# BASIC CONCEPTS OF ABSTRACT INTERPRETATION

Patrick Cousot
*École Normale Supérieure*
*45 rue d'Ulm*
*75230 Paris cedex 05, France*
Patrick.Cousot@ens.fr

Radhia Cousot
*CNRS & École Polytechnique*
*91128 Palaiseau cedex, France*
Radhia.Cousot@polytechnique.fr

**Abstract** A brief introduction to the theory of Abstract Interpretation, examplified by constructing a hierarchy of partial traces, reflexive transitive closure, reachable states and intervals abstract semantics of transition systems.

**Keywords:** Abstract Interpretation, Safety, Specification, Static Analysis, Verification.

## 1. Introduction

Abstract Interpretation [Cousot, 1978] is a theory of approximation of mathematical structures, in particular those involved in the semantic models of computer systems. Abstract interpretation can be applied to the systematic construction of methods and effective algorithms to approximate undecidable or very complex problems in computer science such that the semantics, the proof, the static analysis, the verification, the safety and the security of software or hardware computer systems. In particular, static analysis by abstract interpretation, which automatically infers dynamic properties of computer systems, has been very successful these last years to automatically verify complex properties of real-time, safety-critical embedded systems.

All applications presented in the WCC 2004 topical day on Abstract Interpretation compute an overapproximation of the program reachable states. Hence, we consisely develop the elementary example of reachability static analysis [Cousot and Cousot, 1977]. We limit the necessary mathematical concepts to naïve set theory. A more complete presentation is [Cousot, 2000a] while [Cousot, 1981; Cousot and Cousot, 1992b] can be recommended as first readings and [Cousot and Cousot, 1992a] for a basic exposition to the theory.

## 2. Transition systems

Programs are often formalized as graphs or transition systems $\tau = \langle \Sigma, \Sigma_i, t \rangle$ where $\Sigma$ is a set of states, $\Sigma_i \subseteq \Sigma$ is the set of initial states and $t \subseteq \Sigma \times \Sigma$ is a transition relation between a state and its possible successors [Cousot, 1978; Cousot, 1981]. For example the program `x := 0; while x < 100 do x := x + 1` can be formalized as $\langle \mathbb{Z}, \{0\}, \{\langle x, x' \rangle \mid x < 100 \wedge x' = x + 1\} \rangle$ where $\mathbb{Z}$ is the set of integers.

## 3. Partial trace semantics

A finite partial execution trace $s_0 s_1 \ldots s_n$ starts from any state $s_0 \in \Sigma$ and then moves on through transitions from one state $s_i$, $i < n$, to a possible successor $s_{i+1}$ such that $\langle s_i, s_{i+1} \rangle \in t$. The set of all such finite partial execution traces will be called the *collecting semantics* $\vec{\Sigma^*_\tau}$ of the transition system in that it is the strongest program property of interest (in this paper).

There is no partial trace of length 0 so the set $\Sigma^0_\tau$ of partial traces of length 0 is simply the empty set $\emptyset$. A partial trace of length 1 is $s$ where $s \in \Sigma$ is any state. So the set $\Sigma^1_\tau$ of partial traces of length 1 is simply $\{s \mid s \in \Sigma\}$. By recurrence, a trace of length $n+1$ is the concatenation $\sigma s s'$ of a trace $\sigma s$ of length $n$ with a partial trace $s'$ of length 1 such that the pair $\langle s, s' \rangle \in t$ is a possible state transition. So if $\Sigma^n_\tau$ is the set of partial traces of length $n$ then $\Sigma^{n+1}_\tau = \{\sigma s s' \mid \sigma s \in \Sigma^n_\tau \wedge \langle s, s' \rangle \in t\}$. Then the collecting semantics of $\tau$ is the set $\vec{\Sigma^*_\tau} = \bigcup_{n \geq 0} \Sigma^n_\tau$ of all partial traces of all finite lengths.

## 4. Partial trace semantics in fixpoint form

Observe that $\Sigma^1_\tau \cup \Sigma^{n+1}_\tau = \vec{\mathcal{F}^*_\tau}(\Sigma^n_\tau)$ where:

$$\vec{\mathcal{F}^*_\tau}(X) \quad = \quad \{s \mid s \in \Sigma\} \cup \{\sigma s s' \mid \sigma s \in X \wedge \langle s, s' \rangle \in t\}$$

so that $\vec{\Sigma^*_\tau}$ is a *fixpoint* of $\vec{\mathcal{F}^*_\tau}$ in that $\vec{\mathcal{F}^*_\tau}(\vec{\Sigma^*_\tau}) = \vec{\Sigma^*_\tau}$ [Cousot and Cousot, 1979]. The proof is as follows:

$$\begin{aligned}
& \vec{\mathcal{F}^*_\tau}(\vec{\Sigma^*_\tau}) \quad = \quad \vec{\mathcal{F}^*_\tau}\Big(\bigcup_{n \geq 0} \Sigma^n_\tau\Big) && \text{〈by def. } \vec{\Sigma^*_\tau}\text{〉} \\
= \; & \{s \mid s \in \Sigma\} \cup \{\sigma s s' \mid \sigma s \in \Big(\bigcup_{n \geq 0} \Sigma^n_\tau\Big) \wedge \langle s, s' \rangle \in t\} && \text{〈def. } \vec{\mathcal{F}^*_\tau}\text{〉} \\
= \; & \{s \mid s \in \Sigma\} \cup \bigcup_{n \geq 0} \{\sigma s s' \mid \sigma s \in \Sigma^n_\tau \wedge \langle s, s' \rangle \in t\} && \text{〈set theory〉} \\
= \; & \Sigma^1_\tau \cup \bigcup_{n \geq 0} \Sigma^{n+1}_\tau && \text{〈by def. } \Sigma^1_\tau \text{ and } \Sigma^{n+1}_\tau\text{〉} \\
= \; & \bigcup_{n' \geq 1} \Sigma^{n'}_\tau \quad = \quad \bigcup_{n \geq 0} \Sigma^n_\tau && \text{〈by letting } n' = n+1 \text{ and since } \Sigma^n_\tau = \emptyset\text{.〉}
\end{aligned}$$

Now assume that $\vec{\mathcal{F}^*_\tau}(X) = X$ is another fixpoint of $\vec{\mathcal{F}^*_\tau}$. We prove by recurrence that $\forall n \geq 0 : \Sigma^n_\tau \subseteq X$. Obviously $\Sigma^0_\tau = \emptyset \subseteq X$. $\Sigma^1_\tau = \{s \mid s \in \Sigma\} \subseteq \vec{\mathcal{F}^*_\tau}(X) = X$. Assume by recurrence hypothesis that $\Sigma^n_\tau \subseteq X$. Then $\sigma s \in \Sigma^n_\tau$ implies $\sigma s \in X$ so $\{\sigma s s' \mid \sigma s \in \Sigma^n_\tau \wedge \langle s,\ s'\rangle \in t\} \subseteq \{\sigma s s' \mid \sigma s \in X \wedge \langle s,\ s'\rangle \in t\}$ whence $\Sigma^{n+1}_\tau \subseteq \vec{\mathcal{F}^*_\tau}(\Sigma^n_\tau) \subseteq \vec{\mathcal{F}^*_\tau}(X) = X$. By recurrence $\forall n \geq 0 : \Sigma^n_\tau \subseteq X$ whence $\Sigma^{\vec{*}}_\tau$ is the *least fixpoint* of $\vec{\mathcal{F}^*_\tau}$, written:

$$\Sigma^{\vec{*}}_\tau \quad = \quad \mathrm{lfp}^{\subseteq}_{\emptyset}\, \vec{\mathcal{F}^*_\tau} \quad = \quad \bigcup_{n\geq 0} \vec{\mathcal{F}^*_\tau}^{\,n}(\emptyset)$$

where $f^0(x) = x$ and $f^{n+1}(x) = f(f^n(x))$ are the *iterates* of $f$.

## 5. The reflexive transitive closure as an abstraction of the partial trace semantics

Partial execution traces are too precise to express program properties that do not relate to intermediate computation steps. Considering initial and final states only is an abstraction:

$$\alpha^*(X) \quad = \quad \{\vec{\alpha}(\sigma) \mid \sigma \in X\} \quad \text{where} \quad \vec{\alpha}(s_0 s_1 \ldots s_n) \quad = \quad \langle s_0,\ s_n\rangle\ .$$

Observe that $\alpha^*(\Sigma^{\vec{*}}_\tau)$ is the reflexive transitive closure $t^*$ of the transition relation $t$ viz. the set of pair $\langle s,\ s'\rangle$ such that there is a finite path in the graph $\tau = \langle \Sigma,\ \Sigma_i,\ t\rangle$ from vertex $s$ to vertex $s'$ through arcs of $t$: $\langle x,\ y\rangle \in t^*$ if and only if $\exists s_0, \ldots, s_n \in \Sigma : x = s_0 \wedge \ldots \wedge \langle s_i,\ s_{i+1}\rangle \in t \wedge \ldots \wedge s_n = y$.

Now if $Y$ is a set of pairs of initial and final states, it describes a set of partial traces where the intermediate states are unkown :

$$\gamma^*(Y) \quad = \quad \{\sigma \mid \vec{\alpha}(\sigma) \in Y\} \quad = \quad \{s_0 s_1 \ldots s_n \mid \langle s_0,\ s_n\rangle \in Y\}$$

So if $X$ is a set of partial traces, it is approximated from above by $\alpha^*(X)$ in the sense that $X \subseteq \gamma^*(\alpha^*(X))$.

## 6. Answering concrete questions in the abstract

To answer concrete questions about $X$ one may sometimes answer it using a simpler abstract question on $\alpha^*(X)$. For example the concrete question "Is there a partial trace in X which has $s$, $s'$ and $s''$ as initial, intermediate and final states?" can be replaced by the abstract question "Is there a pair $\langle s,\ s''\rangle$ in $\alpha^*(X)$?". If there is no such a pair in $\alpha^*(X)$ then there is no such a partial trace in $\gamma^*(\alpha^*(X))$ whence none in $X$ since $X \subseteq \gamma^*(\alpha^*(X))$. However if there is such a pair in $\alpha^*(X)$ then we cannot conclude that there is such a trace in $X$ since this trace might be in $\gamma^*(\alpha^*(X))$ but not in $X$. The abstract answer must always be sound but may sometimes be incomplete. However if the concrete question is "Is there a partial trace in X which has respectively $s$ and $s'$ as initial and final states?" then the abstract answer is sound and complete.

## 7. Galois connections

Given any set $X$ of partial traces and $Y$ of pair of states, we have :

$$\begin{aligned}
& \alpha^*(X) \subseteq Y \iff \{\vec{\alpha}(\sigma) \mid \sigma \in X\} \subseteq Y && \wr\text{by def. } \alpha^*\wr \\
\iff & \forall \sigma \in X : \vec{\alpha}(\sigma) \in Y \iff X \subseteq \{\sigma \mid \vec{\alpha}(\sigma) \in Y\} && \wr\text{by def. } \subseteq\wr \\
\iff & X \subseteq \gamma^*(Y) && \wr\text{by def. } \gamma^*\wr
\end{aligned}$$

So $\alpha^*(X) \subseteq Y$ if and only if $X \subseteq \gamma^*(Y)$, which is a characteristic property of *Galois connections*. Galois connections *preserve joins* in that $\alpha^*(\bigcup_{i\in\Delta} X_i) = \{\vec{\alpha}(\sigma) \mid \sigma \in \bigcup_{i\in\Delta} X_i\} = \bigcup_{i\in\Delta}\{\vec{\alpha}(\sigma) \mid \sigma \in X_i\} = \bigcup_{i\in\Delta} \alpha^*(X_i)$. Equivalent formalizations involve Moore families, closure operators, etc [Cousot, 1978; Cousot and Cousot, 1979].

## 8. The reflexive transitive closure semantics in fixpoint form

Since the concrete (partial trace) semantics can be expressed in fixpoint form and the abstract (reflexive transitive closure) semantics is an abstraction of the concrete semantics by a Galois connection, we can also express the abstract semantics in fixpoint form. This is a general principle in Abstract Interpretation [Cousot and Cousot, 1979].

We have $\emptyset \subseteq \gamma^*(\emptyset)$ whence $\alpha^*(\emptyset) \subseteq \emptyset$ proving $\alpha^*(\emptyset) = \emptyset$ by antisymmetry.

For all sets $X$ of partial traces, we have the *commutation property*:

$$\begin{aligned}
& \alpha^*(\vec{\mathcal{F}^*_\tau}(X)) \\
= \ & \alpha^*(\{s \mid s \in \Sigma\} \cup \{\sigma s s' \mid \sigma s \in X \wedge \langle s,\, s'\rangle \in t\}) && \wr\text{def. } \vec{\mathcal{F}^*_\tau}\wr \\
= \ & \{\vec{\alpha}(s) \mid s \in \Sigma\} \cup \{\vec{\alpha}(\sigma s s') \mid \sigma s \in X \wedge \langle s,\, s'\rangle \in t\}) && \wr\text{def. } \alpha^*\wr \\
= \ & \{\langle s,\, s\rangle \mid s \in \Sigma\} \cup \{\langle \sigma_0,\, s'\rangle \mid \exists s : \sigma s \in X \wedge \langle s,\, s'\rangle \in t\}) && \wr\text{def. } \vec{\alpha}\wr \\
= \ & \mathbb{1}_\Sigma \cup \{\langle \sigma_0,\, s'\rangle \mid \exists s : \langle \sigma_0,\, s\rangle \in \alpha^*(X) \wedge \langle s,\, s'\rangle \in t\}) \\
& && \wr\text{def. } \mathbb{1}_S = \{\langle x,\, x\rangle \mid x \in S\} \text{ and } \alpha^*\wr \\
= \ & \mathbb{1}_\Sigma \cup \alpha^*(X) \circ t && \wr\text{def. composition } \circ \text{ of relations}\wr \\
= \ & \mathcal{F}^*_\tau(\alpha^*(X)) && \wr\text{by defining } \mathcal{F}^*_\tau(Y) = \mathbb{1}_\Sigma \cup Y \circ t\wr
\end{aligned}$$

If follows, by recurrence, that the iterates $\vec{\mathcal{F}^*_\tau}^{\,n}(\emptyset)$ of $\vec{\mathcal{F}^*_\tau}$ and those $\mathcal{F}^*_\tau{}^n(\emptyset)$ of $\mathcal{F}^*_\tau$ are related by $\alpha^*$. For the basis, $\alpha^*(\vec{\mathcal{F}^*_\tau}^{\,0}(\emptyset)) = \emptyset = \mathcal{F}^*_\tau{}^0(\emptyset)$. For the induction step, if $\alpha^*(\vec{\mathcal{F}^*_\tau}^{\,n}(\emptyset)) = \mathcal{F}^*_\tau{}^n(\emptyset)$ then $\alpha^*(\vec{\mathcal{F}^*_\tau}^{\,n+1}(\emptyset)) = \alpha^*(\vec{\mathcal{F}^*_\tau}(\vec{\mathcal{F}^*_\tau}^{\,n}(\emptyset)))$ $= \mathcal{F}^*_\tau(\alpha^*(\vec{\mathcal{F}^*_\tau}^{\,n}(\emptyset))) = \mathcal{F}^*_\tau(\mathcal{F}^*_\tau{}^n(\emptyset)) = \mathcal{F}^*_\tau{}^{n+1}(\emptyset)$. It follows that $\alpha^*(\vec{\Sigma^*_\tau}) = \alpha^*(\mathrm{lfp}^{\subseteq}_{\emptyset}\, \vec{\mathcal{F}^*_\tau}()) = \alpha^*(\bigcup_{n\geq 0} \vec{\mathcal{F}^*_\tau}^{\,n}(\emptyset)) = \bigcup_{n\geq 0} \alpha^*(\vec{\mathcal{F}^*_\tau}^{\,n}(\emptyset)) = \bigcup_{n\geq 0} \mathcal{F}^*_\tau{}^n(\emptyset) =$

$\mathrm{lfp}^{\subseteq}_{\emptyset}\, \mathcal{F}^*_\tau$. This can be easily generalized to order theory [Cousot, 1978; Cousot and Cousot, 1979] and is known as the *fixpoint transfer* theorem.

Observe that if $\Sigma$ is finite then the fixpoint definition provides an iterative algorithm for computing the reflexive transitive closure of a relation as $X^0 = \emptyset, \ldots, X^{i+1} = \mathcal{F}^*_\tau(X^i), \ldots,$ until $X^{n+1} = X^n = \mathrm{lfp}^{\subseteq}_{\emptyset}\, \mathcal{F}^*_\tau = t^*$.

## 9. The reachability semantics as an abstraction of the reflexive transitive closure semantics

The reachability semantics of the transition system $\tau = \langle \Sigma,\ \Sigma_i,\ t \rangle$ is the set $\{s' \mid \exists s \in \Sigma_i : \langle s, s' \rangle \in t^*\}$ of states which are reachable from the initial states $\Sigma_i$. This is an abstraction $\alpha^\bullet(t^*)$ of the reflexive transtive closure semantics $t^*$ by defining the right-image $\mathrm{post}[r]Z = \{s' \mid \exists s \in Z : \langle s,\ s' \rangle \in r\}$ of the set $Z$ by the relation $r$ and

$$\alpha^\bullet(Y) \quad = \quad \mathrm{post}[Y]\Sigma_i \quad = \quad \{s' \mid \exists s \in \Sigma_i : \langle s,\ s' \rangle \in Y\}\ .$$

Let $\gamma^\bullet(Z) = \{\langle s,\ s' \rangle \mid s \in \Sigma_i \Longrightarrow s' \in Z\}$. We have the Galois connection:

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

## 10. The reachability semantics in fixpoint form

To establish the commutation property, we prove that

$$\begin{aligned}
&\alpha^\bullet(\mathcal{F}^*_\tau(Y))\\
=\ &\{s' \mid \exists s \in \Sigma_i : \langle s,\ s' \rangle \in (\mathbb{1}_\Sigma \cup Y \circ t)\} && \text{(by def. } \alpha^\bullet \text{ \& } \mathcal{F}^*_\tau\text{)}\\
=\ &\{s' \mid \exists s \in \Sigma_i : s' = s\} \cup \{s' \mid \exists s \in \Sigma_i : \exists s'' : \langle s,\ s'' \rangle \in Y \wedge \langle s'',\ s' \rangle \in t)\}\\
& && \text{(by def. } \mathbb{1}_\Sigma \text{ \& function composition } \circ\text{)}\\
=\ &\Sigma_i \cup \{s' \mid \exists s'' \in \alpha^\bullet(Y) \wedge \langle s'',\ s' \rangle \in t)\} && \text{(by def. } \alpha^\bullet\text{)}\\
=\ &\mathcal{F}^\bullet_\tau(\alpha^\bullet(Y)) && \text{(by defining } \mathcal{F}^\bullet_\tau(Z) = \Sigma_i \cup \mathrm{post}[t]Z\text{.)}
\end{aligned}$$

By the fixpoint transfer theorem, it follows that $\alpha^\bullet(t^*) = \alpha^\bullet(\mathrm{lfp}^{\subseteq}_{\emptyset}\, \mathcal{F}^*_\tau) = \mathrm{lfp}^{\subseteq}_{\emptyset}\, \mathcal{F}^\bullet_\tau$.

Observe that if $\Sigma$ is finite, we have a forward reachability iterative algorithm (since $\mathrm{lfp}^{\subseteq}_{\emptyset}\, \mathcal{F}^\bullet_\tau = \bigcup_{n \geq 0} {\mathcal{F}^\bullet_\tau}^n(\emptyset)$) which can be used to check e.g. that all reachable states satisfy a given safety specification $S$: $\alpha^\bullet(t^*) \subseteq S \iff \forall n : {\mathcal{F}^\bullet_\tau}^n(\emptyset) \subseteq S$.

## 11. The interval semantics as an abstraction of the reachability semantics

In case the set of states of a transition system $\tau = \langle \Sigma, \Sigma_i, t \rangle$ is totally ordered $\langle \Sigma, < \rangle$ with extrema $-\infty$ and $+\infty$[1], the interval semantics $\alpha^{\vdash}(\alpha^{\bullet}(t^*))$ of $\tau$ provides bounds on its reachable states $\alpha^{\bullet}(t^*)$:

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

where $\min Z$ ($\max Z$) is the infimum (resp. supremum) of the set $Z$ and $\min \emptyset = +\infty$ (resp. $\max \emptyset = -\infty$). All empty intervals $[\ell, h]$ with $h < \ell$ are identified to $[+\infty, -\infty]$. By defining the concretization $\gamma^{\vdash}([\ell, h]) = \{s \in \Sigma \mid \ell \leq s \leq h\}$, we can define the abstract implication $[\ell, h] \sqsubseteq [\ell', h']$ as $\gamma^{\vdash}([\ell, h]) \subseteq \gamma^{\vdash}([\ell', h'])$ or equivalently $(\ell' \leq \ell \wedge h \leq h')$. We have a Galois connection:

$$\begin{array}{lr}
\alpha^{\vdash}(Z) \sqsubseteq [\ell, h] \iff [\min Z, \max Z] \sqsubseteq [\ell, h] & \wr \text{def. } \alpha^{\vdash} \wr \\
\iff \ell \leq \min Z \wedge \max Z \leq h & \wr \text{def. } \sqsubseteq \wr \\
\iff Z \subseteq \{s \in \Sigma \mid \ell \leq s \leq h\} & \wr \text{def. min \& max} \wr \\
\iff Z \subseteq \gamma^{\vdash}([\ell, h]) & \wr \text{def. } \gamma^{\vdash} \wr
\end{array}$$

By defining $\bigsqcup_{i \in \Delta} [\ell_i, h_i] = [\min_{i \in \Delta} \ell_i, \max_{i \in \Delta} h_i]$, the characteristic property that Galois connections preserves least upper bounds is now $\alpha^{\vdash}(\bigcup_{i \in \Delta} Z_i) = \bigsqcup_{i \in \Delta} \alpha^{\vdash}(Z_i)$.

## 12. The interval semantics in fixpoint form

Obviously, $\alpha^{\vdash}(\emptyset) = [+\infty, -\infty]$. Moreover:

$$\begin{array}{lr}
\alpha^{\vdash}(\mathcal{F}^{\bullet}_{\tau}(Z)) \quad = \quad \alpha^{\vdash}(\Sigma_i \cup \mathrm{post}[t]Z) & \wr \text{def. } \mathcal{F}^{\bullet}_{\tau} \wr \\
= \quad \alpha^{\vdash}(\Sigma_i) \sqcup \alpha^{\vdash}(\mathrm{post}[t]Z) & \wr \text{Galois connection} \wr \\
\sqsubseteq \quad [\min \Sigma_i, \max \Sigma_i] \sqcup \alpha^{\vdash}(\mathrm{post}[t](\gamma^{\vdash}(\alpha^{\vdash}(Z)))) & \wr \text{def. } \alpha^{\vdash} \text{ and since } Z \subseteq \gamma^{\vdash}(\alpha^{\vdash}(Z)) \text{ so } \mathrm{post}[t]Z \subseteq \mathrm{post}[t](\gamma^{\vdash}(\alpha^{\vdash}(Z))) \text{ whence } \alpha^{\vdash}(\mathrm{post}[t]Z) \sqsubseteq \alpha^{\vdash}(\mathrm{post}[t](\gamma^{\vdash}(\alpha^{\vdash}(Z)))) \wr \\
\sqsubseteq \quad \mathcal{F}^{\vdash}_{\tau}(\alpha^{\vdash}(Z)) & \wr \text{by defining } \mathcal{F}^{\vdash}_{\tau} \text{ such that } [\min \Sigma_i, \max \Sigma_i] \sqcup \alpha^{\vdash} \circ \mathrm{post}[t] \circ \gamma^{\vdash}(I) \sqsubseteq \mathcal{F}^{\vdash}_{\tau}(I) \wr
\end{array}$$

We only have *semi-commutation* $\alpha^{\vdash}(\mathcal{F}^{\bullet}_{\tau}(Z)) \sqsubseteq \mathcal{F}^{\vdash}_{\tau}(\alpha^{\vdash}(Z))$ hence a *fixpoint approximation* [Cousot and Cousot, 1979]: $\alpha^{\vdash}(\alpha^{\bullet}(t^*)) = \alpha^{\vdash}(\mathrm{lfp}^{\subseteq}_{\emptyset} \mathcal{F}^{\bullet}_{\tau}) \sqsubseteq \mathrm{lfp}^{\sqsubseteq}_{[+\infty, -\infty]} \mathcal{F}^{\vdash}_{\tau}$. So questions $\alpha^{\bullet}(t^*) \subseteq \gamma^{\vdash}(S)$ have sound answers $\mathrm{lfp}^{\sqsubseteq}_{[+\infty, -\infty]} \mathcal{F}^{\vdash}_{\tau} \sqsubseteq S$ in the abstract.

[1] or, more generally, form a complete lattice.

## 13. Convergence acceleration

In general, the iterates $\mathrm{lfp}^{\sqsubseteq}_{[+\infty,-\infty]}\,\mathcal{F}^{\vdash}_{\tau} = \bigsqcup_{n\geq 0}\mathcal{F}^{\vdash\,n}_{\tau}([+\infty,-\infty])$ diverge.

For example for the transition system $\langle \mathbb{Z},\ \{0\},\ \{\langle x,\ x'\rangle \mid x' = x+1\}\rangle$ of program `x := 0; while true do x := x + 1`, we get $\mathcal{F}^{\vdash}_{\tau}([\ell,h]) = [0,0] \sqcup [\ell+1, h+1]$ with diverging iterates $[+\infty,-\infty]$, $[0,0]$, $[0,1]$, $\ldots$, $[0,n]$, $\ldots$ which least upper bound is $[0,+\infty]$.

## 14. Widening

Therefore, to accelerate convergence, we introduce a *widening* $\nabla$ [Cousot and Cousot, 1977] such that $I \sqsubseteq I \nabla J$, $J \sqsubseteq I \nabla J$ and the *iterates with widening* defined as $I^0 = [+\infty,-\infty]$, $I^{n+1} = I^n$ if $\mathcal{F}^{\vdash}_{\tau}(I^n) \sqsubseteq I^n$ while $I^{n+1} = I^n \nabla \mathcal{F}^{\vdash}_{\tau}(I^n)$ otherwise do converge. Then their limit $I^{\lambda}$ is finite ($\lambda \in \mathbb{N}$) and is a *fixpoint overapproximation* $\mathrm{lfp}^{\sqsubseteq}_{[+\infty,-\infty]}\,\mathcal{F}^{\vdash}_{\tau} \sqsubseteq I^{\lambda}$.

An example of interval widening consists in choosing a finite ramp $-\infty = r_0 < r_1 < \ldots < r_k = +\infty$, $k \geq 1$ and $[+\infty,-\infty] \nabla [\ell',h'] = [\ell',h']$ while, otherwise, $[\ell,h] \nabla [\ell',h'] = [\text{if } \ell' < \ell \text{ then } \max\{r_i \mid r_i \leq \ell'\} \text{ else } \ell, \text{if } h' > h \text{ then } \min\{r_i \mid h' \leq r_i\} \text{ else } h]$.

For the transition system $\langle \mathbb{Z},\ \{0\},\ \{\langle x,\ x'\rangle \mid x < 100 \wedge x' = x+1\}\rangle$ of program `x := 0; while x < 100 do x := x + 1` and ramp $-\infty < -1 < 0 < 1 < +\infty$, we have $\mathcal{F}^{\vdash}_{\tau}([\ell,h]) = [0,0] \sqcup [\ell+1, \min(99,h)+1]$ and the iterates with widening $I^0 = [+\infty,-\infty]$, $I^1 = I^0 \nabla \mathcal{F}^{\vdash}_{\tau}(I^0) = \mathcal{F}^{\vdash}_{\tau}(I^0) = [0,0] \sqcup [1,1] = [0,1]$, $I^2 = I^1 \nabla \mathcal{F}^{\vdash}_{\tau}(I^1) = [0,1] \nabla [0,2] = [0,+\infty]$. This is the limit of these iterates with widening since $\mathcal{F}^{\vdash}_{\tau}([0,+\infty]) = [0,100] \sqsubseteq [0,+\infty]$.

## 15. Narrowing

The limit of an iteration with widening can be improved by a *narrowing* $\Delta$ [Cousot and Cousot, 1977] such that $J \sqsubseteq I$ implies $J \sqsubseteq I \Delta J \sqsubseteq I$. All terms in the *iterates with narrowing* $J^0 = I^{\lambda}, \ldots, J^{n+1} = J^n \Delta \mathcal{F}^{\vdash}_{\tau}(J^0)$ improve the result obtained by widening since $\mathrm{lfp}^{\sqsubseteq}_{[+\infty,-\infty]}\,\mathcal{F}^{\vdash}_{\tau} \sqsubseteq J^n \sqsubseteq I^{\lambda}$.

An example of interval narrowing is $[\ell,h] \Delta [\ell',h'] = [\text{if } \exists i : \ell = r_i \text{ then } \ell' \text{ else } \ell, \text{if } \exists j : h = r_j \text{ then } h' \text{ else } h]$.

For the program `x := 0; while x < 100 do x := x + 1`, we have $J^0 = [0,+\infty]$, $J^1 = [0,+\infty] \Delta \mathcal{F}^{\vdash}_{\tau}([0,+\infty]) = [0,+\infty] \Delta [0,100] = [0,100]$ and so $J^n = [0,100]$ for $n \geq 1$ since $\mathcal{F}^{\vdash}_{\tau}([0,100]) = [0,100]$.

## 16. Composition of abstractions

We have defined three abstractions of the partial trace semantics $\Sigma^{\vec{*}}_{\tau}$ of a transition system $\tau$. The design was compositional in that the composition

$\langle \alpha^{\sqsupset} \circ \alpha^{\bullet} \circ \alpha^{*},\ \gamma^{*} \circ \gamma^{\bullet} \circ \gamma^{\sqsupset} \rangle$ of Galois connections is a Galois connection so the successive arguments on sound approximations do compose nicely.

## 17. Hierarchy of semantics

The four semantics of a transition system $\tau = \langle \Sigma,\ \Sigma_i,\ t \rangle$ that we have considered form a hierarchy from the partial traces $\vec{\Sigma^{*}_{\tau}}$, to the reflexive transitive closure $\alpha^{*}(\vec{\Sigma^{*}_{\tau}})$, reachability $\alpha^{\bullet} \circ \alpha^{*}(\vec{\Sigma^{*}_{\tau}})$ and interval semantics $\alpha^{\sqsupset} \circ \alpha^{\bullet} \circ \alpha^{*}(\vec{\Sigma^{*}_{\tau}})$, in abstraction order. The complete range of other possible abstract semantics include all classical ones for programming languages [Cousot, 2002]. By undecidability, none is computable, but effective widening/narrowing iterations can be used to compute approximations (which are more precise than resorting to finite abstractions, as in abstract model checking [Cousot and Cousot, 1992b]). More abstract semantics can answer less questions precisely than more concrete semantics but are cheaper to compute or approximate. This covers all static analysis, including dataflow analysis [Cousot and Cousot, 1979], abstract model checking [Cousot, 2000b], typing [Cousot, 1997], etc. In practice the right balance between precision and cost can lead to precise and efficient abstractions, as for example in *Astrée* [Blanchet et al., 2003].

## References


Blanchet, B., Cousot, P., Cousot, R., Feret, J., Mauborgne, L., Miné, A., Monniaux, D., and Rival, X. (2003). A static analyzer for large safety-critical software. *PLDI'2003*, 196–207, ACM.

Cousot, P. (1978). Méthodes itératives de construction et d'approximation de points fixes d'opérateurs monotones sur un treillis, analyse sémantique de programmes. Thèse d'État ès sciences mathématiques, Grenoble University, 21 March 1978.

Cousot, P. (1981). Semantic foundations of program analysis. In Muchnick, S.S. and Jones, N.D., editors, *Program Flow Analysis: Theory and Applications*, ch. 10, 303–342. Prentice-Hall.

Cousot, P. (1997). Types as abstract interpretations. *24th POPL*, 316–331, ACM.

Cousot, P. (2000a). Abstract interpretation based formal methods and future challenges. *« Informatics — 10 Years Back, 10 Years Ahead »*, LNCS 2000, 138–156, Springer.

Cousot, P. (2000b). Partial completeness of abstract fixpoint checking. *SARA'2000*, LNAI 1864, 1–25, Springer.

Cousot, P. (2002). Constructive design of a hierarchy of semantics of a transition system by abstract interpretation. *Theoret. Comput. Sci.*, 277(1—2):47–103.

Cousot, P. and Cousot, R. (1977). Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. *4th POPL*, 238–252, ACM.

Cousot, P. and Cousot, R. (1979). Systematic design of program analysis frameworks. *6th POPL*, 269–282, ACM.

Cousot, P. and Cousot, R. (1992a). Abstract interpretation frameworks. *J. Logic and Comp.*, 2(4):511–547.

Cousot, P. and Cousot, R. (1992b). Comparing the Galois connection and widening/narrowing approaches to abstract interpretation. *PLILP'92*, LNCS 631, 269–295, Springer.