Activity Report 2018

Team MOCQUA

Designing the Future of Computational Models

Inria teams are typically groups of researchers working on the definition of a common project, and objectives, with the goal to arrive at the creation of a project-team. Such project-teams may include other partners (universities or research institutions).

Table of contents

Team MOCQUA

Creation of the Team: 2018 January 01

Keywords:

Computer Science and Digital Science:

        A2.3.2. - Cyber-physical systems
        A2.4.1. - Analysis
        A6.5. - Mathematical modeling for physical sciences
        A7.1.4. - Quantum algorithms
        A7.2. - Logic in Computer Science
        A7.3. - Calculability and computability
        A8.1. - Discrete mathematics, combinatorics
        A8.3. - Geometry, Topology
        A8.6. - Information theory

Other Research Topics and Application Domains:

        B9.5.1. - Computer science
        B9.5.2. - Mathematics
        B9.5.3. - Physics

1. Team, Visitors, External Collaborators

Research Scientists

    Frédéric Dupont-Dupuis [CNRS, Researcher]
    Nazim Fatès [Inria, Researcher]
    Isabelle Gnaedig [Deputy team leader, Inria, Researcher]
    Mathieu Hoyrup [Inria, Researcher]
    Simon Perdrix [CNRS, Researcher]

Faculty Members

    Emmanuel Jeandel [Team leader, Univ de Lorraine, Professor, HDR]
    Emmanuel Hainry [Univ de Lorraine, Associate Professor]
    Irène Marcovici [Univ de Lorraine, Associate Professor, from Sep 2018]
    Romain Péchoux [Univ de Lorraine, Associate Professor]

Post-Doctoral Fellows

    Francesco Arzani [CNRS, from Oct 2018]
    Donald Stull [Inria]
    Vladimir Zamdzhiev [CNRS, from Sep 2018]

PhD Students

    Pierre Mercuriali [Univ de Lorraine]
    Renaud Vilmart [Univ de Lorraine]
    Titouan Carette [Univ de Lorraine, from Sep 2018]

Interns

    Sofien Ben Ayed [Inria, from Jun 2018 until Aug 2018]
    Titouan Carette [CNRS, until Jun 2018]
    Henri de Boutray [Univ de Lorraine, from Feb 2018 until Jul 2018]
    Nicolas Gauville [Univ de Lorraine, Aug 2018]

Louis Lemonnier [Univ de Lorraine, from Jun 2018 until Jul 2018]
Administrative Assistants
Anne Chrétien [Univ de Lorraine, from Apr 2018 until Sep 2018]
Sophie Drouot [Inria]
Sylvie Hilbert [CNRS, from Jun 2018]
Annick Jacquot [CNRS, from Jul 2018]
Visiting Scientists
Alexander Frank [Univ Andres Bello, from Sep 2018 until Oct 2018]
Luis Cristobal Rojas [Univ Andres Bello, Sep 2018]
Victor Selivanov [Univ Kazan, Sep 2018]
Bruce Kapron [University of Victoria, Oct 2018]
Damiano Mazza [CNRS, Université Paris 13, Mar 2018]

2. Overall Objectives

2.1. Designing the future of computational models

The goal of the Mocqua team is to tackle challenges coming from the emergence of new or future computational models. The landscape of computational models has indeed changed drastically in the last few years: the complexity of digital systems is continually growing, which leads to the introduction of new paradigms, while new problems arise due to this larger scale (tolerance to faulty behaviors, asynchronicity) and constraints of the present world (energy limitations). In parallel, new models based on physical considerations have appeared. There is thus a real need to accompany these changes, and we intend to investigate these new models and try to solve their intrinsic problems by computational and algorithmic methods.

While the bit remains undeniably the building block of computer architecture and software, it is fundamental for the development of new paradigms to investigate computations and programs working with inputs that cannot be reduced to finite strings of 0's and 1's. Our team will focus on a few instances of this phenomenon: programs working with qubits (quantum computing), programs working with functions as inputs (higher-order computation) and programs working in infinite precision (real numbers, infinite sequences, streams, coinductive data, ...).

3. Research Program

3.1. Quantum Computing

While it can be argued that the quantum revolution has already happened in cryptography [35] or in optics [34], quantum computers are far from becoming a common commodity, with only a few teams around the world working on a practical implementation. In fact, one of the most commonly known examples of a quantum computer, the D-Wave 2X System, defies the usual definition of a computer: it is not general-purpose, and can only solve (approximately) a very specific hardwired problem.

Most current prototypes of a quantum computer differ fundamentally on the hardware substrate, and it is quite hard to predict which solution will finally be adopted. The landscape of quantum programming languages is also constantly evolving. Comparably to compiler design, the foundation of quantum software therefore relies on an intermediate representation that is suitable for manipulation, easy to produce from software and easily encodable into hardware. The language of choice for this is the ZX-calculus.

Regardless of the actual model that will be accepted by the industry, it is becoming clear that some of the hurdles into scaling up quantum computers from a few qubits to very large arrays will remain. As an example, current implementations of quantum computers working on hundreds of qubits indeed are not able to form and maintain all possible forms of entanglement between qubits. This raises two questions. First, does this restrict the computational power, and the supposed advantage of the quantum computer over the classical computer? Second, how to ensure that a quantum program that was designed for a theoretical quantum computer will work on the practical implementations? This will be investigated, in particular by providing static analysis methods for evaluating a priori how much entanglement a quantum program needs.

3.2. Higher-Order Computing

While programs often operate on natural numbers or finite structures such as graphs or finite strings, they can also take functions as input. In that case, the program is said to perform higher-order computations, or to compute a higher-order functional. Functional programming or object-oriented programming are important paradigms allowing higher-order computations.

While the theory of computation is well developed for first-order programs, difficulties arise when dealing with higher-order programs. There are many non-equivalent ways of presenting inputs to such programs: an input function can be presented as a black-box, encoded in an infinite binary sequence, or sometimes by a finite description. Comparing those representations is an important problem. A particularly useful application of higher-order computations is to compute with infinite objects that can be represented by functions or symbolic sequences. The theory works well in many cases (to be precise, when these objects live in a topological space with a countable basis [40]), but is not well understood in other interesting cases. For instance, when the inputs are the second-order functionals (of type $(\mathbb{N} \to \mathbb{N}) \to (\mathbb{N} \to \mathbb{N})$), the classical theory does not apply and many problems are still open.

3.3. Dynamical Systems

The most natural example of a computation with infinite precision is the simulation of a dynamical system. The underlying space might be $\mathbb{R}^n$ in the case of the simulation of physical systems, or the Cantor space $\{0, 1\}^{\mathbb{Z}}$ in the case of discrete dynamical systems.

From the point of view of computation, the main point of interest is the link between the long-term behavior of a system and its initial configuration. There are two questions here: (a) predict the behavior, (b) design dynamical systems with some prescribed behavior. The first will be mainly examined through the angle of reachability and more generally control theory for hybrid systems.

The model of cellular automata will be of particular interest. This computational model is relevant for simulating complex global phenomena which emerge from simple interactions between simple components. It is widely used in various natural sciences (physics, biology, etc.) and in computer science, as it is an appropriate model to reason about errors that occur in systems with a great number of components.

The simulation of a physical dynamical system on a computer is made difficult by various aspects. First, the parameters of the dynamical systems are seldom exactly known. Secondly, the simulation is usually non exact: real numbers are usually represented by floating-point numbers, and simulations of cellular automata only simulate the behavior of finite or periodic configurations. For some chaotic systems, this means that the simulation can be completely irrelevant.

4. Application Domains

4.1. Quantum Computing

Quantum Computing is currently the most promising technology to extend Moore's law, whose end is expected with the engraving at 7 nm, in less than 5 years. Thanks to the exponential computational power it will bring, it will represent a decisive competitive advantage for those who will control it.

Quantum Computing is also a major security issue, since it allows us to break today's asymmetric cryptography. Hence, mastering quantum computing is also of the highest importance for national security concerns. Recent scientific and technical advances suggest that the construction of the first quantum computers will be possible in the coming years, even if their capabilities will not allow to reach the so-called quantum supremacy at first.

As a result, the major US players in the IT industry have embarked on a dramatic race, mobilizing huge resources: IBM, Microsoft, Google and Intel have each invested between 20 and 50 million euros, and are devoting significant budgets to attract and hire the best scientists on the planet. Some states have launched ambitious national programs, including Great Britain, the Netherlands, Canada, China, Australia, Singapore, and very recently Europe, with the upcoming 10-year FET Flagship program in Quantum Engineering.

While a large part of these resources are going towards R-&-D in quantum hardware, there is still an important need and real opportunities for leadership in the field of quantum software.

The Mocqua team contributes to the computer science approach to quantum computing, aka the quantum software approach. We aim at a better understanding of the power and limitations of the quantum computer, and therefore of its impact on society. We also contribute to ease the development of the quantum computer by filling the gap between the theoretical results on quantum algorithms and complexity and the recent progresses in quantum hardware.

4.2. Higher-Order Computing

The idea of considering functions as first-class citizens and allowing programs to take functions as inputs has emerged since the very beginning of theoretical computer science through Church's λ-calculus and is nowadays at the core of functional programming, a paradigm that is used in modern software and by digital companies (Google, Facebook, ...). In the meantime higher-order computing has been explored in many ways in the fields of logic and semantics of programming languages.

One of the central problems is to design programming languages that capture most of, if not all, the possible ways of computing with functions as inputs. There is no Church thesis in higher-order computing and many ways of taking a function as input can be considered: allowing parallel or only sequential computations, querying the input as a black-box or via an interactive dialog, and so on.

The Kleene-Kreisel computable functionals are arguably the broadest class of higher-order continuous functionals that could be computed by a machine. However their complexity is such that no current programming language can capture all of them. Better understanding this class of functions is therefore fundamental in order to identify the features that a programming language should implement to make the full power of higher-order computation expressible in such a language.

4.3. Simulation of Dynamical Systems by Cellular Automata

We aim at developing various tools to simulate and analyse the dynamics of spatially-extended discrete dynamical systems such as cellular automata. The emphasis of our approach is on the evaluation of the robustness of the models under study, that is, their capacity to resist various perturbations.

In the framework of pure computational questions, various examples of such systems have already been proposed for solving complex problems with a simple bio-inspired approach (e.g. the decentralized gathering problem [39]). We are now working on their transposition to various real-world situations. For example when one needs to understand the behaviour of large-scale networks of connected components such as wireless sensor networks. In this direction of research, a first work has been presented on how to achieve a decentralized diagnosis of networks made of simple interacting components and the results are rather encouraging [27]. Nevertheless, there are various points that remain to be studied in order to complete this model for its integration in a real network.

We have also tackled the question of the evaluation of the robustness of a swarming model proposed by A. Deutsch to mimic the self-organization process observed in various natural systems (birds, fishes, bacteria, etc.) [19]. We now wish to develop our simulation tools to apply them to various biological phenomena where a great number of agents are implied.

We are also currently extending the range of of application of these techniques to the field of Economy. We have started a collaboration with Massimo Amato, a professor in Economy at the Bocconi University in Milan. Our aim is to examine how to propose a decentralized view of a business-to-business market and propose agent-oriented and totally decentralized models of such markets. Various banks and large businesses have already expressed their interest in such modelling approaches.

5. Highlights of the Year

5.1. Highlights of the Year

Completeness of the ZX-Calculus

We have proved this year the completeness of the ZX-calculus. The completeness of the ZX-calculus was the main open question in the field of categorical quantum mechanics and was open for about 10 years. This results has been published at LiCS'18 [17], [16] and also presented at TQC'18 and QIP'19, the main two conferences in quantum information processing.

6. New Software and Platforms

6.1. Software

6.1.1. FiatLux

- Participants: Nazim Fatès, Nicolas Gauville

FiatLux is a simulation program for cellular automata and discrete dynamical systems. It is developed by Nazim Fatès ; the project is currently available at the Inria GForge. The program is published with the CeCILL license. New features have been implemented in 2018, as for example the possibility to define some systems directly in the software by writing the local transition rules in Java. These features were mostly added by Nicolas Gauville, a Master's student who was an intern in the team.

7. New Results

7.1. Completeness of the ZX-calculus

- Participants: Renaud Vilmart, Simon Perdrix, Emmanuel Jeandel

The ZX-Calculus is a powerful graphical language for quantum reasoning and quantum computing introduced by Bob Coecke and Ross Duncan [36]. The ZX-calculus has several applications in quantum information processing [37] (e.g. measurement-based quantum computing, quantum codes, foundations), and can be used through the interactive theorem prover Quantomatic. However, the main obstacle to wider use of the ZX-calculus was the absence of a *completeness* result for a *universal* fragment of quantum mechanics, in order to guarantee that any true property is provable using the ZX-calculus. We have introduced the first complete axiomatisation for a universal fragment of quantum mechanics. We also showed that a single additional rule makes the ZX-calculus complete for the whole pure qubit quantum mechanics. These results have been presented at LICS this year [16], [17] and will be presented at QIP'19, the main conference in quantum information processing.

7.2. Second-order entropy accumulation theorem

- Participants: Frédéric Dupuis

Device-independent cryptography is a way to use quantum mechanics to perform cryptographic tasks using equipment from an untrusted manufacturer. To prove the security of device-independent protocols, the main challenge is to show that a step-by-step procedure involving the untrusted device produces a certain of randomness even from the point of view of the manufacturer. The entropy accumulation theorem [38] provides a generic way to obtain such statements. However, while the bounds provided by this theorem are optimal in the first order (meaning the term that is linear in the number of steps in the process), the second-order sublinear term is bounded more crudely, in such a way that the bounds deteriorate significantly when the theorem is applied directly to protocols where parameter estimation is done by sampling a small fraction of the positions, as is done in most QKD protocols. In [25], we improve this second-order sublinear term and remedy this problem. This paper has been submitted to IEEE Transactions on Information Theory.

7.3. Mixed-state certification

- Participants: Frédéric Dupuis

Mixed-state certification consists of ensuring that a quantum state on n subsystems is close to n copies of a given mixed state, up to a small number of errors, by sampling a small fraction of the positions. While this task makes no sense classically (it effectively amounts to certifying that a string came from a particular probability distribution), it makes sense quantumly if we can ask someone (that we call a prover) to supply purifications of the sampled positions. However, such sampling procedures cannot be analyzed straightforwardly using standard sampling results, and care must be taken even when defining what success means. In [26], we introduced these concepts, and we showed that this sampling protocol offers secure certification in the presence of a possibly dishonest prover. We then applied this result to two-party quantum coin-tossing. This work was presented at QCrypt 2018 and TCC 2018 (and will appear in the proceedings of the latter).

7.4. Descriptive Set Theory

- Participants: Mathieu Hoyrup

Descriptive Set Theory (DST) aims at classifying sets and functions in terms of the complexity of describing them. It is closely related to logic and computation theory, where sets and functions can be described by logical formulas or computer programs. DST was originally developed on a restricted class of topological spaces, the Polish spaces, which does not cover important classes of spaces that are needed in Theoretical Computer Science, especially in programming semantics, notably (Scott) domains or spaces of higher-order (Kleene-Kreisel) functionals. We investigate DST on such spaces and show that it does not work as nicely as on usual spaces. The article [29] is currently submitted. This work has been presented during an invited talk at CiE 2018 [13].

7.5. Semicomputable geometry

- Participants: Mathieu Hoyrup

Semicomputability is a natural notion arising from logic and theoretical computer science. Termination of programs is not decidable but semidecidable. Semicomputability of subsets of the plane is an important notion. For instance whether the famous Mandelbrot set is computable is still an open problem, while its semicomputability is easy to prove. Intuitively, we can write a program that progressively fills out the complement of the set, but we do not know when the picture is complete. We studied semicomputability of much simpler sets, namely filled triangles. While this problem looks simple at first sight, it is considerably rich and raises many questions. What properties should the coordinates of the vertices of a triangle satisfy to make it semicomputable? How can we parametrize such triangles? What happens for other sets such as disks or general convex sets? We developed a thorough study of these problems in [15].

7.6. Resource bounded computation

- Participants: Emmanuel Hainry

Controlling resource consumption is a crucial aspect of programming. Resources such as time, space, intrication are limited, and helping the programmer to avoid overconsumption or pointing problematic code is an important endeavor. We introduced a type-system for an Object Oriented Programming Language (*à la* Java) that gives a guarantee of polynomial-time computability provided that the program halts [12]. This result has several interesting features as it works with complex object data-structures in a real-like programming language; checking the type system is polynomial time decidable; we provided a O bound hence giving an explicit worst case complexity bound.

7.7. Inductive reasoning

- Participants: Isabelle Gnaedig, Sofien Ben Ayed

We are interested in quantifying the power of axiomatic theories. For this purpose, induction is a key concept. We have investigated the different validity proofs of inductive reasoning, the equivalence of induction with the well-ordered principle and well-foundedness, the differences between first and second order forms of the induction principle, and the notion of ω-consistency, qualifying theories interpreting arithmetic for which proving a property for each value of standard integers does not imply that the property is always true. We have also studied the importance of the axiom of choice for induction, and analysed a recent interpretation of induction by Hardin and Taylor through the hat problem [22].

7.8. Cellular automata with stochastic evolutions

- Participants: Nazim Fatès, Irène Marcovici

In order to explore the computing abilities of simple stochastic cellular automata, we tackle the case of Alesia, a two-player zero-sum game which is quite similar to the rock-paper-scissors game. In this game, two players simultaneously move and do not know what the opponent plays at a given round. The simultaneity of the moves implies that there is no deterministic good strategy in this game, otherwise one would anticipate the moves of the opponent and easily win the game. We explored how to build a family of one-dimensional stochastic cellular automata to play this game by progressively increasing the complexity of the transitions. We showed the possibility to construct a family of rules with interesting results, including good performance when confronted to the Nash-equilibrium strategy [14].

The reversibility of classical cellular automata (CA) was examined for the case where the updates of the system are random. In this context, with B. Sethi and S. Das (IIT Karaghpur, India), we studied a particular form of reversibility: the possibility of returning infinitely often to the initial condition after a random number of time steps. This is the recurrence property of the system. We analyzed this property for the simple rules and described the communication graph of the system [21].

We also contributed to the diffusion of some already-established knowledge on the simulation of complex systems in Biology, more precisely in the case of the formation of swarms [19] and in the case of asynchronous cellular automata [20].

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- Project acronym: ANR PRCE SoftQPro (ANR-17-CE25-0009)
  Project title: Solutions logicielles pour l'optimisation des programmes et ressources quantiques.
  Duration: Dec. 2017 - Nov. 2021
  Coordinator: Simon Perdrix
  Other partners: Atos-Bull, LRI, CEA-Saclay.
  Participants: Simon Perdrix, Emmanuel Jeandel, Emmanuel Hainry, and Romain Péchoux
  Abstract: Quantum computers can theoretically solve problems out of reach of classical computers. We aim at easing the crucial back and forth interactions between the theoretical approach to quantum computing and the technological efforts made to implement the quantum computer. Our software-based quantum program and resource optimisation (SoftQPRO) project consists in developing high level techniques based on static analysis, certification, transformations of quantum graphical languages, and optimisation techniques to obtain a compilation suite for quantum programming languages. We will target various computational model back-ends (e.g. QRAM, measurement-based quantum computations) as well as classical simulation. Classical simulation is central in the development of the quantum computer, on both ends: as a way to test quantum programs but also as a way to test quantum computer prototypes. For this reason we aim at designing sophisticated simulation techniques on classical high-performance computers (HPC).

- Project acronym: ANR PRCI VanQuTe (ANR-17-CE24-0035)
  Project title: Validation of near-future quantum technologies.
  Duration: Dec. 2017 - Nov. 2021
  Coordinator: Simon Perdrix
  Other partners: Atos-Bull, LRI, CEA-Saclay.
  Participants: Simon Perdrix, Emmanuel Jeandel, Emmanuel Hainry, and Romain Péchoux
  Abstract: Quantum computers can theoretically solve problems out of reach of classical computers. We aim at easing the crucial back and forth interactions between the theoretical approach to quantum computing and the technological efforts made to implement the quantum computer. Our software-based quantum program and resource optimisation (SoftQPRO) project consists in developing high level techniques based on static analysis, certification, transformations of quantum graphical languages, and optimisation techniques to obtain a compilation suite for quantum programming languages. We will target various computational model back-ends (e.g. QRAM, measurement-based quantum computations) as well as classical simulation. Classical simulation is central in the development of the quantum computer, on both ends: as a way to test quantum programs but also as a way to test quantum computer prototypes. For this reason we aim at designing sophisticated simulation techniques on classical high-performance computers (HPC).

8.1.2. Autres initiatives

- Quantex. Project acronym: PIA-GDN/Quantex. (initially an ITEA3 project finally funded by the *Grands défis du Numérique / Programme d'investissements d'avenir*).
  Project title: Simulation/Emulation of Quantum Computation.
  Duration: Feb. 2018 - Jan 2021.
  Coordinator: Huy-Nam Nguyen (Atos Bull).
  Other partners: Atos-Bull, LRI, CEA Grenoble.
  Participants: Simon Perdrix (WP leader), Emmanuel Jeandel
  Abstract: The lack of quantum computers leads to the development of a variety of software-based simulators to assist in the research and development of quantum algorithms. This proposal focuses on the development of a combined software-based and hardware-accelerated toolbox for quantum computation. A quantum computing stack including specification language, libraries and optimisation/execution tools will be built upon a well-defined mathematical framework mixing classical and quantum computation. Such an environment will be dedicated to support the expression of quantum algorithms for the purpose of investigation and verification.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

Mathieu Hoyrup participates in the Marie-Curie RISE project Computing with Infinite Data coordinated by Dieter Spreen (Univ. Siegen) that has started in April 2017.

8.3. International Initiatives

8.3.1. Inria International Labs

8.3.1.1. IIL projects

Simon Perdrix is the WP leader in the ANR PRCI project VanQuTe (with LIP6, and the Singapore University of Technology and Design, the National University of Singapore, and the Nanyang Technological University). Emmanuel Jeandel is also a member of this project.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Victor Selivanov (Kazan University) was an Inria invited researcher in September 2018. We have worked on the computable aspects of Descriptive Set Theory.
- Cristóbal Rojas (Universidad Andres Bello, Santiago) visited us during one month in September 2018. We have worked on the computable aspects of invariant measures in dynamical systems.
- Alexander Frank (Universidad Andres Bello, Santiago) visited us during three weeks in September-October 2018. We have worked on the computable aspects of invariant measures in dynamical systems.
- Bruce Kapron (University of Victoria, Canada) visited us in October 2018. We have worked on applications of tier based type systems to characterize the class of second order functionals computable in polynomial time.
- Damiano Mazza (CNRS, Université de Paris 13) visited us in March 2018. We have worked on the adaptation of linear logic to a functional programming languages with infinite streams to characterize the class of first order functions over the real computable in polynomial time.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Emmanuel Jeandel organized with three other colleagues the "Jeunes-Chercheurs" school of GDR IM.
- Frédéric Dupuis and Simon Perdrix organized the "Journées informatique quantique" in Nancy, Novembre 2018.
- Nazim Fatès and Irène Marcovici organised a "Journée Charles Hermite" on the theme "Cellular automata and dynamics on networks" (Nancy, Decembre 2018).

9.1.1.2. Member of the Organizing Committees

- Mathieu Hoyrup is member of the Steering Committee of the Conference Series *Computability in Europe* (CiE) for the period 2017-2021.
- Simon Perdrix is in the Scientific Board of the Colloquium IQFA (Montpellier, Novembre 2018).

- Nazim Fatès is a member of the steering committee of the Summer Solstice Conference on Discrete Models of Complex Systems.

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Mathieu Hoyrup was PC member of the workshop Continuity, Computability, Constructivity - From Logic to Algorithms (CCC) 2018, Faro, September 2018.
- Emmanuel Jeandel and Simon Perdrix were PC members of MCU 2018 (https://mcu2018.lacl.fr/).
- Romain Péchoux was PC member of the workshop DICE 2018 (http://cl-informatik.uibk.ac.at/users/zini/events/dice18/).
- Frédéric Dupuis was PC member of QCrypt 2018 (http://2018.qcrypt.net/) and QIP 2019 (http://jila.colorado.edu/qip2019/).
- Nazim Fatès was a PC member of Automata 2018 and ACRI 2018.

9.1.2.2. Reviewer

- Mathieu Hoyrup reviewed articles for LICS, CiE and ICALP.
- Romain Péchoux reviewed articles for DICE, ISMVL and CSL.
- Frédéric Dupuis reviewed articles for QCrypt 2018, QIP 2019, CRYPTO 2018, and AQIS 2018.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- Emmanuel Jeandel is member of the editorial board of RAIRO-ITA (Revue d'Automatique, d'Informatique et de Recherche Opérationnelle: Informatique théorique et applications).
- Romain Péchoux is guest editor for a Theoretical Computer Science special issue on Implicit Computational Complexity (https://www.journals.elsevier.com/theoretical-computer-science/call-for-papers/mplicit-computational-complexity).
- Nazim Fatès is a member of the editorial board of the *Journal of cellular automata*.

9.1.3.2. Reviewer - Reviewing Activities

- Mathieu Hoyrup reviewed articles for Discrete and Continuous Dynamical Systems, Information and Computation, and Theoretical Computer Science.
- Romain Péchoux reviewed articles for Information Processing Letters, Journal of Automated Reasoning and Theoretical Computer Science.
- Frédéric Dupuis reviewed articles for Nature Communications, Quantum, IEEE Transactions on Information Theory, Physical Review A, Journal of Physics A, and the Journal of Mathematical Physics.
- Nazim Fatès reviewed articles on cellular automata for the *Journal of cellular automata*, *Physical Review A*, *Chaos, Solitons & Fractals* and *Informatica*.

9.1.4. Invited Talks

- Mathieu Hoyrup was invited to give a talk at the special session Continuous Computation at CiE 2018.
- Nazim Fatès was invited to give a talk on artificial intelligence in the "Colloque Cathy Dufour 2018" held in Nancy in November 2018.

9.1.5. Scientific Expertise

- Romain Péchoux was expert for the European Commission H2020 Marie Skłodowska-Curie Individual Fellowships.
- Nazim Fatès served as an expert for the Chilean national institute of research CONICYT.

9.1.6. Research Administration

- Simon Perdrix is the Scientific Secretary of the CoNRS Section 6. He was in the panel of the CR and DR recruitments at CNRS section 6.
- Frédéric Dupuis is on the board of the Fédération Charles-Hermite (Université de Lorraine).
- Emmanuel Hainry is a member of the CNU Section 27.
- Nazim Fatès is the vice-chair of the IFIP Working group 1.5 on cellular automata and discrete complex systems.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Licence
    - Isabelle Gnaedig:
        * To the limits of the computable, 6 hours, Opening course-conference of the collegium "Lorraine INP", Nancy, France
    - Emmanuel Hainry:
        * Operating Systems, 30h, L1, IUT Nancy Brabois
        * Algorithmics, 40h, L1, IUT Nancy Brabois
        * Dynamic Web, 60h, L1, IUT Nancy Brabois
        * Databases, 30h, L1, IUT Nancy Brabois
        * Object Oriented Languages, 16h, L2, IUT Nancy Brabois
        * Complexity, 30h, L2, IUT Nancy Brabois
    - Mathieu Hoyrup:
        * Bases de la Programmation Orientée Objet, 20 HETD, L2, Université de Lorraine, France
        * Interfaces Graphiques, 10 HETD, L2, Université de Lorraine, France
    - Emmanuel Jeandel:
        * Algorithmics and Programming 1, 60h, L1 Maths-Info
        * Data Compression, 30h, L2 Informatique
        * Algorithmics and Programming 4, 30h, L3 Informatique
        * Modeling Using Graph Theory, 30h, L3 Informatique
        * Networking, 15h, L3 Informatique
        * Formal Languages, 30h, L3 Informatique
    - Romain Péchoux:
        * Programmation orientée objet, 61,5h, L3 MIASHS
        * Programmation orientée objet, 53,5h, L2 MIASHS
        * Outils logiques pour l'informatique, 35h, L1 MIASHS
        * Bases de données, 40h, L3 Sciences de la Gestion
        * Algorithmic complexity, 30h, L3 MIAGE, IGA Rabat, Morocco.
- Master
    - Isabelle Gnaedig:
        * Design of Safe Software, Coordination of the module, M2, Telecom-Nancy (Université de Lorraine), Nancy, France,

      * Rule-based Programming, 20 hours, M2, Telecom-Nancy (Université de Lorraine), Nancy, France.

   – Emmanuel Jeandel:

      * Algorithmics and Complexity, 30h, M1 Informatique

   – Nazim Fatès:

      * Systèmes distribués adaptatifs, 10h, Master 2, informatique.

      * Agents intelligents et collectifs, 15h, Master 1, sciences cognitives.

9.2.2. Supervision

- PhD in progress: Renaud Vilmart, "Langages graphiques pour calculer et raisonner en quantique", Start: October 2016, Advisors: Emmanuel Jeandel and Simon Perdrix.

- PhD in progress: Titouan Carette, "Langage diagrammatique pour l'ordinateur quantique", Start: October 2018, Advisors: Emmanuel Jeandel and Simon Perdrix.

- PhD in progress: Pierre Mercuriali, "Calcul à base de médiane et structures médianes pour la classification", Start: October 2016, Advisors: Miguel Couceiro and Romain Péchoux.

- PhD in progress: Robert Booth, "Formalismes pour la vérification de technologies quantiques", Start: November 2018, Advisors: Damian Markham and Simon Perdrix.

9.2.3. Juries

- Emmanuel Jeandel reviewed the PhD thesis of Silvère Gangloff (Aix-Marseille Université - Université Toulouse III).

- Simon Perdrix was examiner for the PhD thesis of Alex Bredariol Grilo (IRIF, Université Paris Diderot), April 27 2018.

- Frédéric Dupuis was examiner for the PhD thesis of Christoph Hirche (Universitat Autònoma de Barcelona), May 9, 2018.

9.3. Popularization

9.3.1. Articles and contents

Nazim Fatès and Irène Marcovici presented an article on cellular automata in the wide audience scientific magazine *La recherche* [23]. This article appeared in an issue dedicated to "chaos and complexity" (July-August 2018).

Simon Perdrix has been one of the editors of the ERCIM news special issue on Quantum Computing.

9.3.2. Education

Nazim Fatès participated in a day of training destined to high school teachers of the "Académie de Poitiers" with a conference and discussions with the participants. The meeting was held on April 25, 2018, in the Lycée Victor Hugo of Poitiers and was also followed on the internet by teachers located abroad (DOM-TOM).

9.3.3. Interventions

Nazim Fatès participated to a debate for a large public on the theme "Space and artificial intelligence" in the Cité des sciences et de l'industrie in Paris. This debate was part of a series of events dedicated to celebrations of the fiftieth year of the film *2001, A space Odyssey*.

Nazim Fatès joined the Pariscience Festival for animating a debate on artificial intelligence with high-school students of the region of Paris. The discussion, held together with a researcher from the INSERM institute, followed the projection of the film *IA : votre nouveau cerveau* and a collective game to debate on the question of artificial intelligence.

Nazim Fatès participated in an open debate on the theme: "L'intelligence artificielle, quel avenir pour les artistes et créateurs d'aujourd'hui ?". This debate was held in conjunction with the RING Theater Festival in Nancy (Rencontres Internationales des Nouvelles Générations) in April 2018.

Nazim Fatès participated in an open debate on the general theme of joining science and art in conjunction with the exposition "Retina Pictonique" which was held in July 2018 in Toulouse in the CEMES Laboratory.

Nazim Fatès participated in an open debate on the theme "L'intelligence artificielle est-elle vraiment maligne ?" in the Shadok fab-lab of Strasbourg. The debate gathered more than a hundred persons and was preceded by an interview in the magazine *Rue 89 Strasbourg*.

9.3.4. Internal action

Nazim Fatès gave a talk on artificial intelligence in the *Café-In* meeting, one of the Inria Nancy Grand-Est series of talks destined to all the employees of the laboratory (March 13, 2018).

Frédéric Dupuis also gave a *Café'In* talk on quantum computing (February 13, 2018).

10. Bibliography

Major publications by the team in recent years

[1] O. BOURNEZ, D. GRAÇA, E. HAINRY. *Computation with perturbed dynamical systems*, in "Journal of Computer and System Sciences", August 2013, vol. 79, n⁰ 5, pp. 714-724 [*DOI :* 10.1016/J.JCSS.2013.01.025], http://hal.inria.fr/hal-00861041

[2] N. FATÈS, I. MARCOVICI, S. TAATI. *Two-dimensional traffic rules and the density classification problem*, in "International Workshop on Cellular Automata and Discrete Complex Systems, AUTOMATA 2016", Zürich, France, Lecture Notes of Computer Science, June 2016, vol. 9664 [*DOI :* 10.1007/978-3-319-39300-1_11], https://hal.inria.fr/hal-01290290

[3] H. FÉRÉE, E. HAINRY, M. HOYRUP, R. PÉCHOUX. *Characterizing polynomial time complexity of stream programs using interpretations*, in "Journal of Theoretical Computer Science (TCS)", January 2015, vol. 585, pp. 41-54 [*DOI :* 10.1016/J.TCS.2015.03.008], https://hal.inria.fr/hal-01112160

[4] I. GNAEDIG, H. KIRCHNER. *Proving Weak Properties of Rewriting*, in "Theoretical Computer Science", 2011, vol. 412, pp. 4405-4438 [*DOI :* 10.1016/J.TCS.2011.04.028], http://hal.inria.fr/inria-00592271/en

[5] E. HAINRY, R. PÉCHOUX. *Objects in Polynomial Time*, in "APLAS 2015", Pohang, South Korea, X. FENG, S. PARK (editors), Lecture Notes in Computer Science, Springer, November 2015, vol. 9458, pp. 387–404 [*DOI :* 10.1007/978-3-319-26529-2_21], https://hal.inria.fr/hal-01206161

[6] M. HOYRUP, W. GOMAA. *On the extension of computable real functions*, in "32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017", IEEE Computer Society, 2017, pp. 1–12, https://doi.org/10.1109/LICS.2017.8005067

[7] M. HOYRUP. *The decidable properties of subrecursive functions*, in "International Colloquium on Automata, Languages, and Programming (ICALP) 2016", Rome, Italy, 43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 12-15, 2016, Rome, Italy, July 2016 [*DOI :* 10.4230/LIPIcs.ICALP.2016.108], https://hal.inria.fr/hal-01308224

[8] E. JEANDEL. *Computability of the entropy of one-tape Turing Machines*, in "STACS - Symposium on Theoretical Aspects of Computer Science", Lyon, France, E. MAYR, N. PORTIER (editors), LIPCS, March 2014, vol. 25, pp. 421-432, First version [*DOI :* 10.4230/LIPICS.STACS.2014.421], https://hal.inria.fr/hal-00785232

[9] E. JEANDEL, P. VANIER. *Hardness of Conjugacy, Embedding and Factorization of multidimensional Subshifts of Finite Type*, in "STACS - 30th International Symposium on Theoretical Aspects of Computer Science", Kiel, Germany, N. PORTIER, T. WILKE (editors), Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, February 2013, vol. 20, pp. 490–501 [*DOI :* 10.4230/LIPICS.STACS.2013.490], http://hal.inria.fr/hal-00840384

[10] S. PERDRIX, Q. WANG. *Supplementarity is Necessary for Quantum Diagram Reasoning **, in "41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016)", Krakow, Poland, Leibniz International Proceedings in Informatics (LIPIcs), August 2016, vol. 58, pp. 76:1–76:14 [*DOI :* 10.4230/LIPICS.MFCS.2016.76], https://hal.archives-ouvertes.fr/hal-01361419

Publications of the year

Articles in International Peer-Reviewed Journals

[11] N. A. FATÈS. *Remarks on the cellular automaton global synchronisation problem – deterministic vs. stochastic models*, in "Natural Computing", 2018 [*DOI :* 10.1007/S11047-018-9683-0], https://hal.inria.fr/hal-01653631

[12] E. HAINRY, R. PÉCHOUX. *A Type-Based Complexity Analysis of Object Oriented Programs*, in "Information and Computation", August 2018, vol. 261, n° 1, pp. 78-115, https://arxiv.org/abs/1802.06653 [*DOI :* 10.1016/J.IC.2018.05.006], https://hal.inria.fr/hal-01712506

Invited Conferences

[13] M. HOYRUP. *Topological analysis of representations*, in "CiE 2018 - Fourteenth conference on Computability in Europe", Kiel, Germany, July 2018, https://hal.inria.fr/hal-01919395

International Conferences with Proceedings

[14] N. A. FATÈS. *A pedagogical example: a family of stochastic cellular automata that plays Alesia*, in "ACRI 2018 - 13th International Conference on Cellular Automata for Research and Industry", Como, Italy, International Conference on Cellular Automata (ACRI 2018), September 2018, vol. LNCS, n° 11115 [*DOI :* 10.1007/978-3-319-99813-8_35], https://hal.inria.fr/hal-01936310

[15] M. HOYRUP, D. NAVA SAUCEDO, D. M. STULL. *Semicomputable geometry*, in "ICALP 2018 - 45th International Colloquium on Automata, Languages, and Programming", Prague, Czech Republic, July 2018, https://hal.inria.fr/hal-01770562

[16] E. JEANDEL, S. PERDRIX, R. VILMART. *A Complete Axiomatisation of the ZX-Calculus for Clifford+T Quantum Mechanics*, in "The 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018", Oxford, United Kingdom, Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, July 2018, pp. 559–568, https://arxiv.org/abs/1705.11151 [*DOI :* 10.1145/3209108.3209131], https://hal.archives-ouvertes.fr/hal-01529623

[17] E. JEANDEL, S. PERDRIX, R. VILMART. *Diagrammatic Reasoning beyond Clifford+T Quantum Mechanics*, in "The 33rd Annual Symposium on Logic in Computer Science", Oxford, United Kingdom, Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, July 2018, pp. 569–578, https://arxiv.org/abs/1801.10142 [*DOI :* 10.1145/3209108.3209139], https://hal.archives-ouvertes.fr/hal-01716501

[18] I. MARCOVICI, T. STOLL, P.-A. TAHAY. *Construction of Some Nonautomatic Sequences by Cellular Automata*, in "AUTOMATA 2018 - 24th International Workshop on Cellular Automata and Discrete Complex Systems", Ghent, Belgium, J. M. BAETENS, M. KUTRIB (editors), Cellular Automata and Discrete Complex Systems, Springer International Publishing, June 2018, vol. LNCS-10875, pp. 113-126 [*DOI :* 10.1007/978-3-319-92675-9_9], https://hal.inria.fr/hal-01824876

Scientific Books (or Scientific Book chapters)

[19] N. FATÈS, V. CHEVRIER, O. BOURÉ. *Is there a trade-off between simplicity and robustness? Illustration on a lattice-gas model of swarming*, in "Probabilistic Cellular Automata", P.-Y. LOUIS, F. R. NARDI (editors), Emergence, Complexity and Computation, Springer, 2018 [*DOI :* 10.1007/978-3-319-65558-1_16], https://hal.inria.fr/hal-01230145

[20] N. A. FATÈS. *Asynchronous cellular automata*, in "Encyclopedia of Complexity and Systems Science", R. MEYERS (editor), Springer, 2018, 21 p. , This text has been proposed for the Encyclopedia of Complexity and Systems Science edited by Springer Nature and should appear in 2018 [*DOI :* 10.1007/978-3-642-27737-5_671-1], https://hal.inria.fr/hal-01653675

[21] N. FATÈS, B. SETHI, S. DAS. *On the reversibility of ECAs with fully asynchronous updating: the recurrence point of view*, in "Reversibility and Universality", Springer, 2018 [*DOI :* 10.1007/978-3-319-73216-9_15], https://hal.inria.fr/hal-01571847

Research Reports

[22] S. BEN AYED. *All aspects of inductive reasoning : Validite´, limites, formes et aspects re´cents du raisonnement inductif*, Inria Nancy - Grand Est, August 2018, Stage de 2ème année de l'Ecole Supérieure Nationale des Mines de Nancy, https://hal.archives-ouvertes.fr/hal-01885909

Scientific Popularization

[23] N. A. FATÈS, I. MARCOVICI. *Automates cellulaires : la complexité dans les règles de l'art*, in "La Recherche : l'actualité des sciences", July 2018, https://hal.inria.fr/hal-01847663

Other Publications

[24] M. COUCEIRO, P. MERCURIALI, R. PÉCHOUX, A. SAFFIDINE. *On the complexity of minimizing median normal forms of monotone Boolean functions and lattice polynomials*, 2018, working paper or preprint, https://hal.inria.fr/hal-01905491

[25] F. DUPUIS, O. FAWZI. *Entropy accumulation with improved second-order*, November 2018, https://arxiv.org/abs/1805.11652 - working paper or preprint, https://hal.inria.fr/hal-01925985

[26] F. DUPUIS, S. FEHR, P. LAMONTAGNE, L. SALVAIL. *Secure certification of mixed quantum states with application to two-party randomness generation*, November 2018, https://arxiv.org/abs/1804.04730 - working paper or preprint, https://hal.inria.fr/hal-01926631

[27] N. GAUVILLE. *Système robuste de diagnostic décentralisé à l'aide d'automates cellulaires simples*, Université de Lorraine (Nancy), September 2018, https://hal.inria.fr/hal-01894581

[28] P. GUILLON, E. JEANDEL, J. KARI, P. VANIER. *Undecidable word problem in subshift automorphism groups*, September 2018, https://arxiv.org/abs/1808.09194 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01862896

[29] M. HOYRUP. *Results in descriptive set theory on some represented spaces*, January 2018, working paper or preprint, https://hal.inria.fr/hal-01657883

[30] E. JEANDEL. *The rational fragment of the ZX-calculus*, October 2018, https://arxiv.org/abs/1810.05377 - working paper or preprint, https://hal.inria.fr/hal-01893598

[31] E. JEANDEL, S. PERDRIX, R. VILMART. *A Generic Normal Form for ZX-Diagrams and Application to the Rational Angle Completeness*, May 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01791791

[32] R. VILMART. *A Near-Optimal Axiomatisation of ZX-Calculus for Pure Qubit Quantum Mechanics*, December 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01963426

[33] R. VILMART. *A ZX-Calculus with Triangles for Toffoli-Hadamard, Clifford+T, and Beyond*, April 2018, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01762264

References in notes

[34] A. ASPECT, P. GRANGIER, G. ROGER. *Experimental tests of realistic local theories via Bell's theorem*, in "Phys. Rev. Lett.", 1981, vol. 47, 460 p.

[35] C. H. BENNETT, G. BRASSARD. *Quantum cryptography: Public key distribution and coin tossing*, in "Proceedings of IEEE international Conference on Computers, Systems and Signal Processing, Bangalore, India", New York, IEEE Press, 1984, 175 p.

[36] B. COECKE, R. DUNCAN. *Interacting quantum observables: categorical algebra and diagrammatics*, in "New Journal of Physics", apr 2011, vol. 13, n⁰ 4, 043016 p.

[37] B. COECKE, A. KISSINGER. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*, Cambridge University Press, 2017, http://dx.doi.org/10.1017/9781316219317

[38] F. DUPUIS, O. FAWZI, R. RENNER. *Entropy accumulation*, 2016, Submitted to Communications in Mathematical Physics

[39] N. FATÈS. *Solving the decentralised gathering problem with a reaction-diffusion-chemotaxis scheme - Social amoebae as a source of inspiration*, in "Swarm Intelligence", 2010, vol. 4, n⁰ 2, pp. 91–115, http://dx.doi.org/10.1007/s11721-010-0038-4

[40] K. WEIHRAUCH. *Computable Analysis*, Springer, 2000