

ABSTRACT INTERPRETATION: THEORY AND APPLICATIONS

P. COUSOT

Patrick.Cousot@ens.fr <http://www.di.ens.fr/~cousot>

Second International Summer School in Computational Logic, ISCL 2002

25th—30th August 2002, Acquafredda di Maratea (Basilicata, Italy)

© P. COUSOT, ALL RIGHTS RESERVED.

1. 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/...

REFLEXIVE TRANSITIVE CLOSURE

- Composition:

- $t \circ t' \stackrel{\text{def}}{=} \{ \langle s, s'' \rangle \mid \exists s' : \langle s, s' \rangle \in t \wedge \langle s', s'' \rangle \in t' \}$

- Powers:

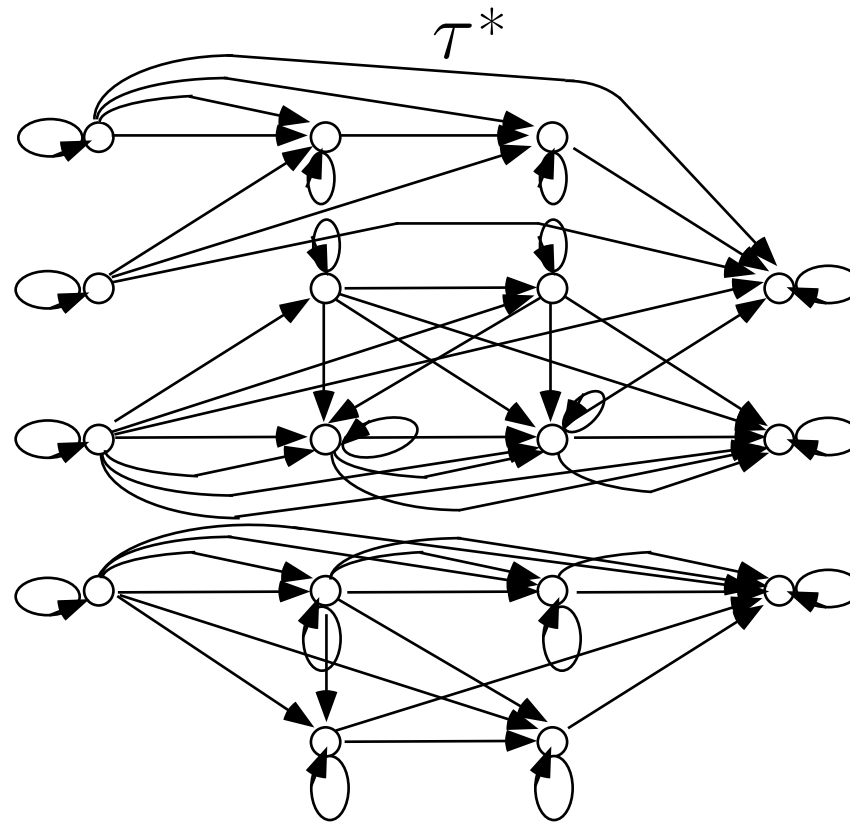
- $t^0 \stackrel{\text{def}}{=} \{ \langle s, s \rangle \mid s \in S \}$

- $t^{n+1} \stackrel{\text{def}}{=} t^n \circ t \quad n \geq 0$

- Reflexive transitive closure:

- $t^* = \bigcup_{n \geq 0} t^n$

EXAMPLE OF TRANSITIVE REFLEXIVE CLOSURE



REFLEXIVE TRANSITIVE CLOSURE IN FIXPOINT FORM

$$t^* = \text{lfp}^{\subseteq} \lambda X . t^0 \cup X \circ t$$

Proof

$$X^0 = \emptyset$$

$$X^1 = t^0 \cup X^0 \circ t = t^0$$

$$X^2 = t^0 \cup X^1 \circ t = t^0 \cup t^0 \circ t = t^0 \cup t^1$$

...

$$X^n = \bigcup_{0 \leq i < n} t^i \quad (\text{induction hypothesis})$$

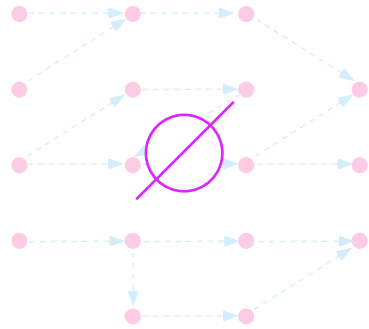
$$\begin{aligned}
X^{n+1} &= t^0 \cup X^n \circ t \\
&= t^0 \cup \left(\bigcup_{0 \leq i < n} t^i \right) \circ t \\
&= t^0 \cup \bigcup_{0 \leq i < n} (t^i \circ t) \\
&= t^0 \cup \bigcup_{1 \leq i+1 < n+1} (t^{i+1}) \\
&= t^0 \cup \left(\bigcup_{1 \leq j < n+1} t^j \right) \circ t \\
&= \bigcup_{0 \leq i < n+1} t^i \\
&\dots \quad \dots
\end{aligned}$$

$$\begin{aligned}
X^\omega &= \bigcup_{n \geq 0} X^n \\
&= \bigcup_{n \geq 0} \bigcup_{0 \leq i < n} t^i \\
&= \bigcup_{n \geq 0} t^n \\
&= t^*
\end{aligned}$$

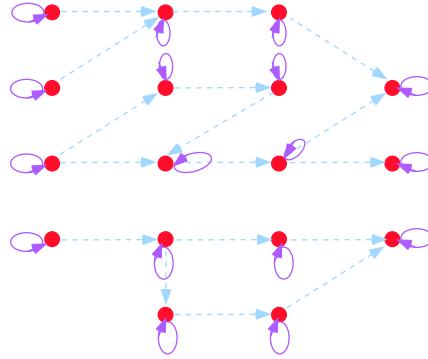
$$\begin{aligned}
X^{\omega+1} &= t^0 \cup X^\omega \circ t \\
&= t^0 \cup \left(\bigcup_{n \geq 0} t^n \right) \circ t \\
&= t^0 \cup \bigcup_{n \geq 0} (t^n \circ t) \\
&= t^0 \cup \bigcup_{n \geq 0} t^{n+1} \\
&= t^0 \cup \bigcup_{k \geq 1} t^k \\
&= \bigcup_{n \geq 0} t^n \\
&= t^*
\end{aligned}$$



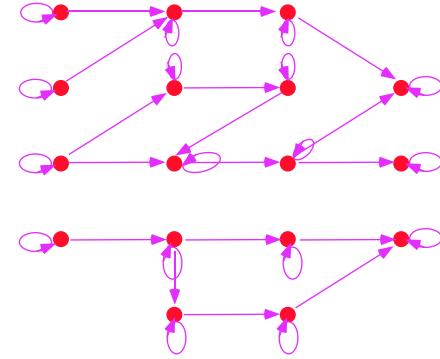
ITERATES



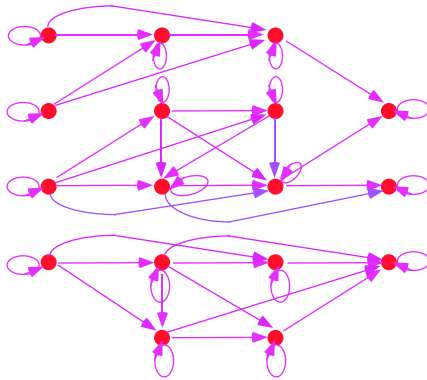
X^0



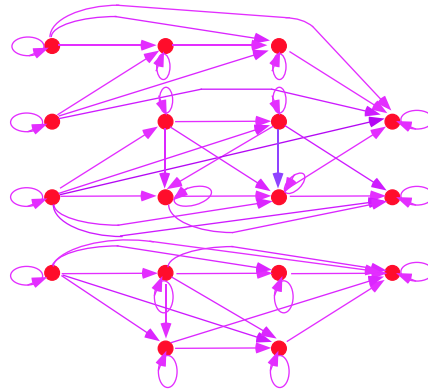
X^1



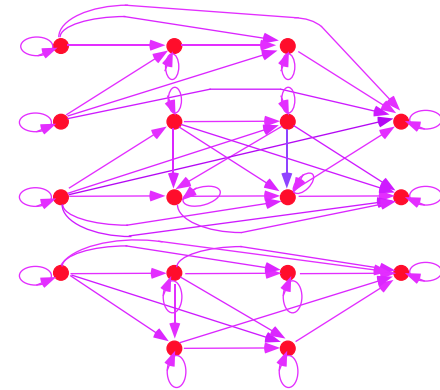
X^2



X^3



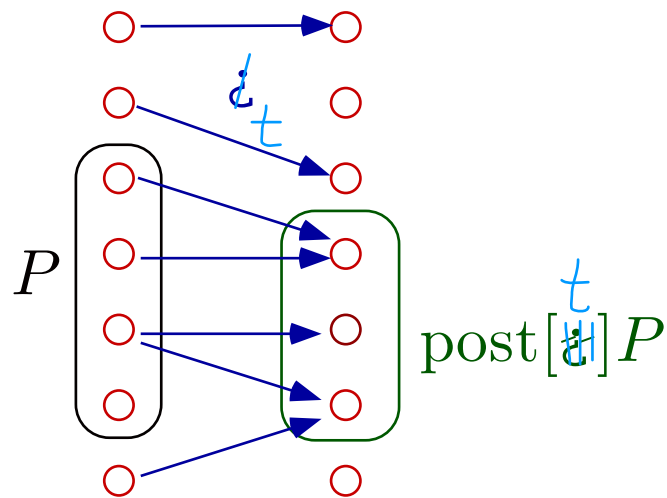
X^4



$X^5 = t^*$

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 $I \in \wp(S)$,

$$\langle \wp(S \times S), \subseteq \rangle \begin{array}{c} \xleftarrow{\gamma} \\ \xrightarrow{\lambda t \cdot \text{post}[t]I} \end{array} \langle \wp(S), \subseteq \rangle$$

$$\text{post}[t]I \subseteq R$$

$$\Leftrightarrow \{s' \mid \exists s \in I : \langle s, s' \rangle \in t\} \subseteq R$$

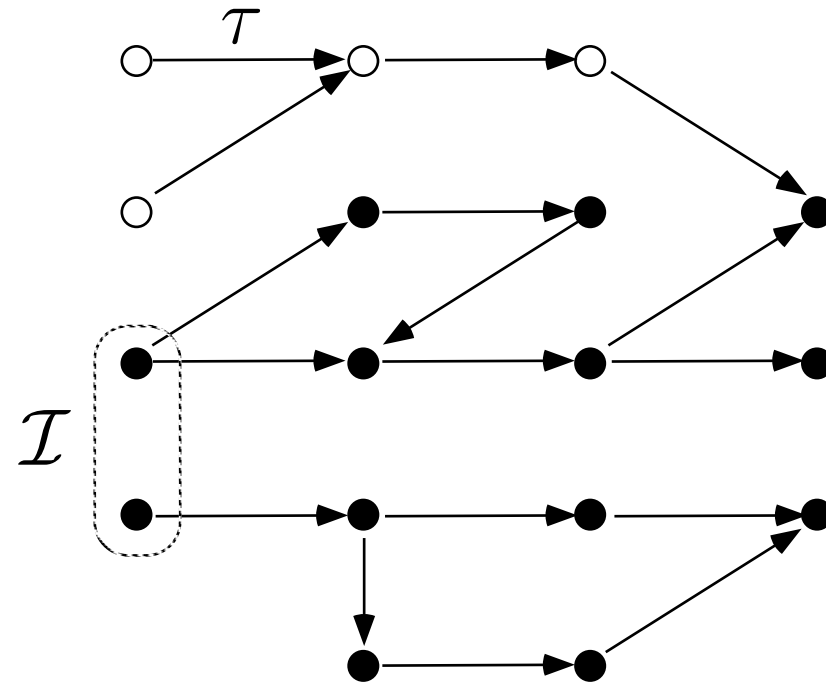
$$\Leftrightarrow \forall s' \in S : (\exists s \in I : \langle s, s' \rangle \in t) \Rightarrow (s' \in R)$$

$$\Leftrightarrow \forall s', s \in S : (s \in I \wedge \langle s, s' \rangle \in t) \Rightarrow (s' \in R)$$

$$\Leftrightarrow \forall s', s \in S : \langle s, s' \rangle \in t \Rightarrow ((s \in I) \Rightarrow (s' \in R))$$

$$\Leftrightarrow t \subseteq \{\langle s, s' \rangle \mid (s \in I) \Rightarrow (s' \in R)\} \stackrel{\text{def}}{=} \gamma(R)$$

REACHABLE STATES



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

FIXPOINT ABSTRACTION, ONCE AGAIN

Let $F \in L \xrightarrow{m} L$ and $\bar{F} \in \bar{L} \xrightarrow{m} \bar{L}$ be respective monotone maps on the cpos $\langle L, \perp, \sqsubseteq \rangle$ and $\langle \bar{L}, \bar{\perp}, \bar{\sqsubseteq} \rangle$ and $\langle L, \sqsubseteq \rangle \xrightleftharpoons[\alpha]{\gamma} \langle \bar{L}, \bar{\sqsubseteq} \rangle$ such that $\alpha \circ F \circ \gamma \dot{\sqsubseteq} \bar{F}$. Then¹:

- $\forall \delta \in \mathbb{O}: \alpha(F^\delta) \bar{\sqsubseteq} \bar{F}^\delta$ (iterates from the infimum);
- The iteration order of \bar{F} is \leq to that of F ;
- $\alpha(\text{lfp}^{\sqsubseteq} F) \bar{\sqsubseteq} \text{lfp}^{\bar{\sqsubseteq}} \bar{F}$;

Soundness: $\text{lfp}^{\bar{\sqsubseteq}} \bar{F} \bar{\sqsubseteq} \bar{P} \Rightarrow \text{lfp}^{\sqsubseteq} F \sqsubseteq \gamma(\bar{P})$.

¹ P. Cousot & R. Cousot. *Systematic design of program analysis frameworks*. ACM POPL'79, pp. 269–282, 1979. Numerous variants!

FIXPOINT ABSTRACTION (CONTINUED)

Moreover, the *commutation condition* $\overline{F} \circ \alpha = \alpha \circ F$ implies²:

- $\overline{F} = \alpha \circ F \circ \gamma$, and
- $\alpha(\text{lfp}^{\sqsubseteq} F) = \text{lfp}^{\sqsubseteq} \overline{F}$;

Completeness: $\text{lfp}^{\sqsubseteq} F \sqsubseteq \gamma(\overline{P}) \Rightarrow \text{lfp}^{\sqsubseteq} \overline{F} \sqsubseteq \overline{P}$.

² P. Cousot & R. Cousot. *Systematic design of program analysis frameworks*. ACM POPL'79, pp. 269–282, 1979. Numerous variants!

REACHABLE STATES IN FIXPOINT FORM

$\text{post}[t^*]I$, I given

$$= \alpha(t^*) \quad \text{where} \quad \alpha(t) = \text{post}[t]I = \{s' \mid \exists s \in I : \langle s, s' \rangle \in t\}$$

$$= \alpha(\text{lfp}^{\subseteq} \lambda X . t^0 \cup X \circ t)$$

$$= \text{lfp}^{\subseteq} \overline{F} ???$$

DISCOVERING \overline{F} BY CALCULUS

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

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

$\text{post}[X \circ t]I$

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

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

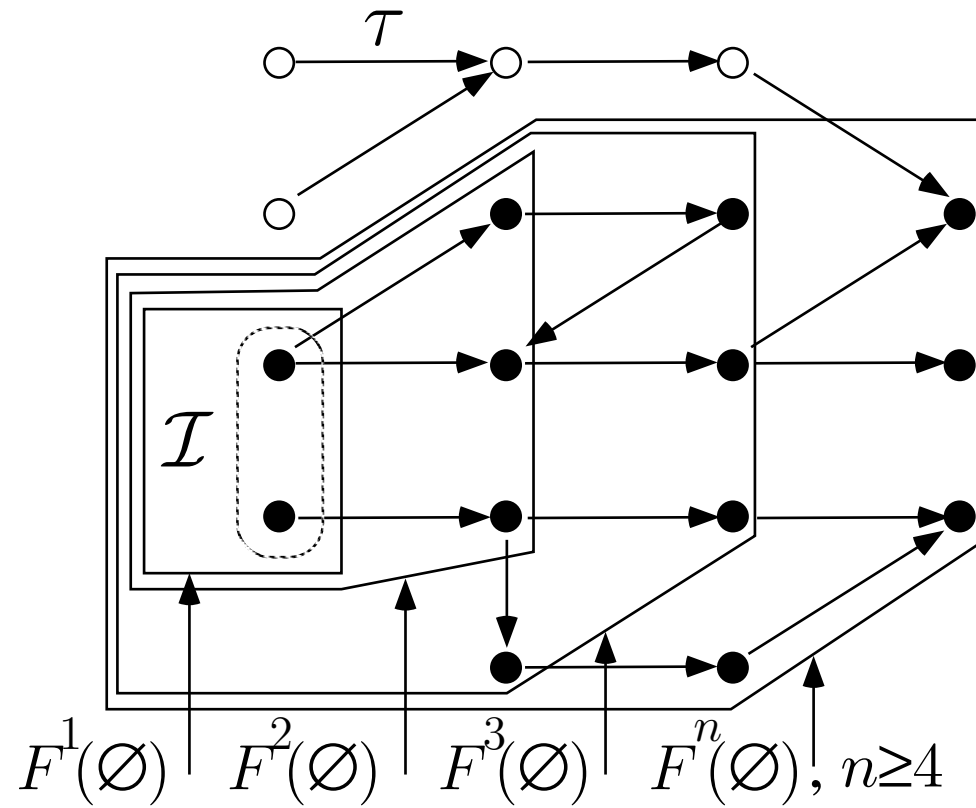
by defining:

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

proving:

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

EXAMPLE OF ITERATION



EXERCICES

- Give a fixpoint characterization for $\text{pre}[t^*]$ where $\text{pre}[t] \stackrel{\text{def}}{=} \text{post}[t^{-1}]$;
- Give a fixpoint characterization for $\bar{\text{pre}}[t^*]$ where $\bar{\text{pre}}[t] \stackrel{\text{def}}{=} \lambda I . \neg \text{pre}[t] \neg I$ (hint: use Park's fixpoint theorem or the Galois connection $\langle \text{post}[t], \bar{\text{pre}}[t] \rangle$).