

The Calculational Design of a Generic Abstract Interpreter

Patrick COUSOT

*LIENS, Département de Mathématiques et Informatique
École Normale Supérieure, 45 rue d'Ulm, 75230 Paris cedex 05, France*

Abstract. We present in extenso the calculation-based development of a generic compositional reachability static analyzer for a simple imperative programming language by abstract interpretation of its formal rule-based/structured small-step operational semantics.

Contents

1. Introduction	3
2. Definitions	4
3. Values	5
3.1 Machine integers	5
3.2 Errors	5
4. Properties of Values	5
5. Abstract Properties of Values	6
5.1 Galois connection based abstraction	6
5.2 Componentwise abstraction of sets of pairs	7
5.3 Initialization and simple sign abstraction	7
5.4 Initialization and interval abstraction	8
5.5 Algebra of abstract properties of values	9
6. Environments	10
6.1 Concrete environments	10
6.2 Properties of concrete environments	10
6.3 Nonrelational abstraction of environment properties	10
6.4 Algebra of abstract environments	12
7. Semantics of Arithmetic Expressions	13
7.1 Abstract syntax of arithmetic expressions	13
7.2 Machine arithmetics	13
7.3 Operational semantics of arithmetic expressions	13
7.4 Forward collecting semantics of arithmetic expressions	14
7.5 Backward collecting semantics of arithmetic expressions	14
8. Abstract Interpretation of Arithmetic Expressions	15
8.1 Lifting Galois connections at higher-order	15