A PROOF-THEORETIC APPROACH TO ABSTRACT INTERPRETATION

Apostolos Tzimoulis

joint work with Vijay D’Silva, Alessandra Palmigiano and Caterina Urban

(with images from Patrick Cousot)

TACL 2017 - Prague
ABSTRACT INTERPRETATION

Possible trajectories
Abstract interpretation
Abstract interpretation

Forbidden zone

Abstraction of the trajectories

Possible trajectories
**Some examples**

A program produces an integer as output. The concrete domain of the outcomes will be $\mathcal{P}(\mathbb{Z})$. The abstraction of the program output is

$$
\begin{array}{c}
\mathcal{P}(\mathbb{Z}) \\
\top \\
\bot \\
\text{Even} \\
\text{Odd}
\end{array}
$$

and let $\gamma : (\mathcal{A}, \sqsubseteq, \sqcup, \sqcap, \sim) \rightarrow (\mathcal{P}(\mathbb{Z}), \subseteq, \cup, \cap, \neg)$ be such that

$\gamma(\top) = \mathbb{Z} \\
\gamma(\text{Even}) = \{2a \in \mathbb{Z} \mid a \in \mathbb{Z}\} \\
\gamma(\bot) = \emptyset \\
\gamma(\text{Odd}) = \{2a + 1 \in \mathbb{Z} \mid a \in \mathbb{Z}\}$
A program produces an integer as output. The concrete domain of the outcomes will be $\mathcal{P}(\mathbb{Z})$. The abstraction of the program output is
A program produces an integer as output. The concrete domain of the outcomes will be $\mathcal{P}(\mathbb{Z})$. The abstraction of the program output is
AIM OF THE PROJECT

- Make the role of logic explicit (c.f Schmidt 2008, d’Silva Urban 2016).
- Apply the logical insights to develop a unifying framework for these phenomena.
- Explore how far can we go.
The formalities

- Let $\text{Var}$ be a set of variables. A structure is a function $\sigma : \text{Var} \rightarrow S$ (where $S$ is a set, e.g. $\mathbb{Z}$).
- The structure $(\mathcal{P}(\text{Struc}), \subseteq)$ is called concrete algebra.
- Let $\mathcal{A} = (A, \sqsubseteq)$ be a bounded lattice.
- Concretization: A monotone function $\gamma : \mathcal{A} \rightarrow (\mathcal{P}(\text{Struc}), \subseteq)$ that preserves maximum and minimum.
- If a concretization exists then we say that $\mathcal{A}$ is an abstraction of $(\mathcal{P}(\text{Struc}), \subseteq)$.
- A transformer $g : A \rightarrow A$ is a sound abstraction of $f : \mathcal{P}(\text{Struct}) \rightarrow \mathcal{P}(\text{Struct})$ if for all $a \in A$ $f(\gamma(a)) \subseteq \gamma(g(a))$. 
**Fig. 3** The lattice of signs and the proof calculus $\vdash$ for the sign logic.
Fig. 6  The lattice of intervals and the proof calculus $\vdash_{\mathcal{I}}$ for the interval logic.
A general recipe

Assume that $|\text{Var}| = 1$. We will generate a logic corresponding to a finite abstraction $\mathcal{A} = (A, \sqsubseteq, Op_A)$ with concretization $\gamma : \mathcal{A} \rightarrow (P(\text{Struct}), \subseteq, Op_c)$.

1. The logical connectives of the language will be the connectives preserved by $\gamma$.
2. for every point $a \in A$ we add a unary predicate symbol $a(x)$ to the language;
3. for every connective that is preserved by $\gamma$ we add the introduction rules appropriate to that connective in the proof system;
4. for every binary connective $\star$ in $\mathcal{L}_A$ such that $a \star b = c$, we add a rule corresponding to the axiom $a(x) \star b(x) \vdash c(x)$ in the proof system;
5. for every unary connective $\star$ such that $\star a = b$, we add a rule corresponding to the axiom $\star a(x) \vdash b(x)$.
6. for all predicates $a(x)$ and $b(x)$ such that $a \leq b$, we add a rule corresponding to the axiom $a(x) \vdash b(x)$. 

Some Results

Let $\mathbb{L}$ be the Lindenbaum-Tarski algebra of $\mathcal{L}_A$.

**Lemma**

The logic $\mathcal{L}_A$ is sound w.r.t. the concretization.

**Lemma**

The algebra $\mathbb{L}$ is isomorphic to $\mathbb{A}$.

**Lemma**

If $\gamma$ is an order-embedding, then $\mathcal{L}_A$ is complete w.r.t. the concretization.
Some Questions

- Cartesian abstractions with many-variable.
- Categories: Can we use the duality to help us?
- Modalities: Abstract transformers.