« Mathematical foundations: (3) Lattice theory — Part I »

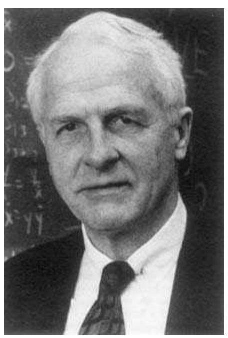
Patrick Cousot

Jerome C. Hunsaker Visiting Professor
Massachusetts Institute of Technology
Department of Aeronautics and Astronautics

cousot@mit.edu
www.mit.edu/~cousot

Course 16.399: "Abstract interpretation"

http://web.mit.edu/afs/athena.mit.edu/course/16/16.399/www/



Garrett Birkhoff

George Grätzer

Posets

Binary relation

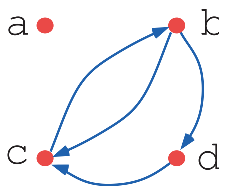
- Given sets $X_1, X_2, \ldots, X_n$, the cartesian product is

$$X_1 \times X_2 \times \ldots \times X_n \stackrel{\mathrm{def}}{=} \{\langle x_1, \ldots, x_n\rangle \mid \bigwedge_{i=1}^{n} \in X_i\}$$

- An n-ary relation r on $X_1, X_2, \ldots, X_n$ is $r \in \wp(X_1 \times X_2 \times \ldots \times X_n)$ i.e. $r \subseteq X_1 \times X_2 \times \ldots \times X_n$
- If $n = 2$, r is binary
- A binary relation r on a set X is $r \in \wp(X \times X)$
- We write $x \; r \; y$ for $\langle x, y\rangle \in r$

Graph of a binary relation

– A relation can be seen as a graph where X is the set of vertices and r is the set of arcs. For example



$$X = \{a, b, c, d\}$$
$$r = \{\langle c,\ b\rangle, \langle b,\ c\rangle, \langle b,\ d\rangle, \langle d,\ c\rangle\}$$

– Familiar relations on $\mathbb{R}$ are $<$, $\geq$, $\neq$, $=$ while on $\wp(X)$, where X is a set, we have $\subseteq$, $\supset$, etc.

Partial order

– A partial order $\leq$ on a set X is a binary relation $\leq$ on X which is

- reflexive i.e. $\forall x \in X : x \leq x$
- antisymetric i.e. $\forall x, y \in X : (x \leq y \wedge y \leq x) \Longrightarrow x = y$
- transitive i.e. $\forall x, y, z \in X : (x \leq y \wedge y \leq z) \Longrightarrow (x \leq z)$

where $x \leq y$ formally means $\langle x,\ y\rangle \in \leq$.

Poset

A poset $\langle X,\ \leq\rangle$ is a set equipped with a partial order $\leq$ on X.

Examples:

– $\langle \mathbb{N},\ \leq\rangle$ is a poset (where $\forall x, y \in \mathbb{N} : x \leq y \iff \exists z \in \mathbb{N} : x + z = y$)

– $\langle \mathbb{N},\ \geq\rangle$ is a poset (where $\forall x, y \in \mathbb{N} : x \geq y \iff x \leq y$)

Strict partial order

– if $\sqsubseteq$ is a partial order then $\sqsubset$ is its strict version $x \sqsubset y \stackrel{\text{def}}{=} x \sqsubseteq y \wedge x \neq y$, sometimes denoted $\sqsubsetneq$.

– $\not\sqsubset$, $\not\sqsubseteq$ is the negation of $\sqsubset$ and $\sqsubseteq$

– $x \not\sqsubseteq y \wedge y \not\sqsubseteq x$ means that x and y are not comparable (sometimes written $x \parallel y$).

– A strict partial order $<$ on a set X is a binary relation $<$ on X which is

- irreflexive i.e. $\forall x \in X : \neg(x < x)$
- transitive i.e. $\forall x, y, z \in X : (x < y \wedge y < z) \Longrightarrow (x < z)$

Correspondence between partial and strict partial orders

THEOREM. If $<$ is a strict partial order on X then $\leq$ defined by $x \leq y \iff x < y \vee x = y$ is a partial order on X ■

PROOF. – $x \leq x \iff x < x \vee x = x = \mathrm{ff} \vee \mathrm{tt} = \mathrm{tt}$

– $x \leq y \wedge y \leq x \iff (x < y \vee x = y) \wedge (y < x \vee x = y)$
  1. if $x = y$ antisymetry is proved
  2. if $x \neq y$ we have $x < y \wedge y < x$ whence $x < x$ by transitivity, in contradiction with irreflexivity, so this case is impossible.

– If $x \leq y \wedge y \leq z$ then $(x < y \vee x = y) \wedge (y < z \vee y = z)$
  1. if $x = y$ then $x < z \vee x = z$ so $x \leq z$
  2. if $y = z$ then $x < z \vee x = z$ so $x \leq z$
  3. Otherwise $x < y \wedge y < z$ so by transitivity $x < z$ □

THEOREM. If $\leq$ is a partial order on X then $<$ defined by $x < y \iff x \leq y \wedge x \neq y$ is a strict partial order on X ■

PROOF. – $x < x \iff x \leq x \wedge x \neq x = \mathrm{tt} \wedge \mathrm{ff} = \mathrm{ff}$

– $x < y \wedge y < z \iff (x \leq y \wedge x \neq y) \wedge (y \leq z \wedge y \neq z)$ which implies $x \leq z \wedge x \neq z$ by transitivity of $\leq$ since $x = z$ would imply $x = y = z$, a contradiction.

□

Preorder

– A preorder $\preceq$ on a set X is a binary relation $\leq$ on X which is
  - reflexive i.e. $\forall x \in X : x \preceq x$
  - transitive i.e. $\forall x, y, z \in X : (x \preceq y \wedge y \preceq z) \Longrightarrow (x \preceq z)$

(but not necessarily antisymetric)

Example: $\preceq$ on $\Sigma^{\vec{+}}$ defined by $\sigma \preceq \sigma' \iff |\sigma| \leq |\sigma'|$ is a preorder but not a partial order (since e.g. $ab \preceq bc$ and $bc \preceq ab$ but $ab \neq bc$).

THEOREM. If $\preceq$ is a preorder then $x \equiv y \stackrel{\text{def}}{=} (x \preceq y) \wedge (y \preceq x)$ is a equivalence relation. ■

PROOF. – $x \equiv x \stackrel{\text{def}}{=} (x \preceq x) \wedge (x \preceq x) = \mathrm{tt}$ since $\preceq$ is reflexive

– $x \equiv y \stackrel{\text{def}}{=} (x \preceq y) \wedge (y \preceq x) \iff (y \preceq x) \wedge (x \preceq y) \stackrel{\text{def}}{=} y \equiv x$

– $x \equiv y \wedge y \equiv z \stackrel{\text{def}}{=} (x \preceq y) \wedge (y \preceq x) \wedge (y \preceq z) \wedge (z \preceq y) \iff (x \preceq y) \wedge (y \preceq z) \wedge (z \preceq y) \wedge (y \preceq x) \Longrightarrow (x \preceq z) \wedge (z \preceq x) \stackrel{\text{def}}{=} x \equiv z$

□

Quotient[1] poset of a preorder

THEOREM. Let $\preceq$ be a preorder on a set X. Let $\equiv$ be the equivalence relation defined by $x \equiv y \iff (x \preceq y) \wedge (y \preceq x)$. Let $X/_{\equiv}$ be the quotient of X by $\equiv$. Define $\preceq_{\equiv}$[2] on $X/_{\equiv}$ by

$$[x]_{\equiv} \preceq_{\equiv} [y]_{\equiv} \stackrel{\text{def}}{=} x \preceq y$$

Then $\langle X/_{\equiv},\ \preceq_{\equiv}\rangle$ is the quotient poset of the preorder $\langle X,\ \preceq\rangle$. ■

[1] Recall that if $\equiv$ is an equivalence relation on a set X then the quotient $X/_{\equiv} \stackrel{\text{def}}{=} \{[x]_{\equiv} \mid x \in X\}$ is the set of equivalence classes $[x]_{\equiv} \stackrel{\text{def}}{=} \{y \in X \mid x \equiv y\}$.

[2] In general, $\preceq_{\equiv}$ is denoted $\preceq$ for short.

PROOF. – First remark that the definition of $\preceq_{\equiv}$ on $X/_{\equiv}$ is independent of the choice of the representants x and y of the classes $[x]_{\equiv}$ and $[y]_{\equiv}$ since $x' \equiv x$ and $y' \equiv y$ implies $x' \preceq x \preceq y \preceq y'$ so $x' \preceq y'$ by transitivity and reciprocally, if $x' \preceq y'$ then $x \preceq x' \preceq y' \preceq y$ so $x \preceq y$

– We have $x \preceq x$ so $[x]_{\equiv} \preceq_{\equiv} [y]_{\equiv}$

– If $[x]_{\equiv} \preceq_{\equiv} [y]_{\equiv}$ and $[y]_{\equiv} \preceq_{\equiv} [x]_{\equiv}$ then $x \preceq y \wedge y \preceq x$ so $x \equiv y$ proving that $[x]_{\equiv} = [y]_{\equiv}$

– If $[x]_{\equiv} \preceq_{\equiv} [y]_{\equiv}$ and $[y]_{\equiv} \preceq_{\equiv} [z]_{\equiv}$ then $x \preceq y \wedge y \preceq z$ whence $x \preceq z$ by transitivity proving that $[x]_{\equiv} \preceq_{\equiv} [z]_{\equiv}$

□

Restriction of a poset to a subset

If r is a binary relation on a set X and $Y \subseteq X$ then

$$r|_Y \stackrel{\text{def}}{=} \{\langle x,\ y\rangle \in r \mid x, y \in Y\}$$

THEOREM. If $\langle X,\ \leq\rangle$ is a poset and $Y \subseteq X$ then $\langle X,\ \leq|_Y\rangle$ is also a poset ■

PROOF. – If $x \in Y$ then $x \leq|_Y x = x \leq x = tt$

– If $x, y \in Y$ then $x \leq|_Y y \wedge y \leq|_Y x$ implies $x \leq y \wedge y \leq x$ so $x = y$

– If $x, y, z \in Y$ then $x \leq|_Y y \wedge y \leq|_Y z$ implies $x \leq y \leq z$ so $x \leq z$ on X hence $x \leq|_Y z$ on Y since $x, z \in Y$.

□

Intervals

It follows that if $\langle X,\ \leq\rangle$ is a poset and $a, b \in X$, then

– $[a, b] \stackrel{\text{def}}{=} \{x \in X \mid a \leq x \leq b\}$

– $[a, b[\stackrel{\text{def}}{=} \{x \in X \mid a \leq x < b\}$

– $]a, b] \stackrel{\text{def}}{=} \{x \in X \mid a < x \leq b\}$

– $]a, b[\stackrel{\text{def}}{=} \{x \in X \mid a < x < b\}$

are all posets for $\leq$.

Equality

THEOREM. The only partial order which is also an equivalence relation is equality. ■

PROOF. Let $\approx$ be an equivalence relation which is a partial order

—	$x \approx y$	
$\Longrightarrow$	$x \approx y \wedge y \approx x$	$\wr$by symmetry of equivalence$\wr$
$\Longrightarrow$	$x = y$	$\wr$by antisymmetry of partial order$\wr$
—	$x = y$	
$\Longrightarrow$	$x \approx y$	$\wr$by reflexivity$\wr$

□

Inverse of a partial order

THEOREM. The inverse of a partial order is a partial order. ■

PROOF. Let $\langle X, \leq\rangle$ be a poset and $\geq$ be the *inverse* of $\leq$: $x \geq y \stackrel{\text{def}}{=} y \leq x$.

- $x \geq x$ since $x \leq x$ (reflexivity)
- $x \geq y \wedge y \geq x \Longrightarrow y \leq x \wedge x \leq y \Longrightarrow x = y$ (antisymmetry)
- $x \geq y \wedge y \geq z \Longrightarrow z \leq y \wedge y \leq x \Longrightarrow z \leq x \Longrightarrow x \geq z$ (transitivity)

□

Covering relation

Let $\langle X, \leq\rangle$ be a poset. The covering relation is

$$x \prec y \stackrel{\text{def}}{=} (x < y) \wedge \neg(\exists z \in X : x < z < y)$$

We say that "y covers x" or "x is covered by y" and write $x \prec y$

Examples:

- The covering relation of $\langle \mathbb{N}, \leq\rangle$ or $\langle \mathbb{Z}, \leq\rangle$ is $x \prec y \stackrel{\text{def}}{=} (y = x + 1)$
- The covering relation of $\langle \mathbb{R}, \leq\rangle$ is ff
- The covering relation of $\langle \wp(X), \subseteq\rangle$ is $X \prec\!\!\subseteq Y \stackrel{\text{def}}{=} \exists x \in Y \setminus X : Y = X \cup \{x\}$

If $\langle X, \leq\rangle$ is a finite poset (i.e. X is a finite set) then

$$x < y = \exists x_0, .., x_n \in X : x = x_0 \prec x_1 \prec \ldots \prec x_n = y$$

so that the order relation $\leq$ is determined by $<$ which is itself determined by the cover $\prec$. So $\langle P, \leq\rangle$ is determined by the (finite) graph of the cover $\langle X, \prec\rangle$, which can be drawn as a Hasse diagram.

Hasse diagram

Let $\langle X, \leq \rangle$ be a finite poset. Its *Hasse diagram* is a set of points

$$\{p(a) \mid a \in X\}$$

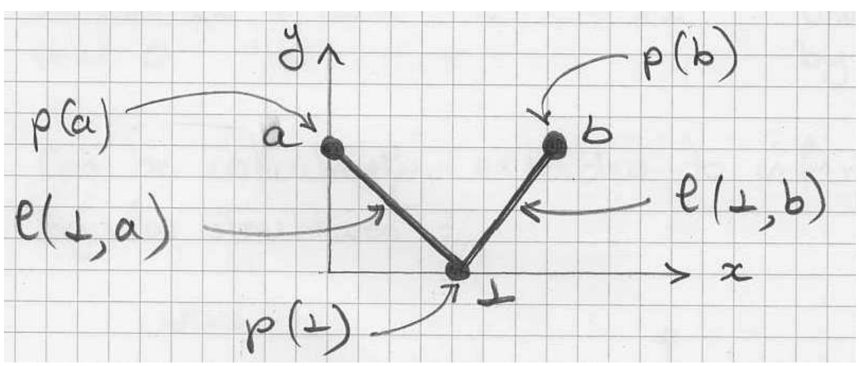
in the Euclidean plane $\mathbb{R}^2$ and a set of lines

$$\{\ell(a, b) \mid a, b \in X \wedge a \prec b\}$$

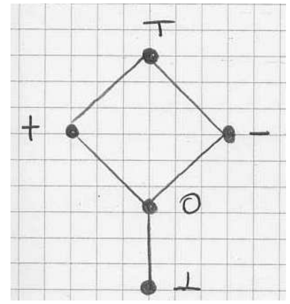
joining $p(a)$ and $p(b)$ such that:

- if $a \prec b$ then $p(a)$ is lower than $p(b)$ (that is the second coordinate of $p(a)$ is strictly less than that of $p(b)$)
- no point $p(c)$ belongs to the line $\ell(a, b)$ when $c \neq a$ and $c \neq b$

Example: $\{\perp, a, b\}$ with $\perp \prec a$, $\perp \prec b$ can be drawn as

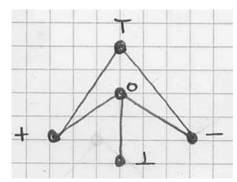


Examples of Hasse diagrams

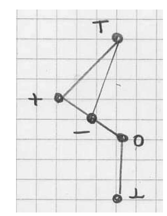


- Cover: $\perp \prec 0$, $0 \prec +$, $0 \prec -$, $+ \prec \top$, $- \prec \top$
- Partial order:
  - $\perp \leq \perp$, $\perp \leq 0$, $\perp \leq +$, $\perp \leq -$, $\perp \leq \top$
  - $0 \leq 0$, $0 \leq +$, $0 \leq -$, $0 \leq \top$
  - $+ \leq +$, $+ \leq \top$
  - $- \leq +$, $- \leq \top$
  - $\top \leq \top$

Bad diagrams for this partial order:

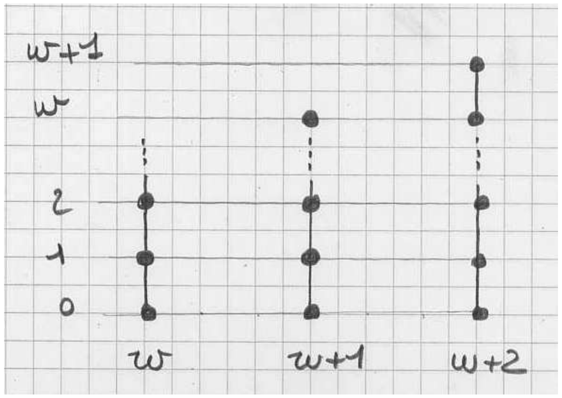


$0 \prec +$ but $+$ lower than 0



line $\ell(0, +)$ cut by $-$

Can be intuitively extended to infinity for regular structures, as shown by the following examples:



Chain

- A chain of a poset $\langle X, \leq \rangle$ is a subset $C \subseteq X$ such that

$$\forall x, y \in C : (x \leq y) \vee (y \leq x)$$

- A poset $\langle X, \leq \rangle$ is a chain iff X is a chain of $\langle X, \leq \rangle$
- Example: $\langle \mathbb{N}, \leq \rangle$

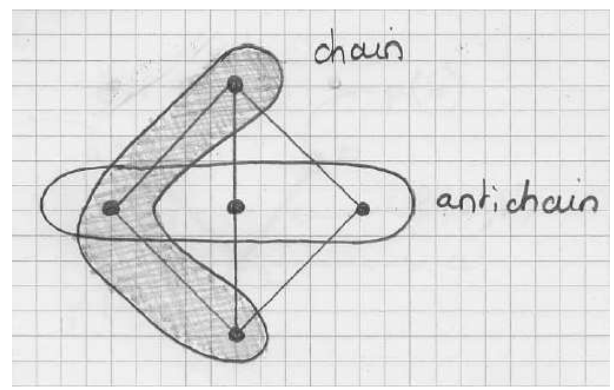
Antichain

- A antichain of a poset $\langle X, \leq \rangle$ is a subset $A \subseteq X$ such that

$$\forall x, y \in A : (x \leq y) \Longrightarrow (x = y)$$

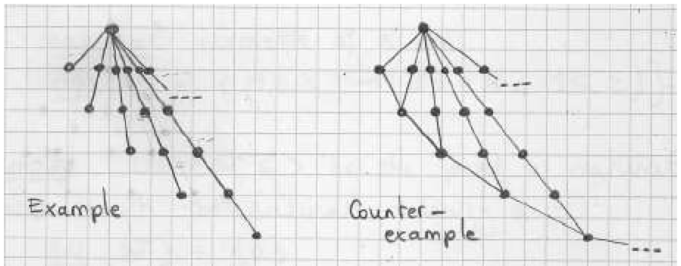
- A poset $\langle X, \leq \rangle$ is an antichain iff X is a antichain of $\langle X, \leq \rangle$
- Example: $\langle \mathbb{N}, = \rangle$

Example of chain and antichain



Chain conditions: infinite chains

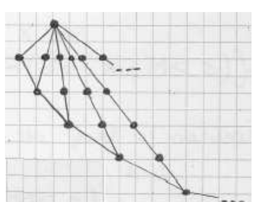
– A poset $\langle P, \leq\rangle$ has no infinite chain iff all chains in P are finite



Chain conditions: ACC

– A poset $\langle P, \leq\rangle$ satisfies the ascending chain condition (ACC) iff any infinite sequence $x_0 \leq x_1 \leq \ldots \leq x_n \leq \ldots$ of elements x_n of P is not strictly increasing that is $\exists k \geq 0 : \forall j \geq k : x_k = x_j$

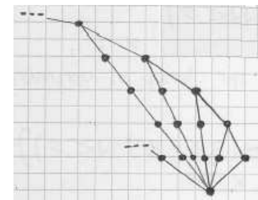
– Example:



Chain conditions: DCC

– A poset $\langle P, \leq\rangle$ satisfies the descending chain condition (DCC) iff any infinite sequence $x_0 \geq x_1 \geq \ldots \geq x_n \geq \ldots$ of elements x_n of P is not strictly decreasing that is $\exists k \geq 0 : \forall j \geq k : x_k = x_j$

– Example:



Toset, Woset

– A poset $\langle P, \leq\rangle$ is total whenever any two elements are comparable:

$$\forall x, y \in P : (x \leq y) \vee (y \leq x)$$

– A toset $\langle P, \leq\rangle$ is a poset such that $\leq$ is total

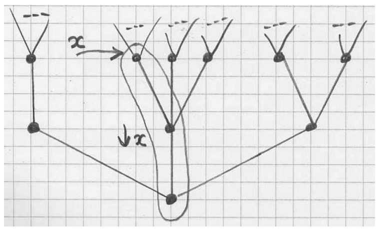
– A woset $\langle P, \leq\rangle$ is a toset satisfying DCC

– Examples and counter-examples:

  - If X is a set with at least two different elements then $\langle \wp(X), \subseteq\rangle$ is not a toset (since not all subsets are comparable)
  - $\langle \mathbb{N}, \leq\rangle$ is a woset
  - $\langle \mathbb{Z}, \leq\rangle$ is a toset but not a woset

Tree

- If $\langle P, \leq \rangle$ is a poset and $x \in P$ then the downset of x is $\downarrow x \stackrel{\text{def}}{=} \{y \in P \mid y \leq x\}$
- A tree is a poset $\langle T, \leq \rangle$ such that for all $x \in T$, $\langle \downarrow x, \leq \rangle$ is a woset
- Example:



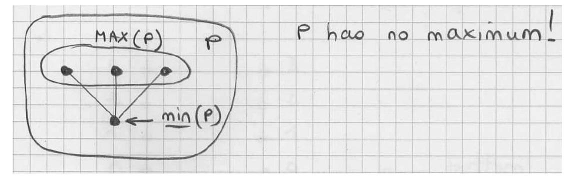
Minimal and maximal elements of a poset

- Let X be a subset of a poset $\langle P, \leq \rangle$
- The minimal elements of X are
$$\text{MIN}(X) \stackrel{\text{def}}{=} \{m \in X \mid \neg(\exists x \in X : x < m)\}$$
- The maximal elements of X are
$$\text{MAX}(X) \stackrel{\text{def}}{=} \{M \in X \mid \neg(\exists x \in X : M < x)\}$$
- Example : let $\langle \mathbb{N}, \leq \rangle$ be the poset of natural numbers with the natural ordering $\leq$:
  - $\text{MIN}(\mathbb{N}) = \{0\}$
  - $\text{MAX}(\mathbb{N}) = \emptyset$

Minimum and maximum

Note the difference with

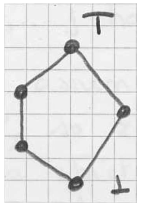
- the minimum $\min(X)$ of X, if any:
$$\min(X) \in X \wedge \forall x \in X : \min(X) \leq x$$
- the maximum $\max(X)$ of X, if any:
$$\max(X) \in X \wedge \forall x \in X : x \leq \max(X)$$



Top and bottom elements of a poset, if any

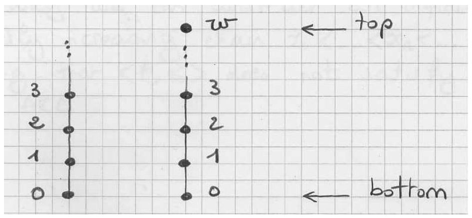
A poset $\langle P, \leq \rangle$ has

- a top element/supremum/maximum $\top$ iff
$$\top \in P \wedge \forall x \in P : x \leq \top$$
- a bottom element/infimumminimum $\perp$ iff
$$\perp \in P \wedge \forall x \in P : \perp \leq x$$
- By antisymmetry, the top and bottom elements are unique, if any



– The bottom element of $\langle \omega, \leq \rangle$ is 0. There is no top.

– The bottom element of $\langle \omega + 1, \leq \rangle$ is 0. The top is ω.



Ascending chain condition (ACC) revisited

THEOREM. A poset $\langle P, \leq \rangle$ satisfies the ACC iff every non-empty subset X of P has a maximal element. ■

PROOF. We prove by contradiction that $\langle P, \leq \rangle$ does not satisfies the ACC iff evry non-empty subset X of P has no maximal element.

– Assume $x_0 < x_1 < \ldots < x_n < \ldots$ in P, then $\{x_0, x_1, \ldots, x_n, \ldots\}$ has no maximal element.

– Reciprocally, assume X is a non-empty subset of P, so $x_0 \in X$. We have constructed a strictly increasing chain $x_0 < \ldots < x_n$ with $n = 0$.
  Assume we have constructed $x_0 < \ldots < x_n$ with $n \geq 0$. Then $\{x_0, x_1, \ldots, x_n\} \subseteq X$ has no maximal element. Therefor $\exists x_{n=1} : x_{n+1} > x_n$, proving that we can construct $x_0 < \ldots < x_n < x_{n+1}$. In this way, we can construct an infinite strictly increasing chain $x_0 < x_1 < \ldots < x_n < \ldots$ in X proving that $\langle P, \leq \rangle$ does not satisfy the ACC.

□

Absence of infinite chains in posets satisfying the ACC and DCC

THEOREM. A poset $\langle P, \leq \rangle$ has no infinite chain iff it satisfies both ACC and DCC ■

PROOF. Clearly if P does not satisfies the ACC and DCC then P has either an infinite strictly inceasing chain of a strict decreasing chain. By contraposition, a poset without infinite chain satisfies both ACC and DCC.

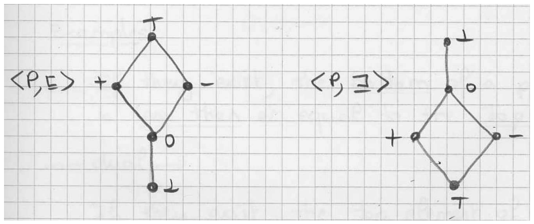
Conversely, let $\langle P, \leq \rangle$ satisfying bothh ACC and DCC. Assume by redution ad absurdum, that *P* contains an infinite chain C: $\forall x, y \in C : x \neq y \Longrightarrow (x < y) \vee (y < x)$. If A is a non empty subset of C, hence of P, by the ACC on P, A has a maximal element m. If $a \in A$ then $a \leq m$ or $m \leq a$ which implies $m = a$ by maximality of m. Hence $\forall a \in A : a \leq m$, proving that any non-empty subset A of C has a greatest element.

Let x_1 be the greatest element of C, let x_2 be the greatest element of $C \setminus \{x_1\}$, …, x_n be the greatest element of $C \setminus \{x_1, \ldots, x_{n-1}\}$; Then $x_1 \succ x_2 \succ x_3 \succ \ldots \succ x_n \succ \ldots$ is an infinite decreasing, covering chain in P, in contardiction withh DCC. □

Dual of a poset

– The dual of a poset $\langle P, \leq\rangle$ is $\langle P, \geq\rangle$ where $\geq$ is the inverse of $\leq$: $x \geq y \iff y \leq x$.

– Example:



Dual statement

– To each statement $\Phi^{\leq}$ about a poset $\langle P, \leq\rangle$ corresponds a dual statement $\Phi^{\geq}$ about the dual $\langle P, \geq\rangle$

– Examples:

Statement $\Phi^{\leq}$	Dual statement $\Phi^{\geq}$
$x \leq y$	$x \geq y$
$x < y$	$x > y$
$\bot$ is the bottom	$\top$ is the top
$\mathrm{MAX}(X)$	$\mathrm{MIN}(X)$
min	max
...	...

Duality principle

– Given a statement $\Phi^{\leq}$ about posets which is true of all posets, the dual statement $\Phi^{\geq}$ is also true of all posets.

Example 1 of dual statement

If they exist, the *bottom* of a poset is *less than* or equal to the *top*

dual $\rightsquigarrow$

If they exist, the *top* of a poset is *greater than* or equal to the *bottom*

Example 2 of dual statement

THEOREM. The top element of a poset, if any, is unique. ■

PROOF. Let $\top \in P$ and $\top' \in P$ be two top elements of a poset $\langle P, \leq \rangle$. So $\forall x \in P : x \leq \top$ and $\forall y \in P : y \leq \top'$. In particular for $x = \top'$ and $y = \top$ we get $\top' \leq \top$ and $\top \leq \top'$ whence $\top = \top'$ by antisymetry. □

THEOREM. The bottom element of a poset, if any, is unique. ■

PROOF. By duality. □

Upset, downset

– Let $\langle P, \leq \rangle$ be a poset

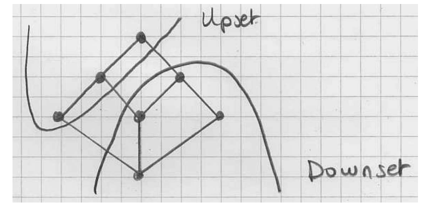
– $D \subseteq P$ is a down-set (or decreasing set or order-ideal or ideal) iff

$$\forall x \in D : \forall y \in P : (y \leq x) \Longrightarrow (y \in D)$$

– Dually, $U \subseteq P$ is a up-set (or increasing set or order-filter or filter) iff

$$\forall x \in U : \forall y \in P : (y \geq x) \Longrightarrow (y \in U)$$

– Example:



– Notations ($X \subseteq P$, $x \in P$):

$$\begin{aligned}
\downarrow X &\stackrel{\text{def}}{=} \{y \in P \mid \exists x \in X : y \leq x\} \\
\downarrow x &\stackrel{\text{def}}{=} \downarrow \{x\} \\
\uparrow X &\stackrel{\text{def}}{=} \{y \in P \mid \exists x \in X : y \geq x\} \\
\uparrow x &\stackrel{\text{def}}{=} \uparrow \{x\}
\end{aligned}$$

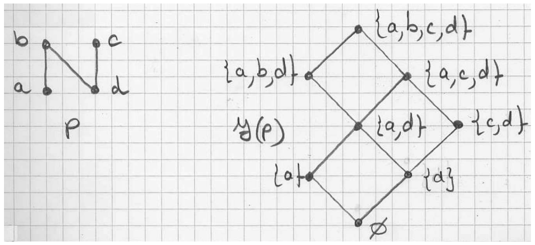
– Let $\langle P, \leq \rangle$ be a poset, $x, y \in P$. The following are equivalent:

$$\begin{aligned}
& x \leq y \\
\Longleftrightarrow\ & \downarrow x \subseteq \downarrow y \\
\Longleftrightarrow\ & \forall X \in \mathcal{I}(P) : y \in X \Longrightarrow x \in X
\end{aligned}$$

– X is a downset of $\langle P, \leq \rangle$ if and only if $P \setminus X$ is an upset of $\langle P, \leq \rangle$

The poset of all downsets of a poset

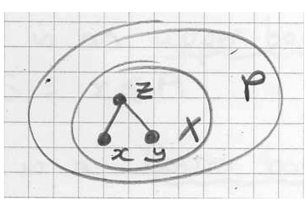
- The set $\mathcal{I}(P)$ of all downsets of a poset $\langle P, \leq\rangle$ is a poset $\langle \mathcal{I}(P), \subseteq\rangle$
- Example:



Directed set

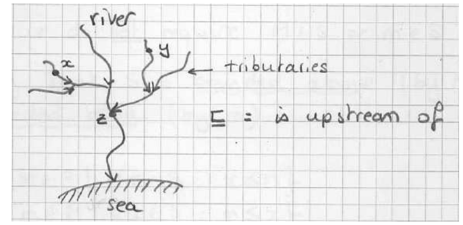
- A subset X of a poset $\langle P, \leq\rangle$ is directed if and only if

$$\forall x, y \in X : \exists z \in X : x \leq z \wedge y \leq z$$



- If X is directed on $\langle P, \leq\rangle$ then $\langle X, \leq\rangle$ is also called a directed order.

- Example:



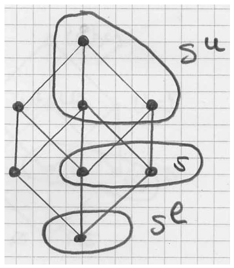
- A subset X of a poset $\langle P, \leq\rangle$ is directed iff for any finite subset X' of X there exists $z \in X$ such that $\forall x \in X' : x \leq z$.

Proof. By induction on the cardinality $|X'|$ of X'. $\square$

Upper and lower bounds

- Let $\langle P, \leq\rangle$ be a poset
- $M \in P$ is an upper bound of $S \subseteq P$ if and only if $\forall x \in S : x \leq M$.
- Dually, $m \in P$ is a lower bound of $S \subseteq P$ if and only if $\forall x \in S : m \leq x$.
- Note: it is not required that $M \in S$ or $m \in S$ as for the maximum and minimum

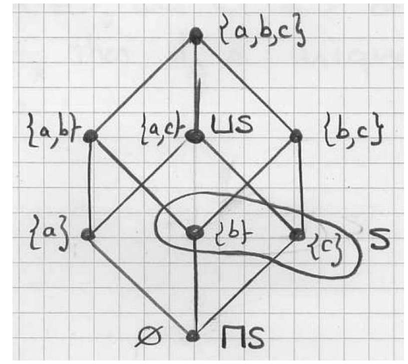
- S is said to be bounded above (by M) or, respectively, bounded below (by m)
- $S^u \stackrel{\text{def}}{=} \{M \in P \mid \forall x \in S : x \leq M\}$
  $S^\ell \stackrel{\text{def}}{=} \{m \in P \mid \forall x \in S : m \leq x\}$
- Example:



Least upper/greatest lower bound

- Let $\langle P, \leq \rangle$ be a poset and $X \subseteq P$
- The least upper bound of X, if any, is x such that:
  - x is an upper bound of X (i.e. $\forall y \in X : x \geq y$)
  - x is the least of the upper bounds of X (i.e. $\forall u \in P : (\forall y \in X : u \geq y) \Longrightarrow (x \leq u)$)
- Notation: if the least upper bound of X exists, it is denoted lub$X$, sup$X$, $\bigvee X$, $\bigsqcup X$, ...
- $\bigsqcup\limits_{x \in \Delta} f(x) \stackrel{\text{def}}{=} \bigsqcup\{f(x) \mid x \in \Delta\}$, $a \sqcup b \stackrel{\text{def}}{=} \bigsqcup\{a, b\}$

- The dual notion is that of greatest lower bound of X (glb$X$, inf$X$, $\bigwedge X$, $\bigsqcap X$, ...)
- Example:



(Move $\sqcup S$ right in the above picture).

Uniqueness of the lub/glb

THEOREM. Let $\langle P, \leq\rangle$ be a poset and $X \subseteq P$. If $\bigsqcup X$ exists, then it is unique. ∎

PROOF. Assume $\bigsqcup X$ exists and X has another lub z. We have
- $\forall x \in X : x \leq z$ since z is an upper bound of X
- $\forall z : (\forall x \in X : x \leq z) \Longrightarrow \bigsqcup X \leq z$ by def. lub so $\bigsqcup X \leq z$
- $\forall x \in X : x \leq \bigsqcup X$ since $\bigsqcup X$ is an upper bound of X so $z \leq \bigsqcup X$ since z is the least upper bound of X
- So $z = \bigsqcup X$ by antisymmetry

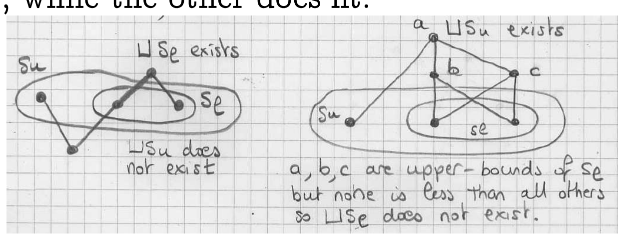
□

THEOREM. Let $\langle P, \leq\rangle$ be a poset and $X \subseteq P$. If $\bigsqcap X$ exists, then it is unique. ∎

PROOF. By duality. □

The join/meet of $\subseteq$-comparable subsets of a poset

- Let $\langle P, \leq\rangle$ be a poset and $S_\ell \subseteq S_u \subseteq P$ be two subsets of P
- The join (and by duality) of meet of S_ℓ or S_u may exist, while the other does'nt:



If $S_\ell \subseteq S_u \subseteq P$ and both $\sqcup S_\ell$ and $\sqcup S_u$ exist in $\langle P, \sqsubseteq\rangle$ the $\sqrt{S_\ell} \sqsubseteq \neg\copyright S_u$.

PROOF. By def. of $\sqcup S_u$: $\forall x \in S_u : x \sqsubseteq \sqcup S_u$. Since $S_\ell \subseteq S_u$, $\forall x \in S_\ell : x \sqsubseteq \sqcup S_u$, so by definition of the lub of S_ℓ, $\sqcup S_\ell \subseteq \sqcup S_u$. □

If $S_\ell \subseteq S_u \subseteq P$ and both $\sqcap S_\ell$ and $\sqcap S_u$ exist in $\langle P, \sqsubseteq\rangle$ the $\sqcap S_\ell \sqsupseteq \sqcap S_u$.

PROOF. By duality. □

Lub and glb properties

THEOREM. Let $\langle P, \leq\rangle$ be a poset. The empty set $\emptyset$ has a lub $\sqcup\emptyset$ in P if and only if P has a bottom (in which case $\sqcup\emptyset = \perp$). ∎

PROOF. – $\forall x \in \emptyset : (x \leq \sqcup\emptyset)$ holds vacuously
– $\forall z \in P : (\forall x \in \emptyset : x \leq z) \Longrightarrow (\sqcup\emptyset \leq z)$
$\Longleftrightarrow$ $\forall z \in P : tt \Longrightarrow (\sqcup\emptyset \leq z)$
$\Longleftrightarrow$ $\forall z \in P : (\sqcup\emptyset \leq z)$
$\Longleftrightarrow$ $\sqcup\emptyset = \perp$ is the infimum of $\langle P, \leq\rangle$

□

THEOREM. Let $\langle P, \leq\rangle$ be a poset. The empty set $\emptyset$ has a glb $\sqcap\emptyset$ in P if and only if P has a supremum (in which case $\sqcap\emptyset = \top$. ∎

PROOF. By duality. □

THEOREM. Let $\langle P, \leq \rangle$ be a poset. Then $\sqcup P$ exists in P if and only if P has a supremum $\top$, in which case $\sqcup P = \top$. ■

PROOF. If $\sqcup P$ exixts then $\forall x \in P : x \leq \sqcup P$ and $\sqcup P \in P$ so $\sqcup P = \top$ is the supremum of $\langle P, \leq \rangle$. □

THEOREM. Let $\langle P, \leq \rangle$ be a poset. Then $\sqcap P$ exists in P if and only if P has a infimum $\perp$, in which case $\sqcap P = \perp$. ■

PROOF. By duality. □

The subset ordering

- Let S be a set
- $\langle \wp(S), \subseteq \rangle$ is a poset
- $\emptyset$ is the infimum
- S is the supremum
- if $X \subseteq \wp(S)$ then lub $X = \cup X$
- if $X \subseteq \wp(S)$ then glb $X = \cap X$

The predicate ordering

- A subset $X \in \wp(S)$ is characterized by the characteristic function

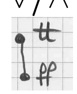
$$f_X \in S \mapsto \mathbb{B}$$
$$f_X(x) \stackrel{\text{def}}{=} (x \in X \mathrel{?} \mathtt{tt} \mathrel{:} \mathtt{ff}) = (x \in X)$$

- If we define $f \leq g$ iff $\forall x \in S : f(x) \Longrightarrow g(x)$ then

$$X \subseteq Y \iff f_X \leq f_Y$$

So, by isomorphism:

- $\langle S \mapsto \mathbb{B}, \leq \rangle$ is a poset
- $\lambda x \cdot \mathtt{ff}$ is the infimum
- $\lambda x \cdot \mathtt{tt}$ is the supremum
- If $F \subseteq (S \mapsto \mathbb{B})$ then
  - lub $F = \lambda x \cdot \bigvee_{f \in F} f(x)$
  - glb $F = \lambda x \cdot \bigwedge_{f \in F} f(x)$

where $\vee / \wedge$ is the lub/glb in the poset $\langle \mathbb{B}, \leq \rangle$ with ordering 

(i.e. $\langle \mathbb{B}, \Longrightarrow \rangle$).

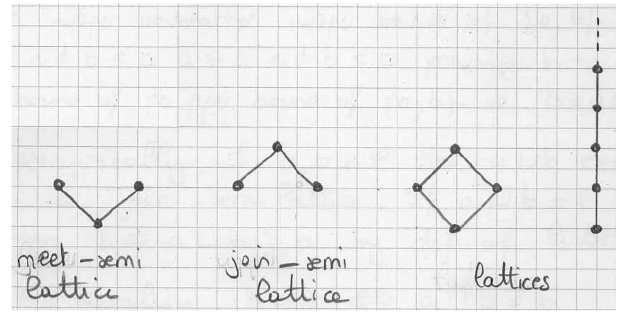
Lattices

Join/meet semi-lattice

- A join semi lattice $\langle P,\ \leq,\ \sqcup\rangle$ is a poset $\langle P,\ \leq\rangle$ such that any two elements $x, y \in P$ have a least upper bound $x \sqcup y$.
- Dually, a meet semi lattice $\langle P,\ \leq,\ \sqcap\rangle$ is a poset $\langle P,\ \leq\rangle$ such that any two elements $x, y \in P$ have a greatest lower bound $x \sqcap y$.

Lattice

- A lattice $\langle P,\ \leq,\ \sqcup,\ \sqcap\rangle$ is both a join semi lattice $\langle P,\ \leq,\ \sqcup\rangle$ and a meet semi lattice $\langle P,\ \leq,\ \sqcap\rangle$.
- Examples



Characterization of the partial order of a join/meet semi-lattice

THEOREM. In a join semi-lattice $\langle P,\ \leq,\ \sqcup\rangle$ we have (for all $a, b \in P$):

$$a \leq b \iff a \sqcup b = b$$

$\blacksquare$

PROOF. – If $a \leq b$ then $b \geq a$ and $b \geq b$ by reflexivity so b is an upper bound of $\{a, b\}$. Let c be another upper bound of $\{a, b\}$ so that $a \leq c$ and $b \leq c$ proving b to be the least upper bound of $\{a, b\}$ that is $a \sqcup b = b$.

– Reciprocally, if $a, b \in P$ the $a \sqcup b$ exists in a join semi-lattive. If $a \sqcup b = b$ then $b = a \sqcup b \geq a$ by def. of lubs.

$\square$

- By duality, $a \geq b \iff a = a \sqcap b$ in a meet semi-lattice
- In a lattice, $a \leq b \iff a \sqcup b = b \iff a = a \sqcap b$

Algebraic properties of join/meet semi-lattices and lattices

In a join semi-lattice $\langle P, \leq, \sqcup \rangle$, we have

- $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$ associativity
- $a \sqcup b = b \sqcup a$ commutativity
- $a \sqcup a = a$ idempotence

In a lattice $\langle P, \leq, \sqcup, \sqcap \rangle$, we have as well:

- $a \sqcap (a \sqcup b) = a$ absorption
- as well as the dual identities

Proof. – $(a \sqcup b)$ is an upper bound of $\{a, b\}$, $(a \sqcup b) \sqcup c$ is an upper bound of $\{a, b\}$ and $\{c\}$ whence of $\{a, b, c\}$ whence of $\{a, b \sqcup c\}$ proving that $(a \sqcup b) \sqcup c \leq a \sqcup (b \sqcup c)$. The inverse is proved in the same way and we conclude by antisymmetry.

- $a \sqcup b$ and $b \sqcup a$ are upper bounds of $\{a, b\} = \{b, a\}$ and being the lub, $a \sqcup b \leq b \sqcup a$ and $b \sqcup a \leq a \sqcup b$ so $a \sqcup b = b \sqcup a$ by antisymmetry
- a is an upper bound of $\{a\} = \{a, a\}$, whence the least, proving that $a \sqcup a = a$
- $a \leq a \sqcap x$ by def. glb. $a \leq a \sqcup b$ so a is a lower bound of $\{a, a \sqcup b\}$ whence $a \sqcap (a \sqcup b) \leq a$ proving $a = a \sqcup (a \sqcup b)$ by antisymmetry.

$\square$

Algebraic definition of a semi-lattice

Theorem. Let L be a set with a binary operation $\sqcup$ such that:

- $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$ associativity
- $a \sqcup b = b \sqcup a$ commutativity
- $a \sqcup a = a$ idempotence

Define $a \leq b \stackrel{\text{def}}{=} a \sqcup b = b$. Then $\langle P, \leq, \sqcup \rangle$ is a join semi-lattice. $\blacksquare$

A dual result holds for meet semi-lattices.

PROOF. – $a \leq a$ since $a \sqcup a = a$, so $\leq$ is reflexive

– $a \leq b \wedge b \leq a$ implies $a \sqcup b = b$ and $b \sqcup a = a$ so $a = a \sqcup b = b \sqcup a = b$ by commutativity, proving $\leq$ to be antisymmetric

– $a \leq b \wedge b \leq c$ implies $a \sqcup b = b$ and $b \sqcup c = c$ so $a \sqcup c = a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c = b \sqcup c = c$ proving $a \leq c$ so that $\leq$ is transitive

– We have $a \sqcup (a \sqcup b) = (a \sqcup a) \sqcup b) = a \sqcup b$ so $a \leq a \sqcup b$. $b \sqcup (a \sqcup b) = b \sqcup (b \sqcup a) = (b \sqcup b) \sqcup a = b \sqcup a = a \sqcup b$ proving $b \leq (a \sqcup b)$ so that $(a \sqcup b)$ is an upper bound of $\{a, b\}$.

– Let x be another upper bound of $\{a, b\}$ so $a \leq x$ and $b \leq x$. We have $a \sqcup x = x$ and $b \sqcup x = x$ so $a \sqcup (b \sqcup x) = x$ hence $(a \sqcup b) \sqcup x = x$ proving $a \sqcup b \leq x$

– If follows that $a \sqcup b = \mathrm{lub}(\{a, b\})$.

$\square$

Algebraic definition of a lattice

THEOREM. Let $\langle P, \sqcup, \sqcap \rangle$ be a set equipped with binary operators such that $\langle P, \sqcup \rangle$ is a join semi-lattice and $\langle P, \sqcap \rangle$ is a meet semi-lattice, and the absorption laws do hold:

– $a \sqcap (a \sqcup b) = a$ absorption

– $a \sqcup (a \sqcap b) = a$

Then $a \sqcup b = b$ if and only if $a \sqcap b = a$ and so $\langle P, \leq, \sqcup, \sqcap \rangle$ is a lattice, with $(a \leq b) \stackrel{\text{def}}{=} (a \sqcup b = b)$. ■

PROOF. – We know that $\langle P, \leq_1, \sqcup \rangle$ is a join semi lattice, with $a \leq_1 b \stackrel{\text{def}}{=} a \sqcup b = b$ and dually that $\langle P, \leq_2, \sqcap \rangle$ is a meet semi lattice, with $a \leq_1 b \stackrel{\text{def}}{=} a \sqcap b = a$.

– If $a \leq_1 b$ then $a \sqcup b = b$ so $a = a \sqcap (a \sqcup b) = a \sqcap b$ proving $a \leq_2 b$. Reciprocally, if $a \leq_2 b$ then $a = a \sqcap b$ so $b = b \sqcup (b \sqcap a) = b \sqcup (a \sqcap b) = b \sqcup a = a \sqcup b$ proving that $a \leq_1 b$. We conclude that $\leq_1 = \leq_2$ which we now write $\leq$.

– Because $\langle P, \leq, \sqcup \rangle$ is a join semi-lattice, any two elements have a lub $a \sqcup b$

– Because $\langle P, \leq, \sqcap \rangle$ is a meet semi-lattice, any two elements have a glb $a \sqcap b$

– We conclude that $\langle P, \leq, \sqcup, \sqcap \rangle$ is a lattice in the order-theoretic sense.

$\square$

Equivalence of the order-theoretic and algebraic definition of a lattice

We have shown the equivalence of the following two definitions (where $a \leq b \stackrel{\text{def}}{=} a \sqcup b = b$ or equivalently $a \leq b \stackrel{\text{def}}{=} a \sqcap b = a$):

– Order-theoretic definition:

> A lattice is a poset $\langle P, \leq \rangle$ such that any two elements $a, b \in P$ have a lub $a \sqcup b$ and a glb $a \sqcap b$.

– Algebraic definition:

A lattice is a set P equipped with two binary operators $\sqcup$ (join) and $\sqcap$ (meet) satisfying[3]:

- $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$ associativity
- $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$
- $a \sqcup b = b \sqcup a$ commutativity
- $a \sqcap b = b \sqcap a$
- $a \sqcup a = a$ idempotence
- $a \sqcap a = a$
- $a \sqcap (a \sqcup b) = a$ absorption
- $a \sqcup (a \sqcap b) = a$

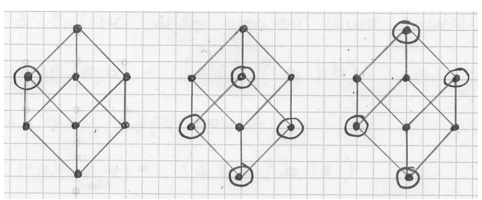
[3] Note that these laws extend to finite sets (but not to infinite ones).

Sublattices

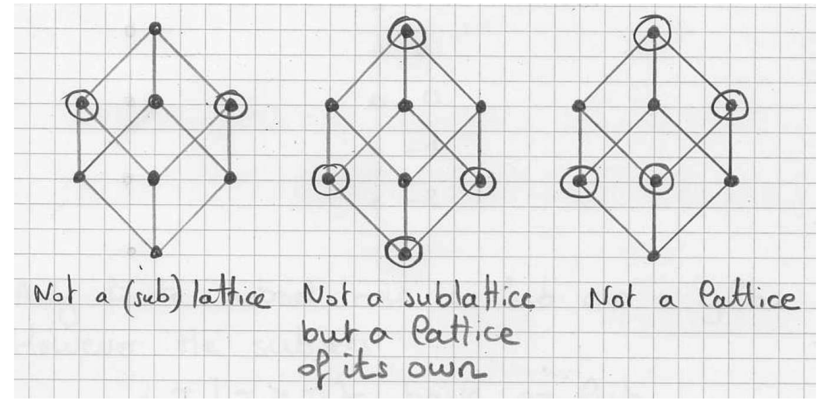
– Let $\langle L, \leq, \sqcup, \sqcap\rangle$ be a lattice. $S \subseteq L$ is a sublattice of L if and only if

$$\forall x, y \in S : x \sqcup y \in S \wedge s \sqcap y \in S$$

– Examples:

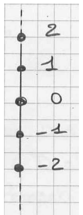


– Counter-examples:



CPOs and Complete Lattices

Infinite meet and join may be missing in a lattice



On the left is represented the (infinite) Hasse diagram of the lattice $\langle \mathbb{Z}, \leq, \min, \max\rangle$ equipped with

$$a \leq b \stackrel{\text{def}}{=} \exists c \in \mathbb{N} : a + c = b \qquad \text{natural ordering}$$
$$\min(a, b) \stackrel{\text{def}}{=} (\!|\, a \leq b \mathrel{?} a \mathrel{:} b \,|\!) \qquad \text{glb}$$
$$\max(a, b) \stackrel{\text{def}}{=} (\!|\, a \leq b \mathrel{?} b \mathrel{:} a \,|\!) \qquad \text{lub}$$

Any finite subset has a lub and a glb. However the infinite subsets

- $\{x \mid x \geq n\}$ have no lub
- $\{x \mid x \leq n\}$ have no glb
- $\mathbb{Z}$ has neither lub nor glb

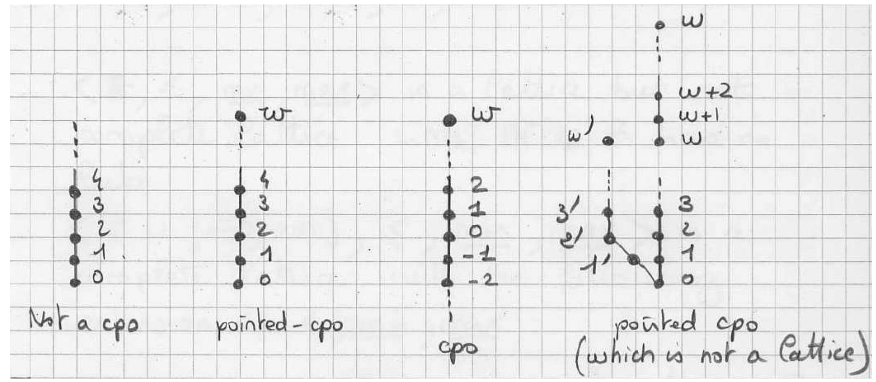
(Pointed) complete partial order (cpo, pcpo)

- A complete partial order (cpo) $\langle P, \sqsubseteq, \sqcup\rangle$ is a poset $\langle P, \sqsubseteq\rangle$ such that any increasing chain of P has a lub in P
- An ω-cpo $\langle P, \sqsubseteq, \sqcup\rangle$ is a poset $\langle P, \sqsubseteq\rangle$ such that any increasing ω-chain [4] of P has a lub in P
- A pointed cpo (pcpo) $\langle P, \sqsubseteq, \bot, \sqcup\rangle$ is a cpo $\langle P, \sqsubseteq, \sqcup\rangle$ which has a bottom $\bot$

The definition using directed chains instead of increasing chains is equivalent.

[4] i.e. of order ω

– Examples:

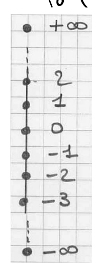


Complete lattice

A complete lattice is a poset $\langle P, \sqsubseteq\rangle$ such that any subset $X \subseteq P$ has a lub $\sqcup X$ in P.

Examples:

- $\langle \wp(S), \subseteq, \cup, \cap\rangle$ is a complete lattice



- On the left is represented the complete lattice $\langle \mathbb{Z} \cup \{-\infty, +\infty\}, \leq, \min, \max\rangle$ with the following extension of $\leq$, min and max:
  - $-\infty \leq -\infty < z < +\infty \leq +\infty$ for all $z \in \mathbb{Z}$
  - $\min(X \cup \{-\infty\}) = -\infty$ for all $X \subseteq \mathbb{Z} \cup \{+\infty\}$
  - $\max(X \cup \{+\infty\}) = +\infty$ for all $X \subseteq \mathbb{Z} \cup \{-\infty\}$

Bottom and top of a complete lattice

- A complete lattice $\langle P, \sqsubseteq, \sqcup\rangle$ has an infimum $\bot = \sqcup\emptyset$
- A complete lattice $\langle P, \sqsubseteq, \sqcup\rangle$ has an supremum $\bot = \sqcup P$
- Examples:
  - In $\langle\wp(S), \subseteq, \cup, \cap\rangle$ the infimum is $\emptyset$ and the supremum is S, written $\langle\wp(S), \subseteq, \emptyset, S, \cup, \cap\rangle$
  - In $\langle\mathbb{Z}\cup\{-\infty, +\infty\}, \leq, \min, \max\rangle$ the infimum is $-\infty$ and the supremum is $+\infty$, written $\langle\mathbb{Z}\cup\{-\infty, +\infty\}, -\infty, +\infty, \leq, \min, \max\rangle$

A complete lattice is not empty

- It follows that a complete lattice is never empty
- Example:
  - The smallest lattice is $\langle\{\bullet\}, =, \bullet, \bullet, \lambda X \cdot \bullet, \lambda X \cdot \bullet\rangle$

A complete lattice has both lubs and glbs

THEOREM. Let $\langle P, \sqsubseteq, \bot, \top, \sqcup\rangle$ be a complete where $\sqcup$ is the lub. Then the glb is:

$$\sqcap X \stackrel{\text{def}}{=} \sqcup\{y \mid \forall x \in X : y \sqsubseteq x\}$$

■

PROOF. – Since P has a bottom $\bot$, the set $\{y \mid \forall x \in X : y \sqsubseteq x\}$ contains $\bot$ whence is not empty

– Any element of $X \subseteq P$ is an upper bound of $\{y \mid \forall x \in X : y \sqsubseteq x\}$ so is greater than or equal to the least upper bound:

$$\forall x \in X : \sqcup\{y \mid \forall x \in X : y \sqsubseteq x\} \sqsubseteq x$$

$$\forall x \in X : \sqcap X \sqsubseteq x$$

proving that $\sqcap X$ is a lower bound of X.

– Let z be any lower bound of X:

$$\forall x \in X : z \sqsubseteq x$$

so $z \in \{y \mid \forall x \in X : y \sqsubseteq x\}$ that is $z \sqsubseteq \sqcap X$ proving that $q \sqcap X$ is the greatest lower bound of X

□

By duality, a complete lattice can be defined as a poset $\langle P, \sqsubseteq\rangle$ such that <u>any</u> subset $X \subseteq P$ has a glb $\sqcap X$ in P.

Finite lattices are complete

THEOREM. Finite lattices are complete. ■

PROOF. Let $\langle L, \sqsubseteq, \sqcup, \sqcap\rangle$ be a finite lattice. Let $S \subseteq L$ be a subset of L. if S has one element x_0 then $\sqcup S = \sqcup\{x_0\} = x_0$. Assume by induction hypothesis that $\sqcup\{x_0, \ldots, x_{n-1}\}$ does exists and $S = \{x_0, \ldots, x_n\}$. Then $\sqcup S = \sqcup\{x_0, \ldots, x_n\} \sqcup x_n$ which exists in L. So by recurrence $\sqcup X$ exists for all finite non-empty subsets of L which, being finite, has no other subsets than the empty set. But L is finite so $L = \{x_0, \ldots, x_n\}$ and $x_0 \sqcap \ldots \sqcap x_n$ is the infimum $\bot$ of L. So $\sqcup\emptyset = \bot$ also exists. The existence of all lubs implies that $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ is a complete lattice. □

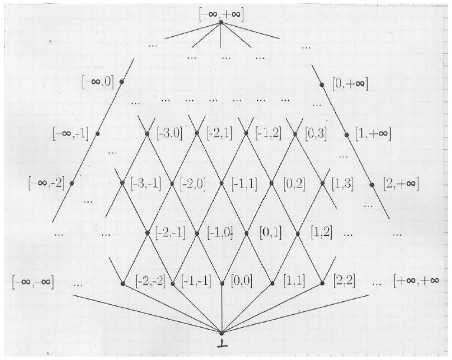
Example: the complete lattice of intervals

Given a complete lattice $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$, the lattice $\mathcal{I}(L)$ of intervals over L is

- $\mathcal{I}(L) \stackrel{\text{def}}{=} \{\bot\} \cup \{[a, b] \mid a, b \in L \wedge a \sqsubseteq b\}$
- The ordering is $\bot \sqsubseteq \bot \sqsubseteq [a, b] \sqsubseteq [c, d]$ provided $a \sqsubseteq c$ and $c \sqsubseteq d$
- The lub is $\bot \sqcup X = X \sqcup \bot = X$ and $[a, b] \sqcup [c, d] \stackrel{\text{def}}{=} [a \sqcap c, b \sqcup d]$
- The glb is $\bot \sqcap X = X \sqcap \bot = \bot$ and $[a, b] \sqcup [c, d] \stackrel{\text{def}}{=}$ let $m = a \sqcup c, M = b \sqcap d$ in $(\!|\, m \sqsubseteq M \ ?\ [m, M] \ ¿\ \bot \,|\!)$
- The infimum is $\bot$ while the supremum is $[\bot, \top]$

Example

For $\langle \mathbb{Z} \cup \{-\infty, +\infty\}, \leq, -\infty, +\infty, \min, \max\rangle$, we get the complete lattice of integer intervals:



Equivalent definition of a complete lattice

THEOREM. Let $\langle P, \sqsubseteq\rangle$ be a non-empty poset. Then the followin are equivalent

(i) P is a complete lattice $\langle P, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$

(ii) P has a top element, and $\sqcap X$ exists in P for every non-empty subset $X \subseteq P$

■

PROOF. – (i) $\Longrightarrow$ (ii) since $\top = \sqcup P = \sqcap\emptyset$ and $\sqcap X$ exists in P for every non-empty subset $X \subseteq P$

– If $\sqcap X$ exists in P for every non-empty subset $X \subseteq P$ the $\sqcup X$ exists for every subset X of P which has an upper bound u in P:
  - Let $U = \{y \in P \mid \forall x \in X : x \sqsubseteq y\}$

- U is not empty since $u \in U$ so $\sqcap U$ exists in P being a non-empty subset $U \subseteq P$
- $\forall x \in X : \forall y \in U : x \sqsubseteq y$
  $\Longrightarrow \forall x \in X : x \sqsubseteq \sqcap U$ by def. glb
  $\Longrightarrow U$ is an upper bound of X
- Let u be any other upper bound of X. We have $\forall x \in X : x \sqsubseteq u$ so $u \in U$ so $\sqcap U \sqsubseteq u$ proving $\sqcap U$ to be the lub of X.

– Since P has a top, every subset X of P has an upper bound $\top$ in P and so

$$\sqcup X = \sqcap\{y \in P \mid \forall x \in X : x \sqsubseteq y\}$$

is the lub in P

$\square$

ACC and lattice completeness

THEOREM. Let $\langle L, \sqsubseteq, \sqcup, \sqcap\rangle$ be a lattice.

– If L has a bottom and satisfies the ACC then it is a complete lattice

– If L has no infinite chains then it is a complete lattice

$\blacksquare$

PROOF. – Let us first prove that if L satisfies ACC then for every non-empty subset X of P, there exists a finite subset F of X such that $\sqcup X = \sqcup F$.

Since $\sqcup F$ exists for all finite subset of L, we can define

$$Y \stackrel{\text{def}}{=} \{\sqcup F \mid F \text{ is a finite non-empty subset of } X\}$$

X is non-empty so Y is non-empty and, being included in L, it satisfies the ascending chain condition, whence has a maximal element m.

So $m = \sqcup F$ for some finite $F \subseteq X$. Let $x \in X$, then $\sqcup(F \cup \{x\}) \in Y$ and $m = \sqcup F \sqsubseteq \sqcup(F \cup \{x\}) \subseteq m$ since m is maximal in Y proving that $m = \sqcup F = \sqcup(F \cup \{x\})$ by antisymmetry. We have $x \subseteq m$ by def. lub proving that m is an upper bound of X.

Let u be any other upper bound of X. Then u is an upper bound of $F \subseteq X$ and hence $m = \sqcup F \sqsubseteq u$ proving that m is the lub pf X, that is $\sqcup X = m = \sqcup F$.

– It L has a bottom and satisfies ACC, the $\sqcup X$ exists for every non-empty subset $X \subseteq L$, so L is complete (we proved the dual).

– If L has no infinite chains, it has a bottom and ACC.

$\square$

Boolean algebras

Distributive and modular inequalities in a lattice

THEOREM. The following inequalities hold in any lattice $\langle L, \leq, \vee, \wedge\rangle$:

(i) $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$

(ii) $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

(iii) $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) \leq (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$

distributive inequalities

(iv) $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee (x \wedge z))$

modular inequalities

■

PROOF. – (iv)

$x \wedge y \leq x$ $\wr$def. glb (a)$\wr$

$x \wedge z \leq x$ $\wr$def. glb (b)$\wr$

$(x \wedge y) \vee (x \wedge z) \leq x$ $\wr$(a), (b), def. lub (c)$\wr$

$x \wedge y \leq y$ $\wr$def. glb (d)$\wr$

$y \leq y \vee (x \wedge z)$ $\wr$def. glb (e)$\wr$

$(x \wedge z) \leq y \vee (x \wedge z)$ $\wr$def. lub (f)$\wr$

$(x \wedge y) \vee (x \wedge z) \leq y \vee (x \wedge z)$ $\wr$(d), (e), (f), transitivity, def. lub (g)$\wr$

$(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee (x \wedge z))$ $\wr$(c), (g), def. lub Q.E.D.$\wr$

– The proof of the distributive inequalities (i), (ii) and (ii) is similar.

□

Equivalence of distributive equalities in a lattice

THEOREM. The following equalities are equivalent in a lattice $\langle L, \leq, \vee, \wedge\rangle$:

(i) $(x \wedge y) \vee (x \wedge z) = x \vee (y \wedge z)$

(ii) $(x \vee y) \wedge (x \vee z) = x \wedge (y \vee z)$

(iii) $(x \vee y) \wedge z \leq x \vee (y \wedge z)$

■

PROOF. – Assume (i), with $x = a \vee b$, $y = a$, $z = c$, we get

$((a \vee b) \wedge a) \vee (a \vee b \wedge c) = (a \vee b) \vee (a \wedge c)$ $\wr$(a)$\wr$

$a \vee ((a \vee b) \wedge c) = (a \vee b) \vee (a \wedge c)$ $\wr$since $a = (a \vee b) \wedge a$ (b)$\wr$

$(c \wedge a) \vee (c \wedge b) = c \vee (a \wedge b)$ $\wr$by (i) with $x = c$, $y = a$, $z = b$ (c)$\wr$

$(a \vee b) \wedge (a \vee c) = a \vee (a \wedge c) \vee (b \wedge c)$ $\wr$(b), (c), commutativity (d)$\wr$

$(a \vee b) \wedge (a \vee c) = a \vee (b \wedge c)$ $\wr$since $a \vee (a \wedge c) = a$, proving (ii)$\wr$

– By duality, (ii) $\Longrightarrow$ (i)

– Assume (ii) holds in L. Then

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \geq (x \vee y) \wedge z$$

since $x \vee z \geq z$ thus proving (iii)

– Conversely, assuming (iii) with $x = a$, $y = b$, $z = a \vee c$ in (iii), we get

$(a \vee b) \wedge (a \vee c) \leq a \vee (b \wedge (a \vee c))$ $\wr$(a)$\wr$

$(a \vee b) \wedge (a \vee c) \leq a \vee ((a \vee c) \wedge b)$ $\wr$commutativity (b)$\wr$

$(a \vee c) \wedge b \leq a \vee (c \wedge b)$ ≀by (iii) with $x = a$, $y = c$, $z = b$ (c)≀

$a \vee ((a \vee c) \wedge b) \leq a \vee (c \wedge b)$ ≀(c) and def. lub (d)≀

$a \vee ((a \vee c) \wedge b) \leq a \vee (c \wedge b)$ ≀(d), associativity, $(a \vee a) = a$ (e)≀

$(a \vee b) \wedge (a \vee c) \geq a \vee (b \wedge c)$ ≀(b), (e), transitivity (f)≀

$(a \vee b) \wedge (a \vee c) \geq a \vee (b \wedge c)$ ≀as proved earlier in any lattice (g)≀

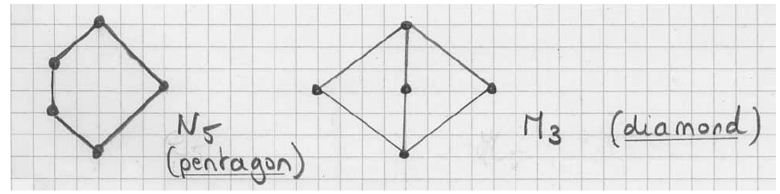
$(a \vee b) \wedge (a \vee c) = a \vee (b \wedge c)$ ≀(f), (g), commutativity, antisymmetry, proving (ii)≀

□

Distributive lattice

- A lattice $\langle L, \leq, \vee, \wedge\rangle$ is distributive if and only if one of the following equivalent conditions is satisfied:
  (i) $(x \wedge y) \vee (x \wedge z) = x \vee (y \wedge z) \iff$
  (ii) $(x \vee y) \wedge (x \vee z) = x \wedge (y \vee z) \iff$
  (iii) $(x \vee y) \wedge z \leq x \vee (y \wedge z)$
- Examples
  - $\langle \wp(S), \subseteq, \cup, \cap\rangle$ is a distributive lattice
  - Any chain is a distributive lattice

- The dual of a distributive lattice is distributive (since (ii) is the dual of (i)).
- Counter-examples:



(Even more precisely, a lattice is distributive, if and only if it has no sublattice isomorphic to one of the lattices N_5 or M_3 [5])

[5] See G. Grätzer, "Lattice theory, first concepts and distributive lattices", Freeman Pub. Co., 1971, Th. 1, p. 70.

(Semi)-infinitely distributive lattice

A lattice $\langle L, \leq, \vee, \wedge\rangle$ is semi-infinitely distributive if and only if it satisfies either of the following conditions (where when the lefthand side of the equation exists, then so does the righth and side, and then they are equal, $S \subseteq L$ and $x \in L$):

$$x \wedge (\bigvee S) = \bigvee_{s \in S} (x \wedge s) \quad \text{Infinite meet distributivity}$$

$$x \vee (\bigwedge S) = \bigwedge_{s \in S} (x \vee s) \quad \text{Infinite join distributivity}$$

A lattice $\langle L, \leq, \vee, \wedge\rangle$ is infinitely distributive if and only if it satisfies both conditions.
Examples:

- $\langle \wp(S), \subseteq, \cup, \cap\rangle$ is infinitely distributive
- any chain is infinitely distributive
- any finite distributive lattice is infinitely distributive

Completely distributive lattice

By recurrence, we get:

$$\bigwedge_{j=1}^{r} \bigvee_{k=1}^{n_j} a_{jk} = \bigvee_{j_1=1}^{n_1} \ldots \bigvee_{j_r=1}^{n_r} (a_{1j_1} \wedge \ldots \wedge a_{rj_r})$$

which, by defining

- $A = \{1, \ldots, r\}$
- $B_1 = \{1, \ldots, n_1\}, \ldots, B_r = \{1, \ldots, n_r\}$
- $\Gamma = \{\gamma \mid \forall j \in A : \gamma(j) \in B_j\}$

can be rewritten as:

$$\bigwedge_{\alpha\in A} \bigvee_{\beta\in B_\alpha} a_{\alpha\beta} = \bigvee_{\gamma\in\Gamma} \bigwedge_{\alpha\in A} a_{\alpha\gamma(\alpha)} \qquad (1)$$

The dual of (1) is

$$\bigvee_{\alpha\in A} \bigwedge_{\beta\in B_\alpha} a_{\alpha\beta} = \bigwedge_{\gamma\in\Gamma} \bigvee_{\alpha\in A} a_{\alpha\gamma(\alpha)} \qquad (2)$$

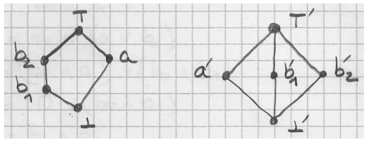
- A complete lattice is meet completely distributive iff it satisfies (1)
- A complete lattice is join completely distributive iff it satisfies (2)
- A complete lattice is completely distributive iff it satisfies both (1) and (2)
- Example:
  - $\langle \wp(S), \subseteq, \emptyset, S, \cup, \cap\rangle$ is completely distributive

Complement

Let $\langle P, \leq, \bot, \top\rangle$ be a poset with infimum $\bot$ and supremum $\top$.
We say that $a \in P$ has a complement b in P iff

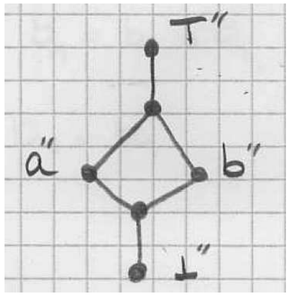
$$a \wedge b = \bot \quad \text{and}$$
$$a \vee b = \top$$

In general the complement may not be unique[6]:



[6] Note that a has complements b_1 and b_2 while b_1 and b_2 have a unique complement a.

In general the complement may not exist at all:



In case a has a unique complement, then it is written a', $\overline{a}$, $\neg a$, etc.

Uniqueness of the complement in distributive lattices with top and bottom elements

THEOREM. Let $\langle L, \leq, 0, 1, \vee, \wedge\rangle$ be a distributive lattice with bottom 0, top 1. Then any element x of L has at most one complement. ■

PROOF. – Assume than b_0 and b_1 are both complement of $a \in L$

– b_0
  $= b_0 \wedge 1$
  $= b_0 \wedge (a \vee b_1)$
  $= (b_0 \wedge a) \vee (b_0 \wedge b_1)$
  $= 0 \vee (b_0 \wedge b_1)$
  $= b_0 \wedge b_1$
– $b_1 = b_0 \wedge b_1$, as above, exchanging b_0 and b_1
– $b_0 = b_1$ by transitivity

□

De Morgan identities

THEOREM. In a distributive lattice $\langle L, \leq, 0, 1, \vee, \wedge\rangle$, if a and b have complements, hence unique ones $\neg a$ and $\neg b$, then:

$$\neg(a \wedge b) = \neg a \vee \neg b$$
$$\neg(a \vee b) = \neg a \wedge \neg b$$

■

PROOF. – $(a \wedge b) \wedge (\neg a \vee \neg b)$
  $= (a \wedge b \wedge \neg a) \vee (a \wedge b \wedge \neg b)$
  $= 0 \vee 0 = 0$
– $(a \wedge b) \vee (\neg a \vee \neg b)$
  $= (a \vee \neg a \vee \neg b) \wedge (b \vee \neg a \vee \neg b)$
  $= 1 \wedge 1 = 1$
– So $\neg(a \wedge b) = (\neg a \vee \neg b)$ by def. complement

– The second law is the dual of the first in the dual lattice $\langle L, \geq, 1, 0, \wedge, \vee\rangle$ which is also distributive, whence holds by the above proof of the first equality.

□

Bounded poset

A bounded poset is a poset $\langle P, \leq\rangle$ which has a top $\top$ and a bottom element $\bot$

Complemented lattice

A complemented lattice is a bounded lattice $\langle L, \leq, \bot, \top, \sqcup, \sqcap\rangle$ in which every element $x \in L$ has a complement in L

Boolean lattice

– A Boolean lattice is a complemented distributive lattice

Boolean algebra

– A boolean algebra $\langle P, \leq, \bot, \top, \vee, \wedge, \neg\rangle$ is a Boolean lattice in which which $\leq$, $\bot$, $\top$ and $\neg$ are also considered as operations:
  - $\langle P, \vee, \wedge\rangle$ is a distributive lattice
  - $x \leq y \stackrel{\text{def}}{=} x \vee y = y \iff x \wedge y = x$
  - $a \vee \bot = a$ and $a \wedge \top = a$ for all $a \in P$
  - $a \vee \neg a = \top$ and $a \wedge \neg a = \bot$ for all $a \in P$

Boolean subalgebra

– A boolean subalgebra of $\langle P,\ \leq,\ \bot,\ \top,\ \vee,\ \wedge,\ \neg\rangle$ is

$$\langle Q,\ \leq,\ \bot,\ \top,\ \vee,\ \wedge,\ \neg\rangle$$

such that:

- $Q \subseteq P$
- $\bot,\ \top \in Q$
- $\forall a \in Q : \neg a \in Q$
- $\langle Q,\ \leq,\ \vee,\ \wedge\rangle$ is a sublattice of $\langle P,\ \leq,\ \vee,\ \wedge\rangle$

Examples of Boolean algebras

– $\langle\{0, 1\},\ \leq,\ 0,\ 1,\ \vee,\ \wedge,\ \neg\rangle$ with $0 \leq 0 < 1 \leq 1$ and

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

	$\neg$
0	1
1	0

– For any set X, let $\neg A = X \setminus A$ then

$$\langle \wp(X),\ \subseteq,\ \emptyset,\ X,\ \cup,\ \cap,\ \neg\rangle$$

is a boolean algebra (called the powerset algebra)

– An algebra of sets (also called *field of sets*) is a Boolean subalgebra of some powerset algebra

$$\langle \wp(X),\ \subseteq,\ \emptyset,\ X,\ \cup,\ \cap,\ \neg\rangle$$

– $2^n \mapsto 2$ where $2 = \{0, 1\}$ is a boolean algebra $\langle 2^n \mapsto 2,\ \dot{\leq},\ \dot{0},\ \dot{1},\ \dot{\wedge},\ \dot{\vee},\ \dot{\neg}\rangle$ such that:

$$\begin{aligned} f \mathrel{\dot{\leq}} g &\stackrel{\text{def}}{=} \forall x_1, \ldots, x_n \in 2 : f(x_1, \ldots, x_n) \leq g(x_1, \ldots, x_n) \\ \dot{0} &\stackrel{\text{def}}{=} \lambda(x_1, \ldots, x_n) \cdot 0 \\ \dot{1} &\stackrel{\text{def}}{=} \lambda(x_1, \ldots, x_n) \cdot 1 \end{aligned}$$

$$\begin{aligned} \dot{\bigvee_{i \in \Delta}} f_i &\stackrel{\text{def}}{=} \lambda(x_1, \ldots, x_n) \cdot \bigvee_{i \in \Delta} f_i(x_1, \ldots, x_n) \\ \dot{\bigwedge_{i \in \Delta}} f_i &\stackrel{\text{def}}{=} \lambda(x_1, \ldots, x_n) \cdot \bigwedge_{i \in \Delta} f_i(x_1, \ldots, x_n) \\ \dot{\neg} f &\stackrel{\text{def}}{=} \lambda(x_1, \ldots, x_n) \cdot \neg f(x_1, \ldots, x_n) \end{aligned}$$

Identities in Boolean lattices

THEOREM. Let $\langle L, \leq, 0, 1, \vee, \wedge, \neg\rangle$ be a Boolean lattice. Then:

(i) $\neg 0 = 1$ and $\neg 1 = 0$

(ii) $\forall a \in L : \neg\neg a = a$

(iii) $\forall a, b \in L : \neg(a \vee b) = \neg a \wedge \neg b$ and $\neg(a \wedge b) = \neg a \vee \neg b$ (De Morgan laws)

(iv) $\forall a, b \in L : a \wedge b = \neg(\neg a \vee \neg b)$ and $\forall a, b \in L : a \vee b = \neg(\neg a \wedge \neg b)$

(v) $\forall a, b \in L : a \wedge \neg b = 0 \iff a \leq b$ where $a \leq b \overset{\text{def}}{=} a \vee b = b \iff a \wedge b = a$

$\blacksquare$

PROOF. – To prove $p = \neg q$ in L, it is sufficient to prove that $p \vee q = 1$ and $p \wedge q = 0$ since the complement is unique in distributive whence Boolean lattices

- This observation makes the proof of (i), (ii) and (iii) entirely routine
- Part (iv) follows from (ii) and (iii)
- Part (v) is an easy exercice

$\square$

Bibliography

- B.A. Davey & H.A. Priestley
  "Introduction to lattices and order"
  Cambridge University Press, 2nd edition, 2002, 298 p.
- G. Birkhoff
  "Lattice theory"
  American mathematical Society, Colloquium Publications, Vol. 25, 3rd edition, 1979, 418 p.
- G. Grätzer
  "General Lattice Theory"
  Birkhüser verlag, Basel, 2nd edition, 1998, 663 p.

THE END

My MIT web site is http://www.mit.edu/~cousot/

The course web site is http://web.mit.edu/afs/athena.mit.edu/course/16/16.399/www/.