A proof-theoretic approach to abstract interpretation

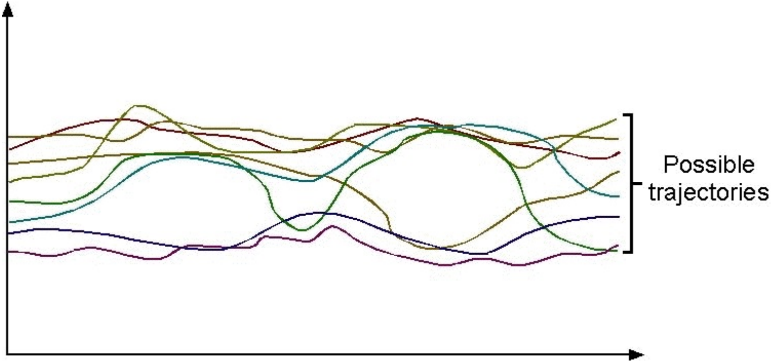
Apostolos Tzimoulis

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

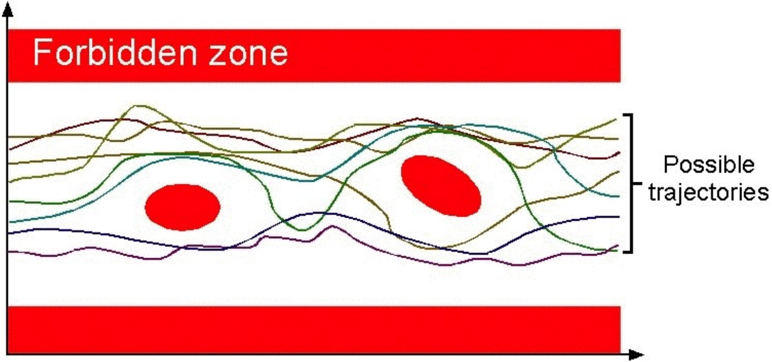
(with images from Patrick Cousot)

TACL 2017 - Prague

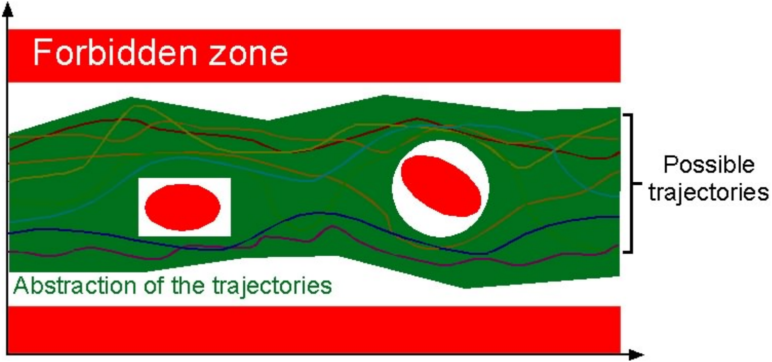
Abstract interpretation



Abstract interpretation

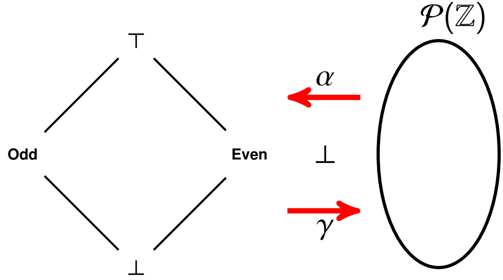


Abstract interpretation



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



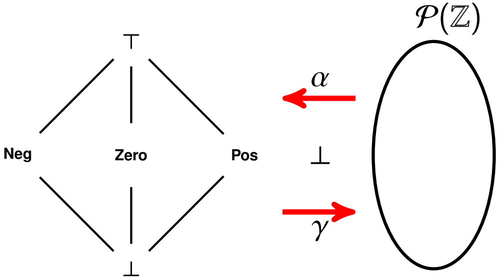
and let $\gamma : (\mathcal{A}, \sqsubseteq, \sqcup, \sqcap, \sim) \to (\mathcal{P}(\mathbb{Z}), \subseteq, \cup, \cap, \neg)$ be such that

$\gamma(\top) = \mathbb{Z} \quad \gamma(\text{Even}) = \{2a \in \mathbb{Z} \mid a \in \mathbb{Z}\}$

$\gamma(\perp) = \varnothing \quad \gamma(\text{Odd}) = \{2a + 1 \in \mathbb{Z} \mid a \in \mathbb{Z}\}$

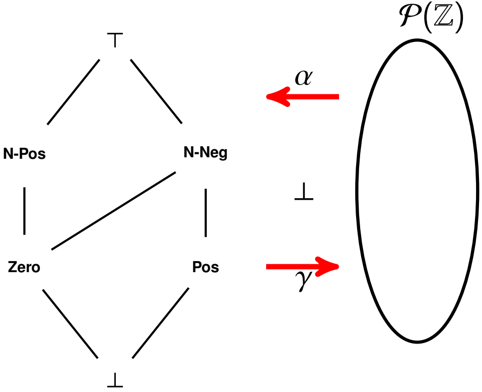
Some examples

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



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



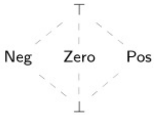
Aim of the project

- 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 *Var* be a set of variables. A structure is a function $\sigma : Var \to S$ (where S is a set, e.g. $\mathbb{Z}$).
- The structure $(\mathcal{P}(Struc), \subseteq)$ is called *concrete algebra*.
- Let $\mathcal{A} = (A, \sqsubseteq)$ be a bounded lattice.
- *Concretization*: A monotone function $\gamma : \mathcal{A} \to (\mathcal{P}(Struc), \subseteq)$ that preserves maximum and minimum.
- If a concretization exists then we say that $\mathcal{A}$ is an *abstraction* of $(\mathcal{P}(Struc), \subseteq)$.
- A transformer $g : A \to A$ is a *sound abstraction* of $f : \mathcal{P}(Struct) \to \mathcal{P}(Struct)$ if for all $a \in A$ $f(\gamma(a)) \subseteq \gamma(g(a))$.

Logic and Lattices



The sign calculus $\vdash_{\mathscr{S}}$

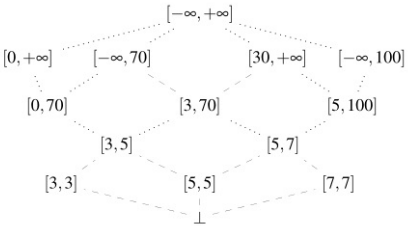
$\vdash_{\text{CORE}}$

$$\frac{}{\Gamma, x < 0, x = 0 \vdash \mathsf{ff}_x}\ \mathsf{ffR}_1$$

$$\frac{}{\Gamma, x = 0, x > 0 \vdash \mathsf{ff}_x}\ \mathsf{ffR}_2$$

$$\frac{}{\Gamma, x < 0, x > 0 \vdash \mathsf{ff}_x}\ \mathsf{ffR}_3$$

Fig. 3 The lattice of signs and the proof calculus $\vdash_{\mathscr{S}}$ for the sign logic.



The interval calculus $\vdash_{\mathscr{I}}$

$\vdash_{\text{CORE}}$

$$[m \leq n]\ \frac{\Gamma, x \leq n \vdash \varphi}{\Gamma, x \leq m \vdash \varphi}\ \text{UB-L}$$

$$[m \leq n]\ \frac{\Gamma \vdash x \leq m}{\Gamma \vdash x \leq n}\ \text{UB-R}$$

$$[m \leq n]\ \frac{\Gamma, x \geq m \vdash \varphi}{\Gamma, x \geq n \vdash \varphi}\ \text{LB-L}$$

$$[m \leq n]\ \frac{\Gamma \vdash x \geq n}{\Gamma \vdash x \geq m}\ \text{LB-R}$$

$$[m < n]\ \frac{}{\Gamma, x \leq m, x \geq n \vdash \mathsf{ff}_x}\ \mathsf{ff}\text{R}_5$$

Fig. 6 The lattice of intervals and the proof calculus $\vdash_{\mathscr{I}}$ for the interval logic.

A GENERAL RECIPE

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

1. The logical connectives of the language will be the connectives preserved by γ.
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 γ 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 $a(x) \star b(x) \dashv\vdash c(x)$ in the proof system;
5. for every unary connective $\star$ such that $\star a = b$, we add a rule corresponding to the axiom $\star a(x) \dashv\vdash b(x)$.
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 $\mathscr{A}$.

Lemma

If γ 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.