Refining Model Checking
by Abstract InterpretationPde------d

Pre- and post-images

$$\mathsf{pre}[t]\,P \overset{\text{def}}{=} \{s \mid \exists s' : \langle s,\, s'\rangle \in t \wedge s' \in P\}$$

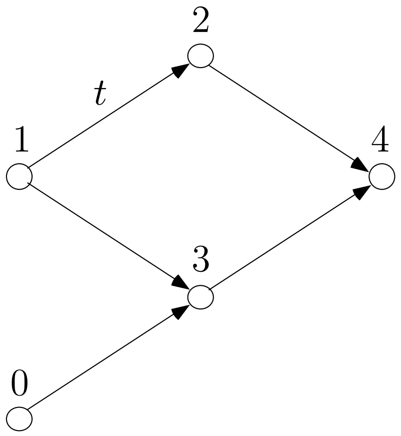
$$\widetilde{\ }\ \sqrt{\ }\ \tilde{\ }[t]\,P \overset{\text{def}}{=} \neg\ \nabla][t](\neg P)$$

$$= \{s \mid \forall s' : \langle s,\, s'\rangle \in t \Longrightarrow s' \in P\}$$

$$\wr\!\int\!\sqcup[t]\,P \overset{\text{def}}{=} \{s' \mid \exists s : s \in P \wedge \langle s,\, s'\rangle \in t\}$$

$$\widetilde{\ }\ \sqrt{\ }\,\}\ [t]\,P \overset{\text{def}}{=} \neg\ \wr\!\int\!\sqcup[t](\neg P)$$

$$= \{s' \mid \forall s : \langle s,\, s'\rangle \in t \Longrightarrow s \in P\}$$



$\mathsf{pre}[t]\{3\} = \{0, 1\}$

$\widetilde{\mathsf{pre}}[t]\{3\} = \{0, 4\}$

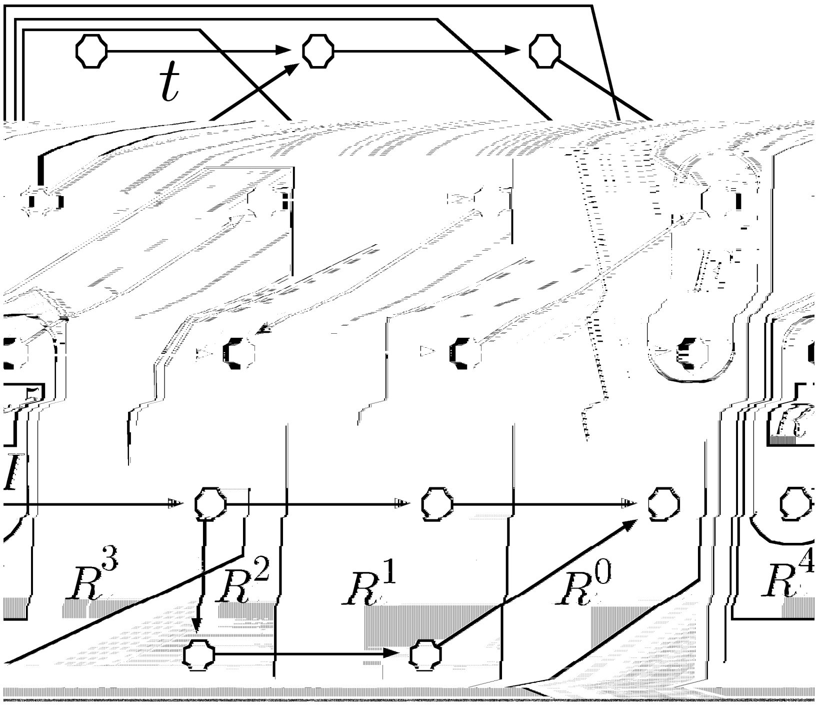
$\mathsf{post}[t]\{1\} = \{2, 3\}$

$\widetilde{\mathsf{post}}[t]\{1\} = \{0, 1, 2\}$

Ma-imum delay algorithm -ma-imum--

procedure cc

--ecution trace of the -ma-imum-- algorithm

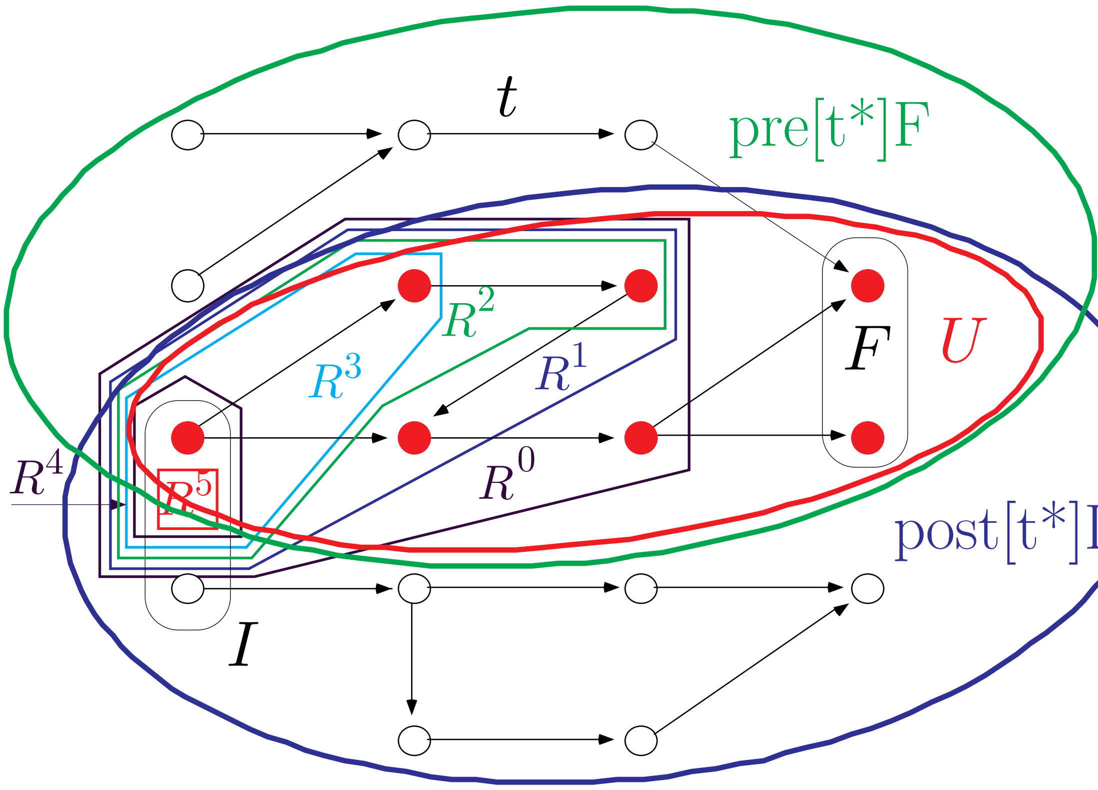


Ma-imum delay algorithm -ma-imum--

-with state search space restriction-

procedure cc

--ecution trace of the -ma-imum-- algorithm



- $\mathcal{A}$\† ⊓ √ √ ⌉∇↖⊣ √ √ ∇≀§⟩⇕$_0$,⊣U_1⟩,≀\.∫. ,$U$$_n$‘ ▷▷▷ *of* U
- $\mathcal{I}$\ ⊔⟨⌉⊒≀∇∫⊔ ⌋⊣$_n$∫⌉=US‘ *hence* ζmaximum2η / ζ

-arski-s --point theorem

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

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

$\langle\dashv\int\ \dashv\ \updownarrow\rceil\dashv\int\sqcup\ \ll\S\ \surd\ \wr\rangle\setminus\sqcup\neg$

$$\updownarrow\{\ \surd\ \varphi = \sqcap\{x \in L \mid \varphi(x) \sqsubseteq x\}$$

$\Leftarrow\int\sqcap\rfloor\langle\ \sqcup\langle\dashv\sqcup$ $\varphi(\mathrm{lfp}\,\varphi) = \mathrm{lfp}\,\varphi$ *and* $\varphi(x) = x$ *implies*
a greatest fixpoint.

$$gfp\,\varphi = \sqcup\{x \in L \mid x \sqsubseteq \varphi(x)\}$$

-i-point characteri

-leenian --point theorem -

-he least --point of an upper-continuous map $\varphi \in L \vdash$
$\langle L,\ \sqsubseteq,\ \perp,\ \sqcup\rangle$ $\rangle\int\neg$

$$\updownarrow\{_{\surd}\ \varphi = \bigsqcup_{n\geq 0} \varphi^n(\perp)$$

where the iterates $\varphi^n(x)$ of φ *from* x *are.*

- $\varphi^0(x) \overset{\text{def}}{=} x,$
- $\varphi^{n+1}(x) \overset{\text{def}}{=} \varphi(\varphi^n(x))$ for all $x \in L$▷

4*Can be generalized to monotonic non›continuous m*

-terati-e characteri

Analysis of the model by abstract interpretation

- 𝒲⌉ ⌋⊣\ ⌋≀⇕ √⊓⊔⌉¬

$$U_0 \supseteq U_1 \supseteq \ldots \supseteq U_n \supseteq U \overset{\text{def}}{=} \text{post}[t^\star]\, I \cap \surd$$

by *abstract interpretation*,

- 𝒯⟨⌉ ⊣⌊∫⊔∇⊣⌋⊔ ⟩\⊔⌉∇ √∇⌉⊔⊣⊔⟩≀\ ⌋⊣\ ⌊⌉ ⌈≀\⌉
  ⌋⟨⌉⌋∥⟩\} ⇐⊣⊔ ⊣↕⇕≀∫⊔ √\≀ ∫⊓ √√↕⌉⇕⌉\⊔⊣∇† ⌋≀∫⊔
- 𝒯⟨⌉ ⊣⌊∫⊔∇⊣⌋⊔ ⟩\⊔⌉∇ √∇⌉⊔⊣⊔⟩≀\ ∇⌉∫⊓↕⊔∫ ⊣∇
  become available to restrict the state search space,
- 𝒮⌉⊑⌉∇⊣↕ ∇⌉∫⊔∇⟩⌋⊔⟩≀\ ≀ √⌉∇⊣⊔≀∇∫ ⟨⊣⊑⌉ ⌊⌉⌉
  ⌋⟨⌉⌋∥⟩\} ⇐⊒⟩⊔⟨ ℬ𝒟𝒟∫ ⇐⌉≀{⊣⌋⊔≀∇⇔ ⌋≀\∫⊔∇⊣
  ⌈∇≀⇔↙

~~∇ℋ⊣↕⌊⊒⊣⌋⟨∫⇔𝒩↙ ⊣\⌈ℛ⊣†⇕≀\⌈⇔𝒫↙ 𝒪\⊔⟨⌉⊓∫⌉~~

$\triangle$ $\triangle$ I
n

-pper appro-imation D of $post[t$ $^{\star}]\, I \;/\; lfp^{\subseteq}_{6}\, \lambda X$

$\triangle\triangle$ by abstract interpretation

1 $\triangleright$ W Consider an abstract domain $\langle L, \sqsubseteq \rangle$

W

$\triangle I_n - \triangle e$

$\triangle\triangle$

$\langle\; WU$

W

$\infty\swarrow \wr\mathcal{B}\Leftarrow\mid\!\leftarrow\ni\exists\prime\leftarrow\dashv\Leftarrow\mathcal{P}\Rightarrow\lfloor\Leftarrow\otimes\sqsupseteq\Leftarrow\Rightarrow\in\prime\infty\}\lfloor\leftarrow\notin\leftarrow$

$\mathit{\Psi}$

$\triangle\triangle rdt43\psi atmbrdt4.nst\leftharpoondown\psi$