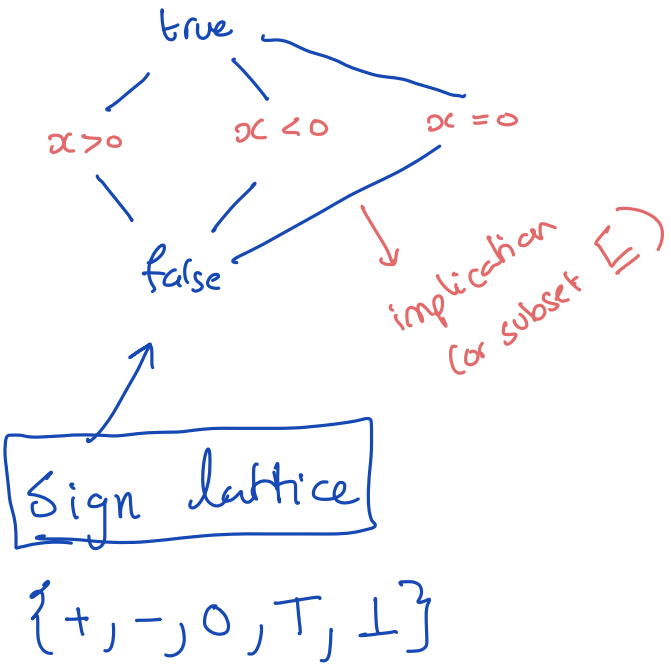
Horn clause ✓

Abstract Interpretation 1977 Cousot and Cousot

E.g. Preds = $\{x>0,\ x<0,\ x=0\}$



false $\Rightarrow x>0$

$x>0 \Rightarrow$ true

Sign lattice

$\{+, -, 0, T, \bot\}$

E.g.

$a = 42$ — $[a \mapsto T,\ b \mapsto T]$

$[a \mapsto +,\ b \mapsto T]$

$b = 87$ — $[a \mapsto +,\ b \mapsto +]$

$b = 0$ — $[a \mapsto +,\ b \mapsto 0,\ c \mapsto T]$

if $(c>0)$

$a = 0$ — $[a \mapsto +,\ b \mapsto 0,\ c \mapsto +]$

$[a \mapsto 0,\ b \mapsto 0,\ c \mapsto +]$

else $c \le 0$

$a = 15$ — $[c \mapsto T,\ a \mapsto +,\ b \mapsto 0]$

$[a \mapsto +,\ b \mapsto 0,\ c \mapsto T]$

join $[a \mapsto T,\ b \mapsto 0,\ c \mapsto T]$

Lattices

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

reflexive transitive antisymmetric

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

"y is a safe overapproximation of x"

---

join (least upper bound lub $\sqcup$)

$X \subseteq S$

$y \in S$ is an upper bound of X if

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

$X \sqsubseteq \bigsqcup X$ $\forall y \in S$. if $X \sqsubseteq y$ then $\bigsqcup X \sqsubseteq y$

$x \sqcup y$

E.g. $S = \mathbb{Z}$ $\sqsubseteq = \leq$

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

$\{1, 2, 3\} \leq 3$

meet (greatest lowerbound) glb $\sqcap$

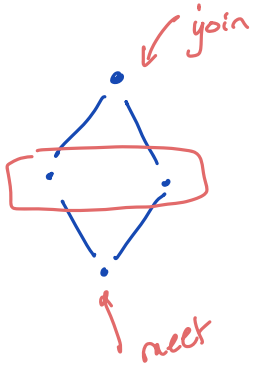
$\sqcap X \sqsubseteq X$ $\forall y \in S$ if $y \sqsubseteq X$ then $y \sqsubseteq \sqcap X$

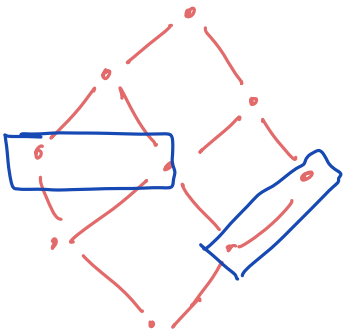
E.g. $X = \{4, 5, 6\}$ $\sqcap X = 4$

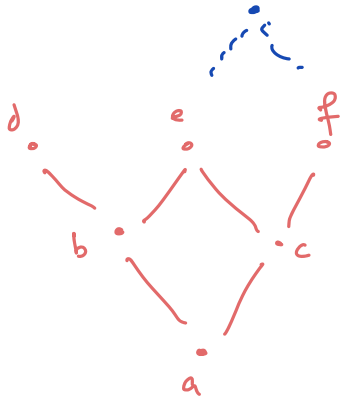
a lattice is $(S, \sqsubseteq)$ and for all $X \subseteq S$

$\sqcap X$, $\sqcup X$ are defined (exist)

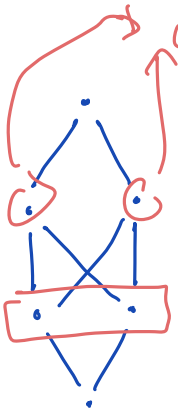
$S = \{\bullet\}$ $S = \{\bullet, \circ\}$







not a lattice



---

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

---

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

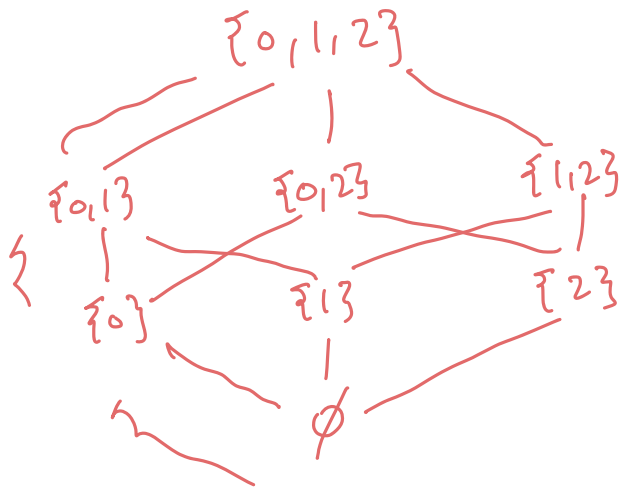
Constructing lattices (powerset lattice)

take any set A $\quad (2^A, \subseteq)$

2^A: powerset; $\subseteq$: subset

e.g. $A = \{0, 1, 2\}$

2^A



$\bigsqcup = \bigcup$

$\bigsqcap = \bigcap$

---

product lattice

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

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

where $\sqsubseteq$ is defined as follows

$$(x_1, \ldots, x_n) \sqsubseteq (x_1', \ldots, x_n')$$

iff

$$x_i \sqsubseteq x_i' \text{ for all } i \in [1, n]$$

L^n

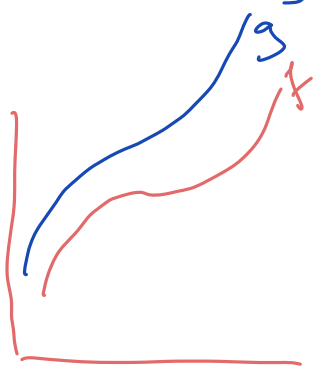
map lattice

if A is a set and L is a lattice

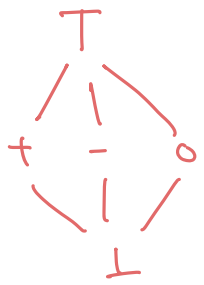
$$A \to L = \{ [a_1 \mapsto x_1, \ldots, a_n \mapsto x_n] \mid A = \{a_1, \ldots, a_n\} \; x_i \in L \}$$

$f \in A \to L \qquad g \in A \to L$

$f \sqsubseteq_{A \to L} g$ iff $f(a_i) \sqsubseteq_L g(a_i)$ for all $a_i \in A$



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



Vars = a set of variables

How can we build a lattice that tracks the sign of all Vars?

$Vars \to Sign \qquad Sign^n$

$Stmt \to (Vars \to Sign)$

↑

Line #s