# Abstract Interpretation

1977 Cousot and Cousot

E.g. predicate abstraction

$$\mathrm{Preds} = \{x>0,\ x<0,\ x=0\}$$

$x>0$
$x<0$
$x=0$
true
false

$$\begin{tikzcd}[column sep=small]
 & \text{true} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
x>0 \arrow[dr, dash] & x<0 \arrow[d, dash] & x=0 \arrow[dl, dash] \\
 & \text{false} &
\end{tikzcd}$$

$\sqsubseteq$

subset or implication relation

Sign lattice $= \{+, -, 0, \top, \bot\}$

true

false

$a = 42 \longrightarrow a \mapsto +,\ b \mapsto \top,\ c \mapsto \top$

$b = 87 \longrightarrow a \mapsto +,\ b \mapsto +,\ c \mapsto \top$

if (input)

$\quad c = a + b \longrightarrow a \mapsto +,\ b \mapsto +,\ c \mapsto +$

else

$\quad c = a - b \longrightarrow \{a \mapsto +,\ b \mapsto +,\ c \mapsto \top\}$

$a \mapsto +,\ b \mapsto +,\ \boxed{c \mapsto \top}$

$x > 0 \lor x < 0 \rightsquigarrow \top$

Lattices

SPA

A partial order is a set $S$ with a relation $\sqsubseteq$

reflexive, transitive, antisymmetric

$\leq$

$x, y \in S$ . if $x \sqsubseteq y$ then

"$y$ is a safe overapproximation of $x$"

---

join (least upper bound $\sqcup$) LUB

let $X \subseteq S$ .

$y \in S$ is an upper bound for $X$

$X \sqsubseteq y$ (if all $x \in X$, $x \sqsubseteq y$)

$X \sqsubseteq \sqcup X$ and $\forall y \in S$ . if $X \sqsubseteq y$ then $\sqcup X \sqsubseteq y$

$x \sqcup y$

---

Let $S = \mathbb{Z}$, $\sqsubseteq = \leq$

$X = \{1, 2, 3\} \subseteq S$

$X \leq \sqcup X$ all $x \in X$ are less than or equal to $\sqcup X = 3$

meet (greatest lower bound) glb

$\sqcap X$

$\sqcap X \sqsubseteq X$ and $\forall y \in S.$ if $y \sqsubseteq X$ then $y \sqsubseteq \sqcap X$

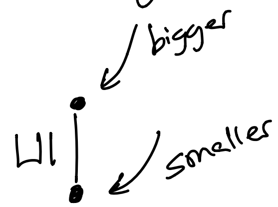
---

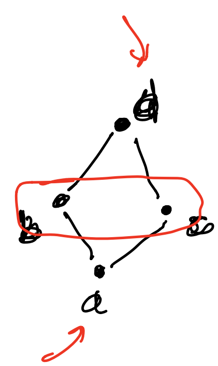
a lattice is a $(S, \sqsubseteq)$ and for all $X \subseteq S$
$\sqcap X$, $\sqcup X$ are defined (exist)

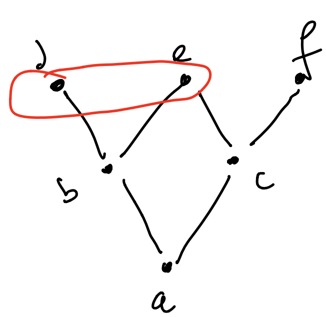
---

E.g. Hasse diagrams

$S = \{\circ\}$

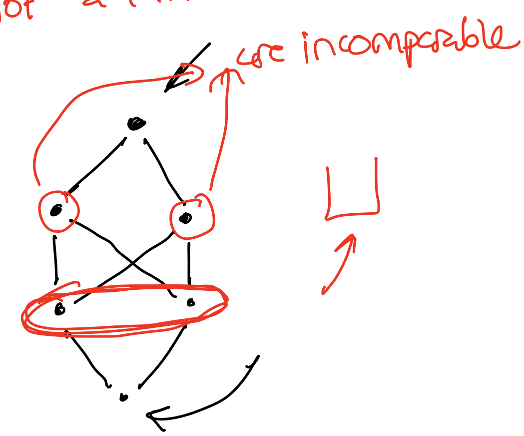



d $\sqcup$ e is not defined

Not a lattice



A lattice has a unique largest element ($\top$) and smallest element ($\bot$)

height of a lattice is the longest path from $\bot$ to $\top$

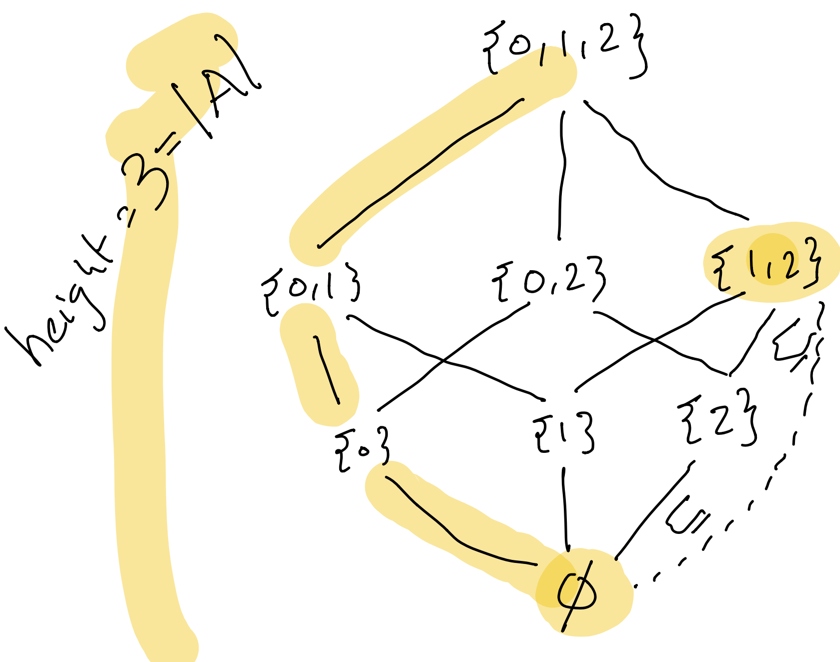
## Constructing lattices

Every finite set $A$, take $(2^A, \subseteq)$

this is a lattice where $\top = A$, $\bot = \emptyset$

powerset lattice

$A = \{0,1,2\}$



## product lattice

if $L_1, \ldots, L_n$ are lattices then

$$L_1 \times \ldots \times L_n = \{(x_1, \ldots, x_n) \mid x_i \in L_i\}$$

where

$$(x_1, \ldots, x_n) \sqsubseteq (x'_1, \ldots, x'_n)$$

iff

$x_i \sqsubseteq x'_i$ for all $i \in [1, n]$

shorthand : $L^n$

## map lattice

if $A$ is a set and $L$ is a lattice, then

$$A \to L = \{[a_1 \mapsto x_1, \dots, a_n \mapsto x_n] \mid A = \{a_1, \dots, a_n\}, \ x_i \in L\}$$

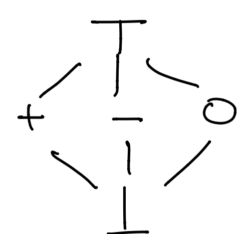
$f \sqsubseteq g$ iff $f(a_i) \sqsubseteq g(a_i)$ for all $a_i \in A$

over $L$

over $A \to L$

---

E.g. $Sign = \{+, -, 0, \top, \bot\}$




Vars: a set of variables

$Vars \to Sign$ lattice

$LN \to (Vars \to Sign)$

line numbers

$x = 10$

$y = x + 5$