Programming Research Laboratory Seoul National University

Basic Concepts of Abstract Interpretation*

Soonho Kong http://ropas.snu.ac.kr/~soon/

May 25, 2007

*Work of P. Cousot and R.Cousot

P. Cousot and R. Cousot.

Basic Concepts of Abstract Interpretation.

In *Building the Information Society*, R. Jacquard (Ed.), pages 359–366. Kluwer Academic Publishers 2004.



Goal

To Understand basic concepts of abstract interpretation.



Contents

- Overview
- Introduction
- Transition Systems
- Partial Trace Semantics
- The Reflexive Transitive Closure Semantics
- The Reachability Semantics
- The Interval Semantics
- Convergence Acceleration

Conclusion



Introduction

Abstract Interpretation:

a theory of approximation of mathematical structures, in particular those involved in the semantic models of computer systems.

Programming Research Laboratory

Transition Systems

Programs are formalized as transition systems τ :

```
\tau = \langle \Sigma, \Sigma_{\texttt{i}}, t \rangle
```

- Σ : a set of states
- $\Sigma_i \subseteq \Sigma$: the set of initial states
- ► t ⊆ Σ × Σ : a transition relation between a state and its possible successors.

Example, the transition system

$$\langle \mathbb{Z}, \{0\}, \{\langle \mathrm{x}, \mathrm{x}'
angle \mid \mathrm{x}' = \mathrm{x}+1\}
angle$$

of program x := 0; while true do x := x + 1.

Partial Trace Semantics

A finite partial execution trace : $\sigma = s_0 s_1 \dots s_n$

►
$$s_0 \in \Sigma$$

$$\blacktriangleright \ \, \text{For all } i < n, \ \langle s_i, s_{i+1} \rangle \in t \\$$

Partial traces of length 0 : ϕ Partial traces of length 1 : $\Sigma^{1}_{\tau} = \{s \mid s \in \Sigma\}$ Partial traces of length n + 1 :

$$\boldsymbol{\Sigma}_{\tau}^{n+1} = \{ \sigma s s' \mid \sigma s \in \boldsymbol{\Sigma}_{\tau}^n \land \langle s, s' \rangle \in t \}$$

Collecting semantics of τ : all partial traces of all finite lengths

$$\Sigma_{\tau}^{\overrightarrow{*}} = \bigcup_{n \geqslant 0} \Sigma_{\tau}^{n}$$

Basic Concepts of Abstract Interpretation,

Partial Trace Semantics in Fixpoint Form

For the function $\mathcal{F}_{\tau}^{\overrightarrow{*}}$

$$\begin{aligned} \mathcal{F}_{\tau}^{\overrightarrow{*}}(X) &= \{s \mid s \in \Sigma\} \cup \{\sigma s s' \mid \sigma s \in X \land \langle s, s' \rangle \in t\} \\ \Sigma_{\tau}^{\overrightarrow{*}} \text{ is the least fixpoint of } \mathcal{F}_{\tau}^{\overrightarrow{*}}, \text{ that is} \\ \blacktriangleright \ \mathcal{F}_{\tau}^{\overrightarrow{*}}(\Sigma_{\tau}^{\overrightarrow{*}}) &= \Sigma_{\tau}^{\overrightarrow{*}} \\ \blacktriangleright \text{ For all X such that } \mathcal{F}_{\tau}^{\overrightarrow{*}}(X) &= X, \ \Sigma_{\tau}^{\overrightarrow{*}} \subseteq X \\ \end{aligned}$$
Therefore,
$$\Sigma_{\tau}^{\overrightarrow{*}} &= \mathtt{lfp} \ \mathcal{F}_{\tau}^{\overrightarrow{*}} &= \bigcup \ \mathcal{F}_{\tau}^{\overrightarrow{*}n}(\varphi) \end{aligned}$$

$$\mathcal{F}^{*}_{\tau} = \mathtt{lfp} \, \mathcal{F}^{*}_{\tau} = \bigcup_{n \geqslant 0} \mathcal{F}^{*}_{\tau} \quad (\phi)$$

Partial Trace Semantics in Fixpoint Form - Proof I

$$\begin{split} \mathfrak{F}_{\tau}^{\overrightarrow{\star}}(\Sigma_{\tau}^{\overrightarrow{\star}}) &= \Sigma_{\tau}^{\overrightarrow{\star}} \\ \text{The proof is as follows:} \end{split}$$

$$\begin{split} \mathcal{F}_{\tau}^{\overrightarrow{*}}(\Sigma_{\tau}^{\overrightarrow{*}}) &= \mathcal{F}_{\tau}^{\overrightarrow{*}}(\bigcup_{n \geqslant 0} \Sigma_{\tau}^{n}) & \text{def.} \Sigma_{\tau}^{\overrightarrow{*}} \\ &= \{s \mid s \in \Sigma\} \cup \{\sigma s s' \mid \sigma s \in (\bigcup_{n \geqslant 0} \Sigma_{\tau}^{n}) \land \langle s, s' \rangle \in t\} & \text{def.} \ \mathcal{F}_{\tau}^{\overrightarrow{*}} \\ &= \{s \mid s \in \Sigma\} \cup \bigcup_{n \geqslant 0} \{\sigma s s' \mid \sigma s \in (\Sigma_{\tau}^{n}) \land \langle s, s' \rangle \in t\} & \text{set theory} \\ &= \Sigma_{\tau}^{1} \cup \bigcup_{n \geqslant 0} \Sigma_{\tau}^{n+1} & \text{def.} \ \Sigma_{\tau}^{1} \text{ and} \ \Sigma_{\tau}^{n+1} \\ &= \bigcup_{n' \geqslant 1} \Sigma_{\tau}^{n'} = \bigcup_{n \geqslant 0} \Sigma_{\tau}^{n} \\ \text{by letting } n' = n + 1 \text{ and since } \Sigma_{\tau}^{n} = \varphi \end{split}$$



Partial Trace Semantics in Fixpoint Form - Proof II

For all X such that $\mathcal{F}_{\tau}^{\overrightarrow{*}}(X) = X$, $\Sigma_{\tau}^{\overrightarrow{*}} \subseteq X$ We prove by induction that $\forall n \ge 0 : \Sigma_{\tau}^n \subseteq X$

- 1. Base Case : $\Sigma^0_{\tau} = \varphi \subseteq X$
- 2. Inductive Hypothesis : $\Sigma_{\tau}^{n} \subseteq X$ Since $\sigma s \in \Sigma_{\tau}^{n} \to \sigma s \in X$, $\{\sigma ss' \mid \sigma s \in \Sigma_{\tau}^{n} \land \langle s, s' \rangle \in t\} \subseteq \{\sigma ss' \mid \sigma s \in X \land \langle s, s' \rangle \in t\}$ Therefore,

$$\Sigma^{n+1}_{\tau} \subseteq \mathfrak{F}^{\overrightarrow{\ast}}_{\tau}(\Sigma^{n}_{\tau}) \subseteq \mathfrak{F}^{\overrightarrow{\ast}}_{\tau}(X) = X$$

The Reflexive Transitive Closure Semantics as an Abstraction

Abstraction of the partial trace semantics

 $\alpha^*(X) = \{ \overrightarrow{\alpha}(\sigma) \mid \sigma \in X \} \qquad \text{where } \overrightarrow{\alpha}(s_0s_1 \dots s_n) = \langle s_0, s_n \rangle$

 $\alpha^*(\Sigma_\tau^{\overrightarrow{\star}})$ is the reflexive transitive closure t^* of the transition relation t.

Concretization

$$\begin{split} \gamma^*(Y) &= \{ \sigma \mid \overrightarrow{\alpha}(\sigma) \in Y \} = \{ s_0 s_1 \dots s_n \mid \langle s_0, s_n \rangle \in Y \} \\ X &\subseteq \gamma^*(\alpha^*(X)) \end{split}$$

Answering Concrete Questions in the Abstract

Answering concrete question about X using a simpler abstract question on $\alpha^*(X)$. Example : $s \dots s' \dots s'' \in X$? $\rightarrow \langle s, s'' \rangle \in \alpha^*(X)$?

Galois Connections

Given any set X of partial traces and Y of pair of states,

$$\alpha^*(X)\subseteq Y \Longleftrightarrow X\subseteq \gamma^*(Y)$$

which is a characteristic property of Galois connections. Proof.

$$\begin{split} \alpha^{*}(X) &\subseteq Y \Longleftrightarrow \{ \overrightarrow{\alpha}^{*}(\sigma) \mid \sigma \in X \} \subseteq Y & \text{def. } \alpha^{*} \\ & \Longleftrightarrow \forall \sigma \in X : \overrightarrow{\alpha}(\sigma) \in Y \\ & \Longleftrightarrow X \subseteq \{ \sigma \mid \overrightarrow{\alpha}(\sigma) \in Y \} & \text{def. } \subseteq \\ & \Longleftrightarrow X \subseteq \gamma^{*}(Y) & \text{def. } \gamma^{*} \end{split}$$

Galois Connections

Galois connections preserve joins.

$$\alpha^*(\bigcup_{i\in I} X_i) = \bigcup_{i\in I} \alpha^*(X_i)$$

Proof.

$$\begin{split} \alpha^*(\bigcup_{i\in I} X_i) &= \{\overrightarrow{\alpha}^*(\sigma) \mid \sigma \in \bigcup_{i\in I} X_i\} \\ &= \bigcup_{i\in I} \{\overrightarrow{\alpha}^*(\sigma) \mid \sigma \in X_i\} \\ &= \bigcup_{i\in I} \alpha^*(X_i) \end{split}$$

The Reflexive Transitive Closure Semantics in Fixpoint Form

- * General Principle in Abstract Interpretation.
 - 1. The concrete(partial trace) semantics is expressed in fixpoint form.

$$\Sigma_{\tau}^{\overrightarrow{*}} = \texttt{lfp}\, \mathfrak{F}_{\tau}^{\overrightarrow{*}}$$

2. The abstract(reflexive transitive closure) semantics is an abstraction of the concrete semantics by a Galois connections and it can be expressed in fixpoint form, too.

$$\alpha^*(\Sigma_{\tau}^{\overrightarrow{*}}) = \operatorname{lfp} \mathcal{F}_{\tau}^*$$

3. 2 can be generalized to order theory, and is known as the fixpoint transfer theorem.

The Reflexive Transitive Closure Semantics in Fixpoint Form - Propositions & Definitions

1. Proposition 1.
$$\alpha^{*}(\phi) = \phi$$

 $\phi \subseteq \gamma^{*}(\phi) \iff \alpha^{*}(\phi) \subseteq \phi$. Therefore $\alpha^{*}(\phi) = \phi$.
2. Propostion 2.
Commutation Property: $\alpha^{*}(\mathcal{F}_{\tau}^{\overrightarrow{*}}(X)) = \mathcal{F}_{\tau}^{*}(\alpha^{*}(X))$
2.1 Definition 1. $\mathbb{I}_{\Sigma} = \{\langle s, s \rangle \mid s \in \Sigma\}$
2.2 Definition 2. $\mathcal{F}_{\tau}^{*}(Y) = \mathbb{I}_{\Sigma} \cup Y \circ t$
 $\alpha^{*}(\mathcal{F}_{\tau}^{\overrightarrow{*}}(X))$
 $= \alpha^{*}(\{s \mid s \in \Sigma\} \cup \{\sigma s s' \mid \sigma s \in X \land \langle s, s' \rangle \in t\})$ def. $\mathcal{F}_{\tau}^{\overrightarrow{*}}$
 $= \{\overrightarrow{\alpha}(s) \mid s \in \Sigma\} \cup \{\overrightarrow{\alpha}(\sigma s s') \mid \sigma s \in X \land \langle s, s' \rangle \in t\})$ def. α^{*}
 $= \{\langle s, s \rangle \mid s \in \Sigma\} \cup \{\langle \sigma_{0}, s' \rangle \mid \exists s : \sigma s \in X \land \langle s, s' \rangle \in t\})$ def. $\overrightarrow{\alpha}$
 $= \mathbb{I}_{\Sigma} \cup \{\langle \sigma_{0}, s' \rangle \mid \exists s : \langle \sigma_{0}, s \rangle \in \alpha^{*}(X) \land \langle s, s' \rangle \in t\})$ def. $\mathbb{I}_{\Sigma}, \alpha^{*}$
 $= \mathbb{I}_{\Sigma} \cup \alpha^{*}(X) \circ t$
 $= \mathcal{F}_{\tau}^{*}(\alpha^{*}(X))$

The Reflexive Transitive Closure Semantics in Fixpoint Form - Proof

Showing

$$\alpha^*(\Sigma_{\tau}^{\overrightarrow{*}}) = \mathtt{lfp}\, \mathfrak{F}_{\tau}^*$$

is equivalent to prove that

$$\alpha^*(\bigcup_{n \geqslant 0} \mathcal{F}_{\tau}^{\overrightarrow{*}^n}(\varphi)) = \bigcup_{n \geqslant 0} \mathcal{F}_{\tau}^{*n}(\varphi)$$

Using induction on

$$\forall \mathfrak{n} : \alpha^*(\mathfrak{F}_{\tau}^{\overrightarrow{*}^n}(\varphi)) = \mathfrak{F}_{\tau}^{*n}(\varphi)$$

Basic Concepts of Abstract Interpretation,

The Reflexive Transitive Closure Semantics in Fixpoint Form - Proof

$$\forall n : \alpha^* (\mathfrak{F}_{\tau}^{\overrightarrow{*}^n}(\varphi)) = \mathfrak{F}_{\tau}^{*n}(\varphi)$$

1. Base Case: $\alpha^*(\mathcal{F}_{\tau}^{\overrightarrow{*}0}(\varphi)) = \varphi = \mathcal{F}_{\tau}^{*0}(\varphi)$ $\xrightarrow{\rightarrow} n$

2. Inductive Hypothesis: $\alpha^*(\mathfrak{F}_{\tau}^{\overrightarrow{*}^n}(\varphi)) = \mathfrak{F}_{\tau}^{*n}(\varphi)$

$$\begin{split} \alpha^*(\mathcal{F}_{\tau}^{\overrightarrow{\ast}\,n+1}(\varphi)) &= \alpha^*(\mathcal{F}_{\tau}^{\overrightarrow{\ast}\,n}(\mathcal{F}_{\tau}^{\overrightarrow{\ast}\,n}(\varphi))) \\ &= \mathcal{F}_{\tau}^*(\alpha^*(\mathcal{F}_{\tau}^{\overrightarrow{\ast}\,n}(\varphi))) \qquad \text{commutative} \\ &= \mathcal{F}_{\tau}^*\mathcal{F}_{\tau}^{*\,n}(\varphi) \qquad \text{inductive hypothesis} \\ &= \mathcal{F}_{\tau}^{*\,n+1}(\varphi) \end{split}$$

The Reachability Semantics as an Abstraction

The reachability semantics of the transition system $\tau = \langle \Sigma, \Sigma_i, t \rangle$

$$\{s' \mid \exists s \in \Sigma_{i} : \langle s, s' \rangle \in t^*\}$$

is the set of states that are reachable from the initial states Σ_i .

The Reachability Semantics as an Abstraction

Definition post[r]Z: The right-image of the set Z by relation r

$$post[r]Z = \{s' \mid \exists s \in Z : \langle s, s' \rangle \in r\}$$

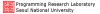
The Reachability Semantics as an Abstraction

Abstraction of the reflexive transitive closure semantics Y is defined as

$$\alpha^{\bullet}(Y) = \{s' \mid \exists s \in \Sigma_{i} : \langle s, s' \rangle \in Y\}$$
$$= post[Y]\Sigma_{i}$$

Concretization of the reachability semantics Z is defined as

$$\gamma^{\bullet}(Z) = \{ \langle s, s' \rangle \mid s \in \Sigma_{i} \Longrightarrow s' \in Z \}$$



Galois Connection

We have the Galois Connection:

$$\alpha^{\bullet}(Y)\subseteq Z \Longleftrightarrow Y\subseteq \gamma^{\bullet}(Z)$$

Proof.

$$\begin{split} \alpha^{\bullet}(Y) &\subseteq \mathsf{Z} \Longleftrightarrow \{s' \mid \exists s \in \Sigma_i : \langle s, s' \rangle \in Y\} \subseteq \mathsf{Z} & \text{def. } \alpha^{\bullet} \\ & \iff \forall s' : \forall s \in \Sigma_i : \langle s, s' \rangle \in Y \Longrightarrow s' \in \mathsf{Z} & \text{def. } \subseteq \\ & \iff \forall \langle s, s' \rangle \in Y : s \in \Sigma_i \Longrightarrow s' \in \mathsf{Z}\} & \text{def. } \Longrightarrow \\ & \iff Y \subseteq \{ \langle s, s' \rangle \mid s \in \Sigma_i \Longrightarrow s' \in \mathsf{Z}\} & \text{def. } \subseteq \\ & \iff Y \subseteq \gamma^{\bullet}(\mathsf{Z}) & \text{def. } \varphi^{\bullet} \end{split}$$

The Reachability Semantics in fixpoint form

- 1. Define $\mathfrak{F}^{\bullet}_{\tau}(Z) = \Sigma_{\mathfrak{i}} \cup post[t]Z.$
- 2. Establish commutation property $\alpha^{\bullet}(\mathfrak{F}^{*}_{\tau}(Y))=\alpha^{\bullet}(\mathfrak{F}^{\bullet}_{\tau}(Y))$

$$\begin{split} &\alpha^{\bullet}(\mathcal{F}^{*}_{\tau}(Y)) \\ = &\{s' \mid \exists s \in \Sigma_{i} : \langle s, s' \rangle \in (\mathbb{I}_{\Sigma} \cup Y \circ t)\} & \text{def. } \alpha^{\bullet} \& \mathcal{F}^{*}_{\tau} \\ = &\{s' \mid \exists s \in \Sigma_{i} : s' = s\} \cup \\ &\{s' \mid \exists s \in \Sigma_{i} : \exists s'' : \langle s, s'' \rangle \in Y \land \langle s'', s' \rangle \in t\} & \text{def. } \mathbb{I}_{\Sigma} \& \circ \\ = &\Sigma_{i} \cup \{s' \mid \exists s'' \in \alpha^{\bullet}(Y) \land \langle s'', s' \rangle \in t\} & \text{def. } \alpha^{\bullet} \\ = &\alpha^{\bullet}(\mathcal{F}^{\bullet}_{\tau}(Y)) & \text{def. } \mathcal{F}^{\bullet}_{\tau}(Z) \end{split}$$

3. By the fixpoint transfer theorem,

$$\alpha^{\bullet}(t^*) = \alpha^{\bullet}(\operatorname{lfp} \mathfrak{F}^*_{\tau}) = \operatorname{lfp} \mathfrak{F}^{\bullet}_{\tau}$$

Basic Concepts of Abstract Interpretation,

The Interval Semantics as an Abstraction

The set of states of a transiton system $\tau = \langle \Sigma, \Sigma_i, t \rangle$ is totally ordered $\langle \Sigma, < \rangle$ with extrema $-\infty$ and $+\infty$, the interval semantics $\alpha^H(\alpha^\bullet(t^*))$ of τ provides bounds on its reachable states $\alpha^\bullet(t*)$:

$$\alpha^{H}(Z) = [\min Z, \max Z]$$

$$\min(\phi) = \infty$$
 $\max(\phi) = -\infty$

Concretization:

$$\gamma^{\mathsf{H}}([\mathfrak{l},\mathfrak{h}]) = \{ s \in \Sigma \mid \mathfrak{l} \leqslant s \leqslant \mathfrak{h} \}$$

Abstract implication:

$$[l,h] \sqsubseteq [l',h'] \Longleftrightarrow (l' \leqslant l \land h \leqslant h')$$

Galois Connection

We have the Galois Connection:

$$\alpha^{H}(Z) \sqsubseteq [l,h] \Longleftrightarrow Z \subseteq \gamma^{H}([l,h])$$

Proof.

$$\begin{split} \alpha^{H}(Z) &\sqsubseteq [\mathfrak{l},\mathfrak{h}] \Longleftrightarrow [\min Z,\max Z] \sqsubseteq [\mathfrak{l},\mathfrak{h}] & \text{def. } \alpha^{H} \\ \Leftrightarrow \mathfrak{l} &\leqslant \min Z \wedge \max Z \leqslant \mathfrak{h} & \text{def. } \sqsubseteq \\ &\Leftrightarrow Z \subseteq \{s \in \Sigma \mid \mathfrak{l} \leqslant s \leqslant \mathfrak{h}\} & \text{def. min}\&\max \\ &\Leftrightarrow Z \subseteq \gamma^{H}([\mathfrak{l},\mathfrak{h}]) & \text{def. } \gamma^{H} \end{split}$$

By defining

$$\bigsqcup_{i \in I} [l_i, h_i] = [\min_{i \in I} l_i, \max_{i \in I} h_i]$$

, Galois connection preserves least upper bounds

$$\alpha^{\mathsf{H}}(\bigcup_{i \in I} \mathsf{Z}_{i}) = \bigsqcup_{i \in I}(\mathsf{Z}_{i})$$

Basic Concepts of Abstract Interpretation,

The Interval Semantics in Fixpoint Form

- 1. Define $[\min \Sigma_i, \max \Sigma_i] \cup \alpha^H \circ post[t] \circ \gamma^H(I) \sqsubseteq \mathcal{F}_{\tau}^H(I)$
- 2. Establish semi-commutation property

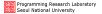
$$\alpha^{\mathsf{H}}(\mathcal{F}^{\bullet}_{\tau}(\mathsf{Z})) \sqsubseteq \mathcal{F}^{\mathsf{H}}_{\tau}(\alpha^{\mathsf{H}}(\mathsf{Z}))$$

$$\begin{split} &\alpha^{H}(\mathfrak{F}^{\bullet}_{\tau}(Z)) = \alpha^{H}(\Sigma_{i} \cup \text{post}[t]Z) & \text{def } \mathfrak{F}^{\bullet}_{\tau} \\ &= \alpha^{H}(\Sigma_{i}) \cup \alpha^{H}(\text{post}[t][Z]) & \text{Galois Connection} \\ &\sqsubseteq [\min \Sigma_{i}, \max \Sigma_{i}] \cup \alpha^{H}(\text{post}[t](\gamma^{H}(\alpha^{H}(Z)))) & \\ &\sqsubseteq \mathfrak{F}^{H}_{\tau}(\alpha^{H}(Z)) \end{split}$$

3. By the fixpoint approximation:

$$\alpha^{H}(\mathfrak{F}^{\bullet}_{\tau}(t^{*})) = \alpha^{H}(\texttt{lfp}\,\mathfrak{F}^{\bullet}_{\tau}) \sqsubseteq \texttt{lfp}\,\mathfrak{F}^{H}_{\tau}$$

Basic Concepts of Abstract Interpretation,



Convergence Acceleration

In general, $\mathtt{lfp} \mathfrak{F}_{\tau}^{H} = \bigsqcup_{n \ge 0} \mathfrak{F}_{\tau}^{H}(\varphi = [+\infty, -\infty])$ diverge. Example, the transition system

$$\langle \mathbb{Z}, \{0\}, \{\langle \mathbf{x}, \mathbf{x}' \rangle \mid \mathbf{x}' = \mathbf{x} + 1\}
angle$$

of program x := 0; while true do x := x + 1.

 $\mathfrak{F}^H_\tau([\mathfrak{l},\mathfrak{h}]) = [0,0] \cup [\mathfrak{l}+1,\mathfrak{h}+1]$

It diverges: $[+\infty, -\infty]$, [0, 0], [0, 1], [0, 2], ...

Widening

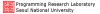
To accelerate convergence, introduce a widening \bigtriangledown such that,

$$(X \sqsubseteq X \bigtriangledown Y) \land (Y \sqsubseteq X \bigtriangledown Y)$$

$$\begin{split} I^{0} &= \varphi = [+\infty, -\infty] \\ I^{n+1} &= I^{n} \\ &= I^{n} \bigtriangledown \mathcal{F}_{\tau}^{\mathsf{H}}(I^{n}) \end{split} \qquad \text{if } \mathcal{F}_{\tau}^{\mathsf{H}}(I^{n}) \sqsubseteq I^{n} \\ &\text{otherwise.} \end{split}$$

limit I^λ is finite($\lambda\in\mathbb{N})$ and is a fixpoint overapproximation

$${\tt lfp}\, {\mathfrak F}^{\sf H}_\tau \sqsubseteq I^\lambda$$



Example of Widening

An example of interval widening

1. choosing finite sequence

$$-\infty = r_0 < r_1 < \cdots < r_k = +\infty$$

2.

$$\begin{split} [+\infty,-\infty] \bigtriangledown [l,h] &= [l,h] \\ [l,h] \bigtriangledown [l',h'] &= [\text{if } l > l' \text{ then } max\{r_i | r_i \leqslant l'\} \text{ else } l, \\ & \text{if } h < h' \text{ then } min\{r_i | h' \leqslant r_i\} \text{ else } h] \end{split}$$



Example of Widening

Example, the transition system

$$\langle \mathbb{Z}, \{0\}, \{\langle \mathbf{x}, \mathbf{x}'
angle \mid \mathbf{x}' = \mathbf{x} + 1\}
angle$$

of program x := 0; while x < 100 do x := x + 1.

 $\mathfrak{F}^{H}_{\tau}([l,h]) = [0,0] \cup [l+1, min(99,h) + 1]$

1. Sequence
$$r=-\infty<-1<0<1<\infty$$
 2.

$$\begin{split} I^0 &= [+\infty, -\infty] \\ I^1 &= [0, 0] \sqcup [1, 1] = [0, 1] \\ I^2 &= [0, 1] \sqcup [0, 2] = [0, +\infty] \\ I^3 &= [0, +\infty] \end{split}$$

Narrowing

The limit of an iteration with widening can be improved by a narrowing $\bigtriangleup,$ such that

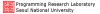
$$X\sqsubseteq Y\Longrightarrow X\sqsubseteq (X\bigtriangleup Y)\sqsubseteq Y$$

All terms in the iterates with narrowing

$$\begin{split} J^0 &= I^\lambda \\ J^{n+1} &= J^n \bigtriangleup \mathfrak{F}^H_\tau(J^0) \end{split}$$

improve the result obtained by widening.

$$\mathtt{lfp}\, \mathfrak{F}^{\mathsf{H}}_{\tau} \sqsubseteq J^{\mathfrak{n}} \sqsubseteq I^{\lambda}$$



Example of Narrowing

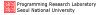
 $[l,h] \triangle [l',h'] = [if \exists i : l = r_i \text{ then } l' \text{ else } l, \text{ if } \exists j : h = r_i \text{ then } h' \text{ else } h]$

Example, the transition system

$$\langle \mathbb{Z}, \{0\}, \{\langle \mathbf{x}, \mathbf{x}' \rangle \mid \mathbf{x}' = \mathbf{x} + 1\}
angle$$

of program x := 0; while x < 100 do x := x + 1.

$$\begin{split} J^0 &= [0, +\infty] \\ J^1 &= [0, +\infty] \bigtriangleup [0, 100] = [0, 100] \\ J^2 &= [0, 100] \bigtriangleup [0, 100] = [0, 100] \end{split}$$



Composition of Abstractions

The design of three abstractions of the partial trace semantics $\Sigma_{\tau}^{\overrightarrow{\star}}$ of a transition system τ was compositional. Composition of Galois connections is a Galois connection so the successive arguments on sound approximation do compose nicely.

$$\alpha^{\mathsf{H}} \circ \alpha^{\bullet} \circ \alpha^{*}$$
, $\gamma^{*} \circ \gamma^{\bullet} \circ \gamma^{\mathsf{H}}$



Hierarchy of Semantics

The four semantics of a transition system $\tau=\langle \Sigma, \Sigma_i, t\rangle$ form a hierarchy

- 1. Partial traces $\Sigma_{\tau}^{\overrightarrow{*}}$
- 2. Reflexive transitive closure $\alpha^*(\Sigma_{\tau}^{\overrightarrow{*}})$
- 3. Reachability $\alpha^{\bullet} \circ \alpha^{*}(\Sigma_{\tau}^{\overrightarrow{*}})$
- 4. Interval semantics $\alpha^{H} \circ \alpha^{\bullet} \circ \alpha^{*}(\Sigma_{\tau}^{\overrightarrow{*}})$



Thanks

Thank you for listening.