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

Patrick Cousot

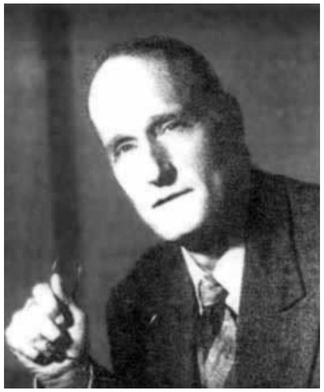
Jerome C. Hunsaker Visiting Professor
Massachusetts Institute of Technology
Department of Aeronautics and Astronautics

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

Course 16.399: “Abstract interpretation”

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

Alfred Tarski



Stephen Cole Kleene

Reference

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

[2] S.C. Kleene. *Introduction to Metamathematics*. D. Van Nostrand, New York, 1952.

Fixpoint iteration

Transfinite iteration on a poset

Let $f \in L \mapsto L$ be an operator on a poset $\langle L, \sqsubseteq, \sqcup, \sqcap \rangle$. The upward iterates of f from $a \in L$ are

$f^0 = a$

$f^{\delta+1} = f(f^\delta)$, successor ordinal

$f^\lambda = \bigsqcup_{\beta<\lambda} f^\beta$, limit ordinal

The downward iterates of f from $a \in L$ are

$f^0 = a$

$f^{\delta+1} = f(f^\delta)$, successor ordinal

$f^\lambda = \bigsqcap_{\beta<\lambda} f^\beta$, limit ordinal

Partially defined on a poset. Well-defined on a cpo/complete lattice. Well-defined up to ω on an ω-cpo. The iterates “up to ϵ” consider only the above definitions for ordinals less than or equal to $\epsilon \in \mathbb{O}$.

Finitary iteration theorem for monotone functions

THEOREM. Let $f \in L \overset{\mathrm{m}}{\longmapsto} L$ be a monotone operator on the poset $\langle L, \sqsubseteq, \sqcup, \sqcap\rangle$. If $a \in \mathsf{prefp}(f)$, the upward iterates $\langle X^\delta,\ \delta \leq \omega\rangle$ do exist up to ω and $X^\omega \in \mathsf{fp}(f)$ then $\langle X^\delta,\ \delta \leq \omega\rangle$ is an increasing chain and $X^\omega = \mathsf{lfp}_a^{\sqsubseteq} f$. ■

PROOF. – $a \in \mathsf{prefp}\, f$ do $a \sqsubseteq f(a)$ whence $X^0 \sqsubseteq X^1$. Assume $X^{n-1} \sqsubseteq X^n$ by monotony $X^n = f(X^{n-1}) \sqsubseteq f(X^n) = X^{n+1}$ proving that $\langle X^n,\ n < \omega\rangle$ is an increasing chain whence so is $\langle X^n,\ n \leq \omega\rangle$ by def. of the lub $X^\omega = \bigsqcup_{n<\omega} X^n$, which exists by hypothesis.

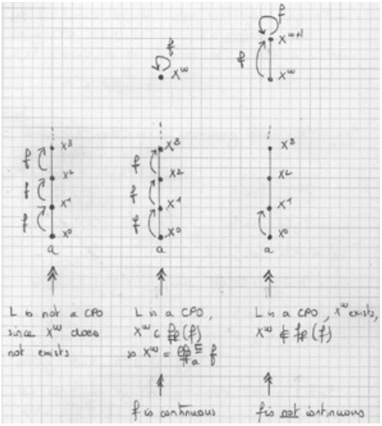
– If $X^\omega \in \mathsf{fp}(f)$ then $a = X^0 \sqsubseteq X^\omega$ so X^ω is a fixpoint of f greater than or equal to a

– Let x be any fixpoint of f greater than or equal to a. We have $X^0 = a \sqsubseteq x$. Assume $X^n \sqsubseteq x$ then $f(X^n) \sqsubseteq f(x) = x$ by monotony and fixpoint proving $\forall n < \omega : X^n \sqsubseteq x$ so by def. of lubs $X^\omega = \bigsqcup_{n<\omega} X^n \sqsubseteq x$.

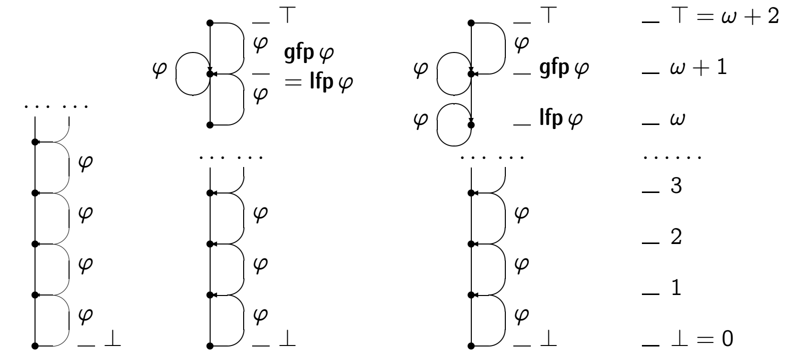
– We conclude that $X^\omega = \mathsf{lfp}_a^{\sqsubseteq} f$.

□

Examples of fixpoint iterations for monotone and continuous functions



Examples of Fixpoints



φ monotonic on a poset

φ monotonic on a complete lattice

φ upper-continuous on a complete lattice

Kleene fixpoint iteration theorem for continuous functions

Theorem. Let $f \in L \overset{\text{uc}}{\longmapsto} L$ be an upper-continuous operator on a cpo $\langle L, \sqsubseteq, \sqcup\rangle$, $a \in \text{prefp}(f)$ and $\langle X^\delta, \delta \leq \omega\rangle$ be the iterates of f from a. Then $X^\omega = \mathsf{lfp}_a^{\sqsubseteq} f$. ■

Proof. – Since $\langle X^\delta, \delta < \omega\rangle$ is an increasing chain, $X^\omega = \bigsqcup_{\delta<\omega} X^\delta$ does exists in a cpo.

– We have:

$$
\begin{array}{lll}
& f(X^\omega) & \\
= & f(\bigsqcup_{\delta<\omega} X^\delta) & \wr \text{def. } X^\omega \wr \\
= & \bigsqcup_{\delta<\omega} f(X^\delta) & \wr \text{continuity} \wr
\end{array}
$$

$$
\begin{array}{lll}
= & \bigsqcup_{0<\delta<\omega} X^\delta & \wr \text{def. iterates} \wr \\
= & a \sqcup \bigsqcup_{0<\delta<\omega} X^\delta & \wr \text{since } \forall \delta \leq \omega : a \sqsubseteq X^\delta \wr \\
= & \bigsqcup_{0\leq\delta<\omega} X^\delta & \wr \text{def. iterates with } X^0 = a \wr \\
= & X^\omega & \wr \text{def. } X^\omega \wr
\end{array}
$$

– We conclude by the previous theorem that $X^\omega = \mathsf{lfp}_a^{\sqsubseteq} f$.

□

Application to the iterative fixpoint definition of the strict/reflexive transitive closure of a binary relation

– Let $r \subseteq S \times S$ be a relation on a set S. We have defined

$$r^\star \stackrel{\text{def}}{=} \bigcup_{n\geq 0} r^n \quad \text{and} \quad r^+ \stackrel{\text{def}}{=} \bigcup_{n\geq 1} r^n$$

– We have shown the existence of

$$r'^\star \stackrel{\text{def}}{=} \mathsf{lfp}\, \lambda X \cdot 1_S \cup X \circ r \quad \text{and} \quad r'^+ \stackrel{\text{def}}{=} \mathsf{lfp}\, \lambda X \cdot r \circ (1_S \cup X)$$

– it remains to show that $r^\star = r'^\star$ and $r^+ = r'^+$.

Proof. – We let $f(X) = 1_S \cup X \circ r$.

$$
\begin{array}{lll}
X^0 = & \emptyset & \\
X^1 = & 1_S \cup \emptyset \circ r = 1_S = r^0 & \\
X^n = & \bigcup_{k<n} r^k & \wr \text{induction hypthesis} \wr \\
X^{n+1} = & 1_S \cup (\bigcup_{k<n} r^k) \circ r & \\
= & r^0 \cup \bigcup_{k<n} (r^k \circ r) & \\
= & r^0 \cup \bigcup_{k<n} (r^{k+1}) & \\
= & r^0 \cup \bigcup_{1\leq j\leq n} (r^j) & \wr j = k+1 \wr \\
= & \bigcup_{0\leq j\leq n} (r^j) &
\end{array}
$$

proving, by recurrence $\forall n \geq 0 : X^n = \bigcup_{k<n} r^k$.

- $X^\omega = \bigcup_{n\geq 0}\bigcup_{k<n} r^k = \bigcup_{n\geq 0} r^n = r^\star$.
- $X^\omega = \bigcup_{n\geq 0} r^n = r^0 \cup \bigcup_{n\geq 1} r^n = r^0 \cup \bigcup_{i\geq 0} r^{i+1} = 1_S \cup \bigcup_{i\geq 0}(r^n \circ r) = 1_S \cup (\bigcup_{i\geq 0} r^n) \circ r = f(X^\omega)$ proving X^ω to be a fixpoint of f
- We conclude by the previous theorem that $X^\omega = \mathsf{lfp}^{\subseteq}_{\emptyset}\, f = \mathsf{lfp}\, f$.

□

Scott fixpoint induction principle

THEOREM. Let $f \in L \xrightarrow{\text{uc}} L$ be an upper-continuous operator on a cpo $\langle L,\ \sqsubseteq,\ \sqcup\rangle$ and $a \in \mathsf{prefp}(f)$. Let $P \subseteq L$, then if

1. $a \in P$
2. $\forall x \in P : f(x) \in P$
3. For any chain $\langle x_i,\ i \in \mathbb{N}\rangle$ of elements of P, $\bigsqcup_{i\in\mathbb{N}} x_i \in P$[1]

then $\mathsf{lfp}^{\sqsubseteq}_{a}\, f \in P$. ■

[1] A property satisfying property (3) is called “*admissible*”.

PROOF. Let $\langle X^\delta,\ \delta \leq \omega\rangle$ be the iterates for f from a. Obviously $X^0 = a \in P$ by (1). If $X^n \in P$ then $X^{n+1} = f(X^n) \in P$ by (2) and $X^\omega \in P$ by (3). By upper-continuity of f, $X^\omega = \mathsf{lfp}^{\sqsubseteq}_{a}\, f$ so $\mathsf{lfp}^{\sqsubseteq}_{a}\, f \in P$. □

P can be thought of as a property of the elements of L and the proof that $\mathsf{lfp}^{\sqsubseteq}_{a}\, f$ has property P consists in showing that all iterates for f from a have this property. This is sufficient by not necessary (take e.g. $P = \{\mathsf{lfp}^{\sqsubseteq}_{a}\, f\}$ where $a \notin P$).

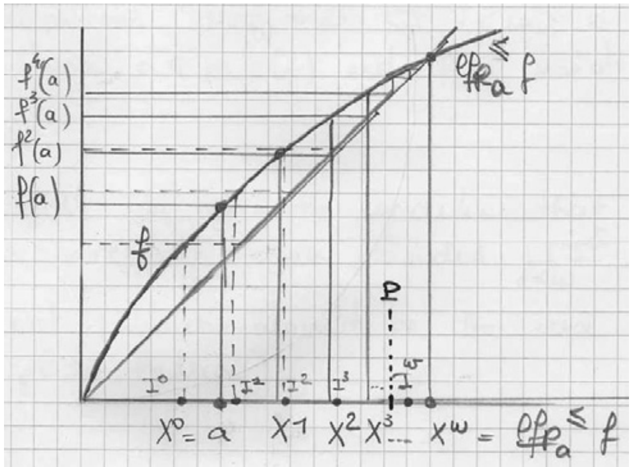
Lower fixpoint induction principle

THEOREM. Let $f \in L \xrightarrow{\text{uc}} L$ be an upper-continuous operator on a cpo $\langle L,\ \sqsubseteq,\ \sqcup\rangle$ and $a \in \mathsf{prefp}(f)$ and $P \subseteq L$.

$$\begin{array}{lll}
 & P \sqsubseteq \mathsf{lfp}^{\sqsubseteq}_{a}\, f & \\
\Longleftrightarrow & \exists\langle I^\delta,\ \delta \leq \omega\rangle \text{ an } \sqsubseteq\text{-increasing chain such that:} & \\
 & \quad I^0 \sqsubseteq a & (1)\\
 & \wedge\, \forall n : 0 < n < \omega \Longrightarrow I^n \sqsubseteq f(I^{n-1}) & (2)\\
 & \wedge\, I^\omega \sqsubseteq \bigsqcup_{n\geq 0} I^n & (3)\\
 & \wedge\, P \sqsubseteq I^\omega & (4)
\end{array}$$

■

Intuition:



PROOF. – (⇐, soundness) Let $\langle X^\delta,\ \delta \leq \omega\rangle$ be the iterates of f from a. By (1), $I^0 \sqsubseteq a = X^0$. Assume $I^{n-1} \sqsubseteq X^{n-1}$, $n > 0$. By continuity, hence monotony, and (2), $I^n \sqsubseteq f(I^{n-1}) \sqsubseteq f(X^{n-1}) = X^n$ proving by recurrence $\forall x \in \mathbb{N} : I^n \sqsubseteq X^n$. Since $\langle I^\delta,\ \delta \leq \omega\rangle$ is an increasing chain, $\bigsqcup_{n\geq 0} I^n$ does exist in a cpo. We have $I^\omega \sqsubseteq \bigsqcup_{n\geq 0} I^n \sqsubseteq X^\omega = \mathsf{lfp}_a^{\sqsubseteq} f$ by continuity of f. By (4), we conclude that $P \sqsubseteq I^\omega \sqsubseteq X^\omega \sqsubseteq \mathsf{lfp}_a^{\sqsubseteq} f$.

– (⇒, completeness) For the converse, chose $\langle I^\delta,\ \delta \leq \omega\rangle$ to be the iterates of f from a. By definition of the iterates and reflexivity, (1), (2) and (3) hold. By continuity $I^\omega = \mathsf{lfp}_a^{\sqsubseteq} f$ and so $P \sqsubseteq I^\omega$ holds by hypothesis. Note that $\langle I^\delta,\ \delta \leq \omega\rangle$ is an increasing chain since $a \in \mathsf{prefp}(f)$ and f is monotone.

□

We can relax the condition that $\langle I^\delta,\ \delta \leq \omega\rangle$ is an increasing chain provided the lub $\bigsqcup_{n\geq 0} I^n$ does exist (e.g. in a complete lattice).

Knaster-Tarski on cpos

THEOREM. Let $f \in L \overset{\text{uc}}{\longmapsto} L$ be an upper-continuous operator on a cpo $\langle L,\ \sqsubseteq,\ \sqcup\rangle$ and $a \in \mathsf{prefp}(f)$. Then

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

■

PROOF. – Let $P = \{x \in L \mid a \sqsubseteq x \wedge f(x) \sqsubseteq x\}$. We know that $\mathsf{lfp}_a^{\sqsubseteq} f$ does exist so $f(\mathsf{lfp}_a^{\sqsubseteq} f) = \mathsf{lfp}_a^{\sqsubseteq} f \in P$ by reflexivity.

– Let $\langle X^\delta,\ \delta \leq \omega\rangle$ be the iterates of f from a (with $X^\omega = \mathsf{lfp}_a^{\sqsubseteq} f$ by continuity of f)

– For any $x \in P$, we have
  - $X^0 = a \sqsubseteq x$
  - $X^n \sqsubseteq x$ by induction hypothesis

  - $X^{n+1} = f(X^n) \sqsubseteq f(x) \sqsubseteq x$ since f is monotonic proving $\forall n < \omega : X^n \sqsubseteq x$ by recurrence

– We have proved:

1. $\mathsf{lfp}_a^{\sqsubseteq} f \in P$
2. $\forall x \in P : \mathsf{lfp}_a^{\sqsubseteq} f \sqsubseteq x$

whence $\mathsf{lfp}_a^{\sqsubseteq} f \sqsubseteq \bigsqcap P$ (since for all other lower bounds y of P, we have $\forall x \in P : y \sqsubseteq x$ so $y \sqsubseteq \mathsf{lfp}_a^{\sqsubseteq} f$ proving $\mathsf{lfp}_a^{\sqsubseteq} f$ to be the greatest lower bound.

– Notice that $\bigsqcap P$ is shown to exist despite the fact taht $\bigsqcap X$ may not exist for an arbitrary subset $X \subseteq L$ of a cpo.

□

Least fixpoints of continuous functionals on monotone/continuous maps are monotone/continous

THEOREM. Let $\langle L, \sqsubseteq\rangle$ be a poset and $\langle M, \leq, \vee\rangle$ be a cpo. Let $\langle L \mapsto M, \dot{\leq}, \dot{\vee}\rangle$ be the cpo of maps of L on M pointwise ordered by $f \mathrel{\dot{\leq}} q$ iff $\forall x \in L : f(x) \leq g(x)$. Let $F \in (L \mapsto M) \overset{\text{uc}}{\longmapsto} (L \mapsto M)$ be a continuous operator on $\langle L \mapsto M, \dot{\leq}, \dot{\vee}\rangle$. Let $f \in \text{prefp}(F)$. Then

1. If $f \in L \overset{\text{m}}{\longmapsto} M$ and $F \in (L \overset{\text{m}}{\longmapsto} M) \overset{\text{uc}}{\longmapsto} (L \overset{\text{m}}{\longmapsto} M)$ then $\mathsf{lfp}^{\sqsubseteq}_{f} F \in (L \overset{\text{m}}{\longmapsto} M)$ is monotone
2. If $\langle L, \sqsubseteq\rangle$ is a cpo, $f \in L \overset{\text{uc}}{\longmapsto} M$ and $F \in (L \overset{\text{uc}}{\longmapsto} M) \overset{\text{uc}}{\longmapsto} (L \overset{\text{uc}}{\longmapsto} M)$ are continuous, then $\mathsf{lfp}^{\sqsubseteq}_{f} F \in (L \overset{\text{m}}{\longmapsto} M)$ is continuous

■

PROOF. Let $\langle F^\delta, \delta \in \omega\rangle$ be the iterates of F from f. Since F is a continuous operator on a cpo $\langle L \mapsto M, \dot{\leq}, \dot{\vee}\rangle$, F^ω exists and is $\mathsf{lfp}^{\sqsubseteq}_{f} F$. $F^0 = f$ is monotonic/continuous. If F^n is monotonic/continuous then so is $F^{n+1} = F(F^n)$ by $F \in (L \overset{\text{m}}{\longmapsto} M) \overset{\text{uc}}{\longmapsto} (L \overset{\text{m}}{\longmapsto} M)/F \in (L \overset{\text{uc}}{\longmapsto} M) \overset{\text{uc}}{\longmapsto} (L \overset{\text{uc}}{\longmapsto} M)$. The lub $F^\omega = \dot{\bigvee\limits_{n \geq 0}} F^n$ exist and is monotonic/continuous whence proving 1./2. □

Least fixpoint theorem for monotone functions on cpos (1) [2]

THEOREM. Let f in $L \overset{\text{m}}{\longmapsto} L$ be a monotone operator on a cpo $\langle L, \sqsubseteq, \sqcup\rangle$. The *transfinite iterates* of f from $a \in L$ are:

$$
\begin{aligned}
& f^0 = a \\
& f^{\delta+1} = f(f^\delta), && \text{successor ordinal} \\
& f^\lambda = \textstyle\bigsqcup_{\beta<\lambda} f^\beta, && \text{limit ordinal}
\end{aligned}
$$

If $a \in \text{prefp}(f)$ then the transfinite iterates of f form an increasing chain which is ultimately stationary and which limit is $\mathsf{lfp}^{\sqsubseteq}_{a} f$. ■

[2] Tarski's complete lattice hypothesis can be weakened to a cpo. in his least fixpoint theorem. We provide two proofs, one using ordinals and chains, the other using directed sets in cpo's (to avoid ordinals).

PROOF. – We have $f^0 = a \sqsubseteq f(a) = f^1$

- Assume by transfinite induction that $\forall \xi < \delta$, we have $\forall \beta \leq \delta : f^\beta \sqsubseteq f^\xi$. We must prove that $\forall \beta \leq \delta : f^\beta \sqsubseteq f^\delta$.
  - If $\delta = \lambda + 1$ is a successor ordinal, then $\forall \beta \leq \lambda : f^\beta \sqsubseteq f^\lambda$ so by monotony, $f^{\beta+1} = f(f^\beta) \sqsubseteq f(f^\lambda) = f^{\lambda+1}$ so $\forall \beta : 1 \leq \beta \leq \lambda + 1 = \delta : f^\beta \sqsubseteq f^\delta$. In particular $f^1 \sqsubseteq f^\delta$ so $f^0 = a \sqsubseteq f(a) = f(1) \sqsubseteq f^\delta$ so $\forall \beta \leq \delta : f^\beta \sqsubseteq f^\delta$.
  - If δ is a limit ordinal then the iterates $\langle f^\beta, \beta < \delta\rangle$ form an increasing chain which has a limit $f^\delta = \bigsqcup_{\beta<\delta} f^\beta$ in the cpo $\langle L, \sqsubseteq, \sqcup\rangle$ proving that f^δ exists. By def. of lubs we have $f^\beta \sqsubseteq f^\delta$ for all $\beta \leq \delta$.
- By transfinite induction $\langle f^\beta, \beta < \mathbb{O}\rangle$ is an increasing chain of elements of the set L.
- Let α be the least ordinal which cardinality is equal to that of L: $|\alpha| = |L|$. We have $f^{\alpha+1}$ which is one of the elements of $\langle f^\beta, \beta < \alpha\rangle$. Let ϵ be the smallest rank of such an element. We have $f^\epsilon \sqsubseteq f^{\epsilon+1} \sqsubseteq f^{\alpha+1}$ since $\epsilon < \alpha + 1$ and $f^{\alpha+1} = f^\epsilon$ so $f^\epsilon = f^{\epsilon+1} = f^{\alpha+1}$. It follows that by definition of $f^{\epsilon+1} = f(f^\epsilon)$ that f^ϵ is a fixpoint of f.

- Observe that after rank ϵ, the chain is stationary, that is $\forall \delta \geq \epsilon : f^{\delta} = f^{\epsilon}$.
  - This holds for $\delta = \epsilon$
  - If $f^{\delta} = f^{\epsilon}$ then $f^{\delta+1} = f(f^{\delta}) = f(f^{\epsilon}) = f^{\epsilon}$
  - If δ is a limit ordinal then $f^{\delta} = \bigsqcup_{\beta<\delta} f^{\beta} = \bigsqcup_{\beta<\epsilon} f^{\beta} = f^{\epsilon}$ since $f^{\beta} \leq f^{\epsilon}$ for all $\beta \leq \epsilon$
  - By transfinite induction, $\forall \delta \geq \epsilon : f^{\delta} = f^{\epsilon}$.
- Let x be any fixpoint of f greater than or equal to a. We have:
  - $f^0 = a \sqsubseteq x = f(x)$
  - Assume, by induction hypothesis, that $f^{\beta} \sqsubseteq x$ for all $\beta < \delta$
    - · If $\delta = \xi + 1$ is a successor ordinal then $f^{\delta} = f^{\xi+1} = f(f^{\xi}) = f(f^{\epsilon}) \sqsubseteq f(x) = x$ by monotony and induction hypothesis
    - · If δ is a limit ordinal then $\forall \beta < \delta : f^{\beta} \sqsubseteq x$ by induction hypothesis do $f^{\delta} = \bigsqcup_{\beta<\delta} f^{\beta} \sqsubseteq x$ by def. of lubs
  - By transfinite induction, $\forall \delta \in \mathbb{O} : f^{\delta} \sqsubseteq x$ so in particular $f^{\epsilon} \sqsubseteq x$.

- In conclusion $a \sqsubseteq f^{\epsilon} = f(f^{\epsilon})$ and $\forall a \sqsubseteq x = f(x) \Longrightarrow f^{\epsilon} \sqsubseteq x$ proving that $f^{\epsilon} = \mathsf{lfp}^{\sqsubseteq}_{a} f$.

□

Reference

[3] P. Cousot and R. Cousot. Constructive versions of Tarski's fixed point theorems. Pacific Journal of Mathematics, Vol. 82, No. 1, 1979, pp. 43–57.

Limit of the iterates [3]

THEOREM. – Let $\langle L, \sqsubseteq, \bot, \sqcup \rangle$ be a cpo and $\varphi \in L \xrightarrow{m} L$ be a monotonic map on L;

– Define ρ as mapping a prefixpoint X of φ to the limit of the iterates of φ starting from X

– ρ is a closure operator.

■

PROOF. – We let $\rho(X) = \varphi^{\epsilon}$ where $\varphi^0 = X$ and ϵ is the order of φ for X. Since the iterates form an incresing chain, $X = \varphi^0 \sqsubseteq \varphi^{\epsilon} = \rho(X)$ so that ρ is extensive;

- Assume $X \sqsubseteq Y$, $X \sqsubseteq \varphi(X)$, $Y \sqsubseteq \varphi(Y)$. Let φ^{κ}_{X} and φ^{κ}_{Y}, $\kappa \in \mathbb{O}$ be the respective iterates starting respectively from X and Y.
  - We have $\varphi^{0}_{X} = X \sqsubseteq Y = \varphi^{0}_{Y}$;
  - Assume $\varphi^{\lambda}_{X} \sqsubseteq \varphi^{\lambda}_{Y}$, $\lambda < \kappa$:
    - · If κ is a successor ordinal, $\kappa = \beta + 1$ and $\varphi^{\beta}_{X} \sqsubseteq \varphi^{\beta}_{Y}$. We have $\varphi^{\kappa}_{X} = \varphi(\varphi^{\beta}_{X}) \sqsubseteq \varphi(\varphi^{\beta}_{Y}) = \varphi^{\kappa}_{Y}$ by monotony;
    - · If κ is a limit ordinal, $\varphi^{\kappa}_{X} = \bigsqcup\limits_{\lambda<\kappa} \varphi^{\lambda}_{X} \sqsubseteq \bigsqcup\limits_{\lambda<\kappa} \varphi^{\lambda}_{Y} = \varphi^{\kappa}_{Y}$ by def. of lubs;

    We conclude $\varphi^{\kappa}_{X} \sqsubseteq \varphi^{\kappa}_{Y}$.
  - Let ϵ (resp. ϵ') be the order of φ for X (resp. Y). $\rho(X) = \varphi^{\epsilon}_{X} = \varphi^{\max(\epsilon,\epsilon')}_{X} \sqsubseteq \varphi^{\max(\epsilon,\epsilon')}_{Y} = \varphi^{\epsilon}_{Y} = \rho(X)$.

  We conclude that ρ is monotonic.
- If $X \sqsubseteq \varphi(X)$ then $\rho(X) = \varphi^{\epsilon}_{X}$ is a fixpoint of φ;
- The iterates of φ starting from a fixpoint X of φ are stationnary and equal to X, so $\rho(X)= X$;
- It follows that ρ is idempotent.

□

Ward theorem (on the image of a complete lattice by a closure operator), reminder

THEOREM. The image $\rho(L) \stackrel{\text{def}}{=} \{\rho(x) \mid x \in L\}$ of a complete lattice

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

by a closure operator ρ is a complete lattice

$$\langle \rho(L),\ \sqsubseteq,\ \rho(\bot),\ \top,\ \lambda S \cdot \rho(\sqcup S),\ \sqcap\rangle \qquad (1)$$

■

Reference

[4] M. Ward. The closure operators of a lattice. *Annals Math.*, 43(1942), see page 193.

PROOF. – $\forall x \in L$: $\bot \sqsubseteq x$ so that $\rho(\bot) \sqsubseteq \rho(x)$ proving that $\rho(\bot)$ is the infimum of $\rho(L)$;

- $\top \sqsubseteq \rho(\top) \sqsubseteq \top$ so that $\rho(\top) = \top$ proving that $\top$ is the supremum of $\rho(L)$;
- Let $\rho(x_i)$, $i \in \Delta$ be a subset of $\rho(L)$.
  - We have $\forall j \in \Delta$: $x_j \sqsubseteq \bigsqcup_{i\in\Delta} x_i \sqsubseteq \bigsqcup_{i\in\Delta} \rho(x_i)$ whence $\rho(x_j) \sqsubseteq \rho(\bigsqcup_{i\in\Delta} \rho(x_i))$;
  - Let $\rho(y)$ be another upper-bound of the $\rho(x_i)$, $i \in \Delta$. We have $\bigsqcup_{i\in\Delta} \rho(x_i) \sqsubseteq \rho(y)$ whence $\rho(\bigsqcup_{i\in\Delta} \rho(x_i)) \sqsubseteq \rho(\rho(y)) = \rho(y)$; It follows that $\rho(\bigsqcup_{i\in\Delta} \rho(x_i))$ is the lub of the $\rho(x_i)$, $i \in \Delta$;
  - $\langle \rho(L), \sqsubseteq\rangle$ is a complete lattice. It remains to characterize the glb;
- We first characterize $\bigsqcap_{i\in\Delta} \rho(x_i)$ where $\rho(x_i)$, $i \in \Delta$ be a subset of $\rho(L)$:
- $\bigsqcap_{i\in\Delta} \rho(x_i) \sqsubseteq \rho(\bigsqcap_{i\in\Delta} \rho(x_i))$ ρ extensive

- $\bigsqcap_{i\in\Delta} \rho(x_i) \sqsubseteq \rho(x_j)$ def. glb
- $\rho(\bigsqcap_{i\in\Delta} \rho(x_i)) \sqsubseteq \rho(\rho(x_j)) \sqsubseteq \rho(x_j)$ monotony & idempotence
- $\rho(\bigsqcap_{i\in\Delta} \rho(x_i)) \sqsubseteq \bigsqcap_{i\in\Delta} \rho(x_i)$ def. glb

We conclude $\rho(\bigsqcap_{i\in\Delta} \rho(x_i)) = \bigsqcap_{i\in\Delta} \rho(x_i)$ by antisymetry.

Let $\rho(x_i)$, $i \in \Delta$ be a subset of $\rho(L)$.

- $\bigsqcap_{i\in\Delta} \rho(x_i)$ is the glb of the $\rho(x_i)$, $i \in \Delta$ in $\langle L, \sqsubseteq\rangle$;
- $\bigsqcap_{i\in\Delta} \rho(x_i) \in \rho(L)$;
- So $\bigsqcap_{i\in\Delta} \rho(x_i)$ is the glb of the $\rho(x_i)$, $i \in \Delta$ in $\langle \rho(L), \sqsubseteq\rangle$.

□

Constructive version of Tarski's fixpoint theorem for monotone operators on complete lattices [3]

THEOREM. The set of fixpoints of a monotonic map $\varphi \in L \overset{\text{m}}{\longmapsto} L$ on a complete lattice $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ is a complete lattice. ■

PROOF. – The map $\lambda X \cdot X \sqcup \varphi(X)$ is monotonic and extensive;

- Let $\rho^{\uparrow}$ be the upper-closure operator which associates the limits of the iterates of $\lambda X \cdot X \sqcup \varphi(X)$ to any $X \in L$;
- By Ward's theorem, the image of $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ by $\rho^{\uparrow}$ is a complete lattice $\langle \rho^{\uparrow}(L),\ \sqsubseteq,\ \rho^{\uparrow}(\bot),\ \top,\ \lambda S \cdot \rho^{\uparrow}(\sqcup S),\ \sqcap\rangle$;

- The elements of $\rho^{\uparrow}(L)$ are fixpoints of $\lambda X \cdot X \sqcup \varphi(X)$ whence postfixpoints of φ (since $X = X \sqcup \varphi(X)$ iff $\varphi(X) \sqsubseteq X$);
- Let $\rho^{\downarrow}$ be the lower-closure operator which associates the limits of the iterates of φ to any postfixpoint $X \in \rho^{\uparrow}(L)$;
- By the dual of Ward's theorem, the image of:

$$\langle \rho^{\uparrow}(L),\ \sqsubseteq,\ \rho^{\uparrow}(\bot),\ \top,\ \lambda S \cdot \rho^{\uparrow}(\sqcup S),\ \sqcap \rangle$$

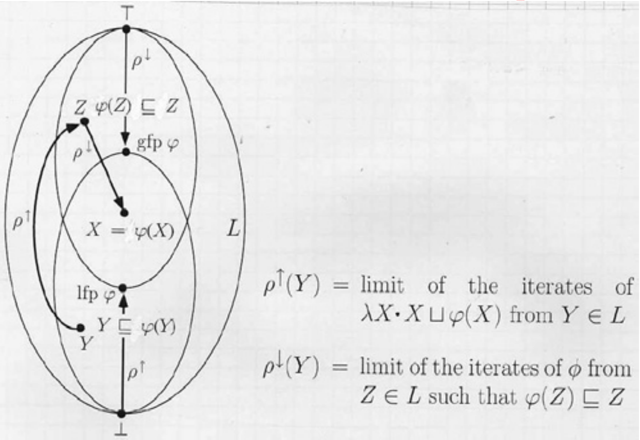
by $\rho^{\downarrow}$ is a complete lattice:

$$\langle \rho^{\downarrow}(\rho^{\uparrow}(L)),\ \sqsubseteq,\ \rho^{\uparrow}(\bot),\ \rho^{\downarrow}(\top),\ \lambda S \cdot \rho^{\uparrow}(\sqcup S),\ \lambda S \cdot \rho^{\downarrow}(\sqcap S) \rangle$$

- The elements of $\rho^{\downarrow}(\rho^{\uparrow}(L))$ are fixpoints of φ;
- Any fixpoint X of φ satisfies $\rho^{\downarrow}(\rho^{\uparrow}(X)) = X$ so that $X \in \rho^{\downarrow}(\rho^{\uparrow}(L))$;
- Hence the set $\rho^{\downarrow}(\rho^{\uparrow}(L))$ of fixpoints of φ is a complete lattice for $\sqsubseteq$;

□

Graphical illustration of the intuition behind the proof of the constructive version of Tarski's fixpoint theorem


$\top$
$\rho^{\downarrow}$
$Z\ \varphi(Z) \sqsubseteq Z$
$\rho^{\downarrow}$
gfp φ
$\rho^{\uparrow}$
$X = \varphi(X)$
L
lfp φ
$Y \sqsubseteq \varphi(Y)$
Y
$\rho^{\uparrow}$
$\bot$
$\rho^{\uparrow}(Y)$ = limit of the iterates of $\lambda X \cdot X \sqcup \varphi(X)$ from $Y \in L$
$\rho^{\downarrow}(Y)$ = limit of the iterates of ϕ from $Z \in L$ such that $\varphi(Z) \sqsubseteq Z$

Least fixpoint theorem on cpos [3]

LEMMA. Let $f \in L \xrightarrow{\text{me}} L$ be a monotone and extensive operator on a cpo $\langle L, \sqsubseteq, \sqcup \rangle$ and $a \in \text{prefp}(f)$. Then $\text{lfp}_a^{\sqsubseteq} f$ does exist. ■

PROOF. – Let L_a be the smallest subset of L such that:

- $a \in L_a$
- if $x \in L_a$ then $f(x) \in L_a$
- if C is a chain of elements of L_a, then $\bigsqcup C$ is in L_a

[3] The second proof of existence is due to Dito Pataria (“A constructive proof of Tarski's fixed-point theorem for dcpo's”. Presented in the 65th Peripatetic Seminar on Sheaves and Logic, in Aarhus, Denmark, November 1997.) and is reported by Martín Escardó (in “Joins in the frame of nuclei”, *Applied Categorical Structures*, Vol. 11, Issue 2, pp. 117–124.
The proof starts with a lemma using the definition of cpo's based on directed sets (any directed set of the poset has a lub in this poset) which is provably equivalent to the definition based on increasing chains (any increasing chain of the poset has a lub in this poset), using the axiom of choice. However, the ordinals are not needed in this second proof.

To prove that L_a does exists, consider:

$$\Phi(X) \stackrel{\text{def}}{=} \{a\} \cup \{f(x) \mid x \in X\} \cup \{\bigsqcup C \mid C \subseteq X \wedge C \text{is a directed subset of } L\}$$

- Then $\Phi \in \wp(L) \mapsto \wp(L)$ is well-defined since $\langle L, \sqsubseteq, \sqcup \rangle$ is a cpo so $\bigsqcup C$ exists for all directed subset $C \subseteq X$ of L.
- Moreover $X \subseteq Y$ implies $\Phi(X) \subseteq \Phi(Y)$ so $\Phi \in \wp(L) \xrightarrow{\text{m}} \wp(L)$ and so by Kanster-Tarski fixpoint theorem, $L_a = \text{lfp}_{\subseteq}^{\emptyset} \Phi$ does exist.
- Observe that $\langle L_a, \sqsubseteq, \sqcup \rangle$ is a cpo since, by definition, for all directed subsets D of L_a, whence of L, $\bigsqcup D$ exists in L and belongs to L_a. So $\bigsqcup D$ is the lub of D in L_a.
- Let $\langle L_a \xrightarrow{\text{me}} L_a, \dot{\sqsubseteq}, \dot{\sqcup} \rangle$ be the set of all monotone and extensive operators on L_a for the pointwise ordering $g \dot{\sqsubseteq} h$ iff $\forall x \in L_a : g(x) \sqsubseteq h(x)$.
- $\lambda x \in L_a \cdot x$ is the infimum of $L_a \xrightarrow{\text{me}} L_a$ since it is monotone and extensive and $\forall g \in L_a \xrightarrow{\text{me}} L_a : x \sqsubseteq g(x)$ so $\lambda x \in L_a \cdot x \dot{\sqsubseteq} g$.

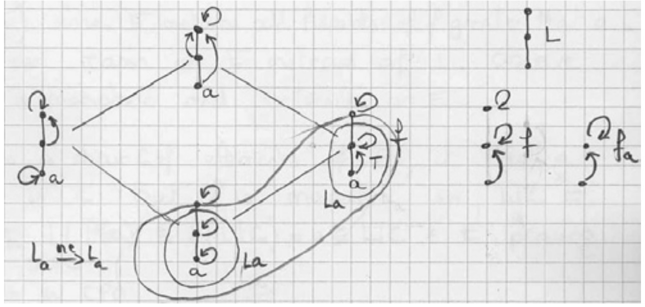
- If $D \subseteq L_a \xmapsto{\text{me}} L_a$ is a directed subset of elements of $L_a \xmapsto{\text{me}} L_a$ and $x \in L$. The set $\{g(x) \mid g \in D\}$ is a directed set in the cpo $\langle L, \sqsubseteq, \sqcup\rangle$, because given $h(x)$ and $g(x)$, $h, g \in D$, we have an $\dot{\sqsubseteq}$-upper bound of h and g in D, say k, so $k \in D$, $h \dot{\sqsubseteq} k$ and $g \dot{\sqsubseteq} k$ whence $h(x) \sqsubseteq k(x)$ and $g(x) \sqsubseteq k(x)$ and $k(x) \in \{g(x) \mid g \in D\}$ proving that $\{g(x) \mid g \in D\}$ is a directed set in $L_a \xmapsto{\text{me}} L_a$. Therefore it has a lub in the cpo $\langle L_a \xmapsto{\text{me}} L_a, \dot{\sqsubseteq}, \dot{\sqcup}\rangle$. Define $T(x) = \bigsqcap\{g(x) \mid g \in D\}$. We observe that $x \sqsubseteq y$ implies $\forall g \in D : g(x) \sqsubseteq g(y)$ so $T(x) = \bigsqcap\{g(x) \mid g \in D\} \sqsubseteq \bigsqcap\{g(y) \mid g \in D\} = T(y)$ proving that T is monotone. Moreover $\forall x \in L_a$, $a \sqsubseteq x \sqsubseteq g(x)$ so $a \sqsubseteq x \sqsubseteq \bigsqcap\{g(x) \mid g \in D\} = T(x)$ proving that $T \in L_a \xmapsto{\text{me}} L_a$. It follows that T is the lub of the directed set D in $L_a \xmapsto{\text{me}} L_a$ proving $\langle L_a \xmapsto{\text{me}} L_a, \dot{\sqsubseteq}, \dot{\sqcup}\rangle$ to be a cpo.
- If $g, h \in L_a \xmapsto{\text{me}} L_a$, we have $\forall x \in L : x \in h(x)$ so $g(x) \sqsubseteq g(h(x))$ whence $g \dot{\sqsubseteq} g \circ h$. Moreover, $h(x) \sqsubseteq g(h(x))$ since g is extensive so $h \dot{\sqsubseteq} g \circ h$. Moreover, if $a \sqsubseteq x$ then $a \sqsubseteq g \circ h(x)$ proving that $g \circ h \in L_a \xmapsto{\text{me}} L_a$. It follows that if $g, h \in L_a \xmapsto{\text{me}} L_a$ then $g \circ h \in L_a \xmapsto{\text{me}} L_a$ is a $\dot{\sqsubseteq}$-upper bound of g and h. So $L_a \xmapsto{\text{me}} L_a$ is a directed subset of $L_a \xmapsto{\text{me}} L_a$. In the cpo $\langle L_a \xmapsto{\text{me}} L_a, \dot{\sqsubseteq}, \dot{\sqcup}\rangle$, it has a lub say $T \in L \xmapsto{\text{me}} L$.

- Let f_a be the restriction $f|_{\{x \in L | a \sqsubseteq x\}}$ of f to L_a. Since $T \in L \xmapsto{\text{me}} L$, we have $f_a \circ T$ which is monotone as the composition of monotone maps and extensive since $x \sqsubseteq T(x)$ so $x \sqsubseteq f_a(x) \sqsubseteq f_a \circ T(x)$ since f_a is extensive and T is monotone. So $f_a \circ T \in\in L \xmapsto{\text{me}} L$ is in the directed set $L \xmapsto{\text{me}} L$ and consequently, it is $\sqsubseteq$-less than to its lub T rpoving that $f_a \circ T \subseteq T$.
- We have $T \subseteq f_a \circ T$ since f_a is extensive, so that by antisymmetry, $T = f_a \circ T$.
- Given any $x \in L_a$, we have $T(x) = f_a \circ T(x)$ so $\forall x \in L : T(x)$ is a fixpoint of f_a whence a fixpoint of f greater than or equal to a.
- Let y be any fixpoint of f and $Y = \{z \in L \mid a \sqsubseteq z \sqsubseteq y\}$. We have:
  - $a \in Y$
  - if $z \in Y$ then $a \sqsubseteq z \sqsubseteq y$ so $a \sqsubseteq f(a) \sqsubseteq f(z) \sqsubseteq f(y) = y$ whence $a \sqsubseteq f(a) \sqsubseteq y$ proving that $f(y) \in Y$.
  - If C is a directed set of elements of Y, we have $\forall z \in C : z \sqsubseteq y$ so $\bigsqcup C$, which exists in L, satisfies $\bigsqcup C \sqsubseteq y$ so $\bigsqcup C$ is also the lub in Y and $\bigsqcup C \in Y$.

- This implies that $\Phi(X) \subseteq Y$ so by Knaster-Tarski's fixpoint theorem $L_a = \mathsf{lfp}^{\emptyset}_{\sqsubseteq} \Phi = \bigcap\{Z\text{if } \Phi(\mathrm{Z}) \subseteq \mathrm{Z}\} \subseteq \mathrm{Y}$.
- We have seen that given any $x \in L_a$, we have $T(x) \in L_a$ which is a fixpoint of f greater than or equal to a. Since $L_a \subseteq Y$, we have $T(x) \in Y$ so that by definition $T(x) \sqsubseteq y$ and therefore $T(x)$ is the <u>least</u> fixpoint $\mathsf{lfp}^{\sqsubseteq}_a f$ of f greater than or equal to a.

□

Example:



Least fixpoint theorem for monotone functions on cpos (2)

THEOREM. Let $f \in L \xmapsto{\text{m}} L$ be a monotone operator on a cpo $\langle L, \sqsubseteq, \sqcup\rangle$ and $a \in \mathsf{prefp}(f)$. Then $\mathsf{lfp}^{\sqsubseteq}_a f$ does exist. ■

PROOF. – Let $E = \{x \in L \mid a \sqsubseteq x \sqsubseteq f(x)\}$. Then $f \in E \mapsto E$ (since $x \in E$ implies $x \sqsubseteq f(x)$ so $a \sqsubseteq x \sqsubseteq f(x) \sqsubseteq f(f(x))$ by monotony whence $f(x) \in E$). So $f \in E \xmapsto{\text{m}} E$ be restriction of a monotone map to a subset. We have $a \in E$ and $\mathsf{fp}(f) = \{x \in L \mid a \sqsubseteq x = f(x)\} = \mathsf{fp}_a(FL_E)$ since E constains all fixpoints of f greater than or equal to a. So we can reason on E instead of L.

- Observe that f is monotone and extensive on E.
- Given a chain C of elements of E, it has a lub $\bigsqcup C$ in L. But f is monotone so $\bigsqcup C = \bigsqcup_{x \in C} x \sqsubseteq \bigsqcup_{x \in C} f(x) \sqsubseteq f(\bigsqcup C) \in E$ proving E to be a cpo.
- By the previous lemma, $\mathsf{lfp}^{\sqsubseteq}_a f$ does exist in E and is the same in L.

□

Variant transfinite fixpoint iteration

THEOREM. Let $f \in L \xmapsto{\text{m}} L$ be a monotone operator on a cpo $\langle L,\ \sqsubseteq,\ \sqcup\rangle$ and $a \in \text{prefp}(f)$. Then the iterates

- $f^0 = a$
- $f^\delta = \bigsqcup_{\beta<\delta} f(f^\beta)$

form an increasing chain which is ultimately stationary at rank ϵ such that $f^\epsilon = \text{lfp}^{\sqsubseteq}_{a}\ f$. ■

PROOF. – The transfinite sequence $\langle f^\delta,\ \delta \in \mathbb{O}\rangle$ is an increasing chain since $f^0 = a \sqsubseteq f(a) = f^1$. If $\delta > 0$ and we have proved $f^\beta \sqsubseteq f(f^\beta)$ for all $\beta < \delta$ whence $\bigsqcup_{\beta<\delta} f^\beta \sqsubseteq \bigsqcup_{\beta<\delta} f(f^\beta) = f^\delta$ so $\forall \beta < \delta : f^\beta \sqsubseteq f^\lambda$. Moreover,

$$\begin{array}{lll}
f(f^\delta) = f(\bigsqcup\limits_{\beta<\delta} f(f^\beta)) & & \\
\sqsupseteq & \bigsqcup\limits_{\beta<\delta} f(f(f^\beta)) & \wr\text{monotony}\wr \\
\sqsupseteq & \bigsqcup\limits_{\beta<\delta} f(f^\beta) & \wr\text{since } f^\beta \sqsupseteq f(f^\beta)\wr \\
= & f^\delta &
\end{array}$$

- Let α be the least ordinal which cardinality is greater than that of L. If the chain $\langle f^\delta,\ \delta \in \mathbb{O}\rangle$ is strictly increasing then all elements are different so its cardinality is at least α which is impossible since it is included in L. It follows that we have $\beta' < \beta$ such that $f^{\beta'} = f^\beta = \bigsqcup_{\delta<\beta} f(f^\delta) \sqsupseteq f^{\beta'}$. We have shown $f^{\beta'} \sqsubseteq f(f^{\beta'})$ so by antisymmetry $f^{\beta'} = f(f^{\beta'})$. We let ϵ be the smallest such that ϵ and call it the *rank of the iterates*.
- We have $\forall \delta \geq \epsilon : f^\delta = f^\epsilon$. To prove this, observe that this holds for $\delta = \epsilon$. If this holds for all $\epsilon \leq \beta < \delta$ then

$$\begin{array}{lll}
f^\delta = & \bigsqcup\limits_{\beta<\delta} f(f^\beta) & \\
= & \bigsqcup\limits_{\beta<\epsilon} f(f^\beta) \sqcup \bigsqcup\limits_{\epsilon\leq\beta<\delta} f(f^\beta) & \\
= & f^\epsilon \sqcup \bigsqcup\limits_{\epsilon\leq\beta<\delta} f(f^\epsilon & \wr\text{by induction hypothesis}\wr \\
= & f^\epsilon \sqcup \bigsqcup\limits_{\epsilon\leq\beta<\delta} f^\epsilon & \wr\text{fixpoint}\wr \\
= & f^\epsilon & \wr\text{def. lub}\wr
\end{array}$$

- Given another fixpoint x of f greater than or equal to a, we have $f^0 = a \sqsubseteq x$. If $f^\beta \sqsubseteq x$ for all $\beta < \delta$ then $f(f^\beta) \sqsubseteq f(x) = x$ so $f^\delta = \bigsqcup_{\beta<\delta} f(f^\beta) \sqsubseteq x$ proving $\forall \delta : f^\delta \sqsubseteq x$ so in particular $f^\epsilon \sqsubseteq x$ proving $f^\epsilon = \text{lfp}^{\sqsubseteq}_{a}\ f$.

□

Fixpoints of a function and its powers

THEOREM. Let $f \in L \xmapsto{\text{m}} L$ be a monotone operator on a cpo $\langle L,\ \sqsubseteq,\ \sqcup\rangle$ and $a \in \text{prefp}(f)$. Then $\forall n \geq 1 :$ $\text{lfp}^{\sqsubseteq}_{a}\ f^n = \text{lfp}^{\sqsubseteq}_{a}\ f$. ■

PROOF. 1. $\forall n \geq 1 : \text{lfp}^{\sqsubseteq}_{a}\ f^n \sqsubseteq \text{lfp}^{\sqsubseteq}_{a}\ f$.

- First observe that $a \sqsubseteq f(a)$ so $a \sqsubseteq f(a)$ so $a \sqsubseteq f^n(a)$ for $n = 1$. If $a \sqsubseteq f(a) \sqsubseteq f(f^n(a)) = f^{n+1}(a)$ by monotony of f so that $\forall n : a \sqsubseteq f^n(a)$. Moreover f^n is monotone as the composition of of monotone functions so $\text{lfp}^{\sqsubseteq}_{a}\ f^n$ does exist.
- We have $f(\text{lfp}^{\sqsubseteq}_{a}\ f) = \text{lfp}^{\sqsubseteq}_{a}\ f$. Assume by induction hypothesis that $f^n(\text{lfp}^{\sqsubseteq}_{a}\ f) = \text{lfp}^{\sqsubseteq}_{a}\ f$ then $f^{n+1}(\text{lfp}^{\sqsubseteq}_{a}\ f) = f(f^n(\text{lfp}^{\sqsubseteq}_{a}\ f)) = f(\text{lfp}^{\sqsubseteq}_{a}\ f) = \text{lfp}^{\sqsubseteq}_{a}\ f$ so $\forall n \geq 1 :$ $f^n(\text{lfp}^{\sqsubseteq}_{a}\ f) = \text{lfp}^{\sqsubseteq}_{a}\ f$ by recurrence on n proving that $\text{lfp}^{\sqsubseteq}_{a}\ f^n \sqsubseteq \text{lfp}^{\sqsubseteq}_{a}\ f$.

2. $\forall n \geq 1 : f^n(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n) = \mathsf{lfp}^{\sqsubseteq}_{a}\, f^n$ so $f \circ f^n(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n) = f(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n)$ so $f^n(f(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n)) = f(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n)$ hence $\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n \sqsubseteq f(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n)$.

– By monotony of f, we get:

$$f(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n) \sqsubseteq f^2(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n)$$
$$f^2(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n) \sqsubseteq f^3(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n)$$
$$\ldots$$
$$f^{n-2}(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n) \sqsubseteq f^{n-1}(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n)$$
$$f^{n-1}(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n) \sqsubseteq f^n(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n) = \mathsf{lfp}^{\sqsubseteq}_{a}\, f^n$$

It follows that

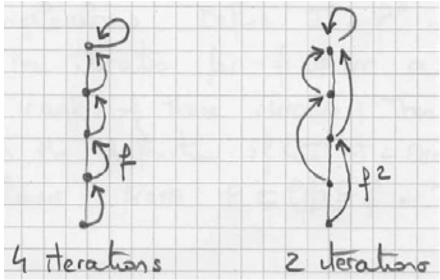
$$f(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n) \sqsubseteq \mathsf{lfp}^{\sqsubseteq}_{a}\, f^n \qquad \wr\text{by transitivity}\wr$$
$$f(\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n) = \mathsf{lfp}^{\sqsubseteq}_{a}\, f^n \qquad \wr\text{by antisymmetry}\wr$$

$$\mathsf{lfp}^{\sqsubseteq}_{a}\, f \sqsubseteq \mathsf{lfp}^{\sqsubseteq}_{a}\, f^n \qquad \wr\text{Knaster-Tarski on } f\wr$$

3. By antisymmetry, we conclude that $\mathsf{lfp}^{\sqsubseteq}_{a}\, f^n = \mathsf{lfp}^{\sqsubseteq}_{a}\, f$.

□

Useful to speed up fixpoint iteration. For example, by squaring:



Transfinite fixpoint induction

THEOREM. Let $f \in L \stackrel{\text{m}}{\longmapsto} L$ be a monotone operator on a cpo $\langle L, \sqsubseteq, \sqcup\rangle$. Given $a \in \text{prefp}(f)$, we have

$$\begin{array}{lr}
P \sqsubseteq \mathsf{lfp}^{\sqsubseteq}_{a}\, f & \\
\iff [\exists \epsilon \in \mathbb{O} : \exists I \in \epsilon + 1 \mapsto L : & \\
\quad I^0 \sqsubseteq a & (1) \\
\quad \wedge\ \forall \delta \leq \epsilon : I^\delta \sqsubseteq \bigsqcup\limits_{\beta<\delta} f(I^\beta) & (2) \\
\quad \wedge\ P \sqsubseteq I^\epsilon] & (3)
\end{array}$$

■

PROOF.

(⇐) *Soundness* Let ϵ' be the order of the iterations $f^0 = a$, $f^\delta = \bigsqcup_{\beta<\delta} f(f^\beta)$ so that $f^{\epsilon'} = \mathsf{lfp}^{\sqsubseteq}_{a}\, f$. Observe that $I^0 \sqsubseteq f^0$ by hypothesis (1). If $\forall \beta < \delta : I^\beta \sqsubseteq f^\beta$ then, by (2), $I^\delta \sqsubseteq \bigsqcup_{\beta<\delta} f(I^\beta) \sqsubseteq \bigsqcup_{\beta<\delta} f(f^\beta) = f^\delta$ proving $\forall \delta \leq \epsilon : I^\delta \sqsubseteq f^\delta$. By (3), we have $P \sqsubseteq I^\epsilon \sqsubseteq f^\epsilon \sqsubseteq f^{\max(\epsilon,\epsilon')} = \mathsf{lfp}^{\sqsubseteq}_{a}\, f$ since $\langle f^\delta, \delta \in \mathbb{O}\rangle$ is increasing and ultimately stationary at rank ϵ'.

(⇒) *Completeness* Define $I^\delta = f^\delta$ where $\langle f^\delta, \delta \in \mathbb{O}\rangle$ are the iterates of f from a and ϵ is the rank of these iterates. Then (1) and (2) follow from the definition of $\langle I^\delta, \delta \in \mathbb{O}\rangle$ while (3) follows from $P \sqsubseteq \mathsf{lfp}^{\sqsubseteq}_{a}\, f = I^\epsilon$.

□

Common fixpoints of commuting monotone operators on a complete lattice

THEOREM. [5] Let F be a family of communing[4] monotone operators on a complete lattice $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ and $a \in \bigcap_{f\in F} \mathsf{prefp}(f)$ then the set of common fixpoints of F greater than or equal to a is a complete lattice ■

Reference

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

[4] i.e; $\forall f, g \in F : f \circ g = g \circ f$.

PROOF. Let $p = \sqcap\{x \in L \mid a \sqsubseteq x \wedge \forall f \in F : f(x) \sqsubseteq x\}$.

1. $\forall f \in F : f(p) \sqsubseteq p$.
   If $a \sqsubseteq x$ and $\forall g \in F : g(x) \sqsubseteq x$
   then $p \sqsubseteq x$
   so $f(p) \sqsubseteq f(x) \sqsubseteq x$
   so $f(p) \sqsubseteq \sqcap\{x \in L \mid a \sqsubseteq x \wedge \forall g \in F : g(x) \sqsubseteq x\}$
   so $f(p) \sqsubseteq p$ Q.E.D.
2. $\forall f \in F : f(p) = p$
   - Given any $f \in F$, we have shown $f(p) \sqsubseteq p$
     so $\forall f \in F : g(f(p)) \sqsubseteq g(p)$ by monotony
     so $\forall f \in F : f(g(p)) \sqsubseteq g(p)$ by commutation
     Moreover a is a lower bound of $\{x \mid a \sqsubseteq x \wedge \forall h \in F : h(x) \sqsubseteq x\}$ so $a \sqsubseteq p$ hence $a \sqsubseteq g(a) \sqsubseteq g(p)$ proving that $\forall g \in F$:
     $g(p) \in \{x \mid a \sqsubseteq x \wedge \forall h \in F : h(x) \sqsubseteq x\}$
     so in particular
     $p = \sqcap\{x \mid a \sqsubseteq x \wedge \forall h \in F : h(x) \sqsubseteq x\}$
     $\sqsubseteq f(p)$.

By antisymmetry $\forall f \in F : f(p) = p$ proving that p is a common fixpoint of the f, $f \in F$.

- Any common fixpoint of the f, $f \in F$ which is greater or equal to a is some x such that:
  $a \sqsubseteq x \wedge \forall f \in F : f(x) = x$
  so $x \in \{x' \mid a \sqsubseteq x \wedge \forall h \in F : h(x') \sqsubseteq x'\}$
  so $p \sqsubseteq x$, proving that p is the least common fixpoint of the $f \in F$.
- Let $\mathsf{fp}(F) = \{x \in L \mid \forall f \in F : f(x) = x\}$. As a subset of $\langle L, \sqsubseteq\rangle$, it is q poset. We have shown that it has an infimum
  $\mathsf{lfp}^{\sqsubseteq}_{a} F \overset{\text{def}}{=} \sqcap\{x \in L \mid a \sqsubseteq x \wedge \forall f \in F : f(x) \sqsubseteq x\}$.
  Let $X \subset \mathsf{fp}(F)$. $\bigsqcup X$ exists in L, so $\mathsf{lfp}^{\sqsubseteq}_{\bigsqcup X} F$ exists in L. It is the least element of $\mathsf{fp}(F)$ which is an upper bound of X, whence greater than a, and therefore the lub of X in $\mathsf{fp}(F)$ which is therefore a complete lattice (although in general not a sublattice of L).

□

Common fixpoints of commuting monotone and extensive operators on a cpo [5]

THEOREM. Let F be a family of commuting monotone and extensive operators on a cpo $\langle L, \sqsubseteq, \sqcup\rangle$ and $a \in \bigcap_{f\in F} \mathsf{prefp}(f)$ then $\mathsf{lfp}^{\sqsubseteq}_{a} F$ does exists. ■

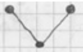
PROOF. – We first prove that the set of all extensive and monotone operator on any non-empty cpo has a common fixpoint.

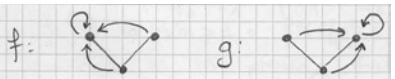
[5] The proof is a trivial generalization of that given in the special case of $a = \bot$ by Martín Escardó (in "Joins in the frame of nuclei", *Applied Categorical Structures*, Vol. 11, Issue 2, pp. 117–124.

- Indeed the set of all extensive monotone operators under the pointwise ordering is a cpo because it is closed under the formation of pointwise directed joins. It is directed because the identity is monotone and extensive and because if f and g are monotone and extensive then $f \circ g$ is a monotone and extensive operator above f and g. By def. cpos, there is a maximum monotone and extensive map T. If f is extensive then $T \mathrel{\dot{\sqsubseteq}} f \circ T$, and, because $f \circ T$ is extensive, $f \circ T \mathrel{\dot{\sqsubseteq}} T$ by construction of T. Therefore $T(x)$ is a common fixpoint of the extensive monotone maps for any element x of the poset. Q.E.D.
- Let L_a be the intersection of all sub-cpos of L which are closed under f for each $f \in F$ and which elements are greater than or equal to a. Then eaxh $f \in F$ restricts to a monotone and extensive map on L_a, and by the previous lemma, the set F has a common fixpoint in L_a, say x. let y be another. The set $Y = \{z \in L \mid a \sqsubseteq z \sqsubseteq y\}$ is a cpo with infimum a and if $d \in Y$ and $f \in F$ then $f(d) \sqsubseteq f(y) = y$ which shows that $f(d) \in Y$. Therefore $x \sqsubseteq y$ because $L_a \subset Y$.

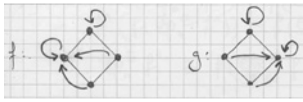
□

This does not generalize to monotone maps on cpos, as shown by the following counter-example:

The cpo is  The family $F = \{f, g\}$ is



They are monotone (but not extensive) and they have no common fixpoint, whereas on a complete lattice, we would have something like:



Least common fixpoints of continuous commuting operators on a cpo

THEOREM. Let $f, g \in L \xrightarrow{\text{uc}} L$ be continuous operators on a cpo $\langle L, \sqsubseteq, \sqcup \rangle$ and $a \in \text{prefp}(f) \cap \text{prefp}(g)$ such that

- $f(a) = g(a)$
- $f \circ g = g \circ f$

Then $\text{lfp}_a^{\sqsubseteq} f = \text{lfp}_a^{\sqsubseteq} g$ ■

PROOF. Let $\langle f^\beta, \beta \in \mathbb{O} \rangle$ and $\langle g^\beta, \beta \in \mathbb{O} \rangle$ be the respective iterates of f and g from a. We have

- $f(f^0) = f(a) = g(a) = g(f^0)$
- If $f(f^\lambda) = g(f^\lambda)$ then

$$\begin{array}{ll l}
 & f(f^{\lambda+1}) & \\
= & f(f(f^\lambda)) & \wr\text{def. iterates}\wr \\
= & f(g(f^\lambda)) & \wr\text{hyp. ind.}\wr \\
= & g(f(f^\lambda)) & \wr\text{commutation}\wr \\
= & g(f^{\lambda+1}) & \wr\text{def. iterates}\wr
\end{array}$$

- If $f(f^\beta) = g(f^\beta)$ for all $\beta < \lambda$, λ limit ordinal then

$$\begin{array}{ll l}
 & f(f^\lambda) & \\
= & f(\bigsqcup_{\beta<\lambda} f^\beta) & \wr\text{def. iterates}\wr \\
= & \bigsqcup_{\beta<\lambda} f(f^\beta) & \wr\text{continuity}\wr \\
= & \bigsqcup_{\beta<\lambda} g(f^\beta) & \wr\text{hyp. ind.}\wr \\
= & g(\bigsqcup_{\beta<\lambda} f^\beta) & \wr\text{continuity}\wr
\end{array}$$

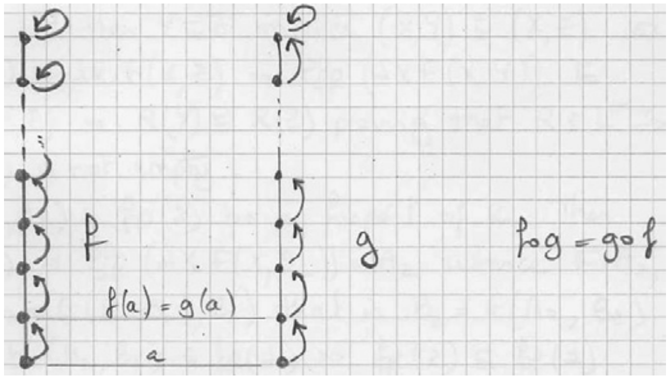
$= g(f^\lambda)$ ≀def. iterates≀

so by transfinite induction, $\forall \beta \in \mathbb{O} : f(f^\beta) = g(f^\beta)$.

- Let ϵ be the rank of the iterates of f (indeed $\epsilon \leq \omega$ by continuity). We have $\mathsf{lfp}_a^{\sqsubseteq} f = f(\mathsf{lfp}_a^{\sqsubseteq} f) = f(f^\epsilon) = g(f^\epsilon) = g(\mathsf{lfp}_a^{\sqsubseteq} f)$ so $\mathsf{lfp}_a^{\sqsubseteq} f$ is a fixpoint og g, proving that $\mathsf{lfp}_a^{\sqsubseteq} g \sqsubseteq \mathsf{lfp}_a^{\sqsubseteq} f$.
- Exchanging the rôles of f and g in the above proof, we have $\mathsf{lfp}_a^{\sqsubseteq} f \sqsubseteq \mathsf{lfp}_a^{\sqsubseteq} g$
- By antisymmetry, $\mathsf{lfp}_a^{\sqsubseteq} g = \mathsf{lfp}_a^{\sqsubseteq} f$

□

The theorem does not hold when f and g are not continuous, as shown by the following monotone counter-example:

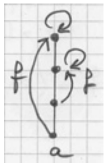


Fixpoints of extensive functions on cpos

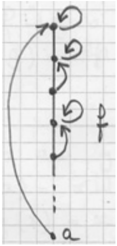
THEOREM. Let $\langle L, \sqsubseteq, \sqcup\rangle$ be a cpo and $f \in L \overset{e}{\longmapsto} L$ be an extensive operator on L i.e. $\forall x \in L : x \sqsubseteq f(x)$. Then $\forall a \in L : \{x \in L \mid a \sqsubseteq x = f(x)\} \neq \emptyset$. ■

PROOF. The iterates of f from a form an increasing chain in L whence cannot be strictly increasing (since otherwise its cardinality would be greater than that of L since all elements in an increasing chain are different). It follows that we have $\beta < \beta'$ such that $f^\beta = f^{\beta'}$ so $f^\beta = f^\delta$ for all $\beta \leq \delta \leq \beta'$ hence $f^\beta = f^\beta + 1 = f(f^\beta)$. The least such β is the *rank of the iterates* and is a fixpoint of f. □

The fixpoint may not be the least one, as shown by the following counter-example:



Indeed there may not be a minimal fixpoint (hence no least one) as shown by the following counter-example:



f is extensive but has not minimal fixpoint greater than or equal to a.

Hoare's fixpoint theorem for extensive operators

THEOREM. Let f, g be extensive operators on a poset $\langle L,\ \sqsubseteq\rangle$. Then $\mathrm{fp}(f \circ g) : \mathrm{fp}(f) \cap \mathrm{fp}(G)$ ■

PROOF.

(⊇) if $x = f(x)$ and $x = g(x)$ then $f \circ g(x) = f(x) = x$.

(⊆) if $f \circ g(x) = x$ then we have

$$\begin{array}{lr} \quad f \circ g(x) \sqsubseteq x & \\ \Longrightarrow g(x) \subseteq x & \wr\text{since } f \text{ is extensive}\wr \\ \Longrightarrow g(x) = x & \wr\text{since } g \text{ is extensive}\wr \\ \Longrightarrow x = f \circ g(x) = f(x) & \end{array}$$

□

THEOREM. Let f, g be extensive operators on a cpo $\langle L,\ \sqsubseteq,\ \sqcup\rangle$ such that $f \mathbin{\dot\sqcup} g$ is well-defined. Then $\mathrm{fp}(f \mathbin{\dot\sqcup} g) = \mathrm{fp}(f) \cap \mathrm{fp}(g)$. ■

PROOF.

(⊇) If $f(x) = x$ and $g(x) = x$ then $(f \mathbin{\dot\sqcup} g)(x) = f(x) \sqcup g(x) = x \sqcup x = x$.

(⊆) if $(f \mathbin{\dot\sqcup} g)(x) = x$ then $f(x) \sqcup g(x) = x$ so $f(x) \sqsubseteq x$ and $g(x) \sqsubseteq x$. By extensivity, $x \sqsubseteq f(x)$ and $x \sqsubseteq g(x)$ so by antisymmetry $f(x) = x$ and $g(x) = x$.

□

Reference

[6] C.A.R. Hoare. Fixed points of increasing functions. *Inf. proc. Letters*, 34(1990), 111–112.

Asynchronous iterations

System of simultaneous fixpoint equations

- $\langle L_i,\ \sqsubseteq_i,\ \perp_i,\ \top_i,\ \bigsqcup_i,\ \bigsqcap_i\rangle$, $i = 1, \ldots, n$ are complete lattices, whence so is $\langle L,\ \sqsubseteq,\ \perp,\ \top,\ \bigsqcup,\ \bigsqcap\rangle$ where $L = \prod_{i=1}^{n} L_i$ for the componentwise ordering $X \sqsubseteq Y = \bigwedge_{i=1}^{n} X_i \sqsubseteq_i Y_i$.
- We let $F \in L \mapsto L$ and $F_i \in L \mapsto L_i$ be $\forall X \in L : F_i(X) \overset{\text{def}}{=} (F(X))_i$.
- The system of fixpoint equations $X = F(X)$ can therefore be writen as the system of equations:

$$\left\{\begin{array}{l} X_i = F_i(X_1, \ldots, X_n) \\ i = 1, \ldots, n \end{array}\right.$$

Jacobi iterations

- $X^0 = D$
- $X^{k+1} = F(X^k)$, $k \in \mathbb{N}$

```
X := D;
repeat
   Y := F(X);
   stop := (X=Y);
   X:=Y;
until stop;
```

The fixpoint theorems for monotone/extensive operators on posets/cpos/complete lattices do apply.

Gauss-Seidel

- $X^0 = D$
- $X_i^{kn+i} = F_i(X^{kn+i-1})$
- $X_j^{kn+i} = X_j^{kn+i-1}$ $k \in \mathbb{N}$, $i = 1, \ldots, n$, $j \in [1, n] \setminus \{i\}$

```
X := D;
repeat
  stop := true;
  for i := 1 to n do
     T := Fi(X1,...,Xn);
     stop := stop & (T=Xi);
      Xi := T;
  od;
until stop;
```

In general, the Jacobi iterates may converge to a fixpoint while Gauss-Seidel iterations don't and inversely.

Chaotic iterations for a system of simultaneous fixpoint equations

Let $\langle J^\delta,\ \delta \in \mathbb{O}\rangle$ be a sequence of subsets of $[1, n]$ which is *weakly fair*:

$$\forall \delta \in \mathbb{O} : \forall i \in [1, n] : \exists \alpha \geq \delta : i \in J^\alpha \qquad \text{(a)}$$

The chaotic iterations from D for F defined by $\langle J^\delta,\ \delta \in \mathbb{O}\rangle$ are

- $X^0 = D$
- $X_i^\delta = X_i^{\delta-1}$ for all successor ordinals δ and every $i \in [1, n] \setminus J^\delta$
- $X_i^\delta = F_i(X^{\delta-1})$ for all successor ordinals δ and every $i \in J^\delta$
- $X^\lambda = \bigsqcup_{\beta<\lambda} X^\beta$ for limit ordinals

Examples of Chaotic Iterations

- *Jacobi iteration method*: $\forall \delta \in \mathbb{O} : J^\delta = [1, n]$
- *Gauss-Seidel iteration method*: $J^1 = \{1\}$, $J^\lambda = \{1\}$, λ is a limit ordinal, $J^\delta = \{1 + (j + 1 \bmod n)\}$ if δ is a successor ordinal and $J^{\delta-1} = \{j\}$.

Convergence theorem

THEOREM. If the $\langle L_i, \sqsubseteq_i \rangle$ are cpos/complete lattices, F is monotonic for the pointwise ordering $\sqsubseteq$ and $D \in$ prefp F then any chaotic iteration for F starting from D is an increasing chain which is ultimately stationary and its limit is $\mathsf{lfp}^{\sqsubseteq}_{D}\, F$. ■

PROOF. A special case of asyncronous iterations, see [7]. □

Reference

[7] P. Cousot. Asynchronous iterative methods for solving a fixed point system of monotone equations in a complete lattice. Res. rep. R.R. 88, Laboratoire IMAG, Université scientifique et médicale de Grenoble, Grenoble, France. Sep. 1977, 15 p.

Asynchronous iterations for a system of simultaneous fixpoint equations

- Let $\langle J^\delta,\ \delta \in \mathbb{O} \rangle$ be a transfinite sequence of subsets of $[1, n]$ which is *weakly fair*:

$$\forall \delta \in \mathbb{O} : \forall i \in [1, n] : \exists \alpha \geq \delta : i \in J^\alpha \qquad \text{(a)}$$

- Let $\langle S^\delta,\ \delta \in \mathbb{O} \rangle$ be a transfinite sequence of elements of $\mathbb{O}^n$ such that

$$\forall i \in [1, n] : \forall \delta \in \mathbb{O} : S^\delta_i < \delta \qquad \text{(b)}$$

$$\forall \delta \in \mathbb{O} : \forall i \in [1, n] : \exists \beta \geq \delta : \forall \alpha \geq \beta : \delta \leq S^\alpha_i \qquad \text{(c)}$$

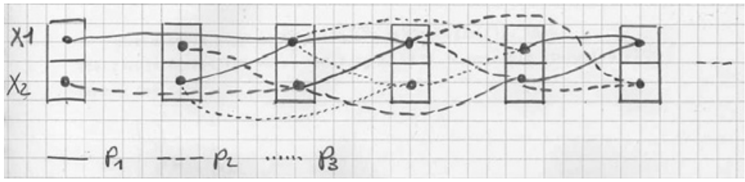
$$\forall \beta, \delta \in \mathbb{O} : [\beta \text{ is a limit ordinal} \wedge \beta < \delta] \implies [\forall i \in [1, n] : \beta \leq S^\delta_i] \qquad \text{(d)}$$

The asynchronous iterations from D for F defined by $\langle J^\delta,\ \delta \in \mathbb{O} \rangle$ and $\langle S^\delta,\ \delta \in \mathbb{O} \rangle$ are

- $X^0 = D$
- $X^\delta_i = X^{\delta-1}_i$ for all successor ordinals δ and every $i \in [1, n] \setminus J^\delta$
- $X^\delta_i = F_i(X_1^{S_1^\delta}, \ldots, X_n^{S_n^\delta})$ for all successor ordinals δ and every $i \in J^\delta$
- $X^\lambda = \bigsqcup_{\beta<\lambda} X^\beta$ for limit ordinals

Example: for chaotic iterations, choose $S^{\delta+1}_i = \delta$.

Intuition for asynchronous iterations for solving a system of simultaneous fixpoint equations on parallel computers



- X is stored in a global shared memory (with mutually exclusive read/write)
- At least one computation process is attached to the computation of $X^\delta_i = F_i(X_1^{S_1^\delta}, \ldots, X_n^{S_n^\delta})$ at time δ

- The processes are not synchronized
- All processes must be ultimately activated (weak fairness/justice) (a)
- The $X_j^{S_j^\delta}$, $j = 1, \ldots, n$ are previously read in the global memory, respectively at time $S_j^\delta < \delta$ (b)
- The computation of $F_i(X_1^{S_1^\delta}, \ldots, X_n^{S_n^\delta})$ is finite so the reading of the $X_j^{S_j^\delta}$, $j = 1, \ldots, n$ before computing X_i at time δ is bounded in time (c)
- In transfinite iterations the $X_j^{S_j^\delta}$, $j = 1, \ldots, n$ cannot be read prior to a limit ordinal

Convergence theorem

THEOREM. If the $\langle L_i, \sqsubseteq_i \rangle$ are cpos/complete lattices, F is monotonic for the pointwise ordering $\sqsubseteq$ and $D \in$ prefp F then any asynchronous iteration for F starting from D is ultimately stationary [6] and its limit is $\mathsf{lfp}_D^{\sqsubseteq} F$. ■

PROOF. A special case of asyncronous iterations with memory, see [8]. □

Reference

[8] P. Cousot. Asynchronous iterative methods for solving a fixed point system of monotone equations in a complete lattice. Res. rep. R.R. 88, Laboratoire IMAG, Université scientifique et médicale de Grenoble, Grenoble, France. Sep. 1977, 15 p.

[6] although it may not be an increasing chain.

The μ-calculus

The μ-calculus on a complete lattice

- $X \in \mathbb{X}$ variables
- $f\backslash n \in \mathbb{F}^n$ symbols of arity $n \in \mathbb{N}$
- $\mathbb{F} = \bigcup_{n\in\mathbb{N}} \mathbb{F}^n$ symbols
- $E \in \mathbb{E}$ μ-expressions over $\mathbb{X}$ and $\mathbb{F}$

$$\begin{array}{rcll}
E & ::= & 0 & \\
 & \mid & 1 & \\
 & \mid & E_1 \vee E_2 & \\
 & \mid & E_1 \wedge E_2 & \\
 & \mid & f\backslash n(E_1, \ldots, E_n) & \text{when } f\backslash n \in \mathbb{F}^n \\
 & \mid & \mu X.E & \\
 & \mid & \nu X.E & \\
 & \mid & X &
\end{array}$$

Interpretation of the μ-calculus

An *interpretation* I of the μ-calculus is

- A complete lattice $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$
- For each $f\backslash n \in \mathbb{F}^n$, $n \in \mathbb{N}$, a monotonic function $I\llbracket f\backslash n\rrbracket \in L^n \xrightarrow{\text{m}} L$

Semantics of the μ-calculus

The *semantics* $S^I \in \mathbb{E} \mapsto (\mathbb{X} \mapsto L) \mapsto L$ of a μ-expression is defined as follows:

$$
\begin{aligned}
S^I\llbracket 0\rrbracket\rho &\stackrel{\text{def}}{=} \bot\\
S^I\llbracket 1\rrbracket\rho &\stackrel{\text{def}}{=} \top\\
S^I\llbracket E_1 \vee E_2\rrbracket\rho &\stackrel{\text{def}}{=} S^I\llbracket E_1\rrbracket\rho \sqcup S^I\llbracket E_2\rrbracket\rho\\
S^I\llbracket E_1 \wedge E_2\rrbracket\rho &\stackrel{\text{def}}{=} S^I\llbracket E_1\rrbracket\rho \sqcap S^I\llbracket E_2\rrbracket\rho\\
S^I\llbracket f\backslash n(E_1, \ldots, E_n)\rrbracket\rho &\stackrel{\text{def}}{=} I\llbracket f\backslash n\rrbracket(S^I\llbracket E_1\rrbracket\rho, \ldots, S^I\llbracket E_n\rrbracket\rho)\\
S^I\llbracket \mu X.E\rrbracket\rho &\stackrel{\text{def}}{=} \mathsf{lfp}^{\sqsubseteq}\ \lambda x \in L \cdot S^I\llbracket E\rrbracket\rho[X := x]\\
S^I\llbracket \nu X.E\rrbracket\rho &\stackrel{\text{def}}{=} \mathsf{gfp}^{\sqsubseteq}\ \lambda x \in L \cdot S^I\llbracket E\rrbracket\rho[X := x]\\
S^I\llbracket X\rrbracket\rho &\stackrel{\text{def}}{=} \rho(X)
\end{aligned}
$$

Well-definedness of the semantics of the μ-calculus

THEOREM. $\forall E \in \mathbb{E} : S^I\llbracket E\rrbracket$ is well-defined. ■

PROOF. – $\langle \mathbb{X} \mapsto L,\ \dot\sqsubseteq,\ \dot\bot,\ \dot\top,\ \dot\sqcup,\ \dot\sqcap\rangle$ is a complete lattice for the pointwise ordering.

- We prove $S^I\llbracket E\rrbracket$ to be monotonic and well-defined by structural induction on E
- the constant functions $S^I\llbracket 0\rrbracket = \lambda\rho \cdot \bot$ and $S^I\llbracket 1\rrbracket = \lambda\rho \cdot \top$ are monotonic and well-defined
- The pointwise join and meet of monotonic and well-define functions on a complete lattice are monotonic and well-defined
- If $S^I\llbracket E\rrbracket$ is well-defined and monotonic then $x \sqsubseteq y$ implies $\rho[x := X] \dot\sqsubseteq \rho[y := X]$ so $S^I\llbracket E\rrbracket\rho[x := X] \sqsubseteq S^I\llbracket E\rrbracket\rho[y := X]$ proving $\lambda x \in L \cdot S^I\llbracket E\rrbracket\rho[x := X]$ to be a monotonic operator on the complete lattice $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ so that, by Kanster-Tarski, $S^I\llbracket \mu X.E\rrbracket \stackrel{\text{def}}{=} \lambda\rho \cdot \mathsf{lfp}^{\sqsubseteq}\ \lambda x \in L \cdot S^I\llbracket E\rrbracket\rho[x := X]$ is well-defined

- To prove that $S^I\llbracket \mu X.E\rrbracket$ is monotonic, assume $\rho \dot\sqsubseteq \rho'$. By antisymmetry, $\rho[x := X] \dot\sqsubseteq \rho'[x := X]$. Hence $S^I\llbracket E\rrbracket\rho[x := X]S^I \sqsubseteq \llbracket E\rrbracket\rho'[x := X]$ since $S^I\llbracket E\rrbracket$ is monotonic by induction hypothesis. It follows that $\lambda x \in L \cdot S^I\llbracket E\rrbracket\rho[x := X] \dot\sqsubseteq \lambda x \in L \cdot S^I\llbracket E\rrbracket\rho'[x := X]$ so that, by the theorem on "fixpoints of pointwise comparable monotone operators on a complete lattice":
$$\mathsf{lfp}^{\sqsubseteq}\ \lambda x \in L \cdot S^I\llbracket E\rrbracket\rho[x := X] \sqsubseteq \mathsf{lfp}^{\sqsubseteq}\ \lambda x \in L \cdot S^I\llbracket E\rrbracket\rho'[x := X]$$
proving $S^I\llbracket \mu X.E\rrbracket = \lambda\rho \cdot \mathsf{lfp}^{\sqsubseteq}\ \lambda x \in L \cdot S^I\llbracket E\rrbracket\rho[x := X]$ to be monotone
- By duality, $S^I\llbracket \nu X.E\rrbracket = \lambda\rho \cdot \mathsf{gfp}^{\sqsubseteq}\ \lambda x \in L \cdot S^I\llbracket E\rrbracket\rho[x := X]$ is well-defined and monotone.
- Finally, $S^I\llbracket X\rrbracket = \lambda\rho \cdot \rho(X)$ is well-defined and monototne since $\rho \dot\sqsubseteq \rho'$ implies $\rho(X) \dot\sqsubseteq \rho(X')$ so $S^I\llbracket X\rrbracket\rho \sqsubseteq S^I\llbracket X\rrbracket\rho'$

□

Kozen's μ-calculus

- $p, q, \ldots \in \mathsf{Prop}$ propositional formuæ
- $X, Y, \ldots \in \mathsf{Var}$ variables
- $a, b, \ldots \in \mathsf{Act}$ actions
- We choose
  - $\mathbb{X} = \mathsf{Var}$
  - $\mathbb{F}^0 = \mathsf{Prop}$
  - $\mathbb{F}^1 = \{[a], {<}a{>} \mid a \in \mathsf{Act}\}$
  - $\mathbb{F}^n = \emptyset$, for $n > 1$

- The interpretation is relative to a labelled transition system $\langle S,\ R,\ I\rangle$ such that
  - S is a non-empty set of states
  - $R \in \mathsf{Act} \mapsto \wp(S \times S)$ assigns a transition relation to each action $a \in \mathsf{Act}$ [7]
  - $I \in \mathsf{Prop} \mapsto \wp(S)$ is an interpretation of the propositional formuæ [8]
  - The considered complete lattice is $\langle \wp(S),\ \subseteq,\ \emptyset,\ S,\ \cup,\ \cap\rangle$
  - The interpretation of the symbols is

[7] so that the classical transition relation is $t = \bigcup_{a \in \mathsf{Act}} R(a)$

[8] $I[\![p]\!]$ is the set of states in which p holds.

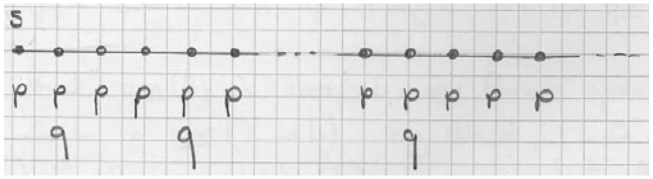
$$\begin{aligned}
I[\![[a]]\!] &\in \wp(S) \mapsto \wp(S)\\
I[\![[a]]\!]X &\stackrel{\text{def}}{=} \mathrm{pre}[R(a)]X\\
&= \{s \mid \exists s' \in X : \langle s,\ s'\rangle \in R(a)\}\\
I[\![{<}a{>}]\!] &\in \wp(S) \mapsto \wp(S)\\
I[\![{<}a{>}]\!]X &\stackrel{\text{def}}{=} \widetilde{\mathrm{pre}}[R(a)]X\\
&= \{s \mid \forall s' : \langle s,\ s'\rangle \in R(a) \Longrightarrow s' \in X\}
\end{aligned}$$

so that the meaning of a formula is the set of states for which the formula is satisfied.

Example: $\mathsf{Act} = \{a\}$, $\mathsf{Prop} = \{p, q\}$. The formula

$$\nu Z.(p \wedge [a](\mu Y.(Z \wedge q) \vee (p \wedge {<}a{>}Y))$$

characterizes all states from which there is a path along which p holds continuously and q holds infinitely often on that path.



Hardly readable for complex statements.

Lattice theoretic fixpoint-based and rule-based formal definitions

Reference

[9] P. Cousot & R. Cousot. Compositional and inductive semantic definitions in fixpoint, equational, constraint, closure-condition, rule-based and game-theoretic form, invited paper. *In : Computer Aided Verification, Proc. 7th International Conference, CAV'95*, P. Wolper (ed.), pp. 293–308. Springer-Verlag. 1995.

Example of equivalent rule-based and fixpoint-based formal definitions

– The set of odd natural numbers is defined as follows:

- 1 is odd
- if n is odd then $n+2$ is odd

– This definition can be understood as a formal system

- Axiom: $1 \in \mathsf{odd}$
- Inference rule: $\dfrac{n \in \mathsf{odd}}{n+2 \in \mathsf{odd}}$

– This formal system can be instanciated in an infinite set of rule, as follows:

- Axiom: $\dfrac{\emptyset}{1}$
- Inference rule: $\dfrac{\{n\}}{n+2}$, $n \in \mathbb{N}$

of the form $\dfrac{P}{c}$ $\begin{array}{l}\leftarrow \text{premisse} \subseteq U \text{ (Universe)}\\ \leftarrow \text{conclusion} \in U\end{array}$

– The rules define a subset $S \subseteq U$ of the universe U, which is the set of all x which can be shown to derive from the rules by a formal proof, that is

- $\forall i \in [1, n] : \exists \dfrac{P}{c_i} : P \subseteq \{c_1, \ldots, c_{i-1}\}$
- $c_n = x$

– For example $1, 3, 5, 7$ is a proof than $7 \in$ odd by $\frac{\emptyset}{1}$, $\frac{1}{3}$, $\frac{3}{5}$ a,d $\frac{5}{7}$.

– To prove that 4 is not odd, observe that $\frac{2}{4}$ is the only rule with 4 as conclusion so we must prove 2 to be odd, $\frac{0}{2}$ is the only rule with 2 as conclusion so we must prove 0 to be odd which is impossible since no rule has 0 as conclusion.

– If we define

$$F \stackrel{\text{def}}{=} \lambda X \cdot \{c \mid \exists \frac{P}{c} : P \subseteq X\}$$

then $S = \mathsf{lfp}^{\subseteq}_{\emptyset}\ F$.

– For example odd $= \mathsf{lfp}^{\subseteq}_{\emptyset}\ \lambda X \cdot \{1\} \cup \{n+2 \mid n \in X\}$ with iterates $\emptyset$, $\{1\}$, $\{1, 3\}$, $\{1, 3, 5\}$, ...

Equivalence of the rule-based and fixpoint-based formal definitions of a set

– A *formal system* is a pair $\langle U, R\rangle$ where the *universe* U is a set and R is a *set of rules* $\langle P, c\rangle$, written $\frac{P}{c}$ where $P \in \wp(U)$ and $c \in U$

– A proof of x by $\langle U, R\rangle$ is a finite sequence $c_1, \ldots, c_n$ of elements $c_i \in U$ such that

- $\forall i \in [1, n] : \exists \frac{P}{c_i} : P \subseteq \{c_1, \ldots, c_{i-1}\}$
- $c_n = x$

– The set S *defined by* $\langle U, R\rangle$ is defined by the *proof-theoretic semantics* as

$$S \stackrel{\text{def}}{=} \{x \in U \mid \exists \text{ a proof of } x \text{ by } \langle U, R\rangle\}$$

– The *operator* for $\langle U, R\rangle$ is

$$F \in \wp(U) \mapsto \wp(U)$$

$$F \stackrel{\text{def}}{=} \lambda X \cdot \{c \mid \exists P \subseteq X : \frac{P}{c} \in R\}$$

– Observe that F is $\subseteq$-monotone and indeed a complete join morphism

- The set *S defined by $\langle U,\ R\rangle$* is defined by the *fixpoint-theoretic semantics* as

$$S \overset{\text{def}}{=} \mathsf{lfp}^{\subseteq}_{\emptyset}\ F$$

THEOREM. The proof-theoretic and fixpoint-theoretic definitions of the set S defined by a formal system $\langle U,\ R\rangle$ are equivalent ■

PROOF. – Observe that F is a complete $\cup$-morphism whence upper-continuous and so the iterates $\langle F^\delta,\ \delta \in \mathbb{O}\rangle$ converge to $\mathsf{lfp}^{\subseteq}_{\emptyset}\ F$ at rank ω by the Kleene fixpoint theorem on page 9.

- Let $x \in S$ with proof $c_1, \ldots, c_n = x$
  - $n = 0$ is impossible since a proof is not empty
  - if $n = 1$ then $\dfrac{\emptyset}{c_1} \in R$ and so $c_1 \in F^1 = F(\emptyset) = \{c \mid \exists P \subseteq \emptyset : \dfrac{P}{c} \in R\} = \{c \mid \dfrac{\emptyset}{c} \in R\}$.
  - Assume, by induction hypothesis that F^{n-1} contains $c_1, \ldots, c_{n-1}$. Then, by def. of proofs, $\exists P >\subseteq \{c_1, \ldots, c_{n-1}\} : \dfrac{P}{c_n} \in R$ so, by induction hypothesis, $\exists P \subseteq F^{n-1} : \dfrac{P}{c_n} \in R$ and so $c_n \in F(F^{n-1}) = \{c \mid \exists P \subseteq F^{n-1} : \dfrac{P}{c} \in R\}$ and so $c_1, \ldots, c_n \in F^n = \bigcup_{k<n} F(F^k)$ (using the alternative definition of the iterates on page 41).
  - Passing to the limit, $x \in F^n \subseteq \bigcup_{n\in\mathbb{N}} F^n = F^\omega = \mathsf{lfp}^{\subseteq}_{\emptyset}\ F = S$

- Inversely, let $\langle F^\delta,\ \delta \leq \omega\rangle$ be the iterates of F. If $x \in F^\omega = \bigcup_{n\geq 0} F^n$ then their exists $n \geq 1$ such that $x \in F^n$. We show that x has a proof by recurrence on n.
  - If $n = 1$, $x \in F^1 = F(\emptyset) = \{c \mid \langle\emptyset,\ c\rangle \in R\}$ so $\dfrac{\emptyset}{x}$ hence the proof of x is simply x
  - Assume that for all $c \in F^{n-1}$, there is a proof of c in $\langle U,\ R\rangle$. If $x \in F^n = F(F^{n-1}) = \{c \mid \exists P \subseteq F^{n-1} : \langle P,\ c\rangle n R\}$, we have $\langle P,\ x\rangle \in R$ with $P \subseteq F^{n-1}$. Assume $P = \{c_1, \ldots, c_k\}$ and let p_i be the proof of c_i, $i = 1, \ldots, k$ which does exist by induction hypothesis. The proof of x is $p_1 p_2 \ldots p_n x$. Since each p_i ends with c_i, $\dfrac{\{c_1, \ldots, c_k\}}{x} \in R$, the proof is well-defined.
- By recurrence, all $x \in F^n$ have a proof, whence all $x \in \mathsf{lfp}^{\subseteq}_{\emptyset}\ F$ have a proof. □

Example 1 of equivalent formal definitions

The universe is $U = \mathbb{N}$. We want to define the subset odd $\subseteq U$ of odd numbers. Then are several equivalent methods

1. Rule-based formal system: odd is defined by the following axiom and rule schemata

$$1 \in \text{odd} \qquad \frac{n \in \text{odd}}{n + 2 \in \text{odd}}$$

2. Fixpoint definition: odd is the $\subseteq$-least solution to the equation

$$X = \{1\} \cup \{n+2 \mid n \in X\}$$

3. Constraint definition: odd is the $\subseteq$-least solution to the constraint

$$\{1\} \cup \{n+2 \mid n \in X\} \subseteq X$$

or equivalently to the set of constraints:

$$\begin{cases} 1 \in X \\ \{n+2 \mid n \in X\} \subseteq X \end{cases}$$

4. Closure conditions: odd is the smallest subset of U satisfying:

$$\begin{cases} \bullet\ 1 \in X \\ \bullet\ n \in X \Longrightarrow n+2 \in X \end{cases}$$

which we can write as

$$\begin{aligned} \forall x \in \wp(\mathbb{N}) : \quad & x \subseteq 1 \Longrightarrow x \subseteq X \\ & \wedge\ x \subseteq \{n+2 \mid n \in X\} \Longrightarrow x \subseteq X \end{aligned}$$

which is equivalent to

$$\forall x \in \wp(\mathbb{N}) : C(x, X) \Longrightarrow x \subseteq X$$

where

$$C(x, X) \overset{\text{def}}{=} (x = \{1\}) \vee (x \subseteq \{n+2 \mid n \in X\})$$

satisfying $C(x, X) \wedge X \subseteq Y \Longrightarrow C(x, Y)$

The reasoning on subsets of the universe U on the complete lattice $\langle \wp(U), \subseteq, \emptyset, S, \cup, \cap \rangle$ [10] can be generalized to a complete lattice $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ with the objective of defining $S \in L$ [9].

The generalization is obtained by replacing subsets by elements of L such as

$$\frac{P}{c} \rightsquigarrow \frac{P}{\{c\}}$$

$$F = \lambda X \cdot \{c \mid \exists \frac{P}{c} \in R : P \subseteq X\} \rightsquigarrow F = \lambda X \cdot \bigcup \{\{c\} \mid \exists \frac{P}{\{c\}} \in R : P \subseteq X\}$$

Reference

[10] P. Aczel. An introduction to inductive definitions. In J. Barwise, editor, *Handbook of Mathematical Logic*, volume 90 of *Studies in Logic and the Foundations of Mathematics*, pages 739–782. Elsevier Science Publishers B.V. (North-Holland), Amsterdam, 1977.

Example 2: set of regular expressions generated by the grammar of regular expressions

- The set $\mathcal{R}(A)$ of regular expressions ρ is defined by the grammar $(a \in A)$:

$$\rho ::= \epsilon \mid a \mid \rho_1 | \rho_2 \mid \rho_1 \rho_2 \mid \rho^\star \mid (\rho)$$

- Fixpoint definition:

$$\begin{aligned} \mathcal{R}(A) = \mathsf{lfp}^{\subseteq}\ \lambda X \cdot\ & \{\epsilon\} \\ & \cup\ A \\ & \cup\ \{\rho_1 | \rho_2 \mid \rho_1 \in X \wedge \rho_2 \in X\} \\ & \cup\ \{\rho_1 \rho_2 \mid \rho_1 \in X \wedge \rho_2 \in X\} \\ & \cup\ \{\rho^\star \mid \rho \in X\} \\ & \cup\ \{(\rho) \mid \rho \in X\} \end{aligned}$$

– Equational definition: $\mathcal{R}(A)$ is the $\subseteq$-least solution to:

$$\begin{array}{rl} X = & \{\epsilon\} \\ & \cup\ A \\ & \cup\ \{\rho_1|\rho_2 \mid \rho_1 \in X \wedge \rho_2 \in X\} \\ & \cup\ \{\rho_1\rho_2 \mid \rho_1 \in X \wedge \rho_2 \in X\} \\ & \cup\ \{\rho^\star \mid \rho \in X\} \\ & \cup\ \{(\rho) \mid \rho \in X\} \end{array}$$

– Constraint-based definition: $\mathcal{R}(A)$ is the $\subseteq$-least solution to the system[9] of constraints:

$$\begin{array}{r} \epsilon \in X \\ A \subseteq X \\ \{\rho_1|\rho_2 \mid \rho_1 \in X \wedge \rho_2 \in X\} \subseteq X \\ \{\rho_1\rho_2 \mid \rho_1 \in X \wedge \rho_2 \in X\} \subseteq X \\ \{\rho^\star \mid \rho \in X\} \subseteq X \\ \{(\rho) \mid \rho \in X\} \subseteq X \end{array}$$

[9] More precisely “conjunction”.

– Closure-condition definition: $\mathcal{R}(A)$ is the $\subseteq$-least element X of $\wp(A^{\vec{*}})$[10] satisfying:

$$\begin{array}{rcl} & \epsilon & \in \ X \\ a \in A & \Longrightarrow & a \in X \\ \rho_1 \in X \wedge \rho_2 \in X & \Longrightarrow & \rho_1|\rho_2 \in X \\ \rho_1 \in X \wedge \rho_2 \in X & \Longrightarrow & \rho_1\rho_2 \in X \\ \rho \in X & \Longrightarrow & \rho^\star \in X \\ \rho \in X & \Longrightarrow & (\rho) \in X \end{array}$$

[10] $\wp(S)$ is the power set, i.e. set of subsets of the set S.

The corresponding informal definition is:

1. ϵ is a regular expression; *empty*
2. If $a \in A$ then a is a regular expression; *letter*
3. If ρ_1 and ρ_2 are regular expressions then:
   3.1 $\rho_1|\rho_2$ *alternative*
   3.2 $\rho_1\rho_2$ *concatenation*
   are regular expressions;
4. If ρ is a regular expression then:
   4.1 $\rho^\star$ *repetition, 0 or more times*
   4.2 (ρ) *parenthesized expression*
   are regular expressions.

- Rule-based definition:
  - Axioms and rule schemata of the formal system defining the regular expressions [11]:

$$\epsilon \in \mathcal{R}(A) \qquad \frac{a \in A}{a \in \mathcal{R}(A)} \qquad \frac{\rho_1 \in \mathcal{R}(A),\ \ \rho_2 \in \mathcal{R}(A)}{\rho_1|\rho_2 \in \mathcal{R}(A)}$$

$$\frac{\rho_1 \in \mathcal{R}(A),\ \ \rho_2 \in \mathcal{R}(A)}{\rho_1\rho_2 \in \mathcal{R}(A)} \qquad \frac{\rho \in \mathcal{R}(A)}{\rho^\star \in \mathcal{R}(A)} \qquad \frac{\rho \in \mathcal{R}(A)}{(\rho) \in \mathcal{R}(A)}$$

[11] These axioms and rule schemata should be understood informally since their meta-semantics has not been formally defined.

- Interpretation of these axioms and rule schemata as a set of rule instances (for all $a \in A$, ρ, ρ_1, $\rho_2 \in A^{\vec{*}}$):

$$\frac{\emptyset}{\epsilon} \qquad \frac{\emptyset}{a} \qquad \frac{\{\rho_1,\ \rho_2\}}{\rho_1|\rho_2}$$

$$\frac{\{\rho_1,\ \rho_2\}}{\rho_1\rho_2} \qquad \frac{\{\rho\}}{\rho^\star} \qquad \frac{\{\rho\}}{(\rho)}$$

- We use here the traditional notation $\frac{P}{c}$ which we have changed to $\frac{P}{\{c\}}$ in order to generalize this classical set-based definition into order-theoretic rule-based inference systems.

Example 3: formal definition of the reflexive transitive closure of a binary relation

- Fixpoint definition: $t^\star = \mathsf{lfp}^{\subseteq}\ \lambda X \cdot 1_S \cup t \circ X$
- Equational definition: $t^\star$ is the $\subseteq$-least solution to $X = 1_S \cup t \circ X$
- Constraint based definition: $t^\star$ is the $\subseteq$-least X satiwfying

$$\begin{cases} 1_S \subseteq X \\ t \circ X \subseteq X \end{cases}$$

- Closure-condition based definition: $t^\star$ is the $\subseteq$-least X satifying

$$\begin{cases} \forall x \in S : \langle x,\ x\rangle \in X \\ \forall x, y, z \in S : (\langle x,\ y\rangle \in t \wedge \langle y,\ z\rangle \in X) \Longrightarrow \langle x,\ z\rangle \in X \end{cases}$$

- Rule-based definition: $t^\star$ is generated by the following axiom and rule schemata:

$$\langle x,\ x\rangle \in X \qquad \frac{\langle x,\ z\rangle \in t \circ X}{\langle x,\ z\rangle \in X}$$

interpreted as follows:

$$R = \left\{ \frac{\emptyset}{\langle x,\ x\rangle} \middle| x \in S \right\} \cup \left\{ \frac{\{\langle y,\ z\rangle\}}{\langle x,\ z\rangle} \middle| \langle x,\ y\rangle \in t \right\}$$

Definition, semantics and equivalence of lattice theoretic formal definitions

- Fixpoint definition: $S = \mathsf{lfp}^{\sqsubseteq} F$ [12] where $F \in L \xrightarrow{\mathrm{m}} L$ on $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$
- Equational definition:
  - Definition: S is the $\sqsubseteq$-least solution to the equation $X = F(X)$ where $F \in L \xrightarrow{\mathrm{m}} L$ on $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$
  - Semantics: $S = \mathsf{lfp}^{\sqsubseteq} F$ [12]
  - Equivalence: trivial

[12] Well-defined by Knaster-Tarski fixpoint theorem.

- Constraint based definition:
  - Definition: S is the $\sqsubseteq$-least solution to the constraint $F(X) \sqsubseteq X$ where $F \in L \xrightarrow{\mathrm{m}} L$ on $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$
  - Semantics: $S = \mathsf{lfp}^{\sqsubseteq} F$ [12]
  - Equivalence: Trivial since $\mathsf{lfp}^{\sqsubseteq} F = \bigsqcap\{X \in L \mid F(X) \sqsubseteq X\}$ by Knaster-Tarski fixpoint theorem so that $\mathsf{lfp}^{\sqsubseteq} F$ is thye elast solution to the constraint $F(X) \sqsubseteq X$ on L

- Closure-condition based definition:
  - Definition: $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ is a complete lattice and $C \in \wp(L \times L)$ satisfies

$$C(x, X) \wedge X \sqsubseteq Y \Longrightarrow C(x, Y) \qquad (2)$$

S is the $\sqsubseteq$-least element of L satisfying

$$\forall x \in L : C(x, X) \Longrightarrow x \sqsubseteq X \qquad (3)$$

  - Semantics: $S = \mathsf{lfp}^{\sqsubseteq} F$ where $F \stackrel{\mathrm{def}}{=} \lambda X \cdot \bigsqcup\{x \in L \mid C(x, X)\}$

Proof. $F \stackrel{\mathrm{def}}{=} \lambda X \cdot \bigsqcup\{x \in L \mid C(x, X)\}$ is monotone since $X \sqsubseteq Y$ implies $\{x \in L \mid C(x, X)\} \subseteq \{x \in L \mid C(x, Y)\}$ so $F(X) = \bigsqcup\{x \in L \mid C(x, X)\} \sqsubseteq \bigsqcup\{x \in L \mid C(x, Y)\} = F(Y)$.

Since $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ is a complete lattice and $F \in L \xrightarrow{\mathrm{m}} L$ is monotonic, $\mathsf{lfp}^{\sqsubseteq} F$ does exist by Knaster-Tarski fixpoint theorem

- If $C(x, \mathsf{lfp}^{\sqsubseteq} F)$ then $x \sqsubseteq \bigsqcup\{y \in L \mid C(y, \mathsf{lfp}^{\sqsubseteq} F)\} = F(\mathsf{lfp}^{\sqsubseteq} F) = \mathsf{lfp}^{\sqsubseteq} F$ so $X = \mathsf{lfp}^{\sqsubseteq} F$ satisfies (3)
- If $X \in L$ satisfies (3), then $F(X) = \bigsqcup\{x \in L \mid C(x, X)\} \sqsubseteq X$ proving $\mathsf{lfp}^{\sqsubseteq} F \sqsubseteq X$ by by Knaster-Tarski fixpoint theorem.
- $S = \mathsf{lfp}^{\sqsubseteq} F$ is therefore the $\sqsubseteq$-least element of L statisfying (3).

□

- Equivalence:
  - If $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ is a complete lattice and $F \in L \xrightarrow{\mathrm{m}} L$ then the closure condition $C(x, X) = x \sqsubseteq F(X)$ defines $S = \mathsf{lfp}^{\sqsubseteq} F$

Proof. - The closure-condition C is monotonic since if $C(x, X) \wedge X \sqsubseteq Y$ then $x \sqsubseteq F(X) \wedge F(X) \sqsubseteq F(Y)$ hence $x \sqsubseteq F(Y)$ that is $C(x, Y)$;

- The $\sqsubseteq$-least S satisfying the closure condition is: $S = \mathsf{lfp}^{\sqsubseteq}\, \lambda X \cdot \bigsqcup\{x \in L \mid C(x, X)\} = \mathsf{lfp}^{\sqsubseteq}\, \lambda X \cdot \bigsqcup\{x \in L \mid x \sqsubseteq F(X)\} = \mathsf{lfp}^{\sqsubseteq}\, \lambda X \cdot F(x) = \mathsf{lfp}^{\sqsubseteq}\, F$.

  Inversely, we have that given a definition $S \in L$ by (3), we can write it in fixpoint form $S = \mathsf{lfp}^{\sqsubseteq}\, F$ where $F(X) = \bigsqcup\{x \in L \mid C(x, X)\}$. □

– Rule-based definition:

- Definition: $\langle L,\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap\rangle$ is a complete lattice and $R = \{\langle P_i,\ c_i\rangle | i \in \Delta\}$ is a set of rules where P_i, $c_i \in L$, $i \in \Delta$
- Semantics: $S = \mathsf{lfp}^{\sqsubseteq}\, F$ [12] where $F = \lambda X \cdot \bigsqcup\{c_i \mid \exists P_i \sqsubseteq X : \dfrac{P_i}{c_i} \in R\}$

- Equivalence:
  - A rule-based definition can obviously be specified in fixpoint form as stated above
  - Inversely, let $F \in L \overset{\mathrm{m}}{\longmapsto} L$. Then $\mathsf{lfp}^{\sqsubseteq}\, F$ can be defined by the rules $R = \{\dfrac{P}{c} \mid c, P \in L \wedge c \sqsubseteq F(P)\}$

  Proof. - We let $\Psi(X) \overset{\mathrm{def}}{=} \{C \mid \exists P \in L : P \sqsubseteq X \wedge C \sqsubseteq F(P)\}$;
  - For all $X \in L$, $X \sqsubseteq X \wedge F(X) \sqsubseteq F(X)$ whence $F(X) \in \Psi(X)$ proving that $F(X) \sqsubseteq \lambda X \cdot \sqcup \Psi(X)$;
  - If $C \in \Psi(X)$, we have $P \sqsubseteq X$ whence $F(P) \sqsubseteq F(X)$ and $C \sqsubseteq F(P)$ whence $C \sqsubseteq F(X)$ proving that $\lambda X \cdot \sqcup \Psi(X) \sqsubseteq F(X)$;
  - By antisymetry, $\lambda X \cdot \sqcup \Psi(X) = F(X)$;
  - In conclusion, R defines $\mathsf{lfp}^{\sqsubseteq}\, \lambda X \cdot \sqcup \Psi(X) = \mathsf{lfp}^{\sqsubseteq}\, F$. □

Derivation (generalizing proofs)

– Let $R = \left\{\dfrac{P_i}{C_i} \;\middle|\; i \in \Delta\right\}$ and $\Phi \overset{\mathrm{def}}{=} \lambda X \cdot \bigsqcup\{C_i \mid \exists i \in \Delta : P_i \sqsubseteq X\}$;

– A *derivation* of an element x of the complete lattice $\langle \mathcal{D},\ \sqsubseteq\rangle$ is a transfinite sequence x_κ, $\kappa \leq \lambda$, $\lambda \in \mathbb{O}$ such that:
  - $x_0 = \bot$,
  - $x_\kappa \sqsubseteq \Phi(\bigsqcup_{\beta<\kappa} x_\beta)$ for all $0 < \kappa \leq \lambda$,
  - $x_\lambda = x$;

– An element x of the complete lattice $\langle \mathcal{D},\ \sqsubseteq\rangle$ is said to be *derivable* whenever it has a derivation;

– An alternative definition of the semantics S of $\langle L,\ R\rangle$ is

$$S = \bigsqcup\{x \in L \mid x \text{ is derivable by } \langle L,\ R\rangle\}$$

Example: derivation of a regular expression

- Axioms and rule instances[13]:

$$\frac{\emptyset}{\epsilon} \qquad \frac{\emptyset}{a} \qquad \frac{\{\rho_1,\ \rho_2\}}{\rho_1|\rho_2} \qquad \frac{\{\rho_1,\ \rho_2\}}{\rho_1\rho_2} \qquad \frac{\{\rho\}}{\rho^\star} \qquad \frac{\{\rho\}}{(\rho)}$$

- $\varPhi(X) = \{\epsilon\} \cup \{a \mid a \in A\} \cup \{\rho_1|\rho_2, \rho_1\rho_2, \rho^\star, (\rho) \mid \rho_1, \rho_2, \rho \in X\}$
- Example of derivation (proof that $(a|b)^\star \in \mathcal{R}(\{a, b\})$):

$$\begin{aligned}
x_0 &= \emptyset \\
x_1 &= \{a\} && \subseteq \varPhi(x_0) \\
x_2 &= \{b\} && \subseteq \varPhi(x_0) \\
x_3 &= \{a|b\} && \subseteq \varPhi(x_1 \cup x_2) \\
x_4 &= \{(a|b)^\star\} && \subseteq \varPhi(x_3)
\end{aligned}$$

[13] We use the traditional $\frac{P}{c}$ for our $\frac{P}{\{c\}}$.

Equivalence of the fixpoint and derivation-based semantics of rule-based formal definitions

An element $x \in \mathcal{D}$ is derivable if and only if $x \sqsubseteq \mathsf{lfp}^{\sqsubseteq}\, \varPhi$ so that:

$$\mathsf{lfp}^{\sqsubseteq}\, \varPhi = \bigsqcup\{x \in \mathcal{D} \mid x \text{ is derivable}\}$$

Proof. – Let $\varPhi^\kappa$, $\kappa \in \mathbb{O}$ be the iterates of $\varPhi$ starting from $\perp$ and x_κ, $\kappa \leq \lambda$ be a derivation of x;

- By transfinite induction, $\forall \kappa \leq \lambda : x_\kappa \sqsubseteq \varPhi^\kappa$:
  - We have $x_0 = \perp = \varPhi^0$.
  - Assume by induction hypothesis that $\forall \beta < \kappa : x_\beta \sqsubseteq \varPhi^\beta$. It follows that $\bigsqcup_{\beta<\kappa} x_\beta \sqsubseteq \bigsqcup_{\beta<\kappa} \varPhi^\beta$ hence $x_\kappa \sqsubseteq \varPhi(\bigsqcup_{\beta<\kappa} x_\beta) \sqsubseteq \varPhi(\bigsqcup_{\beta<\kappa} \varPhi^\beta) = \varPhi^\kappa$;

- Since $\varPhi^\kappa$, $\kappa \in \mathbb{O}$ is an increasing chain which ultimately stabilizes to $\mathsf{lfp}^{\sqsubseteq}\, \varPhi$, it follows that $\forall \kappa \leq \lambda : x_\kappa \sqsubseteq \mathsf{lfp}^{\sqsubseteq}\, \varPhi$ hence in particular $x = x_\lambda \sqsubseteq \mathsf{lfp}^{\sqsubseteq}\, \varPhi$.
- We have shown that $\bigsqcup\{x \in \mathcal{D} \mid x \text{ is derivable}\} \sqsubseteq \mathsf{lfp}^{\sqsubseteq}\, \varPhi$;
- For the reciprocal, the iterates $\varPhi^\kappa, \kappa \leq \lambda$ for $\varPhi$ starting from $\perp$ form a derivation of $\mathsf{lfp}^{\sqsubseteq}\, \varPhi$, since $\mathsf{lfp}^{\sqsubseteq}\, \varPhi$ is some $\varPhi^\epsilon$; It follows that $\mathsf{lfp}^{\sqsubseteq}\, \varPhi \sqsubseteq \bigsqcup\{x \in \mathcal{D} \mid x \text{ is derivable}\}$;
- By antisymetry, $\mathsf{lfp}^{\sqsubseteq}\, \varPhi = \bigsqcup\{x \in \mathcal{D} \mid x \text{ is derivable}\}$;
- All other $x \sqsubseteq \mathsf{lfp}^{\sqsubseteq}\, \varPhi$ are also derivable:
  - Let λ be the least ordinal such that $x \sqsubseteq \varPhi^\lambda$ (such an ordinal exists since $x \sqsubseteq \varPhi^\epsilon = \mathsf{lfp}^{\sqsubseteq}\, \varPhi$);
  - A derivation of x is simply $x_\kappa, \kappa \leq \lambda$ with $x_\kappa = \varPhi^\kappa$ for $\kappa < \lambda$ and $x_\lambda = x$.

□

Join-Irreducible Rules

- Let $\langle \mathcal{D}, \sqsubseteq \rangle$ be a complete lattice satisfying (DCC).
- Let R be a set of rule instances and $\varPhi_R$ be the corresponding R-operator.
- Let $\varPhi_S$ be the S-operator for rule instances:

$$S = \left\{ \frac{P}{c} \;\middle|\; \exists \frac{P}{C} \in R : c \in \mathcal{I}(C) \right\}^{14}$$

- Then $\mathsf{lfp}^{\sqsubseteq}\, \varPhi_S = \mathsf{lfp}^{\sqsubseteq}\, \varPhi_R$.

[14] Recall that $\mathcal{I}(C)$ is the set of join-irreducibles of C.

PROOF. – For all $X \in \mathcal{D}$, $\Phi_R(X) = \bigsqcup\{C \mid \exists\frac{P}{C} \in R : P \sqsubseteq X\} = \bigsqcup\{\bigsqcup\mathcal{I}(C) \mid \exists\frac{P}{C} \in R : P \sqsubseteq X\} = \bigsqcup\{c \mid \exists\frac{P}{C} \in R : c \sqsubseteq C \wedge c \in \mathcal{I}(\mathcal{D}) \wedge P \sqsubseteq X\} = \bigsqcup\{c \mid \exists\frac{P}{c} \in S : P \sqsubseteq X\} = \Phi_S(X)$.

- For the respective iterates Φ_R^κ and Φ_S^κ, $\kappa \in \mathbb{O}$ of Φ_R and Φ_S, we have $\Phi_R^0 = \Phi_S^0 = \bigsqcup\emptyset = \bot$.
- Assume, by induction hypothesis, that $\forall\beta < \kappa$, $\Phi_R^\kappa = \Phi_S^\kappa$. We have $\Phi_R^\kappa = \Phi_R(\bigsqcup_{\beta<\kappa}\Phi_R^\beta\Big) = \Phi_S(\bigsqcup_{\beta<\kappa}\Phi_S^\beta\Big) = \Phi_S^\beta$.
- By induction $\Phi_S^\kappa = \Phi_R^\kappa$ for all $\kappa \in \mathbb{O}$ proving that $\mathsf{lfp}^{\sqsubseteq}\,\Phi_S = \mathsf{lfp}^{\sqsubseteq}\,\Phi_R$.

□

Example: Even Numbers

- Even numbers:

$$\frac{N}{\{0\} \cup \{n+2 \mid n \in N\}}, \quad \emptyset \subseteq N \subseteq \mathbb{N}$$

- $\cup$-join irreducibles conclusions:

$$\frac{N}{\{0\}}, \quad \emptyset \subseteq N \subseteq \mathbb{N} \qquad \frac{N}{\{n+2\}}, \quad \emptyset \subset N \subseteq \mathbb{N},\ n \in N$$

Reduction of the Premiss

- Let S be the element of the complete lattice $\langle\mathcal{D}, \sqsubseteq\rangle$ defined by the rule instances :

$$R \cup \left\{\frac{P'}{C'}, \frac{P''}{C'}\right\}$$

- Let S' be the element of the complete lattice $\langle\mathcal{D}, \sqsubseteq\rangle$ defined by the rule instances :

$$R \cup \left\{\frac{P'}{C'}\right\}$$

- If $P' \sqsubseteq P''$ then $S = S'$.

PROOF. – By definition, this denotes:

$$\begin{aligned} S &= \mathsf{lfp}^{\sqsubseteq}\,\Phi \\ S' &= \mathsf{lfp}^{\sqsubseteq}\,\Phi' \end{aligned}$$

where:

$$\Phi \stackrel{\text{def}}{=} \lambda X \cdot \bigsqcup\{C \mid \frac{P}{C} \in R \wedge P \sqsubseteq X\} \sqcup \{C' \mid P' \sqsubseteq X\} \sqcup \{C' \mid P'' \sqsubseteq X\}$$

$$\Phi' \stackrel{\text{def}}{=} \lambda X \cdot \bigsqcup\{C \mid \frac{P}{C} \in R \wedge P \sqsubseteq X\} \sqcup \{C' \mid P' \sqsubseteq X\}$$

- But $\Phi = \Phi'$ since $P'' \sqsubseteq X \Rightarrow P' \sqsubseteq X$.

□

Example: Even Numbers

- Even numbers:

$$\frac{N}{\{0\}},\quad \emptyset \subseteq N \subseteq \mathbb{N} \qquad \frac{N}{\{n+2\}},\quad \emptyset \subset N \subseteq \mathbb{N},\ n \in N$$

- Reduction of the premisses:

$$\frac{\emptyset}{\{0\}} \qquad \frac{\{n\}}{\{n+2\}},\quad n \in \mathbb{N}$$

- Convention [10]:

$$\frac{\emptyset}{0} \qquad \frac{\{n\}}{n+2},\quad n \in \mathbb{N}$$

Traces

- $\langle \Sigma,\ \tau \rangle$, transition system
- $\tau^{\dot{\vec{n}}} \overset{\text{def}}{=} \{\sigma \in \Sigma^{\vec{n}} \mid \forall i < n-1 : \langle \sigma_i,\ \sigma_{i-1} \rangle \in \tau\}$, finite partial traces of τ of length $n > 0$
- $\tau^{\breve{\vec{n}}} \overset{\text{def}}{=} \{\sigma \in \tau^{\dot{\vec{n}}} \mid \forall s \in \Sigma : \langle \sigma_{n-1},\ s \rangle \not\in \tau\}$, finite complete traces of τ
- $\tau^{\breve{\vec{+}}} \overset{\text{def}}{=} \bigcup_{n>0} \tau^{\hat{\vec{n}}}$, finite complete nonempty traces of τ
- $A \frown B = \{\sigma_0 \ldots \sigma_{n-1}\sigma'_1 \ldots \sigma'_{m-1} \mid \sigma_0 \ldots \sigma_{n-1} \in A \cap \Sigma^{\vec{n}} \wedge \sigma'_0 \ldots \sigma'_{m-1} \in B \cap \Sigma^{\vec{m}} \wedge \sigma_{n-1} = \sigma'_0\}$, junction

Inductive definition of the finite trace operational semantics of a transition system

THEOREM.

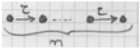
$$\tau^{\breve{\vec{+}}} = \mathsf{lfp}^{\subseteq}_{\emptyset}\ F^{\breve{\vec{+}}} = \mathsf{gfp}^{\subseteq}_{\Sigma^{\vec{+}}}\ F^{\breve{\vec{+}}} \qquad (4)$$

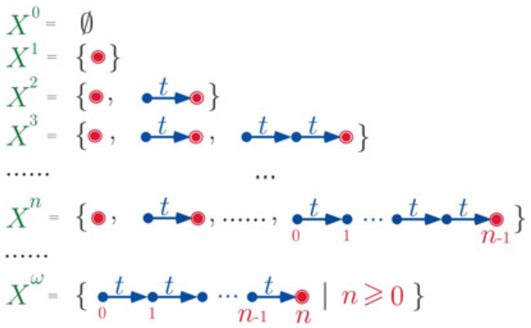
where the set of finite traces transformer $F^{\breve{\vec{+}}}$ is:

$$F^{\breve{\vec{+}}}(X) \overset{\text{def}}{=} \tau^{\breve{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown X \qquad \blacksquare$$

Note: $F^{\breve{\vec{+}}}$ is a complete $\cup$-morphism $\bigcup_i F^{\breve{\vec{+}}}(X_i) = F^{\breve{\vec{+}}}(\bigcup_i X_i)$ and complete $\cap$-morphism $\bigcap_i F^{\breve{\vec{+}}}(X_i) = F^{\breve{\vec{+}}}(\bigcap_i X_i)$.

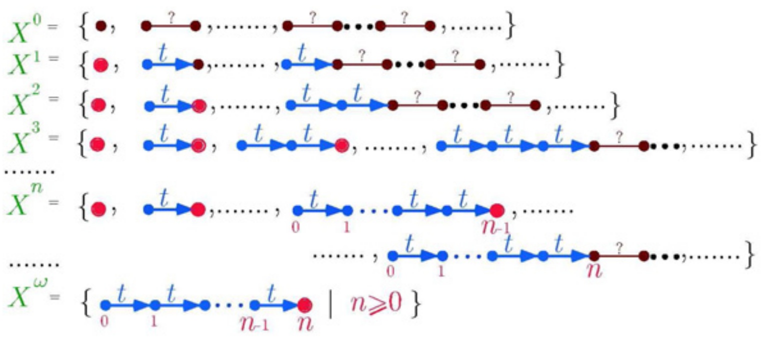
SKETCH OF PROOF. $\tau^{\breve{\vec{+}}} = \bigcup_{i \in \mathbb{N}} \tau^{\breve{\vec{i}}} = \mathsf{lfp}^{\subseteq}_{\emptyset}\ F^{\breve{\vec{+}}}$

- A red point ◉ represents a blocking state $s \in \Sigma : \forall s' \in \Sigma : \langle s,\ s' \rangle \not\in \tau$
- A blue point ● represents a non-blocking state $s \in \Sigma : \exists s' \in \Sigma : \langle s,\ s' \rangle \in \tau$
- A symbolic trace  represents all possible traces where ● are states and $\xrightarrow{\tau}$ are transitions, whereas this is unkown for $\overset{?}{\text{——}}$



$X^0 = \emptyset$
$X^1 = \{$◉$\}$
$X^2 = \{$◉, ●$\xrightarrow{t}$◉$\}$
$X^3 = \{$◉, ●$\xrightarrow{t}$◉, ●$\xrightarrow{t}$●$\xrightarrow{t}$◉$\}$
……
…
$X^n = \{$◉, ●$\xrightarrow{t}$◉, ……, ●$\xrightarrow{t}$● … ●$\xrightarrow{t}$●$\xrightarrow{t}$◉$\}$
0
1
n-1
……
$X^\omega = \{$●$\xrightarrow{t}$●$\xrightarrow{t}$● … ●$\xrightarrow{t}$◉ $\mid n \geqslant 0\}$
0
1
n-1
n

$$\tau^{\check{\vec{+}}} = \bigcup_{i>0} \tau^{\check{\vec{i}}} = \bigcap_{n\in\mathbb{N}} \big(\bigcup_{i=1}^{n} \tau^{\check{\vec{i}}} \cup \tau^{n\dot{\vec{+}}1} \frown \Sigma^{\vec{+}}\big) = \mathsf{gfp}^{\subseteq}_{\Sigma^{\vec{+}}}\ F^{\check{\vec{+}}}$$



X⁰ = {•, •?•, ……, •?••••?•, ……}
X¹ = {•, •t•, ……, •t••?••••?•, ……}
X² = {•, •t•, ……, •t•t••?••••?•, ……}
X³ = {•, •t•, •t•t•, ……, •t•t•t••?•••, ……}
…….
Xⁿ = {•, •t•, ……, •t•···•t•t•, ……
0
1
n-1
……, •t•···•t•t••?•••, ……}
0
1
n
…….
X^ω = {•t•t•···•t• | n⩾0}
0
1
n-1
n

□

PROOF. For a formal proof, we compute the iterates $\langle F^{\delta},\ \delta \leq \omega+1\rangle$ of F.

- $F = \lambda X \cdot \Sigma^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown X$, monotonic for $\subseteq$
- $F^0 = \emptyset$
- $F^1 = F(F^0) = \Sigma^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown \emptyset = \Sigma^{\vec{1}} = \tau^{\dot{\vec{1}}}$
- $F^2 = F(F^1) = \Sigma^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown \tau^{\dot{\vec{1}}} = \tau^{\dot{\vec{1}}} \cup \tau^{\dot{\vec{2}}}$
- $F^n \stackrel{\text{def}}{=} \bigcup_{i=1}^{n} \tau^{\dot{\vec{i}}}$ hyp. ind.
- $F^{n+1} = F(F^n) = \Sigma^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown (\bigcup_{i=1}^{n} \tau^{\dot{\vec{i}}}) = \tau^{\dot{\vec{1}}} \cup \bigcup_{i=1}^{n} (\tau^{\dot{\vec{2}}} \frown \tau^{\dot{\vec{i}}}) = \tau^{\dot{\vec{1}}} \cup \bigcup_{i=1}^{n} \tau^{i\dot{\vec{+}}1} = \tau^{\dot{\vec{1}}} \cup \bigcup_{j=2}^{n+1} \tau^{\dot{\vec{j}}}$

  $= \bigcup_{i=1}^{n+1} \tau^{\dot{\vec{i}}}$ $n+1$-th iterate
- …
- $F^{\omega} = \bigcup_{n\in\mathbb{N}} F^n = \bigcup_{n\in\mathbb{N}} \bigcup_{i=1}^{n} \tau^{\dot{\vec{i}}} = \bigcup_{i\in\mathbb{N}_+} \tau^{\dot{\vec{i}}} = \tau^{\dot{\vec{+}}}$
- $F^{\omega+1} = F(F^{\omega}) = \Sigma^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown \tau^{\dot{\vec{+}}} = \Sigma^{\vec{1}} \cup \tau^{\dot{\vec{2}}} \frown (\bigcup_{i\in\mathbb{N}_+} \tau^{\dot{\vec{i}}}) = \Sigma^{\vec{1}} \cup \bigcup_{i\in\mathbb{N}_+} (\tau^{\dot{\vec{2}}} \frown \tau^{\dot{\vec{i}}}) =$

  $\Sigma^{\vec{1}} \cup \bigcup_{i\in\mathbb{N}_+} \tau^{i\dot{\vec{+}}1} = \bigcup_{i\in\mathbb{N}_+} \tau^{\dot{\vec{i}}} = \tau^{\dot{\vec{+}}} = F^{\omega} = \mathsf{lfp}^{\subseteq}\ F$

□

Co-inductive definition of the infinite trace operational semantics of a transition system

- $\langle \Sigma,\ \tau \rangle$, transition system
- $\Sigma^{\vec{\omega}} \stackrel{\text{def}}{=} \mathbb{N} \mapsto \Sigma$: infinite sequences of states in Σ
- $\tau^{\vec{\omega}} \stackrel{\text{def}}{=} \{\sigma \in \Sigma^{\vec{\omega}} \mid \forall n \geq 0 : \langle \sigma_n,\ \sigma_{n+1}\rangle \in \tau\}$

THEOREM. $$\tau^{\vec{\omega}} = \mathsf{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}}\ F^{\vec{\omega}} \qquad (5)$$

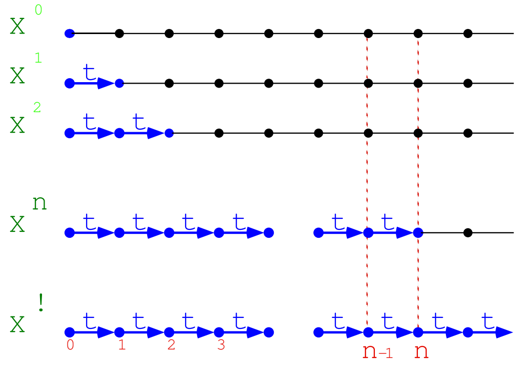
where the set of infinite traces transformer $F^{\vec{\omega}}$ is:

$$F^{\vec{\omega}}(X) \stackrel{\text{def}}{=} \tau^{\dot{\vec{2}}} \frown X$$ ■

Note: $F^{\vec{\omega}}$ is a complete $\cap$-morphism: $\bigcap_i F^{\vec{\omega}}(X_i) = F^{\vec{\omega}}(\bigcap_i X_i)$ and that the least fixpoint of $F^{\vec{\omega}}$ is $\emptyset$.

SKETCH OF PROOF. The black part •—• of the sequence represents any infinite sequence of states in Σ. The blue part •⟶• represents any prefix trace.

$$\tau^{\vec{\omega}} = \bigcap_{n\in\mathbb{N}} \tau^{\dot{\vec{n}}} \frown \Sigma^{\vec{\omega}}\ \mathsf{gfp}^{\subseteq}_{\Sigma^{\vec{\omega}}}\ F^{\vec{\omega}}$$



□

PROOF.

$$
\begin{aligned}
&F^0 = \Sigma^{\vec{\omega}}\\
&\ldots\\
&F^n = t^{\vec{n}} \cdot \Sigma^{\vec{\omega}} && \wr\text{hyp. ind. } (t^{\vec{0}} = \vec{\epsilon})\int\\
&F^{n+1} = F^{\vec{\omega}}(F^n)\\
&\;= \tau^{\dot{\vec{2}}} \frown F^n\\
&\;= \tau^{\dot{\vec{2}}} \frown t^{\vec{n}} \cdot \Sigma^{\vec{\omega}}\\
&\;= t^{n\vec{+}1} \cdot \Sigma^{\vec{\omega}}\\
&\ldots\\
&F^{\omega} = \bigcap_{n\geq 0} F^{\vec{\omega}}(F^n)\\
&= t^{\vec{\omega}}\\
&F^{\omega+1} = F^{\vec{\omega}}(F^{\omega})\\
&\;= \tau^{\dot{\vec{2}}} \frown t^{\vec{\omega}}\\
&\;= t^{\vec{\omega}}
\end{aligned}
$$

□

Bi-inductive definition of the finite and infinite trace operational semantics of a transition system

– The fixpoint characterization of the bifinitary complete trace semantics of a transition system $\langle \Sigma, \tau \rangle$ is:

$$
\begin{aligned}
\tau^{\check{\vec{\infty}}} &= \mathsf{lfp}^{\sqsubseteq} F^{\check{\vec{\infty}}} = \mathsf{gfp}^{\subseteq}_{\Sigma^{\vec{\propto}}} F^{\check{\vec{\infty}}} \qquad (6)\\
F^{\check{\vec{\infty}}} &= \lambda X \cdot \tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown X\\
X \sqsubseteq Y &\overset{\text{def}}{=} (X \cap \Sigma^{\vec{*}} \subseteq Y \cap \Sigma^{\vec{*}}) \wedge (X \cap \Sigma^{\vec{\omega}} \supseteq Y \cap \Sigma^{\vec{\omega}})
\end{aligned}
$$

PROOF. Observe that $\Sigma^{\vec{\infty}} = \Sigma^{\vec{*}} \cup \Sigma^{\vec{\omega}}$ and $\Sigma^{\vec{*}} \cap \Sigma^{\vec{\omega}} = \emptyset$ imply that we have a complete lattice $\langle \wp(\Sigma^{\vec{\infty}}),\ \sqsubseteq,\ \bot,\ \top,\ \sqcup,\ \sqcap \rangle$ where $\bot = \Sigma^{\vec{\propto}}$, $\top = \Sigma^{\vec{\omega}}$, and

$$
\begin{aligned}
\bigsqcup_{i\in\Delta} X_i &\overset{\text{def}}{=} \bigcup_{i\in\Delta}(X_i \cap \Sigma^{\vec{*}}) \cup \bigcap_{i\in\Delta}(X_i \cap \Sigma^{\vec{\omega}})\\
\bigsqcap_{i\in\Delta} X_i &\overset{\text{def}}{=} \bigcap_{i\in\Delta}(X_i \cap \Sigma^{\vec{*}}) \cup \bigcup_{i\in\Delta}(X_i \cap \Sigma^{\vec{\omega}})
\end{aligned}
$$

(by isomorphism with $\langle \wp(\Sigma^{\vec{+}} \times \Sigma^{\vec{\omega}}),\ \subseteq \times \supseteq,\ \langle \emptyset,\ \Sigma^{\vec{\omega}} \rangle,\ \langle \Sigma^{\vec{+}},\ \emptyset \rangle,\ \cup \times \cap,\ \cap \times \cup \rangle$)
For a formal proof, we compute the iterates $\langle F^{\delta},\ \delta \leq \omega + 1 \rangle$ of F.

- $F^{\check{\vec{\infty}}} \overset{\text{def}}{=} \lambda X \cdot \tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown X$
- $F^0 = \Sigma^{\vec{\omega}}$
- $F^1 = F^{\check{\vec{\infty}}}(F^0) = \tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown \Sigma^{\vec{\omega}} =$
- $F^2 = F^{\check{\vec{\infty}}}(F^1) = \tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown (\tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown \Sigma^{\vec{\omega}}) = \tau^{\check{\vec{1}}} \cup \tau^{\check{\vec{2}}} \cup \tau^{\dot{\vec{3}}} \frown \Sigma^{\vec{\omega}}$

- $F^n \overset{\text{def}}{=} \Big(\bigcup_{i=1}^{n} \tau^{\check{\vec{i}}}\Big) \cup \tau^{n\dot{\vec{+}}1} \frown \Sigma^{\vec{\omega}}$ hyp. ind.
- $F^{n+1} = F^{\check{\vec{\infty}}}(F^n)$

$$
\begin{aligned}
&= \tau^{\check{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown \left(\Big(\bigcup_{i=1}^{n} \tau^{\check{\vec{i}}}\Big) \cup \tau^{n\dot{\vec{+}}1} \frown \Sigma^{\vec{\omega}}\right)\\
&= \tau^{\check{\vec{1}}} \cup \Big(\bigcup_{i=1}^{n} \tau^{\dot{\vec{2}}} \frown \tau^{\check{\vec{i}}}\Big) \cup \tau^{\dot{\vec{2}}} \frown \tau^{n\dot{\vec{+}}1} \frown \Sigma^{\vec{\omega}}\\
&= \tau^{\check{\vec{1}}} \cup \Big(\bigcup_{i=1}^{n} \tau^{i\check{\vec{+}}1}\Big) \cup \tau^{n\dot{\vec{+}}2} \frown \Sigma^{\vec{\omega}}\\
&= \tau^{\check{\vec{1}}} \cup \Big(\bigcup_{j=2}^{n+1} \tau^{\check{\vec{j}}}\Big) \cup \tau^{n\dot{\vec{+}}2} \frown \Sigma^{\vec{\omega}}\\
&= \Big(\bigcup_{i=1}^{n+1} \tau^{\check{\vec{i}}}\Big) \cup \tau^{n\dot{\vec{+}}2} \frown \Sigma^{\vec{\omega}} \qquad n+1\text{-th iterate}
\end{aligned}
$$

- . . .

- $F^{\omega} = \bigsqcup_{n\in\mathbb{N}} F^n$

$$= \bigcup_{n\in\mathbb{N}} (F^n \cap \Sigma^{\vec{*}}) \;\cup\; \bigcap_{n\in\mathbb{N}} (F^n \cap \Sigma^{\vec{\omega}})$$

$$= \bigcup_{n\in\mathbb{N}} \bigcup_{i=1}^{n} (\tau^{\breve{\vec{i}}}) \;\cup\; \bigcap_{n\in\mathbb{N}} (\tau^{n\dot{\vec{+}}1} \frown \Sigma^{\vec{\omega}})$$

$$= \bigcup_{i\in\mathbb{N}_+} (\tau^{\breve{\vec{i}}}) \;\cup\; \tau^{\vec{\omega}}$$

$$= \tau^{\breve{\vec{+}}} \;\cup\; \tau^{\vec{\omega}}$$

$$= \tau^{\breve{\vec{\infty}}}$$

- $F^{\omega+1}$

$$= F^{\breve{\vec{\infty}}}(F^{\omega})$$

$$= \tau^{\breve{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown \tau^{\breve{\vec{\infty}}}$$

$$= \tau^{\breve{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown \Big(\bigcup_{i\in\mathbb{N}_+} (\tau^{\breve{\vec{i}}}) \;\cup\; \tau^{\vec{\omega}} \Big)$$

$$= \tau^{\breve{\vec{1}}} \cup \Big(\bigcup_{i\in\mathbb{N}_+} \tau^{\dot{\vec{2}}} \frown \tau^{\breve{\vec{i}}} \Big) \cup (\tau^{\dot{\vec{2}}} \frown \tau^{\vec{\omega}})$$

$$= (\tau^{\breve{\vec{1}}}) \cup \Big(\bigcup_{i\in\mathbb{N}_+} \tau^{i\breve{\vec{+}}1} \Big) \cup \tau^{\vec{\omega}}$$

$$= \Big(\bigcup_{i\in\mathbb{N}_+} \tau^{\breve{\vec{i}}} \Big) \cup \tau^{\vec{\omega}}$$

$$= \tau^{\breve{\vec{+}}} \cup \tau^{\vec{\omega}}$$

$$= \tau^{\breve{\vec{\infty}}}$$

$$= F^{\omega}$$

$$= \mathsf{lfp}^{\sqsubseteq} F$$

□

Continuity of the Trace Transformer $F^{\breve{\vec{\infty}}}$

Unbounded non-determinism does not necessarily imply absence of continuity of the transformer of the fixpoint semantics:

PROOF.

$$\bigsqcup_i F^{\breve{\vec{\infty}}}(X_i) = \bigsqcup_i \tau^{\breve{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown X_i$$

$$= \bigcup_i (\tau^{\breve{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown (X_i \cap \Sigma^{\vec{*}})) \cup \bigcap_i (\tau^{\dot{\vec{2}}} \frown (X_i \cap \Sigma^{\vec{\omega}}))$$

$$= \tau^{\breve{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown (\bigcup_i (X_i \cap \Sigma^{\vec{*}}) \cup \bigcap_i (X_i \cap \Sigma^{\vec{\omega}}))$$

$$= \tau^{\breve{\vec{1}}} \cup \tau^{\dot{\vec{2}}} \frown \bigsqcup_i^{\vec{\propto}} X_i = F^{\breve{\vec{\infty}}}(\bigsqcup_i X_i)$$

□

Bi-inductive definition of the finite and infinite trace operational semantics of (a variant of) SIL — Syntax —

- d ∈ D Digits

  d ⟶ 0 | 1 | 2 | ⋯ | 9
- n ∈ N Numbers

  n ⟶ d | nd
- l ∈ L Letters

  l ⟶ A | B | ⋯ | Z | a | b | ⋯ | z | _
- v ∈ V Variables

  v ⟶ l | vl | vd
- p ∈ P Programs

  p ⟶ n | v | ? | p_1 − p_2 | v := p | if p_1 then p_2 else p_3 |

  p_1 ; p_2 | repeat p_1 until p_2 | while p_1 do p_2

— States —

- $x \in \mathbb{Z}_\Omega$ Values
- $\rho \in \mathsf{V} \mapsto \mathbb{Z}_\Omega$ Environments
- $\mathsf{e} \in \mathsf{E}$ Partially evaluated programs[15]

$$\begin{array}{l}\mathsf{e} \to x \mid \mathsf{n} \mid \mathsf{v} \mid \texttt{?} \mid \mathsf{e}_1 - \mathsf{e}_2 \mid \mathsf{v} := \mathsf{e} \mid \texttt{if } \mathsf{e}_1 \texttt{ then } \mathsf{p}_2 \texttt{ else } \mathsf{p}_3 \mid \\ \quad \mathsf{e}_1 \texttt{ ; } \mathsf{p}_2 \mid \texttt{repeat } \mathsf{p}_1 \texttt{ until } \mathsf{p}_2 \mid \texttt{repetition } \langle \mathsf{e}_1,\ \mathsf{e}_2,\ \mathsf{p}_3 \rangle \mid \\ \quad \texttt{while } \mathsf{p}_1 \texttt{ do } \mathsf{p}_2 \mid \texttt{iteration } \langle \mathsf{e}_1,\ \mathsf{e}_2,\ \mathsf{p}_3 \rangle\end{array}$$

- $\langle \mathsf{e},\ \rho \rangle \in \Sigma \stackrel{\text{def}}{=} \langle \mathsf{E},\ \mathsf{V} \mapsto \mathbb{Z}_\Omega \rangle$ States

— Trace Semantics —

- $\mathcal{S}^{\vec{\infty}}[\![\mathsf{e}]\!] \in \wp(\Sigma^{\vec{\infty}})$ Maximal/complete trace semantics

[15] A partially evaluated program models both a program point, pointing at the code remaining to execute, and an execution stack holding intermediate temporary values during the evaluation of an expression.

— Maximal/Complete Trace Semantics —

Values $\mathcal{S}^{\vec{\infty}}[\![x]\!]$

- $\dfrac{\emptyset}{\langle x,\ \rho \rangle},\ x \in \mathbb{Z}_\Omega$

Numbers $\mathcal{S}^{\vec{\infty}}[\![\mathsf{n}]\!]$

- $\mathcal{N}[\![\mathsf{0}]\!] \stackrel{\text{def}}{=} 0$[16]
- ...
- $\mathcal{N}[\![\mathsf{9}]\!] \stackrel{\text{def}}{=} 9$
- $\mathcal{N}[\![\mathsf{nd}]\!] \stackrel{\text{def}}{=} (10 \times \mathcal{N}[\![\mathsf{n}]\!]) + \mathcal{N}[\![\mathsf{d}]\!]$
- $\dfrac{\emptyset}{\langle \mathsf{n},\ \rho \rangle \bullet \langle \mathcal{N}[\![\mathsf{n}]\!],\ \rho \rangle}$

[16] n can be understood as the ASCII encoding and n as the binary encoding of the number.

Variables $\mathcal{S}^{\vec{\infty}}[\![\mathsf{v}]\!]$

- $\dfrac{\emptyset}{\langle \mathsf{v},\ \rho \rangle \bullet \langle \rho(\mathsf{v}),\ \rho \rangle}$

Random $\mathcal{S}^{\vec{\infty}}[\![\texttt{?}]\!]$

- $\dfrac{\emptyset}{\langle \texttt{?},\ \rho \rangle \bullet \langle i,\ \rho \rangle},\ i \in \mathbb{Z}$

Contexts

- A context $\mathsf{e}[\bullet]$ is a partially evaluated program with a hole in it:

$$\begin{array}{l}\mathsf{e}[\bullet] \to [\bullet] \mid x \mid \mathsf{n} \mid \mathsf{v} \mid \texttt{?} \mid \mathsf{e}_1[\bullet] - \mathsf{e}_2[\bullet] \mid \mathsf{v} := \mathsf{e}[\bullet] \mid \\ \quad \texttt{if } \mathsf{e}_1[\bullet] \texttt{ then } \mathsf{p}_2 \texttt{ else } \mathsf{p}_3 \mid \mathsf{e}_1[\bullet] \texttt{ ; } \mathsf{p}_2 \mid \\ \quad \texttt{repeat } \mathsf{p}_1 \texttt{ until } \mathsf{p}_2 \mid \texttt{repetition } \langle \mathsf{e}_1[\bullet],\ \mathsf{e}_2[\bullet],\ \mathsf{p}_3 \rangle \mid \\ \quad \texttt{while } \mathsf{p}_1 \texttt{ do } \mathsf{p}_2 \mid \texttt{iteration } \langle \mathsf{e}_1[\bullet],\ \mathsf{e}_2[\bullet],\ \mathsf{p}_3 \rangle\end{array}$$

Context Substitution

- If $\mathrm{e}[\bullet]$ is a context and e' is a partially evaluated program then $\mathrm{e}[\mathrm{e}']$ denotes the result of placing e' in the holes of $\mathrm{e}[\bullet]$:

$\mathrm{e}[\bullet]$	$\mathrm{e}[\mathrm{e}']$
$[\bullet]$	e'
x	x
p	p
$\mathrm{e}_1[\bullet] - \mathrm{e}_2[\bullet]$	$\mathrm{e}_1[\mathrm{e}'] - \mathrm{e}_2[\mathrm{e}']$
if $\mathrm{e}_1[\bullet]$ then p_2 else p_3	if $\mathrm{e}_1[\mathrm{e}']$ then p_2 else p_3
$\mathrm{e}_1[\bullet]$; p_2	$\mathrm{e}_1[\mathrm{e}']$; p_2
repetition $\langle \mathrm{e}_1[\bullet],\ \mathrm{e}_2[\bullet],\ \mathrm{p}_3\rangle$	repetition $\langle \mathrm{e}_1[\mathrm{e}'],\ \mathrm{e}_2[\mathrm{e}'],\ \mathrm{p}_3\rangle$
iteration $\langle \mathrm{e}_1[\bullet],\ \mathrm{e}_2[\bullet],\ \mathrm{p}_3\rangle$	iteration $\langle \mathrm{e}_1[\mathrm{e}'],\ \mathrm{e}_2[\mathrm{e}'],\ \mathrm{p}_3\rangle$

Trace Context

- If $\mathrm{e}[\bullet]$ is a context and $\sigma \in \Sigma^{\vec{\infty}}$ is an execution trace then $\mathrm{e}[\sigma]$ is the execution trace where context $\mathrm{e}[\bullet]$ is added to all control components:

$$\forall i < |\sigma| : \mathrm{e}[\sigma]_i = \langle \mathrm{e}[\mathrm{e}'_i],\ \rho_i\rangle \text{ where } \sigma_i = \langle \mathrm{e}'_i,\ \rho_i\rangle$$

- Example:

$$\begin{aligned}\sigma &= \langle \underline{1} - \underline{2},\ \rho\rangle \bullet \langle 1 - \underline{2},\ \rho\rangle \bullet \langle 1 - 2,\ \rho\rangle \bullet \langle -1,\ \rho\rangle\\ [\sigma] - \underline{3} &= \langle \underline{1} - \underline{2} - \underline{3},\ \rho\rangle \bullet \langle 1 - \underline{2} - \underline{3},\ \rho\rangle \bullet \langle 1 - 2 - \underline{3},\ \rho\rangle \bullet\\ &\qquad \langle -1 - \underline{3},\ \rho\rangle\end{aligned}$$

Substraction $\mathcal{S}^{\breve{\vec{\infty}}}[\![\mathrm{e}_1 - \mathrm{e}_2]\!]$

- $$\frac{\langle \mathrm{e}_1,\ \rho\rangle \bullet \sigma \bullet \langle \Omega,\ \rho'\rangle}{\langle \mathrm{e}_1 - \mathrm{e}_2,\ \rho\rangle \bullet [\sigma] - \mathrm{e}_2 \bullet \langle \Omega - \mathrm{e}_2,\ \rho'\rangle \bullet \langle \Omega,\ \rho'\rangle},\ \sigma \in \Sigma^{\vec{*}}$$

- $$\frac{\langle \mathrm{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle i,\ \rho'\rangle, \quad \langle \mathrm{e}_2,\ \rho'\rangle \bullet \sigma_2 \bullet \langle \Omega,\ \rho''\rangle}{\begin{array}{c}\langle \mathrm{e}_1 - \mathrm{e}_2,\ \rho\rangle \bullet [\sigma_1] - \mathrm{e}_2 \bullet \langle i - \mathrm{e}_2,\ \rho'\rangle \bullet\\ i - [\sigma_2] \bullet \langle i - \Omega,\ \rho''\rangle \bullet \langle \Omega,\ \rho''\rangle\end{array}},\ i \in \mathbb{Z}, \sigma \in \Sigma^{\vec{*}}$$

- $$\frac{\langle \mathrm{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle i,\ \rho'\rangle, \quad \langle \mathrm{e}_2,\ \rho'\rangle \bullet \sigma_2 \bullet \langle j,\ \rho''\rangle}{\begin{array}{c}\langle \mathrm{e}_1 - \mathrm{e}_2,\ \rho\rangle \bullet [\sigma_1] - \mathrm{e}_2 \bullet \langle i - \mathrm{e}_2,\ \rho'\rangle \bullet\\ i - [\sigma_2] \bullet \langle i - j,\ \rho''\rangle \bullet \langle i - j,\ \rho''\rangle\end{array}},\ i, j \in \mathbb{Z}, \sigma \in \Sigma^{\vec{*}}$$

- $$\frac{\langle \mathrm{e}_1,\ \rho\rangle \bullet \sigma}{\langle \mathrm{e}_1 - \mathrm{e}_2,\ \rho\rangle \bullet [\sigma] - \mathrm{e}_2},\ \sigma \in \Sigma^{\vec{\omega}}$$

- $$\frac{\langle \mathrm{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle i,\ \rho'\rangle, \quad \langle \mathrm{e}_2,\ \rho'\rangle \bullet \sigma_2}{\langle \mathrm{e}_1 - \mathrm{e}_2,\ \rho\rangle \bullet [\sigma_1] - \mathrm{e}_2 \bullet \langle i - \mathrm{e}_2,\ \rho'\rangle \bullet i - [\sigma_2]},\ \begin{array}{l} i \in \mathbb{Z}, \sigma_1 \in \Sigma^{\vec{*}},\\ \sigma_2 \in \Sigma^{\vec{\omega}}\end{array}$$

Examples

- $\langle \Omega,\ \rho\rangle \in \mathcal{S}^{\breve{\vec{\infty}}}[\![\Omega]\!]$
  $\langle \Omega\ -\ \underline{1},\ \rho\rangle \bullet \langle \Omega,\ \rho\rangle \in \mathcal{S}^{\breve{\vec{\infty}}}[\![\Omega\ -\ \underline{1}]\!]$
  $\langle \Omega\ -\ \underline{1}\ -\ \underline{2},\ \rho\rangle \bullet \langle \Omega\ -\ \underline{2},\ \rho\rangle \bullet \langle \Omega,\ \rho\rangle \in \mathcal{S}^{\breve{\vec{\infty}}}[\![\Omega\ -\ \underline{1}\ -\ \underline{2}]\!]$
  $\langle \Omega\ -\ \underline{1}\ -\ \underline{2}\ -\ \underline{3},\ \rho\rangle \bullet \langle \Omega\ -\ \underline{2}\ -\ \underline{3},\ \rho\rangle \bullet \langle \Omega\ -\ \underline{3},\ \rho\rangle \bullet \langle \Omega,\ \rho\rangle$
  $\in \mathcal{S}^{\breve{\vec{\infty}}}[\![\Omega\ -\ \underline{1}\ -\ \underline{2}\ -\ \underline{3}]\!]$

- $\langle \underline{1},\ \rho\rangle \bullet \langle 1,\ \rho\rangle \in \mathcal{S}^{\breve{\vec{\infty}}}[\![1]\!]$
  $\langle \underline{2},\ \rho\rangle \bullet \langle 2,\ \rho\rangle \in \mathcal{S}^{\breve{\vec{\infty}}}[\![2]\!]$
  $\langle \underline{1}\ -\ \underline{2},\ \rho\rangle \bullet \langle 1\ -\ \underline{2},\ \rho\rangle \bullet \langle 1\ -\ 2,\ \rho\rangle \bullet \langle -1,\ \rho\rangle \in \mathcal{S}^{\breve{\vec{\infty}}}[\![1\ -\ 2]\!]$.

Assignment $\mathcal{S}^{\breve{\vec{\infty}}}[\![\mathsf{v} := \mathsf{e}]\!]$

- $\dfrac{\langle \mathsf{e},\ \rho\rangle \bullet \sigma \bullet \langle \Omega,\ \rho'\rangle}{\langle \mathsf{v} := \mathsf{e},\ \rho\rangle \bullet \mathsf{v} := [\sigma] \bullet \langle \mathsf{v} := \Omega,\ \rho'\rangle \bullet \langle \Omega,\ \rho'\rangle},\ \sigma \in \Sigma^{\vec{*}}$

- $\dfrac{\langle \mathsf{e},\ \rho\rangle \bullet \sigma \bullet \langle i,\ \rho'\rangle}{\langle \mathsf{v} := \mathsf{e},\ \rho\rangle \bullet \mathsf{v} := [\sigma] \bullet \langle \mathsf{v} := i,\ \rho'\rangle \bullet \langle i,\ \rho'[\mathsf{v} := i]\rangle},\ \sigma \in$
  $\Sigma^{\vec{*}},\ i \in \mathbb{Z}$

- $\dfrac{\langle \mathsf{e},\ \rho\rangle \bullet \sigma}{\langle \mathsf{v}\ \ :=\ \ \mathsf{e},\ \rho\rangle \bullet \mathsf{v} := [\sigma]},\ \sigma \in \Sigma^{\vec{\omega}}$

Conditional $\mathcal{S}^{\breve{\vec{\infty}}}[\![\mathtt{if}\ \mathsf{e}_1\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3]\!]$

- $\dfrac{\langle \mathsf{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle \Omega,\ \rho'\rangle}{\begin{array}{c}\langle \mathtt{if}\ \mathsf{e}_1\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3,\ \rho\rangle \bullet \mathtt{if}\ [\sigma_1]\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3 \bullet\\ \langle \mathtt{if}\ \Omega\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3,\ \rho'\rangle \bullet \langle \Omega,\ \rho'\rangle\end{array}}$

- $\dfrac{\langle \mathsf{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle 0,\ \rho'\rangle, \quad \langle \mathsf{p}_2,\ \rho'\rangle \bullet \sigma_2}{\begin{array}{c}\langle \mathtt{if}\ \mathsf{e}_1\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3,\ \rho\rangle \bullet \mathtt{if}\ [\sigma_1]\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3 \bullet\\ \langle \mathtt{if}\ 0\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3,\ \rho'\rangle \bullet \langle \mathsf{p}_2,\ \rho'\rangle \bullet \sigma_2\end{array}}$

- $\dfrac{\langle \mathsf{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle i,\ \rho'\rangle, \quad \langle \mathsf{p}_3,\ \rho'\rangle \bullet \sigma_3}{\begin{array}{c}\langle \mathtt{if}\ \mathsf{e}_1\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3,\ \rho\rangle \bullet \mathtt{if}\ [\sigma_1]\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3 \bullet\\ \langle \mathtt{if}\ i\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3,\ \rho'\rangle \bullet \langle \mathsf{p}_3,\ \rho'\rangle \bullet \sigma_3\end{array}},\ i \in \mathbb{Z} - \{0\}$

- $\dfrac{\langle \mathsf{e}_1,\ \rho\rangle \bullet \sigma_1}{\langle \mathtt{if}\ \mathsf{e}_1\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3,\ \rho\rangle \bullet \mathtt{if}\ [\sigma_1]\ \mathtt{then}\ \mathsf{p}_2\ \mathtt{else}\ \mathsf{p}_3},\ \sigma_1 \in \Sigma^{\vec{\omega}}$

Sequential Composition $\mathcal{S}^{\breve{\vec{\infty}}}[\![\mathsf{e}_1\ ;\ \mathsf{p}_2]\!]$

- $\dfrac{\langle \mathsf{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle \Omega,\ \rho'\rangle}{\langle \mathsf{e}_1\ ;\ \mathsf{p}_2,\ \rho\rangle \bullet [\sigma_1]\ ;\ \mathsf{p}_2 \bullet \langle \Omega\ ;\ \mathsf{p}_2,\ \rho'\rangle \bullet \langle \Omega,\ \rho'\rangle}$

- $\dfrac{\langle \mathsf{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle i,\ \rho'\rangle, \quad \langle \mathsf{p}_2,\ \rho'\rangle \bullet \sigma_2}{\langle \mathsf{e}_1\ ;\ \mathsf{p}_2,\ \rho\rangle \bullet [\sigma_1]\ ;\ \mathsf{p}_2 \bullet \langle i\ ;\ \mathsf{p}_2,\ \rho'\rangle \bullet \langle \mathsf{p}_2,\ \rho'\rangle \bullet \sigma_2},\ i \in$
  $\mathbb{Z}$

- $\dfrac{\langle \mathsf{e}_1,\ \rho\rangle \bullet \sigma_1}{\langle \mathsf{e}_1\ ;\ \mathsf{p}_2,\ \rho\rangle \bullet [\sigma_1]\ ;\ \mathsf{p}_2},\ \sigma_1 \in \Sigma^{\vec{\omega}}$

Repetition $\mathcal{S}^{\check{\vec{\infty}}}[\![\texttt{repeat p}_1\ \texttt{until p}_2]\!]$

$$-\ \frac{\langle \texttt{repetition}\ \langle \texttt{p}_1,\ \texttt{p}_2,\ \texttt{repeat p}_1\ \texttt{until p}_2\rangle,\ \rho\rangle \bullet \sigma}{\langle \texttt{repeat p}_1\ \texttt{until p}_2,\ \rho\rangle \bullet \sigma} \qquad (7)$$

Repetition $\mathcal{S}^{\check{\vec{\infty}}}[\![\texttt{repetition}\ \langle \texttt{e}_1,\ \texttt{e}_2,\ \texttt{p}_3\rangle]\!]$

- [17] $$\frac{\langle \texttt{e}_1,\ \rho\rangle \bullet \sigma_1}{\langle \texttt{repetition}\ \langle \texttt{e}_1,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho\rangle \bullet \texttt{repetition}\ \langle [\sigma_1],\ \texttt{e}_2,\ \texttt{p}\rangle},\ \sigma_1 \in \Sigma^{\vec{\omega}}$$
- [18] $$\frac{\langle \texttt{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle \mathit{\Omega},\ \rho'\rangle}{\begin{array}{c}\langle \texttt{repetition}\ \langle \texttt{e}_1,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho\rangle \bullet \texttt{repetition}\ \langle [\sigma_1],\ \texttt{e}_2,\ \texttt{p}\rangle \bullet \\ \langle \texttt{repetition}\ \langle \mathit{\Omega},\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho'\rangle \bullet \langle \mathit{\Omega},\ \rho'\rangle\end{array}}$$
- [19] $$\frac{\langle \texttt{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle i,\ \rho'\rangle, \quad \langle \texttt{e}_2,\ \rho'\rangle \bullet \sigma_2}{\begin{array}{c}\langle \texttt{repetition}\ \langle \texttt{e}_1,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho\rangle \bullet \texttt{repetition}\ \langle [\sigma_1],\ \texttt{e}_2,\ \texttt{p}\rangle \bullet \\ \langle \texttt{repetition}\ \langle i,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho'\rangle \bullet \texttt{repetition}\ \langle i,\ [\sigma_2],\ \texttt{p}\rangle\end{array}},\ \sigma_2 \in \Sigma^{\vec{\omega}}$$

[17] Body does not terminate.

[18] Body is erroneous, return error.

[19] Body terminates but test does not.

- [20] $$\frac{\langle \texttt{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle i,\ \rho'\rangle, \quad \langle \texttt{e}_2,\ \rho'\rangle \bullet \sigma_2 \bullet \langle \mathit{\Omega},\ \rho''\rangle}{\begin{array}{r}\langle \texttt{repetition}\ \langle \texttt{e}_1,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho\rangle \bullet \texttt{repetition}\ \langle [\sigma_1],\ \texttt{e}_2,\ \texttt{p}\rangle \bullet \\ \langle \texttt{repetition}\ \langle i,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho'\rangle \bullet \texttt{repetition}\ \langle i,\ [\sigma_2],\ \texttt{p}\rangle \bullet \\ \langle \texttt{repetition}\ \langle i,\ \mathit{\Omega},\ \texttt{p}\rangle,\ \rho''\rangle \bullet \langle \mathit{\Omega},\ \rho''\rangle\end{array}}$$
- [21] $$\frac{\langle \texttt{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle i,\ \rho'\rangle, \quad \langle \texttt{e}_2,\ \rho'\rangle \bullet \sigma_2 \bullet \langle 0,\ \rho''\rangle}{\begin{array}{r}\langle \texttt{repetition}\ \langle \texttt{e}_1,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho\rangle \bullet \texttt{repetition}\ \langle [\sigma_1],\ \texttt{e}_2,\ \texttt{p}\rangle \bullet \\ \langle \texttt{repetition}\ \langle i,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho'\rangle \bullet \texttt{repetition}\ \langle i,\ [\sigma_2],\ \texttt{p}\rangle \bullet \\ \langle \texttt{repetition}\ \langle i,\ 0,\ \texttt{p}\rangle,\ \rho''\rangle \bullet \langle i,\ \rho''\rangle\end{array}}$$

[20] Body terminates, test is erroneous, return error.

[21] Body terminates, test is true, return value of the last iteration.

- [22] $$\frac{\begin{array}{c}\langle \texttt{e}_1,\ \rho\rangle \bullet \sigma_1 \bullet \langle i,\ \rho'\rangle,\ \ \langle \texttt{e}_2,\ \rho'\rangle \bullet \sigma_2 \bullet \langle j,\ \rho''\rangle, \\ \texttt{p} = \texttt{repeat e}_1\ \texttt{until e}_2,\ \langle \texttt{repetition}\ \langle \texttt{e}_1,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho''\rangle \bullet \sigma_3\end{array}}{\begin{array}{r}\langle \texttt{repetition}\ \langle \texttt{e}_1,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho\rangle \bullet \texttt{repetition}\ \langle [\sigma_1],\ \texttt{e}_2,\ \texttt{p}\rangle \bullet \\ \langle \texttt{repetition}\ \langle i,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho'\rangle \bullet \texttt{repetition}\ \langle i,\ [\sigma_2],\ \texttt{p}\rangle \bullet \\ \langle \texttt{repetition}\ \langle i,\ j,\ \texttt{p}\rangle,\ \rho''\rangle \bullet \langle \texttt{repetition}\ \langle \texttt{e}_1,\ \texttt{e}_2,\ \texttt{p}\rangle,\ \rho''\rangle \bullet \sigma_3\end{array}} \qquad (8)$$

$$j \in \mathbb{Z} - \{0\}$$

[22] Body terminates, test is false, repeat.

Iteration $\mathcal{S}^{\breve{\vec{\infty}}}[\![\mathtt{while\ p_1\ do\ p_2}]\!]$

$$-\ \frac{\langle \mathtt{iteration}\ \langle \mathtt{p_1},\ \mathtt{p_2},\ \mathtt{while\ p_1\ do\ p_2}\rangle,\ \rho\rangle \bullet \sigma}{\langle \mathtt{while\ p_1\ do\ p_2},\ \rho\rangle \bullet \sigma} \qquad (9)$$

Iteration $\mathcal{S}^{\breve{\vec{\infty}}}[\![\mathtt{iteration}\ \langle \mathtt{e_1},\ \mathtt{e_2},\ \mathtt{p_3}\rangle]\!]$

- [23] $$\frac{\langle \mathtt{e_1},\ \rho\rangle \bullet \sigma_1}{\langle \mathtt{iteration}\ \langle \mathtt{e_1},\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho\rangle \bullet \mathtt{iteration}\ \langle[\sigma_1],\ \mathtt{e_2},\ \mathtt{p}\rangle},\ \sigma_1 \in \Sigma^{\breve{\vec{\omega}}}$$
- [24] $$\frac{\langle \mathtt{e_1},\ \rho\rangle \bullet \sigma_1 \bullet \langle \Omega,\ \rho'\rangle}{\begin{array}{r}\langle \mathtt{iteration}\ \langle \mathtt{e_1},\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho\rangle \bullet \mathtt{iteration}\ \langle[\sigma_1],\ \mathtt{e_2},\ \mathtt{p}\rangle \bullet\\ \langle \mathtt{iteration}\ \langle \Omega,\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho'\rangle \bullet \langle \Omega,\ \rho'\rangle\end{array}}$$
- [25] $$\frac{\langle \mathtt{e_1},\ \rho\rangle \bullet \sigma_1 \bullet \langle i,\ \rho'\rangle}{\begin{array}{r}\langle \mathtt{iteration}\ \langle \mathtt{e_1},\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho\rangle \bullet \mathtt{iteration}\ \langle[\sigma_1],\ \mathtt{e_2},\ \mathtt{p}\rangle \bullet\\ \langle \mathtt{iteration}\ \langle i,\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho'\rangle \bullet \langle i,\ \rho'\rangle\end{array}},$$

$$i \in \mathbb{Z} - \{0\}$$

[23] Test does no terminate.
[24] Test is erroneous, return error.
[25] Test is false, return its value.

- [26] $$\frac{\langle \mathtt{e_1},\ \rho\rangle \bullet \sigma_1 \bullet \langle 0,\ \rho'\rangle, \quad \langle \mathtt{e_2},\ \rho'\rangle \bullet \sigma_2}{\begin{array}{r}\langle \mathtt{iteration}\ \langle \mathtt{e_1},\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho\rangle \bullet \mathtt{iteration}\ \langle[\sigma_1],\ \mathtt{e_2},\ \mathtt{p}\rangle \bullet\\ \langle \mathtt{iteration}\ \langle 0,\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho'\rangle \bullet \mathtt{iteration}\ \langle 0,\ [\sigma_2],\ \mathtt{p}\rangle\end{array}},$$

$$\sigma_2 \in \Sigma^{\breve{\vec{\omega}}}$$

- [27] $$\frac{\langle \mathtt{e_1},\ \rho\rangle \bullet \sigma_1 \bullet \langle 0,\ \rho'\rangle, \quad \langle \mathtt{e_2},\ \rho'\rangle \bullet \sigma_2 \bullet \langle \Omega,\ \rho''\rangle}{\begin{array}{r}\langle \mathtt{iteration}\ \langle \mathtt{e_1},\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho\rangle \bullet \mathtt{iteration}\ \langle[\sigma_1],\ \mathtt{e_2},\ \mathtt{p}\rangle \bullet\\ \langle \mathtt{iteration}\ \langle 0,\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho'\rangle \bullet \mathtt{iteration}\ \langle 0,\ [\sigma_2],\ \mathtt{p}\rangle \bullet\\ \langle \mathtt{iteration}\ \langle 0,\ \Omega,\ \mathtt{p}\rangle,\ \rho''\rangle \bullet \langle \Omega,\ \rho''\rangle\end{array}}$$

[26] Test is true, body does not terminate.
[27] Test is true, body is erroneous, return error.

- [28] $$\frac{\begin{array}{c}\langle \mathtt{e_1},\ \rho\rangle \bullet \sigma_1 \bullet \langle 0,\ \rho'\rangle, \quad \langle \mathtt{e_2},\ \rho'\rangle \bullet \sigma_2 \bullet \langle i,\ \rho''\rangle,\\ \mathtt{p} = \mathtt{while\ e_1\ do\ e_2}, \quad \langle \mathtt{iteration}\ \langle \mathtt{e_1},\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho''\rangle \bullet \sigma_3\end{array}}{\begin{array}{r}\langle \mathtt{iteration}\ \langle \mathtt{e_1},\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho\rangle \bullet \mathtt{iteration}\ \langle[\sigma_1],\ \mathtt{e_2},\ \mathtt{p}\rangle \bullet\\ \langle \mathtt{iteration}\ \langle 0,\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho'\rangle \bullet \mathtt{iteration}\ \langle 0,\ [\sigma_2],\ \mathtt{p}\rangle \bullet\\ \langle \mathtt{iteration}\ \langle 0,\ i,\ \mathtt{p}\rangle,\ \rho''\rangle \bullet \langle \mathtt{iteration}\ \langle \mathtt{e_1},\ \mathtt{e_2},\ \mathtt{p}\rangle,\ \rho''\rangle \bullet \sigma_3\end{array}},\ (10)$$

$$i \in \mathbb{Z}$$

[28] Test is true, further iterations needed.

Well-formedness of the Inductive Definition of the Complete Traces Operational Semantics

– The strict syntactic component relation $\prec$ which is used for the inductive definition is well-founded:

$$\begin{array}{rcl@{\qquad}rcl}
\mathtt{e}_1 & \prec & \mathtt{e}_1 - \mathtt{e}_2 & \mathtt{p}_3 & \prec & \mathtt{if}\ \mathtt{e}_1\ \mathtt{then}\ \mathtt{p}_2\ \mathtt{else}\ \mathtt{p}_3 \\
\mathtt{e}_2 & \prec & \mathtt{e}_1 - \mathtt{e}_2 & \mathtt{e}_1 & \prec & \mathtt{e}_1\ ;\ \mathtt{p}_2 \\
\mathtt{e} & \prec & \mathtt{v} := \mathtt{e} & \mathtt{p}_2 & \prec & \mathtt{e}_1\ ;\ \mathtt{p}_2 \\
\mathtt{e}_1 & \prec & \mathtt{if}\ \mathtt{e}_1\ \mathtt{then}\ \mathtt{p}_2\ \mathtt{else}\ \mathtt{p}_3 & \mathtt{e}_1 & \prec & \mathtt{repetition}\ \langle \mathtt{e}_1,\ \mathtt{e}_2,\ \mathtt{p}_3 \rangle \\
\mathtt{p}_2 & \prec & \mathtt{if}\ \mathtt{e}_1\ \mathtt{then}\ \mathtt{p}_2\ \mathtt{else}\ \mathtt{p}_3 & \mathtt{e}_2 & \prec & \mathtt{repetition}\ \langle \mathtt{e}_1,\ \mathtt{e}_2,\ \mathtt{p}_3 \rangle
\end{array}$$

$$\begin{array}{rcl}
\mathtt{repetition} & & \\
\langle \mathtt{p}_1,\ \mathtt{p}_2,\ \mathtt{repeat}\ \mathtt{p}_1\ \mathtt{until}\ \mathtt{p}_2 \rangle & \prec & \mathtt{repeat}\ \mathtt{p}_1\ \mathtt{until}\ \mathtt{p}_2 \\
\mathtt{e}_1 & \prec & \mathtt{iteration}\ \langle \mathtt{e}_1,\ \mathtt{e}_2,\ \mathtt{p}_3 \rangle \\
\mathtt{e}_2 & \prec & \mathtt{iteration}\ \langle \mathtt{e}_1,\ \mathtt{e}_2,\ \mathtt{p}_3 \rangle \\
\mathtt{iteration}\ \langle \mathtt{p}_1,\ \mathtt{p}_2,\ \mathtt{while}\ \mathtt{p}_1\ \mathtt{do}\ \mathtt{p}_2 \rangle & \prec & \mathtt{while}\ \mathtt{p}_1\ \mathtt{do}\ \mathtt{p}_2
\end{array}$$

Beyond Action Induction

– For loops we cannot use syntactic structural induction because of the recursive definition of the traces e.g. for the `while` loop, $\mathtt{while}\ \ \mathtt{p}_1\ \mathtt{do}\ \ \mathtt{p}_2 \equiv \mathtt{p}_2\ ;\ \mathtt{while}\ \ \mathtt{p}_1\ \mathtt{do}\ \ \mathtt{p}_2$;

– For *finite* traces we can reason by induction on the length of traces (e.g. for the `while` loop, the length of the trace for the next iterate is shorter [29]);

– This is not valid for *infinite* traces;

– We have shown that by providing a suitable order-theoretic interpretation/semantics for rules, the rule-based presentation can be "naturally" extended to infinite behaviors.

[29] This was called *action induction* by R. Milner. *Operational and algebraic semantics of concurrent processes.* In J. van Leeuwen, editor, *Formal Models and Semantics*, vol. B of *Handbook of Theoretical Computer Science*, ch. 19, pages 1201–1242. Elsevier Science Publishers B.V., 1990.

Bibliography

– B.A. Davey & H.A. Priestley
"Introduction to lattices and order"
Cambridge University Press, 2nd edition, 2002, 298 p.

THE END

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

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