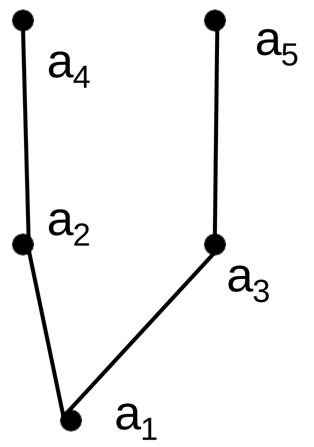
The relation $<$ is not reflexive, and $(Z, <)$ is not a poset

Hasse Diagrams

- Like relations and functions, partial orders have a convenient graphical representation: Hasse Diagrams
  - Consider the digraph representation of a partial order
  - Because we are dealing with a partial order, we know that the relation must be reflexive and transitive
  - Thus, we can simplify the graph as follows
    - Remove all self loops
    - Remove all transitive edges
    - Remove directions on edges assuming that they are oriented upwards
  - The resulting diagram is far simpler

Hasse Diagram: Example

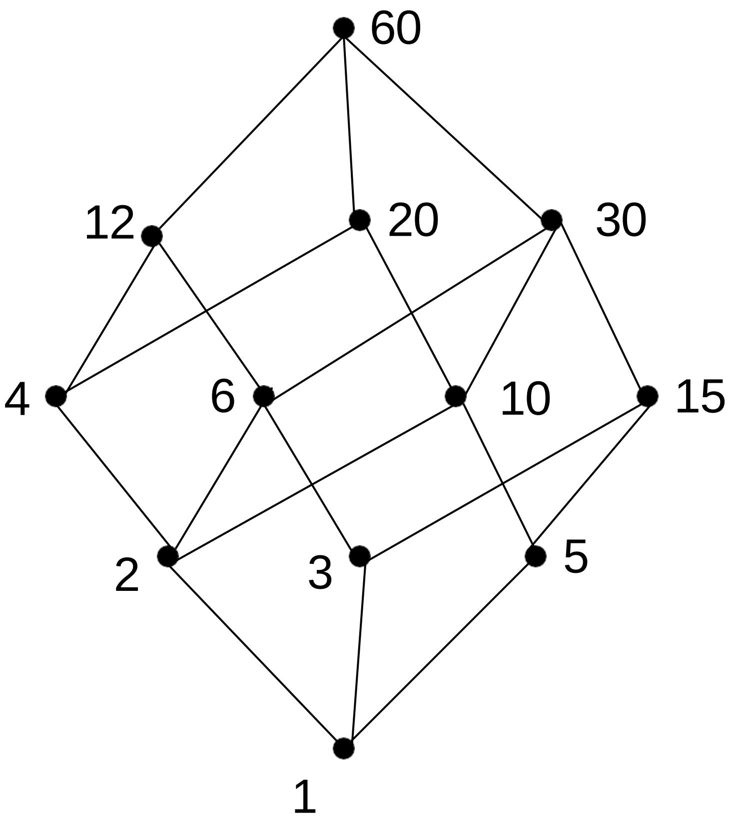




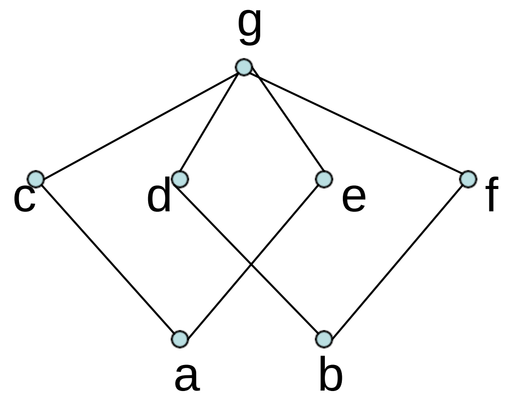
Hasse Diagrams: Example (1)

- Of course, you need not always start with the complete relation in the partial order and then trim everything.
- Rather, you can build a Hasse Diagram directly from the partial order
- Example: Draw the Hasse Diagram
  - for the following partial ordering: {(a,b) | a|b }
  - on the set {1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60}
  - (these are the divisors of 60 which form the basis of the ancient Babylonian base-60 numeral system)

Hasse Diagram: Example (2)



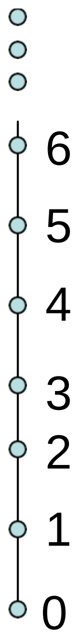
Example



- L= {a,b,c,d,e,f,g}
- ρ ={(a,c), (a,e), (b,d), (b,f), (c,g), (d,g), (e,g), (f,g)}^{RT}

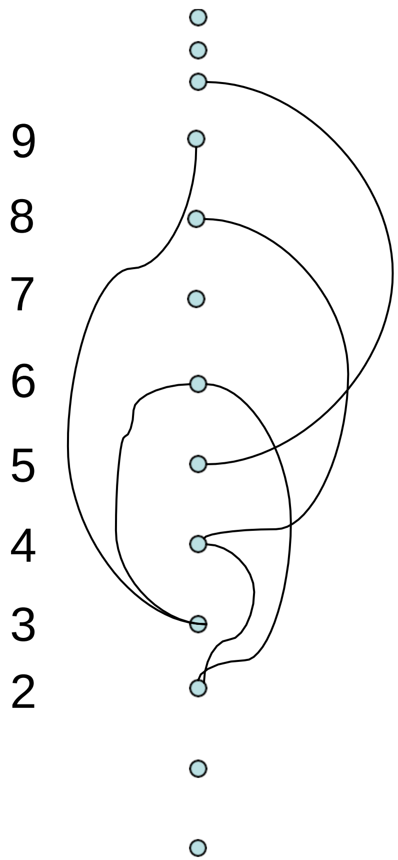
- (L, ρ) is a partial order

Example



- L= N (natural numbers)
- $p = \{(0,1), (1,2), (2,3), (3,4), (4,5), \ldots\}^{RT}$
- (L, p) is a totally ordered set (infinite)

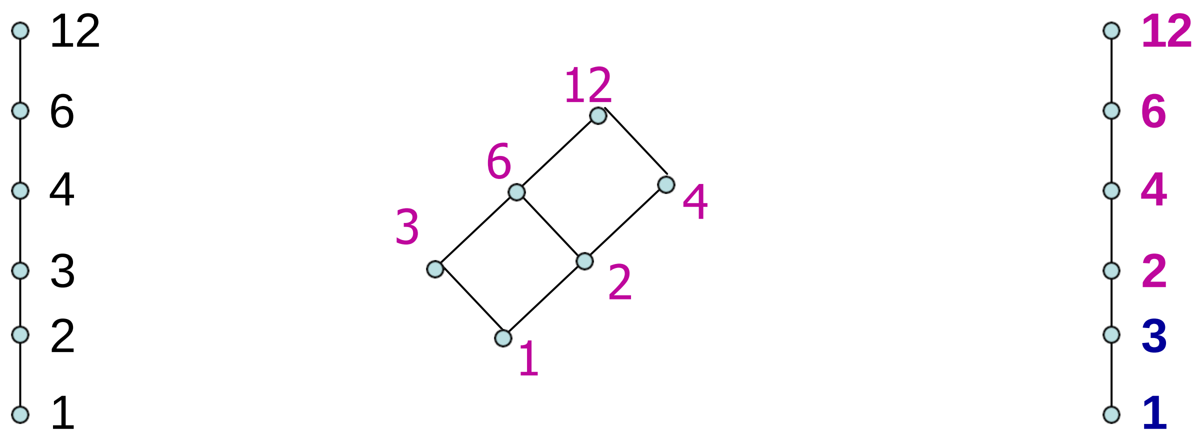
Example



- L= N (natural numbers)
- p ={(n,m): ∃ k such that m=n*k}
- (L, p) is a partially ordered set (infinite)

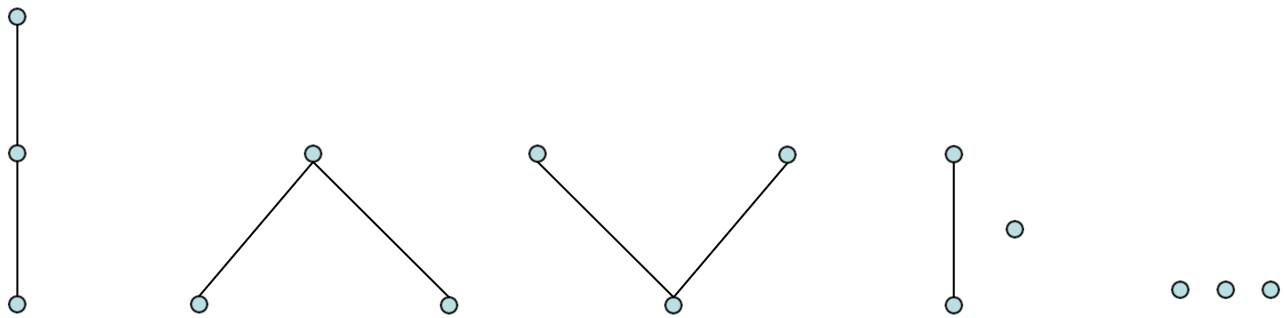
Example

- On the same set E={1,2,3,4,6,12} we can define different partial orders:



Example

- All possible partial orders on a set of three elements (modulo renaming)



Extremal Elements: Summary

We will define the following terms:

- A maximal/minimal element in a poset (S, p)
- The maximum (greatest)/minimum (least) element of a poset (S, p)
- An upper/lower bound element of a subset A of a poset (S, p)
- The greatest lower/least upper bound element of a subset A of a poset (S, p)

Extremal Elements: Maximal

- **Definition**: An element a in a poset (S, p) is called maximal if it is not less than any other element in S. That is: $\neg(\exists b \in S\ (a p b))$
- If there is one unique maximal element a, we call it the maximum element (or the greatest element)

Extremal Elements: Minimal

- **Definition**: An element a in a poset $(S, \preccurlyeq)$ is called <u>minimal</u> if it is not greater than any other element in S. That is: $\neg(\exists b \in S\ (b \prec a))$
- If there is one <u>unique</u> minimal element a, we call it the <u>minimum</u> element (or the <u>least</u> element)

Extremal Elements: Upper Bound

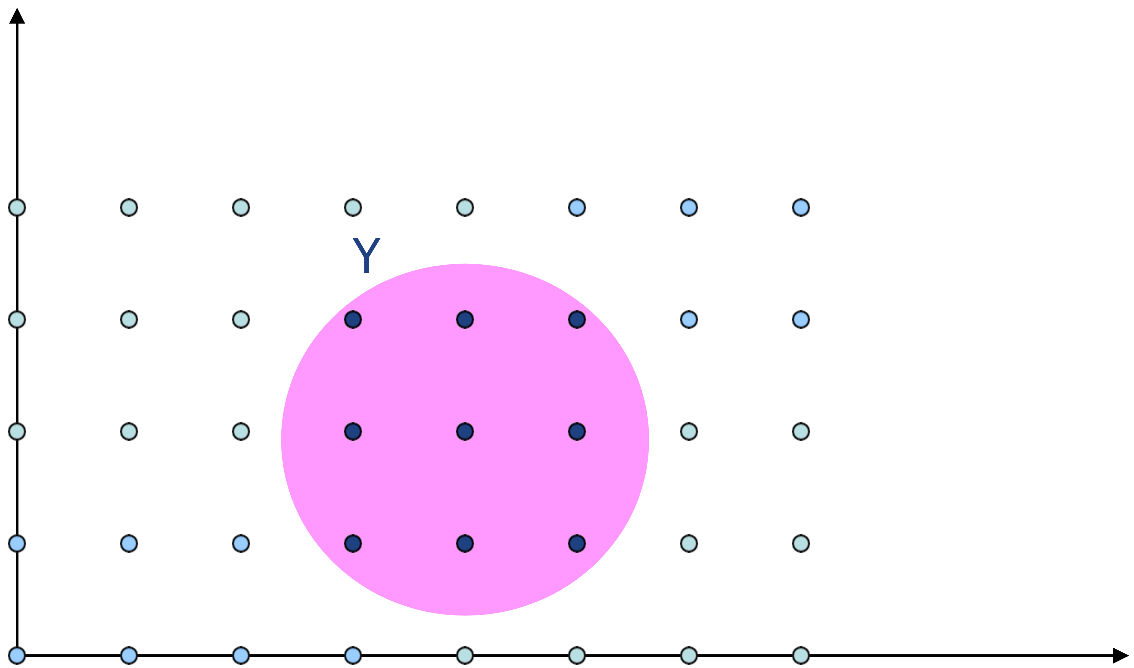
- **Definition**: Let (S,p) be a poset and let $A \subseteq S$. If u is an element of S such that a p u for all $a \in A$ then u is an upper bound of A
- An element x that is an upper bound on a subset A and is less than all other upper bounds on A is called the least upper bound on A. We abbreviate it as lub.

Extremal Elements: Lower Bound

- **Definition**: Let (S,p) be a poset and let $A \subseteq S$. If l is an element of S such that l p a for all $a \in A$ then l is an <u>lower bound of A</u>
- An element x that is a lower bound on a subset A and is greater than all other lower bounds on A is called the <u>greatest lower bound on A</u>. We abbreviate it glb.

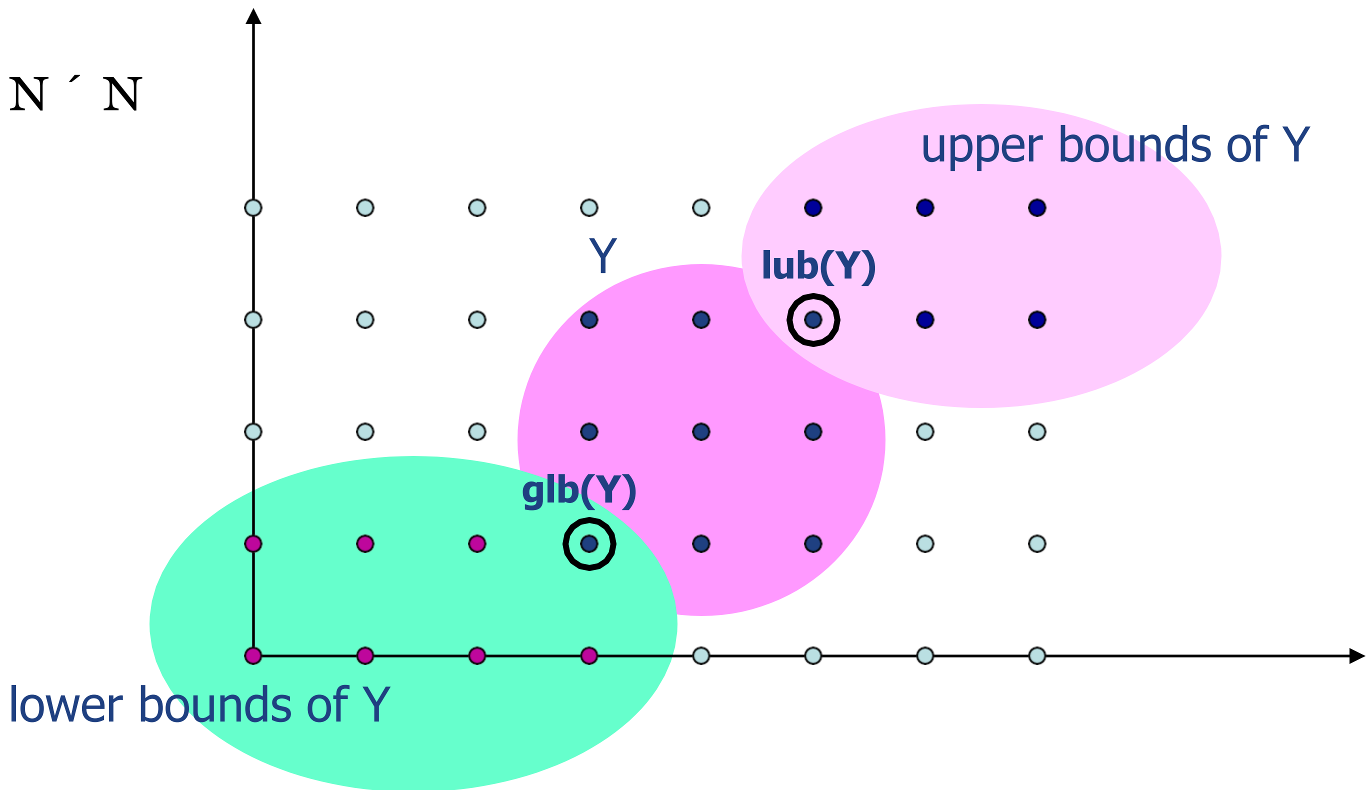
Example

N x N



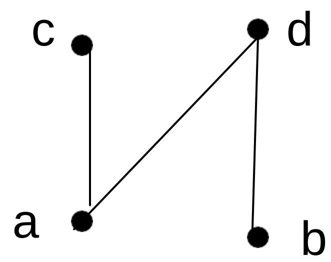
$$(x_1,y_1) \leq_{\mathrm{N\,x\,N}} (x_2,y_2) \Leftrightarrow x_1 \leq_{\mathrm{N}} x_2 \wedge y_1 \leq_{\mathrm{N}} y_2$$

Example



$$(x_1,y_1) \leq_{N \times N} (x_2,y_2) \iff x_1 \leq_N x_2 \wedge y_1 \leq_N y_2$$

Extremal Elements: Example 1



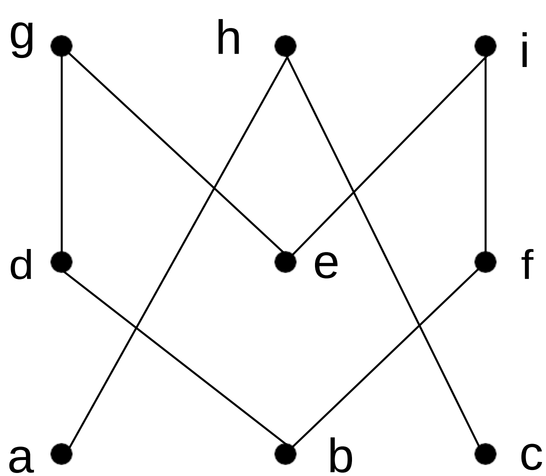
What are the minimal, maximal, minimum, maximum elements?

- Minimal: {a,b}
- Maximal: {c,d}
- There are no unique minimal or maximal elements, thus no minimum or maximum

Extremal Elements: Example 2

Give lower/upper bounds & glb/lub of the sets:

{d,e,f}, {a,c} and {b,d}



{d,e,f}

- Lower bounds: ∅, thus no glb
- Upper bounds: ∅, thus no lub

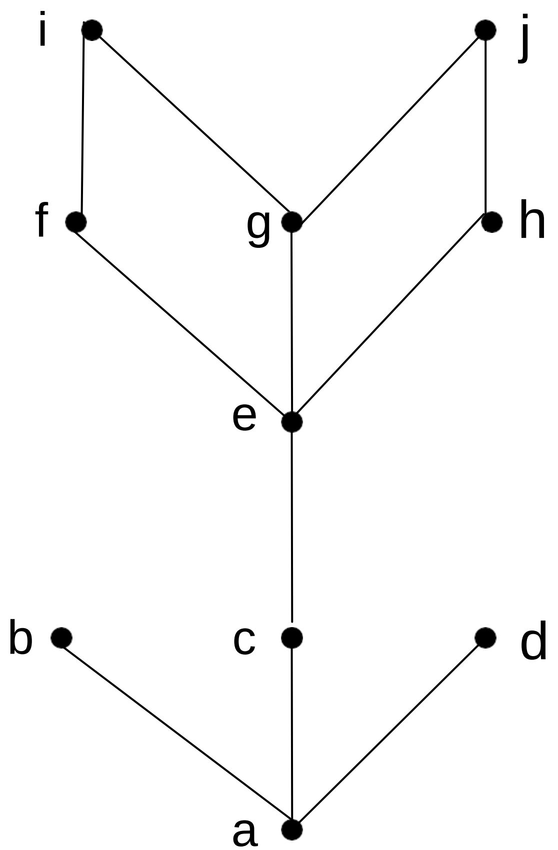
{a,c}

- Lower bounds: ∅, thus no glb
- Upper bounds: {h}, lub: h

{b,d}

- Lower bounds: {b}, glb: b
- Upper bounds: {d,g}, lub: d because dpg

Extremal Elements: Example 3



- Minimal/Maximal elements?
  - Minimal & Minimum element: a
  - Maximal elements: b,d,i,j
- Bounds, glb, lub of {c,e}?
  - Lower bounds: {a,c}, thus glb is c
  - Upper bounds: {e,f,g,h,i,j}, thus lub is e
- Bounds, glb, lub of {b,i}?
  - Lower bounds: {a}, thus glb is c
  - Upper bounds: ∅, thus lub DNE

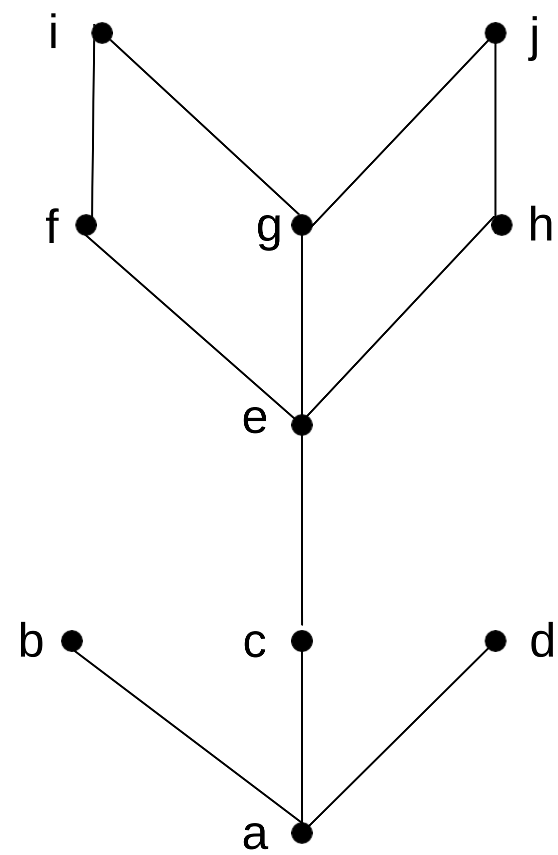
Lattices

- A special structure arises when <u>every</u> pair of elements in a poset has an lub and a glb
- **Definition**: A <u>lattice</u> is a partially ordered set in which <u>every</u> pair of elements has both
  - a least upper bound and
  - a greatest lower bound

Lattices: Example 1

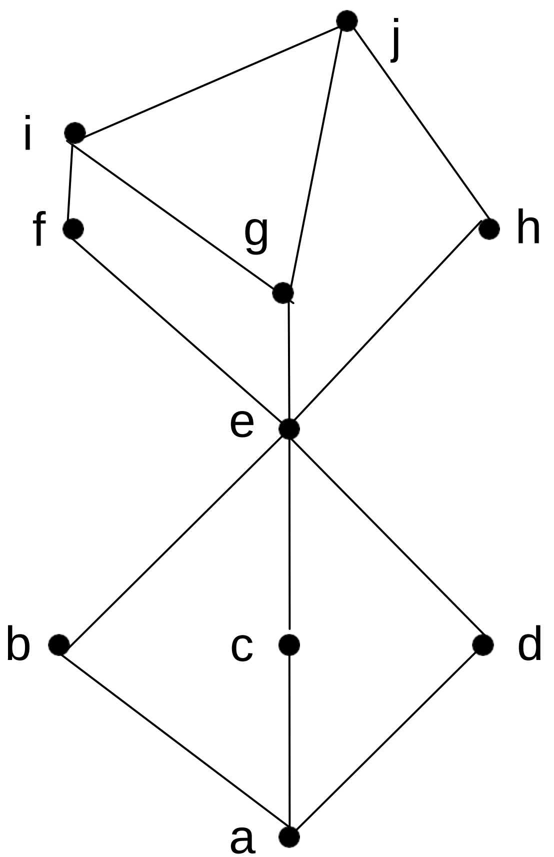
- Is the example from before a lattice?

- **No, because the pair {b,c} does not have a least upper bound**



Lattices: Example 2

- What if we modified it as shown here?



- **Yes, because for any pair, there is an lub & a glb**

A Lattice Or Not a Lattice?

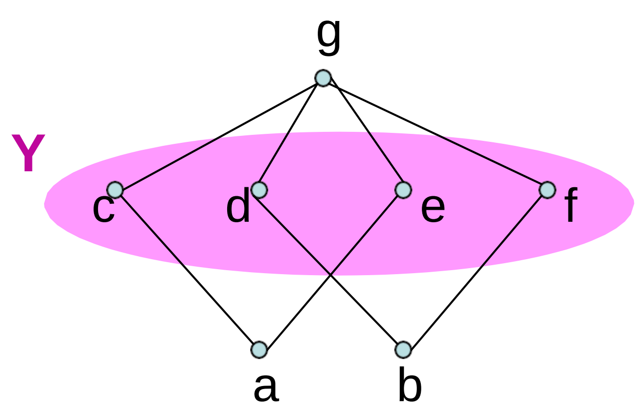
- To show that a partial order is not a lattice, it suffices to find a pair that does not have an lub or a glb (i.e., a counter-example)
- For a pair not to have an lub/glb, the elements of the pair must first be <u>incomparable</u> (Why?)
- You can then view the upper/lower bounds on a pair as a sub-Hasse diagram: If there is no maximum/minimum element in this sub-diagram, then it is not a lattice

Complete lattices

- Definition:
  A lattice A is called a complete lattice if every subset S of A admits a glb and a lub in A.

- Exercise:
  Show that for any (possibly infinite) set E, (P(E),$\subseteq$) is a complete lattice
  (P(E) denotes the powerset of E, i.e. the set of all subsets of E).

Example

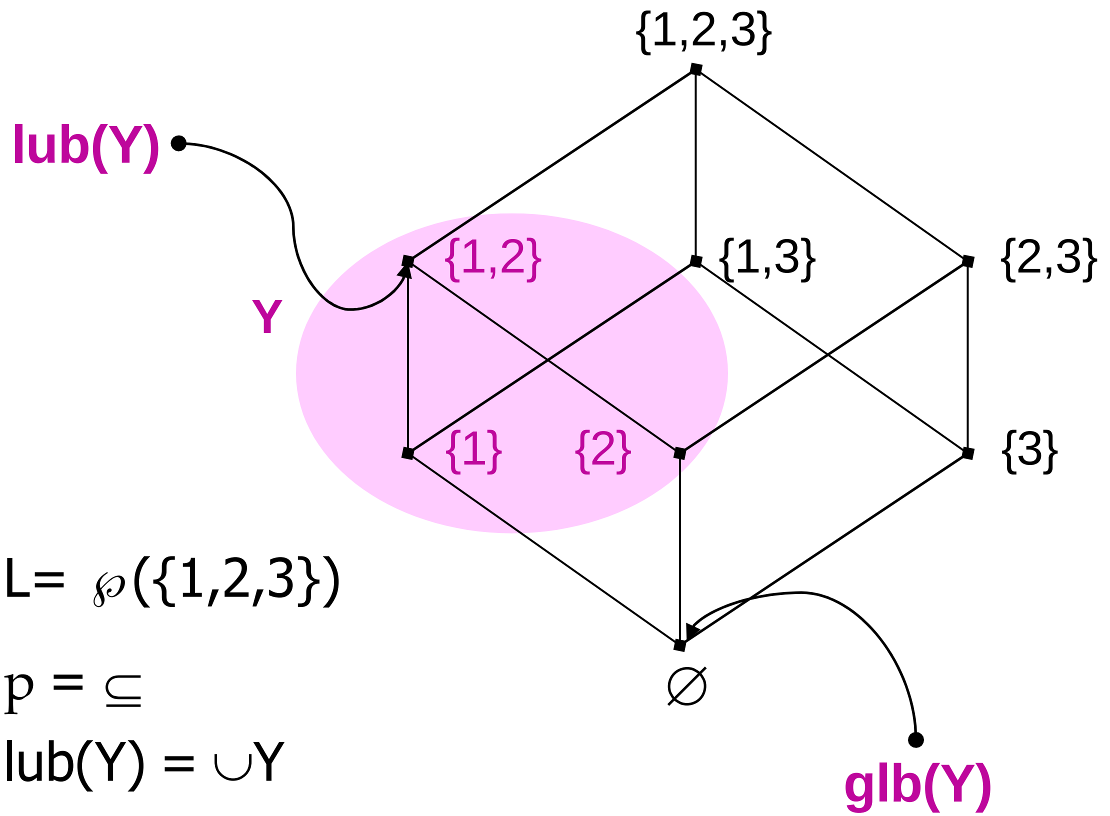


- L= {a,b,c,d,e,f,g}
- $\leq$ ={(a,c), (a,e), (b,d), (b,f), (c,g), (d,g), (e,g), (f,g)}^{T}
- (L,$\leq$) is not a lattice:
  a and b are lower bounds of Y, but a and b are not comparable

Exercise

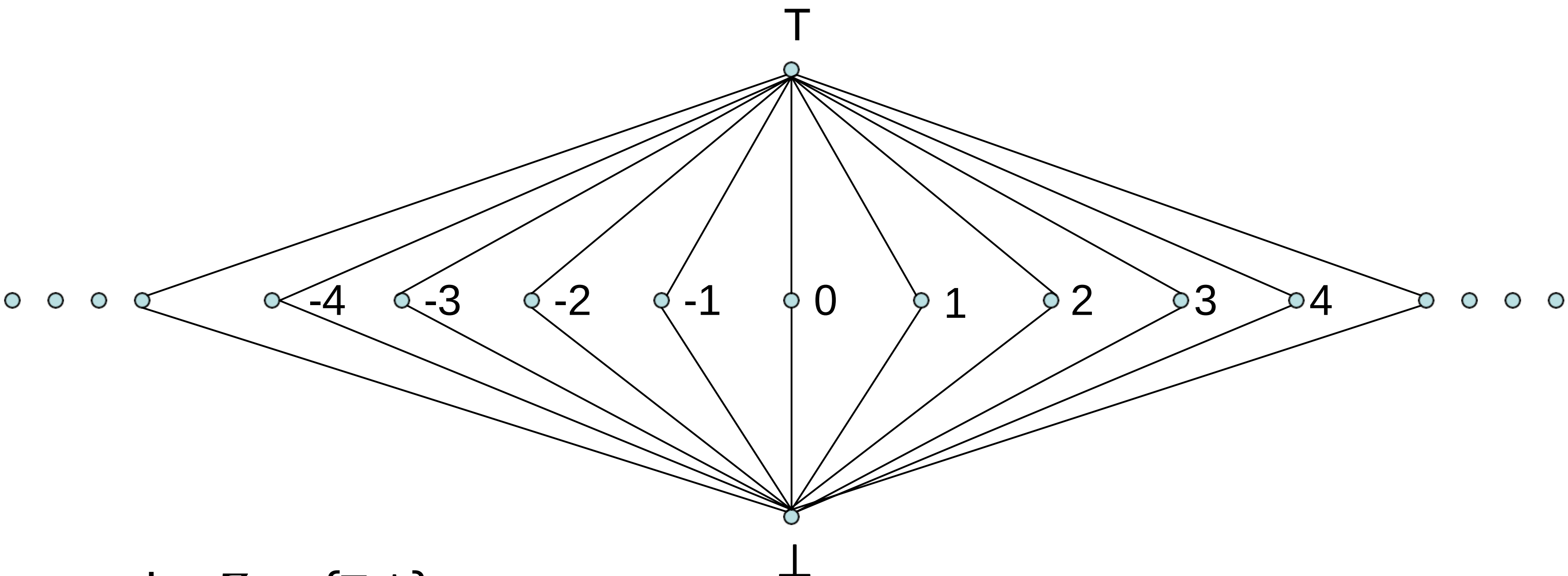
- Prove that "Every finite lattice is a complete lattice".

Example



- L= $\wp(\{1,2,3\})$
- p = $\subseteq$
- lub(Y) = $\cup$Y
- glb(Y) = $\cap$Y

Example



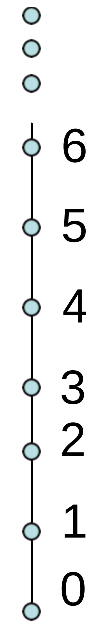
- L= $\mathbb{Z} \cup \{T, \perp\}$
- $\forall\, n \in \mathbb{Z} : \perp p \; n \; p \; T$

Example

- L= Z_+
- p total order on Z_+
- lub = max
- glb = min

It is a lattice, but not complete:

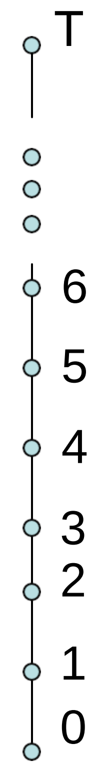
For instance, the set of even numbers has no lub



Example

- L= $Z_+ \cup \{T\}$
- p total order on $Z_+ \cup \{T\}$
- lub = max
- glb = min

This is a complete lattice



Examples

- L=R (real numbers) with $p = \leq$ (total order)
- (R, $\leq$) is not a complete lattice:
  for instance $\{x \in R \mid x > 2\}$ has no lub
- On the other hand,
  for each $x<y$ in R, ($[x,y]$, $\leq$) is a complete lattice

- L=Q (rational numbers) with $p = \leq$ (total order)
- (Q, $\leq$) is not a complete lattice
- The set $\{x \in Q \mid x^2 < 2\}$ has upper bounds but there is no least upper bound in Q.

- **Theorem**:

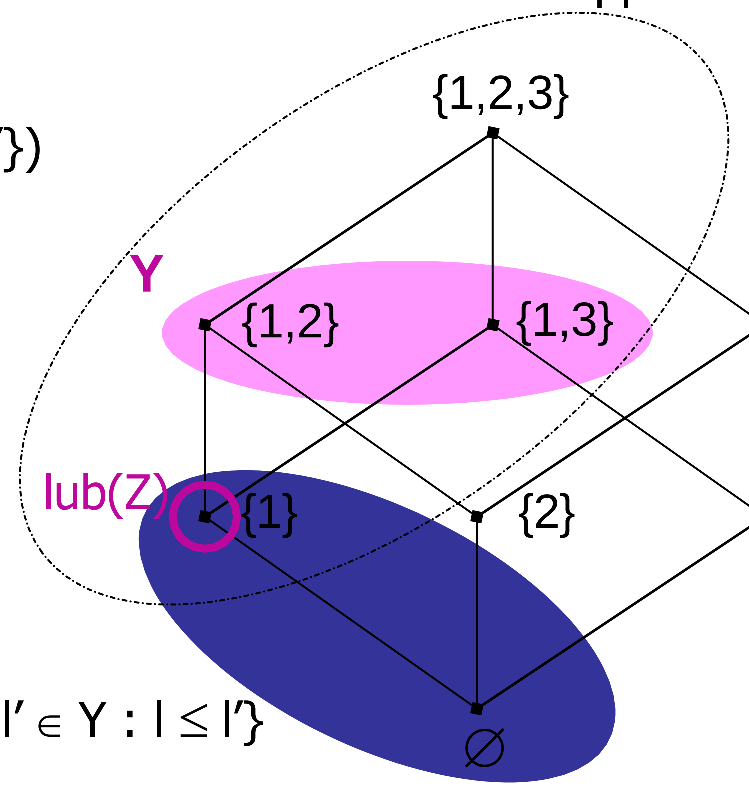
  Let (L, p) be a partial order. The following conditions are equivalent:

  1. L is a complete lattice
  2. Each subset of L has a least upper bound
  3. Each subset of L has a greatest lower bound

- Proof:
  - $1 \Rightarrow 2$ e $1 \Rightarrow 3$ by definition
  - In order to prove that $2 \Rightarrow 1$, let us define for each $Y \subseteq L$

$$glb(Y) = lub(\{l \in L \mid \forall l' \in Y : l \leq l'\})$$

$glb(Y) = lub(\{l \in L \mid \forall l' \in Y : l \leq l'\})$



$Z = \{l \in L \mid \forall l' \in Y : l \leq l'\}$

Functions on partial orders

- Let $(P,\leq_P)$ and $(Q,\leq_Q)$ two partial orders. A function φ from P to Q is said:

- monotone (order preserving) if

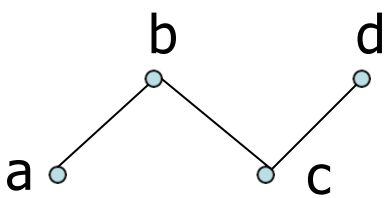
$$p_1 \leq_P p_2 \Rightarrow \varphi(p_1) \leq_Q \varphi(p_2)$$

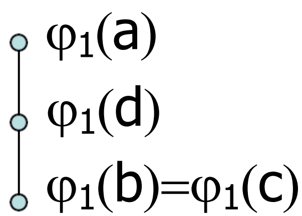
- embedding if

$$p_1 \leq_P p_2 \Leftrightarrow \varphi(p_1) \leq_Q \varphi(p_2)$$

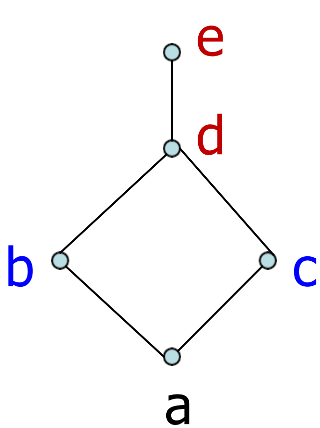
- Isomorphism if it is a surjective embedding

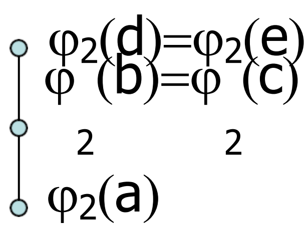
Examples





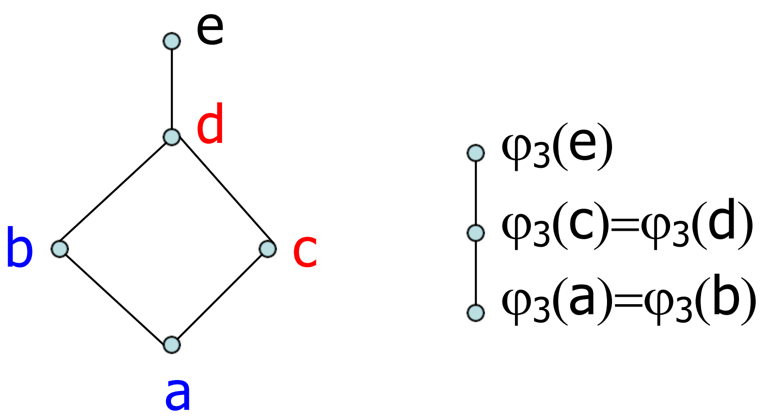
- φ_1 is not monotone



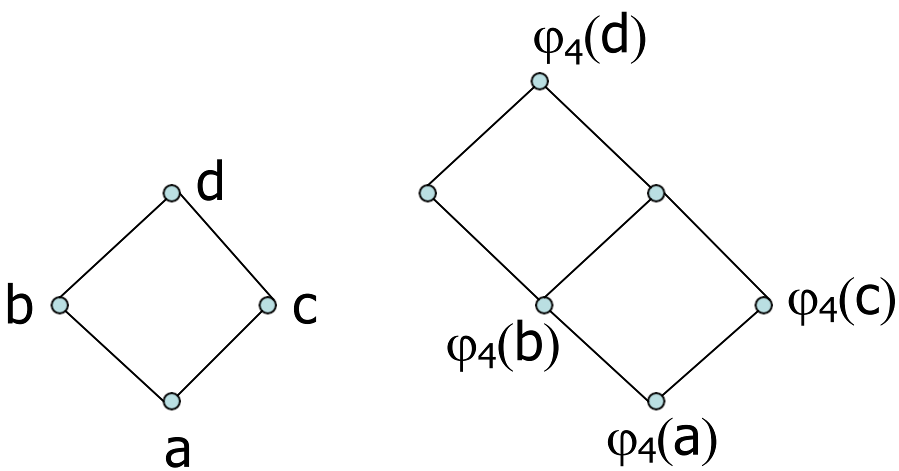


- φ_2 is monotone, but it is not an embedding: $\varphi_2(b) \leq_Q \varphi_2(c)$ but it is not true that $b \leq_P c$

Examples

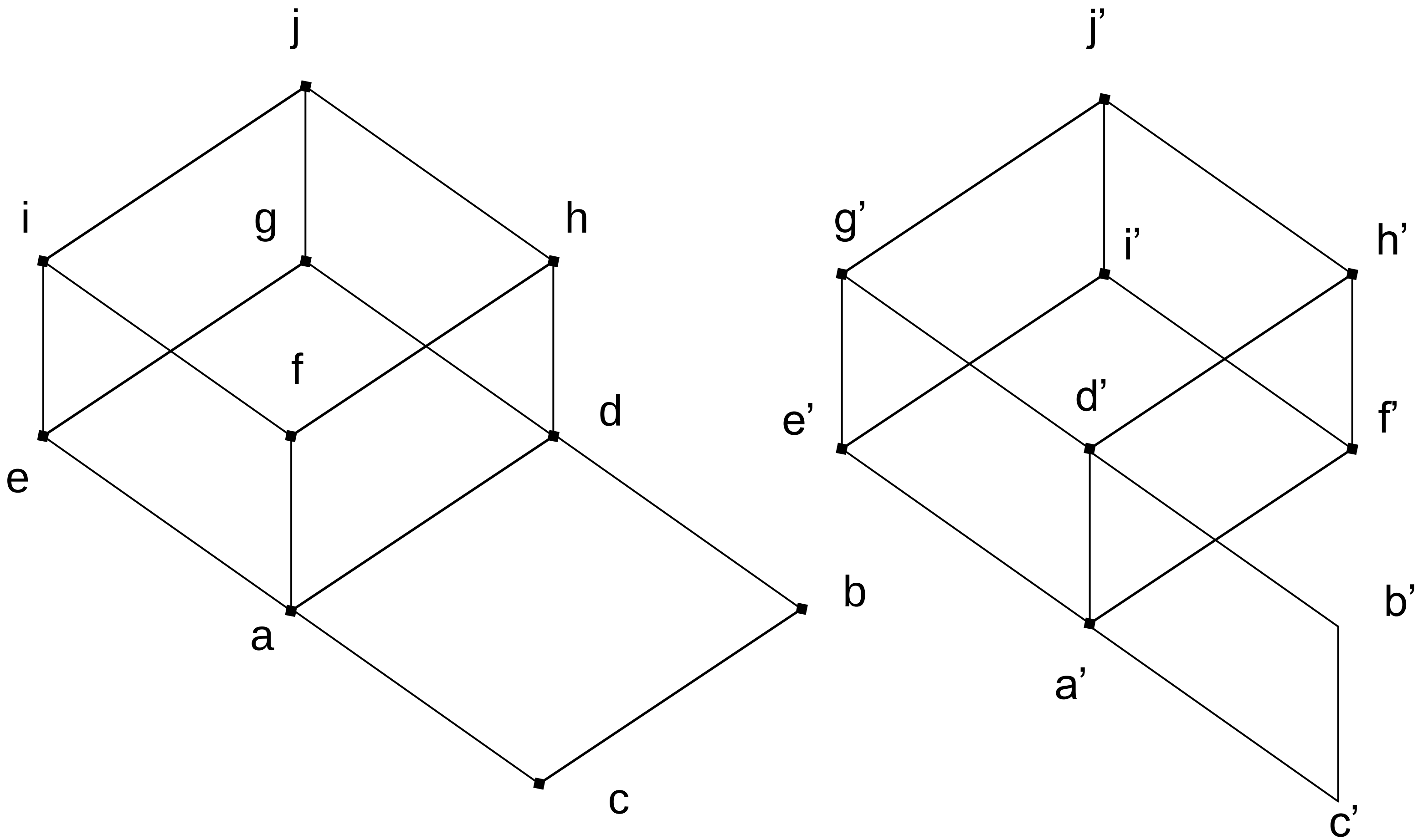


- φ_3 is monotone but it is not an embedding: $\varphi_3(b)\leq_Q\varphi_3(c)$ but it is not true that $b\leq_P c$



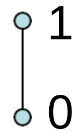
- φ_4 is an embedding, but not an isomorphism.

Isomorphism



Monotone? Embedding? Isomorphism?

- φ from $(\mathbb{Z}, \leq)$ to $(\mathbb{Z}, \leq)$, defined by: $\varphi(x)=x+1$

- φ from $(\wp(S), \subseteq)$ to 

, defined by:

  $\varphi(U)=1$ if U is nonempty, $\varphi(\emptyset)=0$.

- φ from $(\wp(\mathbb{Z}), \subseteq)$ to $(\wp(\mathbb{Z}), \subseteq)$, defined by:

  $\varphi(U)=\{1\}$ if $1 \in U$

  $\varphi(U)=\{2\}$ if $2 \in U$ and 1 does not belong to U

  $\varphi(U)=\emptyset$ otherwise

Ascending chains

- A sequence $(l_n)_{n\in\mathbb{N}}$ of elements in a partial order L is an ascending chain if

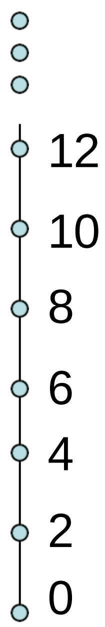
$$n \leq m \Rightarrow l_n \leq l_m$$

- A sequence $(l_n)_{n\in\mathbb{N}}$ converges if and only if

$$\exists\, n_0 \in \mathbb{N} : \forall\, n \in \mathbb{N} : n_0 \leq n \Rightarrow l_{n_0} = l_n$$

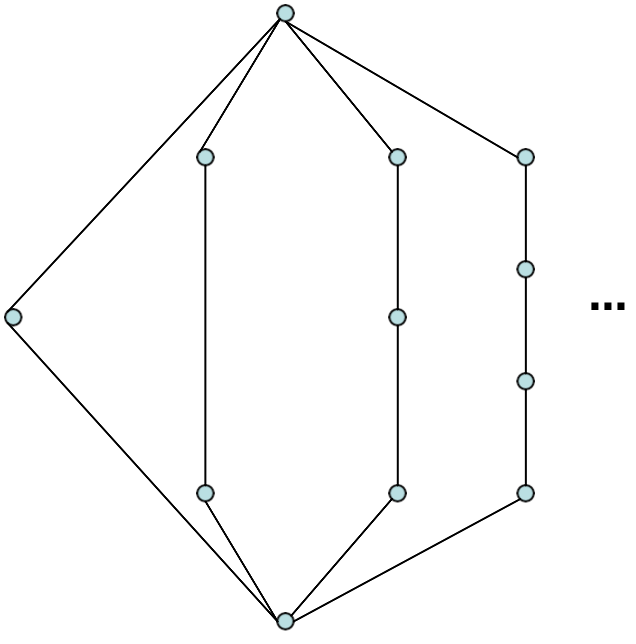
- A partial order $(L,\leq)$ satisfes the ascending chain condition (ACC) iff each ascending chain converges.

Example



- The set of even natural numbers satisfies the descending chain condition, but not the ascending chain condition

Example



- Infinite set
- Satisfies both ACC and DCC

Lattices and ACC

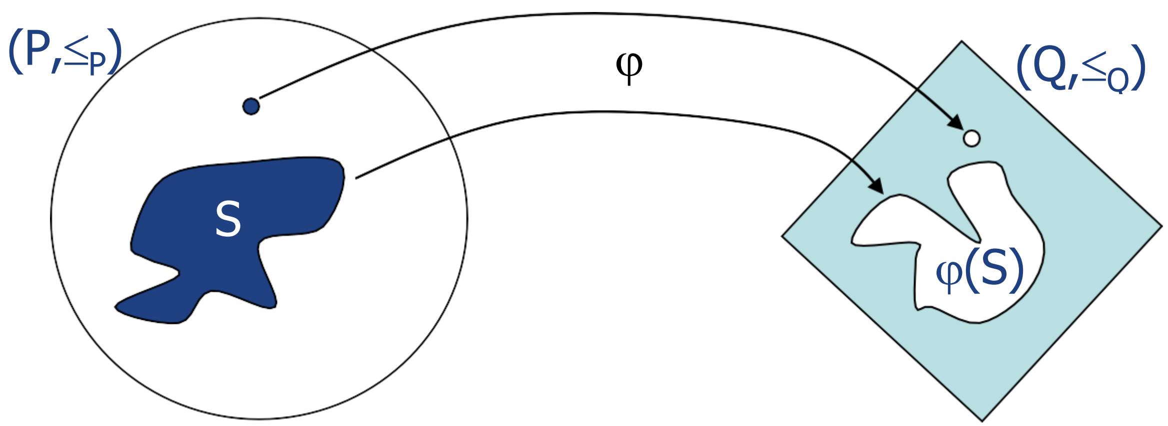
- If P is a lattice, it has a bottom element and satisfies ACC, tyen it is a complete lattice

- If P is a lattice without infinite chains, then it is complete

Continuity

- In Calculus, a function is continuous if it preserves the limits.
- Given two partial orders $(P,\leq_P)$ and $(Q,\leq_Q)$, a functoin φ from P to Q is continuous id for every chain S in P

$$\varphi(\text{lub}(S)) = \text{lub}\{\ \varphi(x) \mid x \in S\ \}$$



Fixpoints

- Consider a monotone function f: $(P,\leq_P) \rightarrow (P,\leq_P)$ on a partial order P.

- An element x of P is a fixpoint of f if f(x)=x.
- The set of fixpoints of f is a subset of P called Fix(f):

$$Fix(f) = \{ l \in P \mid f(l)=l \}$$

Fixpoint on Complete Lattices

- Consider a monotone function $f:L \rightarrow L$ on a complete lattice L.

- Fix(f) is also a complete lattice:

$$lfp(f) = glb(Fix(f)) \in Fix(f)$$
$$gfp(f) = lub(Fix(f)) \in Fix(f)$$

- Tarski Theorem:
  Let L be a complete lattice. If $f:L \rightarrow L$ is monotone then

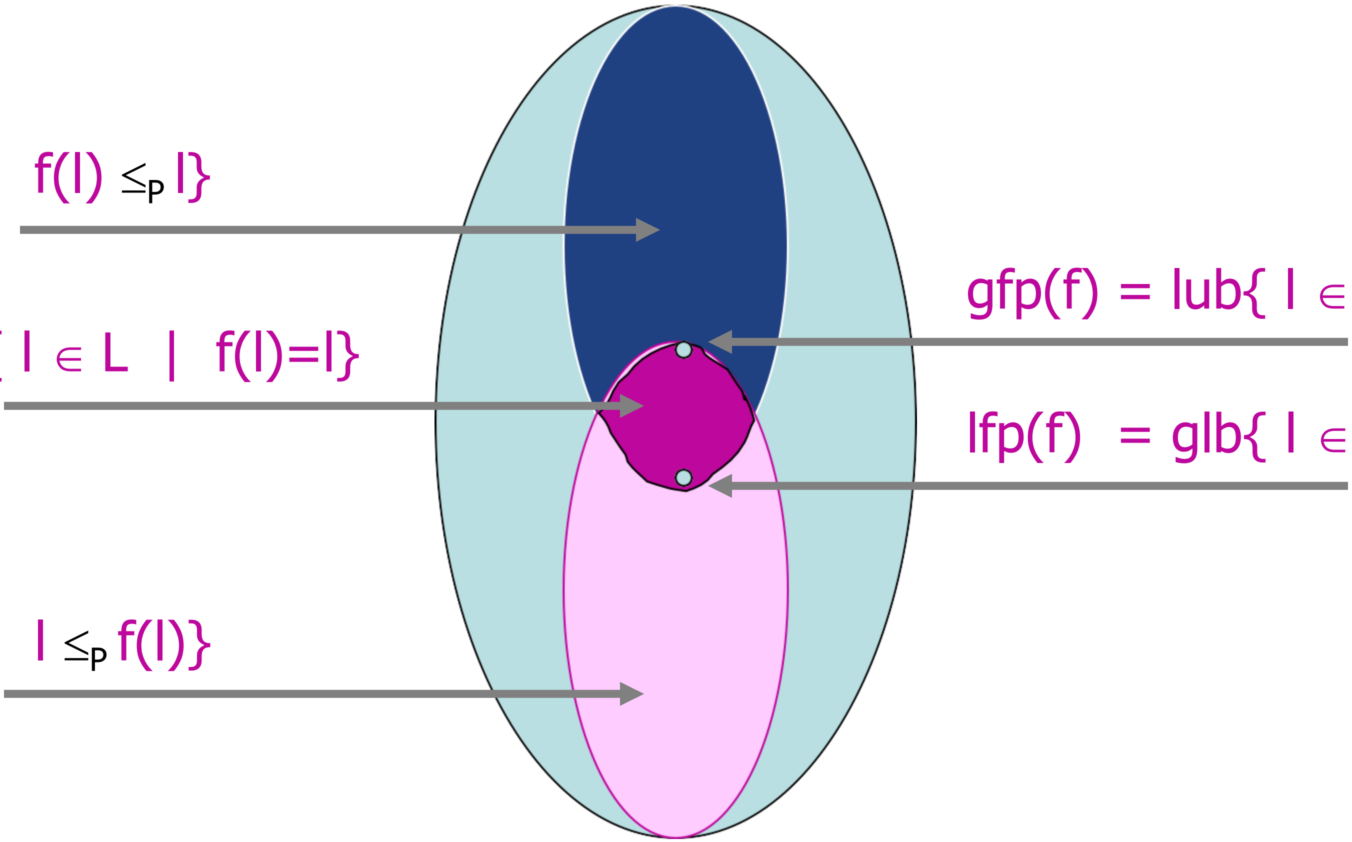
$$lfp(f) = glb\{ l \in L \mid f(l) \leq l \}$$
$$gfp(f) = lub\{ l \in L \mid l \leq f(l) \}$$

Fixpoints on Complete Lattices

$\{ l \in L \mid f(l) \leq_P l \}$

$Fix(f) = \{ l \in L \mid f(l) = l \}$

$\{ l \in L \mid l \leq_P f(l) \}$



$gfp(f) = lub\{ l \in L \mid l \leq f(l) \}$

$lfp(f) = glb\{ l \in L \mid f(l) \leq l \}$

Kleene Theorem

- Let f be a monotone function: $(P,\leq_P) \rightarrow (P,\leq_P)$ on a complete lattice P. Let $\alpha = \bigsqcup_{n\geq 0} f^n(\perp)$
  - If $\alpha \in Fix(f)$ then $\alpha =$ lfp(f)
  - Kleene Theorem
    If f is continuous then the least fixpoint of f esists , and it is equal to α