Carnegie Mellon Electrical & Computer ENGINEERING
Carnegie Mellon SCHOOL OF COMPUTER SCIENCE
NEW YORK UNIVERSITY

Combination of Algebraic and SMT-based-logical Abstract Interpretations

Junjie Chen (PhD student, 1st year) and P. Cousot (advisor)

NSF Expeditions in Computing

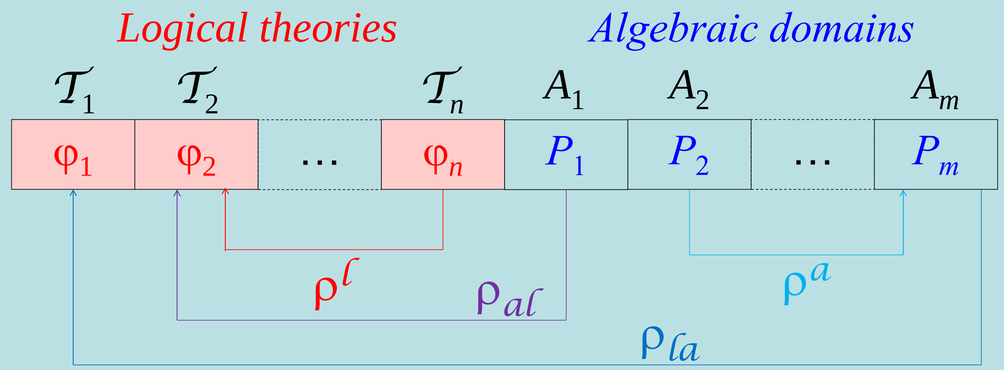
Static Analysis Combining Logical and Algebraic Abstractions

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



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 $\mathcal{A}$ of quantifier-free first-order logical formulæ.
Each domain contains only one theory $\mathcal{T}$ which may be decidable, deductive and complete on $\mathcal{A}$.

Abstract Operators

- Top: $\top \Rightarrow$ tt
- Bottom: $\bot \Rightarrow$ ff
- Abstract Intersection: $\sqcap \Rightarrow \wedge$
- Abstract Union: $\sqcup \Rightarrow \vee$

Abstract Implication

SMT solver is used for the abstract orders $\sqsubseteq$. We ask SMT solver whether $(\exists x_{\psi 1} \cup x_{\psi 2} :)\ \psi_1 \wedge \neg\psi_2$ is satisfied.

- Yes ⇒ $\psi_1 \not\sqsubseteq \psi_2$
- No ⇒ $\psi_1 \sqsubseteq \psi_2$

Abstractions

For a given logical abstract domain, we need to design an abstraction algorithm $\alpha \in F(x,f,p) \rightarrow \mathcal{A}$ to abstract properties in $\mathcal{A}$.

- Quantifier elimination
- Literal elimination

Abstract Transformers

- ✓ Invertible assignment:
  $f_a[\![x:=t]\!]\psi \triangleq \psi[x \leftarrow t_x^{-1}]$
- ✓ Non-invertible assignment:
  $f_a[\![x:=t]\!]\psi \triangleq \exists x' : \psi[x/x'] \wedge x = t$
- ✓ Test: $p[\![\varphi]\!]\psi \triangleq \psi \wedge \varphi$

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.

Patrick Cousot, Radhia Cousot, Laurent Mauborgne: Logical Abstract Domains and Interpretations. The Future of Software Engineering 2010: 48-71.
Patrick Cousot, Radhia Cousot, Laurent Mauborgne: The Reduced Product of Abstract Domains and the Combination of Decision Procedures. FOSSACS 2011: 456-472.