Parsifal

Head: Dale Miller

INRIA Saclay & LIX, Ecole Polytechnique

Comité de Visite AERES, February 3-4, 2009

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE INRIA centre de recherche SACLAY - ÎLE-DE-FRANCE

LIX

ÉCOLE POLYTECHNIQUE

Parsifal

Personnel

Permanents: Despeyroux (CR/INRIA Sophia) ◦ Lengrand (CR/CNRS) ◦ Miller (DR/INRIA) ◦ Straßburger (CR/INRIA)
Assistant: Biercewicz (INRIA)
PhD students: Delande ◦ Guenot ◦ Nigam ◦ Viel ◦ Wirion
Post Docs: Hetzl (from T. U. Vienna)
Interns: Gazeau ◦ Poupon.

Complete PhDs: Saurin (Sep 2008) ◦ Baelde (Dec 2008).
Completed Post Docs: Gabbay, Capelletti, Méhats
Visitors ($\geq$ 1 month): Liang (Hofstra University)◦ Nadathur (University of Minnesota) ◦ Pfenning (CMU) ◦ Pimentel (Univ. Federal de Minas Gerais, Brazil)

Summary of Productivity

Journals (6): Logical Methods in CS, ACM Trans. on Comp. Logic, Info & Comp, TCS, Logic Colloq. [Another 5 submitted]

Conferences (15): CiE, CSL (x 4), IJCAR (x 2), LICS (x 3), LPAR (x 2), PPDP, RTA, TCS [1 invited, 2 more submitted]

Workshop (9): CLC, ESHOL, GaLoP (x 2), Hybrid, SOS, LFMTP (x 3)

Other (11): technical reports, manuals, book chapters, lecture notes, articles in an encyclopedia and in newsletters

Software systems: Bedwyr, Taci. Also: Abella from U. Minnesota

Teaching: X (Lengrand & Miller), ESIEA (Lengrand), MPRI (Miller), (09, Miller), ESSLLI'06 course (Straßburger)

Funded Projects

INFER "Theory and Application of Deep Inference" (ANR Blanc) between LIX, PPS, LORIA. Started Jan 2007 (65Keuros for three years).

Mobius (Mobility, Ubiquity and Security) is part of FP6-2004-IST-FETPI on Proof carrying code (136Keuros for three years).

Slimmer, an INRIA "Equipes Associées", funds collaboration with Nadathur's team at the University of Minnesota since 2006. Currently at 10Keuros a year.

Types contract is a continuation of a series of Types projects dating back to 1992 (some travel funds, completed 04/08).

Various travel grants (PAI). Active: Bern, Vienna, Taiwan. Completed: Madrid.

Visibility

Program Committees: CADE05/07, CSL05/08, ESHOL08, FLOPS08, FOSSACS08, FSTTCS06, LAM08, LFMTP06/07, LPAR05/06, LSFA08, PPDP08, TCS08, TFIT06, WoLLIC07

Editorial boards: ACM Trans. on Comp. Logic, J. of Applied Logic, J. of Functional and Logic Prog., J. of Logic and Comp., Theory and Practice of Logic Prog.

Invited talks: APS08 (Qatar), SOS/CLC08 (Iceland), WFLP08 (Siena), LFMTP08 (Pitt.), IJCAR06 (Seattle), Geometria della Logica 2006 (Rome), Algebraic Process Calculus 2005 (Bertinoro), Structure and Deduction 2005 (Lisbon), TFIT05 (Taiwan)

Awards: 2007 Ackermann Award (Lengrand)

Evaluations: 10 PhD committees, one habilitation committee

Objective

To develop and exploit proof theory and type theory to support the specification and verification of computation. The last 20 years has witnessed exciting ideas in proof theory and computation: e.g., linear logic and deep inference.

We attack this objective via four avenues.

- Research into proof and type systems: eg, identity of proof, proofs-as-certificates, automated deduction, etc
- Design new logical principles, new proof systems, and new theorem proving environments
- Implement prototype systems
- Apply logics and systems to examples.

Research emphasis

Use elements of logic (formulas, types, proofs, etc) as directly as possible to encode computational elements.

We try to bring computation and proof theory as close to each other as possible.

- We gain strong methods for reasoning about computation.
- We discover new possibilities for proof theory.

Some work attempts to equate logic formulas directly with algorithms (the "real" dream $\mathit{Logic} = \mathit{Algorithm}$ from logic programming).

We search for more intimate and targeted connections between logic and the things specified.

Research emphasis

This approach stands in contrast to axiomatizing computations system via *theories*, which, when backed up by powerful provers (ACL2, Coq, etc), yields many success stories.

The focus is not on modeling directly what is *true* but what are the *dynamics*.

Of course, we also look at conventional notions of classical and intuitionistic truth, but with an eye to improve the structure and dynamics of proof search.

Principal research themes

Deep inference: alternative to sequent calculus; framework for proof complexity and non-determinism

- Find deep inference system for richer logics.
- Develop focusing-like restrictions to control the great degree of non-determinism in these proofs.
- Apply results to find new axiomatic description of categories of proofs for various logics.

Formalizing the meta-variables implementation of a proof search

- meta-variables are critical in proof search implementation as representations of incomplete proofs
- relating meta-variables to different kinds of syntax: nominal-based and higher-order abstract syntax

Principal research themes

Stochastic reasoning in (a modal extension of) linear logic

- Application: biochemical reactions in molecular biology:
  - need to model state change (molecules interact) and (probability distribution over possible) delay
- Develop: a logic-based instead of a process-based framework
- Results:
  - HyLL, an hybrid linear logic, equipped with a focused sequent calculus; used to adequately encode stateful systems
  - Example: captures stochastic π-calculus; adding formal logical reasoning
  - possibility of automation of reasoning directly on the specifications (instead of on traces of simulations)

Topic 1: Reasoning about operational semantics

Specification of many computation systems often employ

- relations: eg, SOS for λ-calculus, π-calculus, etc,
- bindings in syntax,
- resource accounting: references, coordination (Petri nets, Linda)

Extensional and functional systems (Coq, NuPRL, Isabelle/HOL, etc) do not directly treat these features.

We developed new designs and theoretical results using:

- various subsets of higher-order linear logic,
- generic judgments, ∇-quantification, and
- two level architecture to separate reasoning from specification.

Topic 1: Reasoning about operational semantics

Systems work

- Bedwyr (LIX/Minnesota): model-checking as deduction, includes ∇-quantification, tabling. A model checker for the (finite) π-calculus.
- Abella (Minnesota/LIX): interactive prover for inductive and coinductive theorem proving. Simple treatment of the POPLmark challenge problems and much more.

Results:

- declarative specifications of many computational systems, including the π-calculus
- complete validation of the underlying theory and designs
- motivated new theory and designs to consider

Topic 2: Focused proof systems

Fundamental and new normal form for sequent calculus proofs.
Many on the team have extended and applied this style of proof.

- critical for any *proof search* activity: logic programming, model checking, theorem proving
- relates to term representations, adequate encodings, and canonical forms
- the exponentials of linear logic have "bad" focusing behavior: can we do without them?
- a new, general normal form at the core of (computational) logic should have huge impacts

Topic 2: Focused proof systems: Specific results

- new focusing proof systems for intuitionistic/classical logic, and fixed points (induction/coinduction)
- a neutral approach to proof and refutation
- replaced exponentials with fixed point or by mixing in classical logic: strong logics with good focusing behavior
- new approach to *canonical* proofs and proof identity
- inspires new connections between game semantics and proofs
- by tuning one focused proof system, we can account for natural deduction, tableaux, sequents, and Herbrand disjunctions.

The Taci proof system being developed currently aims to use focusing proof theory to develop a new automated theorem prover.

Plans and Prospects

Continue our model of theory / design / prototype / examples.

- Find new syntax for proofs; revisit the *identity of proofs*; relate non-determinism in proof search and size of proof.
- New approaches to unifications:
  - formalize meta-variables and partial proofs
  - provide solid foundations for unification and its "dual"
- Reorganize parts of traditional theorem proving and SAT solvers using focusing
- Build and enhance a single prover, incorporating Abella's scope and Taci's automation (also Bedwyr). The treatment of lemmas (tabling) is a central concern.
- Develop methodology for reasoning about operational semantics

Plans and Prospects

Declarative organization of interaction in proof search

- decision procedures for specific domains following the SAT-Modulo-Theory architecture
- some proof-search mechanisms (in, e.g., Coq) that interact with certified decision-procedures (say, in arithmetics)

Develop designs and implementations for a semi-automated prover of type theory based on sequent calculus.

Plans and Prospects

The team is currently heavy on “theory” and “design” and light on “implementation” and “application”.

- Our implementation effort has been largely directed by one PhD student and our close collaboration with the University of Minnesota.
- Currently, our prototypes are just the size of “one PhD thesis”.
- We are hopeful to hire a junior researcher with experience and interest in doing implementations (in addition to having a strong theoretical background).