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

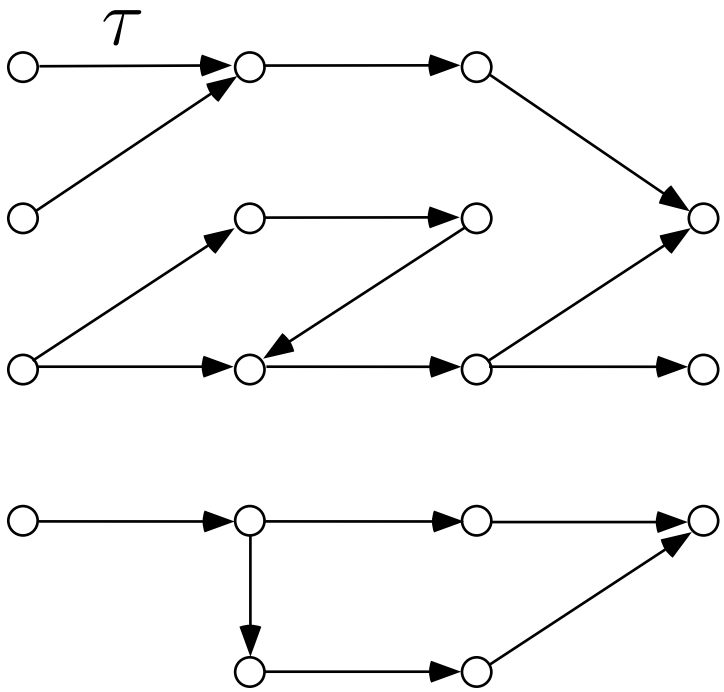
25^{th}—30^{th} August 2002, Acquafredda di Maratea (Basilicata, Italy)

LESSON 3 (2/3-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/...

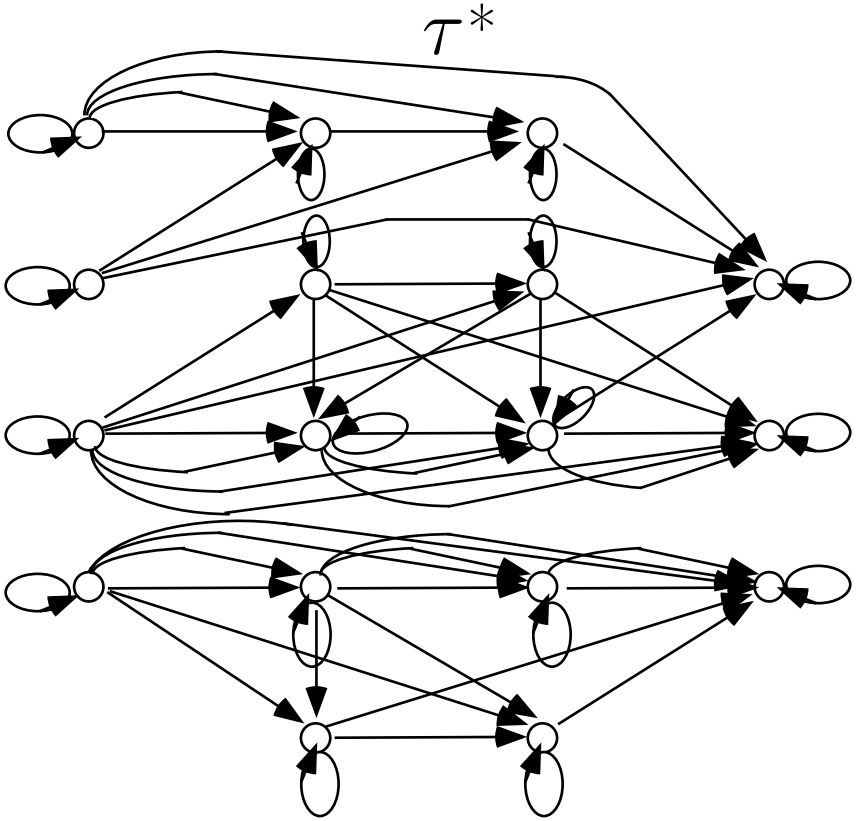
Example of transition system



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:
  - $t^0 \stackrel{\text{def}}{=} \{\langle s, s \rangle \mid s \in S\}$
  - $t^{n+1} \stackrel{\text{def}}{=} t^n \circ t \qquad n \geq 0$
- Reflexive transitive closure:
  - $t^* = \bigcup_{n \geq 0} t^n$

Example of transitive reflexive closure



Reflexive transitive closure in fixpoint form

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

Proof

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

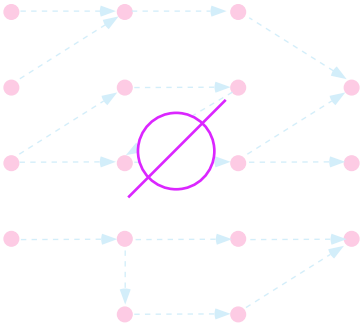
$$
\begin{aligned}
X^{n+1} &= t^0 \cup X^n \circ t \\
&= t^0 \cup \left(\bigcup_{0 \leq i < n} t^i \right) \circ t \\
&= t^0 \cup \bigcup_{0 \leq i < n} \left(t^i \circ t \right) \\
&= t^0 \cup \bigcup_{1 \leq i+1 < n+1} \left(t^{i+1} \right) \\
&= t^0 \cup \left(\bigcup_{1 \leq j < n+1} t^j \right)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

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

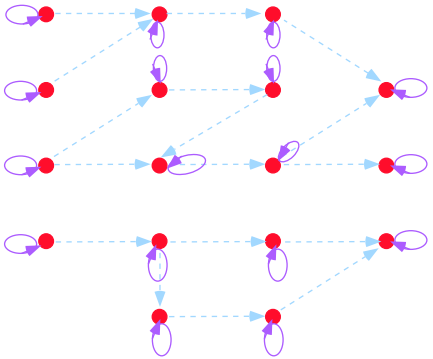
$$
\begin{aligned}
X^{\omega+1} &= t^0 \cup X^\omega \circ t \\
&= t^0 \cup \Big(\bigcup_{n\geq 0} t^n \Big) \circ t \\
&= t^0 \cup \bigcup_{n\geq 0} \big(t^n \circ t \big) \\
&= t^0 \cup \bigcup_{n\geq 0} t^{n+1} \\
&= t^0 \cup \bigcup_{k\geq 1} t^k \\
&= \bigcup_{n\geq 0} t^n \\
&= t^*
\end{aligned}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

□

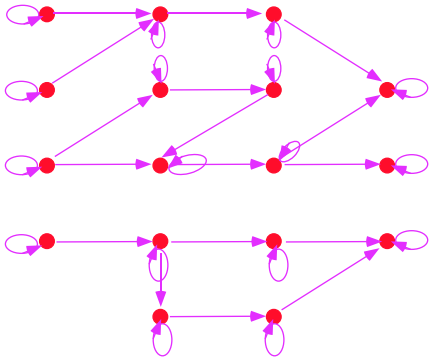
Iterates



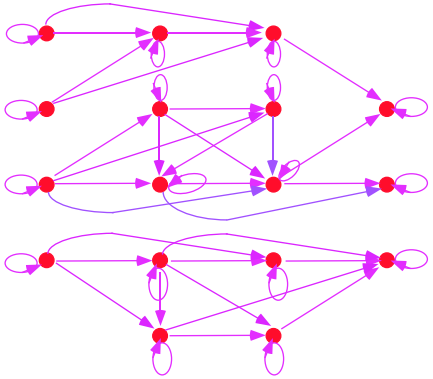
X^0



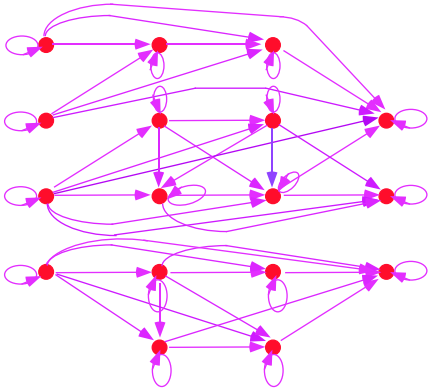
X^1



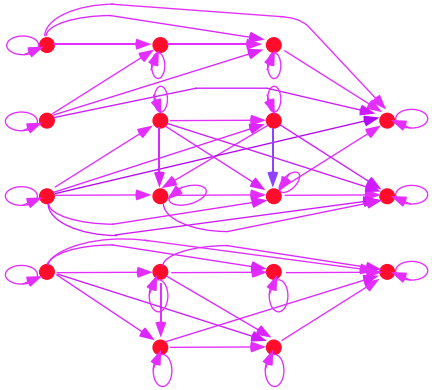
X^2



X^3



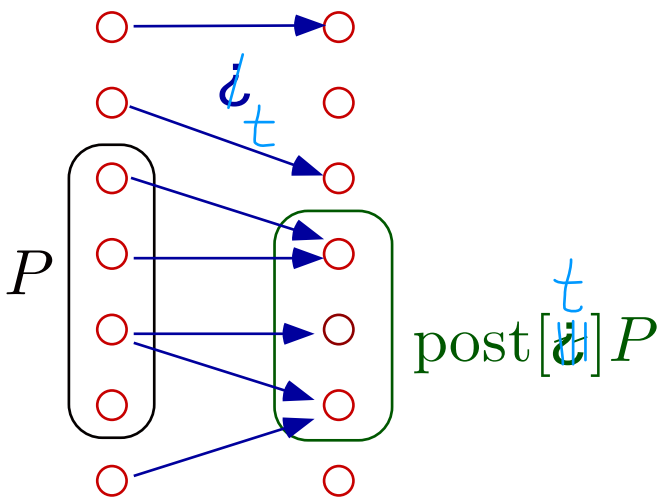
X^4



$X^5 = t^*$

Post-image

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



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

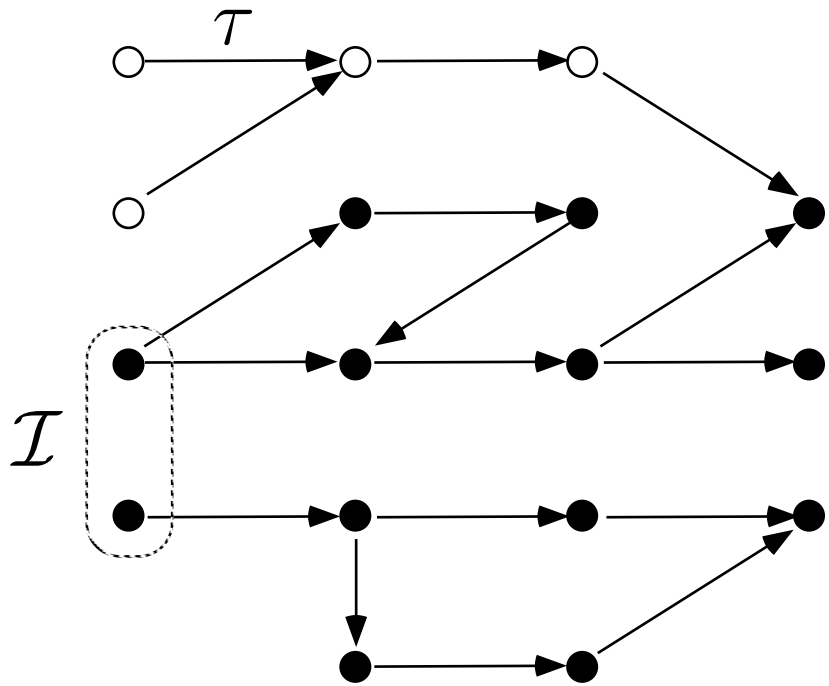
Postimage Galois connection

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

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

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

Reachable states



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

Fixpoint abstraction, once again

Let $F \in L \overset{m}{\longmapsto} L$ and $\overline{F} \in \overline{L} \overset{m}{\longmapsto} \overline{L}$ be respective monotone maps on the cpos $\langle L, \bot, \sqsubseteq \rangle$ and $\langle \overline{L}, \overline{\bot}, \overline{\sqsubseteq} \rangle$ and $\langle L, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \overline{L}, \overline{\sqsubseteq} \rangle$ such that $\alpha \circ F \circ \gamma \dot{\overline{\sqsubseteq}} \overline{F}$. Then [1]:

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

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

[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* $\overline{F} \circ \alpha = \alpha \circ F$ implies [2]:

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

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

[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

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

Discovering $\overline{F}$ by calculus

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

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

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

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

by defining:

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

proving:

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

Example of iteration