TD, week 7 : Abstract Interpretation

Ex. 1 : Abstraction of sets of values using intervals

In the lecture, we studied several abstract domains to represent sets of values. We propose to sudy another more interesting abstraction here, that is based on intervals. An abstract value is either $\bot$ (representing the empty set), or an interval, the bounds of which may be infinite.

1. Formalize the abstraction relation of the lattice of intervals, with both adjoint operators. Prove that these adjoint operators form a Galois connection.

2. Describe the abstract operators on this lattice, to over-approximate concrete addition, subtraction, multiplication and division. Prove the soundness of each operator. For each operator, show whether it is exact or not (prove it if it is exact, and show a counter-example if it is not).

3. Propose approximation for concrete unions and intersections in the lattice of intervals. Prove the soundness of each operator. For each operator, show whether it is exact or not (prove it if it is exact, and show a counter-example if it is not).

Ex. 2 : Abstraction of semantics

We consider a transition system $(\mathbb{S}, \rightarrow, \mathbb{S}_{\mathcal{I}})$, and compare its semantics using abstract interpretation.

1. Recall the definitions of its finite traces semantics, and its semantics of reachable states.

2. Propose an abstraction relation between these two semantics, and prove that it holds. To do that, define a Galois connection between their semantic domains and show that one semantics can be derived from the other by abstraction. What does this mean, in intuitive terms ?

3. Show that this abstraction relation can be derived by abstract interpretation, using the fixpoint definitions of the two semantics (hint: use a fixpoint transfer theorem).

Ex. 3 : Galois insertions, and non relational interval abstraction

A *Galois insertion* is a Galois connection

$$(C, \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \sqsubseteq)$$

such that $\alpha \circ \gamma$ is the identity function.

1. Does the interval abstract domain shown in the first exercise define a Galois insertion ?

2. How about the non relational abstraction, defined from intervals ? Would choosing the lattice of constants or the lattice of signs make a difference ? Give examples, and explain the intuitive meaning of this property.

3. Propose another definition or non-relational abstraction inspired by this property.