« Mathematical foundations: (4) Ordered maps and Galois connexions » 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/

Maps between Posets

(Homo|iso|epi|mono|endo|auto)-morphisms

- A *morphism* (or *homomorphism*) is an application $f \in S_1 \mapsto S_2$ between two sets S_1 and S_2 equipped with operations

$$\begin{array}{r}g \in S_1^n \mapsto S_1\\ g' \in S_2^n \mapsto S_2\end{array}$$

such that $\forall x_1, \ldots, x_n \in S_1$:

$$f(g(x_1, \ldots, x_n)) = g'(f(x_1), \ldots, f(x_n))$$

- If $n = 1$ then $f \circ g = g' \circ f$, diagramatically:

$$\begin{tikzcd}
S_2 \arrow[r, "g'"] & S_2 \\
S_1 \arrow[u, "f"] \arrow[r, "g"] & S_1 \arrow[u, "f"']
\end{tikzcd}$$

- an *isomorphism* is a bijective morphism
- an *epimorphism* is an onto/surjective morphism
- an *monomorphism* is a one-to-one/injective morphism
- an *endomorphism* has $S_1 = S_2$
- an *automorphism* is a bijective endomorphism

- The morphism may be relative to relations $r \subseteq S_1^n$ and $r' \subseteq S_2^n$ such that for all $\langle x_1, \ldots, x_n\rangle \in S_1^n$:

$$\langle x_1, \ldots, x_n\rangle \in r \Longrightarrow \langle f(x_1), \ldots, f(x_n)\rangle \in r'$$

- For binary relations:

$$x_1 \; r \; x_2 \Longrightarrow f(x_1) \; r' \; f(x_2)$$

Complete (homo|iso|epi|mono|endo|auto)-morphisms

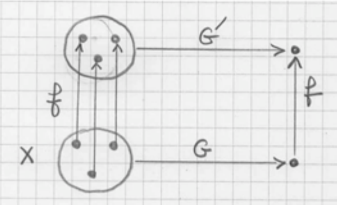
- A *complete morphism* (or *homomorphism*) is an application $f \in S_1 \mapsto S_2$ between two sets S_1 and S_2 equipped with operations

$$G \in \wp(S_1) \mapsto S_1$$
$$G' \in \wp(S_2) \mapsto S_2$$

such that $\forall X \subseteq S_1$:

$$f(G(X)) = G'(f(X)) \text{ where } f(X) \stackrel{\text{def}}{=} \{f(x) \mid x \in X\}$$

- Diagrammatically:



- if f is bijective, onto, one-to-one then f is a *complete iso-*, *epi-*, *mono-morphism*. If $S_1 = S_2$ then f is a *complete endomorphism*, and a *complete automorphism* when f is bijective.

Monotone maps

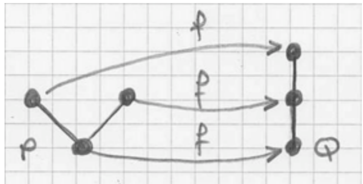
- Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be two posets. A map $f \in P \mapsto Q$ is *monotone* iff

$$\forall x, y \in P : (x \leq y) \implies (f(x) \sqsubseteq f(y))$$

- Alternatives
  - order-preserving
  - isotone
  - increasing

- order morphism
- . . .

– Example:



– Monotony[1] is self-dual (the dual of "monotone" is "monotone")

[1] Also "Monotonicity".

Antitone (decreasing) maps

– Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be two posets. A map $f \in P \mapsto Q$ is *antitone* iff

$$\forall x, y \in P : (x \leq y) \implies (f(x) \sqsupseteq f(y))$$

– Alternatives
  - order-inversing
  - decreasing
  - . . .

– Self-dual notion

Characterization of monotone maps using lubs

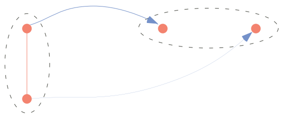
THEOREM. Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be two posets and $f \in P \mapsto Q$. If f is monotone then whenever $S \subseteq P$ and both lubs $\bigvee S$ exists in P and $\bigsqcup f(S)$ exists in Q then:

$$\bigsqcup f(S) \sqsubseteq f(\bigvee S)$$

The reciprocal is false but holds for join-semi-lattices. ■

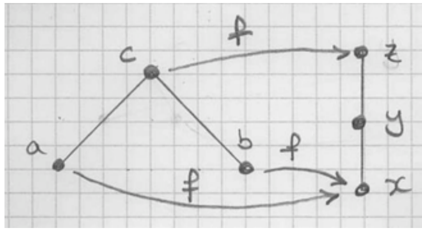
PROOF. – Assume f is monotone, $\bigvee S$ and $\bigsqcup f(S)$ exist. Then $\forall s \in S : s \leq \bigvee S$ so by monototny $f(s) \leq f(\bigvee S)$ whence $\bigsqcup f(S) \sqsubseteq f(\bigvee S)$ by def. lub.

– A counter-example to the reciprocal is



– Conversely, for a join-semi-lattice, if $\bigsqcup f(S) \sqsubseteq f(\bigvee S)$ whenever $\bigvee S$ and $\bigsqcup f(S)$ exist then when $x \leq y$ and $S = \{x, y\}$ we have $\bigvee S = x \vee y = y$ so $f(x) \sqcup f(y)$ exists in the join-semi-lattice and $f(x) \sqcup f(y) = \bigsqcup f(S) \sqsubseteq f(\bigvee S) = f(y)$ whence $f(x) \sqcup f(y) = f(y)$ which implies $f(x) \sqsubseteq f(y)$. □

The inclusion can be strict, as shown by the following example



- f is monotone
- $\bigsqcup f(\{a, b\}) = f(a) \sqcup f(b)$
  $= x \sqcup x = x$

$\sqsubset$ z $= f(c) = f(a \vee b)$

Characterization of monotone maps using glbs

Theorem. Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be two posets and $f \in P \mapsto Q$. If f is monotone then whenever $S \subseteq P$, the glbs $\bigwedge S$ exists in P and $\bigsqcap f(S)$ exists in Q, we have:

$$\bigsqcap f(S) \sqsupseteq f(\bigwedge S) .$$

The reciprocal is false but holds for meet-semi-lattices. ■

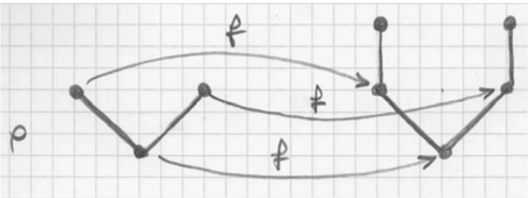
Proof. By duality. □

Order embedding

- Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be two posets A map $f \in P \mapsto Q$ is an *order embedding* (written $f \in P \rightarrowtail Q$ or $f \in P \hookrightarrow Q$) iff

$$\forall x, y \in P : x \leq y \iff f(x) \sqsubseteq f(y)$$

- Example:



An order embedding is injective

Theorem. Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be two posets and $f \in P \hookrightarrow Q$ be an order-embedding. f is injective. ■

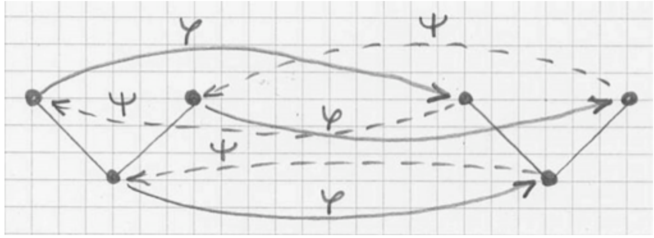
Proof.

$$\begin{array}{ll} & f(x) = f(y) \\ \Longrightarrow & f(x) \sqsubseteq f(y) \wedge f(y) \sqsubseteq f(x) \\ \Longrightarrow & x \leq y \wedge y \leq x \\ \Longrightarrow & x = y \quad \text{and so} \\ & x \neq y \Longrightarrow f(x) \neq f(y) \end{array}$$

□

Order isomorphism

- Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be posets. An *order-isomorphism* is an order-embedding which is onto (whence bijective).
- Example:



- Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be posets. These ordered ordered sets are therefore order-isomorphic if and only if

  $\exists \varphi \in P \mapsto Q : \exists \psi \in Q \mapsto P :$
  - $\varphi \circ \psi = 1_Q$[2]
  - $\psi \circ \varphi = 1_P$
  - φ is monotone
  - ψ is monotone

[2] 1_S is the identity map on set S.

Example of order isomorphism: boolean encoding of finite sets

THEOREM. Let $X = \{x_1, x_2, \ldots, x_n\}$ be a finite set. Define

$$\varphi \;:\; \wp(X) \mapsto 2^n$$
$$\varphi(S) \stackrel{\text{def}}{=} \lambda i \cdot (x_i \in S \;?\; \text{tt} \;:\; \text{ff})$$

The φ is an order-isomorphism between $\langle \wp(X), \subseteq\rangle$ and $\langle 2^n, \dot{\leq}\rangle$ where $\dot{\leq}$ is the componentwise ordering based on $\text{ff} \leq \text{ff} < \text{tt} \leq \text{tt}$. ■

PROOF.

— $\quad x \subseteq Y$

$\iff \quad \forall i \in [1, n] : x_i \in X \Longrightarrow x_i \in Y$

$\iff \quad \forall i \in [1, n] : \varphi(X)_i \leq \varphi(Y)_i$

$\iff \quad \varphi(X) \dot{\leq} \varphi(Y)$ on 2^n

— If $X \neq Y$ then there is a $x_i \in X$ not in Y (or inversely) so $\varphi(x)_i = \text{tt}$ and $\varphi(Y)_i = \text{ff}$ (or inversely), proving that $\varphi(X) \neq \varphi(Y)$ hence φ is injective.

— Given $\langle b_1, \ldots, b_n\rangle \in 2^n$, we take $S = \{x_i \in S \mid b_i = \text{tt}\}$ so that $\varphi(S) = \langle b_1, \ldots, b_n\rangle$ proving that φ is onto. □

Used to encode finite sets as bit vectors.

Embedding of a poset in its powerset

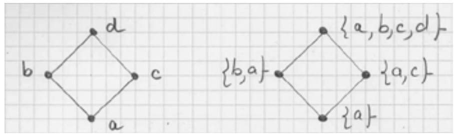
THEOREM. Let $\langle P, \leq\rangle$ be a poset. Then there is a set $Q \subseteq \wp(P)$ of subsets of P such that $\langle P, \leq\rangle$ is oreder-isomorphic to $\langle Q, \subseteq\rangle$ ■

PROOF. – Define $Q = \{\downarrow x \mid x \in P\}$

- Define $\varphi \in P \mapsto Q$ by $\varphi(x) \stackrel{\text{def}}{=} \downarrow x$
- φ is a bijection
- $(x \leq y) \iff (\downarrow x \subseteq \downarrow y)$

□

Example:

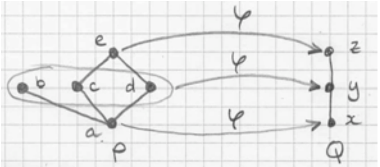


Join/meet preserving maps

- let $\langle p, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be two posets. The map $f \in P \mapsto Q$ is called *join preserving* whenever if $x, y \in P$ and the lub $x \vee y$ exists in P then the lub $f(x) \sqcup f(y)$ does exist in Q and is such that:

$$f(x \vee y) = f(x) \sqcup f(y)$$

- Example:



  - $(f(c \vee d) = f(e) = z = y \sqcup z = f(c) \sqcup f(d)$
  - $b \vee c$ does not exists so the is no requirement on $f(b) \sqcup f(c)$

- It follows that for a join preserving map and a finite subset $X \subseteq P$ for which $\bigvee X$ does exist:

$$f(\bigvee X) = \bigsqcup f(X)^{3}$$

- The dual notion is that of *meet preserving map*:

$$f(\bigwedge X) = \bigsqcap f(X)$$

for all finite subsets $X \subseteq P$ such that $\bigwedge X$ exists.

[3] where $f(X) \stackrel{\text{def}}{=} \{f(x) \mid x \in X\}$.

Join/meet preserving maps are monotone

THEOREM. A join or meet preserving map is monotone ■

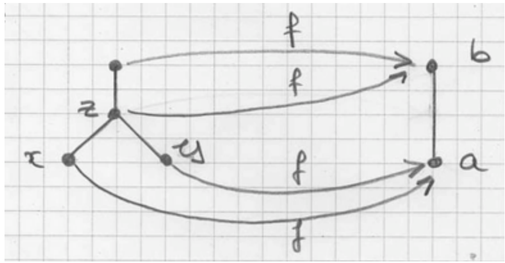
PROOF. – if $x \sqsubseteq y$ then $x \sqcup y = y$ does exists. So $f(s \sqcup y) = f(x)$ hence $f(x) \sqcup f(y) = f(y)$ since f preserves existing, proving that $f(x) \sqsubseteq f(y)$ by def. of lubs.

- By duality a meet-preserving maps is monotone (since the dual of monotone is monotone)

□

Not all monotone maps preserve lubs/glbs

Counter-example:



- f is monotone
- $f(x \vee y) = f(z) = b$
- $f(x) \sqcup f(y) = a \sqcup a = a \neq b$

Complete join preserving maps

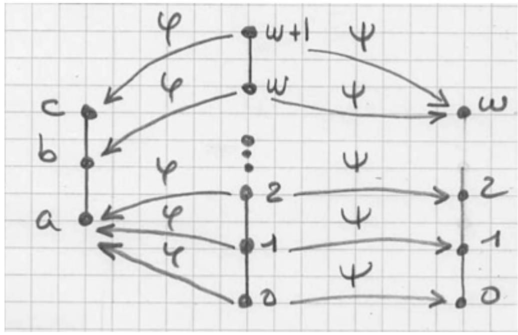
- Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be two posets. The map $f \in P \mapsto Q$ is a *complete join preserving* whenever it preserves existing lubs:

$$\forall X \subseteq P : \bigvee X \text{ exists } \Longrightarrow f(\bigvee X) = \bigsqcup f(X)$$

- The dual notion is that of *complete meet preserving map*:

$$\forall X \subseteq P : \bigwedge X \text{ exists } \Longrightarrow f(\bigwedge X) = \bigsqcap f(X)$$

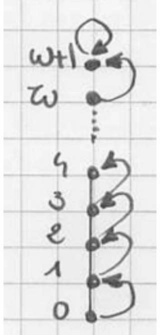
- Example:



- φ is not a complete join morphism:
  $\varphi(\bigcup\omega) = \varphi(\bigcup\{0, 1, 2, \ldots\}) = \varphi(\omega) = b \neq a = \bigcup\{a\} = \bigcup\{\varphi(x) \mid x \in \omega\} = \bigcup\varphi(\omega)$
- φ is a join morphism
- ψ is a complete join morphism

Not all finite join/meet preserving maps are complete

- Example of finite join preserving map which is not a complete join preserving map:



Continuous and co-continuous maps

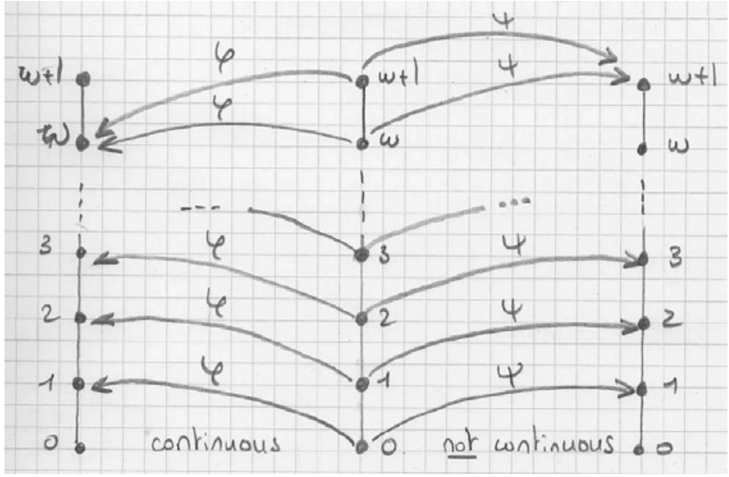
- A map $f \in P \mapsto Q$ from a poset $\langle P, \leq\rangle$ into a poset $\langle Q, \sqsubseteq\rangle$ is *continuous* (or *upper-continuous*) if an only if for all chains C of P such that $\bigvee C$ exists then $\bigsqcup f(C)$ exists and we have

$$f(\bigvee C) = \bigsqcup f(C)$$

- Often this hypothesis is needed only for denumerable chains. f is *ω-continuous* iff for all increasing chains $x_0 \leq x_1 \leq \ldots \leq x_n \leq \ldots$ of P such that $\bigvee_{i\in\mathbb{N}} x_i$ exists then $\bigsqcup_{i\geq 0} f(x_i)$ exists and

$$f(\bigvee_{i\in\mathbb{N}} x_i) = \bigsqcup_{i\in\mathbb{N}} f(x_i)$$

- Example (φ) and counter-example (ψ):



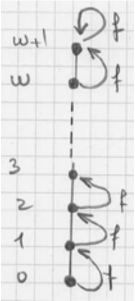
Continuous (or co-continuous) maps are monotone (but not the converse)

THEOREM. Let $f \in P \mapsto Q$, $\langle P, \leq\rangle$ be a poset. If f is ω-continuous (preserves exists lubs of denumerable chains) then f is monotone. ■

PROOF. If $x \leq y$ the denumerable chain $x \leq y \leq y \leq y \leq \ldots$ has a lub y, so by ω-continuity of f, $f(y) = f(\bigvee\{x,y\}) = f(x) \vee f(y)$ proving $f(x) \leq f(y)$ by def. of lubs. □

- By duality, ω-co-continuous maps are monotone

- The reciprocal is not true. A monotone map may not be ω-continuous, as shown by the following counter-example:



- $f(x) = x + 1$, $x \leq \omega$
- $f(\omega + 1) = \omega + 1$
- f is monotone
- f is not continuous since
  $f(\bigcup_{n<\omega}) = f(\omega) = \omega + 1$
  $\bigcup_{n<\omega} f(n) = \bigcup_{n<\omega}(n+1) = \bigcup \omega = \omega$

Chain conditions and continuity

Theorem. Let $\langle P, \leq\rangle$ be a poset statisfying the ascending chain condition (ACC) and $\langle Q, \sqsubseteq\rangle$ be a poset. Then any monotone map $f \in P \mapsto Q$ is continuous. ∎

Proof. Let $\langle x_\delta, \delta \in \mathbb{O}\rangle$ be an increasing chain of elements of P. By the ACC, $\exists k < \omega : \forall \delta > k : x_\delta = x_k$ so that $\bigvee_{\delta\in\mathbb{O}} x_\delta = x_k$. It follows that $f(\bigvee_{\delta\in\mathbb{O}} x_\delta) = f(x_k)$. Since $\forall \delta \in \mathbb{O} : x_\delta \leq x_k$ and f is monotone, we have $f(x_\delta) \sqsubseteq f(x_k)$ whence $\bigsqcup_{\delta\in\mathbb{O}} f(x_\delta) \sqsubseteq f(x_k)$. But $f(x_k) \in \{f(x_\delta) \mid \delta \in \mathbb{O}\}$ so $f(x_k) \sqsubseteq \bigsqcup_{\delta\in\mathbb{O}} f(x_\delta)$ and by antisymmetry $\bigsqcup_{\delta\in\mathbb{O}} f(x_\delta) = f(x_k)$. It follows that $\bigsqcup_{\delta\in\mathbb{O}} f(x_\delta) = f(x_k) = f(\bigvee_{\delta\in\mathbb{O}} x_\delta)$, proving continuity. □

By duality, if $\langle P, \leq\rangle$ is a poset satisfying the descending chain condition (DCC) and $\langle Q, \sqsubseteq\rangle$ is a poset then any monotone map $f \in P \mapsto Q$ is co-continuous.

Boolean lattice morphism

- Let $\langle P, \vee, \wedge\rangle$ and $\langle Q, \sqcup, \sqcap\rangle$ be lattices. A *lattice morphism* $f \in P \mapsto Q$ satisfies:

$$\begin{aligned} f(x \vee y) &= f(x) \sqcup f(y) \\ f(x \wedge y) &= f(x) \sqcap f(y) \end{aligned}$$

- Let $\langle P, 0, 1, \vee, \wedge, \neg\rangle$ and $\langle Q, \bot, \top, \sqcup, \sqcap, '\rangle$ be boolean algebras. A *Boolean algebra morphism* $f \in P \mapsto Q$ if and only if:
  - f is a lattice morphism
  - $f(0) = \bot$
  - $f(1) = \top$
  - $f(\neg x) = f(x)'$

- Terminology:
  - Homomorphism: morphism
  - Isomorphism: bijective morphism
  - Endomorphism: P=Q
  - Monomorphism: injective morphism
  - Epimorphism: surjective morphism

  (The conditions defining a boolean algebra morphism are not independent, see below).

On the conditions defining the Boolean lattice morphisms

Theorem. Let $\langle P, 0, 1, \vee, \wedge, \neg\rangle$ and $\langle Q, \bot, \top, \sqcup, \sqcap, '\rangle$ be boolean algebras. Assume f is a lattice morphism.

(i) (a) $f(0) = \bot$ and $f(1) = \top$

$\Longleftrightarrow$ (b) $f(\neg a) = (f(a))'$, $\forall a \in P$

(ii) If $f(\neg a) = (f(a))'$, then

(c) $f(a \vee b) = f(a) \sqcup f(b)$

$\Longleftrightarrow$ (d) $f(a \wedge b) = f(a) \sqcap f(b)$

∎

PROOF.(i) Assume (a), then:

$$\bot = f(0) = f(a \wedge -a) = f(a) \sqcap f(-a)$$
$$\top = f(1) = f(a \vee -a) = f(a) \surd sqcup f(-a)$$

proving that $f(-a) = (f(a))'$ whence (b)

Assume (b), then

$$f(0) = f(a \wedge -a) = f(a) \wedge (f(a))' = 0$$
$$f(1) = d(a \vee -a) = f(a) \vee (f(a))' = 1$$

proving (a)

(ii) Assume f preserves complement and join.

$$\begin{aligned} f(a \wedge b) &= f(-(-a \vee -b)) \\ &= (f(-a \vee -b))' \\ &= (f(-a) \sqcup f(-b))' \\ &= ((f(a))' \sqcup (f(b))')' \\ &= f(a) \sqcap f(b) \end{aligned}$$

□

Notations for monotone, lub/glb preserving and (co-)continuous maps

Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be posets. We define:

$\langle P, \leq\rangle \xmapsto{\text{m}} \langle Q, \sqsubseteq\rangle$ (or $P \xmapsto{\text{m}} Q$ if $\leq$ and $\sqsubseteq$ are understood) to be the set of *monotone* maps of P into Q

$\langle P, \leq\rangle \xmapsto{\sqcup} \langle Q, \sqsubseteq\rangle$ (or $P \xmapsto{\sqcup} Q$ if $\leq$ and $\sqsubseteq$ are understood) to be the set of *complete lub-preserving* maps of P into Q

$\langle P, \leq\rangle \xmapsto{\sqcap} \langle Q, \sqsubseteq\rangle$ (or $P \xmapsto{\sqcap} Q$ if $\leq$ and $\sqsubseteq$ are understood) to be the set of *complete glb-preserving* maps of P into Q

$\langle P, \leq\rangle \xmapsto{\text{uc}} \langle Q, \sqsubseteq\rangle$ (or $P \xmapsto{\text{uc}} Q$ if $\leq$ and $\sqsubseteq$ are understood) to be the set of *ω-upper-countinuous* maps of P into Q

$\langle P, \leq\rangle \xmapsto{\text{lc}} \langle Q, \sqsubseteq\rangle$ (or $P \xmapsto{\text{lc}} Q$ if $\leq$ and $\sqsubseteq$ are understood) to be the set of *ω-lower-continuous* maps of P into Q

We use $\rightarrowtail$ for *injective* maps

$\mapsto\!\!\!\!\twoheadrightarrow$ for *surjective* maps

$\rightarrowtail\!\!\!\!\twoheadrightarrow$ for *bijective* maps

The complete lattice of pointwise ordered maps on a complete lattice

THEOREM. Let P be a set and $\langle Q, \sqsubseteq, \bot, \top, \sqcap, \sqcup\rangle$ be a complete lattice. Let $\dot{\sqsubseteq}$ be the *pointwise ordering* of maps $f \in P \mapsto L$: $f \mathrel{\dot{\sqsubseteq}} g \iff \forall x \in P : f(x) \sqsubseteq g(x)$. Then $\langle P \mapsto Q, \dot{\sqsubseteq}, \dot{\bot}, \dot{\top}, \dot{\sqcap}, \dot{\sqcup}\rangle$ (where $\dot{\bot} \stackrel{\text{def}}{=} \lambda x \cdot \bot$, $\dot{\top} = \lambda x \cdot \top$, $\dot{\bigsqcup} F \stackrel{\text{def}}{=} \lambda x \cdot \bigsqcup_{f \in F} f(x)$ and $\dot{\bigsqcap} F \stackrel{\text{def}}{=} \lambda x \cdot \bigsqcap_{f \in F} f(x)$) is a complete lattice. ■

PROOF. – $f \mathrel{\dot\sqsubseteq} f$ since $\forall x \in P : f(x) \sqsubseteq f(x)$ because $\sqsubseteq$ is reflexive

- $f \mathrel{\dot\sqsubseteq} g$ and $g \mathrel{\dot\sqsubseteq} f$ then $\forall x \in P : f(x) \sqsubseteq g(x) \wedge g(x) \sqsubseteq f(x)$ so $\forall x \in P : f(x) = g(x)$ by antisymmetry, proving that $f = g$
- $f \mathrel{\dot\sqsubseteq} g \wedge g \mathrel{\dot\sqsubseteq} h$ implies $\forall x \in P : f(x) \sqsubseteq g(x) \sqsubseteq h(x)$ so $f \mathrel{\dot\sqsubseteq} h$ proving transitivity
- Let $F \subseteq P \mapsto Q$. $\forall f \in F : f(x) \in \{g(x) \mid g \in F\}$ so $f(x) \sqsubseteq \bigsqcup\{g(x) \mid g \in F\} = (\dot{\bigsqcup} F)(x)$ whence $f \mathrel{\dot\sqsubseteq} \dot{\bigsqcup} F$ proving $\dot{\bigsqcup} F$ to be a $\dot\sqsubseteq$-upper bound of F.
- Let u be another upper bound of F. We have $\forall f \in F : f \mathrel{\dot\sqsubseteq} u$ so $\forall x \in P : f(x) \sqsubseteq u(x)$ so $\bigsqcup_{f \in F} f(x) \sqsubseteq u(x)$ hence $(\dot{\bigsqcup} F)(x) \sqsubseteq u(x)$ and $\dot{\bigsqcup} F \mathrel{\dot\sqsubseteq} u$. It follows that $\dot{\bigsqcup} F$ is the $\dot\sqsubseteq$-least upper bound of F
- By duality, the glb is $\dot{\bigsqcap} F \stackrel{\text{def}}{=} \lambda x \cdot \bigsqcap\{f(x) \mid f \in F\}$
- The infimum is $\dot{\bot}$ since $\forall x \in P : \bot \sqsubseteq f(x)$ implies $\dot{\bot} \mathrel{\dot\sqsubseteq} f$
- By duality, the supremum is $\dot{\top} = \lambda x \cdot \top$

□

The complete lattice of pointwise ordered monotone maps on a complete lattice

THEOREM. Let $\langle P, \leq\rangle$ be a poset and $\langle Q, \sqsubseteq, \bot, \top, \sqcap, \sqcup\rangle$ be a complete lattice. The set of monotonic maps of P into Q is a complete lattice $\langle P \xrightarrow{\text{m}} Q, \dot\sqsubseteq, \dot\bot, \dot\top, \dot\sqcap, \dot\sqcup\rangle$ ■

PROOF. – The ordering $f \mathrel{\dot\sqsubseteq} g \iff \forall x \in P : f(x) \sqsubseteq g(x)$ makes $\langle P \mapsto Q, \dot\sqsubseteq\rangle$ a complete lattice

- Since $(P \xrightarrow{\text{m}} Q) \subseteq (P \mapsto Q)$, is follows that $\langle P \xrightarrow{\text{m}} Q, \dot\sqsubseteq\rangle$ is a poset
- The lub in $\langle P \mapsto Q, \dot\sqsubseteq\rangle$ is $\dot\bigsqcup$ such that $(\dot{\bigsqcup\limits_{i \in \Delta}} f_i)(x) = \bigsqcup_{i \in \Delta}(f_i(x))$
- Observe that $\dot{\bigsqcup\limits_{i \in \Delta}} f_i$ is monotone since $x \leq y$ implies $\forall i \in \Delta : f_i(x) \sqsubseteq f_i(y)$ since $f_i \in P \xrightarrow{\text{m}} Q$ so $\forall i \in \Delta : f_i(x) \sqsubseteq \bigsqcup_{i \in \Delta} f_i(y)$ proving $(\bigsqcup_{i \in \Delta} f_i)(x) = \bigsqcup_{i \in \Delta} f_i(x) \sqsubseteq \bigsqcup_{i \in \Delta} f_i(y) = (\bigsqcup_{i \in \Delta} f_i)(y)$ that is $\dot{\bigsqcup\limits_{i \in \Delta}} f_i \in P \xrightarrow{\text{m}} Q$ whenever $\forall i \in \Delta : P \xrightarrow{\text{m}} Q$
- It follows that $\dot{\bigsqcup\limits_{i \in \Delta}} f_i$ is also the lub in $P \xrightarrow{\text{m}} Q$

□

The complete lattice of pointwise ordered, lub-preserving maps on a complete lattice

THEOREM. Let $\langle P, \leq, 0, 1, \vee, \wedge\rangle$ and $\langle L, \sqsubseteq, \bot, \top, \sqcap, \sqcup\rangle$ be complete lattices. The set of complete join morphism of P into Q is a complete lattice $\langle P \xrightarrow{\sqcup} Q, \dot\sqsubseteq, \dot\bot, \dot\top, \tilde\sqcap, \dot\sqcup\rangle$ ■

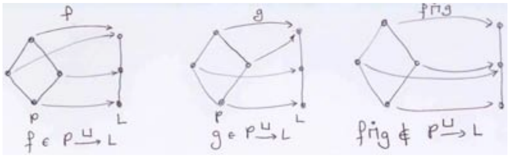
PROOF. – The subset $P \xrightarrow{\sqcup} Q$ of the poset $\langle P \xrightarrow{\text{m}} Q, \dot\sqsubseteq\rangle$ is a poset for $\dot\sqsubseteq$

- The lub $\dot\bigsqcup$ in $\langle P \xrightarrow{\text{m}} Q, \dot\sqsubseteq\rangle$ is also the lub in $P \xrightarrow{\sqcup} Q$ since $\dot{\bigsqcup\limits_{i \in \Delta}} f_i \in P \xrightarrow{\sqcup} Q$ whenever $\forall i \in \Delta : f_i \in P \xrightarrow{\sqcup} Q$. Indeed

$$(\dot{\bigsqcup_{i \in \Delta}} f_i)(\bigvee_{j \in \Gamma} x_j)$$

$$
\begin{aligned}
&= \bigsqcup_{i\in\Delta}(f_i(\bigvee_{j\in\Gamma} x_j)) && \wr\text{def. } \dot{\bigsqcup}\,\wr\\
&= \bigsqcup_{i\in\Delta}\bigsqcup_{j\in\Gamma} f_i(x_j) && \wr f_i \in P \xmapsto{\sqcup} Q\,\wr\\
&= \bigsqcup_{j\in\Gamma}\bigsqcup_{i\in\Delta} f_i(x_j) && \wr\text{commutativity}\wr\\
&= \bigsqcup_{j\in\Gamma}(\dot{\bigsqcup_{i\in\Delta}} f_i)(x_j) && \wr\text{def. } \dot{\bigsqcup}\,\wr
\end{aligned}
$$

– Since $P \xmapsto{\sqcup} Q$ has lubs $\dot{\sqcup}$, it also has glbs $\widetilde{\sqcap}$ which may not coincide with the pointwise glb $\dot{\sqcap}$ in $\langle P \xmapsto{m} Q,\ \dot{\sqsubseteq}\rangle$, as shown by the following counter-example:



f
P
L
$f \in P \xrightarrow{\sqcup} L$
g
P
L
$g \in P \xrightarrow{\sqcup} L$
$f \sqcap g$
$f \sqcap g \notin P \xrightarrow{\sqcup} L$

$\sqsubset$

Encoding Maps between Posets

Claude Elwood Shannon

Randal E. Bryant

Reference

[1] R. E. Bryant, "Graph-Based Algorithms for Boolean Function Manipulation". IEEE Transactions on Computers, Vol. C-35, No. 8 (August, 1986), pp. 677-691.

Encoding of Boolean functions by Boolean terms

Boolean terms

- Let $\langle B, 0, 1, \vee, \wedge, \neg\rangle$ be a boolean algebra
- Let $\mathcal{V}$ be a set of variables and $\langle x_1, \ldots, x_n\rangle \in \mathcal{V}^n$
- The *boolean terms* $\mathrm{Bt}(B, \langle x_1, \ldots, x_n\rangle)$ are defined by the following grammar:

$$T ::= x_i \mid 0 \mid 1 \mid T_1 \vee T_2 \mid T_1 \wedge T_2 \mid \neg T_1 \mid (T_1)$$

The interpretation of Boolean terms

- The *semantics* or *interpretation* $\mathcal{S}[\![T]\!] \in 2^n \mapsto 2$ of $T \in \mathrm{Bt}(B, \langle x_1, \ldots, x_n\rangle)$ is defined by

$$\begin{aligned}
\mathcal{S}[\![x_i]\!](v_1,\ldots,v_n) &\stackrel{\text{def}}{=} v_i\\
\mathcal{S}[\![0]\!](v_1,\ldots,v_n) &\stackrel{\text{def}}{=} 0\\
\mathcal{S}[\![1]\!](v_1,\ldots,v_n) &\stackrel{\text{def}}{=} 1\\
\mathcal{S}[\![T_1 \vee T_2]\!](v_1,\ldots,v_n) &\stackrel{\text{def}}{=} \mathcal{S}[\![T_1]\!](v_1,\ldots,v_n) \vee \mathcal{S}[\![T_2]\!](v_1,\ldots,v_n)\\
\mathcal{S}[\![T_1 \wedge T_2]\!](v_1,\ldots,v_n) &\stackrel{\text{def}}{=} \mathcal{S}[\![T_1]\!](v_1,\ldots,v_n) \wedge \mathcal{S}[\![T_2]\!](v_1,\ldots,v_n)\\
\mathcal{S}[\![\neg T_1]\!](v_1,\ldots,v_n) &\stackrel{\text{def}}{=} \neg\mathcal{S}[\![T_1]\!](v_1,\ldots,v_n)\\
\mathcal{S}[\![(T_1)]\!](v_1,\ldots,v_n) &\stackrel{\text{def}}{=} \mathcal{S}[\![T_1]\!](v_1,\ldots,v_n)
\end{aligned}$$

Encoding of Boolean functions by Boolean terms

- The *encoding* of $v = \langle v_1, \ldots, v_n\rangle \in 2^n$ over variables $\langle x_1, \ldots, x_n\rangle$ is:

$$\begin{aligned}
\mathrm{Te}(v)\langle x_1, \ldots, x_n\rangle = {} & (\, v_1 = 1 \;?\; x_1 : \neg x_1) \wedge \ldots \wedge\\
& (\, v_n = 1 \;?\; x_n : \neg x_n)
\end{aligned}$$

- The *encoding* of $f \in 2^n \mapsto 2$ over variables $\langle x_1, \ldots, x_n\rangle$ is:

$$\begin{aligned}
\mathrm{Te}(f)\langle x_1, \ldots, x_n\rangle = \bigvee\{\mathrm{Te}(v)\langle x_1, \ldots, x_n\rangle \mid {}\\
v \in 2^n \wedge f(v) = 1\}
\end{aligned}$$

THEOREM. For all $a = \langle a_1, \ldots, a_n\rangle \in 2^n$ and $b = \langle b_1, \ldots, b_n\rangle \in 2^n$:

$$\begin{aligned}
\mathcal{S}[\![\mathrm{Te}(a)\langle x_1, \ldots, x_n\rangle]\!]b &= 1 \qquad \text{iff} \quad b = a\\
&= 0 \qquad \text{iff} \quad b \neq a
\end{aligned}$$

■

PROOF.

$$\begin{aligned}
& \mathcal{S}[\![\mathrm{Te}(a)\langle x_1, \ldots, x_n\rangle]\!]b\\
= {} & (\, a_1 = 1 \;?\; \mathcal{S}[\![x_1]\!]b : \neg\mathcal{S}[\![x_1]\!]b) \wedge \ldots \wedge (\, a_n = 1 \;?\; \mathcal{S}[\![x_n]\!]b : \neg\mathcal{S}[\![x_n]\!]b)\\
= {} & (\, a_1 = 1 \;?\; b_1 : \neg b_1) \wedge \ldots \wedge (\, a_n = 1 \;?\; b_n : \neg b_n)\\
= {} & (a_1 = b_1 \wedge \ldots \wedge a_n = b_n)\\
= {} & a = b\\
= {} & \begin{cases} 1 & \text{iff} \quad a = b\\ 0 & \text{iff} \quad a \neq b \end{cases}
\end{aligned}$$

□

Bijection between Boolean functions and their encodings by Boolean terms

THEOREM. $2^n \mapsto 2$ and $\{\mathrm{Te}(f)\langle x_1, \ldots, x_n\rangle \mid f \in 2^n \mapsto 2\}$ are isomorphic by $\langle \mathcal{S}, \mathrm{Te}\rangle$. ■

PROOF.

— $\mathcal{S}[\![\mathrm{Te}(f)\langle x_1, \ldots, x_n\rangle]\!]b$ where $b = \langle b_1, \ldots, b_n\rangle$

$= \bigvee\{\mathcal{S}[\![\mathrm{Te}(v)\langle x_1, \ldots, x_n\rangle]\!]b \mid f(v) = 1\}$

$= \bigvee\{(\!| b = v \mathbin{?} 1 \mathbin{:} 0 |\!) \mid f(v) = 1\}$

$= f(b) = 1$

$= f(b)$

— Let $T \in \{\mathrm{Te}(f)\langle x_1, \ldots, x_n\rangle \mid f \in 2^n \mapsto 2\}$. We must show that $\mathrm{Te}(\mathcal{S}[\![T]\!]) = T$. Given $f \in 2^n \mapsto 2$, we have $\mathrm{Te}(\mathcal{S}[\![\mathrm{Te}(f)\langle x_1, \ldots, x_n\rangle]\!]) = \mathrm{Te}(f)$, Q.E.D. □

Boolean terms in disjunctive normal forms

– A Boolean tern over $\{x_1, \ldots, x_n\}$ is in disjunctive normal form (DNF) iff it is in the form

$$\bigvee_{i=1}^{k} \bigwedge_{j=1}^{n} \ell_{ij} \quad \text{where } \ell_{ij} \text{ is } x_j \text{ or } \neg x_j$$

– Any boolean term T can be put in equivalent DNF[4]

[4] Since $\mathcal{S}[\![T]\!] = \mathcal{S}[\![\mathrm{Te}(\mathcal{S}[\![T]\!])\langle x_1, \ldots, x_n\rangle]\!]$ and $\mathrm{Te}(\mathcal{S}[\![T]\!])\langle x_1, \ldots, x_n\rangle$ is in DNF.

– Algorithm:

- Use De Morgarn's laws to reduce the term to meets and joins of literals x_j or $\neg x_j$
- Use the distributive laws, with the lattice identities to obtains a join of meets of literals
- Finally, each x_j (or $\neg x_j$) should appear once and only once in each meet term:
  1. Drop any meet term containing x_i and $\neg x_i$ for some $i = 1, \ldots, n$
  2. If neither x_j nor $\neg x_j$ occurs in $\bigwedge\limits_{k \in K} x_k^{\epsilon_k}$ (where $\epsilon_k \in \{0, 1\}$, $x^1 = x$, $x^0 = \neg x$) then:

$$\begin{aligned}\bigwedge_{k \in K} x_k^{\epsilon_k} &= (\bigwedge_{k \in K} x_k^{\epsilon_k}) \wedge (x_j \vee \neg x_j)\\ &= (\bigwedge_{k \in K} x_k^{\epsilon_k} \wedge x_j) \vee (\bigwedge_{k \in K} x_k^{\epsilon_k} \wedge \neg x_j)\end{aligned}$$

  Repeating this process for each missing variable will lead to a term in DNF

Example (conditional)

$$\begin{aligned} & f(x, y, z) = (\!| x \mathbin{?} y \mathbin{:} z |\!)\\ = \ & (x \wedge y) \vee (\neg x \wedge z)\\ = \ & ((\neg x \wedge z) \wedge (y \vee \neg y)) \vee ((x \wedge y) \wedge (z \vee \neg z))\\ = \ & (\neg x \wedge \neg y \wedge z) \vee (\neg x \wedge y \wedge z) \vee (x \wedge y \wedge \neg z) \vee (x \wedge y \wedge z)\end{aligned}$$

in so called "disjunctive normal form".

Encoding of Boolean functions by BDDs

The presentation follows: Laurent Mauborgne: "Abstract Interpretation Using Typed Decision Graphs" Science of Computer Programming, 31(1):91–112, may 1998.

Example of Shannon trees

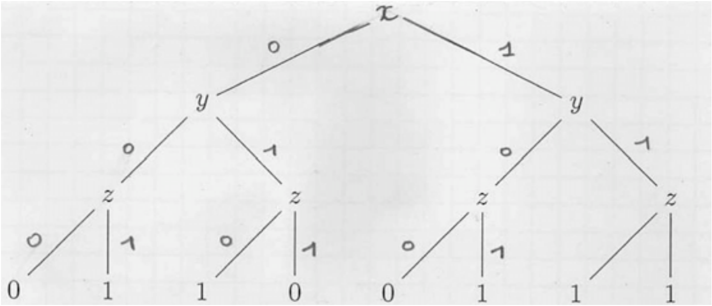
A BDD (Binary Decision Diagram) discovered by Randal Bryant in 1986 is a compact representation of a Shannon tree of a boolean expression.

Example:

- $f(x, y, z) = (x \wedge y) \wedge (y \wedge \neg z) \vee (z \vee \neg y)$
- Table representation:

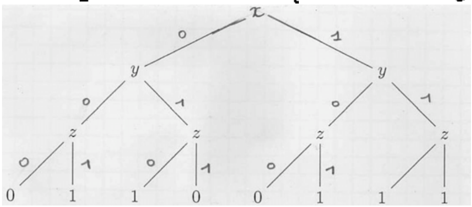
x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
f	0	1	1	0	0	1	1	1

- Shannon tree representation (with $x < y < z$)



Example of Reduction of a Shannon tree into an [Ordered] Boolean Decision Diagram — [O]BDD

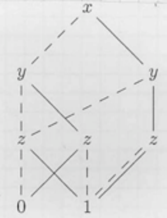
- Shannon tree representation (with $x < y < z$)



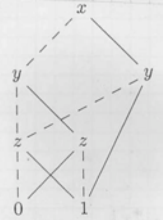
(1) Sharing: merge redundant subtrees (to get a Directed Acyclic Graph — DAG)

- - - - : left (0) branch

———— : right (1) branch



(2) Elimination of the useless nodes (where the different possible values of the variable lead to the same result):



Shannon decomposition of Boolean functions

- Let $\langle \mathsf{Var}, <^v \rangle$ be a totally strictly ordered set of variables
- Let $\mathsf{Var}_n = \{V \subseteq \mathsf{Var} \mid |V| = n\}$ be the set of n variables $\{x_1, \ldots, x_n\}$ where, by convention, $x_1 <^v \ldots <^v x_n$
- Let $B_n = \mathsf{Var}_n \times (\{0,1\}^n \mapsto \{0,1\})$ be the set of pairs $\langle \{x_1, \ldots, x_n\},\ f \rangle$ denoted $f(x_1, \ldots, x_n)$ which value at point $x_1 = b_1, \ldots, x_n = b_n$ is $f(b_1, \ldots, b_n)$
- Let $V(f(x_1, \ldots, x_n)) = \{x_1, \ldots, x_n\}$ where $x_1 <^v \ldots <^v x_n$

- Let $B = \bigcup_{n \in \mathbb{N}} B_n$
- Shannon expansion theorem:

THEOREM. Let $f(x_1, \ldots, x_n) \in B_n$. $\forall i \in [1, n] : \exists! \langle f_{\bar{x}_i},\ f_{x_i} \rangle$[5] $\in B_{n-1} \times B_{n-1}$ such that

$$f(x_1, \ldots, x_n) = (\neg x_i \wedge f_{\bar{x}_i}) \vee (x_i \wedge f_{x_i})$$

■

PROOF. Choose:

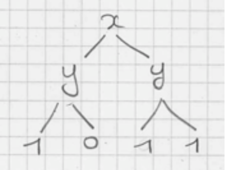
$$\begin{aligned} f_{\bar{x}_i}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) &= f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \\ f_{x_i}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) &= (x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \end{aligned}$$

□

[5] $\exists! x : P$ means "there exists a unique x such that P" i.e. $\exists x : P \wedge \forall y, z : (P[x := y] \wedge P[x := z]) \Longrightarrow (y = z)$.

Shannon tree

- A Shannon tree over variables $x_1 <^v \ldots <^v x_n$ is
  - if $n = 0$ then 1 or 0
  - if $n > 0$ then $\langle x_1,\ t_1,\ t_2 \rangle$ where t_1, t_2 are Shannon trees over $x_2 <^v \ldots <^v x_n$
- Example $x_1 = x <^v x_2 = y$



$\langle x,\ \langle y,\ 1,\ 0 \rangle,\ \langle y,\ 1,\ 1 \rangle \rangle$

Isomorphism between Shannon trees and Boolean functions

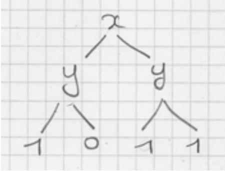
- A Shannon tree t over variables $x_1 <^v \ldots <^v x_n$ represents a Boolean function

$$\begin{array}{rcl} f(t)(x_1, \ldots, x_n) & = & \texttt{match } t \texttt{ with} \\ & & \| \; 0|1 \to t \text{ — case } n = 0 \\ & & \| \; \langle x_1,\, t_1,\, t_2 \rangle \to \quad (x_1 \wedge f(t_1)(x_2, \ldots, x_n)) \\ & & \qquad\qquad\quad \vee \; (\neg x_1 \wedge f(t_2)(x_2, \ldots, x_n)) \end{array}$$

- The Shannon tree representing a Boolean fonction $f(x_1, \ldots, x_n)$ with $x_1 <^v \ldots <^v x_n$ is:

$$\begin{array}{rcl} \mathtt{Sh}(f(x_1, \ldots, x_n)) & = & (n = 0 \mathrel{?} f() \mathrel{:} \\ & & \langle x_1,\, \mathtt{Sh}(\lambda x_2, \ldots, x_n \cdot f(0, x_2, \ldots, x_n)), \\ & & \quad \mathtt{Sh}(\lambda x_2, \ldots, x_n \cdot f(1, x_2, \ldots, x_n))\rangle) \end{array}$$

- Example



x	0	0	1	1
y	0	1	0	1
$f(x, y)$	1	0	1	1

$\langle x,\ \langle y,\ 1,\ 0\rangle,\ \langle y,\ 1,\ 1\rangle\rangle$

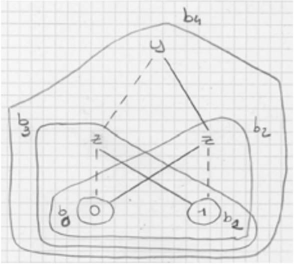
Definition of Boolean Decision Diagrams (BDD)

The BDDs are recursively defined as follows:

- 0 is a BDD
- 1 is a BDD
- if b_1, b_2 are BDDs, $x \in \mathsf{Var}$ is a variable then $b = \langle x,\ b_1,\ b_2\rangle$ is a BDD (with $\mathsf{var}(b) = x$, $\mathsf{left}(b) = b_1$, $\mathsf{right}(b) = b_2$)

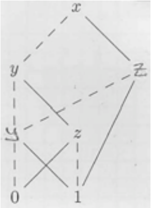
Example:

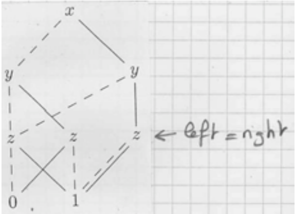
$$\begin{array}{rcl} b_0 & = & 0 \\ b_1 & = & 1 \\ b_2 & = & \langle z,\ b_1,\ b_0\rangle \\ b_3 & = & \langle z,\ b_0,\ b_1\rangle \\ b_4 & = & \langle y,\ b_3,\ b_2\rangle \\ & = & \langle y,\ \langle z,\ 0,\ 1\rangle,\ \langle z,\ 1,\ 0\rangle\rangle \end{array}$$



Ordered Boolean Decision Diagram (OBDD)

- Let $\langle \mathrm{Var}, <^v \rangle$ be a totally strictly ordered set of variables
- A BDD t is *ordered* ($\mathrm{ordered}(b) = \mathrm{tt}$) if and only if either $b \in \{0, 1\}$ or
  - If $\mathrm{left}(b) \notin \{0, 1\}$ then $\mathrm{var}(b) <^v \mathrm{var}(\mathrm{left}(b))$
  - If $\mathrm{right}(b) \notin \{0, 1\}$ then $\mathrm{var}(b) <^v \mathrm{var}(\mathrm{right}(b))$
  - $\mathrm{left}(b) \neq \mathrm{right}(b)$
- Counter-examples:





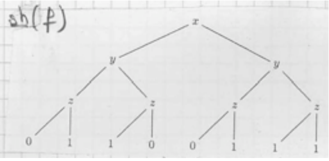
Representation of a Shannon tree by an Ordered Boolean Decision Diagram (OBDD)

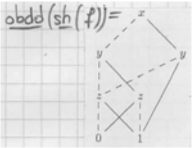
- The OBDD $\mathrm{obdd}(t)$ representing a Shannon tree t is defined as follows

$$
\begin{array}{l}
\mathrm{obdd}(t) = \mathbf{match}\ t\ \mathbf{with} \\
\qquad [\ 0|1 \rightarrow t \\
\qquad [\ \langle x,\ t_1,\ t_2 \rangle \rightarrow \\
\qquad\qquad (t_1 = t_2\ ?\ \mathrm{obdd}(t_1)\ ¿\ \langle x,\ \mathrm{obdd}(t_1),\ \mathrm{obdd}(t_2) \rangle)
\end{array}
$$

- Example:

x	0 0 0 0 1 1 1 1
y	0 0 1 1 0 0 1 1
z	0 1 0 1 0 1 0 1
f	0 1 1 0 0 1 1 1





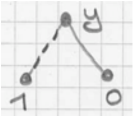
- Since the OBDD encoding of a Boolean function is unique, an implementation can share identical subtrees and test equality of OBDDs by the physical equality of the addresses of their implementations.

Boolean functions represented by an Ordered Boolean Decision Diagram (OBDD)

- An OBDD no longer represents one function of B but rather all functions whose results are the same regardless of the assignment of additional variables absent in the BDD
- Example: If $\forall x, y, z : f(x, y, z) = g(y)$ then

  $\mathrm{obdd}(\mathrm{sh}(f(x, y, z))) = \mathrm{obdd}(\mathrm{sh}(g(y)))$

  For example if $g(y) = \neg y$ then this OBDD is



- If this does not matter, then it is sufficient to memorize the OBDD as well as the corresponding set of variables ($\{x, y, z\}$ or $\{y\}$ in the above example).

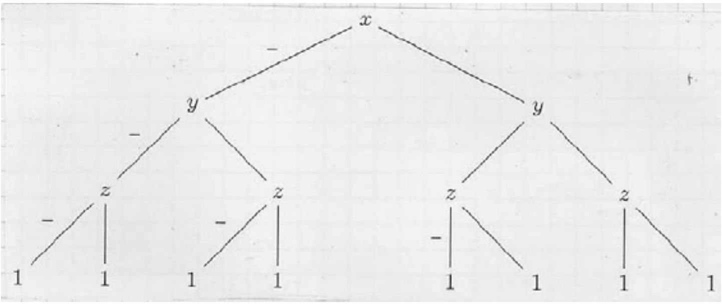
Typed Shannon tree

- The idea of *typed Shannon tree* [2] came from the remark that
$$\neg f = (\neg x \wedge \neg f_{\bar{x}}) \vee (\neg x \wedge \neg f_x)$$
so that the Shannon trees $\mathsf{Sh}(f)$ and $\mathsf{Sh}(\neg f)$ of f and $\neg f$ are identical except at the leaves where 0 and 1 are exchanged
- So one can use $+\mathsf{Sh}(f)$ for $\mathsf{Sh}(f)$ and $-\mathsf{Sh}(f)$ for $\mathsf{Sh}(\neg f)$ with $+1 = 1$ and $-1 = 0$

Reference

[2] S.B. Akers. Binary Decision Diagrams. *IEEE Transactions on computers*. 1978.

- Example (+ is omitted)



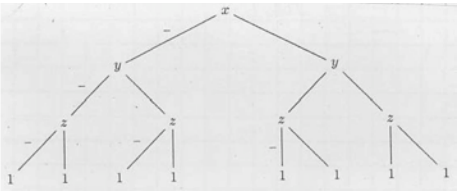
- Formally a *typed Shannon tree* t over $x_1 <^v \ldots <^v x_n$ is either
  - a leave 1 when $n = 0$, or
  - a node $\langle x, \langle s_1, t_1\rangle, \langle s_2, t_2\rangle\rangle$ where $s_1, s_2 \in \{+, -\}$ and t_1, t_2 are typed Shannon trees over $x_1 <^v \ldots <^v x_n$

Boolean functions represented by a Typed Shannon tree

- The Boolean function $\mathsf{bf}(t)$ represented by a typed Shannon tree t over $x_1 <^v \ldots <^v x_n$ is
-
```
bf(t) = match t with
[ 0|1 → $\lambda().t$ — case $n = 0$
[ $\langle x, \langle s_1, t_1\rangle, \langle s_2, t_2\rangle\rangle$ →
    let $f_1(x_2, \ldots, x_n)$ = bf($t_1$)
    and $f_2(x_2, \ldots, x_n)$ = bf($t_2$) in
      $\lambda x_1, \ldots, x_n \cdot\ (x_1 \wedge \mathsf{bo}(s_1)(f_1(x_2, \ldots, x_n)))$
                         $\vee\ (\neg x_1 \wedge \mathsf{bo}(s_2)(f_2(x_2, \ldots, x_n))$
```
where $\mathsf{bo}(+)(b) = b$ while $\mathsf{bo}(-)(b) = \neg b$

– Example:

$t =$



$\mathrm{f}(t) =$

x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
f	0	1	1	0	0	1	1	1

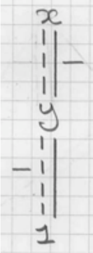
Typed Shannon trees representing a Boolean function

– Let $f(x_1, \ldots, x_n) \in B_n$ be a Boolean function over the variables $x_1 <^v \ldots <^v x_n$. The typed Shannon tree encoding f is:

$$
\begin{array}{l}
\mathsf{tsh}(f(x_1, \ldots, x_n)) \ = \\
\quad \llparenthesis\, n = 1 \mathrel{?} \langle x,\ \llparenthesis\, f(0) \mathrel{?} \langle +,\ 1\rangle \mathrel{:} \langle -,\ 1\rangle \rrparenthesis, \\
\qquad\qquad \llparenthesis\, f(1) \mathrel{?} \langle +,\ 1\rangle \mathrel{:} \langle -,\ 1\rangle \rrparenthesis \rangle \\
\quad \mathrel{:} \mathsf{let}\ \langle s_1,\ t_1\rangle = \llparenthesis\, f(0, 1, \ldots, 1) = 1 \mathrel{?} \\
\qquad\qquad\qquad \langle +,\ \mathsf{tsh}(\lambda x_2, \ldots, x_n \cdot f(0, x_2, \ldots, x_n))\rangle \\
\qquad\qquad\quad \mathrel{:} \ \langle -,\ \mathsf{tsh}(\lambda x_2, \ldots, x_n \cdot \neg f(0, x_2, \ldots, x_n))\rangle \\
\quad\ \mathsf{and}\ \langle s_2,\ t_2\rangle = \llparenthesis\, f(1, 1, \ldots, 1) = 1 \mathrel{?} \\
\qquad\qquad\qquad \langle +,\ \mathsf{tsh}\lambda x_2, \ldots, x_n \cdot (f(1, x_2, \ldots, x_n))\rangle \\
\qquad\qquad\quad \mathrel{:} \ \langle -,\ \mathsf{tsh}(\lambda x_2, \ldots, x_n \cdot \neg f(1, x_2, \ldots, x_n))\rangle \\
\quad \mathsf{in}\ \langle x_1,\ \langle s_1,\ t_1\rangle,\ \langle s_2,\ t_2\rangle\rangle \rrparenthesis
\end{array}
$$

– Examples:

- $\mathsf{tsh}(\lambda y \cdot (0 = \neg y)) = \langle y,\ \langle -,\ 1\rangle,\ \langle +,\ 1\rangle\rangle$
- $\mathsf{tsh}(\lambda y \cdot \neg(0 = \neg y)) = \langle y,\ \langle -,\ 1\rangle,\ \langle +,\ 1\rangle\rangle$
- $\mathsf{tsh}(\lambda x, y \cdot (x = \neg y)) =$
  $\langle x,\ \langle +,\ \langle y,\ \langle -,\ 1\rangle,\ \langle +,\ 1\rangle\rangle\rangle,\ \langle -,\ \langle y,\ \langle -,\ 1\rangle,\ \langle +,\ 1\rangle\rangle\rangle\rangle$
  which can be represented by the following TDG



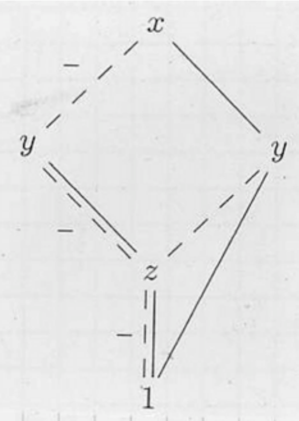
x	0	0	1	1
y	0	1	0	1
f(x,y)	0	1	1	0

Encoding of a Typed Shannon tree by a Typed Decision Graph (TDG)

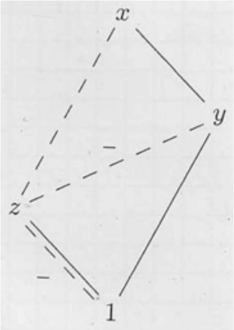
If t is a typed Shannon tree, the the corresponding TDG is obtained by applying the previous sharing and elimination rules:

$$
\begin{array}{l}
\mathsf{tdg}(t) = \llparenthesis\, t = \langle s,\ 1\rangle \mathrel{?} \langle s,\ 1\rangle \\
\qquad\qquad \mathrel{\|} t = \langle x,\ \langle s_1,\ t_1\rangle,\ \langle s_2,\ t_2\rangle\rangle \mathrel{?} \\
\qquad\qquad\quad \llparenthesis\, (s_1 = s_2 \wedge t_1 = t_2) \mathrel{?} \llparenthesis\, s_1 = + \mathrel{?} t_1 \mathrel{:} \neg t_1 \rrparenthesis \\
\qquad\qquad\quad \mathrel{:} \langle x,\ \langle s_1,\ \mathsf{tdg}(t_1)\rangle,\ \langle s_2,\ \mathsf{tdg}(t_2)\rangle\rangle \rrparenthesis \rrparenthesis
\end{array}
$$

– Example 1: $f(x, y, z) = (x \wedge y) \vee (y \wedge \neg z) \vee (z \wedge \neg y)$



– Example 2: $f(x, y, z) = (y \wedge x) \vee (x \wedge \neg z) \vee (z \wedge \neg x)$



The size of TDGs, although very sensitive to the variable order, is often reasonable but can be exponential in the number of variables.

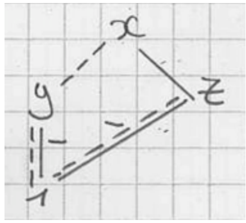
Boolean functions represented by a Typed Decision Graph (TDG)

The Boolean function $\mathsf{bf}(t)$ represented by a TDG t over variables $x_1, \ldots, x_n$ is

```
$\mathsf{bf}(t)(x_1, \ldots, x_n)$ = match $t$ with
  | $1 \rightarrow 1$
  | $\langle x,\ \langle s_1,\ t_1\rangle,\ \langle s_2,\ t_2\rangle\rangle \rightarrow$
      ($x = x_1$ ? let $f_1(x_2, \ldots, x_n) = \mathsf{bf}(t_1)(x_2, \ldots, x_n)$
                  and $f_2(x_2, \ldots, x_n) = \mathsf{bf}(t_2)(x_2, \ldots, x_n)$
                  in   $(x_1 \wedge \mathsf{bo}(s_1)(f_1(x_2, \ldots, x_n)))$
                     $\vee\ (\neg x_1 \wedge \mathsf{bo}(s_2)(f_2(x_2, \ldots, x_n)))$
  ¿ $\mathsf{bf}(t)(x_2, \ldots, x_n)$)
```

where $\mathsf{bo}(+)(b) = b$ and $\mathsf{bo}(-) = \neg b$, $b \in \{0, 1\}$

Example:



– $\mathsf{bf}(\langle y,\ \langle +,\ 1\rangle,\ \langle -,\ 1\rangle\rangle)(y, z)$
  $= (y \wedge \mathsf{bo}(+)(\mathsf{bf}(1)(z))) \vee$
  $(\neg y \wedge \mathsf{bo}(-)(\mathsf{bf}(1)(z)))$
  $= (y \wedge 1) \vee (\neg y \wedge \neg 1) = y$

– $\mathsf{bf}(\langle z,\ \langle -,\ 1\rangle,\ \langle +,\ 1\rangle\rangle)(y, z)$
  $= \mathsf{bf}(\langle z,\ \langle -,\ 1\rangle,\ \langle +,\ 1\rangle\rangle)(z)$
  $= (z \wedge \mathsf{bo}(-)(\mathsf{bf}(1)(z))) \vee (\neg z \wedge \mathsf{bo}(+)(\mathsf{bf}(1)(z)))$
  $= (z \wedge \neg 1) \vee (\neg z \wedge 1) = \neg z$

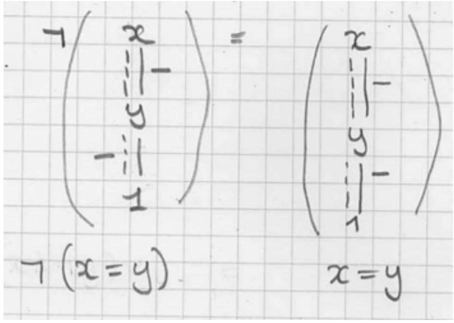
– $\mathsf{bf}(\langle x,\ \langle +,\ t_1\rangle,\ \langle +,\ t_2\rangle\rangle)(x, y, z)$ where $t_1 = \langle y,\ \langle +,\ 1\rangle,\ \langle -,\ 1\rangle\rangle$ and $t_2 = \langle z,\ \langle -,\ 1\rangle,\ \langle +,\ 1\rangle\rangle$
  $= ((x \wedge \mathsf{bo}(+)(\mathsf{bf}(t_1)(y, z))) \vee (\neg x \wedge \mathsf{bo}(+)(\mathsf{bf}(t_2)(y, z)))$
  $= ((x \wedge \mathsf{bf}(t_1)(y, z)) \vee (\neg x \wedge \mathsf{bf}(t_2)(y, z))$
  $= (x \wedge y) \vee (\neg x \vee \neg z)$

Operations on Typed Decision Graphs (TDG)

- Since the representation of a Boolean function by a TDG is unique , equality of Boolean functions can be represented by the equality (of the physical addresses) of the representations
- Negation just inverts the signs at the leaves

$$
\begin{array}{l}
-t(x_1,\ldots,x_n) \;=\; \textsf{match } t \textsf{ with} \qquad \textsf{— case } n \geq 1\\
\mid\ \langle x_1,\ \langle s_1,\ 1\rangle,\ \langle s_2,\ 1\rangle\rangle \rightarrow \langle x_1,\ \langle -s_1,\ 1\rangle,\ \langle -s_2,\ 1\rangle\rangle\\
\mid\ \langle x_1,\ \langle s_1,\ 1\rangle,\ \langle s_2,\ t_2\rangle\rangle \rightarrow \langle x_1,\ \langle -s_1,\ 1\rangle,\ \langle s_2,\ -t_2\rangle\rangle\\
\mid\ \langle x_1,\ \langle s_1,\ t_1\rangle,\ \langle s_2,\ 1\rangle\rangle \rightarrow \langle x_1,\ \langle s_1,\ -t_1\rangle,\ \langle -s_2,\ 1\rangle\rangle\\
\mid\ \langle x_1,\ \langle s_1,\ t_1\rangle,\ \langle s_2,\ t_2\rangle\rangle \rightarrow \langle x_1,\ \langle s_1,\ -t_1\rangle,\ \langle s_2,\ -t_2\rangle\rangle
\end{array}
$$

where $-(+) = -$ and $-(-) = +$

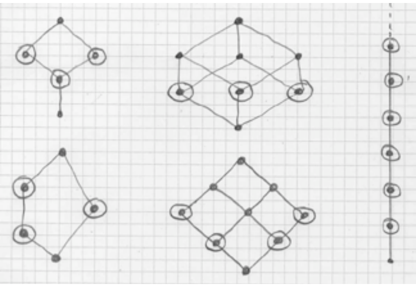


- Other operations use the Shannon decomposition (as well as memoization by a hash table to avoid identical recursive calls)

Encoding of complete join morphisms with join irreducibles

Join irreducible elements of a poset

- Let $\langle P, \leq\rangle$ be a poset. An element $x \in P$ is join irreducible iff
  1. x is not the infimum of P
  2. if $x = a \vee b$ then $x = a$ or $x = b$, for all $a, b \in P$
- Examples:



- Counter-examples:

  The lattice of open subsets of $\mathbb{R}$ (that is subsets which are unions of open intervals $]a, b[$) has no join-irreducible element.
- When the second condition is generalized to arbitrary joins $\bigvee_{i \in \Delta} a_i$, x is called completely join-irreducible
- In a lattice the second condition 2. is equivalence to:

  2'. $\forall a, b \in P : (x < a \wedge x < b) \Longrightarrow (a \vee b < x)$[6]
- The meet irreducible elements are defined dually
- We let $\mathcal{J}(P)$ and $\mathcal{M}(P)$ be the set of join-irreducible and meet-irreducible elements of P

[6] Assume x is join irreducible. We have $(x < a \wedge x < b) \Longrightarrow (a \vee b \leq x) \Longrightarrow (a \vee b < x) \vee (a \vee b = x)) \Longrightarrow (a \vee b < x)$ since $a \vee b = x$ implies $(x = a \vee x = b)$ since x is reducible in contradiction with $(x < a \wedge x < b)$. Reciprocally, if $(x = a \vee b)$ then $(x \geq a \wedge x \geq b)$. If $(x < a \wedge x < b) \Longrightarrow (a \vee b < x)$ is in contradiction with assumption $(x = a \vee b) \Longrightarrow (x = a \vee x = b)$. So either $(x = a)$ or $(x = b)$ holds.

Decomposition of elements of a lattice satisfying the descending chain condition (DCC) into join irreducibles

THEOREM. Let $\langle L, \leq, \vee \rangle$ be a lattice satisfying the DCC.

$$\forall a \in L : \bigvee \{x \in \mathcal{J}(L) \mid x \leq a\} = a$$

■

PROOF. (i) $\forall a, b \in L : (a \not\leq b) \Longrightarrow (\exists x \in \mathcal{J}(L) : x \leq a \wedge x \not\leq b$

Assume $a \not\leq b$. Let $S = \{x \in L \mid x \leq a \wedge x \not\leq b\}$. The set S is not empty since $a \in S$. Since L satisfies the DCC, there exists a minimal element x of S. This element is join-irreducible since $x = c \vee d$ with $c < x$ and $d < x$ implies, by the minimality of x that $c \notin S$ and $d \notin S$. We have $c < x \leq a$ so $c \leq a$ and similarly $d \leq a$. Therefore $c, d \notin S$ implies $c \leq b$ and $d \leq b$. But then $x = c \vee d \leq b$, a contradiction. Thus $x \in \mathcal{J}(L) \cap S$, which proves (i).

(ii) Let $a \in L$ and $T = \{x \in \mathcal{J}(L) \mid x \leq a\}$. a is an upper-bound of T. Let c be any upper bound of T. We have $a \leq c$ since otherwise $a \not\leq c$ implies $a \not\leq a \wedge c$. by (i) there exists $x \in \mathcal{J}(L)$ with $x \leq a$ and $a \not\leq a \wedge c$. Hence $x \in T$ and so $x \leq c$ since c is an upper-bound of T. Thus x is a lower bound of $\{a, c\}$ and consequently $x \leq a \wedge c$, a contradiction. Hence $a \leq c$ proving that $a = \bigvee T$ in L proving that $a = \forall a \in L : \bigvee \{x \in \mathcal{J}(L) \mid x \leq a\}$. □

Encoding of complete join morphisms on lattices satisfying the descending chain condition (DCC) by the image of join irreducibles

THEOREM. Let $\langle L, \leq, \vee \rangle$ be a lattice satisfying the DCC. Let $f \in L \overset{\sqcup}{\longmapsto} L$ be a complete join morphism. Define $g \overset{\text{def}}{=} f \upharpoonright \mathcal{J}(L)$, that is g coincide with f on join-irreducibles. Define $f'(a) = \bigvee \{g(x) \mid x \in \mathcal{J}(L) \wedge x \leq a\}$ Then $f' = f$. ■

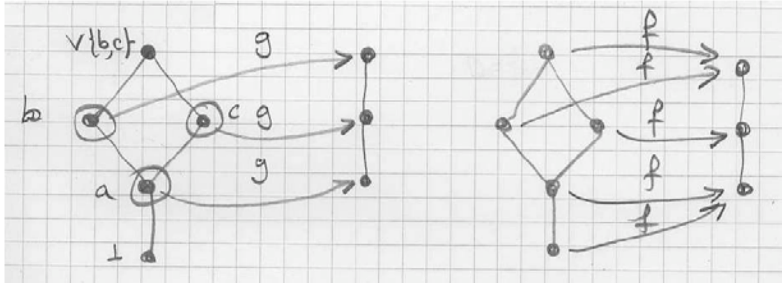
PROOF.

$$\begin{array}{ll} & f(a) \\ = & f(\bigvee \{x \in \mathcal{J}(L) \mid x \leq a\}) \qquad \langle L \text{ satisfies DCC} \rangle \end{array}$$

$$
\begin{aligned}
&= \bigvee\{f(x) \in \mathcal{J}(L) \mid x \le a\} && \wr\ f \in L \overset{\sqcup}{\longmapsto} L \wr \\
&= \bigvee\{g(x) \in \mathcal{J}(L) \mid x \le a\} && \wr \text{def. } g \wr \\
&= f'(a) && \wr \text{def. } f' \wr
\end{aligned}
$$

□

- Example:



Atoms

- Let $\langle P, \le, \perp\rangle$ be a poset with an infimum $\perp$. An atom of p is $a \in P$ such that $\perp \prec a$ in P (i.e. $\perp < a$ and $\nexists b \in P : \perp < b < a$).
- The set of atoms of $\langle P, \le, \perp\rangle$ is denoted $\mathcal{A}(P)$.

Atoms and join irreducibles in Boolean lattices

THEOREM. Let $\langle L, \le, \perp, \vee\rangle$ be a lattice with infimum $\perp$. Then

(i) $\perp \prec x \in L \Longrightarrow x \in \mathcal{J}(L)$

(ii) If L is a boolean lattice then $\mathcal{J}(L) \subseteq \mathcal{A}(L)$

■

PROOF.(i) Assume $\_ \prec x$ and $x = a \vee b$ with $a < x$ and $b < x$. Since $\_ \prec x$, we have $a = b = \_$ whence $x = \_$, a contradiction proving that $x \in \mathcal{J}(L)$.

(ii) Let L be a Boolean lattice and $x \in \mathcal{J}(L)$. Assume $\_ \le y < x$. We have:

$$
\begin{aligned}
x &= x \vee y \\
&= (x \vee y) \wedge (-y \vee y) \\
&= (x \wedge -y) \vee y
\end{aligned}
$$

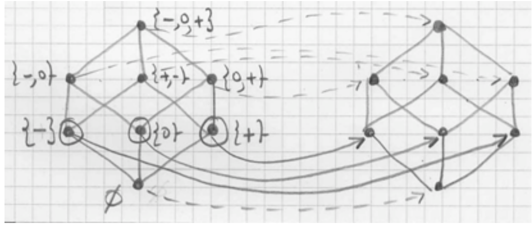
Since $x \in \mathcal{J}(L)$ and $y < x$, we must have $x = x \wedge -y$ whence $x \le -y$. But then $y = x \wedge y \le -y \wedge y = \_$ so $y = \_$. This proves $\_ \prec x$ so $x \in \mathcal{A}(L)$ whence $\mathcal{J}(L) \subseteq \mathcal{A}(L)$.

□

So in Boolean lattices it suffices to know complete join morphisms on the atoms.

Encoding of complete join morphisms on Boolean lattices satisfying the DCC by the image of atoms

- Atoms may no exist in infinite lattices (for example in $\langle \mathbb{R}^+, \leq \rangle$). However if they exist, they can replace join irreducible to encode complete join morphisms.
- Example:



THEOREM. Let $\langle L, \leq, \bot, \vee \rangle$ be a Boolean lattice satisfying the DCC. Let $f \in L \overset{\sqcup}{\longmapsto} L$ be a complete join morphism. Define $g \overset{\text{def}}{=} f \upharpoonright \mathcal{A}(L)$, that is g coincide with f on atoms. Then $f = \lambda a \cdot \bigvee \{ g(x) \mid x \in \mathcal{A}(L) \wedge x \leq a \}$. ■

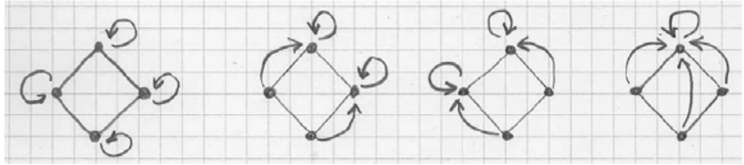
PROOF. Immediate consequence of the previous two theorems. □

Closure Operators

Kazimierz Kuratowski

Definition of an upper closure operator

- An operator on a set P is a map of P into P
- An upper closure operator ρ on a poset $\langle P, \leq \rangle$ is
  - extensive: $\forall x \in P : x \leq \rho(x)$
  - monotone: $\forall x, y \in P : (x \leq y) \Longrightarrow (\rho(x) \leq \rho(y))$
  - idempotent: $\rho(\rho(x)) = \rho(x)$
- Examples:



Definition of a lower closure operator

The dual notion is that of lower closure operator, which is

- reductive: $\forall x \in P : \rho(x) \leq x$
- monotone
- idempotent

Example of upper closure operator: reflexive transitive closure

- Let Σ be a set and $t \subseteq (\Sigma \times \Sigma)$ be a relation on Σ
  - $t^0 \stackrel{\text{def}}{=} 1_\Sigma$, $t^{n+1} \stackrel{\text{def}}{=} t^n \circ t = t \circ t^n$ $\circ$: composition of relations
  - $t^* \stackrel{\text{def}}{=} \bigcup_{n \in \mathbb{N}} t^n$ $t^+ \stackrel{\text{def}}{=} \bigcup_{n > 0} t^n$
- We have
  - $t \subseteq t^*$ extensive
  - $t \subseteq t' \Longrightarrow t^* \subseteq t'^*$ monotone
  - $(t^*)^*$ idempotent

  so that * is an upper closure operator on $\langle \wp(\Sigma \times \Sigma), \subseteq \rangle$.
- Same for t^+

Topological closure operator

- A topological closure operator[7] ρ on a poset $\langle P, \leq, \perp, \vee \rangle$ with infimum $\perp$ and lub $\vee$, if any, satisfies
  - strict: $\rho(\perp) = \perp$
  - extensive: $\forall x \in P : x \leq \rho(x)$
  - join morphism: $\forall x, y \in P : \rho(x \vee y) = (\rho(x) \vee \rho(y))$[8]
  - idempotent: $\rho(\rho(x)) = \rho(x)$

[7] This is the original definition given by K. Kuratowski on $\langle \wp(S), \subseteq \rangle$ to characterize a unique topology on S: Let ρ be a topological closure operator on S. Let $T = \{S \setminus A \mid A \subseteq S \wedge \rho(A) = A\}$. Then T is a topology on S and $\rho(A)$ is the T-closure of A for each subset A of S.

[8] This implies that ρ is monotonic.

Morgado Theorem (on upper closure operators)

THEOREM. An operator ρ on a poset $\langle P, \leq\rangle$ is an upper closure operator if and only if

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

■

PROOF. – Let ρ be an upper closure operator

$$
\begin{array}{ll}
\quad x \leq \rho(y) & \\
\Longrightarrow \rho(x) \leq \rho(\rho(y)) & \wr\text{monotony}\wr \\
\Longrightarrow \rho(x) \leq \rho(y) & \wr\text{idempotence}\wr \\
\Longrightarrow x \leq \rho(x) \leq \rho(y) & \wr\text{extensive}\wr \\
\Longrightarrow x \leq \rho(y) & \wr\text{transitivity}\wr
\end{array}
$$

– Conversely, let ρ satisfying the above condition.

$$
\begin{array}{ll}
- \quad \forall x : \rho(x) \leq \rho(x) & \\
\Longrightarrow x \leq \rho(x) & \wr\rho \text{ is extensive}\wr \\
- \quad x \leq y & \\
\Longrightarrow x \leq y \leq \rho(y) & \wr\text{proving that } \rho \text{ is extensive}\wr \\
\Longrightarrow \rho(x) \leq \rho(y) & \wr\text{proving } \rho \text{ to be monotone}\wr \\
- \quad x \leq \rho(x) & \wr\rho \text{ is extensive}\wr \\
\Longrightarrow \rho(x) \leq \rho(\rho(x)) & \wr\text{by above condition with } y = \rho(x)\wr \\
\quad\ \rho(x) \leq \rho(x) & \wr\leq \text{ is reflexive}\wr \\
\Longrightarrow \rho(\rho(x)) \leq \rho(x) & \wr\text{by above condition with } x' = \rho(x) \text{ and } y' = x\wr \\
\Longrightarrow \rho(x) = \rho(\rho(x)) & \wr\text{by antisymmetry}\wr
\end{array}
$$

□

Fixpoints of a closure operator

The set of fixpoints of an operator $f \in P \mapsto P$ on a set P is $\{x \mid f(x) = x\}$.

THEOREM. A closure operator is uniquely defined by its fixpoints ■

PROOF. Let ρ_1 and ρ_2 be two upper closure operators on a poset $\langle P, \leq\rangle$ with identical fixpoints:

$$\forall x \in P : \rho_1(x) = x \iff \rho_2(x) = x$$

We prove that $\rho_1 = \rho_2$.

- $\forall z \in P : z \leq \rho_1(z)$ so $\rho_2(z) \leq \rho_2(\rho_1(z))$ by extensivity of ρ_1 and monotony of ρ_2
- $\rho_1(\rho_1(z)) = \rho_1(z)$ by idempotence so $\rho_2(\rho_1(z)) = \rho_1(z)$ since ρ_1 and ρ_2 have the same fixpoints.
- It follows that $\rho_2(z) \leq \rho_2(\rho_1(z)) = \rho_1(z)$

- Exchanging the rôles of ρ_1 and ρ_2, we get $\rho_1(z) \leq \rho_2(z)$ in the same way.
- By antisymmetry, we conclude that $\rho_1(z) = \rho_2(z)$
- By duality, a lower closure operator is uniquely determined by its fixpoints.

□

Galois Connections

Evarist Galois

Definition of a Galois connection

- Let $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$ be posets. A pair $\langle\alpha, \gamma\rangle$ of maps $\alpha \in P \mapsto Q$ and $\gamma \in Q \mapsto P$ is a Galois connection if and only if

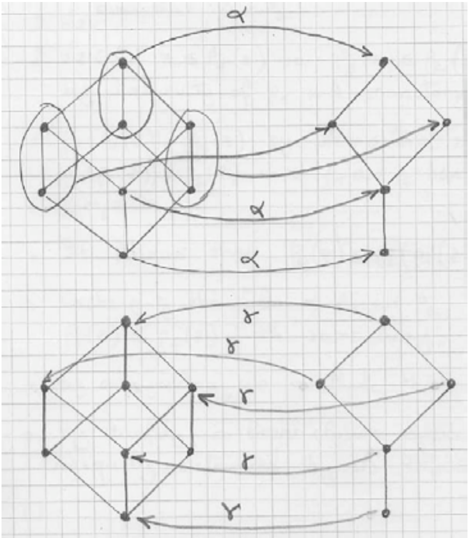
$$\forall x \in P : \forall y \in Q : \alpha(x) \sqsubseteq y \iff x \leq \gamma(y)$$

which is written:

$$\langle P, \leq\rangle \xleftarrow[\alpha]{\gamma} \langle Q, \sqsubseteq\rangle$$

- α is the lower adjoint
- γ is the upper adjoint

- Example:



Example of Galois connection: bijection

Let P and Q be two sets and $b \in P \rightarrowtail\!\!\!\!\twoheadrightarrow Q$ be a one-to-one map of p onto q with inverse b^{-1}. Then

$$\langle P,\ =\rangle \underset{b}{\overset{b^{-1}}{\leftrightarrows}} \langle Q,\ =\rangle$$

(where $\langle P,\ =\rangle$ is P ordered by equality)

Proof.

$$\begin{array}{ll} & b(x) = y \\ \Longleftrightarrow & x = b^{-1} \end{array} \qquad \text{⦃by def. bijection⦄}$$

$\square$

Example of Galois connection: functional abstraction

Let C and A be sets an $f \in C \mapsto A$. Define

$$\alpha(X) \stackrel{\text{def}}{=} \{f(x) \mid x \in X\}$$
$$\gamma(Y) \stackrel{\text{def}}{=} \{x \mid f(x) \in Y\}$$

then

$$\langle \wp(C),\ \subseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \wp(A),\ \subseteq\rangle$$

Proof.

$$\begin{array}{lll} & \alpha(X) \subseteq Y & \\ \Longleftrightarrow & \{f(x) \mid x \in X\} \subseteq Y & \text{⦃def. } \alpha\text{⦄} \\ \Longleftrightarrow & \forall x \in X : f(x) \in Y & \text{⦃def. } \subseteq\text{⦄} \\ \Longleftrightarrow & X \subseteq \{x \mid f(x) \in Y\} & \text{⦃def. } \subseteq\text{⦄} \\ \Longleftrightarrow & X \subseteq \gamma(Y) & \text{⦃def. } \gamma\text{⦄} \end{array}$$

$\square$

– Example:
  - $C = \mathbb{Z},\ A = \{-1, 0, +1\}$
  - $f(x) = (x < 0\ ?\ -1 \parallel x = 0\ ?\ 0 : +1)$
  - $\alpha(\{0, 1, 2\}) = \{0, +1\}$
  - $\gamma(\{0, +1\}) = \{x \in \mathbb{Z} \mid x \geq 0\} = \mathbb{N}$

Example of Galois connections with Pre and Post

Recall that given a set Σ and $t \subseteq \Sigma \times \Sigma$, we have defined

$$\begin{array}{rcl} \mathrm{post}[t]X & \stackrel{\text{def}}{=} & \{x' \mid \exists x \in X : \langle x,\ x'\rangle \in t\} \\ \mathrm{pre}[t]X & \stackrel{\text{def}}{=} & \mathrm{post}[t^{-1}]X \\ & = & \{x \mid \exists x' \in X : \langle x,\ x'\rangle \in t\} \\ \widetilde{\mathrm{post}}[t]X & \stackrel{\text{def}}{=} & \neg\mathrm{post}[t](\neg X) \\ & = & \{x' \mid \forall x : \langle x,\ x'\rangle \in t \Longrightarrow x \in X\} \\ \widetilde{\mathrm{pre}}[t]X & \stackrel{\text{def}}{=} & \neg\mathrm{pre}[t](\neg X) \\ & = & \{x \mid \forall x' : \langle x,\ x'\rangle \in t \Longrightarrow x' \in X\} \end{array}$$

We have

$$\langle \wp(\Sigma),\ \subseteq\rangle \underset{\text{post}[t]}{\overset{\widetilde{\text{pre}}[t]}{\leftrightarrows}} \langle \wp(\Sigma),\ \subseteq\rangle$$

By letting $t' = t^{-1}$, we get in the same way

$$\langle \wp(\Sigma),\ \subseteq\rangle \underset{\text{pre}[t]}{\overset{\widetilde{\text{post}}[t]}{\leftrightarrows}} \langle \wp(\Sigma),\ \subseteq\rangle$$

PROOF.

$$\begin{array}{ll}
\quad \text{post}[t]X \subseteq Y & \\
\Longleftrightarrow \{x' \mid \exists x \in X : \langle x,\ x'\rangle \in t\} \subseteq & \lbag \text{def. post} \rbag \\
\Longleftrightarrow \forall x' : (\exists x \in X : \langle x,\ x'\rangle \in t) \Longrightarrow (x' \in Y) & \lbag \text{def.} \subseteq \rbag \\
\Longleftrightarrow \forall x, x' : (x \in X : \langle x,\ x'\rangle \in t) \Longrightarrow (x' \in Y) & \lbag \text{def.} \Longrightarrow \rbag \\
\Longleftrightarrow \forall x : (x \in X) \Longrightarrow (\forall x' : \langle x,\ x'\rangle \in t \Longrightarrow x' \in Y) & \lbag \text{def.} \Longrightarrow \rbag \\
\Longleftrightarrow X \subseteq \{x \mid \forall x' : \langle x,\ x'\rangle \in t \Longrightarrow x' \in X\} & \lbag \text{def.} \subseteq \rbag \\
\Longleftrightarrow X \subseteq \widetilde{\text{pre}}[t]X & \lbag \text{def. } \widetilde{\text{pre}} \rbag
\end{array}$$

□

Example of Galois connections induced by upper closure operators

Recall Morgado's theorem for an upper closure operator on a poset $\langle P,\ \leq\rangle$

$$\forall x, y \in P : x \leq \rho(y) \quad \Longleftrightarrow \quad \rho(x) \leq \rho(y)$$

Let $\rho(P) = \{\rho(x) \mid x \in P\}$. This can be written as follows (with $z = \rho(y)$)

$$\forall x \in P : \forall z \in \rho(P) : x \leq 1_P(z) \quad \Longleftrightarrow \quad \rho(x) \leq z$$

which by definition of a Galois connection implies that

$$\langle P,\ \leq\rangle \underset{\rho}{\overset{1_P}{\leftrightarrows}} \langle \rho(P),\ \leq\rangle$$

Reciprocally, this implies that

$$\forall x \in P : \forall z \in \rho(P) : \rho(x) \leq z \quad \Longleftrightarrow \quad x \leq 1_P(z)$$

$$\Longrightarrow \forall x \in P : \forall y \in P : \rho(x) \leq \rho(y) \quad \Longleftrightarrow \quad x \leq \rho(y)$$

$$\lbag z = \rho(y) \rbag$$

so that

THEOREM. ρ is an upper closure of $\langle P,\ \leq\rangle$ if and only if

$$\langle P,\ \leq\rangle \underset{\rho}{\overset{1_P}{\leftrightarrows}} \langle \rho(P),\ \leq\rangle$$

■

Unique adjoints

THEOREM. In a Galois connection

$$\langle P,\ \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle$$

one adjoint uniquely determines the other, in that

$$\alpha(x) = \bigsqcap\{y \mid x \leq \gamma(y)\} \qquad \gamma(y) = \bigvee\{x \mid \alpha(x) \sqsubseteq y\}$$

■

PROOF. – The set $\{y \mid \alpha(x) \sqsubseteq y\}$ has a glb which is precisely $\alpha(x)$ so $\alpha(x) = \bigsqcap\{y \mid \alpha(x) \sqsubseteq y\} = \bigsqcap\{y \mid x \leq \gamma(y)\}$ since $\alpha(x) \sqsubseteq y \iff x \leq \gamma(y)$.

– The set $\{x \mid x \leq \gamma(y)\}$ has a lub which is precisely $\gamma(y)$ so $\gamma(y) = \bigvee\{x \mid x \leq \gamma(y)\} = \bigvee\{x \mid \alpha(x) \sqsubseteq y\}$ since $\alpha(x) \sqsubseteq y \iff x \leq \gamma(y)$.

□

Characteristic property of Galois connections

– Let $\langle P,\ \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle$ then

- α is monotone
- γ is monotone
- $1_P \dot{\leq} \gamma \circ \alpha$
- $\alpha \circ \gamma \dot{\sqsubseteq} 1_Q$

PROOF. - $\alpha(x) \sqsubseteq \alpha(y) \Longrightarrow x \leq \gamma \circ \alpha(x)$

- $\gamma(x) \leq \gamma(y) \Longrightarrow \alpha \circ \gamma(y) \sqsubseteq y$
- $x \leq y \Longrightarrow x \leq \gamma \circ \alpha(x) \Longrightarrow \alpha(x) \sqsubseteq \alpha(y)$
- $x \sqsubseteq y \Longrightarrow \alpha(\gamma(x)) \sqsubseteq y \Longrightarrow \gamma(x) \leq \gamma(y)$

□

– $\alpha \circ \gamma \circ \alpha = \alpha$ and $\gamma \circ \alpha \circ \gamma = \gamma$

PROOF. - $\alpha \circ \gamma(x) \sqsubseteq x$ so $\alpha \circ \gamma \circ (y) \sqsubseteq \alpha(y)$ when $x = \alpha(y)$. $1_P \dot{\sqsubseteq} \gamma \circ \alpha$ so $\alpha \dot{\sqsubseteq} \alpha \circ \gamma \circ \alpha$ by monotony, concluding $\alpha \circ \gamma \circ \alpha = \alpha$ by antisymmetry.

- $x \leq \gamma \circ \alpha(x)$ so $\gamma(y) \leq \gamma \circ \alpha \circ \gamma(y)$ for $x = \gamma(y)$ so $\alpha \circ \gamma(y) \sqsubseteq y$ so $\gamma \circ \alpha \circ \gamma(y) \sqsubseteq \gamma(y)$ by monotony, concluding $\gamma \circ \alpha \circ \gamma = \gamma$ by antisymmetry.

□

– $\alpha \circ \gamma$ is a lower closure operator on $\langle P,\ \leq\rangle$

– $\gamma \circ \alpha$ is a upper closure operator on $\langle Q,\ \sqsubseteq\rangle$

Equivalent definition of a Galois connection

THEOREM.

$$\begin{aligned} &\langle P,\ \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle \\ \iff\ &\alpha \text{ is monotone} \wedge \gamma \text{ is monotone} \wedge \\ &\alpha \circ \gamma \text{ is reductive} \wedge \gamma \circ \alpha \text{ is extensive} \end{aligned}$$

■

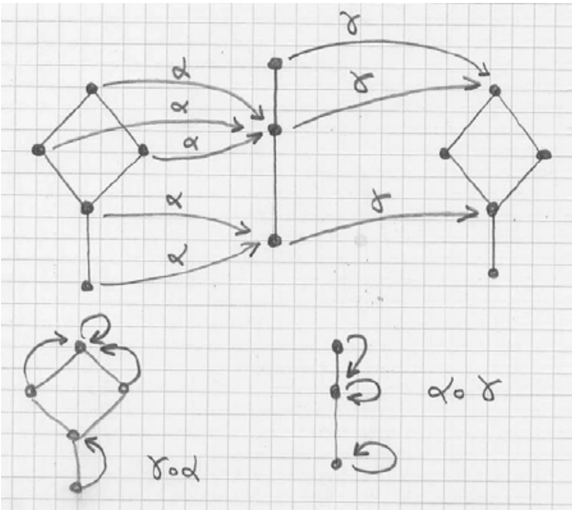
PROOF. – We have already proved $\Longrightarrow$

– Reciprocally, for all $x \in P$ and $y \in Q$

$$\begin{array}{ll}
\quad \alpha(x) \sqsubseteq y & \\
\Longrightarrow \gamma \circ \alpha(x) \leq \gamma(y) & \wr \gamma \text{ monotone} \wr \\
\Longrightarrow x \leq \gamma(y) & \wr \gamma \circ \alpha \text{ is extensive and transitivity} \wr \\
\Longrightarrow \alpha(x) \sqsubseteq \alpha \circ \gamma(y) & \wr \alpha \text{ is monotone} \wr \\
\Longrightarrow \alpha(x) \sqsubseteq y & \wr \alpha \circ \gamma \text{ is reductive and transitivity} \wr
\end{array}$$

□

Example:



The upper adjoint of a Galois connection preserves existing lubs

THEOREM. Let $\langle P, \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q, \sqsubseteq\rangle$ be a Galois connection and $X \subseteq P$ such that its lub $\bigvee X$ does exists in P. Then $\alpha(\bigvee X)$ is the lub of $\{\alpha(x) \mid x \in X\}$ in Q, that is $\alpha(\bigvee X) = \bigsqcup \alpha(X)$. ■

PROOF. – $\forall x \in X : x \leq \bigvee X$ by existence of the lub $\bigvee X$ so $\forall x \in X : \alpha(x) \sqsubseteq \alpha(\bigvee X)$ by monotony of α proving that $\alpha(\bigvee X)$ is an upper bound of the set $\{\alpha(x) \mid x \in X\}$ in Q.

– Let y be another upper bound of $\{\alpha(x) \mid x \in X\}$ in Q.

$$\forall x \in X : \alpha(x) \sqsubseteq y \qquad \text{(def. upper bound)}$$
$$\Longrightarrow \forall x \in X : x \leq \gamma(y) \qquad \text{(def. Galois connection)}$$

$$\Longrightarrow \bigvee X \leq \gamma(y) \qquad \text{(def. lub)}$$
$$\Longrightarrow \alpha(\bigvee X) \sqsubseteq y \qquad \text{(def. Galois connection)}$$

proving that $\alpha(\bigvee X)$ is the least of the upper bounds of $\{\alpha(x) \mid x \in X\}$.

– If we write $\bigsqcup Y$ for the lub of $Y \subseteq Q$ in $\langle Q, \sqsubseteq\rangle$ whenever it exists, then we have proved that α preserves existing lubs, in that $(\alpha(X) = \{\alpha(x) \mid x \in X\})$

> If $\bigvee X$ exists in $\langle P, \leq\rangle$ then $\bigsqcup \alpha(X)$ does exists in $\langle Q, \sqsubseteq\rangle$ and $\alpha(\bigvee X) = \bigsqcup \alpha(X)$.

□

Galois connection induced by lub preserving maps

THEOREM. Let $\alpha \in P \overset{\sqcup}{\longmapsto} Q$ be a complete join preserving map between posets $\langle P, \leq\rangle$ and $\langle Q, \sqsubseteq\rangle$. Define:

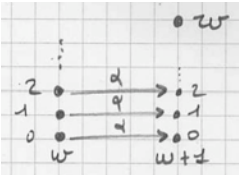
$$\gamma = \lambda y \cdot \bigvee \{z \mid \alpha(z) \sqsubseteq y\}$$

If γ is well-defined then

$$\langle P, \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q, \sqsubseteq\rangle$$

■

PROOF. – Assume that for all $y \in Q$, $\bigvee\{z \mid \alpha(z) \sqsubseteq y\}$ does exist. A counter-example is



α is the identity on $P = \omega$. Then $\omega \in \omega + 1 = Q$. $\{z \mid \alpha(z) \sqsubseteq \omega\} = \omega$ but $\bigvee\{z \mid \alpha(z) \sqsubseteq y\} = \bigvee\{0, 1, 2, \ldots\}$ does not exist in ω!

– The proof that $\langle\alpha,\, \gamma\rangle$ is a Galois connection proceeds as follows:

$$\begin{aligned}
& \alpha(x) \sqsubseteq y \\
\Longrightarrow\ & x \in \{z \mid \alpha(z) \sqsubseteq y\} \\
\Longrightarrow\ & x \leq \bigvee\{z \mid \alpha(z) \sqsubseteq y\} && \text{⟅lub assumed to exsist!⟆} \\
\Longrightarrow\ & x \leq \gamma(y) \\
\Longrightarrow\ & \alpha(x) \sqsubseteq \alpha(\bigvee\{z \mid \alpha(z) \sqsubseteq y\}) && \text{⟅def. } \gamma \text{ and } \alpha \text{ monotone⟆} \\
\Longrightarrow\ & \alpha(x) \sqsubseteq \bigsqcup\{\alpha(z) \mid \alpha(z) \sqsubseteq y\} && \text{⟅}\alpha \text{ preserves existing lubs⟆} \\
\Longrightarrow\ & \alpha(x) \sqsubseteq y && \text{⟅def. lub⟆}
\end{aligned}$$

□

Similarly[9], if γ preserves glbs and $\alpha = \lambda x \cdot \bigsqcap\{y \mid x \leq \gamma(y)\}$ is well-defined then $\langle P,\, \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\, \sqsubseteq\rangle$.

[9] More precisely, by duality, see later on page 131.

Duality principle for Galois connections

THEOREM. We have $\langle P,\, \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\, \sqsubseteq\rangle$
iff $\langle Q,\, \sqsupseteq\rangle \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} \langle P,\, \geq\rangle$
whence the dual of a Galois connection $\langle\alpha,\, \gamma\rangle$ is $\langle\gamma,\, \alpha\rangle$ (exchange of adjoints). ■

PROOF.

$$\begin{aligned}
& \langle P,\, \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\, \sqsubseteq\rangle \\
\overset{\text{def}}{=}\ & \forall x \in P : \forall y \in Q : \alpha(x) \sqsubseteq y \iff x \leq \gamma(y) \\
\iff\ & \forall y \in Q : \forall x \in P : \gamma(y) \geq x \iff y \sqsupseteq \alpha(x) \\
\overset{\text{def}}{=}\ & \langle Q,\, \sqsupseteq\rangle \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} \langle P,\, \geq\rangle
\end{aligned}$$

□

Examples:

- The dual of "α preserves existing lubs" is "γ preserves existing glbs"
- The dual of $\alpha(x) = \bigsqcap\{y \mid x \leq \gamma(y)\}$ is $\gamma(y) = \bigvee\{y \mid x \sqsupseteq \alpha(y)\}$ that is $\gamma(y) = \bigvee\{x \mid \alpha(x) \sqsubseteq y\}$
- The dual of $\alpha \circ \gamma \circ \alpha = \alpha$ is $\gamma \circ \alpha \circ \gamma = \gamma$

Composition of Galois connections

THEOREM. The composition of Galois connections is a Galois connection: if

$$\langle P,\ \leq\rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle \text{ and } \langle Q,\ \sqsubseteq\rangle \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \langle R,\ \preceq\rangle$$

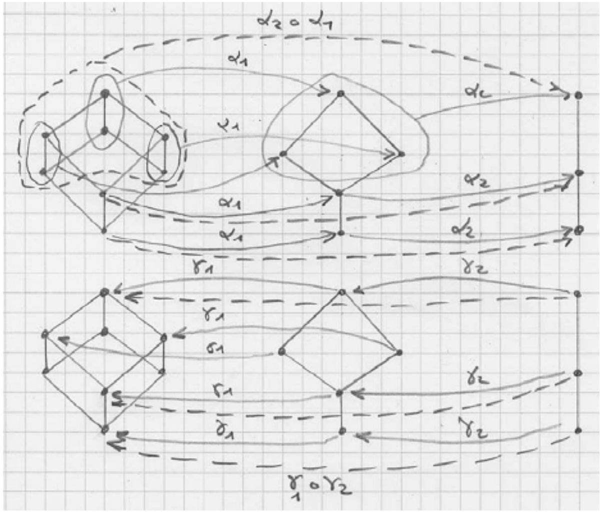
then $\langle P,\ \leq\rangle \underset{\alpha_2\circ\alpha_1}{\overset{\gamma_1\circ\gamma_2}{\leftrightarrows}} \langle R,\ \preceq\rangle$ ■

PROOF. Assume $\langle P,\ \leq\rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle$ and $\langle Q,\ \sqsubseteq\rangle \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \langle R,\ \preceq\rangle$ then $\forall x \in P : \forall z \in R$:

$$\begin{aligned} & \alpha_2 \circ \alpha_1(x) \preceq z \\ \Longleftrightarrow\ & \alpha_1(x) \sqsubseteq \gamma_2(z) \\ \Longleftrightarrow\ & x \leq \gamma_1 \circ \gamma_2(z) \end{aligned}$$

□

– Example:



The original Galois correspondances do not compose

– A Galois correspondence, as originally defined by Galois [10], is a pair $\langle\alpha,\ \gamma\rangle$ of functions on posets (originally powersets with the subset ordering, such that

$$\langle P,\ \leq\rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle Q,\ \sqsupseteq\rangle.$$

[10] Évariste Galois introduced such "correspondences" as the basis of his criterion for solvability of a polynomial equation of degree ≥ 5 by radicals and for the constructibility by straight-edge and compass. If E is a given field then let $\mathrm{Inv}\ G \stackrel{\mathrm{def}}{=} \{a \in E \mid \forall \eta \in G : \eta(a) = a\}$ for a group G of automorphisms in E. The *Galois group* Gal E/F of E over a subfield F is the set of automorphisms η of E such that $\eta(a) = a$ for every $a \in F$. The maps $\alpha(F) = \mathrm{Gal}\ E/F$ and $\gamma(F) = \mathrm{Gal}\ E/F$ are such that:

$$\begin{array}{ll} (F_1 \subseteq F_2) \Rightarrow (\alpha(F_1) \supseteq \alpha(F_2)) & (G_1 \supseteq G_2) \Rightarrow (\gamma(G_1) \subseteq \gamma(G_2)) \\ F \subseteq \gamma(\alpha(F)) & \alpha(\gamma(G)) \supseteq G \end{array}$$

– So α is antitone: $x \leq y \Longrightarrow \alpha(x) \sqsupseteq \alpha(y)$

– Hence when composing $\alpha_2 \circ \alpha_1$ is monotonic, hence not a Galois correspondance

– This justifies the introduction of Galois connections in [3] (by taking semi-dual Galois correspondances).

Reference

[3] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In \emphConference Record of the Sixth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, pages 269–282, San Antonio, Texas, 1979. ACM Press, New York, U.S.A.

Galois surjections (insertions)

THEOREM. If $\langle P,\ \leq\rangle \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle$ then

α is onto

$\Longleftrightarrow$ γ is one-to-one

$\Longleftrightarrow$ $\alpha \circ \gamma = 1_Q$

■

PROOF. – Assume that α is onto $(\forall y \in Q : \exists x \in P : \alpha(x) = y)$

– Assume $\gamma(x) = \gamma(y)$. $\exists x', y' \in P : \alpha(x') = y$ and $\alpha(y') = y$, and so

$$\gamma(\alpha(x')) = \gamma(\alpha(y'))$$

$\Longrightarrow x' \leq \gamma(\alpha(y'))$ $\qquad\qquad$ $\wr$since $x' \leq \gamma \circ \alpha(x')\int$

$\Longrightarrow \alpha(x) \sqsubseteq \alpha(y')$ $\qquad\qquad$ $\wr$by def. Galois connection$\int$

$\Longrightarrow x \sqsubseteq y$

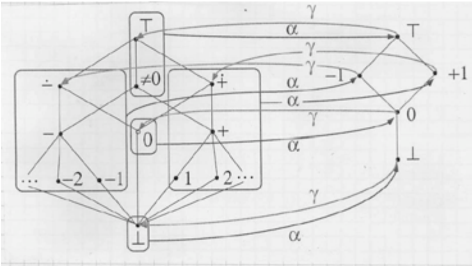
Exchanging the rôles of x and y, we get $y \sqsubseteq x$ so $x = y$ by antisymmetry, proving that $x \neq y \Longrightarrow \gamma(x) \neq \gamma(y)$, by composition.

– $\alpha \circ \gamma(y) = \alpha \circ \gamma \circ \alpha(y')$ where $\alpha(y') = y$. So $\alpha \circ \gamma(y) = \alpha(y') = y$ so $\alpha \circ \gamma = 1_Q$

– Assume $\alpha \circ \gamma = 1_Q$. Then given $y \in Q$, we have $\alpha \circ \gamma(y) = y$ proving that $\exists x = \gamma(y) : \alpha(x) = y$, α is onto.

□

Example of Galois surjection:



Galois injections

THEOREM. By duality, if $\langle P,\ \leq\rangle \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle$ then

γ is onto

$\Longleftrightarrow$ α is one-to-one

$\Longleftrightarrow$ $\gamma \circ \alpha = 1_P$

■

Notations:

– $\langle P,\ \leq\rangle \overset{\gamma}{\underset{\alpha}{\substack{\longleftarrow \\ \twoheadrightarrow}}} \langle Q,\ \sqsubseteq\rangle \overset{\text{def}}{=} \langle P,\ \leq\rangle \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle \wedge \alpha$ is onto

– $\langle P,\ \leq\rangle \overset{\gamma}{\underset{\alpha}{\substack{\twoheadleftarrow \\ \longrightarrow}}} \langle Q,\ \sqsubseteq\rangle \overset{\text{def}}{=} \langle P,\ \leq\rangle \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle \wedge \alpha$ is one-to-one

– $\langle P,\ \leq\rangle \overset{\gamma}{\underset{\alpha}{\substack{\twoheadleftarrow \\ \twoheadrightarrow}}} \langle Q,\ \sqsubseteq\rangle \overset{\text{def}}{=} \langle P,\ \leq\rangle \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle \wedge \alpha$ is bijective

Conjugate Galois connections in a Boolean algebra

THEOREM. Let $\langle P,\ \le,\ 0,\ 1,\ \vee,\ \wedge,\ \neg\rangle$ and $\langle Q,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap,\ \neg\rangle$ be Boolean algebras and the Galois connection

$$\langle P,\ \le\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle$$

Define the *conjugates*[11] $\tilde{\alpha} = \neg\alpha(\neg x)$ and $\tilde{\gamma} = \neg\gamma(\neg x)$. Then

$$\langle P,\ \ge\rangle \underset{\tilde{\alpha}}{\overset{\tilde{\gamma}}{\leftrightarrows}} \langle Q,\ \sqsupseteq\rangle$$

■

PROOF.

$$\tilde{\alpha}(a) \sqsupseteq y$$

[11] This is also called the *dual*, but this may cause confusion with lattice duality.

$$\begin{aligned}
&\iff -\alpha(-x) \sqsupseteq y && \text{\{def. } \tilde{\alpha}\text{\}}\\
&\iff \alpha(-x) \sqsubseteq -y &&\\
&\iff -x \le \gamma(-x) && \text{\{Galois connection\}}\\
&\iff x \ge -\gamma(-x) && \text{\{\}}\\
&\iff x \ge \tilde{\gamma}(y) && \text{\{def. } \tilde{\gamma}\text{\}}
\end{aligned}$$

□

THEOREM. It follows that $\langle Q,\ \sqsubseteq\rangle \underset{\tilde{\gamma}}{\overset{\tilde{\alpha}}{\leftrightarrows}} \langle P,\ \le\rangle$ ■

PROOF.

$$\begin{aligned}
&\tilde{\gamma}(y) \le x\\
\iff\ & y \sqsubseteq \tilde{\alpha}(x)
\end{aligned}$$

□

Example of dual Galois connections in a Boolean algebra: Pre, Post and their duals

We have

$$\langle \wp(\Sigma),\ \subseteq\rangle \underset{\mathrm{post}[t]}{\overset{\widetilde{\mathrm{pre}}[t]}{\leftrightarrows}} \langle \wp(\Sigma),\ \subseteq\rangle$$

By conjugate/complement duality, we get

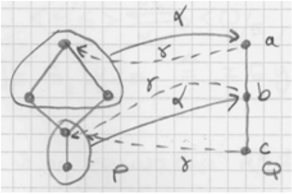
$$\langle \wp(\Sigma),\ \supseteq\rangle \underset{\widetilde{\mathrm{post}}[t]}{\overset{\mathrm{pre}[t]}{\leftrightarrows}} \langle \wp(\Sigma),\ \supseteq\rangle$$

since $\widetilde{\widetilde{\mathrm{pre}}} = \mathrm{pre}$, hence by order duality

$$\langle \wp(\Sigma),\ \subseteq\rangle \underset{\mathrm{pre}[t]}{\overset{\widetilde{\mathrm{post}}[t]}{\leftrightarrows}} \langle \wp(\Sigma),\ \subseteq\rangle$$

Example of reduction of a Galois connection

- Assume a Galois connection is not a surjection, for example:

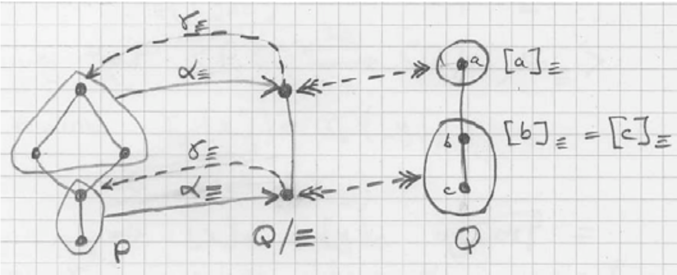


$$\langle P,\ \le\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle$$

- It is always possible to reduce Q by identifying elements with the same γ-image

$$x \equiv y \overset{\mathrm{def}}{=} \gamma(x) = \gamma(y)$$

and to reduce Q to the quotient $Q/_{\equiv}$, in which case α becomes surjective:



$$\alpha_{\equiv}(x) = [\alpha(x)]_{\equiv}$$
$$\gamma_{\equiv}([y]_{\equiv}) = \gamma(y)$$
$$[x]_{\equiv} \sqsubseteq_{\equiv} [y]_{\equiv} \stackrel{\text{def}}{=} x \sqsubseteq y \text{ on } Q/_{\equiv}$$

Reduction of a Galois connection

THEOREM. If $\langle P, \leq\rangle \xleftrightarrow[\alpha]{\gamma} \langle Q, \sqsubseteq\rangle$, $x \equiv y \stackrel{\text{def}}{=} \gamma(x) = \gamma(y)$, $\alpha_{\equiv}(x) = [\alpha(x)]_{\equiv}$ and $\gamma_{\equiv}([y]_{\equiv}) = \gamma(y)$, then
$$\langle P, \leq\rangle \xleftrightarrow[\alpha_{\equiv}]{\gamma_{\equiv}} \langle Q/_{\equiv}, \sqsubseteq_{\equiv}\rangle$$
where $[x]_{\equiv} \sqsubseteq_{\equiv} [y]_{\equiv} \stackrel{\text{def}}{=} x \sqsubseteq y$ on $Q/_{\equiv}$ ■

PROOF. – $\equiv$ is an equivalence relation. We let $[x]_{\equiv}$ be the equivalence class of $x \in Q$ in the quotient $Q/_{\equiv}$.

– We have a Galois connection $\langle P, \leq\rangle \xleftrightarrow[\alpha_{\equiv}]{\gamma_{\equiv}} \langle Q/_{\equiv}, \sqsubseteq_{\equiv}\rangle$ as follows:

$$\begin{array}{lll} & \alpha(x) \sqsubseteq_{\equiv} [y]_{\equiv} & \\ \Longleftrightarrow & [\alpha(x)]_{\equiv} \sqsubseteq_{\equiv} [y]_{\equiv} & \wr\text{def. } \alpha_{\equiv}(x)\wr \\ \Longleftrightarrow & \alpha(x) \sqsubseteq y & \wr\text{def. } \sqsubseteq_{\equiv}\wr \end{array}$$

$$\begin{array}{lll} \Longleftrightarrow & x \leq \gamma(y) & \wr\text{original Galois connection}\wr \\ \Longleftrightarrow & x \leq \gamma_{\equiv}([y]_{\equiv}) & \wr\text{def. } \gamma_{\equiv}\wr \end{array}$$

– To prove that $\gamma_{\equiv}$ is injective (which implies $\alpha_{\equiv}$ is surjective), assume

$$\begin{array}{lll} & \gamma_{\equiv}([x]_{\equiv}) = \gamma_{\equiv}([y]_{\equiv}) & \\ \Longrightarrow & \gamma(x) = \gamma(y) & \wr\text{by def. } \gamma_{\equiv}\wr \\ \Longrightarrow & [x]_{\equiv} \sqsubseteq_{\equiv} [y]_{\equiv} & \wr\text{by def. } \equiv\wr \\ \Longrightarrow & [x]_{\equiv} = [y]_{\equiv} \text{ on } Q/_{\equiv} & \wr\text{by def. } Q/_{\equiv}\wr \end{array}$$

□

Linear Sum of Galois connections

THEOREM. Let $\langle P_1, \leq_1\rangle \xleftrightarrow[\alpha_1]{\gamma_1} \langle Q_1, \sqsubseteq_1\rangle$ and $\langle P_2, \leq_2\rangle \xleftrightarrow[\alpha_2]{\gamma_2} \langle Q_2, \sqsubseteq_2\rangle$ be Galois connections. Define the linear (ordinal) sums of posets $\langle P, \leq\rangle \stackrel{\text{def}}{=} \langle P_1, \leq_1\rangle \oplus \langle P_2, \leq_2\rangle$ and $\langle Q, \sqsubseteq\rangle \stackrel{\text{def}}{=} \langle Q_1, \sqsubseteq_1\rangle \oplus \langle Q_2, \sqsubseteq_2\rangle$ as well as $\alpha = \alpha_1 \oplus \alpha_2$ and $\gamma = \gamma_1 \oplus \gamma_2$ as follows:

$$\begin{array}{ll} \alpha(\langle 0, x\rangle) \stackrel{\text{def}}{=} \langle 0, \alpha_1(x)\rangle & \gamma(\langle 0, x\rangle) \stackrel{\text{def}}{=} \langle 0, \gamma_1(x)\rangle \\ \alpha(\langle 1, x\rangle) \stackrel{\text{def}}{=} \langle 1, \alpha_2(x)\rangle & \gamma(\langle 1, x\rangle) \stackrel{\text{def}}{=} \langle 1, \gamma_2(x)\rangle \end{array}$$

then
$$\langle P, \leq\rangle \xleftrightarrow[\alpha]{\gamma} \langle Q, \sqsubseteq\rangle$$
■

PROOF. $\alpha(\langle i,\ x\rangle) \sqsubseteq \langle j,\ y\rangle$

(i) if $i = j = 0$ then

$$\begin{aligned}
&\iff \alpha_1 \leq_1 y\\
&\iff x \sqsubseteq_1 \gamma_1(y)\\
&\iff \langle 0,\ x\rangle \sqsubseteq \langle 0,\ \gamma_1(y)\rangle\\
&\iff \langle 0,\ x\rangle \sqsubseteq \gamma(\langle 0,\ y\rangle)\\
&\iff \langle i,\ x\rangle \sqsubseteq \gamma(\langle j,\ y\rangle)
\end{aligned}$$

(ii) if $i = 0,\ j = 1$ then $\langle i,\ x\rangle = \langle 0,\ x\rangle \sqsubseteq \langle 1,\ \gamma_2(y)\rangle = \gamma(\langle 1,\ y\rangle) = \gamma(\langle j,\ y\rangle)$

(iii) if $i = j = 1$ then

$$\begin{aligned}
&\iff \alpha_2 \leq_2 y\\
&\iff x \sqsubseteq_2 \gamma_2(y)\\
&\iff \langle 1,\ x\rangle \sqsubseteq \langle 1,\ \gamma_2(y)\rangle
\end{aligned}$$

$$\begin{aligned}
&\iff \langle 1,\ x\rangle \sqsubseteq \gamma(\langle 1,\ y\rangle)\\
&\iff \langle i,\ x\rangle \sqsubseteq \gamma(\langle j,\ y\rangle)
\end{aligned}$$

□

Disjoint sum of Galois connections

THEOREM. Let $\langle P_1,\ \leq_1\rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle Q_1,\ \sqsubseteq_1\rangle$ and $\langle P_2,\ \leq_2\rangle \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \langle Q_2,\ \sqsubseteq_2\rangle$ be Galois connections. Define the disjoint sums of posets $\langle P,\ \leq\rangle \overset{\text{def}}{=} \langle P_1,\ \leq_1\rangle + \langle P_2,\ \leq_2\rangle$ and $\langle Q,\ \sqsubseteq\rangle \overset{\text{def}}{=} \langle Q_1,\ \sqsubseteq_1\rangle + \langle Q_2,\ \sqsubseteq_2\rangle$ as well as $\alpha = \alpha_1 + \alpha_2$ and $\gamma = \gamma_1 + \gamma_2$ as follows:

$$\begin{aligned}
\alpha(\langle 0,\ x\rangle) &\overset{\text{def}}{=} \langle 0,\ \alpha_1(x)\rangle & \gamma(\langle 0,\ x\rangle) &\overset{\text{def}}{=} \langle 0,\ \gamma_1(x)\rangle\\
\alpha(\langle 1,\ x\rangle) &\overset{\text{def}}{=} \langle 1,\ \alpha_2(x)\rangle & \gamma(\langle 1,\ x\rangle) &\overset{\text{def}}{=} \langle 1,\ \gamma_2(x)\rangle
\end{aligned}$$

then

$$\langle P,\ \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle$$

■

PROOF.

$$\begin{aligned}
&\ \alpha(\langle i,\ x\rangle) \sqsubseteq \langle j,\ y\rangle\\
&\iff \langle i,\ \alpha_i(x)\rangle \sqsubseteq \langle j,\ y\rangle\\
&\iff i = j \wedge \alpha_i(x) \leq_i y\\
&\iff i = j \wedge x \leq_i \gamma_j(y)\\
&\iff \langle i,\ x\rangle \leq \langle j,\ \gamma_j(y)\rangle\\
&\iff \langle i,\ x\rangle \leq \gamma(\langle j,\ y\rangle)
\end{aligned}$$

□

Similar results hold for the smashed disjoint sum.

Product of Galois connections

THEOREM. Let $\langle P_1,\ \leq_1\rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle Q_1,\ \sqsubseteq_1\rangle$ and $\langle P_2,\ \leq_2\rangle \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \langle Q_2,\ \sqsubseteq_2\rangle$ be Galois connections. Define the cartesian product of posets $\langle P,\ \leq\rangle \stackrel{\text{def}}{=} \langle P_1,\ \leq_1\rangle \times \langle P_2,\ \leq_2\rangle$ and $\langle Q,\ \sqsubseteq\rangle \stackrel{\text{def}}{=} \langle Q_1,\ \sqsubseteq_1\rangle \times \langle Q_2,\ \sqsubseteq_2\rangle$ as well as $\alpha = \alpha_1 \times \alpha_2$ and $\gamma = \gamma_1 \times \gamma_2$ as follows:

$$\alpha(\langle x,\ y\rangle) \stackrel{\text{def}}{=} \langle \alpha_1(x),\ \alpha_2(y)\rangle$$
$$\gamma(\langle x,\ y\rangle) \stackrel{\text{def}}{=} \langle \gamma_1(x),\ \gamma_2(y)\rangle$$

then

$$\langle P,\ \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle$$

$\blacksquare$

PROOF.

$$
\begin{aligned}
& \alpha(\langle x,\ y\rangle \sqsubseteq \langle x',\ y'\rangle \\
\Longleftrightarrow\ & \langle \alpha_1(x),\ \alpha_2(y)\rangle \sqsubseteq \langle x',\ y'\rangle \\
\Longleftrightarrow\ & \alpha_1(x) \sqsubseteq_1 x' \wedge \alpha_2(y) \sqsubseteq_1 y' \\
\Longleftrightarrow\ & x \leq_1 \gamma_1(x') \wedge y \leq_2 \gamma_1(y') \\
\Longleftrightarrow\ & \langle x,\ y\rangle \sqsubseteq \gamma(\langle x',\ y'\rangle)
\end{aligned}
$$

$\square$

This can be generalized to $\langle P,\ \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle Q,\ \sqsubseteq\rangle$ implies $\langle P^n,\ \leq^n\rangle \underset{\alpha^n}{\overset{\gamma^n}{\leftrightarrows}} \langle Q^n,\ \sqsubseteq^n\rangle$ where

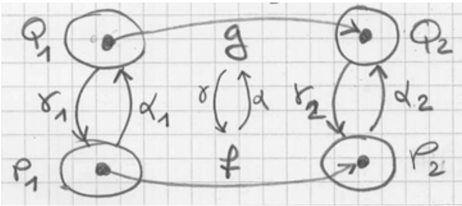
$$\alpha^n(\langle x_1,\ \ldots,\ x_n\rangle) = \langle \alpha(x_1),\ \ldots,\ \alpha(x_n)\rangle$$
$$\gamma^n(\langle y_1,\ \ldots,\ y_n\rangle) = \langle \gamma(y_1),\ \ldots,\ \gamma(y_n)\rangle$$

Power of Galois connections

THEOREM. Let $\langle P_1,\ \leq_1\rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle Q_1,\ \sqsubseteq_1\rangle$ and $\langle P_2,\ \leq_2\rangle \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \langle Q_2,\ \sqsubseteq_2\rangle$ be Galois connections and $\langle P_1 \stackrel{\text{m}}{\longmapsto} P_2,\ \dot{\leq}_2\rangle$ as well as $\langle Q_1 \stackrel{\text{m}}{\longmapsto} Q_2,\ \dot{\sqsubseteq}_2\rangle$ be sets of monotone maps with the pointwise ordering. Then

$$\langle P_1 \stackrel{\text{m}}{\longmapsto} P_2,\ \dot{\leq}_2\rangle \underset{\lambda f \cdot \alpha_2 \circ f \circ \gamma_1}{\overset{\lambda g \cdot \gamma_2 \circ g \circ \alpha_1}{\leftrightarrows}} \langle Q_1 \stackrel{\text{m}}{\longmapsto} Q_2,\ \dot{\sqsubseteq}_2\rangle$$

$\blacksquare$



$$\alpha = \lambda f \cdot \alpha_2 \circ f \circ \gamma_1$$
$$\gamma = \lambda g \cdot \gamma_2 \circ g \circ \alpha_1$$

PROOF.

$$
\begin{aligned}
& \alpha(f)\ \dot{\sqsubseteq}_2\ g \\
\Longleftrightarrow\ & \alpha_2 \circ f \circ \gamma_1\ \dot{\sqsubseteq}_2\ g && \text{(def. } \alpha\text{)} \\
\Longleftrightarrow\ & \forall x : \alpha_2(f(\gamma_1(x))) \sqsubseteq_2 g(x) && \text{(def. } \dot{\sqsubseteq}_2 \text{ and } \circ\text{)} \\
\Longleftrightarrow\ & \forall x : f(\gamma_1(x)) \leq_2 \gamma_2(g(x)) && \text{(Galois connection)} \\
\Longrightarrow\ & \forall y : f(\gamma_1(\alpha_1(y))) \leq_2 \gamma_2(g(\alpha_1(y))) && \text{(by setting } x = \alpha_1(y)\text{)} \\
\Longrightarrow\ & \forall y : f(y) \leq_2 \gamma_2(g(\alpha_1(y))) && \text{(since } y \leq_1 \gamma_1(\alpha_1(y) \text{ and } f \text{ monotone)} \\
\Longrightarrow\ & f\ \dot{\leq}_2\ \gamma_2 \circ g \circ \alpha_1 && \text{(def. } \dot{\leq}_2 \text{ and } \circ\text{)} \\
\Longrightarrow\ & f\ \dot{\leq}_2\ \gamma(g) && \text{(def. } \gamma\text{)} \\
\Longrightarrow\ & f\ \dot{\leq}_2\ \gamma_2 \circ g \circ \alpha_1 && \text{(def. } \gamma\text{)} \\
\Longrightarrow\ & f \circ \gamma_1\ \dot{\leq}_2\ \gamma_2 \circ g \circ \alpha_1 \circ \gamma_1 && \text{(def. } \dot{\leq}_2\text{)} \\
\Longrightarrow\ & f \circ \gamma_1\ \dot{\leq}_2\ \gamma_2 \circ g && \text{(since } \alpha_1 \circ \gamma_1 \text{ reductive and } \gamma_2 \text{ and } g \text{ monotone)} \\
\Longrightarrow\ & \alpha_2 \circ f \circ \gamma_1\ \dot{\sqsubseteq}_2\ \alpha_2 \circ \gamma_2 \circ g && \text{(since } \alpha_2 \text{ monotone)}
\end{aligned}
$$

$$\Longrightarrow \quad \alpha_2 \circ f \circ \gamma_1 \mathrel{\dot{\sqsubseteq}_2} g \qquad \text{(since } \alpha_2 \circ \gamma_2 \text{ reductive)}$$

$$\Longrightarrow \quad \alpha(f) \mathrel{\dot{\sqsubseteq}_2} g \qquad \text{(def. } \alpha\text{)}$$

and so $\alpha(f) \mathrel{\dot{\sqsubseteq}_2} g \iff f \mathrel{\dot{\leq}_2} \gamma(g)$. □

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/.