« Mathematical foundations: (6) Abstraction — 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/


THESE

présentée à

Université Scientifique et Médicale de Grenoble
Institut National Polytechnique de Grenoble

pour obtenir le grade de
DOCTEUR ES SCIENCES MATHEMATIQUES

par

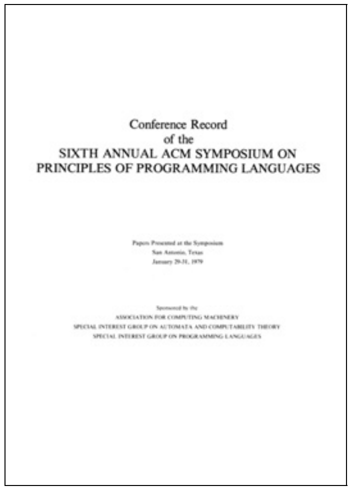
Patrick COUSOT

METHODES ITERATIVES DE CONSTRUCTION ET D'APPROXIMATION DE PCINTS FIXES D'OPERATEURS MONOTONES SUR UN TREILLIS, ANALYSE SEMANTIQUE DES PROGRAMMES.

Thèse soutenue le 21 mars 1978 devant la Commission d'Examen :

Président : L. BOLLIET

Examinateurs : C. BENZAKEN
Ph. JORRAND
B. LORHO
C. PAIR
F. ROBERT
M. SINTZOFF


Conference Record
of the
SIXTH ANNUAL ACM SYMPOSIUM ON
PRINCIPLES OF PROGRAMMING LANGUAGES

Papers Presented at the Symposium
San Antonio, Texas
January 29-31, 1979

Sponsored by the
ASSOCIATION FOR COMPUTING MACHINERY
SPECIAL INTEREST GROUP ON AUTOMATA AND COMPUTABILITY THEORY
SPECIAL INTEREST GROUP ON PROGRAMMING LANGUAGES

Exact fixpoint abstraction

Property transformer abstraction

Let

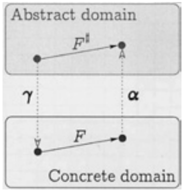
- $\langle L, \leq, 0, 1, \wedge, \vee\rangle$ be complete lattice
- $F \in L \stackrel{\text{m}}{\longmapsto} L$ be a monotonic transfer fonction
- $\alpha \in L \mapsto \overline{L}$ be an abstraction

We would like to:

- compute $\alpha(\mathsf{lfp}\, F)$
- without computing $\mathsf{lfp}\, F$ (which is, in general, impossible)

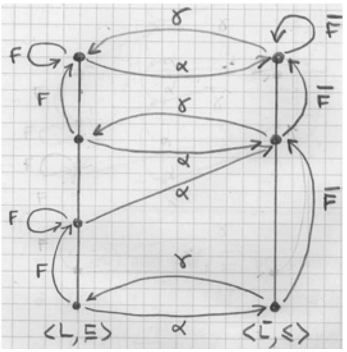
One solution is to have:

- an abstract transformer $\overline{F} \in \overline{L} \mapsto \overline{L}$
- such that $\alpha(\mathsf{lfp}\, F) = \mathsf{lfp}\, \overline{F}$
- to exclude trivial solutions (like $\overline{F} = \lambda X \cdot \alpha(\mathsf{lfp}\, F)$), more must be imposed on the choice of $\overline{F}$
- for monotonic functions, one way may be to use higher-order abstraction



$$\langle P, \subseteq\rangle \langle \alpha, \gamma\rangle \langle Q, \sqsubseteq\rangle$$
$$\Longrightarrow$$
$$\langle P \overset{\mathrm{m}}{\longmapsto} P, \dot{\subseteq}\rangle \underset{\lambda F \cdot \alpha \circ F \circ \gamma}{\overset{\lambda \overline{F} \cdot \gamma \circ \overline{F} \circ \alpha}{\leftrightarrows}} \langle Q \overset{\mathrm{m}}{\longmapsto} Q, \dot{\sqsubseteq}\rangle$$

- In general however, $\langle L, \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \overline{L}, \sqsubseteq\rangle$, $F \in L \overset{\mathrm{m}}{\longmapsto} L$ and $\overline{F} = \alpha \circ F \circ \gamma$ does not imply $\alpha(\mathsf{lfp}^{\leq} F) = \mathsf{lfp}^{\sqsubseteq} \overline{F}$ as shown by the following counter-example:

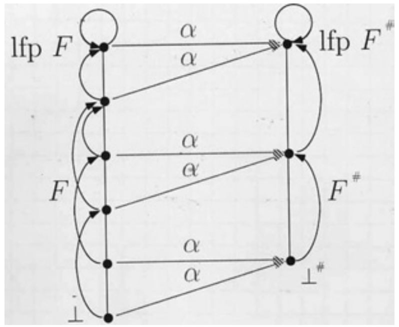


So we are interested in studying fixpoint abstraction:

- Exact abstraction: $\alpha(\mathsf{lfp}\, F) = \mathsf{lfp}\, \overline{F}$
- Approximate abstraction: $\alpha(\mathsf{lfp}\, F) \sqsubset \mathsf{lfp}\, \overline{F}$

À la Kleene exact fixpoint abstraction with Galois connections [1]

Example:



[1] also called fixpoint fusion, fixpoint inducing, lifting, morphism, transfer, precise abstraction, etc…

THEOREM. If

- $\langle L, \leq\rangle$ and $\langle M, \sqsubseteq\rangle$ are posets;
- $\langle L, \leq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle M, \sqsubseteq\rangle$ and $F^\sharp \in M \mapsto M$

or $\langle L, \leq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle M, \sqsubseteq\rangle$ and $F^\sharp \in M \stackrel{m}{\longmapsto} M$

- $F \in L \stackrel{m}{\not\longmapsto} L$ is a monotonic partial map
- $\perp \leq F(\perp)$
- $F^0 = \perp$, $F^{\delta+1} = F(F^\delta)$, $\bigvee_{\beta<\lambda} F^\beta$ exists when λ is a limit ordinal and $F^\lambda = \bigvee_{\beta<\lambda} F^\beta$
- $\forall \delta : \alpha \circ F(F^\delta) = F^\sharp \circ \alpha(F^\delta)$

then:

- $F^\sharp = \alpha \circ F \circ \gamma$
- $\alpha(\mathsf{lfp}_\perp^{\leq} F) = \mathsf{lfp}_{\alpha\perp}^{\sqsubseteq} F^\sharp$
- The iteration order of $F^\sharp$ is less than or equal to that of F

■

PROOF.

Lemma 1

$\forall \delta \in \mathbb{O} : \alpha(F^\delta) = F^{\sharp\delta}$ where $F^{\sharp 0} = \perp^\sharp \stackrel{\text{def}}{=} \alpha(\perp)$, $F^{\sharp\delta+1} = F^\sharp(F^{\sharp\delta})$ and $F^{\sharp\lambda} = \bigsqcup_{\beta<\lambda} F^{\sharp\beta}$ is well-defined when λ is a limit ordinal.

PROOF. By transfinite induction on δ:

- $\alpha(\perp) = \perp^\sharp$, — def. $\perp^\sharp$
- The induction hyp. $\alpha(F^\delta) = F^{\sharp\delta}$ implies

$\alpha(F^{\delta+1})$	
$= \alpha(F(F^\delta))$	def. $F^{\sharp\delta+1}$
$= F^\sharp(\alpha(F^\delta))$	commutation property
$= F^\sharp(F^{\sharp\delta})$	ind. hyp.
$= F^{\sharp\delta+1}$	def. $F^{\sharp\delta}$

- If $\alpha(F^\beta) = F^{\sharp\beta}$ for $\beta < \lambda$, λ limit ordinal by induction hyp., then

$\alpha(F^\lambda)$	
$= \alpha(\bigvee_{\beta<\lambda} F^\beta)$	def. F^λ where the lub is assumed to exist
$= \bigsqcup_{\beta<\lambda} \alpha(F^\beta)$	since α preserves existing lubs so $\bigsqcup_{\beta<\lambda} \alpha(F^\beta)$ exists
$= \bigsqcup_{\beta<\lambda} F^{\sharp\beta}$	induction hyp.
$= F^{\sharp\lambda}$	def. $F^{\sharp\lambda}$ for λ limit ordinal.

□

Lemma 2

$F^\delta, \delta \in \mathbb{O}$ is a $\sqsubseteq$-increasing chain.

PROOF. By transfinite induction on δ:

- $F^0 = \perp \leq F(\perp) = F^1$ — since $\perp$ is assumed to be a prefixpoint
- If $F^\delta \leq F^{\delta+1}$ — induction hyp.
  $\Longrightarrow F^{\delta+1} = F(F^\delta) \leq F(F^{\delta+1}) = F^{\delta+2}$ — by monotony
- $\forall \delta < \lambda$, λ limit ordinal:
  $F^\delta \leq \bigsqcup_{\beta<\lambda} F^\beta = F^\lambda$ — by def. of lubs and F^δ assumed to exist.

□

Lemma 3

$$\exists \epsilon \in \mathbb{O} : F(F^{\epsilon}) = F^{\epsilon}.$$

PROOF. – The chain $F^{\delta}, \delta \in \mathbb{O}$ cannot be strictly increasing since it is included in the set L so that its cardinality must be less than that of L proving that $\exists \epsilon < \epsilon' : F^{\epsilon} = F^{\epsilon'}$ where ϵ' is the least ordinal with the same cardinality as L.

– $F^{\epsilon} \leq F^{\epsilon+1} \leq F^{\epsilon'} = F^{\epsilon}$ so that $F^{\epsilon} = F^{\epsilon+1} = F(F^{\epsilon})$ by antisymmetry and definition of the iterates. $\square$

Lemma 4

$$\text{If } \bot \leq X = F(X) \text{ then } \forall \delta \in \mathbb{O} : F^{\delta} \leq X.$$

PROOF. By transfinite induction on δ:

– $F^0 = \bot \leq X$ by hypothesis;

– If $F^{\delta} \leq X$ by induction hyp., then

$F^{\delta+1} = F(F^{\delta}) \leq F(X) = X$ by ind. hyp., monotonicity and fixpoint property;

– if $F^{\beta} \leq X$ for all $\beta < \lambda$, λ limit ordinal, then: $F^{\delta} = \bigsqcup_{\beta<\lambda} F^{\beta} \leq X$ by def. of lub (assumed to exist). $\square$

Lemma 5

$$\text{If } \exists \epsilon \in \mathbb{O} : F^{\epsilon} = \mathsf{lfp}^{\leq}_{\bot} F.$$

PROOF. By lemma 2, $\bot = F^0 \leq F^{\epsilon}$ and $F(F^{\epsilon}) = F^{\epsilon}$ by lemma 3.

If $\bot \leq X = F(X)$ then, by lemma 4, $F^{\epsilon} \leq X$ proving that F^{ϵ} is the least fixpoint of F greater than or equal to $\bot$, so $F^{\epsilon} = \mathsf{lfp}^{\leq}_{\bot} F$. $\square$

Lemma 6

$$\text{If } F^{\sharp^{\epsilon}} = F^{\sharp}(F^{\sharp^{\epsilon}}).$$

PROOF. $F^{\sharp^{\epsilon+1}} = F^{\sharp}(F^{\sharp^{\epsilon}}) = F^{\sharp}(\alpha(F^{\epsilon})) = \alpha(F(F^{\epsilon})) = \alpha(F^{\epsilon}) = F^{\sharp^{\epsilon}}$ by def. $F^{\sharp^{\epsilon+1}}$ =, lemma 1, commutation property, lemma 3, lemma 1. $F^{\sharp^{\epsilon}}$ exists by lemma 1. $\square$

Lemma 7

$F^{\sharp}$ is monotonic.

PROOF.

$\alpha \circ F = F^{\sharp} \circ \alpha$ — commutation property

$\Longrightarrow \lambda x \cdot \alpha \circ F \circ \gamma(x) = F^{\sharp} \circ \alpha \circ \gamma(x)$ — def. = on functions

$\Longrightarrow \alpha \circ F \circ \gamma = F^{\sharp}$ since $\alpha \circ \gamma(x) = x$ when α is surjective in a Galois connection

$\Longrightarrow F^{\sharp}$ is monotonic, as a composition of monotonic functions. $\square$

Note: Instead of α surjective and $F^{\sharp} \in M \mapsto M$, we can also assume that $F^{\sharp} \in M \overset{\text{m}}{\longmapsto} M$ without assuming α surjective.

Lemma 8

$$\text{If } \alpha(\bot) \sqsubseteq Y = F^{\sharp}(Y) \text{ then } \forall \delta \in \mathbb{O} : F^{\sharp^{\delta}} \sqsubseteq Y.$$

PROOF. Identical to that of lemma 4, using lemma 7 (or the corresponding hypothesis $F^{\sharp} \in M \overset{\text{m}}{\longmapsto} M$). $\square$

Lemma 9

$$F^{\sharp^{\epsilon}} = \mathsf{lfp}^{\sqsubseteq}_{\alpha\bot} F^{\sharp}.$$

PROOF. $\bot \leq F^{\epsilon}$ hence $\alpha(\bot) \sqsubseteq \alpha(F^{\epsilon}) = F^{\sharp^{\epsilon}}$ by lemma 2, α is monotonic, lemma 1. We have $F^{\sharp}(F^{\sharp^{\epsilon}}) = F^{\sharp^{\epsilon}}$ by lemma 6. If $\alpha(\bot) \sqsubseteq Y = F^{\sharp}(Y)$ then $F^{\sharp^{\epsilon}} \sqsubseteq Y$ by lemma 8. $\square$

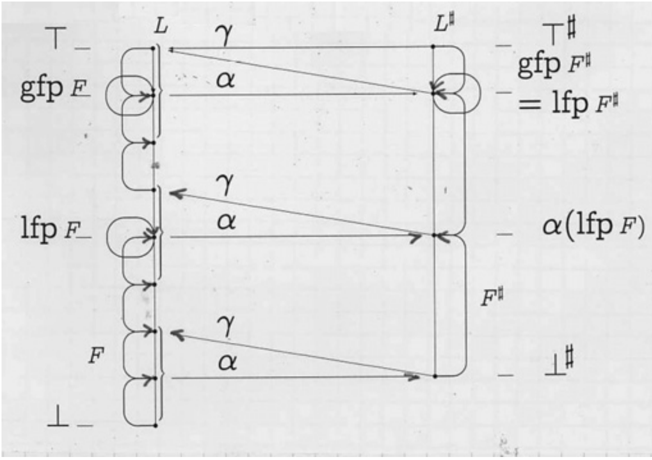
PROOF. (of the theorem)

$$\begin{array}{lll} & \alpha(\mathsf{lfp}^{\leq}_{\bot} F) & \\ = & \alpha(F^{\epsilon}) & \text{by lemma 5} \\ = & F^{\sharp^{\epsilon}} & \text{by lemma 1} \\ = & \mathsf{lfp}^{\sqsubseteq}_{\alpha\bot} F^{\sharp} & \text{by lemma 9} \end{array}$$

$\square$

$\square$

example:



À la Kleene exact fixpoint abstraction with continuous abstraction

THEOREM. If

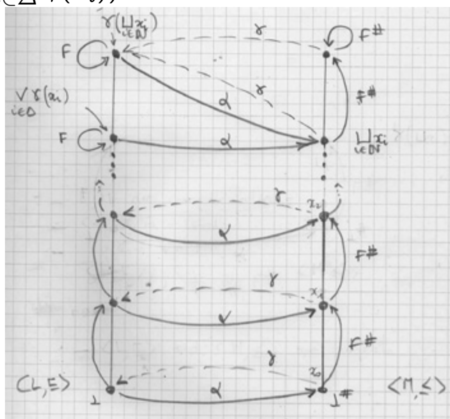
- $\langle L, \leq\rangle$ and $\langle M, \sqsubseteq\rangle$ are posets
- $F \in L \overset{\text{m}}{\longmapsto} L$ is a monotonic partial map on L
- $F^\sharp \in M \overset{\text{m}}{\longmapsto} M$ is a monotonic map on M
- $\alpha \in L \mapsto M$ is upper continuous
- $\perp \leq F(\perp)$
- $F^0 = \perp$, $F^{\delta+1} = F(F^\delta)$, $\bigvee_{\beta<\lambda} F^\beta$ exists when λ is a limit ordinal in which case $F^\lambda = \bigvee_{\beta<\lambda} F^\beta$
- $\forall \delta \in \mathbb{O} : \alpha \circ F(F^\delta) = F^\sharp \circ \alpha(F^\delta)$

then

- $\alpha(\mathsf{lfp}^{\leq}_{\perp} F) = \mathsf{lfp}^{\sqsubseteq}_{\alpha(\perp)} F^\sharp$

PROOF. Essentially identical to that of the previous theorem. One first prove lemma 2 by monotony of F and then lemma 1 since α is upper continuous and the iterates pf F from $\perp$ form an increasing chain. The proofs of lemmata 3 to 6 and 8 to 9 are unchanged while lemma 7 is now an hypothesis. The rpoof of the theorem is identical. ☐

Note: the commutation condition does not work with γ for $\mathsf{lfp}\ F$ (it does, by duality, for $\mathsf{gfp}\ F$). A counter-example is $(\gamma(\bigsqcup_{i\in\Delta} x_i) \neq \bigvee_{i\in\Delta} \gamma(x_i))$:



We have

- $\langle L, \leq\rangle$ and $\langle M, \sqsubseteq\rangle$ are posets
- F, $F^\sharp$ are monotone
- $\langle L, \leq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle L, \sqsubseteq\rangle$
- $\gamma \circ F^\sharp = F \circ \gamma$

but

- $\alpha(\mathsf{lfp}\ F) \neq \mathsf{lfp}\ F^\sharp$

À la Tarski exact fixpoint abstraction

THEOREM. If $\langle \mathcal{D}^\natural, \sqsubseteq^\natural, \perp^\natural, \sqcup^\natural \rangle$ and $\langle \mathcal{D}^\sharp, \sqsubseteq^\sharp, \perp^\sharp, \sqcup^\sharp \rangle$ are complete lattices, $F^\natural \in \mathcal{D}^\natural \xrightarrow{m} \mathcal{D}^\natural$, $F^\sharp \in \mathcal{D}^\sharp \xrightarrow{m} \mathcal{D}^\sharp$ are monotonic and

- α is a complete $\sqcap$-morphism (a)
- $F^\sharp \circ \alpha \sqsubseteq^\sharp \alpha \circ F^\natural$ (b)
- $\forall y \in \mathcal{D}^\sharp : F^\sharp(y) \sqsubseteq^\sharp y \Longrightarrow \exists x \in \mathcal{D}^\natural : \alpha(x) = y \wedge F^\natural(x) \sqsubseteq^\natural x$ (c)

then

$$\alpha(\mathsf{lfp}^{\sqsubseteq^\natural} F^\natural) = \mathsf{lfp}^{\sqsubseteq^\sharp} F^\sharp$$

■

PROOF.

$$\begin{array}{lll}
\text{(d)} & F^\natural(x) \sqsubseteq^\natural x & \\
& \Longrightarrow \alpha \circ F^\natural(x) \sqsubseteq^\natural \alpha(x) & \text{since } \alpha \text{ is monotonic by (a)} \\
& \Longrightarrow F^\sharp \circ \alpha(x) \sqsubseteq^\natural \alpha(x) & \text{by (b)}
\end{array}$$

$$\text{(e)}\quad \{\alpha(x) \mid F^\natural(x) \sqsubseteq^\natural x\} = \{y \mid F^\sharp(y) \sqsubseteq^\sharp y\} \qquad \text{by (c) and (d)}$$

$$\begin{array}{lll}
\text{(f)} & \sqcap^\sharp\{\alpha(x) \mid F^\natural(x) \sqsubseteq^\natural x\} = \sqcap^\sharp\{y \mid F^\sharp(y) \sqsubseteq^\sharp y\} & \text{by (e)} \\
& \Longrightarrow \alpha(\sqcap^\natural\{x \mid F^\natural(x) \sqsubseteq^\natural x\}) = \sqcap^\sharp\{y \mid F^\sharp(y) \sqsubseteq^\sharp y\} & \text{by (a)} \\
& \Longrightarrow \alpha(\mathsf{lfp}^{\sqsubseteq^\natural} F^\natural) = \mathsf{lfp}^{\sqsubseteq^\sharp} F^\sharp & \text{by Tarski's fixpt th.}
\end{array}$$

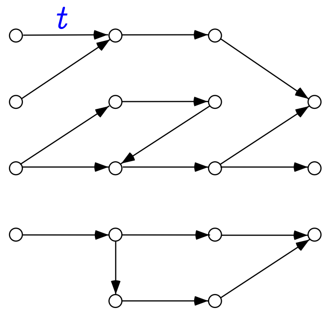
□

Example: application to reachability

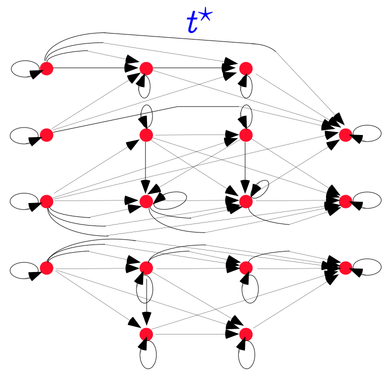
Transition systems

- $\langle S, t \rangle$ where:
  - S is a set of states/vertices/...
  - $t \in \wp(S \times S)$ is a transition relation/set of arcs/...

Example of transition system



The reflexive transitive closure of the example transition system



Reflexive closure of transition systems

Let r be a relation on x:

- $r^0 \stackrel{\text{def}}{=} 1_x$ powers
- $r^{n+1} \stackrel{\text{def}}{=} r^n \circ r \ (= r \circ r^n)$
- $r^\star \stackrel{\text{def}}{=} \bigcup_{n \in \mathbb{N}} r^n$ reflexive transitive closure
- $r^+ \stackrel{\text{def}}{=} \bigcup_{n \in \mathbb{N} \setminus \{0\}} r^n$ strict transitive closure

  so $r^\star = r^+ \cup 1_x$

Reflexive transitive closure in fixpoint form

$$t^* = \mathsf{lfp}^{\subseteq} \lambda X \cdot t^0 \cup X \circ t$$

PROOF.

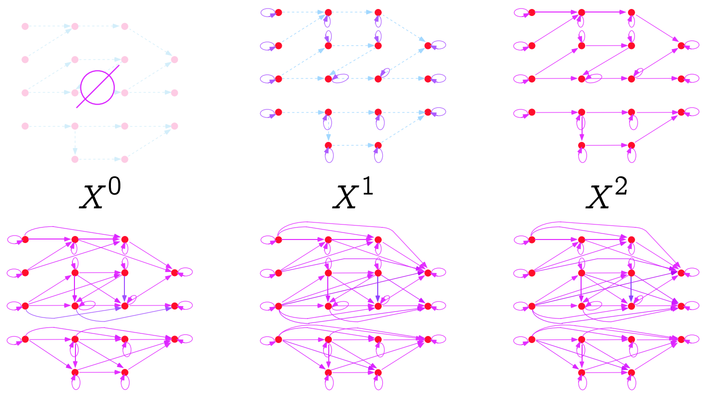
$$\begin{aligned}
X^0 &= \emptyset \\
X^1 &= t^0 \cup X^0 \circ t \ = \ t^0 \\
X^2 &= t^0 \cup X^1 \circ t \ = \ {}^0 \cup t^0 \circ t \ = \ t^0 \cup t^1 \\
\ldots & \quad \ldots \\
X^n &= \bigcup_{0 \le i < n} t^i \qquad \text{(induction hypothesis)}
\end{aligned}$$

$$\begin{aligned}
X^{n+1} &= t^0 \cup X^n \circ t \\
&= t^0 \cup \Big(\bigcup_{0 \le i < n} t^i\Big) \circ t \\
&= t^0 \cup \bigcup_{0 \le i < n} (t^i \circ t) \\
&= t^0 \cup \bigcup_{1 \le i+1 < n+1} (t^{i+1}) \\
&= t^0 \cup \Big(\bigcup_{1 \le j < n+1} t^j\Big) \circ t \\
&= \bigcup_{0 \le i < n+1} t^i
\end{aligned}$$

$$
\begin{aligned}
\ldots \quad & \ldots \\
X^\omega &= \bigcup_{n\geq 0} X^n \\
&= \bigcup_{n\geq 0} \bigcup_{0\leq i<n} t^i \\
&= \bigcup_{n\geq 0} t^n \\
&= t^*
\end{aligned}
\qquad
\begin{aligned}
X^{\omega+1} &= t^0 \cup X^\omega \circ t \\
&= t^0 \cup (\bigcup_{n\geq 0} t^n) \circ t \\
&= t^0 \cup \bigcup_{n\geq 0} (t^n \circ t) \\
&= t^0 \cup \bigcup_{n\geq 0} t^{n+1} \\
&= t^0 \cup \bigcup_{k\geq 1} t^k \\
&= \bigcup_{n\geq 0} t^n \\
&= t^*
\end{aligned}
$$

□

Examples of iterates

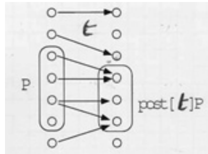


X^0 X^1 X^2

X^3 X^4 $X^5 = t^*$

Post-image

$$\text{post}[t]I = \{s' \mid \exists s \in I : \langle s, s'\rangle \in t\}$$



We have $\text{post}[\bigcup_{i\in\Delta} t^i]I = \bigcup_{i\in\Delta} \text{post}[t^i]I$ so $\alpha = \lambda t \cdot \text{post}[t]I$ is the lower adjoint of a Galois connection.

Postimage Galois connection

Given $I \in \wp(S)$,

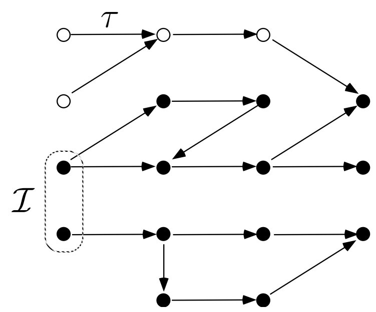
$$\langle \wp(S \times S), \subseteq\rangle \underset{\lambda t\cdot \text{post}[t]I}{\overset{\gamma}{\leftrightarrows}} \langle \wp(S), \subseteq\rangle$$

Proof.

$$
\begin{aligned}
& \text{post}[t]I \subseteq R \\
\Leftrightarrow\ & \{s' \mid \exists s \in I : \langle s, s'\rangle \in t\} \subseteq R \\
\Leftrightarrow\ & \forall s' \in S : (\exists s \in I : \langle s, s'\rangle \in t) \Rightarrow (s' \in R) \\
\Leftrightarrow\ & \forall s', s \in S : (s \in I \wedge \langle s, s'\rangle \in t) \Rightarrow (s' \in R) \\
\Leftrightarrow\ & \forall s', s \in S : \langle s, s'\rangle \in t \Rightarrow ((s \in I) \Rightarrow (s' \in R)) \\
\Leftrightarrow\ & t \subseteq \{\langle s, s'\rangle \mid (s \in I) \Rightarrow (s' \in R)\} \stackrel{\text{def}}{=} \gamma(R)
\end{aligned}
$$

□

Reachable states



$$\mathsf{post}[t^*]\mathcal{I}$$

Reachable states in fixpoint form

$$\begin{aligned}
&\mathsf{post}[t^*]I, \quad I \text{ given} \\
&= \alpha(t^*) \quad \text{where} \quad \alpha(t) = \mathsf{post}[t]I = \{s' \mid \exists s \in I : \langle s, s' \rangle \in t\} \\
&= \alpha(\mathsf{lfp}^{\subseteq}\, \lambda X \cdot t^0 \cup X \circ t) \\
&= \mathsf{lfp}^{\subseteq}\, \overline{F} \ ???
\end{aligned}$$

Discovering the abstract transformer by calculus

$$\begin{aligned}
&\alpha \circ (\lambda X \cdot t^0 \cup X \circ t) \\
&= \lambda X \cdot \alpha(t^0 \cup X \circ t) \\
&= \lambda X \cdot \alpha(t^0) \cup \alpha(X \circ t) \\
&= \lambda X \cdot \mathsf{post}[t^0]I \cup \mathsf{post}[X \circ t]I
\end{aligned}$$

$$\begin{aligned}
&\mathsf{post}[t^0]I \\
&= \{s' \mid \exists s \in I : \langle s, s' \rangle \in t^0\} \\
&= \{s' \mid \exists s \in I : \langle s, s' \rangle \in \{\langle s, s \rangle \mid s \in S\}\} \\
&= \{s' \mid \exists s \in I\} \\
&= I
\end{aligned}$$

$$
\begin{aligned}
& \text{post}[X \circ t]I \\
= \ & \{s' \mid \exists s \in I : \langle s, s' \rangle \in (X \circ t)\} \\
= \ & \{s' \mid \exists s \in I : \langle s, s' \rangle \in \{\langle s, s'' \rangle \mid \exists s' : \langle s, s" \rangle \in X \wedge \langle s', s'' \rangle \in t\}\} \\
= \ & \{s' \mid \exists s \in I : \exists s'' \in S : \langle s, s" \rangle \in X \wedge \langle s', s'' \rangle \in t\} \\
= \ & \{s' \mid \exists s'' \in S : (\exists s \in I : \langle s, s" \rangle \in X) \wedge \langle s', s'' \rangle \in t\} \\
= \ & \{s' \mid \exists s'' \in S : s'' \in \{s'' \mid \exists s \in I : \langle s, s" \rangle \in X\} \wedge \langle s', s'' \rangle \in t\} \\
= \ & \{s' \mid \exists s'' \in S : s'' \in \text{post}[X]I \wedge \langle s', s'' \rangle \in t\} \\
= \ & \text{post}[t](\text{post}[X]I) \\
= \ & \text{post}[t](\alpha(X))
\end{aligned}
$$

$$
\begin{aligned}
& \alpha \circ (\lambda X \cdot t^0 \cup X \circ t) \\
= \ & \ldots \\
= \ & \lambda X \cdot \text{post}[t^0]I \cup \text{post}[X \circ t]I \\
= \ & \lambda X \cdot I \cup \text{post}[t](\alpha(X)) \\
= \ & \lambda X \cdot \overline{F}(\alpha(X))
\end{aligned}
$$

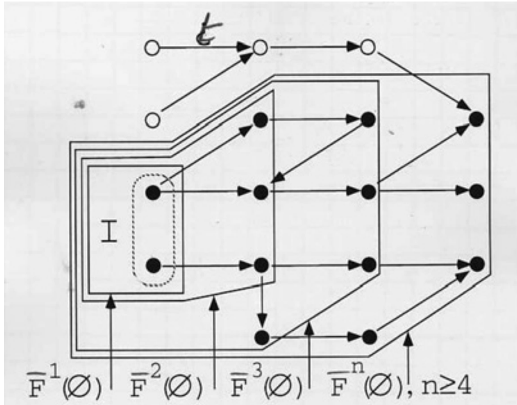
by defining:

$$\overline{F} = \lambda X \cdot I \cup \text{post}[t](X)$$

proving:

$$\text{post}[t^*](I) = \text{lfp}^{\subseteq} \lambda X \cdot I \cup \text{post}[t](X)$$

Example of iteration



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/.