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

Poset Images

The image of a complete lattice by a complete join preserving map is a complete lattice

Theorem. Let $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ be a complete lattice, $\langle M, \leq\rangle$ be a poset and $f \in L \overset{\sqcup}{\longmapsto} M$ which preserves existing lubs. Then $F(L) \overset{\text{def}}{=} \{f(x) \mid x \in L\}$ is a complete lattice (so M is a complete lattice when f is surjective). ■

Proof. – Any subset X of $f(L)$ is the image by f of some subset X' of L: $f(X') = X$ where $X' \overset{\text{def}}{=} \{x \in L \mid f(x) \in X\}$. $\sqcup X'$ exists in the complete lattice L so $f(\sqcup X') = \bigvee f(X')$ where $\bigvee f(X')$ is the lub of $f(X')$ in M, which exists since f preserves existing lubs.

- It follows that $\forall x \in X' : \exists y \in X : f(y) = x$ and $x = f(y) \leq \bigvee f(X')$ by def. of lubs in M so $\forall x \in X' : x \leq \bigvee X$ proving that $\bigvee X$ is an upper bound of X in M. But $\bigvee X = \bigvee f(X') = f(\bigsqcup X')$ belongs to $f(L)$ so $\bigvee X$ is an upper bound of X in $f(L)$.
- Let z be any other upper bound of X in $f(L)$. Let $z' \in L : f(z') = z$. We have $\forall x \in X : x \leq z$ so $\forall x' \in X' : f(x') \leq f(z')$ so $\bigvee f(X') \leq f(z')$ in M because $\bigvee f(X')$ is the lub of $f(X')$ in M. But $\bigvee f(X') = f(\bigsqcup X') \in F(L)$ so $\bigvee f(X') \leq f(z')$ in $f(L)$ that is $\forall z \in f(L) : \forall x \in X : x \leq z \Longrightarrow \bigvee X \leq z$ so $\bigvee X$ is the lub of X in $f(L)$.
- By definition $\langle f(L), \leq, \vee\rangle$ is a complete lattice.

□

Image of a complete lattice by a Galois connection

THEOREM. Let $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ be a complete lattice, $\langle P, \leq\rangle$ be a poset and $\langle L, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle P, \leq\rangle$ be a Galois connection. Then $\langle \alpha(L), \leq, \alpha(\bot), \alpha(\top), \lambda X \cdot \alpha(\sqcup\gamma(X)), \lambda X \cdot \alpha(\sqcap\gamma(X))\rangle$ is a complete lattice. ■

PROOF. – In a Galois connection α preserves existing lubs, so $\langle\alpha(L), \leq\rangle$ is a complete lattice.

- We have $\forall y \in P : \bot \sqsubseteq \gamma(x)$ so $\alpha(\bot) \leq x$ proving that $\alpha(\bot)$ is the infimum of P and of $\alpha(L)$.
- $\forall x \in L : x \leq \top$ so $\alpha(x) \leq \alpha(\top)$ by monotony, proving that $\alpha(\top)$ is the supremum of $\alpha(L)$.

- Given $X \subseteq \alpha(L)$, X is the image of $X' \subseteq L : \alpha(X') = X$. We have shown that $\bigvee X = \alpha(\bigsqcup X')$. Since α preserves existsing lubs, $\alpha(\bigsqcup X') = \bigvee(\alpha(X')) = \bigvee \alpha \circ \gamma \circ \alpha(X') = \alpha(\bigsqcup(\gamma \circ \alpha(X')) = \alpha(\bigsqcup \gamma(X))$ proving that $\bigvee X = \alpha(\bigsqcup \gamma(X))$.
- $\forall x \in X : \bigsqcap \gamma(X) = \bigsqcap_{x' \in X} \gamma(x') \sqsubseteq \gamma(x)$ so that by monotony $\alpha(\bigsqcap_{x' \in X} \gamma(x')) \leq \alpha \circ \gamma(x) \leq x$ since $\alpha \circ \gamma$ is reductive. It follows that $\alpha(\bigsqcap \gamma(X))$ is a lower bound of X.
- Let y be another lower bound of X: $\forall x \in X : y \sqsubseteq x$. By monotony, $\gamma(y) \sqsubseteq \gamma(x)$ so $\gamma(y) \sqsubseteq \bigsqcap_{x \in X} \gamma(x) = \bigsqcap \gamma(X)$ by def. of glb. So $y \sqsubseteq \alpha(\bigsqcap \gamma(X))$ by def. of Galois connections. It follows that $\alpha(\sqcap\gamma(X))$ is the glb of X.

□

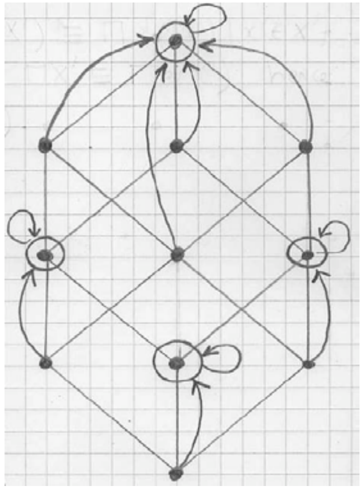
The image of a complete lattice by a closure operator is a complete lattice

THEOREM. Let ρ be an upper closure operator on a complete lattice $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$. Then $\langle \rho(L), \sqsubseteq, \rho(\bot), \top, \lambda X \cdot \rho(\sqcup X), \sqcap\rangle$ is a complete lattice. ■

Reference

[1] M. Ward, The Closure Operators of a Lattice, Annals of Mathematics 43 (1942), 191–199.

Example:



PROOF. We have shown that $\langle P,\ \leq\rangle \underset{\rho}{\overset{1_P}{\leftrightarrows}} \langle \rho(P),\ \leq\rangle$ and so we have a complete lattice $\langle \rho(L),\ \sqsubseteq,\ \rho(\bot),\ \rho(\top),\ \lambda X \cdot \rho(\sqcup X),\ \lambda X \cdot \rho(\sqcap X)\rangle$

- Since ρ is extensive, we have $\top \sqsubseteq \rho(\top)$ and by def. of top $\rho(\top) \sqsubseteq \top$ so by antisymmetry $\rho(\top) = \top$.
- For all $X \subseteq \rho(L)$ there exists an $X' \subseteq L$ such that $\rho(X') = X$ so $\rho(\sqcap X) = \rho(\sqcap \rho(X')) \sqsubseteq \sqcap \rho(\rho(X')) = \sqcap \rho(X') = \sqcap X$ by monotony, idempotence and $\rho(X') = X$. Moreover $\sqcap X \sqsubseteq \rho(\sqcap X)$ by extensivity. By antisymmetry, we conclude that $\rho(\sqcap X) = \sqcap X$.
- We conclude that $\langle \rho(L),\ \sqsubseteq,\ \rho(\bot),\ \top,\ \lambda X \cdot \rho(\sqcup X),\ \sqcap\rangle$ is a complete lattice.

$\sqsubset$

Closure operator induced by a Moore family

THEOREM. Let $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ be a complete lattice and $\mathcal{M} \subseteq L$ be a Moore family of L (i.e. $\forall X \subseteq \mathcal{M} : \bigsqcap X \in \mathcal{M}$). The operator $\rho \in L \mapsto L$ defined by

$$\rho(x) \stackrel{\text{def}}{=} \bigsqcap\{y \in \mathcal{M} \mid x \sqsubseteq y\}$$

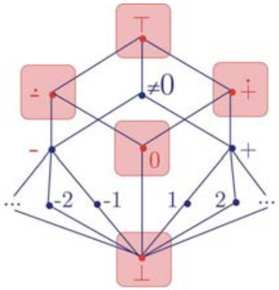
is a closure operator on L such that $\rho(L) = \mathcal{M}$ ■

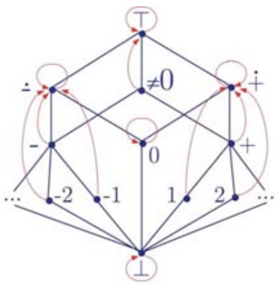
PROOF.

- If : $x \sqsubseteq y$ then $y \sqsubseteq z \Longrightarrow x \sqsubseteq z$ so $\{z \in \mathcal{M} \mid y \sqsubseteq z\} \subseteq \{z \in \mathcal{M} \mid x \sqsubseteq z\}$ hence $\bigsqcap\{z \in \mathcal{M} \mid x \sqsubseteq z\} \sqsubseteq \bigsqcap\{z \in \mathcal{M} \mid y \sqsubseteq z\}$ that is $\rho(x) \sqsubseteq \rho(y)$, proving ρ to be monotone.
- We have $\forall z \in \{y \in \mathcal{M} \mid x \sqsubseteq y\} : x \sqsubseteq z$ so $x \sqsubseteq \bigsqcap\{y \in \mathcal{M} \mid x \sqsubseteq y\}$ hence $x \sqsubseteq \rho(x)$, proving that ρ is extensive.

- if $x \in L$ then $\rho(x) = \bigsqcap\{y \in \mathcal{M} \mid x \sqsubseteq y\} \in \mathcal{M}$ since $\mathcal{M}$ is a Moore family. So $\rho(\rho(x)) = \bigsqcap\{y \in \mathcal{M} \mid \rho(x) \sqsubseteq y\} \sqsubseteq \rho(x)$ since $\rho(x) \in \{y \in \mathcal{M} \mid \rho(x) \sqsubseteq y\}$ by reflexivity. Moreover $x \sqsubseteq \rho(x)$ so $\rho(x) \sqsubseteq \rho(\rho(x))$ by monotony. By antisymmetry, $\rho(x) = \rho(\rho(x))$, proving ρ to be idempotent.
- By definition of a Moore family $\rho(x) \in \mathcal{M}$ so $\rho(L) \subseteq \mathcal{M}$. Now if $x \in \mathcal{M}$ then $\rho(x) = x$ so $x \in \rho(L)$, proving $\rho(L) = \mathcal{M}$.

$\sqsubset$





The least closure operator greater than or equal to a monotone operator on a complete lattice

THEOREM. Let f be an operator on a complete lattice $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$. Then $\text{uclo}(f) \stackrel{\text{def}}{=} \lambda x \cdot \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\}$ is the $\dot\sqsubseteq$-least closure operator on L which is $\dot\sqsubseteq$-greater than or equal to f. ■

PROOF. – $\forall z \in \{y \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\}$, we have $x \sqsubseteq z$ so $x \sqsubseteq \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\} = \text{uclo}(f)(x)$ so $\text{uclo}(f)$ is extensive.

- If $x \sqsubseteq x'$ then $(x' \sqsubseteq y \wedge f(y) \sqsubseteq y) \Longrightarrow (x \sqsubseteq y \wedge f(y) \sqsubseteq y)$ so $\{y \mid x' \sqsubseteq y \wedge f(y) \sqsubseteq y\} \subseteq \{y \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\}$ whence $\text{uclo}(f)(x) = \bigsqcap\{y \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\} \sqsubseteq \bigsqcap\{y \mid x' \sqsubseteq y \wedge f(y) \sqsubseteq y\} = \text{uclo}(f)(x')$ proving that $\text{uclo}(f)$ is monotonic.
- $\text{uclo}(f)(x) \sqsubseteq \text{uclo}(f)(\text{uclo}(f)(x))$ since $\text{uclo}(f)$ is extensive and monotone.

- If $f(y) \sqsubseteq y$ then $y \in \{z \mid y \leq z \wedge f(z) \sqsubseteq z\}$ so $\mathsf{uclo}(f)(y) = \bigsqcap\{z \in L \mid x \sqsubseteq z \wedge f(z) \sqsubseteq z\} \sqsubseteq y$. So $(x \sqsubseteq y \wedge f(y) \sqsubseteq y) \Longrightarrow (x \sqsubseteq y \wedge \mathsf{uclo}(f)(y) \sqsubseteq y)$ hence $\{y \in L \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\} \subseteq \{y \in L \mid x \sqsubseteq y \wedge \mathsf{uclo}(f)(y) \sqsubseteq y\}$ so $\mathsf{uclo}(f)(\mathsf{uclo}(f)(x)) = \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge \mathsf{uclo}(f)(y) \sqsubseteq y\} \sqsubseteq \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\} = \mathsf{uclo}(f)(y)$
- By antisymmetry, $\mathsf{uclo}(f)(\mathsf{uclo}(f)(x)) = \mathsf{uclo}(f)(x)$ proving idempotence.
- Let ρ be a closure operator on L such that $\forall x \in L = f(x) \sqsubseteq \rho(x)$. We have $\forall x \in L : x \sqsubseteq \rho(x)$ and $f(\rho(x)) \sqsubseteq \rho(\rho(x)) = \rho(x)$ proving $\mathsf{uclo}(f)(x) \sqsubseteq \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\} \sqsubseteq \rho(x)$ whence that $\mathsf{uclo}(f)$ is the $\dot{\sqsubseteq}$-least closure operator on L which is $\dot{\sqsubseteq}$-greater than or equal to f.

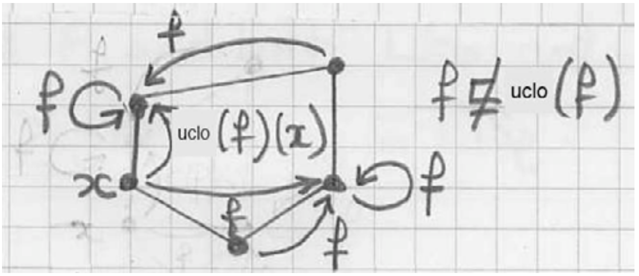
$\sqsubset$

A closure operator on monotonic functions

Theorem. Let $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ be a complete lattice. The operator $\mathsf{uclo}(f) \stackrel{\text{def}}{=} \lambda x \cdot \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\}$ is an upper closure operator in $\langle L \stackrel{\text{m}}{\longmapsto} L, \dot{\sqsubseteq}, \dot{\bot}, \dot{\top}, \dot{\sqcup}, \dot{\sqcap}\rangle$ (but in general not on $L \mapsto L$). ■

Proof. – We have shown that uclo is monotone on $L \mapsto L$ whence it is on the subset $L \stackrel{\text{m}}{\longmapsto} L$ since for all f, $\mathsf{uclo}(f)$ is monotone.

- We have shown that if ρ is a closure operator such that $f \dot{\sqsubseteq} \rho$ then $\mathsf{uclo}(f) \dot{\sqsubseteq} \rho$ so that in particular for $f = \rho = \mathsf{uclo}(g)$ we get $\mathsf{uclo}(\mathsf{uclo}(g)) \dot{\sqsubseteq} \mathsf{uclo}(g)$ since $\mathsf{uclo}(g)$ is a closure operator.
- Notice that $\mathsf{uclo}(f)$ may not be extensive on $L \mapsto L$ as shown by the following counter example:



- However if $f \in L \stackrel{\text{m}}{\longmapsto} L$ is monotone, we have $\forall x \in L : (x \sqsubseteq y \wedge f(y) \sqsubseteq y) \Longrightarrow (f(y) \sqsubseteq y)$ so $f(x) \sqsubseteq \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\} = \mathsf{uclo}(f)(x)$ proving $\forall f \in L \stackrel{\text{m}}{\longmapsto} L : f \dot{\sqsubseteq} \mathsf{uclo}(f)$
- By monotony, $\mathsf{uclo}(g) \dot{\sqsubseteq} \mathsf{uclo}(\mathsf{uclo}(g))$ since $\mathsf{uclo}(g)$ is an upper closure operator whence monotone, so $\mathsf{uclo}(g) = \mathsf{uclo}(\mathsf{uclo}(g))$ by antisymmetry, proving the idempotence of uclo.

$\sqsubset$

The complete lattice of closure operators on a complete lattice

Theorem. Let $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ be a complete lattice. The set of upper closure operators on L is a complete lattice $\langle \mathsf{uclo}(L \stackrel{\text{m}}{\longmapsto} L), \dot{\sqsubseteq}, \lambda x \cdot x, \dot{\top}, \lambda X \cdot \mathsf{uclo}(\dot{\sqcup} X), \dot{\sqcap}\rangle$ ■

Reference

[2] M. Ward, The Closure Operators of a Lattice, Annals of Mathematics 43 (1942), 191–196.

Proof. – Let C_L be the set of all closure operators on L. We have $C_L \subseteq (L \overset{m}{\longmapsto} L)$ since closure operators are monotonic. We let uclo $\overset{\text{def}}{=} \lambda f \cdot \lambda x \cdot \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\}$ as before.

- We have shown that uclo$(L \overset{m}{\longmapsto} L) \subseteq C_L$ since uclo(f) is an upper closure operator whenever f is monotonic.
- Conversely, if $\rho \in C_L$, uclo(ρ) is the least upper closure operator pointwise greater than or equal to ρ, that is ρ itself. So $C_L \subseteq$ uclo$(L \overset{m}{\longmapsto} L)$.
- By antisymmetry, $C_L =$ uclo$(L \overset{m}{\longmapsto} L)$.
- Since $\langle L \overset{m}{\longmapsto} L, \dot{\sqsubseteq}, \dot{\bot}, \dot{\top}, \dot{\sqcup}, \dot{\sqcap}\rangle$ is a complete lattice, its image $C_L =$ uclo$(L \overset{m}{\longmapsto} L)$ by the closure operator uclo is also a complete lattice $\langle C_L, \dot{\sqsubseteq},$ uclo$(\dot{\bot}), \dot{\top}, \lambda X \cdot$ uclo$(\dot{\sqcup} X), \dot{\sqcap}\rangle$.
- For the infimum, uclo$(\dot{\bot})$, observe that

$$\begin{aligned}\text{uclo}(\dot{\bot}) &= \lambda x \cdot \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge \dot{\bot}(y) \sqsubseteq y\}\\ &= \lambda x \cdot \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge \bot \sqsubseteq y\}\\ &= \lambda x \cdot \bigsqcap\{y \in L \mid x \sqsubseteq y \;=\; \lambda x \cdot x\}\end{aligned}$$

which is the $\dot{\sqsubseteq}$-least closure operator.

□

The complete lattice of Galois connections on a complete lattice

Theorem. – Let $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ be a complete lattice

- Let $\mathsf{GC}(L) = \{\langle \alpha, \gamma\rangle \mid \exists \langle M, \leq\rangle : \langle L, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle M, \leq\rangle\}$
- Let $\equiv$ be the equivalence relation on $\mathsf{GC}(L)$ defined by $\langle \alpha_1, \gamma_1\rangle \equiv \langle \alpha_2, \gamma_2\rangle$ iff $\gamma_1 \circ \alpha_1 = \gamma_2 \circ \alpha_2$.
- $\langle \mathsf{GC}(L)|_{\equiv}, \sqsubseteq_{\equiv}, [\langle \lambda x \cdot x, 1_L\rangle]_{\equiv}, [\langle \lambda x \cdot \top, 1_L\rangle]_{\equiv},$

$$\lambda X \cdot [\langle \text{uclo}(\dot{\bigsqcup_{\langle \alpha, \gamma\rangle \in X}} \gamma \circ \alpha), 1_L\rangle]_{\equiv}, \lambda X \cdot [\langle \dot{\bigsqcap_{\langle \alpha, \gamma\rangle \in X}} \gamma \circ \alpha, 1_L\rangle]_{\equiv}\rangle$$

where uclo $\overset{\text{def}}{=} \lambda f \cdot \lambda x \cdot \bigsqcap\{y \in L \mid x \sqsubseteq y \wedge f(y) \sqsubseteq y\}$.

■

Proof. – $\equiv$ is obviously reflexive, symmetric and transitive, when an equivalence relation

- Observe that $\langle L, \sqsubseteq\rangle \underset{\gamma \circ \alpha}{\overset{1_L}{\leftrightarrows}} \langle L, \sqsubseteq\rangle$ and $1_L \circ \gamma \circ \alpha = \gamma \circ \alpha$ so $\langle \gamma \circ \alpha, 1_L\rangle \equiv \langle \alpha, \gamma\rangle$. Let C_L be the set of upper closure operators on L. $\gamma \circ \alpha \in C_L$. Define $\Pi([\langle \alpha, \gamma\rangle]_{\equiv}) \overset{\text{def}}{=} \gamma \circ \alpha$ and $\Pi^{-1}(\rho) \overset{\text{def}}{=} [\langle \rho, 1_L\rangle]_{\equiv}$. Then Π is a bijection between $\mathsf{GC}(L)$ and C_L. Since C_L is a complete lattice, $\mathsf{GC}(L)$ inherits its structure up to the isomorphism Π.

□

The complete lattice of safety properties

Bifinitary traces

- Σ: set of states
- $\Sigma^{\vec{n}} \stackrel{\text{def}}{=} \{0, \ldots, n-1\} \mapsto \Sigma$, finite sequences σ of length $|\sigma| = n$. The i-th element of $\sigma \in x^{\vec{n}}$ is $\sigma(i)$ abbreviated σ_i so $\sigma = \sigma_0\sigma_1 \ldots \sigma_{n-1}$ including the empty sequence $\Sigma^{\vec{0}} \stackrel{\text{def}}{=} \{\vec{\epsilon}\}$
- $\Sigma^{\vec{\star}} \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}} \Sigma^{\vec{n}}$ finite sequences
- $\Sigma^{\vec{+}} \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}\setminus\{0\}} \Sigma^{\vec{n}}$ finite nonempty sequences

- $\Sigma^{\vec{\omega}} \stackrel{\text{def}}{=} \mathbb{N} \mapsto \Sigma$ infinite sequences σ of length $|\sigma| = \omega$ where $\forall i \in \mathbb{N} : i < \omega$
- $\Sigma^{\vec{\propto}} \stackrel{\text{def}}{=} \Sigma^{\vec{\star}} \cup \Sigma^{\vec{\omega}}$ bifinitary sequences
- $\Sigma^{\vec{\infty}} \stackrel{\text{def}}{=} \Sigma^{\vec{+}} \cup \Sigma^{\vec{\omega}}$ nonempty bifinitary sequences

Prefixes of bifinitary traces

The prefix:

$$\sigma \swarrow p$$

of length $p \in \mathbb{N}$ of a sequence $\sigma \in \Sigma^{\vec{\propto}}$ is:

- $\sigma = \sigma_0 \ldots \sigma_{n-1} \in \Sigma^{\vec{n}}$ finite sequences
  - $\sigma \swarrow 0 = \vec{\epsilon}$
  - $\sigma \swarrow p = \sigma_0 \ldots \sigma_{p-1}$ $\quad 1 \leq p \leq n$
  - $\sigma \swarrow p = \sigma \swarrow n = \sigma$ $\quad p \geq n$
- $\sigma = \sigma_0 \ldots \sigma_n \ldots \in \Sigma^{\vec{\omega}}$ infinite sequences
  - $\sigma \swarrow 0 = \vec{\epsilon}$
  - $\sigma \swarrow p = \sigma_0 \ldots \sigma_{p-1}$ $\quad p \geq 1$
- $\forall \sigma \in \Sigma^{\vec{\propto}} : \forall p \in \mathbb{N} : \sigma \swarrow p \in \Sigma^{\vec{\star}}$;

Prefix closure

- Prefixes of bifinitary sequences:

$$\mathsf{PCl}(\sigma) \stackrel{\text{def}}{=} \{\sigma \swarrow p \mid p \in \mathbb{N}_+\} \qquad \sigma \in \Sigma^{\vec{\propto}}$$

- Prefix closure of sets of bifinitary sequences:

$$\mathsf{PCl}(X) \stackrel{\text{def}}{=} \bigcup_{\sigma\in X} \mathsf{PCl}(\sigma) \qquad X \in \wp(\Sigma^{\vec{\propto}})$$

Prefix partial ordering

- The order relation “is a prefix of” $(\sigma, \zeta \in \Sigma^{\vec{\infty}})$ is
  $\sigma \preceq \zeta \overset{\text{def}}{=} \exists \beta \in \Sigma^{\vec{\infty}} : \sigma \bullet \beta = \zeta$ prefix ordering
  $\sigma \prec \zeta \overset{\text{def}}{=} \sigma \preceq \zeta \wedge \sigma \neq \zeta$ strict partial ordering
- $\sigma \preceq \zeta \Leftrightarrow (\sigma \in \mathsf{PCl}(\zeta) \vee \sigma = \zeta \in \Sigma^{\vec{\omega}})$
- $\sigma \preceq \zeta \Leftrightarrow \mathsf{PCl}(\sigma) \subseteq \mathsf{PCl}(\zeta)$
- $\sigma = \zeta \Leftrightarrow \mathsf{PCl}(\sigma) = \mathsf{PCl}(\zeta)$
- $\sigma \in \Sigma^{\vec{*}} \Leftrightarrow |\mathsf{PCl}(\sigma)| < \omega$
- $\sigma \in \mathsf{PCl}(\zeta) \Leftrightarrow (\sigma \in \Sigma^{\vec{+}} \wedge \exists \beta : \sigma \bullet \beta = \zeta)$
- $\mathsf{PCl}(X) = \{\sigma \in \Sigma^{\vec{+}} \mid \exists \zeta \in X : \sigma \preceq \zeta\}$

Properties of the prefix closure

- For finite sequences, PCl is a *topological closure operator* on $\wp(\Sigma^{\vec{*}})$ and $\wp(\Sigma^{\vec{+}})$:
  - $\mathsf{PCl} \in \wp(\Sigma^{\vec{*}}) \mapsto \wp(\Sigma^{\vec{*}})$
  - $\mathsf{PCl} \in \wp(\Sigma^{\vec{+}}) \mapsto \wp(\Sigma^{\vec{+}})$
  - $X \subseteq \mathsf{PCl}(X)$ increasing/extensive
  - $\mathsf{PCl}(\mathsf{PCl}(X)) = \mathsf{PCl}(X)$ idempotent
  - $\mathsf{PCl}(X \cup Y) = \mathsf{PCl}(X) \cup \mathsf{PCl}(Y)$ [1] additive
  - $\mathsf{PCl}(\emptyset) = \emptyset$ $\emptyset$-preserving

[1] This implies $X \subseteq Y \Rightarrow \mathsf{PCl}(X) \subseteq \mathsf{PCl}(Y)$.

- For bifinitary sequences, PCl satisfies:
  - $\mathsf{PCl} \in \wp(\Sigma^{\vec{\infty}}) \mapsto \wp(\Sigma^{\vec{*}})$
  - $\mathsf{PCl} \in \wp(\Sigma^{\vec{\infty}}) \mapsto \wp(\Sigma^{\vec{+}})$
  - $X \not\subseteq \mathsf{PCl}(X)$, when $X \cap \Sigma^{\vec{\omega}} \neq \emptyset$
  - $\mathsf{PCl}(\mathsf{PCl}(X)) = \mathsf{PCl}(X)$ idempotent
  - $\mathsf{PCl}(X \cup Y) = \mathsf{PCl}(X) \cup \mathsf{PCl}(Y)$ [2] additive
  - $\mathsf{PCl}(\emptyset) = \emptyset$ $\emptyset$-preserving

[2] This implies $X \subseteq Y \Rightarrow \mathsf{PCl}(X) \subseteq \mathsf{PCl}(Y)$.

Galois connection between sets of finite traces and their prefix closure

$$\begin{tikzcd} \langle \wp(\Sigma^{\vec{*}}), \subseteq \rangle \arrow[r, shift right, two heads, "\mathsf{PCl}"'] & \langle \mathsf{PCl}(\wp(\Sigma^{\vec{*}})), \subseteq \rangle \arrow[l, shift right, "1"'] \end{tikzcd}$$

$$\begin{tikzcd} \langle \wp(\Sigma^{\vec{+}}), \subseteq \rangle \arrow[r, shift right, two heads, "\mathsf{PCl}"'] & \langle \mathsf{PCl}(\wp(\Sigma^{\vec{+}})), \subseteq \rangle \arrow[l, shift right, "1"'] \end{tikzcd}$$

PROOF. – $\mathsf{PCl}(X) \subseteq Y$

$\Rightarrow X \subseteq Y$ [PCl is extensive]

$\Rightarrow X \subseteq 1(Y)$ [1 is identity]

$\Rightarrow \mathsf{PCl}(X) \subseteq \mathsf{PCl}(Y)$ [1 is identity and PCl is monotonic]

$\Rightarrow \mathsf{PCl}(X) \subseteq \mathsf{PCl}(\mathsf{PCl}(Z))$ [since $Y \in \mathsf{PCl}(\wp(\Sigma^{\vec{*}}))$ so $\exists Z \subseteq \Sigma^{\vec{*}} : Y = \mathsf{PCl}(Z)$]

$\Rightarrow \mathsf{PCl}(X) \subseteq \mathsf{PCl}(Z)$ [since PCl is idempotent]

$\Rightarrow \mathsf{PCl}(X) \subseteq Y$ [since $Y = \mathsf{PCl}(Z)$]

□

Limits of chains of traces

- Let $\alpha_0 \preceq \alpha_1 \preceq \ldots \preceq \alpha_n \preceq \ldots$ be a $\preceq$-increasing chain;
  - If the chain is finite or stationnary at rank ℓ, its limit is $\lim\limits_{n} \alpha_n = \alpha_\ell$,
  - Else, the chain is infinite, always eventually strictly increasing, in which case its limit is $\lim\limits_{n\in\mathbb{N}} \alpha_n = \lambda \in \Sigma^{\vec{\omega}}$ such that:

$$\forall n \in \mathbb{N} : \lambda\swarrow|\alpha_n| \;=\; \alpha_n$$

- The limit exists and is unique;

Limits of sets of bifinitary traces

- If $L \subseteq \Sigma^{\vec{\propto}}$ then:

$$\lim L \overset{\text{def}}{=} \{\lim_{n} \alpha_n \mid \alpha_0 \preceq \alpha_1 \preceq \ldots \preceq \alpha_n \preceq \ldots \subseteq L\}$$

- Lim is a topological closure operator on $\wp(\Sigma^{\vec{\propto}})$.

Proof. - $X \subseteq \lim X$ extensive

- $\lim X \cup Y = \lim X \cup \lim Y$ additive
  (since any infinite sequence in $\alpha_0 \prec \alpha_1 \prec \ldots \prec \alpha_n \prec \ldots$ is $X \cup Y$ has infinitely many elements hence its limits in X else has finitely many elements in X and infinitely many elements hence its limits in Y.)
- $\lim \lim X \;=\; \lim X$ idempotent
- $\lim \emptyset = \emptyset$ $\emptyset$-strict

□

Galois connection between sets of bifinitary traces and their prefix closure

$$\langle\wp(\Sigma^{\vec{\propto}}),\ \subseteq\rangle \underset{\mathsf{PCl}}{\overset{\lim}{\leftrightarrows}} \langle\mathsf{PCl}(\wp(\Sigma^{\vec{+}})),\ \subseteq\rangle \qquad (1)$$

Proof. – $\mathsf{PCl}(X) \subseteq Y$

$\Rightarrow \{\sigma \in \Sigma^{\vec{+}} \mid \exists\zeta \in X : \sigma \preceq \zeta\} \subseteq Y$

$\Rightarrow \forall\sigma \in \Sigma^{\vec{+}} : \forall\zeta \in X : (\sigma \preceq \zeta) \Rightarrow (\sigma \in Y)$

$\Rightarrow X \subseteq \{\zeta \mid \forall\sigma \in \Sigma^{\vec{+}} : (\sigma \preceq \zeta) \Rightarrow (\sigma \in Y)\}$

- If $\zeta \in \Sigma^{\vec{+}}$, $\zeta \preceq \zeta$ so $\zeta \in Y$ hence $\zeta \in \lim Y$;
- If $\zeta \in \Sigma^{\vec{\omega}}$, we have $\mathsf{PCl}(\zeta) \subseteq Y$ whence $\lim \mathsf{PCl}(\zeta) = \zeta \in \lim Y$;

$\Rightarrow X \subseteq \lim Y$.

- Reciprocally, if $X \subseteq \lim Y$ then $\mathsf{PCl}(X) \subseteq \mathsf{PCl}(\lim Y)$ and we must show that $\mathsf{PCl}(\lim Y) \subseteq Y$;
  - $\lim Y$ contains Y plus infinite traces λ;
  - We must show that $\mathsf{PCl}(\lambda) \subseteq Y$;
  - Otherwise let σ a prefix of λ not in Y;
  - $\lambda = \lim\limits_{n} \alpha_n$ with $\alpha_0 \prec \alpha_1 \prec \ldots \prec \alpha_n \ldots$. Let n be miniimal such that $|\alpha_n| \geqq |\sigma|$. We have $\sigma \preceq \alpha_n$, $\alpha_n \in Y$ and $Y \in \mathsf{PCl}(\wp(\Sigma^{\vec{+}}))$ so $\sigma \in Y$, a contradiction.

□

Closure by prefix and limits

$$\mathsf{Lim} \circ \mathsf{Pcl} \text{ is a topological closure operator.} \qquad (2)$$

Proof. – Lim and Pcl are both topological closure operators so that it remains to prove that:

$$\mathsf{Lim} \circ \mathsf{Pcl} \circ \mathsf{Lim} \circ \mathsf{Pcl} \;=\; \mathsf{Lim} \circ \mathsf{Pcl}$$

which follows from (1) which implies $\mathsf{Lim} \circ \mathsf{Pcl} \circ \mathsf{Lim} = \mathsf{Lim}$.

□

Corollary ($1 \overset{\text{def}}{=} \lambda x \cdot x$ is the identity):

$$\langle \wp(\Sigma^{\vec{\infty}}),\ \subseteq\rangle \underset{\mathsf{Lim}\circ\mathsf{Pcl}}{\overset{1}{\leftrightarrows}} \langle \mathsf{Lim} \circ \mathsf{Pcl}(\wp(\Sigma^{\vec{\infty}})),\ \subseteq\rangle \qquad (3)$$

Closure by prefix and limits

Lim is idempotent so that $\mathsf{Lim} \circ \mathsf{Pcl}$ is limit closed:

$$\mathsf{Lim} \circ \mathsf{Pcl}(P) = \mathsf{Lim} \circ \mathsf{Lim} \circ \mathsf{Pcl}(P) \qquad (4)$$

as well as prefix closed:

$$\mathsf{Lim} \circ \mathsf{Pcl}(P) = \mathsf{Pcl} \circ \mathsf{Lim} \circ \mathsf{Pcl}(P) \qquad (5)$$

Proof. – $\mathsf{Lim} \circ \mathsf{Pcl}(P) \subseteq \mathsf{Pcl} \circ \mathsf{Lim} \circ \mathsf{Pcl}(P)$ since Pcl is a closure operator hence extensive;

– The inverse $\mathsf{Pcl} \circ \mathsf{Lim} \circ \mathsf{Pcl}(P) \subseteq \mathsf{Lim} \circ \mathsf{Pcl}(P)$ follows from the remark that limits of prefix-closed sets cannot introduce new prefixes.

□

Definition of Safety

– $S \subseteq \Sigma^{\vec{\infty}}$ is a *safety* property if and only if [3]:

$$\mathsf{Safe}(S) = S\,^{3}$$

where:

$$\mathsf{Safe} \overset{\text{def}}{=} \mathsf{Lim} \circ \mathsf{Pcl} \qquad (6)$$

Reference

[3] B. Alpern & F.B. Schneider. *Defining Liveness.* Information Processing Letters 21 (1985) 181–185.

[3] Otherwise stated S is *closed* in the topology induced by the topological closure operator $\mathsf{Lim} \circ \mathsf{Pcl}$ which fixpoints are the closed sets.

Characterization of safety properties

Safety properties S can be disproved by looking only at some finite partial program behavior:

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

Proof. $\mathsf{Lim} \circ \mathsf{Pcl}(S) = S$

$\iff \mathsf{Lim} \circ \mathsf{Pcl}(S) \subseteq S$

$\iff \{\sigma \in \Sigma^{\vec{\infty}} \mid \forall i \geq 1 : \sigma\swarrow i \in \mathsf{Pcl}(S)\} \subseteq S$

$\iff \{\sigma \in \Sigma^{\vec{\infty}} \mid \forall i \geq 1 : \exists \beta \in \Sigma^{\vec{\infty}} : \sigma\swarrow i \centerdot \beta \in S\} \subseteq S$

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

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

$\iff \forall \sigma \in \Sigma^{\propto} : (\sigma \notin S) \iff (\exists i \geq 1 : \forall \beta \in \Sigma^{\propto} : \sigma\swarrow i \bullet \beta \notin S)$

since if $\exists i \geq 1 : \forall \beta \in \Sigma^{\propto} : \sigma\swarrow i \bullet \beta \notin S$ then in particular for $\beta = \sigma\nearrow n$, we have $\sigma = \sigma\swarrow i \bullet \sigma\nearrow n \notin S$.

$\iff \forall \sigma \in \Sigma^{\propto} : (\sigma \notin S) \iff (\exists i \geq 1 : \sigma\swarrow i \notin S)$[4]

since $\forall \beta \in \Sigma^{\propto} : \sigma\swarrow i \bullet \beta \notin S \iff \sigma\swarrow i \notin S$

$\Rightarrow$ choose $\beta = \vec{\epsilon}$

$\Leftarrow$ S is a safety property so $\mathsf{PCl}(S) = S$ hence $(\sigma\swarrow i \bullet \beta \in S) \Longrightarrow (\sigma\swarrow i \in S)$ so $(\sigma\swarrow i \notin S) \Longrightarrow (\sigma\swarrow i \bullet \beta \notin S)$.

□

[4] This corresponds to the usual explanation of safety: if a "bad thing" does occur (i.e. $\sigma \notin S$) then this can be recognized in finite time. Otherwise stated, there is a finite observation where something undesired happened which is irremediable, because it cannot be fixed in the future no matter how it is extended.

The complete lattice of safety properties

- $\mathsf{Safe}(P)$ is the least safety property including $P \subseteq \Sigma^{\propto}$; (7)
- $\langle \mathsf{Safe}(\wp(\Sigma^{\propto}))$[5], $\subseteq, \emptyset, \Sigma^{\propto}, \lambda S \cdot \mathsf{Lim}(\cup S), \cap\rangle$ is a complete lattice;
- Safe is a topological closure operator (2) but not a complete join morphism.

PROOF. – By (6) and (3), Safe is an upper-closure operator so that $\mathsf{Safe}(P)$ is the least soundness property including $P \subseteq \Sigma^{\propto}$ since $P \subseteq Y = \mathsf{Safe}(Y)$ implies $\mathsf{Safe}(P) \subseteq \mathsf{Safe}(Y) = Y$;

[5] $\mathsf{Safe}(X) \stackrel{\text{def}}{=} \{\mathsf{Safe}(x) \mid x \in X\}$.

- By Ward theorem, $\langle \mathsf{Safe}(\Sigma^{\propto}),, \sqsubseteq, \mathsf{Safe}(\emptyset), \Sigma^{\propto}, \lambda S \cdot \mathsf{Safe}(\cup S), \cap\rangle$ is a complete lattice with $\mathsf{Safe}(\emptyset) = \emptyset$ and $\mathsf{Safe}(\bigcup_i S_i)$

  $= \mathsf{Lim} \circ \mathsf{PCl}(\bigcup_i S_i)$

  $= \mathsf{Lim}(\bigcup_i \mathsf{PCl}(S_i))$ by (1)

  $= \mathsf{Lim}(\bigcup_i \mathsf{PCl} \circ \mathsf{Lim} \circ \mathsf{PCl} S_i)$

  since $S_i \in \mathsf{Safe}(\wp(\Sigma^{\propto}))$ so $\mathsf{Lim} \circ \mathsf{PCl} S_i = S_i$

  $= \mathsf{Lim}(\bigcup_i \mathsf{Lim} \circ \mathsf{PCl} S_i)$ by (5)

  $= \mathsf{Lim}(\bigcup_i S_i)$ since $S_i \in \mathsf{Safe}(\wp(\Sigma^{\propto}))$.
- To show that Safe is not a complete join morphism, consider $X_n = \{a\}^n$. We have $\bigcup_{n \in \mathbb{N}} \mathsf{Safe}(X_n) = \bigcup_{n \in \mathbb{N}} X_n = \{a\}^{*}$ whereas $\mathsf{Safe}(\bigcup_{n \in \mathbb{N}} X_n) = \mathsf{Safe}(\{a\}^{*}) = \{a\}^{\propto}$.

□

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.

- Laurent Mauborgne “Abstract Interpretation Using Typed I
  Science of Computer Programming, 31(1):91–112, may 1998.

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/.