IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2015

Project-Team CARTE

Theoretical adverse computations, and safety

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

RESEARCH CENTER
Nancy - Grand Est

THEME
Security and Confidentiality

Table of contents

Project-Team CARTE

Creation of the Project-Team: 2009 January 01, updated into Team: 2016 January 01

Keywords:

Computer Science and Digital Science:

1.1.11. - Quantum architectures
2.4.1. - Analysis
4.1.1. - Malware analysis
4.5. - Formal methods for security
7.13. - Quantum algorithms
7.4. - Logic in Computer Science
7.8. - Information theory
7.9. - Graph theory

Other Research Topics and Application Domains:

9.4.1. - Computer science
9.4.2. - Mathematics

1. Members

Research Scientists

Isabelle Gnaedig [Inria, Researcher]
Mathieu Hoyrup [Inria, Researcher]
Simon Perdrix [CNRS, Researcher]

Faculty Members

Emmanuel Jeandel [Team leader, Univ. Lorraine, Professor, HdR]
Guillaume Bonfante [Univ. Lorraine, Associate Professor, HdR]
Martin Delacourt [Univ. Lorraine, ATER, from Sep 2015]
Emmanuel Hainry [Univ. Lorraine, Associate Professor]
Jean-Yves Marion [Univ. Lorraine, Professor, HdR]
Romain Péchoux [Univ. Lorraine, Associate Professor]

Engineers

Philippe Antoine [Univ. Lorraine, from Sep 2015]
Fabrice Sabatier [Inria, granted by Univ. Lorraine in Nov 2015 and CNRS, since Dec 2015]
Nicolas Scherrmann [Univ. Lorraine]

PhD Students

Hugo Férée [Univ. Lorraine, until Aug 2015]
Hubert Godfroy [Inria]

Post-Doctoral Fellow

Quanlong Wang [Univ. Lorraine, Advanced Research position, from Apr 2015]

Visiting Scientists

Walid Gomaa [Alexandria E-Just University, apr 2015 and Nov 2015]
Daniel Leivant [Indiana University in Bloomington, Professor, from Jun 2015 to Jul 2015]

Administrative Assistants

Emmanuelle Deschamps [Inria]
Delphine Hubert [Univ. Lorraine]

Martine Kuhlmann [CNRS]

Others

Nidhal Hamrit [Inria, M2 Telecom ParisTech, until Feb 2015]
Benjamin Rouxel [Univ. Lorraine, M2 Univ. Rennes I, from Feb 2015 to June 2015]
Diego Nava Saucedo [Univ. Lorraine, M2 Ens Lyon, from Feb 2015 to Jun 2015]

2. Overall Objectives

2.1. Overall Objectives

The aim of the CARTE research team is to take into account adversity in computations, which is implied by actors whose behaviors are unknown or unclear. We call this notion adversary computation.

The project combines two approaches. The first one is the analysis of the behavior of systems, using tools coming from Continuous Computation Theory. The second approach is to build defenses with tools coming from logic, rewriting and, more generally, from Programming Theory.

The activities of the CARTE team are organized around two research actions:

- Computation over Continuous Structures
- Computer Virology.

3. Research Program

3.1. Computer Virology

From a historical point of view, the first official virus appeared in 1983 on Vax-PDP 11. At the same time, a series of papers was published which always remains a reference in computer virology: Thompson [76], Cohen [46] and Adleman [35]. The literature which explains and discusses practical issues is quite extensive [51], [53]. However, there are only a few theoretical/scientific studies, which attempt to give a model of computer viruses.

A virus is essentially a self-replicating program inside an adversary environment. Self-replication has a solid background based on works on fixed point in λ-calculus and on studies of von Neumann [80]. More precisely we establish in [42] that Kleene's second recursion theorem [65] is the cornerstone from which viruses and infection scenarios can be defined and classified. The bottom line of a virus behavior is

1. a virus infects programs by modifying them,
2. a virus copies itself and can mutate,
3. it spreads throughout a system.

The above scientific foundation justifies our position to use the word virus as a generic word for self-replicating malwares. There is yet a difference. A malware has a payload, and virus may not have one. For example, a worm is an autonomous self-replicating malware and so falls into our definition. In fact, the current malware taxonomy (virus, worms, trojans, ...) is unclear and subject to debate.

3.2. Computation over continuous structures

Classical recursion theory deals with computability over discrete structures (natural numbers, finite symbolic words). There is a growing community of researchers working on the extension of this theory to continuous structures arising in mathematics. One goal is to give foundations of numerical analysis, by studying the limitations of machines in terms of computability or complexity, when computing with real numbers. Classical questions are : if a function $f : \mathbb{R} \to \mathbb{R}$ is computable in some sense, are its roots computable? in which time? Another goal is to investigate the possibility of designing new computation paradigms, transcending the usual discrete-time, discrete-space computer model initiated by the Turing machine that is at the base of modern computers.

While the notion of a computable function over discrete data is captured by the model of Turing machines, the situation is more delicate when the data are continuous, and several non-equivalent models exist. In this case, let us mention computable analysis, which relates computability to topology [50], [79]; the Blum-Shub-Smale model (BSS), where the real numbers are treated as elementary entities [41]; the General Purpose Analog Computer (GPAC) introduced by Shannon [74]with continuous time.

3.3. Rewriting

The rewriting paradigm is now widely used for specifying, modelizing, programming and proving. It allows one to easily express deduction systems in a declarative way, and to express complex relations on infinite sets of states in a finite way, provided they are countable. Programming languages and environments with a rewriting based semantics have been developed ; see ASF+SDF [43], MAUDE [45], and TOM [71].

For basic rewriting, many techniques have been developed to prove properties of rewrite systems like confluence, completeness, consistency or various notions of termination. Proof methods have also been proposed for extensions of rewriting such as equational extensions, consisting of rewriting modulo a set of axioms, conditional extensions where rules are applied under certain conditions only, typed extensions, where rules are applied only if there is a type correspondence between the rule and the term to be rewritten, and constrained extensions, where rules are enriched by formulas to be satisfied [37], [49], [75].

An interesting aspect of the rewriting paradigm is that it allows automatable or semi-automatable correctness proofs for systems or programs: the properties of rewriting systems as those cited above are translatable to the deduction systems or programs they formalize and the proof techniques may directly apply to them.

Another interesting aspect is that it allows characteristics or properties of the modeled systems to be expressed as equational theorems, often automatically provable using the rewriting mechanism itself or induction techniques based on completion [48]. Note that the rewriting and the completion mechanisms also enable transformation and simplification of formal systems or programs.

Applications of rewriting-based proofs to computer security are various. Approaches using rule-based specifications have recently been proposed for detection of computer viruses [77], [78]. For several years, in our team, we have also been working in this direction. We already proposed an approach using rewriting techniques to abstract program behaviors for detecting suspicious or malicious programs [38], [39].

4. Application Domains

4.1. Computer Virology

4.1.1. The theoretical track

It is rightful to wonder why there are only a few fundamental studies on computer viruses while it is one of the important flaws in software engineering. The lack of theoretical studies explains maybe the weakness in the anticipation of computer diseases and the difficulty to improve defenses. For these reasons, we do think that it is worth exploring fundamental aspects, and in particular self-reproducing behaviors.

4.1.2. The virus detection track

The crucial question is how to detect viruses or self-replicating malwares. Cohen demonstrated that this question is undecidable. The anti-virus heuristics are based on two methods. The first one consists in searching for virus signatures. A signature is a regular expression, which identifies a family of viruses. There are obvious defects. For example, an unknown virus will not be detected, like ones related to a 0-day exploit. We strongly suggest to have a look at the independent audit [52] in order to understand the limits of this method. The second one consists in analyzing the behavior of a program by monitoring it. Following [54], this kind of methods is not yet really implemented. Moreover, the large number of false-positive implies this is barely usable. To end this short survey, intrusion detection encompasses virus detection. However, unlike computer virology, which has a solid scientific foundation as we have seen, the IDS notion of “malwares” with respect to some security policy is not well defined. The interested reader may consult [72].

4.1.3. The virus protection track

The aim is to define security policies in order to prevent malware propagation. For this, we need (i) to define what is a computer in different programming languages and setting, (ii) to take into consideration resources like time and space. We think that formal methods like rewriting, type theory, logic, or formal languages, should help to define the notion of a formal immune system, which defines a certified protection.

4.1.4. The experimentation track

This study on computer virology leads us to propose and construct a "high security lab" in which experiments can be done in respect with the French law.

4.2. Computations and Dynamical Systems

4.2.1. Continuous computation theories

Understanding computation theories for continuous systems leads to studying hardness of verification and control of these systems. This has been used to discuss problems in fields as diverse as verification (see e.g., [36]), control theory (see e.g., [44]), neural networks (see e.g., [73]), and so on. We are interested in the formal decidability of properties of dynamical systems, such as reachability [64], the Skolem-Pisot problem [40], the computability of the ω-limit set [63]. Those problems are analogous to verification of safety properties.

Contrary to computability theory, complexity theory over continuous spaces is underdeveloped and not well understood. A central issue is the choice of the representation of objects by discrete data and its effects on the induced complexity notions. As for computability, it is well known that a representation is gauged by the topology it induces. However more structure is needed to capture the complexity notions: topologically equivalent representations may induce different classes of polynomial-time computable objects, e.g., developing a sound complexity theory over continuous structures would enable us to make abstract computability results more applicable by analyzing the corresponding complexity issues. We think that the preliminary step towards such a theory is the development of higher-order complexity, which we are currently carrying out.

In contrast with the discrete setting, it is of utmost importance to compare the various models of computation over the reals, as well as their associated complexity theories. In particular, we focus on the General Purpose Analog Computer of Claude Shannon [74], on recursive analysis [79], on the algebraic approach [70] and on Markov computability [66]. A crucial point for future investigations is to fill the gap between continuous and discrete computational models. This is one deep motivation of our work on computation theories for continuous systems.

4.2.2. Analysis and verification of adversary systems

The other research direction on dynamical systems we are interested in is the study of properties of adversary systems or programs, i.e., of systems whose behavior is unknown or indistinct, or which do not have classical expected properties. We would like to offer proof and verification tools, to guarantee the correctness of such systems. On one hand, we are interested in continuous and hybrid systems. In a mathematical sense, a hybrid system can be seen as a dynamical system, whose transition function does not satisfy the classical regularity hypotheses, like continuity, or continuity of its derivative. The properties to be verified are often expressed as reachability properties. For example, a safety property is often equivalent to (non-)reachability of a subset of unsure states from an initial configuration, or to stability (with its numerous variants like asymptotic stability, local stability, mortality, etc ...). Thus we will essentially focus on verification of these properties in various classes of dynamical systems.

We are also interested in rewriting techniques, used to describe dynamic systems, in particular in the adversary context. As they were initially developed in the context of automated deduction, the rewriting proof techniques, although now numerous, are not yet adapted to the complex framework of modelization and programming. An important stake in the domain is then to enrich them to provide realistic validation tools, both in providing finer rewriting formalisms and their associated proof techniques, and in developing new validation concepts

in the adversary case, i.e., when usual properties of the systems like, for example, termination are not verified. For several years, we have been developing specific procedures for property proofs of rewriting, for the sake of programming, in particular with an inductive technique, already applied with success to termination under strategies [55], [56], [57], to weak termination [58], sufficient completeness [59] and probabilistic termination [61]. The last three results take place in the context of adversary computations, since they allow for proving that even a divergent program, in the sense where it does not terminate, can give the expected results. A common mechanism has been extracted from the above works, providing a generic inductive proof framework for properties of reduction relations, which can be parametrized by the property to be proved [60], [62]. Provided program code can be translated into rule-based specifications, this approach can be applied to correctness proof of software in a larger context. A crucial element of safety and security of software systems is the problem of resources. We are working in the field of Implicit Computational Complexity. Interpretation based methods like Quasi-interpretations (QI) or sup-interpretations, are the approach we have been developing these last years [67], [68], [69]. Implicit complexity is an approach to the analysis of the resources that are used by a program. Its tools come essentially from proof theory. The aim is to compile a program while certifying its complexity.

5. Highlights of the Year

5.1. Highlights of the Year

The paper [21] published at the International Conference on Functional Programming (ICFP 2015) has given a positive answer to an open problem, conjectured to be true for a long time: the question is to know whether inductive and coinductive data types can be added to light logic based systems without breaking the complexity of the system (i.e. staying within the class of polynomial time computable functions). This issue is analog to the issue of adding inductive and coinductive data types to system F without breaking normalization, which is known to hold for a long time. To tackle this challenging question, we have studied the problem of defining algebras and coalgebras in the Light Affine Lambda Calculus, a system characterizing the complexity class FPTIME. In this system, the principle of stratification limits the ways we can use parametric polymorphism, and in general the way we can write our programs. We have shown that while stratification poses some issues to the standard System F encodings, it still permits to encode some weak form of algebra and coalgebra. Using the algebra encoding one can define in the Light Affine Lambda Calculus the traditional inductive types. Unfortunately, the corresponding coalgebra encoding permits only a very limited form of coinductive data types. To extend this class, we have studied an extension of the Light Affine Lambda Calculus by distributive laws for the modality §.

5.1.1. Awards

Hugo Férée has received the Ackermann award for his PhD thesis “complexité d’ordre supérieur et analyse récursive”.

6. New Software and Platforms

6.1. CoDisasm

FUNCTIONAL DESCRIPTION

Codisasm is a new disassembly program which supports self-modifying code and code overlapping. Up to our knowledge, it is the first which copes both aspects of program obfuscation. The tool is based on the notion of “wave” developed in the group.
It is written in C and contains about 3k lines of code.

- Contact: Fabrice Sabatier
- URL: http://www.lhs.loria.fr/wp/?p=289

6.2. DynamicTracer

FUNCTIONAL DESCRIPTION

DynamicTracer is a new tool with a public web interface which provides run traces of executable files. The trace is obtained by recording a dynamic execution in a safe environment. It contains instruction addresses, instruction opcodes and other optional information.
It is written in C++ and contains about 2.5k lines of code.

- Contact: Fabrice Sabatier
- URL: http://www.lhs.loria.fr

6.3. Gorille

FUNCTIONAL DESCRIPTION

Gorille (formerly MMDEX) is a virus detector based on morphological analysis. It is composed of our own disassembler tool, of a graph transformer and a specific tree-automaton implementation. The tool is used in the EU-Fiware project and by some other partners (e.g., DAVFI project).
It is written in C and contains about 100k lines of code.
APP License, IDDN.FR.001.300033.000.R.P.2009.000.10000, 2009.

- Contact: Philippe Antoine
- URL: http://www.lhs.loria.fr

7. New Results

7.1. Computability and Complexity

- **Complexity of stream functions and higher-order complexity.** We have pursued our works on higher-order complexity and the complexity of stream functions. Both notions are closely related as any function from natural numbers to natural numbers can be seen as a stream (an infinite list) of natural numbers:
  - A characterization of the class of Basic Feasible Functionals using term rewrite systems on streams and interpretation methods has been proposed in [13]. This result is part of Hugo Férée's PhD thesis for which he has obtained the Ackermann award.
  - In [14], we have provided some interpretation criteria useful to ensure two kinds of stream properties: space upper bounds and input/output upper bounds. Our space upper bounds criterion ensures global and local upper bounds on the size of each output stream element expressed in term of the maximal size of the input stream elements. The input/output upper bounds criterion considers instead the relations between the number of elements read from the input stream and the number of elements produced on the output stream.
  - The paper [21] has extended the light affine lambda calculus with inductive and coinductive data types using the category theory notions of (weak) initial algebra and coalgebra.
- **Complexity analysis of Object-Oriented programs.** We have proposed a type system based on non-interference and data ramification (tiering) principles in [22]. We have captured the set of functions computable in polynomial time on OO programs. The studied language is general enough to capture most OO constructs and the characterization is quite expressive as it allows the analysis of a combination of imperative loops and of data ramification scheme based on Bellantoni and Cook's safe recursion using function algebra.

- **Rice-like theorem for primitive recursive functions.** We have studied the following question: what are the properties of primitive recursive functions that are decidable (by a Turing machine), given a primitive recursive presentation of the function. We give a complete characterization of these properties. We show that they can be expressed as unions of elementary properties of being compressible. If $h : \mathbb{N} \to \mathbb{N}$ is a computable increasing unbounded function (like $\log(n)$ or 2^n), we say that a function $f : \mathbb{N} \to \mathbb{N}$ is h-compressible if for each n there is a primitive recursive program of size at most $h(n)$ computing a function that coincides with f on entries $0, 1, ..., n$. Whether f is h-compressible is decidable given a primitive recursive program for f, and every decidable property can be obtained as a combination of such elementary properties. This result actually holds for any class of total functions that admits a sound and complete programming language. An article is currently in preparation.
- **Parametrization of geometric figures.** During the master internship of Diego Nava Saucedo, we have studied the semi-computability of geometric figures. A figure is semi-computable if there is a program that semi-decides whether a pixel intersects the figure. Our goal is to understand the semi-computability of a figure in terms of the parameters describing the figure. It turns out that the usual ways of parameterizing simple figures such as triangles, squares or disks do not behave well in terms of semi-computability. We have actually proved that no *finite* parametrization behaves well.
- **Symbolic Dynamics on Groups.** In an effort to better understand the interplay of geometry and computability in tiling theory, E. Jeandel has studied tiling problems on general Cayley graphs, and has obtained a significant number of new results. He has proven that groups with an (strongly) aperiodic tiling system have decidable word problem [30], and provided examples of new groups (in particular monster groups) with such tiling systems, and proved that all nontrivial nilpotent groups have an aperiodic tiling system and an undecidable domino problem [31]. He also showed how the new concept of translation-like actions from geometric group theory can be used to prove that many groups, in particular the Grigorchuk groups and most groups with a nontrivial center, have an undecidable domino problem [33].
- **The smallest aperiodic tileset.** In a joint work with Michael Rao, E. Jeandel has proven that there exists an aperiocic set of 11 Wang tiles [34], and furthermore that this number is optimal.

7.2. Quantum Computing

- **On Weak Odd Domination and Graph-based Quantum Secret Sharing.** In this work published in the journal Theoretical Computer Science [15], Simon Perdrix and his co-authors Sylvain Gravier, Jérôme Javelle and Mehdi Mhalla study weak odd domination in graphs and its application in quantum secret sharing. A weak odd dominated (WOD) set in a graph is a subset B of vertices for which there exists a distinct set of vertices C such that every vertex in B has an odd number of neighbors in C. They point out the connections of weak odd domination with odd domination, [σ,ρ]-domination, and perfect codes. They introduce bounds on κ(G), the maximum size of WOD sets of a graph G, and on κ'(G), the minimum size of non-WOD sets of G. Moreover, they prove that the corresponding decision problems are NP-complete. The study of weak odd domination is mainly motivated by the design of graph-based quantum secret sharing protocols: a graph G of order n corresponds to a secret sharing protocol whose threshold is κQ(G)=max(κ(G),n-κ'(G)). These graph-based protocols are very promising in terms of physical implementation, however all such graph-based protocols studied in the literature have quasi-unanimity thresholds (i.e. κQ(G)=n-o(n) where n is the order of the graph G underlying the protocol). In this paper, they show using probabilistic methods the existence of graphs with smaller κQ (i.e. κQ(G)$\leq$0.811n where n is the order of G). They also prove that deciding for a given graph G whether κQ(G)$\leq$k is NP-complete, which means that one cannot efficiently double check that a graph randomly generated has actually a κQ smaller than 0.811n.
- **Minimum Degree up to Local Complementation: Bounds, Parameterized Complexity, and Exact Algorithms.** In this work presented at ISAAC [25], David Cattaneo and Simon Perdrix

introduce new upper bounds and exact algorithms for the local minimum degree. The author also prove the W[2]-membership of the corresponding decision problem. The local minimum degree of a graph is the minimum degree that can be reached by means of local complementation. For any n, there exist graphs of order n which have a local minimum degree at least $0.189n$, or at least $0.110n$ when restricted to bipartite graphs. Regarding the upper bound, they show that the local minimum degree is at most $3/8n + o(n)$ for general graphs and $n/4 + o(n)$ for bipartite graphs, improving the known $n/2$ upper bound. They also prove that the local minimum degree is smaller than half of the vertex cover number (up to a logarithmic term). The local minimum degree problem is NP-Complete and hard to approximate. They show that this problem, even when restricted to bipartite graphs, is in W[2] and FPT-equivalent to the EvenSet problem, whose W[1]-hardness is a long standing open question. Finally, they show that the local minimum degree is computed by a $O_*(1.938n)$-algorithm, and a $O_*(1.466n)$-algorithm for the bipartite graphs.

- **The ZX Calculus is incomplete for Clifford+T quantum mechanics.** The ZX calculus is a diagrammatic language for quantum mechanics and quantum information processing. In this paper[17], Simon Perdrix and Harny Wang prove that the ZX-calculus is not complete for the Clifford+T quantum mechanics. The completeness for this fragment has been stated as one of the main current open problems in categorical quantum mechanics. The ZX calculus was known to be incomplete for quantum mechanics, on the other hand, it has been proved complete for Clifford quantum mechanics (a.k.a. stabilizer quantum mechanics), and for single-qubit Clifford+T quantum mechanics. The question of the completeness of the ZX calculus for Clifford+T is a crucial step in the development of the ZX calculus because of its (approximate) universality for quantum mechanics (i.e. any unitary evolution can be approximated using Clifford and T gates only). They exhibit a property which is know to be true in Clifford+T quantum mechanics and prove that this equation cannot be derived in the ZX calculus, by introducing a new sound interpretation of the ZX calculus in which this particular property does not hold. Finally, we propose to extend the language with a new axiom. This result has been presented as invited speakers in the conferences "Quantum Theory: from foundations to technologies" in Vaxjo Sweden, and "Higher TQFT and categorical quantum mechanics" at the Scrounger Institute in Vienna. The authors also presented these results at the workshop of the CNRS groupe de travail Informatique Quantique du GDR IM, in Grenoble.
- **Block Representation of Reversible Causal Graph Dynamics.** In this work presented at the conference on Foundation of computer science (FCT'15) [18], Pablo Arrighi, Simon Martiel and Simon Perdrix, consider a reversible version of the causal graph dynamics. Causal Graph Dynamics extend Cellular Automata to arbitrary, bounded-degree, time-varying graphs. The whole graph evolves in discrete time steps, and this global evolution is required to have a number of physics-like symmetries: shift-invariance (it acts everywhere the same) and causality (information has a bounded speed of propagation). We study a further physics-like symmetry, namely reversibility. More precisely, we show that Reversible Causal Graph Dynamics can be represented as finite-depth circuits of local reversible gates.
- **Reversibility in the Extended Measurement-based Quantum Computation.** In this work by Nidal Hamrit and Simon Perdrix has been presented at the conference on Reversible Computation in Grenoble [23]. When applied on some particular quantum entangled states, measurements are universal for quantum computing. In particular, despite the fondamental probabilistic evolution of quantum measurements, any unitary evolution can be simulated by a measurement-based quantum computer (MBQC). They consider the extended version of the MBQC where each measurement can occur not only in the X,Y-plane of the Bloch sphere but also in the X,Z- and Y,Z-planes. The existence of a gflow in the underlying graph of the computation is a necessary and sufficient condition for a certain kind of determinism. They extend the focused gflow (a gflow in a particular normal form) defined for the X,Y-plane to the extended case, and provide necessary and sufficient conditions for the existence of such normal forms.
- **Quantum Circuits for the Unitary Permutation Problem.** In this paper presented at

TAMC'15 [20] Stefano Facchni and Simon Perdrix consider the *Unitary Permutation* problem which consists, given n quantum gates $U_1, ..., U_n$ and a permutation σ of $\{1, ..., n\}$, in applying the quantum gates in the order specified by σ, i.e., in performing $U_{\sigma(n)} \circ ... \circ U_{\sigma(1)}$. This problem has been introduced and investigated in [47] where two models of computations are considered. The first is the (standard) model of query complexity: the complexity measure is the number of calls to any of the quantum gates U_i in a quantum circuit which solves the problem. The second model is roughly speaking a model for higher order quantum computation, where quantum gates can be treated as objects of second order. In both model the existing bounds are improved, in particular the upper and lower bounds for the standard quantum circuit model are established by pointing out connections with the *permutation as substring* problem introduced by Karp.

8. Partnerships and Cooperations

8.1. Regional Initiatives

Simon Perdrix is the principal investigator of the project "measurement-based quantum computing" funded by Région Lorraine and Université de Lorraine.

8.2. National Initiatives

8.2.1. ANR

- The team is a funding partner in ANR Elica (2014-2019), "Elargir les idées logistiques pour l'analyse de complexité". The Carte team is well-known for its expertise in implicit computational complexity.
- The team is a funding partner in ANR Binsec (2013-2017), whose aim is to fill part of the gap between formal methods over executable code, and binary-level security analyses currently used in the security industry. Two main applicative domains are targeted: vulnerability analysis and virus detection. Two other closely related applications will also be investigated: crash analysis and program deobfuscation.

8.3. International Initiatives

8.3.1. Inria Associate Teams not involved in an Inria International Labs

- Submission of an Inria associate team proposal ACRA (Applications of Complexity to Resource Analysis) in collaboration with Computer Science and Engineering department, State University New York, Buffalo. The french principal investigator is Romain Péchoux, the US principal investigator is Marco Gaboardi.

8.3.2. Participation In other International Programs

- An Hubert Curien Partnership (PHC) PHC Imhotep from the French Ministry of Foreign Affairs and with the support of the French Ministry of National Education and Ministry of Higher Education and Research holds between members of EPC Carte and Alexandria E-Just University.
- Foundations of Quantum Computation: Syntax and Semantics (FoQCoSS), Regional Program STIC-AmSud. This 2-year project has been accepted in late 2015. The Argentinian-Brazilian-French consortium consists of: Pablo ARRIGHI (Université Aix-Marseille, France), Alejandro DIAZ-CARO (Universidad Nacional de Quilmes, Argentina), Gilles DOWEK (Inria, France), Juliana KAIZER VIZZOTTO (Universidade Federal de Santa Maria, Brazil), Simon PERDRIX (CNRS/Carte, France) and Benoît VALIRON (CentraleSupélec – LRI, France). The ultimate goal of this project is to study the foundations of quantum programming languages and related formalisms. With this goal in mind, we will study topics such as parallelism, probabilistic systems, isomorphisms, etc. The interest goes beyond having a working programming language for quantum computing; we are interested, on one hand, in its individual characteristics and its consequences for classical systems, and, on the other hand, in its implications for the foundations of quantum physics.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Walid Gomaa, associate professor at Alexandria E-Just University, was invited during two months (April and November) in the team.
- Daniel Leivant, professor at Indiana University in Bloomington, was invited in June and July.
- Mizuhito Ogawa was invited in the group to discuss about models of self-modifying code based on pushdown automata. He came back in October for further collaboration.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committees

- Guillaume Bonfante and Jean-Yves Marion participated to the organisation of the partnership meeting between JAIST and LORIA in Nancy, October 2015
- Simon Perdrix has been member of the organizing committee of the Workshop of the Groupe de Travail informatique Quantique in Grenoble 26-27 November 2015.
- Simon Perdrix has been member of the organizing committee of the Workshop of the Groupe de Travail GeoCal-LAC-LTP in Nancy 12-14 October 2015.

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committees

- Guillaume Bonfante was co-chair of the 8th international symposium on foundation and practice of security 2015.
- Guillaume Bonfante was in the Program Committee of Protection and Reverse Engineering Workshop 2015.
- Guillaume Bonfante was in the Program Committee of the workshop on Logic and Computational Complexity (LCC) 2015.
- Emmanuel Jeandel was in the Program Committee of Computability in Europe (CiE) 2015.
- Jean-Yves Marion was in the Program Committee of the 8th international symposium on foundation and practice of security 2015.
- Jean-Yves Marion was in the Program Committee of Protection and Reverse Engineering Workshop 2015.
- Romain Péchoux was in the Program Committee of FOundational and Practical Aspects of Resource Analysis (FOPARA) 2015.
- Simon Perdrix was in the Program Committee of Asian Quantum Information Science Conference (AQIS) 2015.
- Simon Perdrix is in the Program Committee of Quantum Physics and Logic (QPL), forthcoming: QPL'16 in Glasgow in June 2016.

9.1.2.2. Reviewer

Mathieu Hoyrup reviewed articles for:

- MFCS 2015
- STACS 2015

Emmanuel Jeandel reviewed articles for:

- MFCS 2015
- STACS 2015

Romain Péchoux reviewed articles for:

- FOPARA 2015
- ISMVL 2015
- FOSSACS 2016

Simon Perdrix reviewed articles for:

- AQIS 2015
- ICALP 2015
- LICS 2015
- QPL 2016

9.1.3. Journal

9.1.3.1. Reviewer - Reviewing activities

Emmanuel Hainry reviewed articles for:

- *Theoretical Computer Science*
- *Applicable Analysis and Discrete Mathematics*

Mathieu Hoyrup reviewed articles for:

- *Journal of Symbolic Logic*
- *Information and Computation*
- *Mathematical Structures in Computer Sciences*
- *Logical Methods in Computer Science*
- *Theory of Computing Systems*

Emmanuel Jeandel reviewed articles for:

- *Discrete Mathematics and Theoretical Computer Science*
- *Ergodic Theory and Dynamical Systems*

Romain Péchoux reviewed articles for:

- *Computability - Journal of the association Computability In Europe*
- *Information and Computation*

Simon Perdrix reviewed articles for:

- *Quantum Information and Computation*

9.1.4. Invited talks

- Guillaume Bonfante was invited to give a talk on implicit complexity within NC at the Shonan Meeting on Low Level Code Analysis and Application to Computer Security.
- Mathieu Hoyrup was invited to give a talk at the annual workshop Continuity, Computability, Constructivity (CCC 2015) in Kochel am See, Germany, September 2015.
- Simon Perdrix was invited to give a talk:
  - "The ZX Calculus is incomplete for Clifford+T quantum mechanics", at "Quantum Theory: from foundations to technologies – QTFT", Vaxjo, Sweden, June 2015,
  - "Supplementary of Interacting Frobenius Algebras" at the Workshop on "Higher topological quantum field theory and categorical quantum mechanics" Erwin Schrödinger International Institute, Vienna, October 2015
  - "Informatique quantique et théorie des graphes" at Journées Graphes et Algorithmes 2015, Orléans, Novembre 2015.

9.1.5. Scientific expertise

Romain Péchoux is external expert for the European commission Horizon 2020 program.

9.1.6. Research administration

Isabelle Gnaedig is:

- vice-leader of the team Carte.

Emmanuel Hainry is:

- member of the CNU (Conseil National des Universités), Section 27.
- organizer of the Carte Seminar.

Mathieu Hoyrup is:

- principal investigator of a PHC Imhotep with Walid Gomaa (Alexandria E-Just University).
- organizer of the Formal Methods Seminar at Loria.

Romain Péchoux is:

- responsible of the Project-team Carte activity report 2015.
- principal investigator of the Inria associate team Acra proposal.

Simon Perdrix is:

- responsible of GT IQ (groupe de travail Informatique quantique) at the CNRS GdR IM (groupe de recherche Informatique Mathématique).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Unless explicitly stated, the teachings below are given at Université de Lorraine.

Licence:

- Guillaume Bonfante
  - Java, L3, Mines Nancy
- 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, 12h, L2, IUT Nancy Brabois
  - Complexity, 30h, L2, IUT Nancy Brabois
- Mathieu Hoyrup
  - Programmation C, 15h, L1 PACES
  - Programmation JAVA, 56h, L1, IUT Charlemagne
- Emmanuel Jeandel
  - Algorithmics and Programming 1, 60h, L1 Maths-Info
  - Algorithmics and Programming 4, 30h, L3 Informatique
  - Modelling Using Graph Theory, 30h, L3 Informatique
  - Networking, 15h, L3 Informatique
  - Data Compression, 45h, L2 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 Casablanca, Morocco.
- Simon Perdrix
  - Structure de données, 72h, L1, IUT Charlemagne
  - Licence : Modelling Using Graph Theory, 15h, L3 Informatique

Master:

- Guillaume Bonfante
  - Modelling and UML, M1, Mines Nancy
  - Video Games, M1, Mines Nancy
  - Semantics, M1, Mines Nancy
  - Safety of Software, M2, Mines Nancy
- Isabelle Gnaedig
  - Design of Safe Software, Coordination of the module, M2, Telecom-Nancy
  - Rule-based Programming, 20h, M2, Telecom-Nancy
- Emmanuel Hainry
  - Implicit Complexity, 15h, M2 Informatique
- Emmanuel Jeandel
  - Algorithmics and Complexity, 30h, M1 Informatique
  - Combinatorial Optimization, 36h, M1 Informatique
- Romain Péchoux
  - Mathematics for computer science, 30h, M1 SCA
  - Advanced Java, 52,5h, M1 MIAGE
  - Implicit Complexity, 15h, M2 Informatique

9.2.2. Supervision

PhD in progress: Hubert Godfroy, Semantics of Self-modifying Programs, Jean-Yves Marion (director).

PhD in progress: David Cattanéo, Combinatorial Modelization in Quantum Computation and Generalized Cover Problems, Pablo Arrighi (director), Simon Perdrix (co-advisor).

PhD: Thanh Dinh Ta, 11 May 2015, Malware Algebraic Modeling and Detection, started Sept. 2010, Jean-Yves Marion (director) and Guillaume Bonfante (co-advisor).

PhD: Aurélien Thierry, 11 March 2015, Morphological Analysis of Malware, Jean-Yves Marion (director).

PhD in progress: Paul Bakouche, Mesure de complexité en topologie de petites dimensions, Florian Deloup (co-advisor) and Guillaume Bonfante (director).

9.2.3. Juries

Isabelle Gnaedig was:

- member of the Inria hiring committee for young researchers,
- member of the Telecom-Nancy engineering school admission committee.

Emmanuel Jeandel was:

- Reviewer and Examiner of Simon Martiel's PhD Defense on "Approches informatique et mathématique des dynamiques causales de graphes", defended in Université de Nice Sophia Antipolis, July 6th 2015
- Reviewer of Ilkka Törmä's PhD on "Structural and Computational Existence Results for Multidimensional Subshifts", defended in Turku (Finland), July 31st 2015
- Reviewer of Rodrigo Torres' PhD on "Some Dynamical Properties of Turing Machines Dynamical Models", to be defended in January 2016, Santiago de Chile (Chile)

9.3. Popularization

- Isabelle Gnaedig is member of the scientific vulgarization committee of Inria Nancy - Grand Est. This committee is a choice and guidance instance helping the direction of the center and the person in charge of popularization events to elaborate a strategy, to realize events and to help researchers to get involved in various actions aiming at popularizing our research themes, and more generally computer science and mathematics.
- Mathieu Hoyrup wrote an article on his recent work for Images des Mathématiques.

10. Bibliography

Major publications by the team in recent years

[1] G. BONFANTE, J.-Y. MARION, J.-Y. MOYEN. *Quasi-interpretations a way to control resources*, in "Theoretical Computer Science", May 2011, vol. 412, n^{o} 25, pp. 2776-2796 [*DOI :* 10.1016/J.TCS.2011.02.007], http://hal.inria.fr/hal-00591862/en

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

[3] J. CALVET, J. FERNANDEZ, J.-Y. MARION. *The case for in-the-lab botnet experimentation: creating and taking down a 3000-node botnet*, in "Annual Computer Security Applications Conference", Austin, Texas États-Unis, 12 2010, pp. 141-150, http://hal.inria.fr/inria-00536706/en/

[4] 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

[5] H. FÉRÉE, W. GOMAA, M. HOYRUP. *Analytical properties of resource-bounded real functionals*, in "J. Complexity", 2014, vol. 30, n^{o} 5, pp. 647–671, http://dx.doi.org/10.1016/j.jco.2014.02.008

[6] 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

[7] E. HAINRY, J.-Y. MARION, R. PÉCHOUX. *Type-based complexity analysis for fork processes*, in "16th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS)", Rome, Italy, F. PFENNING (editor), Lecture Notes in Computer Science, Springer, 2013, vol. 7794, pp. 305-320 [*DOI :* 10.1007/978-3-642-37075-5_20], http://hal.inria.fr/hal-00755450

[8] M. HOYRUP. *Irreversible computable functions*, in "STACS - 31st Symposium on Theoretical Aspects of Computer Science - 2014", Lyon, France, March 2014, pp. 362-373, https://hal.inria.fr/hal-00915952

[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] J.-Y. MARION. *A type system for complexity flow analysis*, in "Twenty-Sixth Annual IEEE Symposium on Logic in Computer Science - LICS 2011", Toronto, Canada, ACM, June 2011, pp. 1–10, http://hal.inria.fr/hal-00591853/en

Publications of the year

Articles in International Peer-Reviewed Journals

[11] G. BONFANTE, F. DELOUP, A. HENROT. *Real or Natural numbers interpretations and their effect on complexity*, in "Theoretical Computer Science", 2015, 23 p. , https://hal.archives-ouvertes.fr/hal-01093579

[12] G. BONFANTE, R. KAHLE, J.-Y. MARION, I. OITAVEM. *Two function algebras defining functions in NC k boolean circuits*, in "Journal of Information and Computation", 2016, accepté à Information and Computation, https://hal.inria.fr/hal-01113342

[13] 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

[14] M. GABOARDI, R. PÉCHOUX. *On Bounding Space Usage of Streams Using Interpretation Analysis*, in "Science of Computer Programming", January 2015, 44 p. , Accepted. To be published, https://hal.inria.fr/hal-01112161

[15] S. GRAVIER, J. JAVELLE, M. MHALLA, S. PERDRIX. *On weak odd domination and graph-based quantum secret sharing*, in "Journal of Theoretical Computer Science (TCS)", September 2015, vol. 598 [*DOI :* 10.1016/J.TCS.2015.05.038], https://hal.inria.fr/hal-01249271

[16] E. JEANDEL, P. VANIER. *Hardness of conjugacy, embedding and factorization ofmultidimensional subshifts*, in "Journal of Computer and System Sciences", May 2015, vol. 81, n^{o} 8, pp. 1648–1664 [*DOI :* 10.1016/J.JCSS.2015.05.003], https://hal.archives-ouvertes.fr/hal-01150419

Invited Conferences

[17] S. PERDRIX, Q. WANG. *The ZX Calculus is incomplete for Clifford+T quantum mechanics*, in "Quantum Theory: from foundations to technologies – QTFT", Vaxjo, Sweden, June 2015, https://hal.inria.fr/hal-01249274

International Conferences with Proceedings

[18] P. ARRIGHI, S. MARTIEL, S. PERDRIX. *Block Representation of Reversible Causal Graph Dynamics*, in "20th International Symposium on Fundamentals of Computation Theory", Gdańsk, Poland, Fundamentals of

Computation Theory, August 2015, vol. 9210, 14 p. [*DOI :* 10.1007/978-3-319-22177-9_27], https://hal.inria.fr/hal-01249272

[19] G. BONFANTE, M. EL-AQQAD, B. GREENBAUM, M. HOYRUP. *Immune Systems in Computer Virology*, in "Computability in Europe 2015", Bucharest, Romania, Evolving Computability, Springer, June 2015, vol. 9136, 10 p. [*DOI :* 10.1007/978-3-319-20028-6_13], https://hal.inria.fr/hal-01208454

[20] S. FACCHINI, S. PERDRIX. *Quantum Circuits for the Unitary Permutation Problem*, in "TAMC 2015", Singapore, Singapore, Theory and Applications of Models of Computation, May 2015, vol. 9076, pp. 324-331 [*DOI :* 10.1007/978-3-319-17142-5_28], https://hal.inria.fr/hal-00994182

[21] M. GABOARDI, R. PÉCHOUX. *Algebras and Coalgebras in the Light Affine Lambda Calculus*, in "The 20th ACM SIGPLAN International Conference on Functional Programming (ICFP 2015)", Vancouver, Canada, ACM (editor), August 2015, https://hal.inria.fr/hal-01112165

[22] 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

[23] N. HAMRIT, S. PERDRIX. *Reversibility in Extended Measurement-based Quantum Computation*, in "7th Conference on Reversible Computation", Grenoble, France, Reversible Computation, July 2015, vol. 9138, 10 p. [*DOI :* 10.1007/978-3-319-20860-2_8], https://hal.archives-ouvertes.fr/hal-01132861

[24] M. HOYRUP, C. ROJAS. *On the information carried by programs about the objects they compute*, in "STACS15", Munich, Germany, March 2015, https://hal.inria.fr/hal-01067618

Conferences without Proceedings

[25] D. CATTANÉO, S. PERDRIX. *Minimum Degree up to Local Complementation: Bounds, Parameterized Complexity, and Exact Algorithms*, in "26th International Symposium on Algorithms and Computation (ISAAC 2015)", Nagoya, Japan, Algorithms and Computation (ISAAC'2015), December 2015, vol. 9472, 12 p. [*DOI :* 10.1007/978-3-662-48971-0_23], https://hal.archives-ouvertes.fr/hal-01132843

[26] E. HAINRY, R. PÉCHOUX. *Higher order interpretations for Basic Feasible Functions*, in "DICE 2015 - Developments in Implicit Computational Complexity", London, United Kingdom, April 2015, https://hal.inria.fr/hal-01207910

[27] E. HAINRY, R. PÉCHOUX. *Implicit computational complexity in Object Oriented Programs*, in "DICE 2015 - Developments in Implicit Computational Complexity", London, United Kingdom, April 2015, https://hal.inria.fr/hal-01207918

Research Reports

[28] M. HOYRUP. *A Rice-like theorem for primitive recursive functions*, Inria Nancy - Grand Est (Villers-lès-Nancy, France) ; Loria, March 2015, https://hal.inria.fr/hal-01130868

Scientific Popularization

[29] M. HOYRUP. *Que calcule cet algorithme ?*, September 2015, Article de vulgarisation présentant un travail de recherche récent, https://hal.inria.fr/hal-01202984

Other Publications

[30] E. JEANDEL. *Aperiodic Subshifts of Finite Type on Groups*, January 2015, New version. Adding results about monster groups, https://hal.inria.fr/hal-01110211

[31] E. JEANDEL. *Aperiodic Subshifts on Polycyclic Groups*, October 2015, working paper or preprint, https://hal.inria.fr/hal-01213364

[32] E. JEANDEL. *Enumeration in Closure Spaces with Applications to Algebra*, April 2015, working paper or preprint, https://hal.inria.fr/hal-01146744

[33] E. JEANDEL. *Translation-like Actions and Aperiodic Subshifts on Groups*, August 2015, working paper or preprint, https://hal.inria.fr/hal-01187069

[34] E. JEANDEL, M. RAO. *An aperiodic set of 11 Wang tiles*, June 2015, working paper or preprint, https://hal.inria.fr/hal-01166053

References in notes

[35] L. ADLEMAN. *An Abstract Theory of Computer Viruses*, in "Advances in Cryptology — CRYPTO'88", Lecture Notes in Computer Science, 1988, vol. 403

[36] E. ASARIN, O. MALER, A. PNUELI. *Reachability analysis of dynamical systems having piecewise-constant derivatives*, in "Theoretical Computer Science", February 1995, vol. 138, n^{o} 1, pp. 35–65

[37] F. BAADER, T. NIPKOW. *Term rewriting and all that*, Cambridge University Press, New York, NY, USA, 1998

[38] P. BEAUCAMPS, I. GNAEDIG, J.-Y. MARION. *Behavior Abstraction in Malware Analysis*, in "1st International Conference on Runtime Verification", St. Julians, Malte, G. ROSU, O. SOKOLSKY (editors), Lecture Notes in Computer Science, Springer-Verlag, August 2010, vol. 6418, pp. 168-182, http://hal.inria.fr/inria-00536500/en/

[39] P. BEAUCAMPS, I. GNAEDIG, J.-Y. MARION. *Abstraction-based Malware Analysis Using Rewriting and Model Checking*, in "ESORICS", Pisa, Italie, S. FORESTI, M. YUNG (editors), LNCS, Springer, 2012, vol. 7459, pp. 806-823 [*DOI :* 10.1007/978-3-642-33167-1], http://hal.inria.fr/hal-00762252

[40] P. BELL, J.-C. DELVENNE, R. JUNGERS, V. D. BLONDEL. *The Continuous Skolem-Pisot Problem: On the Complexity of Reachability for Linear Ordinary Differential Equations*, 2008, http://arxiv.org/abs/0809.2189

[41] L. BLUM, M. SHUB, S. SMALE. *On a theory of computation and complexity over the real numbers; NP completeness, recursive functions and universal machines*, in "Bulletin of the American Mathematical Society", July 1989, vol. 21, n^{o} 1, pp. 1–46

[42] G. BONFANTE, M. KACZMAREK, J.-Y. MARION. *On abstract computer virology: from a recursion-theoretic perspective*, in "Journal in Computer Virology", 2006, vol. 1, n^{o} 3-4

[43] M.G.J. VAN DEN. BRAND, A. VAN. DEURSEN, J. HEERING, H.A. DE JONG, M. DE JONGE, T. KUIPERS, P. KLINT, L. MOONEN, P. OLIVIER, J. SCHEERDER, J. VINJU, E. VISSER, J. VISSER. *The ASF+SDF Meta-Environment: a Component-Based Language Development Environment*, in "Compiler Construction (CC '01)", R. WILHELM (editor), Lecture Notes in Computer Science, Springer, 2001, vol. 2027, pp. 365–370

[44] M. S. BRANICKY. *Universal computation and other capabilities of hybrid and continuous dynamical systems*, in "Theoretical Computer Science", 6 February 1995, vol. 138, n^{o} 1, pp. 67–100

[45] M. CLAVEL, F. DURÁN, S. EKER, P. LINCOLN, N. MARTÍ-OLIET, J. MESEGUER, C. TALCOTT. *The Maude 2.0 System*, in "Proceedings of the 14th International Conference on Rewriting Techniques and Applications", R. NIEUWENHUIS (editor), Lecture Notes in Computer Science, Springer, June 2003, vol. 2706, pp. 76-87

[46] F. COHEN. *Computer Viruses*, University of Southern California, January 1986

[47] T. COLNAGHI, G. M. D'ARIANO, S. FACCHINI, P. PERINOTTI. *Quantum computation with programmable connections between gates*, in "Physics Letters A", 2012, vol. 376, n^{o} 45, pp. 2940 - 2943, http://dx.doi.org/10.1016/j.physleta.2012.08.028

[48] H. COMON. *Inductionless Induction*, in "Handbook of Automated Reasoning", A. ROBINSON, A. VORONKOV (editors), Elsevier Science, 2001, vol. I, chap. 14, pp. 913-962

[49] N. DERSHOWITZ, D. PLAISTED. *Rewriting*, in "Handbook of Automated Reasoning", A. ROBINSON, A. VORONKOV (editors), Elsevier Science, 2001, vol. I, chap. 9, pp. 535-610

[50] A. EDALAT, P. SÜNDERHAUF. *A domain-theoretic approach to computability on the real line*, in "Theoretical Computer Science", 1999, vol. 210, n^{o} 1, pp. 73–98

[51] E. FILIOL. *Computer Viruses: from Theory to Applications*, Springer-Verlag, 2005

[52] E. FILIOL. *Malware Pattern Scanning Schemes Secure Against Black-box Analysis*, in "Journal in Computer Virology", 2006, vol. 2, n^{o} 1, pp. 35-50

[53] E. FILIOL. *Techniques virales avancées*, Springer, 2007

[54] E. FILIOL, G. JACOB, M. LE LIARD. *Evaluation methodology and theoretical model for antiviral behavioural detection strategies*, in "Journal in Computer Virology", 2007, vol. 3, n^{o} 1, pp. 23-37

[55] O. FISSORE, I. GNAEDIG, H. KIRCHNER. *Termination of rewriting with local strategies*, in "Selected papers of the 4th International Workshop on Strategies in Automated Deduction", M. P. BONACINA, B. GRAMLICH (editors), Electronic Notes in Theoretical Computer Science, Elsevier Science Publishers, 2001, vol. 58

[56] O. FISSORE, I. GNAEDIG, H. KIRCHNER. *CARIBOO : An induction based proof tool for termination with strategies*, in "Proceedings of the Fourth International Conference on Principles and Practice of Declarative Programming", Pittsburgh (USA), ACM Press, October 2002, pp. 62–73

[57] O. FISSORE, I. GNAEDIG, H. KIRCHNER. *Outermost ground termination*, in "Proceedings of the Fourth International Workshop on Rewriting Logic and Its Applications", Pisa, Italy, Electronic Notes in Theoretical Computer Science, Elsevier Science Publishers, September 2002, vol. 71

[58] O. FISSORE, I. GNAEDIG, H. KIRCHNER. *A proof of weak termination providing the right way to terminate*, in "First International Colloquium on Theoretical Aspect of Computing", Guiyang, China, Lecture Notes in Computer Science, Springer, September 2004, vol. 3407, pp. 356-371

[59] I. GNAEDIG, H. KIRCHNER. *Computing Constructor Forms with Non Terminating Rewrite Programs*, in "Proceedings of the Eighth ACM-SIGPLAN International Symposium on Principles and Practice of Declarative Programming", Venice, Italy, ACM Press, July 2006, pp. 121–132

[60] I. GNAEDIG, H. KIRCHNER. *Termination of Rewriting under Strategies*, in "ACM Transactions on Computational Logic", 2009, vol. 10, n^{o} 2, pp. 1-52, http://hal.inria.fr/inria-00182432/en/

[61] I. GNAEDIG. *Induction for Positive Almost Sure Termination*, in "Proceedings of the 9th ACM-SIGPLAN International Symposium on Principles and Practice of Declarative Programming - PPDP 2007", Wroclaw, Pologne, ACM, 2007, pp. 167-177, http://hal.inria.fr/inria-00182435/en/

[62] I. GNAEDIG, H. KIRCHNER. *Narrowing, Abstraction and Constraints for Proving Properties of Reduction Relations*, in "Rewriting, Computation and Proof - Essays Dedicated to Jean-Pierre Jouannaud on the Occasion of His 60th Birthday", Paris, France, H. COMON, C. KIRCHNER, H. KIRCHNER (editors), Lecture Notes in Computer Science, Springer, 2007, vol. 4600, pp. 44-67, http://hal.inria.fr/inria-00182434/en/

[63] E. HAINRY. *Computing omega-limit Sets in Linear Dynamical Systems*, in "Unconventional Computation", Autriche Vienne, C. S. CALUDE, J. F. COSTA, R. FREUND, M. OSWALD, G. ROZENBERG (editors), Springer, 2008, vol. 5204, pp. 83–95, http://hal.inria.fr/inria-00250111/en/

[64] E. HAINRY. *Reachability in linear dynamical systems*, in "Computability in Europe Logic and Theory of Algorithms", Grèce Athènes, A. BECKMANN, C. DIMITRACOPOULOS, B. LÖWE (editors), Springer, 2008, vol. 5028, pp. 241-250, http://hal.inria.fr/inria-00202674/en/

[65] S. KLEENE. *Introduction to Metamathematics*, Van Nostrand, 1952

[66] K.-I. KO. *Complexity Theory of Real Functions*, Birkhäuser, 1991

[67] J.-Y. MARION. *Complexité implicite des calculs, de la théorie à la pratique*, Université Nancy 2, 2000, Habilitation à diriger les recherches

[68] J.-Y. MARION, J.-Y. MOYEN. *Efficient first order functional program interpreter with time bound certifications*, in "Logic for Programming and Automated Reasoning, 7th International Conference, LPAR 2000, Reunion Island, France", M. PARIGOT, A. VORONKOV (editors), Lecture Notes in Computer Science, Springer, Nov 2000, vol. 1955, pp. 25–42

[69] J.-Y. MARION, R. PÉCHOUX. *Resource Analysis by Sup-interpretation*, in "FLOPS", Lecture Notes in Computer Science, Springer, 2006, vol. 3945, pp. 163–176

[70] C. MOORE. *Recursion Theory on the Reals and Continuous-Time Computation*, in "Theor. Comput. Sci.", 1996, vol. 162, n^{o} 1, pp. 23-44

[71] P.-E. MOREAU, C. RINGEISSEN, M. VITTEK. *A Pattern Matching Compiler for Multiple Target Languages*, in "12th Conference on Compiler Construction, Warsaw (Poland)", G. HEDIN (editor), LNCS, Springer-Verlag, May 2003, vol. 2622, pp. 61–76, http://www.loria.fr/~moreau/Papers/MoreauRV-CC2003.ps.gz

[72] B. MORIN, L. MÉ. *Intrusion detection and virology: an analysis of differences, similarities and complementariness*, in "Journal in Computer Virology", 2007, vol. 3, n^{o} 1, pp. 33-49

[73] P. ORPONEN. *A Survey of Continuous-Time Computation Theory*, in "Advances in Algorithms, Languages, and Complexity", D.-Z. DU, K.-I. KO (editors), Kluwer Academic Publishers, 1997, pp. 209-224, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.1991

[74] C. E. SHANNON. *Mathematical Theory of the Differential Analyser*, in "Journal of Mathematics and Physics MIT", 1941, vol. 20, pp. 337-354

[75] TERESE. *Term Rewriting Systems*, Cambridge Tracts in Theoretical Computer Science, Cambridge University Press, 2003, n^{o} 55

[76] K. THOMPSON. *Reflections on Trusting Trust*, in "Communication of the ACM", august 1984, vol. 27, pp. 761–763, Also appears in ACM Turing Award Lectures: The First Twenty Years 1965-1985

[77] M. WEBSTER, G. MALCOLM. *Detection of metamorphic computer viruses using algebraic specification*, in "Journal in Computer Virology", 2006, vol. 2, n^{o} 3, pp. 149-161

[78] M. WEBSTER, G. MALCOLM. *Detection of metamorphic and virtualization-based malware using algebraic specification*, in "Journal in Computer Virology", 2009, vol. 5, n^{o} 3, pp. 221-245

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

[80] J. VON NEUMANN. *Theory of Self-Reproducing Automata*, University of Illinois Press, Urbana, Illinois, 1966, edited and completed by A.W.Burks