Présentation de l'équipe-projet ABSTRACTION

Patrick Cousot

Rocquencourt, 13 Janvier 2011

The Team:

- Julien Bertrane, ATER ENS
- Patrick Cousot, Prof. ENS
- Radhia Cousot, DR2 CNRS
- Jérôme Feret, CR1 INRIA
- Antoine Miné, CR2 CNRS
- Xavier Rival, CR1 INRIA
- Visitors (~10), PhD students (3), Post-docs (Alessandro Romanel), Interns (I)

Recent former members:
- David Monniaux (Vérimag),
- Bruno Blanchet (Cascade),
- Laurent Mauborgne (IMDEA),
- Liqian Chen (NUDT, Changsha, China),
- Elodie-Jane Sims (CMU-Silicon Valley)

Abstract interpretation: from theory to practice

Theory

- Develop formal semantics of systems (description of the possible evolution of discrete/continuous/hybrid systems over time)
- Formalize the specification and inference of properties of such semantics
- Develop precise, efficient, and scalable abstractions of system behavior properties
- Apply (maybe with approximation) to the inference of execution properties of systems
- Develop automatic static analysers
- Industrialize these static analysers

Practice

Foundations

Abstract Domains

Abstract domain

- Algebraic structure (implemented as an analyzer module)

$$\langle A, \sqsubseteq, \bot, \top, \sqcup, \sqcap, \nabla, \Delta, \bar{\mathsf{f}}, \bar{\mathsf{b}}, \bar{\mathsf{p}}, \ldots \rangle$$

such that

$\overline{P}, \overline{Q}, \ldots \in A$	abstract properties
$\sqsubseteq \in A \times A \to \mathcal{B}$	abstract partial order
$\bot, \top \in A$	infimum, supremum
$\sqcup, \sqcap, \nabla, \Delta \in A \times A \to A$	abstract join, meet, widening, narrowing
$\ldots$	
$\bar{\mathsf{f}} \in (\mathbb{x} \times \mathbb{E}(\mathbb{x}, \mathbb{f}, \mathbb{p})) \to A \to A$	abstract forward assignment transformer
$\bar{\mathsf{b}} \in (\mathbb{x} \times \mathbb{E}(\mathbb{x}, \mathbb{f}, \mathbb{p})) \to A \to A$	abstract backward assignment transformer
$\bar{\mathsf{p}} \in \mathbb{C}(\mathbb{x}, \mathbb{f}, \mathbb{p}) \to A \to A$	abstract condition transformer

---

Abstract Domains

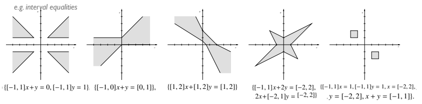
(I) Numerical Domains

Problems in numerical abstract domains

- Traditional linear/polyedral abstract domains are implemented with the double description method, using rationals for soundness
  - Inequalities: $P = \{x \mid Ax = b, Cx \geq d\}$.
  - Generators: $P = \{x \mid x = L\lambda + R\mu + V\nu, \mu, \nu \geq 0, \sum \nu = 1\}$
- Results: sound algorithms using floats (with the inequalities representation only) and generalizations
- Current research:
  - For *efficiency*, use the double description with floats while remaining sound
  - For *precision*, non-linear and sound abstract domains

New numerical abstract domains

- Expressivity (non-convex relational domains)

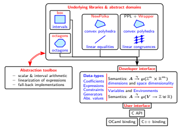


- Efficiency (sound implementations with floats not rationals)

Liqian Chen, Antoine Miné, Ji Wang, and Patrick Cousot. Linear Absolute Value Relation Analysis. ESOP 2011, to appear.
Liqian Chen, Antoine Miné, Ji Wang, Patrick Cousot: An Abstract Domain to Discover Interval Linear Equalities. VMCAI 2010: 112-128
Liqian Chen, Antoine Miné, Ji Wang, Patrick Cousot: Interval Polyhedra: An Abstract Domain to Infer Interval Linear Relationships. SAS 2009: 309-325
Liqian Chen, Antoine Miné, Patrick Cousot: A Sound Floating-Point Polyhedra Abstract Domain. APLAS 2008: 3-18

APRON Library

- Freely available (LGPL) library of numerical domains developed with INRIA-RA, including a web-based sample analyzer for demonstration, teaching and prototyping (*Interproc*)
- Common, AI-based API for numerical abstract domains with reference implementation of classic domains (intervals, polyhedra, octagons, ...)
- Easy to prototype new analyses or domains (e.g., interval polyhedra) with support for
  - integer, rational, machine-integer and float data-types
  - linear, non-linear and float expressions
  - C, C++, Java, OCaml



Bertrand Jeannet, Antoine Miné: Apron: A Library of Numerical Abstract Domains for Static Analysis. CAV 2009: 661-667

Abstract Domains

(II) Symbolic domains

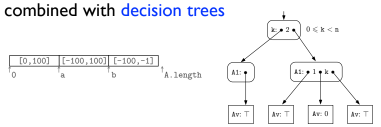
Abstract Domains

(II) Symbolic domains

(a) Array content analysis

Array content analysis

- Existing abstract domains are imprecise or do not scale up
- We have developed efficient, expressive & scalable abstract domain functors based on the idea of symbolic segmentation with dynamic bounds combined with decision trees



Patrick Cousot, Radhia Cousot, Laurent Mauborgne: A Scalable Segmented Decision Tree Abstract Domain. Essays in Memory of Amir Pnueli 2010: 72-95
Patrick Cousot, Radhia Cousot, & Francesco Logozzo. A Parametric Segmentation Functor for Fully Automatic and Scalable Array Content Analysis. POPL 2011, 105—118, 2011.

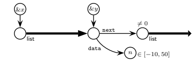
Abstract Domains

(II) Symbolic domains

(b) Shape analysis

Shape abstract domains

- Challenges:
  - dynamic structures with destructive updates
  - complex structural invariants (red-black trees, call-stack, ...)
- We develop relational and expressive parametric abstract domains based on inductive properties and disjointness of regions



- Ongoing work: standardization of abstract domain interfaces to build composite abstractions (shape-shape and shape-numerical)

Vincent Laviron, Bor-Yuh Evan Chang, Xavier Rival: Separating Shape Graphs. ESOP 2010: 387-406 20
Pascal Sotin, Bertrand Jeannet, Xavier Rival: Concrete Memory Models for Shape Analysis. Electr. Notes Theor. Comput. Sci. 267(1): 139-150 (2010)
Bor-Yuh Evan Chang, Xavier Rival: Relational inductive shape analysis. POPL 2008: 247-260

Abstract Domains

(II) Symbolic domains

(c) Combining algebraic and logical abstract domains

Logical & algebraic abstraction

- Algebraic abstractions: in *inference tools*, based on the iterated reduced product of a combination of abstract domains
- Logical abstraction: in *verification tools*, based on the Nelson-Oppen satisfiability procedure for combination f theories (SMT solvers)
- The approaches can be combined by
  - Generalizing logical abstractions (widenings, …)
  - Understanding Nelson-Oppen satisfiability procedure as an iterated reduced product

Patrick Cousot, Radhia Cousot, & Laurent Mauborgne. Logical Abstract Domains and Interpretations. In *The Future of Software Engineering*, S. Nasr (Ed.). © Springer 2010, Pages 48—71.

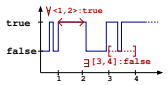
Patrick Cousot, Radhia Cousot, and Laurent Mauborgne. The reduced product of abstract domains and the combination of decision procedures, FoSMaCs 2011, to appear.

Abstract Domains

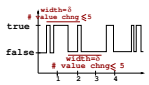
(III) Temporal domains

Temporal abstract domains

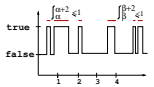
- Contraints to relate values and time



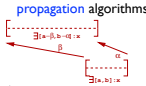
- Value changes counting to express stability specifications



- Integral bounding to express quantitative properties (average...)



- Fast abstract information propagation algorithms



$\overline{\Psi}^{\#}(\exists[a;b]:x) \triangleq \exists[a-\beta;b-\alpha]:x$

for the $\mathrm{DELAY}_{[\alpha,\beta]}$ gate.

Julien Bertrane: Proving the Properties of Communicating Imperfectly Clocked Synchronous Systems. SAS 2006: 370–386

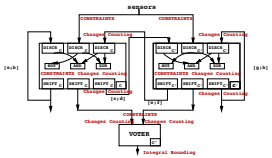
Application: Static Analysis of Dynamic Systems

Static Analysis and Verification

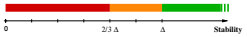
(I) Quasi-synchronous systems

Example

- Two communicating redundant units, imperfect clocks & voter:



- Result of the static analysis:



Counter-example ??? Specification proved

Julien Bertrane: Static Analysis by Abstract Interpretation of the Quasi-synchronous Composition of Synchronous Programs. VMCAI 2005: 97–112

Static Analysis and Verification

(II) Parallel Programs

Static analysis of parallel software

- Critical embedded software are now parallel (e.g., IMA [Integrated Modular Avionics])
- Semantic challenges:
  - implicit communications through shared memory
  - weak memory consistency
  - strict priorities of real-time schedulers
- Abstraction challenges, to scale up while being precise:
  - history-sensitive abstractions of interleaved control flows
  - fixpoint strategies to compute interferences
- Ongoing work on the Thésée prototype

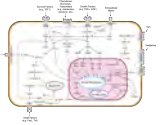
Antoine Miné, Static Analysis of Run-Time Errors in Embedded Critical Parallel C Programs, ESOP 2011, to appear.

Static Analysis

(III) Biological systems

Reachability analysis (of signaling pathways)

- Focus on models of signaling pathways described by collating biochemical interactions.
- These systems usually suffer from a huge combinatorial complexity in the number of chemical species (i.e. chemical complexes) which may be formed at run-time.
- We design scalable and precise analyses of the reachable chemical species.
- Applications:
  - debug models during modeling;
  - precompute properties so as to enable fast stochastic simulation;
  - automatic simplification of the model;
  - compute an idiomatic description of the systems.

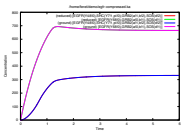


Vincent Danos, Jérôme Feret, Walter Fontana, Jean Krivine: Abstract Interpretation of Cellular Signalling Networks. VMCAI 2008: 83–97

Jérôme Feret: Reachability Analysis of Biological Signalling Pathways by Abstract Interpretation. ICCMSE 2007: 619–622

Model reduction

- Quantitative (ODEs and stochastic) semantics are hard to compute, due to the combinatorial complexity (~10^{20} variables).
- We use an approximation of the control flow between regions of chemical species, so as to compute exact projections of these semantics.



Ground model: 356 variables.
Reduced model: 38 variables.
The two models match

Jérôme Feret, Vincent Danos, Jean Krivine, Russell Harmer, Walter Fontana: Internal coarse-graining of molecular systems. PNAS, volume 106.(16), 6 pages.

Vincent Danos, Jérôme Feret, Walter Fontana, Russell Harmer, Jean Krivine: Abstracting the Differential Semantics of Rule-Based Models: Exact and Automated Model Reduction. LICS 2010: 362–381.

Russ Harmer, Vincent Danos, Jérôme Feret, Jean Krivine, Walter Fontana: Intrinsic information carriers in combinatorial dynamical systems. Chaos, volume 20.(3), 16 pages.

Jérôme Feret, Thomas A. Henzinger, Heinz Koeppl, Tatjana Petrov: Lumpability Abstractions of Rule-based Systems MeCBIC 2010: 142–161.

Software developed

Static analyzers

ASTRÉE (commercialized)

- Routinely used by Airbus France (A380, A400M, A350)
- Now in the industrialization and commercialization phase (AbsInt)

Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, Xavier Rival: Why does Astrée scale up? Formal Methods in System Design 35(3): 229-264 (2009)

THÉSÉE (in development)

- Challenging application to the FWS (A380, A400M, A350)

Antoine Miné, Static Analysis of Run-Time Errors in Embedded Critical Parallel C Programs, ESOP 2011, to appear.

Dissemination

Dissemination

- In the academic world (tutorials, summer schools, invited talks, conference organization, …)
- In the industrial world (conferences, training, …)

Mike Hinchey, Michael Jackson, Patrick Cousot, Byron Cook, Jonathan P. Bowen, & Tiziana Margaria. Software engineering and formal methods. CACM 51(9): 54—59 (2008).

Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, & Xavier Rival. Why does Astrée scale up? Formal Methods in System Design 35 (3): 229—264 (2009).

Patrick Cousot & Radhia Cousot. A gentle introduction to formal verification of computer systems by abstract interpretation. Logics and Languages for Reliability and Security, J. Esparza, O. Grumberg, & M. Broy (Eds), NATO Science Series III: Computer and Systems Sciences, © IOS Press, 2010, 1—29.

Julien Bertrane, Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, & Xavier Rival. Static Analysis and Verification of Aerospace Software by Abstract Interpretation. AIAA Infotech@Aerospace 2010, Atlanta, GA, © AIAA (best paper of the conference).

Julien Bertrane, Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, & Xavier Rival. Static Analysis by Abstract Interpretation of Embedded Critical Software. Third IEEE International workshop UML and Formal Methods, 2010, Shanghai, China, © IEEE.

Daniel Kästner, Stephan Wilhelm, Stefana Nenova, Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, & Xavier Rival. ASTRÉE: Proving the Absence of Runtime Errors. Embedded Real Time Software and Systems (ERTS2 2010). Toulouse, France, 2010.

Conferences recently organized

- SAS 2010 (Perpignan)
  SASB in 2011 (Venice)
- NSAD 2010
- SASB 2010
- TAPAS 2010

Program committees

ESOP 2010/11, HSCC 2009/11, PLDI 2010, POPL 2011, SAS 2010/11, VMCAI 2009/10/11, …

Radhia Cousot, Matthieu Martel: Static Analysis - 17th International Symposium, SAS 2010, Perpignan, France, September 14-16, 2010. Proceedings Springer 2010

David Delmas, Xavier Rival: Preface. Electr. Notes Theor. Comput. Sci. 267(2): 1 (2010)

Antoine Miné, Ilaria Rodríguez-Carbonell: Preface. Electr. Notes Theor. Comput. Sci. 267(1): 1-2 (2010)

Research Contracts

Ongoing contracts

- SURVOL: FNRAE, *Logiciel de Commande Embarqués: robustesse et sécurité*, avec MIP-Univ. P. Sabatier, Toulouse, 2008 — 2011
- ASCERT: FNRAE, *Analyses Statiques Certifiées*, avec INRIA Rennes, Rocquencourt, Grenoble, 2009 — 2012
- SARDANES: *Sémantique, analyse et transformation des applications numériques embarquées synchrones*, FNRAE avec Université de Perpignan & Université de Brest, 2009 — 2012
- AbstractCell, long-term Junior ANR Chair of Excellence, J. Feret, Dec 2009 — Nov 2013.
- Abstract Interpretation and Code Obfuscation, Royal Society UK, avec Imperial College, 2010 — 2012
- ANASTASY: Airbus France, Analyse statique et dynamique, 2010 — 2014

FNRAE : Fondation de Recherche pour l'Aéronautique et l'Espace

Starting contracts

- MBAT: *Model-based Analysis and Testing of Embedded Systems*, European project, Artemis programme, with Airbus, Daimler, Volvo, Eads, Thales, Rockwell Collins, … & Univ. Munich, Univ. Aalborg …, 2011 — 2014

Submitted contract applications

- ANR (appel à projets bioinformatiques):
  - DYALOG: *Hierarchical dynamical modelling and analysis of large regulatory networks controlling cell fate decisions*, avec IBEns/Ens, Institut Curie, Université Montpellier 2, projet INRIA Contraintes, Pasteur, IBisc (Evry), Technologies avancées pour le Génome et la clinique (Marseille), 13 December 2010

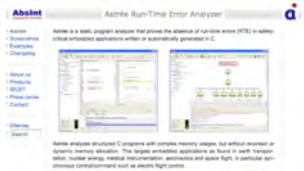
Forthcoming contract applications

- ANR:
  - THÉSÉE: *Static analysis of embedded parallel programs*, avec Airbus France, March 2011
- Europe (FP7):
  - EvolBrid: *A correct-by-evolution design and verification framework for hybrid-modeled complex embedded systems*, FP7 (7 partners), January 2011
  - Ratis: *Secure programming of embedded systems*, FP7 (8 partners), December 2011

Main industrial collaborations

AbsInt Angewandte Informatik

- Industrialization of ASTRÉE www.absint.com/astree/



- 3 full-time engineers, everyday collaboration

Daniel Kästner, Stephan Wilhelm, Stefana Nenova, Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, & Xavier Rival. ASTRÉE: Proving the Absence of Runtime Errors. In *Proc. of the Embedded Real Time Software and Systems (ERTS2 2010)*. Toulouse, France, May 19—21, 2010.

Astrium

- Verification of space software

Sagem

- Analysis of inertial unit software

O. Bouissou, E. Conquet, P. Cousot, R. Cousot, J. Feret, K. Ghorbal, E. Goubault, D. Lesens, L. Mauborgne, A. Miné, S. Putot, X. Rival, M. Turin. Space software validation using Abstract Interpretation. Proc. 1st Data Systems in Aerospace, DASIA 2009, Istanbul, Turkey, 26-29 May 2009, © Eurospace, Paris.

Airbus France

- Verification of parallel programs, mainly the FWS

Daniel Kästner, Stephan Wilhelm, Stefana Nenova, Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, & Xavier Rival. ASTRÉE: Proving the Absence of Runtime Errors. In *Proc. of the Embedded Real Time Software and Systems (ERTS2 2010)*. Toulouse, France, May 19—21, 2010.

Microsoft Research Redmond

- Verification of code contracts in Clousot (now distributed with Visual Studio Ultimate)
- Design of *scalable abstract domains* for
  - Array content analysis
  - Contract precondition inference from assertions

Patrick Cousot, Radhia Cousot, Laurent Mauborgne: A Scalable Segmented Decision Tree Abstract Domain. Essays in Memory of Amir Pnueli 2010: 72-95

Patrick Cousot, Radhia Cousot, & Francesco Logozzo. A Parametric Segmentation Functor for Fully Automatic and Scalable Array Content Analysis. POPL 2011, 105—118, 2011.

Conclusion

Ongoing work …

- Analysis of complex discrete/continuous systems:
  - Parallel programs: complex data structures, interference, real-time, scheduling with dynamic priorities (e.g. priority ceiling protocols), …
  - Biological systems
  - Closed loop analysis of control/command systems
- Verification of complex properties:
  - Security properties
  - Probabilistic properties
  - Eventuality properties

Conclusion

- Small team, smart project, great scientific ambitions :-)