Abstract Interpretation Based Static Analysis of Hybrid and Embedded Systems, P. Cousot [1]

- **Abstract Interpretation**: a set-theoretic theory of approximation (mainly used for program static analysis, abstract model-checking, etc.);
- **Static Analysis**: approximate analysis of computer programs/systems for testing predefined specifications without execution (as opposed to debugging).

---

[1] cole normale sup rieure, 45 rue d'Ulm, 75230 Paris cedex 05, France.

What has already been achieved?

- **Hybrid Systems**: *academic* use of abstract interpretation based polyhedral approximations for model checking hybrid systems;
- **Embedded Systems**: *industrial* use of abstract interpretation based program static analysis of:
  - Absence of run-time errors (e.g. for Ariane 5 flight software) by PolySpace Polyspace Technologies;
  - Timing verification of real-time programs by AbsInt Angewandte Informatik GmbH.

What are the potential benefits of abstract interpretation?

Static analysis does not try to prove everything, but:

- Is completely automatic (no model to design, no decidability hypothesis, no abstraction to guess, no prover to help, etc.)
- Is reusable (no endless case studies);
- Always offers a full coverage [2];
- Scales up [3];
- Is therefore **cost-effective** [4].

---

[2] can only fail with false alarms in 5 to 10% of the possible cases.
[3] combinatorial explosion mastered by dynamic approximation.
[4] 25 cents/line of code, costing up to 50$!

Some recent relevant advances in abstract interpretation

- **Industrial development**, *does scale up*:
  - now up to 220 000 lines of C;
- **Academic research**, *new semantic models of complex systems*:
  - Geometric models unifying discrete and continuous time (also avoiding interleaving explosions);
  - Synthesis of schedulers of asynchronous processes;
  - Probabilistic analyses;
  - Modular analyses of distributed/mobile systems (on dynamic networks, within unknown environments, etc);

What are the problems?

- **Where is the market ?** the design of static analyzers is costly so must be highly reusable:
  - it is the case for embedded critical software (e.g. C);
  - what about hybrid systems?
- **Where are the researchers ?** the very few researchers working on abstract interpretation are already very busy.

Strong encouragements will be needed before researchers on abstract interpretation seriously consider a new area of potential application.