Some background on Algebraic Structures: 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?

Partial Orderings: Definitions

- **Definitions**:
  - A relation R on a set S is called a partial order if it is
    - Reflexive $(a,a)\in R$
    - Antisymmetric if $(a,b)\in R$ and $(b,a)\in R$ then $a=b$
    - Transitive if $(a,b)\in R$ and $(b,c)\in R$ then $(a,c)\in R$
  - A set S together with a partial ordering R is called a partially ordered set (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

Partial Orderings: Notation

- We use the notation:

  $a \prec b$, when $(a,b) \in R$

- The notation $\prec$ is not to be mistaken for “less than” ($\prec$ versus $\leq$)
- The notation $\prec$ is used to denote <u>any</u> partial ordering:
  - $(a,b) \in R$ if ‘a must be done before b can be done’
  - $(a,b) \in R$ if ‘a is greater than b’
  - …

Comparability: Definition

- **Definition**:
  - The elements a and b of a poset $(S, \prec)$ are called <u>comparable</u> if either $a \prec b$ or $b \prec a$.
  - When for $a,b \in S$, we have neither $a \prec b$ nor $b \prec a$, we say that a,b are <u>incomparable</u>

Total orders: Definition

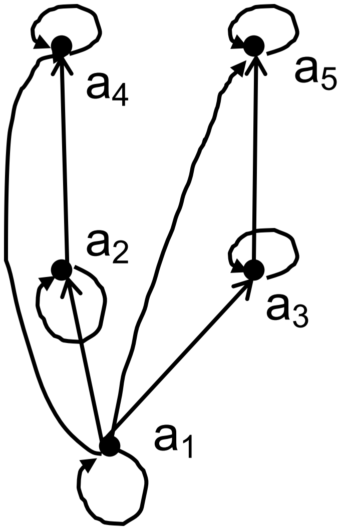
- **Definition**:
  - If $(S,\prec)$ is a poset and every two elements of S are comparable, S is called a <u>totally ordered set</u>.
  - The relation $\prec$ is said to be a <u>total order</u>
- Example
  - The relation "less than or equal to" over the set of integers $(\mathbb{Z}, \leq)$ since for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

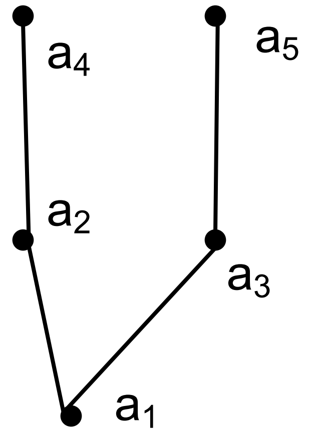
The relation $<$ is not reflexive, and $(\mathbb{Z},<)$ is not a poset

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

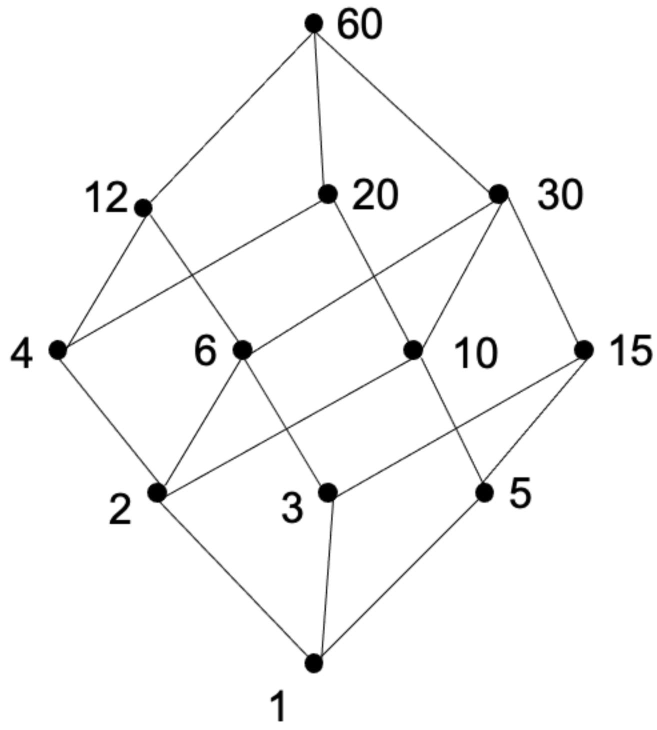
Hasse Diagram: Example



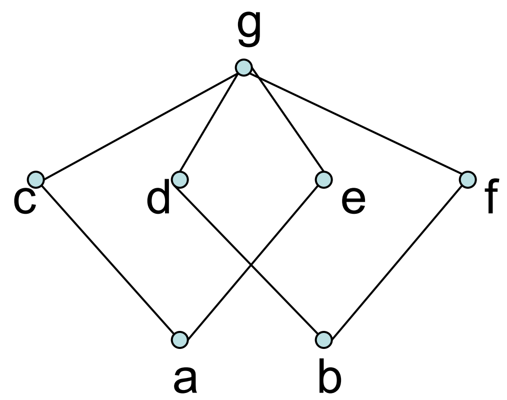


Hasse Diagrams: Example (1)

- We can build a Hasse Diagram directly from the partial order
- Example: Draw the Hasse Diagram
  - for the following partial ordering: $\{(a,b) \mid a,b \in Z\text{: } a \text{ divides } b\}$
  - 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



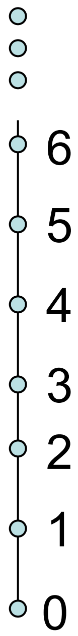
Example



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

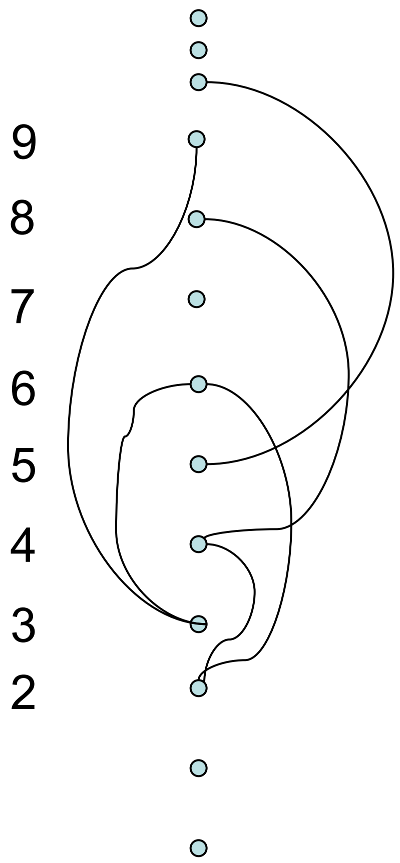
- (L, $\prec$) is a partial order

Example



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

Example

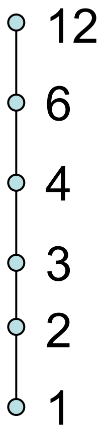


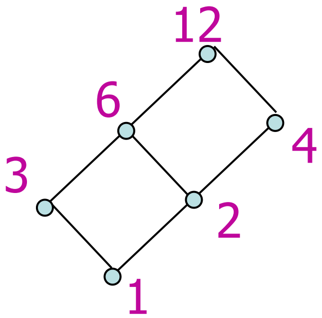
- L= N   (natural numbers)
- $\prec$ ={(n,m): $\exists$ k such that m=n*k}

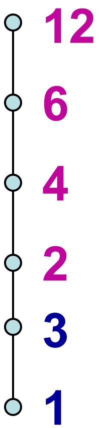
- (L, $\prec$) is a partially ordered set (infinite)

Example

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

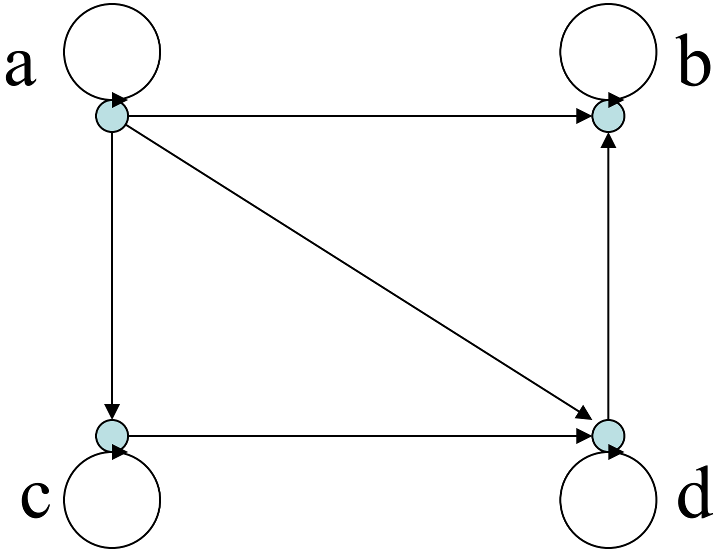






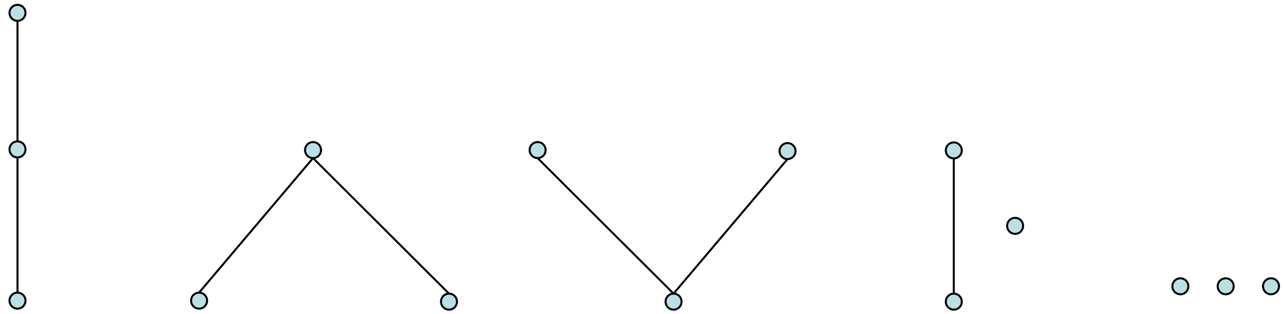
Exercise

Consider this directed graph. Is it a partial order?



Example

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



Extremal Elements: Maximal & minimal

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

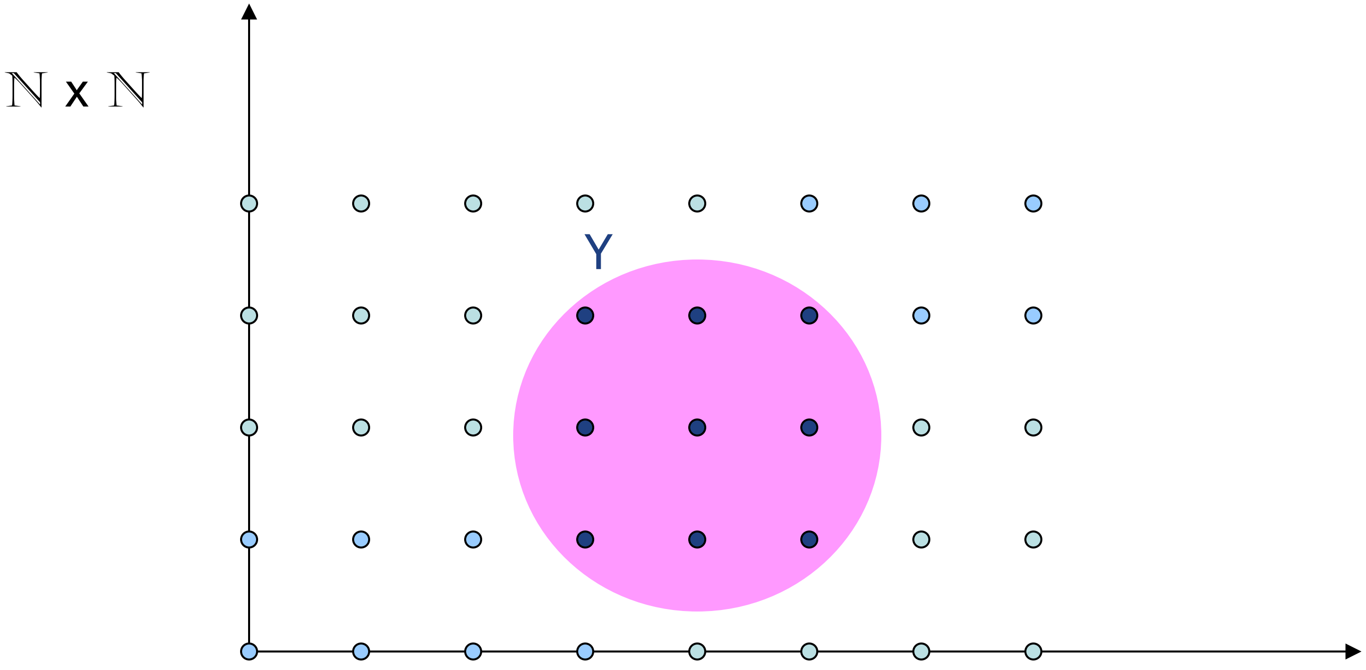
- **Definition**: An element a in a poset $(S, \prec)$ is called minimal if it is not greater than any other element in S. That is: $\neg(\exists b \in S\ (b \prec a))$
- If there is one unique minimal element a, we call it the minimum element (or the least element)

Upper Bounds & Lower Bounds

- **Definition**: Let $(S,\prec)$ be a poset and let $A \subseteq S$. If u is an element of S such that $a \prec u$ for all $a \in A$ then u is an <u>upper bound of A</u>
- 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 <u>least upper bound on A</u>. We abbreviate it as **lub**.

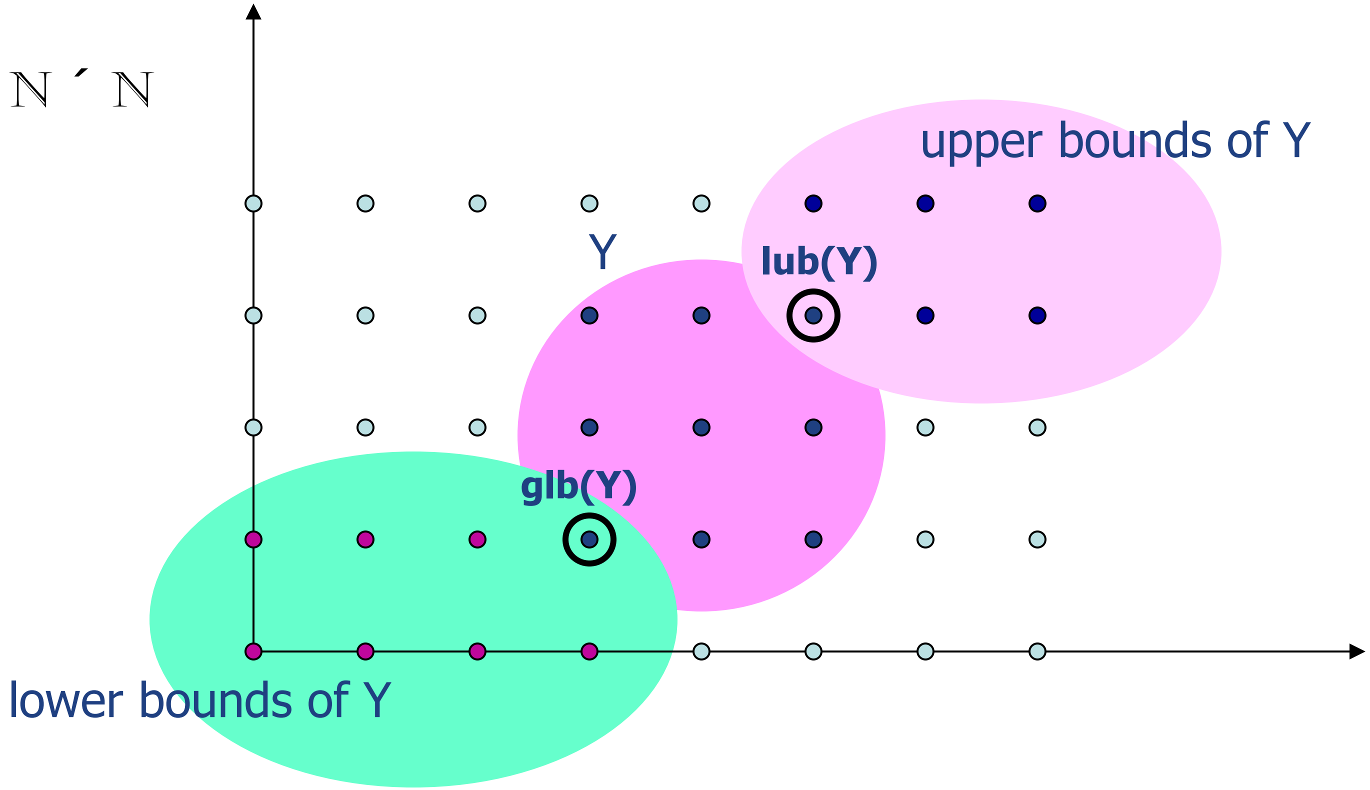
- **Definition**: Let $(S,\prec)$ be a poset and let $A \subseteq S$. If l is an element of S such that $l \prec a$ for all $a \in A$ then l is an <u>lower bound of A</u>
- An element x that is a lower bound on a subset A and is greater than all other lower bounds on A is called the <u>greatest lower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

Example



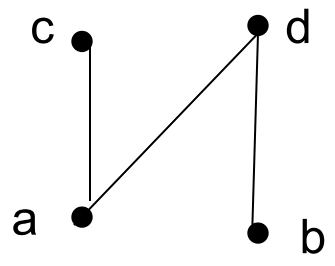
$$(x_1,y_1) \leq_{\mathbb{N} \times \mathbb{N}} (x_2,y_2) \Leftrightarrow x_1 \leq_{\mathbb{N}} x_2 \wedge y_1 \leq_{\mathbb{N}} y_2$$

Example



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

Extremal Elements: Example 1



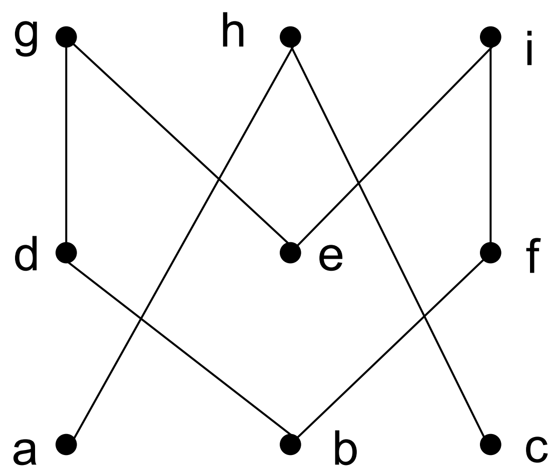
What are the minimal, maximal, minimum, maximum elements?

- 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

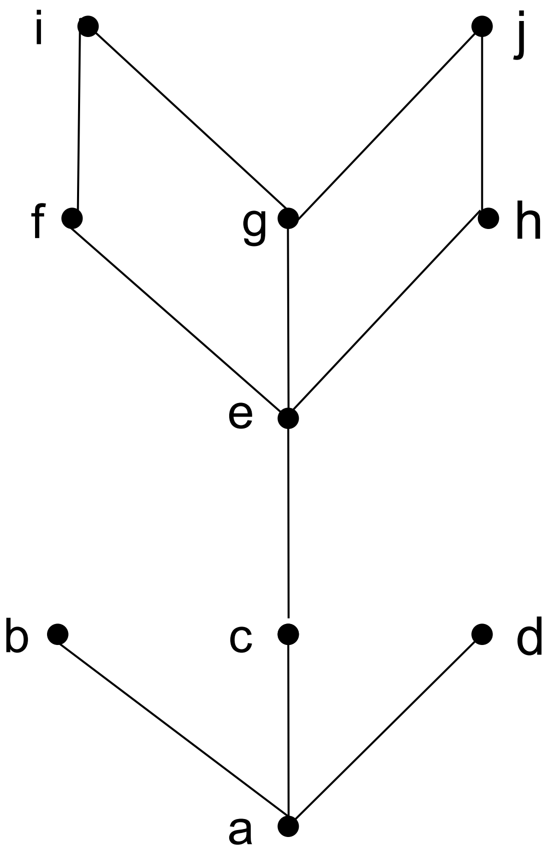
{a,c}

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

{b,d}

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

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 a
  - Upper bounds: ∅, thus lub DNE

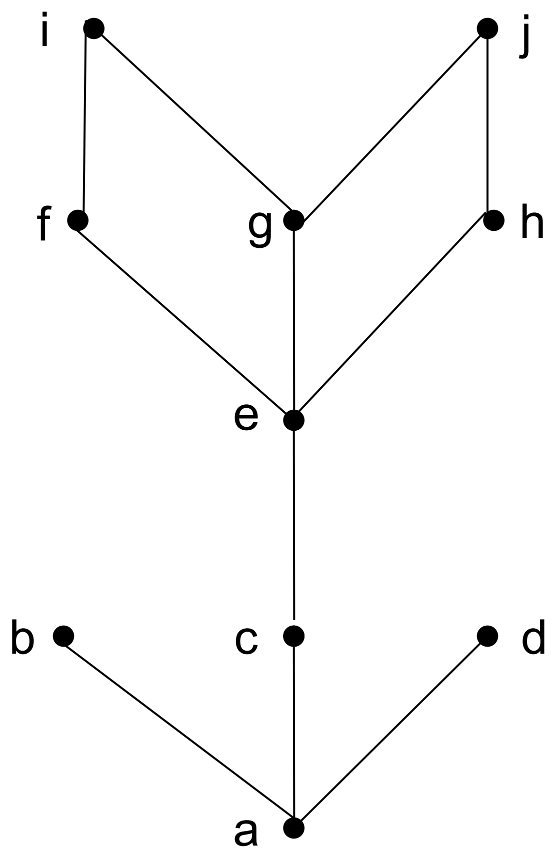
Lattices

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

Lattices: Example 1

- Is the example from before a lattice?

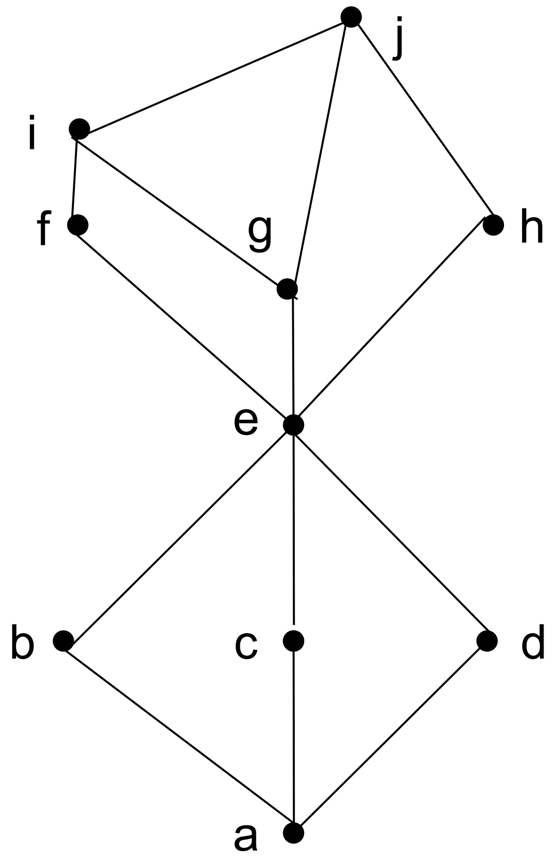
- **No, because the pair {b,c} does not have a least upper bound**



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?

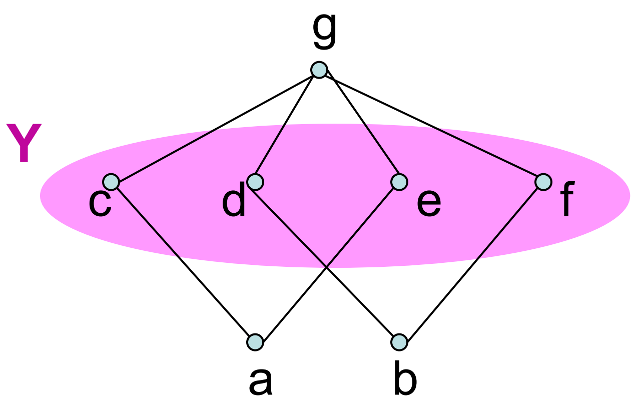
- To show that a partial order is not a lattice, it suffices to find a pair that does not have a lub or a glb (i.e., a counter-example)
- For a pair not to have an lub/glb, the elements of the pair must first be <u>incomparable</u> (Why?)
- You can then view the upper/lower bounds on a pair as a sub-Hasse 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

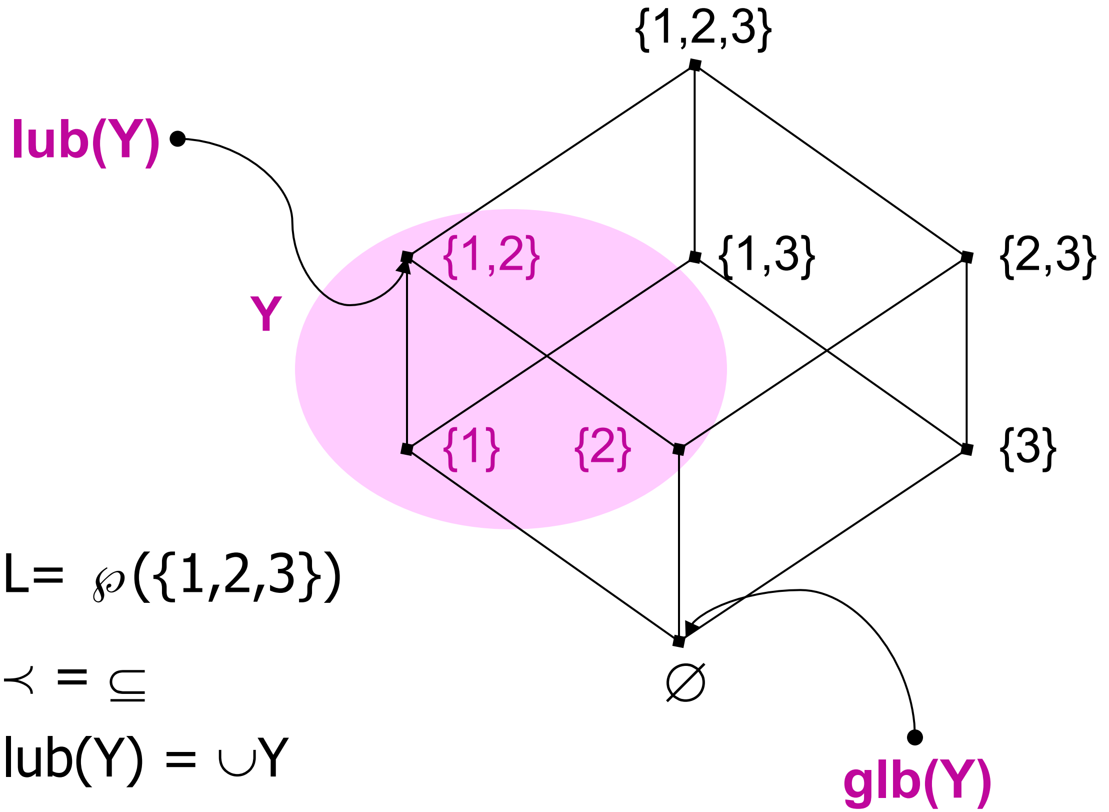


- L= {a,b,c,d,e,f,g}
- $\leq$ ={(a,c), (a,e), (b,d), (b,f), (c,g), (d,g), (e,g), (f,g)}^{T}
- (L,$\leq$) is not a lattice:
  a and b are lower bounds of Y, but a and b are not comparable

Exercise

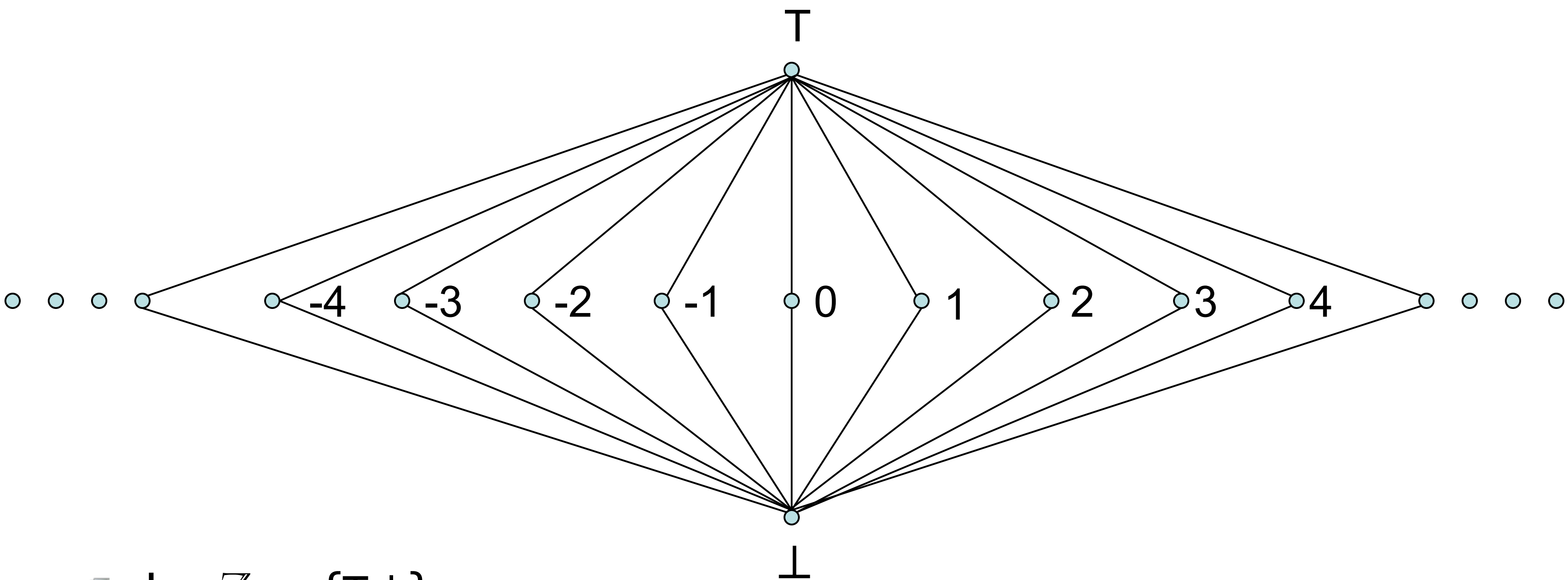
- Prove that "Every finite lattice is a complete lattice".

Example



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

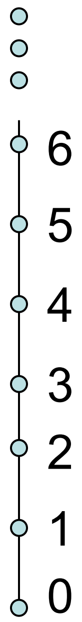
Example



- L= $\mathbb{Z} \cup \{T,\perp\}$
- $\forall\ n \in \mathbb{Z} : \perp \prec n \prec T$
- This is a complete lattice, with infinite elements

Example

- L= $\mathbb{Z}_+$
- $\prec$ total order on $\mathbb{Z}_+$
- lub = max
- glb = min



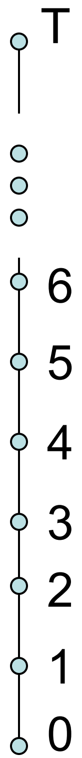
It is a lattice, but not complete:

For instance, the set of even numbers has no lub

Example

- L= $\mathbb{Z}_+ \cup \{T\}$
- $\prec$ total order on $\mathbb{Z}_+ \cup \{T\}$
- lub = max
- glb = min

This is a complete lattice



Examples

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

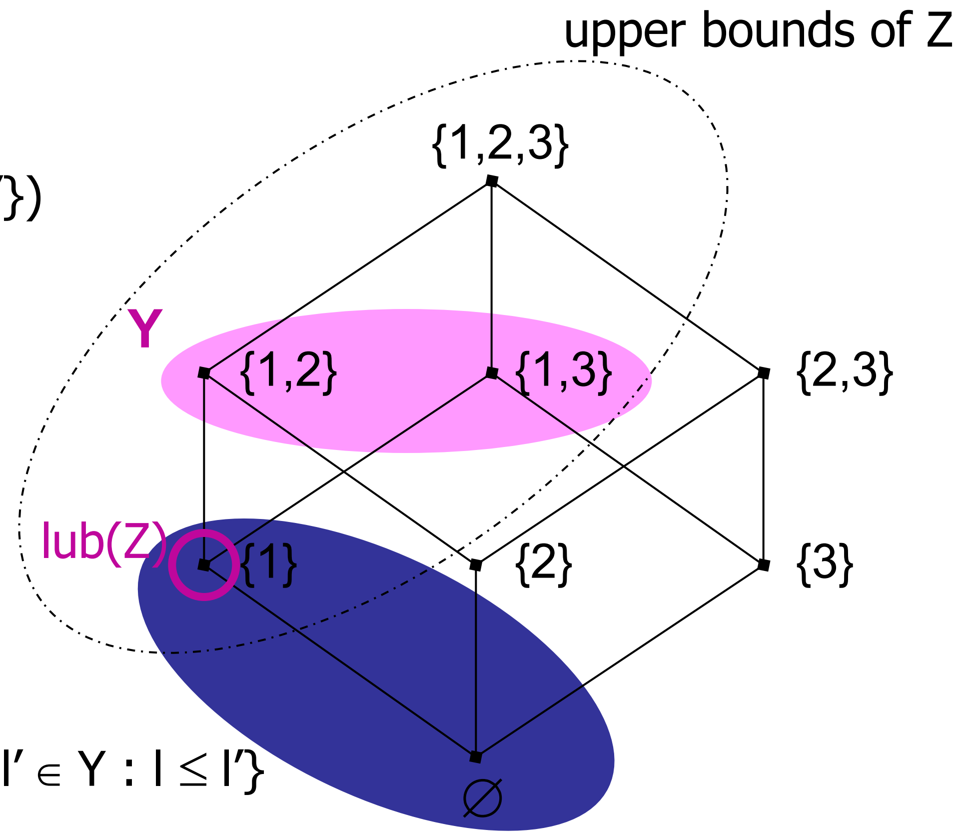
- L=Q (rational numbers) with $\prec \, = \, \leq$ (total order)
- (Q, $\leq$) is not a complete lattice
- The set $\{x \in Q \mid x^2 < 2\}$ has upper bounds but there is no least upper bound in Q.

- Theorem:
  Let $(L, \prec)$ 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:
  - $1 \Rightarrow 2$ and $1 \Rightarrow 3$ by definition
  - In order to prove that $2 \Rightarrow 1$, let us define for each $Y \subseteq L$

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

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



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

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

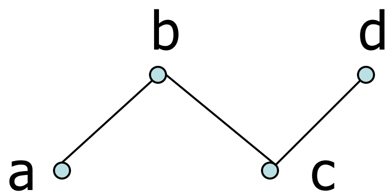
$$p_1 \leq_P p_2 \Rightarrow \varphi(p_1) \leq_Q \varphi(p_2)$$

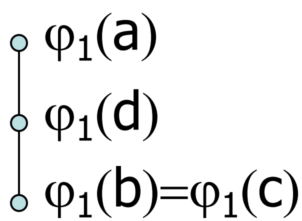
- embedding if

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

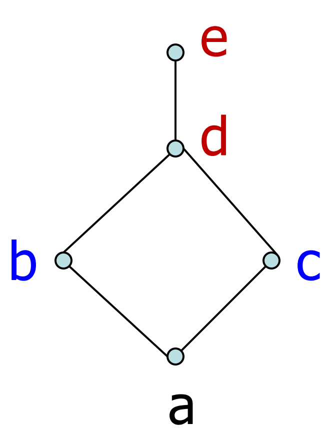
- Isomorphism if it is a surjective embedding

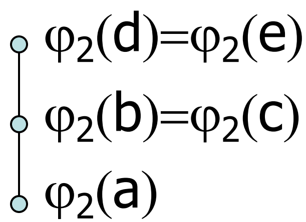
Examples





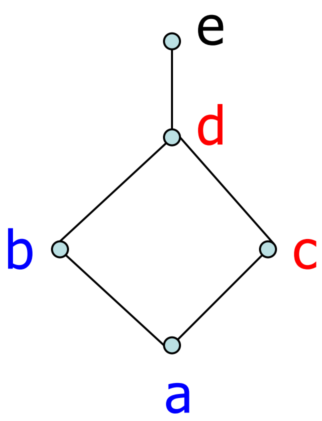
- φ_1 is not monotone

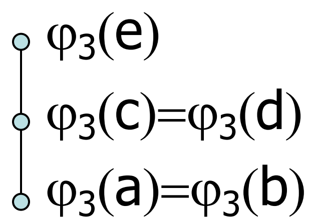




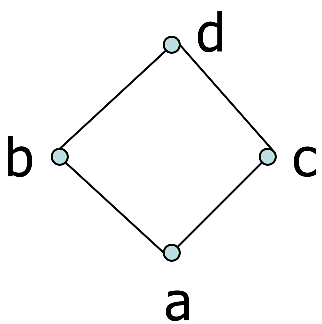
- φ_2 is monotone, but it is not an embedding: $\varphi_2(b) \leq_Q \varphi_2(c)$ but it is not true that $b \leq_P c$

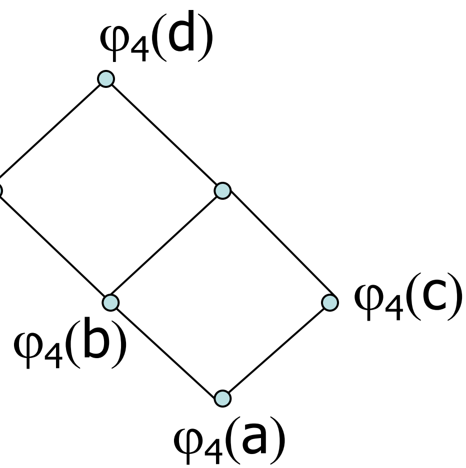
Examples





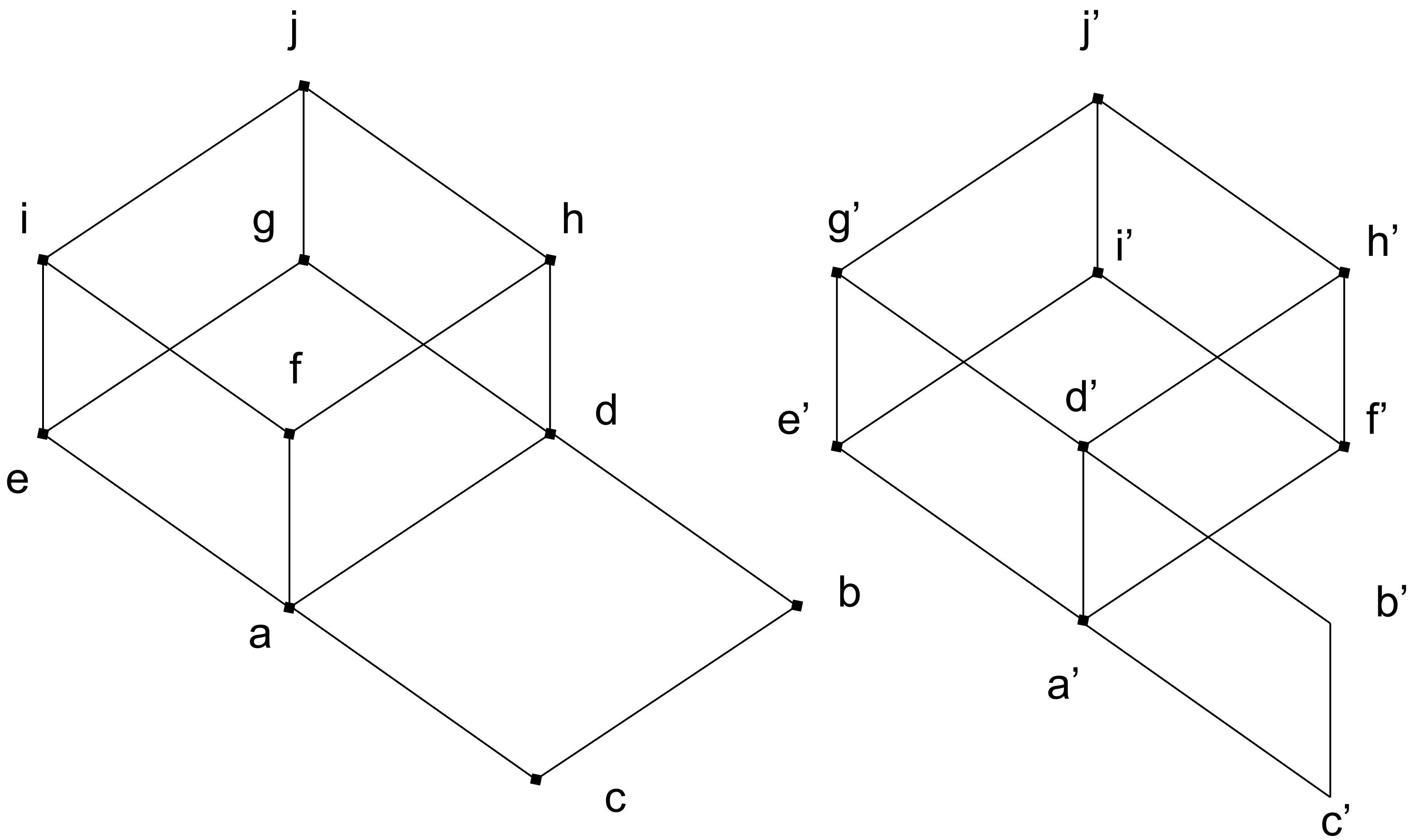
- φ_3 is monotone but it is not an embedding: $\varphi_3(b) \leq_Q \varphi_3(c)$ but it is not true that $b \leq_P c$





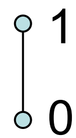
- φ_4 is an embedding, but not an isomorphism.

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, $\varphi(\varnothing)=0$.

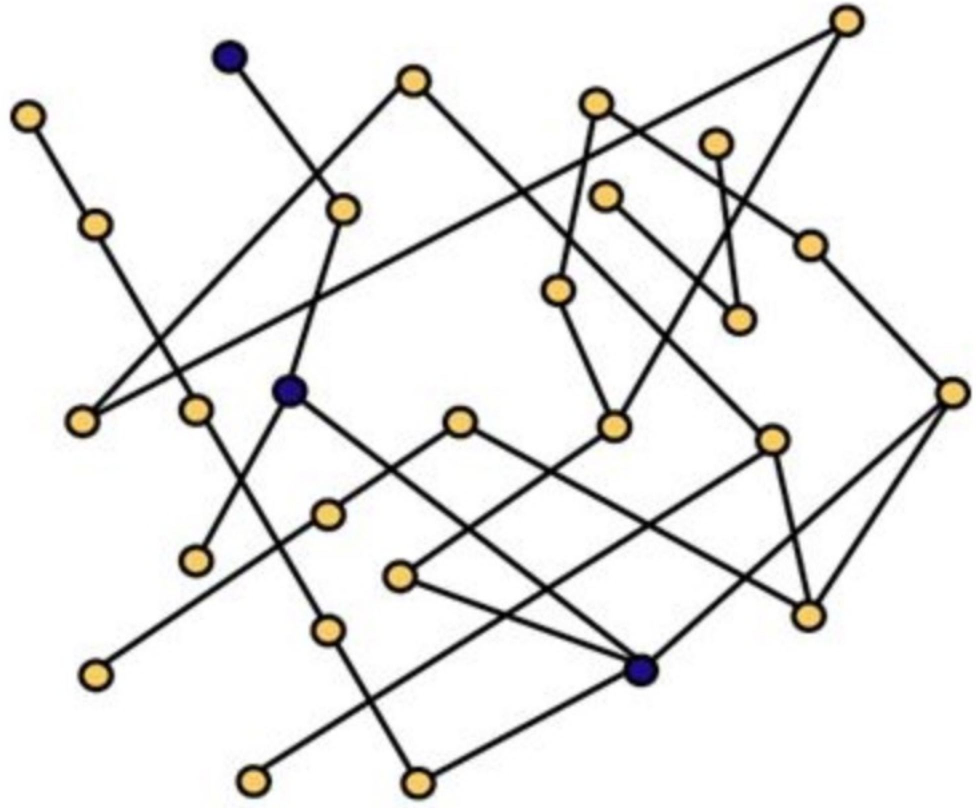
- φ from $(\wp(\mathbb{Z}), \subseteq)$ to $(\wp(\mathbb{Z}), \subseteq)$, defined by:

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

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

  $\varphi(U)= \varnothing$ otherwise

Chains



- A set of points in a poset is a chain if every pair of points in the set are comparable.
- Here, the set of blue points is a chain

Ascending chains

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

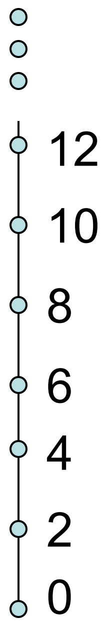
$$n \leq m \Rightarrow l_n \leq l_m$$

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

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

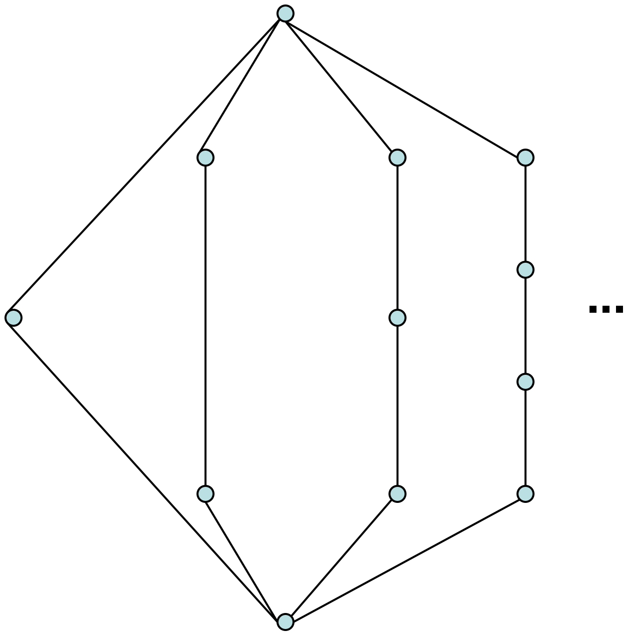
- A partial order $(L, \leq)$ satisfes the ascending chain condition (ACC) iff each ascending chain converges.

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

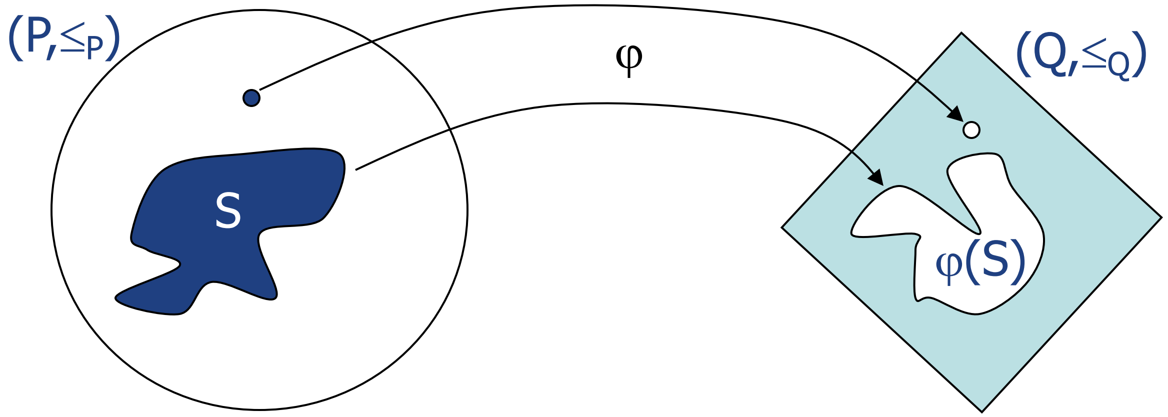
- If P is a lattice, it has a bottom element and satisfies ACC, then it is a complete lattice

- 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

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



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):

$$\mathrm{Fix}(f) = \{\, I \in P \;\mid\; f(I)=I \,\}$$

Fixpoint on Complete Lattices

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

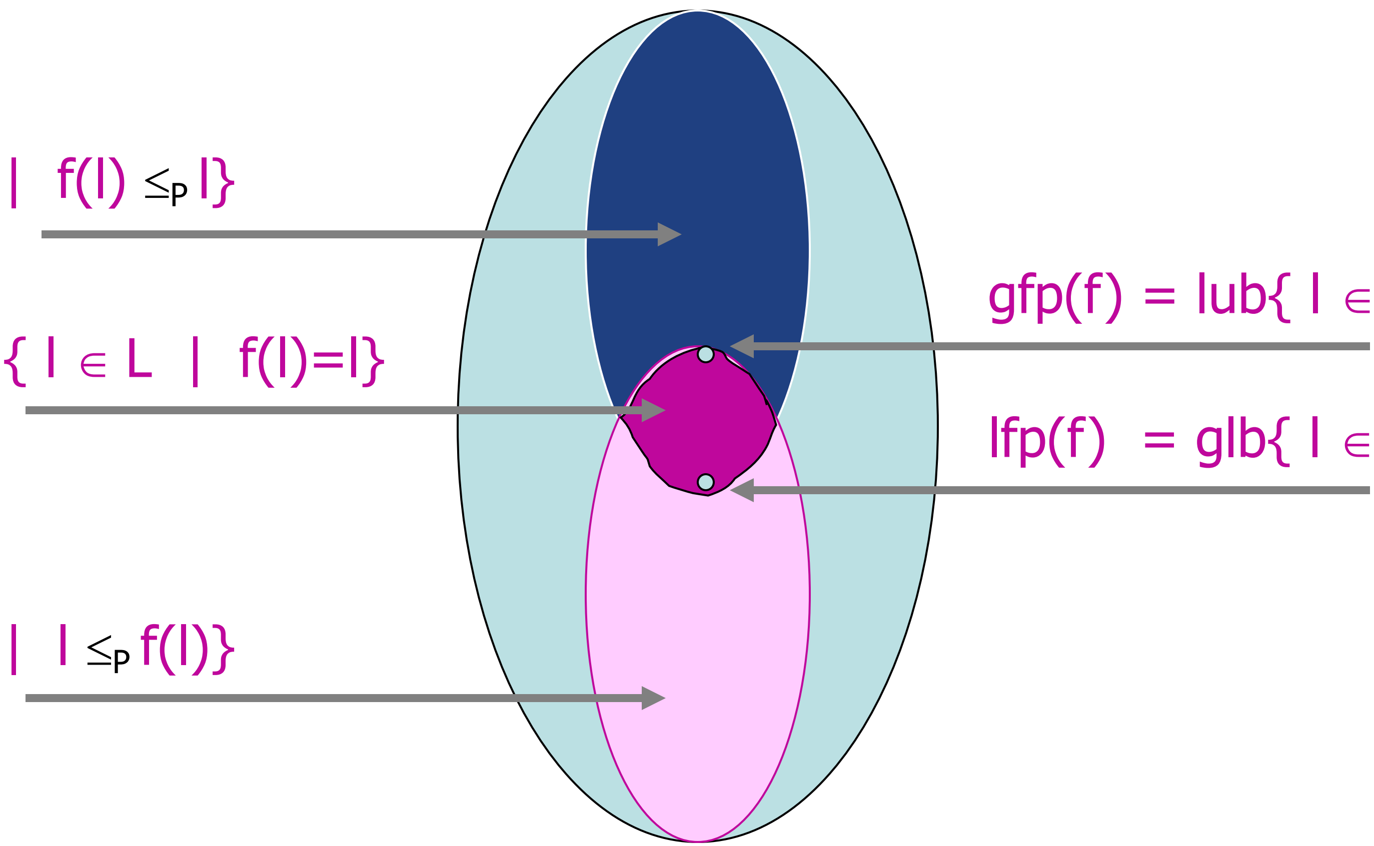
- Fix(f) is also a complete lattice:

$$\begin{aligned} lfp(f) &= glb(Fix(f)) && \in Fix(f) \\ gfp(f) &= lub(Fix(f)) && \in Fix(f) \end{aligned}$$

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

$$\begin{aligned} lfp(f) &= glb\{\, l \in L \mid f(l) \leq l \,\} \\ gfp(f) &= lub\{\, l \in L \mid l \leq f(l) \,\} \end{aligned}$$

Fixpoints on Complete Lattices



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 exists , and it is equal to α

Concluding remarks: why did we do it?

- Partial orders provide a **mathematical foundation** for reasoning about program execution, abstract domains, concurrency, and dependency resolution in static analysis.
- By structuring program properties and constraints as **partially ordered sets**, static analysis can efficiently **approximate behavior, detect errors, and prove correctness**.