Combination of Algebraic and SMT-based-logical Abstract Interpretations
Junjie Chen (PhD student, 1st year) and P. Cousot (advisor)

Static Analysis Combining Logical and Algebraic Abstractions

Proof theoretic/logical abstractions are a particular case of algebraic abstractions.

Nelson-Oppen procedure is a particular case of reduced product.

A new combination of logical and algebraic abstractions can be proposed by this unifying point of view.

Reduced Product of Logical and Algebraic Domains

Logical theories

\[ \phi_1 \quad \phi_2 \quad \ldots \quad \phi_n \]

Algebraic domains

\[ P_1 \quad P_2 \quad \ldots \quad P_m \]

\[ \rho^l \quad \rho_{\alpha l} \quad \rho^a \]

Easy introducing new abstractions on either side
⇒ Extensible expressive static analyzers / verifiers.

SMT Solver Based Logical Abstract Domains

Abstract Properties
Universal representation of abstract properties by a set \( A \) of quantifier-free first-order logical formulae.
Each domain contains only one theory \( T \) which may be decidable, deductive and complete on \( A \).

Abstract Operators
- Top: \( \top \Rightarrow t \)
- Bottom: \( \bot \Rightarrow f \)
- Abstract Intersection: \( \cap \Rightarrow \land \)
- Abstract Union: \( \cup \Rightarrow \lor \)

Abstract Transformations
- Invertible assignment:
  \[ f_{x := t} \psi \equiv \psi[x \leftarrow t^{-1}] \]
- Non-invertible assignment:
  \[ f_{x := t} \psi \equiv \exists x' : \psi[x/x'] \land x = t \]
- Test:
  \[ p[q] \psi \equiv \psi \land \varphi \]

Abstract Implication
SMT solver is used for the abstract orders \( \subseteq \). We ask SMT solver whether \( (\exists x \psi_1 \cup x \psi_2) \) \( \psi_1 \land \neg \psi_2 \) is satisfied.
- Yes ⇒ \( \psi_1 \not\subseteq \psi_2 \)
- No ⇒ \( \psi_1 \subseteq \psi_2 \)

Widening
- Designing a universal widening for logical abstract domain is difficult.
- We can always ask the end-user.
- Alternative method: widening in polyhedral abstract domain.

Proof theoretic/logical abstractions are a particular case of algebraic abstractions.

Nelson-Oppen procedure is a particular case of reduced product.

A new combination of logical and algebraic abstractions can be proposed by this unifying point of view.