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

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/

Moore families

Robert Lee Moore

Moore family

Let $\langle P, \sqsubseteq\rangle$ be a poset with top element $\top$. A *Moore family* is $M \subseteq P$, such that:

- $\top \in M$
- If $X \in \wp(M) \setminus \{\emptyset\}$ then $\sqcap X$ exists in P and $\sqcap X \in M$

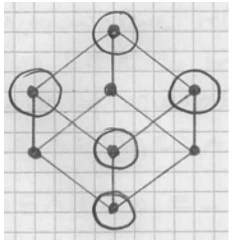
or equivalently [1]

- If $X \in \wp(M)$ then $\sqcap X$ exists in P and $\sqcap X \in M$

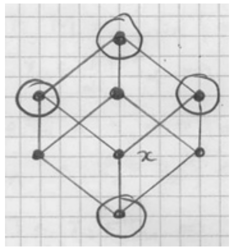
that is M is closed under meet.

[1] Since $\sqcap\emptyset = \top$.

– Example:



– Counter-example:



x is missing!

Moore closure

A Moore closure $\mathcal{M}$ is for the particular case of $\langle \wp(X),\ \subseteq,\ \emptyset,\ X,\ \cup,\ \cap \rangle$:

– $X \in \mathcal{M}$

– If $Y \subseteq \mathcal{M}$ then $\cap Y \in \mathcal{M}$

The elements of $\mathcal{M}$ are called *Moore closed sets* or *closed sets* or *saturated sets*, etc..., depending on the mathematical context. A Moore closure is also called *Moore collection*, *closed system*, $\cap$-structure, etc.

Example of Moore closure

– Let $\equiv$ be an equivalence relation on a set X

– Let us define $S \subseteq X$ to be $\equiv$-*saturated* iff it is a union of equivalence classes:

$$\forall x_1, x_2 \in X : (x_1 \in S \wedge x_2 \equiv x_1) \Longrightarrow (x_2 \in S)$$

– Let $\mathcal{M} = \{S \subseteq X \mid S \text{ is } \equiv\text{-saturated}\}$

– $\mathcal{M}$ is a Moore family in $\langle \wp(X),\ \subseteq,\ \emptyset,\ X,\ \cup,\ \cap \rangle$

PROOF. Assume $M = \{S_\alpha \mid \alpha \in \Delta\} \subseteq \mathcal{M}$. Then $x_1 \in \bigcap M \Longrightarrow x_1 \in \bigcap_{\alpha \in \Delta} S_\alpha \Longrightarrow \forall \alpha \in \Delta : x_1 \in S_\alpha \Longrightarrow (\forall \alpha \in \Delta : (x_1 \in S_\alpha \wedge x_2 \equiv x_1) \Longrightarrow (x_2 \in S_\alpha))$ whence $((x_1 \in \bigcap_{\alpha \in \Delta} S_\alpha \wedge x_2 \equiv x_1) \Longrightarrow (x_2 \in \bigcap_{\alpha \in \Delta} S_\alpha))$ so $x_1 \in \bigcap M \wedge x_2 \equiv x_1 \Longrightarrow x_2 \in \bigcap M$ proving that $\bigcap M \in \mathcal{M}$. □

Example: convex subsets of a poset

Let $\langle P,\ \leq \rangle$ be a pre-order ($\leq$ is reflexive and transitive). Given $a, b \in P$, define

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

Call $S \subseteq P$ to be *convex* whenever

$$a, b \in S \Longrightarrow [a, b] \subseteq S$$

Then $\mathcal{M} = \{S \subseteq P \mid S \text{ is convex}\}$ is a Moore family of $\langle \wp(P),\ \subseteq,\ \emptyset,\ P,\ \cup,\ \cap \rangle$

PROOF. – Let S_α, $\alpha \in \Delta$ be a family of convex subsets of P i.e. $\forall \alpha \in \Delta : S_\alpha \in \mathcal{M}$.
If $a, b \in \bigcap_{\alpha \in \Delta} S_\alpha$ then $\forall \alpha \in \Delta : a, b \in S_\alpha$ so $\forall \alpha \in \Delta : [a, b] \subseteq S_\alpha$ (since S_α is convex) whence $[a, b] \subseteq \bigcap_{\alpha \in \Delta} S_\alpha$ (def. of glb) proving that $\bigcap_{\alpha \in \Delta} S_\alpha \in \mathcal{M}$.

- If $\bigcap_{\alpha \in \Delta} S_\alpha$ is $\emptyset$, then $\emptyset$ is convex, so in that case $\bigcap_{\alpha \in \Delta} S_\alpha \in \mathcal{M}$
- If Δ is empty, $\bigcap_{\alpha \in \emptyset} S_\alpha = P$ which is convex
- $\mathcal{M}$ is closed under arbitrary intersections whence is a Moore family

□

A Moore family in a poset is a complete lattice

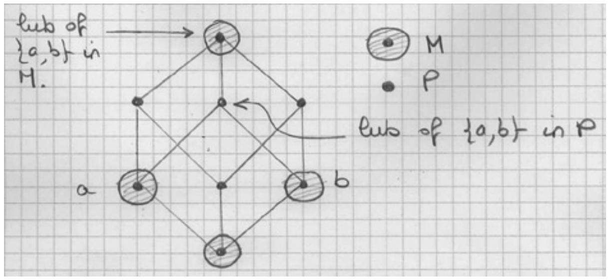
THEOREM. Let $\langle P, \sqsubseteq, \sqcap, \sqcup \rangle$ be a topped poset and $M \subseteq P$ be a Moore family then $\langle M, \sqsubseteq \rangle$ is a complete lattice $\langle M, \sqsubseteq, \sqcap M, \top \rangle$. ■

PROOF. Since $\langle P, \sqsubseteq \rangle$ is a poset and $M \subseteq P$, $\langle M, \sqsubseteq \rangle$ is a poset. Being a Moore family it is topped and any subset $S \subseteq M$ has $\sqcap S \in M$ so $\sqcap$ is the meet in M. It follows that M is a complete lattice, which lub is:

$$\sqcup S = \sqcap \{y \in M \mid \forall x \in S : x \sqsubseteq y\} \in M$$

The infimum is $\sqcap M \in M$. □

Note that in general, the lub in the Moore family M is not the same as the lub in the original poset P:



So in general a Moore family of a complete lattice is not a complete sublattice of this complete lattice.

Moore family/complete lattice of safety properties

Let Σ be a set of states and $\Sigma^{\vec{\infty}}$ be the set of finite or infinite sequences on Σ. A *trace property* is $P \subseteq \Sigma^{\vec{\infty}}$. A *safety property* is $S \subseteq \Sigma^{\vec{\infty}}$ such that:

$$\forall \sigma \in \Sigma^{\vec{\infty}} : (\sigma \notin S) \iff (\exists i \geq 1 : \sigma \swarrow i \notin S) \qquad (1)$$

where $\sigma \swarrow i = \sigma_0 \ldots \sigma_{\min\{i,|\sigma|\}-1}$ and $|\sigma|$ is the length of σ.

THEOREM. The set $\mathsf{Safe}(\Sigma^{\vec{\infty}})$ of safety properties on
$$\langle \wp(\Sigma^{\vec{\infty}}), \subseteq, \emptyset, \Sigma^{\vec{\infty}}, \cup, \cap \rangle$$
is a Moore family whence a complete lattice. ■

PROOF. – The top element $\Sigma^{\vec{\infty}}$ is a safety property since both sides of the implication are false in the definition (1)

– Let P_α, $\alpha \in \Delta$ be a family of safety properties: $\forall \sigma \in \Sigma^{\vec{\infty}} : (\sigma \notin P_\alpha) \iff (\exists i \geq 1 : \sigma \swarrow i \notin P_\alpha)$

- $\forall \sigma \in \Sigma^{\vec{\infty}} : \sigma \notin \bigcap_{\alpha \in \Delta} P_\alpha \Longrightarrow \exists \alpha : \sigma \notin P_\alpha \Longrightarrow (\exists i \geq 1 : \sigma \swarrow i \notin P_\alpha) \Longrightarrow (\exists i \geq 1 : \sigma \swarrow i \notin \bigcap_{\alpha \in \Delta} P_\alpha)$.
- Conversely, $\forall \sigma \in \Sigma^{\vec{\infty}} : (\exists i \geq 1 : \sigma \swarrow i \notin \bigcap_{\alpha \in \Delta} P_\alpha) \Longrightarrow (\exists \alpha \in \Delta : \exists i \geq 1 : \sigma \swarrow i \notin P_\alpha) \Longrightarrow (\exists \alpha \in \Delta : \sigma \notin P_\alpha) \Longrightarrow \sigma \notin \bigcap_{\alpha \in \Delta} P_\alpha$

It follows that $\bigcap_{\alpha \in \Delta} P_\alpha$ is a safety property since $\forall \sigma \in \Sigma^{\vec{\infty}} : (\sigma \notin \bigcap_{\alpha \in \Delta} P_\alpha) \iff (\exists i \geq 1 : \sigma \swarrow i \notin \bigcap_{\alpha \in \Delta} P_\alpha)$.

So Safe($\Sigma^{\vec{\infty}}$) contains the top and is closed under intersection whence is a Moore family hence is a complete lattice. □

Note that Safe($\Sigma^{\vec{\infty}}$) is not a complete sublattice of $\langle \wp(\Sigma^{\vec{\infty}}), \subseteq \rangle$ since $\forall n \in \mathbb{N} : \{a^n b\}$ is a safety property whereas $\bigcup_{n \in \mathbb{N}} \{a^n b\} = a^\star b$ is not (since it is not closed by limits).

Combinations of posets

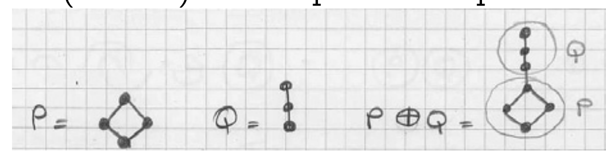
Linear (ordinal) sum of posets

Let $\langle P, \leq \rangle$ and $\langle Q, \sqsubseteq \rangle$ be two posets. Their linear (ordinal) sum is $\langle P, \leq \rangle \oplus \langle Q, \sqsubseteq \rangle \stackrel{\text{def}}{=} \langle P \oplus Q, \preceq \rangle$ such that:

– $P \oplus Q \stackrel{\text{def}}{=} \{\langle 0, x \rangle \mid x \in P\} \cup \{\langle 1, y \rangle \mid y \in Q\}$

– $\langle i, x \rangle \preceq \langle j, y \rangle \stackrel{\text{def}}{=} \quad (i = j = 0 \land x \leq y) \lor (i = 0 \land j = 1) \lor (i = j = 1 \land x \sqsubseteq y)$

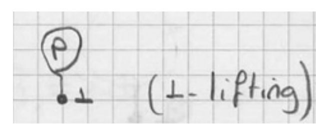
The linear (ordinal) sum of posets is a poset. Example:



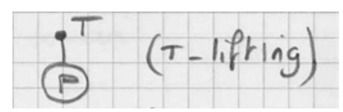
Bottom/top lifting

Given the posets $\langle P, \leq \rangle$, $\langle \perp, = \rangle$ and $\langle \top, = \rangle$

– bottom lifting $P_\perp \stackrel{\text{def}}{=} \{\perp\} \oplus P$ adds a bottom to P:

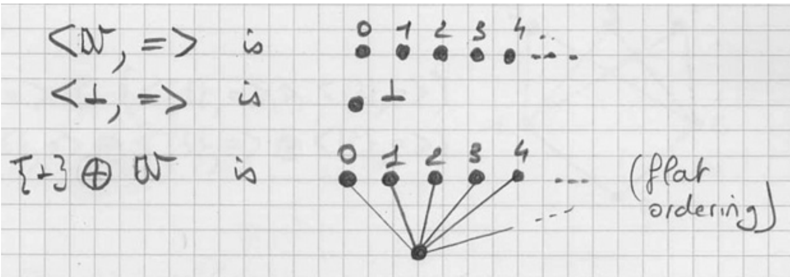


– top lifting $P^\top \stackrel{\text{def}}{=} P \oplus \{\top\}$ adds a top to P:



Flat ordering

Given a set S, and posets $\langle S, =\rangle$ and $\langle\{\bot\}, =\rangle$, Scott's flat ordering is $S_\bot$. For example:



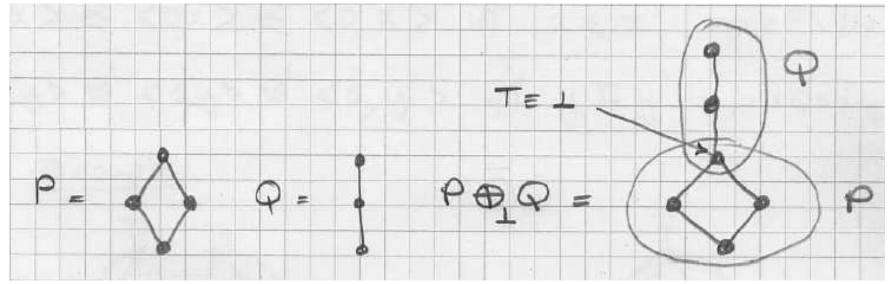
Smashed linear sum (or smashed ordinal sum) of posets

Let $\langle P, \leq, \top\rangle$ and $\langle Q, \sqsubseteq, \bot\rangle$ be two posets such that P has a top $\top$ and Q has a bottom $\bot$. Their smashed linear sum (or smashed ordinal sum) is

$$\begin{aligned}\langle P, \leq\rangle \oplus_\bot \langle Q, \sqsubseteq\rangle &\stackrel{\text{def}}{=} \langle P \setminus \{\top\}, \leq\rangle \oplus \langle Q, \sqsubseteq\rangle \\ &\sim \langle P, \leq\rangle \oplus \langle Q \setminus \{\bot\}, \sqsubseteq\rangle\end{aligned}$$

(so that it is obtained from the linear sum $\langle P, \subseteq\rangle \oplus \langle Q, \sqsubseteq\rangle$ by identifying the top $\top$ of P with the bottom $\bot$ of Q).

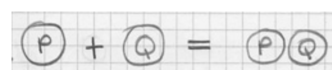
Example:



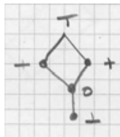
Disjoint (cardinal) sum of posets

Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be two posets. Their disjoint (cardinal) sum is $\langle P, \leq\rangle + \langle Q, \sqsubseteq\rangle \stackrel{\text{def}}{=} \langle P + Q, \preceq\rangle$ such that:

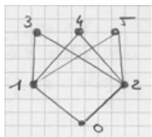
- $P + Q \stackrel{\text{def}}{=} \{\langle 0, x\rangle \mid x \in P\} \cup \{\langle 1, y\rangle \mid y \in Q\}$
- $\langle i, x\rangle \preceq \langle j, y\rangle \stackrel{\text{def}}{=} \begin{array}{l}(i = j = 0 \wedge x \leq y) \\ \vee\ (i = j = 1 \wedge x \sqsubseteq y)\end{array}$
- Intuition:



- Example 1: $\langle\{\bot\},\ =\rangle \oplus \langle\{0\},\ =\rangle \oplus (\langle\{-\},\ =\rangle + \langle\{+\},\ =\rangle) \oplus \langle\{\top\},\ =\rangle$ is (up to an isomorphism):



- Example 2: $\langle\{0\},\ =\rangle \oplus (\langle\{1\},\ =\rangle + \langle\{2\},\ =\rangle) \oplus (\langle\{3\},\ =\rangle + \langle\{4\},\ =\rangle + \langle\{5\},\ =\rangle)$is (up to an isomorphism):



Smashed disjoint (cardinal) sum of posets

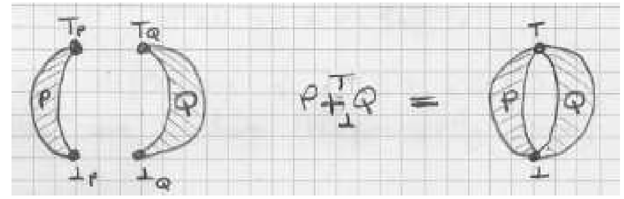
Let $\langle P,\ \leq,\ \bot_P,\ \top_P\rangle$ and $\langle Q,\ \sqsubseteq,\ \bot_P,\ \top_P\rangle$ be two posets. The smashed disjoint sum $\langle P,\ \leq\rangle +_\bot^\top \langle Q,\ \sqsubseteq\rangle$ is $\langle P +_\bot^\top Q,\ \leq\rangle$ where:

$$P +_\bot^\top Q \stackrel{\text{def}}{=} \{\langle 0,\ x\rangle \mid x \in P \setminus \{\bot_P, \top_P\}\} \cup \{\langle 1,\ y\rangle \mid y \in Q \setminus \{\bot_Q, \top_Q\}\} \cup \{\bot, \top\}$$

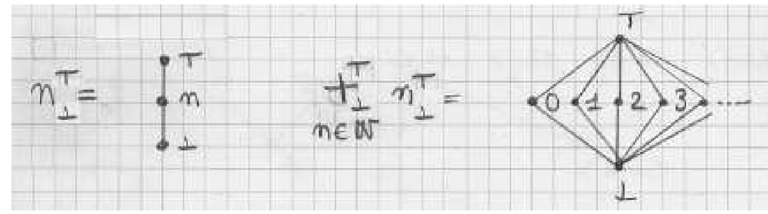
with ordering $\leq$ such that:

- $\bot \leq \bot \leq \langle 0,\ x\rangle \leq \top \leq \top$ for all $x \in P \setminus \{\bot_P, \top_P\}$
- $\bot \leq \langle 1,\ y\rangle \leq \top$ for all $y \in Q \setminus \{\bot_Q, \top_Q\}$
- $\langle 0,\ x\rangle \leq \langle 0,\ x'\rangle$ iff $x \leq x'$ and $x, x' \in P \setminus \{\bot_P, \top_P\}$
- $\langle 1,\ y\rangle \leq \langle 1,\ y'\rangle$ iff $y \sqsubseteq y'$ and $y, y' \in Q \setminus \{\bot_Q, \top_Q\}$

Intuition:



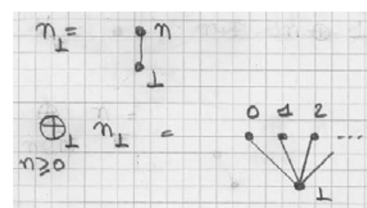
Example:



More generally, we can write:

- $+$ for the cardinal sum
- $+_\bot$ for the $\bot$-smashed cardinal sum
- $+^\top$ for the $\top$-smashed cardinal sum
- $+_\bot^\top$ for the $\bot$ and $\top$-smashed cardinal sum

For example:



The cartesian (cardinal, componentwise) product of posets

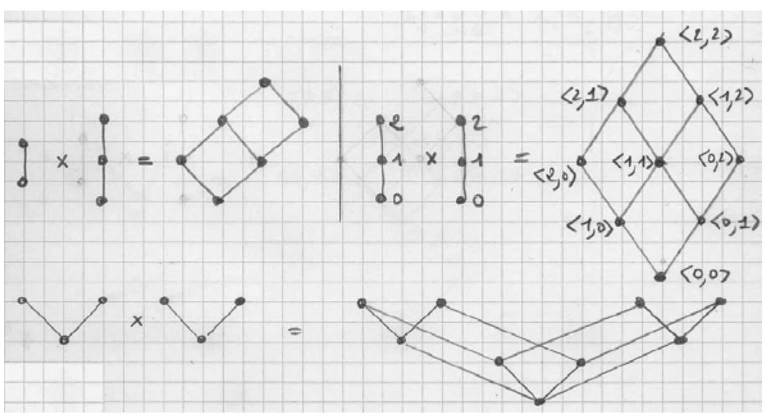
Let $\langle P_1, \leq_1\rangle, \ldots, \langle P_n, \leq_n\rangle$ be posets. The cartesian product

$$P_1 \times \ldots \times P_n \stackrel{\text{def}}{=} \{\langle x_1, \ldots, x_n\rangle \mid \bigwedge_{i=1}^{n} x_i \in P_i\}$$

can be made a poset $\langle P_1 \times \ldots \times P_n, \dot{\leq}\rangle$ with the componentwise ordering:

$$\langle x_1, \ldots, x_n\rangle \dot{\leq} \langle y_1, \ldots, y_n\rangle \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n} x_i \leq_i y_i$$

Examples:



The componentwise ordering $\dot{\leq}$ is sometimes denoted $\leq_1 \times \ldots \times \leq_n$.

If the relations $\leq_i$, $i = 1, \ldots, n$ are reflexive, symmetric, antisymmetric, transitive, a preorder, an equivalence, a directed order or a partial order then so is the componentwise ordering.

Smashed cartesian (cardinal, componentwise) product of posets

Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be posets with infima $\bot_P$, $\bot_Q$ and suprema $\top_P$ and $\top_Q$.
The smashed cartesian product $\langle P, \leq\rangle \times_\bot \langle Q, \sqsubseteq\rangle$ of $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ is $\langle P \times_\bot Q, \preceq\rangle$ such that:

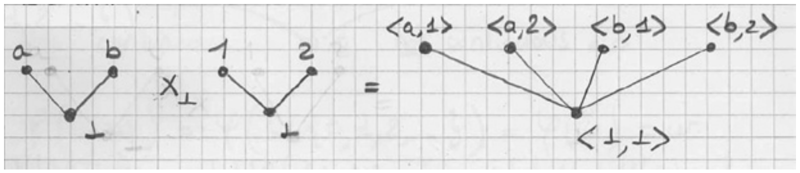
$$P \times_\bot Q \stackrel{\text{def}}{=} \{\langle x, y\rangle \mid x \in P \setminus \{\bot_P, \top_P\} \wedge y \in Q \setminus \{\bot_Q, \top_Q\}\} \cup \{\bot, \top\}$$

where $\bot, \top \notin P \cup Q$ and

- $\bot \preceq \bot \preceq \langle x, y\rangle \preceq \top \preceq \top$ for all $x \in P \setminus \{\bot_P, \top_P\}$ and $y \in Q \setminus \{\bot_Q, \top_Q\}$
- $\langle x, y\rangle \preceq \langle x', y'\rangle$ iff $x \leq x' \wedge y \sqsubseteq y'$ for all $x, x' \in P \setminus \{\bot_P, \top_P\}$ and $y, y' \in Q \setminus \{\bot_Q, \top_Q\}$

Same definitions if $\langle P,\ \leq\rangle$ and $\langle Q,\ \sqsubseteq\rangle$ have only one bottom or top.

Example:



The lexicographic (ordinal) product of posets

Given posets $\langle P_1,\ \leq_1\rangle, \ldots, \langle P_n,\ \leq_n\rangle$, the cartesian product

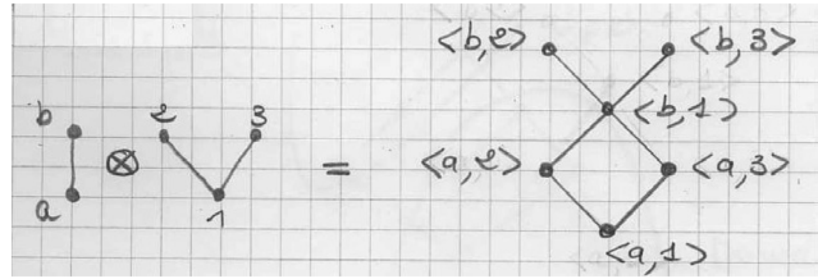
$$P_1 \times \ldots \times P_n \stackrel{\text{def}}{=} \{\langle x_1,\ \ldots,\ x_n\rangle \mid \bigwedge_{i=1}^{n} x_i \in P_i\}$$

can be made a poset by the lexicographic ordering $\leq^n$:

$$\langle x_1,\ \ldots,\ x_n\rangle <^n \langle y_1,\ \ldots,\ y_n\rangle \stackrel{\text{def}}{=} \exists i \in [1,n] : \forall j < i : x_j = y_j \wedge x_i <_i y_i$$

$$\langle x_1,\ \ldots,\ x_n\rangle \leq^n \langle y_1,\ \ldots,\ y_n\rangle \stackrel{\text{def}}{=} \langle x_1,\ \ldots,\ x_n\rangle <^n \langle y_1,\ \ldots,\ y_n\rangle \vee \bigwedge_{i=1}^{n} x_i = y_i$$

Example:



Pointwise ordering of maps on posets

Let $f, g \in D \mapsto P$ be maps on the poset $\langle P,\ \leq\rangle$. The pointwise ordering between such maps is

$$f \stackrel{.}{\leq} g \stackrel{\text{def}}{=} \forall x \in D : f(x) \leq g(x)$$

Example:

$$f \in \mathbb{N} \mapsto \mathbb{N}\ f(x) = 2x$$
$$g \in \mathbb{N} \mapsto \mathbb{N}\ g(x) = 3x$$

We have $f \stackrel{.}{\leq} g$ since $\forall x \in \mathbb{N} : f(x) = 2x \leq 3x = g(x)$.

If the cartesian product $P^n = \underbrace{P \times \ldots \times P}_{n \text{ times}}$ is seen as a map of $[1,n] \mapsto P$, then the componentwise ordering on P^n coincide with the pointwise ordering on $[1,n] \mapsto P$.

Cardinal power of posets

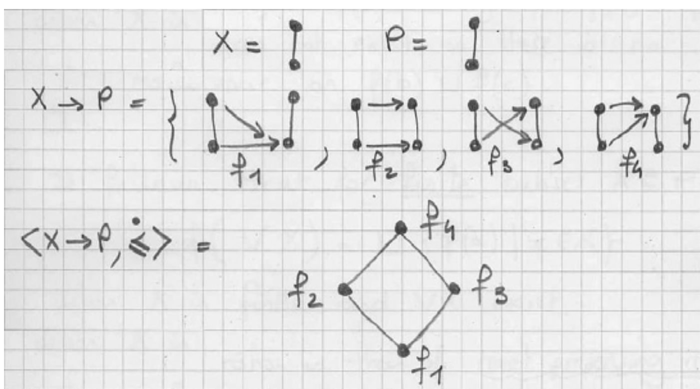
Given a set X and a poset $\langle P, \leq \rangle$, the cardinal power P^X is the poset $\langle X \mapsto P, \dot{\leq} \rangle$ of maps of X into P for the pointwise ordering $f \dot{\leq} g \stackrel{\text{def}}{=} \forall x \in X : f(x) \leq g(x)$.

Since $n = \{0, \ldots, n-1\}$, P^n can be isomorphically viewed as:

– The cardinal product $\{\langle x_0, \ldots, x_n \rangle \mid \bigwedge_{i=1}^{n-1} x_i \in P\}$

– The set of maps $n \mapsto P$

Example:



Ordinal/cardinal sum/product/power of posets/cpos/lattices/complete lattices

Let $\langle P, \leq \rangle$ and $\langle Q, \sqsubseteq \rangle$ be posets. If $\langle P, \leq \rangle$ and $\langle Q, \sqsubseteq \rangle$ are respectively

– posets

– cpos

– lattices

– complete lattices

then

– the ordinal sum $P \oplus Q$

– the smashed ordinal sum $P \oplus_\perp Q$

– the cardinal sum $P + Q$

– the smashed cardinal sum $P +_\perp Q$

– the ordinal product $P \otimes Q$

– the cardinal product Q^P

is respectively

– a poset

– a cpo

– a lattice

– a complete lattice

Proof. tedious but trivial. □

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/.