michelepasqua.github.io/
michele.pasqua@univr.it

UNIVERSITÀ di VERONA
Dipartimento di INFORMATICA

Principles and Applications of Abstract Interpretation

Program Semantics

Michele Pasqua, PhD

Verona, IT

October 2024

PhD Course @ UniVR 2024/2025

Transition System Semantics

Program execution modeled as discrete transitions between states

- $\mathbb{S} = \mathbb{L} \times \mathbb{M}$ set of states
- $\tau \subseteq \mathbb{S} \times \mathbb{S}$ transition relation

$\mathbb{s} \; \tau \; \mathbb{s}'$ models one step of execution of the language interpreter $\textsc{Exec}[\cdot]$

Program execution modeled as discrete transitions between states

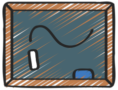
- $\mathbb{S} = \mathbb{L} \times \mathbb{M}$ set of states
- $\tau \subseteq \mathbb{S} \times \mathbb{S}$ transition relation

$$\mathbb{s}\ \tau\ \mathbb{s}' \text{ models one step of execution of the language interpreter } \textsc{Exec}[\cdot]$$

We can individuate:

- a set of initial states $I \subseteq \mathbb{S}$, e.g., $I \triangleq \{\mathtt{0}\} \times \mathbb{M}$
- a set of final states $F \subseteq \mathbb{S}$, e.g., $F \triangleq \{\mathtt{e}\} \times \mathbb{M}$

The transition relation τ is defined by structural induction on programs



Prefix trace semantics $\mathsf{T}_p \triangleq \bigcup_{n\in\mathbb{N}}\{\mathbb{s}_0\mathbb{s}_1\dots\mathbb{s}_n \mid \mathbb{s}_0 \in I \wedge \forall i < n\,.\,\mathbb{s}_i \;\tau\; \mathbb{s}_{i+1}\}$

Prefix trace semantics $\mathsf{T}_p \triangleq \bigcup_{n\in\mathbb{N}}\{\mathbb{s}_0\mathbb{s}_1\ldots\mathbb{s}_n \mid \mathbb{s}_0 \in I \wedge \forall i < n\,.\,\mathbb{s}_i \;\tau\; \mathbb{s}_{i+1}\}$

Other choices

all not computable

- Reachability semantics
- Maximal semantics
- Relational semantics

Prefix trace semantics $\mathsf{T}_p \triangleq \bigcup_{n\in\mathbb{N}}\{\mathbb{s}_0\mathbb{s}_1\ldots\mathbb{s}_n \mid \mathbb{s}_0 \in I \land \forall i < n\,.\,\mathbb{s}_i\ \tau\ \mathbb{s}_{i+1}\}$

Other choices

all not computable

- Reachability semantics
- Maximal semantics
- Relational semantics

We can use abstract interpretation to:

- express all these semantics uniformely as fixpoints
- relate these semantics by abstractions
- choose the best semantics for each class of properties to prove

Finite traces

Finite sequences of elements from $\mathbb{S}$

- ϵ is the empty trace
- $\mathbb{s}$ is a trace of length 1
- $\mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_{n-1}$ is a trace of length n
- $\mathbb{S}^n$ is the set of traces of length n
- $\mathbb{S}^{\leq n} \triangleq \bigcup_{i \leq n} \mathbb{S}^i$ is the set of traces of length at most n
- $\mathbb{S}^* \triangleq \bigcup_{i \leq \mathbb{N}} \mathbb{S}^i$ is the set of all finite traces

Length: $|\mathbb{t}| \in \mathbb{N}$ of a trace $\mathbb{t} \in \mathbb{S}^*$

Concatenation: $\mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n \cdot \mathbb{s}'_0\mathbb{s}'_1 \dots \mathbb{s}'_m \triangleq \mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n\mathbb{s}'_0\mathbb{s}'_1 \dots \mathbb{s}'_m$

Junction: $\mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n \frown \mathbb{s}'_0\mathbb{s}'_1 \dots \mathbb{s}_m \triangleq \mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n\mathbb{s}'_1 \dots \mathbb{s}'_m$ when $\mathbb{s}_n = \mathbb{s}'_0$, undefined otherwise

Length: $|\mathbb{t}| \in \mathbb{N}$ of a trace $\mathbb{t} \in \mathbb{S}^*$

Concatenation: $\mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n \cdot \mathbb{s}'_0\mathbb{s}'_1 \dots \mathbb{s}'_m \triangleq \mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n\mathbb{s}'_0\mathbb{s}'_1 \dots \mathbb{s}'_m$

Junction: $\mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n \frown \mathbb{s}'_0\mathbb{s}'_1 \dots \mathbb{s}_m \triangleq \mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n\mathbb{s}'_1 \dots \mathbb{s}'_m$ when $\mathbb{s}_n = \mathbb{s}'_0$, undefined otherwise

Extension to sets of traces

- $X \cdot Y \triangleq \{\mathbb{t} \cdot \mathbb{t}' \mid \mathbb{t} \in X \wedge \mathbb{t}' \in Y\}$
- $X \frown Y \triangleq \{\mathbb{t} \frown \mathbb{t}' \mid \mathbb{t} \in X \wedge \mathbb{t}' \in Y \wedge \mathbb{t} \frown \mathbb{t}' \text{ defined}\}$

Operations on traces

Length: $|\mathbb{t}| \in \mathbb{N}$ of a trace $\mathbb{t} \in \mathbb{S}^*$

Concatenation: $\mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n \cdot \mathbb{s}'_0\mathbb{s}'_1 \dots \mathbb{s}'_m \triangleq \mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n\mathbb{s}'_0\mathbb{s}'_1 \dots \mathbb{s}'_m$

Junction: $\mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n \frown \mathbb{s}'_0\mathbb{s}'_1 \dots \mathbb{s}_m \triangleq \mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n\mathbb{s}'_1 \dots \mathbb{s}'_m$ when $\mathbb{s}_n = \mathbb{s}'_0$, undefined otherwise

Extension to sets of traces

- $X \cdot Y \triangleq \{\mathbb{t} \cdot \mathbb{t}' \mid \mathbb{t} \in X \wedge \mathbb{t}' \in Y\}$
- $X \frown Y \triangleq \{\mathbb{t} \frown \mathbb{t}' \mid \mathbb{t} \in X \wedge \mathbb{t}' \in Y \wedge \mathbb{t} \frown \mathbb{t}' \text{ defined}\}$

$$\begin{aligned} X^0 &\triangleq \{\epsilon\} \\ X^{n+1} &\triangleq X \cdot X^n \\ X^* &\triangleq \bigcup_{n\in\mathbb{N}} X^n \end{aligned} \qquad\qquad \begin{aligned} X^{\frown 0} &\triangleq \mathbb{S} \\ X^{\frown n+1} &\triangleq X \frown X^{\frown n} \\ X^{\frown *} &\triangleq \bigcup_{n\in\mathbb{N}} X^{\frown n} \end{aligned}$$

Semantics Abstraction

Prefix trace semantics

$$\mathsf{T}_p \triangleq \bigcup_{n\in\mathbb{N}} \{ \mathbb{s}_0 \mathbb{s}_1 \dots \mathbb{s}_n \mid \mathbb{s}_0 \in I \wedge \forall i < n \,.\, \mathbb{s}_i \;\tau\; \mathbb{s}_{i+1} \} = \bigcup_{n\in\mathbb{N}} I \frown (\tau^{\frown n})$$

$$\mathsf{T}_p \triangleq \bigcup_{n\in\mathbb{N}} \{\mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n \mid \mathbb{s}_0 \in I \wedge \forall i < n \,.\, \mathbb{s}_i \;\tau\; \mathbb{s}_{i+1}\} = \bigcup_{n\in\mathbb{N}} I \frown (\tau^{\frown n})$$

The prefix trace semantics can be expressed in fixpoint form:

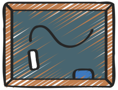
$$\mathsf{T}_p = \mathsf{lfp}^{\subseteq}\, \mathsf{f}_p \text{ where } \mathsf{f}_p \triangleq \lambda X \,.\, I \cup X \frown \tau$$

$$\mathsf{T}_p \triangleq \bigcup_{n\in\mathbb{N}} \{\mathbb{s}_0\mathbb{s}_1 \dots \mathbb{s}_n \mid \mathbb{s}_0 \in I \wedge \forall i < n \,.\, \mathbb{s}_i \;\tau\; \mathbb{s}_{i+1}\} = \bigcup_{n\in\mathbb{N}} I \frown (\tau^{\frown n})$$

The prefix trace semantics can be expressed in fixpoint form:

$$\mathsf{T}_p = \mathsf{lfp}^{\subseteq}\, \mathsf{f}_p \text{ where } \mathsf{f}_p \triangleq \lambda X \,.\, I \cup X \frown \tau$$

f_p is Scott-continuous on the complete lattice $\langle \wp(\mathbb{S}^*), \subseteq, \cup, \cap, \emptyset, \mathbb{S}^* \rangle$



Prefix partial order $\preceq \subseteq \mathbb{S}^* \times \mathbb{S}^*$

$$\mathbb{t} \preceq \mathbb{t}'' \triangleq \exists \mathbb{t}' \in \mathbb{S}^* . \mathbb{t} \cdot \mathbb{t}' = \mathbb{t}''$$

Prefix closure

Prefix partial order $\preceq \subseteq \mathbb{S}^* \times \mathbb{S}^*$

$$\mathbb{t} \preceq \mathbb{t}'' \triangleq \exists \mathbb{t}' \in \mathbb{S}^* \,.\, \mathbb{t} \cdot \mathbb{t}' = \mathbb{t}''$$

Prefix closure $\eta^{\preceq} : \wp(\mathbb{S}^*) \to \wp(\mathbb{S}^*)$

$$\eta^{\preceq} \triangleq \lambda X \,.\, \{\mathbb{t} \in \mathbb{S}^* \mid \exists \mathbb{t}' \in X \,.\, \mathbb{t} \preceq \mathbb{t}'\}$$

Prefix partial order $\preceq \subseteq \mathbb{S}^* \times \mathbb{S}^*$

$$\mathbb{t} \preceq \mathbb{t}'' \triangleq \exists \mathbb{t}' \in \mathbb{S}^* . \mathbb{t} \cdot \mathbb{t}' = \mathbb{t}''$$

Prefix closure $\eta^{\preceq} : \wp(\mathbb{S}^*) \to \wp(\mathbb{S}^*)$

$$\eta^{\preceq} \triangleq \lambda X . \{\mathbb{t} \in \mathbb{S}^* \mid \exists \mathbb{t}' \in X . \mathbb{t} \preceq \mathbb{t}'\}$$

The prefix trace semantics is closed by prefixes: $\eta^{\preceq}(\mathrm{T}_p) = \mathrm{T}_p$

- Good for safety properties but not for liveness properties (e.g., termination)

Forward state operator $\text{post}_\tau : \wp(\mathbb{S}) \to \wp(\mathbb{S})$

$$\text{post}_\tau \triangleq \lambda X \,.\, \{\mathbb{s}' \mid \exists \mathbb{s} \in \mathbb{S} \,.\, \mathbb{s} \;\tau\; \mathbb{s}'\}$$

Forward state operator $\text{post}_\tau : \wp(\mathbb{S}) \to \wp(\mathbb{S})$

$$\text{post}_\tau \triangleq \lambda X \,.\, \{\mathbb{s}' \mid \exists \mathbb{s} \in \mathbb{S} \,.\, \mathbb{s} \;\tau\; \mathbb{s}'\}$$

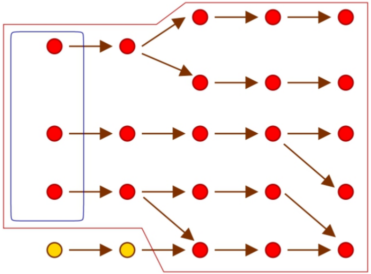
States reachable from I in the transition system

$$\mathsf{R} \triangleq \{\mathbb{s}_n \mid \exists \mathbb{s}_0 \ldots \mathbb{s}_n \in \mathbb{S}^* \,.\, \mathbb{s}_0 \in I \wedge \forall i < n \,.\, \mathbb{s}_i \;\tau\; \mathbb{s}_{i+1}\} = \bigcup_{n \in \mathbb{N}} \text{post}_r^n(I)$$

The reachable state semantics can expressed in fixpoint form:

$$\mathsf{R} = \text{lfp}^{\subseteq}\, \mathsf{f}_r \text{ where } \mathsf{f}_r \triangleq \lambda X \,.\, I \cup \text{post}_\tau(X)$$

f_r is Scott-continuous on the complete lattice $\langle \wp(\mathbb{S}), \subseteq, \cup, \cap, \emptyset, \mathbb{S} \rangle$



Abstract the trace semantics into the reachable state semantics

- Collect the final state of partial executions

Abstract the trace semantics into the reachable state semantics

- Collect the final state of partial executions

Abstraction $\alpha_r \triangleq \lambda X \,.\, \{\mathbb{s} \mid \exists \mathbb{s}_0 \dots \mathbb{s}_n \in X \,.\, \mathbb{s} = \mathbb{s}_n\}$

Concretization $\gamma_r \triangleq \lambda X \,.\, \{\mathbb{s}_0 \dots \mathbb{s}_n \mid \mathbb{s}_n \in X\}$

We have a Galois Insertion

$$\langle \wp(\mathbb{S}^*), \subseteq \rangle \underset{\alpha_r}{\overset{\gamma_r}{\leftrightarrows}} \langle \wp(\mathbb{S}), \subseteq \rangle$$

We can abstract semantics operators and their least fixpoints

- $\mathrm{T}_p = \mathrm{lfp}^{\subseteq}\, \mathrm{f}_p$ where $\mathrm{f}_p \triangleq \lambda X \,.\, I \cup X \frown \tau$
- $\mathrm{R} = \mathrm{lfp}^{\subseteq}\, \mathrm{f}_r$ where $\mathrm{f}_r \triangleq \lambda X \,.\, I \cup \mathrm{post}_\tau(X)$
- $\langle \wp(\mathbb{S}^*), \subseteq \rangle \underset{\alpha_r}{\overset{\gamma_r}{\leftrightarrows}} \langle \wp(\mathbb{S}), \subseteq \rangle$

We can abstract semantics operators and their least fixpoints

- $\mathsf{T}_p = \mathsf{lfp}^{\subseteq}\, \mathsf{f}_p$ where $\mathsf{f}_p \triangleq \lambda X\,.\, I \cup X \frown \tau$
- $\mathsf{R} = \mathsf{lfp}^{\subseteq}\, \mathsf{f}_r$ where $\mathsf{f}_r \triangleq \lambda X\,.\, I \cup \mathsf{post}_\tau(X)$
- $\langle \wp(\mathbb{S}^*), \subseteq \rangle \underset{\alpha_r}{\overset{\gamma_r}{\leftrightarrows}} \langle \wp(\mathbb{S}), \subseteq \rangle$

We have that $\alpha_r \circ \mathsf{f}_p = \mathsf{f}_r \circ \alpha_p$

By fixpoint transfer we get $\alpha_r(\mathsf{T}_p) = \mathsf{R}$

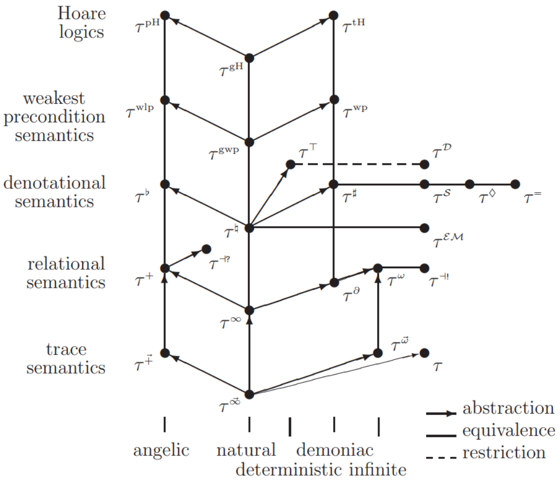
(proof) $\alpha_r \circ \mathrm{f}_p = \mathrm{f}_r \circ \alpha_p$

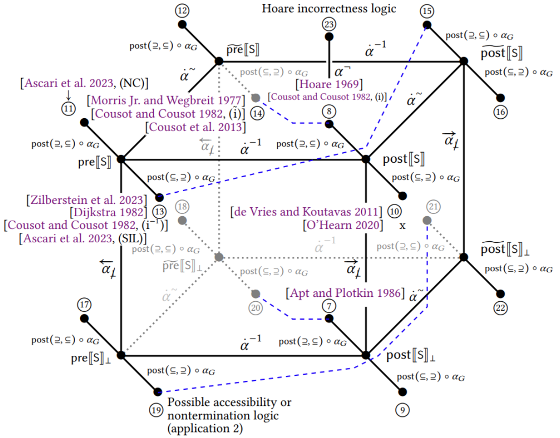
$$
\begin{aligned}
(\alpha_r \circ \mathrm{f}_p)(X) &= \\
&= \alpha_r(I \cup X \frown \tau) \\
&= \{\mathbb{s} \mid \exists \mathbb{s}_0 \ldots \mathbb{s}_n \in I \cup X \frown \tau \,.\, \mathbb{s} = \mathbb{s}_n\} \\
&= I \cup \{\mathbb{s} \mid \exists \mathbb{s}_0 \ldots \mathbb{s}_n \in X \frown \tau \,.\, \mathbb{s} = \mathbb{s}_n\} \\
&= I \cup \{\mathbb{s} \mid \exists \mathbb{s}_0 \ldots \mathbb{s}_n \in X \,.\, \mathbb{s}_n \ \tau \ \mathbb{s}\} \\
&= I \cup \mathrm{post}_\tau(\{\mathbb{s} \mid \exists \mathbb{s}_0 \ldots \mathbb{s}_n \in X \,.\, \mathbb{s} = \mathbb{s}_n\}) \\
&= I \cup \mathrm{post}_\tau(\alpha_r(X)) \\
&= (\mathrm{f}_r \circ \alpha_r)(X)
\end{aligned}
$$

Relations between semantics

R	reachable states	$\langle \wp(\mathbb{S}), \subseteq \rangle$
$\alpha_r \uparrow$		
T_p	prefix finite traces	$\langle \wp(\mathbb{S}^*), \subseteq \rangle$
$\alpha_I \uparrow$		
T	partial finite traces	$\langle \wp(\mathbb{S}^*), \subseteq \rangle$
$\alpha_* \uparrow$		
T_∞	partial traces	$\langle \wp(\mathbb{S}^\infty), \sqsubseteq \rangle$
$\alpha_\leq \uparrow$		
M	maximal traces	$\langle \wp(\mathbb{S}^\infty), \sqsubseteq \rangle$

Hierarchy of semantics





Galois connection (different logics to prove the same property)

© P. Cousot

Thanks for the attention!

LaTeX is the way

UNIVERSITÀ di VERONA
Dipartimento di INFORMATICA

Additional Slides

Further reading

C-TCS-2002 “Constructive Design of a Hierarchy of Semantics of a Transition System by Abstract Interpretation”, P. Cousot, In: *Theoretical Computer Science* (2002)

C-POPL-2024 “Calculational Design of [In]Correctness Transformational Program Logics by Abstract Interpretation”, P. Cousot, In: *Proc. of ACM Principles of Programming Languages* (2024)