« Mathematical foundations: (5) Fixpoint theory » Part I

Patrick Cousot

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

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

Course 16.399: “Abstract interpretation”

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

Alfred Tarski

Reference

[1] A. Tarski. “A lattice-theoretical fixpoint theorem and its applications”. Pacific J. of Math., 5:285–310, 1955.

Fixpoints

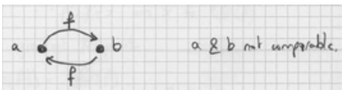
Fixpoint

- A fixpoint of an operator f on a set L is $x \in L$ such that $f(x) = x$
- An operator may have 0, 1 or many fixpoints (e.g. $\lambda x \cdot x$)

Fixpoints, prefixpoint and postfixpoints of an operator on a poset

Let $f \in L \mapsto L$ be an operator on a poset $\langle L, \sqsubseteq \rangle$. We define its

- set of fixpoints: $\mathsf{fp}(f) \stackrel{\text{def}}{=} \{x \in L \mid f(x) = x\}$
- set of pre-fixpoints: $\mathsf{prefp}(f) \stackrel{\text{def}}{=} \{x \in L \mid x \sqsubseteq f(x)\}$
- dual set of post-fixpoints: $\mathsf{postfp}(f) \stackrel{\text{def}}{=} \{x \in L \mid x \sqsupseteq f(x)\}$
- Note that $\mathsf{fp}(f) \subseteq \mathsf{prefp}(f)$, $\mathsf{fp}(f) \subseteq \mathsf{postfp}(f)$ by reflexivity and $\mathsf{fp}(f) = \mathsf{prefp}(f) \cap \mathsf{postfp}(f)$ by antisymmetry
- In general, these sets can be empty:

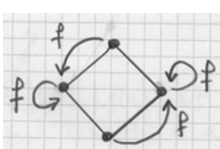


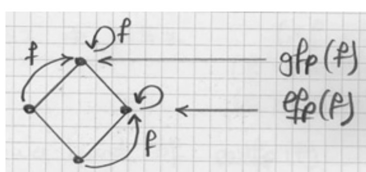
a and b not comparable for $=$

Extreme (least/greatest) fixpoints

A fixpoint x of an operator $f \in L \mapsto L$ on a poset $\langle L, \sqsubseteq \rangle$ is:

- The least fixpoint of f iff $\forall y \in L : (f(y) = y) \Longrightarrow (x \sqsubseteq y)$
- Dually, the greatest fixpoint of f iff $\forall y \in L : (f(y) = y) \Longrightarrow (x \sqsupseteq y)$





Notations for extreme (least/greatest) fixpoints

- $\mathsf{lfp}\,(f)$ least fixpoint (if any)
  - $f(\mathsf{lfp}\, f) = \mathsf{lfp}\, f$
  - $\forall x \in L : (f(x) = x) \Longrightarrow (\mathsf{lfp}\, f \sqsubseteq x)$
- $\mathsf{gfp}\, f$ greatest fixpoint (if any)
  - $f(\mathsf{gfp}\, f) = \mathsf{gfp}\, f$
  - $\forall x \in L : (f(x) = x) \Longrightarrow (\mathsf{gfp}\, f \sqsupseteq x)$

If the order $\sqsubseteq$ is not clear from the context, we write $\mathsf{lfp}^{\sqsubseteq}\, f$ and $\mathsf{gfp}^{\sqsubseteq}\, f$ to make it explicit.

Iterates

Iterates of an operator on a set

- Let f be an operator on a set L. The iterates of f from $a \in L$ are:

$$f^0(a) = a$$
$$f^{n+1}(a) = f(f^n(a)) \quad n \in \mathbb{N}$$

so that $f^n = \underbrace{f \circ f \circ \ldots \circ f}_{n \text{ times}}$. We have (by recurrence):

$$f^{n+1} = f^n \circ f$$
$$f^n \circ f^m = f^{n+m}$$
$$(f^n)^m = f^{n \times m}$$

Computation of the iterates

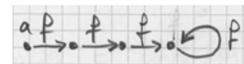
- Since

$$f^{2n} = (f^n)^2$$
$$f^{2n+1} = f \circ (f^n)^2$$

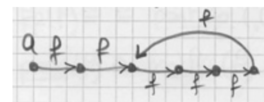
we can compute f^n in time $\mathcal{O}(\ln\ n)$ PROVIDED f^n can be computed in the same time as f (which is often not the case except in few cases like functions represented by polynomials or BDDs which can be composed symbollically before doing the computation)

Iterates of an operator on a finite set

- Let $\langle f^n(a),\ n \in \mathbb{N}\rangle$ be the iterates[1] of $f \in L \mapsto L$
- If L is finite of cardinality $|L| < \aleph_0$, we have $\forall k > |L| : \exists n \leq |L| : f^k(a) = f^n(a)$ and so
  - either the iterates reach a fixpoint:



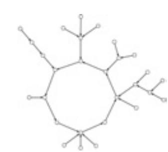
  - or they reach a cycle:



[1] also called "orbit".

Basin of attraction

- All iterates ending in the same cycle are called a basin of attraction



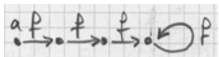
- The relation $x \equiv y \iff \exists i, j \in \mathbb{N} : f^i(x) = f^j(y)$ is an equivalence[2]. Each class contains exactly one cycle (including the particular case of fixpoints). And so the set L is partitionned into disjoint basins of attraction.

[2] For transitivity, if $f^i(x) = f^j(y)$ and $f^k(y) = f^\ell(z)$ and e.g. $j \leq k$ then $f^{i+d} = f^{j+d} = f^k(y) = f^\ell(z)$ where $d = j - k \geq 0$

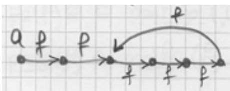
Iterates of an operator on an infinite set

If L is infinite of cardinality $|L| \geq \aleph_0$, we have three possibilities

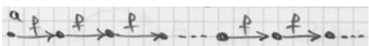
– either the iterates reach a fixpoint:



– or they reach a cycle:



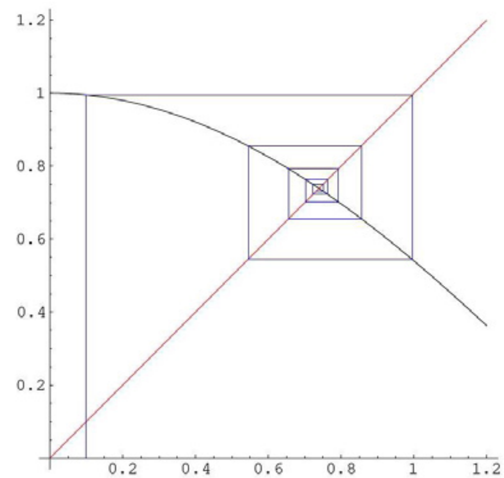
– or the iteration is infinite:



Fixpoint Examples

Fixpoint example 1: Numerical fixpoint

– Example of iterates converging to a fixpoint $\cos x = x$



Fixpoint example 2: Equivalence relation

Fixpoint example 3: Grammar semantics

Example of fixpoint definition: equivalence relations

Let S be a set. We have the complete lattice of relations $\langle \wp(S \times S), \subseteq, \emptyset, S \times S, \cup, \cap \rangle$. Given $r \subseteq S \times S$, let $f(r) = \lambda x \cdot 1_S \cup r \cup x^{-1} \cup x \circ x$. $f(r)$ is monotonic. Its least fixpoint $\mathsf{lfp}_{\emptyset}^{\subseteq} f(r)$ is the least equivalence relation including r. The map $\mathcal{E} \stackrel{\text{def}}{=} \lambda r \cdot \mathsf{lfp}_{\emptyset}^{\subseteq} f(r)$ is an upper closure operator which fixpoints are exactly the equivalence relations on $S \times S$, which by Ward's theorem is therefore a complete lattice $\langle \mathcal{E}(\wp(S \times S)), \subseteq, 1_S, S \times S, \lambda X \cdot \mathcal{E}(\cup X)$ [3], $\cap \rangle$.

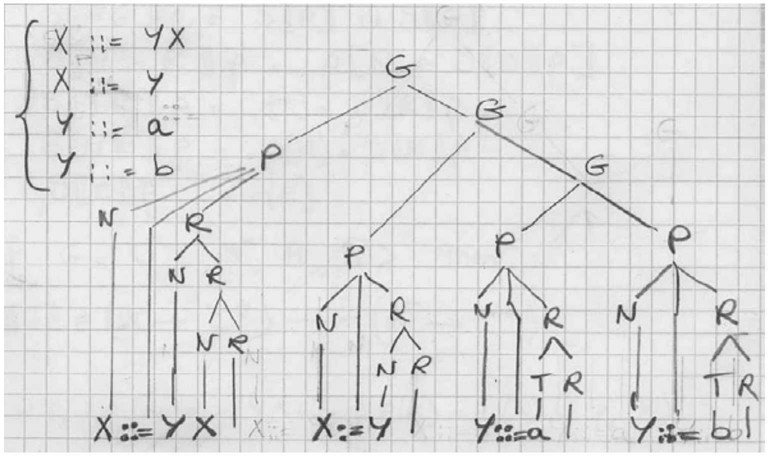
[3] The union of equivalence relations need not be an equivalence relation, but the transitive closure of a union of equivalence relations is an equivalence relation, indeed the least.

Example of fixpoint definition: semantics of context free grammars

The meta syntax of grammars is:

T	Terminals $T \in \mathcal{T}$
N	Nonterminals $N \in \mathcal{N}$
ε	Empty
$G ::= P \mid PG$	Grammar
$P ::= N$ '::=' R	Production/rule $P \in \mathcal{P}$
$R ::= TR \mid NR \mid \varepsilon$	righthand side

Example of meta derivation



Example of grammar semantics

Let $\ell(X)$ be the language generated by the nonterminal X in grammar G. The Rice-Ginsburgh/Schützenberger equations:

$$\begin{aligned} \ell(X) &= \ell(Y) \cdot \ell(X) \cup \ell(Y) \\ \ell(Y) &= \{a\} \cup \{b\} \end{aligned}$$

(where the concatenation of languages is $\mathcal{X} \cdot \mathcal{Y} = \{\sigma\sigma' \mid \sigma \in \mathcal{X} \wedge \sigma' \in \mathcal{Y}\}$) have a least fixpoint which associate the language generated by the grammar to each nonterminal $\ell = \{X \rightarrow (a|b)^+, Y \rightarrow a|b\}$.

The above equations have exactly the same least fixpoint as:

$$\begin{aligned} \ell(X) &= \ell(Y) \cdot \ell(X) \cup \ell(Y) \cup \ell(X) \\ \ell(Y) &= \{a\} \cup \{b\} \cup \ell(Y) \end{aligned}$$

The equations can be rewritten as:

$$\begin{aligned} \ell = {} & \ell[X := \ell(Y) \cdot \ell(X)] \,\dot\cup\, \ell[X := \ell(Y)] \,\dot\cup\, \ell[X := \ell(X)] \\ & \dot\cup\, \ell[Y := \{a\}] \,\dot\cup\, \ell[Y := \{b\}] \,\dot\cup\, \ell[Y := \ell(Y)] \end{aligned}$$

that is

$$\ell = F(\ell)$$

where

$$\begin{aligned} F(\ell) = {} & \ell[X := \ell(Y) \cdot \ell(X)] \,\dot\cup\, \ell[X := \ell(Y)] \,\dot\cup\, \ell[X := \ell(X)] \\ & \dot\cup\, \ell[Y := \{a\}] \,\dot\cup\, \ell[Y := \{b\}] \,\dot\cup\, \ell[Y := \ell(Y)] \end{aligned}$$

The operator $F = \mathcal{S}[\![G]\!]$ associated to a grammar G can be defined by structural induction on the metagrammar.

Structural definition of the grammar semantics

Given a grammar $G = \langle \mathcal{T}, \mathcal{N}, A, \mathcal{P} \rangle$ with axiom $A \in \mathcal{N}$, define $\mathcal{S}[\![G]\!] \in (\mathcal{N} \mapsto \mathcal{T}^{\vec{*}}) \xrightarrow{\text{m}} (\mathcal{N} \mapsto \mathcal{T}^{\vec{*}})$ by

$$\begin{aligned} \mathcal{S}[\![PG]\!]\ell &= \mathcal{S}[\![P]\!]\ell \,\dot\cup\, \mathcal{S}[\![G]\!]\ell \\ \mathcal{S}[\![N \text{ `::=' } R]\!]\ell &= \ell[N := \mathcal{S}[\![R]\!]\ell] \\ \mathcal{S}[\![TR]\!]\ell &= \{T\} \cdot \mathcal{S}[\![R]\!]\ell \\ \mathcal{S}[\![NR]\!]\ell &= \ell(N) \cdot \mathcal{S}[\![R]\!]\ell \\ \mathcal{S}[\![\varepsilon]\!] &= \{\vec{\epsilon}\} \end{aligned}$$

The semantics of G is $(\mathsf{lfp}^{\dot\subseteq}_{\dot\emptyset}\, \mathcal{S}[\![G]\!])(A)$

Example

$$G = X ::= YX \quad X \text{ `::=' } Y \quad Y \text{ `::=' } a \quad Y \text{ `::=' } b$$

$$\begin{aligned}
& \mathcal{S}[\![X ::= YX \quad X \text{ `::=' } Y \quad Y \text{ `::=' } a \quad Y \text{ `::=' } b]\!]\ell \\
= \; & \mathcal{S}[\![X ::= YX]\!]\ell \mathbin{\dot\cup} \mathcal{S}[\![X \text{ `::=' } Y \quad Y \text{ `::=' } a \quad Y \text{ `::=' } b]\!]\ell \\
= \; & \mathcal{S}[\![X ::= YX]\!]\ell \mathbin{\dot\cup} \mathcal{S}[\![X \text{ `::=' } Y]\!]\ell \mathbin{\dot\cup} \mathcal{S}[\![Y \text{ `::=' } a \quad Y \text{ `::=' } b]\!]\ell \\
= \; & \mathcal{S}[\![X ::= YX]\!]\ell \mathbin{\dot\cup} \mathcal{S}[\![X \text{ `::=' } Y]\!]\ell \mathbin{\dot\cup} \mathcal{S}[\![Y \text{ `::=' } a]\!]\ell \mathbin{\dot\cup} \mathcal{S}[\![Y \text{ `::=' } b]\!]\ell \\
= \; & \ell[X := \mathcal{S}[\![YX]\!]\ell] \mathbin{\dot\cup} \ell[X := \mathcal{S}[\![Y]\!]\ell] \mathbin{\dot\cup} \ell[Y := \mathcal{S}[\![a]\!]\ell] \mathbin{\dot\cup} \ell[Y := \mathcal{S}[\![b]\!]\ell] \\
= \; & \ell[X := \mathcal{S}[\![YX]\!]\ell \mathbin{\dot\cup} \mathcal{S}[\![Y]\!]\ell] \mathbin{\dot\cup} \ell[Y := \mathcal{S}[\![a]\!]\ell \mathbin{\dot\cup} \mathcal{S}[\![b]\!]\ell] \\
= \; & \ell[X := \ell(Y) \cdot \mathcal{S}[\![X]\!]\ell \mathbin{\dot\cup} \mathcal{S}[\![Y]\!]\ell] \mathbin{\dot\cup} \ell[Y := \mathcal{S}[\![a]\!]\ell \mathbin{\dot\cup} \mathcal{S}[\![b]\!]\ell] \\
= \; & \ell[X := \ell(Y) \cdot \ell(X) \cdot \mathcal{S}[\![\varepsilon]\!]\ell \mathbin{\dot\cup} \ell(Y) \cdot \mathcal{S}[\![\varepsilon]\!]\ell] \mathbin{\dot\cup} \ell[Y := \{a\} \cdot \mathcal{S}[\![\varepsilon]\!]\ell \mathbin{\dot\cup} \{b\} \cdot \mathcal{S}[\![\varepsilon]\!]\ell] \\
= \; & \ell[X := \ell(Y) \cdot \ell(X) \cdot \{\vec\epsilon\} \mathbin{\dot\cup} \ell(Y) \cdot \{\vec\epsilon\}] \mathbin{\dot\cup} \ell[Y := \{a\} \cdot \{\vec\epsilon\} \mathbin{\dot\cup} \{b\} \cdot \{\vec\epsilon\}] \\
= \; & \ell[X := \ell(Y) \cdot \ell(X) \cup \ell(Y)] \cup \ell[Y := \{a\} \mathbin{\dot\cup} \{b\}]
\end{aligned}$$

so that the equation

$$\ell = \mathcal{S}[\![G]\!]\ell$$

is

$$\begin{cases} \ell(X) = \ell(Y) \cdot \ell(X) \cup \ell(Y) \cup \ell(X) \\ \ell(Y) = \{a\} \cup \{b\} \cup \ell(Y) \\ \ell(Z) = \ell(Z) & \text{when } Z \notin \{X, Y\} \end{cases}$$

Iterative resolution of the equations

$$\begin{cases} \mathcal{X} = \mathcal{Y} \cdot \mathcal{X} \cup \mathcal{Y}) \cup \mathcal{X} \\ \mathcal{Y} = \{a\} \cup \{b\} \cup \mathcal{Y} \\ \mathcal{Z} = \mathcal{Z} & \text{when } Z \notin \{X, Y\} \end{cases}$$

- $\mathcal{X}^0 = \mathcal{Y}^0 = \mathcal{Z}^0 = \emptyset$
- $\mathcal{X}^1 = \emptyset$, $\mathcal{Y}^1 = \{a, b\}$, $\mathcal{Z}^1 = \emptyset$
- $\mathcal{X}^2 = \{a, b\}$, $\mathcal{Y}^2 = \{a, b\}$, $\mathcal{Z}^2 = \emptyset$
- $\mathcal{X}^3 = \{a, b\} \cdot \{a, b\} \cup \{a, b\} \cup \{a, b\} = \{aa, ab, ba, bb, a, b\} = \bigcup_{i=1}^{2} (a|b)^i$
- ...
- $\mathcal{X}^n = \bigcup_{i=1}^{n-1} (a|b)^i$ induction hypothesis
- $$\begin{aligned} \mathcal{X}^{n+1} &= \mathcal{X}^n \cdot \mathcal{Y}^n \cup \mathcal{Y}^n \cup \mathcal{X}^n \\ &= \bigcup_{i=1}^{n-1} (a|b)^i \cdot (a|b)^1 \cup (a|b)^1 \cup \bigcup_{i=1}^{n-1} (a|b)^i \\ &= \bigcup_{i=1}^{n-1} (a|b)^{i+1} \cup \bigcup_{i=1}^{n-1} (a|b)^i \\ &= \bigcup_{j=2}^{n} (a|b)^j \cup \bigcup_{i=1}^{n-1} (a|b)^i & j = i + 1 \\ &= \bigcup_{j=1}^{n} (a|b)^j \end{aligned}$$

- ...
- $\mathcal{X}^\omega = \bigcup_{n<\omega} \mathcal{X}^n = \bigcup_{2 \le n < \omega} \bigcup_{i=1}^{n-1} (a|b)^i \bigcup_{n<\omega} \bigcup_{i=1}^{n-1} (a|b)^i = \bigcup_{n \ge 1} (a|b)^n = (a|b)^+$
- $$\begin{aligned} \mathcal{X}^{\omega+1} &= \mathcal{X}^\omega \cdot \mathcal{Y}^\omega \cup \mathcal{Y}^\omega \cup \mathcal{X}^\omega \\ &= (a|b)^+ \cdot (a|b) \cup (a|b) \cup (a|b)^+ = (a|b)^+ = \mathcal{X}^\omega \end{aligned}$$

  so $\mathsf{lfp}^{\dot\subseteq}_{\dot\emptyset}\, \mathcal{S}[\![G]\!] = \{X \to (a|b)^+, Y \to (A|b)\}$ whence for the axiom $\mathsf{lfp}^{\dot\subseteq}_{\dot\emptyset}\, \mathcal{S}[\![G]\!](X) = (a|b)^+$.

Fixpoint example 4: Lattice of closure operators

The complete lattice of monotone operators on a complete lattice

Let $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ be a complete lattice and define

$$\mathsf{mon} \stackrel{\text{def}}{=} \lambda f \cdot \lambda x \cdot \bigsqcup\{f(y) \mid y \sqsubseteq x\}$$

LEMMA. Given $f \in L \mapsto L$, $\mathsf{mon}(f)$ is the least monotone operator $\sqsubseteq$-greater than of equal to f ■

PROOF. – Given $a, b \in L$ such that $a \sqsubseteq b$, we have $y \sqsubseteq b$ implies $a \sqsubseteq y$ so $\{f(y) \mid y \sqsubseteq a\} \subseteq \{f(y) \mid y \sqsubseteq b\}$ proving $\mathsf{mon}(f)a \subseteq \mathsf{mon}(f)b$ so $\mathsf{mon}(f)$ is monotone.

– Observe that $x \subseteq x$ so $f(x) \in \{f(y) \mid y \sqsubseteq x\}$ proving that $f \mathrel{\dot\sqsubseteq} \mathsf{mon}(f)$.

– Let $g \in L \stackrel{\text{m}}{\longmapsto} L$ be such that $f \mathrel{\dot\sqsubseteq} g$. We have $\forall y \in L : f(y) \sqsubseteq g(y)$ so that $\forall a \in L : \mathsf{mon}(f)(a) = \bigsqcup\{f(y) \mid y \sqsubseteq a\} \sqsubseteq \bigsqcup\{g(y) \mid y \sqsubseteq a\} \sqsubseteq \bigsqcup\{g(y) \mid g(y) \sqsubseteq g(a)\} \sqsubseteq g(a)$ proving that $\mathsf{mon}(f) \mathrel{\dot\sqsubseteq} g$

– We conclude that $\mathsf{mon}(f) \in L \stackrel{\text{m}}{\longmapsto} L$ and if $f \mathrel{\dot\sqsubseteq} g \in L \stackrel{\text{m}}{\longmapsto} L$ then $\mathsf{mon}(f) \mathrel{\dot\sqsubseteq} g$.

□

THEOREM. The set $L \stackrel{\text{m}}{\longmapsto} L$ of monotone maps on a complete lattice $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ is a complete lattice $\langle L \stackrel{\text{m}}{\longmapsto} L, \dot\sqsubseteq, \dot\bot, \dot\top, \dot\sqcup, \dot\sqcap\rangle$ ■

PROOF. Observe that mon is an upper closure operator and $L \stackrel{\text{m}}{\longmapsto} L = \mathsf{mon}(L \mapsto L)$. By Ward theorem, $\langle L \stackrel{\text{m}}{\longmapsto} L, \dot\sqsubseteq, \mathsf{mon}(\dot\bot), \dot\top, \lambda S \cdot \mathsf{mon}(\dot\sqcup S), \dot\sqcap\rangle$ is a complete lattice. By duality, we can define

$$\mathsf{mon}' \stackrel{\text{def}}{=} \lambda f \cdot \lambda x \cdot \bigsqcap\{f(y) \mid y \sqsupseteq x\}$$

so that mon' is a lower closure operator and $L \stackrel{\text{m}}{\longmapsto} L = \mathsf{mon}'(L \mapsto L)$. By the dual of Ward theorem, $\langle L \stackrel{\text{m}}{\longmapsto} L, \dot\sqsubseteq, \dot\bot, \mathsf{mon}'(\dot\top), \dot\sqcup, \lambda S \cdot \mathsf{mon}(\dot\sqcap S)\rangle$ is a complete lattice. Combining the two results, we get $\mathsf{mon}(\dot\bot) = \dot\bot$ and $\lambda S \cdot \mathsf{mon}(\dot\sqcap S) = \dot\sqcap$ whence the complete lattice $\langle L \stackrel{\text{m}}{\longmapsto} L, \dot\sqsubseteq, \dot\bot, \dot\top, \dot\sqcup, \dot\sqcap\rangle$. □

The complete lattice of extensive operators on a complete lattice

THEOREM. Let $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ be a complete lattice. Define $\mathsf{ext} \stackrel{\text{def}}{=} \lambda f \cdot \lambda x \cdot x \sqcup f(x)$. Then $\mathsf{ext}(f)$ is the least extensive operator greater than of equal to $f \in L \mapsto L$. ext is an upper closure operator. The set $\langle \mathsf{ext}(L \mapsto L), \dot\sqsubseteq, \lambda x \cdot x, \dot\top, \dot\sqcup, \dot\sqcap\rangle$ is the complete latttice of extensive operators on L. ■

PROOF. – An operator f on L is extensive iff $\mathsf{ext}(f) = f$.

– If $f \mathrel{\dot\sqsubseteq} g$ and g is extensive then $\mathsf{ext}(f) = \lambda x \cdot x \sqcup f(x) \mathrel{\dot\sqsubseteq} \lambda x \cdot x \sqcup g(x) = g$.

– So $\langle \mathsf{ext}(L \mapsto L), \dot\sqsubseteq, \mathsf{ext}(\dot\bot), \dot\top, \lambda S \cdot \mathsf{ext}(\dot\sqcup S), \dot\sqcap\rangle$ is a complete lattice by Ward's theorem.

– But $\mathrm{ext}(\dot{\bot}) = \lambda x \cdot x$ and if $S \subseteq \mathrm{ext}(L \mapsto L)$ is a set of extensive opeartors on L then $\forall x \in L : x \sqsubseteq f(x)$ so $x \sqsubseteq \bigsqcup_{f \in S} f(x) = (\dot{\bigsqcup} S)(x)$ proving $\dot{\bigsqcup} S$ to be extensive so $\lambda S \cdot \mathrm{ext}(\dot{\sqcup} S) = \lambda S \cdot \dot{\bigsqcup} S = \dot{\bigsqcup}$.

□

Fixpoint definition of the closure operators on a complete lattice

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

$$\mathrm{uclo} \stackrel{\mathrm{def}}{=} \lambda f \cdot \lambda x \cdot \mathsf{lfp}\,(\lambda y \cdot x \sqcup \mathrm{mon}(f)(y))$$

Then $\mathrm{uclo}(f)$ is the least upper closure operator greater than of equal to $f \in L \mapsto L$. ■

PROOF. – Given $f \in L \mapsto L$, $\mathrm{mon}(f)$ is monotone and so is $\lambda y \cdot x \sqcup \mathrm{mon}(f)(y)$ so that by Knaster-Tarski fixpoint theorem (on page 39), $\mathsf{lfp}\,(\lambda y \cdot x \sqcup \mathrm{mon}(f)(y))$ exists for all $x \in L$ and so uclo is well defined.

– If $x_1 \sqsubseteq x_2$ then $\lambda y \cdot x_1 \sqcup \mathrm{mon}(f)(y) \sqsubseteq \lambda y \cdot x_2 \sqcup \mathrm{mon}(f)(y)$ so that, by the fispoint comparison theorem (on page 73), we have $\mathrm{uclo}(f)(x_1) = \mathsf{lfp}\,(\lambda y \cdot x_1 \sqcup \mathrm{mon}(f)(y)) \sqsubseteq \mathsf{lfp}\,(\lambda y \cdot x_2 \sqcup \mathrm{mon}(f)(y)) = \mathrm{uclo}(f)(x_2)$ proving $\mathrm{uclo}(f)$ to be monotonic.

– We have $\mathrm{uclo}(f)(x) = \mathsf{lfp}\,(\lambda y \cdot x \sqcup \mathrm{mon}(f)(y))$ so $\mathrm{uclo}(f)(x) = x \sqcup \mathrm{mon}(f)(\mathrm{uclo}(f)(x))) \sqsupseteq x$, proving $\mathrm{uclo}(f)$ to be extensive.

– We have $x \sqsubseteq \mathrm{uclo}(f)(x)$ so $\mathrm{mon}(f)(x) \sqsubseteq \mathrm{mon}(f)(\mathrm{uclo}(f)(x))$ by monotony. Hence $\mathrm{mon}(f)(x) \sqsubseteq \mathrm{uclo}(f)(x)$ since $\mathrm{uclo}(f)(x) = \mathsf{lfp}\,(\lambda y \cdot x \sqcup \mathrm{mon}(f)(y))$.

For idempotency, $\mathrm{uclo}(f)(\mathrm{uclo}(f)(x)) = \mathsf{lfp}\,(\lambda y \cdot \mathrm{uclo}(f)(x) \sqcup \mathrm{mon}(f)(y))$.

The iterates are

$$\begin{aligned}
y^0 &= \bot \\
y^1 &= \mathrm{uclo}(f)(x) \sqcup \mathrm{mon}(f)(\bot)) \\
&= \mathrm{uclo}(f)(x) \quad \wr\text{since } \mathrm{uclo}(f)(x) \sqsupseteq \mathrm{mon}(f)(x) \sqsupseteq \mathrm{mon}(f)(\bot)\text{, by monotoony.}\wr \\
y^2 &= \mathrm{uclo}(f)(x) \sqcup \mathrm{mon}(f)(\mathrm{uclo}(f)(x))) \\
&= \mathrm{uclo}(f)(x) \sqcup \mathrm{uclo}(f)(x) \qquad \wr\text{since } \mathrm{uclo}(f)(x) \text{ is monotonic}\wr \\
&= \mathrm{uclo}(f)(x)
\end{aligned}$$

which is the limit of the iteration sequence.

– We have proved $\mathrm{uclo}(f) \mathrel{\dot{\sqsubseteq}} \mathrm{mon}(f) \mathrel{\dot{\sqsubseteq}} f$ so that $\mathrm{uclo}(f)$ is pointwise greater than of equal to f.

– If $f \mathrel{\dot{\sqsubseteq}} g$ then $\lambda y \cdot x \sqcup \mathrm{mon}(f)(y) \mathrel{\dot{\sqsubseteq}} \lambda y \cdot x \sqcup \mathrm{mon}(g)(y)$ so $\mathsf{lfp}\,(\lambda y \cdot x \sqcup \mathrm{mon}(f)(y)) \mathrel{\dot{\sqsubseteq}} \mathsf{lfp}\,(\lambda y \cdot x \sqcup \mathrm{mon}(f)(y))$ by forthcoming fixpoint comparison theorem (on page 73) proving that $\mathrm{uclo}(f) \mathrel{\dot{\sqsubseteq}} \mathrm{uclo}(g)$ whence that uclo is monotonic

– Let ρ be a closure operator. We have $\mathrm{uclo}(\rho)(x) = \mathsf{lfp}\,(\lambda y \cdot x \sqcup \mathrm{mon}(\rho)(y)) = \mathsf{lfp}\,(\lambda y \cdot x \sqcup \rho(y))$ since ρ is monotone. Let us compute the transfinite iterates

$$\begin{aligned}
y^0 &= \bot \\
y^1 &= x \sqcup \rho(\bot) \\
&\sqsubseteq \rho(x) \qquad \wr\text{since } \bot \sqsubseteq x \text{ so } \rho(\bot) \sqsubseteq \rho(x) \text{ by monotony and } x \sqcup \rho(\bot) \sqsubseteq \rho(x) \sqcup \rho(\bot) = \rho(x)\wr \\
y^\delta &\sqsubseteq \rho(x) \qquad \wr\text{induction hyppthesis}\wr \\
y^{\delta+1} &= x \sqcup \rho(y^\delta) \\
&\sqsubseteq x \sqcup \rho(\rho(x)) \qquad \wr\text{by monotony}\wr
\end{aligned}$$

$$= x \sqcup \rho(x) \quad \text{(by idempotency)}$$
$$= \rho(x) \quad \text{(by extensivity)}$$

If λ is a limit ordinal and $\forall \beta < \lambda : y^\beta \sqsubseteq \rho(x)$ then $y^\lambda = \bigsqcup_{\beta<\lambda} y^\beta \sqsubseteq \rho(x)$. By transfinite induction all iterates are upper bounded by $\rho(x)$ whence so is the least fixpoint $\mathsf{lfp}\,(\lambda y \cdot x \sqcup \mathsf{mon}(f)(y))$ which is one of these transfinite iterates (by forthcoming constructive fixpoint theorem. We conclude that $\mathsf{uclo}(f)(x) \sqsubseteq \rho(x)$.

- Finally, given a closure operator ρ greater that or equal to f, we have $f \mathrel{\dot\sqsubseteq} \rho$ which implies by monotony $\mathsf{uclo}(f) \mathrel{\dot\sqsubseteq} \mathsf{uclo}(\rho) = \rho$ so that $\mathsf{uclo}(f)$ is the <u>least</u> upper closure operator greater than or equal to f.

□

Corollary. The set $\mathsf{uclo}(L \mapsto L)$ of upper closure operator on a complete lattice $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ is a complete lattice $\langle \mathsf{uclo}(L \mapsto L), \mathrel{\dot\sqsubseteq}, \lambda x \cdot x, \dot\top, \lambda S \cdot \mathsf{uclo}(\dot\bigsqcup S), \dot\sqcap\rangle$ ■

Proof. By Ward's theorem. □

Fixpoint theorems

Knaster-Tarski fixpoint theorem for monotone operators on a complete lattice

Theorem. A monotonic map $\varphi \in L \mapsto L$ on a complete lattice:

$$\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$$

has a least fixpoint:

$$\begin{aligned} \mathsf{lfp}\,\varphi &= \sqcap \mathsf{postfp}(\varphi), \\ &= \sqcap\{x \in L \mid \varphi(x) \sqsubseteq x\} \end{aligned} \tag{1}$$

and, dually, a greatest fixpoint:

$$\begin{aligned} \mathsf{gfp}\,\varphi &= \sqcup\,\mathsf{prefp}\,\varphi, \\ &= \sqcup\{x \in L \mid x \sqsubseteq \varphi(x)\} \end{aligned} \tag{2}$$

■

Reference

[2] A. Tarski. A lattice theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5:285–310, 1955.

Proof. – Let $a = \sqcap P$ and $P = \mathsf{postfp}(\varphi) = \{x \in L \mid \varphi(x) \sqsubseteq x\}$.

- For all $x \in P$, we have:
  - $a \sqsubseteq x$ [a glb of P]
  - $\varphi(a) \sqsubseteq \varphi(x)$ [φ monotonic]
  - $\varphi(a) \sqsubseteq x$ [def. P and transitivity]

  whence $\varphi(a)$ is a lower bound of P.
- $\varphi(a) \sqsubseteq a$ [$\varphi(a)$ lower bound of P and a glb of P]
  $\Longrightarrow \varphi(\varphi(a)) \sqsubseteq \varphi(a)$ [φ monotonic]
  $\Longrightarrow \varphi(a) \in P$ [def. P]
  $\Longrightarrow a \sqsubseteq \varphi(a)$ [a lower bound of P]
  $\Longrightarrow \varphi(a) = a$ [antisymmetry]
- If $\varphi(x) = x$ then $x \in P$ whence $a \sqsubseteq x$ since a is the greatest lower bound of P.
- $\mathsf{gfp}\,\varphi = \sqcup\,\mathsf{prefp}\,\varphi$ by duality (replacing $\sqsubseteq, \bot, \top, \sqcup, \sqcap$ respectively by $\sqsupseteq, \top, \bot, \sqcap, \sqcup$ in the above proof).

□

THEOREM. The set of fixpoints of a monotone operator $f \in L \overset{m}{\longmapsto} L$ on a complete lattice $\langle L, \sqsubseteq, \perp, \top, \sqcup, \sqcap \rangle$ is a complete lattice. ■

PROOF. – We know that $\mathsf{fp}(f)$ is not empty.

- Let $X \subseteq \mathsf{fp}(f)$
  - The interval $L' = [\bigsqcup X, \top]$ is a complete lattice
  - Let $a = \mathbf{lfp}\, f|_{L'}$ be the least fixpoint of f restricted to L'
  - We have
    1. $a \in \mathsf{fp}(f)$
    2. $\forall x \in X : x \sqsubseteq \sqcup X \sqsubseteq a$ since $\bigsqcup X$ is the infimum of L'
    3. if $y \in \mathsf{fp}(f)$ is such that $\forall x \in X : x \sqsubseteq y$, we have $\bigsqcup X \sqsubseteq y$ so $y \in L'$ proving that $a \sqsubseteq y$

Reference

[3] A. Tarski. A lattice theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5:285–310, 1955.

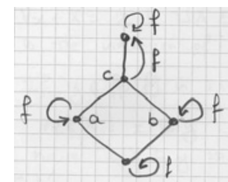
- It follows that a is the lub of $X \subseteq \mathsf{fp}(f)$ in $\mathsf{fp}(f)$ for $\sqsubseteq$ proving that $\langle \mathsf{fp}(f), \sqsubseteq \rangle$ is a complete lattice.

□

– The fixpoint can be unique:

but in general there are many.

– In general, the set of fixpoints is not a sublattice of L. A counter example is



a and b are fixpoints of f but $c = a \sqcup b$ is not.

Reflexive/strict transitive closure of a binary relation on a set (remainder from lecture 4)

Let S be a set and $r, r_1, r_2 \subseteq S \times S$ be relations on S:

- $r_1 \circ r_2 \stackrel{\text{def}}{=} \{\langle x,\ z\rangle \mid \exists y : x\ r_1\ y \wedge y\ r_2\ z\}$ composition
- $1_S \stackrel{\text{def}}{=} \{\langle x,\ x\rangle \mid x \in S\}$ identity
- $r^0 \stackrel{\text{def}}{=} \mathbf{1}_S$ powers
- $r^{n+1} \stackrel{\text{def}}{=} r^n \circ r\ (= r \circ r^n)$
- $r^\star \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}} r^n$ reflexive transitive closure
- $r^+ \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}\setminus\{0\}} r^n$ strict transitive closure

so $r^\star = r^+ \cup \mathbf{1}_S$

Least fixpoint definition of the reflexive/strict transitive closure

THEOREM.

$$r^\star = \mathsf{lfp}^{\subseteq}\, \lambda X \cdot 1_S \cup X \circ r$$
$$r^+ = \mathsf{lfp}^{\subseteq}\, \lambda X \cdot r \circ (1_S \cup X)$$

■

PROOF. – $\langle \wp(S \times S), \subseteq, \emptyset, S, \cup, \cap\rangle$ is a complete lattice

– $\lambda X \cdot 1_S \cup X \circ r$ is monotone since

$$\begin{aligned} & X \subseteq Y \\ \Longrightarrow\ & X \circ r \subseteq Y \circ r \\ \Longrightarrow\ & 1_S \cup X \circ r \subseteq 1_S \cup Y \circ r \end{aligned}$$

– $\lambda X \cdot r \circ (1_S \cup X)$ is monotone since

$$\begin{aligned} & X \subseteq Y \\ \Longrightarrow\ & (1_S \cup X) \subseteq (1_S \cup Y) \\ \Longrightarrow\ & r \circ (1_S \cup X) \subseteq r \circ (1_S \cup Y) \end{aligned}$$

– The existence of the fixpoints follows from Knaster-Tarski theorem

– We have $r^\star = \bigcup_{n\in\mathbb{N}} r^n = r^0 \cup \bigcup_{n>0} r^n = r^0 \cup \bigcup_{n\geq 0} r^{n+1} = r^0 \cup \bigcup_{n\geq 0}(r \circ r^n) = r^0 \cup r \circ (\bigcup_{n\geq 0} r^n) = 1_S \cup r \circ r^\star$ so that $r^\star$ is a fixpoint of $\lambda X \cdot 1_S \cup X$. Let R be another fixpoint that is $R = 1_S \cup X \circ R$. We have $r^0 = 1_S \subseteq = 1_S \cup X \circ R = R$. Assume by induction hypothesis that $r^n \subseteq R$ then $r^{n+1} = r \circ r^n \subseteq r \circ R \subseteq 1_S \cup X \circ R = R$. By recurrence, $\forall n : r^n \subseteq R$ proving $r^\star = \bigcup_{n\in\mathbb{N}} r^n \subseteq R$ to be the least fixpoint.

– The proof is similar for r^+

□

Least fixpoint definition of the lefthand side restriction of the reflexive/strict transitive closure

Let S be a set, $r \subseteq S \times S$ be a relation on S, and $E, F \subseteq S$. We define

$$E \upharpoonleft r \stackrel{\text{def}}{=} \{\langle x,\, y\rangle \in r \mid x \in E\} \quad \text{left restriction}$$
$$r \upharpoonright F \stackrel{\text{def}}{=} \{\langle x,\, y\rangle \in r \mid y \in F\} \quad \text{right restriction}$$

We have

THEOREM.

$$E \upharpoonleft r^\star = \mathsf{lfp}^{\subseteq}\, \lambda X \cdot E \upharpoonleft 1_S \cup X \circ r$$
$$r^\star \upharpoonright F = \mathsf{lfp}^{\subseteq}\, \lambda X \cdot 1_S \upharpoonright F \cup X \circ r$$

■

PROOF.

$$\begin{aligned}
& r^\star = \lambda X \cdot 1_S \cup X \circ r \\
\Longrightarrow\ & r^\star = \bigcap\{X \mid 1_S \cup X \circ r \subseteq X\} && \text{Knaster-Tarski} \\
\Longrightarrow\ & E \upharpoonleft r^\star = E \upharpoonleft \bigcap\{X \mid 1_S \cup X \circ r \subseteq X\} \\
& = \bigcap\{E \upharpoonleft X \mid 1_S \cup X \circ r \subseteq X\} \\
& = \bigcap\{E \upharpoonleft X \mid E \upharpoonleft (1_S \cup X \circ r) \subseteq E \upharpoonleft X\} \\
& = \bigcap\{E \upharpoonleft X \mid E \upharpoonleft 1_S \cup (E \upharpoonleft X) \circ r \subseteq E \upharpoonleft X\} \\
& = \bigcap\{Y \mid (E \upharpoonleft 1_S) \cup Y \circ r \subseteq Y\} && \text{by letting } Y = (E \upharpoonleft X) \\
& = \mathsf{lfp}^{\subseteq}\, \lambda X \cdot E \upharpoonleft 1_S \cup X \circ r && \text{Knaster-Tarski}
\end{aligned}$$

The proof is similar for $r^\star \upharpoonright F$.

□

Banach's lemma

Theorem. Let A and B be two sets and suppose there exist two maps $f \in A \mapsto B$ and $g \in B \mapsto A$. Then there exist partitions $A = A_1 \cup A_2$ with $A_1 \cap A_2 = \emptyset$ and $B = B_1 \cup B_2$ with $B_1 \cap B_2 = \emptyset$ such that $f(A_1) = B_1$ and $g(B_2) = A_2$. ■

Proof. $\langle \wp(A),\ \subseteq,\ \emptyset,\ A,\ \cup,\ \cap\rangle$ is a complete lattice. Define $F(X) = A \setminus g(B \setminus f(X))$. If $X \subseteq Y$ then $f(X) = \{f(x) \mid x \in X\} \subseteq \{f(x) \mid x \in Y\} = f(Y)$ so $(B \setminus f(X)) \supseteq (B \setminus f(Y))$ so $g(B \setminus f(X)) \supseteq g(B \setminus f(Y))$ whence $(A \setminus g(B \setminus f(X))) \subseteq (A \setminus g(B \setminus f(X)))$, that is $F(X) \subseteq F(Y)$, proving F to be monotone. By Knaster-Tarski, we can define $A_1 = \mathsf{lfp}^{\subseteq}_{\emptyset} F$. Moreover define $A_2 = A \setminus A_1$, $B_1 = f(A_1)$ and $B_2 = B \setminus B_1$ so that we have partitions. It remains to prove that $g(B_2) = A_2$. Indeed $A \setminus g(B_2) = A \setminus g(B \setminus B_1) = A \setminus g(B \setminus f(A_1)) = F(A_1) = A_1$ by the fixpoint property. It follows that $g(B_2) = A \setminus (A \setminus g(B_2)) = A \setminus A_1 = A_2$ Q.E.D. □

The Cantor-Schröder-Bertein theorem

Corollary. Let A and B be two sets and suppose there exist injective maps $f \in A \rightarrowtail B$ and $g \in B \rightarrowtail A$. Then there exists a bijective map $h \in A \rightarrowtail\!\!\!\!\rightarrow B$ of X onto Y. ■

Proof. We apply Banach's lemma and by injectivity $|A_1| = |B_1|$ and $|A_2| = |B_2|$ so $|A| = |B|$. □

David Park upper fixpoint induction principle [4]

Theorem. Let $f \in L \xrightarrow{\text{m}} L$ on $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$.

$$\begin{aligned} & \mathsf{lfp}^{\sqsubseteq} f \sqsubseteq P \\ \iff\ & \exists I \in L : f(I) \sqsubseteq I \wedge I \sqsubseteq P \end{aligned}$$

■

Proof. ($\Leftarrow$) Soundness
If $f(I) \sqsubseteq I$ then $I \in \{X \in L \mid F(X) \sqsubseteq X\}$ so by Knaster-Tarski $\mathsf{lfp}^{\sqsubseteq} f = \bigsqcap\{X \in L \mid F(X) \sqsubseteq X\} \sqsubseteq I$, whence by $I \sqsubseteq P$ and transitivity, $\mathsf{lfp}^{\sqsubseteq} f \sqsubseteq P$

($\Rightarrow$) Relative completenesss
Assume $\mathsf{lfp}^{\sqsubseteq} f \sqsubseteq P$. Choose $I = \mathsf{lfp}^{\sqsubseteq} f$. Then $f(I) \sqsubseteq I$ by reflexivity and $I \sqsubseteq P$ by hypothesis and def. I.

□

[4] This induction principle is very important and underlies many safety proof methods (such as Floyd/Naur for partial correctness). By analogy, I is called an *invariant*.

Application to the relational forward deductive positive proof principle

Theorem.

$$\begin{aligned} & \forall \underline{s}, \overline{s} \in S : (\underline{s} \in E \wedge \langle \underline{s},\ \overline{s}\rangle \in t^{\star} \wedge \overline{s} \in F) \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in \Psi \\ \Leftrightarrow\ & \exists I : \forall \underline{s}, s', \overline{s} : \underline{s} \in E \Longrightarrow \langle \underline{s},\ \underline{s}\rangle \in I \\ & \wedge (\langle \underline{s},\ s'\rangle \in I \wedge \langle s',\ s''\rangle \in t) \Longrightarrow \langle \underline{s},\ s''\rangle \in I \\ & \wedge (\langle \underline{s},\ \overline{s}\rangle \in I \wedge \overline{s} \in F) \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in \Psi \end{aligned}$$

■

Proof.

$$\begin{aligned} & \forall \underline{s}, \overline{s} \in S : (\underline{s} \in E \wedge \langle \underline{s},\ \overline{s}\rangle \in t^{\star} \wedge \overline{s} \in F) \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in \Psi \\ \Longleftrightarrow\ & \forall \underline{s}, \overline{s} \in S : (\langle \underline{s} \in E \wedge \underline{s},\ \overline{s}\rangle \in t^{\star}) \Longrightarrow (\underline{s} \in F \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in \Psi) \end{aligned}$$

$$
\begin{aligned}
&\Longleftrightarrow E \upharpoonright t^\star \subseteq P \qquad \wr \text{where } P = \{\langle \underline{s},\ \overline{s}\rangle \in S^2 \mid (\overline{s} \in F) \Longrightarrow (\langle \underline{s},\ \overline{s}\rangle \in \Psi)\} \wr \\
&\Longleftrightarrow (\mathsf{lfp}^{\subseteq}\ \lambda X \cdot E \upharpoonright 1_S \cup X \circ t) \subseteq P \\
&\Longleftrightarrow \exists I \in L : (E \upharpoonright 1_S \cup I \circ t) \sqsubseteq I \wedge I \sqsubseteq P \\
&\Longleftrightarrow \exists I \in L : E \upharpoonright 1_S \sqsubseteq I \wedge I \circ t \sqsubseteq I \wedge I \sqsubseteq P \\
&\Longleftrightarrow \exists I \in L : \forall \underline{s}, \overline{s} \in S : [\underline{s} \in E \wedge \underline{s} = \overline{s} \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in I] \wedge [\exists s' : \langle \underline{s},\ s'\rangle \in \\
&\qquad I \wedge \langle s',\ \overline{s}\rangle \in t \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in I] \wedge [\langle \underline{s},\ \overline{s}\rangle \in I \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in P] \\
&\Longleftrightarrow \exists I : \forall \underline{s}, s', \overline{s} : [\underline{s} \in E \Longrightarrow \langle \underline{s},\ \underline{s}\rangle \in I] \wedge [(\langle \underline{s},\ s'\rangle \in I \wedge \langle s',\ \overline{s}\rangle \in t) \Longrightarrow \\
&\qquad \langle \underline{s},\ \overline{s}\rangle \in I] \wedge [(\langle \underline{s},\ \overline{s}\rangle \in I \wedge \overline{s} \in F) \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in \Psi]
\end{aligned}
$$

□

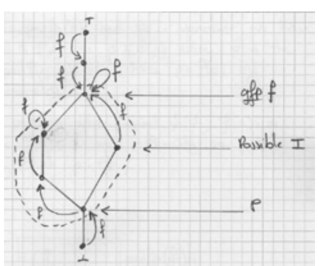
David Park lower fixpoint induction principle

THEOREM. Let $f \in L \xrightarrow{\mathrm{m}} L$ on $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$.

$$
\begin{aligned}
& P \sqsubseteq \mathsf{gfp}^{\sqsubseteq} f \\
\Longleftrightarrow\ & \exists I \in L : I \sqsubseteq f(I) \wedge P \sqsubseteq I
\end{aligned}
$$

■

PROOF. By duality.



A variant of the Knaster-Tarski fixpoint theorem for monotone operators on a poset

THEOREM. Let $f \in L \xrightarrow{\mathrm{m}} L$ be a monotone operator on a poset $\langle L,\ \sqsubseteq\rangle$ which possesses a least postfixpoint p:

$$f(p) \sqsubseteq p \wedge \forall x \in L : (f(x) \sqsubseteq x) \Longrightarrow (p \sqsubseteq x)$$

then

$$\mathsf{lfp}^{\sqsubseteq} f = p \wedge \forall x \in L : (f(x) \sqsubseteq x) \Longrightarrow (\mathsf{lfp}^{\sqsubseteq} f \sqsubseteq x)$$

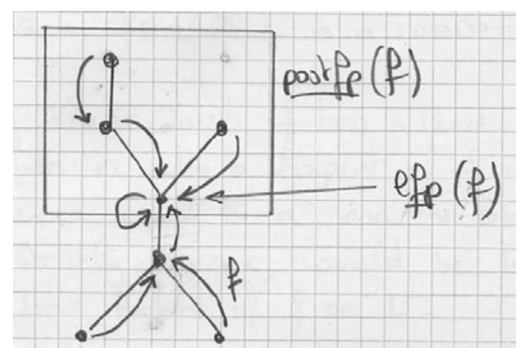
■

PROOF. – Since p postfp(f) and f is monotone, we hace $f(f(p)) \sqsubseteq f(p)$ so $p \sqsubseteq f(p)$ since p is the least postfixpoint of f, we get $f(p) = p$ by antisymmetry.

– Let x be any fixpoint of f. $f(x) = x$ implies $f(x) \sqsubseteq x$ by reflexivity so $p \sqsubseteq x$ proving that $p = \mathsf{lfp}^{\sqsubseteq} f$.

□

Example:



Least fixpoint of a monotone operator greater than or equal to a given prefixpoint

We write $\mathsf{lfp}^{\sqsubseteq}_a\, f$ for the $\sqsubseteq$-least fixpoint of $f \in L \mapsto L$ on the poset $\langle L,\ \sqsubseteq\rangle$ greater than or equal to a (if it ever exists):

- $a \sqsubseteq \mathsf{lfp}^{\sqsubseteq}_a\, f = f(\mathsf{lfp}^{\sqsubseteq}_a\, f)$
- $\forall x \in L : [a \sqsubseteq x = f(x)] \Longrightarrow [\mathsf{lfp}^{\sqsubseteq}_a\, f \sqsubseteq x]$

THEOREM. If $f \in L \overset{\mathrm{m}}{\longmapsto} L$ on $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ and $a \in \mathsf{prefp}(f)$ then $\mathsf{lfp}^{\sqsubseteq}_a\, f$ exists. ■

PROOF. – $L' \stackrel{\mathrm{def}}{=} [a, \top] \sqsubseteq L$ is a complete lattice and $f \in L' \overset{\mathrm{m}}{\longmapsto} L'$ since $x \in L' \Longrightarrow a \sqsubseteq x \Longrightarrow f(a) \sqsubseteq f(x) \Longrightarrow a \sqsubseteq f(x)$ since $a \sqsubseteq f(a)$. By Knaster-Tarki $\mathsf{lfp}^{\sqsubseteq}\, f|_{L'}$ exists on L' and is a fixpoint of $f \in L \mapsto L$ greater than or equal to a

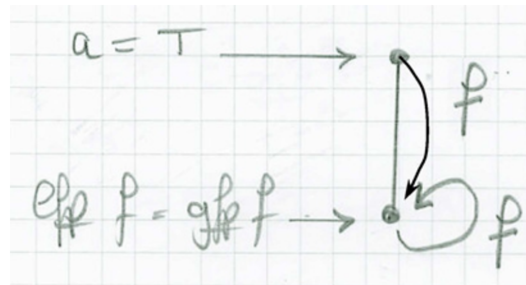
– It is the least since any other one x would have $a \sqsubseteq x = f(x) = f|_{L'}(x)$ would not be the least one of $f|_{L'}$ on L'.

□

COROLLARY. If $f \in L \overset{\mathrm{m}}{\longmapsto} L$ on $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ and $a \in \mathsf{prefp}(f)$ then $\mathsf{lfp}^{\sqsubseteq}_a\, f = \bigsqcap\{x \in L \mid a \sqsubseteq x \wedge f(x) \sqsubseteq x\}$. ■

PROOF. By Knaster-Tarski, $\mathsf{lfp}^{\sqsubseteq}_a\, f = \mathsf{lfp}^{\sqsubseteq}\, f|_{L'} = \bigsqcap\{x \in L' \mid f|_{L'}(x) \sqsubseteq x\} = \bigsqcap\{x \in L \mid a \sqsubseteq x \wedge f(x) \sqsubseteq x\}$. □

Taking $a = \bot$, we get the Knaster-Tarski classical result. Observe that if $a \not\sqsubseteq f(a)$ then $\mathsf{lfp}^{\sqsubseteq}_a\, f$ may not exist, as shown by the following counter-example:



David Park upper fixpoint induction principle revisited

THEOREM. If $f \in L \overset{\mathrm{m}}{\longmapsto} L$ on $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ and $a \in \mathsf{prefp}(f)$, $P \in L$ then

$$\begin{aligned} & \mathsf{lfp}^{\sqsubseteq}_a\, f \sqsubseteq P \\ \Longleftrightarrow\ & \exists I \in L : a \sqsubseteq I \wedge F(I) \sqsubseteq I \wedge I \sqsubseteq P. \end{aligned}$$

■

PROOF. by Park upper fixpoint induction principle on $L' = [a, \top]$. □

By duality,

THEOREM. If $f \in L \overset{m}{\longmapsto} L$ on $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ and $a \in \mathrm{postfp}(f)$, $P \in L$ then the greatest fixpoint of f less than or equal to a exists and is

$$\mathsf{gfp}^{\sqsubseteq}_a f = \bigsqcap\{x \in L \mid x \sqsubseteq f(x) \wedge x \sqsubseteq a\}$$

$$P \sqsubseteq \mathsf{gfp}^{\sqsubseteq}_a f \iff \exists I \in L : P \sqsubseteq I \wedge I \sqsubseteq F(I) \wedge I \sqsubseteq a$$

■

Characterization of the least fixpoint of a monotone operator greater than or equal to a given prefixpoint [5]

THEOREM. If $f \in L \overset{m}{\longmapsto} L$ on $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ and $a \in \mathrm{prefp}(f)$ then $\mathsf{lfp}^{\sqsubseteq}_a f = \mathsf{lfp}^{\sqsubseteq}_{\bot} \lambda x \cdot a \sqcup f(x)$. ■

PROOF. Let $A = \mathsf{lfp}^{\sqsubseteq}_a f$ and $B = \mathsf{lfp}^{\sqsubseteq}_{\bot} \lambda x \cdot a \sqcup f(x)$

1. $A = f(A)$ and $a \sqsubseteq A$ so $a \sqcup f(A) \sqsubseteq A \sqcup A = A$ proving that $A \in \mathrm{postfp}(\lambda x \cdot a \sqcup f(x))$ whence $B \sqsubseteq A$ by Knaster-Tarski.
2. We have $B = a \sqcup f(B)$ whence $a \sqsubseteq B$ so $f(a) \sqsubseteq f(B)$. By hypothesis $a \sqsubseteq f(a)$ so that by transitivity, $a \sqsubseteq f(B)$. It follows that $a \sqcup f(B) = f(B)$ whence $B = f(B)$ and $a \sqsubseteq B$ so $A \sqsubseteq B$, and by antisymmetry, we get $A = B$. □

5 Observe that we get the variant of Park induction principle on page 60 by applying the classical principle of page 51 to B.

Conjugate of an operator on a complete boolean lattice (reminder)

- Let $f \in L \mapsto L$ be an operator on the complete boolean lattice $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap, \neg\rangle$. We define
$$\widetilde{f} \stackrel{\text{def}}{=} \lambda x \cdot \neg f(\neg x)$$
to be the *conjuguate* of f in L.
- $\widetilde{f}$ is sometimes denoted $f^{\star}$ (which may be confusing with the reflexive transitive closure notation)
- $\widetilde{f}$ is sometimes called the dual of f (which is confusing with the lattice dual, but is consistent since $x \sqsubseteq y \iff \neg x \sqsubseteq \neg x$).

- we have $\langle L \overset{m}{\longmapsto} L, \dot\sqsubseteq\rangle \underset{\lambda f \cdot \widetilde{f}}{\overset{\lambda f \cdot \widetilde{f}}{\leftrightarrows}} \langle L \overset{m}{\longmapsto} L, \dot\sqsupseteq\rangle$

PROOF.

$$\begin{aligned}
& \lambda f \cdot \widetilde{f}(g) \dot\sqsubseteq h \\
\iff & \widetilde{g} \dot\sqsubseteq h \\
\iff & \forall x \in L : \neg g(\neg x) \dot\sqsubseteq h(x) \\
\iff & \forall x \in L : g(\neg x) \dot\sqsubseteq \neg h(x) \\
\iff & \forall x \in L : g(\neg x) \dot\sqsubseteq \neg h(x) \\
\iff & \forall y \in L : g(y) \dot\sqsubseteq \neg h(\neg y) && \wr\text{by letting } y = \neg x\wr \\
\iff & g \dot\sqsubseteq \widetilde{h} \\
\iff & g \dot\sqsubseteq \lambda f \cdot \widetilde{f}(h)
\end{aligned}$$

□

Park conjugate (dual) fixpoint theorem in complete boolean lattices

THEOREM. Let $f \in L \stackrel{m}{\longmapsto} L$ be a monotone operator on the complete boolean lattice $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap, \neg\rangle$. Then

$$\begin{aligned} \mathsf{gfp}\ f &= \neg \mathsf{lfp}\ \lambda x \cdot \neg f(\neg x) \\ \mathsf{lfp}\ f &= \neg \mathsf{gfp}\ \lambda x \cdot \neg f(\neg x) \end{aligned}$$

■

PROOF. If $x \sqsubseteq y$ then $\neg y \sqsubseteq \neg x$ so $f(\neg y) \sqsubseteq f(\neg x)$ whence $\neg f(\neg x) \sqsubseteq \neg f(\neg y)$ proving $\lambda x \cdot \neg f(\neg x) \in L \stackrel{m}{\longmapsto} L$ whence by Knaster-Tarski that the extreme fixpoints do exist.

We have

$$\begin{aligned} & \neg \mathsf{lfp}\ \lambda x \cdot \neg f(\neg x) \\ = \ & \neg \bigsqcap \{x \mid \neg f(\neg x) \sqsubseteq x\} && \text{(Knaster-Tarski)} \\ = \ & \bigsqcup \{\neg x \mid \neg f(\neg x) \sqsubseteq x\} && \text{(Complete bool. lattice)} \\ = \ & \bigsqcup \{\neg x \mid \neg x \sqsubseteq f(\neg x)\} && \text{(Complete bool. lattice)} \\ = \ & \bigsqcup \{y \mid y \sqsubseteq f(y)\} && \text{(by letting } y = \neg x\text{)} \\ = \ & \mathsf{gfp}\ f && \text{(Knaster-Tarski)} \end{aligned}$$

By duality $\mathsf{lfp}\ f = \neg \mathsf{gfp}\ \lambda x \cdot \neg f(\neg x)$. □

Park unique fixpoint condition in a complete boolean lattice

THEOREM. Let $f \in L \stackrel{m}{\longmapsto} L$ be a monotone operator on the complete boolean lattice $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap, \neg\rangle$. Then

(1) $\mathsf{lfp}\ \lambda x \cdot \neg f(\neg x) \sqcap \mathsf{lfp}\ f = \bot$

(2) $(\mathsf{lfp}\ \lambda x \cdot \neg f(\neg x) \sqcup \mathsf{lfp}\ f = \top) \iff (\mathsf{lfp}\ f = \mathsf{gfp}\ f)$

■

PROOF.

(1) $\quad \mathsf{lfp}\ f \sqsubseteq \mathsf{gfp}\ f$

$\Longrightarrow \quad \neg \mathsf{gfp}\ f \sqsubseteq \neg \mathsf{lfp}\ f$

$\Longrightarrow \quad \neg \mathsf{gfp}\ f \sqcap \neg \mathsf{lfp}\ f \sqsubseteq \neg \mathsf{lfp}\ f \sqcap \mathsf{lfp}\ f$

$\Longrightarrow \quad \neg \mathsf{gfp}\ f \sqcap \neg \mathsf{lfp}\ f \sqsubseteq \bot$

$\Longrightarrow \quad \neg \mathsf{gfp}\ f \sqcap \neg \mathsf{lfp}\ f = \bot$

$\Longrightarrow \quad \mathsf{lfp}\ \lambda x \cdot \neg f(\neg x) \sqcap \mathsf{lfp}\ f = \bot$

(2, $\Leftarrow$) $\mathsf{lfp}\ \lambda x \cdot \neg f(\neg x) = \neg \mathsf{gfp}\ f$ so $\mathsf{lfp}\ f = \mathsf{gfp}\ f$ implies $\top = \neg \mathsf{lfp}\ f \sqcup \mathsf{lfp}\ f = \neg \mathsf{gfp}\ f \sqcup \mathsf{lfp}\ f = \mathsf{lfp}\ \lambda x \cdot \neg f(\neg x) \sqcup \mathsf{lfp}\ f = \top$

(2, $\Rightarrow$) By (1) and the hypothesis $\mathsf{lfp}\ \lambda x \cdot \neg f(\neg x) \sqcup \mathsf{lfp}\ f = \top$, we get $\mathsf{lfp}\ \lambda x \cdot \neg f(\neg x)$ and $\mathsf{lfp}\ f$ are complement hence $\neg(\mathsf{lfp}\ \lambda x \cdot \neg f(\neg x)) = \mathsf{lfp}\ f$ proving that is $\mathsf{lfp}\ f = \mathsf{gfp}\ f$ by the previous theorem due to Park. □

Application to the relational forward predictive contrapositive proof principle

THEOREM.

$$\forall \underline{s}, \overline{s} \in S : (\underline{s} \in E \wedge \langle \underline{s},\ \overline{s}\rangle \in t^\star \wedge \overline{s} \in F) \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in \Psi$$

$$\Leftrightarrow \exists I : \forall \underline{s}, \overline{s} : (\underline{s} \in E \wedge \langle \underline{s},\ \overline{s}\rangle \notin \Psi) \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in I$$
$$\wedge \langle \underline{s},\ \overline{s}\rangle \in I \Longrightarrow [\forall s' \in S : \langle \underline{s},\ s'\rangle \in t \Longrightarrow \langle s',\ \overline{s}\rangle \in I]$$
$$\wedge \overline{s} \in F \Longrightarrow \langle \overline{s},\ \overline{s}\rangle \notin I \qquad \blacksquare$$

PROOF.

$$\Longleftrightarrow \forall \underline{s}, \overline{s} \in S : (\underline{s} \in E \wedge \langle \underline{s},\ \overline{s}\rangle \in t^\star \wedge \overline{s} \in F) \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in \Psi$$
$$\Longleftrightarrow \forall \underline{s}, \overline{s} \in S : (\langle \underline{s},\ \overline{s}\rangle \in t^\star \wedge \overline{s} \in F) \Longrightarrow (\underline{s} \in E \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in \Psi)$$
$$\Longleftrightarrow t^\star \upharpoonright F \subseteq \{\langle \underline{s},\ \overline{s}\rangle \in S^2 \mid (\overline{s} \in E) \Longrightarrow (\langle \underline{s},\ \overline{s}\rangle \in \Psi)\}$$
$$\Longleftrightarrow t^\star \upharpoonright F \subseteq P \qquad \wr P = \{\langle \underline{s},\ \overline{s}\rangle \in S^2 \mid (\overline{s} \in E) \Longrightarrow (\langle \underline{s},\ \overline{s}\rangle \in \Psi)\}\wr$$

$$\Longleftrightarrow \mathsf{lfp}\, \lambda X \cdot t \circ X \cup 1_S \upharpoonright F \subseteq P$$
$$\Longleftrightarrow \neg\mathsf{gfp}\, \lambda X \cdot \neg(t \circ (\neg X) \cup 1_S \upharpoonright F) \subseteq P$$
$$\Longleftrightarrow \neg P \subseteq \mathsf{gfp}\, \lambda X \cdot \neg(t \circ (\neg X)) \cap \neg(1_S \upharpoonright F)$$
$$\Longleftrightarrow \exists I : \neg P \subseteq I \wedge I \subseteq \neg(t \circ (\neg I)) \wedge I \subseteq \neg(1_S \upharpoonright F)$$
$$\Longleftrightarrow \exists I : \neg P \subseteq I \wedge I \subseteq \neg(t \circ (\neg I)) \wedge (1_S \upharpoonright F) \subseteq \neg I$$
$$\Longleftrightarrow \exists I : \forall \underline{s}, \overline{s} : (\underline{s} \in E \wedge \langle \underline{s},\ \overline{s}\rangle \notin \Psi) \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in I \wedge \langle \underline{s},\ \overline{s}\rangle \in I \Longrightarrow \neg[\exists s' \in S : \langle \underline{s},\ s'\rangle \in t \wedge \langle s',\ \overline{s}\rangle \notin I] \wedge \overline{s} \in F \Longrightarrow \langle \overline{s},\ \overline{s}\rangle \notin I$$
$$\Longleftrightarrow \exists I : \forall \underline{s}, \overline{s} : (\underline{s} \in E \wedge \langle \underline{s},\ \overline{s}\rangle \notin \Psi) \Longrightarrow \langle \underline{s},\ \overline{s}\rangle \in I \wedge \langle \underline{s},\ \overline{s}\rangle \in I \Longrightarrow [\forall s' \in S : \langle \underline{s},\ s'\rangle \in t \Longrightarrow \langle s',\ \overline{s}\rangle \in I] \wedge \overline{s} \in F \Longrightarrow \langle \overline{s},\ \overline{s}\rangle \notin I$$

$\square$

Other equivalent induction principles are found in [4].

Reference

[4] P. Cousot and R. Cousot. Induction principles for proving invariance properties of programs. In *Tools & Notions for Program Construction: an Advanced Course*, D. Néel (Ed.), Cambridge University Press, Cambridge, UK, pp. 75–119, August 1982.

Fixpoint of the composition of monotone functions

THEOREM. Let $\langle L,\ \sqsubseteq\rangle$ and $\langle M,\ \leq\rangle$ be complete lattices and $f \in L \overset{\mathrm{m}}{\longmapsto} M$, $g \in M \overset{\mathrm{m}}{\longmapsto} L$. Then $g(\mathsf{lfp}\, f \circ g) = \mathsf{lfp}\, g \circ f$. $\blacksquare$

PROOF. – $(g \circ f)(g(\mathsf{lfp}\, f \circ g) = g(f \circ g(\mathsf{lfp}\, f \circ g)) = g(\mathsf{lfp}\, f \circ g)$ so $g(\mathsf{lfp}\, f \circ g) \in \{x \mid g \circ f(x) \sqsubseteq x\}$ so, by Knaster-Tarski, $\mathsf{lfp}\, g \circ f = \sqcap\{x \mid g \circ f(x) \sqsubseteq x\} \sqsubseteq g(\mathsf{lfp}\, f \circ g)$.

– Let $x \in L$ be such that $g \circ f(x) \sqsubseteq x$.

$$\Longrightarrow f(g \circ f(x)) \leq f(x) \qquad \wr\text{by monotony}\wr$$
$$\Longrightarrow f \circ g(f(x)) \leq f(x) \qquad \wr\text{by def. } \circ\wr$$
$$\Longrightarrow \mathsf{lfp}\, f \circ g \leq f(x) \qquad \wr\text{Knaster-Tarski}\wr$$

$$\Longrightarrow g(\mathsf{lfp}\, f \circ g) \sqsubseteq g \circ f(x) \qquad \wr\text{by monotony}\wr$$
$$\Longrightarrow g(\mathsf{lfp}\, f \circ g) \sqsubseteq x \qquad \wr\text{by hyp. } g \circ f(x) \sqsubseteq x \text{ and transitivity }\wr$$

So $g(\mathsf{lfp}\, f \circ g) \sqsubseteq \sqcap\{x \mid g \circ f(x) \sqsubseteq x\} = \mathsf{lfp}\, g \circ f$ by def. glb and Knaster-Tarski

– By antisymmetry, $g(\mathsf{lfp}\, f \circ g) = \mathsf{lfp}\, g \circ f$.

$\square$

Fixpoints of pointwise comparable monotone operators on a complete lattice

THEOREM. Let $f, g \in L \overset{\text{m}}{\longmapsto} L$ be a pointwise comparable monotone operators on the complete boolean lattice $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap,\ \neg\rangle$: $f \mathrel{\dot{\sqsubseteq}} g$. Then $\mathsf{lfp}\, f \sqsubseteq \mathsf{lfp}\, g$. ■

PROOF. $f \mathrel{\dot{\sqsubseteq}} g$ implies $\{x \mid f(x) \sqsubseteq x\} \subseteq \{x \mid g(x) \sqsubseteq x\}$ whence $\sqcap\{x \mid g(x) \sqsubseteq x\} \sqsubseteq \sqcap\{x \mid f(x) \sqsubseteq x\}$ by def. of lubs whence $\mathsf{lfp}\, f \sqsubseteq \mathsf{lfp}\, g$ by Knaster-Tarski. □

Abstraction soundness

COROLLARY.

$$\begin{array}{ll} & \mathsf{lfp}\, f \sqsubseteq P \\ \Longleftrightarrow & \exists g \in L \overset{\text{m}}{\longmapsto} L : f \mathrel{\dot{\sqsubseteq}} g \wedge \mathsf{lfp}\, g \sqsubseteq P \end{array}$$

■

The soundness of static analysis or abstract model checking directly results from this principle since concrete verification conditions for f are replaced by mode abstract verification conditions for g with which the proof is performed.

The Bekić–Leszczylowski fixpoint theorem

THEOREM. Let $F \in L^{n+m} \overset{\text{m}}{\longmapsto} L^n$ and $G \in L^{n+m} \overset{\text{m}}{\longmapsto} L^m$ be monotone operators and $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ be a complete lattice. We write $\langle X,\ Y\rangle = \langle X_1,\ \ldots,\ x_n,\ Y_1,\ \ldots,\ Y_m\rangle$ when $x \in L^n$ and $Y \in L^m$. Let us consider the set of equations

$$(1) \quad \begin{cases} X = F(X, Y) \\ Y = G(X, Y) \end{cases}$$

the resolvant $R = \lambda Y \cdot \mathsf{lfp}\, \lambda X \cdot F(X, Y)$ and the system of equations:

$$(2) \quad \begin{cases} X = R(Y) \\ Y = G(R(Y), Y) \end{cases}$$

Let us write $\mathsf{fp}(I)$ and $\mathsf{lfp}\,(i)$, $i = 1, 2$ for the respective set of fixpoints and least componentwise solution of (i). We have

$$\mathsf{fp}(2) \subseteq \mathsf{fp}(1) \quad \text{and} \quad \mathsf{lfp}\,(2) = \mathsf{lfp}\,(1)$$

■

PROOF. – If $Y, Z \in L^m$ then $Y \sqsubseteq Z$ implies $\langle X,\ Y\rangle \mathrel{\dot{\sqsubseteq}} \langle X,\ Z\rangle$ so $\lambda X \cdot F(X, Y) \mathrel{\dot{\sqsubseteq}} \lambda X \cdot F(X, Z)$ so $\mathsf{lfp}\, \lambda X \cdot F(X, Y) \mathrel{\dot{\sqsubseteq}} \lambda X \cdot F(X, Z)$ whence $R(Y) \mathrel{\dot{\sqsubseteq}} R(Z)$ proving that $R \in L^m \overset{\text{m}}{\longmapsto} L^n$ whence $\mathsf{fp}(2)$ is not empty.

- Let $\langle A_2 B_2,\ \in\rangle\, \mathsf{fp}(2)$ be a fixpoint of (2). Then $A_2 = R(B_2)$ so $\mathsf{lfp}\, \lambda X \cdot F(X, B_2) = A_2$ whence $A_2 = F(A_2, B_2)$ and $B_2 = G(R(B_2), B_2)$ that is $B_2 = G(A_2, B_2)$ proving that $\langle A_2 B_2,\ \in\rangle\, \mathsf{fp}(1)$ so $\mathsf{fp}(2) \subseteq \mathsf{fp}(1)$.
- In general $\mathsf{fp}(2) \neq \mathsf{fp}(1)$. A counter-example is provided by $L = \{\bot, \top\}$ with $\bot \sqsubseteq \bot \sqsubseteq \top \sqsubseteq \top$,

  $$\begin{cases} F(X, Y) = X \sqcap Y \\ G(X, Y) = X \sqcup Y \end{cases}$$

  so that the resolvant is $R = \lambda Y \cdot \mathsf{lfp}\, \lambda X \cdot F(X, Y) = \lambda Y \cdot \mathsf{lfp}\, \lambda X \cdot X \sqcap Y = \lambda Y \cdot \bot$. The system of equation (1) has the solution $\langle \top,\ \top\rangle$ which is not a solution of (2) in that particular case.
- Since $\mathsf{lfp}\,(2) \in \mathsf{fp}(1)$ we have $\mathsf{lfp}\,(1) \mathrel{\dot{\sqsubseteq}} \mathsf{lfp}\,(2)$.

– Let $\langle A_1 B_1, \in\rangle$ fp(1) be a fixpoint of (1). We have $F(A_1, B_1) = A_1$ whence $F(A_1, B_1) \dot{\sqsubseteq} A_1$ whence A_1 is a pointfixpoint of $\lambda X \cdot F(X, B_1)$ which implies by Knaster-Tarski that $\mathsf{lfp}\, \lambda X \cdot F(X, B_1) \dot{\sqsubseteq} A_1$ that is $R(B_1) \dot{\sqsubseteq} A_1$. Since $\langle R(B_1),\ B_1\rangle \dot{\sqsubseteq} \langle A_1,\ B_1\rangle$ and G is monotone $G(R(B_1), B_1) \dot{\sqsubseteq} G(A_1, B_1) \dot{\sqsubseteq} B_1$ since $\langle A_1,\ B_1\rangle$ is a postfixpoint of (1). It follows that $\langle A_1,\ B_1\rangle$ is a postfixpoint of (2) which implies $\mathsf{lfp}\,(2) \dot{\sqsubseteq} \langle A_1,\ B_1\rangle$ in particular $\mathsf{lfp}\,(2) \dot{\sqsubseteq} \mathsf{lfp}\,(1)$.

– By antisymmetry, $\mathsf{lfp}\,(1) = \mathsf{lfp}\,(2)$.

□

Fixpoint clipping

THEOREM. Let $f \in L \xrightarrow{m} L$ be a monotone operator on the complete boolean lattice $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap,\ \neg\rangle$ and $P \in L$. Then

$$\mathsf{lfp}\, f \sqsubseteq P \iff f(\mathsf{lfp}\, f \sqcap P) \sqsubseteq (\mathsf{lfp}\, f \sqcap P)$$

■

PROOF.

($\Leftarrow$) $f(\mathsf{lfp}\, f \sqcap P) \sqsubseteq (\mathsf{lfp}\, f \sqcap P)$

$\Longrightarrow \mathsf{lfp}\, f \sqsubseteq \mathsf{lfp}\, f \sqcap P$ ⦃Knaster-Tarski⦄

$\Longrightarrow \mathsf{lfp}\, f = \mathsf{lfp}\, f \sqcap P$ ⦃$\mathsf{lfp}\, f \sqcap P \sqsubseteq \mathsf{lfp}\, f$ and antisymmetry⦄

$\Longrightarrow \mathsf{lfp}\, f \sqsubseteq P$ ⦃def. glb⦄

($\Rightarrow$) (a) $\mathsf{lfp}\, f \sqsubseteq P$

$\Longrightarrow \mathsf{lfp}\, f \sqcap P = \mathsf{lfp}\, f$ ⦃def. glb⦄

(b) $\mathsf{lfp}\, f \sqsubseteq P$

$\Longrightarrow f(\mathsf{lfp}\, f) \sqsubseteq f(P)$ ⦃monotony⦄

$\Longrightarrow \mathsf{lfp}\, f \sqsubseteq f(P)$ ⦃fixpoint⦄

$\Longrightarrow \mathsf{lfp}\, f = \mathsf{lfp}\, f \sqcap P$ ⦃def. glb⦄

(c) if $\mathsf{lfp}\, f \sqsubseteq P$ then

$f(\mathsf{lfp}\, f \sqcap P)$

$\sqsubseteq f(\mathsf{lfp}\, f) \sqcap f(P)$ ⦃monotony and def. glb⦄

$= \mathsf{lfp}\, f \sqcap f(P)$ ⦃fixpoint⦄

$= \mathsf{lfp}\, f$ ⦃by (b)⦄

$= \mathsf{lfp}\, f \sqcap P$ ⦃by (a)⦄

□

Fixpoint induction with clipping

THEOREM. Let $f \in L \xrightarrow{m} L$ be a monotone operator on the complete boolean lattice $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap,\ \neg\rangle$ and $P \in L$. Then

$$\begin{aligned} &\mathsf{lfp}\, f \sqsubseteq P \\ \iff\ &\exists I \in L : f(I) \sqcap P \sqsubseteq I \wedge f(I) \sqsubseteq P \end{aligned}$$

■

PROOF.

($\Rightarrow$) Let $I = \mathsf{lfp}\, f$. $f(I) \sqcap P = f(\mathsf{lfp}\, f) \sqcap P = \mathsf{lfp}\, f \sqcap P = \mathsf{lfp}\, f = I$ since $\mathsf{lfp}\, f \sqsubseteq P$. Moreover, $f(I) = f(\mathsf{lfp}\, f) = \mathsf{lfp}\, f \sqsubseteq P$ proving that $\exists I \in L : f(I) \sqcap P \sqsubseteq I \wedge f(I) \sqsubseteq P$.

($\Leftarrow$) Reciprocally, $f(I) \sqsubseteq P$ so $f(I) \sqcap P = f(I)$ which by $f(I) \sqcap P \sqsubseteq I$ implies $f(I) \sqsubseteq I$, proving $\mathsf{lfp}\, f \sqsubseteq I$ by Knaster-tarski. Since f is monotone $\mathsf{lfp}\, f = f(\mathsf{lfp}\, f) \sqsubseteq f(I) \sqsubseteq P$ proving $\mathsf{lfp}\, f \sqsubseteq P$ by transitivity.

$\square$

Application to the proof of absence of runtime errors

- $\Sigma[\![P]\!]$: set of states of a program P
- $t[\![P]\!] \subseteq \Sigma[\![P]\!] \times \Sigma[\![P]\!]$: small-step operational semantics
- $E[\![P]\!] \subseteq \Sigma[\![P]\!]$: initial states
- $\Omega[\![P]\!] \subseteq \Sigma[\![P]\!]$: erroneous state

The absence of run-time errors is $\forall \underline{s}, s \in \Sigma[\![P]\!]$:

$$\underline{s} \in E \wedge \langle \underline{s},\ s \rangle \in (t[\![P]\!])^\star \Longrightarrow s \notin \Omega[\![P]\!]$$

$\Longleftrightarrow$ $E[\![P]\!] \rceil (t[\![P]\!])^\star \subseteq (1_{\Sigma[\![P]\!]} \upharpoonright \neg\Omega[\![P]\!])$ $\wr$def. $\subseteq\wr$

$\Longleftrightarrow$ $\mathsf{lfp}\, f \subseteq S$ $\wr$by the fixpoint definition of the lefthand side restriction of the reflexive transitive closure on page 47 and, where $f \stackrel{\text{def}}{=} \lambda X \cdot E[\![P]\!] \rceil 1_{\Sigma[\![P]\!]} \cup X \circ t[\![P]\!]$ and $S \stackrel{\text{def}}{=} 1_{\Sigma[\![P]\!]} \upharpoonright \neg\Omega[\![P]\!]\wr$

$\Longleftrightarrow$ $\exists I \in \Sigma[\![P]\!] \times \Sigma[\![P]\!] : f(I) \cap S \subseteq I \wedge f(I) \subseteq S$

So the proof consists in:

1. Finding an invariant I[6] with the semantics clipped by absence of runtime errors:
   - $\forall \underline{s} \in \Sigma[\![P]\!] : (\underline{s} \in E \wedge \underline{s} \notin \Omega[\![P]\!]) \Longrightarrow \langle \underline{s},\ \underline{s} \rangle \in I$
   - $\forall \underline{s}, s', s \in \Sigma[\![P]\!] : (\langle \underline{s},\ s' \rangle \in I \wedge \langle s',\ s \rangle \in t \wedge s \notin \Omega[\![P]\!]) \Longrightarrow (\langle \underline{s},\ s \rangle \in I)$
2. Checking the absence of runtime error:
   - $\forall \underline{s} \in \Sigma[\![P]\!] : \underline{s} \in E \Longrightarrow \underline{s} \notin \Omega[\![P]\!]$
   - $\forall \underline{s}, s', s \in \Sigma[\![P]\!] : (\langle \underline{s},\ s' \rangle \in I \wedge \langle s',\ s \rangle \in t) \Longrightarrow (s \notin \Omega[\![P]\!])$

[6] e.g. by automatic static analysis

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/.