Parallel Combination of Abstract Interpretation and Model-Based Automatic Analysis of Software

Patrick COUSOT
École Normale Supérieure
DMI, 45, rue d’Ulm
75230 Paris cedex 05
France
cousot@dimi.ens.fr
http://www.ens.fr/~cousot

Radhia COUSOT
CNRS & École Polytechnique
LIX
91440 Palaiseau cedex
France
rcousot@lix.polytechnique.fr
http://lix.polytechnique.fr/~radhia

AAS’97, Paris, January 14, 1997

Combining Model-Checking and Abstract Interpretation

How?

1. Abstract symbolic methods:
   - Use symbolic representations of properties (BDDs, convex polyhedra, ...)
   - One can make approximations (e.g. widenings)
   ⇒ Approximate properties of an exact model

2. Model abstraction:
   - The finite model is an abstraction of the system
   ⇒ Exact properties of an approximate model

3. In this paper...

Combining Model-Checking and Abstract Interpretation

Why?

- Model-checking:
  - Finite state space
  - Sound and complete property verification
- Abstract Interpretation:
  - Infinite state space
  - Sound but uncomplete property determination

Parallel combination of model-checking and abstract interpretation:

  - Model-checking:
    * Exact symbolic representation of properties
    * The model is an exact representation of the system
    ⇒ Exact properties of exact model
  - Abstract interpretation:
    * Preliminary/parallel analysis of the model by abstract interpretation
    ⇒ Limit the state search space
  ⇒ Exact properties of an exact sub-model
**Example: Maximum Delay Problem**

Find the maximum delay to reach a final state starting from some initial state:

![Diagram of a state transition graph]

**Maximum Delay Algorithm “maximum1”**

```plaintext
procedure maximum1 (I, F);
    R' := S;
    n := 0;
    R := (S - F);
    while (R ≠ R' ∧ R ∩ I ≠ ∅) do
        R' := R;
        n := n + 1;
        R := pre[t] R' ∩ (S - F);
    od;
    return if (R' = R) then ∞ else n;
```

**Execution trace of the “maximum1” algorithm**

It is useless to explore the states which are not:
- descendants of the initial states;
- ascendants of the initial states.

**Maximum Delay Algorithm “maximum2”**

(with state search space restriction)

```plaintext
procedure maximum2 (I, F);
    R' := S;
    n := 0;
    R := (U₀ - F);
    while (R ≠ R' ∧ R ∩ I ≠ ∅) do
        R' := R;
        n := n + 1;
        R := pre[t] R' ∩ (Uₙ - F);
    od;
    return if (R' = R) then ∞ else n;
```

where: \( n ≥ 0 : Uₙ ⊇ U \triangleq \text{post}[t⁺] I \cap \text{pre}[t⁺] F \)
Execution trace of the “maximum2” algorithm

![Diagram showing execution trace]

- Any upper-approximations $U_0, U_1, \ldots, U_n, \ldots$ of $U$ can be used;
- In the worst case $U_n = S$ (all states), hence “maximum2” = “maximum1”.

Analysis of the model by abstract interpretation

- We can compute:
  $$U_0 \supseteq U_1 \supseteq \ldots \supseteq U_n \supseteq U \equiv \text{post}[t^*] I \cap \text{pre}[t^*] F$$
  by abstract interpretation;
- The abstract interpretation can be done in parallel with the model-checking (at almost no supplementary cost);
- The abstract interpretation results are used on the fly for $U_n$ as they become available to restrict the state search space;
- Several restriction operators have been proposed for symbolic model checking (with BDDs & convex polyhedra).

Upper approximation $D$ of post$[t^*] I = \text{lfp} D \subseteq \lambda X. I \cup \text{post}[t] X$ by abstract interpretation.

1. Consider an abstract domain $\langle I, \sqsubseteq \rangle$ approximating sets of states $\langle \psi(S), \sqsubseteq \rangle$;
2. define a correspondence:
   $$\langle \psi(S), \sqsubseteq \rangle \xrightarrow{\gamma} \langle I, \sqsubseteq \rangle$$
   which is a Galois connection:
   $$\forall P \in \psi(S) : \forall Q \in I : \alpha(P) \subseteq Q \iff P \subseteq \gamma(Q) .$$
   The abstract value $\alpha(P)$ is the approximation of $P \subseteq S$: $P \subseteq \gamma(\alpha(P))$.

3. Define an abstract post-image transformer $F \in I \mapsto L$:
   $$\forall Q \in I : \alpha \circ (\lambda X. I \cup \text{post}[t] X) \circ \gamma(Q) \sqsubseteq F(Q)$$

4. Define a widening operator $\triangledown \in L \times L \mapsto L$:
   - it is an upper approximation$^5$,
   - it enforces finite convergence of $F$-upward iterates$^6$;

5. The upward forward iteration sequence with widening:
   $$\hat{F}^0 \equiv \alpha(\emptyset),$$
   $$\hat{F}^{i+1} \equiv \hat{F}^i \triangledown F(\hat{F}^i) \quad \text{if} \; F(\hat{F}^i) \subseteq \hat{F}^i$$
   $$\hat{F}^{i+1} \equiv \hat{F}^i \quad \text{otherwise}$$
   is ultimately stationary;
   its limit $\hat{F}$ is a sound upper approximation of $\text{post}[t^*] I$ in that:
   $$\text{post}[t^*] I \subseteq \gamma(\text{lfp} \subseteq F) \subseteq \gamma(\hat{F}) .$$

---

$^4$ Cousot, P. and Cousot, R. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints.

$^5$ Cousot, P. and Cousot, R. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints.

$^6$ Cousot, P. and Cousot, R. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints.

---


---

6. Define a *narrowing operator* \( \Delta \in L \times L \mapsto L \) such that:
   - it is an upper approximation \(^1\),
   - it enforces finite convergence of \( \mathcal{F} \)-downward iterates \(^2\).

7. The *downward forward iteration sequence with narrowing*:

   \[
   \begin{align*}
   \hat{x}^0 & \equiv \hat{x}, \\
   \hat{x}^{i+1} & \equiv \hat{x}^i & \text{if } \mathcal{F}(\hat{x}^i) = \hat{x}^i \\
   \hat{x}^{i+1} & \equiv \hat{x}^i \Delta \mathcal{F}(\hat{x}^i) & \text{otherwise}
   \end{align*}
   \]

   is ultimately stationary;

   its limit \( \hat{x} \) is a better sound upper approximation \( \text{post}[t^*] \) in that:

   \[
   \text{post}[t^*] I \subseteq \gamma(\text{lfp}^\infty \mathcal{F}) \subseteq \gamma(\hat{x}) \subseteq \gamma(\hat{x}).
   \]

---

**Abstract interpretation design**

- The design of:
  - the abstract algebra \( \langle L, \subseteq, \perp, T, \cup, \cap, \triangledown, \Delta, f_1, \ldots, f_n \rangle \)
  - the transformer \( \mathcal{F} \) (usually composed out of the primitives \( f_1, \ldots, f_n \))

are problem dependent;

- Natural choices in the model-checking context are:
  - BDDs (discrete systems),
  - Convex polyhedra (hybrid systems);

for which widening operators have been defined \(^3\) \(^4\).

---

6. Define a narrowing operator \( \Delta \in L \times L \mapsto L \) such that:
   - it is an upper approximation \(^1\),
   - it enforces finite convergence of \( \mathcal{F} \)-downward iterates \(^2\).

7. The *downward forward iteration sequence with narrowing*:

   \[
   \begin{align*}
   \hat{x}^0 & \equiv \hat{x}, \\
   \hat{x}^{i+1} & \equiv \hat{x}^i & \text{if } \mathcal{F}(\hat{x}^i) = \hat{x}^i \\
   \hat{x}^{i+1} & \equiv \hat{x}^i \Delta \mathcal{F}(\hat{x}^i) & \text{otherwise}
   \end{align*}
   \]

   is ultimately stationary;

   its limit \( \hat{x} \) is a better sound upper approximation \( \text{post}[t^*] \) in that:

   \[
   \text{post}[t^*] I \subseteq \gamma(\text{lfp}^\infty \mathcal{F}) \subseteq \gamma(\hat{x}) \subseteq \gamma(\hat{x}).
   \]

---

**Abstract interpretation design**

- The design of:
  - the abstract algebra \( \langle L, \subseteq, \perp, T, \cup, \cap, \triangledown, \Delta, f_1, \ldots, f_n \rangle \)
  - the transformer \( \mathcal{F} \) (usually composed out of the primitives \( f_1, \ldots, f_n \))

are problem dependent;

- Natural choices in the model-checking context are:
  - BDDs (discrete systems),
  - Convex polyhedra (hybrid systems);

for which widening operators have been defined \(^3\) \(^4\).

---

*Upper approximation* \( A \) of \( \text{pre}[t^*] F = \text{lfp}^\infty \lambda X \cdot F \cup \text{pre}[t] X \) by abstract interpretation \(^11\)

Use the same abstract algebra \( \langle L, \subseteq, \perp, T, \cup, \cap, \triangledown, \Delta, f_1, \ldots, f_n \rangle \):

8. Define an abstract pre-image transformer \( \mathcal{F} \in L \mapsto m \mapsto L \):

   \[
   \forall Q \in L : \alpha \circ (\lambda X \cdot F \cup \text{pre}[t] X) \circ \gamma(Q) \subseteq B(Q)
   \]

9. First use an *upward backward iteration sequence with widening* finitely converging to \( B \);

10. Improve by a *downward iteration sequence with narrowing* finitely converging to \( B \) such that:

    \[
    \text{pre}[t^*] F = \text{lfp}^\infty \lambda X \cdot F \cup \text{pre}[t] X \subseteq \gamma(\text{lfp}^\infty B) \subseteq \gamma(\hat{B}) \subseteq \gamma(B)
    \]

---

**Sequence of upper approximations**

\( U_0, U_1, \ldots, U_n, \ldots \) of \( U = \text{post}[t^*] I \cap \text{pre}[t^*] F \) by abstract interpretation \(^12,13\)

- \( U_0 = S \); all states;
- \( U_1 \) is the \( \gamma \)-concretization of the limit of the upward forward iteration sequence with widening for \( \mathcal{F} \);
- \( U_2 \) is the \( \gamma \)-concretization of the limit of the corresponding downward forward iteration sequence with narrowing for \( \mathcal{F} \) starting from \( U_0 \);
- \( \ldots \)

---

\(^1\) Via \( \delta \in L \times L \mapsto L \), \( \delta \subseteq L \times L \).

\(^2\) For all decrasing chains \( \hat{x}^0 \geq \hat{x}^1 \geq \cdots \) the decrasing chain defined by \( \gamma(\hat{x}^0) \geq \gamma(\hat{x}^1) \geq \cdots \) is not strictly decrasing.

\(^3\) Cousot, P. and Cousot, R., Abstract interpretation and application to logic programs. J. Log. Prog., 13, 2-3, 303-339. (The editor of JLP has mistakenly published the erroneous galley proof. For a correct version of this paper, see http://www-rocq.inria.fr/"cousot.


\(^6\) Cousot, F. and Cousot, R. Abstract interpretation and application to logic programs. J. Log. Prog., 13, 2-3, 303-339. (The editor of JLP has mistakenly published the erroneous galley proof. For a correct version of this paper, see http://www-rocq.inria.fr/"cousot.

---

**Sequence of upper approximations**

\( U_0, U_1, \ldots, U_n, \ldots \) of \( U = \text{post}[t^*] I \cap \text{pre}[t^*] F \) by abstract interpretation \(^12,13\)

- \( U_0 = S \); all states;
- \( U_1 \) is the \( \gamma \)-concretization of the limit of the upward forward iteration sequence with widening for \( \mathcal{F} \);
- \( U_2 \) is the \( \gamma \)-concretization of the limit of the corresponding downward forward iteration sequence with narrowing for \( \mathcal{F} \) starting from \( U_0 \);
- \( \ldots \)
$U^{4n+3}$ is the $\gamma$-concretization of the limit of the upward backward iteration sequence with widening for $\lambda X \cdot (U^{4n+2} \sqcap B(X))$;

$U^{4n+4}$ is the $\gamma$-concretization of the limit of the corresponding downward backward iteration sequence with narrowing for $\lambda X \cdot (U^{4n+2} \sqcap B(X))$ starting from $U^{4n+3}$;

$U^{4n+5}$ is the $\gamma$-concretization of the limit of the upward forward iteration sequence with widening for $\lambda X \cdot (U^{4n+4} \sqcap \mathcal{F}(X))$;

$U^{4n+6}$ is the $\gamma$-concretization of the limit of the corresponding downward forward iteration sequence with narrowing for $\lambda X \cdot (U^{4n+4} \sqcap \mathcal{F}(X))$ starting from $U^{4n+5}$;

The sequence $U_0, U_1, U_2, \ldots, U^{4n+3}, U^{4n+4}, U^{4n+5}, U^{4n+6}, \ldots$ is a descending chain;

$\Rightarrow$ The restriction is more and more precise as the model-checking goes on;

All elements $U_k$ is the sequence are sound:

$U_k \subseteq \text{post}(i^*) I \cap \text{pre}(i^*) F$

Stop the abstract interpretation computation with a narrowing or when the parallel model-checking terminates;

**PROBLEMATIC TERMINATION**

- The abstract interpretation always terminate;

- The abstract interpretation is approximate so the state-space restriction may not be finite;

$\Rightarrow$ The parallel combination of abstract interpretation and model-checking is incomplete since it may not terminate;

- In case of nontermination the information gathered by abstract interpretation is reusable for verification by:
  - abstract symbolic methods,
  - model abstraction;
  - which are also incomplete but guarantee termination.

**CONCLUSION**

- We have proposed a method for the parallel combination of model-analysis by abstract interpretation and verification by model-checking where the verification:
  - makes no approximation on states and transitions,
  - explores an (hopefully finite) subgraph;

- Semi-algorithm since there is no guarantee that the explored subgraph will be finite:
  - classical model-checking would have failed anyway,
  - case by case experimentation is needed;

- The method should be used before resorting to model-checking of a more abstract model (the information gathered about the exact model being reusable).