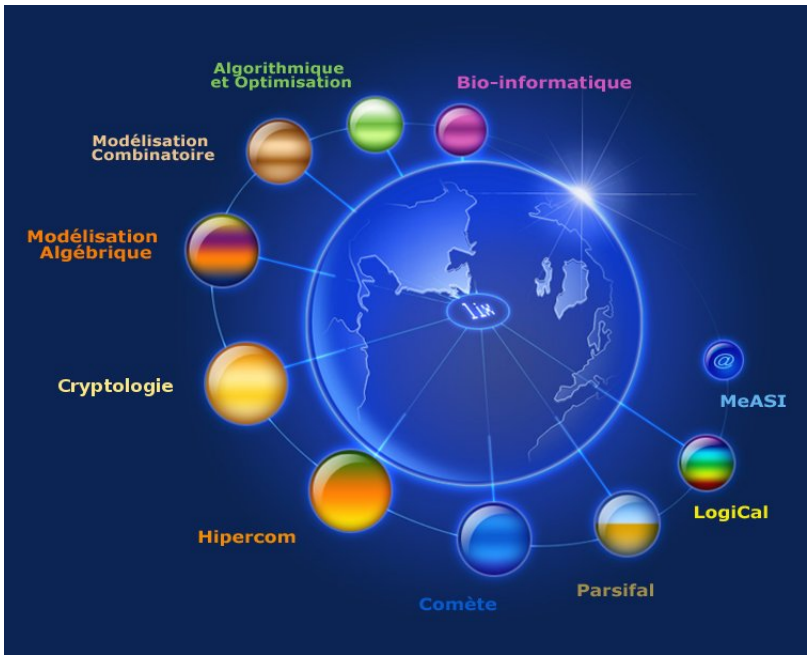
RESEARCH REPORT

NOVEMBER 2007

Director :
Jean-Pierre Jouannaud

Vice Director :
Philippe Baptiste



UMR CNRS 7161 LIX, École Polytechnique, F-91128 Palaiseau
Tel : +33169334073, Fax : +33169333014
www.lix.polytechnique.fr

ÉCOLE POLYTECHNIQUE

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

INRIA

Organigramme du LIX

Directeur : Jean-Pierre Jouannaud
Directeur adjoint : Philippe Baptiste

Assistantes :
Nicole Dubois (CNRS)[ALGORITHMIQUE ET OPTIMISATION, MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES, MODÈLES COMBINATOIRES],
Lydie Fontaine (INRIA)[COMÈTE,HIPERCOM, LOGICAL],
Isabelle Biercewicz (INRIA)[ALIEN, PARSIFAL],
Evelyne Rayssac (X)[BIO-INFORMATIQUE, CRYPTOLOGIE, MEASI].

Les assistantes sont rattachées aux équipes indiquées entre crochets. Nicole Dubois s'occupe de la gestion CNRS, et Evelyne Rayssac de la gestion École Polytechnique.

Équipes de recherches :

Algorithmes	Réseaux	Méthodes formelles
ALGORITHMIQUE ET OPTIMISATION Philippe Baptiste		COMÈTE Catuscia Palamidessi
BIO-INFORMATIQUE Jean-Marc Steyaert	HIPERCOM Philippe Jacquet	PARSIFAL Dale Miller
MODÈLES COMBINATOIRES Gilles Schaeffer	CRYPTOLOGIE François Morain	LOGICAL Benjamin Werner
MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES Marc Giusti		MEASI Daniel Krob

Équipe technique chargée des moyens informatiques :
Matthieu Guionnet, Pierre Lafon, James Régis

Introduction

LIX is the Laboratory for Informatics at X, the nickname of École Polytechnique. For that reason, LIX must be the flag of informatics research for the students of the school, in order to attract them, and for the alumnis, some of them holding important positions in the french economy. This implies some diversity in our activities, a constant quest for excellence, a world-wide reputation, strong industrial relationships, and, last but not least, a clear vision of the informatics landscape in the coming years.

LIX is a research unit common to École Polytechnique and CNRS. The laboratory has now reached and slightly passed a total of 120 members, teaching staff, full-time researchers, postdocs, phds and support staff. The numerous interns are not considered laboratory members even those finishing their master. Visitors are not counted either, unless they stay at least 6 months in the laboratory. LIX is organized into 10 teams described below, among which 6 of them host an INRIA project, and one is common with CEA-LIST[1].

As of today, the activities of the laboratory can be categorized into three different fundamental areas, each area grouping from 2 to 4 research teams of a comparable size :

Algorithmics, with four teams :

1. *Algebraic Models and Symbolic Computations* (MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES) nicknamed MAX, is interested in algebraic models, that is, based on commutative or differential algebra, and in their applications to geometry, control theory, signal analysis and informatics. MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES host the INRIA project ALIEN[2].
2. *Algorithms and optimisation* (ALGORITHMIQUE ET OPTIMISATION) is interested in combinatorial optimisation problems and in their resolution by tractable algorithms, possibly to the price of a probabilistic or a heuristic approach.
3. *Bio-informatics* (BIO-INFORMATIQUE) is interested in the modelling of biological entities (such as the genome) in order to propose effectively computable, predictive models of structure and functionality.
4. *Combinatorial models* (MODÈLES COMBINATOIRES) studies the combinatorial properties of complex objects (sandpiles, random graphs, graph embeddings, digitalized signals) with applicative goals in statistical physics and informatics (algorithmic geometry, web queries, graph design).

Communication networks, with two teams :

5. HIPERCOM is interested in routing protocols that scale up for very large ad'hoc networks with a garanteed quality of service, and their normalization by IETF. HIPERCOM is part of a large INRIA project of the same name currently located at INRIA-Rocquencourt[3].
6. *Cryptology* (CRYPTOLOGIE) is specialized in algorithmic number theory for cryptography based on algebraic curves, aiming at building ressource-efficient cryptosystems for smart card or RFID applications. CRYPTOLOGIE hosts the INRIA project TANC.

Formal methods with four teams :

7. LOGICAL is specialized in the design of logical systems and the implementation of proof assistants that can support formal proofs of mathematical statements, in order to carrying out the correctness proof of critical software. LOGICAL hosts the INRIA project of the same name.

[1] The *Commissariat à l'Énergie Atomique* is one of the major french research and development institutions and *the Laboratoire pour l'Intégration des Systèmes et des Technologies* is the laboratory for computer science at CEA.

[2] ALIEN is colocated at INRIA-Saclay-Île-de-France and INRIA-Nord-Picardie.

[3] Although the LIX part of Hipercom has been very active at École Polytechnique for over two years, the decision of colocating Hipercom at both INRIA-Rocquencourt and INRIA-Saclay-Île-de-France has not been formally taken yet but is expected for the end of 2007.

8. PARSIFAL studies the logical foundations of programming and verification, aiming at designing theorem provers based on proof search as are logic programming interpreters. PARSIFAL hosts the INRIA project of the same name.
9. COMÈTE is interested in models for concurrent, distributed, probabilistic computations, aiming at building tools for programming applications distributed over a mobile networks, and verifying their correct behaviour by probabilistic model checking techniques. COMÈTE has been located at École Polytechnique from the beginning, and should become an INRIA project very soon[4].
10. MEASI is interested in the modelling, design and verification of *Complex Industrial Systems* built themselves from components which are complex systems, the basic components being either software or hardware systems.

    MEASI is a common research team of CEA-LIST and LIX, with a LIST component and a LIX component. We describe here the activities of the LIX part, some of which are carried out in common with the CEA-LIST part.

Besides this activity of the research teams centered around an individual project with focused goals, the laboratory tries to organize the research on a larger scale by providing a friendly research environment suitable for collaborations. In particular, we support a small cafeteria, seminars, working groups, an annual colloquium of a growing reputation, and have started an ambitious research project involving many teams in the laboratory. We indeed like to promote a double reading of the activities in the laboratory. The first reading is the team description, while the second is by target areas : telecommunications -in a broad sense- and bio-informatics are two important areas in which we try or plan to focus our efforts.

Telecommunications is the first area of expertise of the lab. Our claimed goal is to develop a global expertise in telecommunications, and we think that we already cover a fair spectrum of it. Teams in algorithmics are interested in many problems of a combinatorial nature that exist in mobile communications, for which the underlying hard optimisation problems may need approximations. MAX (via the INRIA project ALIEN) is also interested in signal processing, in particular in presence of drastic variations of the signal's parameters. Teams in networking are even more concerned since routing communications and ensuring their protection is their main activity. Teams in formal methods are also interested as an application area of the techniques they develop : security of the crytographic protocols (assuming perfect encrytion) and safety of the communication protocols are key questions in this area that they address. This expertise in telecommunications is at work in our research project mentionned before.

Bio-informatics is the second area, in which we try to build complementary forces. Besides the BIO-INFORMATIQUE team, several other teams are also interested in problems that arise in this area. MODÈLES COMBINATOIRES is interested in molecular biology because of the data structures needed to represent and query efficiently molecules as 3-D structures, and ALGORITHMIQUE ET OPTIMISATION is interested as well in the numerous optimisation problems that arise when reconstructing these 3-D structures. Besides, logic is now heavily used to represent and understand the activity of biological entities viewed as concurrent agents propagating some sort of information. These questions have recently been considered in COMÈTE.

LIX is a laboratory common to École Polytechnique and CNRS, with a growing influence from INRIA, with respect to both the scientific personnel and the research goals. But LIX is not an INRIA laboratory. Besides, CNRS and INRIA evaluations obey very different modalities, and happen at different times. This situation has an important impact on the daily life of the laboratory, on its management, and even on the writing of this report. In particular, this report is written in english. One reason is that we wanted to reuse the reports written for the recent INRIA evaluations. Another was to allow for non-french external evaluators. A last reason was to have an english-written scientific document describing our research in details for posting on our website. The overal quality of our english is probably mediocre. We beg our english-speaking colleagues for their forgiveness.

Which research organism a researcher or staff member belongs to is by no means an issue at LIX. As a consequence, all researchers are listed on the

[4]Its current exact status is an INRIA-action, which is a preliminary step before the project creation which is expected for the end of 2007.

reasearch staff of their team. There is indeed one exception : researchers from CEA-LIST do not belong to LIX. What actually belongs to LIX (and to CEA-LIST) are the activities carried out in common by the CEA-LIST and LIX members of the team MeASI that we have initiated together. Not all LIX members are comfortable or even familiar with these subtleties that reflect the richness of the french research system.

The remainder of this report is divided into chapters written by the team leaders and their collaborators. Each chapter has its own list of references including the bibliography of the team during the last four years (or since it joined the laboratory). Each bibliography is generated by the bibtex ralix style developped by François Morain. References published before 2004, or containing no author from LIX are automatically collected as *External References*. The others are categorized as they should, thanks to a special field in the bib file. This scientific description of the teams will be followed by a short description of our project *Systèmes Complexes Distribués Mobiles Sécurisés*. These descriptions will in turn be followed by a chapter describing our scientific project for the next 4 years contract and by a sorted bibliography of the laboratory during the last four years. Several annexes will conclude the report : manpower, funding, computing infrastruture, and training plan.

Algorithmique et optimisation

Team members

Team leader

Philippe BAPTISTE

Permanent members

- Philippe BAPTISTE, Chargé de recherches au CNRS
- Christoph DÜRR, Chargé de recherches au CNRS (at LIX since september 1st, 2005)
- Miki HERMANN, Chargé de recherches au CNRS.

Claire Kenyon, Prof. at Ecole Polytechnique and junior member of "Institut Universitaire de France", left the lab in late 2004.

Postdocs

- Ruslan SADYKOV, postdoc, since september 15th, 2006
- Leo LIBERTI, postdoc (jointly with MEASI team), from september 2005 to september 2006
- Gustav NORDH, postdoc, since September 2007
- Yann HENDEL, postdoc, since September 2007.

Phds

- Konstantin ARTIOUCHINE, bourse Thales, defended in december, 2005
- Claus GWIGGNER, bourse Eurocontrol, defended in september 11, 2007
- Mathilde HURAND, bourse BDX, since september 1st, 2005
- Thang Kim NGUYEN, bourse BDX, since september 1st, 2006
- Giacomo NANNICINI, bourse CIFRE Mediamobile (jointly with the MEASI team), since september 2006
- Florian RICHOUX, bourse MESR, since september 1st, 2006
- Emilie WINTER, bourse CIFRE Thales, defended in 2007.

Interns

- Adriana LOPEZ, MIT, from june 4, 2007 to july 28, 2007
- Vincent RUDELLI, élève ingénieur X-2004, from April 1st, 2007 to June 30, 2007
- Bechir TOURKI, stagiaire MPRI jointly with Thales, from march to septemebr 2007
- Rudolf van den BEUKEL, Department of Information and Computing Sciences, Utrecht University, from november 2007 to may 2008.

Guests

- Ioannis MILIS, Associate Professor, Athens University, May 2005
- Ed COFFMANN, Professor Columbia University, March 2005
- Alexander KONONOV, Senior Researcher, Sobolev Institute of Mathematics, November–December 2007
- Maxim SVIRIDENKO, Researcher at IBM Yorktown, November 2006
- Marek CHROBAK, Professor at U. of California Riverside, Ecole Polytechnique invited researcher from October 11, 2007 to December 11, 2007.

Research domain

We study *discrete optimization constraint satisfaction* problems both from a theoretical and a practical point of view. For this latter purpose, we work closely with several *industrial partners* and we provide *Operations Research* tools to help with decision making in real-world.

Discrete Optimization problems can be unformally defined as follows : Given a set of variables taking values in discrete sets, a set of constraints that allow variables to take on certain values but exclude others and an objective function, we look for an assignement of values to variables that meet all constraints and that minimizes the objective function. Among discret optimization problems, our group is very interested in scheduling problems. Such problems arise in many areas, including air traffic control, buffer management in network routers, production management.

We study several aspects of discrete optimization problems.

- We design *combinatorial optimization algorithms* to solve instances of problems (that are hard in general), by exploring efficiently the solution space. These algorithms rely on Constraint Programming as well as on Mixed Integer Programming.
- We study *scheduling theory* and we exhibit structural properties of optimal schedules. This allows us to design improved algorithm and/or to prove new *complexity results*. Along this line of research, we have exhibited, for several combinatorial optimization problems, (continuous) linear programs that always yields to an integer solution. The rationale for this behaviour is still unknown.

Constraint Satisfaction Problems (CSP) represent an obvious and concise way of defining and solving problems in combinatorics, graph theory, database theory, logics, etc. We study several aspects of CSP problems, like decision, counting, enumeration, optimization, and approximation.

Goals

Team Management and Objecives

Discrete optimization is a multidisciplinary research at the crossroad of mathematical programming, algorithmics, complexity, constraint satisfaction, computational game theory, etc. Our ambition is *to setup a research team that assembles expertise in several areas related to discrete optimization*. The team is small but is growing steadily : Vincent Jost (graph theory and combinatorial optimization), as well as Manuel Bodirsky (constraint satisfaction, finite and infinite model theory, infinite permutation groups, clones with infinite domains, logic in computer science, descriptive complexity, combinatorial games) will join us very soon as a CR2 CNRS. On top of this, we have very strong links with Leo Liberti an expert in global optimization working in the MEASI team.

Scientific Goals

We want to pursue a research program balancing fundamental research and innovative applications. We see industrial collaborations as a fundamental aspect of research. Because of the nature of optimization, it

is fundamental to evaluate theoretical results and optimization systems on realistic applications. It is also critical to push the frontiers of optimization, balancing short-term and long-term impact.

LP One of our current goal is to understand better why some families of linear programs always yield integer optimal solutions. While most of them correspond to flow problems and are well understood, there remains a mysterious subclass which we do not understand well at the moment.

Scheduling theory We want to carry on our work in scheduling theory (complexity, algorithms, etc). On top of these "classical" scheduling problems on which we want to work, we are also very interested in practical problems that require theoretica breakthrough. For instance, we want to work on processor scaling for energy minimization : Transistors sizes keep shrinking, but now heating issues and power supply make it impossible to maintain the same rate of increase of the processor speed as in the past. Therefore the current processors can work at different speeds, which permits the operation system to control the consumed energy and the produced heat. Many interesting scheduling problems arise in this situation, where we want to maintain a certain quality of service (respecting deadlines of jobs for example, or keeping the total flow time under some threshold) while respecting the energy consumption or heat production low. We would like to come up with good performance algorithms for these questions.

Nash Scheduling is about centralized planing, knowing all job characteristics in advance and assign them to machines and time slots. In some situations such a centralized organization is not possible, and we have several actors (players) who try to assign their jobs in concurrence to machines, so to minimize their own cost. The important object to study in these situations are Nash equilibria, which are configurations where no actor has an incentive to deviate from its choice. Clearly these configurations can have a worse social cost than a centralized planed optimal solution. There are many interesting questions related to equilibria, how hard is it to find one, are there always equilibria in given game, and if not, how hard is to to decide if there is one ? What is the social cost of an equilibrium with respect to the optimum ? The next step is then to find ways (mechanism designs) to distribute the social cost to the actors in such a way that the resulting equilibria have good social costs. Clearly this is not possible for all games. A lot of work has already be done on these questions for scheduling games, we are studying at the moment the facility location games.

CSP We study different constraint satisfaction problems (CSP) by algebraic and logic means. The main goal in our studies is an establishment of a complete characterization of complexity for all algebraically closed classes of constraints for decision, counting, enumeration, optimization, and approximation variants of the considered problems.

Results

Scheduling Theory

In a general scheduling problem, each job j comes with a distinct processing time p_j. Now in some situations we can in fact assume that all jobs have the same length p, for example TCP/IP packets in a local Ethernet network are in general 1500 bytes long, or in a production site there are tasks that take a job independent time. Now with this *equal processing time assumption* (which we do from now on in this paragraph), some problems actually become easier. For example if jobs have a release time before which they cannot be scheduled, and if the goal is to minimize the total completion time of the jobs, then we can assume that there are only $O(n^2)$ time points where jobs can possibly complete in a optimal schedule. This structure permits worst case polynomial time algorithms in some cases.

In [**?**] we study the scheduling problem when jobs come with regularly repeated time windows where they are allowed to be scheduled. In [**?**] we study the problem of scheduling equal sized jobs with given release times, on parallel machine allowing preemptions and minimizing total completion time. This problem was solved in 2004 with a linear program using a complicated post-processing, and we provide a very simple and elegant linear program, which solves the

problem directly. Now let's consider the problem for a single machine, but this time, we do not allow preemption and wish to minimize the number of jobs that miss their deadlines. We found out that an algorithm from 1981 for that problem was not correct, and provided an $O(n^4)$ algorithm for it, using a completely different approach. In [**?**] we studied a completely new objective function in scheduling, namely the energy consumption. Here a computer can be turned off when idle for sufficiently long time, so naturally we want to produce a schedule for a given set of jobs with release times and deadlines, that minimize the number of idle periods. While [**?**] provided a first solution to this problem for a special case, in [**?**] we improved the algorithm and solved the general problem as well. Some scheduling problems are solved with time indexed linear programs (a variable $X_{jt} = 1$ means that job j is scheduled at time t) that always have an integer solution. In [40] we simplified these solution and gave combinatorial algorithms for them, improving on the way the worst case running time.

In [25] we study the problem of scheduling packets in a router, who is connected to the next hop with several parallel links. We have to retransmit arriving packets (of different length) on one of the links, so to preserve the order of the arrival times of the jobs on the next hop, since reordering packets may decrease quality of service of some network applications. The goal is to minimize the maximal flow time, which is the latency experienced by the applications. We provide an $O(\sqrt{n/m})$-competitive online algorithm and a matching lower bound on the competitive ratio, even randomized. Here m is the number of links, and n the number of jobs.

On Solving Combinatoirial Optimization Problems

One of our line of research is to design efficient procedures to solve combinatorial optimization problems. "Solving" means here that, given a problem and an instance of the problem, we aim to find the optimum (and to prove that it is the optimum). Most often we compare several approchaes relying on Mixed Integer Programing, Constraint Programming or Branch and Bound techniques. The combinatorial problems we have chosen to study are either academic problems for which there is a tough competition among research teams or practical problems that arise from our industrial collaborations.

Air Trafic Control This research has been led jointly with Thales (Konstatin Artiouchine PhD) and Eurocontrol. When aircraft reach the final descent in the "Terminal Radar Approach CONontrol" area (TRACON), a set of disjoint time windows in which the landing is possible, can be automatically assigned to each aircraft. The objective is then to determine landing times, within these time windows, which maximize the minimum time elapsed between consecutive landings. We have studied the complexity of the problem and we have described several special cases that can be solved in polynomial time. We have also provided a compact Mixed Integer Programming formulation that allows us to solve large instances of the general problem when all time windows have the same size. We have also introduced a general hybrid branch and cut framework to solve the problem with arbitrary time windows [**?**, 21].
We have also studied the same problem under a constraint programing framework [17]. This led us to study the "inter-distance constraint", also known as the global minimum distance constraint, that ensures that the distance between any pair of variables is at least equal to a given value. When this value is 1, the inter-distance constraint reduces to the all-different constraint. We have introduced an algorithm to propagate this constraint and we show that, when variables domains are intervals, our algorithm achieves arc-B-consistency (the xistence of such an algorithm was an open question). It provides tighter bounds than generic scheduling constraint propagation algorithms (like edge-finding) that could be used to capture this constraint.

We also analyze fligth data to identify the weaknesses of current models for flight scheduling. Uncertainties (e.g delay from connecting flights, technical failure) create gaps in flight schedules. This causes safety problems and non-optimal uses of capacity. While the main sources of uncertainties are known, the mechanisms of how they disturb the planning flow remain unknown.

Our main results are twofold :

There are systematic gaps in schedules and such gaps are a natural property of the flow sys-

tem. Based on this we propose ideas improving the current flow optimization algorithm [33], [41], [68].

These gaps propagate in a perfectly expected way through the sector network. This makes it unlikely that there is a system-wide strategy to absorb gaps. Based on this one can construct a flow model that minimizes the long-term impact of uncertainties in schedules [69].

Radar Scheduling This is joint work with Thales TAS (PhD of Emilie Winter). Among several other tasks, the radar of a fighter has to search, track and identify potential targets. The waveforms used by the radar for each of these tasks are most often incompatible and hence, cannot be processed simultaneously. Moreover, these tasks are repeated several times in a cyclic fashion. Altogether, this defines a complex scheduling problem that impacts a lot on the quality of the radar's output. We have defined a formal framework for this real time scheduling problem and we have introduced several techniques based on Mixed Integer Programing and column generation to compute efficient schedules for the radar [20].

Single Machine Scheduling The most simple scheduling situtation happens when all jobs have to be scheduled on the same machine and hence cannot overlap in time. Even this problem is hard as soon as we have release dates and deadlines. A huge amount of research has been spent on this problem to come with efficient procedures for many standard objective functions such as total completion time, tardiness, number of late jos, etc. We have reviewed all existing lower bounds [24] and we have introduced new compact MIP formulations for arbitrary objective functions [39]. Motivated by industrial applications (jointly with ILOG), we have studied the scheduling situation where the objective is to minimize a regular sum objective function $\sum_i f_i$ where $f_i(C_i)$ corresponds to the cost of the completion of job J_i at time C_i. On top of this, we also take into account setup times and setup costs between families of jobs as well as the fact that some jobs can be "unperformed" to reduce the load of the machine [11].

Nash Equilibrium

A completely different work is [52], where we study a novel game, the Voronoi game on graphs. Here we are given discrete vertex set with a metric (given by the graph) and every player is to choose a vertex in that set which then represents a facility. Users are assigned to closest facilities, as in the k-median problem, and the gain of every player is the amount of users assigned to it. This game models naturally games, where each player wants to conquer as much as possible from some area, representing a market. We discovered that there are not always pure Nash equilibria in that game, it depends in fact on the given graph and the number of players and deciding this property is NP-hard. We also studied the social cost of these equilibria.

Complexity of CSPs

Miki Hermann with Philippe Chapdelaine and Ilka Schnoor established a complete classification of complexity for reasoning in the default logic in [48]. Miki Hermann presented a new proof of the 25 Boolean primitive positive clones in [19]. Miki Hermann with Reinhard Pichler presented a large analysis of the counting complexity of propositional abduction in [51]. Miki Hermann together with Nadia Creignou, Andrei Krokhin, and Gernot Salzer studied in [15] the complexity of constraints on finite totally ordered domains, where the atomic literals are of the form $x \geq d$ and $x \leq d$ for a variable x and a domain value d. Miki Hermann together with Arnaud Durand and Phokion Kolaitis studied the possibility of reductions preserving the counting classes and complete problems in the counting complexity hierarchy in [13], establishing also new counting complexity results for the circumscription problem, as well as other problems in automated deduction.

Quantum Computing

We got a few results on quantum computing, which is not part of the research areas of the group, and which have been conducted while Christoph Dürr was not yet member of the group, but appeared when we already joined LIX. In [12] we studied the quantum query complexity of testing whether a given black-box function is injective or not. This is an important property for digital signatures. In [16] we got

tight lower and upper bounds for the quantum query complexity of several graph problems, when the graph is given as an oracle which can only be accessed by queries of the type *"What is the i-th neighbor of vertex u ?"* or *"Is there an edge between u and v ?"* (two different query models). In [37] we studied the quantum query complexity of various computational geometry problems : given a sequence of points, is the described polygon intersection-free, what is the pair of closest points, what is the pair of furthest points, etc. ?

Software, pattents and contracts

Software

The team has developped several pieces software in the area of optimisation. Each one is dedicated to a specific application (often carried out as part of our industrial collaborations). Most of the exisiting code consists is built on top of constraint solvers such as Ilog Solver or on top of Linear Programming packages.

It is our goal to start a software project that would capatalize these efforts in the form of a generic optimisation software dedicated to scheduling that would enable one to model and solve specific scheduling applications.

Patents

The following patent has been filed at the national French patent office : "Estimation de trafic dans un réseau routier (méthode basée sur les flots)". Owners : LIX, Mediamobile. Inventors : Ph. Baptiste, G. Barbier, D. Krob, L. Liberti.

Contracts

- Title : "Exploiting Implicit Structures to Better Solve Combinatorial Problems : An Application to Time-Slot Allocation for Air Traffic Control" ;
  Period : 01/04/2003 – 01/04/2007 ;
  Type : Contract with Eurocontrol ;
  Object : Funding the Phd of Claus Gwiggner ;
- Title : "Des outils d'optimisation combinatoire et d'ordonnancement pour la gestion de radars embarqués" ;
  Period : 01/04/2004 – 01/04/2007 ;
  Type : Contract with Thales-TAS ;
  Object : Funding the Phd of Emilie Winter ;
- Title : "Shortest paths in dynamic road networks" ;
  Period : 2006-2009 ;
  Type : Contract with Medimobile ;
  Object : Funding the Phd of Giacomo Nancinni ;

International scientific cooperations

- Title : Scheduling Problems with Blocking and Flexible Routings ;
  Period : 2005–2006 ;
  Type : PROCOPE (PAI CNRS) with Osnabrueck University (Germany) ;
  Object : We consider a very general scheduling model which has a wide range of applications in areas like production scheduling, railway scheduling, air control problems, sports league planning or distribution of information in networks, etc. We have developped efficient algorithm to solve the problem.
- Title : Offline and Online Algorithms for Job Scheduling Problems ;
  Period : from january 1, 2004 to december 31, 2006 ;
  Type : CNRS-NSF US-France cooperative research ;
  Subject : The project concerns job scheduling algorithms. More specifically, it focuses on offline and online algorithms for various scheduling problems where the objective function is the weighted number of jobs completed within their due date. This objective function is called *throughput*. Scheduling problems of this nature arise frequently in *overloaded systems* and in applications with *quality of service* constraints.
- Title : ANR Alpage (Algorithms for Large Scale Platforms) ;
  Period : from september 1, 2005 to august 31, 2008 ;
  Type : ANR ;
  Subject : Algorithm design and scheduling techniques as well as macro-communication primitives and routing protocols for peer-to-peer architectures and distributed systems.

Teaching, dissemination and service

Miki Hermann teaches an introductory course of 12 hours on Computability and Complexity in the *Master Parisien de Recherche en Informatique*.

Miki Hermann wrote with Pierre Lescanne a popular article on computational complexity and the P versus NP problem [65].

Philippe Baptiste is "Professeur chargé de cours" at Ecole Polytechnique. Christoph Dürr is "Chargé d'enseignement".

Philippe Baptiste, Christoph Dürr and Leo Liberti (MEASI team) teach every year in the Master course MPRI on *optimization techniques for scheduling problems*.

Philippe Baptiste also teaches for undergraduates "Constraint programming and combinatorial optimization" (INF581) and "Fundamentals of Programming and Algorithms" (INF421). Christoph Dürr and Ruslan Sadykov participate as teaching assistants.

Philippe Baptiste is a member of the "comité national de la recherche scientifique", "commission de spécialistes de l'Université Paris 6 (27eme)", "comité scientifique du GdR RO", "expert du comité productique du CNRS". Miki Hermann is the "Secrétaire Scientifique de la Commission Interdisciplinaire 44 du CNRS" and is a member of "Commissions des Spécialistes 27^{e} section" de l'Université d´Orléans et de l'Université de Provence.

Visibility

Miki Hermann was an Examinateur of the Habilitation of Nicolas Peltier at the University Grenoble in June 2007. Philippe Baptiste a participé aux jurys de thèse/HDR suivants :

- Rapporteur de la thèse de Boris Detienne (Univ. Catholique de l'ouest). "Planification et Ordonnancement : Méthodes de Décomposition et Génération de Coupes". Juin 2007.
- Examinateur de l'habilitation de Laurent Péridy (Institut de Mathématiques Appliquées, Angers). Juin 2007.
- Rapporteur de la thèse de Renaud Sirdey (UTC). "Modèles et algorithmes pour la reconfiguration de
- systèmes répartis utilisés en téléphonie cellulaire". Mars 2007.
- Rapporteur de la thèse de Jérôme Fortin (IRIT, Toulouse). " Analyse d'intervalles flous, applications à l'ordonnancement dans l'incertain". Nov 2006.
- Rapporteur de la thèse de Lionnel Eyraud (IMAG, Grenoble). " Théorie et pratique de l'ordonnancement d'applications sur les systèmes distribués". Octobre 2006.
- Examinateur de la thèse d'Hadrien Cambazard (Ecole des Mines de Nantes). " Résolution de problèmes combinatoires par des approches fondées sur la notion d'explication". Novembre 2006
- Rapporteur de la thèse de P. Lennartz (Universiteit Utrecht). "No-Wait Job Shop Scheduling. A Constraint Programming Approach», printemps 2006.
- Rapporteur de la thèse de Marta Flamini (Roma 3). "Job-Shop scheduling algorithms with applications to railway traffic control", printemps 2006.
- Rapporteur de la thèse de Thomas Rivière (Toulouse, INPT) "Optimisation de graphes sous contrainte géométrique : création d' un réseau de routes aériennes pour un contrôle Sector-Less ». printemps 2006.
- Rapporteur de la thèse de Yann Hendel (LIP6) " Contributions 'a l'ordonnancement juste-à-temps» Novembre 2005.
- Rapporteur de la thèse de Ruslan Sadykov (CORE, Unversité de Louvain La Neuve), printemps 2006.
- Rapporteur de la thèse de Cyril Canon. "Application des techniques de recherche opérationnelle à la planification de personnel dans un centre de contacts multi-compétent", Université de Tours, dec 2005.
- Rapporteur de la thèse de Rabia Nessah. "Ordonnancement de la production pour la minimisation des encours" Université de Technologie de Troyes, 2005.
- Rapporteur de la thèse de Fabrice Tercinet. " Méthodes arborescentes pour la résolution des problèmes d'ordonnancement, conception d'un outil d'aide au développement", Université de Tours, novembre 2005.
- Rapporteur de la thèse de Benoît Lardeux. "Conception de réseaux de télécommunications multicouches et évolutifs ». Université de technologie de Compiègne / FT R&D, septembre

2005.
- Examinateur de la thèse de F. Clautiaux "Bornes inférieures et méthodes exactes pour le problème de bin-packing en deux dimensions avec orientations fixes", soutenue à l'Université de Technologie de Compiègne le 30 mars 2005.
- Examinateur de la thèse de Thèse de LA Hoang Trung, "Utilisation d'ordres partiels pour la caractérisation de solutions robustes en ordonnancement", Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS, Institut National des Sciences Appliquées de Toulouse, 24 janvier 2005.

National scientific cooperations

- Nadia Creignou (professor at the *Université de la Méditerrannée*), Arnaud Durand (professor at the *Université Paris 7*), and Bruno Zanuttini (assistant professor at the *Université de Caen*) work with Miki Hermann on the complexity of constraint satisfaction problems

International scientific cooperations

- with Marek Chrobak from UCR, we have a common research grant, and several joint articles.
- Phokion Kolaitis (senior research scientist at IBM Almaden and formerly a full professor at the University of California in Santa Cruz) worked with Miki Hermann on counting complexity of constraint satisfaction problems
- Gernot Salzer and Reinhard Pichler (both professors at the *Technische Universität Wien*) work with Miki Hermann on several problems concerning computational complexity

Conference and seminar invitations

Philippe Baptiste has been invited to give a talk at the "Master Class of CPAIOR07" and to the "second Second International Summer School of Constraint Programming" (Samos, June 2006).

Christoph Dürr gave a tutorial on algorithmic game theory at the "RIVF'07 conference" in Hanoi and in the seminar of the LIP Ens-Lyon (2007).

Claire Kenyon gave an invited talk at STATCS 2004.

Conference organisation

- Christoph Dürr participated to the organization of QIP'06.
- Philippe Baptiste and Christoph Dürr participated to the organization of MISTA'07.
- Miki Hermann organized the 13th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR 2006), November 13-17, in Phnom Penh (Cambodia).

Program committees

- Miki Hermann was a program comittee member of the iternational conference LPAR 2005 and the co-chairperson of LPAR 2006 [42].
- Philippe Baptiste participated to the program committee of CPAIOR 05, 06, 06, MISTA'05 and 07, RIVF, ROADEF and ICRAT (every year).
- Christoph Dürr participated to the program committee of STACS'05, Renpar'06 and MISTA'07.
- Claire Kenyon was in the PC of ESA 2004 (European Symposium on Algorithms) and WAOA 2004 (Workshop on Approximation and Online Algorithms)

Journal editorial boards

- Philippe Baptiste is an associate editor of Journal of Scheduling, Operations Research Letters and Discrete Optimization.

References

Books and chapters in books

2004

[1] BAPTISTE, P., AND BRUCKER, P. *HandBook of Scheduling : Algorithms, Models and Performance Analysis*. CRC Press, 2004, ch. Scheduling Equal Processing Time Jobs.

[2] BAPTISTE, P., NÉRON, E., AND SOURD, F. *Modèles et algorithmes en ordonnancement. Exercice et problèmes corrigés (18 auteurs)*. Ellipses, 2004.

[3] JOUGLET, A., BAPTISTE, P., AND CARLIER, J. *HandBook of Scheduling : Algorithms, Models and Performance Analysis*. CRC Press, 2004, ch. Branch-and-Bound Algorithms for Total Weighted Tardiness.

2005

[4] NÉRON, E., ARTIGUES, C., BAPTISTE, P., CARLIER, J., DEMASSEY, S., AND LABORIE, P. *Topics in modern project scheduling*. Kluwer, 2005, ch. Lower bounds computation for RCPSP chapitre de Topics in modern project scheduling.

2006

[5] BAPTISTE, P., LABORIE, P., PAPE, C. L., AND NUIJTEN, W. *Handbook of Constraint Programming*. Elsevier, 2006, ch. Constraint-Based Scheduling and Planning.

International journals

2004

[6] BAPTISTE, P., BRUCKER, P., KNUST, S., AND TIMKOVSKY, V. G. Ten notes on equal-processing-time scheduling. *4OR : Quarterly Journal of the Belgian, French and Italian Operations Research Societies 2* (2004), 111–127.

[7] BAPTISTE, P., CHROBAK, DURR, C., JAWOR, AND VAKHANIA. Preemptive scheduling of equal-length jobs to maximize weighted throughput. *Operations Research Letters 32*, 3 (2004), 258–264.

[8] BAPTISTE, P., AND DEMASSEY, S. Tight lp bounds for resource constrained project scheduling. *OR Spectrum 26* (2004), 251–262.

[9] BAPTISTE, P., AND TIMKOVSKY, V. Shortest path to nonpreemptive schedules of unit-time jobs on two identical parallel machines with minimum total completion time. *Mathematical Methods of Operations Research (ZOR) 60*, 1 (2004), 145–153.

[10] PH. BAPTISTE, J. C., AND JOUGLET, A. A branch-and-bound procedure to minimize total tardiness on one machine with arbitrary release dates. *European Journal of Operational research 158* (2004), 595–608.

2005

[11] BAPTISTE, P., AND PAPE, C. L. Scheduling a single machine to minimize a regular objective function under setup constraints. *Discrete Optimization 2* (2005), 83–99.

[12] BUHRMAN, H., DÜRR, C., HEILIGMAN, M., HØYER, P., MAGNIEZ, F., SANTHA, M., AND DE WOLF, R. Quantum algorithms for element distinctness. *SIAM J. Comput. 34*, 6 (2005), 1324–1330.

[13] DURAND, A., HERMANN, M., AND KOLAITIS, P. G. Subtractive reductions and complete problems for counting complexity classes. *Theoretical Computer Science 340*, 3 (2005), 496–513.

2006

[14] CHROBAK, M., DÜRR, C., JAWOR, W., KOWALIK, L., AND KUROWSKI, M. A note on scheduling equal-length jobs to maximize throughput. *Journal of Scheduling 9*, 1 (2006), 71–73.

[15] CREIGNOU, N., HERMANN, M., KROKHIN, A., AND SALZER, G. Complexity of clausal constraints over chains. *Theory of Computings Systems x*, x (2006), xx–xx. To appear.

[16] DÜRR, C., HEILIGMAN, M., HØYER, P., AND MHALLA, M. Quantum query complexity of some graph problems. *SIAM J. of Computing 35*, 6 (2006), 1310–1328.

2007

[17] ARTIOUCHINE, K., AND BAPTISTE, P. Arc-b-consistency of the inter-distance constraint. *Constraints 12*, 1 (2007), 3–19.

[18] BAPTISTE, P., BRUCKER, P., CHROBAK, M., DÜRR, C., KRAVCHENKO, S., AND SOURD, F. The complexity of mean flow time scheduling problems with release times. *Journal of Scheduling 10*, 2 (2007), 139–146.

[19] HERMANN, M. On Boolean primitive positive clones. *Discrete Mathematics x*, x (2007), xx–xx.

[20] WINTER, E., AND BAPTISTE, P. On scheduling a multifunction radar. *Aerospace Science and Technology 11*, 4 (2007), 289–294.

2008

[21] ARTIOUCHINE, K., BAPTISTE, P., AND DURR, C. Runway sequencing with holding patterns. *European Journal of Operational Research* (2008). To appear.

[22] ARTIOUCHINE, K., BAPTISTE, P., AND MATTIOLI, J. The k king problem, an abstract model for computing aircraft landing trajectories : On modeling a dynamic hybrid system with constraints. *INFORMS Journal on Computing* (2008). To appear.

[23] BAPTISTE, P., FLAMINI, M., AND SOURD, F. Lagrangian bounds for just-in-time job-shop scheduling. *Computers & Operations Research 35* (2008), 906–915.

[24] BAPTISTE, P., JOUGLET, A., AND SAVOUREY, D. Lower bounds for parallel machine scheduling problems. *International Journal of Operational Research* (2008). To appear.

[25] JAWOR, W., CHROBAK, M., AND DÜRR, C. Competitive analysis of scheduling algorithms for aggregated links. *Algorithmica* (2008).

[26] JOUGLET, A., SAVOUREY, D., CARLIER, J., AND BAPTISTE, P. Dominance-based heuristics for one-machine total cost scheduling problems. *European Journal of Operational Research* (2008). To appear.

National journals

2005

[27] DAC, H. T., AND BAPTISTE, P. Airspace sectorization with constraints. *RAIRO Operations Research 39* (2005), 105–122.

International conferences with proceedings

2004

[28] BAPTISTE, P., AND BRUCKER, P. Scheduling parallel machines to minimize total completion time and total number of late jobs. In *Proceedings of the Proc. of the 9th International Workshop on Project Management and Scheduling* (2004).

[29] BAPTISTE, P., AND SOURD, F. Lower bounds for the earliness-tardiness scheduling problem on parallel machines. In *Proceedings of the Proc. of the 9th International Workshop on Project Management and Scheduling* (2004).

[30] BAULAND, M., CHAPDELAINE, P., CREIGNOU, N., HERMANN, M., AND VOLLMER, H. An algebraic approach to the complexity of generalized conjunctive queries. In *Proceedings 7th International Conference on Theory and Applications of Satisfiability Testing, (SAT 2004), Vancouver (British Columbia, Canada)* (May 2004), H. H. Hoos and D. G. Mitchell, Eds., vol. 3542 of *Lecture Notes in Computer Science*, "Springer-Verlag", pp. 30–45.

[31] GIL, A., HERMANN, M., SALZER, G., AND ZANUTTINI, B. Efficient algorithms for constraint description problems over finite totally ordered domains. In *Proceedings 2nd International Joint Conference on Automated Reasoning (IJCAR'04). Cork (Ireland)* (July 2004), D. Basin and M. Rusinowitch, Eds., vol. 3097 of *Lecture Notes in Computer Science*, "Springer-Verlag", pp. 244–258.

[32] GOTTLOB, G., HERMANN, M., AND RUSINOWITCH, M. 2nd International Workshop on Complexity in Automated Deduction (CiAD) – Foreword. *Theory of Computings Systems 37*, 6 (2004), 639–640.

[33] GWIGGNER, C., BAPTISTE, P., AND DUONG, V. Some spatio-temporal characteristics of the planning error in European ATFM. In *Proceedings of the IEEE Intelligent Transportation Systems Conference. ITSC 2004* (2004), Washington D.C., U.S.A., IEEE Press.

2005

[34] ARTIOUCHINE, K., AND BAPTISTE, P. Interdistance constraint : An extension of the all-different constraint for scheduling equal length jobs. In *Proc. of the 11th International Conference, CP (Principles and Practice of Constraint Programming)* (Sitges, Spain, 2005), vol. 3709 of *Lecture Notes in Computer Science*.

[35] BAPTISTE, P., CHROBAK, M., DURR, C., AND SOURD, F. Preemptive multi-machine scheduling of equal length jobs to minimize the average flow time. In *Models and Algorithms for Planning and Scheduling Problems, Siena, Italy* (2005).

[36] PAPE, C. L., AND BAPTISTE, P. Scheduling a single machine to minimize a regular objective function under setup constraints. In *2nd Multidisciplinary International Conference on Scheduling : Theory and Applications* (2005).

2006

[37] BAHADUR, A., DÜRR, C., KULKARNI, R., AND LAFAYE, T. Quantum query complexity in computational geometry. In *Proc. of the Conference on Quantum Information and Computation IV by The International Society for Optical Engineering (SPIE)* (2006).

[38] BAPTISTE, P. Scheduling unit tasks to minimize the number of idle periods : A polynomial time algorithm for offline dynamic power management. In *Proc. of SODA'06, ACM-SIAM Symposium on Discrete Algorithms* (2006).

[39] BAPTISTE, P., AND SADYKOV, R. Compact mip formulations for minimizing total weighted tardiness. In *10th International Workshop on Project Management and Scheduling* (2006).

[40] DÜRR, C., AND HURAND, M. Finding total unimodularity in optimization problems solved by linear programs. In *Proc. of the 14th Annual European Symposium on Algorithms (ESA)* (2006), pp. 315–326.

[41] GWIGGNER, C., AND DUONG, V. Averages, Uncertainties and Interpretation in Flow Planning. In *Proceedings of the 2nd International Conference on Research in Air Transportation* (2006), Belgrad, Serbia.

[42] HERMANN, M., AND VORONKOV, A., Eds. *Proceedings 13th International Conference : Logic for Programming, Artificial Intelligence, and Reasoning (LPAR 2006)* (Phnom Penh (Cambodia), Nov. 2006), vol. 4246 of *Lecture Notes in Artificial Intelligence*, Springer Verlag.

[43] JAWOR, W., CHROBAK, M., AND DÜRR, C. Competitive analysis of scheduling algorithms for aggregated links. In *Proceedings of Latin American Theoretical INformatics (LATIN)* (2006), pp. 617–628.

[44] WINTER, E., AND BAPTISTE, P. On scheduling a single machine to minimize a function of distances between pairs of tasks : Scheduling a multifunction radar. In *International Conference on Service Systems and Service Management* (2006).

[45] WINTER, E., AND LUPINSKI, L. On scheduling the dwells of a multifunction radar. In *International Conference on Radar* (2006).

2007

[46] BAPTISTE, P., CHROBAK, M., AND DÜRR, C. Polynomial time algorithms for minimum energy scheduling. In *Proc. of the 15th Annual European Symposium on Algorithms (ESA)* (2007).

[47] BAPTISTE, P., KONONOV, A., AND SVIRIDENK, M. New lower bound for the flow shop scheduling. In *Eighth Workshop On Models And Algorithms For Planning And Scheduling Problems* (2007).

[48] CHAPDELAINE, P., HERMANN, M., AND SCHNOOR, I. Complexity of default logic on generalized conjunctive queries. In *Proceedings 9th International Conference on Logic Programming and Nonmonotonic Reasoning (LPNMR 2007), Tempe (Arizona, USA)* (May 2007), C. Baral, G. Brewka, and J. Schlipf, Eds., vol. 4483 of *Lecture Notes in Artificial Intelligence*, Springer Verlag, pp. 58–70.

[49] CHROBAK, M., AND HURAND, M. Better bounds for incremental medians. In *Proc. 5th Workshop on Approximation and Online Algorithms (WAOA)* (2007).

[50] CHROBAK, M., HURAND, M., AND SGALL, J. Fast algorithms for testing fault-tolerance of sequenced jobs with deadlines. In *Proc. 28th IEEE Real-Time Systems Symposium (RTSS)* (2007).

[51] HERMANN, M., AND PICHLER, R. Counting complexity of propositional abduction. In *20th International Joint Conference on Artificial Intelligence (IJCAI 2007)* (Jan. 2007), M. M. Veloso, Ed., AAAI Press, pp. 417–422.

[52] NGUYEN, K. T., AND DÜRR, C. Nash equilibria in Voronoi games on graphs. In *Proc. of the 15th Annual European Symposium on Algorithms (ESA)* (2007).

[53] WINTER, E., AND SADYKOV, R. Computing lower bounds for the schedule of a multifunction radar. In *MISTA 2007* (2007).

National conferences with proceedings

2004

[54] SAVOUREY, D., JOUGLET, A., BAPTISTE, P., AND CARLIER, J. Méthode tabou pour minimiser le retard total pondéré sur une machine avec dates de disponibilité. In *MOSIM, Conférence Francophone de Modélisation et Simulation* (2004).

2005

[55] ARTIOUCHINE, K., BAPTISTE, P., AND MATTIOLI, J. Le problème des n-rois : un modèle des systèmes dynamiques. In *Sixième congrès de la société Française de Recherche Opérationnelle et Aide à la Décision* (2005).

[56] BAPTISTE, P., AND BRUCKER, P. Scheduling equal processing time jobs on parallel machines : A survey. In *Troisieme Conference Internationale en Informatique Recherche, Innovation & Vision du Futur* (Can Tho, Vietnam, 2005).

[57] BAPTISTE, P., CROCE, F. D., GROSSO, A., AND T'KINDT, V. On some compact integer programming formulations of machine scheduling problems. In *Sixième congrès de la société Française de Recherche Opérationnelle et Aide à la Décision* (2005).

[58] GWIGGNER, C., BAPTISTE, P., AND DUONG, V. Conditions et lois : une analyse des données du trafic aérien. In *Sixième congrès de la société Française de Recherche Opérationnelle et Aide à la Décision* (2005).

[59] SAVOUREY, D., JOUGLET, A., AND BAPTISTE, P. Règles de dominance pour l'ordonnancement de jobs avec dates de disponibilité sur machines parallèles. In *Sixième congrès de la société Française de Recherche Opérationnelle et Aide à la Décision* (2005).

[60] WINTER, E., BAPTISTE, P., LUPINSKI, L., AND CHAMOUARD, E. Modélisation des problèmes d'ordonnancement de tâches sur des radars embarqués. In *Sixième congrès de la société Française de Recherche Opérationnelle et Aide à la Décision* (2005).

2006

[61] E. WINTER, P. B. On scheduling a multifunction radar. In *Commande, Optimisation, Gestion Intelligente et architecture des Senseurs pour les systèmes* (2006).

2007

[62] BAPTISTE, P., AND SADYKOV, R. A new mip formulation for single machine scheduling. In *Conférence conjointe FRANCORO V / ROADEF 2007* (2007).

[63] NANNICINI, G., BAPTISTE, P., KROB, D., AND LIBERTI, L. Fast point-to-point shortest path queries on dynamic road networks with interval data. In *Cologne/Twente Workshop on Graphs and Combinatorial Optimization 2007, CTW 200* (may 2007).

[64] SAVOUREY, D., BAPTISTE, P., AND JOUGLET, A. Méthode exacte pour problèmes à machines parallèles. In *Conférence conjointe FRANCORO V / ROADEF 2007* (2007).

Dissemination

2005

[65] HERMANN, N., AND LESCANNE, P. Est-ce que « P = NP » ? *Les Dossiers de La Recherche 20* (août-octobre 2005), 64–68.

PhD Thesis

2006

[66] ARTIOUCHINE, K. *Optimisation combinatoire et contrôle aérien : Planification des horaires et des trajectoires*. PhD thesis, Ecole Polytechnique, 2006.

2007

[67] GWIGGNER, C. *Analyse des incertitudes dans les flux du trafic aérien*. PhD thesis, Ecole Polytechnique, 2007.

Miscellaneous

2007

[68] GWIGGNER, C. Consequences of independence assumptions in ATFM. *Submitted to International Journal of Production Research* (2007).

2008

[69] GWIGGNER, C. Propagation of airspace congestion. A vector correlation analysis. *Submitted to 3rd International Conference on Research in Air Transportation* (2008).

Bioinformatique

Team members

Team leader

Jean-Marc STEYAERT

Permanent members

- Philippe CHASSIGNET, maître de conférences à l'École polytechnique
- Pierre NICODÈME, Chargé de recherches CNRS
- Jean-Marc STEYAERT, professeur à l'École Polytechnique

Phds

- Jérôme WALDISPÜHL, ATER-Paris 7, until September 2004
- Behshad BEHZADI, allocation AMX, until September 2005
- Quang THAI, allocation AMX then ALCYANE consultant, since October 2003
- Xavier WERTZ, allocation Institut Pasteur-Collège de France, since October 2005
- Mohamed GANJTABESH, co-tutelle Iran, from October 2006 to September 2007
- Van Du Thuong TRAN, allocation AMX, since October 2007
- Mahsa BEHZADI, allocation MRES, since October 2007

Interns

- Abdulaziz Al HARBI, ENSIETA, from April to June 2005
- Fheed Al SUBAIE, ENSIETA, from April to June 2005
- David MAROLLEAU, master Bioinformatique de Poitiers, from May to September 2005
- Hamed AMINI, Ecole polytechnique, from May to September 2005
- Irina-Mihaela DRAGOMIR, from November 2005 to April 2006
- Daniel VOINEA, Ecole polytechnique, from November 2005 to April 2006
- Yang ZHOU, master BIBS-Orsay, from March to July 2006
- Mishal Al BAHOUTH, ENSIETA, from April to

June 2006
- Humoud Al NGHIMSHI, ENSIETA, from April to June 2006
- Mahsa BEHZADI, master 1 Ecole polytechnique, from May to September 2006
- Mahsa BEHZADI, master 2 Ecole polytechnique, from May to September 2007
- Thuong Van Du TRAN, master 2 Ecole polytechnique, from May to September 2007
- Dheeraj MEHRA, bachelor IIT-Delhi, from June to July 2007
- Vaibhav SINGH, bachelor IIT-Delhi, from June to July 2007

PostDocs

- Valentina BOEVA, École Polytechnique, from March 1st, 2007 to March 31st, 2008

Guests

- Peter CLOTE, Professor at Boston College, April 2007
- Laurent SCHWARTZ, Medical doctor, PhD, AP-HP, since 2006

Research domain

The Bioinformatics team develops and uses tools from more traditional aeras of computer science : combinatorics, formal language theory, complexity, algorithmics and geometry. The goal is to explain biological phenomena, most of them relevant to classical cell mechanisms, by appropriate modelling of the physical or chemical configurations. Several types of questions can then arise which provide information useful to the biologist :
— Is the configuration standard or exceptional ? To what extent does it correspond to some interesting biological phenomemon ?
— What is the best possible configuration that can be obtained w.r.t. some physical criteria ?
— Is it possible to reconstruct the configuration from another one, according to a set of rules ? What is the optimal way to perform the reconstruction ?
These examples are typical of the activity of a bio-computer-scientist, whose main purpose is to propose combinatorial models for biological phenomena in a first step, then to implement these models in a software or in a mathematical framework, and finally to produce informations that can be interpreted by biologists.
Typical applications are : identification of binding sites on the genome, structure prediction for RNAs and proteins, evolution distances in order to construct philogenetic trees.

Goals

We have been working on five main problems :
1. the identification of transmembrane proteins with alpha-bundels or beta-barels ;
2. the computation of the distributions of thermodynamic energies for RNA structures without pseudoknots ;
3. the distribution of q-grams in random sequences by means of analytic combinatorics ;
4. the computation of the evolutionary distance for minisatellites under several models ;
5. softwares and statistics for medical studies related to cancer.

Results

The first four goals enumerated in the preceeding section all pertain to the same classical aera of combinatorial modelling and algorithmics. The first two are in fact a core problem which has been studied in the team for years, starting in the 90's : how is it possible to model biological structures such as RNAs and proteins — at least some non trivial families — in order to design efficient tools for structure prediction and for the evaluation of energy distributions. After some years of continuous work we now have developed computer and mathematical tools that are operational.
The third and fourth are classical combinatorial and algorithmic problems relevant to sequence analysis.
The last series aggregates a number of questions inspired by our contacts with biologists and medical doctors. The tools come from computer science but also include statistical methods, simulations, signal analysis, control theory, etc. This activity is new in many respects.

Transmembrane proteins (P. Chassignet, J.-M. Steyaert, J. Waldispühl)

A great deal of this work has been done by J. Waldispühl from the background of the gene-

ric software MTSAG which was the main result of F. Lefebvre's PhD thesis in 1997 — "Grammaires S-attribuées multi-bandes et applications à l'analyse de séquences biologiques". In his PhD thesis, defended in November 2004 [13], J. Waldispühl proposed two combinatorial models based on multitape S-attributed grammars to express the fact that a sequence of aminoacids is amenable to form a bindel or a barrel composed of alpha-helices or beta-strands. In these models three difficulties have to be tackled :
1. Express in terms of qualitative constraints the properties of the sequence of aminoacids that is supposed to rearrange spatially into a barrel : local properties (regular type) are required to express the capacity of a 12-20 polypeptidic sequence to form an alpha-helix or a beta-strand ; in order to express the links between two adjacent strands or helices we can use contextfree grammars, but in fact we do have two sets of overlapping CF constraints to express ; and furthermore the last constraint is between two strands that are far apart on the original sequence.
2. The second difficulty is to determine the solidity of the structure that we propose as a tentative secondary structure ; therefore one has to express the internal and external interactions of the aminoacids in terms of the membrane nature and the hydrogen bonds between them. Some indications and values can be found in the litterature, but their accuracy is poor.
3. One could then think of optimizing the parameters by learning as has been done for previous softwares based on statistical learning ; the point is that the number of known structures is very small — less than a few dozens — so that learning is not that different from enumeration.
The first version of this work, dedicated to alpha-barrels has been published in [3].
Now, the full version of this software, named *transFold*, is operational and has been used by D. Marolleau on the bacteria E. coli in order to check the possibility to screen a whole genome, which has been done. A biproduct of this study is an easy discrimination criterion for globular proteins vs. transmembrane proteins derived from the pseudoenergy computed by *transFold* that has been implemented by an SVM.

Further work has been done with P. Clote (Boston College) and B. Berger (MIT) [4] in order to improve the values given to the hydrophobicity parameter and make *transFold* more selective depending on the type of membrane users are working with. The software can also be accessed on a Web server.

Recently, P. Chassignet, Tran Van Du and J.-M. Steyaert have started to develop new improvements for beta-barrels, based on a precise geometry of interactions between the two strands ; the energy function is new and the results obtained so far are promising. They have also developed a new interface to produce images at the PDB format.

RNAs energy distributions (B. Behzadi, M. Ganjtabesh, P. Nicodème, J.-M. Steyaert, J. Waldispühl)

The question of describing accurately the landscape of the free energies of RNA structures is a long addressed problem. However, no exact formula is known, even now. Some physicists have performed extensive computer simulations in order to give some intuition in the case of simple energy models. In 2002, B. Behzadi, J.-M. Steyaert and J. Waldispühl presented at ECCB a work on "an approximate matching algorithm for finding (sub-)optimal sequences in S-attributed grammars". In this paper they were investigating the variations in the energy of the optimal RNA structure induced by a small number of modifications (insertion, deletion or mutation) on a given sequence : the energy model was Zuker model. Surprisingly, they illustrated on a number of examples that a few number of modifications can modify dramatically the RNA structure while improving drastically its stability.
With P. Clote they addressed the more general question of computing the partition function of the energies in the Nussinov model for RNA secondary structure. More exactly, they again make up to k modifications on the sequence and want to compute the landscape of the modified energies. No closed formula can be expected but they therefore designed an algorithm inspired by the one on S-attributed grammars which solves the problem. One is then able to compute numerically the tail distributions of the energy. Evidence is quite generally presented that the k-superoptimal secondary structure is often closer, as measured by base pair distance and two additional distance measures, to the secondary structure derived by comparative sequence analysis than that derived by the Zuker minimum free energy structure of the original (wild type or unmutated) RNA. This result [2] gives a more general basis to the observation made in 2002.

M. Ganjtabesh, a PhD student from Tehran, and J.-M. Steyaert have a few preliminary results as to the enumeration of RNA structures with pseudoknots un-

der a variety of constraints. They are able to obtain information on the generating functions for these structures and should get full asymptotics for the number of configurations.

M. Ganjtabesh, P. Nicodème and J.-M. Steyaert have also started with P. Clote a combinatorial study of the partition functions of RNAs, without pseudoknots, aiming at showing different behaviours at infinity according to the energy model : Nussinov vs. Turner or even more complex. A proved difference could be interpreted in terms of biological stability.

Combinatorics of q-grams (P. Nicodème)

Some alignment algorithms use a filtering preprocessing phase that discards putative alignments of two sequences with too few common q-grams ; P. Nicodème considered the associated probabilistic problem, as follows : given an integer q and a Bernoulli model, what could be said (i) of the number of repeated q-grams in one sequence, (ii) of the number of q-grams occuring at least once in each sequence ? Stated differently, question (i) relates to the number of internal nodes at depth q of a suffix-tree built over a random sequence, while question (ii) relates to the superposition of two suffix-trees with a color assigned to each tree, and counting the number of bicolored nodes at depth q.

P. Nicodème has improved upon his previous work [9] presented at Discrete Random Walks'03 and on works by P. Jacquet and W. Szpankowski and gives a more precise analysis of the average profiles of tries and suffix-trees. Using Poissonization-Depoissonization, the progress for the analysis of tries profile was done by using Mellin transform techniques ; this required use of an inverse Mellin transform that needed application of saddle-point integrals ; Pierre Nicodème's work [9] did not solve completely the problem, but laid the foundations for the full proof obtained later in collaboration with G. Park (University of Wisconsin), Hsien-Kuei Hwang (Academica Sinica, Taiwan) and W. Szpankowski (University of Purdue). In particular he remarked that there are on the vertical line of inverse Mellin integration an infinite number of saddle-points.

Since 2005, These four coauthors have given a full characterization of the profiles of the tries, including the second moment and the limiting distribution. The corresponding quite technical article has been submitted and is available on Archive.

A joint work of F. Bassino (Université of Marne-la-Vallee), J. Clément (Université de Caen), J. Fayolle (Université d'Orsay) and P. Nicodème [10] solved the problem of words counting in random texts, in the general case where a word can be a factor of another word, also known as non-reduced case. This was known to have a solution by constructing the Aho-Corasick automaton and translating into generating functions by the Chomsky-Schützenberger algorithm. There seemed to be no direct solution available ; however Noonan and Zeilberger (1999) proposed Maple programs solving the problem by inclusion-exclusion ; their publication remained mostly unnoticed in the combinatorial and applied probability communities ; Bassino, Clément, Fayolle and Nicodème then rediscovered the method, providing explicit formulas and adding proofs of correctness. The method relays on an extension of the Goulden-Jackson approach (1979). They plan to extend the result to the case of Markov or dynamical sources.

Minisatellites and evolution distances (B. Behzadi, J.-M. Steyaert)

Minisatellite maps are special regions in the genome whose evolution is rather special and in the long range produces sequences of short repeated units, called variants. The typical length of a variant is 20-40 nucleotids and a sequence is composed of blocks of a variant repeated 5-100 times. Such sequences can be found for instance in the Y-specific locus MSY1, a haploid minisatellite of the Y chromosome, and are used to trace male descendence proximity in populations.

In order to compare minisatellite sequences, one usually considers a evolutionary model with five operations : amplification, contraction, mutation, insertion and deletion with variable hypotheses concerning the respective costs of the operations. The problem is to find as fast as possible one or all the possible evolutions of smallest cost, given a model.

B. Behzadi and J.-M. Steyaert have designed several algorithms [14, 7, 8, 1] which improve on the first results by Bérard and Rivals in three ways : the model is more general with arbitrary costs, long runs of the same variant are encoded by their lengths and ultimately the algorithms are more efficient. More recently with M. Abouelhoda and R. Giegerich (Ulm and Bielefeld) [11], they propose a new algorithm for the alignment of minisatellite maps based on the computation of a minimum spanning tree.

Medical studies related to cancer (M. Behzadi, V. Boeva, L. Schwartz, J.-M. Steyaert, X. Wertz)

The presence in the team of L. Schwartz, a cancer specialist, introduced a new activity of slightly different nature : develop mathematical and computational tools and concepts to explain and analyze this phenomenon.
We got an important funding from Philip Morris in order to study cancer epidemiology with a group of statisticians originating from Paris-Dauphine. We have shown, [6, 12], that the evolution of cancers depends mainly on the way of living, food habits and general activities. In order to get these results we have developed new tools for datamining and statistic analysis that allow an efficient treatment of temporal series.
These results suggest then new questions about cancer and progressive changes in the cell metabolism. Starting from a monography on cell metabolism by M. Israel and L. Schwartz, M. Behzadi, V. Boeva, L. Schwartz and J.-M. Steyaert have started a simulation of a number of metabolic cycles linked to energy consumption and glucose transformations in the cell.
X. Wertz and P. Chassignet have worked on bone growth and have discovered a possible link between mechanical activity and growth during childhood [5]. A more mathematical approach is being developed from this observation.
Finally X. Wertz is implied in a big project of software engineering with P. Kourilsky at College de France and Institut Pasteur. The goal of this project is to analyze as automatically as possible the immunitary response of children that have received a genetic therapy. The new version of *Immunoscope* is now almost operational and should receive some new improvements allowing a more precoce diagnosis of cancerous evolution.

Software, pattents and contracts

Software

transFold
This software analyzes protein sequences and tries to determine whether they correspond to possible transmembrane proteins. *transFold* develops the general approach of multi-tape S-attribute grammars for the structure prediction of both TM alpha-helical bundles and of TM beta-barrels ; the web server allows one to stipulate the pore type as being either non water-filled or water-filled (see original papers for more details). Other parameters are automatically assigned default values by the web server.
http ://bioinformatics.bc.edu/clotelab/transFold/

Patents

We have initiated in 2005 the patent deposit process for our software *transFold*, but after two years we have stopped.

Contracts

– Contract with Philip Morris : The goal of the studies are to perform data mining and exploratory statistics on public data related to cancer and way of living. (covers 2004 to 2007).

Teaching, communication and service

P. Chassignet organizes labs for two courses, INF311 and INF431. He is a major actor in the maintenance of software environments for teaching and represents the Department in a number of organisational meetings.

J.-M. Steyaert teaches the second part of INF431 (the major course of Year 2) and teaches in Year 3 (Automata-Langages-Computability) and prepares a new course on Datamining ; he also participates to a course on Bioinformatics. In Master MPRI, he proposes a series of lectures on combinatorics related to biology. J.-M. Steyaert is chair of the Department and has been elected as member of the Conseil d'Administration. He is also correspondent for Computer Science in ParisTech.

J.-M. Steyaert has organized with R. Khosrovshahi and M. Shahshahani (IPM Iran) a Spring school on Bioinformatics and Biomathematics in April 11-21, 2005

Visibility

National scientific cooperations

– Program PGP (2003-2006) : with T. Simonson (LBIOC, Polytechnique) and P. Dessen (Institut Gustave Roussy) : Protein Struture Prediction.
– ACI IMPBio-2004 : with T. Meinnel (ISV, Gif/Yvette) and F. Dardel (Univ. Paris 5-Pharmacy) : A study about N-Myristilation.

International scientific cooperations

- with Boston College : several articles coauthored with Peter Clote (Boston College) ; hiring of Jérôme Waldispühl as research assistant ; Regular visits of Peter Clote at École Polytechnique as invited professor.
- Regular cooperation with IPM-Iran and the University of Tehran ; joint Phd of M. Ganjtabesh with Pr Ahrabian (University of Tehran). and J.-M. Steyaert.
- Frequent one month visits of P. Nicodème to M. Vingron at the MPI for Molecular Genetics in Berlin (2005-2007).

Seminar invitations

- P. Nicodème gave a talk in 2005 at the Free-University of Berlin-Dahlem to the group of Bioinformatics and in 2006 at the bioinformatics group of MIT, Boston.
- J.-M. Steyaert gave talks at the University of Tehran in 2005, 2006 and 2007 ; he has been invited by M. Vingron at the MPI for Molecular Genetics in 2006.
- J.-M. Steyaert has been invited as keynote speaker at RIVF'07 in Hanoi (VietNam).

Conference organisation

- P. Nicodème has organized the LIX Automn Colloquium on Bioinformatics in 2005.

Program committees

- J.-M. Steyaert was in the program committee of CISCC'06 in Tehran (Iran).

Journal editorial boards

- J.-M. Steyaert is member of the editorial board of RAIRO-"Theoretical informatics and Applications" and of the Journal of Virology.

References

International journals

2005

[1] BEHZADI, B., AND STEYAERT, J.-M. An improved algorithm for generalized comparison of minisatellites. *J. Discrete Algorithms 3* (2005), 375–385.

[2] CLOTE, P., WALDISPÜHL, J., BEHZADI, B., AND STEYAERT, J.-M. Energy landscape of k-point mutants of an rna molecule. *Bioinformatics 21* (2005), 4140–4147.

[3] WALDISPÜHL, J., AND STEYAERT, J.-M. Modeling and predicting all-alpha transmembrane proteins including helix-helix pairing. *Theor. Comput. Sci. 335* (2005), 67–92.

2006

[4] WALDISPÜHL, J., BERGER, B., CLOTE, P., AND STEYAERT, J.-M. transfold : a web server for predicting the structure and residue contacts of transmembrane beta-barrels. *Nucleic Acids Research (Web-Server-Issue) 34* (2006), 189–193.

[5] WERTZ, X., SCHWARTZ, L., SCHOËVAËRT, D., MAITOURNAM, H., AND CHASSIGNET, P. Is the effect of testosterone on bone growth mediated through mechanical stresses ? *C.R.A.S. Biologies 329* (2006), 79–85.

National journals

2006

[6] GETTLER-SUMMA, M., STEYAERT, J.-M., VAUTRAIN, F., SCHWARTZ, L., AND HAFNER, N. Multiple time series : new approches and new tools in data mining ; applications to cancer epidemiology. *revue MODULAD* (2006), 37–46.

International conferences with proceedings

2004

[7] BEHZADI, B., AND STEYAERT, J.-M. The minisatellite transformation problem revisited : A run length encoded approach. In *Algorithms In Bioinformatics : 4th International Workshop, WABI 2004, Bergen, Norway, September 17-21, 2004* (2004), I. Jonassen and J. Kim, Eds., vol. 3240 of *LNBI*, Springer-Verlag, pp. 290–301.

[8] BEHZADI, B., AND STEYAERT, J.-M. On the transformation distance problem. In *String Processing And Information Retrieval : 11th International Conference, Spire 2004, Padova, Italy, October 5-8, 2004* (2004), A. Apostolico and M. Melucci, Eds., vol. 3246 of *LNCS*, Springer-Verlag, pp. 310–320.

2005

[9] NICODÈME, P. Average profiles, from tries to suffix-trees. In *Proceedings of the 2005 Conference on Analysis of Algorithms* (2005), DMTCS, proc. AD, pp. 257–266. Barcelona.

2007

[10] BASSINO, F., CLÉMENT, J., FAYOLLE, J., AND NICODÈME, P. Counting occurrences for a finite set of words : an inclusion-exclusion approach. In *Proceedings of the 2007 Conference on Analysis of Algorithms* (2007), DMTCS, pp. 29–42. Juan-Les-Pins.

2008

[11] ABOUELHODA, M., GIEGERICH, R., BEHZADI, B., AND STEYAERT, J.-M. Alignment of minisatellite maps : A minimum spanning tree based approach. In *Sixth Asia Pacific Bioinformatics Conference Kyoto, Japan, 14-17 January 2008* (2008), Advances in Bioinformatics and Computational Biology. "a paraitre".

National conferences with proceedings

2006

[12] GETTLER-SUMMA, M., STEYAERT, J.-M., AND VAUTRAIN, F. New approaches in multiple multidimensional time series. application to geographical cancer trends clustering. In *Actes de EGC 2006 : Fouille de données temporelles* (2006), pp. 1–10. Villeneuve d'Ascq.

PhD Thesis

2004

[13] WALDISPÜHL, J. *Modélisation et prédiction de la structure des protéines transmembranaires*. PhD thesis, École Polytechnique, 2004. dir. J.-M. Steyaert.

2005

[14] BEHZADI, B. *Comparaison efficace de structures d'évolution de séquences : approche par la programmation dynamique*. PhD thesis, École Polytechnique, 2005. dir. J.-M. Steyaert.

Modèles Combinatoires

Team members

Team leader

Gilles SCHAEFFER

Permanent members

- Robert CORI, Professeur à l'École Polytechnique et à l'université Bordeaux I
- Daniel KROB, Directeur de recherches CNRS, professeur chargé de cours à l'École Polytechnique(until august 2006)
- Gilles SCHAEFFER, Directeur de Recherches CNRS, professeur chargé de cours à temps partiel à l'École Polytechnique
- Ekaterina VASSILIEVA, Chargée de recherche au CNRS.

Phds

- Luca Castelli ALEARDI, bourse de l'université de Milan et du ministère des affaires étrangères. Phd defended the 12th of december, 2006
- Eric FUSY, corps des télécoms, détaché à l'INRIA Rocquencourt. PhD defended the 11th of june, 2007
- Guillaume CHAPUY, bourse AMN, since september 1st, 2007.

Guests

- Pr. M. BODIRSKY, Humbold U. Berlin, invited researcher (one week, winter 2006)
- Dr. M. KANG, Humbold U. Berlin, invited researcher (one week, winter 2006)
- Pr. S. RINALDI, Siena U., invited researcher (one week, autumn 2006).

Research domain

Keywords Graph embeddings and colorings, enumeration, random discrete structures, analysis and design of algorithms and data structures, combinatorics in statistical physics.

Presentation Our main domain of interest is combinatorics and its algorithmic aspects. We believe that a key to efficient algorithms often lies in combinatorial properties of the fundamental structures of computer science, like words, trees or graphs. Our aim is to study these combinatorial models, ranging from elementary algorithms on words or graphs (depth/breadth first searches, orientations, colorings, pattern occurrences...) to dynamical systems (chip firing games, jumping particles,...), that are often not only of interest in computer science but also in mathematics and statistical physics. A typical instance of our approach starts from enumerative results which are used to uncover deep combinatorial properties and develop algorithmic consequences, with a particular emphasis on compact data structures and combinatorial representation of geometric objects.

Goals

During the last three years compact data structures for geometric structures have attracted a lot of our interest and we believe that this line of research is fruitful in the context of massive data structures. We aim particularly at optimal compacity results, which by essence rely very much on combinatorial methods.

At a more fundamental level we pursue the study of colorings and graph exploration processes for embedded graphs. Classical algorithms like breadth- or depth-first-search have remarkable properties when applied to embedded graphs. Understanding these properties leads to various results ranging from encodings and data structures as mentioned above to interactions with statistical physics and average case analysis of graph algorithms.

Results

Embedded graphs and maps A large part of our research is concerned with the topic of embedded graphs and more precisely of planar maps. The notion of planar map is for 2d geometric objects (discretized surfaces, tilings, etc) what the combinatorial concept

of tree is to tree-like structures : a mathematical abstraction which is very useful to study the generic properties of these structures.

The combinatorics of classical graph exploration processes. We have discovered the recurrent existence in numerous types of maps of some canonical covering trees associated to the classical graph exploration processes (breadth first search, depth first search, etc), which can be completely characterized in terms of context free grammars. For instance, to any planar triangulation, D. Poulalhon and G. Schaeffer [12] associate a unique tree that encodes it, in a way that the set of trees we use is simple to describe (in this case, the set of plane trees such that each inner node is adjacent to exactly two leaves).

These remarkable combinatorial properties were first found while trying to understand the remarkably simple enumeration formulas that W.T. Tutte derived in the 60s for the enumeration of planar maps. The postulate of bijective combinatorics, driving part of our research, is that any nice formula should be explained by an elegant combinatorial property. This is indeed what we was able to show in the previous example : the number of triangulations with n vertices is given by a simple formula because to each triangulation is associated a tree and it is well known that these trees are easy to count.

Several results of this type were obtained in our group, uncovering unexpected relations between various classical combinatorial result. In particular E. Fusy and G. Schaeffer, in collaboration with D. Poulalhon were able to relate 3-connected planar graphs and binary trees [18] on one hand, bipolar structures on maps and non crossing triple of Dyck paths on the other hand [29]. E. Fusy obtained relations between simple quadrangulations and ternary trees, and between irreducible triangulations and quaternary trees. In a slightly different context G. Schaeffer and E. Vassilieva proposed a bijection relating bicolor unicellular maps (not necessarily planar) to plane trees and partial permutations using a variant of the famous last passage tree construction used in the proof of the BEST theorem for the number of Eulerian circuits in a graph [24].

As we will see, these combinatorial results, at first suggested by enumeration, have various consequences in quite different directions.

The algorithmics of maps. New properties of classical graph exploration processes naturally find their first applications in algorithmics. As a matter of fact the definition of simple canonical covering trees has allowed us to develop the first asymptotically optimal encoding algorithms for triangulations and more generally for various types of planar maps. Here optimality means that no encoding exists that would use shorter words in the worse or average case. Another type of algorithmic application is illustrated by the results of E. Fusy on automatic drawing of graphs and by the average quality analysis that we have developped for these drawings [17, 23].

All these algorithms require linear running time (encoding, decoding, sampling or drawing), and their simplicity has allowed that they be implemented and used both in and outside our group.

Relations with quantum geometry and enumerative topology. We have also shown how to use these new combinatorial properties of classical exploration processes to study the intrinsic metric of the standard discretized version of 2d quantum geometry, uncovering a link that has a number of sequels in statistical physics and probability. Indeed the objects that we consider happen to be underlying a model of random discrete surfaces that is widely considered in physics to model quantum geometry in dimension 2. Rougly speaking, for the purpose of quantum geometry, the standard euclidian metric must be replaced by a random metric, and a good discrete approximation of this random metric is given by the graph metric on uniform random planar maps.

The study of such a family of trees with P. Chassaing had lead us a few years ago to propose the first method allowing to obtain results on the intrinsic metric of these random surfaces in their infinite discrete and rescaled limits (another method was simultanement proposed by O. Angel for the infinite discrete limit (Angel 2005). Our work, which builds on earlier constructions by Cori and Vauquelin (Cori-Vauquelin 1984), has been used and extended in particular by J. Bouttier et al. (Bouttier-Di Francesco-Guitter 2005) to compute some critical exponents describing the metric of these random surfaces that had been conjectured before. They were also at the origin of a series of papers in probability trying to describe the continum scaling limit of these discrete random surfaces (Marckert-Mokkadem 2005), culminating with

the recent work of J.F. Le Gall and F. Paulin proving that the possible limits can only be spheres (Le Gall 2007). Recently we have obtained new combinatorial results in this direction that open the way to an extension of the theory beyond the planar case, to higher genus surfaces.

Compact data structures The optimal encoding algorithm proposed by D. Poulalhon and G. Schaeffer for triangulations (as already discussed above) has raised some interest in computational geometry and computer graphics community, in relation with mesh compression. Indeed, as shown by Isenburg and Snoeyink [31], our algorithm can be reformulated in the context of conquest encoding algorithms, and from this point of view we have shown that the exceptional codes used by these algorithms can be avoided, at least in the case of meshes with spherical topology.

These connections with mesh compression have led us to consider more generally the design of compact representations for geometric data structures, which attracts currently a large attention in relation with the general problematics of the treatment of large data sets. As opposed to compression, intended for storage or transmission, the aim is here to develop compact representations that can be considered as valid data structures, in the sense that they efficiently support query on the objets without requiring decompression.

In this context, L. Castelli Aleardi and G. Schaeffer have developed, with O. Devillers, a series of compact data structures for various types of meshes : in particular we obtained asymptotically optimal solutions for triangular and polygonal meshes with boundaries [15, 20, 14]. These works have inspired more practical solutions, proposed in a further work in collaboration with A. Mebarki and O. Devillers [19]. These results were developed in the framework of the cooperative project ACI GeoComp.

Going further in this direction, L. Castelli Aleardi, with J. Barbay, M. He and I. Munro [25] have recently proposed the first succinct representation for the case of labelled graphs

Combinatorics and non-equilibrium statistical physics. As opposed to the relations between enumerative combinatorics and classical (equilibrium) statistical physics, the link between enumerative combinatorics and non-equilibrium statistical physics has not been much explored. In this context G. Schaeffer has studied with E. Duchi a fundamental model of transportation of particles called the one-dimensional asymmetric simple exclusion process. This process is a Markov chain which, although relatively simple to describe, has remarkable phase transition properties explaining that it has been studied for many years in physics and in probability.

In agreement with the above mentioned postulat of enumerative combinatorics, we have shown that the remarkable formulas of Derrida et al that describe the entries of the stationary distribution of this chain are the trace of deeper combinatorial properties of the model. In particular we were able to described these properties thanks to a covering of the basic Markov chain that has a particularly simple behavior [6]. Not only could we give in this way elegant proofs of earlier results of Derrida, and new extensions of the model, but our method of proof has inspired further work (Corteel 2006, Williams 2007) and, together with an alternative elegant construction of O. Angel (Angel 2005), has been an ingredient in the remarkable solution of the k-type model by P. Ferrari and J. Martin (Ferrari-Martin 2005).

Boltzman random sampling. Boltzman sampling is a probabilistic method, proposed by P. Duchon, P. Flajolet. G. Louchard and G. Schaeffer [4] to design random sampling algorithms, which is based on an fruitful analogy with technics of analytic combinatorics for the enumeration of combinatorial structures. Using this approach, E. Fusy [7] proposed the first uniform random sampler for planar graphs that run in quasi linear time (while the best known algorithms were in $O(n^5)$). E. Fusy has also extended the Boltzmann framework for structures subject to symmetries (unlabelled framework) [28, 26], and has developed very efficient Boltzmann samplers for plane partitions, in colaboration with Carine Pivoteau and Olivier Bodini [21]. More generally we believe that Bolzmann random sampling, in view of its simplicity and efficiency, should replace the previous random sampling tools based on the recursive method that are currently used in symbolic computation programs like `Maple` or in the design of test suite for programm checking.

Analytic Combinatorics for bioinformatics G. Chapuy has studied the combinatorial notion of "si-

milarity" between two lists, introduced by biostatisticians in the context of DNA chips : after modeling the problem in terms of a combinatorial statistics on random permutations, he studied the associated process and describes a continuous limit in terms of multivariate-time Gaussian processes [27].

Combinatorial Methods in Telecommunications A part of our research activities was focused on the application of combinatorial methods in the field of mobile communications. The first subject we addressed concerned the performance evaluation of demodulation protocols featuring diversity. D. Krob and E. Vassilieva [9] found out that a classical bijection of D. Knuth between binary matrices and Young tableaus of similar shape allowed the rewrite the Barret's Formula into a numerically stable expression. The second subject dealt with the use of a combinatorial approach to the issue of robust indexation of Gaussian vector quantizers commonly used in CDMA cellular telephony for encoding of non predictive components of voice within the eX-CELP protocol. E. Vassilieva, D. Krob and J. M. Steyaert [13] discovered that approximating the n-dimensional Gaussian law by the binomial law and using the natural bijection between binomial coefficients and binary words of a given hamming weight allowed to split a Gaussian vector quantizer in natural geometrical regions associated to code words of given Hamming weight. They proved that giving to each codevector of the Quantizer, a random codeword associated with the region it belongs to reduced very much the distortion due to one bit error during codeword transmission over the network with respect to random index assignment. They used this principle to derive a very low complexity algorithm for quantizer indexation outperforming classical combinatorial approaches in the field and by far faster than heuristic methods traditionally used.

Teaching, dissemination and service

R. Cori and G. Schaeffer manage the combinatorics programm in the Master Parisien de Recherche en Informatique (MPRI). Robert Cori also gives lectures within the computer science department of the Ecole Polytechnique (3rd year course in Advanced Algorithmics, and first year course in Programming Languages)

Visibility

National scientific cooperations

- Our team leads the *GeoComp* project within the french ACI « Masse de données », 2004-2007, bringing together teams from LIX, INRIA Sophia-Antipolis, LaBRI (université Bordeaux 1), and the theoretical physics center of the CEA Saclay.
- Our team took part in the projet « Structures Aléatoires Discrètes et Algorithmes » (*SADA*), funded by the french ANR for 2006-2009.

International scientific cooperations

- Luca Castelli Aleardi collaborates with researchers of the University of Waterloo (Ontario, Ca), a paper was recently written with J. Barbay, M. He and I. Munro.
- Eric Fusy colaborates with Bilyana Shoilekova, from Oxford, on graph enumeration problems, with Mihyun Kang and Manuel Bodirsky, from Humboldt Universitaet Berlin, on further extensions of the Boltzmann sampling framework and graph enumeration problems —two articles [26, 30], with Stefan Felsner, from Technische Universitaet Berlin, on bijective results related to orientations of planar structures — one article, and with Konstantinos Panagiotou, from ETH Zurich, on statistical properties of planar graphs.
- Gilles Schaeffer, in association with Enrica Duchi (LIAFA) regularly colaborates with researcher of the university of Siena, in particular an article was written in this period with Pr. S. Rinaldi. Gilles Schaeffer collaborates with Manuel Bodirsky and Mihyun Kang, from Humbold University in Berlin.

Conference and seminar invitations

Gilles Schaeffer gave seminars in the LIP general seminar at ENS Lyon, in the random surface working group of the math department of l'université Paris Sud, in INRIA Rocquencourt, invited talks and lectures at the 4th colloquium on Mathematics and Computer Science around algorithms, trees, combinatorics and probability, at the 54th Lotharingien seminar, at the 6th french workshop on computer geometry, at the

EMS-SCM joint workshop and at the CRM in Barcelona.

Robert Cori gave an invited talk at the international conference "SandPiles Models and Related Fileds (EURANDOM)" in Eindhoven (septembre 2007)

Éric Fusy gave seminars in the LIP general seminar at ENS Lyon, in the random surface working group of the math department of l'université Paris Sud, in INRIA Rocquecourt, at the 57th Lotharingien seminar, at the algorithmic seminar of ETH Zurich, at the algorithmic seminar of Humboldt Universitaet Berlin, at the weekly seminar on Discrete Mathematics at Technische Universitaet Berlin, at the seminar on Combinatorial Theory at Oxford, at the CRM in Barcelona, and gave an invited talk at the CRM in Montreal.

Conference organisation

- The team organized several short workshops (2-3 days) within the ACI Geocomp and ANR Sada framework.
- Robert Cori organized a workshop in october 2007 in Bordeaux in honor of Professor Knuth.

Program committees

- Gilles Schaeffer was in the PC of the 22th international *Symposium on Theoretical Aspects of Computer Science*, *STACS 2005*, in Stuttgart.
- Gilles Schaeffer was in the PC of the 19th international conference *Formal Power Series and Algebraic Combinatorics*, *FPSAC 2007*, in Nankin.
- Gilles Schaeffer was in the PC of the 4th international workshop *Analytic Algorithms and Combinatorics*, *ANALCO 2007*, in New Orleans.
- Gilles Schaeffer was in the PC of the 13th international conference *Analysis of Algorithms, AofA 2007*, in Juan les Pins.
- Éric Fusy is in the PC of the 5th international workshop *Analytic Algorithms and Combinatorics*, *ANALCO 2008*, in San Francisco.

Journal editorial boards

- Gilles Schaeffer is a member, since january 2007, of the advisory board of the *Journal of Combinatorial Theory, Series A*, edited by Elsevier.
- Gilles Schaeffer is a member, since 2005, of the editorial board of *ESAIM : Probability and Statistics* (European Society for Applied and Industrial Mathematics), edited by EDP Science.
- Gilles Schaeffer is a member, since 2006, of the editorial board of *PuMA, Algebra and Theoretical Computer Science*, edited by Budapest and Siena universities.

Awards

- Gilles Schaeffer's proposal for a communication about bijective combinatorics was selected by the *Académie des Sciences* and presented at the session "Recent advances in information and communication sciences", which took place on October 9th, 2007.
- Gilles Schaeffer received the "2007 European Price in Combinatorics" at the Real Alcazar of Sevilla in september 2007.

References

Books and chapters in books

2005

[1] POULALHON, D., AND SCHAEFFER, G. Counting, coding, and sampling with words. In *Applied Combinatorics on Words*, J. Berstel and D. Perrin, Eds. Cambridge University Press, 2005.

International journals

2004

[2] CHASSAING, P., AND SCHAEFFER, G. Random planar lattices and integrated superbrownian excursion. *Probability Theory and Related Fields 128*, 2 (2004), 161–212.

[3] CORTEEL, S., GOUPIL, A., AND SCHAEFFER, G. Content evaluation and class symmetric functions. *Advances in Mathematics 188*, 2 (2004).

[4] DUCHON, P., FLAJOLET, P., LOUCHARD, G., AND SCHAEFFER, G. Boltzmann random sampling. *Combinatorics, Probability & Computing 13*, 4-5 (2004), 577–625.

[5] FLAJOLET, P., SALVY, B., AND SCHAEFFER, G. Airy phenomena and analytic combinatorics of connected graphs. *Electronic Journal of Combinatorics 11*, 1 (2004), #R34, 1–30.

2005

[6] DUCHI, E., AND SCHAEFFER, G. A combinatorial approach of jumping particles. *Journal of Combinatorial Theory, Series A 110*, 1 (2005), 1–24.

[7] FUSY, É. Quadratic exact size and linear approximate size random generation of planar graphs. *Discrete Mathematics and Theoretical Computer Science AD* (2005), 125–138.

[8] SCHAEFFER, G., AND ZINN-JUSTIN, P. On the asymptotic number of planar curves and prime alternating knots. *Experimental Mathematics 13*, 4 (2005).

[9] VASSILIEVA, E., AND KROB, D. Performance evaluation of demodulation with diversity – a combinatorial approach ii : Bijective methods. *Discrete Applied Mathematics 145(3)* (2005), 403 – 421.

2006

[10] BACHER, R., AND SCHAEFFER, G. On generating series of coloured planar trees. *Journal du Séminaire Lotharingien de Combinatoire 55* (2006).

[11] BONICHON, N., GAVOILLE, N., HANUSSE, N. AND.POULALHON, D., AND SCHAEFFER, G. Planar graphs, via well orderly trees and triangulations. *Graph & Combinatorics 22*, 2 (2006), 185–202.

[12] POULALHON, D., AND SCHAEFFER, G. Optimal coding and sampling of triangulations. *Algorithmica 46*, 3-4 (2006), 505–526.

2007

[13] E. VASSILIEVA, D. K., AND STEYAERT, J. M. Using geometrical properties for fast indexation of gaussian vector quantizers. *EURASIP Journal on Advances in Signal Processing 2007* (2007), Article ID 63192, 11 pages. doi :10.1155/2007/63192.

International conferences with proceedings

2005

[14] ALEARDI, L. C., DEVILLERS, O., AND SCHAEFFER, G. Dynamic updates of succinct triangulations. In *Proc. of 17th Canadian Conference on Computational Geometry (CCCG)* (2005), pp. 135–138.

[15] ALEARDI, L. C., DEVILLERS, O., AND SCHAEFFER, G. Succinct representation of triangulations with a boundary. In *Proc. 9th Workshop on Algorhtms and Data Structures (WADS)* (2005), vol. 3608 of *LNCS*, Springer, pp. 134–145.

[16] DUCHI, E., AND SCHAEFFER, G. A combinatorial approach to jumping particles : the parallel tasep. In *Proc. 17th Intl. Conf. Formal Power Series and Algebraic Combinatorics* (Taormina, 2005).

[17] FUSY, É. Transversal structures on triangulations, with application to straight-line drawing. In *Proceedings of Graph Drawing'05* (2005), vol. 3843 of *LNCS*, Springer, pp. 177–188. Full paper to be published in Discr. Math., available at `http ://arxiv.org/abs /math.CO/0602163`.

[18] FUSY, É., POULALHON, D., AND SCHAEFFER, G. Dissections and trees, with applications to optimal mesh encoding and to random sampling. In *16th Annual ACM-SIAM Symposium on Discrete Algorithms* (2005). Full paper to be published in Transactions on Algorithms, available at `http ://algo.inria.fr/fusy /Articles/FuPoScArticle.pdf`.

2006

[19] ALEARDI, L. C., DEVILLERS, O., AND MEBARKI, A. 2d triangulation representation using stable catalogs. In *Proc. of 18th Canadian Conference on Computational Geometry (CCCG)* (2006), pp. 71–74.

[20] ALEARDI, L. C., DEVILLERS, O., AND SCHAEFFER, G. Optimal succinct representations of planar maps. In *Proc. of 22nd ACM Annual Symposium on Computational Geometry (SoCG)* (2006), pp. 309–318.

[21] BODINI, O., FUSY, É., AND PIVOTEAU, C. Random sampling of plane partitions. In *Gascom 2006* (Dijon, France, 2006), R. Pinzani and V. Vajnovszki, Eds., LE2I, pp. 124–135.

[22] DUCHI, E., RINALDI, S., AND SCHAEFFER, G. The number of z-convex polyominos. In *Proc. 18th Intl. Conf. Formal Power Series and Algebraic Combinatorics* (San Diego, 2006).

[23] FUSY, É. Straight-line drawing of quadrangulations. In *Proceedings of Graph Drawing'06* (2006), vol. 4372 of *LNCS*, Springer, pp. 234–239.

[24] VASSILIEVA, E., AND SCHAEFFER, G. A bijection for unicellular partitioned bicolored maps. *Formal Power Series and Algebraic Combinatorics (FPSAC'06)* (2006), 326 – 336.

2007

[25] BARBAY, J., ALEARDI, L. C., HE, M., AND MUNRO, I. Succinct representations of labeled graphs. In *Proc. of the Int. Symposium on Algorithms and Computation (ISAAC)* (2007). to appear.

[26] BODIRSKY, M., FUSY, É., KANG, M., AND VIGERSKE, S. An unbiased pointing operator for unlabeled structures, with applications to counting and sampling. In *18th ACM-SIAM Symposium on Discrete Algorithms, New Orleans* (2007), pp. 356–365.

[27] CHAPUY, G. Random permutations and their discrepancy process. In *Proc. of Intl Conf. on Analysis of Algorithms* (2007), P. Jacquet, Ed., DMTCS.

[28] FLAJOLET, P., FUSY, É., AND PIVOTEAU, C. Boltzmann sampling of unlabelled structures. In *Proceedings of the 4th Workshop on Analytic Algorithms and Combinatorics, ANALCO'07 (New Orleans)* (2007), SIAM, pp. 201–211.

[29] FUSY, É., POULALHON, D., AND SCHAEFFER, G. Bijective counting of plane bipolar orientations. In *Proceedings of Eurocomb'07* (2007).

Miscellaneous

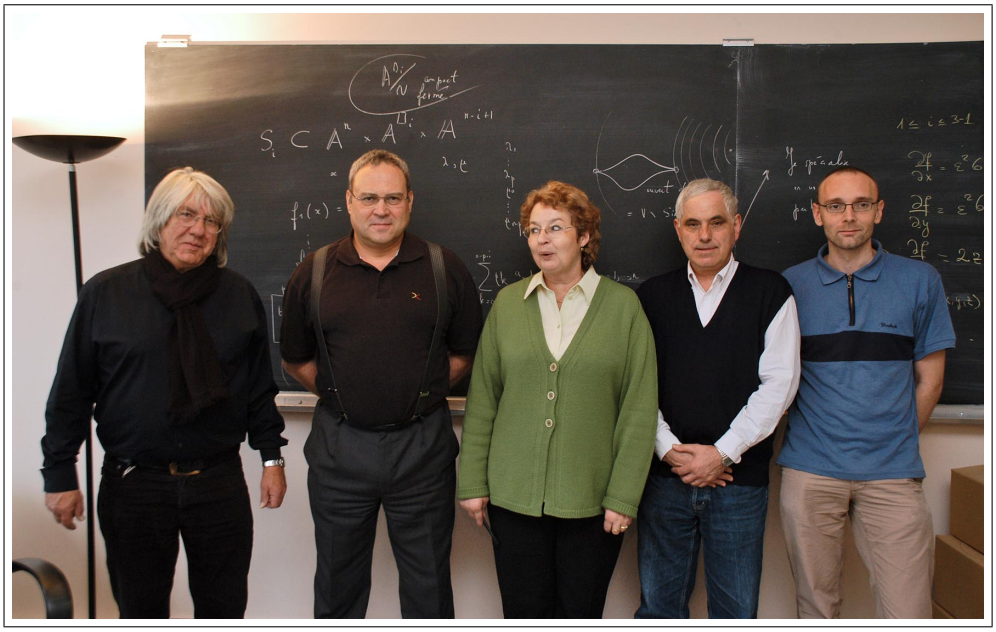
2007

[30] BODIRSKY, M., FUSY, É., KANG, M., AND VIGERSKE, S. Enumeration and asymptotic properties of unlabeled outerplanar graphs. To be published in the Electronic Journal of Combinatorics, 2007.

External references

[31] ISENBURG, M., AND SNOEYINK, J. Graph coding and connectivity compression, 2004. manuscript.

MAX
Modélisation Algébrique et Calculs Symboliques



Team members

Team leader

Marc GIUSTI, Directeur de Recherche au CNRS

Permanent members

- Michel FLIESS, Directeur de Recherche au CNRS
- Marc GIUSTI, Directeur de Recherche au CNRS
- Jean MOULIN-OLLAGNIER, Professeur à l'université de Créteil
- François OLLIVIER, Chargé de Recherche au CNRS
- Éric SCHOST, Maître de Conférence à l'École polytechnique (jusqu'en 2006).

Postdocs

- Frank WOITTENEK, bourse DGA, from april 2007.

Phds

- Xavier DAHAN, bourse EDX, from October 2003 to November 2006 ([54])
- Saïd MOUTAOUAKIL, bourse du royaume marocain, gave up in December 2005.

Guests

- Antonio CAFURE, Universidad de Buenos Aires, Universidad Nacional de General Sarmiento, Argentina, Polytechnique invited researcher from mid October to mid December 2006
- Joos HEINZ, Universidad de Buenos Aires, Faculdad de Ciencias Exactas y Naturales, Argentina, April 2006
- Guillermo MATERA, Universidad de Buenos Aires, Faculdad de Ciencias Exactas y Naturales, Argentina, Polytechnique invited researcher, from November 1st to November 30, 2006
- José Enrique MORAIS SAN MIGUEL, Universidad Publica de Navarra, Spain, Polytechnique

invited researcher, from March 1st to June 30, 2005
- Andrzej NOWICKI, University Nicolas Copernic, Institute for Mathematics, Toruń, Poland, Polytechnique invited researcher, from May 1st to May 31, 2006
- Luis Miguel PARDO, Universidad de Cantabria, Facultad de Ciencias, Depto. de Matemáticas, Estadistica y Computación, Spain, Polytechnique invited researcher, 2 months in March 2005 and 2007
- Pablo SOLERNÓ, Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Buenos Aires, Argentina, Polytechnique invited researcher, 2 months January and February 2006.

Research domain

Research in team MAX spans the area of symbolic computations dealing with the resolution of algebraic or differential-algebraic systems. In particular, we try to focus our efforts on improving the complexity of resolution algorithms.

The study of differential systems includes applications to control theory, by means of identification and observability tests, the study of flat systems (Monge's problem) and the discovery of criteria for flatness.

Michel Fliess leads the INRIA-Futur ALIEN project, which is located at both INRIA-Saclay-Île-de-France and INRIA-Nord-Picardie and is devoted to the study of new techniques for identification and observability. This research is yet another evidence of the contributions of algebraic methods in control theory and signal analysis.

Results

Resolution of algebraic systems

Triangular decompositions

Among the many ways to solve polynomial systems, triangular decompositions turn out to be well-suited to many practical problems ; however, many complexity questions are still open for these objects. As a first step, Xavier Dahan, Marc Moreno Maza, Éric Schost, Wenyuan Wu and Yuzhen Xie introduced in [30] the notion of *equiprojectable decomposition*, a geometrically-defined way to obtained a canonical decomposition ; they also showed how lifting algorithms can be adapted to this context.

Change of order in positive dimension

Many operations with multivariate polynomials, such as implicitization, rely on manipulations involving one or several lexicographic orders. Triangular representations appear as a natural tool to handle such situations, where orders on the variables matter. Xavier Dahan, Xin Jin, Marc Moreno Maza and Éric Schost designed in [38] a modular method, reducing the problem to computations in dimension zero and one, very similar in spirit to those previously proposed by Giusti, Heintz *et al.* for geometric resolution algorithms.

On the complexity of the D5 principle

The so-called *D5 principle* was introduced in 1985 by Jean Della Dora, Claire Dicrescenzo and Dominique Duval, to automatize reasoning based on case discussion for algebraic numbers. Following this idea, Xavier Dahan, Marc Moreno Maza, Éric Schost and Yuzhen Xie showed in [39] how to obtain the first quasi-linear time algorithms for arithmetic computations modulo triangular sets.

Bivariate triangular sets

The seemingly easy task of *changing order* in bivariate triangular representations actually has a wide range of applications, from Trager's factorization algorithm to rational function integration. Cyril Pascal and Éric Schost gave in [44] sharp complexity estimates for this operation, in the continuation of the work mentioned above for algebraic numbers.

Multivariate power series multiplication

The subroutines at the heart of our algorithms for polynomial systems also rely on power series multiplication in several variables. It turns out that no fast algorithms were known for this operation. This is all the more surprising as the question appears in many other contexts. We unearthed links between this question and that of polynomial evaluation and interpolation, connecting the geometry of the set of monomials involved to the complexity of the computations, through "deformation techniques" [35]. As a

first consequence, we proved that Lecerf's Newton iteration has a complexity less than quadratic.

Computations with algebraic numbers

The computation of annihilating polynomials for the sum or the product of algebraic numbers is one of the basic operations at the heart of computer algebra, with applications to many higher-level algorithms. Alin Bostan, Philippe Flajolet, Bruno Salvy and Éric Schost gave quasi-optimal algorithms for these operations, with extensions to the more difficult problem of *diamond product*. Our solutions rely on techniques developed previously or concurrently (algorithm transposition, power series multiplication).

Linear algebra.

Structured linear systems (involving so-called Toeplitz-like, Vandermonde-like matrices) can be solved much more efficiently than general ones, using so-called *displacement operators* to obtain compact data structures. Alin Bostan, Claude-Pierre Jeannerod and Éric Schost have showed how to reduce the cost of such algorithms for families of matrices having large *displacement rank* [45] ; this yields as a by-product improved algorithms for algebraic approximation or multivariate polynomial interpolation.

Fast computation of isogenies

In the Schoof-Elkies-Atkin algorithm that computes the cardinality of an elliptic curve over a finite field, isogenies between elliptic curves are used in a crucial way. Alin Bostan, François Morain, Bruno Salvy and Éric Schost introduced in [20] a new algorithm that computes such isogenies in quasi-linear complexity (in large characteristic), relying on algorithms for power series expansions of the solutions of differential equations.

Recurrences with polynomial coefficients

The question of computing one (or several terms) in a recurrence with polynomial coefficients has, surprinsingly, many applications. In [19], Alin Bostan, Pierrick Gaudry and Éric Schost gave improved algorithms for this operation ; this has consequences for the complexity of factoring integers deterministically, and for point-counting of hyperelliptic curves, using the Cartier-Manin operator.

Geometric methods

The main and characteristic problem in the real situation is to exhibit - with a good complexity - a point in every connected component of a real algebraic variety, given by equations. In collaboration with Bernd Bank, Joos Heintz and Luis Miguel Pardo Vasallo, Marc Giusti generalized the classical notion of polar variety, allowing then a unified framework to treat both the compact (previous work) and the non-compact case. The complexity of the algorithm depends on extrinsic (dimension, degree and evaluation complexity of the input equations) as well as intrinsic quantities of degree type. All together, the upper bound obtained for the complexity of this algorithm is better than any other known.

A first approach establishes the property of Cohen-Macaulay for these generalized polar varieties [3], first technical step. The definitive result (smoothness) [11] is published in the Special Issue of *J. of Complexity* in honour of Arnold Schönhage.

From geometry to numerical analysis

In the early of the eighties, Mike Shub and Steve Smale developped a quantitative analysis of the Newton method applied to systems of polynomial equations. In particular their celebrated α-theory yields an effective criterion to insure a quadratic convergence to a simple zero, requiring only informations on the initial point of the iteration.

Generalization of this theory to multiple isolated zeros (and its numerical avatar, clusters of zeros) is a big challenge. In this case the convergence is no longer quadratic, but it is known how to perturb the Newton operator in the Schröder operator to restore it.

Inspired by the symbolic deflation algorithm designed by Grégoire Lecerf in his thesis, Marc Giusti, Grégoire Lecerf, Bruno Salvy and Jean-Claude Yakoubsohn studied a general criterion to detect and approximate a cluster of zeros. They succeeded first for analytic functions, as follows : the convergence is still quadratic when the iteration is stopped on time, computing a point located at a distance of the order of the diameter of the cluster. This result is published in [13].

Second they achieved the generalization to multiple zeroes of analytic systems under the hypothesis of embedding dimension one [23].

Differential algebra

Integration in closed form

Jean Moulin-Ollagnier continues his work on integration in closed form of polynomial vector fields, alone and in collaboration with several french and foreign colleagues : Jean-Marie Strelcyn (Rouen), Andrzej Nowicki and Andrzej Maciejewski (Torùn, Poland), Arno van den Essen (Nimègue, Netherlands).

Several papers were published since January 2005 [6, 18] and [24], which precise and complete a previous publication [5].

From formal to numerical computations

A collaboration with CNES AND ONERA in the frame of the CARINS project finished at the end of 2004. It was an expertise activity, related to the realization of a numerical code, integrating a symbolic tool. The goal was to simulate the behaviour of a rocket engine with liquid ergols.

This activity gave us a practical know-how on the symbolic precomputations needed to the numerical integration of a system. The use of a free computer algebra software in this domain was presented to a public of engineers in a conference organized by the SEE in may 2005 [52].

Jacobi's bound

Around 1836, Jacobi proposed a sharp bound on the order of a system of n ordinary differential equations $u_i(f_1, \ldots, f_n)$. Jacobi alive neither published his result, which can be expressed as the maximum $\max_{\sigma \in S^n} a_{i,\sigma(i)}$, with $a_{i,j} = \operatorname{ord}_{f_j} u_i$, nor the original algorithm he invented to compute it in polynomial time (assignement problem).

Manuscripts were partly published in Latin around 1860 [56, 57], but were quickly forgotten apartoutside some restricted circles of experts in differential algebra. Proof of this oblivion, Jacobi's algorithm was rediscovered by Kuhn only in 1955[5], under the name of hungarian method. The assignement problem interested highly the mathematical community [6] since the end of World War II, to solve optimization problems in economy.

F. Ollivier is finishing a translation of these texts, including unpublised manuscripts he discovered in the archives of the Academy of Science of Berlin, in a double spirit of history of science and original developments in algorithmics and computer algebra. Indeed, precious and yet unexploited indications lie in Jacobi's work.

Historical researches were presented in a poster at the conference *Differential Algebra and Related Topics* in April 2007 at Rutgers University (Newark, New Jersey) and some results on normal forms at a special session of the AMS conference *Differential Algebra*, at Stevens Institute of Technology, Hoboken (New Jersey).

In collaboration with Brahim Sadik (Université Cadi Ayyad, Marrakech, Moroccao), François Ollivier gave a new proof of Jacobi's bound, under hypotheses close to the work of Kondratieva *et al.*, in the framework of the geometry of diffieties ([26]). Furthermore this yields a proof of the condition given by Jacobi under which the bound is attained, and makes precise how to find a normal form in this case.

The result was also extended to under-determined systems.

Difference Algebras

Saïd Moutaouakil begun in 2003 a PhD (with adviser Michel Fliess) on delay identification. François Ollivier became adviser in September 2004, refocusing the work on difference algebras. Results were published in [25]. They are based on a free interpretation of the ALIEN method described below, from successive part integrations.

Saïd Moutaouakil gave up research in December 2005 to create a computer software company.

ALIEN method

ALIEN is an INRIA project headed by Michel Fliess. Michel Fliess and François Ollivier are the only ALIEN members belonging to LIX. We describe here the research of the LIX part of the ALIEN project.

The manifold success of our viewpoint in various branches of mathematical engineering is indicating directions for researches in a near future.

[5] The fifthiest anniversary of this success was celebrated in Budapest on October 2005.

[6] as famous researchers as J. von Neumann.

Algorithmic and numerical aspects of estimation

Our calculations are resting on the two following aspects :

- Algebraic elimination of some system variables. Here again the use of non classical data structures form a keystone for accelarating algebraic computations and eventually producing naturally efficient numerical programs.
- Manipulation of matrices, which are ill-conditioned since the integration time is very short.

Improving our results will therefore necessitate a combination of algorithms stemming from computer algebra and numerical analysis which needs to be better understood.

Note that ALIEN aims at developing algorithms, but no commercial software.

New concrete examples in control

New concrete examples from various technological fields will be investigated. It is worth noticing that several experimental benchmarks are already available at LAGIS laboratory (mobile robots, stepper motor, cart-pendulum) as well as at ECS laboratory (benchmark on multi-cell chopper).

Collaborative robots The cooperation between several agents is a challenging trend from both economical and scientific points of view. A large number of applicative fields can be cited : Transportation (unit of mobile robots), Health (remotely-operated surgery robots), Environment or Defence (fleet of drones or UAV), Space (constellation of satellites), Machining (over-actuated systems)... The cooperating devices have to fulfill a common objective, subject to environment perturbations and using a limited number of sensors. Then, it makes sense to use fast reconstruction of state variables as well as of exogenous parameters (force feedback, obstacle positions...). It is aimed at designing computationally efficient algorithms, based on algebraic estimation techniques, and working out the required information on the basis of the available sensors and communication links.

Magnetic levitation Magnetic levitation systems have received much attention as a way of eliminating Coulomb friction due to mechanical contact. Levitation bearing has been used from the beginning in rotating machinery to support rotors without friction providing low energy consumption, high rotational speed, with no lubrication and greater reliability. It also allows a simpler and safer mechanical design as in the case of pumps used in nuclear installations where fluid leakage avoidance is of primary importance. Magnetic bearings are also becoming increasingly popular in the precision industry, with significant demands on accurate positioning. One can quote nanometric servo-position actuator in microlithography industry as well as vibration isolation in precision scientific instruments. High-speed ground transportation systems constitute another application, probably the most famous : Japanese “Maglev” and German “Transrapid” are very fast trains using the principle of a linear motor hanged up over a magnetic rail.

Magnetic levitation systems highlight phenomena like strong nonlinearities, fast dynamics, actuator saturations and uncertain parameters. Many control techniques have been quite successfully implemented on levitation systems. Within the control methodologies, one can cite, for instance, feedback linearization control, flatness based control, passivity based control, or backstepping design approach. However the performances are limited by the model relevance as well as its parameters accuracy. Estimation of these parameters is a motivating problem and it is aimed at developing and testing control laws based on closed-loop identification methods. In the next few months, a magnetic shaft benchmark will be developed in Lille in collaboration with Dr. Joachim Rudolph from the University of Dresden.

Friction Modelling or estimating *on-line* the viscous or dry friction in mechanical systems is a challenging problem with an industrial impact. To mention only the regional framework of “Region Nord - Pas de Calais”, several programs are concerned with brake systems management (ST2 pole[7], *i*-TRANS[8]) as well as friction compensation (ERT CEMODyNE[9]).

By using the fast estimation capabilities, we hope to drastically simplify some difficult modelling problems arising while studying friction. Two bench-

[7] Science and Technologies for Safe Transport, the theme 4 of which is devoted to braking mechanics : `http ://www.polest2.fr.`

[8] French *Pôle de compétitivité* on “Railway at the heart of the innovative transport systems”.

[9] See `http ://www.lille.ensam.fr/cemodyne`.

marks at LAGIS can be used to illustrate the efficacy of the algebraic methods for the control of electromechanical systems with friction : A linear drive actuating a cart-pendulum, and a stepper motor. Note that the latter is a flat system and so, a linearizing control law based on the fast and robust estimation of the time derivatives of the sensor signals can be considered.

Multi-cell chopper Multi-cell chopper and converter are more and more popular in power electronic, due to three main reasons : (1) The possibility with the same switching component of covering a wide voltage scale. (2) The modularity and flexibility introduced in the design of such chopper or converter. (3) The drastic decreasing of the dv over dt phenomenon.

Unfortunately, due to the complexity of the control (i.e. hybrid system, non universal input...), many of the industrial applications are considered in the vicinity of a given, *static* requested behavior. The algebraic techniques could be considered so to design an observer-based control algorithm valid for more general *dynamic* behaviors. Application domains of such a breakthrough are, for instance, railway traction and active filters for networks.

Linear delay systems

Delay estimation may also be a crucial question in concrete situations, since most of the efficient control techniques need the delay as a parameter. Real time identification of delay was considered as an open problem. Scarce results manage an asymptotic identification, the convergence time of which does not guaranty an efficient combination with control or fault diagnosis techniques. The approach introduced in [36] opens a promising track to fast estimation of delays, including the case of variable ones. Several fields of application are concerned.

Process engineering

A wide class of plants (chemical engineering, food industry...) can be approached efficiently by a simple linear model with input delay. If it turns out to be possible, proposing a software that provides both the model and the associate controller from industrial data mining (thus, off-line data) is very relevant to industrial concerns.

Aeronautics Among the various approaches that model the longitudinal flight of an aircraft through a vertical gust, a delay-based description was introduced so to represent the effects of the penetration of the aircraft through the gust. Combining this description with a fast identification algorithm constitutes a track for the aerodynamic coefficients identification. Tests will be carried out at the Flight Analysis laboratory of the DCSD of ONERA in Lille. During those experiments, a model of civil aircraft equipped with an embedded instrumentation will be catapulted and will cross, during a free flight, a turbulence generated by a vertical blower.

Networked control Communication networks (ethernet, wifi, internet, CAN...) have a huge impact on the flexibility and integration of control systems (remote control, wireless sensors, collaborative systems, embedded systems...). However, a network unavoidably introduces time delays in the control loops, which may put the stability and safety performances at risk. Such delays are varying (jitter) and efficient control techniques (predictor-based) take advantage of their knowledge. Two approaches have to be combined : (1) use delay identification algorithms and improve the control ; (2) design control/estimation algorithms that can stand variations of the delay.

Signal, image, and video processing

Multi-user detection In the direct-sequence *code-division multiple access* (DS-CDMA) system, several users share a common propagation channel, by use of spread spectrum signalling. Each user is assigned a unique code sequence corresponding to its *signature*. This signature sequence allows the user to modulate and spread the information-bearing signal across the available frequency band. It is also on the base of this signature that the receiver distinguishes and separates the corresponding user among the others.

As the different users access the channel asynchronously, the optimum maximum likelihood receiver, which is based on a bench of correlators, has a computational complexity which grows exponentially with the number of users. It seems that our method should leads to a most efficient detection with a reasonable level of complexity.

Direction-of-arrival estimation The problem of estimating the direction-of-arrival of multiple sources incident on a uniform array has received much attention in recent years, especially for wide band sources for which the existing solutions are rather computationally demanding. If $s_k(t)$, $k = 1, \ldots, M$, denotes the k^{th} source signal, the signal $y_i(t)$ received then by

the i^{th} sensor, $i = 1, \ldots, N$ is of the form :

$$y_i(t) = \sum_{k=1}^{M} s_i(t - \tau_i(\theta_k)) + n_i(t),$$

where :

- $n_i(t)$ is an additive noise,
- $\tau_i(\theta_k)$ is the (relative) delay of a signal from direction θ_k.

The problem of estimating the direction-of-arrival is equivalent to the estimation of those delays. When a model for the source signal is known, as it is the case, for instance, in radar and sonar applications, this problem admits in our approach a simple and straightforward real-time solution. In a blind situation, where no signal model is available, our method yields good estimates provided the real-time constraint is relaxed.

Turbo-codes The famous discovery of *turbo-codes* by Prof. C. Berrou and the late Prof. A. Glavieux has certainly been the main achievement in the 90s of the theory of error control codes. Besides completely changing not only the theory but also the practical implications of this field, it has given birth to various extensions in signal processing such as *turbo-equalisation*. It seems that turbo-decoding might benefit from our new understanding of estimation.

Watermarking This which is becoming a hot topic and may be viewed as a type of cryptography where a hidden message has to be inserted in an image or a video. Our approach to image and video processing, which unfortunately could not be reviewed in this report for legal reasons, has already given promising preliminary results in this field.

Cryptography

After Pecora and Carroll (1991) successfully synchronized two identical chaotic systems with different initial conditions, chaos synchronization has been intensively studied in various fields and in particular in secure communications (because chaotic systems are extremely sensitive to their initial conditions and parameters). The idea is to use the output a particular dynamical (chaotic) system to drive the response of an identical system so that they oscillate in a synchronized manner. An interesting application in secure communication uses such a chaotic master dynamics to mask a message and a synchronized slave system to recover the message.

Since the work of Nijmeijer and Mareels (1997), the chaotic system synchronization problem has been intimately related to the design of a nonlinear state observer for the chaotic encoding system. Many techniques issued from observation theory have been applied to the problem of synchronization, where the receiving system asymptotically tracks the states of the transmitting system : observers with linearizable dynamics, adaptive or sliding mode observers, generalized hamiltonian form based observers, etc.

The key issue here is to take an algebraic viewpoint for the state estimation problem associated with the chaotic encryption-decoding problem and to emphasize its use for the efficient and fast computation of accurate approximations to the successive time derivatives of the transmitted observable output signal received at the decoding end. Those methods should also be useful in new encryption algorithms that require fast estimation of the state variables and the masked message.

Note that the technological aspects of this new kind of cryptography has nothing to do with number-theoretic cryptography which has become very popular in computer science.

Comparison with other methodologies

People of the project who belong to LAGIS, as well as Jean-Pierre Barbot, have been working for many years on other methods for fast estimation (of state variables or unknown parameters). Those techniques, that have been widely developed during the last decade in the literature, are often referred as "finite time" observers or estimators : The knowledge of the variables or the parameters is theoretically recovered after a finite time and not asymptotically (as it is usually the case). This approach involves notions such as homogeneous functions or discontinuous functions (one can refer to higher order sliding mode theory or the larger area of variable structure systems). Thus, for several fields of applications, the members of the project have the required background to perform comparisons of variable structure techniques and algebraic methods in the framework of fast estimation and identification.

Software, patents and contracts

Software

- Programs used in the numeric simulations described in [25] are available from : `www.lix.polytechnique.fr-/~ollivier/LogicielFr.htm`.

– The work described by Xavier Dahan and Éric Schost in [27, 30] has been implemented by F. LEMAIRE, M. MORENO MAZA and Y. XIE in the library `RegularChains` of the commercial package MAPLE, since version 10.

Contracts

– Michel Fliess participates to the DGA project *Systèmes Complexes Distribués Mobiles Sécurisés* described later.

Teaching, dissemination and service

Michel Fliess has given 12 hours lectures on Alien's estimation methods in the framework of the Multi-partner Marie Curie Training Site, entitled Control Training Site.

Michel Fliess has given 25 hours lectures at École polytechnique of Tunis in 2006.

Marc Giusti, François Ollivier and Éric Schost participate to the course "Algorithms for Computer Algebra and Control Theory" of the Master Parisien de Recherche en Informatique.

Jean Moulin-Ollagnier is a regular collaborator of *Mathematical Reviews*.

François Ollivier participated to the technical workshop "Journée technique « Les applications scientifiques et industrielles du logiciel libre »", organised jointly by ISA-France and SEE with the patronage of GIMELEC [52].

Éric Schost taught a "Symbolic Computation" course at École Polytechnique.

Phd Committees

Marc Giusti was a member of the PhD jurys of

– Raouf Dridi « Utilisation de la méthode d'équivalence de Cartan dans la construction d'un solveur d'équations différentielles », (with a report by François Ollivier), Université des Sciences et Technologies de Lille, 2007 ;
– María del Carmen Martínez Fernández « Códigos y Grafos sobre Anillos de Enteros Complejos », Universitad de Cantabria, Santander, Espagne, 2007 ;
– Lutz Lehmann « Wavelet-Konstruktion als Anwendung der algorithmischen reellen algebraischen Geometrie », Humboldt Universität zu Berlin, Allemagne, 2007 ;
– Mohammed Mahir « Sur l'intégrabilité des systèmes différentiels », (with a report by François Ollivier), Université des Sciences et Technologies de Lille, 2005.

Jean Moulin-Ollagnier was a member of the PhD jury of

– Maria-Teresa Grau à l'Université Autonome de Barcelone, december 2004.
– Morteza Mohammad-Noori à l'Université Paris XI (LRI), july 2005.

François Ollivier was a referee of the thesis of María Elisabet D'Alfonso, University of Buenos Aires, september 2006.

Éric Schost a été membre du jury de la thèse d'Ali Ayad, soutenue at Université de Rennes I.

Visibility

National scientific cooperations

– ALIEN is an INRIA project lead by lead by Michel Fliess, which includes the team of Jean-Pierre Richard, École Centrale de Lille, Mamadou Mboup (universitéParis V), and Cédric Join (Centre de Recherche en Automatique de Nancy).
– Marc Giusti leads of one of the four teams who received an ANR grant for the project GECKO, which includes the projects "Algorithmes" (INRIA-Rocquencourt), le Laboratoire J. A. Dieudonné (Université de Nice - Sophia-Antipolis), le LIX (École polytechnique) et le Laboratoire MIP (Université Paul Sabatier). Funding : 94 281,5 euros for 3 years, see `http ://gecko.inria.fr/`.
– Marc Giusti participated in 2004 and 2005 to the ACI « MathSTIC », lead by Grégoire Lecerf and Éric Schost, à hauteur de 33% : "Conception d'algorithmes efficaces assistés par la géométrie". Funding : 15 000 euros.
– Algebraic methods for real-time estimation – The case of adherence coefficients for tyre efforts. Grant supported by GdR CNRS 717 MACS "Modélisation, Analyse et Commande des Systèmes dynamiques" (Modelling, Analysis and Control of dynamic Systems). Category "Exploratory research on interdisciplinary

joint research". H. MOUNIER (manager), Institut d'Electronique Fondamentale, CNRS and University of Paris 11, 8 KEuros.

International scientific cooperations

- Éric Schost and Xavier Dahan had a long standing collaboration since september 2004 with Marc Moreno Maza and his team at University of Western Ontario, especialy Yuxhen Xie [30, 38, 39].
- Marc Giusti has a long standing collaboration with the university of Buenos-Aires and the university of Cantabria at Santander, Spain.
- Michel Fliess participates to a project STIC-INRIA with Tunisia "Modelisation et identification des systèmes".
- The team has a long standing collaboration with the Laboratory of number theory and symbolic computations of the faculty of sciences Semlalia at Marrakech [25, 26].
- Jean Moulin-Ollagnier has a regular collaboration with Jean-Marie Strelcyn from Rouen, Andrzej Nowicki et Andrzej Maciejewski from Torùn, and Arno van den Essen from Nimeguen [6, 18, 24].
- Nicole Dubois, Marc Giusti, François Ollivier and Éric Schost (until 2006) participate tothe european project SCIEnce (Symbolic Computation Infrastructure in Europe), FP6, Research Infrastructure action, I3 (Integrated Insfrastructure Initiatives) since april 2006 (http ://www.medicis.polytechnique.fr/science, http :www.science.org). The project is form 5 years, with a funding of 194 KEuros for MAX. Other particpants are the universities of St Andrews and Heriot Watt (Scotland), university of Paderborn (Germany), Johannes Kepler university (Austria), Technical universities of Eindhoven (Netherlands) and Berlin (Germany), the intitute E-Austria at Timisoara (Roumania), and Waterloo Maple Inc. (Ontario, Canada). The goal of the project is to ease the use of symbolic computation systems by developpers from the various application domains.

Conference and seminar invitations

- Marc Giusti : « Constraint Databases, Geometric Elimination and Geographic Information Systems », Dagstuhl Seminar, Allemagne, Mai 2007.
- Marc Giusti at FoCM'05 (Foundations of Computational Mathematics), Santander, Espagne, *« Semi-plenary speaker »*, 2005.
- Marc Giusti : Numerics on Manifolds, Luminy, mai 2005.
- Jean Moulin-Ollagnier : *Les fonctions suppléantes et le défi liouvillien*, *Journées de l'ANR Intégrabilité*, École Normale Supérieure de Lyon.
- Jean Moulin-Ollagnier : *Darboux polynomials at Darboux points*, 1st Spanish-French meeting of mathematics at Saragossa, july 2007.
- François Ollivier gave a talk on Jacobi's bound at LIFL, june 2006.
- Éric Schost presented his results at INRIA-Rocquencourt, three times in 2005 and once in 2006 ; at University of North Carolina, Raleigh (2006) ; at Dagsthul in 2006 for the workshop on Challenges in Symbolic Computation Software ; at the Waterloo Workshop on Computer Algebra in 2006 ; at Rennes in 2006 ; and at the workshop on Curves, isogenies and cryptologic applications in 2006.

Conference organisation

- First `SCIEnce` workshop, Palaiseau (Nicole Dubois, Marc Giusti, François Ollivier), janvier 2007 ;
- Conference in honnor of the 60th birthday of Michel Fliess, Institut Henri Poincaré, Paris, 30 and 31 march 2006 ; (Nicole Dubois, Marc Giusti, François Ollivier). Marc Giusti is co-editor of the proceedings to appear in a special issue of the est co-éditeur des actes du colloque, volume spécial *International Journal of Control*.
- Marc Giusti was a member of the organizing committee of FoCM'05 (Santander, 2005) and in charge with Bernd Bank (Humboldt Universität zu Berlin) of the poster session.
- Marc Giusti participated to the organization of the workshop MathSTIC : *Liens Calcul Formel - Calculs Numériques*, Luminy, 2005.
- Michel was scientific coordinator of the ALIEN Summer School « Fast estimation and identification methods in control and signal », 2006.

Program committees

- Marc Giusti was a member of the scientific committee of « Computational Algebraic Geometry and Applications », a conference in honnor of the 60th birthday of André Galligo, Université de Nice, 2006.
- Marc Giusti was a PC member of MEGA 2005 (Méthodes Effectives en Géométrie Algébrique).
- François Ollivier is a PC member of the conference *Differential Algebra and Related Computer Algebra* in memory of Giuseppa Carrà Ferro, to take place in Catana, 26–29 march 2008.
- Éric Schost was a PC member of *Trangressive Computing*, 2006.

Journal editorial boards

- Michel Fliess is an editor of the Journal of Dynamical and Control Systems, International Mathematical Forum.
- Marc Giusti is editor (in chief since january 21, 2006), of Applicable Algebra in Engineering, Communication and Computing (AAECC), Springer Verlag.

Awards

- *Distinguished Paper Award* given to Éric Schost and Xavier Dahan at ISSAC 2004 [27].
- *Best Student Author Award* given to Xavier Dahan at ISSAC 2005 [30].
- Prix Jacques-Louis Lions awarded to Michel Fliess by the french academy of sciences, 2007.

References

Books and chapters in books

2005

[1] FLIESS, M., JOIN, C., AND SIRA-RAMÍREZ, H. Closed-loop fault-tolerant control for uncertain nonlinear systems. In *Control and Observer Design for Nonlinear Finite and Infinite Dimensional Systems* (2005), pp. 217–233.

2007

[2] FLIESS, M., AND SIRA-RAMIREZ, H. Closed-loop parametric identification for continuous-time linear systems via new algebraic techniques. In *Continuous-Time Model Identification from Sampled Data* (2007), H. Garnier and L. Wang, Eds.

International journals

2004

[3] BANK, B., GIUSTI, M., HEINTZ, J., AND PARDO, L. M. Generalized polar varieties and an efficient real elimination procedure. *Kybernetika 40*, 5 (2004), 519–550.

[4] FLIESS, M., JOIN, C., AND SIRA-RAMÍREZ, H. Robust residual generation for linear fault diagnosis : an algebraic setting with examples. *International Journal of Control 77*, 14 (2004), 1223–1242.

[5] MACIEJEWSKI, A., MOULIN-OLLAGNIER, J., AND NOWICKI, A. Generic polynomial vector fields are not integrable. *Indagationes mathematicae 15*, 1 (2004), 55–72.

[6] MOULIN-OLLAGNIER, J. Algebraic closure of a rational function. *Qualitatitive Theory of Dynamical Systems 5*, 2 (2004), 285–300.

[7] MOULIN-OLLAGNIER, J. Corrections and complements to "liouvillian integration of the lotka-volterra system". *Qualitatitive Theory of Dynamical Systems 5* (2004), 275–284.

[8] MOULIN-OLLAGNIER, J. Simple darboux points of polynomial planar vector fields. *Journal of Pure and Applied Algebra 189* (2004), 247–262.

[9] MOULIN-OLLAGNIER, J., AND NOWICKI, A. Constants and darboux polynomials for tensor products of polynomial algebras with derivations. *Communications in Algebra 33*, 1 (2004), 379–389.

[10] RECONSTRUCTORS, S. M. fliess and h. sira-ramirez. *Comptes rendus de l'académie des sciences, Mathématiques 338*, 1 (2004), 91–96.

2005

[11] BANK, B., GIUSTI, M., HEINTZ, J., AND PARDO, L. M. Generalized polar varieties :

geometry and algorithms. *Journal of Complexity 21*, 4 (2005), 377–412.

[12] FLIESS, M., JOIN, C., AND MOUNIER, H. An introduction to nonlinear fault diagnosis with an application to a congested internet router. *Advances in Communication Control Networks 338* (2005), 327–343.

[13] GIUSTI, M., LECERF, G., SALVY, B., AND YAKOUBSOHN, J.-C. Location and approximation of clusters of zeroes of analytic functions. *Foundations of Computational Mathematics 5*, 3 (2005), 257–311.

2006

[14] BOSTAN, A., FLAJOLET, P., SALVY, B., AND SCHOST, É. Fast computation of special resultants. *Journal of Symbolic Computation 41*, 1 (2006), 1–29.

[15] FLIESS, M. Analyse non standard du bruit. *C.R. Acad. Sci. Paris 342* (may 2006), 797–802.

[16] GAUDRY, P., SCHOST, É., AND THIÉRY, N. M. Evaluation properties of symmetric polynomials. *International Journal on Algebra and Computation 16*, 3 (2006), 505–524.

[17] SIRA-RAMÍREZ, H., AND FLIESS, M. An algebraic state estimation approach for the recovery of chaotically encrypted messages. *International Journal of Bifurcation and Chaos 16*, 2 (2006), 295–309.

[18] VAN DEN ESSEN, A., MOULIN-OLLAGNIER, J., AND NOWICKI, A. Rings of constants of the form $k[f]$. *Communications in Algebra 34* (2006), 3315–3321.

2007

[19] BOSTAN, A., GAUDRY, P., AND SCHOST, É. Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator. *SIAM Journal on Computing 36*, 6 (2007), 1777–1806.

[20] BOSTAN, A., MORAIN, F., SALVY, B., AND SCHOST, É. Fast algorithms for computing isogenies between elliptic curves. *Mathematics of Computation* (2007). à paraître.

[21] FLIESS, M. Probabilités et fluctuations quantiques (probabilities and quantum fluctuations). *Comptes rendus de l'académie des sciences, Mathématiques 344* (2007), 663–668.

[22] FLIESS, M., JOIN, C., AND SIRA-RAMIREZ, H. Non-linear estimation is easy. *Int. J. Modelling, Identification and Control* (2007).

[23] GIUSTI, M., LECERF, G., SALVY, B., AND YAKOUBSOHN, J.-C. On location and approximation of clusters of zeroes : case of embedding dimension one. *Foundations of Computational Mathematics 7*, 1 (2007), 1–58.

[24] MACIEJEWSKI, A., MOULIN-OLLAGNIER, J., AND NOWICKI, A. Correction and complements à l'article : Generic polynomial vector fields are not integrable. *Indagationes mathematicae* (2007). à paraître.

[25] OLLIVIER, F., MOUTAOUAKIL, S., AND SADIK, B. Une méthode d'identification pour un système linéaire à retards. *Comptes rendus de l'académie des sciences, Mathématiques 344*, 11 (2007), 709–714.

[26] OLLIVIER, F., AND SADIK, B. La borne de jacobi pour une diffiété définie par un système quasi régulier. *Comptes rendus de l'académie des sciences, Mathématiques 345*, 3 (2007), 139–144.

International conferences with proceedings

2004

[27] DAHAN, X., AND SCHOST, É. Sharp estimates for triangular sets. In *ISSAC '04 : Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation* (2004), ACM Press, pp. 103–110.

[28] FLECK, C., PAULUS, T., SCHÖNBOHM, A., ABEL, D., AND OLLIVIER, F. Flatness based open loop control for the twin roll strip casting process. In *Symposium on Nonlinear Control Systems (NOLCOS-2004)* (2004).

[29] FLIESS, M., AND SIRA-RAMIREZ, H. Control via state estimations of some nonlinear systems. In *IFAC Symposium on Nonlinear Control Systtems (NOLCOS 2004)* (2004).

2005

[30] DAHAN, X., MORENO MAZA, M., SCHOST, É., WU, W., AND XIE, Y. Lifting techniques

for triangular decompositions. In *ISSAC'05* (2005), ACM, pp. 108–115.

[31] FLIESS, M., JOIN, C., MBOUP, M., AND SEDOGLAVIC, A. Estimation des dérivées d'un signal multidimensionnel avec applications aux images et aux vidéos. In *Actes* 20^e *coll. GRETSI* (2005).

[32] FLIESS, M., JOIN, C., MBOUP, M., AND SIRA-RAMÍREZ, H. Analyse et représentation de signaux transitoires : application à la compression, au débruitage et à la détection de ruptures. In *Actes* 20^e *coll. GRETSI* (2005).

[33] JOIN, C., SIRA-RAMÍREZ, H., AND FLIESS, M. Control of an uncertain three-tank-system via on-line parameter identification and fault detection. In *IFAC World Congress on Automatic Control* (2005), IFAC.

[34] REGER, J., SIRA-RAMÍREZ, H., AND FLIESS, M. On non-asymptotic observation of nonlinear systems. In *Proc. CDC-ECC'05* (2005).

[35] SCHOST, É. Multivariate power series multiplication. In *International Symposium on Symbolic and Algebraic Computation, ISSAC'05* (2005), ACM, pp. 293–300.

2006

[36] BELKOURA, L., RICHARD, J.-P., AND FLIESS, M. On-line identification of systems with delayed inputs. In *MTNS'06, 16th Conf. Mathematical Theory of Networks & Systems* (2006).

[37] DAAFOUZ, J., FLIESS, M., AND MILLERIOUX, G. Une approche intrinsèque des observateurs linéaires à entrées inconnues. In *Conf. Internat. Francophone d'Automatique (CIFA), Bordeaux, France* (2006).

[38] DAHAN, X., JIN, X., , MAZA, M. M., AND SCHOST, E. Change of ordering for regular chains in positive dimension. In *Maple conference 2006* (2006), I. Kotsireas Ed.

[39] DAHAN, X., MORENO MAZA, M., SCHOST, É., AND XIE, Y. On the complexity of the D5 principle. In *Transgressive Computing* (2006), pp. 149–168.

[40] FILATEI, A., LI, X., MORENO MAZA, M., AND SCHOST, É. Implementation techniques for fast polynomial arithmetic in a high-level programming environment. In *ISSAC'06* (2006), pp. 93–100.

[41] FLIESS, M., JOIN, C., MBOUP, M., AND SIRA-RAMÍREZ, H. Vers une commande multivariable sans modèle. In *Conférence internationale francophone d'automatique (CIFA 2006)* (2006).

[42] FLIESS, M., JOIN, C., AND SIRA-RAMÍREZ, H. Complex continuous nonlinear systems : Their black box identification and their control. In *Proc. 14th IFAC Symposium on System Identification (SYSID 2006)* (2006).

[43] NEVES, A., MBOUP, M., AND FLIESS, M. An algebraic receiver for full response cpm demodulation. In *International Telecommunications Symposium (ITS 2006)* (2006).

[44] PASCAL, C., AND SCHOST, É. Change of order for bivariate triangular sets. In *ISSAC'06* (2006), ACM, pp. 277–284.

2007

[45] ALIN BOSTAN, CLAUDE-PIERRE JEANNEROD, É. S. Solving Toeplitz- and Vandermonde-like linear systems with large displacement rank. In *ISSAC'07* (2007), ACM, pp. 33–40.

[46] BELKOURA, L., RICHARD, J.-P., AND FLIESS, M. Real time identification of delay systems. In *Ifac Worshop on Time delay Systems* (2007).

[47] BOSTAN, A., CHYZAK, F., OLLIVIER, F., SALVY, B., SCHOST, E., AND SEDOGLAVIC, A. Fast computation of power series solutions of systems of differential equations. In *SODA'07, ACM-SIAM Symposium on Discrete Algorithms* (2007), pp. 1012–1021.

[48] BOURDAIS, R., FLIESS, M., JOIN, C., AND PERRUQUETTI, W. Towards a model-free output tracking of switched nonlinear systems. In *NOLCOS 2007 - 7th IFAC Symposium on Nonlinear Control Systems* (2007).

[49] MBOUP, M., JOIN, C., AND FLIESS, M. A revised look at numerical differentiation with an application to nonlinear feedback control. In *The 15th Mediterranean Conference on Control and Automation - MED'2007* (2007).

National conferences with proceedings

2006

[50] FLIESS, M., FUCHSHUMER, S., SCHLACHER, K., AND SIRA-RAMÍREZ, H. Discrete-time linear parametric identification : An algebraic approach. In *2e Journées Identification et Modélisation Expérimentale - JIME'2006* (2006).

[51] JOIN, C., MASSE, J., AND FLIESS, M. Commande sans modèle pour l'alimentation de moteurs : résultats préliminaires et comparaisons. In *2e Journées Identification et Modéisation Expérimentale - JIME'2006* (2006).

Dissemination

2005

[52] OLLIVIER, F. Maxima et les logiciels libres de calcul formel. *Revue de l'Électricité et de lÉlectronique 11* (2005), 89–93.

2006

[53] FLIESS, M., AND MBOUP, M. Towards new estimation techniques : Reconciling signal processing and control. In *ICASSP* (Toulouse, May 2006). Tutorial Note.

PhD Thesis

2006

[54] DAHAN, X. *Sur la complexité des représentations des systèmes polynomiaux : triangulation, méthodes modulaires, évaluation dynamique*. PhD thesis, École polytechnique, novembre 2006.

Miscellaneous

2006

[55] FLIESS, M. Approche intrinsèque des fluctuations quantiques en mécanique stochastique (an intrinsic approach to the quantum fluctuations in stochastic mechanics). Tech. rep., HAL INRIA, `http://hal.inria.fr/inria-00118460`, 2006.

External references

[56] JACOBI, C. De investigando ordine systematis æquationum differentialum vulgarium cujuscunque. *Journal für die reine und angewandte Mathematik LXIV*, 4 (1865), 297–320.

[57] JACOBI, C. *Vorlesungen über Dynamik von C. G. J. Jacobi nebstes fünf hinterlassenen Abhandlungen desselben*. Druck und Verlag von Georg Reimer, 1866, ch. De æquationum differentialum systemate non normali ad formam normalem revocando, pp. 550–578.

Cryptologie
Théorie Algorithmique des Nombres pour la Cryptographie

Team members

Team leader

François MORAIN

Permanent members

- François MORAIN, professeur à l'École polytechnique
- Andreas ENGE, Chargé de recherches INRIA
- Pierrick GAUDRY, Chargé de recherches au CNRS (moved to LORIA/Spaces on 2005-09-01)
- Jerôme MILAN, Ingénieur expert INRIA and Digiteo (since sept. 1st, 2005)

Postdocs

- Annegret WENG, started 2004-08-01, but stopped soon after for personal reasons.

Phds

- Éric BRIER, ingénieur GemPlus, starting 2002-09-01.
- Régis DUPONT, Corps des Télécom [2003-09-01 till 2006-04-07].
- Thomas HOUTMANN, CNRS/DGA since 2004-09-01.

Interns

- Benoît LIBERT, Belgian phD student, co-advisor A. Enge
- Jean-René REINHARD, DEA Algo, April-July 2004
- Fabien DÉLEN, Université de Versailles-St Quentin, April-July 2005
- Thomas RAVARY, stagiaire MPRI, April–July 2006
- El Maati BOULFAKHR, École polytechnique, April–July 2006

- Pamkaj BOTREL, ENS Cachan, June–July 2006
- Luca de FEO, stagiaire MPRI, April–August 2007
- Jean-François BIASSE, stagiaire MPRI, April–August 2007
- Guillaume GUERPILLON, École polytechnique, April –July 2007.

Guests

- Isabelle DÉCHÈNE, Univ. Waterloo, 2006-07-17 until 2006-07-21
- Anton STOLBUNOV, Univ. St Petersbourg, 2006-07-17 until 2006-07-19
- Gagan GARG, Bangalore, 2006-06-05 till 2006-06-25
- Osmanbey UZUNKOL, TU Berlin, 2005-12-19 until 2005-12-23
- Anita KRAHMANN, TU Berlin, 2005-12-19 until 2005-12-23
- Igor SHPARLINSKI, Macquarie University, 2007-09-07/14
- Damien VERGNAUD, Postdoc, 2006-04-24/26
- Thorsten KLEINJUNG, Univ. Bonn, 2005-02-23/27
- Edlyn TESKE, Univ. Waterloo, 2006-07-17/19.

Research domain

The aim of the Cryptology team which hosts the INRIA TANC project is to promote the study, implementation and use of robust and verifiable asymmetric cryptosystems based on algorithmic number theory.

It is clear from this sentence that we combine high-level mathematics and efficient programming. Our main area of competence and interest is that of algebraic curves over finite fields, most notably the computational aspects of these objects, that appear as a substitute of good old-fashioned cryptography based on modular arithmetic. One of the reasons for this change is the key size that is smaller for an equivalent security. We participate in the recent bio-diversity mood that tries to find substitutes for RSA, in case some attack would appear and destroy the products that employ it.

Whenever possible, we produce certificates (proofs) of validity for the objects and systems we build. For instance, an elliptic curve has many invariants, and their values need to be proved, since they may be difficult to compute.

Goals

Our research area includes :

- **Fundamental number theoretic algorithms :** we are interested in primality proving algorithms based on elliptic curves (F. Morain being the world leader in this topic), integer factorisation, and the computation of discrete logarithms over finite fields. These problems lie at the heart of the security of arithmetic based cryptosystems. We want to push primality and factorization as far as we can.
- **Algebraic curves over finite fields :** the algorithmic problems that we tackle deal with the efficient computation of group laws on Jacobians of curves, evaluation of the cardinality of these objects, and the study of the security of the discrete logarithm problem in such groups. These topics are the crucial points to be solved for potential use in real crypto products.
- **Complex multiplication :** the theory of complex multiplication is a meeting point of algebra, complex analysis and algebraic geometry. Its applications range from primality proving to the efficient construction of elliptic or hyperelliptic cryptosystems.

Results

Fundamental number theoretic algorithms

F. Morain worked on a fast variant of ECPP, called fastECPP, which led him to gain one order of magnitude in the complexity of the problem (see [18, 2]), reaching heuristically $O((\log N)^{4+\epsilon})$, compared to $O((\log N)^{5+\epsilon})$ for the basic version. By comparison, the best proven version of AKS [54] has complexity $O((\log N)^{6+\epsilon})$ and has not been implemented so far ; the best randomised version [58] reaches the same $O((\log N)^{4+\epsilon})$ bound but suffers from memory problems and is not competitive yet. F. Morain implemented fastECPP and was able to routinely prove the primality of $10,000$ decimal digit numbers [18], as opposed to $5,000$ for the basic (historical) version. F. Morain set the current world record to 20,562 decimal digits in early June 2006. This record was made

possible using an MPI-based implementation run on a cluster of 64-bit bi AMD Opteron(tm) Processors 250 at 2.39 GHz.

In ECPP, one looks for an auxiliary imaginary quadratic field having some special properties : if N is the number to be proven prime, one looks for a discriminant $D > 0$ such that $N = (U^2 + DV^2)/4$ (in integers U and V). The dominant step of the algorithm is the computation of $\sqrt{-D}$ modulo N. In fastECPP, this cost is reduced by using a basis of square roots of small q_i subproducts of which are assembled to get the D.

Once such a good D is known, there exists an elliptic curve E defined over $\mathbb{Z}/N\mathbb{Z}$ whose cardinality is $m = N + 1 - U$. If this number happens to be easy to factor (say $m = cN'$ with N' a probable prime and c a completely factored number), then the algorithm proceeds to compute an equation for E in the form $Y^2 = X^3 + AX + B$. The success of this part of the algorithm relies on the ability of computing rapidly class polynomials using complex multiplication (CM) techniques as explained in the section of same name below, say $H_D(X)$. This huge polynomial has to have roots modulo N, and these are found using the Cantor-Zassenhaus algorithm, after the splitting field of $H_D(X)$ has been decomposed into cyclic extensions (see [46, 45] and [51], where a fast reconstruction algorithm for algebraic integers is presented). Finally, a primality proof emerges as a point P of proven order N', and a recursive proof for N' is appended to complete the job.

Another improvement was introduced for finding quasi-smooth integers m. It uses an improved version of Bernstein's algorithm. This fast sieving procedure is described in [21].

Algebraic curves over finite fields

Group laws : After hyperelliptic curves, the next promising candidates for cryptosystems based on the discrete logarithm problem are superelliptic (of the form $Y^n = f(X)$) and so-called $C_{a,b}$ curves (of the form $Y^n - X^d = h(X, Y)$ with h of comparatively low degree). These curves, necessarily of genus 3 or higher, are attractive since their non-singular model has a unique point at infinity, so that the arithmetic in the Jacobian boils down to the arithmetic in the divisor class group. Algorithms have been presented in [49], relying on LLL, and [43], relying on Gröbner basis computation with an unknown complexity. Together with researchers from LIP 6, we have developed a new algorithm using basis changes in Gröbner bases, and ultimately simple linear algebra [4]. The relative simplicity of the algorithm has allowed us to develop explicit formulæ for the arithmetic expressed by operations in the ground field, and no more with polynomials over this field [19]. The formulæ are publicly available as MAGMA code and held the record for the lowest operation count at the time of publication.

Concerning the arithmetic of hyperelliptic curves of genus 2, the closest competitors to elliptic curves, substantial progress has been made by P. Gaudry. Using the theory of theta functions, he has been able to obtain novel formulæ on the Kummer surface of the curve that beat all previous formulæ and, when taking into account the different field sizes for an appropriate level of security in the two cases, appears to render genus 2 curves faster then elliptic ones [15].

Cardinality in genus 1 and large characteristic : F. Morain, helped by A. Enge and P. Gaudry, has been revisiting the SEA algorithm in genus 1, to see what was left to be improved since the last record, which was achieved in 1995 [42]. This led first to new easy records resulting from Moore's law. The program was completely rewritten in NTL and new algorithms were introduced, concerning mainly the fast search for eigenvalues ; this work was presented at ISSAC 2006 [29]. In [33], a new approach to the eigenvalue computation is described and proven.

Together with A. Bostan, B. Salvy (from the project ALGO), and É. Schost (team MAX at LIX), F. Morain gave quasi-linear algorithms for computing the explicit form of a strict isogeny between two elliptic curves, another important block in the SEA algorithm [14]. Note that isogenies now live their own lives in cryptography (see [57]) and that they are becoming an interesting computational primitive in cryptosystems. This is the reason why we organised a one-day workshop on that topic in July 2006.

The new record is currently (September 2007) for a prime p of 2500 decimal digits (again compared to 500dd back in 1995). This was made possible only because of A. Enge's new algorithm [40] for computing modular equations of index greater than 2000. These equations are still a stumbling block to reach higher cardinalities.

Cardinality in genus larger than 1 : After the ground breaking works of [47, 55], our team has been involved in developing algorithms for computing the cardinalities of curves of genus greater than 1 over fields of relatively small characteristic p. The common feature of all these algorithms is that they lift the problem to a p-adic field.

In large characteristic, the equivalent of the Schoof–Elkies–Atkin algorithm for elliptic curves is the only viable approach to point counting. P. Gaudry and É. Schost have developed an algebraic approach (relying on resultant computation) to obtain modular equations in genus 2 [7], already reduced modulo the field characteristic and specialised in the given curve. They reach a level of about 20, which should be compared to the gigabytes of data filled by the complete multivariate modular equation computed for levels 2 and 3 by R. Dupont [35]. Together with a clever adaptation of the random walk, birthday paradox approach to the L-polynomial of a genus 2 curve [23], this enables them to obtain a random curve of cryptographic size of about 160 bits over a prime field [22]. Together with A. Bostan, they obtain even larger cardinalities of about 192 bits over medium characteristic extension fields by profiting of the Cartier–Manin operator that yields information modulo p [20]. These implementations are currently the only ones obtaining random non-elliptic curves over medium to large characteristic fields that are suitable for cryptography.

Isogenies : Together with A. Bostan, B. Salvy (from projet ALGO), and É. Schost, F. Morain gave quasi-linear algorithms for computing the explicit form of a strict isogeny between two elliptic curves, another important block in the SEA algorithm [14]. This article contains a survey of previous methods, all applicable in the large characteristic case. Joux and Lercier have recently announced a p-adic approach for computing isogenies in medium characteristic.

For the small case, the old algorithms of Couveignes and Lercier were studied from scratch, and Lercier's algorithm reimplemented in NTL by F. Morain, as a benchmark for other methods still being developped. A master intern (L. De Feo) was put on cleaning the most recent of them, known as CouveignesII, that involves building the explicit p^k torsion of the curve and finding isomorphisms between Artin-Schreier towers. This work already led to the clarification of the complexities involved, and a fresh implementation in NTL is needed, that will be his first thesis work. A publication on the first results obtained is in preparation.

Discrete log on curves : Concerning the discrete logarithm problem on algebraic curves, the most promising algorithms rely on creating relations as smooth principal divisors on the curve and use linear algebra to deduce the discrete logarithms. Two research directions can be distinguished, that are both pursued by our team. The first approach consists of deriving complexity results for the genus tending to infinity and the size of the finite field growing only moderately. Typically, this results in algorithms of subexponential complexity $L(1/2)$. This direction has been followed by A. Enge in his doctoral thesis and later in collaboration with P. Gaudry. The second approach consists in analysing essentially the same algorithms for fixed genus, but with the field size tending to infinity. Typically, the outcome are exponential algorithms, but these may nevertheless be faster than generic algorithms of square root complexity and thus consist a threat for the cryptographic use of algebraic curves. This approach has been founded by P. Gaudry in his doctoral thesis.

Making clever use of the notion of large primes, P. Gaudry, N. Thériault, E. Thomé and C. Diem have succeeded in lowering the complexity of the above mentioned discrete logarithm algorithms for fixed genus so much that curves of genus 5 or higher are definitely eliminated from cryptography [16]. Curves of genus 1 or 2 are not affected, while those of genus 3 or 4 require the key size to be slightly increased and thus might survive in special situations.

For the very first time in algebraic curve cryptography, A. Enge and P. Gaudry have exhibited a class of curves in which the discrete logarithm problem is attacked by a subexponential algorithm of complexity less than $L(1/2)$. Precisely, the complexity is in $L(1/3)$ for the preliminary phase of computing the group structure and $L(1/3 + \varepsilon)$ for any $\varepsilon > 0$ for the discrete logarithms themselves. This shows that the corresponding algebraic curve cryptosystems, essentially based on $C_{a,b}$ curves with the degrees in X and Y growing in a special way with the genus, are no more secure than RSA and thus of no cryptographic interest. This result is a major step towards the goal of the TANC project to catalogue all classes of curves suited for cryptography. The publication [32]

was rewarded as one of the three best papers at the Eurocrypt 2007 conference, and we are invited to submit an extended version to *Journal of Cryptology*. A comparative implementation of the different algorithms of complexity $L(1/2)$ resp. $L(1/3)$ is underway by a master student of A. Enge's, J.-F. Biasse.

Complex multiplication

Genus 1 : The heart of the fastECPP algorithms is the ability to compute class polynomials easily. Classically, one builds the Hilbert class field $\mathbf{K}_H$ of an imaginary quadratic field $\mathbf{K} = \mathbb{Q}(\sqrt{-D})$ using special values of the classical modular function $j(q) = 1/q + 744 + \cdots$ (with $q = \exp(2i\pi\tau)$ for τ in the upper complex half plane). The sought minimal polynomial is

$$H_D[j](X) = \prod_{Q \in \mathrm{Cl}(-D)} (X - j(\tau_Q))$$

where $Q = (a, b, c)$ runs through a set of canonical representatives of $\mathrm{Cl}(-D)$ or in other words primitive reduced quadratic forms of discriminant $-D < 0$; for such Q, $\tau_Q = (-b + \sqrt{-D})/(2a)$. This polynomial has logarithmic height that can be approximated by :

$$\pi\sqrt{D} \sum_{[A,B,C] \in Cl(-D)} \frac{1}{A}$$

$$= O(\sqrt{D}(\log h)^2) = \tilde{O}(h),$$

where h is the class number and also the degree of the extension $\mathbf{K}_H/\mathbf{K}$.

In practice, even small values of $-D$ yield huge coefficients. Since Weber, the modular function j can be replaced with so-called *class invariants* that generate the same field, but with much smaller minimal polynomials. All the theory needed to find class invariants is now based on Shimura's reciprocity law, a nice version of it being given by Schertz. We dispose of a lot of possible invariants for a given $-D$ and we explained in [48] how to select the "smallest one".

To handle gigantic floating point numbers with up to several hundreds of thousands of bits, optimised libraries need to be used. Together with P. Zimmermann, A. Enge has written such a library for complex numbers, MPC [41], on top of MPFR. The library works at arbitrary precision and provides a precise semantics for rounding so that the result does not depend on the platform. It is freely available under the LGPL.

A further library, also available under LGPL, implements polynomials over the reals (MPFR) respectively the complex numbers (MPC). It implements asymptotically fast algorithms for multiplication such as Karatsuba, 3-way Toom–Cook and the FFT, as well as fast division using Newton iterations.

Our approach enabled us to compute class polynomials for discriminants used in fastECPP as large as $4,587,151,443$ (three hours CPU) or huge class numbers such as $14,720$ (1 hour and a half), Galois decomposition included.

Genus 2 : Our first contribution in this context is the 2-adic CM method, which is a more efficient alternative to the classical one. This was a joint work between P. Gaudry, T. Houtmann, D. R. Kohel, C. Ritzenthaler and A. Weng. The underlying problem is to compute Igusa class polynomials. Indeed computing Igusa class polynomials whose class number associated to the CM field was greater than ten was out of reach before our work. It is now possible for class numbers between fifty and a hundred. One direct application is to construct more secure cryptographic protocols based on hyperelliptic curves of genus two. Even if nobody has found a concrete attack against curves with small class numbers, it it desirable to be able to build curves with as large a class number as possible. This has at least the effect of enlarging the set of candidates.

Another problem was raised by our work : a correct definition of Igusa class polynomials in terms of exactly describing the CM variety associated to this polynomial system. We gave a full solution to the problem, see [38] and [28].

The second scientific achievement is the fundamental work of R. Dupont, which appears in [35, 9]. To understand the impact of his results, we have to mention that the real bottleneck of the CM method is the floating-point computation of special numbers, which are the equivalent of Siegel's singular values in genus two, namely the j-invariants of hyperelliptic curves of genus two having complex multiplication by the ring of integers of a special quartic CM field. In genus 1, the famous Arithmetic-Geometric-Mean (AGM) of Gauss can be used to compute the j-invariant of an elliptic curve. R. Dupont showed how to replace the AGM by sequences ruled by the Borchardt mean. He studied the action of the modular groups on theta constants in genus two and com-

pletely described modular equations ruling the theta constants. We have to notice that those formulæ are fundamental as they provide the foundations of the very efficient machinery of theta functions. R. Dupont studied several applications for his algorithms. The first one is the evaluation of theta constants in genus two, which leads to computing class polynomials and modular polynomials. He was the first to compute the modular polynomial for $p = 2$ and $p = 3$ in genus two[10]. A second application is evaluating holonomic functions and the final one is evaluating Riemann matrices of hyperelliptic curves of genus two or higher.

The third contribution is due to T. Houtmann on the classical CM method for genus two. He traced back the foundations of the CM method and designed a new approach pursuing A.-M. Spallek's and A. Weng's works. He divided the method into fundamental steps, which appeared to be much closer to Shimura's original results. He founded some algorithmic notions useful to understand how far the efficiency of the method could be pushed. He collaborated with R. Dupont to develop software for the analytic phase of the method where theta constants in genus two have to be computed. As a result, he obtained the most efficient and most general CM method for genus two and was able to compute Igusa class polynomials of a size previously beyond reach. The original limitations of A.-M. Spallek's, A. Weng's and P. van Wamelen's versions were taken away. He recollected mathematical facts and designed a new and more general representation of quartic CM fields and worked on the construction phase of hyperelliptic curves of genus two suitable for cryptography, i. e., the generation of models of curves starting with precomputed Igusa class polynomials. Here he pursued and generalised A.-M. Spallek's and A. Weng's work. He solved several open problems posed by A. Weng. Publications for those results are in preparation. In the same way the software he developed will be available in the near future.

Identity cards of elliptic curves

One of the main goals of the TANC project is to determine the *identity card* of an elliptic curve, that collects and certifies properties of potential relevance for its cryptographic security. These include the cardinality (already discussed) and the endomorphism ring (see paragraph on complex multiplication, that permits to construct a curve with a given endomorphism ring).

For a random curve, the class group of its endomorphism ring, an order in an imaginary quadratic number field, is of interest ; some cryptographic standards, for instance, prescribe a minimum size of this class group [44]. G. Guerpillon, master student of A. Enge's, has implemented and optimised a subexponential algorithm for computing these class groups. The currently undertaken parallelisation of his implementation should enable us to reach a new record for this kind of computation. One of the main ingredients, the Hermite normal form computation of an integral matrix, has been reused by J.-F. Biasse in the context of discrete logarithms on $C_{a,b}$ curves, see Section .

The subexponential algorithm returns the group as a product of cyclic groups with their generators. For the case when all elements need to be explicitly enumerated, A. Enge has developed quasi-linear algorithms in [39].

A topic not listed yet : cryptographic protocols, networks

In this section, we describe some of the exploratory directions we underwent in the last years, before coming back to our basis. We tried to approach some other parts of cryptography and applications relying on properties of elliptic curves. This is the reason why we hired two postdoctoral students, namely J. Herranz and F. Laguillaumie.

ID based cryptography : This was actually our first incursion into the protocol world. Everybody knows that the most difficult problem in modern cryptography, and more precisely its would-be widespread use, is the key authentication problem, or more generally that of authenticating principals on an open network. The "classical" approach to this problem is that of a *public key infrastructure* (PKI), in which some centralised or distributed authority issues certificates for authenticating the different users. Another approach, less publicised, is that of *identity based cryptography* (ID), in which the public key of a user can be built very easily from his email address for instance. The cryptographic burden is then put on the shoulders of the *private key generator* (PKG) that

[10] available at `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/MODPOL_2.tar.gz`

must be contacted by the users privately to get their secret keys and open their emails. The ID approach can be substituted to the PKI approach in some cases, where some form of ideal trustable PKG exists (private networks, etc.).

This ID idea is not new, but no efficient and robust protocol was known prior to the ideas of Boneh et al. using pairings on elliptic curves. R. Dupont and A. Enge have worked on such an ID-system. They have defined a notion of security for such a protocol and have given a proof of security of a generalisation of a system of Sakai, Ohgishi and Kasahara's in this model [10].

CM is the only way of obtaining secure ordinary elliptic curves suitable for such pairing-based systems. Our experience in the field has enabled us to be among the first to propose CM constructions in this context [5].

Following these first excursions into the protocol world, A. Enge has co-supervised B. Libert's PhD thesis, which led to a six months visit in our team. B. Libert's thesis [56] makes important contributions to the topic of ID based cryptography using bilinear pairings on algebraic curves. Among others, it suggests faster variants of the Boneh–Franklin encryption scheme and presents the fastest identity based signcryption scheme on the market. After his visit, he stayed in contact with our team and worked with our postdoc F. Laguillaumie on signature schemes with special properties [31], see below.

Aggregate signatures : a current area of research is related to the aggregation of different signatures on different messages. In many applications, it is desirable to be able to transform many signatures on different messages into a single signature, in such a way that the length of this (aggregate) signature is much less than the total length of the initial signatures. A recipient should be able to verify the correctness of all the initial signatures by using only the list of messages and the aggregate signature, ideally with less computational efforts than in the case where he has to verify all the signatures one by one.

For traditional PKI-based signature schemes, some efficient proposals of aggregate signature schemes have been proposed [50, 52]. In particular, in [50], the length of the resulting aggregate signature is constant, independent of the number of messages and the number of signers. This proposal uses bilinear pairings as a tool. Using RSA techniques, the obtained aggregate signatures have a length which is independent of the number of messages, but still linear with respect to the number of signers.

In the scenario of identity-based signatures, none of the existing signature schemes allows an efficient aggregation of signatures, in the sense that resulting aggregate signatures have a length which is always linear with respect to the number of messages. To partially solve this problem, J. Herranz has proposed in [12] a new identity-based signature scheme, which allows to obtain an aggregate signature whose length is independent of the number of messages, but linear with respect to the number of signers. In situations where one wants to aggregate many signatures coming from a small set of signers (even a unique signer) the length of the resulting signatures is simply constant.

Special (short) signatures : To achieve specific properties desired in real-world applications of cryptography, variants of the classical digital signatures have been designed. Undeniable signatures and confirmer signatures are examples of such variants. Directed signatures differ from the well-known confirmer signatures in that the signer has the simultaneous abilities to confirm, deny and individually convert a signature. The universal conversion of these signatures has remained an open problem since their introduction in 1993. F. Laguillaumie, in collaboration with P. Paillier (Gemplus) and D. Vergnaud (Univ. Caen) provides in the Asiacrypt'05 paper "Universally Convertible Directed Signatures" [24] a positive answer to this quest by showing a very efficient design for universally convertible directed signatures, both in terms of computational complexity and signature size. The construction relies on the so-called xyz-trick, previously introduced by F. Laguillaumie and D. Vergnaud, applicable to bilinear map groups.

F. Laguillaumie, in collaboration with D. Vergnaud, also introduced a new undeniable signature scheme which is existentially unforgeable and anonymous under chosen message attacks in the standard model [53]. The scheme is an embedding of Boneh and Boyen's recent short signature scheme into a group where the decisional Diffie-Hellman problem is assumed to be difficult. The anonymity of the scheme relies on a decisional variant of the strong Diffie-Hellman assumption, while its unforgeability relies

on the strong Diffie-Hellman assumption.

In collaboration with B. Libert and J.-J. Quisquater [31], F. Laguillaumie designed two fairly efficient universal designated verifier signature (UDVS) schemes which are secure (in terms of unforgeability and anonymity) in the *standard model* (i.e. without random oracles). Their security relies on algorithmic assumptions which are much more classical than assumptions involved in the two only known UDVS schemes in standard model to date. The latter schemes rely on the Strong Diffie-Hellman assumption and the strange-looking *knowledge of exponent assumption* (KEA). The proposed schemes are also the first random oracle-free constructions with the anonymity property.

Finally, J. Herranz and F. Laguillaumie proposed in [30] a blind ring signature scheme based on pairings on algebraic curves. They formally prove the security (anonymity, blindness and unforgeability) of their scheme in the random oracle model, under quite standard assumptions. Blind ring signatures are useful, for instance, to design secure e-cash systems involving several banks.

Security in *ad'hoc* networks : F. Morain and D. Augot (CODES) participate in the ACI SERAC (SEcuRity models and protocols for Ad-hoC Networks), which started in September 2004. Their interest there is to understand the (new ?) cryptographic needs and to try to invent new trust models.

It is clear that the recent arrival of HIPERCOM (also a member of SERAC) at École polytechnique triggers new collaborations in that direction.

A collaboration between TANC (J. Herranz, F. Laguillaumie) and CODES (R. Bhaskar) via the SERAC project of the ACI S&I has led to [26].

Achieving secure routing in ad-hoc networks is a big challenge. The typical way to prevent or reduce the possible attacks is to use mechanisms to authenticate the origin of all messages. Standard (asymmetric) signature schemes provide these mechanisms, but may result in inefficient implementations, especially when many nodes (and thus many signatures) are expected.

Some of these efficiency problems can be reduced by using aggregate signatures, which improve the length and the cost of managing many different signatures. In this article, they propose a new concept, aggregate designated verifier signature schemes, which can be implemented in a more efficient way than standard aggregate signatures (for example by using MACs). Such schemes can be sufficient to authenticate the establishment of routes in reactive protocols. Formal definitions for the new primitive and the required security properties are given. Moreover a specific and efficient scheme is proposed which uses MACs, and is proven secure in the random oracle model.

The article [13] is an extension of [26] : they especially add the ID-based feature.

Together with HIPERCOM, we have recently proposed to Digiteo an OMT[11] named *CryptoNet*. The aim of Cryptonet is to study how elliptic curves over finite fields can be used to provide security mechanisms for ad'hoc networks. The main interest of elliptic curves in that setting is the low cost and (a priori) low bandwith required for a given level of security, as compared to traditional finite field based systems. The proposal has been accepted, allowing to hire an engineer who will implement our encryption techniques in a network simulator.

Algebraic geometry codes : Daniel Augot is studying the decoding of error correcting codes based on algebraic curves (algebraic geometry codes). These codes are a successful generalization of the Reed-Solomon codes, because they provide good error correction capacities. The main drawback of these codes is that the known decoding algorithms of these codes have a too large complexity, that is to say, higher than quadratic in terms of the length of the code. Project-Team TANC has successfully used techniques and advanced algorithms from computer algebra to obtain fast algorithms in the domain of cryptography. Daniel Augot wants to build upon this knowledge to get efficient decoding algorithms of algebraic geometry codes. The first step is to efficiently decode Hermitian codes, whose decoding complexity is currently in $O(n^{7/3})$. These codes are indeed the most understood of AG codes, and they are also good candidates for using the Guruswami-Sudan principles for list-decoding.

[11] *Opération de Maturation Technologique*

Software, patents and contracts

Software

ECPP

F. Morain has been continuously improving his primality proving algorithm called ECPP, originally developed in the early '90. Binaries for version 6.4.5 are available since 2001 on his web page[12]. Proving the primality of a 512 bit number requires less than a second on a GHz PC. His personal record is about 20,000 decimal digits, with the fast version he started developing in 2003.

mpc

The `mpc` library, developed in C by A. Enge in collaboration with P. Zimmermann, implements the basic operations on complex numbers in arbitrary precision, which can be tuned to the bit. This library is based on the multiprecision libraries `gmp` and `mpfr`. Each operation has a precise semantics, in such a way that the results do not depend on the underlying architecture. Several rounding modes are available. This software, licensed under the GNU Lesser General Public License (LGPL), can be downloaded freely from the URL `http://www.lix.polytechnique.fr/Labo/Andreas.Enge/Software.html`.

The latest version 0.4.6 has been released in September 2007. The library currently benefits from an Opération de développement logiciel of INRIA.

The `mpc` library is used in our team to build curves with complex multiplication and to compute modular polynomials (cf. Section), and it is *de facto* incorporated in the ECPP program.

mpfrcx

The `mpfrcx` library is developed in C by A. Enge to implement the arithmetic of univariate polynomials with floating point coefficients of arbitrary precision, be they real (`mpfr`) or complex (`mpc`). The first version 0.1, published in October 2007 and available at

`http://www.lix.polytechnique.fr/Labo/Andreas.Enge/Software.html`,

contains the functionality needed for the author's complex multiplication programme. Advanced asymptotically fast algorithms have been implemented, such as Karatsuba and Toom–Cook multiplication, various flavours of the FFT and division with remainder by Newton iterations. Special algorithms of symbolic computation such as fast multievaluation are also available.

Publishing `mpfrcx` is part of an ongoing effort to make A. Enge's programme for building elliptic curves with complex multiplication available. This programme is a very important building block for cryptographic purposes as well as for primality proving (fastECPP).

Industrial Contracts

– Title : Gemplus ; Period : 2002–2004 ; Type : accompanying contract for E. Brier's thesis.

Teaching, dissemination and service

Teaching

F. Morain : 192 hours at École polytechnique at various levels from L123 to M1. He is also vice-head of the DIX (Computer Science Department) and reprensents École polytechnique in the Commission des études of the MPRI (Master Parisien de Recherches en Informatique).

A. Enge : 96 hours per year at École polytechnique, teaching computer science at all levels.

A doctorate level course of 9 hours on algebraic curve cryptography at the Université Bordeaux I in 2004.

Participation in various summer schools on algebraic curves and cryptography : Bedlewo, Poland, 2003 ; Bochum, Germany, 2004 ; Montpellier 2005.

A multimedia lecture on selected topics in cryptography at École polytechnique in 2004, since then available at the site of ParisTech.

T. Houtmann : 64 hours as moniteur at École polytechnique.

Dissemination

– In 2005, A. Enge has taken part in the INRIA booth during the "Salon des jeux et de la culture mathématiques" in Paris with a presentation of public key cryptography aimed at a general public.

[12] `http://www.lix.polytechnique.fr/Labo/Francois.Morain`

– In 2005, A. Enge and R. Dupont have presented INRIA at the Forum des métiers scientifiques at École polytechnique. During the welcoming seminar of INRIA, A. Enge has given an overview of the TANC project.

Service

A. Enge is a member of the International Relations Working Group (GTRI) at the Scientific and Technological Orientation Council (COST) of INRIA. As such, he has participated in selection of postdoc positions for the European ERCIM consortium and in the selection of international Associated teams.

Visibility

National scientific cooperations

– ACI SÉCURITÉ CESAM : elliptic curves for the security of mobile networks.
– ACI SÉCURITÉ SERAC : SEcuRity models and protocols for Ad-hoC networks.
– ANR Cado (2006–) : two meetings (18-19/01/07 in Nancy for the kickoff and 21-21/06/07 in Paris).

International scientific cooperations

– Together with the CODES project at INRIA Rocquencourt, the project TANC participates in ECRYPT, a NoE in the Information Society Technologies theme of the 6th European Framework Programme (FP6).
– 2005–2006 : PAI "Procope" with the group "Algebra and Number Theory" of the TU-Berlin (Florian Heß).
– The TANC project is involved in the associated team ECHECS (“Extreme Computing for (Hyper-)Elliptic Cryptographic Systems”) with É. Schost of University of Western Ontario, London, continuing a long-standing collaboration. Our joint work is concerned with using advanced algorithms of symbolic computation (speciality of the Canadian team) in the context of elliptic and hyperelliptic curve cryptography (speciality of TANC), in particular for the instantiation of secure cryptosystems.

Conference and seminar invitations

A. Enge has been an invited speaker at Moraviacrypt ’05 — The 5th Central European Conference on Cryptography at Brno, Czech Republic.

He has presented his work at the seminars of the SPACES project at Nancy, of the Algebra and Number Theory group at the TU-Berlin and of the Crypto group at Université Catholique de Louvain. He has spent one week in December with the Algebra and Number Theory group in Berlin. A. Enge has been invited to give a talk entitled “An $L(1/3)$ algorithm for the discrete logarithm problem in low degree curves” at Elliptic Curve Cryptography ECC 2006 in Toronto. He has presented his results at the Journées Nationales de Calcul Formel 2005 at Luminy, the Second Irsee Conference on Finite Geometries 2006 and the Ecrypt workshop “Curves, isogenies and cryptologic applications” at École polytechnique. He has given seminar talks at the Technische Universität Berlin and the universities of Caen, Leiden and Limoges. A. Enge has been invited as a plenary lecturer to ACISP 2007 – 12th Australasian Conference on Information Security and Privacy at Townsville, Australia, with a talk entitled "Constructing cryptographic curves" ; and to Fq8 – 8th International Conference on Finite Fields and Applications at Melbourne, speaking on "The discrete logarithm problem for algebraic curves". [32] has been presented at Eurocrypt 2007 in Barcelona by A. Enge ; it has been elected as one of the three best papers of the conference by the programme committee. A. Enge has given two lectures on “Constructing elliptic curves by complex multiplication” and “Subexponential discrete logarithm algorithms for finite fields” at the ICE-EM RNSA Workshop on Pairing Based Cryptography, Brisbane, Australia.

F. Morain : Barcelona 28-29/10. Winter school CIMPA in Bangalore. SHARCS (Paris, 24-25/02), Eurocrypt’05 (Aarhus, 23-26/05/05) ; visited University of Calgary (“The end of primality”) and workshop in Banff (“SEA++”), November 2005. F. Morain : Calgary (his talk : The end of primality ?) /Banff 2005-11-03 till 2005-11-10 (invited to a workshop, spoke about SEA++) ; in Séminaire Algo (29/05), he spoke about *fast isogeny computations*. He attended ANTS-VII in Berlin (July 23–29). F. Morain has been invited as a plenary lecturer to the “Workshop on Computational challenges arising in algorithmic number theory and Cryptography”, October 30- November 3, 2006, in the Fields Institute in Toronto (Ca-

nada). There he presented [33].

N. Gürel has given talks in Limoges (March), Paris 6 (April), ENSTA (October), Rennes (November) and Versailles (December).

Javier Herranz attended Crypto'05 (August 14-18, 2005, Sta. Barbara, California, USA) and the 2nd OLSR Interop & Workshop (July 28-29, 2005, Palaiseau, France, together with F. Morain. A. Enge and T. Houtmann). He spent one week (October 1st-7th, 2005) at Radboud University, invited by the Security of Systems group of that university, in Nijmegen (The Netherlands). There he has given a seminar (October 5th, 2005), entitled 'Aggregate Signatures'. J. Herranz attended the 'Journées de Sécurité INRIA', in Grenoble (France), December 12-14, 2005. He gave there the talk 'Cryptography and routing protocols'.

F. Laguillaumie attended Asiacrypt'05 (December 4–8, Chennai - India) and Indocrypt'05 (December 10–12, Bangalore - India). During Asiacrypt'05, F. Laguillaumie also participates to a meeting between indian and french experts to organize some possible collaborations. F. Laguillaumie attended - Information Security ISC 2006 - Samos (Greece) - August 30 - September 2, 2006. He gave talks in Limoges, ENSTA, IRMAR/CELAR, Versailles St-Quentin-en-Yvelines.

R. Dupont attended "Journées Codage et Cryptographie" (Aussois), Februrary 4, 2005 and presented *Évaluation rapide de formes modulaires via l'AGM* ; Number theory seminar, Technische Universität Berlin (Germany), February 9, 2005 : *Borchardt's mean, theta constants and applications to the evaluation of Riemann matrices and modular forms* ; Séminaire SPACES (LORIA, Nancy), March 3, 2005 : *Theta constantes et moyenne de Borchardt, applications* ; Séminaire ALGO (INRIA Rocquencourt), November 7, 2005 : *AGM, theta constantes et applications* ; Journées Nationales de Calcul Formel (CIRM, Luminy), November 25, 2005 : *Évaluation rapide de fonctions modulaires via l'AGM*. R. Dupont has given a talk on "AGM et évaluation rapide de fonctions modulaires" at the Séminaires CF et CAA at Limoges. He attended Indocrypt'06 in Calcutta.

T. Houtmann has given talks in Aussois (Journées Codes et Cryptographie 2005), in Caen (April 2005). He attended Eurocrypt'05 in Aarhus, CAEN'05 and XVI-ièmes rencontres arithmétiques de Caen. He attended FICS summer school on elliptic curve cryptography in Copenhagen, ECC2005 in Copenhagen too. He visited the KANT group in Berlin (5-9/12/2005). T. Houtmann has given a talk in Eymoutiers (Journées «Codes et Cryptographie» 2006). He presented joint work with P. Gaudry, D. Kohel, C. Ritzenthaler and A. Weng in Shanghai (Asiacrypt'06). He was invited to Sydney. He attended ANTS-VII in Berlin, ECC2006 in Toronto, a workshop on computational aspects arising in algorithmic number theory and cryptography in Toronto and Indocrypt'06 in Calcutta.

J. Milan attended the GForge seminar at INRIA Futurs on 2006-02-09.

Conference organisation

- A. Enge and F. Morain organized a one-day workshop on isogenies in July 2006 at LIX.

Program committees

- F. Morain has been a member of the programme committee of Indocrypt 2005, held in Bangalore, India, in December. F. Morain was in the program committee of ANTS-VII, held in Berlin, July 2006.
- A. Enge has co-organised the Journées Nationales du Calcul Formel 2005 from November 21 to 25 at Luminy. A. Enge took part in the programme committees of Pairing 2007 – First International Conference on Pairing-Based Cryptography in Tokio and WCC 2007 – International Workshop on Coding and Cryptography in Versailles. He acted on the scientific advisary board of the Journées Nationales de Calcul Formel 2007 at Luminy.
- J. Herranz was in the committee of the Workshop ACIS'06 : Applied Cryptography and Information Security (in conjuction with ICCSA'06), May 8-11, 2006, Glasgow, UK.
- F. Laguillaumie participated in the program committee of the Workshop on Collaboration and Security (COLSEC'06), held at The 2006 International Symposium on Collaborative Technologies and Systems (CTS'06).

Journal editorial boards

- A. Enge is editor of "Designs, Codes and Cryptography". He has co-edited the special issue "Algorithmic Number Theory and Its Applica-

tions" of the Japan Journal of Industrial and Applied Mathematics.

Awards

- A. Enge has been awarded a 2004 Kirkman Medal of the Institute for Combinatorics and its Applications. The medal recognises outstanding work by ICA members in their early research careers.
- F. Morain was dubbed "Chevalier des Palmes Académiques" on January 19, 2006.

References

Books and chapters in books

2005

[1] GAUDRY, P. Chapter 7 : Hyperelliptic curves and the HCDLP. In *Advances in Elliptic Curve Cryptography* (2005), I. Blake, G. Seroussi, and N. Smart, Eds., vol. 317 of *London Mathematical Society Lecture Note Series*, Cambridge University Press. In press.

[2] MORAIN, F. Elliptic curves for primality proving. In *Encyclopedia of cryptography and security*, H. C. A. van Tilborg, Ed. Springer, 2005.

International journals

2004

[3] ENGE, A., AND SCHERTZ, R. Constructing elliptic curves over finite fields using double eta-quotients. *Journal de Théorie des Nombres de Bordeaux 16* (2004), 555–568.

2005

[4] BASIRI, A., ENGE, A., FAUGÈRE, J.-C., AND GÜREL, N. The arithmetic of Jacobian groups of superelliptic cubics. *Math. Comp. 74* (2005), 389–410.

[5] DUPONT, R., ENGE, A., AND MORAIN, F. Building curves with arbitrary small MOV degree over finite prime fields. *J. of Cryptology 18*, 2 (2005), 79–89.

[6] ENGE, A., AND SCHERTZ, R. Modular curves of composite level. *Acta Arith. 118*, 2 (2005), 129–141.

[7] GAUDRY, P., AND SCHOST, É. Modular equations for hyperelliptic curves. *Math. Comp. 74* (2005), 429–454.

[8] GÜREL, N. Extracting bits from coordinates of a point of an elliptic curve. Preprint, `http://eprint.iacr.org/2005/324`, 2005.

2006

[9] DUPONT, R. Fast evaluation of modular functions using Newton iterations and the AGM. *Math. Comp. XXX* (2006). To appear.

[10] DUPONT, R., AND ENGE, A. Provably secure non-interactive key distribution based on pairings. *Discrete Applied Mathematics 154*, 2 (2006), 270–276.

[11] GAUDRY, P., SCHOST, É., AND THIÉRY, N. M. Evaluation properties of symmetric polynomials. *Internat. J. Algebra Comput. 16*, 3 (2006), 505–523.

[12] HERRANZ, J. Deterministic identity-based signatures for partial aggregation. *The Computer Journal 49*, 3 (2006), 322–330.

2007

[13] BHASKAR, R., HERRANZ, J., AND LAGUILLAUMIE, F. Aggregate designated verifier signatures and application to secure routing. *International Journal of Security and Networks - Special Issue on Cryptography in Networks*, 3/4 (2007), 192–201.

[14] BOSTAN, A., MORAIN, F., SALVY, B., AND SCHOST, É. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp. xxx* (2007), yyy. To appear.

[15] GAUDRY, P. Fast genus 2 arithmetic based on Theta functions. *Journal of Mathematical Cryptology 1* (2007), 243–265.

[16] GAUDRY, P., THOMÉ, E., THÉRIAULT, N., AND DIEM, C. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comp. 76* (2007), 475–492.

[17] MORAIN, F. Computing the cardinality of CM elliptic curves using torsion points. To appear in *J. Théor. Nombres Bordeaux.*, `http://arxiv.org/ps/math.NT/0210173`, June 2007.

[18] MORAIN, F. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm. *Math. Comp. 76* (2007), 493–505.

International conferences with proceedings

2004

[19] BASIRI, A., ENGE, A., FAUGÈRE, J.-C., AND GÜREL, N. Implementing the arithmetic of $C_{3,4}$ curves. In *Algorithmic Number Theory — ANTS-VI* (Berlin, 2004), D. Buell, Ed., vol. 3076 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 87–101.

[20] BOSTAN, A., GAUDRY, P., AND SCHOST, É. Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves. In *Finite Fields and Applications, 7th International Conference, Fq7* (2004), G. Mullen, A. Poli, and H. Stichtenoth, Eds., vol. 2948 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 40–58.

[21] FRANKE, J., KLEINJUNG, T., MORAIN, F., AND WIRTH, T. Proving the primality of very large numbers with fastecpp. In *Algorithmic Number Theory* (2004), D. Buell, Ed., vol. 3076 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 194–207. 6th International Symposium, ANTS-VI, Burlington, VT, USA, June 2004, Proceedings.

[22] GAUDRY, P., AND SCHOST, É. Construction of secure random curves of genus 2 over prime fields. In *Advances in Cryptology – EUROCRYPT 2004* (2004), C. Cachin and J. Camenisch, Eds., vol. 3027 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 239–256.

[23] GAUDRY, P., AND SCHOST, É. A low memory parallel version of Matsuo, Chao and Tsujii's algorithm. In *ANTS-VI* (2004), D. Buell, Ed., vol. 3076 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 208–222.

2005

[24] LAGUILLAUMIE, F., PAILLIER, P., AND VERGNAUD, D. Universally convertible directed signatures. In *Advances in Cryptology - Asiacrypt 2005* (2005), B. Roy, Ed., vol. 3788 of *Lecture Notes in Comput. Sci.*, Springer, pp. 682–701.

[25] LAGUILLAUMIE, F., AND VERGNAUD, D. Short undeniable signatures without random oracles : the missing link. In *Progress in Cryptology - Indocrypt 2005* (2005), R. V. S. Maitra, C. E. Veni Madhavan, Ed., vol. 3797 of *Lecture Notes in Comput. Sci.*, Springer, pp. 283–296.

2006

[26] BHASKAR, R., HERRANZ, J., AND LAGUILLAUMIE, F. Efficient authentication for reactive routing protocols. In *AINA'06 (SNDS'06)* (2006), vol. II, IEEE Computer Society, pp. 57–61.

[27] GALINDO, D., AND HERRANZ, J. A generic construction for token-controlled public key encryption. In *Financial Cryptography and Data Security* (2006), G. D. Crescenzo and A. Rubin, Eds., vol. 4107 of *Lecture Notes in Comput. Sci.*, Springer Verlag, pp. 177–190. 10th International Conference, FC 2006 Anguilla, British West Indies, February 27-March 2.

[28] GAUDRY, P., HOUTMANN, T., KOHEL, D., RITZENTHALER, C., AND WENG, A. The 2-adic CM method for genus 2 with application to cryptography. In *Advances in Cryptology – ASIACRYPT 2006* (2006), X. Lai and K. Chen, Eds., vol. 4284 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 114–129.

[29] GAUDRY, P., AND MORAIN, F. Fast algorithms for computing the eigenvalue in the Schoof-Elkies-Atkin algorithm. In *ISSAC '06 : Proceedings of the 2006 international symposium on Symbolic and algebraic computation* (New York, NY, USA, 2006), ACM Press, pp. 109–115.

[30] HERRANZ, J., AND LAGUILLAUMIE, F. Blind ring signatures secure under the chosen target CDH assumption. In *Information Security, ISC 2006* (2006), S. K. Katsikas, J. Lopez, M. Backes, S. Gritzalis, and B. Preneel,

Eds., vol. 4176 of *Lecture Notes in Comput. Sci.*, Springer, pp. 117–130.

[31] LAGUILLAUMIE, F., LIBERT, B., AND QUISQUATER, J.-J. Universal Designated Verifier Signatures Without Random Oracles or Non-Black Box Assumptions. In *Fifth Conference on Security and Cryptography for Networks (SCN'06)* (2006), R. D. Prisco and M. Yung, Eds., vol. 4116 of *Lecture Notes in Comput. Sci.*, Springer Verlag, pp. 63–77.

2007

[32] ENGE, A., AND GAUDRY, P. An $L(1/3 + \varepsilon)$ algorithm for the discrete logarithm problem for low degree curves. In *Advances in Cryptology — Eurocrypt 2007* (Berlin, 2007), M. Naor, Ed., vol. 4515 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 367–382.

[33] MIHĂILESCU, P., MORAIN, F., AND SCHOST, É. Computing the eigenvalue in the Schoof-Elkies-Atkin algorithm using Abelian lifts. In *ISSAC '07 : Proceedings of the 2007 international symposium on Symbolic and algebraic computation* (New York, NY, USA, 2007), ACM Press, pp. 285–292.

Dissemination

2006

[34] MORAIN, F. *Encyclopédie de l'informatique et des systèmes d'information (sous la direction de J. Akoka et I. Comyn-Wattiau)*. Vuibert, 2006, ch. Algorithmes algébriques.

PhD Thesis

2006

[35] DUPONT, R. *Moyenne arithmético-géométrique, suites de Borchardt et applications*. PhD thesis, École polytechnique, `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf`, 2006.

Miscellaneous

2004

[36] GAUDRY, P. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. Cryptology ePrint Archive : Report 2004/073, `http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/semweil.ps.gz`, 2004.

[37] MORAIN, F. La primalité en temps polynomial [d'après Adleman, Huang ; Agrawal, Kayal, Saxena]. *Astérisque 294* (2004), Exp. No. 917, ix, 205–230. Séminaire Bourbaki. Vol. 2002/2003.

2005

[38] GAUDRY, P., HOUTMANN, T., KOHEL, D., RITZENTHALER, C., AND WENG, A. The p-adic method for genus 2. Preprint, `http://arxiv.org/abs/math.NT/0503148`, 2005.

2006

[39] ENGE, A. The complexity of class polynomial computation via floating point approximations. HAL-INRIA 1040, INRIA, `http://hal.inria.fr/inria-00001040`, 2006.

2007

[40] ENGE, A. Computing modular polynomials in quasi-linear time. HAL-INRIA 143084 et ArXiv 0704.3177, INRIA, `http://hal.inria.fr/inria-00143084`, 2007.

[41] ENGE, A., AND ZIMMERMANN, P. `mpc` — a library for multiprecision complex arithmetic with exact rounding, `http://www.lix.polytechnique.fr/Labo/Andreas.Enge/Software.html`, 2007. Version 0.4.6.

External references

[42] MORAIN, F. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *J. Théor. Nombres Bordeaux 7* (1995), 255–282.

[43] ARITA, S. Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log based public key cryptosystems. *IEICE Transactions J82-A*, 8 (1999), 1291–1299. In Japanese. English translation in the proceedings of the Conference on The Mathematics of Public Key Cryptography, Toronto 1999.

[44] BSI (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). Geeignete Kryptoalgorithmen gemäß § 17 (2) SigV. `http://www.bsi.de/aufgaben/projekte/pbdigsig/download/kryptalg.pdf`, 1999.

[45] HANROT, G., AND MORAIN, F. Solvability by radicals from a practical algorithmic point of view. Submitted, `http://www.lix.polytechnique.fr/Labo/Francois.Morain`, Nov. 2001.

[46] HANROT, G., AND MORAIN, F. Solvability by radicals from an algorithmic point of view. In *Symbolic and algebraic computation* (2001), B. Mourrain, Ed., ACM, pp. 175–182. Proceedings ISSAC'2001, London, Ontario.

[47] KEDLAYA, K. S. Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society 16*, 4 (2001), 323–338.

[48] ENGE, A., AND MORAIN, F. Comparing invariants for class fields of imaginary quadratic fields. In *Algorithmic Number Theory* (2002), C. Fieker and D. R. Kohel, Eds., vol. 2369 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 252–266. 5th International Symposium, ANTS-V, Sydney, Australia, July 2002, Proceedings.

[49] GALBRAITH, S. D., PAULUS, S. M., AND SMART, N. P. Arithmetic on superelliptic curves. *Math. Comp. 71*, 237 (2002), 393–405.

[50] BONEH, D., GENTRY, C., LYNN, B., AND SHACHAM, H. Aggregate and verifiably encrypted signatures from bilinear maps. In *Advances in Cryptology – EUROCRYPT 2003* (2003), E. Biham, Ed., vol. 2656 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 416–432.

[51] ENGE, A., AND MORAIN, F. Fast decomposition of polynomials with known Galois group. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (2003), M. Fossorier, T. Høholdt, and A. Poli, Eds., vol. 2643 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 254–264. 15th International Symposium, AAECC-15, Toulouse, France, May 2003, Proceedings.

[52] LYSYANSKAYA, A., MICALI, S., REYZIN, L., AND SHACHAM, H. Sequential aggregate signatures from trapdoor permutations. In *Advances in Cryptology – EUROCRYPT 2004* (2004), C. Cachin and J. Camenisch, Eds., vol. 3027 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 74–90.

[53] LAGUILLAUMIE, F., AND VERGNAUD, D. Short Undeniable Signatures Without Random Oracles : the Missing Link. In *Progress in Cryptology - Proceedings of Indocrypt'05* (2005), R. V. S. Maitra, C. E. Veni Madhavan, Ed., vol. 3797 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 283–296.

[54] LENSTRA, JR., H. W., AND POMERANCE, C. Primality testing with Gaussian periods. Preprint, `http://www.math.dartmouth.edu/~carlp/PDF/complexity072805.pdf`, July 2005.

[55] LAUDER, A. G. B., AND WAN, D. Counting points on varieties over finite fields of small characteristic. In *Algorithmic Number Theory : Lattices, Number Fields, Curves and Cryptography* (Cambridge, 2006), J. P. Buhler and P. Stevenhagen, Eds., Mathematical Sciences Research Institute Publications, Cambridge University Press. To appear ; preprint available since 2002.

[56] LIBERT, B. *New Secure Applications of Bilinear Maps in Cryptography*. Thèse de doctorat, Université catholique de Louvain, Louvain-la-Neuve, 2006.

[57] TESKE, E. An elliptic trapdoor system. *J. of Cryptology 19*, 1 (2006), 115–133.

[58] BERNSTEIN, D. Proving primality in essentially quartic expected time. *Math. Comp. 76* (2007), 389–403.

HIgh PERformance COMmunication

[13]

Team members

Team leader

Philippe JACQUET

Permanent members

- Thomas CLAUSEN, Maître de Conférence à l'École Polytechnique
- Emmanuel BACCELLI, Chargé de Recherche INRIA, since October 2006
- Philippe JACQUET, Directeur de Recherche INRIA.

Phds

- Emmanuel BACCELLI, bourse CIFRE, until February 2006 ;
- Song Yean CHO, bourse Egide-INRIA, since September 2005
- Georgios RODOLAKIS, bourse INRIA, until June 2007

Interns

- Frederic GALANO, École Polytechnique, spring 2005
- Julien GARNIER, École Polytechnique, spring 2005
- Guillaume BANDET, École Polytechnique, spring 2006
- Florent BRUNEAU, École Polytechnique, spring 2006
- Juan Antonio Cordero FUERTES, Technical University of Catalonia UPC (Spain), Masters Thesis, 2006
- Alexandru DRAGUSIN, Cornell University, undergraduate internship, 2007
- Ulrich HERDEBERG, TU München, Master Thesis, from September 2006 to June 2007
- Andreas SCHONHAUG, NTU, Norway, Masters Thesis, 2007
- Hiep Hoang VU, École Polytechnique, spring 2007

Guests

Research domain

Hipercom project-team aims to design, evaluate and optimize the telecommunication algorithms. The aimed areas are protocols, new telecommunication standards and quality of service management in networks. The aimed activity fields are centered around the new networks and services supporting internet. Although we address the whole spectrum of telecommunication domain, practically the Hipercom project team is specialized in local area networking, local loops, in particular mobile ad hoc networking. However the thematic extends to the information theory and modelization of internet graph and traffics.

[13] A nice picture of Hipercom team members (as provided by their team leader)

Goals

The goals of HIPERCOM are :

- Evaluation of performance and limits of massive mobile dense wireless networks
- Standardisation of OLSR protocol, design of related new services and protocols
- Design of wireless and wired backbone convergence

Results

Massive mobile dense wireless networks

Scaling and spatial capacity in non uniform wireless networks We found a more precise instance of Gupta- Kumar result by using a simple but realistic network model based on slotted ALOHA with Poisson traffic. It turns out that when the traffic density increases then the average node neighborhood area shrinks so that the average encircled traffic load remains constant with an analytical expression..

In their original model Gupta and Kumar assume that the traffic density is constant, which is far from realistic. However we have derived similar generalized results when the traffic density is not uniform. In this case, the heavier is the local traffic, the smaller are the local neighborhood and the larger is the number of hops needed to cross the congested region. Therefore the shortest paths (in hop number as computed by OLSR) will have a natural tendancy to avoid congested areas. The path tend to follow trajectory that have analogy in non linear optic with variable indices.

Overhead reduction in large networks The first limitation of multihop wireless network is the size of the overhead per node that increases linearly with the size of the network. This is a huge improvement compared to classic internet protocols which have quadratic overhead increases. Nevertheless this still limits the network size to some thousands. We have analyzed the performance of OLSR with Fisheye feature that significantly reduce the overhead with respect to distance. In theory the overhead reduction allows to network size of several order of magnitude. Anyhow the tuning of the overhead attenuation with distance must be carefully done when the network is mobile, in order to avoid tracking failure. We showed that an overhead reduction within square root of the network size achieve this goal.

An alternative way to overhead reduction is ad hoc hierarchical routing and Distributed Hashing Table. Work has just begun in this area.

Intermittent and delay tolerant networks We consider the problem of routing in these networks, with the sole assumption that the speed of the node mobility is less than the speed of transmitting a packet to a neighbour. We compare this problem with sound propagation in liquid. We show that various pattern of mobility and network clustering can be described by a single parameter such as the information speed propagation.

We introduce new algorithms that route a packet toward a remote destination. The different algorithms vary depending on the buffering and the capacity capabilities of the network (i.e. if one or more copies of a packet can be sent and/or be kept). All algorithms are based on link aging rumors across connected components. The packet bounces from connected components to connected components, thanks to node mobility. We establish several analytical properties using an analogy with the sound propagation in liquid where molecules creates temporary connected components where sounds travel very fast.

New services and protocols

Optimized Link State Routing (OLSR) The routing protocol OLSR is universally known in the mobile wireless community (more than 475,000 hits on Google). It has numerous implementations and is used in many wireless networks. It is a proactive protocol with full internet legacy which is based on partial topology information exchange, that non the less provide optimal path with additive metrics (such as BGP/OSPF). It is an experimental RFC within IETF and soon will become a full standard under the name OLSRv2.

Routing based on packet delay distribution in multihop ad hoc network Since propagation delays between routers are negligible, most delays occur in queueing and medium access control processing.

Contrary to previous common belief there is no need of network synchronization. The objective is to proactively determine the delay in absence of packet data traffic. The estimate of delay distribution is done via analytical method. In order to keep control on quality of service flows we use source routing forwarding options.

Multicast services in mobile ad hoc networks We have designed the Multicast extension for the Optimized Link State Routing protocol (MOLSR). MOLSR is in charge of building a multicast structure in order to route multicast traffic in an ad-hoc network. MOLSR is based on natural radio broadcast. This multicast protocol has also been implemented on the MANET/OLSR demonstrator of CELAR (MoD). A new version of the multicast protocol called MOST uses unicast traffic.

We have derived a theoretical upper bound of the multicast capacity in wireless network. This result is an extension of Gupta and Kumar result about unicast capacity in wireless network. It is shown that the multicast delivery allows an increase of capacity of the order of the square root of the size of the multicast group compared to the attainable capacity if only parallel unicast connections were used. We have also shown that the protocol MOST actually attains this upper bound.

Network coding We have just started the work in this area. We have proven optimality of network coding in 1D and 2D dense network and have designed a practical protocol, DRAGONCAST, that fits these properties.

Autoconfiguration Thomas Clausen is co-chair of the IETF working group *Autoconfiguration in MANET*.

A preconditioning for all routing protocols, OLSR included, is that each node is identifiable through an unique identifier We have developed, and published, a simple auto-configuration mechanism for OLSR networks, aiming a solving the simple but common problem of one or more nodes emerging in an existing network. Our solution is simple, allowing nodes to acquire an address in two steps : first, acquiring a locally unique address from a neighbor node. Then, with that locally unique address and using the neighbor from which the address was acquired as proxy, obtaining a globally unique address.

0.1 Integration wireless and backbone

Optimized Database exchange and check The problem of unreliable broadcast and less frequent update is that a missing routing information information can lead to lasting problems (loops, disconnections). We have specified an integrity check of distributed databases. We have replaced the heavy check done in wired world that exchanges database headers line by line by a collective check based on signature broadcast and exchange. That way the routing database are synchronized more quickly and discrepant part identified with a logarithmic cost instead of a cost linear to the database size.

OSPF-MPR The INRIA proposal is based on OLSR, in particular the optimization feature called MultiPoint Relay. The overhead reduction is similarly based on flooding reduction, and topology reduction. In particular OSPF-MPR supports optimized routing based on general additive metrics as in OSPF and adapt its topology reduction to those metrics. Compared to OLSR, OSPF-MPR has a feature called adjacency reduction inherited from OSPF, using broadcasted acknowledgement that enhances routing database synchronization. This feature is also optimized with MPR.

Gateway OSPF/OLSR The MANET extension protocols being largely experimental, we have developped a software that enable a gateway between OSPF and OLSR and allows the convergence of both protocols on existing software. This software has been implemented on the MANET/OLSR demonstrator of CELAR (MoD).

Software, pattents and contracts

Software

- OLSR : wireless routing protocol, several versions, including QoS ;
- MOLSR : multicast wireless routing protocol building a tree-structure ;

- SMOLSR : optimized network flooding ;
- MOST : multicast wireless routing protocol based on an overlay network ;
- OSPF-MPR ;
- SOLSR

Most software are downloadable from http ://hipercom.inria.fr/olsr/.

Pattents

Contracts

- MOBISIC ; from October 2007 ; Pole de compétitivité SYSTEMATIC ; Design and experiment a modular system (Plug & Play), scalable adapted to events securing and local crisis management

- SARAH : from February 2007 ; RNRT ; Service Avances pour Reseaux Ad Hoc : to study, develop and experiment an architecture of hybrid ad hoc network for the deployment of advanced multimedia systems, relying on information about the localized discovery of the environment.
- HITACHI : from April 2006 to June 2006 ; Optimized link state routing for mobile ad hoc networks.

Teaching, dissemination and service

Thomas Clausen teaches
- Foundation of programing languages at ecole polytechnique
- Modex networking at ecole polytechnique

Philippe Jacquet teaches :
- mobile ad hoc networks in the MPRI Master (Paris) ;
- foundation of computer science at the Ecole Polytechnique,
- security in mobile and wireless networks at the EPITA school,
- telecommunication in the MISIC master at the Ecole Polytechnique.

Visibility

National scientific cooperations

- INRIA-Rocquencourt, Hipercom project
- Paris 11, LRI

International scientific cooperations

- University Macquarie, Australia
- Keio University, Japan
- Niigata University, Japan
- Hitachi SDL, Japan
- Berlin Freie Universität, Germany

Seminar invitations

Conference organisation

- Thomas Clausen has organized the first, second and third OLSR interop ;
- Philippe Jacquet has organized the Analysis of Algorithms conference 2007

Program committees

-
- Philippe Jacquet serves as program committee member for AINTEC, Mathinfo, ISCIS, AofA and ISIT.

Journal editorial boards

- Philippe Jacquet belongs to the editorial board of DMTCS ;

Awards

- Prix Science et Défense granted to Philippe Jacquet (with Paul Muhlethaler) in 2004,
- Prix de Thèse École Polytechnique granted to Emmanuel Baccelli in 2007.

References

Books and chapters in books

2006

[1] CHO, K., AND JACQUET, P. Technologies for advanced heterogeneous networks. *First Asian Internet Engineering Conference* (2006).

International journals

2004

[2] ADJIH, C., BACCELLI, E., CLAUSEN, T., JACQUET, P., AND RODOLAKIS, R. Fish eye olsr scaling properties. *JCN* (2004).

[3] ALLARD, G., GEORGIADIS, L., JACQUET, P., AND MANS, B. Bandwidth reservation in multihop wireless networks : Complexity, heuristics and mechanisms. *International Journal of Wireless and Mobile Computing* (2004).

[4] BADIS, H., AND AGHA, K. A. Qolsr, qos routing for ad hoc wireless networks using olsr. *European Transactions on Telecommunications* (2004).

[5] CLAUSEN, T., JACQUET, P., AND VIENNOT, L. Analyzing control traffic overhead versus mobility and data traffic activity in mobile ad-hoc network protocols. *ACM Wireless Networks journal (Winet)* (2004).

[6] JACQUET, P., AND SZPANKOWSKI, W. Markov types and minimax redundancy for markov sources. *IEEE Transactions on IT* (2004).

[7] JACQUET, P., SZPANKOWSKI, W., AND VEY, B. M. Compact suffix trees resemble patricia tries : Limiting distribution of the depth. *JIRSS* (2004).

[8] PLESSE, T., ADJIH, C., MINET, P., LAOUITI, A., PLAKOO, A., BADEL, M., MUHLETHALER, P., JACQUET, P., AND LECOMTE, J. Olsr performance measurement in a military mobile ad-hoc network. *Ad Hoc Networks Journal, special issue on Data communication and topology control in ad-hoc networks* (2004).

[9] PLESSE, T., LECOMTE, J., ADJIH, C., BADEL, M., JACQUET, P., LAOUITI, A., MINET, P., MUHLETHALER, P., AND PLAKOO, A. A testbed for olsr in military ad-hoc networks. *Revue Scientifique et Technique de la Défense* (2004).

2005

[10] ADJIH, C., JACQUET, P., AND VIENNOT, L. Computing connected dominated sets with multipoint relays. *Ad Hoc& Sensor Wireless Networks* (2005).

2006

[11] ADJIH, C., GEORGIADIS, L., JACQUET, P., AND SZPANKOWSKI, W. Multicast tree structure and the power law - information theory. *IEEE Transactions on Information Theory* (2006).

[12] RODOLAKIS, G., SIACHALOU, S., AND GEORGIADIS, L. Replicated server placement with qos constraints. *IEEE Transactions on Parallel and Distributed Systems* (2006).

2007

[13] JACQUET, P., MERAIHI-NAIMI, A., AND RODOLAKIS, G. Asymptotic delay analysis for cross-layer delay-based routing in ad hoc networks. *Hindawi Publishing Corporation : Advances in Multimedia* (2007).

[14] JACQUET, P., SEROUSSI, G., AND SZPANKOWSKI, W. On the entropy of a hidden markov process. *TCS* (2007).

International conferences with proceedings

2004

[15] AHRENHOLZ, J., BACCELLI, E., CLAUSEN, T., HENDERSON, T., JACQUET, P., AND SPAGNOLO, P. Ospfv2 wireless interface type. In *IETF Internet Draft* (2004).

[16] BACCELLI, E., CLAUSEN, T., AND JACQUET, P. Ad-hoc and internet convergence : Adapting ospf-style database exchanges for ad-hoc networks. In *Hetnet* (2004).

[17] BACCELLI, E., CLAUSEN, T., AND JACQUET, P. Database exchange and reliable synchronization in mobile ad hoc networks. In *Conference on Wireless Networks and Emerging technologies* (2004).

[18] BACCELLI, E., CLAUSEN, T., AND JACQUET, P. Db exchange for ospfv2 wireless interface type. In *IETF Internet Draft* (2004).

[19] BACCELLI, E., CLAUSEN, T., AND JACQUET, P. Ospf-style database exchange and reliable synchronization in the optimized link-state routing protocol. In *SECON 2004* (2004).

[20] BACCELLI, E., CLAUSEN, T., AND WAKIKAWA, R. Nemo route optimisation problem statement. In *IETF Internet Draft* (2004).

[21] BACCELLI, E., AND JACQUET, P. Diffusion mechanisms for multimedia broadcasting in mobile ad hoc networks. In *IASTED IMSA* (2004).

[22] CLAUSEN, T., AND MASE, K. Link buffering for manets. In *IETF Internet Draft* (2004).

[23] CLAUSEN, T., MINET, P., AND PERKINS, C. Multipoint relay flooding for manets. In *IETF Internet Draft* (2004).

[24] CLAUSEN, T., STUPAR, P., AND RUFFINO, S. Autoconfiguration in a manet : connectivity scenarios and technical issues. In *IETF Internet Draft* (2004).

[25] CLAUSEN, T., STUPAR, P., AND RUFFINO, S. Autoconfiguration in a manet : connectivity scenarios and technical issues. In *IETF Internet Draft* (2004).

[26] JACQUET, P. Space-time information propagation in mobile ad hoc wireless networks. In *ITW* (2004).

[27] JACQUET, P., SEROUSSI, G., AND SZPANKOWSKI, W. On the entropy of a hidden markov process. In *DCC* (2004).

[28] RAFFO, D., ADJIH, C., CLAUSEN, T., AND MUHLETHALER, P. An advanced signature system for olsr. In *SASN* (2004).

[29] RAFFO, D., ADJIH, C., CLAUSEN, T., AND MUHLETHALER, P. Olsr with gps information. In *IC* (2004).

2005

[30] ADJIH, C., BOUDJIT, S., JACQUET, P., LAOUITI, A., MUHLETHALER, P., AND MASE, K. Address autoconfiguration in optimized link state routing protocol. In *IETF Internet Draft* (2005).

[31] ADJIH, C., MINET, P., PLESSE, T., LAOUITI, A., PLAKOO, A., MUHLETHALER, P., JACQUET, P., AND LECOMTE, J. Experiments with olsr routing in a manet. In *Information Systems Technology NATO Symposium* (2005).

[32] ALLARD, G., JACQUET, P., AND MANS, B. Routing in extremely mobile networks. In *IFIP MedHocNet* (2005).

[33] BACCELLI, E. Olsr trees : A simple clustering mechanism for olsr. In *IFIP MED-HOC-NET* (2005).

[34] BACCELLI, E., AND CLAUSEN, T. A simple address autoconfiguration mechanism for olsr. In *IEEE International Symposium on Circuits and Systems (ISCAS)* (2005).

[35] BACCELLI, E., CLAUSEN, T., AND GARNIER, J. Duplicate address detection in olsr networks. In *IEEE Conference on Wireless Personal Multimedia Communications (WPMC)* (2005).

[36] BACCELLI, E., CLAUSEN, T., AND WAKIKAWA, R. Route optimization in nested mobile networks (nemo) using olsr. In *International Conference on Networks and Communication Systems (NCS)* (2005).

[37] BOURAOUI, L., JACQUET, P., LAOUITI, A., AND VIENNOT, L. Ad hoc communications between intelligent vehicles. In *ITST* (2005).

[38] CHO, S.-Y., AND ADJIH, C. Optimized multicast based on multipoint relaying. In *WICON* (2005).

[39] CLAUSEN, T. Jitter considerations in manets. In *IETF Internet Draft* (2005).

[40] CLAUSEN, T. Olsrv2 link hysteresis. In *IETF Internet Draft* (2005).

[41] CLAUSEN, T., AND AL. Generalized olsrv2 packet/message format. In *IETF Internet Draft* (2005).

[42] CLAUSEN, T., AND AL. Olsr passive duplicate address detection. In *IETF Internet Draft* (2005).

[43] CLAUSEN, T., AND JACQUET, P. The optimized link-state routing protocol version 2. In *IETF Internet Draft* (2005).

[44] E. BACCELLI, T. C. Securing olsr problem statement. In *IETF Internet Draft* (2005).

[45] JACQUET, P. Information in extremely mobile networks. In *PanHellenic conference* (2005).

[46] JACQUET, P., NAIMI, A., AND RODOLAKIS, G. Performance of binary exponential backoff csma in wifi and optimal routing in mobile ad hoc networks. In *AOFA* (2005).

[47] JACQUET, P., NAIMI, A., AND RODOLAKIS, G. Routing on asymptotic delays in ieee 802.11 wireless ad hoc networks. In *RAWNET* (2005).

[48] JACQUET, P., AND RODOLAKIS, G. Analytical evaluation of autocorrelations in tcp traffic. In *AINTEC* (2005).

[49] JACQUET, P., AND RODOLAKIS, G. Multicast scaling properties in massively dense ad hoc networks. In *Parallel and Distributed Systems* (2005).

[50] RAFFO, D., ADJIH, C., CLAUSEN, T., AND MUHLETHALER, P. Securing olsr using node locations. In *EW* (2005).

[51] RODOLAKIS, G., SIACHALOU, S., AND GEORGIADIS, L. Replicated server placement with qos constraints. In *QoS IP* (2005).

2006

[52] BACCELLI, E. Olsr scaling with hierarchical routing and dynamic tree clustering. In *International Conference on Networks and Communication Systems (NCS)* (2006).

[53] BACCELLI, E., CLAUSEN, T., AND JACQUET, P. Ospf mpr extension for ad hoc networks. In *IETF Internet Draft* (2006).

[54] BADIS, H., AND AGHA, K. A. Ceqmm : A complete and efficient quality of service model for manets. In *ACM PE-WASUN* (2006).

[55] BADIS, H., AND AGHA, K. A. Ceqmm : A complete and efficient quality of service model for manets. In *IETF Internet Draft* (2006).

[56] BADIS, H., AND AGHA, K. A. Quality of service the for ad hoc optimized link state routing protocol (qolsr). In *IETF Internet Draft* (2006).

[57] CLAUSEN, T., AND AL. Neighborhood discovery for olsrv2. In *IETF Internet Draft* (2006).

[58] JACQUET, P. Common nodes between two random suffix trees. In *Summer school in probabilistic methods in combinatorics* (2006).

[59] JACQUET, P. Common words between two random strings. In *AofA* (2006).

[60] JACQUET, P. Control of mobile ad hoc networks. In *ITW* (2006).

[61] JACQUET, P., AND SZPANKOWSKI, W. On (d,k) sequences not containing a given word. In *International Symposium on Information Theory* (2006).

2007

[62] ADJIH, C., BACCELLI, E., MINET, P., MUHLETHALER, P., AND PLESSE, T. Qos support, security and ospf interconnection in a manet using olsr. In *Military Communications and Information Systems (MCC)* (2007).

[63] BACCELLI, E., CLAUSEN, T., JACQUET, P., AND NGUYEN, D. Integrating vanets in the internet core with ospf : the mpr-ospf approach. In *International Conference on ITS Telecommunications (ITST)* (2007).

[64] BACCELLI, E., MASE, K., RUFFINO, S., AND SINGH, S. Address autoconfiguration for manet : Terminology and problem statement. In *IETF Internet Draft* (2007).

[65] CHO, S.-Y., ADJIH, C., AND JACQUET, P. An association discovery protocol for hybrid wireless mesh networks. In *Med hoc Net* (2007).

[66] CHO, S.-Y., ADJIH, C., AND JACQUET, P. Heuristics for network coding in wireless networks. In *International Wireless Internet Conference* (2007).

[67] CHO, S.-Y., ADJIH, C., AND JACQUET, P. Near optimal broadcast with network coding in large sensor networks. In *International Workshop on Information Theory for Sensor Networks* (2007).

[68] CHO, S.-Y., ADJIH, C., AND JACQUET, P. Rate selection heuristics for network coding in wireless networks. In *Sigcomm* (2007).

[69] JACQUET, P. Common words in two random strings. In *ISIT* (2007).

[70] JACQUET, P., AND MANS, B. Routing in intermittently connected networks : Age rumors in connected components. In *PERCOM* (2007).

[71] JACQUET, P., SEROUSSI, G., AND SZPANKOWSKI, W. Noisy constrained capacity. In *ISIT* (2007).

[72] T.CLAUSEN, AND DEARLOVE, C. Nemo route optimisation problem statement. In *IETF Internet Draft* (2007).

[73] T.CLAUSEN, AND DEARLOVE, C. Representing multi-value time in manets. In *IETF Internet Draft* (2007).

[74] T.CLAUSEN, DEARLOVE, C., AND DEAN, J. Manet neighborhood discovery protocol (nhdp). In *IETF Internet Draft* (2007).

[75] T.CLAUSEN, MACKER, J., AND CHAKERES, I. Mobile ad hoc network architecture. In *IETF Internet Draft* (2007).

Dissemination

2006

[76] BACCELLI, E. Algorithmes pour les reseaux ad hoc. *Interstices)i(Journal* (2006).

PhD Thesis

2006

[77] BACCELLI, E. *Routing and Mobility in Large Heterogeneous Packet Networks*. PhD thesis, École polytechnique, 2006.

[78] RODOLAKIS, G. *Analytical Models and Performance Evaluation in Massive Mobile Ad hoc Networks*. PhD thesis, École polytechnique, 2006.

Miscellaneous

2007

[79] BACCELLI, E., ZAHN, T., AND SCHILLER, J. Dht-olsr. In *INRIA Research Report, RR-6194* (2007).

[80] CLAUSEN, T. A manet architectural model. In *INRIA Research Report, RR-6145* (2007).

[81] JACQUET, P. Rights and wrongs about wireless network centralized or meshed schemes performance. In *INRIA Research Report, RR-6121* (2007).

[82] JACQUET, P. Theoretical results on flooding performance in mobile ad hoc networks. In *INRIA Research Report, RR-6122* (2007).

[83] VIENNOT, L., AND JACQUET, P. Biconnectivity, k-connectivity and multipoint relays. In *INRIA Research Report, RR-6169* (2007).

External references

[84] ADJIH, C., CLAUSEN, T., JACQUET, P., LAOUITI, A., MINET, P., MUHLETHALER, P., QAYYUM, A., AND VIENNOT, L. Optimized link state routing (olsr), rfc3626. In *IETF Request For Comment* (2003).

Comète
Concurrence, Mobilité et Transactions

Team members

Team leader

Catuscia Palamidessi, DR INRIA

Permanent members

- Frank D. Valencia, CR CNRS
- Bernadette Charron-Bost, CR CNRS

Phds

- Konstantinos Chatzikokolakis, bourse BDX, since October 1st, 2004 till October 26th, 2007
- Antoine Gaillard, grant Caspar Monge, since October 1st, 2005
- Romain Beauxis, bourse Region Ile de France, since December 1st, 2005
- Carlos Olarte, bourse INRIA/CORDIS, since October 1st, 2006
- Sylvain Pradalier, bourse ENS Cachan, since May 1st, 2006. Co-supervised by Cosimo Laneve, University of Bologna, Italy
- Jesus Aranda, funded by CROUS and by the University Javeriana, Cali, Colombia. Since Oct 1st, 2006. Co-supervised by Juan Francisco Diaz, Universidad del Valle, Colombia
- Christelle Braun, bourse BDX, since October 1st, 2007

Postdocs

- Tom Chothia, from September 1st, 2004, till December 31st, 2005
- Jun Pang, from August 1st, 2004, till October 1st, 2005
- Peng Wu, from September 1st, 2005, till September 30th, 2007
- Angelo Troina, since September 1st, 2006
- Josef Widder, since May 1st, 2007
- Jean Krivine, since March 1st, 2007

Interns

- Mohit Bhargava, from IIT Delhi, India. From May 1st, 2004 till July 31st, 2004
- Jean-Baptiste Bianquis, from ENS Ulm. From April 1st, 2004 till September 30th, 2004
- Kostas Chatzikokolakis, from DEA Programmation. From April 1st, 2004 till September 30th, 2004
- Axelle Ziegler, from ENS Ulm. From April 1st, 2004 till September 30th, 2004
- Andres Aristizabal, from Universidad Javeriana Cali. From May 1st, 2005 till July 31st, 2005
- Adrian Balan, from the Ecole Polytechnique. From November 1st, 2004 till march 31st, 2005
- Romain Beauxis, from Master informatique Orsay. From April 1st, 2005 till November 30th, 2005
- Sylvain Pradalier, from ENS Cachan. From April 1st, 2005 till September 1st, 2005
- Oleksii Maniatchenko, from Univ. de Versailles. From June 1st, 2005 till September 1st, 2005
- Purnima Gupta, from IIT, New Delhi. From may 1st, 2006 till July 31st, 2006

Guests

- Robin Milner, Professor at the University of Cambridge, UK. Chair Blaise Pascal from October 1st, 2007, till September 30th, 2007
- Moreno Falaschi, Professor at the University of Siena, Italy. Ecole Polytechnique invited researcher, from June 1st, 2006, till July 31st, 2006, and INRIA invited reseacher from October 15th, 2007 till January 15th, 2008
- Mila Majster-Cederbaum, Professor at the University of Mannheim. From May 1st, 2005 till July 31st, 2005
- Cosimo laneve, Professor at the University of Bologna, Italy. Ecole Polytechnique invited researcher. From may 15th, 2007 till July 15th, 2007
- Nino Salibra, Professor at the University of Venice, Italy. Ecole Polytechnique invited researcher. From October 15th, 2007 till December 15th, 2007
- André Schiper, Professor at EPFL, invited researcher from October 1st, 2004 till August 31st, 2005
- Jennifer Welch, Professor at A&T University, invited researcher from May 1st, 2005 till June 30th, 2005
- Josef Widder, Associate Professor at VUT, DGA invited researcher from May 1st, 2007 till April 31st, 2008
- Diletta Romana Cacciagrano, Assistant Professor at the University of Camerino, Italy. From November 1st, 2006, till November 30th, 2006
- Elaine Pimentel, Associate Professor at the University of Belo Orizonte, Brazil. From November 20th till December 20th, 2005
- Maria Grazia Vigliotti, PostDoc at Imperial College, UK. From February 1st, 2005, till April 30th, 2005
- Cinzia Di Giusto, PhD student at the University of Bologna, Italy. From March 1st, 2006, till September 30th, 2006
- Troels C. Damgaard, Ph.D. Student at the IT University of Copenhagen. From August 15th, 2007, till February 15th, 2008
- Andrea Turrini, PhD student at the University of Verona, Italy. From September 15th, 2007, till December 15th, 2007

Research domain

Our times are characterized by the massive presence of highly distributed and mobile systems consisting of diverse and specialized devices, forming heterogeneous networks, and providing different services and applications. The resulting computational systems are usually referred to as *Ubiquitous Computing*, (see, e.g., the UK Grand Challenge initiative under the name *Sciences for Global Ubiquitous Computing* [71]).

The genesis and subsequent development of these systems comprised a complex series of impressive engineering efforts, but the results does not always exhibit a satisfactory level of robustness, reliability, security and integration. The key to these shortcomings lies in the lack of underlying principles and science behind the engineering activities in this domain. This situation contrasts sharply with other fields of engineering, where impressive mathematical and physical modeling tools are scrupulously used.

What kind of science would be suitable for Ubiquitous Computing ? We envisage it in two principal

modes : *modeling* and *design*. Modeling is the bedrock upon which most sciences are founded : we understand actual systems by constructing models which provide predictive behavioral analyses. In our case, models will range from abstract mathematical structures representing distributed networks and protocols to more concrete syntactic models of specification and programming formalisms.

Design is the transition process from models to applications : as in all experimental sciences, we need feedback from the applications to validate the models, improve their usability, and increase our confidence in the objects we build through them. Notably, in computer science the feedback from applications is rarely as concrete and immediate as in the physical sciences, where a measurement is sufficient to disprove a theory. That is the reason why we envisage the development of a science for Ubiquitous Computing to be an inextricable mix of modeling and design.

The contribution of Comète to the development of a science for Ubiquitous Computing focuses on the following topics :

- The study of models and formalisms for concurrency from the point of view of their expressive power : Development of criteria to assess the expressive power of a model or formalism in a distributed setting, comparison between existing models and formalisms, and definition of new ones according to an intended level of expressiveness. It is to be remarked that there is often a trade off between expressivity and (efficient) implementability ; in our study we pay particular attention to this latter aspect as well.
- The study of fault-tolerant systems for mobile networks, as well for message-passing systems as for shared-memory systems. Handling such complex environments is an imperative requirement for numerous distributed applications.
- The probabilistic aspects of systems and protocols. The need for copying with probabilities can arise for various reasons : First, algorithms for distributed computing and security protocols sometimes use randomization. Second, the modeling of the physical world often requires to cope with uncertain and approximate information, which one can refine by statistical measurements, and which can then be naturally represented using a probabilistic formalism. (An example of this situation is the number of the requests that are received by a web server during various times of the day.) Third, reality can sometimes be to complicated to be represented and analyzed in detail ; probabilistic and stochastic models offer then a convenient abstraction mechanism.
- Specification and verification of mobile distributed systems, in particular security protocols. Typically specification and verification consists of developing formalisms and reasoning techniques (and tools to support these) to specify systems and properties and to guarantee that the intended properties are indeed satisfied. In our particular case, the challenges are (a) to find suitably expressive formalisms which capture essential new features such as mobility, presence of uncertain information, and potentially hostile environment, (b) to build suitably representative models in which to interpret these formalisms, and (c) to design efficient tools to perform the verification in presence of these new features.
- One formalism in which we are particularly focusing our efforts is the probabilistic asynchronous π-calculus, a probabilistic variant of the asynchronous π-calculus, that is a formalism designed for mobile and distributed computation [68, 66, 67]. A characteristic of our calculus is the presence of both probabilistic and nondeterministic aspects. This combination is essential to represent probabilistic algorithms and protocols and express their properties in presence of unpredictable (nondeterministic) users and adversaries.

Goals

The main objectives of Comète are the following :

1. Investigation of models and formalisms for concurrency from the point of view of their expressive power.
2. Investigation of new computational models for fault-tolerant distributed systems.
3. Formalization of probabilistic aspects of systems and protocols.
4. Specification and verification of security protocols.

Results

Investigation of models and formalisms for concurrency from the point of view of their expressive power

Infinite Behavior and Name Scoping in Process Calculi In literature there are several process calculi differing in the constructs for the specification of infinite behavior and in the scoping rules for channel names. In [19] we have studied various representatives of these calculi based upon both their relative expressiveness and the decidability of divergence. We regard any two calculi as being equally expressive if and only if for every process in each calculus, there exists a weakly bisimilar process in the other. By providing weak bisimilarity preserving mappings among the various variants, we showed that in the context of relabeling-free and finite summation calculi : (1) CCS with parameterless (or constant) definitions is equally expressive to the variant with parametric definitions. (2) The CCS variant with replication is equally expressive to that with recursive expressions and static scoping. From (1) and the well-known fact that parametric definitions can replace injective relabellings, we showed that injective relabellings are redundant in CCS.

In [59, 26] we have surveyed various definitions of scope and infinite behavior proposed in literature, and we have pointed out their impact in the expressive power of concurrent formalisms.

More recently in [40] we proved that the CCS variant with replication mentioned above can faithfully (deterministically) encode regular languages but not context-free ones. We also proved that the languages generated by the processes of this variant are context-sensitive.

Synchronous vs Asynchronous Communication One of the early results about the asynchronous π-calculus which significantly contributed to its popularity is the capability of encoding the output prefix of the (choiceless) π-calculus in a natural and elegant way. Encodings of this kind were proposed by Honda and Tokoro, by Boudol, and by Nestmann. In [27, 11], we have investigated whether the above encodings preserve De Nicola and Hennessy's testing semantics. It turns out that, under some general conditions, no encoding of output prefix is able to preserve the must testing. This negative result is due to (a) the non atomicity of the sequences of steps which are necessary in the asynchronous π-calculus to mimic synchronous communication, and (b) testing semantics's sensitivity to divergence.

Linearity vs Persistence In [36] and more recently in [43] we have compared the expressive power of linear and persistent communication in the context of weak bisimilarity. We have consider four fragments of the π-calculus, corresponding to combinations of linearity/persistence also present in other frameworks such as Concurrent Constraint Programming and several calculi for security. The study is presented by providing (or proving the non-existence of) encodings among the fragments, a processes-as-formulae interpretation and a reduction from Minsky machines.

Distributed Agreement In [25] we have systematized a collection of results on the expressiveness of process calculi obtained by the means of impossibility results in the field of distributed computing. In particular, we have focused on the *symmetric leader election problem* which allows to classify languages based on their capability of achieving a distributed agreement.

Fairness In [44] we have defined fair computations in the π-calculus. We have followed Costa and Stirling's approach for CCS-like languages but exploited a more natural labeling method of process actions to filter out unfair process executions. The new labeling allowed us to prove all the significant properties of the original one, such as unicity, persistence and disappearance of labels. It also turned out that the labeled π-calculus is a conservative extension of the standard one. We contrasted the existing fair testing notions with those that naturally arise by imposing weak and strong fairness. This comparison provides the expressiveness of the various fair testing-based semantics and emphasizes the discriminating power of the one already proposed in the literature.

Decidability results for Linear Temporal Logic In [8] we have established new positive decidability results for timed ccp as well as for LTL. In particular, we have proved that the following problems are decidable : (1) The strongest postcondition equivalence for the so-called locally-independent ntcc fragment ; unlike other fragments for which similar results have

been published, this fragment can specify infinite-state systems. (2) Verification for locally-independent processes and negation-free first-order formulas of the ntcc LTL. (3) Implication for such formulas. (4) Satisfiability for a first-order fragment of Manna and Pnueli' LTL. The purpose of the last result is to illustrate the applicability of ccp to well-established formalisms for concurrency.

Furthermore, recently in [64] we proved that the negation restriction in (4) is necessary for decidability : I.e., satisfiability is undecidable for the first-order fragment of Manna and Pnueli' LTL with flexible variables.

Comparison of the concurrent constraint paradigm and the pi-calculus paradigm. In [8] we showed that timed ccp cannot encode Turing Machines. In [65] we introduced an extension of timed ccp and show it can encode Turing Machines due to its ability to express mobility in the sense of the π-calculus (i.e., communication of private links). Furthermore, we showed the extension admits processes-as-formulae temporal logic interpretation.

Investigation of new computational models for fault-tolerant distributed systems

Uniform Consensus is harder than Consensus In [4] we compared the consensus and uniform consensus problems in synchronous systems. In contrast to consensus, uniform consensus is not solvable with byzantine failures. This still holds for the omission failure model if a majority of processes may be faulty. For the crash failure model, both consensus and uniform consensus are solvable, no matter how many processes are faulty. In this failure model, we examined the number of rounds required to reach a decision in the consensus and uniform consensus algorithms. We showed that if uniform agreement is required, one additional round is needed to decide, and so uniform consensus is also harder than consensus for crash failures. This is based on a new lower bound result for the synchronous model that we state for the uniform consensus problem. Finally, we presented an algorithm that achieves this lower bound.

Validity Conditions in Agreement Problems and Time Complexity In [18] we studied the time complexity of different distributed agreement problems in the synchronous model with crash failures, by varying their validity condition. We first introduced a continuous class of agreement problems, the *k-TAg problems*, which includes both *Consensus* and *Non-Blocking Atomic Commitment*. We then exhibited a general early-deciding algorithm, that we instantiate to solve every problem in this class. In all cases, the algorithm achieves the previously established lower bounds for time complexity showing that these lower bounds are tight.

Reductions in Distributed Computing In [57, 58] we introduced several notions of reduction in distributed computing, and investigate reduction properties of two fundamental agreement tasks, namely Consensus and Atomic Commitment.

We first proposed the notion of reduction "*à la* Karp", an analog for distributed computing of the classical Karp reduction. We then defined a weaker reduction which is the analog of Cook reduction. These two reductions are called K- reduction and C-reduction, respectively. We also introduced the notion of C^*-reduction which has no counterpart in classical (namely, non distributed) systems, and which naturally arises when dealing with symmetric tasks.

We established various reducibility and irreducibility theorems with respect to these three reductions. Our main result is an incomparability statement for Consensus and Atomic Commitment tasks : we showed that they are incomparable with respect to the C-reduction, except when the resiliency degree is 1, in which case Atomic Commitment is strictly harder than Consensus. A side consequence of these results is that our notion of C-reduction is strictly weaker than the one of K-reduction, even for unsolvable tasks.

In a second part, we extended the results of Part I by considering a new class of agreement tasks, the so-called k-Threshold Agreement tasks (previously introduced by Charron-Bost and Le Fessant). These tasks naturally interpolate between Atomic Commitment and Consensus. Moreover, they constitute a valuable tool to derive irreducibility results between Consensus tasks only. In particular, they allow us to show that (A) for a fixed set of processes, the higher the resiliency degree is, the harder the Consensus task is, and (B) for a fixed resiliency degree, the smaller the set of processes is, the harder the Consensus task is.

The proofs of these results led us to consider new oracle-based reductions, involving a weaker variant of the C-reduction introduced in Part I. We also discussed the relationship between our results and previous ones relating f-resiliency and wait-freedom.

The Heard-Of Model : Computing in Distributed Systems with benign failures Problems in fault-tolerant distributed computing have been studied in a variety of models. These models are structured around two central ideas :

1. Degree of synchrony and failure model are two *independent* parameters that determine a particular type of system.
2. The notion of *faulty component* is helpful and even necessary for the analysis of distributed computations when failures occur.

In [12, 63], we questioned these two basic principles of fault-tolerant distributed computing, and showed that it is both possible and worthy to renounce them in the context of benign failures : we presented a computational model, suitable for systems with benign failures, which is based only on the notion of *transmission failure*.

In this model, computations evolve in rounds, and messages missed at a round are lost. Only information transmission is represented : for each round r and each process p, our model provides the set of processes that p "hears of" at round r (*heard-of set*) namely the processes from which p receives some message at round r. The features of a specific system are thus captured as a whole, just by a predicate over the collection of heard-of sets. We showed that our model handles benign failures, be they static or dynamic, permanent or transient, in a unified framework.

Using this new approach, we were able to give shorter and simpler proofs of important results (non-solvability, lower bounds). In particular, we proved that in general, Consensus cannot be solved without an implicit and permanent consensus on heard-of sets. We also examined Consensus algorithms in our model. In light of this specific agreement problem, we showed how our approach allows us to devise new interesting solutions.

Tolerating Corrupted Communication Consensus encapsulates the inherent problems of building fault tolerant distributed systems. The classic model of Byzantine faulty processes can be restated such that messages from a subset of processes can be arbitrarily corrupted (including addition and omission of messages).

In [41] we considered the case of dynamic and transient faults, that may affect all processes and that are not permanent. We modeled them via corrupted communication. For corrupted communication it is natural to distinguish between the safety of communication, which is concerned with the number of altered messages, and the liveness of communication, which restricts message loss.

We presented two algorithms that solve consensus, together with sufficient conditions on the system to ensure correctness. Our first algorithm needs strong conditions on safety but requires weak conditions on liveness in order to terminate. Our second algorithm tolerates a lower degree of communication safety at the price of stronger liveness conditions.

Our algorithms allow us to circumvent the resilience lower bounds from Santoro/Widmayer and Martin/Alvisi.

Formalization of probabilistic aspects of systems and protocols

The probabilistic asynchronous π-calculus In [7] we have proposed an extension of the π_a-calculus, to the purpose of using it as an intermediate language for the (randomized) implementation of the π-calculus. In order to be able to write a randomized encoding, we needed to enhance π_a with a construct for random draws. Furthermore, we wanted the implementation to be robust with respect to adverse conditions, namely "bad interleaving sequences". In other words we needed to express, in the execution model of the intermediate language, the nondeterministic (i.e. unpredictable) decisions of an external scheduler. Thus we needed two notions of choice : one probabilistic, associated to the random draws controlled by the process, and one nondeterministic, associated to the possible interleavings generated by the scheduler.

Our proposal, π_{pa} (probabilistic asynchronous π-calculus) is based on the model of probabilistic automata of Segala and Lynch, which has the above discussed characteristic of distinguishing between probabilistic and nondeterministic behavior.

Encoding π in π_{pa} Still in [7], we have defined a uniform, compositional encoding from π to π_{pa}. Our

encoding involves solving a resource allocation problem that can be regarded as a generalization of the dining philosophers problem, in the sense that there may be more philosophers than forks. The correctness of the encoding is proved with respect to a notion of testing semantics adapted to the probabilistic asynchronous pi-calculus. More precisely, we have shown that our encoding is correct with probability 1 with respect to any adversary.

Bisimulation semantics In [14] we have studied a process calculus which combines both nondeterministic and probabilistic behavior in the style of Segala and Lynch's probabilistic automata. We have considered various strong and weak behavioral equivalences, and we have provided complete axiomatizations for finite-state processes, restricted to guarded definitions in case of the weak equivalences. We conjecture that in the general case of unguarded recursion the "natural" weak equivalences are undecidable.

This has been the first work, to our knowledge, to provide a complete axiomatization for weak equivalences in the presence of recursion and both nondeterministic and probabilistic choice.

In [2] we have extended this investigation to the case of a process calculus with parallel composition.

Metrics In [32], we have studied metric semantic for a general framework that we call *Action-labeled Quantitative Transition Systems* (AQTS). This framework subsumes some other well-known quantitative systems such as probabilistic automata, reactive and generative models, and (a simplified version of) weighted automata.

The metric semantics that we have investigated in [32] is based on rather sophisticated techniques. In particular, we needed to resort to the notion of Hutchinson distance.

Still in [32], we have considered two extended examples which show that our results apply to both probabilistic and weighted automata as special cases of AQTS. In particular, we have shown that the operators of the corresponding process algebras are nonexpansive, which is the metric correspondent of the notion of congruence.

Probability and guards In [37] we have proposed a probabilistic extension of the π-calculus whose main novelty is a probabilistic *mixed choice* operator, that is, a choice construct with a probability distribution on the branches, and where input and output actions can both occur as guards. We have developed the operational semantics of this calculus, and we have investigated its expressiveness. In particular, we have compared it with the sublanguage with the two *separate choices*, where input and output guards are not allowed together in the same choice construct. Our main result is that the separate choices can encode the mixed one. Further, we have showed that *input-guarded* choice can encode *output-guarded* choice and vice versa.

Extending the language In order to obtain a language suitable for the specification and verification of a large class of security protocols, we aim at enriching the probabilistic π-calculus with value passing, encryption and decryption, other primitive functions, and data types, along the lines of the *applied π-calculus* [69]. Some preliminary work in this direction is represented by [50].

Model checking Model checking is the main tool that we aim at developing for the verification of security protocols.

In [55] we have introduced a weak symbolic bisimulation for the probabilistic π-calculus to overcome the infinite branching problem in checking ground bisimulations between probabilistic systems. The definition of weak symbolic bisimulation does not rely on the random capability of adversaries and suggests a solution to the open problem on the axiomatization for weak bisimulation in the case of unguarded recursion. Furthermore, we have presented an efficient characterization of symbolic bisimulations for the calculus, which allows the "on-the-fly" instantiation of bound names and dynamic construction of equivalence relations for quantitative evaluation. This has directly resulted in a local decision algorithm that can explore just a minimal portion of the state spaces of the probabilistic processes in question.

In [51], in collaboration with the PRISM team at Oxford, we have established the basis for an implementation of model checking for the probabilistic π-calculus. Building upon the (non-probabilistic) π-calculus model checker MMC [70], we have developed an automated procedure for constructing a Markov decision process representing a probabilistic π-calculus process. This representation can then be veri-

fied using existing probabilistic model checkers such as PRISM. Secondly, we have demonstrated how for a large class of systems an efficient, compositional approach can be applied, which uses our extension of MMC on each parallel component of the system and then translates the results into a higher-level model description for the PRISM tool.

Specification and verification of security protocols

A framework for analyzing probabilistic protocols In [22] and [6] we have developed a framework for analyzing probabilistic security protocols using a probabilistic extension of the π-calculus inspired by the work in [7]. In order to express security properties in this calculus, we have extended the notion of testing equivalence to the probabilistic setting. We have have applied these techniques to verify the Partial Secret Exchange, a protocol which uses a randomized primitive, the Oblivious Transfer, to achieve fairness of information exchange between two parties.

Probabilistic aspects of anonymity and privacy The protocols for ensuring anonymity and privacy often use random mechanisms which can be described probabilistically, while the agents' interest in performing the anonymous action may be totally unpredictable, irregular, and hence expressible only nondeterministically. In the past, formal definitions of the concepts of anonymity and privacy have been investigated either in a totally nondeterministic framework, or in a purely probabilistic one. We have proposed a notion which combines both probability and nondeterminism, and which is suitable for describing the most general situation in which both the systems and the user can have both probabilistic and nondeterministic behavior. We have also investigated the properties of the definition for the particular cases of purely nondeterministic users and purely probabilistic users.

We have investigated notions of strong anonymity in [21] and [35, 60]. One interesting feature of our approach is that in the purely probabilistic case, strong anonymity turns out to be independent from the probability distribution of the users. In [48, 29, 9] we have also investigated notions of weak anonymity. These are more realistic in the sense that they are more likely to be satisfied by the anonymity protocols used in practice.

Interplay between probability and nondeterminism It has been observed recently that in security the combination of nondeterminism and probability can be harmful, in the sense that the resolution of the nondeterminism can reveal the outcome of the probabilistic choices even though they are supposed to be secret [72]. This is known as the problem of the *information-leaking scheduler*. In [45] we have developed a linguistic (process-calculus) approach to this problem, and we have shown how to apply it to control the behavior of the scheduler in various anonymity examples.

Information-Theory applied to anonymity and privacy In [30, 13] we have proposed a framework in which anonymity protocols are interpreted as particular kinds of channels, and the degree of anonymity provided by the protocol as the converse of the channel's capacity. We have then illustrated how various notions of anonymity can be expressed in this framework, and showed the relation with some definitions of probabilistic anonymity in literature. Finally, we have discussed how to compute the channel matrix on the basis of the transition system associated to the protocol, and how to perform the computation automatically using a model-checker like PRISM.

In [46] we have investigated how the adversary can test the system to try to infer the user's identity, and we have studied how the probability of error depends on the characteristics of the channel. In particular we have considered the Bayes approach, and we have been able to characterize the associated probability of error (Bayes risk) in terms of the solution of certain systems of equations derived from the channel. This has allowed us to compute tight bounds for the Bayes risk, thus improving long-standing results in literature.

In [33], we have proposed a probabilistic process calculus to describe protocols for ensuring anonymity, and used the notion of relative entropy to measure the degree of anonymity that these protocols can guarantee. We have proved that the operators in the probabilistic process calculus are non-expansive, with respect to this measuring method. We have illustrated our approach by using the example of the Dining Cryptographers Problem.

Software, patents and contracts

Software

In collaborations with Dave Parker, Gethin Norman and Marta Kwiatkowska from the University of Oxford, we are developing a model checker for the probabilistic π-calculus based on MMC techniques. Case studies with several large examples, including Dining Cryptographers Protocol, Partial Secret Exchange Protocol and Mobile Communication Network, have shown the efficiency of the approach.

In the meanwhile we are also attempting a direct and more flexible approach to the development of a model checker for the probabilistic π-calculus, using OCaml. This should allow to extend the language more easily, to include cryptographic primitives and other features useful for the specification of security protocols. As the result of our preliminary steps in this direction we have developed a rudimentary model checker, available at the following URL : `http://vamp.gforge.inria.fr/`.

Contracts

- ASSERT. An European PI whose primary goal is to define a new system and software development process, and experiment on real industrial cases. It will replace the traditional approach, which is very empirical, with a more scientific method. ASSERT will define a continuous proof-based process to ensure the correctness of computer systems for aerospace applications. Period : from September 1, 2005 to April 1st 2006 ;
- OISA. A contract with DGA having as objective the development of formal methods for autonomous systems. Period : from October 15, 2007 to October 14, 2008 ;
- ARC project ProNoBiS : *Probability and Nondeterminism, Bisimulations and Security*. Main partners : ENS Cachan and INRIA Futurs (team SECSI) (responsible J. Goubault-Larrecq), INRIA Futurs (team Comète) (responsible C. Palamidessi), PPS (responsible V. Danos), University of Oxford (responsible M. Kwiatkowska) and Università di Verona (responsible R. Segala). 2006-2007. `http://www.lsv.ens-cachan.fr/~goubault/ProNobis/pronobis1index.html`. Some publications representative of this collaboration are [50, 51, 55].
- DREI project PRINTEMPS : *PRobability and INformation ThEory for Modeling anonymity, Privacy, and Secrecy*. Teams involved : INRIA Futurs (responsible C. Palamidessi), McGill University (responsible P. Panangaden). 2006-2007. `http://www.lix.polytechnique.fr/comete/Projects/Printemps/`. Some publications representative of this collaboration are [30, 13, 46, 45].
- INRIA-FNQRT Teams involved : INRIA Futurs (responsible C. Palamidessi), McGill University (responsible P. Panangaden). 2006-2007.
- ACI Securité project Rossignol : *Verification of Cryptographic Protocols*. Teams involved : LIF (responsible D.Lugiez), INRIA Futurs (responsible C. Palamidessi), LSV (responsible F. Jacquemard) and VERIMAG (responsible Y. Lakhnech). 2003-2006. `http://www.lif.univ-mrs.fr/~lugiez/aci-rossignol.html`. A publication representative of this collaboration is [21].
- REACT : Robust theories for Emerging Applications in Concurrency Theory. Teams involved : Pontificia Universidad Javeriana (responsible C. Rueda), INRIA Futurs (responsible F. Valencia) and IRCAM, France. 2006-2008. `http://cic.puj.edu.co/wiki/doku.php?id=grupos:avispa:react`. Some publications representative of this collaboration are [5, 20, 53, 34].
- PAI project MONACO : *MOdels for New Applications of COncurrency*. Teams involved : Imperial College (responsible I. Phillips), INRIA Futurs (responsible C. Palamidessi) and Technische Universität Berlin (responsible U. Nestmann). 2007.

Teaching, dissemination and service

Advanced schools :

- Catuscia Palamidessi has been teaching the course “The process-calculus approach to security” at the CIMPA-UNESCO School on Security of Computer Systems and Networks. Ban-

galore, INDIA, Jan-Feb 2005.
- Frank Valencia has given a tutorial on “Mobility in Concurrent Languages” at the Latino-American Congress on Informatics (CLEI 2005). Oct, 2005.

Postgraduate courses :

Catuscia Palamidessi has been teaching the following courses :
- “Concurrence” at the MPRI (Master Parisien de Recherche en Informatique). Winter semester 2006-07. (Together with Pierre-Louis Curien, Roberto Amadio and Francesco Zappa Nardelli.)
- “Concurrence” at the MPRI. Winter semester 2005-06. (Together with Jean-Jacques Lévy, Pierre-Louis Curien, Eric Goubault and James Leifer.)
- “Concurrence” at the MPRI. Winter semester 2004-05. (Together with Jean-Jacques Lévy, Pierre-Louis Curien, Erik Goubault and James Leifer.)

Frank Valencia has been teaching the following course :
- “Computability Theory” at the PhD School of Informatics at Universidad del Valle, Colombia. January 2004, January 2005 and January 2007.

Bernadette Charron has given courses in Mastere 2 at the Ecole polytechnique “Distributed Computing and Fault-tolerance”.

Undergraduate courses :

- Frank D. Valencia has been a teaching assistant of "Infomatique Fondamentale" at Ecole Polytechnique. February-May 2005.
- Frank D. Valencia has been a lecturer on "Concurrency Theory" at Universidad Javeriana de Cali. July 2005 and July 2006.

Visibility

National scientific cooperations

- Jean Goubault-Larrecq, ENS Cachan, ARC project ProNoBiS
- Vincent Danos, University of Paris VII, ARC project ProNoBiS and DREI project PRINTEMPS
- D.Lugiez, University of Marseille, ACI project Rossignol
- Y. Lakhnech, VeRIMAG, ACI project Rossignol
- NOVALTIS, Inria, Gérard Le Lann (External consultant)
- GET, ENST, Lirida Naviner and Philippe Matherat

International scientific cooperations

- Marta Kwiatkowska and her team, University of Oxford, UK. ARC project ProNoBiS
- Roberto Segala and his team, Universirty of Verona, Italy. ARC project ProNoBiS
- Prakash Panangaden, McGill University, Canada. DREI project PRINTEMPS
- Uwe Nestmann, University of Berlin, Germany. PAI Project MONACO
- Iain Phillips and Maria Grazia Vigliotti, Imperial College, London, UK. PAI Project MONACO
- Flavio Corradini and Diletta Cacciagrano, University of Camerino, Italy. Collaboration on some papers.
- Maurizio Gabbrielli and Cinzia Di Giusto, University of Bologna, Italy. Collaboration on some papers.
- Vijay Saraswat, IBM, USA. Collaboration on some papers.
- Björn Victor, Uppsala University, Sweden. Collaboration on some papers.
- LSR at EPFL, André Schiper and Martin Hutle. Collaboration on some papers.
- VUT, Ulrich Schmid. Collaboration on some papers.
- A & T University, Texas, Jennifer Welch. Collaboration on some papers.

Conference and seminar invitations

Catuscia Palamidessi has been invited speaker at the following conferences and workshops :
- MFPS XXI, the Twenty-first Conference on the Mathematical Foundations of Programming Semantics. University of Birmingham, UK, May 2005.

- PAuL'07. 2nd International Workshop on Probabilistic Automata and Logics. Wroclaw, Poland, July 9, 2007.
- PERAD 2007. Pervasive Adaptive Joint FET - EATCS Workshop. Brussels, Belgium, January 2007.
- PLID'07. Programming Language Interference and Dependence. Kongens Lyngby, Denmark, August, 2007.

Frank D. Valencia has been an invited speaker at :

- The Latino American Congress on Informatics (CLEI 2005). Cali, Colombia, October 2005.

Catuscia Palamidessi has been an invited panelist at :

- The 19th IEEE Symposium on Computer Security Foundations. Venice, Italy, July 2006. The topic of the panel was "Nondeterminism in Security Modeling".

Conference organisation

- Catuscia Palamidessi has been co-organizer of SecCo'07, the 5th International Workshop on Security Issues in Concurrency. Lisbon, Portugal, September 2007.
- Catuscia Palamidessi and Frank Valencia have organized the LIX Colloquium on *Emerging Trends in Concurrency Theory*, Palaiseau, France, 13-15 November 2006.
- Catuscia Palamidessi has been the Program Committee Chair of ICALP 2005 Track B. 32nd International Colloquium on Automata, Languages and Programming. Lisboa, Portugal, 11-15 July 2005.
- Bernadette Charron-Bost has been the Program Committeee Chair of the *31th Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM)*, 2004

Program committees

Catuscia Palamidessi is or has been a member of the program committee of the following conferences :

- QEST'08. International Conference on Quantitative Evaluation of SysTems. September 2008.
- FICS'08. Foundations of Informatics, Computing and Software. Shanghai, China, June 2008.
- MFPS XXIV. Twenty-fourth Conference on the Mathematical Foundations of Programming Semantics. University of Pennsylvania, Philadelphia, USA, May 2008.
- LICS 2008. 23rd Symposium on Logic in Computer Science. Pittsburgh, USA. June 2008.
- VMCAI 2008. 9th International Conference on Verification, Model Checking, and Abstract Interpretation. San Francisco, USA. January 2008.
- CiE 2008. Logic and Theory of Algorithms. Athens, Greece. June 2008.
- ESOP 2008. European Symposium on Programming. (Part of ETAPS 2008.) Budapest, Hungary, March-April 2008.
- QEST'07. International Conference on Quantitative Evaluation of SysTems. Edinburgh, Scotland, September 2007.
- Concur 2007. International Conference on Concurrency Theory. Lisbon, Portugal, September 2007.
- FCT 2007. International Symposium on Fundamentals of Computation Theory Budapest, Hungary, August 2007.
- ESOP 2007. European Symposium on Programming. (Part of ETAPS 2007.) Braga, Portugal, March-April 2007.
- LPAR 2006.International Conference on Logic for Programming Artificial Intelligence and Reasoning. Phnom Penh, Cambodia, November 2006.
- CONCUR 2006. International Conference on Concurrency Theory. Bonn, Germany, August 2006.
- MFPS XXII. Twenty-second Conference on the Mathematical Foundations of Programming Semantics. Genova, Italy, May 2006.
- FOSSACS 2006. International Conference on Foundations of Software Science and Computation Structures. (Part of ETAPS 2006.) Vienna, Austria, March-April 2006.
- LPAR 2005. International Conference on Logic for Programming Artificial Intelligence and Reasoning. Montego Bay, Jamaica, December 2005.
- ICLP 2005. International Conference on Logic Programming. Barcelona, Spain, October 2005.
- CONCUR 2005. International Conference on Concurrency Theory. San Francisco, California, USA, August 2005.
- ESOP 2005. European Symposium on Programming. (Part of ETAPS 2005.) Edinburgh, Scotland, April 2005.

- SOFSEM 2005 Track on Foundations of Computer Science. 31st Annual Conference on Current Trends in Theory and Practice of Informatics, Liptovsky Jan, Slovak Republic, January 2005.

Catuscia Palamidessi has been a member of the program committee of the following workshops :

- FInCo 2007. Workshop on the Foundations of Interactive Computation. Braga, Portugal, March-April 2007.
- EXPRESS'06. 12th International Workshop on Expressiveness in Concurrency. Bonn, Germany, August 2006.
- FInCo 2005. Workshop on the Foundations of Interactive Computation. Edinburgh, Scotland, April 2005.

Frank D. Valencia has been a member of the program committee of the following conferences :

- ICLP 2005. 21st International Conference on Logic Programming. Barcelona, Spain, October 2005.
- CLEI 2005. Latino-American Congress on Informatics. Cali, Colombia, October 2005.

Bernadette Charron-Bost has been a member of the program committee of the following conferences :

- SIROCCO 2004. Colloquium on Structural Information and Communication Complexity
- ICDCS 2005. 25th International Conference on Distributed Computing Systems
- ICDCS 2007. 27th International Conference on Distributed Computing Systems

Carlos Olarte has been PC member of SAC 2007, the Track on Constraint Solving and Programming of the 22nd Annual ACM Symposium on Applied Computing.

Editorial activity

Editorial boards

- Catuscia Palamidessi is member of the Editorial Board of the journal *Mathematical Structures in Computer Science*, published by the Cambridge University Press.
- Catuscia Palamidessi is member of the Editorial Board of the journal *Theory and Practice of Logic Programming*, published by the Cambridge University Press.
- Catuscia Palamidessi is member of the Editorial Board of the *Electronic Notes of Theoretical Computer Science*, published by Elsevier Science.
- Frank D. Valencia is area editor (for the area of Concurrency) of the *ALP Newsletter*.

Edited volumes

- Catuscia Palamidessi has been co-editor of the special issue dedicated to selected papers of ICALP 2005, *Theoretical Computer Science* 380(1-2). Pages 1-218, 2007.
- Catuscia Palamidessi and Frank Valencia have edited the post-proceedings of the LIX Colloquium on *Emerging Trends in Concurrency Theory* held in Palaiseau, France, during November 2006. The post-proceedings will appear as a volume on the *Electronic Notes in Theoretical Computer Science*.
- Catuscia Palamidessi has been co-editor of the proceedings of ICALP 2005, *Lecture Notes in Computer Science* 3580, Springer-Verlag, 2005.

Awards

Tom Chothia has received the best paper award at FORTE 2006 for his paper [31].

Steering Committees

Catuscia Palamidessi is member of :

- The IFIP Technical Committee 1 – Foundations of Computer Science. Since 2007
- The Council of EATCS, the European Association for Theoretical Computer Science. Since 2005
- The IFIP Working Group 2.2 – Formal Description of Programming Concepts. Since 2001

Bernadette Charron Bost is member of the steering Committee of the Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM). Since 2005

Other services to the community

- Catuscia Palamidessi has been rapporteur and member of the jury at the PhD defense of Florent Garnier (Loria). September 2007.
- Catuscia Palamidessi has been a member of the "jury d'ammissibilité" in the 2007 INRIA competition for CR2 posts.

– Catuscia Palamidessi has been rapporteur and member of the jury at the PhD defense of Jean Krivine, October 2006.
– Catuscia Palamidessi has been a member of the assessment panel for the evaluation of the project proposal to the initiative FOCUS of the Dutch National Science Foundation. May 2006.
– Bernadette Charron Bost has been Committee member of the *Prix d'Alembert, French Mathematical Society*, 2004 and 2006.

References

Books and chapters in books

2005

[1] CAIRES, L., ITALIANO, G. F., MONTEIRO, L., PALAMIDESSI, C., AND YUNG, M., Eds. *Automata, Languages and Programming, 32nd International Colloquium, ICALP 2005, Lisbon, Portugal, July 11-15, 2005, Proceedings* (2005), vol. 3580 of *Lecture Notes in Computer Science*, Springer.

[2] DENG, Y., PALAMIDESSI, C., AND PANG, J. Compositional reasoning for probabilistic finite-state behaviors. In *Processes, Terms and Cycles : Steps on the Road to Infinity*, A. Middeldorp, V. van Oostrom, F. van Raamsdonk, and R. C. de Vrijer, Eds., vol. 3838 of *Lecture Notes in Computer Science*. Springer, 2005, pp. 309–337.

2007

[3] ITALIANO, G. F., AND PALAMIDESSI, C. *Special issue of* Theoretical Computer Science *dedicated to a selection of the best papers presented at ICALP'05. 380(1-2)*. Elsevier, 2007.

International journals

2004

[4] CHARRON-BOST, B., AND SCHIPER, A. Uniform consensus is harder than consensus. *Journal of Algorithms 51*, 1 (2004), 15–37.

[5] RUEDA, C., AND VALENCIA, F. D. On validity in modelization of musical problems by CCP. *Soft Computing 8*, 9 (2004), 641–648.

2005

[6] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. A framework for analyzing probabilistic protocols and its application to the partial secrets exchange. *Theoretical Computer Science* (2005). `www.lix.polytechnique.fr/~catuscia/papers/PartialSecrets/TCSreport.pdf`.

[7] PALAMIDESSI, C., AND HERESCU, O. M. A randomized encoding of the π-calculus with mixed choice. *Theoretical Computer Science 335*, 2-3 (2005), 373–404.

[8] VALENCIA, F. D. Decidability of infinite-state timed CCP processes and first-order LTL. *Theoretical Computer Science 330*, 3 (2005), 577–607.

2006

[9] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. Probable innocence revisited. *Theoretical Computer Science 367*, 1-2 (2006), 123–138.

[10] WU, P., AND LIN, H. Model-based testing of concurrent programs with predicate sequencing constraints. *International Journal of Software Engineering and Knowledge Engineering 16*, 5 (2006), 727–746.

2007

[11] CACCIAGRANO, D., CORRADINI, F., AND PALAMIDESSI, C. Separation of synchronous and asynchronous communication via testing. *Theoretical Computer Science* (2007). `www.lix.polytechnique.fr/~catuscia/papers/Diletta/Must/tcs.pdf`.

[12] CHARRON-BOST, B., AND SCHIPER, A. Harmful Dogmas in Fault-Tolerant Distributed Computing. In *The SIGACT News Distributed Computing Column* (2007), vol. 142, pp. 287–295. Available at www.acm.org/sigactnews/online/.

[13] CHATZIKOKOLAKIS, K., PALAMIDESSI, C., AND PANANGADEN, P. Anonymity protocols

as noisy channels. *Information and Computation* (2007). www.lix.polytechnique.fr/~catuscia/papers/Anonymity/Channels/full.pdf.

[14] DENG, Y., AND PALAMIDESSI, C. Axiomatizations for probabilistic finite-state behaviors. *Theoretical Computer Science 373*, 1-2 (2007), 92–114.

[15] LANOTTE, R., MAGGIOLO-SCHETTINI, A., AND TROINA, A. Parametric probabilistic transition systems for system design and analysis. *Formal Aspects of Computing 19*, 1 (2007), 93–109.

[16] PHILLIPS, I., VIGLIOTTI, M. G., AND PALAMIDESSI, C. Expressiveness via leader election problems. *Theoretical Computer Science* (2007). www.lix.polytechnique.fr/~catuscia/papers/Diletta/Must/tcs.pdf.

[17] WIDDER, J., AND SCHMID, U. Booting clock synchronization in partially synchronous systems with hybrid process and link failures. *Distributed Computing 20*, 2 (Aug. 2007), 115–140.

International conferences with proceedings

2004

[18] CHARRON-BOST, B., AND LE FESSANT, F. Validity conditions in agreement problems and time complexity. In *Proceedings 30th Annual Conference on Current Trends in Theory and Practice of Informatics* (2004), vol. 2234 of *Lecture Notes in Computer Science*, Springer, pp. 196–207.

[19] GIAMBIAGI, P., SCHNEIDER, G., AND VALENCIA, F. D. On the expressiveness of infinite behavior and name scoping in process calculi. In *Proceedings of the 7th International Conference on the Foundations of Software Science and Computation Structures (FOSSACS 2004)* (2004), I. Walukiewicz, Ed., vol. 2987 of *Lecture Notes in Computer Science*, Springer, pp. 226–240.

[20] RUEDA, C., AND VALENCIA, F. Non-viability deductions in arc-consistency computation. In *Proc. of the Nineteenth International Conference on Logic Programming (ICLP 2004)* (2004), B. Demoen and V. Lifschitz, Eds., vol. 3132 of *Lecture Notes in Computer Science*, Springer, pp. 343–355.

2005

[21] BHARGAVA, M., AND PALAMIDESSI, C. Probabilistic anonymity. In *Proceedings of CONCUR* (2005), M. Abadi and L. de Alfaro, Eds., vol. 3653 of *Lecture Notes in Computer Science*, Springer, pp. 171–185.

[22] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. A framework for analyzing probabilistic protocols and its application to the partial secrets exchange. In *Proceedings of the Symp. on Trustworthy Global Computing* (2005), vol. 3705 of *Lecture Notes in Computer Science*, Springer, pp. 146–162.

[23] CHOTHIA, T., AND CHATZIKOKOLAKIS, K. A survey of anonymous peer-to-peer file-sharing. In *Proceedings of the IFIP International Symposium on Network-Centric Ubiquitous Systems (NCUS 2005)* (2005), vol. 3823 of *Lecture Notes in Computer Science*, Springer, pp. 744–755.

[24] DENG, Y., AND PALAMIDESSI, C. Axiomatizations for probabilistic finite-state behaviors. In *Proceedings of FOSSACS'05* (2005), vol. 3441 of *Lecture Notes in Computer Science*, Springer, pp. 110–124.

[25] PALAMIDESSI, C., PHILLIPS, I., AND VIGLIOTTI, M. G. Expressiveness via leader election problems. In *Postproceedings of the 4th International Symposium on Formal Methods for Components and Objects (FMCO)* (2005), F. S. de Boer, M. M. Bonsangue, S. Graf, and W. P. de Roever, Eds., vol. 4111 of *Lecture Notes in Computer Science*, Springer, pp. 172–194.

2006

[26] ARANDA, J., GIUSTO, C. D., PALAMIDESSI, C., AND VALENCIA, F. Expressiveness of recursion, replication and scope mechanisms in process calculi. In *Postproceedings of the 5th International Symposium on Formal Methods for Components and Objects (FMCO'06)* (2006), F. de Boer and M. Bonsangue, Eds., LNCS, Springer.

www.brics.dk/~fvalenci/papers/rec-rep-scope.pdf.

[27] CACCIAGRANO, D., CORRADINI, F., AND PALAMIDESSI, C. Separation of synchronous and asynchronous communication via testing. In *Proceedings of the 12th International Workshop on Expressiveness in Concurrency (EXPRESS 2005)* (San Francisco, USA, 2006), vol. 154 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 95–108.

[28] CHARRON-BOST, B., AND SCHIPER, A. Improving Fast Paxos : being optimistic with no overhead. In *Proceedings of the 12th Pacific Rim Int. Symp. on Dependable Computing (PRDC)* (2006), LNCS-2485, pp. 287–295.

[29] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. Probable innocence revisited. In *Third International Workshop on Formal Aspects in Security and Trust (FAST 2005), Revised Selected Papers* (2006), T. Dimitrakos, F. Martinelli, P. Y. A. Ryan, and S. A. Schneider, Eds., vol. 3866 of *Lecture Notes in Computer Science*, Springer, pp. 142–157.

[30] CHATZIKOKOLAKIS, K., PALAMIDESSI, C., AND PANANGADEN, P. Anonymity protocols as noisy channels. In *Proceedings of the Symposium on Trustworthy Global Computing (TGC)* (2006), vol. 4661 of *Lecture Notes in Computer Science*, Springer, pp. 281–300.

[31] CHOTHIA, T. Analysing the mute anonymous file-sharing system using the pi-calculus. In *26th IFIP WG 6.1 international conference on formal techniques for networked and distributed systems – FORTE 2006* (September 2006), E. Najm, J.-F. Pradat-Peyre, and V. Viguié Donzeau-Gouge, Eds., no. 4229 in Lecture Notes in Computer Science, Springer, pp. 115–130. Best paper award at FORTE 2006.

[32] DENG, Y., CHOTHIA, T., PALAMIDESSI, C., AND PANG, J. Metrics for action-labelled quantitative transition systems. In *Proceedings of the Third Workshop on Quantitative Aspects of Programming Languages (QAPL 2005)* (2006), vol. 153 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science Publishers, pp. 79–96.

[33] DENG, Y., PANG, J., AND WU, P. Measuring anonymity with relative entropy. In *Proceedings of the 4th International Workshop on Formal Aspects in Security and Trust (FAST)* (2006), T. Dimitrakos, F. Martinelli, P. Y. A. Ryan, and S. A. Schneider, Eds., vol. 4691 of *Lecture Notes in Computer Science*, Springer, pp. 65–79.

[34] LÓPEZ, H. A., PALAMIDESSI, C., PÉREZ, J. A., RUEDA, C., AND VALENCIA, F. D. A declarative framework for security : Secure concurrent constraint programming. In *Proceedings of the 22nd International Conference on logic Programming, (ICLP)* (2006), S. Etalle and M. Truszczynski, Eds., vol. 4079 of *Lecture Notes in Computer Science*, Springer, pp. 449–450.

[35] PALAMIDESSI, C. Probabilistic and nondeterministic aspects of anonymity. In *Proceedings of the 21st Conference on the Mathematical Foundations of Programming Semantics (MFPS XXI)* (Birmingham, UK, 2006), vol. 155 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 33–42.

[36] PALAMIDESSI, C., SARASWAT, V. A., VALENCIA, F. D., AND VICTOR, B. On the expressiveness of linearity vs persistence in the asynchronous pi-calculus. In *Proceedings of the Twenty First Annual IEEE Symposium on Logic in Computer Science (LICS)* (2006), IEEE Computer Society, pp. 59–68.

[37] PRADALIER, S., AND PALAMIDESSI, C. Expressiveness of probabilistic π-calculi. In *Proceedings of the 4th International Workshop on Quantitative Aspects of Programming Languages (QAPL)* (2006), vol. 164 (3) of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 119–136.

[38] ZIEGLER, A., MILLER, D., AND PALAMIDESSI, C. A congruence format for name-passing calculi. In *Proceedings of the 2nd Workshop on Structural Operational Semantics (SOS'05)* (Lisbon, Portugal, 2006), vol. 156 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 169–189.

2007

[39] ANCEAUME, E., DELPORTE-GALLET, C., FAUCONNIER, H., HURFIN, M., AND WIDDER, J. Clock synchronization in the

Byzantine-recovery failure model. In *International Conference On Principles Of DIstributed Systems (OPODIS'07)* (Guadeloupe, French West Indies, Dec. 2007), LNCS, Springer Verlag. (to appear).

[40] ARANDA, J., GIUSTO, C. D., NIELSEN, M., AND VALENCIA, F. CCS with replication in the Chomsky hierarchy : The expressive power of divergence. In *Proc. of The Fifth ASIAN Symposium on Programming Languages (APLAS'07)* (2007), LNCS, Springer. www.brics.dk/~fvalenci/papers/aplas.pdf.

[41] BIELY, M., CHARRON-BOST, B., GAILLARD, A., HUTTLE, M., SCHIPER, A., AND WIDDER, J. Tolerating corrupted communications. In *Proceedings of PODC* (Portland, USA, 2007), pp. 244–253.

[42] BIELY, M., HUTLE, M., PENSO, L. D., AND WIDDER, J. Relating stabilizing timing assumptions to stabilizing failure detectors regarding solvability and efficiency. In *9th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'07)* (Paris, Nov. 2007), vol. 4838 of *LNCS*, Springer Verlag. (to appear).

[43] CACCIAGRANO, D., CORRADINI, F., ARANDA, J., AND VALENCIA, F. Persistence and testing semantics in the asynchronous pi calculus. In *Proc. of 14th International Workshop on Expressiveness of Concurrency, (EXPRESS'07)* (2007), R. Amadio and T. Hildenbrandt, Eds., ENTCS, Elsevier. www.brics.dk/~fvalenci/papers/pers-test.pdf.

[44] CACCIAGRANO, D., CORRADINI, F., AND PALAMIDESSI, C. Fair π. In *Proceedings of the 13th International Workshop on Expressiveness in Concurrency (EXPRESS'06)* (2007), vol. 175 (3) of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 3–26.

[45] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. Making random choices invisible to the scheduler. In *Proceedings of CONCUR'07* (2007), L. Caires and V. T. Vasconcelos, Eds., vol. 4703 of *Lecture Notes in Computer Science*, Springer, pp. 42–58.

[46] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. Probability of error in information-hiding protocols. In *Proceedings of the 20th IEEE Computer Security Foundations Symposium (CSF20)* (2007), IEEE Computer Society, pp. 341–354.

[47] CREDI, A., GARAVELLI, M., LANEVE, C., PRADALIER, S., SILVI, S., AND ZAVATTARO, G. Modelization and simulation of nano devices in nanoκ calculus. In *Proceedings of the International Conference on Computational Methods in Systems Biology, (CMSB)* (2007), M. Calder and S. Gilmore, Eds., vol. 4695 of *Lecture Notes in Computer Science*, Springer, pp. 168–183.

[48] DENG, Y., PALAMIDESSI, C., AND PANG, J. Weak probabilistic anonymity. In *Proceedings of the 3rd International Workshop on Security Issues in Concurrency (SecCo)* (2007), vol. 180 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 55–76.

[49] FALASCHI, M., OLARTE, C., PALAMIDESSI, C., AND VALENCIA, F. D. Declarative diagnosis of temporal concurrent constraint programs. In *Proceedings of The 23rd International Conference in Logic Programming (ICLP'07)* (2007), V. Dahl and I. Niemelä, Eds., vol. 4670 of *Lecture Notes in Computer Science*, Springer, pp. 271–285.

[50] GOUBAULT-LARRECQ, J., PALAMIDESSI, C., AND TROINA, A. A probabilistic applied pi-calculus. In *Proceedings of the 5th Asian Symposium on Programming Languages and Systems (APLAS'07)* (2007), LNCS, Springer. www.lix.polytechnique.fr/~catuscia/papers/Angelo/aplas.pdf.

[51] NORMAN, G., PALAMIDESSI, C., PARKER, D., AND WU, P. Model checking the probabilistic pi-calculus. In *4th International Conference on the Quantitative Evaluation of SysTems (QEST)* (2007), Lecture Notes in Computer Science, Springer. www.lix.polytechnique.fr/~catuscia/papers/Wu/qest1.pdf.

[52] OLARTE, C., PALAMIDESSI, C., AND VALENCIA, F. D. Universal timed concurrent constraint programming. In *Proceedings of the 23rd International Conference in Logic Programming (ICLP'07)* (2007), V. Dahl and I. Niemelä, Eds., vol. 4670 of *Lecture Notes in Computer Science*, Springer, pp. 464–465.

[53] RUEDA, J. G. J. P. C., AND VALENCIA., F. Timed concurrent constraint programming for analyzing biological systems. In *Proceedings of Workshop on Membrane Computing and Biologically Inspired Process Calculi.* (2007), vol. 171 (2) of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 117–137.

[54] WIDDER, J., GRIDLING, G., WEISS, B., AND BLANQUART, J.-P. Synchronous consensus with mortal Byzantines. In *Proceedings of the International Conference on Dependable Systems and Networks (DSN'07)* (Edinburgh, UK, June 2007), pp. 102–111.

[55] WU, P., PALAMIDESSI, C., AND LIN, H. Probabilistic systems. In *Proceedings of 4th International Conference on the Quantitative Evaluation of SysTems (QEST)* (2007), Lecture Notes in Computer Science, Springer. www.lix.polytechnique.fr/~catuscia/papers/Wu/qest2.pdf.

PhD Thesis

2007

[56] CHATZIKOKOLAKIS, K. *Probabilistic and Information-Theoretic Approaches to Anonymity*. PhD thesis, LIX, École Polytechnique, Oct. 2007. www.lix.polytechnique.fr/~kostas/thesis.pdf.

Miscellaneous

2004

[57] CHARRON-BOST, B. Reductions in distributed computing. part i : Consensus and Atomic Commitment Tasks. Tech. Rep. LIX/10/2004, LIX, 2004. Available from ArXiv as number cs.DC/04/12115.

[58] CHARRON-BOST, B. Reductions in distributed computing. part ii : k-Threshold Agreement Tasks. Tech. Rep. LIX/12/2004, LIX, 2004. Available from ArXiv as number cs.DC/04/12116.

2005

[59] PALAMIDESSI, C., AND VALENCIA, F. Recursion vs replication in process calculi : Expressiveness. *Bulletin of the EATCS 87* (2005), 105–125.

2006

[60] PALAMIDESSI, C. Anonymity in probabilistic and nondeterministic systems. In *Proceedings of the Workshop on "Essays on Algebraic Process Calculi" (APC 25)* (Bertinoro, Italy, 2006), vol. 162 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 277–279.

[61] PALAMIDESSI, C., AND BHARGAVA, M. Probabilistic anonymity. In *Foundations of Global Computing* (2006), J. L. Fiadeiro, U. Montanari, and M. Wirsing, Eds., no. 05081 in Dagstuhl Seminar Proceedings, Internationales Begegnungs- und Forschungszentrum (IBFI), Schloss Dagstuhl, Germany. drops.dagstuhl.de/opus/volltexte/2006/299.

[62] PALAMIDESSI, C., AND VALENCIA, F. Languages for concurrency. *Bulletin of the European Association for Theoretical Computer Science 90* (Oct. 2006), 155–171. Column : Programming Languages.

2007

[63] CHARRON-BOST, B., AND SCHIPER, A. The Heard-Of model : Computing in distributed systems with benign failures. Tech. Rep. LSR/2007-004, Département Systèmes de Communication, EPFL, 2007.

[64] OLARTE, C., AND VALENCIA, F. On the expressiveness of universal concurrent constraint programming. Tech. rep., LIX, Ecole Polytechnique, 2007. www.lix.polytechnique.fr/~colarte/reportb.pdf.

[65] OLARTE, C., AND VALENCIA, F. A process calculus for universal concurrent constraint programming : Semantics, logic and application. Tech. rep., LIX, Ecole Polytechnique, 2007. www.lix.polytechnique.fr/~colarte/reporta.pdf.

External references

[66] HONDA, K., AND TOKORO, M. An object calculus for asynchronous communication. In *Proceedings of the European Conference on Object-Oriented Programming (ECOOP)* (1991), P. America, Ed., vol. 512 of *Lecture Notes in Computer Science*, Springer, pp. 133–147.

[67] BOUDOL, G. Asynchrony and the π-calculus (note). Rapport de Recherche 1702, INRIA, Sophia-Antipolis, `www.inria.fr/rrrt/rr-1702.html`, 1992.

[68] MILNER, R., PARROW, J., AND WALKER, D. A calculus of mobile processes, I and II. *Information and Computation 100*, 1 (1992), 1–40 & 41–77.

[69] ABADI, M., AND FOURNET, C. Mobile values, new names, and secure communication. In *28th Annual Symposium on Principles of Programming Languages (POPL)* (Jan. 2001), ACM, pp. 104–115.

[70] YANG, P., RAMAKRISHNAN, C. R., AND SMOLKA, S. A. A logical encoding of the pi-calculus : model checking mobile processes using tabled resolution. *International Journal on Software Tools for Technology Transfer 6*, 1 (2004), 38–66.

[71] HOARE, T., AND MILNER, R. Grand challenges for computing research. *Computer Journal 48*, 1 (2005), 49–52.

[72] CANETTI, R., CHEUNG, L., LYNCH, N., AND PEREIRA, O. On the role of scheduling in simulation-based security. Cryptology ePrint Archive, Report 2007/102, 2007.

PARSIFAL
Preuves Automatiques et Raisonnement sur des SpécIFicAtions Logiques

Team members

Team leader

Dale MILLER

Permanent members

- Stéphane LENGRAND, chargé de recherches CNRS (from 1 January 2008)
- Dale MILLER, directeur de recherches INRIA
- Lutz STRASSBURGER, chargé de recherches INRIA (since 1 December 2005).

Phds

- David BAELDE, AMN (Allocation et Monitorat pour Normalien), since September 2005
- Olivier DELANDE, Bourse Monge, since 1 October 2006
- Vivek NIGAM, Mobius Contract, since Oct 2006
- Alexis SAURIN, AMN (Allocation et Monitorat pour Normalien), since Sept 2004.

Post Docs

- Kaustuv CHAUDHURI, PhD Carnegie Mellon University, from 1 November 2006 to 31 October 2007
- Murdoch J. GABBAY, Phd Cambridge University, from 1st september 2004 to 31 august 2005
- Laurent MÉHATS, PhD Toulouse III, from 1 September 2007 to 31 August 2008.

Interns

- Nicolas GUENOT, MPRI, from March 5, 2007 to August 31, 2007
- David BAELDE, MPRI, 2005.
- Axelle ZIEGLER, MPRI, 2004 (co-supervised with Catuscia Palamidessi of Comète).

Guests

- Joëlle DESPEYROUX, CR INRIA-Sophia (at LIX one day a week since 1 September 2005)
- Chuck LIANG, Associate Professor at Hofstra University, New York, was an INRIA invited researcher from September to December 2006 and June 2007
- Gopalan NADATHUR, Professor at the University of Minnesota, spent three months of his sabbatical taken at LIX in Spring 2004
- Frank PFENNING, Professor at Carnegie Mellon University, Pittsburgh was an INRIA invited research during June and July 2006.

Research domain

Software correctness is a key aspect of many computing systems. For example, computers and software are used to help control nuclear power plants, avionic controls, and automobiles and, in such safety-critical systems, incorrect software can cause serious problems. Similarly, errors in networking software, operating systems, browsers, etc, can leave computer systems open for computer viruses and security breeches. In order to avoid errors in such complex and interacting systems, one must be able to prove the correctness of individual application programs as well as a wide range of software systems that analyze and manipulate them : these range from compilers and linkers, to parsers and type checkers, to high-level properties of entire programming languages. In the face of this increasing need for program correctness, an international community of researchers is developing many approaches to the correctness of software. Formal methods are gaining acceptance as one viable approach to addressing program correctness and this project will focus on using such methods to address this problem.

The Parsifal team aims at elaborating methods and tools for specifying and reasoning about computation systems such as compilers, security protocols, and concurrent programs. A central challenge here is proving properties of programs that manipulate other programs. The specification of such computational systems today is commonly given using operational semantics, supplanting the well-established but restrictive approach using denotational semantics. Operational semantics is generally given via inference rules using relations between different items of the computation, and for this reason, it is an example of a relational specification. Inference rules over relations are also used for specifying the static semantics for programming languages as well (type inference, for example). The use of denotational style presentations of computational systems naturally leads to the use of functional programming-based executable specifications. Similarly, the use of inference systems for the presentation of operational semantics provides a natural setting for exploiting logic programming-based implementations.

The Parsifal project will exploit recent developments in proof search, logic programming, and type theory to make the specification of operational semantics more expressive and declarative and will develop techniques and tools for animating and reasoning directly on logic-based specifications.

Goals

More specifically, the Parsifal project focuses on the following goals.

Foundations We plan to exploit the proof theory of expressive logics for the specification of computations and to develop a logics for reasoning about proof search specifications. Such meta-logics will likely be based on higher-order intuitionistic logic and will include proof principles for induction and co-induction. We shall also consider its analogous design as a type system.

Prototypes We plan to build prototype components needed for the implementation of proof search (including unification, search, tabling, binding and substitution in syntax, etc) and use these components to build specific research prototypes for a range of applications. We shall explore architectures for provers that allow differing amounts of interaction and automation.

Applications We will test the feasibility of incorporating our deductive tools into various applications that can benefit from mixing computation and deduction. Application areas we have in mind are security, global computing, proof-carrying code, and mobile code.

Results

Work in the team over the past three years has focused mainly on *developing* results in proof theory, especially results establish connections to computation, and in *exploiting* such results by applying them to designing prototype implementations and methodologies for reasoning about computation. Various avenues of our development are described below.

Formalized reasoning about computation systems A major effort during each of the past three years has been the development of a methodology for reasoning about logical specifications. Relational specifications are widely used to describe the static and dynamic semantics of programming and specification languages. Such specifications are common for typing judgments and are used widely in *structured operational semantics*. One approach to formally specifying such relational specifications uses the *higher-order abstract syntax* approach found in meta-logics (such as in the foundations of λProlog) or a dependently typed λ-calculus (such as in the foundations of Twelf). While there are competing approaches to this style of specification, it is one of the first approaches to have been developed : it also has a well-understood semantics and numerous implementations. While it has been well-known for many years how to effectively automate and use higher-order abstract syntax, much less is know about how to formally reason with such specifications. Along these lines, the team has taken a number of steps forward. In particular, Miller and Alwen Tiu have developed a logic, called LINC, that includes a new quantifier ∇ that is central to our formal reasoning approach [34, 4]. The general methodology of this approach has been outlined in the invited paper [24]. Further evidence that this methodology and logic provides a direct and natural approach to the metatheory of computation comes from the paper [21] in which Miller, Palamidessi, and Ziegler use LINC to naturally extend a previous framework that related bisimulation and congruences to the case of processes with name mobility.

Bedwyr : model checking linguistic systems In order to provide some practical validation of the formal results mentioned above regarding the logic LINC and the quantifier ∇, we picked a small but expressive subset of that logic for implementation. While that subset did not involve the proof rules for induction and co-induction (which are difficult to automate) the subset did allow for model-checking style computation. During the summer of 2006, members of Parsifal along with colleagues from the University of Minnesota and the Australian National University designed and implemented the Bedwyr system. This system, described in the conference papers [20, 27] and in the user manuals [35, 38], was implemented in OCaml and has been available for download since November 2005 (close to 200 downloads have been made to-date). The system served well to validate the underlying theoretical considerations while at the same time providing a useful tool for exploring some applications. Probably the most interesting application is the specification of both the operational semantics and open bisimulation for the π-calculus [12, 4] : these specifications are essentially immediate and declarative versions of the usual ways that practitioners specify the π-calculus.

Focusing proof systems : foundations for proof search automation The team has also invested a great deal of energy in developing new normal form theorems regarding cut-free proofs in various logics. These normal forms, usually called *focused proofs systems* following an early paper by Jean-Marc Andreoli in 1992, have important implications for the automation of proof search. Focusing proof systems provide ways to organize the structure of "don't-known" and "don't care" non-determinism. Andreoli's work in linear logic has been augmented in two ways within the team. Miller and Saurin in [31] have provided a new style proof of the completeness of focusing in linear logic. Chaudhuri *et.al.* in [7] developed an intuitionistic linear variant of focusing and observed that focusing can naturally account for different forms of resolution in (linear versions of) Horn clauses. Miller and Liang in [29] have studied in detail a general framework to describe focusing in intuitionistic logic. Since a next step for the team is to move away from automation of simple logic programming and model checking engines to the (partial) automation of proofs involving induction and co-induction, it was important to develop a general approach to proof search for these inference rules. Baelde and Miller have derived just such results in [28] and provide the first focusing results for a proof systems containing induction and co-induction.

Applications of focusing proof systems To help validate our energies at exploring focusing proof systems, the team has looked at various applications of such proof theoretic results. Miller and Nigam in [30] have shown how focusing proof systems can be exploited to provide a declarative approach to the use of tables in proof search (addressing the issue of lemma *reuse* instead of *reproof* in the case of atomic lemmas). The system of static collection analysis proposed by Miller in [23] makes use of linear logic to describe invariants among sets and multisets : theorem provers for such invariants have been simple to design based on the focusing theorem. Finally, there appears to be a very close connection between focusing proof systems and certain kinds of game semantics for proof search. The team has been working on understanding a "neutral approach to proof and refutation" : partial results were announced by Miller and Saurin in [15, 25] and Olivier Delande is attempting to complete the picture (for the MALL fragment of linear logic).

Specification of logical systems The study of computational logic properties are now sufficiently advanced that many properties of logic can be inferred automatically. For example, Pimentel and Miller have designed a framework in which inference rules for logics can be faithfully specified. This framework, as described in the papers [2, 17] use linear logic programming as the actual framework. Sufficient conditions are offered for cut-elimination and initial-elimination to hold. These conditions are easily expressed by the fact that certain small formulas in linear logic can be proved. Provability of such formulas is also decidable. As a result, determining, for example, cut-elimination for a wide range of logics is an entirely automatic process.

A logic for systems biology Systems in molecular biology, such as, those for regulatory gene networks or protein-protein interactions, can be seen as state transition systems that have an additional notion of *rate* of change. Methods for specifying such systems is an active research area : one current and prominent method uses process calculi, such as the stochastic π-calculus, that has a built in notion of rate.[14] Process calculi, however, have the deficiency that reasoning about the specifications is external to the specifications themselves, usually depending on simulations and trace analysis. Kaustuv Chaudhuri and Joëlle Despeyroux have been considering the problem of giving a *logical* instead of a *process-based* treatment both to specify and to reason about biological systems in a uniform linguistic framework. The particular logic they used, called HyLL, is an extension of (intuitionistic) linear logic with a modal situated truth that may be reified by means of the $\downarrow$ operator from *hybrid logic*, and given a variety of semantic interpretation as the rates of formation. Among the technical results obtained is an adequate encoding of the stochastic π-calculus in HyLL. A technical report and a conference submission are in preparation.

Proof nets for linear logic with units By using the insights of *deep inference*, François Lamarche (LORIA) and Lutz Straßburger where able to extend ordinary proof nets for multiplicative linear logic by the two units, in such a way that the proof identifications made by the new proof nets are exactly the same proof identifications as they are enforced by the axioms of *-autonomous categories. Algebraically speaking, Lamarche and Straßburger gave a concrete construction of the free *-autonomous category. The results are published in [11] and [5].

Categorical axiomatization of proofs in classical logic One reason for using categories in proof theory is to give a precise algebraic meaning to the identity of proofs : two proofs are the same if and only if they give rise to the same morphism in the category. Finding the right axioms for the identity of proofs for classical propositional logic for long been thought to be impossible, due to "Joyal's Paradox". For the same reasons, it was believed for a long time that it it not possible to have proof nets for classical logic. Nonetheless, Lutz Straßburger and François Lamarche provided proof nets for classical logic in [14], and analyzed the category theory behind them in [13]. In [8, 26], one can find a deeper analysis of the category theoretical axioms for proof identification in classical logic. Particular focus is on the so-called *medial rule* which plays a central role in the deep inference deductive system for classical logic.

[14] See Blossey, Cardelli,and Phillips. "A Compositional Approach to the Stochastic Dynamics of Gene Networks", Trans. on Computational Systems Biology, LNCS 3939 (2006).

Proof nets for second order multiplicative linear logic Exploring the ideas of [5] which allowed including the units into the theory of proof nets, Lutz Straßburger developed a new theory of proof nets that also includes the quantifiers, without relying on boxes, as in Girard's original work. The results are not yet published, but available from Straßburger's webpage[15].

Combinatorial characterization of deep inference deduction rules Geometric or combinatoric correctness criteria are important for studying proofs independently from syntax. In [32], Lutz Straßburger gives such a criterion for the medial rule. Thus there are now two independent approaches towards a notion of proof identification : First, via algebraic considerations, i.e., categories, and second, via combinatorial or graph-theoretical considerations, i.e., proof nets and correctness criteria.

Deep inference for hybrid logics Hybrid languages are modal languages which use formulas to refer to specific points in a model. There is a fast growing community because of many applications. In [33] Lutz Straßburger presents a deep inference deductive system for hybrid logic. Thus, the rich proof theory related to deep inference is made available for hybrid logics, which so far have mainly been studied via model theory.

Software, pattents and contracts

Software

Bedwyr is a generalization of logic programming that allows model checking directly on syntactic expression possibly containing bindings. This system, written in OCaml, is a direct implementation of two recent advances in the theory of proof search.

1. It is possible to capture both finite success and finite failure in a sequent calculus [20]. Proof search in such a proof system can capture both may and must behavior in operational semantics.
2. Higher-order abstract syntax is directly supported using term-level lambda-binders, the nabla-quantifier, higher-order pattern unification, and explicit substitutions. These features allow reasoning directly on expressions containing bound variables.

The distributed system comes with several example applications, including the finite pi-calculus (operational semantics, bisimulation, trace analysis, and modal logics), the spi-calculus (operational semantics), value-passing CCS, the lambda-calculus, winning strategies for games, and various other model checking problems.

While the system has been written to validate certain theoretic results and to help suggest new theoretical directions, we believe that the system can be of use to others interested more in reasoning about computer systems than about proof theory foundations.

Bedwyr is an open source project : its source and user manual are available online [38]. The developers behind the current distribution are :

- David Baelde and Dale Miller (INRIA and LIX/Ecole Polytechnique)
- Andrew Gacek and Gopalan Nadathur (University of Minneapolis)
- Alwen Tiu (Australian National University and NICTA).

During the summer of 2007, Baelde (LIX PhD student) and visiting intern Zachery Snow (PhD student from the University of Minnesota) built a prototype theorem prover, called *Taci*, that we are currently using "in-house" to experiment in a number of large examples and a few different logics. We hope to make the tool available eventually once we have settled into the exact logic that it should support.

Contracts

Mobius, Integrated Project in response to the call FP6-2004-IST-FETPI (September 2005 - August 2009). This proposal involve numerous site in Europe attempting to develop the proof carrying code infrastructure for mobile computer networks.

ANR Programme Blanc 2006 (Jan 2007 - Dec 2009) "INFER — Theory and Application of Deep Inference". This project aims at refining the potential of deep inference and at applying it to problems related to the foundations of logic and to more practical questions in the algorithmics of deductive systems.

[15] `http://www.lix.polytechnique.fr/~lutz/`

Slimmer, "Equipes Associées" from INRIA and funds from NSF (Jan 2005 –). Funds trips and exchanges between LIX and the University of Minnesota. The current focus of the research is on developing and implementing a formal framework for the specification of structured operational semantics of computational systems and for formally reasoning about properties of these specifications.

PAI Germaine De Staël "Deep Inference and the Essence of Proofs" (Jan 2007 - Dec 2008). Money for traveling between Paris and Bern. The participants are working on using deep inference to better understand the structure, semantics, and identity of proofs.

PAI Amadeus "The Realm of Cut Elimination" (Jan 2007 - Dec 2008). Money for traveling between Paris and Vienna. The participants are working on aspects of proof theory, particular, the analysis and uses of cut-elimination in deductive systems.

Teaching, dissemination and service

- Dale Miller was a professor at Ecole Polytechnique during 2004-2006 during which time he taught a number of introductory and advanced course on programming languages, theory of computing, and logic.
- Dale Miller, along with Roberto Di Cosmo, wrote an article on “Linear Logic” for the *Stanford Encyclopedia of Philosophy* [3].
- Lutz Straßburger gave a course at ESSLLI’06 in Malaga on *Proof nets and the identity of proofs*, and wrote lecture notes for the course, which are available as INRIA Research Report [41].
- Lutz Straßburger is teaching a course “Introduction to deep inference and proof nets” within the International Master’s programme “Computational Logic” in Dresden, December 2007.

External Evaluation for Habilitation

Miller has been an external examiner for the habilitation of Agata Ciabattoni at Technische Universität Wien, March 2007.

External Evaluation for PhD

Miller was an external evaluator for the following PhD thesis defense.

- Stéphane Lengrand, Université Paris VII & University of St Andrews, 8 Dec 2006 (examinateur).
- Nicolas Oury, LRI, University of Paris Sud, 15 September 2006 (examinateur).
- James Brotherston, LFCS, University of Edinburgh, 6 September 2006 (external examiner).
- Gabriele Pulcini, University of Rome 3, 28 April 2006 (rapporteur).
- Sylvain Salvati, Institut National Polytechnique de Lorraine, 13 June 2005 (examinateur).
- Xiaochu Qi, Computer Science Department, University of Minnesota proposal defense, 22 April 2005.
- Didier Le Botlan, INRIA-Rocquencort, École polytechnique, 6 May 2004 (examinateur).
- Sorin Craciunescu, INRIA-Rocquencort, École polytechnique, March 2004 (rapporteur).

Visibility

Dale Miller participated to the jury of habilitazion of Agata Ciabattoni, Technische Universität Wien, March 2007.

Dale Miller participated to the jury of the following phd theses : Stéphane Lengrand, Université Paris VII & University of St Andrews, 8 Dec 2006 (examinateur) ; Nicolas Oury, LRI, University of Paris Sud, 15 September 2006 (examinateur) ; James Brotherston, LFCS, University of Edinburgh, 6 September 2006 (external examiner) ; Gabriele Pulcini, University of Rome 3, 28 April 2006 (rapporteur) ; Sylvain Salvati, Institut National Polytechnique de Lorraine, 13 June 2005 (examinateur) ; Xiaochu Qi, Computer Science Department, University of Minnesota proposal defense, 22 April 2005 ; Didier Le Botlan, INRIA-Rocquencort, École polytechnique, 6 May 2004 (examinateur) ; Sorin Craciunescu, INRIA-Rocquencort, École polytechnique, March 2004 (rapporteur).

[16] http://www.lix.polytechnique.fr/~lutz/orgs/infer.html

National scientific cooperations

– Lutz Straßburger is coordinator of and ANR "blanc" *Theory and Application of Deep Inference (INFER)*[16]. Other partners are PPS (Paris 7) and the LORIA (Nancy).

International scientific cooperations

– Lutz Straßburger is coordinator of an PAI Germaine De Stael with IAM, Universität Bern. Title : *Deep Inference and the Essence of Proofs*
– Dale Miller is coordinator of an PAI Amadeus with Theory and Logic Group, Technische Universität Wien. Title : *The Realm of Cut Elimination*.
– Dale Miller is coordinator of an INRIA "Equipes Associées" Slimmer for joint work with the Univiersity of Minneapolis. This effort also involves researchers from the Australian National University and from Hofstra University (New York).
– Dale Miller is involved in the Mobius integrated project under the FET Global Computing Proactive Initiative (6th Framework program).

Conference and seminar invitations

– Lutz Straßburger was invited to present his work at the logic seminar of the University of Utrecht, Netherlands on February 22, 2007 (*On proof nets for second-order propositional multiplicative linear logic*), and at the seminar of the logic group of the University of Bath, UK on May 3, 2007 (*On the axiomatization of Boolean categories with and without medial*)
– Dale Miller was invited to present his work at the following places : IJCAR 2006 : Joint Conference on Automated Reasoning, Seattle, 16-21 August 2006 • Università di Roma Tre, 28-29 April 2006 • Algebraic Process Calculus : The first 25 years and beyond, Bertinoro, Italy, 5 August 2005 • Structure and Deduction 2005, Lisbon, 16-17 July 2005 • 2nd Taiwanese-French Conference in Information Technologies, Tainan, Taiwan, 23-25 March 2005 • CSL 2004 : 13th Annual Conference of the European Association for Computer Science Logic, Karkonoski National Park, Poland, 20-23 September 2004 • TPHOLs 2003 : International Conference on Theorem Proving in Higher Order Logics, 9-12 September 2003, Rome • Wollic 2003 : 10th Workshop on Logic, Language, Information and Computation, 29 July - 1 August 2003, Ouro Preto, Brazil • Workshop on Process Algebra, Bertinoro, Italy, 23 July 2003 • UNIF 2003 : 17th International Workshop on Unification, 8-9 June 2003, Valencia.

Conference organisation

– Miller and Straßburger organized a workshop on *Logic Programming and Concurrency*[17] from February 27 to March 3, 2006, in Marseille within the *Geometry of Computation 2006* meeting (GEOCAL06).
– Straßburger organized a small workshop on *The Realm of Cut Elimination*[18] on May 14, 2007, at LIX.
– Straßburger organized a small workshop on *Theory and Application of Deep Inference*[19] on June 21, 2007.

Program committees

Miller has been on the program committees of the following meetings.

2007 LFMTP'07 : Workshop on Logical Frameworks and Meta-Languages : Theory and Practice, August, Bremem, Germany. • WoLLIC'07 : Fourteenth Workshop on Logic, Language, Information and Computation, Rio de Janeiro, 2-5 July. • CADE-21 : 21st Conference on Automated Deduction, 17 - 20 July Bremen, Germany.

2006 FSTTCS'06 : Foundations of Software Technology and Theoretical Computer Science, Kolkata, India. 13-15 December. • LPAR-13 : 13th International Conference on Logic for Programming Artificial Intelligence and Reasoning, Phnom Penh, Cambodia. 13-17 November. • LFMTP'06 : Workshop on Logical Frameworks and Meta-Languages : Theory and

[17] http://www.lix.polytechnique.fr/~lutz/orgs/lpc_geocal06.html
[18] http://www.lix.polytechnique.fr/~lutz/orgs/amadeus2007.html
[19] http://www.lix.polytechnique.fr/~lutz/orgs/INFERmeetingJune2007.html

Practice, 16 August. • TFIT'06 : Taiwanese-French Conference on Information Technology, Nancy, France. 28-30 March. • Geocal Workshop on Logic Programming and Concurrency, 27 February - 3 March, CIRM, Luminy, France (Program Committee co-Chair)

2005 MoVeLog'05 : A Workshop on Mobile Code Safety and Program Verification Using Computational Logic Tools. Barcelona, Spain, 5 October. • LPAR-11 : 11th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning. Montevideo, Uruguay, 14-18 March • CSL05 : 14th Annual Conference of the European Association for Computer Science Logic, 22-25 August, Oxford, UK • CADE-20 : Conference on Automated Deduction, Tallinn, Estonia, 22-27 July.

2004 ICLP'04 : Twentieth International Conference on Logic Programming, Saint-Malo, France, 6-9 September. • LFM04 : Fourth International Workshop on Logical Frameworks and Meta-Languages.

Journal editorial boards

Miller has the following editorial duties.

- *ACM Transactions on Computational Logic* (TOCL). Area editor for *Proof Theory*. Published by ACM. Since 1999.
- *Journal of Applied logic*, published by Elsevier. Since 2003.
- *Journal of Functional and Logic Programming*, published by European Association for Programming Languages and Systems (EAPLS). Permanent member of the Editorial Board. Since 1996.
- *Journal of Logic and Computation*, published by Oxford University Press. Associate editor. Since 1989.
- *Theory and Practice of Logic Programming*, published by Cambridge University Press. Editorial Advisor. Since 1999.
- *Journal of Logic Programming*, published by Elsevier Science. Editorial Advisor. 1990 – 1999.

References

Books and chapters in books

2004

[1] MILLER, D. Overview of linear logic programming. In *Linear Logic in Computer Science*, T. Ehrhard, J.-Y. Girard, P. Ruet, and P. Scott, Eds., vol. 316 of *London Mathematical Society Lecture Note*. Cambridge University Press, 2004, pp. 119 – 150.

[2] MILLER, D., AND PIMENTEL, E. Linear logic as a framework for specifying sequent calculus. In *Logic Colloquium '99 : Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic*, J. van Eijck, V. van Oostrom, and A. Visser, Eds., Lecture Notes in Logic. A K Peters Ltd, 2004, pp. 111–135.

2006

[3] DICOSMO, R., AND MILLER, D. Linear logic. In *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed. Stanford University, 2006.

International journals

2005

[4] MILLER, D., AND TIU, A. A proof theory for generic judgments. *ACM Trans. on Computational Logic 6*, 4 (Oct. 2005), 749–783.

2006

[5] LAMARCHE, F., AND STRASSBURGER, L. From proof nets to the free *-autonomous category. *Logical Methods in Computer Science 2*, 4 :3 (2006), 1–44.

[6] STRASSBURGER, L. On the axiomatisation of Boolean categories with and without medial, `http://arxiv.org/abs/cs.LO/0512086`, 2006. To appear in Theory and Applications of Categories.

2007

[7] CHAUDHURI, K., PFENNING, F., AND PRICE, G. A logical characterization of forward and ba-

ckward chaining in the inverse method. J. of Automated Reasoning, June 2007.

[8] STRASSBURGER, L. On the axiomatisation of Boolean categories with and without medial, 2007. Accepted for publication in *TAC*.

International conferences with proceedings

2004

[9] GABBAY, M. J., AND CHENEY, J. A sequent calculus for nominal logic. In *Proc. 19th IEEE Symposium on Logic in Computer Science (LICS 2004)* (2004), pp. 139–148.

[10] MILLER, D. Bindings, mobility of bindings, and the ∇-quantifier. In *18th International Workshop CSL 2004* (2004), J. Marcinkowski and A. Tarlecki, Eds., vol. 3210 of *LNCS*, p. 24.

[11] STRASSBURGER, L., AND LAMARCHE, F. On proof nets for multiplicative linear logic with units. In *Computer Science Logic, CSL 2004* (2004), J. Marcinkowski and A. Tarlecki, Eds., vol. 3210 of *LNCS*, Springer-Verlag, pp. 145–159.

[12] TIU, A., AND MILLER, D. A proof search specification of the π-calculus. In *3rd Workshop on the Foundations of Global Ubiquitous Computing* (Sept. 2004), vol. 138 of *ENTCS*, pp. 79–101.

2005

[13] LAMARCHE, F., AND STRASSBURGER, L. Constructing free boolean categories. In *20th IEEE Symposium on Logic in Computer Science (LICS 2005)* (2005), IEEE Computer Society, pp. 209–218.

[14] LAMARCHE, F., AND STRASSBURGER, L. Naming proofs in classical propositional logic. In *Typed Lambda Calculi and Applications, TLCA 2005* (2005), P. Urzyczyn, Ed., vol. 3461 of *LNCS*, Springer-Verlag, pp. 246–261.

[15] MILLER, D., AND SAURIN, A. A game semantics for proof search : Preliminary results. In *GaLoP 2005 : Games for Logic and Programming Languages* (2005), D. Ghica and G. McCusker, Eds.

[16] MILLER, D., AND SAURIN, A. A game semantics for proof search : Preliminary results. In *Proceedings of the Mathematical Foundations of Programming Semantics (MFPS)* (2005).

[17] PIMENTEL, E., AND MILLER, D. On the specification of sequent systems. In *LPAR 2005 : 12th International Conference on Logic for Programming, Artificial Intelligence and Reasoning* (2005), no. 3835 in LNAI, pp. 352–366.

[18] SAURIN, A. Separation with streams in the $\lambda\mu$-calculus. In *20th IEEE Symposium on Logic in Computer Science (LICS 2005)* (2005), IEEE Computer Society, pp. 356–365.

[19] SAURIN, A. Typing streams in the $\Lambda\mu$-calculus : extended abstract. short paper accepted to LPAR 2007, october 2005.

[20] TIU, A., NADATHUR, G., AND MILLER, D. Mixing finite success and finite failure in an automated prover. In *Proceedings of ESHOL'05 : Empirically Successful Automated Reasoning in Higher-Order Logics* (December 2005), pp. 79 – 98.

[21] ZIEGLER, A., MILLER, D., AND PALAMIDESSI, C. A congruence format for name-passing calculi. In *Proceedings of SOS 2005 : Structural Operational Semantics* (Lisbon, Portugal, July 2005), Electronic Notes in Theoretical Computer Science, Elsevier Science B.V., pp. 169–189.

2006

[22] LEAVENS, G. T., ABRIAL, J.-R., BATORY, D., BUTLER, M., COGLIO, A., FISLER, K., HEHNER, E., JONES, C., MILLER, D., PEYTON-JONES, S., SITARAMAN, M., SMITH, D. R., AND STUMP, A. Roadmap for enhanced languages and methods to aid verification. In *Fifth International Conference on Generative Programming and Component Engineering (GPCE)* (Oct. 2006), ACM, pp. 221–235.

[23] MILLER, D. Collection analysis for Horn clause programs. In *Proceedings of PPDP 2006 : 8th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming* (July 2006), pp. 179 – 188.

[24] MILLER, D. Representing and reasoning with operational semantics. In *Proceedings of IJ-*

CAR : International Joint Conference on Automated Reasoning (Aug. 2006), U. Furbach and N. Shankar, Eds., vol. 4130 of *LNAI*, pp. 4–20.

[25] MILLER, D., AND SAURIN, A. A game semantics for proof search : Preliminary results. In *Proceedings of the Mathematical Foundations of Programming Semantics (MFPS05)* (2006), no. 155 in Electr. Notes Theor. Comput. Sci, pp. 543–563.

[26] STRASSBURGER, L. What could a boolean category be ? In *Classical Logic and Computation 2006 (Satellite Workshop of ICALP'06)* (2006), S. van Bakel, Ed.

2007

[27] BAELDE, D., GACEK, A., MILLER, D., NADATHUR, G., AND TIU, A. The Bedwyr system for model checking over syntactic expressions. In *21th Conference on Automated Deduction* (2007), F. Pfenning, Ed., no. 4603 in LNAI, Springer, pp. 391–397.

[28] BAELDE, D., AND MILLER, D. Least and greatest fixed points in linear logic. vol. 4790 of *LNCS*, pp. 92–106. LPAR07 : Logic for Programming, Artificial Intelligence, and Reasoning.

[29] LIANG, C., AND MILLER, D. Focusing and polarization in intuitionistic logic. In *CSL 2007 : Computer Science Logic* (2007), J. Duparc and T. A. Henzinger, Eds., vol. 4646 of *LNCS*, Springer-Verlag, pp. 451–465.

[30] MILLER, D., AND NIGAM, V. Incorporating tables into proofs. In *CSL 2007 : Computer Science Logic* (2007), J. Duparc and T. A. Henzinger, Eds., vol. 4646 of *LNCS*, Springer-Verlag, pp. 466–480.

[31] MILLER, D., AND SAURIN, A. From proofs to focused proofs : a modular proof of focalization in linear logic. In *CSL 2007 : Computer Science Logic* (2007), J. Duparc and T. A. Henzinger, Eds., vol. 4646 of *LNCS*, Springer-Verlag, pp. 405–419.

[32] STRASSBURGER, L. A characterisation of medial as rewriting rule. In *Term Rewriting and Applications, RTA'07* (2007), F. Baader, Ed., vol. 4533 of *LNCS*, Springer-Verlag, pp. 344–358.

[33] STRASSBURGER, L. Deep inference for hybrid logic. In *International Workshop on Hybrid Logic 2007 (Part of ESSLLI'07)* (2007).

PhD Thesis

2004

[34] TIU, A. *A Logical Framework for Reasoning about Logical Specifications*. PhD thesis, Pennsylvania State University, May 2004.

Miscellaneous

2004

[35] TIU, A. *Level 0/1 Prover : A tutorial*, September 2004. Available online.

[36] ZIEGLER, A. Un format pour que la bisimulation soit une congruence dans les langages de processus avec mobilité. Tech. rep., INRIA Futurs, LIX and ENS, 2004.

2005

[37] BAELDE, D. Logique linéaire et algèbre de processus. Tech. rep., INRIA Futurs, LIX and ENS, 2005.

2006

[38] BAELDE, D., GACEK, A., MILLER, D., NADATHUR, G., AND TIU, A. *A User Guide to Bedwyr*, November 2006.

[39] LIANG, C., AND MILLER, D. On focusing and polarities in linear logic and intuitionistic logic. Unpublished report, December 2006.

[40] MILLER, D. Logic and logic programming : A personal account. ALP Newsletter, February 2006. Vol. 19, No. 1.

[41] STRASSBURGER, L. Proof nets and the identity of proofs. Research Report 6013, INRIA, `https://hal.inria.fr/inria-00107260`, Oct. 2006. Lecture notes for ESSLLI'06.

2007

[42] BAELDE, D., AND MILLER, D. Least and greatest fixed points in linear logic : extended version. Technical report, available from the first author's web page, http://www.lix.polytechnique.fr/~dbaelde/productions/pool/mumall_draft_long.pdf, April 2007.

LogiCal
Logique et Calculs

Team members

Team leader

Benjamin WERNER, chargé de recherches INRIA, professeur chargé de cours à l'école Polytechnique

Permanent members

- Gilles DOWEK, professeur à l'école Polytechnique
- Jean-Pierre JOUANNAUD, professeur à l'Université Paris-Sud, on leave from september 2006
- Bruno BARRAS, chargé de recherches INRIA
- Hugo HERBELIN, chargé de recherches INRIA
- Assia MAHBOUBI, chargé de recherches INRIA (at LIX since september 1st 2007)
- Ian MACKIE, chargé de recherches CNRS
- Jean-Marc NOTIN, Ingénieur de recherches CNRS (since 1st december 2005)
- Benjamin WERNER, chargé de recherches INRIA, professeur chargé de cours à École Polytechnique.

Phds

- Lisa ALLALI, région IdF, since december 2006
- Bruno BERNARDO, DGA, since august 2006
- Mathieu BOESPFLUG, AMN, from september 2007
- Denis COUSINEAU, MERT, since september 2006
- Olivier HERMANT, MERT, until 2005
- Florent KIRCHNER, École Polytechnique, until august 2007
- Sylvain LEBRESNE, MERT, since october 2005
- Jullien NARBOUX, MERT, until 2006
- Elie SOUBIRAN, MERT, since september 2006
- Vincent SILÈS, AMN, since september 2007
- Francois-Régis SINOT, École Polytechnique, until april 2006
- Arnaud SPIWACK, AMN (Cachan), since sep-

tember 2006
- Pierre-Yves STRUB, EADS, since february 2005
- Roland ZUMKELLER, MERT, since october 2004.

PostDocs

- Gyesik LEE, 2006-2007 (18 months)
- Evgeny MAKAROV, 2007 (12 months)
- Weiwen XU, 2004-2005 (12 months).

Interns

- Lisa ALLALI, ENS Cachan, from march 2006 til september 2006
- Bruno BERNARDO, École Polytechnique, from march 2006 til august 2006
- Christophe CALVÈS, from march 2007 til august 2007
- Denis COUSINEAU, Université Paris 7, from march 2006 til august 2006
- François GARILLOT, from march 2007 til august 2007
- Danko ILIK, from may 2006 til august 2006
- Elie SOUBIRAN, Université Paris 7, from march 2006 til august 2006
- Vincent SILÈS, ENS Lyon, from march 2007 til august 2007
- Arnaud SPIWACK, ENS Cachan, from march 2006 til august 2006.

Guests

Professor Femke van Raamsdonk from Amsterdam visited us for one month in 2005. Professor Makoto Tatsuta from NII visited us for one month in 2006. Benjamin Wack, phd from Protheo, visited 3 months in 2006.

Research domain

The team's objective is to enhance tools for formal reasoning and the mechanical checking of mathematical reasoning. This is a long term effort which materializes mainly through the development of the Coq proof system.

Mechanically checked proofs give a very high, if not the highest, degree of certitude of correctness for a mathematical argument. This is especially important when assessing the accuracy of a critical piece of soft- or hardware. Indeed, Coq is used to this extent by various teams, in industry or research, in France or abroad. Our effort aims therefore at guaranteeing the reliability and security of software-prevalent systems.

At the origin of our approach lies the idea that the choice of the logical formalism is crucial for building a proof system that is at the same time practical and clearly implemented. In our view, a proof system implements a formalism quite in the same way a compiler/programming environment implements a programming language. A formalism should not only be expressive, but also yield formal proofs that are as concise as possible, allow the user to stick to mathematical intuition, and be well suited for automation.

In this regard, a point which we have particularly focused on in the last ten years is the interaction between deduction and computation steps. In type theory, the mathematical objects are fundamentally typed functional programs. As such, they have a built-in notion of computation ; the crucial point is that the objects are logically identified modulo computation. In some cases, this can allow dramatic shortcuts in the proofs, thus pushing further the frontier of the statements that are within grasp of formal systems. Our special interest in this point is the reason for the name of the project.

Because we view the formalism as essential for the practical tool, and because Coq's formalism is still evolving, we are careful to also have an important research activity in proof theory, especially on topics related to formal proofs.

More generally, we believe there is a need for "general purpose" proof systems which can be used for purely mathematical formalizations and more applied work in the computing world. In the latter case, the proof system can sometimes be used by itself, and sometimes in combination with more specialized tools. For instance, Coq can be used as a back-end for Why or Krakatoa, tools supporting program verification, which are developped by the INRIA project PROVAL, an outspring of LogiCal located at INRIA-Futurs. In the former case, the proof system is mostly used by itself. In particular, we use it ourselves for developping various mathematical formalizations, sometimes in collaboration with the MSR-INRIA laboratory located nearby.

Goals

Our broad objective is to contribute to the use of formal methods in computer science, computer industry and mathematics. Specifically, we want Coq to remain one of the main competitors in the field of proof systems. We have an edge over the competition through the ability of Coq to intertwin efficient computations with deduction. We want to deepen this strength by enhancing further Coq's computing abilities, and by contributing to, and federating the effort for providing large and usable libraries for the system.

Results

Formalization of real mathematics

Project-team positioning

In the past years, formalization of "pure" mathematics, or mathematics for themselves, was not considered central to the team's activities : the work on the system itself on one hand, and on program certification technologies on the other were viewed as the top priorities. Since the separation of the project into two, LOGICAL at LIX and ProVal at LRI, it seemed reasonable to address this issue again inside the team.

Four-color theorem

The full formalization of the proof of the four color theorem (finished dec. 2004) attracted a lot of attention, including by non-scientific or popular science media. The main author was Georges Gonthier [105], now at Microsoft Research in Cambridge, but a lot of the work was carried on in collaboration with Benjamin Werner. It seems also clear that Coq gained a lot of visibility thanks to this result. Also, the fact that this proof requires a lot of computing power was a strong motivation for integrating Benjamin Grégoire's compiler into Coq.

The proof of the four color theorem is probably the most complex formal proof as of today. It follows the general outline of an informal proof of 1995 by Robertson et. al. Its achievement took more than five years. In addition to quite complex programs to check the reducibility of the 633 configurations, the full formalization involved a discrete formalization of graphs based on hypermaps. An important side effect of this work are inovating additions to Coq's tactic language and new techniques for formalization ; both are now energically promoted by Georges Gonthier and further developped and used inside the INRIA-MSR joint laboratory.

Primality proofs

The fact that a (large) number is prime is typically assessed through computations. It was therefore tempting to test the new computing power of Coq by looking at primality proofs. Together with Benjamin Grégoire and Laurent Théry (Sophia-Antipolis), Benjamin Werner used formal results on Pocklington's criteria in order to prove the primality of numbers of up to 1000 decimal digits. This is an order of magnitude larger than what had been done before, and probably than what can be done is all or almost all other proof systems. Currently, this is done by generating Pocklington certificates with a dedicated C program, these certificates being then checked inside Coq.

The Kepler conjecture

The work on the four color theorem raised the attention of Thomas Hales : he had completed the first proof of the four-hundred years old Kepler Conjecture[20] and had difficulties to have it published because the proof, in addition of being long and complex, relied heavily on machine computations. The programs involved being quite complex, the referees felt they could not form a strong enough opinion about this part.

Since then, Hales has become a strong proponent of formal proofs and has undertaken an (administratively) unformal effort to formalize his proof. He named this effort *Flyspeck.*

Roland Zumkeller participates to Flyspeck under the supervision of Benjamin Werner. He concentrates on a part of the proof which is well-suited to Coq's computing abilities and which is also interesting in regard to other applications. It mainly consists of using optimization techniques to solve complicated real inequalities automatically.

Interestingly, the computational techniques involved come from very different fields like theoretical physics (physicists do not want particles to crash into

[20]The Kepler conjecture states that the intuitive close packings (either cubic or hexagonal close packing, both of which have maximum densities of $\pi/(3\sqrt{2})$) are the densest possible sphere packings.

the walls of their accelerator) or robotics (when calculating the force necessary for a certain movement). This also means that this work should be interesting for other purposes than just very abstract mathematics.

Currently, Roland Zumkeller has implemented the main routines for the matter in Coq [47] and now works on their correctness proof.

Geometry

Julien Narboux formalized the first 8 chapters of Schwabhäuser, Szmielev and Tarski's book on Tarski's geometry, thus providing a solid basis for further development in geometry. He also certified the Chou-Gao-Zhang area method for deciding affine geometry. He then used this when building the newly released software GEOPROOF. This is a graphical interface to draw geometry statements and to solve them, automatically or interactively, in Coq. This is a promising tool as it constitutes the first experiment making a geometry software and a proof assistant working together. This experiment opens the door to various domain-specific graphical methods of proof. A typical domain is diagrammatic reasoning in abstract rewriting for which Julien Narboux gave an original characterization of the class of graphically provable statements.

Results in logic : Executive summary

Scientific achievements

The work on relations between set theory and type theory has been one of the active research topics of Alexandre Miquel, a former student of our group, now member of the lab "Proofs, Programs and Systems" at the University of Paris 7. However, LOGICAL has been active in this area as Gilles Dowek and Alexandre Miquel have carried out a joint work on the expression of Zermelo set theory in Deduction modulo. This work has lead to another, on relative normalization proofs (*i.e.* proofs of theorems of the form "If the theory T1 has a (omega-) model, then the theory T2 has the normalization property").

On the characterization of theories that can be expressed in Deduction modulo with computation rules only, the work has been mostly focused on arithmetic : several successive presentations of arithmetic in this framework have been proposed. The first by Gilles Dowek and Benjamin Werner used an infinite number of rules. A second one proposed by Florent Kirchner, uses only a finite number of rules. And a third one, taking advantage of the decidability of equality in arithmetic, has been proposed by Lisa Allali in her Master thesis. The negative results in this area are still anecdotical.

Three other lines of research have emerged during this four year period. The first is the use of model theoretic methods to prove cut elimination results in Deduction modulo. In his Doctoral dissertation, Olivier Hermant has unified several classical and intuitionistic model theoretical cut elimination proofs. More importantly, he has given methods to prove cut elimination for theories that do not have the normalization property, refuting the conjecture that cut elimination and normalization were equivalent in Deduction modulo. This work is now merging with another approach followed by Gilles Dowek based on a generalization of the notion of Heyting algebra that allows to give model theoretic proofs both for normalization and for cut elimination.

The second new direction is an extension of the work of Jean-Pierre Jouannaud and Frédéric Blanqui on extension of Pure Type Systems with rewrite rules. Gilles Dowek and Denis Cousineau have proved that even when we restricted the type system to the simplest allowing dependent types (the lambda-Pi-calculus), then all functional and normalizing Pure Type Systems (such as the Calculus of Constructions) could be expressed with rewrite rules. Alexandre Miquel, from the lab "Proofs, Programs and Systems" has shown that Zermelo set theory could also be expressed in lambda-Pi-modulo. Jean-Pierre Jouannaud, in collaboration with Albert Rubio from Barcelona, has described new automable techniques for proving the strong normalization property of higher-order calculi based on rewrite rules.

A third, related new direction initiated by Jean-Pierre Jouannaud and Frédéric Blanqui, a former member of LOGICAL now at INRIA-Lorraine, is the use of decision procedures as blackboxes instead of rewrite rules for extending Pure (and impure) Type Systems. This mecanism appears to be very powerful, as the decision procedure is invoked with all relevant assumptions that appear in the proof context. Because decision procedures may not be trustable, theyb are assumed they come along with a mecanism for generating certificates that can then be checked inside

Coq. This work constitutes the phd thesis of Pierre-Yves Strub to be defended at the beginning of 2008.

Danko Ilik and Hugo Herbelin have recently started a Coq definition of an algorithm transforming potential contradiction proofs in ZFC to contradiction proofs in ZF. This promising work has been interrupted at the end of Danko Ilik's internship.

Benjamin Wack, from Loria, has spent three month in our group, working with Gilles Dowek on the relation between Deduction modulo and supernatural deduction.

We have a traditional interest in logically founded new computation paradigms. Dan Hernest Mircea has obtained new understandings on the computational behavior of Gödel's Dialectica (common PhD with Münich). François-régis Sinot completed his PhD about implementation oriented variants of λ-calculus with named variables.

The development of the Coq system

Personnel

Bruno Barras, Hugo Herbelin, Jacek Chrząszcz (PhD until 2003), Benjamin Grégoire (PhD until 2003), Clément Renard (PhD interrupted in 2005), Julien Narboux (PhD ended in 2006), Florent Kirchner (PhD), Sylvain Lebresne (PhD), Claudio Sacerdoti Coen PostDoc 2004-05), Pierre-Yves Strub (PhD), Pierre Castéran (on secondment from LaBRI 2004-2005), Jean-Marc Notin (from December 2005).

Personnel from other INRIA teams and other academic sites have also contributed to the development of the Coq system : Christine Paulin (ProVal), Jean-Christophe Filliâtre (ProVal), Pierre Letouzey (ProVal and Paris 7), Claude Marché (ProVal), Pierre Corbineau (ProVal), Pierre Courtieu (ProVal, CNAM), Nicolas Ayache (ProVal), Matthieu Sozeau (ProVal), Benjamin Monate (ProVal), Yves Bertot (Marelle), Laurent Théry (Marelle), Julien Forest (ProVal, Everest), Assia Mahboubi (Marelle, now LOGICAL).

The set of persons implied in the development of Coq, inside or outside of LOGICAL, is collectively designed as *the Coq development team*.

The Coq system is born from the work of Gérard Huet and Thierry Coquand on the logical formalism known as the Calculus of Construction [80]. The main characteristic of this formalism is that it is both a logical foundation of mathematics and a programming language. First implemented in 1984, the Coq system is a software of the kind of "proof assistant", following a terminology made popular at the beginning of the 90's. Coq includes a proof checker but it is specially designed for interactive development of proofs, an approach pioneered by Milner's LCF system [79]. Along these lines, it differs from the historical style of proof checking that Boyer and Moore initiated.

In 1990, the logic of Coq has been extended to the Calculus of Inductive Constructions, a purely constructive formalism (i.e. with no axioms) of a strength comparable to set theory.

Twenty-two years after the first implementation started, Coq is one of the top 7 proof assistants in the world. To our knowledge, the main competitors are : ACL2, a texan proof checking system derived from the original Boyer and Moore's system that is largely used in the industry, especially for circuit verification ; HOL, a largely used Cambridge-made proof assistant derived from Milner's LCF system ; HOL-light, a variant version of HOL used both for the formalisation of mathematics and for circuit verification ; Isabelle, a joint Cambridge-Munich proof assistant that is largely used by academics and industry, for both mathematical formalisation and program verification (especially JavaCard programs) ; PVS, a product from SRI that is also largely used for program verifications.

We also have to cite Mizar, a proof assistant designed for the formalisation of mathematics in set theory and which certainly currently has the largest database of formal mathematics.

There are also systems of smaller audiences focusing on more specific and experimental features. In our community typical examples include the Swedish Alfa/Agda and the English Epigram, both based on "improvements" of the language of Coq ; the PhoX system, developed in Chambéry with a focus on teaching.

Interestingly enough, a challenging proof assistant based on the same language as Coq is under development at the university of Bologna. This experimental proof assistant, called MATITA, is an opportunity for testing alternative approaches in the design of some of the Coq features. We have a strong collaboration with the development team of Matita. We were part of a common european project MoWGLI and one of the main implementors, Claudio Sacerdoti Coen was a post-doc in LOGICAL.

The main feature of Coq compared to most of its competitors is that it includes an expressive typed pro-

gramming languages and that reasoning is done modulo evaluation of programs.

Coq's underlying formalism is logically powerful and computationally expressive but this is not the only strength of Coq. The trusted computing base of Coq, i.e. the part that checks that the proof is a correct, is relatively small (15000 lines of Objective Caml code while the whole system has 120000 lines of Objective Caml code + 65000 lines of libraries written in the own language of Coq). Moreover, Coq produces proof objects that could possibly be verified by independent proof checkers.

LOGICAL is the leading team for the development of Coq but the development of Coq is not restricted to the personnel of LOGICAL. Former PhD students from LOGICAL, such as Benjamin Grégoire, or from ProVal, such as Pierre Letouzey, Pierre Courtieu, Pierre Corbineau and Julien Forest still provide contributions to Coq. There is also a long-standing collaboration with Marelle (ex-Lemme) that resulted in the last four years to the integration of contributions from Yves Bertot, from Assia Mahboubi, and from Laurent Théry.

As a tool, Coq is used by different teams, especially in Sophia-Antipolis and in the context of the INRIA-Microsoft Research joint centre.

Scientific achievements

In the last four years, the Coq development team released three major new versions. In the list below, the main achievements delivered by these releases are highlighted.

- Coq version 7.4 (February 2003)
  This version provided a higher order module system à la ML. This has been the result of a long process of maturation, starting from the purely logical study of a module system by Judicaël Courant [81] to the implementation by Jacek Chrząszcz [90] of a "real-life" module system that also takes care of the numerous non-logical aspects of Coq.
- Coq version 8.0 (April 2004)
  This version is a major release. First, it provided a new syntax that we believe to be more intuitive and that allows for much richer notations, including the standard arithmetical operations. Indeed, after 20 years of evolution and maturation, the concrete syntax had become clumsy and with so few degrees of freedom that reasonable extensions were impossible.
  The change of syntax has been performed in coordination with Pierre Castéran and Yves Bertot while they were writing their book on the practical uses of Coq (the Coq'Art [100]). A few minimal changes in the standard library have also been performed so that it gets a better uniformity.
  Secondly, the underlying formalism has been slightly weakened in order to make it logically compatible with standard axioms used by mathematicians such as the axiom of choice and classical logic. This change is basically a two lines change in the implementation but it opens the door to a much larger spectrum of mathematical theories to be formalized in Coq without leading to logical paradoxes as it was the case with the *strongly intuitionistic* logic implemented in the previous versions.
  In addition to these two points which motivated the change of the major version number, Coq 8.0 came with an integrated graphical interface developed by members of the ProVal INRIA team. This new interface improved on the previous through its simplicity of use and by more efficient error location. Especially, it sped up significantly the starting period for Coq's beginner, as we could observe it in the classes on Coq that the members of the team were in charge of.
  Finally, many small extensions were made by members of the team, most noticeably tactics (proof methods), searching tools, and various other features convenient in a daily use.
- Coq version 8.1 (beta release in June 2006)
  This version adds many novelties realized by members of the team.
  The most striking achievement is Benjamin Grégoire's compiler for the Coq programming language [87]. Based on Objective Caml's abstract machine which was extended in order to also perform strong reduction, it provided a very important speed up for formal applications that relies on intensive computation (e.g. the four color theorem, primality proofs, Coq tactics written in the Coq language – the reflection mechanism).
  Another achievement, by Pierre Corbineau, is the development of a decision procedure for first-order arithmetic [24] that works uniformly

on a generic notion of connectives and quantifiers (the only primitive of Coq is universal quantification – all others connectives and quantifiers can occur in arbitrary and possibly non standard ways : that is what the decision procedure recognizes).
A third achievement done by Claudio Sacerdoti Coen during his postdoc in LOGICAL is the development of a powerful mechanism for rewriting over arbitrary relations [23].
Otherwise, the underlying theory has been made smoother. Hugo Herbelin added sort-polymorphism for inductive types. Christine Paulin (ProVal) added recursively non uniform inductive parameters.
Many outside contributions have been integrated : Pierre Corbineau, as a postdoc in Nijmegen developed a mathematical style of proof for Coq in the spirit of Mizar's style of formalization ; Benjamin Grégoire (as a member of Everest) and Assia Mahboubi (Marelle), with the help of Bruno Barras, contributed an improved implementation of the simplification procedure on rings ; Laurent Théry (Marelle) with the help of Bruno Barras, contributed a library on strings and an improved implementation of the simplification procedure on fields ; Jean-Christophe Filliâtre (ProVal) and Pierre Letouzey (ProVal and University Paris 7) contributed a certification of Objective Caml libraries on maps and sets ; Pierre Letouzey also contributed a library on rational numbers ; Pierre Courtieu (CNAM), Julien Forest (Everest and CNAM) and Yves Bertot (Marelle), in paper collaboration with Gilles Barthe (Marelle) and David Pichardie (Everest) contributed tools for reasoning over the structure of recursive functions ; Matthieu Sozeau (ProVal) contributed a sub-language of Coq with subtyping and proof obligations ; Frédéric Blanqui (Protheo) contributed a library called Color for performing termination proofs of rewrite programs which has won a competition organized at the last IJCAR.
Another feature, of limited originality but promising consequences, is the implementation by Hugo Herbelin, Jean-Christophe (ProVal) and Nicolas Ayache (ProVal) of mechanisms to allow Coq to call external provers or computer algebra systems.

Collaborations of the Coq development team

The team has strong interactions with the INRIA teams Protheo, ProVal, Marelle and Everest to enhance Coq's developments, and with the University of Bordeaux, especially Pierre Castéran who wrote the Coq'Art book with Yves Bertot. This book has had a large success and has contributed to the success of Coq in the last years.

External support for Coq

The european project MoWGLI provided support for web-based searching and browsing of mathematical libraries (work led by the University of Bologna in collaboration with the University of Nijmegen and Sophia-Antipolis).

The european TYPES working group.

The EADS Foundation.

Self assessment

In the last four years, Coq has, as expected, gained in speed (thanks to the internal compiler) and in automation (new decision procedures and possibility to connect external provers). It also gained in extensibility and opening onto the outside tools.

The work on libraries that was anticipated four years ago has been partially realized in Coq version 8.0 but a lot more needs to be done to get a uniform library that could serve as a solid basis for the foundation of formal mathematics.

Coq is not only used worldwide but its development becomes more and more multi-site. We believe that this is something our team can be proud of. However, according to the blind publication-based evaluation mechanism, the main developers and maintainers of Coq did not manage to valorize their work. And still, documentation (to cite one possible way of being refered to) is missing on many aspects of the system.

Valorization and technology transfer

Coq is or has been used, among others by :
- Trusted Logic (prosperous company doing software certification)
- Gemalto (worldwide leader in smartcards)
- France-Telecom
- Various teams working themselves on the transfer of technologies like proo-carying code

– Microsoft Research (in addition to the activities in the joint lab)

Academic impact

It is difficult to estimate the number of users of Coq in academia. However, we know of at least 10 INRIA Project/Teams using the system in an important way. Outside École Polytechnique, Coq is used for teaching purposes in Nancy, Warsaw and Taipei to name a few.

The Coq mailing list has 450 members ; most in academia.

Software, patents and contracts

Software

Coq

The Coq proof-system is the main material output of the team's work. It is distributed under LGPL license and largely described above.

Geometrica

Julien Narboux's GeoProof is now distributed under GPL.

Contracts

– Title : Complexité en ressources de programmes embarqués efficaces
Period : 01-12-2003 au 30-11-2006
Type : with France Telecom
Object : developping a new kernel for Coq allowing for better automation.

– Title : Dévelopement d'un langage de programmation pour la preuve formelle
Period : 01/02/2004 - 31/01/2007 ;
Type : with EADS Foundation ;
Object : funding the Phd of Pierre-Yves Strub.

Teaching, dissemination and service

Teaching

– Jean-Pierre Jouannaud teached until 2006 at Orsay (Licence, ca. 50 hours), Polytechnique (20 hours) and Master (20 hours).

– Gilles Dowek teaches at undergraduate and master's lever at Ecole polytechnique (30 hours for the latter).
– Benjamin Werner teaches at master (20 hours) and gave a course on Coq and Caml at ENSTA (20 hours).
– Hugo Herbelin and Bruno Barras teach in master (between 20 and 10 hours)

The master courses are all in MPRI (Master Parisien de Recherche en Informatique) which is the major way of recruting new PhD students.

Dissemination

Benjamin Werner and/or Gilles Dowek have been cited by, among others, La Recherche, Science et Vie, le Télégramme de Brest, New Scientist, Le Figaro, Le Monde on topics concerning the four color theorem's proof, the INRIA-Microsoft Research joint centre or Gilles Dowek's recent book.

Benjamin Werner and Gilles Dowek gave also separate interviews on Radio-France Inernational in 2007.

Service

– Gilles Dowek is Vice-Chair of the Department of Computer Science at École Polytechnique.
– Jean-Pierre Jouannaud has been the director of LIX since januray 1st, 2001.
– Jean-Pierre Jouannaud has been a member of the council of European Association for Theoretical Computer Science from 2001 to 2007, and the president of its french chapter from 1999 to 2006.
– Jean-Pierre Jouannaud has been a member of the Jury awarding the EATCS Price for lifetime achievement (2003-2005) ; He is a member of the jury of the Gödel price (2007-2009).
– Jean-Pierre Jouannaud has been a member of the Irish Science Foundation panel (computer science section) for the Stokes Chairs program.

Visibility

National scientific cooperations

– Modulogic (7,5 k euros) is an INRIA-ARC common with Protheo (Nancy) and Focal (U. Paris 6). It concerns investigation of how to

make software specification as modular as possible.
- MAO is an INRIA-ARC common with André Hirschowitz' team of algebraic geometry in Nice. It is about making Coq more attractive and well-suited for the needs of mathematicians.
- Several researchers from LOGICAL participate to the project *mathematical Components* based on Coq carried out at the INRIA-Microsoft Research joint centre.

International scientific cooperations

- The TYPES european working group is very important to us ; much more than through the funding. It is concerned by using types and type theory for formal proofs, proof systems and safe programming. Budget run by LOGICAL : 60 k euros.
- MOWGLI was a european project to help the construction of formal mathematics on the web.
- We collaborate with Jose Meseguer's team from the University of Illinois at Urbana Champaign on *rewriting logic*. This collaboration is funded by a billateral contract between the UIUC and CNRS.
- We collaborate with Pawel Urzyczyn's team from Warsaw University on type theory and Coq. This collaboration is funded by a contract of the Ministère des Affaires Étrangères.
- We also have informal collaborations with the research teams at the Universities of Amsterdam, Bologna, Catalogna, Nijmegen, Keio among others, and with NASA.

Conference and seminar invitations

- Gilles Dowek gave invited presentations at .
  Gilles Dowek gave a series of conferences organised by *Alliance Française* in the indian IT's in 2006.
- Hugo Herbelin gave invited presentations at Classical Logic and Computation, a satellite workshop of ICALP, Venice, Italy, 2006 ; Higher Order Rewriting, a satellite workshop of FLOC at Seattle, USA, 2006.
- Jean-Pierre Jouannaud gave invited presentations at the 2nd International Symposium on Automated Technology for Verification and Analysis, Taipei, Taiwan, 2004 ; the 9th Artificial Intelligence Conference, Taipei, Taiwan, 2004 ; the International Conference on Rewriting techniques and Applications, Nara, Japan, 2005 ; the Workshop on Programming Logics in memory of Harld Ganzinger, Sarrebrücken, Germany, 2005 ; the second Taiwanese-French conference in Information Technologies, Tainan, Taiwan, 2005 ; the 13th LPAR Conference, Pnomh Penh, Cambodge, 2006 ; the International Workshop on Mathematical Theories of Abstraction, Substitution and Naming in Computer Science, ICMS, Edinburgh, UK, May 2007.
  Jean-Pierre Jouannaud gave a series of conferences organised by *Alliance Française* in the indian IT's in 2005.

Conference organisation

- Hugo Herbelin and Benjamin Werner were members of the organising committee of the European TYPES 2004 workshop held 15-18 December in Jouy-en-Josas, France.
- Hugo Herbelin co-organised the MoWGLI meeting in Palaiseau.
- Jean-Pierre Jouannaud was a member of the organizing committee for the international conference held at San Diego in honor of Joseph Goguen on the occasion of his 65 birthday.
- Benjamin Werner co-organized, with Benjamin Grégoire and Laurent Théry, a workshop on *Proofs and Numbers* in Orsay, co-sponsored by TYPES and the INRIA-MSR centre in 2006.

Program and steering committees

- Gilles Dowek served as a proramm comittee member for LICS in 2004 and RTA in 2006.
- Hugo Herbelin was a member of the program committees of "Classical Logic and Computing" (CL&C '06 – satellite workshop of ICALP '06 in Venice, Italy), of "Strategies in Automated Deduction" (STRATEGIES '06 – satellite workshop of IJCAR '06 in Seattle, Washington, USA), of the program committee of "Programming Languages meets Program Verification" (PLPV '06 – satellite workshop of IJCAR '06 in Seattle, Washington, USA), of the "International Conference on Functio-

nal Programming" (ICFP '03) and of the "Journées Francophones des Langages Applicatifs" (JFLA '04).
- Jean-Pierre Jouannaud was a member of the program committee for the international conference held at San Diego in honor of Joseph Goguen on the occasion of his 65 birthday (LNCS proceedings) ; he is a member of the steering committee of TFIT ; he is the program chair of LICS 2010 in Edinburgh.
- Benjamin Werner co-edited the proceedings of TYPES 2004 (Springer LNCS) ; he is PC member of the JFLA 2007 and FLOPS 2008 (LNCS proceedings).

PhD commitees

Benjamin Werner served as a referee on the PhD examinations of Sylvain Boulmé (Paris 6) and Vincent Bernat (ENS Cachan). He is member of Assia Mahboubi's PhD jury. Jean-Pierre Jouananud has been a member of the phd juries of xX at ENS Cachan, and of xX of at UTC Barcelona.

Hugo Herbelin was a referee member of Silvia Likavec's PhD examination committee (Turin, Italy, February 2005) and of Samuel Howse's PhD examination committee (Halifax, Canada, October 2006). He was a member of Sylvain Baro's PhD thesis committee (Paris, 2003).

Gilles Dowek served in several PhD comitees.

Jean-Pierre Jouannaud served in several PhD and habilitation comitees in France and Spain.

Awards

- Gilles Dowek received the *Grand Prix de Philosophie de l'Académie Française* in 2007 for his book *Les Métamorphoses du Calcul*.
- Gilles Schaeffer's proposal for a communication about bijective combinatorics was selected by the *Académie des Sciences* and presented at the session "Recent advances in information and communication sciences", which took place on October 9th, 2007.
- Georges Gonthier and Benjamin Werner's proposal for a communication about the four color theorem's proof ws selected by the *Académie des Sciences* and presented at the session "Recent advances in information and communication sciences", which took place on October 9th, 2007.

References

Books and chapters in books

2006

[1] FILLIÂTRE, J.-C., PAULIN-MOHRING, C., AND WERNER, B., Eds. *Types for Proofs and Programs, International Workshop, TYPES 2004, Jouy-en-Josas, France, December 15-18, 2004, Revised Selected Papers* (2006), vol. 3839 of *Lecture Notes in Computer Science*, Springer.

International journals

2005

[2] ARRIGHI, P., AND DOWEK, G. A computational definition of the notion of vectorial space. In *Proceedings of the Fifth International Workshop on Rewriting Logic and Its Applications (WRLA 2004)* (2005), Electronic Notes in Theoretical Computer Science 117, pp. 249–261.

[3] FERNÁNDEZ, M., MACKIE, I., AND SINOT, F.-R. Closed reduction : explicit substitutions without alpha-conversion. *Mathematical Structures in Computer Science 15*, 2 (2005), 343–381.

[4] FERNÁNDEZ, M., MACKIE, I., AND SINOT, F.-R. Interaction nets vs. the rho-calculus : Introducing bigraphical nets. *Electronic Notes in Theoretical Computer Science* (2005).

[5] FERNÁNDEZ, M., MACKIE, I., AND SINOT, F.-R. Lambda-calculus with director strings. *Journal of Applicable Algebra in Engineering, Communication and Computing 15*, 6 (April 2005), 393–437.

[6] HERNEST, M.-D., AND KOHLENBACH, U. A complexity analysis of functional interpretations. *Theoretical Computer Science 338, Issues 1-3* (2005), 200–246.

[7] SINOT, F.-R. Director strings revisited : A generic approach to the efficient representation of

free variables in higher-order rewriting. *Journal of Logic and Computation 15*, 2 (2005), 201–218.

[8] SINOT, F.-R., AND MACKIE, I. Macros for interaction nets : A conservative extension of interaction nets. *Electronic Notes in Theoretical Computer Science 127*, 5 (2005).

2006

[9] CIRSTEA, H., FAURE, G., FERNÁNDEZ, M., MACKIE, I., AND SINOT, F.-R. New evaluation strategies for functional languages. *Electronic Notes in Theoretical Computer Science* (2006).

[10] DOWEK, G., , AND JIANG, Y. Eigenvariables, bracketing and the decidability of positive minimal predicate logic. *TCS 360* (2006), 193–208.

[11] JOUANNAUD, J.-P., AND XU, W. Automatic complexity analysis for programs extracted from coq proof. *Electr. Notes Theor. Comput. Sci. 153*, 1 (2006), 35–53.

[12] NARBOUX, J. A graphical user interface for formal proofs in geometry. *the Journal of Automated Reasoning special issue on User Interface for Theorem Proving* (2006). to appear.

[13] SINOT, F.-R. Call-by-need in token-passing nets. *Mathematical Structures in Computer Science 16*, 4 (2006).

[14] SINOT, F.-R. Token-passing nets : Call-by-need for free. *Electronic Notes in Theoretical Computer Science 135*, 3 (Mar. 2006), 129–139.

2007

[15] ARIOLA, Z. M., AND HERBELIN, H. Control reduction theories : the benefit of structural substitution. *Journal of Functional Programming* (2007). to appear.

[16] ARIOLA, Z. M., HERBELIN, H., AND SABRY, A. A proof-theoretic foundation of abortive continuations. *Higher Order and Symbolic Computation* (2007). to appear.

[17] ARIOLA, Z. M., HERBELIN, H., AND SABRY, A. A type-theoretic foundation of delimited continuations. *Higher Order and Symbolic Computation* (2007). to appear.

[18] JOUANNAUD, J.-P., AND MACKIE, I. Preface. *Electr. Notes Theor. Comput. Sci. 171*, 3 (2007), 1–2.

[19] JOUANNAUD, J.-P., AND RUBIO, A. Polymorphic higher-order recursive path orderings. *J. ACM 54*, 1 (2007), 1–48.

National journals

2004

[20] DOWEK, G. La théorie des types et les systèmes informatiques de traitement des démonstrations mathématiques. *Mathématiques et Sciences Humaines 165* (2004), 13–29.

International conferences with proceedings

2004

[21] ABADI, M., GONTHIER, G., AND WERNER, B. Choice in dynamic linking. In Walukiewicz [101], pp. 12–26.

[22] ARIOLA, Z. M., HERBELIN, H., AND SABRY, A. A type-theoretic foundation of continuations and prompts. In *Proceedings of the Ninth ACM SIGPLAN International Conference on Functional Programming (ICFP '04), Snowbird, Utah, September 19-21, 2004* (2004), ACM, pp. 40–53.

[23] COEN, C. S. A semi-reflexive tactic for (sub-)equational reasoning. In Filliâtre et al. [1], pp. 98–114.

[24] CORBINEAU, P. First-order reasoning in the Calculus of Inductive Constructions. In Berardi et al. [99], pp. 162–177.

[25] JOUANNAUD, J.-P. Theorem proving languages for verification. In Wang [102], pp. 11–14.

[26] NARBOUX, J. A decision procedure for geometry in coq. In *Proceedings of TPHOLs'2004* (2004), S. Konrad, B. Annett, and G. Ganesh, Eds., vol. 3223 of *Lecture Notes in Computer Science*, Springer-Verlag.

2005

[27] BARRAS, B., AND GRÉGOIRE, B. On the role of type decorations in the calculus of inductive constructions. In *CSL'05* (2005), LNCS, Springer-Verlag.

[28] DOWEK, G. What do we know when we know that a theory is consistent ?. In Nieuwenhuis [109], pp. 1–6.

[29] DOWEK, G. What do we know when we know that a theory is consistent. In *Automated Deduction* (2005), R. Nieuwenhuis, Ed., Lecture Notes in Artificial Intelligence, 3632, Springer-Verlag, pp. 1–6.

[30] DOWEK, G., AND WERNER, B. Arithmetic as a theory modulo. In *Term rewriting and applications* (2005), J. Giesel, Ed., Lecture Notes in Computer Science 3467, Springer-Verlag, pp. 423–437.

[31] GOUBAULT-LARRECQ, J., AND JOUANNAUD, J.-P. Finite semantic trees suffice for ordered resolution and paramodulation. In *Workshop on Programming Logics in memory of Harld Ganzinger* (june 2005), LNCS, Springer-Verlag.

[32] HERBELIN, H. On the degeneracy of sigma-types in presence of computational classical logic. In *Seventh International Conference, TLCA '05, Nara, Japan. April 2005, Proceedings* (2005), P. Urzyczyn, Ed., vol. 3461 of *Lecture Notes in Computer Science*, Springer, pp. 209–220.

[33] HERNEST, D.-M. Light functional interpretation. In *Computer Science Logic : 19th International Workshop, CSL 2005* (2005), L. Ong, Ed., vol. 3634 of *Lecture Notes in Computer Science*, pp. 477–492.

[34] JOUANNAUD, J.-P. Higher-order rewriting : Framework, confluence and termination. In Middeldorp et al. [108], pp. 224–250.

[35] JOUANNAUD, J.-P. Twenty years later. In Giesl [104], pp. 368–375.

[36] SINOT, F.-R. Call-by-name and call-by-value as token-passing interaction nets. In *Proceedings of Typed Lambda Calculi and Applications (TLCA'05)* (2005), vol. 3461 of *Lecture Notes in Computer Science*, pp. 386–400.

2006

[37] BENJAMIN GRÉGOIRE, L. T., AND WERNER, B. A computational approach to pocklington certificates in type theory. In *FLOPS 2006* (2006), M. Hagiya and P. Wadler, Eds., vol. 3945 of *LNCS*, Springer.

[38] BLANQUI, F., JOUANNAUD, J.-P., AND RUBIO, A. Higher-order termination : From kruskal to computability. In Hermann and Voronkov [110], pp. 1–14.

[39] CHRZASZCZ, J., AND JOUANNAUD, J.-P. From obj to ml to coq. In Futatsugi et al. [41], pp. 216–234.

[40] DOWEK, G. Truth values algebras and proof normalization. In Altenkirch and McBride [112], pp. 110–124.

[41] FUTATSUGI, K., JOUANNAUD, J.-P., AND MESEGUER, J., Eds. *Algebra, Meaning, and Computation, Essays Dedicated to Joseph A. Goguen on the Occasion of His 65th Birthday* (2006), vol. 4060 of *Lecture Notes in Computer Science*, Springer.

[42] JOUANNAUD, J.-P. Modular church-rosser modulo. In Pfenning [111], pp. 96–107.

[43] JOUANNAUD, J.-P., AND RUBIO, A. Higher-order orderings for normal rewriting. In Pfenning [111], pp. 387–399.

[44] KIRCHNER, F., AND MUÑOZ, C. PVS# : Streamlined tacticals for PVS. In *Proc. 6th Int. Workshop on Strategies in Automated Deduction* (Aug. 2006), vol. 174/11 of *Electronic Notes in Theoretical Computer Science*, Elsevier, pp. 47–58.

[45] KIRCHNER, F., AND SINOT, F.-R. Rule-based operational semantics for and imperative language. In *Proc. 7th Int. Workshop on Rule Based Programming* (Aug. 2006), vol. 174 of *Electronic Notes in Theoretical Computer Science*, Elsevier, pp. 35–47.

[46] WERNER, B. On the strength of proof-irrelevant type theories. In *Int. Joint Conf. Automated Reasoning — IJCAR 2006* (2006), U. Furbach and N. Shankar, Eds., vol. 4130 of *LNAI*, Springer.

[47] ZUMKELLER, R. Formal global optimisation with taylor models. In *Int. Joint Conf. Automa-*

ted Reasoning — IJCAR 2006 (2006), U. Furbach and N. Shankar, Eds., vol. 4130 of *LNAI*, Springer.

2007

[48] BARRAS, B., AND BERNARDO, B. The implicit calculus of constructions as a programming language with dependent types. In *Workshop on Type theory, Proof theory, and Rewriting* (2007).

[49] BLANQUI, F., JOUANNAUD, J.-P., AND RUBIO, A. Horpo with computational closure : a reconstruction. In Dershowitz and Voronkov [114].

[50] BLANQUI, F., JOUANNAUD, J.-P., AND STRUB, P.-Y. Building decision procedures in the calculus of inductive constructions. In Duparc and Henzinger [115], pp. 328–342.

[51] COQUAND, T., AND SPIWACK, A. Towards constructive homological algebra in type theory. In *Proceedings of 14th Symposium, Calculemus 2007, 6th International Conference, MKM 2007* (2007), Springer.

[52] COUSINEAU, D., AND DOWEK, G. Embedding pure type systems in the lambda-pi-calculus modulo. In Rocca [116], pp. 102–117.

[53] DOWEK, G., AND HERMANT, O. A simple proof that super-consistency implies cut elimination. In Baader [113], pp. 93–106.

[54] GARILLOT, F., AND WERNER, B. Simple types in type theory : Deep and shallow encodings. In Schneider and Brandt [117], pp. 368–382.

[55] GONTHIER, G., MAHBOUBI, A., RIDEAU, L., TASSI, E., AND THÉRY, L. A modular formalisation of finite group theory. In Schneider and Brandt [117], pp. 86–101.

[56] HERNEST, M.-D. Light Dialectica program extraction from a classical Fibonacci proof. *Electronic Notes in Theoretical Computer Science 171*, 3 (2007), 43–53. Elsevier.

[57] HERNEST, M.-D. Synthesis of moduli of uniform continuity by the Monotone Dialectica Interpretation in the proof-system MINLOG. *Electronic Notes in Theoretical Computer Science 174*, 5 (2007), 141–149. Elsevier.

[58] KIRCHNER, F. A finite first-order theory of classes. In *Types for Proofs and Programs, International Workshop, TYPES 2006, Nottingham, UK, April 18-21, 2006, Revised Selected Papers* (2007), Lecture Notes in Computer Science, Springer.

National conferences with proceedings

2004

[59] C. MUÑOZ, G. D., AND CARREÑO, V. Modeling and verification of an air traffic concept of operations. In *International Symposium on software testing and analysis* (2004).

[60] JOUANNAUD, J.-P. Formal mathematics : Application to software safety and internet security. In *Invited presentation, 9th Articifial Intelligence Conference, Taipei* (2004).

[61] JOUANNAUD, J.-P. Theorem proving languages for verification. In *Invited presentation,2nd International Symposium on Automated Technology for Verification and Analysis, Taipei* (2004).

2005

[62] BERTHOMÉ, P., LEBRESNE, S., AND NGUYEN, K. Computation of chromatic polynomials using triangulations and clique trees. In Kratsch [107], pp. 362–373.

[63] KIRCHNER, F. Store-based operational semantics. In *Seizièmes Journées Francophones des Langages Applicatifs* (2005), INRIA.

[64] NARBOUX, J. Toward the use of a proof assistant to teach mathematics. In *Proceedings of ICTMT7* (2005).

2006

[65] ARRIGHI, P., AND DOWEK, G. Linear-algebraic lambda-calculus. In *International workshop on quantum programming languages* (2006), P. Selinger, Ed., Turku Centre for Computer Science General Publication, 33.

[66] NARBOUX, J. Mechanical theorem proving in Tarski's geometry. In *Proceedings of Automatic Deduction in Geometry 06* (2006).

Dissemination

2003

[67] CHARDIN, G., DOWEK, G., LACHIÈZE-REY, M., AND THIS, H. *Quand la science a dit c'est bizarre !* Le Pommier, 2003.

2005

[68] DOWEK, G., BOURGUIGNON, J.-P., NOVELLI, J.-C., AND RITTAUD, B. *Jeux mathématiques et vice versa*. Le Pommier - La cité des sciences et de l'industrie, 2005.

2006

[69] WERNER, B. La vérité et la machine. In *Images des Mathématiques – 2006* (2006), J. I. Etienne Ghys, Ed., Société Mathématique de France.

2007

[70] DOWEK, G. *Les Métamorphoses du Calcul*. Le Pommier, 2007.

[71] GONTHIER, G., AND WERNER, B. Le théorème des quatre couleurs : ingénierie d'une preuve formelle. *La lettre de l'Académie des sciences 21* (2007).

PhD Thesis

2004

[72] CHRZĄSZCZ, J. *Modules in Type Theory with Generative Definitions*. PhD thesis, Warsaw Univerity and University of Paris-Sud, Jan 2004.

2005

[73] HERBELIN, H. *C'est maintenant qu'on calcule, au cœur de la dualité*. PhD thesis, Université Paris-Sud, 2005. Habilitation à diriger des Recherches.

[74] HERMANT, O. *Méthodes Sémantiques en Déduction Modulo*. PhD thesis, Université Paris 7 - Denis Diderot, 2005.

2006

[75] HERNEST, M.-D. *Optimized programs from (non-constructive) proofs by the light (monotone) Dialectica interpretation*. PhD Thesis, École Polytechnique and Universität München, 2006. http ://www.brics.dk/~danher/teza/.

[76] NARBOUX, J. *Formalisation et automatisation du raisonnement géométrique en Coq*. Thése de doctorat, spécialité informatique, Université Paris-Sud, September 2006.

[77] SINOT, F.-R. *Efficient Strategies and Implementation Models for Functional Languages*. Thése de doctorat, spécialité informatique, Ecole Polytechnique, école Polytechnique, France, September 2006.

2007

[78] KIRCHNER, F. *Interoperable proof systems*. PhD thesis, École Polytechnique, 2007.

External references

[79] GORDON, M. J. C., MILNER, R., AND WADSWORTH, C. P. *Edinburgh LCF*, vol. 78 of *Lecture Notes in Computer Science*. Springer, 1979.

[80] COQUAND, T., AND HUET, G. P. The calculus of constructions. *Inf. Comput. 76*, 2/3 (1988), 95–120.

[81] COURANT, J. *Un calcul de modules pour les systèmes de types purs*. Thèse de doctorat, Ecole Normale Supérieure de Lyon, 1998.

[82] ALT, H., AND FERREIRA, A., Eds. *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes - Juan les Pins, France, March 14-16, 2002, Proceedings* (2002), vol. 2285 of *Lecture Notes in Computer Science*, Springer.

[83] BAAZ, M., AND VORONKOV, A., Eds. *Logic for Programming, Artificial Intelligence, and Reasoning, 9th International Conference, LPAR 2002, Tbilisi, Georgia, October 14-18, 2002, Proceedings* (2002), vol. 2514 of *Lecture Notes in Computer Science*, Springer.

[84] BLANQUI, F., JOUANNAUD, J.-P., AND OKADA, M. Inductive-data-type systems. *Theor. Comput. Sci. 272*, 1-2 (2002), 41–68.

[85] DOWEK, G. What is a theory ? In Alt and Ferreira [82], pp. 50–64.

[86] DOWEK, G., HARDIN, T., AND KIRCHNER, C. Binding logic : Proofs and models. In Baaz and Voronkov [83], pp. 130–144.

[87] GRÉGOIRE, B., AND LEROY, X. A compiled implementation of strong reduction. In *ICFP* (2002), pp. 235–246.

[88] MIQUEL, A., AND WERNER, B. The not so simple proof-irrelevant model of cc. In Geuvers and Wiedijk [94], pp. 240–258.

[89] ARIOLA, Z. M., AND HERBELIN, H. Minimal classical logic and control operators. In *Thirtieth International Colloquium on Automata, Languages and Programming, ICALP '03, Eindhoven, The Netherlands, June 30 - July 4, 2003* (2003), vol. 2719 of *Lecture Notes in Computer Science*, Springer, pp. 871–885.

[90] CHRZĄSZCZ, J. Implementation of modules in the coq system. In *Theorem Proving in Higher Order Logic, TPHOLs 2003* (2003), vol. 2758 of *LNCS*, Springer, pp. 270–286.

[91] DOWEK, G. Confluence as a cut elimination property. In Nieuwenhuis [97], pp. 2–13.

[92] DOWEK, G., HARDIN, T., AND KIRCHNER, C. Theorem proving modulo. *J. Autom. Reasoning 31*, 1 (2003), 33–72.

[93] DOWEK, G., AND WERNER, B. Proof normalization modulo. *Journal of Symbolic Logic 68-4* (2003), 1289–1316.

[94] GEUVERS, H., AND WIEDIJK, F., Eds. *Types for Proofs and Programs, Second International Workshop, TYPES 2002, Berg en Dal, The Netherlands, April 24-28, 2002, Selected Papers* (2003), vol. 2646 of *Lecture Notes in Computer Science*, Springer.

[95] GRÉGOIRE, B. *Compilation des termes de preuves : un (nouveau) mariage entre Coq et Ocaml.* Thése de doctorat, spécialité informatique, Université Paris 7, école Polytechnique, France, `http://www-sop.inria.fr/everest/personnel/Benjamin.Gregoire/Publi/gregoire_these.ps.gz`, December 2003.

[96] MUÑOZ, C., CARREÑO, V., DOWEK, G., AND BUTLER, R. W. Formal verification of conflict detection algorithms. *STTT 4*, 3 (2003), 371–380.

[97] NIEUWENHUIS, R., Ed. *Rewriting Techniques and Applications, 14th International Conference, RTA 2003, Valencia, Spain, June 9-11, 2003, Proceedings* (2003), vol. 2706 of *Lecture Notes in Computer Science*, Springer.

[98] WALUKIEWICZ-CHRZĄSZCZ, D. *Termination of Rewriting in the Calculus of Constructions*. PhD thesis, Warsaw University and Université de Paris-Sud, 2003.

[99] BERARDI, S., COPPO, M., AND DAMIANI, F., Eds. *Types for Proofs and Programs, International Workshop, TYPES 2003, Torino, Italy, April 30 - May 4, 2003, Revised Selected Papers* (2004), vol. 3085 of *Lecture Notes in Computer Science*, Springer.

[100] BERTOT, Y., AND CASTERAN, P. *Interactive Theorem Proving and Program Development Coq'Art : The Calculus of Inductive Constructions*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2004.

[101] WALUKIEWICZ, I., Ed. *Foundations of Software Science and Computation Structures, 7th International Conference, FOSSACS 2004, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2004, Barcelona, Spain, March 29 - April 2, 2004, Proceedings* (2004), vol. 2987 of *Lecture Notes in Computer Science*, Springer.

[102] WANG, F., Ed. *Automated Technology for Verification and Analysis : Second International Conference, ATVA 2004, Taipei, Taiwan, ROC, October 31-November 3, 2004. Proceedings* (2004), vol. 3299 of *Lecture Notes in Computer Science*, Springer.

[103] AYDEMIR, B. E., BOHANNON, A., FAIRBAIRN, M., FOSTER, J. N., PIERCE, B. C., SEWELL, P., VYTINIOTIS, D., WASHBURN, G., WEIRICH, S., AND ZDANCEWIC, S. Mechanized metatheory for the masses : The poplmark challenge. In Hurd and Melham [106], pp. 50–65.

[104] GIESL, J., Ed. *Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings* (2005), vol. 3467 of *Lecture Notes in Computer Science*, Springer.

[105] GONTHIER, G. A computer checked proof of the four-color theorem. available on the web, `http://research.microsoft.com/~gonthier/`, 2005.

[106] HURD, J., AND MELHAM, T. F., Eds. *Theorem Proving in Higher Order Logics, 18th International Conference, TPHOLs 2005, Oxford, UK, August 22-25, 2005, Proceedings* (2005), vol. 3603 of *Lecture Notes in Computer Science*, Springer.

[107] KRATSCH, D., Ed. *Graph-Theoretic Concepts in Computer Science, 31st International Workshop, WG 2005, Metz, France, June 23-25, 2005, Revised Selected Papers* (2005), vol. 3787 of *Lecture Notes in Computer Science*, Springer.

[108] MIDDELDORP, A., VAN OOSTROM, V., VAN RAAMSDONK, F., AND DE VRIJER, R. C., Eds. *Processes, Terms and Cycles : Steps on the Road to Infinity, Essays Dedicated to Jan Willem Klop, on the Occasion of His 60th Birthday* (2005), vol. 3838 of *Lecture Notes in Computer Science*, Springer.

[109] NIEUWENHUIS, R., Ed. *Automated Deduction - CADE-20, 20th International Conference on Automated Deduction, Tallinn, Estonia, July 22-27, 2005, Proceedings* (2005), vol. 3632 of *Lecture Notes in Computer Science*, Springer.

[110] HERMANN, M., AND VORONKOV, A., Eds. *Logic for Programming, Artificial Intelligence, and Reasoning, 13th International Conference, LPAR 2006, Phnom Penh, Cambodia, November 13-17, 2006, Proceedings* (2006), vol. 4246 of *Lecture Notes in Computer Science*, Springer.

[111] PFENNING, F., Ed. *Term Rewriting and Applications, 17th International Conference, RTA 2006, Seattle, WA, USA, August 12-14, 2006, Proceedings* (2006), vol. 4098 of *Lecture Notes in Computer Science*, Springer.

[112] ALTENKIRCH, T., AND MCBRIDE, C., Eds. *Types for Proofs and Programs, International Workshop, TYPES 2006, Nottingham, UK, April 18-21, 2006, Revised Selected Papers* (2007), vol. 4502 of *Lecture Notes in Computer Science*, Springer.

[113] BAADER, F., Ed. *Term Rewriting and Applications, 18th International Conference, RTA 2007, Paris, France, June 26-28, 2007, Proceedings* (2007), vol. 4533 of *Lecture Notes in Computer Science*, Springer.

[114] DERSHOWITZ, N., AND VORONKOV, A., Eds. *Logic for Programming, Artificial Intelligence, and Reasoning, 14th International Conference, LPAR 2007, Yerevan, Armenia, November 15-19, 2007, Proceedings* (2007), vol. 4790 of *Lecture Notes in Computer Science*, Springer.

[115] DUPARC, J., AND HENZINGER, T. A., Eds. *Computer Science Logic, 21st International Workshop, CSL 2007, 16th Annual Conference of the EACSL, Lausanne, Switzerland, September 11-15, 2007, Proceedings* (2007), vol. 4646 of *Lecture Notes in Computer Science*, Springer.

[116] ROCCA, S. R. D., Ed. *Typed Lambda Calculi and Applications, 8th International Conference, TLCA 2007, Paris, France, June 26-28, 2007, Proceedings* (2007), vol. 4583 of *Lecture Notes in Computer Science*, Springer.

[117] SCHNEIDER, K., AND BRANDT, J., Eds. *Theorem Proving in Higher Order Logics, 20th International Conference, TPHOLs 2007, Kaiserslautern, Germany, September 10-13, 2007, Proceedings* (2007), vol. 4732 of *Lecture Notes in Computer Science*, Springer.

MeASI
Modélisation et Analyse des Systèmes en Interaction

Team members

Team leader

Daniel KROB

Permanent members

- Daniel KROB, Directeur de recherches CNRS, professeur chargé de cours à l'École Polytechnique
- Leo LIBERTI, maître de conférences à l'École Polytechnique.

Postdocs

- Sylvain PEYRONNET, since september 1st, 2006 (salary paid for by Chaire Thales up to august 2007)
- Hugo GIMBERT, since september 1st, 2006 (salary paid for by École Polytechnique up to october 2007)
- Fabrizio MARINELLI, since march 1st, 2007 (salary paid for by Allocations Postdoctorales de l'Île-de-France up to october 2007)
- Fabien TARISSAN, since october 1st, 2007 (salary paid for by the EU Morphex project, jointly with the CREA laboratoire, up to september 2008 but extensible).

Phds

- Giacomo NANNICINI, Contrat CIFRE with Mediamobile, since november 1st, 2006

Guests

- Dan FREY, Associate Professor at MIT, from 21st to 27th oct. 2006 (seminar Chaire Thalès)
- Dominik SCHULTES, Ph.D. student at Karlsruhe University, 19th to 22nd june 2007 (joint MeASI-AlgOpt seminar and collaboration with Leo Liberti and Giacomo Nannicini)
- Laura DI GIACOMO, Postdoctoral Fellow at

Università di Roma "La Sapienza", 26th to 29th june 2007 (joint MeASI-AlgOpt seminar and collaboration with Leo Liberti)
- Olivier DE WECK, Associate Professor at MIT, from 2nd to 6th oct. 2007 (invited lecture at Colloque du LIX 2007, guest lecture for Krob and Liberti's Software Modelling course at LIX and collaboration with Daniel Krob and Leo Liberti)
- Andrea LODI, Professor at Università di Bologna, 19th to 22nd oct. 2007 (LIX seminar and collaboration with Leo Liberti)
- Giacomo PATRIZI, Associate Professor at Università di Roma "La Sapienza", 3rd to 9th dec. 2007 (LIX seminar).

History

MEASI was created in september 2006, it is the most recent team at LIX. Its team leader, Daniel Krob, was previously a member of MODÈLES COMBINATOIRES. The precise name of the team is ERC[21] MEASI, and is common to CNRS, École Polytechnique and CEA, in the sense that activities carried out in common belong to all three research institutions. The listed members of the team constitute its LIX part. The CEA members are not listed, but the complete list of MEASI members can be found on our web server. Indeed, MEASI is the first common resarch team which emerged from Digiteo[22].

MEASI is assigned the task to become the backbone of the chair *Systèmes Industriels Complexes* created by École Polytechnique and Thalès[23]. It is expected to become the major french actor in the area of systems engineering, in both education by developping the *Master des Systèmes Industriels Complexes*[24], and in research by developing strong research collaborations with the Pôle mondial SYSTEM@TIC in which Thalès plays a major role.

Research domain

MEASI's main research focus is the modelling, analysis and synthesis of industrial complex systems. This term usually refers to systems (or systems of systems), practically arising in industrial settings, whose complexity makes it difficult, or impossible, to study under more classical frameworks such as worst-case time or space complexity theory, or network theory. In particular, this is a hybrid research domain : it can roughly be partitioned in three main sub-themes : modelling, optimization and verification/validation. Modelling itself requires knowledge from a wide range of different disciplines, because it is often the case that each complex industrial system requires a type of modelling unto itself. Optimization is usually carried out by describing the system by means of mathematical programming techniques, and then applying some standardized or purpose-built solution algorithms to determine the optimal value of all involved decision variables. Verification and validation includes, among others, techniques drawn from the well-established field of software verification and formal languages.

Goals

The research team has the twin goal of pursuing excellence in research concerning complex industrial systems, and keeping all research as applicable as possible. The conception of most of the novel techniques proposed by our team is motivated by some real case encountered in mixed-scale industrial settings.

A more short-term goal is that of defining the interfaces of the three main sub-themes of the team. The interface between modelling and optimization is already quite well established, but work is currently under way as regards the often neglected but all-important case of problems exhibiting time dependency. The interface between modelling and verification is also quite well established, as a software program can be considered at all effects a formal model of a given problem (here, again, work is under way in related aspects displaying gaps). The interface

[21] Équipe de Recherche Commune

[22] Digiteo is one of the 13 *Réseaux Thématique de Recherche Avancée* awarded last year by the french governement, and the only one entirely in informatics. Digiteo was created by a number of laboratories located on the Plateau de Saclay and belonging to CEA, CNRS,École Polytechnique,INRIA,UPS and SUPELEC.

[23] Thalès is a major european industrial actor on the defense market. Its research facility is located on the campus of École Polytechnique

[24] MISIC is lead by École Polytechnique, the other main actors being CEA, Thalès and UPS.

between optimization and verification is, however, almost non-existent. The works in the literature are few and far between, and address very specific problems. A substantial amount of work is currently being done in this specific interface, and specially in using optimization techniques for solving problems relating to the static analysis of software.

Results

This section consists of a research report summary for the LIX (Laboratoire d'Informatique de l'École Polytechnique) research group MeASI (Modélisation et Analyse de Systèmes en Interaction) for the academic year 2006/2007.

Introduction

MEASI is organizationally mixed and scientifically hybrid. Although this requires a considerable amount of coordination (both scientific and administrative), it makes it a veritable mine of ideas and an exciting working environment. The main hood under which all our research is carried out is that of *Complex Industrial Systems*, i.e. possibly recursive systems — occurring in real industrial settings — whose (often recursively propagated) complexity makes them impenetrable to classical analysis, synthesis and prediction frameworks. Our work can be roughly subdivided into three main themes : modelling, optimization and verification/validation (we remark once again that this LIX report only deals specifically with modelling and optimization because the part of the team that deals with verification/validation is organizationally under the responsibility of CEA rather than LIX). Some of the most exciting new developments occur at the interface between these disciplines.

Complex systems modelling

In the modern world, complex industrial systems are just everywhere even if they are so familiar for us that we usually forgot their underlying technological complexity. Transportation systems (such as airplanes, cars or trains), industrial equipments (such as microelectronic or telecommunication systems) and information systems are for instance typical examples of complex industrial systems that we are using or dealing with in the everyday life.

"Complex" refers here to the fact that the engineering of these industrial systems relies on incredibly complex technical and managerial processes. Such systems are indeed characterized by the intrinsic difficulty of their design, due both to an important technological heterogeneity and to the large number of sub-systems they involve. To face this huge complexity, engineers developed a number of methodological tools, popularized in the industry under the name of *system engineering*, that fundamentally rely on the fact that complex industrial systems can be always recursively decomposed in a series of coupled subsystems, up to arriving to totally elementary systems which can be completely handled. In such a framework, system engineering provides then methods for helping both the design, the architecture, the progressive integration and the final validation and qualification steps that structure the construction of an industrial complex system.

This methodological environment is however not a fully satisfactory answer to the problems that engineers must permanently solve in practice to handle this complexity. This empirical and operational engineering approach indeed hides the fact that there are basically no theoretical tools for dealing with systems at a global level. The key problem comes here in particular from the fact that the notion of an industrial system in its whole is not very well defined and rather subjective, even if it clearly corresponds to a strong industrial reality.

The purpose of all our researches in system modelling is therefore to handle this problem by going back to the very fundamentals of what is a system, that is to say by developing an *unified point of view of an industrial system* based on an architectural approach. Our main results in this direction are the following : we first began to provide a low level unified framework for describing both continuous and discrete systems in the same way and in the lines of the usual algorithmic complexity theory (see [37]). We also developed a higher level coherent framework for dealing with software systems (see [43]). Finally we proposed a formal method for measuring the intrinsic complexity of a system architectural schema, obtained as an abstraction of the previous frameworks (see [31]). All these works are presently under integration in a coherent architectural analysis methodology for complex systems that we are still constructing.

Markov Decision Processes

Hugo Gimbert studied Markov decision processes (MDPs), which are useful for the analysis and simulation of complex systems. MDPs are natural models for controllable discrete event systems with stochastic transitions. Gimbert studied the existence of pure and stationary optimal controllers in MDPs with finitely many states and actions [45]. An example of this kind is multi-discounted MDPs. Multi-discounted MDPs can be used to approximate parity and mean-payoff MDPs, leading to new class of MDPs suitable for modelling discrete event systems [46]. Moreover, multi-discounted MDPs can be used to define the notion of Blackwell optimal strategies in parity MDPs [47].

Systems optimization

A system model is used both for describing the model and for computing model solutions : mathematical programming is a discipline of operations research that studies the solution algorithms that can be applied to optimization models, also known as mathematical programming formulations. A mathematical programming formulation is a precise description for an optimization problem, and consists of a set of parameters (the problem *instance*), a set of decision variables, one or more objective functions, and a set of constraints. A solution algorithm for a mathematical programming formulation is an algorithm that finds an assignment of values to the decision variables such that all the constraints are satisfied and such that the objective function is at an optimum (either maximum or minimum) value.

Quadratic programming problems are mathematical programming problems having quadratic terms in the decision variables in both objective function and constraints. Many different applications can be modelled as quadratic programming problems. The Kissing Number Problem [23] determines maximum number of unit D-spheres that can be placed adjacent to a central unit D-sphere, where $D \in \mathbb{N}$; for example the Kissing Number in 2 dimensions is 6 (hexagonal lattice) in 3 dimensions it is 12 (the twelve spheres problem) and in 4 dimensions it was recently determined to be 24. The Molecular Distance Geometry Problem (a quadratic feasibility problem) finds an immersion in $\mathbb{R}^3$ of a given weighted graph, such that the edge weight are the same as the Euclidean inter-vertex distances [4, 59, 8, 27]. The Hartree-Fock Problem, a quartic problem which can be easily reformulated to quadratic, is formulated to find the solution of a set of Hartree-Fock equations, which are used to determine the spatial orbitals of certain atoms [22, 28]. Combinatorial optimization problems such as scheduling with communication delays which depend on quantity of task-exchanged data and processor topology distances [44] can be cast as quadratic programming problems on binary variables. Some real-life bioenergy production problems can also be formulated as quadratic (bilinear) programming problems [42] with mixed continuous-binary products. In general, when a quadratic programming problem, be it integer or continuous or mixed, is subject to some linear equality constraint, exact simplifying reformulations (based on appropriate subsets of Reformulation-Linearization Technique constraints [10]) are possible [20, 25].

In general, quadratic programming problems belong to the class of global optimization (GO) problems. Software packages for solving Mixed-Integer Nonlinear Optimization Problems (MINLPs) are usually complex pieces of codes. There are three main difficulties in coding a good GO software : embedding third-party local optimization codes within the main GO algorithm ; providing efficient memory representations of the optimization problem ; making sure that every part of the code is fully re-entrant. Finding good software engineering solutions for these difficulties is not enough to make sure that the outcome will be a GO software that works well, of course. However, starting from a sound software design makes it easy to concentrate on improving the efficiency of the GO algorithm implementation. In [5] we discuss the main issues that arise when writing a GO software package, namely software architecture and design, symbolic manipulation of mathematical expressions, choice of local solvers and implementation of global solvers. We also perform a literature review of the most common GO algorithms and related software packages. More details concerning implementation of GO algorithms can be found in the edited book [6].

Combinatorial optimization

Several combinatorial optimization problems on graphs (such as [51]) and integer programming problems arise from the analysis of complex industrial systems. The most successful solution method is the Branch-and-Cut algorithm, which relies on a Branch-

and-Bound process where the lower bounding relaxation problem is tightened by adding valid cuts. We study two classes of new cuts in [26, 49].

Traffic systems modelling

Efficiently computing fast paths in large scale dynamic road networks (where dynamic traffic information is known over a part of the network) is a practical problem faced by several traffic information service providers who wish to offer a realistic fast path computation to GPS terminal enabled vehicles. The heuristic solution method we propose in [58] is based on a highway hierarchy-based shortest path algorithm for static large-scale networks ; we maintain a static highway hierarchy and perform each query on the dynamically evaluated network. We also propose a PTAS heuristic based on appropriately clustering the network nodes into regions providing an approximation guarantee in [50].

This research topic is partially funded by Mediamobile, a subsidiary of Télédiffusion De France (TDF). Specifically, mediamobile has funded a pilot study, for which [58] is the concluding report, is co-funding the Ph.D. thesis of G. Nannicini at LIX under the CIFRE scheme, and is expected in the near future to partially fund some in-depth work on a specific time-dependent shortest path algorithm that should eventually lead to a patent. Two shared LIX/Mediamobile patents on the heuristic evaluation of travelling times on road networks are currently undergoing evaluation process.

Ongoing work

F. Marinelli (postdoctoral fellow at LIX, funded by an Île-de-France project) is pursuing two different lines of work. With D. Krob, L. Liberti and O. de Weck (MIT), an investigation on the modelling of complex industrial systems is under way from the point of view of the optimization of platforming-related decisions. With E. Goubault, M. Martel and L. Liberti, a work on mathematical programming approaches to verification of software correctness — particularly from the point of view of definition ranges of floating point numbers — is currently being carried out. Other approaches to software verification from a probabilistic point of view are taken in [24] by S. Peyronnet.

Software, patents and contracts

Patents

The following patents are being deposited at the national French patent office.

1. Estimation de trafic dans un réseau routier (méthode basé sur le flots). Owners : LIX, Mediamobile. Inventors : Ph. Baptiste, G. Barbier, D. Krob, L. Liberti.
2. Estimation de trafic dans un réseau routier (méthode heuristique). Owners : LIX, Mediamobile. Inventor : G. Nannicini.

Contracts

- *Modelling of complex and hybrid systems*
  - Period : January 2006-December 2007
  - Type : Contract Etat-Région (within the “pôle de compétitivité" System@tic)
  - Object : Developing new operational models for complex and hybrid systems.
- *Fastest paths in a road network using partial trafic informations*
  - Period : January-April 2006
  - Type : Contract with V-trafic (Mediamobile)
  - Object : Proof of concept (showing that it is algorithmically possible to find in real time the fastest (in terms of time and depending on the real trafic) path to go from a point A to a point B of a road network.
- *Clusterization of an information system map*
  - Period : October 2006 – March 2007
  - Type : Contract with Bouygues Telecom
  - Object : Proof of concept (showing that it is algorithmically possible to find semantically meaninfull clusters within the architecture schema that describes all technical systems of a real information system).
- *Computation of fastest paths in structured networks at random dynamics : an application to road networks*
  - Period : October 2006 – September 2009
  - Type : CIFRE PhD Contract with V-trafic (Mediamobile)
  - Object : Industrial PhD.
- *Allocations post-doctorales Île-de-France*
  - Period : March 2007 – September 2008
  - Type : 18 months post-doctoral funding

– Object : Modelling of complex industrial systems.

Teaching, dissemination and service

D. Krob is responsible of the master programme “Engineering of complex industrial systems" of Ecole Polytechnique (a joint programme with Institut National des Sciences et Technologies Nucléaires and University Paris Sud 11).

D. Krob teaches both in the third year of the Ecole Polytechnique cursus (lecture : "Software modeling for the working engineer") and in the second year of the master programme “Engineering of complex industrial systems" (lecture : "Introduction to system modeling").

D. Krob gave several communication talks for propagating the system modelling approach in different academic and industrial environments during the last two years.

L. Liberti teaches in the second/third year of Ecole Polytechnique cursus (introductory C++ courses, assistant to D. Krob’s software modelling course for DIX, full C++ course for DMAP), in the master programme “Engineering of complex industrial systems” (Operations Research course) and in the Master Parisien de Recherche en Informatique (Scheduling and Optimization course).

Visibility

D. Krob was invited as guest key speaker in different national and international conferences during the last two years. He gave there the following talks :

– Un premier bilan de 2 ans d’existence de la chaire “Ingénierie des Systèmes Complexes, Forum Académique sur la Formation à l’Ingénierie Système, 4-ième conférence de l’association Française d’Ingénierie Système (AFIS 2006), Toulouse, 2006
– Modelling of Complex Software Systems : a Reasoned Overview, “International Conference on Formal Methods for Networked and Distributed Systems" - 26-ième édition (FORTE 2006), IFIP (TC6, WG 6.1), Paris, 2006
– Repenser le système d’information dans une architecture agile, “Urbanisation de systèmes d’information & Architecture d’entreprise 2007", Marcus Evans Conferences, Paris, Mars 2007
– Systèmes de systèmes : concepts, problématiques, ingénierie et architecture, Tutoriel N. 1, avec J. Printz, Ecole des Systèmes de systèmes, DGA, Paris, Mars 2007
– Architecture of complex systems : why, what and how ?, COgnitive systems with Interactive Sensors (COGIS’07), Stanford University (USA), Novembre 2007.

National scientific cooperations

L. Liberti is the Principal Investigator of the *Automatic Reformulation Search (ARS)* ANR Jeunes Chercheuses/Jeunes Chercheurs research project (2007/2010).

International scientific cooperations

Participation to the research project ‘Morphogenesis and gene regulatory networks in plants and animals : a complex systems modelling approach" of the EEC FP7 programme “New and Emerging Science and Technology" (MORPHEX ; Programme NEST ; coordinator : M. Morvan (ENS Lyon, France) ; 2007/2010).

Seminar invitations

D. Krob was invited to present his research works to different academic and industrial seminars during the last two years (CNAM, LIAFA, Journées Internationales d’Etudes “Vers des ingénieries et des technologies communes aux transports terrestres, maritimes, aériens et spatiaux" (ITCT 2006), etc.).

L. Liberti was invited to present his research work in several academic and industrial seminars during 2006/2007 (T.J. Watson IBM Research Center, LIF Université de Marseille, Università di Roma “La Sapienza”, PRISM Université de Versailles, LAMSADE Université Paris IX, LIAFA Université Paris VI, COPPE Universidade Federal do Rio de Janeiro, LINA Université de Nantes, LRI Université Paris XI, LIP6 Université Paris VI, CEDRIC CNAM, LIPN Université Paris XIII).

Conference organisation

H. Gimbert, D. Krob and L. Liberti are the co-organizers of the 2007 edition of the “Colloque d’Au-

tomne du LIX" devoted to Complex Industrial Systems. Scientific contributions were invited by senior academics (such as P. Hansen (GERAD), G. Cornuéjols (CMU), O. De Weck (MIT), S. Gaubert (INRIA)), industrial researchers (with representatives from AirBus, Bouygtel and Alstom) and junior researchers alike. The event has been deemed a great success by all participants.

Program committees

D. Krob was a member of the scientific committee of the Journées Internationales d'Etudes "Vers des ingénieries et des technologies communes aux transports terrestres, maritimes, aériens et spatiaux" (ITCT 2006).

L. Liberti is a member of the scientific committee of the Cologne-Twente Workshop (CTW) in Graphs and Combinatorial Optimization (yearly international workshop).

Journal editorial boards

D. Krob is member of the editorial board of the electronic journal *Discrete Mathematics and Theoretical Computer Science* (since 2001).

L. Liberti is an associate editor for *Journal of Global Optimization* (since 2006) and *International Transactions in Operations Research* (since 2007). He is also a guest editor for special issues in *Discrete Applied Mathematics* [7, 9] and *Discrete Optimization* [3].

References

Books and chapters in books

2004

[1] LIBERTI, L. *Introduction to Global Optimization*. Sociedad Matematica Peruana, Lima, 2004.

[2] LIBERTI, L., AND MAFFIOLI, F., Eds. *CTW04 Workshop on Graphs and Combinatorial Optimization* (Amsterdam, 2004), vol. 17 of *Electronic Notes in Discrete Mathematics*, Elsevier.

2006

[3] FAIGLE, U., LIBERTI, L., MAFFIOLI, F., AND PICKL, S. Special issue preface : Graphs and combinatorial optimization. *Discrete Optimization 3* (2006), 179.

[4] LAVOR, C., LIBERTI, L., AND MACULAN, N. Computational experience with the molecular distance geometry problem. In Pintér [63], pp. 213–225.

[5] LIBERTI, L. Writing global optimization software. In Liberti and Maculan [6], pp. 211–262.

[6] LIBERTI, L., AND MACULAN, N., Eds. *Global Optimization : from Theory to Implementation*. Springer, Berlin, 2006.

2007

[7] FAIGLE, U., LIBERTI, L., MAFFIOLI, F., AND PICKL, S. Special issue preface : Graphs and combinatorial optimization. *Discrete Applied Mathematics 155* (2007).

2008

[8] C. LAVOR, L. LIBERTI, N. M. An overview of distinct approaches for the molecular distance geometry problem. In Floudas and Pardalos [64]. to appear.

[9] LIBERTI, L., AND MACULAN, N. Special issue preface : Reformulation techniques in mathematical programming. *Discrete Applied Mathematics* (2008). to appear.

[10] SHERALI, H., AND LIBERTI, L. Reformulation-linearization methods for global optimization. In Floudas and Pardalos [64]. to appear.

International journals

2004

[11] LIBERTI, L. Reduction constraints for the global optimization of nlps. *International Transactions in Operations Research 11*, 1 (2004), 34–41.

[12] LIBERTI, L. Reformulation and convex relaxation techniques for global optimization. *4OR 2* (2004), 255–258.

2005

[13] BLOCH, A., KROB, D., AND NG, A. Modeling commercial processes and customer behaviors to estimate the diffusion rate of new products. *Journal of Systems Science and Systems Engineering 14*, 4 (2005), 436–453.

[14] KROB, D., AND THIBON, J. Higher order peak algebras. *Annals of Combinatorics 9* (2005), 411–430.

[15] KROB, D., AND VASSILIEVA, E. Performance evaluation of demodulation with diversity–a combinatorial approach ii : bijective methods. *Discrete Applied Mathematics 145*, 3 (2005), 403–421.

[16] LIBERTI, L. Linearity embedded in nonconvex programs. *Journal of Global Optimization 33*, 2 (2005), 157–196.

[17] LIBERTI, L., AND KUCHERENKO, S. Comparison of deterministic and stochastic approaches to global optimization. *International Transactions in Operations Research 12* (2005), 263–285.

2006

[18] BLIUDZE, S., AND KROB, D. A combinatorial approach to evaluation of reliability of the receiver output for BPSK modulation with spatial diversity. *Electronic Journal of Combinatorics 13*, 1 (2006).

[19] BLIUDZE, S., AND KROB, D. Towards a functional formalism for modelling complex industrial systems. *ComPlexUs, special Issue : Complex Systems - European Conference 2005 2*, 3–4 (2006), 163–176.

[20] LIBERTI, L., AND PANTELIDES, C. An exact reformulation algorithm for large nonconvex nlps involving bilinear terms. *Journal of Global Optimization 36* (2006), 161–189.

2007

[21] KROB, D., STEYAERT, J., AND VASSILIEVA, E. Using geometrical properties for fast indexation of gaussian vector quantizers. *EURASIP Journal on Applied Signal Processing* (2007).

[22] LAVOR, C., LIBERTI, L., MACULAN, N., AND CHAER NASCIMENTO, M. Solving hartree-fock systems with global optimization metohds. *Europhysics Letters 5*, 77 (2007), 50006p1–50006p5.

2008

[23] KUCHERENKO, S., BELOTTI, P., LIBERTI, L., AND MACULAN, N. New formulations for the kissing number problem. *Discrete Applied Mathematics* (2008). to appear.

[24] LASSAIGNE, R., AND PEYRONNET, S. Probabilistic verification and approximation. *Annals of Pure and Applied Logic* (2008). to appear.

[25] LIBERTI, L. Compact linearization of binary quadratic problems. *4OR* (2008). to appear.

[26] LIBERTI, L. Spherical cuts for integer programming problems. *International Transactions in Operations Research* (2008). accepted for publication.

[27] LIBERTI, L., LAVOR, C., MACULAN, N., AND MARINELLI, F. Double variable neighbourhood search with smoothing for the molecular distance geometry problem. *Journal of Global Optimization* (2008). accepted for publication.

[28] LIBERTI, L., LAVOR, C., NASCIMENTO, M. C., AND MACULAN, N. Reformulation in mathematical programming : an application to quantum chemistry. *Discrete Applied Mathematics* (2008). accepted for publication.

National journals

2004

[29] LIBERTI, L. On a class of nonconvex problems where all local minima are global. *Publications de l'Institut Mathématique 76*, 90 (2004), 101–109.

2005

[30] LIBERTI, L., AMALDI, E., MACULAN, N., AND MAFFIOLI, F. Mathematical models and a constructive heuristic for finding minimum fundamental cycle bases. *Yugoslav Journal of Operations Research 15*, 1 (2005).

2008

[31] CASEAU, Y., KROB, D., AND PEYRONNET, S. Complexité des systemes d'information : une famille de mesures de la complexité scalaire d'un schema d'architecture. *Génie Logiciel* (2008). A paraitre.

International conferences with proceedings

2004

[32] AMALDI, E., LIBERTI, L., MACULAN, N., AND MAFFIOLI, F. Efficient edge-swapping heuristics for finding minimum fundamental cycle bases. In Ribeiro and Martins [62], pp. 15–29.

[33] AMALDI, E., LIBERTI, L., MAFFIOLI, F., AND MACULAN, N. Algorithms for finding minimum fundamental cycle bases in graphs. In Liberti and Maffioli [2], pp. 29–33.

[34] LIBERTI, L., MACULAN, N., AND KUCHERENKO, S. The kissing number problem : a new result from global optimization. In Liberti and Maffioli [2], pp. 203–207.

2005

[35] BLIUDZE, S., BILLY, N., AND KROB, D. On optimal Hybrid ARQ control schemes for HSDPA with 16QAM. In *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'2005)* (2005), J. Conan and S. Pierre, Eds., vol. 1, IEEE, pp. 121–127.

[36] BLIUDZE, S., AND KROB, D. Performance evaluation of demodulation with diversity - a combinatorial approach iii : Analysis of the threshold case. In *Proceedings of the 7th Workshop on Algorithm Engineering and Experiments and the 2nd Workshop on Analytic Algorithmics and Combinatorics (ANALCO'05)* (2005), C. Demetrescu, R. Sedgewick, and R. Tamassia, Eds., SIAM, pp. 195–205.

[37] BLIUDZE, S., AND KROB, D. Towards a functional formalism for modelling complex industrial systems. In *European Conference on Complex Systems (ECCS' 05)* (2005), P. Bourgine, F. Kepes, and M. Schoenauer, Eds.

[38] KROB, D., AND NG, A. Understanding the diffusion rate of new products through a simple customer behaviour model. In *IEEE 2005 International Conference on Services Systems and Services Management (ICSSSM'05)* (2005), J. Chen, Ed., vol. 1, IEEE, pp. 237–243.

[39] LAVOR, C., LIBERTI, L., AND MACULAN, N. Grover's algorithm applied to the molecular distance geometry problem. In *Proc. of VII Brazilian Congress of Neural Networks, Natal, Brazil* (2005).

[40] LIBERTI, L., AND DRAŽIC, M. Variable neighbourhood search for the global optimization of constrained nlps. In *Proceedings of GO Workshop, Almeria, Spain* (2005).

[41] LIBERTI, L., LAVOR, C., AND MACULAN, N. Double vns for the molecular distance geometry problem. In *Proc. of Mini Euro Conference on Variable Neighbourhood Search, Tenerife, Spain* (2005).

2006

[42] BRUGLIERI, M., AND LIBERTI, L. Modelling the optimal design of a biomass-based energy production process. In *ORMMES Conference Proceedings* (Coimbra, 2006).

[43] KROB, D. Modelling of complex software systems : a reasoned overview. In *26th IFIP WG 6.1 International Conference on Formal Methods for Networked and Distributed Systems (FORTE'2006)* (2006), E. Najm, J.-F. Pradat-Peyre, and V. V. Donzeau-Gouge, Eds., Springer Verlag, pp. 1–22.

2007

[44] DAVIDOVIĆ, T., LIBERTI, L., MACULAN, N., AND MLADENOVIĆ, N. Towards the optimal solution of the multiprocessor scheduling problem with communication delays. In *MISTA Proceedings* (2007).

[45] GIMBERT, H. Pure stationary optimal strategies in markov decision processes. In *STACS* (2007).

[46] GIMBERT, H., AND ZIELONKA, W. Limits of multi-discounted markov decision processes. In *LICS* (2007).

[47] GIMBERT, H., AND ZIELONKA, W. Perfect information stochastic priority games. In *ICALP* (2007).

[48] HURINK, J., KERN, W., POST, G., AND STILL, G., Eds. *Proceedings of the 6th Cologne-Twente Workshop on Graphs and Combinatorial Optimization* (Enschede, 2007), University of Twente.

[49] LIBERTI, L. A useful characterization of the feasible region of binary linear programs. In Hurink et al. [48], pp. 103–106.

[50] NANNICINI, G., BAPTISTE, P., KROB, D., AND LIBERTI, L. Fast point-to-point shortest path queries on dynamic road networks with interval data. In Hurink et al. [48], pp. 115–118.

[51] PLATEAU, M., LIBERTI, L., AND ALFANDARI, L. Edge cover by bipartite subgraphs. In Hurink et al. [48], pp. 127–131.

PhD Thesis

2004

[52] LIBERTI, L. *Reformulation and Convex Relaxation Techniques for Global Optimization*. PhD thesis, Imperial College London, UK, Mar. 2004.

Miscellaneous

2004

[53] DAVIDOVIĆ, T., LIBERTI, L., MACULAN, N., AND MLADENOVIĆ, N. Mathematical programming-based approach to scheduling of communicating tasks. Tech. Rep. G-2004-99, Cahiers du GERAD, 2004.

[54] LIBERTI, L. Automatic reformulation of bilinear minlps. Tech. Rep. 2004.24, DEI, Politecnico di Milano, July 2004.

[55] LIBERTI, L., AND KUCHERENKO, S. Comparison of deterministic and stochastic approaches to global optimization. Tech. Rep. 2004.25, DEI, Politecnico di Milano, July 2004.

2005

[56] LAVOR, C., LIBERTI, L., MACULAN, N., AND CHAER NASCIMENTO, M. Solving a quantum chemistry problem with deterministic global optimization. Tech. Rep. 1175, Optimization Online, 2005.

[57] LIBERTI, L. Compact linearization for bilinear mixed-integer problems. Tech. Rep. 1124, Optimization Online, 2005.

2006

[58] BAPTISTE, P., BARBIER, G., KROB, D., AND LIBERTI, L. Fast paths in large-scale dynamic road networks. Tech. Rep. cs.NI/0704.1068, arXiv, 2006.

[59] LIBERTI, L., LAVOR, C., AND MACULAN, N. Discretizable molecular distance geometry problem. Tech. Rep. q-bio.BM/0608012, arXiv, 2006.

2007

[60] BAPTISTE, P., KROB, D., AND LIBERTI, L. Procédé de propagation des informations partielles de trafic dans un réseau routier, 2007. Procédé de propagation des informations partielles de trafic dans un réseau routier dont le brevet â été déposé par la societe Mediamobile.

[61] NANNICINI, G. Procédé de propagation des informations partielles de trafic dans un réseau routier, 2007. Procédé de propagation des informations partielles de trafic dans un réseau routier dont le brevet â été déposé par la societe Mediamobile.

External references

[62] RIBEIRO, C., AND MARTINS, S., Eds. *Experimental and Efficient Algorithms* (2004), vol. 3059 of *LNCS*, Springer.

[63] PINTÉR, J., Ed. *Global Optimization : Scientific and Engineering Case Studies*. Springer, Berlin, 2006.

[64] FLOUDAS, C., AND PARDALOS, P., Eds. *Encyclopoedia of Optimization*. Springer, New York, 2008. to appear.

Network Centric Systems

This section describes a collaborative project of LIX called *Systèmes Complexes Distribués Mobiles Sécurisés*. The laboratory is indeed interested in a category of complex systems called *network centric systems* in the defense jargon, where it is anticipated that these systems will become the basic infrastructure of future defense systems for the theater of operations. A good example of such a system is indeed provided by a modern defense system controlling fighters, military vehicles as well as infantry-men. Similar problems arise in the civilian world, for example with projects for automating traffic control on highways via GPS localization, or deploying an assistance team in an emergency situation originating from a cataclysm. These technologies have an enormous potential market, and raise many scientific as well as engineering challenges.

For our purpose, the kernel of a (two level) SCDMS is an ad'hoc network made of mobile actors A carrying powerful, (hence heavy) resources (GPS, medium-range radio transmission, powerful computation resources, decision making systems) operated by a specialized human actor. The network is a service provider for a second category of mobile actors B carrying limited lightweight resources (GPS, short-range radio transmission, limited computing power, light captors, decision making system) possibly communicating via a vocal interface to free their hands.

Communication among the various actors would obey a protocol for ad'hoc networks like OLSRv2, whose communications would be encrypted using a pair of asymmetric keys. Access to the network services would need authentication. In this context, however, relying on a public key infrastructure is unrealistic, therefore requiring identity-based encryption. Actors B would need sending their most complex computations, like speech recognition, to the network kernel which would therefore become a fault-tolerant server for mobile distributed computations. The most critical software systems operating on the network, like authentication protocols, ciphering and deciphering primitives, the infrastructure for mapping and scheduling on the network kernel, should satisfy formal specifications including security and fault-tolerant properties.

Despite its apparent simplicity (there are indeed more than two levels in the targeted defense applications), such a network raises a lot of difficult questions relating to the underlying mobile network, to the hierarchy of networks, to the use of the network kernel as a trustable server for distributed mobile computations, and to the verification of the many formal properties to be satisfied by the system's components and by the whole system itself. Because this project is very ambitious, our goal is not to build an infrastructure for simulating such networks, or even to build a prototype network, but to address the questions that have been raised and propose solutions that can be implemented by appropriate actors.

So far, we have been working on several aspects of the problem with funding provided by DGA[25] for one part, and by Digiteo and Hitachi for the other part. Development and normalization by IETF of the routing protocol OLSRv2 is well advanced, with support from Hitachi (HIPERCOM). Development of encryption mechanisms for these networks has started and is supported by Digiteo, this is the OMT CryptoNet (CRYPTOLOGIE and HIPERCOM). Understanding the behaviour of a distributed network has started as well : fault-tolerant algorithms for election and scheduling have been investigated (COMÈTE). We are also considering the specific difficulties related to signal analysis in this context of a dynamic topology of the network (MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES). We have also started building the necessary Coq infrastructure to verify the encryption and decryption algorithms (LOGICAL). And, of course, modelling such a system made of many software and hardware components is at the heart of the activity of MEASI. Most teams are therefore involved in this effort, even if they do not all get specific funds for this activity.

[25] Direction Générale de l'Armement.

Contracts

– Title : “CryptoNet” ;
Period : 01/11/2007 – 01/11/2008 ;
Type : OMT Digiteo ;
Object : Funding Jerome Milan, research engineer ;

– Title : “Systèmes Complexes Distribués Mobiles Sécurisés“ ;
Period : 2007 ;
Type DGA ;
Object : Funding postdocs and visitors.

Computing resources

SYSRES is considered as a team in the laboratory, with specific goals described below. These goals are discussed and decided with the laboratory bodies (conseil de laboratoire, director, and vice-director).

Permanent members

Managing the computer ressources at LIX is entirely done by a small team of three :

- Matthieu GUIONNET, Ingénieur d'Études CNRS
- Pierre LAFON, Ingénieur de Recherches CNRS
- James RÉGIS, Ingénieur d'Études CNRS

Context

The main task assigned to this small team is to manage the laboratory computing ressources. As shown on the figure, these ressources are made of

- a subnetwork named LIX, which provides standard computer access to the PCs installed in the laboratory offices ; specific computing ressources are also available for users who perform heavy calculations (mostly CRYPTOLOGIE and LOGICAL) ;
- a subnetwork named MEDICIS, which provides computer access and dedicated ressources to an international community interested in symbolic computations, made mostly of the members of the european project SCIENCE ; ;
- a WiFi connection for visitors, despite unsuited security regulations at École Polytechniquewhich continue forbiding WiFi terminals installed in laboratories.

Access to internet is provided by École Polytechnique, and we therefore need to comply to the general policy of the school. In particular, each laboratory member must sign a declaration that he or she will follow the school policy when using Internet services.

Goals

The objectives assigned to the team are essentialy

- A service available 24 hours a day, 7 days a week, 52 weeks a year. Constant availability is an important requirement for carrying out col-

laborative work with our colleagues all around the world.
- A flexible service, allowing us to install any needed software or update without service disturbance, and, in particular, without interuption.
- A flexible architecture, allowing us to install without disturbance new users or new teams, or even new subnetworks, which will surely be helpful when moving in the new Digiteo building in 2010.
- A cheap service, based on free software when possible.
- Besides, our support staff needs accessing specific data bases from CNRS, INRIA and École Polytechnique, for which a Windows installation is necessary.

The laboratory insists on availability 24 hours a day, but this need is hardly understood by the school services, and sometimes by our own staff. In the past, power shutdowns decided by the service of infrastructures of École Polytechnique have sometimes made the service unavailable for a couple of days during a hiring process, a conference organisation or an IETF meeting. Unavailability of some important web services alledgedly unsecure (are there secure web services ?) has forced some teams to migrate specific web-severs on external computing services.

Principles

Currently, the laboratory has 17 servers, 110 PCs and 50 laptops. Besides, several laboratory members own their laptop and use it even in their office.

All our machines (servers and PC) operate under Linux distributions (CentOS and Fedora), except for the support staff whose machines operate under Windows.

Most servers are racked in cabinets in order to save space in the dedicated room.

Servers and PCs are renewed on a four years basis. Currently, most PCs have a flat screen. We sometimes use older screens to absorb the spring wave of interns. The peaks in the budget given below have several explanations : the constant growth of the laboratory which forces us to increase the number of PCs every year ; the budget allocations which must be spent by the end of the fiscal year ; the change of habits, in particular the increasing demand for laptops.

Budget

Year	Amount in k-euros
2004	45
2005	127
2006	132
2007	27

Future development

To satisfy the laboratory requirements, SYSRES has decided to implement a new system architecture based on virtualisation that should increase availability, flexibility and performance of services.

To this end, we have already bought a SAN in order to get better access performance, on line storage maintenance and server redundancy. On the other hand, virtualisation should allow us to reduce the number of servers, ease restarting the system in case of a crash or an attack, and test updates before their definitive installation.

Network structure and services

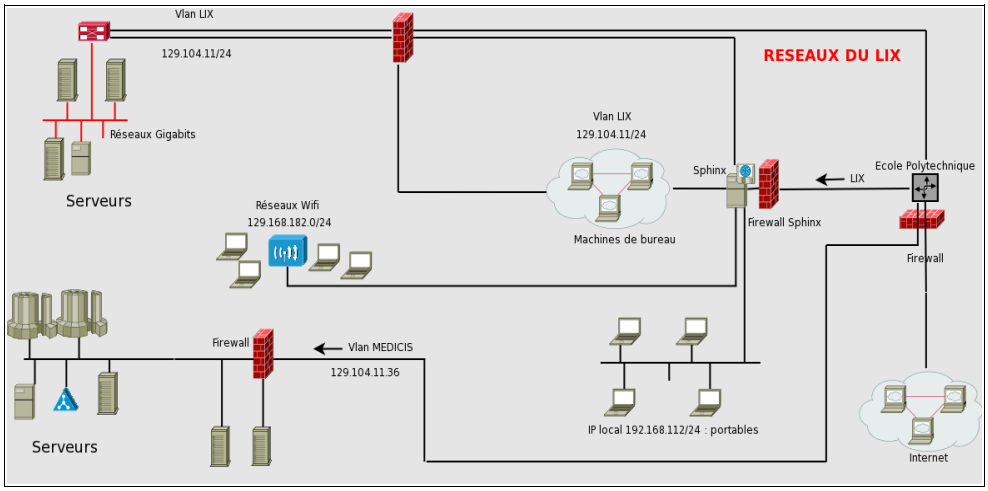


FIG. 1 – LIX Network

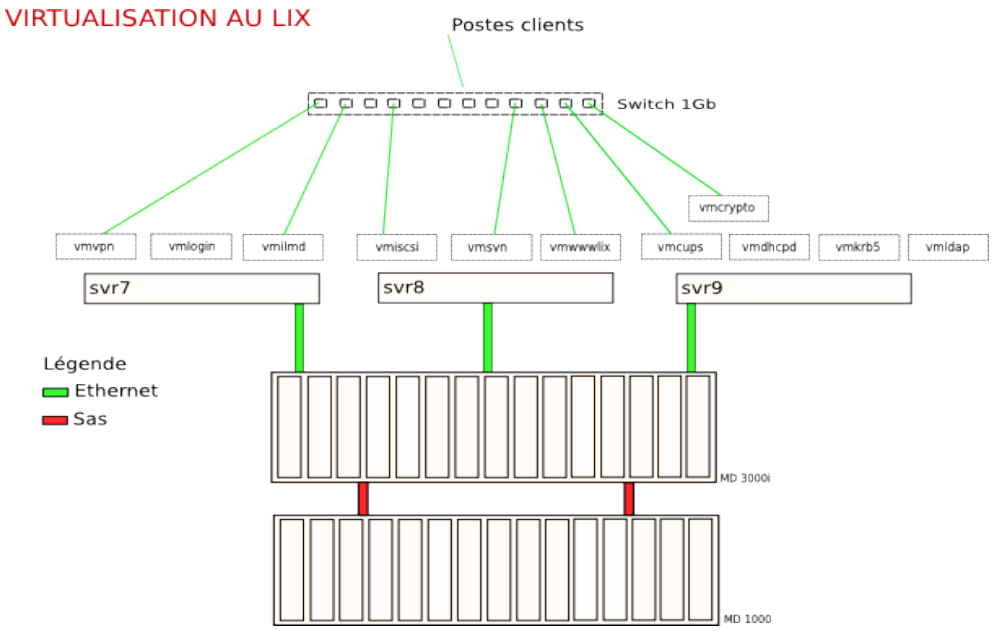


FIG. 2 – Virtualization

System architecture and networks of LIX.

Network services	- Network TCPIP Gigabit. - Firewal et gateway (NAT) via Iptables. - Statics/dynamics IP attribution with/without MAC address (according to the usage). - 5 address ranges (including 4 privates) for pc, servers, laptops, virtual servers. - WIFI : Keyless captive portal.
DNS	Bind, Delegation under domain : LIX et MEDICIS.
File server	NFS for Linux, local account for Windows
Authentication	NIS, LDAP.
Mail services	Postfix (pop, imap, pops, imaps), webmail Squirrelmail.
Web services	- Apache (http, https), proxy reverse. - Mailing listes (Mailman), shared agenda, Php, Mysql,... - Intranet : Zope, Zwiki, Plone, Tracker,...
Other servers	- Server login Ssh, server CVS, application server (Maple,...), etc...
Management applications	- Xlab, Girafe, Cirpanet, Ciel compta.
Telephony	- ToIP
Backup	- Bacula (LIX), Tina (X) - 200 Gigas backup - One full backup every month - A differential backup every week. - A incremental backup everyday.

Clusters.

Internal cluster (team Crypto)	- 14 rackable PC. - Based on LIX systems and network architecture. - 2 teras data storage.
Cluster MEDICIS (team Max)	- 30 rackable PC (Linux 32 et 64 bits). - Systems architecture and networks completely independent of LIX. - Server NFS, NIS, DNS, Firewall IPTABLE. - Network services : server login Ssh + private key, scp, etc... - Licences server. - Load balancing : LSF. - Web services : Mail, Mailing list, Php, Mediawiki. etc... - More than 30 applications in network.

Scientific Project 2009-2012

Achievements

History

The recent history of LIX has been somewhat chaotic. Created as a small UMR[26] in the past with a strong initial leadership, internal difficulties ended up in its downgrading as FRE by CNRS from January 1st, 2003, until December 31, 2004. Back again as a UMR on January 1st, 2005[27], LIX absorbed the major part of the STIX lab ("Sciences et Technologies de l'Information et de la Communication à Polytechnique"), another FRE from École Polytechnique carrying out research in computer science and mathematics, and was then able to benefit from extremely favourable circumstances to expand its activities :

- A strong support from École Polytechnique, CNRS, and INRIA ;
- The creation by École Polytechnique and Thalès of the Chair *Complex Industrial Systems* ;
- The creation of Digiteo ;
- The creation of ANR[28].

During the past three years, 3 new teams have been created at LIX (MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES, MEASI and HIPERCOM), as well as 4 new INRIA projects (ALIEN, HIPERCOM, PARSIFAL and COMÈTE), and all teams were successful hiring CNRS and/or INRIA researchers or teaching staff at École Polytechnique. As a result, the size of the lab went from 65 people on January 1st, 2005, to 123 three years later. These figures do not account for the numerous undergraduate interns from École Polytechnique or other schools, nor for the master students from the several master programs we participate to.

Managing such a fast expansion raises difficulties. Above all, the expansion in size must go along with an even bigger increase in research output. We hope to have demonstrated this in the technical descriptions, but can also point out the high quality of the recent hiring campaign which shows a worldwide attractively of LIX.

The expansion must also go along with an increase of the budget. The figures given in annex show that this has indeed been the case, thanks to the strong support by École Polytechnique, CNRS and INRIA, to the Thalès Chair, and to the numerous research contracts that we have won recently, in particular since the creation of ANR.

Finally, everybody needs a desk : we have built extensions of the lab twice successively, in 2003 and 2006 again. We had to reorganized the office space this year to crowd more people in the existing space, and can now accommodate 124 persons. Two other offices will be transferred to LIX at the end of 2008, allowing us to accommodate two new permanent staff : it should be clear that we do not have any flexibility left. We give more details later.

Goals

During the last five years, our first ambition was to structure the laboratory as a collection of individual research teams focusing their activity on a research project which identifies an important scientific area, clear long term goals and the ways to realize them, both in terms of budget and man power. Developing a software system allowing to demonstrate the team's expertise and research progress is an important component of a research project at LIX. Industrial collaborations allowing to feed the project with concrete questions is another important aspect in our view of what a project should be. Obtaining re-

[26] Unité Mixte de Recherche is the normal name for a laboratory located in a institution for higher education, here École Polytechnique, when it enjoys the support from CNRS. Fédération de Recherche en Évolution is the name for a laboratory which is either a candidate for becoming UMR or a former UMR in which important -possibly temporary- problems have been identified.

[27] This change of status resulted in a change of denomination, with successively UMR7650, FRE2653, and now UMR7161. Each time, the LABINTEL application which is supposed to help directors managing their laboratory's resources and activity was reinitialized without notice and we lost all our data. Each time, we had to key in, among other data, all laboratory members again. As one peculiar consequence, even the historic members of LIX appear on the CNRS data base LABINTEL as having started on January 1st, 2005.

[28] The Agence Nationale de la Recherche is a recently created french research funding institution awarding grants on a project basis.

sources via contracts allowing a project to reach critical mass and scientific excellence should eventually follow from the previous view. The same is true of attracting bright students and distinguished visitors.

A danger of this view is to have self-centered project-teams, the laboratory being a simple addition of them. Our second ambition was therefore to develop and exploit synergy between the different projects. To this end, we rely on three mechanisms. First, we rely on our theory and problem-solving groups, MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES in mathematics, MODÈLES COMBINATOIRES in combinatorics and ALGORITHMIQUE ET OPTIMISATION in combinatorial optimization, have the practice to solve problems of others, besides their own ones : MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES has collaborations with CRYPTOLOGIE and MEASI, for example, while MODÈLES COMBINATOIRES collaborates with *Bioinformatique* and ALGORITHMIQUE ET OPTIMISATION with MEASI again. Second, we also rely on our networking group HIPERCOM to create research problems outside its area of expertise, like problems in security that can feed the other teams : a collaboration has developed between HIPERCOM and CRYPTOLOGIE, leading to the OMT CryptoNet. The third mechanism is the development of large projects which need expertise from different areas, like our project *Système Complexes Distribués Mobiles Sécurisés*, of which CryptoNet is an important sub-project.

Another danger is to have a self-centered laboratory ignorant from its local environment. Our third ambition was therefore to develop strong interactions with the computer science teaching department at École Polytechnique. In particular, a major mission assigned by École Polytechnique is to provide the department with the adequate teaching staff in the major sub-disciplines of computer science as well as in some flashy application areas in order to attract more students from the school to the computer science curriculum and to research in computer science. We have as an important objective that all our research teams have an undergraduate as well as graduate teaching activity, and propose attractive projects to the students who apply for an internship at the laboratory. This effort has been quite successful, and the number of interns in the laboratory has grown over the years. This is true of the students of École Polytechnique, and of students from abroad as well.

The local environment outside the computer science department is of course important as well : the other departments at École Polytechnique, the other research laboratories on the Plateau de Saclay and the local companies whose activity can be related to ours. It turned out that LIX emerged as an important research entity on the Plateau de Saclay at the best possible time, when the different actors in computer science decided to group together and coordinate their research activity. A major goal of LIX has been to become an important force within this movement which culminated with the creation of Digiteo, the major french academic actor in software-intensive systems located on the Plateau de Saclay, and the creation of SYSTEM@TIC, the major french industry-lead *Pôle Mondial* in complex software systems located in Île-de-France.

Research excellence goes also along with strong collaborations at the international level. We do not consider that incentives are needed to force researchers collaborating with the other side of the world. We therefore look at international collaborations as a measure of excellence rather than a target.

We now will consider how much of these various goals have been achieved, and how.

Teaching

There are three kinds of teaching staff at École Polytechnique :

- holding a permanent position -it is then mandatory to join one of the research laboratories at École Polytechnique-,
- holding a part-time position and enrolled in a research laboratory of École Polytechnique -we call them *residents*-,
- holding a part-time position and doing their research in a laboratory elsewhere -we call them *external teaching staff*-, in Île de France for most of them.

People holding a part-time position are almost all full-time researchers from INRIA, CNRS or CEA. Part-time teaching staff members are contracted for at most 12 years (2+5+5). Note that there is a consensus at École Polytechnique that the third category is important : our students should be taught by the very best people in all taught sub-disciplines, and we cannot cover them all with insiders.

Currently, most, but not all, basic courses in computer science are taught by permanent or resident tea-

ching staff, which is more comfortable for the students since they have an easier access to them. This is not true of the courses in data bases or compilers, since there is no team yet at LIX in these two areas. With some exceptions, non-basic courses in areas of expertise of a LIX team are taught by those people in the team that hold either a permanent or a part-time teaching position. When this rule is violated, this is usually for historic reasons. For example, HIPERCOM joined LIX after we hired an external teaching staff member specialized in networking. Note also that all teams participate to the teaching activity both at the undergraduate and graduate level, with the exception of MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES since Eric Schost moved to the University of western Ontario as an associate professor.

A claimed goal of the school is to reach an equal number of people in each of the three categories. In computer science, most teaching staff belonged to the third category in the past. The situation has largely improved but the current figure (8, 11, 16) shows that we are still lacking permanent teaching positions. This is a major weakness of the computer science department : the administrative load that comes with the teaching rests on a small number of people. We therefore need to continue improving these figures, and hire new permanent teaching staff. We will describe our plans for expanding this category later.

Hiring strategy

The computer science department's hiring strategy was to give priority to the teaching needs and at the same time to the growth of the laboratory by creating many sometimes small but strong research groups in well-chosen areas of computer science, expecting that many other goals would simply follow by gravity. In a second stage, we tried to achieve critical mass for these teams, a task that had been almost completed by the hiring campaign this year. It is now time to open again the research spectrum by creating new research teams, a task that we already anticipated each time we had an opportunity.

The hiring process at École Polytechnique has four stages. First, we discuss our hiring needs and plans with the school's directors (one for teaching and one for research), possibly resulting in opening positions. Then, a permanent committee short-lists a selection of interesting candidates for interview. After that, all department members discuss the respective merits of the candidate and set up an ordered list for the recruiting committee. This committee is made of the school directors, the department president and vice-presidents (the LIX director is vice-president for research), as well as some colleagues from computer science and other sciences appointed by the school directors. A decision is made by this committee and proposed to the school. This process ensures a good adequacy between the policies of the school and of the laboratory.

One of the strength of École Polytechnique is the possibility of hiring researchers as part-time teaching staff, who then join one of the teams of the laboratory (or sometimes come with their entire team when several of them are hired on this part-time basis). Therefore, we do not have difficulties hiring part-time teaching staff. This may be different for hiring full-time teaching staff of the highest quality. In this case, we have as a rule to set up an international search committee for each professorship, whose task is to identify and select applications at the highest academic level only

Another rule of École Polytechnique is that *Maîtres de Conférences* should be hired from outside. Similar rules apply for the CNRS and INRIA applicants.

These mechanisms allow us to hire many international staff : one quarter of our teaching and research staff is non french : four Germans, two Italian, one English, one Danish, one Russian, one American and one Colombian. As a result, two teams have more foreigners than nationals among their staff, including the team-leaders. Besides, several french staff members hold Ph.D.'s from abroad. Our recently hired professor, Frank Nielsen, albeit french, returned from Japan where he worked at SONY research laboratories for 10 years. A weakness, though, is the small number of female researchers in the laboratory.

Top rank professors from abroad has a cost : we sometimes need to work hard setting up a complex package involving several financial sources (for example, École Polytechnique and CNRS or École Polytechnique and INRIA) which makes the hiring process long and complex and is likely to result for that reason in a failure. We failed twice successively during the last four years, in particular this year when trying to attract here a world-class leader in optimization and constraint programming.

Despite this failure, the hiring campaign this year

was quite successful, with Frank Nielsen as professor, 3 *chargés de recherche* CNRS, 2 *chargés de recherche* INRIA, and one *Ingénieur de recherche CNRS*. Most teams have now grown to the point where they can move ahead confidently.

Excellence

Reading the previous scientific chapters should be enough, we think, to convince oneself that all LIX teams focus on a research project which identifies clear long term goals, and have now at their disposal the necessary resources, in terms of budget and manpower, to achieve them.

Considering the scientific impact of the teams, we want to stress that most LIX teams have achieved the highest level of excellence by listing the many success stories -at least we think these are success stories- they enjoyed during the recent years.

- MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES : leader of the Science network funded by the EEC under the program FP6, Research Infrastructure action, Integrated Infrastructure Initiatives.
- ALGORITHMIQUE ET OPTIMISATION : The team has solved several open questions in scheduling theory and has introduced new solutions for algorithmic problems in power management. Despite a tough competition, this single team recruited several new CNRS researchers.
- MODÈLES COMBINATOIRES : its team leader Gilles Schaeffer was this year the youngest CNRS researcher in computer science ever promoted as Research Director ; he received the "2007 European Price in Combinatorics" at the Real Alcazar, Sevilla, this September ; Gilles Shaeffer's proposal for a talk about his work in combinatorics is one of the six submissions chosen by the *Académie des Sciences* on a day dedicated to information and communication sciences ; he also went also through the first round of the *young leader* program of the European Research Council.
- HIPERCOM is the author of an Internet standard, the Optimal Link State Routing protocol for ad'hoc networks ; the french price *Science et Défense* was consequently awarded in 2003 to Philip Jacquet, leader of HIPERCOM, and one of his collaborators ; an improved version of the protocol is on its way to be normalised by IETF under the name OLSRv2.
- CRYPTOLOGIE owns the world record for proving that a (large) randomly chosen number is a prime and outputting a proof certificate, as well as the world records for breaking a discrete logarithm and for constructing a large finite number field. These records demonstrate their excellence as mathematicians and their talent as computer scientists ; A. Enge has been awarded a 2004 Kirkman Medal of the Institute for Combinatorics and its Applications, which recognises outstanding work by its members in their early research careers ;
- LOGICAL : the *Grand Prix de Philosophie de l'Académie Française* was awarded this year to Gilles Dowek, former head of LOGICAL, for his book *Les Métamorphoses du Calcul* ; In december 2005, Georges Gonthier, a former INRIA researcher and former member of the teaching staff at École Polytechnique, and Benjamin Werner from LIX, completed the first formal proof of the 4 colors theorem, whose solution had required more than one century of efforts by mathematicians, by using the proof-assistant COQ developed by LOGICAL ; Georges Gonthier and Benjamin Werner's proposal for a talk about the four color theorem's proof is another one of the six submissions chosen by the *Académie des Sciences* on a day dedicated to information and communication sciences.
- PARSIFAL : Dale Miler's h-index is about to reach level 40, from which point on he will be listed on Google scholar for his research achievements ; the prestigious Ackerman price in Computer Science logic was awarded this summer to Stephane Lengrand, a new CNRS researcher who joined PARSIFAL on october 1st.
- COMÈTE : Robin Milner, a Turing medalist, was awarded a Chair Blaise Pascal of the Region Île de France to spend the whole year at LIX in the COMÈTE team ; the LIX colloquium organized by COMÈTE this year was said on blogs to be the *concurrency meeting of the year*, attracting two Turing medalists ; Tom Chothia received the best paper award at the conference FORTE 2006.
- MEASI is the new research team created to

support the *Chaire des Systèmes Industriels Complexes* funded by Thalès.

These success stories illustrate our credo that excellence goes with a strong theoretical background and an ambitious research project identifying clear long-term goals.

Resources

As a consequence of excellence, our applications to the various calls for projects, by ANR and European research programs in particular, have been extremely successful to a point that it is sometimes hard to motivate the team leaders to apply to new calls coming out permanently. Most funds raised that way are used for hiring new phd students or postdocs, resulting in a number of phds and postdocs by far greater than the number of research staff holding an habilitation[29]. The financial annex and others give the precise figures supporting these claims.

Another consequence of excellence is the constant flow of foreign visitors in the laboratory to a point that we sometimes hear or read complaints that broken English has become the usual communication language at LIX. One of our next acquisitions will be an English-speaking coffee machine preparing Italian espresso.

Raising the excellence of the laboratory at every moment has always been our rule, we now harvest its many fruits.

Software development

LIX had a long lasting reputation of being a laboratory of theoreticians. We do not want to refute this reputation, but to complete it. Most teams have as one of their main objectives the development of a software system that can demonstrate their expertise in their research field and compete with similar software developed by our colleagues elsewhere. This is kind of a standard at INRIA and CEA, and we have six INRIA projects and one common team with CEA among the current ten groups. Among the three remaining teams, ALGORITHMIQUE ET OPTIMISATION is about to launch a software project *Tools for combinatorial optimization*. There is therefore some small place left for improvement.

Here is a short description of the important software projects as well as the emerging ones :

1. LOGICAL develops the COQ system. COQ is used worldwide, with many academic users and a few industrial ones, like *Trusted Logics*. Hugo Herbelin, CR INRIA, is in charge of the COQ system, helped by Jean-Marc Notin, a CNRS research engineer. One reason for the success of COQ is the richness of the modelisation mechanisms that are implemented, in particular the inductive types and the module system.
2. HIPERCOM develops tools for implementing routing protocols for ad'hoc networks. Their success in obtaining that their protocols are successfully considered by IETF as a norm depended essentially on these tools and their wide international use. Making them available on line was at the root of the wide success of OLSR among individual users and had a clear impact on the IETF decisions.
3. CRYPTOLOGIE develops tools for implementing cryptographic protocols. These tools, based for most of them on (large) finite number fields defined on elliptic curves, comprise a fast arithmetic package, an extremely fast primality checker, sophisticated tools for computing discrete logarithms, etc. The word *fast* is the important one here, since cryptographic applications on smart cards or RFIDs need be resource efficient.
4. COMÈTE has just started developing a probabilistic model checker. Model checkers have proved to be extremely important in hardware verification, as well as for verification of protocols. Despite their potential usefulness for analysing many protocols that have probabilistic rather than deterministic properties, there are very few probabilistic model checkers on the market.
5. ALGORITHMIQUE ET OPTIMISATION has not started yet a software project, but has been using small software packages of their own for modeling and solving various optimization problems arising in industrial applications. Time is ripe to turn these ad'hoc tools into a generic software that can be tuned to address applications on demand.

[29] Habilitation is the diploma necessary to apply for a professorship, or to enroll phd students. It usually takes from 4 to 6 years after the doctorate.

6. Two other teams (*Bio-informatique*, PARSIFAL) should launch a software project in the future, when they succeed getting enough manpower to plan a long term software tool.

All these tools have a high potential for being used by other academic teams, and some have a high potential for becoming used for industrial applications. Besides COQ , this is the case, we think, in this order, of the projects developed or planned by ALGORITHMIQUE ET OPTIMISATION, HIPERCOM, CRYPTOLOGIE and COMÈTE.

Some, but not all our industrial collaborations are based on these software products. ALGORITHMIQUE ET OPTIMISATION and MEASI have extremely active industrial collaborations and are in even greater demand. HIPERCOM has a strong collaboration with Hitachi essentially, and we expect several Hitachi research staff members to arrive soon in the laboratory (there are already joint phd students). CRYPTOLOGIE is willing to transfer its expertise to industry but is lacking the adequate partner. We expect the awarded OMT CryptoNet to improve this situation. The free software COQ is used by several companies who use to hire members of LOGICAL as consultants. COMÈTE and *Bio-informatique* are not yet ready for transferring their expertise, while MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES, MODÈLES COMBINATOIRES and PARSIFAL are more theory-oriented, and do not have precise plans yet to boost their (limited) interactions with industry.

A research team developing a software product that is then going to be used is subjected to a very strong pressure that can hardly be endured without the help of high-level software engineers that can help organizing the software development and management tasks. It is an important aspect of the strategy of the lab to provide these teams with the adequate support. For the moment, we have obtained one CNRS Research Engineer for LOGICAL, and a second for COMÈTE should be coming very soon. We have obtained one Research Engineer from Digiteo as a result of the OMT CryptoNet who will help CRYPTOLOGIE. We have asked and will continue asking more software engineers from CNRS, École Polytechnique, INRIA and Digiteo. We plan to cover most of our needs that we evaluate to 4 new research engineers by the end of the coming four years contract.

Phds and Postdocs

A weakness of computer science is its low attractivity for the students of École Polytechnique, a phenomenon that has been observed repeatedly, but no remedy has been found yet. As a consequence, there are more phd students at LIX originating from the Écoles Normales Supérieures (Ulm, Cachan and Lyon) than from École Polytechnique. Therefore, there is no impact of this weakness on the quality of our phds. On the other hand, there is a growing interest by students from Europe, Asia and South-America essentially, to join the lab for a doctorate or a post-doctorate. This explains the large number of phds and postdocs currently working at LIX. We nevertheless continue our efforts to attract more students of the school in the computer science courses and at LIX as well. We hope that developing attractive, practical, high level courses when possible, for example in computational photography, will result in significant progress.

The number of phd theses defended by students from LIX is surprisingly low until 2005 included. There are two reasons for that. First, some teams (COMÈTE, PARSIFAL, MEASI) are very recent, they have not yet contributed much to these numbers. Second, the laboratory has grown very rapidly during the last four years, and the number of theses defended in 2005 corresponds to the phd students enrolled in 2001/2002, at a time where the laboratory was very small, around 40 people in total. This is therefore no surprise that the number of phds theses defended has grown suddenly in 2006. For 2007, it is a little early to announce a convincing figure, since most theses are usually defended during the fall. This is due to the deadline for applications to the *Liste d'aptitude aux fonctions de Maître de Conférences*, which is a necessary step before to apply to a position of *Maître de Conférences*[30].

Saclay's research network

LIX is one of the founding members of Digiteo, a research consortium located on the plateau de Saclay, created by CEA, CNRS, École Polytechnique, INRIA-Saclay-Île-de-France, SUPELEC and Université Paris-Sud at Orsay. This consortium was awarded the RTRA status a year ago, one among 13 RTRA for whole France. Digiteo is the only RTRA entirely in computer science, and received an initial funding of

[30] This corresponds to assistant professor.

24 million euros to develop its research activities. Additional funding has been obtained since then by the Digiteo research foundation by submitting research (and development) proposals to the authorities of Île de France.

Digiteo had an immediate important impact on LIX, since CRYPTOLOGIE won one of the four *Operations de Maturation Technologique* awarded by Digiteo in 2007. Thanks to these funds, CRYPTOLOGIE was able to hire one *expert engineer* to develop software aiming at being transferred to industry.

Another important impact of Digiteo are the funds obtained for building office space at CEA-Saclay, École Polytechnique and UPS. These buildings will host research teams from the different Digiteo organisations. For example, the office space built at École Polytechnique will host the LIX teams, of course, but also CEA and INRIA teams which are not part of LIX. And indeed, MEASI is the first DIGITEO team common to at least 3 partners, CEA, CNRS and École Polytechnique, making of LIX a laboratory which hosts researchers from 4 of the six Digiteo founding institutions.

Digiteo has been very active organizing workshops on various topics of interest for several participating laboratories, in order to identify potential synergies among the participants, and then support the collaborative projects that are later submitted and selected. We of course participate to this movement each time we can, and have been successful obtaining funding for several phds and postdocs co-supervised by colleagues from Digiteo.

The rôle of SYSTEM@TIC, on the other hand, is to develop innovative industry-lead projects. To achieve this goal requires the Digiteo research expertise. Digiteo teams participate to various working groups initiated by SYSTEM@TIC, in order to build proposals submitted to french or European calls. While our participation to Digiteo is strong, this is not yet the case of our participation to SYSTEM@TIC (our major participation is via MEASI), a weakness that we share with the other laboratories involved in Digiteo. One reason is that companies involved in SYSTEM@TIC have given priority to projects initiated before the creation of SYSTEM@TIC. The situation may therefore improve as these early projects have all become funded, and ideas for new project are now expected to involve Digiteo teams.

Scientific Relationships

École Polytechnique. Because of its strategy of developing research in areas with a strong mathematical content, new synergies should develop in the future with the department of applied mathematics. As we have already seen, optimization, control, signal processing, vision, Monte Carlo methods and more generally the use of probabilities are common grounds for developing strong collaborations which are currently only emerging. Collaboration has also slowly started with the biology department, and should also develop with the department *Humanités et Sciences Sociales* if we succeed hiring a professor for developing research in the area of information engineering.

Plateau de Saclay. We have four kinds of collaborations on the Plateau de Saclay :

- Our collaborations within Digiteo are strong with some Digiteo teams (at INRIA-Saclay-Île-de-France, LRI, CEA-LIST and ENS-Cachan) but only emerging with the others (Supelec, IEF, LIMSI). We hope that new collaborations will naturally emerge, as money is there and acts like gravity to move forward,
- The Master *Ingénierie des Systèmes Industriels Complexes* has been the occasion for developing new collaborations when building this curriculum in common (École Polytechnique, UPS, CEA, Thalès).
- Collaborations with System@tic are not yet very active, as explained.
- Collaborations with the laboratory INRIA-MicroSoft Research are quite active, since several members of the laboratory participate to the project *mathematical components* developed there and using Coq as a main tool for developing formal proofs of mathematical theorems.

Île de France Strong collaborations exist outside the Plateau de Saclay, with PPS (LOGICAL) and LIAFA (MODÈLES COMBINATOIRES), both laboratories at Paris 7, with CODES (CRYPTOLOGIE) and ALGO (MODÈLES COMBINATOIRES, CRYPTOLOGIE), both INRIA Projects at Rocquencourt, and with Paris 6 (ALIEN). The arrival of Frank Nielsen should naturally result in a new collaborations with École Normale Supérieure and École des Ponts.

Besides these research collaborations, LIX is also participating to the *Master Parisien de Recherche en Informatique* together with Université Paris 7, ENS-Ulm, ENS-Cachan and INRIA as the other co-founders. More than half of our phds come from that Master. These collaborations based on teaching result often in later research projects carried out in common.

France Outside Île-de-France, we have strong scientific collaborations with many colleagues who have participated or participate with us to national programs like RNRT and RNTL (verification of telecommunication protocols, with Nancy, Grenoble and France-Telecom R&D), ACI *Sécurité* (cryptography and security, with Nancy), ACI *Grandes Masses de données* (with Bordeaux), or ACI *Signal* (with Lille). Some of these collaborations have also companies as participants.

Europe Half of the teams participate to collaborative projects belonging to programs funded by the EEC : CRYPTOLOGIE (ECRYPT), MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES(SCIEnce, coordinator), LOGICAL (MOWGLI, TYPES), PARSIFAL (Mobius), MEASI (MORPHEX).

All teams in the laboratory have collaborations with other teams in EEC countries or Switzerland that result in co-authored publications. Many of them are on an individual basis, while some others happen inside established research networks supported by EEC. To name a few who led to common publications, let us mention Austria (TU Wien, PARSIFAL), Germany (TU-Berlin, CRYPTOLOGIE and COMÈTE ; Humbold University, BIO-INFORMATIQUE and MODÈLES COMBINATOIRES ; Osnabrueck, ALGORITHMIQUE ET OPTIMISATION), Italy (Padova, MODÈLES COMBINATOIRES ; Siena, COMÈTE ; Verona, COMÈTE ; Camerino, COMÈTE), Netherland (Amsterdam, LOGICAL), Poland (Varsaw, LOGICAL), Spain (Barcelona, LOGICAL), Sweden (Göteborg, LOGICAL ; Uppsala, COMÈTE), Switzerland (Bern, PARSIFAL ; EPFL, COMÈTE ; ETH Zürich, MODÈLES COMBINATOIRES), UK (Oxford, COMÈTE ; King's college London, LOGICAL ; Imperial college, COMÈTE), etc.

North-America We have strong research collaborations outside Europe. We will mention those which have led to joint publications. With Urbana-Champaign : a collaboration supported by the UIUC-CNRS program, which has led to collaborative software in the area of proof assistants ; with the University of Minneapolis (PARSIFAL) ; with Mac Gill University at Montreal (COMÈTE) ; with NASA (LOGICAL) ; with University of California at Riverside (ALGORITHMIQUE ET OPTIMISATION) ; with University of Waterloo (MODÈLES COMBINATOIRES) ; with University of Western Ontario (CRYPTOLOGIE, MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES) ; with University of Texas (COMÈTE), etc.

South-America South-American students go naturally to north-america for a phd. However, thanks to a Colombian researcher that we recently hired at CNRS, our relationships there have developed rapidly, with at least one Colombian intern each year continuing in phd.

We also have relationships with Brazil (Buenos-Aires, MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES).

Africa We have relationships with Tunisia (Tunis and Marrakesh, MODÈLES ALGÉBRIQUES ET CALCULS SYMBOLIQUES).

Asia Asia is an important target of LIX for collaborations :

- Japan : we have many research collaborations with Japan. École Polytechnique has signed a collaboration agreement with Keio university in Tokyo to support the collaboration between HIPERCOM and the project WIDE on one hand, and the collaboration between LOGICAL and the laboratory of Okada-sensei on the other hand. Both collaborations have resulted in many co-authored papers.
- Taiwan : we were among the founders of the Taiwan-French conference in Information technology, and Jean-Pierre Jouannaud is a member of the organizing committee. The fourth conference is planned next march at Academia Sinica in Taipei.
- China has become an important market for postdocs. We have limited research collaborations with China for the moment, but these relation should develop rapidly in a near future, in

relationship with LIAMA, the joint laboratory of CNRS, INRIA and the Chinese Academy of Sciences.
- India : we benefit from the large number of Indian students looking for an internship or a postdoctoral fellowship, but few of them apply for a doctorate. Many laboratory members have been invited to give seminars in India, in particular those organised by *Alliance Francaise*, but this has not resulted in active research relationships yet.
- There are many students from Vietnam at École Polytechnique, and many of them continue for a phd. On the other hand, we have no research relationship with Vietnamese institutions.

Computing services

LIX has a network of PCs connected to various servers, for mail, for collaborative services, for computations, for storage, etc. A Web service has also been installed, as well as an Intranet to provide with the needed documentation and tools.

On the other hand, the laboratory has bought many laptops for its permanent members and phds who ask for. Since École Polytechnique is a bit shy with the installation of WiFi connections, arguing for security reasons, we have decided to equip our area with (easily removable) devices for our visitors to access Internet when needed.

Because computer equipment has become so cheap, our equipment is clearly up to date and can be renewed when needed. When specific expensive equipment is needed, like the one asked by HIPERCOM to carry out large scale routing experiments involving hundreds of moving nodes, we can always make a specific demand, to INRIA, CNRS or Digiteo for example. Finding the money is not an issue when a project has a clear scientific and practical impact.

Office space

Our expansion has been extremely fast, raising management difficulties. We have built a first extension of the laboratory in 2003, whose cost (230000 euros) was entirely supported by École Polytechnique, to accommodate our first important growth : CNRS researchers either hired or moving from other laboratories to LIX, two new professors hired at LIX, an INRIA-project (LOGICAL) moving in from Rocquencourt, and two new emerging INRIA-projects. A second extension was built recently, whose cost (320000) euros was this time shared by CNRS and INRIA. This allowed us to accommodate new people hired at École Polytechnique, a new project partly moving in from Rocquencourt (HIPERCOM), and the CEA-CNRS-École Polytechnique common research team. To accommodate all people from INRIA and CNRS hired this year, we had to reorganize the office space, the expenses being shared by LIX and École Polytechnique, to crowd more people in the existing space, and can now accommodate up to 123 persons. Two other offices will be transferred to LIX at the end of 2008, allowing us to accommodate two new professors, we indeed expect at least three full-professorships to be opened during the coming four years. Therefore, we do not have any flexibility left. In the coming two years, we will need using temporary solutions, that is, first, transform our conference room into an open office space to crowd in most phds, and second crowd temporary people, the interns and the remaining phds, inside temporary office space that can be quickly installed on the ground outside the building and removed when it becomes superfluous.

We will not build any more temporary office space as we did in the past before we eventually move in the planned Digiteo building sometimes in 2010. This building will be one of three Digiteo buildings erected at Orsay (on the campus of UPS), Palaiseau (on the campus of École Polytechnique) and Saclay (on the campus of CEA). This brand new building will host various teams from Digiteo, including all teams from LIX, some INRIA teams and some CEA teams as well. An extension will follow shortly after. The cost of these buildings is taken care of by four Digiteo partners, CEA, CNRS, UPS and École Polytechnique, and by Région Île de France. At the end of these constructions, LIX should have much more space than now, allowing for an important growth in the coming years. This growth, we think, will continue at the same current speed until the end of the next four years contract, that is the end of 2012.

Self assessment

Project-teams at LIX are young, as is the laboratory, very active nationally and internationally, and of very good quality. All are important with respect to the objectives of the laboratory. All should therefore continue to receive the necessary resources for

their development. So, rather than canceling a research team, we will instead open new ones in the coming years. In the next section, we describe in more details what are our priorities.

Looking ahead

From the beginning, the credo of LIX has been to invest in research areas that need a strong mathematical background. The reason for this deliberate choice is the strong image of the school in hard sciences. It is not clear, however, that this strategic decision is still adequate with the profile of the students of École Polytechnique, who are for most of them far more interested now by careers in private companies, especially in the financial business, than by careers in the academia. Nevertheless, we strongly believe that innovation in information technologies relies on ideas that need a strong background. To cite but one example, Google illustrates our credo.

During the next four years, we plan to create two new teams : one in vision with a strong emphasis on computational photography, and one in distributed data bases with a strong emphasis on management engineering. The leader of the first team has just been hired, we need to give him or help him finding the necessary resources, including a software engineer, to develop its research activities. In the second case, we first need to find a team leader before to help him putting up a project and grow his activities. We would of course also favor the coming at LIX of other INRIA projects that could help satisfying our teaching needs, for example in compilation, operating systems and hardware.

At the same time, we also plan to develop our activities in three important areas : bio-informatics, networking and optimization. In the first case, scattered forces exist at École Polytechnique and Université Paris-Sud that need to be structured. In the second case, two strong teams exist at École Polytechnique (ALGORITHMIQUE ET OPTIMISATION at LIX and one at CMAP[31]) and several other teams at LIX have also developed expertise in the area ; working together towards a common goal would allow to scale up their visibility. In the third case, a strong team at LIX (HIPERCOM) collaborates closely with another one at LRI, the computer science laboratory at Université Paris Sud and more loosely with CRYPTOLOGIE at LIX ; the situation is ripe for very ambitious projects in this area.

In the next section, we describe the kind of organisation we plan to build in order to achieve these goals.

Chairs and "Institut des Systèmes Complexes"

Chair at École Polytechnique are funded by an industrial partener or by a group of industrial partners.

Complex industrial systems is the first, already existing chair, currently supported by *Thalès*. We are actively working now for its renewal, possibly with several industrial partners. Complexity of systems can be measured in various ways, but a system's size, its structural complexity, and the heterogeneity (software/hardware) of its components are three well-accepted measures. Many complex systems are embedded, and therefore inherit the usual safety requirements for embedded software. Again, this area needs skills from very different subareas of computer science (automata's theory, specification languages, verification, software analysis) and control theory, and the lab has strong teams in all these different areas.

We have identified six areas in which we believe that a chair can be setup. All these areas have to do with *complexity*, complexity of software, of data, of biological processes, of interactions, of communications, and some mix several of these different aspects of complexity. We believe that there are hard scientific problems in all these areas, which all need mathematical skills to be resolved. At the same time that there is a clear existing or potential market for all of them.

1. *Optimization* is an interdisciplinary area where the industrial demand for specialists and collaborations is highest. We are actively working for structuring this research area and developing an optimization track at the master level in collaboration with the department of applied mathematics. We need manpower, in particular at the senior level to help the current team leader Philippe Baptiste who will replace the current head of the lab soon.
2. *Mobile Networks* based on radio transmission will be a main component of the so-called information society. These networks raise a num-

[31] Centre de Mathématiques Appliquées et Probabilités.

ber of scientific questions, among which routing, quality of service and protection of the information are the most important. Again, we have started working on a specific master track, as well as on a possible industrial support. Software projects already exist, in the area of ad'hoc networks, but manpower is needed too.

3. *Security* is a major issue in computer science, which is closely related to the current technology based on a network infrastructure which supports ubiquitous communications. This area is therefore in close interaction with the previous one. The need for security (and for privacy) will grow with our uses. The laboratory is quite strong in this area, with the CRYPTOLOGIE team which is at the top of the discipline, and the formal method groups that have a very strong experience in analysing all kinds of software models, either deterministic or probabilistic. It is not clear yet whether a chair can be built, or if *Mobile Networks* and *Security* should be grouped together into a single chair.
4. *Complex Data Processing* is a rapidly evolving area. The need for processing complex data arises in particular from the numerous applications in which a 3D computer model of the world is used. These models are becoming more and more complex, made of highly parametrized numerical data that need to be efficiently represented and queried. These data can therefore be seen as living in a metric space whose dimension can be very large. This emerging area sometimes called *geometry of information*, has already become an extremely interesting source of scientific problems of a geometrical nature and has a high potential for many important practical applications. Frank Nielsen and INRIA colleagues have already submitted an ANR project together, which structures the emerging forces on the Plateau de Saclay in this area and could rapidly lead to a new INRIA project.
5. *Organizations Engineering* is an emerging area, at the frontier of several scientific subdisciplines, distributed data bases, Web search, optimization, control theory and decision making. While the first four are in information technologies, the last is in management, that is, in the HSS department at École Polytechnique. Note that decision making requires a lot of software infrastructure and tools from all the above areas that need to be integrated in some complex system. We have preliminary contacts with a computer scientist who is also a specialist of decision making and management, but are still lacking the adequate person in distributed data bases and web search, an extremely hot area indeed.

6. *Bio-informatics* is an important interdisciplinary area in which Microsoft has announced its decision to support activities at École Polytechnique. There are two teams in this area at École Polytechnique, one in computer science and one in biology. Besides, there are other Digiteo teams or individuals at Université Paris-Sud as well as at INRIA. All these teams have been loosely collaborating for some time already (common seminar and a few joint papers) and aim at integrating their activities in a large teaching and research project that would then benefit from the existence of a chair supported by Microsoft Research. A preliminary research project has been submitted to INRIA, but needs further elaboration before becoming a new INRIA project/team located at École Polytechnique for one part and at Université Paris Sud for the other part. Despite these moves, it is still unclear whether these recent advances will materialize in a near future.

For all of the candidate chairs mentioned above (but *organisations engineering*) there is a clearly identified potential leader : our strategy is to build on our existing strengths, and to open the door to new ideas and diversity. The last area needs a professorship to be created, and a professor to be hired and then start the process of building a team and finally a chair. Of course, we do not think that we will be able to put up all these chairs during the next 4-years contract. This is a long term goal, and we would like to see some significant progress towards this goal before the end of year 2012.

The policy of École Polytechnique is to group chairs with high interaction potential into institutes. We hope to be able to setup an *Institut des Systèmes Complexes* soon.

Personnel

We now come to one important weakness of LIX : the investment of École Polytechnique in personnel.

LIX has four full-time professors, one administrative assistant and no computer engineer provided by École Polytechnique[32]. To make our point, let us compare our situation with that of the maths laboratories, since our activities are similar in nature. École Polytechnique has two renown laboratories in mathematics, CMAP for applied maths and CMAT for pure maths, about the size of LIX altogether. CMAP has 2 administrative assistants and 4 research engineers, among which 5 are paid by École Polytechnique. CMAT has 2 administrative assistants and 4 engineers, among which 5 are paid by CNRS. In total, CMAT and CMAP together have 4 administrative assistants and 8 engineers, one half paid by CNRS and the other half by École Polytechnique. On January 1st, 2008, LIX will have 4 administrative assistants (one paid by École Polytechnique, one by CNRS and two by INRIA), 5 engineers paid by CNRS, and two others on a temporary position paid by INRIA and Digiteo respectively. This shows the low support from École Polytechnique to Computer Science in terms of support staff. The same is actually true of the full-time teaching staff : we have only 3 full professors, one associate professor and three assistant professors (the maths departments together have 8 full professors and 2 associates). The rest of the teaching staff is made of researchers (mostly CNRS or INRIA) that hold a part-time position. Apart from a few exceptions (one of the CNRS research directors is also the head of the Master ISIC), these researchers have priorities that are different from those of the full-time teaching staff. If the size of LIX has reached the size of CMAP and CMAT combined, the reason is that LIX has a large number of INRIA and CNRS researchers, and more phd students and postdocs.

Our goal with these comparisons is to emphasize the low level investment of École Polytechnique in personnel in our laboratory. The strong support of both CNRS and INRIA has allowed us a steady growth and at the same time to constantly raise the overall quality of the lab. This stage is now over. We need more permanent teaching staff from École Polytechnique to help us with the teaching and administrative tasks, and more research engineers to help our teams in their software developments. If the school does not fulfill its promises, we will not be able to reach our goals.

One may ask the question of what is more important, support or teaching staff ? Both are. We desperately need more support staff, and we desperately need more full-time teaching staff. École Polytechnique puts a lot of pressure on its personnel for improving the teaching figures, increase the amount of contract money, develop collaborations with foreign countries, etc. This needs a lot of devoted staff, and experience shows that people devoted to the school are usually those hired on a permanent basis by the school, the others being normally devoted to their own institution. Since there is few permanent teaching staff, a major weakness of the Computer Science department is the lack of devoted people. We think that we lack at least 3 (full-time) professors, 5 full-time professeurs chargés de cours and 3 (full time) maîtres de conférences to run the teaching department and laboratory smoothly.

[32] We omit here for simplicity of our argument the other categories of personnel, maîtres de conférences and part time teaching staff.

List of Publications

We provide a list of the papers published by LIX researchers over the last four years. The list is sorted according to the following categories.

- Books and chapters in books
- International journals
- National journals
- International conferences with proceedings
- National conferences with proceedings
- Dissemination
- PhD Thesis
- Miscellaneous
- External references

To make a clear distinction between the list of publications of the whole lab and the list of publications provided by each of the team at the end of its report, we have added the LIX logo in front of each item of the whole lab publication list

Books and chapters in books

2004

[LIX1] BAPTISTE, P., AND BRUCKER, P. *HandBook of Scheduling : Algorithms, Models and Performance Analysis*. CRC Press, 2004, ch. Scheduling Equal Processing Time Jobs.

[LIX2] BAPTISTE, P., NÉRON, E., AND SOURD, F. *Modèles et algorithmes en ordonnancement. Exercice et problèmes corrigés (18 auteurs)*. Ellipses, 2004.

[LIX3] JOUGLET, A., BAPTISTE, P., AND CARLIER, J. *HandBook of Scheduling : Algorithms, Models and Performance Analysis*. CRC Press, 2004, ch. Branch-and-Bound Algorithms for Total Weighted Tardiness.

[LIX4] LIBERTI, L. *Introduction to Global Optimization*. Sociedad Matematica Peruana, Lima, 2004.

[LIX5] LIBERTI, L., AND MAFFIOLI, F., Eds. *CTW04 Workshop on Graphs and Combinatorial Optimization* (Amsterdam, 2004), vol. 17 of *Electronic Notes in Discrete Mathematics*, Elsevier.

[LIX6] MILLER, D. Overview of linear logic programming. In *Linear Logic in Computer Science*, T. Ehrhard, J.-Y. Girard, P. Ruet, and P. Scott, Eds., vol. 316 of *London Mathematical Society Lecture Note*. Cambridge University Press, 2004, pp. 119 – 150.

[LIX7] MILLER, D., AND PIMENTEL, E. Linear logic as a framework for specifying sequent calculus. In *Logic Colloquium '99 : Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic*, J. van Eijck, V. van Oostrom, and A. Visser, Eds., Lecture Notes in Logic. A K Peters Ltd, 2004, pp. 111–135.

2005

[LIX8] CAIRES, L., ITALIANO, G. F., MONTEIRO, L., PALAMIDESSI, C., AND YUNG, M., Eds. *Automata, Languages and Programming, 32nd International Colloquium, ICALP 2005, Lisbon, Portugal, July 11-15, 2005, Proceedings* (2005), vol. 3580 of *Lecture Notes in Computer Science*, Springer.

[LIX9] DENG, Y., PALAMIDESSI, C., AND PANG, J. Compositional reasoning for probabilistic finite-state behaviors. In *Processes, Terms and Cycles : Steps on the Road to Infinity*, A. Middeldorp, V. van Oostrom, F. van Raamsdonk, and R. C. de Vrijer, Eds., vol. 3838 of *Lecture Notes in Computer Science*. Springer, 2005, pp. 309–337. `http://www.lix.polytechnique.fr/~catuscia/papers/Yuxin/BookJW/par.pdf`.

[LIX10] FLIESS, M., JOIN, C., AND SIRA-RAMÍREZ, H. Closed-loop fault-tolerant control for uncertain nonlinear systems. In *Control and Observer Design for Nonlinear Finite and Infinite Dimensional Systems* (2005), pp. 217–233.

[LIX11] GAUDRY, P. Chapter 7 : Hyperelliptic curves and the HCDLP. In *Advances in Elliptic Curve Cryptography* (2005), I. Blake, G. Seroussi, and N. Smart, Eds., vol. 317 of *London Mathematical Society Lecture Note Series*, Cambridge University Press. In press.

[LIX12] MORAIN, F. Elliptic curves for primality proving. In *Encyclopedia of cryptography and security*, H. C. A. van Tilborg, Ed. Springer, 2005.

[LIX13] NÉRON, E., ARTIGUES, C., BAPTISTE, P., CARLIER, J., DEMASSEY, S., AND LABORIE, P. *Topics in modern project scheduling*. Kluwer, 2005, ch. Lower bounds computation for RCPSP chapitre de Topics in modern project scheduling.

[LIX14] POULALHON, D., AND SCHAEFFER, G. Counting, coding, and sampling with words. In *Applied Combinatorics on Words*, J. Berstel and D. Perrin, Eds. Cambridge University Press, 2005.

2006

[LIX15] BAPTISTE, P., LABORIE, P., PAPE, C. L., AND NUIJTEN, W. *Handbook of Constraint Programming*. Elsevier, 2006, ch. Constraint-Based Scheduling and Planning.

[LIX16] DICOSMO, R., AND MILLER, D. Linear logic. In *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed. Stanford University, 2006.

[LIX17] FAIGLE, U., LIBERTI, L., MAFFIOLI, F., AND PICKL, S. Special issue preface : Graphs and combinatorial optimization. *Discrete Optimization 3* (2006), 179.

[LIX18] FILLIÂTRE, J.-C., PAULIN-MOHRING, C., AND WERNER, B., Eds. *Types for Proofs and Programs, International Workshop, TYPES 2004, Jouy-en-Josas, France, December 15-18, 2004, Revised Selected Papers* (2006), vol. 3839 of *Lecture Notes in Computer Science*, Springer.

[LIX19] LAVOR, C., LIBERTI, L., AND MACULAN, N. Computational experience with the molecular distance geometry problem. In Pintér [486], pp. 213–225.

[LIX20] LIBERTI, L. Writing global optimization software. In Liberti and Maculan [21], pp. 211–262.

[LIX21] LIBERTI, L., AND MACULAN, N., Eds. *Global Optimization : from Theory to Implementation*. Springer, Berlin, 2006.

2007

[LIX22] FAIGLE, U., LIBERTI, L., MAFFIOLI, F., AND PICKL, S. Special issue preface : Graphs and combinatorial optimization. *Discrete Applied Mathematics 155* (2007).

[LIX23] FLIESS, M., AND SIRA-RAMIREZ, H. Closed-loop parametric identification for continuous-time linear systems via new algebraic techniques. In *Continuous-Time Model Identification from Sampled Data* (2007), H. Garnier and L. Wang, Eds.

2008

[LIX24] C. LAVOR, L. LIBERTI, N. M. An overview of distinct approaches for the molecular distance geometry problem. In Floudas and Pardalos [495]. to appear.

[LIX25] LIBERTI, L., AND MACULAN, N. Special issue preface : Reformulation techniques in mathematical programming. *Discrete Applied Mathematics* (2008). in preparation.

[LIX26] SHERALI, H., AND LIBERTI, L. Reformulation-linearization methods for global optimization. In Floudas and Pardalos [495]. to appear.

International journals

2004

[LIX27] BANK, B., GIUSTI, M., HEINTZ, J., AND PARDO, L. M. Generalized polar varieties and an efficient real elimination procedure. *Kybernetika 40*, 5 (2004), 519–550.

[LIX28] BAPTISTE, P., BRUCKER, P., KNUST, S., AND TIMKOVSKY, V. G. Ten notes on equal-processing-time scheduling. *4OR : Quarterly Journal of the Belgian, French and Italian Operations Research Societies 2* (2004), 111–127.

[LIX29] BAPTISTE, P., CHROBAK, DURR, C., JAWOR, AND VAKHANIA. Preemptive scheduling of equal-length jobs to maximize weighted throughput. *Operations Research Letters 32*, 3 (2004), 258–264.

[LIX30] BAPTISTE, P., AND DEMASSEY, S. Tight lp bounds for resource constrained project scheduling. *OR Spectrum 26* (2004), 251–262.

[LIX31] BAPTISTE, P., AND TIMKOVSKY, V. Shortest path to nonpreemptive schedules of unit-time jobs on two identical parallel machines with minimum total completion time. *Mathematical Methods of Operations Research (ZOR) 60*, 1 (2004), 145–153.

[LIX32] CHARRON-BOST, B., AND SCHIPER, A. Uniform consensus is harder than consensus. *Journal of Algorithms 51*, 1 (2004), 15–37.

[LIX33] CHASSAING, P., AND SCHAEFFER, G. Random planar lattices and integrated superbrownian excursion. *Probability Theory and Related Fields 128*, 2 (2004), 161–212.

[LIX34] CORTEEL, S., GOUPIL, A., AND SCHAEFFER, G. Content evaluation and class symmetric functions. *Advances in Mathematics 188*, 2 (2004).

[LIX35] DUCHON, P., FLAJOLET, P., LOUCHARD, G., AND SCHAEFFER, G. Boltzmann random sampling. *Combinatorics, Probability & Computing 13*, 4-5 (2004), 577–625.

[LIX36] ENGE, A., AND SCHERTZ, R. Constructing elliptic curves over finite fields using double eta-quotients. *Journal de Théorie des Nombres de Bordeaux 16* (2004), 555–568.

[LIX37] FLAJOLET, P., SALVY, B., AND SCHAEFFER, G. Airy phenomena and analytic combinatorics of connected graphs. *Electronic Journal of Combinatorics 11*, 1 (2004), #R34, 1–30.

[LIX38] FLIESS, M., JOIN, C., AND SIRA-RAMÍREZ, H. Robust residual generation for linear fault diagnosis : an algebraic setting with examples. *International Journal of Control 77*, 14 (2004), 1223–1242.

[LIX39] LIBERTI, L. Reduction constraints for the global optimization of nlps. *International Transactions in Operations Research 11*, 1 (2004), 34–41.

[LIX40] LIBERTI, L. Reformulation and convex relaxation techniques for global optimization. *4OR 2* (2004), 255–258.

[LIX41] MACIEJEWSKI, A., MOULIN-OLLAGNIER, J., AND NOWICKI, A. Generic polynomial vector fields are not integrable. *Indagationes mathematicae 15*, 1 (2004), 55–72.

[LIX42] MOULIN-OLLAGNIER, J. Algebraic closure of a rational function. *Qualitatitive Theory of Dynamical Systems 5*, 2 (2004), 285–300.

[LIX43] MOULIN-OLLAGNIER, J. Corrections and complements to "liouvillian integration of the lotka-volterra system". *Qualitatitive Theory of Dynamical Systems 5* (2004), 275–284.

[LIX44] MOULIN-OLLAGNIER, J. Simple darboux points of polynomial planar vector fields. *Journal of Pure and Applied Algebra 189* (2004), 247–262.

[LIX45] MOULIN-OLLAGNIER, J., AND NOWICKI, A. Constants and darboux polynomials for tensor products of polynomial algebras with derivations. *Communications in Algebra 33*, 1 (2004), 379–389.

[LIX46] PH. BAPTISTE, J. C., AND JOUGLET, A. A branch-and-bound procedure to minimize total tardiness on one machine with arbitrary release dates. *European Journal of Operational research 158* (2004), 595–608.

[LIX47] RECONSTRUCTORS, S. M. fliess and h. sira-ramirez. *Comptes rendus de l'académie des sciences, Mathématiques 338*, 1 (2004), 91–96.

2005

[LIX48] ARRIGHI, P., AND DOWEK, G. A computational definition of the notion of vectorial space. In *Proceedings of the Fifth International Workshop on Rewriting Logic and Its Applications (WRLA 2004)* (2005), Electronic Notes in Theoretical Computer Science 117, pp. 249–261.

[LIX49] BANK, B., GIUSTI, M., HEINTZ, J., AND PARDO, L. M. Generalized polar varieties : geometry and algorithms. *Journal of Complexity 21*, 4 (2005), 377–412.

[LIX50] BAPTISTE, P., AND PAPE, C. L. Scheduling a single machine to minimize a regular objective function under setup constraints. *Discrete Optimization 2* (2005), 83–99.

[LIX51] BASIRI, A., ENGE, A., FAUGÈRE, J.-C., AND GÜREL, N. The arithmetic of Jacobian groups of superelliptic cubics. *Math. Comp. 74* (2005), 389–410.

[LIX52] BLOCH, A., KROB, D., AND NG, A. Modeling commercial processes and customer behaviors to estimate the diffusion rate of new products. *Journal of Systems Science and Systems Engineering 14*, 4 (2005), 436–453.

[LIX53] BUHRMAN, H., DÜRR, C., HEILIGMAN, M., HØYER, P., MAGNIEZ, F., SANTHA, M., AND DE WOLF, R. Quantum algorithms for element distinctness. *SIAM J. Comput. 34*, 6 (2005), 1324–1330.

[LIX54] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. A framework for analyzing probabilistic protocols and its application to the partial secrets exchange. *Theoretical Computer Science* (2005). To appear. A short version of this paper appeared in the *Proceedings of the Symposium on Trustworthy Global Computing (TGC)*, volume 3705 of LNCS, pages 146-162. Springer, `http://www.lix.polytechnique.fr/~catuscia/papers/PartialSecrets/TCSreport.pdf`.

[LIX55] DUCHI, E., AND SCHAEFFER, G. A combinatorial approach of jumping particles. *Journal of Combinatorial Theory, Series A 110*, 1 (2005), 1–24.

[LIX56] DUPONT, R., ENGE, A., AND MORAIN, F. Building curves with arbitrary small MOV degree over finite prime fields. *J. of Cryptology 18*, 2 (2005), 79–89.

[LIX57] DURAND, A., HERMANN, M., AND KOLAITIS, P. G. Subtractive reductions and complete problems for counting complexity classes. *Theoretical Computer Science 340*, 3 (2005), 496–513.

[LIX58] ENGE, A., AND SCHERTZ, R. Modular curves of composite level. *Acta Arith. 118*, 2 (2005), 129–141.

[LIX59] FERNÁNDEZ, M., MACKIE, I., AND SINOT, F.-R. Closed reduction : explicit substitutions without alpha-conversion. *Mathematical Structures in Computer Science 15*, 2 (2005), 343–381.

[LIX60] FERNÁNDEZ, M., MACKIE, I., AND SINOT, F.-R. Interaction nets vs. the rho-calculus : Introducing bigraphical nets. *Electronic Notes in Theoretical Computer Science* (2005).

[LIX61] FERNÁNDEZ, M., MACKIE, I., AND SINOT, F.-R. Lambda-calculus with director strings. *Journal of Applicable Algebra in Engineering, Communication and Computing 15*, 6 (April 2005), 393–437.

[LIX62] FLIESS, M., JOIN, C., AND MOUNIER, H. An introduction to nonlinear fault diagnosis with an application to a congested internet router. *Advances in Communication Control Networks 338* (2005), 327–343.

[LIX63] FUSY, É. Quadratic exact size and linear approximate size random generation of planar graphs. *Discrete Mathematics and Theoretical Computer Science AD* (2005), 125–138.

[LIX64] GAUDRY, P., AND SCHOST, É. Modular equations for hyperelliptic curves. *Math. Comp. 74* (2005), 429–454.

[LIX65] GIUSTI, M., LECERF, G., SALVY, B., AND YAKOUBSOHN, J.-C. Location and approximation of clusters of zeroes of analytic functions. *Foundations of Computational Mathematics 5*, 3 (2005), 257–311.

[LIX66] GÜREL, N. Extracting bits from coordinates of a point of an elliptic curve. Preprint, `http://eprint.iacr.org/2005/324`, 2005.

[LIX67] HERNEST, M.-D., AND KOHLENBACH, U. A complexity analysis of functional interpretations. *Theoretical Computer Science 338, Issues 1-3* (2005), 200–246.

[LIX68] KROB, D., AND THIBON, J. Higher order peak algebras. *Annals of Combinatorics 9* (2005), 411–430.

[LIX69] KROB, D., AND VASSILIEVA, E. Performance evaluation of demodulation with diversity–a combinatorial approach ii : bijective methods. *Discrete Applied Mathematics 145*, 3 (2005), 403–421.

[LIX70] LIBERTI, L. Linearity embedded in nonconvex programs. *Journal of Global Optimization 33*, 2 (2005), 157–196.

[LIX71] LIBERTI, L., AND KUCHERENKO, S. Comparison of deterministic and stochastic approaches to global optimization. *International Transactions in Operations Research 12* (2005), 263–285.

[LIX72] PALAMIDESSI, C., AND HERESCU, O. M. A randomized encoding of the π-calculus with mixed choice. *Theoretical Computer Science 335*, 2-3 (2005), 373–404. `http://www.lix.polytechnique.fr/~catuscia/papers/prob_enc/report.pdf`.

[LIX73] SCHAEFFER, G., AND ZINN-JUSTIN, P. On the asymptotic number of planar curves and prime alternating knots. *Experimental Mathematics 13*, 4 (2005).

[LIX74] SINOT, F.-R. Director strings revisited : A generic approach to the efficient representation of free variables in higher-order rewriting. *Journal of Logic and Computation 15*, 2 (2005), 201–218.

[LIX75] SINOT, F.-R., AND MACKIE, I. Macros for interaction nets : A conservative extension of interaction nets. *Electronic Notes in Theoretical Computer Science 127*, 5 (2005).

[LIX76] VALENCIA, F. D. Decidability of infinite-state timed CCP processes and first-order LTL. *Theoretical Computer Science 330*, 3 (2005), 577–607.

[LIX77] VASSILIEVA, E., AND KROB, D. Performance evaluation of demodulation with diversity – a combinatorial approach ii : Bijective methods. *Discrete Applied Mathematics 145(3)* (2005), 403 – 421.

2006

[LIX78] BACHER, R., AND SCHAEFFER, G. On generating series of coloured planar trees. *Journal du Séminaire Lotharingien de Combinatoire 55* (2006).

[LIX79] BLIUDZE, S., AND KROB, D. A combinatorial approach to evaluation of reliability of the receiver output for BPSK modulation with spatial diversity. *Electronic Journal of Combinatorics 13*, 1 (2006).

[LIX80] BLIUDZE, S., AND KROB, D. Towards a functional formalism for modelling complex industrial systems. *ComPlexUs, special Issue : Complex Systems - European Conference 2005 2*, 3–4 (2006), 163–176.

[LIX81] BONICHON, N., GAVOILLE, N., HANUSSE, N. AND.POULALHON, D., AND SCHAEFFER, G. Planar graphs, via well orderly trees and triangulations. *Graph & Combinatorics 22*, 2 (2006), 185–202.

[LIX82] BOSTAN, A., FLAJOLET, P., SALVY, B., AND SCHOST, É. Fast computation of special resultants. *Journal of Symbolic Computation 41*, 1 (2006), 1–29.

[LIX83] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. Probable innocence revisited. *Theoretical Computer Science 367*, 1-2 (2006), 123–138. `http://www.lix.polytechnique.fr/~catuscia/papers/Anonymity/tcsPI.pdf`.

[LIX84] CHROBAK, M., DÜRR, C., JAWOR, W., KOWALIK, L., AND KUROWSKI, M. A note on scheduling equal-length jobs to maximize throughput. *Journal of Scheduling 9*, 1 (2006), 71–73.

[LIX85] CIRSTEA, H., FAURE, G., FERNÁNDEZ, M., MACKIE, I., AND SINOT, F.-R. New evaluation strategies for functional languages. *Electronic Notes in Theoretical Computer Science* (2006).

[LIX86] CREIGNOU, N., HERMANN, M., KROKHIN, A., AND SALZER, G. Complexity of clausal constraints over chains. *Theory of Computings Systems x*, x (2006), xx–xx. To appear.

[LIX87] DOWEK, G., , AND JIANG, Y. Eigenvariables, bracketing and the decidability of positive minimal predicate logic. *TCS 360* (2006), 193–208.

[LIX88] DUPONT, R. Fast evaluation of modular functions using Newton iterations and the AGM. *Math. Comp. XXX* (2006). To appear.

[LIX89] DUPONT, R., AND ENGE, A. Provably secure non-interactive key distribution based on pairings. *Discrete Applied Mathematics 154*, 2 (2006), 270–276.

[LIX90] DÜRR, C., HEILIGMAN, M., HØYER, P., AND MHALLA, M. Quantum query complexity of some graph problems. *SIAM J. of Computing 35*, 6 (2006), 1310–1328.

[LIX91] FLIESS, M. Analyse non standard du bruit. *C.R. Acad. Sci. Paris 342* (may 2006), 797–802.

[LIX92] GAUDRY, P., SCHOST, É., AND THIÉRY, N. M. Evaluation properties of symmetric polynomials. *International Journal on Algebra and Computation 16*, 3 (2006), 505–524.

[LIX93] GAUDRY, P., SCHOST, É., AND THIÉRY, N. M. Evaluation properties of symmetric polynomials. *Internat. J. Algebra Comput. 16*, 3 (2006), 505–523.

[LIX94] HERRANZ, J. Deterministic identity-based signatures for partial aggregation. *The Computer Journal 49*, 3 (2006), 322–330.

[LIX95] JOUANNAUD, J.-P., AND XU, W. Automatic complexity analysis for programs extracted from coq proof. *Electr. Notes Theor. Comput. Sci. 153*, 1 (2006), 35–53.

[LIX96] LIBERTI, L., AND PANTELIDES, C. An exact reformulation algorithm for large nonconvex nlps involving bilinear terms. *Journal of Global Optimization 36* (2006), 161–189.

[LIX97] NARBOUX, J. A graphical user interface for formal proofs in geometry. *the Journal of Automated Reasoning special issue on User Interface for Theorem Proving* (2006). to appear.

[LIX98] POULALHON, D., AND SCHAEFFER, G. Optimal coding and sampling of triangulations. *Algorithmica 46*, 3-4 (2006), 505–526.

[LIX99] SINOT, F.-R. Call-by-need in token-passing nets. *Mathematical Structures in Computer Science 16*, 4 (2006).

[LIX100] SINOT, F.-R. Token-passing nets : Call-by-need for free. *Electronic Notes in Theoretical Computer Science 135*, 3 (Mar. 2006), 129–139.

[LIX101] SIRA-RAMÍREZ, H., AND FLIESS, M. An algebraic state estimation approach for the recovery of chaotically encrypted messages. *International Journal of Bifurcation and Chaos 16*, 2 (2006), 295–309.

[LIX102] STRASSBURGER, L. On the axiomatisation of Boolean categories with and without medial, `http://arxiv.org/abs/cs.LO/0512086`, 2006. To appear in Theory and Applications of Categories.

[LIX103] VAN DEN ESSEN, A., MOULIN-OLLAGNIER, J., AND NOWICKI, A. Rings of constants of the form $k[f]$. *Communications in Algebra 34* (2006), 3315–3321.

2007

[LIX104] ARIOLA, Z. M., AND HERBELIN, H. Control reduction theories : the benefit of structural substitution. *Journal of Functional Programming* (2007). to appear.

[LIX105] ARIOLA, Z. M., HERBELIN, H., AND SABRY, A. A proof-theoretic foundation of abortive continuations. *Higher Order and Symbolic Computation* (2007). to appear.

[LIX106] ARIOLA, Z. M., HERBELIN, H., AND SABRY, A. A type-theoretic foundation of delimited continuations. *Higher Order and Symbolic Computation* (2007). to appear.

[LIX107] ARTIOUCHINE, K., AND BAPTISTE, P. Arc-b-consistency of the inter-distance constraint. *Constraints 12*, 1 (2007), 3–19.

[LIX108] BAPTISTE, P., BRUCKER, P., CHROBAK, M., DÜRR, C., KRAVCHENKO, S., AND SOURD, F. The complexity of mean flow time scheduling problems with release times. *Journal of Scheduling 10*, 2 (2007), 139–146.

[LIX109] BHASKAR, R., HERRANZ, J., AND LAGUILLAUMIE, F. Aggregate designated verifier signatures and application to secure routing. *International Journal of Security and Networks - Special Issue on Cryptography in Networks*, 3/4 (2007), 192–201.

[LIX110] BOSTAN, A., GAUDRY, P., AND SCHOST, É. Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator. *SIAM Journal on Computing 36*, 6 (2007), 1777–1806.

[LIX111] BOSTAN, A., MORAIN, F., SALVY, B., AND SCHOST, É. Fast algorithms for computing isogenies between elliptic curves. *Mathematics of Computation* (2007). à paraître.

[LIX112] BOSTAN, A., MORAIN, F., SALVY, B., AND SCHOST, É. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp. xxx* (2007), yyy. To appear.

[LIX113] CHARRON-BOST, B., AND SCHIPER, A. Harmful Dogmas in Fault-Tolerant Distributed Computing. In *The SIGACT News Distributed Computing Column* (2007), vol. 142, pp. 287–295. Available at http ://www.acm.org/sigactnews/online/.

[LIX114] CHAUDHURI, K., PFENNING, F., AND PRICE, G. A logical characterization of forward and backward chaining in the inverse method. To appear in the J. of Automated Reasoning, June 2007.

[LIX115] DENG, Y., AND PALAMIDESSI, C. Axiomatizations for probabilistic finite-state behaviors. *Theoretical Computer Science 373*, 1-2 (2007), 92–114. `http://www.lix.polytechnique.fr/~catuscia/papers/Prob_Axiom/tcs.pdf`.

[LIX116] E. VASSILIEVA, D. K., AND STEYAERT, J. M. Using geometrical properties for fast indexation of gaussian vector quantizers. *EURASIP Journal on Advances in Signal Processing 2007* (2007), Article ID 63192, 11 pages. doi :10.1155/2007/63192.

[LIX117] FLIESS, M. Probabilités et fluctuations quantiques (probabilities and quantum fluctuations). *Comptes rendus de l'académie des sciences, Mathématiques 344* (2007), 663–668.

[LIX118] FLIESS, M., JOIN, C., AND SIRA-RAMIREZ, H. Non-linear estimation is easy. *Int. J. Modelling, Identification and Control* (2007).

[LIX119] GAUDRY, P. Fast genus 2 arithmetic based on Theta functions. *Journal of Mathematical Cryptology 1* (2007), 243–265.

[LIX120] GAUDRY, P., THOMÉ, E., THÉRIAULT, N., AND DIEM, C. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comp. 76* (2007), 475–492.

[LIX121] GIUSTI, M., LECERF, G., SALVY, B., AND YAKOUBSOHN, J.-C. On location and approximation of clusters of zeroes : case of embedding dimension one. *Foundations of Computational Mathematics 7*, 1 (2007), 1–58.

[LIX122] HERMANN, M. On Boolean primitive positive clones. *Discrete Mathematics x*, x (2007), xx–xx.

[LIX123] JOUANNAUD, J.-P., AND MACKIE, I. Preface. *Electr. Notes Theor. Comput. Sci. 171*, 3 (2007), 1–2.

[LIX124] JOUANNAUD, J.-P., AND RUBIO, A. Polymorphic higher-order recursive path orderings. *J. ACM 54*, 1 (2007), 1–48.

[LIX125] KROB, D., STEYAERT, J., AND VASSILIEVA, E. Using geometrical properties for fast indexation of gaussian vector quantizers. *EURASIP Journal on Applied Signal Processing* (2007).

[LIX126] LAVOR, C., LIBERTI, L., MACULAN, N., AND CHAER NASCIMENTO, M. Solving hartree-fock systems with global optimization metohds. *Europhysics Letters 5*, 77 (2007), 50006p1–50006p5.

[LIX127] MACIEJEWSKI, A., MOULIN-OLLAGNIER, J., AND NOWICKI, A. Correction and complements à l'article : Generic polynomial vector fields are not integrable. *Indagationes mathematicae* (2007). à paraître.

[LIX128] MORAIN, F. Computing the cardinality of CM elliptic curves using torsion points. To appear in *J. Théor. Nombres Bordeaux.*, `http://arxiv.org/ps/math.NT/0210173`, June 2007.

[LIX129] MORAIN, F. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm. *Math. Comp. 76* (2007), 493–505.

[LIX130] OLLIVIER, F., MOUTAOUAKIL, S., AND SADIK, B. Une méthode d'identification pour un système linéaire à retards. *Comptes rendus de l'académie des sciences, Mathématiques 344*, 11 (2007), 709–714.

[LIX131] OLLIVIER, F., AND SADIK, B. La borne de jacobi pour une diffiété définie par un système quasi régulier. *Comptes rendus de l'académie des sciences, Mathématiques 345*, 3 (2007), 139–144.

[LIX132] PHILLIPS, I., VIGLIOTTI, M. G., AND PALAMIDESSI, C. Expressiveness via leader election problems. *Theoretical Computer Science* (2007). to appear.

[LIX133] STRASSBURGER, L. On the axiomatisation of Boolean categories with and without medial, 2007. Accepted for publication in *TAC*.

[LIX134] WIDDER, J., AND SCHMID, U. Booting clock synchronization in partially synchronous systems with hybrid process and link failures. *Distributed Computing 20*, 2 (Aug. 2007), 115–140.

[LIX135] WINTER, E., AND BAPTISTE, P. On scheduling a multifunction radar. *Aerospace Science and Technology 11*, 4 (2007), 289–294.

2008

[LIX136] ARTIOUCHINE, K., BAPTISTE, P., AND DURR, C. Runway sequencing with holding patterns. *European Journal of Operational Research* (2008). To appear.

[LIX137] ARTIOUCHINE, K., BAPTISTE, P., AND MATTIOLI, J. The k king problem, an abstract model for computing aircraft landing trajectories : On modeling a dynamic hybrid system with constraints. *INFORMS Journal on Computing* (2008). To appear.

[LIX138] BAPTISTE, P., FLAMINI, M., AND SOURD, F. Lagrangian bounds for just-in-time job-shop scheduling. *Computers & Operations Research 35* (2008), 906–915.

[LIX139] BAPTISTE, P., JOUGLET, A., AND SAVOUREY, D. Lower bounds for parallel machine scheduling problems. *International Journal of Operational Research* (2008). To appear.

[LIX140] CHATZIKOKOLAKIS, K., PALAMIDESSI, C., AND PANANGADEN, P. Anonymity protocols as noisy channels. *Information and Computation* (2008). To appear.

[LIX141] JAWOR, W., CHROBAK, M., AND DÜRR, C. Competitive analysis of scheduling algorithms for aggregated links. *Algorithmica* (2008).

[LIX142] JOUGLET, A., SAVOUREY, D., CARLIER, J., AND BAPTISTE, P. Dominance-based heuristics for one-machine total cost scheduling problems. *European Journal of Operational Research* (2008). To appear.

[LIX143] KUCHERENKO, S., BELOTTI, P., LIBERTI, L., AND MACULAN, N. New formulations for the kissing number problem. *Discrete Applied Mathematics* (2008). to appear.

[LIX144] LASSAIGNE, R., AND PEYRONNET, S. Probabilistic verification and approximation. *Annals of Pure and Applied Logic* (2008). to appear.

[LIX145] LIBERTI, L. Compact linearization of binary quadratic problems. *4OR* (2008). to appear.

[LIX146] LIBERTI, L. Spherical cuts for integer programming problems. *International Transactions in Operations Research* (2008). accepted for publication.

[LIX147] LIBERTI, L., LAVOR, C., MACULAN, N., AND MARINELLI, F. Double variable neighbourhood search with smoothing for the molecular distance geometry problem. *Journal of Global Optimization* (2008). accepted for publication.

National journals

2004

[LIX148] DOWEK, G. La théorie des types et les systèmes informatiques de traitement des démonstrations mathématiques. *Mathématiques et Sciences Humaines 165* (2004), 13–29.

[LIX149] LIBERTI, L. On a class of nonconvex problems where all local minima are global. *Publications de l'Institut Mathémathique 76*, 90 (2004), 101–109.

2005

[LIX150] DAC, H. T., AND BAPTISTE, P. Airspace sectorization with constraints. *RAIRO Operations Research 39* (2005), 105–122.

[LIX151] LIBERTI, L., AMALDI, E., MACULAN, N., AND MAFFIOLI, F. Mathematical models and a constructive heuristic for finding minimum fundamental cycle bases. *Yugoslav Journal of Operations Research 15*, 1 (2005).

2008

[LIX152] CASEAU, Y., KROB, D., AND PEYRONNET, S. Complexité des systemes d'information : une famille de mesures de la complexité scalaire d'un schema d'architecture. *Génie Logiciel* (2008). A paraitre.

International conferences with proceedings

2004

[LX153] ABADI, M., GONTHIER, G., AND WERNER, B. Choice in dynamic linking. In Walukiewicz [468], pp. 12–26.

[LX154] AMALDI, E., LIBERTI, L., MACULAN, N., AND MAFFIOLI, F. Efficient edge-swapping heuristics for finding minimum fundamental cycle bases. In Ribeiro and Martins [466], pp. 15–29.

[LX155] AMALDI, E., LIBERTI, L., MAFFIOLI, F., AND MACULAN, N. Algorithms for finding minimum fundamental cycle bases in graphs. In Liberti and Maffioli [5], pp. 29–33.

[LX156] ARIOLA, Z. M., HERBELIN, H., AND SABRY, A. A type-theoretic foundation of continuations and prompts. In *Proceedings of the Ninth ACM SIGPLAN International Conference on Functional Programming (ICFP '04), Snowbird, Utah, September 19-21, 2004* (2004), ACM, pp. 40–53.

[LX157] BAPTISTE, P., AND BRUCKER, P. Scheduling parallel machines to minimize total completion time and total number of late jobs. In *Proceedings of the Proc. of the 9th International Workshop on Project Management and Scheduling* (2004).

[LX158] BAPTISTE, P., AND SOURD, F. Lower bounds for the earliness-tardiness scheduling problem on parallel machines. In *Proceedings of the Proc. of the 9th International Workshop on Project Management and Scheduling* (2004).

[LX159] BASIRI, A., ENGE, A., FAUGÈRE, J.-C., AND GÜREL, N. Implementing the arithmetic of $C_{3,4}$ curves. In *Algorithmic Number Theory — ANTS-VI* (Berlin, 2004), D. Buell, Ed., vol. 3076 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 87–101.

[LX160] BAULAND, M., CHAPDELAINE, P., CREIGNOU, N., HERMANN, M., AND VOLLMER, H. An algebraic approach to the complexity of generalized conjunctive queries. In *Proceedings 7th International Conference on Theory and Applications of Satisfiability Testing, (SAT 2004), Vancouver (British Columbia, Canada)* (May 2004), H. H. Hoos and D. G. Mitchell, Eds., vol. 3542 of *Lecture Notes in Computer Science*, "Springer-Verlag", pp. 30–45.

[LX161] BOSTAN, A., GAUDRY, P., AND SCHOST, É. Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves. In *Finite Fields and Applications, 7th International Conference, Fq7* (2004), G. Mullen, A. Poli, and H. Stichtenoth, Eds., vol. 2948 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 40–58.

[LX162] CHARRON-BOST, B., AND LE FESSANT, F. Validity conditions in agreement problems and time complexity. In *Proceedings 30th Annual Conference on Current Trends in Theory and Practice of Informatics* (2004), vol. 2234 of *Lecture Notes in Computer Science*, Springer, pp. 196–207.

[LX163] COEN, C. S. A semi-reflexive tactic for (sub-)equational reasoning. In Filliâtre et al. [18], pp. 98–114.

[LX164] CORBINEAU, P. First-order reasoning in the Calculus of Inductive Constructions. In Berardi et al. [462], pp. 162–177.

[LX165] DAHAN, X., AND SCHOST, É. Sharp estimates for triangular sets. In *ISSAC '04 : Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation* (2004), ACM Press, pp. 103–110.

[LX166] FLECK, C., PAULUS, T., SCHÖNBOHM, A., ABEL, D., AND OLLIVIER, F. Flatness based open loop control for the twin roll strip casting process. In *Symposium on Nonlinear Control Systems (NOLCOS-2004)* (2004).

[LX167] FLIESS, M., AND SIRA-RAMIREZ, H. Control via state estimations of some nonlinear systems. In *IFAC Symposium on Nonlinear Control Systtems (NOLCOS 2004)* (2004).

[LX168] FRANKE, J., KLEINJUNG, T., MORAIN, F., AND WIRTH, T. Proving the primality of very large numbers with fastecpp. In *Algorithmic Number Theory* (2004), D. Buell, Ed., vol. 3076 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 194–207. 6th International Symposium, ANTS-VI, Burlington, VT, USA, June 2004, Proceedings.

[LX169] GABBAY, M. J., AND CHENEY, J. A sequent calculus for nominal logic. In *Proc. 19th IEEE Symposium on Logic in Computer Science (LICS 2004)* (2004), pp. 139–148.

[LX170] GAUDRY, P., AND SCHOST, É. Construction of secure random curves of genus 2 over prime fields. In *Advances in Cryptology – EUROCRYPT 2004* (2004), C. Cachin and J. Camenisch, Eds., vol. 3027 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 239–256.

[LX171] GAUDRY, P., AND SCHOST, É. A low memory parallel version of Matsuo, Chao and Tsujii's algorithm. In *ANTS-VI* (2004), D. Buell, Ed., vol. 3076 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 208–222.

[LX172] GIAMBIAGI, P., SCHNEIDER, G., AND VALENCIA, F. D. On the expressiveness of infinite behavior and name scoping in process calculi. In *Proceedings of the 7th International Conference on the Foundations of Software Science and Computation Structures (FOSSACS 2004)* (2004), I. Walukiewicz, Ed., vol. 2987 of *Lecture Notes in Computer Science*, Springer, pp. 226–240.

[LX173] GIL, A., HERMANN, M., SALZER, G., AND ZANUTTINI, B. Efficient algorithms for constraint description problems over finite totally ordered domains. In *Proceedings 2nd International Joint Conference on Automated Reasoning (IJCAR'04). Cork (Ireland)* (July 2004), D. Basin and M. Rusinowitch, Eds., vol. 3097 of *Lecture Notes in Computer Science*, "Springer-Verlag", pp. 244–258.

[LX174] GOTTLOB, G., HERMANN, M., AND RUSINOWITCH, M. 2nd International Workshop on Complexity in Automated Deduction (CiAD) – Foreword. *Theory of Computings Systems 37*, 6 (2004), 639–640.

[LX175] JOUANNAUD, J.-P. Theorem proving languages for verification. In Wang [469], pp. 11–14.

[LX176] LIBERTI, L., MACULAN, N., AND KUCHERENKO, S. The kissing number problem : a new result from global optimization. In Liberti and Maffioli [5], pp. 203–207.

[LX177] MILLER, D. Bindings, mobility of bindings, and the ∇-quantifier. In *18th International Workshop CSL 2004* (2004), J. Marcinkowski and A. Tarlecki, Eds., vol. 3210 of *LNCS*, p. 24.

[LX178] NARBOUX, J. A decision procedure for geometry in coq. In *Proceedings of TPHOLs'2004* (2004), S. Konrad, B. Annett, and G. Ganesh, Eds., vol. 3223 of *Lecture Notes in Computer Science*, Springer-Verlag.

[LX179] RUEDA, C., AND VALENCIA, F. Non-viability deductions in arc-consistency computation. In *Proc. of the Nineteenth International Conference on Logic Programming (ICLP 2004)* (2004), LNCS, Springer-Verlag.

[LX180] TIU, A., AND MILLER, D. A proof search specification of the π-calculus. In *3rd Workshop on the Foundations of Global Ubiquitous Computing* (Sept. 2004), vol. 138 of *ENTCS*, pp. 79–101.

2005

[LX181] ALEARDI, L. C., DEVILLERS, O., AND SCHAEFFER, G. Dynamic updates of succinct triangulations. In *Proc. of 17th Canadian Conference on Computational Geometry (CCCG)* (2005), pp. 135–138.

[LX182] ALEARDI, L. C., DEVILLERS, O., AND SCHAEFFER, G. Succinct representation of triangulations with a boundary. In *Proc. 9th Workshop on Algorhtms and Data Structures (WADS)* (2005), vol. 3608 of *LNCS*, Springer, pp. 134–145.

[LIX183] ARTIOUCHINE, K., AND BAPTISTE, P. Inter-distance constraint : An extension of the all-different constraint for scheduling equal length jobs. In *Proc. of the 11th International Conference, CP (Principles and Practice of Constraint Programming)* (Sitges, Spain, 2005), vol. 3709 of *Lecture Notes in Computer Science*.

[LIX184] BAPTISTE, P., CHROBAK, M., DURR, C., AND SOURD, F. Preemptive multi-machine scheduling of equal length jobs to minimize the average flow time. In *Models and Algorithms for Planning and Scheduling Problems, Siena, Italy* (2005).

[LIX185] BARRAS, B., AND GRÉGOIRE, B. On the role of type decorations in the calculus of inductive constructions. In *CSL'05* (2005), LNCS, Springer-Verlag.

[LIX186] BHARGAVA, M., AND PALAMIDESSI, C. Probabilistic anonymity. In *Proceedings of CONCUR* (2005), M. Abadi and L. de Alfaro, Eds., vol. 3653 of *Lecture Notes in Computer Science*, Springer, pp. 171–185. `http://www.lix.polytechnique.fr/~catuscia/papers/Anonymity/concur.pdf`.

[LIX187] BLIUDZE, S., BILLY, N., AND KROB, D. On optimal Hybrid ARQ control schemes for HSDPA with 16QAM. In *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'2005)* (2005), J. Conan and S. Pierre, Eds., vol. 1, IEEE, pp. 121–127.

[LIX188] BLIUDZE, S., AND KROB, D. Performance evaluation of demodulation with diversity - a combinatorial approach iii : Analysis of the threshold case. In *Proceedings of the 7th Workshop on Algorithm Engineering and Experiments and the 2nd Workshop on Analytic Algorithmics and Combinatorics (ANALCO'05)* (2005), C. Demetrescu, R. Sedgewick, and R. Tamassia, Eds., SIAM, pp. 195–205.

[LIX189] BLIUDZE, S., AND KROB, D. Towards a functional formalism for modelling complex industrial systems. In *European Conference on Complex Systems (ECCS' 05)* (2005), P. Bourgine, F. Kepes, and M. Schoenauer, Eds.

[LIX190] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. A framework for analyzing probabilistic protocols and its application to the partial secrets exchange. In *Proceedings of the Symp. on Trustworthy Global Computing* (2005), vol. 3705 of *Lecture Notes in Computer Science*, Springer, pp. 146–162. `http://www.lix.polytechnique.fr/~catuscia/papers/PartialSecrets/tgc05.pdf`.

[LIX191] CHOTHIA, T., AND CHATZIKOKOLAKIS, K. A survey of anonymous peer-to-peer file-sharing. In *Proceedings of the IFIP International Symposium on Network-Centric Ubiquitous Systems (NCUS 2005)* (2005), vol. 3823 of *Lecture Notes in Computer Science*, Springer, pp. 744–755.

[LIX192] DAHAN, X., MORENO MAZA, M., SCHOST, É., WU, W., AND XIE, Y. Lifting techniques for triangular decompositions. In *ISSAC'05* (2005), ACM, pp. 108–115.

[LIX193] DENG, Y., AND PALAMIDESSI, C. Axiomatizations for probabilistic finite-state behaviors. In *Proceedings of FOSSACS'05* (2005), vol. 3441 of *Lecture Notes in Computer Science*, Springer, pp. 110–124. `http://www.lix.polytechnique.fr/~catuscia/papers/Prob_Axiom/fossacs05.pdf`.

[LIX194] DOWEK, G. What do we know when we know that a theory is consistent ?. In Nieuwenhuis [481], pp. 1–6.

[LIX195] DOWEK, G. What do we know when we know that a theory is consistent. In *Automated Deduction* (2005), R. Nieuwenhuis, Ed., Lecture Notes in Artificial Intelligence, 3632, Springer-Verlag, pp. 1–6.

[LIX196] DOWEK, G., AND WERNER, B. Arithmetic as a theory modulo. In *Term rewriting and applications* (2005), J. Giesel, Ed., Lecture Notes in Computer Science 3467, Springer-Verlag, pp. 423–437.

[LIX197] DUCHI, E., AND SCHAEFFER, G. A combinatorial approach to jumping particles : the parallel tasep. In *Proc. 17th Intl. Conf. Formal Power Series and Algebraic Combinatorics* (Taormina, 2005).

[LIX198] FLIESS, M., JOIN, C., MBOUP, M., AND SEDOGLAVIC, A. Estimation des dérivées d'un signal multidimensionnel avec applications aux images et aux vidéos. In *Actes* 20^e *coll. GRETSI* (2005).

[LIX199] FLIESS, M., JOIN, C., MBOUP, M., AND SIRA-RAMÍREZ, H. Analyse et représentation de signaux transitoires : application à la compression, au débruitage et à la détection de ruptures. In *Actes* 20^e *coll. GRETSI* (2005).

[LIX200] FUSY, É. Transversal structures on triangulations, with application to straight-line drawing. In *Proceedings of Graph Drawing'05* (2005), vol. 3843 of *LNCS*, Springer, pp. 177–188. Full paper to be published in Discr. Math., available at `http ://arxiv.org/abs /math.CO/0602163`.

[LIX201] FUSY, É., POULALHON, D., AND SCHAEFFER, G. Dissections and trees, with applications to optimal mesh encoding and to random sampling. In *16th Annual ACM-SIAM Symposium on Discrete Algorithms* (2005). Full paper to be published in Transactions on Algorithms, available at `http ://algo.inria.fr/fusy /Articles/FuPoScArticle.pdf`.

[LIX202] GOUBAULT-LARRECQ, J., AND JOUANNAUD, J.-P. Finite semantic trees suffice for ordered resolution and paramodulation. In *Workshop on Programming Logics in memory of Harld Ganzinger* (june 2005), LNCS, Springer-Verlag.

[LIX203] HERBELIN, H. On the degeneracy of sigma-types in presence of computational classical logic. In *Seventh International Conference, TLCA '05, Nara, Japan. April 2005, Proceedings* (2005), P. Urzyczyn, Ed., vol. 3461 of *Lecture Notes in Computer Science*, Springer, pp. 209–220.

[LIX204] HERNEST, D.-M. Light functional interpretation. In *Computer Science Logic : 19th International Workshop, CSL 2005* (2005), L. Ong, Ed., vol. 3634 of *Lecture Notes in Computer Science*, pp. 477–492.

[LIX205] JOIN, C., SIRA-RAMÍREZ, H., AND FLIESS, M. Control of an uncertain three-tank-system via on-line parameter identification and fault detection. In *IFAC World Congress on Automatic Control* (2005), IFAC.

[LIX206] JOUANNAUD, J.-P. Higher-order rewriting : Framework, confluence and termination. In Middeldorp et al. [480], pp. 224–250.

[LIX207] JOUANNAUD, J.-P. Twenty years later. In Giesl [471], pp. 368–375.

[LIX208] KROB, D., AND NG, A. Understanding the diffusion rate of new products through a simple customer behaviour model. In *IEEE 2005 International Conference on Services Systems and Services Management (ICSSSM'05)* (2005), J. Chen, Ed., vol. 1, IEEE, pp. 237–243.

[LIX209] LAGUILLAUMIE, F., PAILLIER, P., AND VERGNAUD, D. Universally convertible directed signatures. In *Advances in Cryptology - Asiacrypt 2005* (2005), B. Roy, Ed., vol. 3788 of *Lecture Notes in Comput. Sci.*, Springer, pp. 682–701.

[LIX210] LAGUILLAUMIE, F., AND VERGNAUD, D. Short undeniable signatures without random oracles : the missing link. In *Progress in Cryptology - Indocrypt 2005* (2005), R. V. S. Maitra, C. E. Veni Madhavan, Ed., vol. 3797 of *Lecture Notes in Comput. Sci.*, Springer, pp. 283–296.

[LIX211] LAVOR, C., LIBERTI, L., AND MACULAN, N. Grover's algorithm applied to the molecular distance geometry problem. In *Proc. of VII Brazilian Congress of Neural Networks, Natal, Brazil* (2005).

[LIX212] LIBERTI, L., AND DRAŽIC, M. Variable neighbourhood search for the global optimization of constrained nlps. In *Proceedings of GO Workshop, Almeria, Spain* (2005).

[LIX213] LIBERTI, L., LAVOR, C., AND MACULAN, N. Double vns for the molecular distance geometry problem. In *Proc. of Mini Euro Conference on Variable Neighbourhood Search, Tenerife, Spain* (2005).

[LIX214] MILLER, D., AND SAURIN, A. A game semantics for proof search : Preliminary results. In *GaLoP 2005 : Games for Logic and Programming Languages* (2005), D. Ghica and G. McCusker, Eds.

[LIX215] MILLER, D., AND SAURIN, A. A game semantics for proof search : Preliminary results. In *Proceedings of the Mathematical Foundations of Programming Semantics (MFPS)* (2005).

[LIX216] MILLER, D., AND TIU, A. A proof theory for generic judgments. *ACM Trans. on Computational Logic 6*, 4 (Oct. 2005), 749–783.

[LIX217] PALAMIDESSI, C., PHILLIPS, I., AND VIGLIOTTI, M. G. Expressiveness via leader election problems. In *Postproceedings of the 4th International Symposium on Formal Methods for Components and Objects (FMCO)* (2005), F. S. de Boer, M. M. Bonsangue, S. Graf, and W. P. de Roever, Eds., vol. 4111 of *Lecture Notes in Computer Science*, Springer, pp. 172–194. `http://www.lix.polytechnique.fr/~catuscia/papers/2006/MariaGrazia/FMCO/fmco-06.pdf`.

[LIX218] PAPE, C. L., AND BAPTISTE, P. Scheduling a single machine to minimize a regular objective function under setup constraints. In *2nd Multidisciplinary International Conference on Scheduling : Theory and Applications* (2005).

[LIX219] PIMENTEL, E., AND MILLER, D. On the specification of sequent systems. In *LPAR 2005 : 12th International Conference on Logic for Programming, Artificial Intelligence and Reasoning* (2005), no. 3835 in LNAI, pp. 352–366.

[LIX220] REGER, J., SIRA-RAMÍREZ, H., AND FLIESS, M. On non-asymptotic observation of nonlinear systems. In *Proc. CDC-ECC'05* (2005).

[LIX221] SAURIN, A. Separation with streams in the $\lambda\mu$-calculus. In *20th IEEE Symposium on Logic in Computer Science (LICS 2005)* (2005), IEEE Computer Society, pp. 356–365.

[LIX222] SCHOST, É. Multivariate power series multiplication. In *International Symposium on Symbolic and Algebraic Computation, ISSAC'05* (2005), ACM, pp. 293–300.

[LIX223] SINOT, F.-R. Call-by-name and call-by-value as token-passing interaction nets. In *Proceedings of Typed Lambda Calculi and Applications (TLCA'05)* (2005), vol. 3461 of *Lecture Notes in Computer Science*, pp. 386–400.

[LIX224] TIU, A., NADATHUR, G., AND MILLER, D. Mixing finite success and finite failure in an automated prover. In *Proceedings of ESHOL'05 : Empirically Successful Automated Reasoning in Higher-Order Logics* (December 2005), pp. 79 – 98.

[LIX225] ZIEGLER, A., MILLER, D., AND PALAMIDESSI, C. A congruence format for name-passing calculi. In *Proceedings of SOS 2005 : Structural Operational Semantics* (Lisbon, Portugal, July 2005), Electronic Notes in Theoretical Computer Science, Elsevier Science B.V., pp. 169–189.

2006

[LIX226] ALEARDI, L. C., DEVILLERS, O., AND MEBARKI, A. 2d triangulation representation using stable catalogs. In *Proc. of 18th Canadian Conference on Computational Geometry (CCCG)* (2006), pp. 71–74.

[LIX227] ALEARDI, L. C., DEVILLERS, O., AND SCHAEFFER, G. Optimal succinct representations of planar maps. In *Proc. of 22nd ACM Annual Symposium on Computational Geometry (SoCG)* (2006), pp. 309–318.

[LIX228] BAHADUR, A., DÜRR, C., KULKARNI, R., AND LAFAYE, T. Quantum query complexity in computational geometry. In *Proc. of the Conference on Quantum Information and Computation IV by The International Society for Optical Engineering (SPIE)* (2006).

[LIX229] BAPTISTE, P. Scheduling unit tasks to minimize the number of idle periods : A polynomial time algorithm for offline dynamic power management. In *Proc. of SODA'06, ACM-SIAM Symposium on Discrete Algorithms* (2006).

[LIX230] BAPTISTE, P., AND SADYKOV, R. Compact mip formulations for minimizing total weighted tardiness. In *10th International Workshop on Project Management and Scheduling* (2006).

[LIX231] BELKOURA, L., RICHARD, J.-P., AND FLIESS, M. On-line identification of systems with delayed inputs. In *MTNS'06, 16th Conf. Mathematical Theory of Networks & Systems* (2006).

[LIX232] BENJAMIN GRÉGOIRE, L. T., AND WERNER, B. A computational approach to pocklington certificates in type theory. In *FLOPS 2006* (2006), M. Hagiya and P. Wadler, Eds., vol. 3945 of *LNCS*, Springer.

[LIX233] BHASKAR, R., HERRANZ, J., AND LAGUILLAUMIE, F. Efficient authentication for reactive routing protocols. In *AINA'06 (SNDS'06)* (2006), vol. II, IEEE Computer Society, pp. 57–61.

[LIX234] BLANQUI, F., JOUANNAUD, J.-P., AND RUBIO, A. Higher-order termination : From kruskal to computability. In Hermann and Voronkov [482], pp. 1–14.

[LIX235] BODINI, O., FUSY, É., AND PIVOTEAU, C. Random sampling of plane partitions. In *Gascom 2006* (Dijon, France, 2006), R. Pinzani and V. Vajnovszki, Eds., LE2I, pp. 124–135.

[LIX236] BRUGLIERI, M., AND LIBERTI, L. Modelling the optimal design of a biomass-based energy production process. In *ORMMES Conference Proceedings* (Coimbra, 2006).

[LIX237] CACCIAGRANO, D., CORRADINI, F., AND PALAMIDESSI, C. Fair π. In *Proceedings of the 13th International Workshop on Expressiveness in Concurrency (EXPRESS)* (2006), Electronic Notes in Theoretical Computer Science, Elsevier Science B.V.

[LIX238] CACCIAGRANO, D., CORRADINI, F., AND PALAMIDESSI, C. Separation of synchronous and asynchronous communication via testing. *Theoretical Computer Science* (2006). To appear. `http://www.lix.polytechnique.fr/~catuscia/papers/Diletta/Must/tcs.pdf`.

[LIX239] CACCIAGRANO, D., CORRADINI, F., AND PALAMIDESSI, C. Separation of synchronous and asynchronous communication via testing. In *Proceedings of the 12th International Workshop on Expressiveness in Concurrency (EXPRESS 2005)* (San Francisco, USA, 2006), vol. 154 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 95–108. `http://www.lix.polytechnique.fr/~catuscia/papers/Diletta/Must/report.pdf`.

[LIX240] CHARRON-BOST, B., AND SCHIPER, A. Improving Fast Paxos : being optimistic with no overhead. In *Proceedings of the 12th Pacific Rim Int. Symp. on Dependable Computing (PRDC)* (2006), LNCS-2485, pp. 287–295.

[LIX241] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. Probable innocence revisited. In *Third International Workshop on Formal Aspects in Security and Trust (FAST 2005), Revised Selected Papers* (2006), T. Dimitrakos, F. Martinelli, P. Y. A. Ryan, and S. A. Schneider, Eds., vol. 3866 of *Lecture Notes in Computer Science*, Springer, pp. 142–157.

[LIX242] CHATZIKOKOLAKIS, K., PALAMIDESSI, C., AND PANANGADEN, P. Anonymity protocols as noisy channels. In *Proceedings of the Symposium on Trustworthy Global Computing (TGC)* (2006), vol. 4661 of *Lecture Notes in Computer Science*, Springer, pp. 281–300. `http://www.lix.polytechnique.fr/~catuscia/papers/Anonymity/Channels/tgc.pdf`.

[LIX243] CHRZASZCZ, J., AND JOUANNAUD, J.-P. From obj to ml to coq. In Futatsugi et al. [256], pp. 216–234.

[LIX244] DAAFOUZ, J., FLIESS, M., AND MILLERIOUX, G. Une approche intrinsèque des observateurs linéaires à entrées inconnues. In *Conf. Internat. Francophone d'Automatique (CIFA), Bordeaux, France* (2006).

[LIX245] DAHAN, X., JIN, X., , MAZA, M. M., AND SCHOST, E. Change of ordering for regular chains in positive dimension. In *Maple conference 2006* (2006), I. Kotsireas Ed.

[LIX246] DAHAN, X., MORENO MAZA, M., SCHOST, É., AND XIE, Y. On the complexity of the D5 principle. In *Transgressive Computing* (2006), pp. 149–168.

[LIX247] DENG, Y., CHOTHIA, T., PALAMIDESSI, C., AND PANG, J. Metrics for action-labelled quantitative transition systems. In *Proceedings of the Third Workshop on Quantitative Aspects of Programming Languages (QAPL 2005)* (2006), vol. 153 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science Publishers, pp. 79–96. `http://www.lix.polytechnique.fr/~catuscia/papers/Metrics/QAPL/gts.pdf`.

[LIX248] DENG, Y., PANG, J., AND WU, P. Measuring anonymity with relative entropy. In *Proceedings of the 4th International Workshop on Formal Aspects in Security and Trust (FAST)* (2006), Lecture Notes in Computer Science, Springer. To appear.

[LIX249] DOWEK, G. Truth values algebras and proof normalization. In Altenkirch and McBride [488], pp. 110–124.

[LIX250] DUCHI, E., RINALDI, S., AND SCHAEFFER, G. The number of z-convex polyominos. In *Proc. 18th Intl. Conf. Formal Power Series and Algebraic Combinatorics* (San Diego, 2006).

[LIX251] DÜRR, C., AND HURAND, M. Finding total unimodularity in optimization problems solved by linear programs. In *Proc. of the 14th Annual European Symposium on Algorithms (ESA)* (2006), pp. 315–326.

[LIX252] FILATEI, A., LI, X., MORENO MAZA, M., AND SCHOST, É. Implementation techniques for fast polynomial arithmetic in a high-level programming environment. In *ISSAC'06* (2006), pp. 93–100.

[LIX253] FLIESS, M., JOIN, C., MBOUP, M., AND SIRA-RAMÍREZ, H. Vers une commande multivariable sans modèle. In *Conférence internationale francophone d'automatique (CIFA 2006)* (2006).

[LIX254] FLIESS, M., JOIN, C., AND SIRA-RAMÍREZ, H. Complex continuous nonlinear systems : Their black box identification and their control. In *Proc. 14th IFAC Symposium on System Identification (SYSID 2006)* (2006).

[LIX255] FUSY, É. Straight-line drawing of quadrangulations. In *Proceedings of Graph Drawing'06* (2006), vol. 4372 of *LNCS*, Springer, pp. 234–239.

[LIX256] FUTATSUGI, K., JOUANNAUD, J.-P., AND MESEGUER, J., Eds. *Algebra, Meaning, and Computation, Essays Dedicated to Joseph A. Goguen on the Occasion of His 65th Birthday* (2006), vol. 4060 of *Lecture Notes in Computer Science*, Springer.

[LIX257] GALINDO, D., AND HERRANZ, J. A generic construction for token-controlled public key encryption. In *Financial Cryptography and Data Security* (2006), G. D. Crescenzo and A. Rubin, Eds., vol. 4107 of *Lecture Notes in Comput. Sci.*, Springer Verlag, pp. 177–190. 10th International Conference, FC 2006 Anguilla, British West Indies, February 27-March 2.

[LIX258] GAUDRY, P., HOUTMANN, T., KOHEL, D., RITZENTHALER, C., AND WENG, A. The 2-adic CM method for genus 2 with application to cryptography. In *Advances in Cryptology – ASIACRYPT 2006* (2006), X. Lai and K. Chen, Eds., vol. 4284 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 114–129.

[LIX259] GAUDRY, P., AND MORAIN, F. Fast algorithms for computing the eigenvalue in the Schoof-Elkies-Atkin algorithm. In *ISSAC '06 : Proceedings of the 2006 international symposium on Symbolic and algebraic computation* (New York, NY, USA, 2006), ACM Press, pp. 109–115.

[LIX260] GUTIERREZ, J., PEREZ, J., RUEDA, C., AND VALENCIA, F. Timed concurrent constraint programming for analyzing biological systems. In *Proceedings of Workshop on Membrane Computing and Biologically Inspired Process Calculi* (2006), Electronic Notes in Theoretical Computer Science, Elsevier Science B.V. to appear.

[LIX261] HERMANN, M., AND VORONKOV, A., Eds. *Proceedings 13th International Conference : Logic for Programming, Artificial Intelligence, and Reasoning (LPAR 2006)* (Phnom Penh (Cambodia), Nov. 2006), vol. 4246 of *Lecture Notes in Artificial Intelligence*, Springer Verlag.

[LIX262] HERRANZ, J., AND LAGUILLAUMIE, F. Blind ring signatures secure under the chosen target CDH assumption. In *Information Security, ISC 2006* (2006), S. K. Katsikas, J. Lopez, M. Backes, S. Gritzalis, and B. Preneel, Eds., vol. 4176 of *Lecture Notes in Comput. Sci.*, Springer, pp. 117–130.

[LIX263] JAWOR, W., CHROBAK, M., AND DÜRR, C. Competitive analysis of scheduling algorithms for aggregated links. In *Proceedings of Latin American Theoretical INformatics (LATIN)* (2006), pp. 617–628.

[LIX264] JOUANNAUD, J.-P. Modular church-rosser modulo. In Pfenning [485], pp. 96–107.

[LIX265] JOUANNAUD, J.-P., AND RUBIO, A. Higher-order orderings for normal rewriting. In Pfenning [485], pp. 387–399.

[LIX266] KIRCHNER, F., AND MUÑOZ, C. PVS# : Streamlined tacticals for PVS. In *Proc. 6th Int. Workshop on Strategies in Automated Deduction* (Aug. 2006), vol. 174/11 of *Electronic Notes in Theoretical Computer Science*, Elsevier, pp. 47–58.

[LIX267] KIRCHNER, F., AND SINOT, F.-R. Rule-based operational semantics for and imperative language. In *Proc. 7th Int. Workshop on Rule Based Programming* (Aug. 2006), vol. 174 of *Electronic Notes in Theoretical Computer Science*, Elsevier, pp. 35–47.

[LIX268] KROB, D. Modelling of complex software systems : a reasoned overview. In *26th IFIP WG 6.1 International Conference on Formal Methods for Networked and Distributed Systems (FORTE'2006)* (2006), E. Najm, J.-F. Pradat-Peyre, and V. V. Donzeau-Gouge, Eds., Springer Verlag, pp. 1–22.

[LIX269] LAGUILLAUMIE, F., LIBERT, B., AND QUISQUATER, J.-J. Universal Designated Verifier Signatures Without Random Oracles or Non-Black Box Assumptions. In *Fifth Conference on Security and Cryptography for Networks (SCN'06)* (2006), R. D. Prisco and M. Yung, Eds., vol. 4116 of *Lecture Notes in Comput. Sci.*, Springer Verlag, pp. 63–77.

[LIX270] LAMARCHE, F., AND STRASSBURGER, L. From proof nets to the free *-autonomous category. *Logical Methods in Computer Science 2*, 4 :3 (2006), 1–44.

[LIX271] LEAVENS, G. T., ABRIAL, J.-R., BATORY, D., BUTLER, M., COGLIO, A., FISLER, K., HEHNER, E., JONES, C., MILLER, D., PEYTON-JONES, S., SITARAMAN, M., SMITH, D. R., AND STUMP, A. Roadmap for enhanced languages and methods to aid verification. In *Fifth International Conference on Generative Programming and Component Engineering (GPCE)* (Oct. 2006), ACM, pp. 221–235.

[LIX272] LÓPEZ, H. A., PALAMIDESSI, C., PÉREZ, J. A., RUEDA, C., AND VALENCIA, F. D. A declarative framework for security : Secure concurrent constraint programming. In *Proceedings of the 22nd International Conference on logic Programming, (ICLP)* (2006), S. Etalle and M. Truszczynski, Eds., vol. 4079 of *Lecture Notes in Computer Science*, Springer, pp. 449–450.

[LIX273] MILLER, D. Collection analysis for Horn clause programs. In *Proceedings of PPDP 2006 : 8th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming* (July 2006), pp. 179 – 188.

[LIX274] MILLER, D. Representing and reasoning with operational semantics. In *Proceedings of IJCAR : International Joint Conference on Automated Reasoning* (Aug. 2006), U. Furbach and N. Shankar, Eds., vol. 4130 of *LNAI*, pp. 4–20.

[LIX275] MILLER, D., AND SAURIN, A. A game semantics for proof search : Preliminary results. In *Proceedings of the Mathematical Foundations of Programming Semantics (MFPS05)* (2006), no. 155 in Electr. Notes Theor. Comput. Sci, pp. 543–563.

[LIX276] NEVES, A., MBOUP, M., AND FLIESS, M. An algebraic receiver for full response cpm demodulation. In *International Telecommunications Symposium (ITS 2006)* (2006).

[LIX277] PALAMIDESSI, C. Probabilistic and nondeterministic aspects of anonymity. In *Proceedings of the 21st Conference on the Mathematical Foundations of Programming Semantics (MFPS XXI)* (Birmingham, UK, 2006), vol. 155 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 33–42. `http://www.lix.polytechnique.fr/~catuscia/papers/Anonymity/MFPS/paper.pdf`.

[LIX278] PALAMIDESSI, C., SARASWAT, V. A., VALENCIA, F. D., AND VICTOR, B. On the expressiveness of linearity vs persistence in the asynchronous pi-calculus. In *Proceedings of the Twenty First Annual IEEE Symposium on Logic in Computer Science (LICS)* (2006), IEEE Computer Society, pp. 59–68. `http://www.lix.polytechnique.fr/~catuscia/papers/Frank/LICS_06/main.pdf`.

[LIX279] PALAMIDESSI, C., AND VALENCIA, F. Expressiveness of recursion, replication and scope mechanisms in process calculi. In *Postproceedings of the 5th International Symposium on Formal Methods for Components and Objects (FMCO)* (2006), Lecture Notes in Computer Science, Springer. `http://www.lix.polytechnique.fr/~catuscia/papers/Frank/FMCO_06/paper.pdf`.

[LIX280] PASCAL, C., AND SCHOST, É. Change of order for bivariate triangular sets. In *ISSAC'06* (2006), ACM, pp. 277–284.

[LIX281] PRADALIER, S., AND PALAMIDESSI, C. Expressiveness of probabilistic π-calculi. In *Proceedings of the 4th International Workshop on Quantitative Aspects of Programming Languages (QAPL)* (2006), vol. 164, pp. 119–136. To appear. `http://www.lix.polytechnique.fr/~catuscia/papers/Sylvain/QAPL06/FinalBis.pdf`.

[LIX282] STRASSBURGER, L. What could a boolean category be ? In *Classical Logic and Computation 2006 (Satellite Workshop of ICALP'06)* (2006), S. van Bakel, Ed.

[LIX283] VASSILIEVA, E., AND SCHAEFFER, G. A bijection for unicellular partitioned bicolored maps. *Formal Power Series and Algebraic Combinatorics (FPSAC'06)* (2006), 326 – 336.

[LIX284] WERNER, B. On the strength of proof-irrelevant type theories. In *Int. Joint Conf. Automated Reasoning — IJCAR 2006* (2006), U. Furbach and N. Shankar, Eds., vol. 4130 of *LNAI*, Springer.

[LIX285] WINTER, E., AND BAPTISTE, P. On scheduling a single machine to minimize a function of distances between pairs of tasks : Scheduling a multifunction radar. In *International Conference on Service Systems and Service Management* (2006).

[LIX286] WINTER, E., AND LUPINSKI, L. On scheduling the dwells of a multifunction radar. In *International Conference on Radar* (2006).

[LIX287] ZIEGLER, A., MILLER, D., AND PALAMIDESSI, C. A congruence format for name-passing calculi. In *Proceedings of the 2nd Workshop on Structural Operational Semantics (SOS'05)* (Lisbon, Portugal, 2006), vol. 156(1) of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 169–189. `http://www.lix.polytechnique.fr/~catuscia/papers/Axelle/SOS_05/report.pdf`.

[LIX288] ZUMKELLER, R. Formal global optimisation with taylor models. In *Int. Joint Conf. Automated Reasoning — IJCAR 2006* (2006), U. Furbach and N. Shankar, Eds., vol. 4130 of *LNAI*, Springer.

2007

[LIX289] ALIN BOSTAN, CLAUDE-PIERRE JEANNEROD, É. S. Solving Toeplitz- and Vandermonde-like linear systems with large displacement rank. In *ISSAC'07* (2007), ACM, pp. 33–40.

[LIX290] ANCEAUME, E., DELPORTE-GALLET, C., FAUCONNIER, H., HURFIN, M., AND WIDDER, J. Clock synchronization in the Byzantine-recovery failure model. In *International Conference On Principles Of DIstributed Systems (OPODIS'07)* (Guadeloupe, French West Indies, Dec. 2007), LNCS, Springer Verlag. to appear.

[LIX291] ARANDA, J., GIUSTO, C. D., NIELSEN, M., AND VALENCIA, F. CCS with replication in the Chomsky hierarchy : The expressive power of divergence. In *Proc. of The Fifth ASIAN Symposium on Programming Languages (APLAS'07)* (2007), LNCS, Springer. To appear.

[LIX292] ARANDA, J., GIUSTO, C. D., PALAMIDESSI, C., AND VALENCIA, F. Expressiveness of recursion, replication and scope mechanisms in process calculi. In *Postproceedings of the 5th International Symposium on Formal Methods for Components and Objects (FMCO'07)* (2007), F. de Boer and M. Bonsangue, Eds., LNCS, Springer. To appear.

[LIX293] BAELDE, D., GACEK, A., MILLER, D., NADATHUR, G., AND TIU, A. The Bedwyr system for model checking over syntactic expressions. In *21th Conference on Automated Deduction* (2007), F. Pfenning, Ed., no. 4603 in LNAI, Springer, pp. 391–397.

[LIX294] BAELDE, D., AND MILLER, D. Least and greatest fixed points in linear logic. Accepted to LPAR07, `http://www.lix.polytechnique.fr/Labo/Dale.Miller/papers/lpar07final.pdf`, April 2007.

[LIX295] BAPTISTE, P., CHROBAK, M., AND DÜRR, C. Polynomial time algorithms for minimum energy scheduling. In *Proc. of the 15th Annual European Symposium on Algorithms (ESA)* (2007).

[LIX296] BAPTISTE, P., KONONOV, A., AND SVIRIDENK, M. New lower bound for the flow shop scheduling. In *Eighth Workshop On Models And Algorithms For Planning And Scheduling Problems* (2007).

[LIX297] BARBAY, J., ALEARDI, L. C., HE, M., AND MUNRO, I. Succinct representations of labeled graphs. In *Proc. of the Int. Symposium on Algorithms and Computation (ISAAC)* (2007). to appear.

[LIX298] BARRAS, B., AND BERNARDO, B. The implicit calculus of constructions as a programming language with dependent types. In *Workshop on Type theory, Proof theory, and Rewriting* (2007).

[LIX299] BELKOURA, L., RICHARD, J.-P., AND FLIESS, M. Real time identification of delay systems. In *Ifac Worshop on Time delay Systems* (2007).

[LIX300] BIELY, M., CHARRON-BOST, B., GAILLARD, A., HUTTLE, M., SCHIPER, A., AND WIDDER, J. Tolerating corrupted communications. In *Proceedings of PODC* (Portland, USA, 2007), pp. 244–253.

[LIX301] BIELY, M., HUTLE, M., PENSO, L. D., AND WIDDER, J. Relating stabilizing timing assumptions to stabilizing failure detectors regarding solvability and efficiency. In *9th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'07)* (Paris, Nov. 2007), vol. 4838 of *LNCS*, Springer Verlag. to appear.

[LIX302] BLANQUI, F., JOUANNAUD, J.-P., AND RUBIO, A. Horpo with computational closure : a reconstruction. In Dershowitz and Voronkov [491].

[LIX303] BLANQUI, F., JOUANNAUD, J.-P., AND STRUB, P.-Y. Building decision procedures in the calculus of inductive constructions. In Duparc and Henzinger [492], pp. 328–342.

[LIX304] BODIRSKY, M., FUSY, É., KANG, M., AND VIGERSKE, S. An unbiased pointing operator for unlabeled structures, with applications to counting and sampling. In *18th ACM-SIAM Symposium on Discrete Algorithms, New Orleans* (2007), pp. 356–365.

[LIX305] BOSTAN, A., CHYZAK, F., OLLIVIER, F., SALVY, B., SCHOST, E., AND SEDOGLAVIC, A. Fast computation of power series solutions of systems of differential equations. In *SODA'07, ACM-SIAM Symposium on Discrete Algorithms* (2007), pp. 1012–1021.

[LIX306] BOURDAIS, R., FLIESS, M., JOIN, C., AND PERRUQUETTI, W. Towards a model-free output tracking of switched nonlinear systems. In *NOLCOS 2007 - 7th IFAC Symposium on Nonlinear Control Systems* (2007).

[LIX307] CACCIAGRANO, D., CORRADINI, F., ARANDA, J., AND VALENCIA, F. Persistence and testing semantics in the asynchronous pi calculus. In *Proc. of 14th International Workshop on Expressiveness of Concurrency, (EXPRESS'07)* (2007), R. Amadio and T. Hildenbrandt, Eds., ENTCS, Elsevier. To appear.

[LIX308] CHAPDELAINE, P., HERMANN, M., AND SCHNOOR, I. Complexity of default logic on generalized conjunctive queries. In *Proceedings 9th International Conference on Logic Programming and Nonmonotonic Reasoning (LPNMR 2007), Tempe (Arizona, USA)* (May 2007), C. Baral, G. Brewka, and J. Schlipf, Eds., vol. 4483 of *Lecture Notes in Artificial Intelligence*, Springer Verlag, pp. 58–70.

[LIX309] CHAPUY, G. Random permutations and their discrepancy process. In *Proc. of Intl Conf. on Analysis of Algorithms* (2007), P. Jacquet, Ed., DMTCS.

[LIX310] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. Making random choices invisible to the scheduler. In *Proceedings of CONCUR'07* (2007), Lecture Notes in Computer Science, Springer. `http://www.lix.polytechnique.fr/~catuscia/papers/Scheduler/report.pdf`.

[LIX311] CHATZIKOKOLAKIS, K., AND PALAMIDESSI, C. Probability of error in information-hiding protocols. In *Proceedings of the 20th IEEE Computer Security Foundations Symposium (CSF20)* (2007), IEEE Computer Society. `http://www.lix.polytechnique.fr/~catuscia/papers/ProbabilityError/full.pdf`.

[LIX312] CHROBAK, M., AND HURAND, M. Better bounds for incremental medians. In *Proc. 5th Workshop on Approximation and Online Algorithms (WAOA)* (2007).

[LIX313] CHROBAK, M., HURAND, M., AND SGALL, J. Fast algorithms for testing fault-tolerance of sequenced jobs with deadlines. In *Proc. 28th IEEE Real-Time Systems Symposium (RTSS)* (2007).

[LIX314] COQUAND, T., AND SPIWACK, A. Towards constructive homological algebra in type theory. In *Proceedings of 14th Symposium, Calculemus 2007, 6th International Conference, MKM 2007* (2007), Springer.

[LIX315] COUSINEAU, D., AND DOWEK, G. Embedding pure type systems in the lambda-pi-calculus modulo. In Rocca [493], pp. 102–117.

[LIX316] DAVIDOVIĆ, T., LIBERTI, L., MACULAN, N., AND MLADENOVIĆ, N. Towards the optimal solution of the multiprocessor scheduling problem with communication delays. In *MISTA Proceedings* (2007).

[LIX317] DENG, Y., PALAMIDESSI, C., AND PANG, J. Weak probabilistic anonymity. In *Proceedings of the 3rd International Workshop on Security Issues in Concurrency (SecCo)* (2007), vol. 180 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 55–76. `http://www.lix.polytechnique.fr/~catuscia/papers/Anonymity/report_wa.pdf`.

[LIX318] DOWEK, G., AND HERMANT, O. A simple proof that super-consistency implies cut elimination. In Baader [489], pp. 93–106.

[LIX319] ENGE, A., AND GAUDRY, P. An $L(1/3 + \varepsilon)$ algorithm for the discrete logarithm problem for low degree curves. In *Advances in Cryptology — Eurocrypt 2007* (Berlin, 2007), M. Naor, Ed., vol. 4515 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 367–382.

[LIX320] FALASCHI, M., OLARTE, C., PALAMIDESSI, C., AND VALENCIA, F. D. Declarative diagnosis of temporal concurrent constraint programs. In *Proceedings of The 23rd International Conference*

in Logic Programming (ICLP'07) (2007), Lecture Notes in Computer Science, Springer. `http://www.lix.polytechnique.fr/~catuscia/papers/Carlos/iclp07.pdf`.

[LIX321] FLAJOLET, P., FUSY, É., AND PIVOTEAU, C. Boltzmann sampling of unlabelled structures. In *Proceedings of the 4th Workshop on Analytic Algorithms and Combinatorics, ANALCO'07 (New Orleans)* (2007), SIAM, pp. 201–211.

[LIX322] FUSY, É., POULALHON, D., AND SCHAEFFER, G. Bijective counting of plane bipolar orientations. In *Proceedings of Eurocomb'07* (2007).

[LIX323] GARILLOT, F., AND WERNER, B. Simple types in type theory : Deep and shallow encodings. In Schneider and Brandt [494], pp. 368–382.

[LIX324] GIMBERT, H. Pure stationary optimal strategies in markov decision processes. In *STACS* (2007).

[LIX325] GIMBERT, H., AND ZIELONKA, W. Limits of multi-discounted markov decision processes. In *LICS* (2007).

[LIX326] GIMBERT, H., AND ZIELONKA, W. Perfect information stochastic priority games. In *ICALP* (2007).

[LIX327] GONTHIER, G., MAHBOUBI, A., RIDEAU, L., TASSI, E., AND THÉRY, L. A modular formalisation of finite group theory. In Schneider and Brandt [494], pp. 86–101.

[LIX328] GOUBAULT-LARRECQ, J., PALAMIDESSI, C., AND TROINA, A. A probabilistic applied pi-calculus. In *Proceedings of the 5th Asian Symposium on Programming Languages and Systems (APLAS'07)* (2007), LNCS, Springer. To appear.

[LIX329] HERMANN, M., AND PICHLER, R. Counting complexity of propositional abduction. In *20th International Joint Conference on Artificial Intelligence (IJCAI 2007)* (Jan. 2007), M. M. Veloso, Ed., AAAI Press, pp. 417–422.

[LIX330] HERNEST, M.-D. Light Dialectica program extraction from a classical Fibonacci proof. *Electronic Notes in Theoretical Computer Science 171*, 3 (2007), 43–53. Elsevier.

[LIX331] HERNEST, M.-D. Synthesis of moduli of uniform continuity by the Monotone Dialectica Interpretation in the proof-system MINLOG. *Electronic Notes in Theoretical Computer Science 174*, 5 (2007), 141–149. Elsevier.

[LIX332] HURINK, J., KERN, W., POST, G., AND STILL, G., Eds. *Proceedings of the 6th Cologne-Twente Workshop on Graphs and Combinatorial Optimization* (Enschede, 2007), University of Twente.

[LIX333] KIRCHNER, F. A finite first-order theory of classes. In *Types for Proofs and Programs, International Workshop, TYPES 2006, Nottingham, UK, April 18-21, 2006, Revised Selected Papers* (2007), Lecture Notes in Computer Science, Springer.

[LIX334] LIANG, C., AND MILLER, D. Focusing and polarization in intuitionistic logic. In *CSL 2007 : Computer Science Logic* (2007), J. Duparc and T. A. Henzinger, Eds., vol. 4646 of *LNCS*, Springer-Verlag, pp. 451–465.

[LIX335] LIBERTI, L. A useful characterization of the feasible region of binary linear programs. In Hurink et al. [332], pp. 103–106.

[LIX336] MBOUP, M., JOIN, C., AND FLIESS, M. A revised look at numerical differentiation with an application to nonlinear feedback control. In *The 15th Mediterranean Conference on Control and Automation - MED'2007* (2007).

[LIX337] MIHĂILESCU, P., MORAIN, F., AND SCHOST, É. Computing the eigenvalue in the Schoof-Elkies-Atkin algorithm using Abelian lifts. In *ISSAC '07 : Proceedings of the 2007 international symposium on Symbolic and algebraic computation* (New York, NY, USA, 2007), ACM Press, pp. 285–292.

[LIX338] MILLER, D., AND NIGAM, V. Incorporating tables into proofs. In *CSL 2007 : Computer Science Logic* (2007), J. Duparc and T. A. Henzinger, Eds., vol. 4646 of *LNCS*, Springer-Verlag, pp. 466–480.

[LIX339] MILLER, D., AND SAURIN, A. From proofs to focused proofs : a modular proof of focalization in linear logic. In *CSL 2007 : Computer Science Logic* (2007), J. Duparc and T. A. Henzinger, Eds., vol. 4646 of *LNCS*, Springer-Verlag, pp. 405–419.

[LIX340] NANNICINI, G., BAPTISTE, P., KROB, D., AND LIBERTI, L. Fast point-to-point shortest path queries on dynamic road networks with interval data. In Hurink et al. [332], pp. 115–118.

[LIX341] NGUYEN, K. T., AND DÜRR, C. Nash equilibria in Voronoi games on graphs. In *Proc. of the 15th Annual European Symposium on Algorithms (ESA)* (2007).

[LIX342] NORMAN, G., PALAMIDESSI, C., PARKER, D., AND WU, P. Model checking the probabilistic pi-calculus. In *4th International Conference on the Quantitative Evaluation of SysTems (QEST)* (2007), Lecture Notes in Computer Science, Springer. To appear.

[LIX343] OLARTE, C., PALAMIDESSI, C., AND VALENCIA, F. D. Universal timed concurrent constraint programming. In *Proceedings of the 23rd International Conference in Logic Programming (ICLP'07)* (2007), Lecture Notes in Computer Science, Springer. `http://www.lix.polytechnique.fr/~catuscia/papers/Carlos/iclp07DC.pdf`.

[LIX344] PLATEAU, M., LIBERTI, L., AND ALFANDARI, L. Edge cover by bipartite subgraphs. In Hurink et al. [332], pp. 127–131.

[LIX345] STRASSBURGER, L. A characterisation of medial as rewriting rule. In *Term Rewriting and Applications, RTA'07* (2007), F. Baader, Ed., vol. 4533 of *LNCS*, Springer-Verlag, pp. 344–358.

[LIX346] STRASSBURGER, L. Deep inference for hybrid logic. In *International Workshop on Hybrid Logic 2007 (Part of ESSLLI'07)* (2007).

[LIX347] WIDDER, J., GRIDLING, G., WEISS, B., AND BLANQUART, J.-P. Synchronous consensus with mortal Byzantines. In *Proceedings of the International Conference on Dependable Systems and Networks (DSN'07)* (Edinburgh, UK, June 2007), pp. 102–111.

[LIX348] WINTER, E., AND SADYKOV, R. Computing lower bounds for the schedule of a multifunction radar. In *MISTA 2007* (2007).

[LIX349] WU, P., PALAMIDESSI, C., AND LIN, H. Probabilistic systems. In *Proceedings of 4th International Conference on the Quantitative Evaluation of SysTems (QEST)* (2007), Lecture Notes in Computer Science, Springer. `http://www.lix.polytechnique.fr/~catuscia/papers/Wu/qest2.pdf`.

National conferences with proceedings

2004

[LIX350] C. MUÑOZ, G. D., AND CARREÑO, V. Modeling and verification of an air traffic concept of operations. In *International Symposium on software testing and analysis* (2004).

[LIX351] JOUANNAUD, J.-P. Formal mathematics : Application to software safety and internet security. In *Invited presentation, 9th Articifial Intelligence Conference, Taipei* (2004).

[LIX352] JOUANNAUD, J.-P. Theorem proving languages for verification. In *Invited presentation,2nd International Symposium on Automated Technology for Verification and Analysis, Taipei* (2004).

[LIX353] SAVOUREY, D., JOUGLET, A., BAPTISTE, P., AND CARLIER, J. Méthode tabou pour minimiser le retard total pondéré sur une machine avec dates de disponibilité. In *MOSIM, Conférence Francophone de Modélisation et Simulation* (2004).

2005

[LIX354] ARTIOUCHINE, K., BAPTISTE, P., AND MATTIOLI, J. Le problème des n-rois : un modèle des systèmes dynamiques. In *Sixième congrès de la société Française de Recherche Opérationnelle et Aide à la Décision* (2005).

[LIX355] BAPTISTE, P., AND BRUCKER, P. Scheduling equal processing time jobs on parallel machines : A survey. In *Troisieme Conference Internationale en Informatique Recherche, Innovation & Vision du Futur* (Can Tho, Vietnam, 2005).

[LIX356] BAPTISTE, P., CROCE, F. D., GROSSO, A., AND T'KINDT, V. On some compact integer programming formulations of machine scheduling problems. In *Sixième congrès de la société Française de Recherche Opérationnelle et Aide à la Décision* (2005).

[LIX357] BERTHOMÉ, P., LEBRESNE, S., AND NGUYEN, K. Computation of chromatic polynomials using triangulations and clique trees. In Kratsch [475], pp. 362–373.

[LIX358] GWIGGNER, C., BAPTISTE, P., AND DUONG, V. Conditions et lois : une analyse des données du trafic aérien. In *Sixième congrès de la société Française de Recherche Opérationnelle et Aide à la Décision* (2005).

[LIX359] KIRCHNER, F. Store-based operational semantics. In *Seizièmes Journées Francophones des Langages Applicatifs* (2005), INRIA.

[LIX360] NARBOUX, J. Toward the use of a proof assistant to teach mathematics. In *Proceedings of ICTMT7* (2005).

[LIX361] SAVOUREY, D., JOUGLET, A., AND BAPTISTE, P. Règles de dominance pour l'ordonnancement de jobs avec dates de disponibilité sur machines parallèles. In *Sixième congrès de la société Française de Recherche Opérationnelle et Aide à la Décision* (2005).

[LIX362] WINTER, E., BAPTISTE, P., LUPINSKI, L., AND CHAMOUARD, E. Modélisation des problèmes d'ordonnancement de tâches sur des radars embarqués. In *Sixième congrès de la société Française de Recherche Opérationnelle et Aide à la Décision* (2005).

2006

[LIX363] ARRIGHI, P., AND DOWEK, G. Linear-algebraic lambda-calculus. In *International workshop on quantum programming languages* (2006), P. Selinger, Ed., Turku Centre for Computer Science General Publication, 33.

[LIX364] E. WINTER, P. B. On scheduling a multifunction radar. In *Commande, Optimisation, Gestion Intelligente et architecture des Senseurs pour les systèmes* (2006).

[LIX365] FLIESS, M., FUCHSHUMER, S., SCHLACHER, K., AND SIRA-RAMÍREZ, H. Discrete-time linear parametric identification : An algebraic approach. In *2e Journées Identification et Modélisation Expérimentale - JIME'2006* (2006).

[LIX366] JOIN, C., MASSE, J., AND FLIESS, M. Commande sans modèle pour l'alimentation de moteurs : résultats préliminaires et comparaisons. In *2e Journées Identification et Modéisation Expérimentale - JIME'2006* (2006).

[LIX367] NARBOUX, J. Mechanical theorem proving in Tarski's geometry. In *Proceedings of Automatic Deduction in Geometry 06* (2006).

2007

[LIX368] BAPTISTE, P., AND SADYKOV, R. A new mip formulation for single machine scheduling. In *Conférence conjointe FRANCORO V / ROADEF 2007* (2007).

[LIX369] NANNICINI, G., BAPTISTE, P., KROB, D., AND LIBERTI, L. Fast point-to-point shortest path queries on dynamic road networks with interval data. In *Cologne/Twente Workshop on Graphs and Combinatorial Optimization 2007, CTW 200* (may 2007).

[LIX370] SAVOUREY, D., BAPTISTE, P., AND JOUGLET, A. Méthode exacte pour problèmes à machines parallèles. In *Conférence conjointe FRANCORO V / ROADEF 2007* (2007).

Dissemination

2003

[LIX371] CHARDIN, G., DOWEK, G., LACHIÈZE-REY, M., AND THIS, H. *Quand la science a dit c'est bizarre !* Le Pommier, 2003.

2005

[LIX372] DOWEK, G., BOURGUIGNON, J.-P., NOVELLI, J.-C., AND RITTAUD, B. *Jeux mathématiques et vice versa*. Le Pommier - La cité des sciences et de l'industrie, 2005.

[LIX373] HERMANN, N., AND LESCANNE, P. Est-ce que « P = NP » ? *Les Dossiers de La Recherche 20* (août-octobre 2005), 64–68.

[LIX374] OLLIVIER, F. Maxima et les logiciels libres de calcul formel. *Revue de l'Électricité et de lÉlectronique 11* (2005), 89–93.

2006

[LIX375] FLIESS, M., AND MBOUP, M. Towards new estimation techniques : Reconciling signal processing and control. In *ICASSP* (Toulouse, May 2006). Tutorial Note.

[LIX376] MORAIN, F. *Encyclopédie de l'informatique et des systèmes d'information (sous la direction de J. Akoka et I. Comyn-Wattiau)*. Vuibert, 2006, ch. Algorithmes algébriques.

[LIX377] WERNER, B. La vérité et la machine. In *Images des Mathématiques – 2006* (2006), J. I. Etienne Ghys, Ed., Société Mathématique de France.

2007

[LIX378] DOWEK, G. *Les Métamorphoses du Calcul*. Le Pommier, 2007.

[LIX379] GONTHIER, G., AND WERNER, B. Le théorème des quatre couleurs : ingénierie d'une preuve formelle. *La lettre de l'Académie des sciences 21* (2007).

PhD Thesis

2004

[LIX380] CHRZĄSZCZ, J. *Modules in Type Theory with Generative Definitions*. PhD thesis, Warsaw Univerity and University of Paris-Sud, Jan 2004.

[LIX381] LIBERTI, L. *Reformulation and Convex Relaxation Techniques for Global Optimization*. PhD thesis, Imperial College London, UK, Mar. 2004.

[LIX382] TIU, A. *A Logical Framework for Reasoning about Logical Specifications*. PhD thesis, Pennsylvania State University, May 2004.

2005

[LIX383] HERBELIN, H. *C'est maintenant qu'on calcule, au cœur de la dualité*. PhD thesis, Université Paris-Sud, 2005. Habilitation à diriger des Recherches.

[LIX384] HERMANT, O. *Méthodes Sémantiques en Déduction Modulo*. PhD thesis, Université Paris 7 - Denis Diderot, 2005.

2006

[LIX385] DAHAN, X. *Sur la complexité des représentations des systèmes polynomiaux : triangulation, méthodes modulaires, évaluation dynamique*. PhD thesis, École polytechnique, novembre 2006.

[LIX386] DUPONT, R. *Moyenne arithmético-géométrique, suites de Borchardt et applications*. PhD thesis, École polytechnique, `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf`, 2006.

[LIX387] HERNEST, M.-D. *Optimized programs from (non-constructive) proofs by the light (monotone) Dialectica interpretation*. PhD Thesis, École Polytechnique and Universität München, 2006. http ://www.brics.dk/~danher/teza/.

[LIX388] NARBOUX, J. *Formalisation et automatisation du raisonnement géométrique en Coq*. Thése de doctorat, spécialité informatique, Université Paris-Sud, September 2006.

[LIX389] SINOT, F.-R. *Efficient Strategies and Implementation Models for Functional Languages*. Thése de doctorat, spécialité informatique, Ecole Polytechnique, école Polytechnique, France, September 2006.

2007

[LIX390] KIRCHNER, F. *Interoperable proof systems*. PhD thesis, École Polytechnique, 2007.

Miscellaneous

[LIX391] OLARTE, C., AND VALENCIA, F. On the expressiveness of universal concurrent constraint programming. Tech. rep., LIX, Ecole Polytechnique, `http://www.lix.polytechnique.fr/~colarte`. in preparation.

[LIX392] OLARTE, C., AND VALENCIA, F. A process calculus for universal concurrent constraint programming : Semantics, logic and application. Tech. rep., LIX, Ecole Polytechnique, `http://www.lix.polytechnique.fr/~colarte`. in preparation.

2004

[LIX393] CHARRON-BOST, B. Reductions in distributed computing. part i : Consensus and Atomic Commitment Tasks. Tech. Rep. LIX/10/2004, LIX, 2004. Available from ArXiv as number cs.DC/04/12115.

[LIX394] CHARRON-BOST, B. Reductions in distributed computing. part ii : k-Threshold Agreement Tasks. Tech. Rep. LIX/12/2004, LIX, 2004. Available from ArXiv as number cs.DC/04/12116.

[LIX395] DAVIDOVIĆ, T., LIBERTI, L., MACULAN, N., AND MLADENOVIĆ, N. Mathematical programming-based approach to scheduling of communicating tasks. Tech. Rep. G-2004-99, Cahiers du GERAD, 2004.

[LIX396] GAUDRY, P. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. Cryptology ePrint Archive : Report 2004/073, http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/publis/semweil.ps.gz, 2004.

[LIX397] LIBERTI, L. Automatic reformulation of bilinear minlps. Tech. Rep. 2004.24, DEI, Politecnico di Milano, July 2004.

[LIX398] LIBERTI, L., AND KUCHERENKO, S. Comparison of deterministic and stochastic approaches to global optimization. Tech. Rep. 2004.25, DEI, Politecnico di Milano, July 2004.

[LIX399] MORAIN, F. La primalité en temps polynomial [d'après Adleman, Huang ; Agrawal, Kayal, Saxena]. *Astérisque 294* (2004), Exp. No. 917, ix, 205–230. Séminaire Bourbaki. Vol. 2002/2003.

[LIX400] TIU, A. *Level 0/1 Prover : A tutorial*, September 2004. Available online.

[LIX401] ZIEGLER, A. Un format pour que la bisimulation soit une congruence dans les langages de processus avec mobilité. Tech. rep., INRIA Futurs, LIX and ENS, 2004.

2005

[LIX402] BAELDE, D. Logique linéaire et algèbre de processus. Tech. rep., INRIA Futurs, LIX and ENS, 2005.

[LIX403] GAUDRY, P., HOUTMANN, T., KOHEL, D., RITZENTHALER, C., AND WENG, A. The p-adic method for genus 2. Preprint, http://arxiv.org/abs/math.NT/0503148, 2005.

[LIX404] LAVOR, C., LIBERTI, L., MACULAN, N., AND CHAER NASCIMENTO, M. Solving a quantum chemistry problem with deterministic global optimization. Tech. Rep. 1175, Optimization Online, 2005.

[LIX405] LIBERTI, L. Compact linearization for bilinear mixed-integer problems. Tech. Rep. 1124, Optimization Online, 2005.

[LIX406] PALAMIDESSI, C., AND VALENCIA, F. Recursion vs replication in process calculi : Expressiveness. *Bulletin of the EATCS 87* (2005), 105–125. Column : Concurrency. http://www.lix.polytechnique.fr/~catuscia/papers/Frank/EATCS_05/recrep.pdf.

2006

[LIX407] BAELDE, D., GACEK, A., MILLER, D., NADATHUR, G., AND TIU, A. *A User Guide to Bedwyr*, November 2006.

[LIX408] BAPTISTE, P., BARBIER, G., KROB, D., AND LIBERTI, L. Fast paths in large-scale dynamic road networks. Tech. Rep. cs.NI/0704.1068, arXiv, 2006.

[LIX409] ENGE, A. The complexity of class polynomial computation via floating point approximations. HAL-INRIA 1040, INRIA, http://hal.inria.fr/inria-00001040, 2006.

[LIX410] ENGE, A. Computing modular polynomials in quasi-linear time. http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/modcomp.pdf, 2006.

[LIX411] FLIESS, M. Approche intrinsèque des fluctuations quantiques en mécanique stochastique (an intrinsic approach to the quantum fluctuations in stochastic mechanics). Tech. rep., HAL INRIA, http://hal.inria.fr/inria-00118460, 2006.

[LIX412] LIANG, C., AND MILLER, D. On focusing and polarities in linear logic and intuitionistic logic. Unpublished report, December 2006.

[LIX413] LIBERTI, L., LAVOR, C., AND MACULAN, N. Discretizable molecular distance geometry problem. Tech. Rep. q-bio.BM/0608012, arXiv, 2006.

[LIX414] MILLER, D. Logic and logic programming : A personal account. ALP Newsletter, February 2006. Vol. 19, No. 1.

[LIX415] PALAMIDESSI, C. Anonymity in probabilistic and nondeterministic systems. In *Proceedings of the Workshop on "Essays on Algebraic Process Calculi" (APC 25)* (Bertinoro, Italy, 2006), vol. 162 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science B.V., pp. 277–279. http://www.lix.polytechnique.fr/~catuscia/papers/Anonymity/Bertinoro/paper.pdf.

[LIX416] PALAMIDESSI, C., AND BHARGAVA, M. Probabilistic anonymity. In *Foundations of Global Computing* (2006), J. L. Fiadeiro, U. Montanari, and M. Wirsing, Eds., no. 05081 in Dagstuhl Seminar Proceedings, Internationales Begegnungs- und Forschungszentrum (IBFI), Schloss Dagstuhl, Germany.

[LIX417] PALAMIDESSI, C., AND VALENCIA, F. Languages for concurrency. *Bulletin of the European Association for Theoretical Computer Science 90* (Oct. 2006), 155–171. Column : Programming Languages. http://www.lix.polytechnique.fr/~catuscia/papers/Frank/EATCS_06/paper.pdf.

[LIX418] STRASSBURGER, L. Proof nets and the identity of proofs. Research Report 6013, INRIA, https://hal.inria.fr/inria-00107260, Oct. 2006. Lecture notes for ESSLLI'06.

2007

[LIX419] BAELDE, D., AND MILLER, D. Least and greatest fixed points in linear logic : extended version. Technical report, available from the first author's web page, http://www.lix.polytechnique.fr/~dbaelde/productions/pool/mumall_draft_long.pdf, April 2007.

[LIX420] BAPTISTE, P., KROB, D., AND LIBERTI, L. Procédé de propagation des informations partielles de trafic dans un réseau routier, 2007. Procédé de propagation des informations partielles de trafic dans un réseau routier dont le brevet â été déposé par la societe Mediamobile.

[LIX421] BODIRSKY, M., FUSY, É., KANG, M., AND VIGERSKE, S. Enumeration and asymptotic properties of unlabeled outerplanar graphs. To be published in the Electronic Journal of Combinatorics, 2007.

[LIX422] CHARRON-BOST, B., AND SCHIPER, A. The Heard-Of model : Computing in distributed systems with benign failures. Tech. Rep. LSR/2007-004, Département Systèmes de Communication, EPFL, 2007.

[LIX423] ENGE, A. Computing modular polynomials in quasi-linear time. HAL-INRIA 143084 et ArXiv 0704.3177, INRIA, http://hal.inria.fr/inria-00143084, 2007.

[LIX424] ENGE, A., AND ZIMMERMANN, P. mpc — a library for multiprecision complex arithmetic with exact rounding, http://www.lix.polytechnique.fr/Labo/Andreas.Enge/Software.html, 2007. Version 0.4.6.

[LIX425] NANNICINI, G. Procédé de propagation des informations partielles de trafic dans un réseau routier, 2007. Procédé de propagation des informations partielles de trafic dans un réseau routier dont le brevet â été déposé par la societe Mediamobile.

Cross References

[LIX426] JACOBI, C. De investigando ordine systematis æquationum differentialum vulgarium cujuscunque. *Journal für die reine und angewandte Mathematik LXIV*, 4 (1865), 297–320.

[LIX427] JACOBI, C. *Vorlesungen über Dynamik von C. G. J. Jacobi nebstes fünf hinterlassenen Abhandlungen desselben*. Druck und Verlag von Georg Reimer, 1866, ch. De æquationum differentialum systemate non normali ad formam normalem revocando, pp. 550–578.

[LIX428] GORDON, M. J. C., MILNER, R., AND WADSWORTH, C. P. *Edinburgh LCF*, vol. 78 of *Lecture Notes in Computer Science*. Springer, 1979.

[LIX429] COQUAND, T., AND HUET, G. P. The calculus of constructions. *Inf. Comput. 76*, 2/3 (1988), 95–120.

[LIX430] HONDA, K., AND TOKORO, M. An object calculus for asynchronous communication. In *Proceedings of the European Conference on Object-Oriented Programming (ECOOP)* (1991), P. America, Ed., vol. 512 of *Lecture Notes in Computer Science*, Springer, pp. 133–147.

[LIX431] BOUDOL, G. Asynchrony and the π-calculus (note). Rapport de Recherche 1702, INRIA, Sophia-Antipolis, `http://www.inria.fr/rrrt/rr-1702.html`, 1992.

[LIX432] MILNER, R., PARROW, J., AND WALKER, D. A calculus of mobile processes, I and II. *Information and Computation 100*, 1 (1992), 1–40 & 41–77. A preliminary version appeared as Technical Reports ECF-LFCS-89-85 and -86, University of Edinburgh, 1989.

[LIX433] MORAIN, F. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *J. Théor. Nombres Bordeaux 7* (1995), 255–282.

[LIX434] COURANT, J. *Un calcul de modules pour les systèmes de types purs*. Thèse de doctorat, Ecole Normale Supérieure de Lyon, 1998.

[LIX435] ARITA, S. Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log based public key cryptosystems. *IEICE Transactions J82-A*, 8 (1999), 1291–1299. In Japanese. English translation in the proceedings of the Conference on The Mathematics of Public Key Cryptography, Toronto 1999.

[LIX436] BSI (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). Geeignete Kryptoalgorithmen gemäß § 17 (2) SigV. `http://www.bsi.de/aufgaben/projekte/pbdigsig/download/kryptalg.pdf`, 1999.

[LIX437] ALVAREZ, G., DIAZ, J., QUESADA, L., RUEDA, C., TAMURA, G., VALENCIA, F., AND ASSAYAG, G. Integrating constraints and concurrent objects in musical applications : A calculus and its visual language. *Constraints 6* (2001), 21–25.

[LIX438] HANROT, G., AND MORAIN, F. Solvability by radicals from a practical algorithmic point of view. Submitted, `http://www.lix.polytechnique.fr/Labo/Francois.Morain`, Nov. 2001.

[LIX439] HANROT, G., AND MORAIN, F. Solvability by radicals from an algorithmic point of view. In *Symbolic and algebraic computation* (2001), B. Mourrain, Ed., ACM, pp. 175–182. Proceedings ISSAC'2001, London, Ontario.

[LIX440] KEDLAYA, K. S. Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society 16*, 4 (2001), 323–338.

[LIX441] ALT, H., AND FERREIRA, A., Eds. *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes - Juan les Pins, France, March 14-16, 2002, Proceedings* (2002), vol. 2285 of *Lecture Notes in Computer Science*, Springer.

[LIX442] BAAZ, M., AND VORONKOV, A., Eds. *Logic for Programming, Artificial Intelligence, and Reasoning, 9th International Conference, LPAR 2002, Tbilisi, Georgia, October 14-18, 2002, Proceedings* (2002), vol. 2514 of *Lecture Notes in Computer Science*, Springer.

[LIX443] BLANQUI, F., JOUANNAUD, J.-P., AND OKADA, M. Inductive-data-type systems. *Theor. Comput. Sci. 272*, 1-2 (2002), 41–68.

[LX444] DOWEK, G. What is a theory ? In Alt and Ferreira [441], pp. 50–64.

[LX445] DOWEK, G., HARDIN, T., AND KIRCHNER, C. Binding logic : Proofs and models. In Baaz and Voronkov [442], pp. 130–144.

[LX446] ENGE, A., AND MORAIN, F. Comparing invariants for class fields of imaginary quadratic fields. In *Algorithmic Number Theory* (2002), C. Fieker and D. R. Kohel, Eds., vol. 2369 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 252–266. 5th International Symposium, ANTS-V, Sydney, Australia, July 2002, Proceedings.

[LX447] GALBRAITH, S. D., PAULUS, S. M., AND SMART, N. P. Arithmetic on superelliptic curves. *Math. Comp. 71*, 237 (2002), 393–405.

[LX448] GRÉGOIRE, B., AND LEROY, X. A compiled implementation of strong reduction. In *ICFP* (2002), pp. 235–246.

[LX449] MIQUEL, A., AND WERNER, B. The not so simple proof-irrelevant model of cc. In Geuvers and Wiedijk [457], pp. 240–258.

[LX450] ARIOLA, Z. M., AND HERBELIN, H. Minimal classical logic and control operators. In *Thirtieth International Colloquium on Automata, Languages and Programming, ICALP '03, Eindhoven, The Netherlands, June 30 - July 4, 2003* (2003), vol. 2719 of *Lecture Notes in Computer Science*, Springer, pp. 871–885.

[LX451] BONEH, D., GENTRY, C., LYNN, B., AND SHACHAM, H. Aggregate and verifiably encrypted signatures from bilinear maps. In *Advances in Cryptology – EUROCRYPT 2003* (2003), E. Biham, Ed., vol. 2656 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 416–432.

[LX452] CHRZĄSZCZ, J. Implementation of modules in the coq system. In *Theorem Proving in Higher Order Logic, TPHOLs 2003* (2003), vol. 2758 of *LNCS*, Springer, pp. 270–286.

[LX453] DOWEK, G. Confluence as a cut elimination property. In Nieuwenhuis [460], pp. 2–13.

[LX454] DOWEK, G., HARDIN, T., AND KIRCHNER, C. Theorem proving modulo. *J. Autom. Reasoning 31*, 1 (2003), 33–72.

[LX455] DOWEK, G., AND WERNER, B. Proof normalization modulo. *Journal of Symbolic Logic 68-4* (2003), 1289–1316.

[LX456] ENGE, A., AND MORAIN, F. Fast decomposition of polynomials with known Galois group. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (2003), M. Fossorier, T. Høholdt, and A. Poli, Eds., vol. 2643 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 254–264. 15th International Symposium, AAECC-15, Toulouse, France, May 2003, Proceedings.

[LX457] GEUVERS, H., AND WIEDIJK, F., Eds. *Types for Proofs and Programs, Second International Workshop, TYPES 2002, Berg en Dal, The Netherlands, April 24-28, 2002, Selected Papers* (2003), vol. 2646 of *Lecture Notes in Computer Science*, Springer.

[LX458] GRÉGOIRE, B. *Compilation des termes de preuves : un (nouveau) mariage entre Coq et Ocaml.* Thése de doctorat, spécialité informatique, Université Paris 7, école Polytechnique, France, `http://www-sop.inria.fr/everest/personnel/Benjamin.Gregoire/Publi/gregoire_these.ps.gz`, December 2003.

[LX459] MUÑOZ, C., CARREÑO, V., DOWEK, G., AND BUTLER, R. W. Formal verification of conflict detection algorithms. *STTT 4*, 3 (2003), 371–380.

[LX460] NIEUWENHUIS, R., Ed. *Rewriting Techniques and Applications, 14th International Conference, RTA 2003, Valencia, Spain, June 9-11, 2003, Proceedings* (2003), vol. 2706 of *Lecture Notes in Computer Science*, Springer.

[LX461] WALUKIEWICZ-CHRZĄSZCZ, D. *Termination of Rewriting in the Calculus of Constructions*. PhD thesis, Warsaw University and Université de Paris-Sud, 2003.

[LX462] BERARDI, S., COPPO, M., AND DAMIANI, F., Eds. *Types for Proofs and Programs, International Workshop, TYPES 2003, Torino, Italy, April 30 - May 4, 2003, Revised Selected Papers* (2004), vol. 3085 of *Lecture Notes in Computer Science*, Springer.

[LX463] BERTOT, Y., AND CASTERAN, P. *Interactive Theorem Proving and Program Development Coq'Art : The Calculus of Inductive Constructions*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2004.

[LX464] ISENBURG, M., AND SNOEYINK, J. Graph coding and connectivity compression, 2004. manuscript.

[LX465] LYSYANSKAYA, A., MICALI, S., REYZIN, L., AND SHACHAM, H. Sequential aggregate signatures from trapdoor permutations. In *Advances in Cryptology – EUROCRYPT 2004* (2004), C. Cachin and J. Camenisch, Eds., vol. 3027 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 74–90.

[LX466] RIBEIRO, C., AND MARTINS, S., Eds. *Experimental and Efficient Algorithms* (2004), vol. 3059 of *LNCS*, Springer.

[LX467] STRASSBURGER, L., AND LAMARCHE, F. On proof nets for multiplicative linear logic with units. In *Computer Science Logic, CSL 2004* (2004), J. Marcinkowski and A. Tarlecki, Eds., vol. 3210 of *LNCS*, Springer-Verlag, pp. 145–159.

[LX468] WALUKIEWICZ, I., Ed. *Foundations of Software Science and Computation Structures, 7th International Conference, FOSSACS 2004, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2004, Barcelona, Spain, March 29 - April 2, 2004, Proceedings* (2004), vol. 2987 of *Lecture Notes in Computer Science*, Springer.

[LX469] WANG, F., Ed. *Automated Technology for Verification and Analysis : Second International Conference, ATVA 2004, Taipei, Taiwan, ROC, October 31-November 3, 2004. Proceedings* (2004), vol. 3299 of *Lecture Notes in Computer Science*, Springer.

[LX470] AYDEMIR, B. E., BOHANNON, A., FAIRBAIRN, M., FOSTER, J. N., PIERCE, B. C., SEWELL, P., VYTINIOTIS, D., WASHBURN, G., WEIRICH, S., AND ZDANCEWIC, S. Mechanized metatheory for the masses : The poplmark challenge. In Hurd and Melham [474], pp. 50–65.

[LX471] GIESL, J., Ed. *Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings* (2005), vol. 3467 of *Lecture Notes in Computer Science*, Springer.

[LX472] GONTHIER, G. A computer checked proof of the four-color theorem. available on the web, `http://research.microsoft.com/~gonthier/`, 2005.

[LX473] HOARE, T., AND MILNER, R. Grand challenges for computing research. *Computer Journal 48*, 1 (2005), 49–52.

[LX474] HURD, J., AND MELHAM, T. F., Eds. *Theorem Proving in Higher Order Logics, 18th International Conference, TPHOLs 2005, Oxford, UK, August 22-25, 2005, Proceedings* (2005), vol. 3603 of *Lecture Notes in Computer Science*, Springer.

[LX475] KRATSCH, D., Ed. *Graph-Theoretic Concepts in Computer Science, 31st International Workshop, WG 2005, Metz, France, June 23-25, 2005, Revised Selected Papers* (2005), vol. 3787 of *Lecture Notes in Computer Science*, Springer.

[LX476] LAGUILLAUMIE, F., AND VERGNAUD, D. Short Undeniable Signatures Without Random Oracles : the Missing Link. In *Progress in Cryptology - Proceedings of Indocrypt'05* (2005), R. V. S. Maitra, C. E. Veni Madhavan, Ed., vol. 3797 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 283–296.

[LX477] LAMARCHE, F., AND STRASSBURGER, L. Constructing free boolean categories. In *20th IEEE Symposium on Logic in Computer Science (LICS 2005)* (2005), IEEE Computer Society, pp. 209–218.

[LX478] LAMARCHE, F., AND STRASSBURGER, L. Naming proofs in classical propositional logic. In *Typed Lambda Calculi and Applications, TLCA 2005* (2005), P. Urzyczyn, Ed., vol. 3461 of *LNCS*, Springer-Verlag, pp. 246–261.

[LX479] LENSTRA, JR., H. W., AND POMERANCE, C. Primality testing with Gaussian periods. Preprint, `http://www.math.dartmouth.edu/~carlp/PDF/complexity072805.pdf`, July 2005.

[LX480] MIDDELDORP, A., VAN OOSTROM, V., VAN RAAMSDONK, F., AND DE VRIJER, R. C., Eds. *Processes, Terms and Cycles : Steps on the Road to Infinity, Essays Dedicated to Jan Willem Klop, on the Occasion of His 60th Birthday* (2005), vol. 3838 of *Lecture Notes in Computer Science*, Springer.

[LX481] NIEUWENHUIS, R., Ed. *Automated Deduction - CADE-20, 20th International Conference on Automated Deduction, Tallinn, Estonia, July 22-27, 2005, Proceedings* (2005), vol. 3632 of *Lecture Notes in Computer Science*, Springer.

[LX482] HERMANN, M., AND VORONKOV, A., Eds. *Logic for Programming, Artificial Intelligence, and Reasoning, 13th International Conference, LPAR 2006, Phnom Penh, Cambodia, November 13-17, 2006, Proceedings* (2006), vol. 4246 of *Lecture Notes in Computer Science*, Springer.

[LX483] LAUDER, A. G. B., AND WAN, D. Counting points on varieties over finite fields of small characteristic. In *Algorithmic Number Theory : Lattices, Number Fields, Curves and Cryptography* (Cambridge, 2006), J. P. Buhler and P. Stevenhagen, Eds., Mathematical Sciences Research Institute Publications, Cambridge University Press. To appear ; preprint available since 2002.

[LX484] LIBERT, B. *New Secure Applications of Bilinear Maps in Cryptography*. Thèse de doctorat, Université catholique de Louvain, Louvain-la-Neuve, 2006.

[LX485] PFENNING, F., Ed. *Term Rewriting and Applications, 17th International Conference, RTA 2006, Seattle, WA, USA, August 12-14, 2006, Proceedings* (2006), vol. 4098 of *Lecture Notes in Computer Science*, Springer.

[LX486] PINTÉR, J., Ed. *Global Optimization : Scientific and Engineering Case Studies*. Springer, Berlin, 2006.

[LX487] TESKE, E. An elliptic trapdoor system. *J. of Cryptology 19*, 1 (2006), 115–133.

[LX488] ALTENKIRCH, T., AND MCBRIDE, C., Eds. *Types for Proofs and Programs, International Workshop, TYPES 2006, Nottingham, UK, April 18-21, 2006, Revised Selected Papers* (2007), vol. 4502 of *Lecture Notes in Computer Science*, Springer.

[LX489] BAADER, F., Ed. *Term Rewriting and Applications, 18th International Conference, RTA 2007, Paris, France, June 26-28, 2007, Proceedings* (2007), vol. 4533 of *Lecture Notes in Computer Science*, Springer.

[LX490] BERNSTEIN, D. Proving primality in essentially quartic expected time. *Math. Comp. 76* (2007), 389–403.

[LX491] DERSHOWITZ, N., AND VORONKOV, A., Eds. *Logic for Programming, Artificial Intelligence, and Reasoning, 14th International Conference, LPAR 2007, Yerevan, Armenia, November 15-19, 2007, Proceedings* (2007), vol. 4790 of *Lecture Notes in Computer Science*, Springer.

[LX492] DUPARC, J., AND HENZINGER, T. A., Eds. *Computer Science Logic, 21st International Workshop, CSL 2007, 16th Annual Conference of the EACSL, Lausanne, Switzerland, September 11-15, 2007, Proceedings* (2007), vol. 4646 of *Lecture Notes in Computer Science*, Springer.

[LX493] ROCCA, S. R. D., Ed. *Typed Lambda Calculi and Applications, 8th International Conference, TLCA 2007, Paris, France, June 26-28, 2007, Proceedings* (2007), vol. 4583 of *Lecture Notes in Computer Science*, Springer.

[LX494] SCHNEIDER, K., AND BRANDT, J., Eds. *Theorem Proving in Higher Order Logics, 20th International Conference, TPHOLs 2007, Kaiserslautern, Germany, September 10-13, 2007, Proceedings* (2007), vol. 4732 of *Lecture Notes in Computer Science*, Springer.

[LX495] FLOUDAS, C., AND PARDALOS, P., Eds. *Encyclopoedia of Optimization*. Springer, New York, 2008. to appear.

[LX496] LIBERTI, L., LAVOR, C., NASCIMENTO, M. C., AND MACULAN, N. Reformulation in mathematical programming : an application to quantum chemistry. *Discrete Applied Mathematics* (2008). accepted for publication.