Beliefs and Plausibilities in Abstract Interpretation

Maja H. Kirkeby* MAJAHT@RUC.DK
Roskilde University, Denmark

Holger Axelsen FUNKSTAR@DI.KU.DK
Edlund A/S, Denmark

Poster Abstract

Static Analysis of programs deduces properties of programs without executing them. They either deduce possible properties, what may/could happen, or guaranteed properties, what must always happen.

Static analyses may be expressed using Abstract Interpretation (Cousot and Cousot, 1977). Each program denotes computations in some *concrete* universe of objects, i.e., represented by a poset $(C, \sqsubseteq_C)$ and a monotone transfer function $f : C \to C$. An Abstract Interpretation of a program describes computations of the program in another universe of *abstract* objects, i.e., a poset $(A, \sqsubseteq_A)$, so that the result of the abstract execution, i.e., abstract monotone transfer function $g : A \to A$, give some information on the actual computations, i.e., there exists a Galois connection (C, α, γ, A) where $\alpha : C \to A$ and $\gamma : A \to C$ are defined such that $\alpha(C) \sqsubseteq_A A \Leftrightarrow C \sqsubseteq_C \gamma(A)$. Depending on the purpose of the analysis g and f relates differently; g is an upwards (downwards) approximation of f when $f \sqsubseteq_C (\sqsupseteq_C)\gamma \circ g \circ \alpha$ and $g \sqsupseteq_A (\sqsubseteq_A)\alpha \circ f \circ \gamma$.

Using a set-function to carry a probability measure we can create a belief and a plausibility function bel, pl (Dempster, 1967). We show that Abstract Interpretation deduce bel and pl as lower and upper bound for the correct probability of program properties w.r.t. a discrete program input probability. Furthermore, we present a method and sufficient criteria for lifting existing Abstract Interpretation Analyses, creating new analyses that derive safe bounds for the probability of the properties in the form of belief or a plausibility functions over the program properties. So, given a Galois Connection (C, α, γ, A) with transfer functions f and g (satisfying the criteria) we construct a new Galois connection $(BEL, \alpha', \gamma', M)$ with posets $(BEL = \{bel \mid bel : C \to [0,1]\}, \leq)$, $(M = \{m \mid m : A \to [0,1]\}, \sqsubseteq_m)$, and transfer functions f', g' where g' is a downwards approximation of f'. This ensures $f' \geq \gamma' \circ g' \circ \alpha'$ allowing $\gamma' \circ g' \circ \alpha'(bel)$ to serve as a safe lower bound of $f'(bel)$.

References

P. Cousot and R. Cousot. Abstract Interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints, 1977. ISSN 00900036.

A. P. Dempster. Upper and lower probabilities induced by a multiple-valued mapping. *Ann. Math. Stat.*, 38:325–339, 1967.

*. The research leading to these results has been supported by EU FP7 project 318337, ENTRA - Whole-Systems Energy Transparency