**APRON: Numerical Program Analysis**

http://apron.cri.enmp.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

#### Semantic equations

\[
\begin{align*}
X_1 &= \top \\
X_2 &= [x \leftarrow y \leftarrow 0]X_1 \sqcup X_5 \\
X_3 &= [x \leftarrow x + 2](X_2 \cap (x \leq 100)) \\
X_4 &= [y \leftarrow y + 1]X_3 \\
X_5 &= X_3 \sqcup X_4 \\
X_6 &= X_2 \cap (x > 100)
\end{align*}
\]

### 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.

### Joint work: Common interface

#### Lattices Libraries

- Analysis Tools
  - Astrée
  - PIPS
  - NBAC
  - ... 

- Common Interface
  - Intervals
  - Octagons
  - New_Polka
  - PPL
  - POLYLIB
  - ...

### 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.