Team: CAPP
Scientific leader: R. Echahed
Reporting Period : January 1^{st}, 2005 to September 30^{th} 2009

Web site: `http://equipes-liglab.imag.fr/capp/`
Parent Organizations: Université Grenoble 1, Université Grenoble 2, Grenoble INP, CNRS, INRIA

Contents

1 General presentation

Scientific and Technological Project

Research on the foundations of programming and on automated deduction very often leads to the development and investigation of computational models that formalize the considered programming paradigms and logics. This requires the development of notations, languages, mathematical structures, logics and other theoretical tools specifically tailored to investigate different aspects of the underlying model. Among these aspects of interest are the expressive power of the models, the way they behave, the decidability and complexity issues, and the development of automated procedures for checking the validity of the computations and/or for detecting errors. These researches also lead to the development of hardware or software artifacts that implement or simulate these calculi, so that they can be applied to practical problems, in which their specific features may be of considerable interest.

Considering the proliferation of interactive computing devices with very different natures and purposes , we are faced with increasingly complex and conflicting issues of design, efficiency, control, quality, security... Moreover, the development of physics and biology has inspired non-standard models of computation with several interesting properties that can be used for the encoding of data and for transforming and transferring information. These models raise the question of the relationship between natural phenomena and computing science. We need a deeper understanding of the nature of computation, of how it can be realized, how it can be specified, and how it is possible to reason about it. These aspects of computation are closely related to each other, and are central to tackling the issues mentioned above.

The CAPP team contributes to the development of different aspects of standard and non-standard computational models with a focus on algorithms, programs and proofs.

Team History

The CAPP group was founded in 2004. Its members came from three different groups working respectively on proof techniques, foundations of multiparadigm programming and quantum computation.

2 Team Composition

Permanent Researchers				
Name	First name	Function	Institution	Arrival date
Echenim	Mnacho	Associate Professor	GINP	Sep 07
Caferra	Ricardo	Associate Professor	GINP	Jan 04
Arrighi	Pablo	Associate Professor	UJF	Sep 05
Prost	Frédéric	Associate Professor	UJF	Jan 04
Puitg	François	Associate Professor	UJF	Jan 04
Jorrand	Philippe	Research Director (EMERITE)	CNRS	Jan 04
Boy de la tour	Thierry	Research Scientist	CNRS	Jan 04
Mhalla	Mehdi	Research Scientist	CNRS	Jan 06
Peltier	Nicolas	Research Scientist	CNRS	Jan 04
Echahed	Rachid	Research Scientist	CNRS	Jan 04

Doctoral Students				
Name	University	Supervisors	Funding (sources and dates)	Date of first registration
Fargetton R.	UJF	Jorrand Philippe, Arrighi Pablo	MENRT Oct 07 - Sep 11	Oct 07
Diaz caro A.	UJF	Peltier Nicolas, Arrighi Pablo	Oct 08 - Oct 11	Oct 08
Aravantinos V.	GINP	Peltier Nicolas , Caferra Ricardo	MENRT Sep 07 - Oct 10	Sep 07
Bensaid H.	GINP	Caferra Ricardo, Peltier Nicolas	Other Oct 07 - Oct 12	Oct 07

Habilitation Theses defended during period				
Name	First name	Defense date	University	Current position
Peltier	Nicolas	01.06.2007	GINP	CR1-CNRS
Arrighi	Pablo	15.06.2009	UJF	MdC-UJF

Past team members

Past Members Oct. 2005-Oct. 2009					
Name	First name	Position	Employer	Arrival date	Departure date
Jorrand	Philippe	Research Director	CNRS	Jan 07	Aug 07
Kashefi	Elham	Research Scientist	CNRS	Oct 07	Jan 09

Past Doctoral students	
Name	First Name
Pedrix	Simon
Lalire	Marie
Echenim	Mnacho
Countcham	Prakash

Past post-doctoral researchers, engineers and visitors					
First name	Name	Function	Date of arrival	Date of departure	Home Institution
Julien	Degorre	Post-doc	Feb 08	Jun 09	CNRS
Jonathan	Grattage	Post-doc	Sep 07	Feb 09	CNRS
Vincent	Nesme	Visitor	2009-03-26	2009-03-27	Post-doctoral Researcher (Braunschweig)
Marc	Kaplan	Visitor	2008-12-09	2008-12-11	PhD student, LRI
Sébastian	Gambs	Visitor	2008-12-04	2008-12-05	Postdoctoral researcher, Toulouse
Lionel	Vaux	Visitor	2008-11-07	2008-11-07	Postdoc at the Institut de Mathématiques de Luminy
Gilles	Dowek	Visitor	2008-11-07	2008-11-07	Professor at l'École polytechnique
Benoît	Valeron	Visitor	2008-11-03	2008-11-07	LIX Postdoc
Howard	Barnum	Visitor	2008-09-29	2008-10-03	Team Leader, Los Alamos National Laboratory
Benoît	Valiron	Visitor	2008-04-07	2008-04-13	Researcher (Ottawa)
Simon	Perdrix	Visitor	2008-04-07	2008-04-07	Research Officer (Oxford)
Vincent	Nesme	Visitor	2008-04-07	2008-04-08	Researcher (Braunschweig)
Damian	Markham	Visitor	2008-04-03	2008-04-09	CNRS Research Fellow (PPS Paris 7)
Minh-Dung	Dang	Visitor	2008-03-13	2008-03-14	Ph.D. student, Telecom Paris
Damian	Markham	Visitor	2008-03-08	2008-03-14	CNRS Research Fellow (PPS Paris 7)
Alejandro	Díaz-Caro	Visitor	2008-03-06	2008-03-15	Student, Rosario National University, Argentina
Jiannis K.	Pachos	Visitor	2008-02-06	2008-02-09	Research Fellow of the Royal Society - University of Leeds

continued on next page

continued from previous page					
Past post-doctoral researchers, engineers and visitors					
First name	Name	Function	Date of arrival	Date of departure	Home Institution
Lionel	Vaux	Visitor	2008-01-16	2008-01-18	ATER, Institut de Mathématiques de Luminy
Damian	Markham	Visitor	2008-01-14	2008-01-22	CNRS Research Fellow (PPS Paris 7)
Anne	Broadbent	Visitor	2008-01-13	2008-01-19	Ph.D. student, University of Montreal
Ellie	D'Hondt	Visitor	2008-01-10	2008-01-25	FWO Post-doc
Vincent	Nesme	Visitor	2008-01-07	2008-01-11	Post-doctoral Researcher (Braunschweig)
Jaques	Patricia	Visitor	2007-12	2007-1	CAPES BRESIL
Song	Fangmin	Visitor	2007-12-11	2007-12-14	Professor (University of Nánjing)
Neil	de Beaudrap	Visitor	2007-11-27	2007-12-09	PhD Student (ICQ, University of Waterloo)
Simon	Perdrix	Visitor	2007-11-26	2007-11-27	Research Officer (Oxford)
Julien	Degorre	Visitor	2007-11-15	2007-11-16	European CNRS Research Fellow
Echenim	Mnacho	Visitor	2007-4	2007-7	autre

Evolution of the team

CAPP group has been successful in hiring four new researchers: P. Arrighi (2005) and M. Echenim (2007) as Maîtres de conférence and M. Mhalla (2005) and E. Kashefi (2007) as Chargés de recherche (CNRS). Ph. Jorrand is Directeur de recherche *émérite* since 2007. E. Kashefi is on leave at the University of Edinburgh since January 2009.

3 Research Themes

3.1 Models of computation

List of participants: P. Arrighi, R. Echahed, R. Fargetton, Ph. Jorrand, M. Mhalla, F. Prost

Scientific issues and positioning of the team:

There is a huge gap between sheer reality and theory especially in the field of computer science. There is an ongoing challenge to define, develop and study models of computation that capture particular aspects of reality and provide a useful abstraction. We have worked on several models of computation that build such bridges: The quantum graph states model is based on graph theory to exploit entanglement for quantum computation, the categorical approach to graph rewriting can be used to model pointer issues in a mathematically neat way, quantum cellular automata model quantum computation in a very natural way and thus may be a good candidate for quantum computer construction, quantum lambda-calculi together with their typing systems are developed in order to both understand and manage quantum programs using extensions of the functional programming paradigm.

Key references: [40, 12, 44, 77, 56, 29, 51, 13, 28]

Major results Jan. 2005-Oct. 2009:

We have defined garbage collection in terms of functors using our categorical approach to graph rewriting. This high level approach has made the design of a simple, yet powerful static analysis for memory usage of programs with pointers possible. We have studied and proved several equivalences between quantum cellular automata and quantum circuit and established universality result for quantum cellular automata. We have proved equivalences between axiomatic and operational quantum cellular automata definitions. We have developed several typing systems for quantum lambda calculi. We have shown that full linearity is not mandatory, and proposed simpler type systems in which linearity is only required for purely quantum parts. Based on these type systems we have developed a Hoare-like logic in order to reason about the entanglement of quantum bits.

Perspectives:

There are two main lines of evolution to be considered. The first one relies on further studies of already defined computational models: e.g. investigating how to use graph states for communication protocols, what type system/logic can be inferred for quantum lambda calculi, how to define universal quantum cellular automata with fewer states. The second one is the definition of new model of computation in order to grasp different aspects of reality: new binders/type constructors may be required to obtain a uniform approach to typing for quantum lambda calculi, new graph rewriting frameworks allowing more operations (cloning for instance) could be investigated as well.

3.2 Algorithmics

List of participants: Thierry Boy de la Tour, Mnacho Echenim, Mehdi Mhalla.

Scientific issues and positioning of the team:

The algorithmic problems we consider lie within two categories: graph theoretic algorithms for quantum measurement based computing (or using the quantum circuit model) and group theoretic algorithms for automated reasoning in the presence of symmetries (or isomorphisms). These problems involve interesting complexity classes, such as the *graph isomorphism* class GI (intermediate between P and NP). In measurement based quantum computing, the computation is performed by measuring in a sequence several qubits one at a time, starting from a quantum state represented by a so-called *graph state*. Algorithmic and complexity issues concern both the preparation of these initial states and their use for computation (by sequences of measurements).

Key references: [60, 50, 11, 35, 15, 17, 40]

Major results Jan. 2005-Oct. 2009: We have analyzed the complexity in time and space (number of qubits) of preparing graph states in different models of computation. As not all graph states permit to perform a proper computation (i.e. simulate a unitary transformation), we provided algorithms to test this property on a given graph state and also to provide the time complexity of computing with it (i.e. measuring qubits). We have also investigated the complexity in the quantum circuit model of several standard graph problems (connectivity, shortest path,..) for which we were able to characterize exactly the quantum complexity. We defined a so-called *unify-stable* class of linear permutative equational theories together with an exponential unification algorithm, and proved that testing membership of a theory to this class, considered modulo semantic equivalence, belongs to the Luks complexity class (slightly simpler than GI). We also proved the undecidability of unification modulo unrestricted linear permutative equational theories.

Perspectives: We are currently investigating the use of graph states for secret sharing, in protocols where some information is shared among several parties and where we want to provide means to access the information only to a subset of the participants. We also intend to devise a way of extracting a unify-stable presentation from a given set of equational axioms, in order to feed it to our unification algorithm and eliminate the symmetries they would otherwise generate, in a way that would maximize the number of eliminated symmetries.

3.3 Rewriting

List of participants: P. Arrighi, R. Caferra, A. Díaz-Caro, R. Echahed, N. Peltier, F. Prost

Scientific issues and positioning of the team:

Rewriting techniques constitute a major area of theoretical computer science. They play an important rôle in the foundation of very high level programming languages and contribute to the development of a large number of theorem provers. The CAPP team is developing new rewriting techniques with the aim of defining a unified rule-based framework dedicated to computing with general data-structures, and particularly those built by means of pointers. This line of research is central to the ANR project ARROWS led by our group. Another aspect of our research on rewriting techniques consists in integrating untyped lambda calculus and linear algebra encoded as a term rewrite system. This line of research is motivated by the encoding of quantum circuits. We are also considering program properties related to the investigated rewrite systems.

Key references: [5, 7, 38, 37, 52, 57, 64, 63, 61, 62]

Major results Oct. 2006-Oct. 2009:

We have proposed a general framework for handling rewrite rules operating on graphs that encode data-structures with pointers. We have defined a new simplified algorithmic approach to graph transformation, based on elementary actions on graphs. This algorithmic approach corresponds to an algebraic approach we also have proposed for data-structure transformation. We have investigated the confluence property for the proposed class of graph rewrite systems. This property is often required to ensure the uniqueness of the computed values and is undecidable in general. We have devised a new subclass of graph rewrite systems for which we have shown the confluence of rewriting. Since confluence is not guaranteed in the general case (even in the presence of orthogonal systems), we have introduced the notion of graphs with priority (ordering over nodes). Such priorities allow the programmer to control the transformation of graphs if necessary. The use of total priority orderings makes rewriting purely deterministic, which is not always efficient in practice. To overcome this issue, we have also shown how to define more flexible strategies, which yield shorter derivations and may avoid useless rewriting steps. We have also presented particular graph rewrite strategies which rewrite only needed redexes. In addition we have devised a new narrowing procedure capable of solving goals and synthesizing solutions with cyclic graphs. Furthermore, regarding our proposal of the integration of lambda calculus with linear algebra, we have succeeded in showing the confluence of the proposed calculus and we have proposed a typing system of this calculus recently.

Perspectives:

The class of data-structure rewriting systems is very promising. We intend to pursue our investigation of the properties of this class. The notion of *interference* has been used either in defining new rewrite strategies in presence of graphs with priorities or in investigating security properties such as *information leakage* in the presence of (term and process) rewrite systems. We intend to improve our way to infer interference between nodes and investigate new ways to prove properties of graph transformation. We are also investigating logics for denoting quantum programs and reasoning about them – hopefully allowing a better understanding of the inner nature of quantum information. By the Curry-Howard isomorphism, these logics should arise from the study of the type system of quantum programming languages (e.g. the linear algebraic λ-calculus).

3.4 Methods for testing satisfiability

List of participants: H. Bensaid, T. Boy de la Tour, R. Caferra, M. Echenim, N. Peltier

Scientific issues and positioning of the team: Disproving a formula (i.e. proving that it is not valid) is useful – even essential – for various applications, ranging from program verification to computer-aided mathematics. This enables for instance to detect bugs in programs. This problem is a very hard one, theoretically infeasible in general, and has been recognized as essential since the very beginning of research in computer science. The identification of sufficiently expressive classes of formulas for which decision procedures exist induces a quantitative leap in the amount of information obtained about the disproved formula. The CAPP team was among the pioneers on these topics and has published a book that is a reference on automated model building. The group is still conducting innovative research on satisfiability detection.

Key references: [2, 45, 18, 23, 42, 6, 4, 48, 49, 47]

Major results Oct. 2006-Oct. 2009: New techniques for constructing counterexamples have been devised. Some rely on algorithmic group theory to discard isomorphic models, others enumerate finite representations of infinite models. It is sometimes sufficient to guarantee that a formula is not provable, without exhibiting a counterexample. Thus termination results were proven for various resolution/paramodulation strategies, especially on classes of formulas that come from software verification problems, where non-ground clauses axiomatize theories of data structures: Satisfiability Modulo Theories (SMT) problems. To enforce termination on more general classes, methods for detecting lemmas that are based on the regularities of the search space have also been implemented.

Perspectives: The automatic generation of lemmas will potentially be useful to prove inductive theorems by using implicit induction (or, equivalently, proofs by consistency). However, expressivity is not the only issue that needs to be addressed for this topic, and new techniques are being devised to combine generic decision procedures with more basic tools capable of efficiently handling the boolean part of potentially large formulas. This will be particularly useful to solve SMT problems efficiently, and this work will be followed by research on the application of automated model building techniques to SMT problems and investigations of the counter-examples that are best suited to solve these problems.

3.5 Extensions of proof procedures

List of participants: V. Aravantinos, H. Bensaid, R. Caferra, R. Echahed, M. Echenim, N. Peltier

Scientific issues and positioning of the team: The power of a proof procedure is related to the way the logical information is represented. More expressive formalisms (and logics) yield shorter proofs (e.g. resolution proofs are non elementarily longer than the ones obtained with a full logical calculus). Unfortunately, the most powerful (non analytic) calculi are not suitable for mechanization. We try to overcome this problem by proposing languages allowing a better representation of logical information, and by extending efficient, practically successful, proof procedures in order to handle these languages. The goal is to improve efficiency, to extend the expressive power (in particular to capture reasoning underlying new computational models such as quantum computing), to share similar inference steps or to avoid divergence.

Key references: [27, 24, 25, 22, 55, 14, 9, 41, 10, 30, 62, 5]

Major results Oct. 2006-Oct. 2009: We have designed resolution-based proof procedures operating on more compact representations of clause sets, which reduce the length of the proofs by an exponential or even double exponential factor. A clausal logic allowing to handle term-graphs has been defined. We have also investigated proof procedures based on term schematisation languages (i.e. formalisms denoting infinite sequences of iterated terms). We have proposed new schematisation languages with extended expressive power and good computational properties. On the practical side, we have developed the first running theorem prover that is capable of handling term schematisations.

Perspectives: We are currently investigating logics for handling formulas/proofs schemas, especially iteration schemas with indexed symbols that turn out to be extremely useful for the formalization of mathematical proofs (to express infinite proof sequences). We plan to launch a cooperation project on this subject with the Theory and Logic Group from the TU Vienna (ANR-FWF project "ASAP", submitted).

4 Contracts and grants

4.1 External contracts and grants (Industry, European, National)

- QICS, 6th European Framework, Jan. 2007 - Dec. 2009, "Foundational Structures in Quantum Information and Computation"
- ARROWS, ANR-SSIA, 2005 - 2009. "Safe Pointer-Based Data Structures, graph transformation".
- France-Japan CNRS-JST ICT agreement, Jan. 2008 - Dec. 2010, "One-way quantum computation"
- CNRS-ST2I projet PEPS, 2007, "Calcul quantique par mesures projectives à partir des géométries finies"
- France-Canada Research Foundation Grant, May 2005 - Aug. 2007, "Computational properties of quantum information"

4.2 Internal Funding

- Bonus Qualité Recherche (BQR), "Machines quantiques abstraites", University of Grenoble (UJF), 2005-2006
- Q&S (Calculs quantiques et symboliques), projet IMAG, 2005-2006

5 Principal International collaborations

With Joint publications

- University at Albany SUNY (Paliath Narendran)
- University of Verona (M.P. Bonacina)
- National Security Agency (Mark Heiligman)

- Universite of Calgary (Peter Hoye)
- University College London (Dan Browne)
- University of Hannover (R.F. Werner)
- University of Edingurgh (E. Kashefi)
- University of Valladolid (Manuel Gadella)
- NEC Laboratories America, Princeton,(J. Roland)

With grants

- University of Oxford (Samson Abramsky and Bob Coecke)
- University of Bristol (Richard Jozsa)
- University of York (Sam Braunstein)
- TU Braunschweig (Reinhard Werner)
- University of Innsbruck (Hans Briegel)
- McGill University (Prakash Panangaden)
- National Institute of Informatics (NII), Japan, (Kae Nemoto)

6 Visibility, Scientific and Public Prominence

6.1 Contribution to the Scientific Community

Organisation of International Workshops with programme committees

- STRATEGIES'06, Boy de la Tour PC co-chair, Seattle, 2006
- WFLP07 Functional and Logic Programming, R. Echahed, PC chair, Paris, 2007
- FTP 2009, First-Order Theorem Proving, N. Peltier, PC co-chair, Oslo, 2009

Organisation of Workshops without programme committees

- Symbolic Calculi, R. Echahed and F. Prost co-organizers, Grenoble,December 2005
- Information et communication quantique , P. Arrighi organizer, June 2007
- Foundational principles in Quantum Information, P. Arrighi organizer, Grenoble, June 2009

Program committee members

- *WCFLP 2005 Curry and Functional and Logic Programming*, R. Echahed, 2005
- *SecReT 2006, First International Workshop on Security and Rewriting Techniques*. R. Echahed, 2006
- *SBMF 06, The Brazilian Symposium on Formal Methods*, R. Echahed, 2006
- *17th International Workshop on Functional and (Constraint) Logic Programming*, R. Echahed, 2008
- *UNIF 08, 22nd International Workshop on Unification*, R. Echahed, 2008
- *GCM2008, 2nd International Workshop on Graph Computation Models 2008*, R. Echahed, 2008
- *PPDP 2009, 11th International ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming*, R. Echahed, 2009
- *RTA 2009 20th International Conference on Rewriting Techniques and Applications*, R. Echahed, 2009
- *TERMGRAPH 2009, 5th International Workshop on Computing with Terms and Graphs*, R. Echahed, 2009
- *WFLP 2009, 18th Int'l Workshop on Functional and (Constraint) Logic Programming*, R. Echahed, 2009
- *FTP 2005, International Workshop on First-Order Theorem Proving*, N. Peltier, 2005
- *FTP 2007 International Workshop on First-Order Theorem Proving*, N. Peltier, 2007
- *TABLEAUX 2009, 18th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods*, N. Peltier, 2009

National expertise

- AeRES expert for the evaluation of the strategy of the University of Mulhouse, P. Arrighi, June 2008.
- CIR expert for the evaluation of private sector research entitling to tax reductions (Three companies), P. Arrighi, 2006-2008.

6.2 Prizes and Awards

- M. Echenim. Grenoble INP PhD thesis award 2005.
- S. Perdrix. Grenoble INP PhD thesis award 2006.

7 Educational Activities

Teaching

- L1 Level
  - Unix and C, UJF (P. Arrighi)
  - Logics, UJF (P. Arrighi)
  - Algorithmic and Programming, UJF (F. Puitg)
  - Programming techniques and computer science methods, UJF (F. Puitg)
  - Functional programming, UJF (F. Prost)
  - Operating Systems
- L2 Level
  - Languages and Automata, UJF (P. Arrighi)
  - Introduction to logic, UJF (F. Puitg)
  - Automata theory, UJF (F. Prost)
- L3 Level
  - Logic and formal systems, UJF (N. Peltier)
  - Logic for computer science, Ensimag (R. Caferra)
  - Object Oriented Programming, UJF (P. Arrighi)
  - Designing internet applications, UJF (F. Puitg)
  - Introduction to networks and telecommunication, Ensimag (M. Echenim)
  - Formal Language and automata theory, Ensimag (M. Echenim and R. Echahed)
  - Introduction to computability, Ensimag (R. Echahed)
- M1 Level
  - Logic and the automation of reasoning, Ensimag (R. Caferra)
  - Object Oriented Programming, UJF (P. Arrighi)
  - Project supervision, UJF (F. Puitg)
  - Logica and constraint programming, UJF (F. Puitg)
  - Compiler theory, Ensimag (M. Echenim)
  - Computability, complexity, UJF (F. Prost)
  - Logic for mathematicians, Prépa Agreg, UJF (F. Prost)
  - Introduction to Rewrite Techniques, UJF (R. Echahed)
- M2 Level
  - Logic and the automation of reasoning, UJF-Ensimag (T. Boy de la Tour and N. Peltier)
  - Quantum information, causality and cellular automata, UJF (P. Arrighi)
  - Quantum cryptography, UJF (P. Arrighi)
  - Quantum computation, UJF (P. Arrighi)
  - Computer security, UJF (P. Arrighi)
  - Machine Languages, UJF (F. Puitg)
  - Distributed software project, Ensimag (M. Echenim)
  - Introduction to the .NET framework, Ensimag (M. Echenim)
  - Evaluation of financial structured products, Ensimag (M. Echenim)
  - Advanced programming, UJF-INPG (R. Echahed)
- PhD Level
  - Introduction to theoretical physics, UJF (P. Arrighi)
  - History of computer science, UJF (F. Prost)

Academic responsibilities

- Co-responsibility of the "option FICV (Fondements de l'Informatique: Conception et Validation)" of the M2R Informatics, M2 level,UJF-INPG (R. Echahed)
- Responsibility of the Compiler project, M1 level, UJF (P. Arrighi)
- Responsibility of the research and industrial internships, M1 level, UJF (P. Arrighi and F. Prost)
- Responsibility of the "Algorithmic and functionnal programming" class, L1 level, UJF (F. Puitg)
- Responsibility of the computer science correspondence (L1/L2/L3) at the CSJF drôme ardèche (F. Prost)
- Cooperation with the University of Bamako for the development of a FAST Bachelor degree (F. Prost)
- Internship supervision, Ensimag (M. Echenim)
- Internship supervision, UJF (F. Puitg)

8 Industrialization, patents and technology transfer

Floralis (www.floralis.fr/us/) project employing two software engineers full-time and aiming at a transfer of technology, P. Arrighi, 2009-2010.

9 Self-Assessment

- *Strengths* Despite the recent foundation (2004) of our team, it already enjoys an international recognition in its different lines of research. We have been successful in attracting several visitors and in animating a lively seminar (Capp-Café). Furthermore, most of our research topics are original and are not tackled by other French teams. These topics are risky and challenging but allow us to gather new and specific expertise.
- *Weakness* Currently, only four students are preparing their PhDs in our group (three of them are expected to defend their theses in 2010). We are having obvious difficulties to attract students preparing their Master's project in theoretical computer science, despite our involvement in the organization of the theoretical computer science courses of the Master2R programme in informatics. This difficulty is increased by the fact that courses cannot take place unless there are at least twelve participating students.

10 Perspectives for the research team

CAPP is one of the very few French research teams that conducts basic research on original models of computations such as quantum computing models, graph rewriting systems or new proof techniques in presence of enhanced formula representation. In the forthcoming years, we plan to develop the following directions. Our research areas contribute to the following flagship domains of the LIG : Theoretical Computer Science, Security and Embedded Systems.

- *Models of computation*: We plan to deepen our investigations regarding quantum models of computation. We will study flow in quantum information with the aim of covering a very general set of possible network tasks (so called graph-state schemes), incorporating computation, error correction, secret sharing and other protocols in one general framework. We plan also to explore new enquiries regarding quantum cellular automata. We will also continue to investigate integration of lambda-calculus and term rewriting techniques with the purpose of designing a high-level typed framework to write and analyse quantum and classical programs.
- *Rewriting*: Our ways of tackling graph transformations, using both algebraic and algorithmic approaches are original and depart from existing methods. They are appropriate to define semantics of modern declarative languages handling complex data structures. Our approaches are being used by other researchers such as S. Antoy (Portland, Or) or M. Hanus (Univ. Kiel). A prototype based on our algorithmic approach has been also implemented by Pareo team at LORIA as part of the TOM system. We plan to pursue our efforts in investigating the theory and practice of graph transformation. This research is currently suffering from the lack of human resources. We wish to fill this gap as soon as possible.
- *Proofs*: We will continue our efforts to enhance reasoning capabilities of theorem provers. Our goal is not only to improve their efficiency, but also to introduce qualitative improvements by modeling reasoning techniques

that are commonly used by human beings but that are neglected by existing systems, e.g. analogy reasoning, use of symmetries, schematisation of terms and formulas, ...

11 Publications

International peer reviewed journal [ACL]

2009

[1] M. P. Bonacina and M. Echenim. Theory decision by decomposition. *Journal of Symbolic Computation*, pages 1–42, June 2009. to appear.

[2] N. Peltier. Constructing Infinite Models Represented By Tree Automata. *Annals of Mathematics and Artificial Intelligence*, 2009.

[3] F. Prost. Twilight Chess - A Chess Variant Designed to Rehabilitate Human vs. Computer Challenge. *International Computer Games Association Journal*, 32(2), 2009.

2008

[4] M. P. Bonacina and M. Echenim. On Variable-inactivity and Polynomial T-Satisfiability Procedures. *J. Log. Comput.*, 18(1):77–96, 2008.

[5] R. Caferra, R. Echahed, and N. Peltier. A Term-Graph Clausal Logic: Completeness and Incompleteness Results. *Journal of Applied Non-Classical Logics*, 18(4):373–411, 2008.

[6] R. Caferra and N. Peltier. Accepting/Rejecting Propositions from Accepted/Rejected Propositions: a Unifying Overview. *International Journal of Intelligent Systems*, 23(10):999–1020, 2008.

[7] R. Echahed. On Term-Graph Rewrite Strategies. *Electr. Notes Theor. Comput. Sci.*, 204:99–110, 2008.

[8] P. Jorrand and S. Perdrix. Towards a Quantum Calculus: (Work in Progress, Extended Abstract). *Electr. Notes Theor. Comput. Sci.*, 210:75–83, 2008.

[9] N. Peltier. Bottom-up Construction of Semantic Tableaux. *Journal of Logic and Computation*, 2008.

[10] N. Peltier. Extended Resolution Simulates Binary Decision Diagrams. *Discrete Applied Mathematics*, 156:825–837, 2008.

2007

[11] T. Boy De La Tour and M. Echenim. Permutative Rewriting and Unification. *Information and Computation*, 25(4):624–650, Apr. 2007.

[12] D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix. Generalized Flow and Determinism in Measurement-based Quantum Computation. *New Journal of Physics*, 9:250, 2007.

[13] D. Duval, R. Echahed, and F. Prost. Modeling Pointer Redirection as Cyclic Term-graph Rewriting. *Electr. Notes Theor. Comput. Sci.*, 176(1):65–84, 2007.

[14] N. Peltier. A Resolution Calculus with Shared Literals. *Fundamenta Informaticae*, 76(4):449–480, 2007.

2006

[15] C. Dürr, M. Heiligman, P. Høyer, and M. Mhalla. Quantum Query Complexity of Some Graph Problems. *SIAM J. Comput.*, 35(6):1310–1328, 2006.

[16] S. Gravier, P. Jorrand, M. Mhalla, and C. Payan. Quantum Octal Games. *Int. J. Found. Comput. Sci.*, 17(4):919–932, 2006.

[17] P. Høyer, M. Mhalla, and S. Perdrix. Resources required for preparing graph states. In *ISAAC*, pages 638–649, 2006.

[18] N. Peltier. Some Techniques for Proving Termination of the Hyperresolution Calculus. *Journal of Automated Reasoning*, 35:391–427, 2006.

[19] S. Perdrix and P. Jorrand. Classically controlled quantum computation. *Mathematical Structures in Computer Science*, 16(4):601–620, 2006.

[20] S. Perdrix and P. Jorrand. Classically-controlled Quantum Computation. *Electr. Notes Theor. Comput. Sci.*, 135(3):119–128, 2006.

2005

[21] É. Duchene, S. Gravier, and M. Mhalla. Around Wythoff's game. *Electronic Notes in Discrete Mathematics*, 22:167–172, 2005.

[22] N. Peltier. A Resolution Calculus for Shortening Proofs. *Logic Journal of the Interest Group in Pure and Applied Logics*, 13:307–333, 2005.

[23] N. Peltier. Representing and Building Models for Decidable Subclasses of Equational Clausal Logic. *Journal of Automated Reasoning*, 33(2):133–170, 2005.

International peer-reviewed conference proceedings [ACT]

2009

[24] V. Aravantinos, R. Caferra, and N. Peltier. A DPLL Proof Procedure for Propositional Iterated Schemata. In *Workshop "Structures and Deduction 2009" (ESSLI)*, 2009.

[25] V. Aravantinos, R. Caferra, and N. Peltier. A Schemata Calculus For Propositional Logic. In *18th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods (Tableaux 2009)*. Springer, 2009. LNAI.

[26] P. Arrighi and A. Díaz-Caro. Scalar System F for Linear-Algebraic λ-Calculus: Towards a Quantum Physical Logic. In *Proceedings of the 6th International Workshop on Quantum Physics and Logic*, pages 206–215, Oxford, UK, 2009.

[27] H. Bensaid, R. Caferra, and N. Peltier. DEI: A Theorem Prover for Terms with Integer Exponents. In *CADE 22 (22nd International Conference on Automated Deduction)*. Springer, 2009.

[28] D. Duval, R. Echahed, and F. Prost. A Heterogeneous Pushout Approach to Term-Graph Transformation. In *Proceedings of Rewriting Techniques and Application 2009 (RTA'09)*, 2009.

[29] F. Prost and C. Zerrari. Reasoning about entanglement and separability in quantum higher-order functions. In *Proceedings of Unconventional Computation 2009 (UC'09)*, volume 5715 of *Lecture Notes in Computer Science*, pages 219–235. Springer, 2009.

2008

[30] V. Aravantinos, R. Caferra, and N. Peltier. More Flexible Term Schematisations via Extended Primal Grammars. In *Tenth International Symposium on Artificial Intelligence and Mathematics (ISAIM)*, Jan. 2008.

[31] P. Arrighi and G. Dowek. Linear-algebraic lambda-calculus: Higher-Order, Encodings, and Confluence. In *Proceedings of RTA, Lecture Notes in Compter Science*, page 17. Springer, 2008.

[32] P. Arrighi and F. R. The Bloch representation of quantum states. In *To appear in Proceedings of QCMC*. AIP Conference series, 2008.

[33] P. Arrighi and N. V. Quantizations of Cellular Automata. In B. Durand, editor, *First Symposium on Cellular Automata "Journées Automates Cellulaires" (JAC 2008), Uzès, France, April 21-25, 2008. Proceedings*, pages 204–215. MCCME Publishing House, Moscow, 2008.

[34] P. Arrighi, N. V., and W. R. F. Quantum cellular automata over finite, unbounded configurations. In *Proceedings of MFCS, Lecture Notes in Computer Science*, volume 5196, pages 64–75. Springer, 2008.

[35] T. Boy De La Tour, M. Echenim, and P. Narendran. Unification and Matching Modulo Leaf-Permutative Equational Presentations. In A. Armando, P. Baumgartner, and G. Dowek, editors, *4th International Joint Conference, IJCAR 2008*, LNAI 5195, pages 332–347, Sydney, Australia, Aug. 2008. Springer Verlag.

[36] A. Díaz-Caro, P. Arrighi, M. Gadella, and J. Grattage. Measurements and confluence in quantum lambda calculi with explicit qubits. In *Proceedings of QPL, to appear in Electronic Notes in Computer Science*, 2008.

[37] R. Echahed. Inductively Sequential Term-Graph Rewrite Systems. In *Graph Transformations, 4th International Conference, ICGT 2008, Leicester, United Kingdom, September 7-13, 2008. Proceedings*, volume 5214 of *Lecture Notes in Computer Science*, pages 84–98. Springer, 2008.

[38] R. Echahed and N. Peltier. A Needed Rewriting Strategy for Data-Structures with Pointers. In *Rewriting Techniques and Applications, 19th International Conference, RTA 2008*, volume 5117 of *Lecture Notes in Computer Science*, pages 63–78. Springer, 2008.

[39] J. Grattage. An overview of QML with a concrete implementation in Haskell. In 5^{th} *International Workshop on Quantum Physics and Logic, 2008, to appear in Electronic Notes in Theorectical Computer Science*, Amsterdam, The Netherlands, 2008. Elsevier Science Publishers B. V. Also arXiv:quant-ph/0806.2735v2.

[40] M. Mhalla and S. Perdrix. Finding Optimal Flows Efficiently. In *ICALP (1)*, pages 857–868, 2008.

[41] N. Peltier. A Unified View of Tree Automata and Term Schematisations. In *Fifth IFIP International Conference On Theoretical Computer Science - TCS 2008*, volume 273 of *IFIP*, pages 491–505. Springer, 2008.

[42] N. Peltier. Automated Model Building: From Finite to Infinite Models. In *9th International Conference on Artificial Intelligence and Symbolic Computation*, volume 5144, pages 155–169. Springer LNCS, 2008.

2007

[43] T. Altenkirch, J. Grattage, J. Kaizer Vizzotto, and A. Sabry. An Algebra of Pure Quantum Programming. In 3^{rd} *International Workshop on Quantum Programming Languages, 2005, published in Electronic Notes in Theorectical Computer Science*, volume 170, pages 23–47, Amsterdam, The Netherlands, 2007. Elsevier Science Publishers B. V. Also arXiv:quant-ph/0506012v1.

[44] P. Arrighi and R. Fargetton. Intrinsically universal one-dimensional quantum cellular automata. In *Proceedings of DCM*, 2007.

[45] H. Bensaid, R. Caferra, and N. Peltier. Towards Systematic Analysis of Theorem Provers Search Spaces: First Steps. In *Proc. Wollic'07 (Workshop on Logic, Language, Information and Computation)*, pages 38–52. Springer, July 2007. LNCS 4576.

[46] M. P. Bonacina and M. Echenim. Decision procedures for variable-inactive theories and two polynomial T-satisfiability procedures (Position paper). In *Notes of the First Workshop on Automated Deduction: Decidability, Complexity, Tractability (ADDCT), Twenty-first International Conference on Automated Deduction (CADE)*, pages 65–67, July 2007.

[47] M. P. Bonacina and M. Echenim. Rewrite-based decision procedures. In T. Boy De La Tour, editor, *Proceedings of the Sixth Workshop on Strategies in Automated Deduction (STRATEGIES), Third International Joint Conference on Automated Reasoning (IJCAR) and Fourth Federated Logic Conference (FLoC), August 2006*, volume 174(11) of *Electronic Notes in Theoretical Computer Science*, pages 27–45. Elsevier, July 2007.

[48] M. P. Bonacina and M. Echenim. Rewrite-based satisfiability procedures for recursive data structures. In *Proceedings of the Fourth Workshop on Pragmatics of Decision Procedures in Automated Reasoning (PDPAR), Third International Joint Conference on Automated Reasoning (IJCAR) and Fourth Federated Logic Conference (FLoC), August 2006*, volume 174(8) of *Electronic Notes in Theoretical Computer Science*, pages 55–70. Elsevier, June 2007.

[49] M. P. Bonacina and M. Echenim. T-Decision by Decomposition. In *Automated Deduction - CADE-21, 21st International Conference on Automated Deduction, Bremen, Germany, July 17-20, 2007, Proceedings*, volume 4603 of *Lecture Notes in Computer Science*, pages 199–214. Springer, 2007.

[50] T. Boy De La Tour and M. Echenim. Determining Unify-Stable Presentations. In F. Baader, editor, *18th International Conference on Rewriting Techniques and Applications, RTA 2007*, Lecture Notes In Computer Science 4533, Paris, France, June 2007. Springer Verlag.

[51] D. Duval, R. Echahed, and F. Prost. Adjunction for Garbage Collection with Application to Graph Rewriting. In *Proceedings of Rewriting Techniques and Application 2007 (RTA'07)*, volume 4533 of *Lecture Notes in Computer Science*. Springer, 2007.

[52] R. Echahed and N. Peltier. Non Strict Confluent Rewrite Systems for Data-Structures with Pointers. In *Proceedings of RTA (Rewriting Techniques and Applications)*. Springer LNCS 4533, June 2007.

[53] P. Jorrand. Quantum information processing and communication: the computer science perspective. In *ACM Southeast Regional Conference*, page 509, 2007.

[54] P. Jorrand. The quantum challenge to computer science. In *Conf. Computing Frontiers*, pages 195–196, 2007.

[55] N. Peltier. A Bottom-up Approach to Clausal Tableaux. In *TABLEAUX'07 (International Conference on Automated Reasoning with Analytic Tableaux and Related Methods)*. Springer LNAI 4548, July 2007. Aix en Provence, France.

[56] F. Prost. Taming Non-Compositionality Using New Binders. In *Proceedings of Unconventional Computation 2007 (UC'07)*, volume 4618 of *Lecture Notes in Computer Science*. Springer, 2007.

2006

[57] R. Caferra, R. Echahed, and N. Peltier. Rewriting Term-Graphs with Priority. In *Proceedings of the Eighth ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming*, pages 109–120. ACM Press, 2006.

[58] D. Duval, R. Echahed, and F. Prost. Modeling Pointer Redirection as Cyclic Term-graph Rewriting. In *Proceedings of the Third International Workshop on Term Graph Rewriting(TERMGRAPH'06)*, Vienna, Austria, Apr. 2006.

[59] R. Echahed and N. Peltier. Narrowing Data-Structures with Pointers. In *Proceedings of ICGT (International Conference of Graph Transformation)*. Springer LNCS 4178, Sept. 2006.

2005

[60] T. Boy De La Tour and M. Echenim. Unification in a class of permutative theories. In J. Giesl, editor, *16th International Conference on Rewriting Techniques and Applications, RTA 2005*, Lecture Notes In Computer Science 3467, pages 105–119, Nara, Japan, apr 2005. Springer Verlag.

[61] N. Brauner, R. Echahed, G. Finke, H. Gregor, and F. Prost. Specializing Narrowing for Timetable Generation: A Case Study. In *Proceedings of Practical Aspects of Declarative Languages (PADL'05)*, Long Beach, California, Jan. 2005.

[62] R. Caferra, R. Echahed, and N. Peltier. A Graph Clausal Logic. In R. Letz, editor, *FTP'05 (International Workshop First-Order Theorem Proving).*, pages 85–96. Technical Report, Universität Koblenz-Landau., Sept. 2005. Koblenz, Germany.

[63] R. Echahed and F. Prost. Handling Declared Information Leakage. In *Proceedings of Workshop on Issues in the Theory of Security (WITS'05)*, Long Beach, California, Jan. 2005.

[64] R. Echahed and F. Prost. Security Policy in a Declarative Style. In *Proceedings of the* 7^{th} *International Conference on Principles and Practice of Declarative Programming (PPDP '05)*, Lisboa, Portugal, July 2005.

Book or Proceedings editing [DO]

2008

[65] R. Echahed, editor. volume 216 of *Electr. Notes Theor. Comput. Sci.* Elsevier, July 2008.

[66] R. Echahed, editor. *Selected papers from WFLP*, volume 216 of *Electronic Notes in Theoretical Computer Science*. Elsevier, July 2008.

2007

[67] T. Boy De La Tour, editor. *Proceedings of the 6th International Workshop on Strategies in Automated Deduction (Strategies 2006)*, volume 174 of *Electronic Notes in Theoretical Computer Science*. Elsevier, May 2007.

[68] R. Echahed, editor. *16th International Workshop on Functional and (Constraint) Logic Programming (WFLP 2007)*. Paris, June 2007.

Invited conferences [INV]

2007

[69] R. Echahed. On Term-Graph Rewrite Strategies. In *Invited talk at 7th International Workshop on Reduction Strategies in Rewriting and Programming, June, Paris*, 2007.

[70] R. Echahed. Term-Graph Rewriting. In *Invited lecture at the International School on Rewriting, July, Nancy*, 2007.

2006

[71] R. Echahed. Rewrite Techniques and Programming with pointers. In *Conférence invité au colloque international sur l'Informatique et ses application, Novembre, Oujda*, 2006.

Doctoral Dissertations and Habilitations Theses [TH]

2009

[72] P. Arrighi. *Quantum Cellular Automata*. Habilitation à diriger des recherches, UJF, June 2009.

2007

[73] N. Peltier. *Contributions à une approche qualitative de la déduction automatique*. Habilitation à diriger des recherches, Grenoble INP, June 2007.

Other Publications [AP]

2009

[74] P. Arrighi and A. Díaz-Caro. A System F accounting for scalars. Preprint: arXiv:0903.3741, July 2009. To appear.

[75] P. Arrighi and D. G. A quantum extention of Gandy's theorem (manuscript.). Current work., 2009.

[76] P. Arrighi and G. John. Intrinsically universal n-dimensional quantum cellular automata (manuscript.). To be submitted., 2009.

2008

[77] F. Prost and C. Zerrari. A logical analysis of entanglement and separability in quantum higher-order functions. Technical report, LIG, 2008.

2007

[78] P. Arrighi, N. V., and W. R. Unitarity plus causality implies locality. Arxiv preprint arXiv:0711.3975, 2007.

2005

[79] D. Duval, R. Echahed, and F. Prost. Data-Structure Rewriting. Technical report, Mar. 2005.

Summary

	2005	2006	2007	2008	2009	**Total**
International peer reviewed journal [ACL]	3	6	4	7	3	14
International peer-reviewed conference proceedings [ACT]	5	3	14	14	6	41
Book or Proceedings editing [DO]	0	0	2	2	0	4
Invited conferences [INV]	0	1	2	0	0	3
Doctoral Dissertations and Habilitations Theses [TH]	0	0	1	0	1	2
Other Publications [AP]	1	0	1	1	3	6
Total	9	10	24	24	13	80