APRON: Numerical Program Analysis

http://apron.cri.ensmp.fr/

CRI/École des Mines — École Normale Supérieure — École Polytechnique — Vérimag/CNRS — INRIA

Approach

- Static analysis by abstract interpretation
- Define an invariant at each program point
  (semantic fixpoint equations)
- Solve the equations using
  - abstract semantics (abstract properties)
  - extrapolation

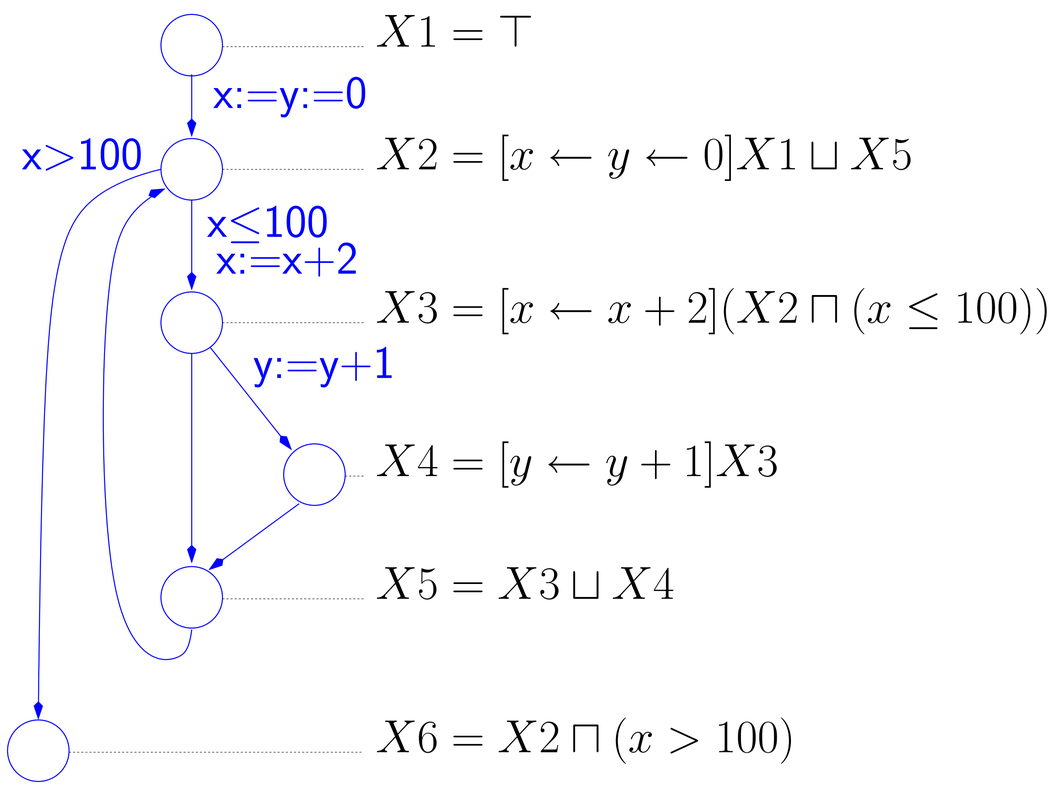
Previous success stories

Astrée [ENS/CNRS]: Successful analysis of the A380 flight control software (700 KLoC).

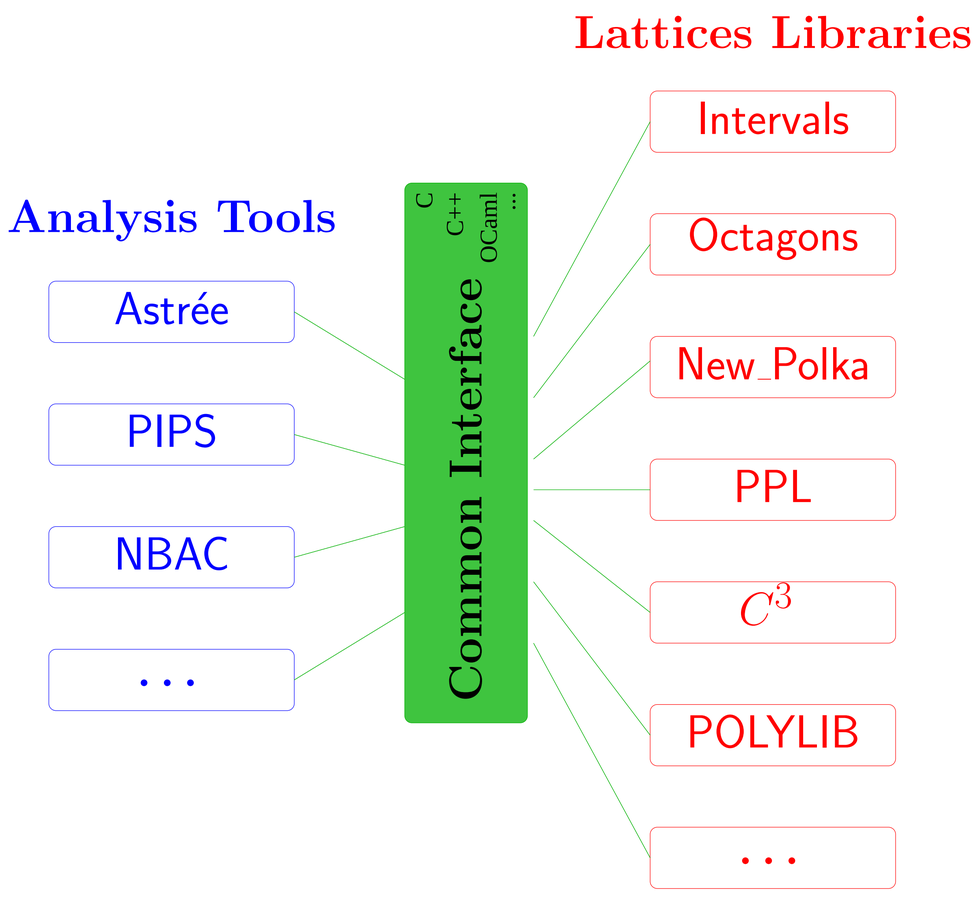
Two companies:

- PolySpace Technologies: Analysis of runtime errors.
- AbsInt Angewandte Informatik GmbH: Precise evaluation of worst case execution time.

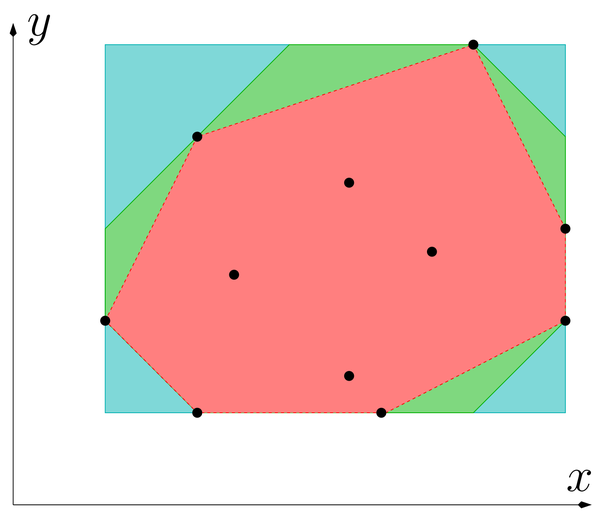
Semantic equations



Joint work: Common interface



Numerical lattices



Intervals: $x \in [1,6] \quad y \in [1,5]$

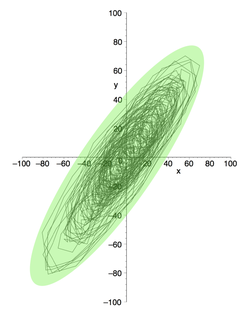
Octagons: $x \in [1,6], y \in [1,5], (x+y) \in [3,10], (x-y) \in [-2,4]$

Polyhedra: $1 \leq y \leq 2x \leq 12\ ,\ 3-y \leq x \leq 2+2y\ ,\ 2x+y \leq 15$

- Representation, Normal form
- Emptiness decision
- Lattice operations ($\sqcup, \sqcap, \sqsubseteq$)
- Image by an assignment, guard, substitution
- Extrapolation operators

Ongoing work

- Relational analysis of floating-point computations: discover sound bounds taking rounding into account.
- Non-linear abstractions of domain-specific properties: analysis of complex code patterns (e.g., digital filtering, slowly diverging geometric sequences).



- Functional properties: modular proofs that implementations of elementary numerical functions satisfy their specifications.
- Parameterized abstractions: symbolic analyzes parameterized by numerical domains (shape analysis, class invariants).
- Automatic termination proofs using semidefinite programming optimization.
- Abstract acceleration on polyhedra: compute, when possible, the exact limit of fixpoint iterations in the lattice of polyhedra.
- DBMs with disequalities: a new lattice for representing order and disequality ($x \neq y$) relations between variables.