A Few Remarks on the Abstraction and Equivalence of Semantics

P. Cousot
DMI - École Normale Supérieure
45 rue d’Ulm, 75230 Paris cedex 05, France

cousot@mi.ens.fr
http://www.dmi.ens.fr/cousot

Objective

- Assume that we are given any transition system:
  \[ \langle S, t \rangle \]
  state space \( \rightarrow \) transition relation

- We first define all semantics of this given transition system in the hierarchy of semantics as abstractions of the natural trace semantics;
- We then constructively derive fixpoint characterizations of all semantics in the hierarchy by abstraction of a fixpoint characterization of the natural trace semantics of the transition system.

The Hierarchy of Semantics

Description of the hierarchy of semantics as abstractions of the natural trace semantics
**NATURAL TRACE SEMANTICS**

- The system/program we are interested in is assumed to be specified by a transition system:
  \[ \langle S, t \rangle \]
  - state space \( S \)
  - transition relation \( t \)

- Its natural trace semantics is:

\[
\mathcal{T}^\parallel = \begin{cases}
\{ \bullet \rightarrow \bullet \rightarrow \cdots \rightarrow \bullet \rightarrow \bullet \text{ blocking} \} & \to \text{finite traces} \\
\cup \{ \bullet \rightarrow \bullet \rightarrow \cdots \rightarrow \bullet \rightarrow \bullet \} & \to \text{infinite traces}
\end{cases}
\]

\[
\downarrow \quad \downarrow 
\]

\[
\text{any state} \quad \text{transition}
\]

**RELATIONAL SEMANTICS**

\[ \alpha \in \text{Traces} \mapsto \varphi(S \times S_\perp), \quad S_\perp = S \cup \{ \perp \} \]

\[ \mathcal{R} = \alpha(\mathcal{T}) \]

\[ \begin{array}{cccccc}
& a & b & a \\
\{ \bullet, \bullet \} & \bullet \rightarrow \bullet \rightarrow \cdots \rightarrow \bullet \rightarrow \bullet \in \mathcal{T} \\
a & a \\
\cup \{ \bullet, \perp \} & \bullet \rightarrow \bullet \rightarrow \cdots \rightarrow \bullet \rightarrow \bullet \rightarrow \cdots \in \mathcal{T}
\end{array} \]

\[ \alpha \] is a Galois connection.

---

**NATURAL, DEMONIAC & ANGELIC SEMANTICS**

- Natural trace semantics: \( \mathcal{T}^\parallel \);

- Angelic abstraction \( ^\wedge \):
  \[ \alpha(\mathcal{T}^\parallel) = \{ \bullet \rightarrow \bullet \rightarrow \cdots \rightarrow \bullet \rightarrow \bullet \mid \bullet \rightarrow \bullet \rightarrow \cdots \rightarrow \bullet \rightarrow \bullet \in \mathcal{T}^\parallel \}; \]

- Demoniac abstraction \( ^\vee \):
  \[ \alpha(\mathcal{T}^\parallel) = \mathcal{T}^\parallel \cup \{ \bullet \rightarrow \bullet \rightarrow \cdots \rightarrow \bullet \rightarrow \bullet \mid \bullet \rightarrow \bullet \rightarrow \cdots \rightarrow \bullet \rightarrow \bullet \rightarrow \cdots \in \mathcal{T}^\parallel \}. \]

The \( \alpha \)'s are Galois connections.

---

**NON-DETERMINISTIC DENOTATIONAL SEMANTICS**

\[ \alpha \in \varphi(S \times S_\perp) \mapsto (S \mapsto \varphi(S_\perp)) \]

\[ \mathcal{D} = \alpha(\mathcal{R}) \]

\[ \begin{array}{cccccc}
& a & b & a \\
\lambda s \{ s' \in S_\perp \mid \langle s, s' \rangle \in \mathcal{R} \} & \text{right image}
\end{array} \]

\[ \alpha \] is a Galois isomorphism.
**Predicate Transformer Semantics**

\[ \alpha \in (\mathcal{S} \mapsto \varphi(\mathcal{S}_\perp)) \mapsto (\varphi(\mathcal{S}_\perp) \mapsto \varphi(\mathcal{S})) \]

\[ \mathcal{W} = \alpha(\mathcal{D}) \]

\[ = \lambda Q \{ s \in \mathcal{S} \mid \forall s' \in \mathcal{S}_\perp : s' \in \mathcal{D}(s) \Rightarrow s' \in Q \} \]

\( \alpha \) is a Galois injection.

---

**Axiomatic Semantics**

\[ \alpha \in (\varphi(\mathcal{S}) \mapsto \varphi(\mathcal{S}_\perp)) \mapsto \varphi(\varphi(\mathcal{S}) \times \varphi(\mathcal{S}_\perp)) \]

\[ \mathcal{H} = \alpha(\mathcal{W}) \]

\[ = \{ \langle P, Q \rangle \mid P \subseteq \mathcal{W}(Q) \} \]

\( \alpha \) is a Galois injection.

---

**Fixpoint presentation of the semantics in the hierarchy**

---

**Fixpoint presentation of a semantics**

- Fixpoint presentations of a semantic:

  \[
  \begin{array}{c}
  \mathcal{T} = \text{Izf} \sqsubseteq \mathcal{F} \\
  \Rightarrow \quad \text{semantics} \quad \text{monotonic transformer}
  \end{array}
  \]

- \textbf{Problem}: find a fixpoint characterization of all semantics in the hierarchy.
The known fixpoint characterizations look similar; So there should be a simple way of transferring/lifting fixpoint definitions through abstractions $\alpha$ (as we do in abstract interpretation [CC77]);

I failed for some time and will explain some of the crucial steps to have this idea work properly.

---

**References**


---

**Difficulty 1: Orderings**

- Because "natural" semantics describe both finite and infinite behaviors simultaneously, we cannot use lfp for $\subseteq$. But we could use gfp $\subseteq$;  
- Unfortunately the abstraction of the gfp $\subseteq$ fixpoint semantics for natural traces does not lead to Scott’s denotational semantics;  
- So we resort to two orderings:
  1. $\subseteq$ (approximation, refinement, logical implication, …) for Galois connections $\alpha$;  
  2. $\sqsubseteq$ (computational ordering) for fixpoints.

---

**Natural Trace Fixpoint Semantics**

Let $X$ and $Y$ be sets of complete traces:

- $X \subseteq Y$, refinement  
- $X \sqsubseteq Y$, computational ordering

\[
\begin{align*}
X^+ &\triangleq X^+ \subseteq Y^+ \land X^\omega \supseteq Y^\omega \\
X^+ &\triangleq \text{the finite traces of } X \\
X^\omega &\triangleq \text{the infinite traces of } X \\
\mathcal{T} &\triangleq \text{lfp} \subseteq \mathcal{F} \\
\mathcal{F} &\triangleq \sqsubseteq \mathcal{T} \cup \{X\}
\end{align*}
\]

traces of length 1 ending in blocking states  
traces of $X$ prefixed by an initial transition

---

**Difficulty 2: The Computational Ordering**

- There is only one approximation ordering;  
- There are many possible computational orderings;  
- Theorem (very rough sketch) lfp $\subseteq \mathcal{F} = \text{lfp} \subseteq' \mathcal{F}$ iff when ordering the transfinite iterates of $\mathcal{F}$ from $\perp$ by $\sqsubseteq$ and $\sqsubseteq'$, the respective lubs will lead to the same limit.

More precisely …
**Fixpoint Iterates Reordering**

- Let \( \langle D, \subseteq, \bot, \sqcup \rangle, F \) be a fixpoint semantic specification;
- Let \( E \) be a set and \( \preceq \) be a binary relation on \( E \), such that:
  1. \( \preceq \) is a pre-order on \( E \);
  2. all iterates \( F^\delta, \delta \in \| \) of \( F \) belong to \( E \);
  3. \( \bot \) is the \( \preceq \)-infimum of \( E \);
  4. the restriction \( F|_E \) of \( F \) to \( E \) is \( \preceq \)-monotone;
  5. for all \( x \in E \), if \( \lambda \) is a limit ordinal and \( \forall \delta < \lambda : F^\delta \preceq x \) then \( \bigcup_{\delta < \lambda} F^\delta \preceq x \).

- Then \( \text{lf}_{\preceq} F \subseteq \text{lf}_{\preceq} F|_E \in E \).

**Possible Demoniac Iterate Orderings**

\[
\begin{align*}
\{a, b\} & \quad \{a\} \\
\{a\} & \quad \emptyset \\
\{a, b, \bot\} & \quad \{a, b\} \\
\{a, b, \bot\} & \quad \{a\}
\end{align*}
\]

Demoniac ordering \( \sqsubseteq^\# \)  
Demoniac ordering \( \sqsubseteq^\circ \)

\[
\begin{align*}
\{a\} & \quad \{b\} \\
\{a\} & \quad \{a, b\} \\
\{a, b, \bot\} & \quad \{a, b\} \\
\{a, b, \bot\} & \quad \{a\}
\end{align*}
\]

Smyth ordering \( \sqsubseteq^\triangledown \)  
Flat ordering \( \sqsubseteq^\flat \)

**Orderings for the Nondeterministic Denotational Semantics, \( S = \{a, b\} \)**

\[
\begin{align*}
\{a, b\} & \quad \{a, b\} \\
\{a\} & \quad \{a\} \\
\{a, b, \bot\} & \quad \{a, b, \bot\} \\
\{a, b, \bot\} & \quad \{a, b, \bot\} \\
\emptyset & \quad \emptyset \\
\{a, \bot\} & \quad \{a, \bot\} \\
\{b, \bot\} & \quad \{b, \bot\} \\
\{\bot\} & \quad \{\bot\}
\end{align*}
\]

Computational ordering \( \sqsubseteq \)  
Egli-Milner ordering \( \sqsubseteq^{\text{EM}} \)

\[\text{possibly iterates of } \mathcal{F}\]

**Difficulty 3: Fixpoint transfer**

- Fixpoint transfer/lifting theorems based upon:
  - Kleene def. of fixpoints
  - Tarski
- May not be applicable;

- However, fixpoint transfer/lifting may work by parts.
**Kleene Fixpoint Transfer Theorem**

If \( \langle D, F \rangle \) and \( \langle D^\#, F^\# \rangle \) are semantic specifications and
\[
\alpha(\bot) = \bot^#
\]
\[
F^\# \circ \alpha = \alpha \circ F
\]
\[
\forall \sqsubseteq\text{-increasing chains } X_K, K \in \Delta : \alpha(\bigsqcup_{K \in \Delta} X_K) = \bigsqcup_{K \in \Delta} \alpha(X_K)
\]
then
\[
\alpha(\text{lfp} \sqsubseteq F) = \text{lfp} \sqsubseteq^# F^#
\]

**Note 1:** The condition \( F^\# \circ \alpha = \alpha \circ F \) provides guidelines for designing \( F^\# \) when knowing \( F \) and \( \alpha \).

**Note 2:** \( F^\# \) convergence is faster than that of \( F \).

---

**Tarski Fixpoint Transfer Theorem**

If \( \langle \mathcal{D}, \sqsubseteq, \bot, \top \rangle \) and \( \langle \mathcal{D}^\#, \sqsubseteq^#, \bot^#, \top^# \rangle \) are complete lattices,
\( F \in \mathcal{D} \rightarrow \mathcal{D} \), \( F^\# \in \mathcal{D}^\# \rightarrow \mathcal{D}^\# \) are monotonic and

- \( \alpha \) is a complete \( \sqsubseteq \)-morphism
- \( F^\# \circ \alpha \sqsubseteq^# \alpha \circ F \)
- \( \forall y \in \mathcal{D}^# : F^#(y) \sqsubseteq^# y \Rightarrow \exists x \in \mathcal{D} : \alpha(x) = y \land F(x) \sqsubseteq^# x \)

then
\[
\alpha(\text{lfp} \sqsubseteq F) = \text{lfp} \sqsubseteq^# F^#
\]

---

**Example: Traces to Relation Abstraction**

- Problem for \( \alpha \in \text{Traces} \rightarrow \text{Relation} \):
  - \( \alpha \) is continuous for \( \subseteq \)
  - \( \alpha \) is not continuous for \( \sqsubseteq \):
    - \( \Rightarrow \) Kleene fixpoint transfer not applicable,
    - \( \Rightarrow \) But applicable to finite traces;
  - \( \alpha \) is not a complete \( \sqsubseteq \)-morphism (because not complete \( \sqsubseteq \)-morphism):
    - \( \Rightarrow \) Tarski fixpoint transfer not applicable,
    - \( \Rightarrow \) But applicable to infinite traces (since \( \alpha \) is a complete \( \sqsubseteq \)-morphism);
- Solution: split, transfer by parts, combine.

---

**Difficulty 4: Predicate transformer transformer**

- For the predicate transformer semantics, the fixpoint characterization has the form:
  \[
  \mathcal{W} = \text{lfp} \sqsubseteq \mathcal{F} \uparrow \quad \uparrow
  \]
  predicate transformer  predicate transformer
• Use the further abstraction:

\[ \alpha_Q \subseteq (\varphi(S) \mapsto \varphi(S)) \mapsto \varphi(S) \]

\[ \alpha_Q(W) = \mathcal{W}(Q) \]

which consists in fixing the postcondition \( Q \subseteq S \) to get Dijkstra’s fixpoint:

\[ \mathcal{W} = \lambda Q \cdot \text{lfp} \subseteq \mathcal{F}(Q) \]

\[ \uparrow \]

\[ \text{predicate transformer} \]

\[ \uparrow \]

\[ \text{predicate transformer} \]

**Example 1: Predicate Transformers**

\[ (S \mapsto \varphi(S)) \mapsto \alpha \mapsto (\varphi(S) \mapsto \varphi(S)) \]

+ \( \alpha \) surjective

\[ \Rightarrow \]

\[ (S \mapsto \varphi(S)) \mapsto \alpha \mapsto (\varphi(S) \mapsto \varphi(S)) \]

**Example 2: Hoare Logics**

\[ \text{Predicate transformer} \quad \text{Hoare logic} \]

\[ (\varphi(S) \mapsto \varphi(S)) \mapsto \alpha \mapsto \varphi(\varphi(S) \times \varphi(S)) \]

+ \( \alpha \) surjective

\[ \Rightarrow \]

\[ (\varphi(S) \mapsto \varphi(S)) \mapsto \alpha \mapsto \varphi(S) \otimes \varphi(S) \]

**Exercise:** what is \( \otimes \)?
• Tensor product:

\[ \langle D, \Box \rangle \otimes \langle D^\mathbb{Z}, \Box^\mathbb{Z} \rangle \triangleq \{ H \in \wp(D \times D^\mathbb{Z}) \mid (1) \land (2) \land (3) \} \]

where the conditions are:

1. \( (X \subseteq X' \land \langle X', Y' \rangle \in H \land Y' \subseteq Y) \Rightarrow (\langle X, Y \rangle \in H) \)

   (consequence rule of Hoare logic)

2. \( (\forall i \in \Delta : \langle X_i, Y \rangle \in H) \Rightarrow (\bigcup_{i \in \Delta} X_i, Y \in H) \)

3. \( (\forall i \in \Delta : \langle X, Y_i \rangle \in H) \Rightarrow (\bigcap_{i \in \Delta} X, Y_i \in H) \)

   (by induction on the program structure, 2 and 3 follow from Hoare logic rules).

---

**DIFFICULTY 6: FROM FIXPOINT TO PROOF RULE SEMANTICS**

1) For safety/invariance, use Park induction (\( F \) monotonic on complete lattice):

\[ \exists I: F(I) \subseteq I \land I \subseteq P \]

---

**Galois Connection Commutative Diagram**

\[ \langle \langle D, \Box \rangle, \langle D^\mathbb{Z}, \Box^\mathbb{Z} \rangle \rangle \]

2) For inevitability/liveness, use Scott induction? No (\( F \) monotonic on cpo):

\[ \exists I \in \wp(\Sigma) : I \subseteq F(\bigcup_{\beta \leq \delta} I^\beta) \land P \subseteq I^\epsilon \]
**CONCLUSION**

- Synthetic and uniformizing (although somewhat contemplative) work;
- Shows that abstract interpretation formalizes semantics abstraction nicely;
- Help to compare abstract interpretation based program analysis methods;
- Help to understand their limitations (e.g. denotational semantics + $\subseteq = \subseteq \Rightarrow$ failure for binding time analysis + strictness analysis);

---

**RESEARCH WORK**

- Extend the hierarchy to other semantics of transition systems;
- Extend to a programming calculus with interpretations at all levels in the hierarchy;
- Extend at higher-order to the $\lambda$-calculus\(^*\).

---

**REFERENCE**

For technical details and references, see:


---

\(^*\) The original text should be "but is it really worth looking at?"