Activity Report 2013

Section New Results

<div style="text-align:center; color:red">**CAMUS Team**</div>

6. New Results

6.1. VMAD and APOLLO

The goal of the APOLLO project is to provide a set of annotations (pragmas) that the user can insert in the source code to perform advanced analyses and optimizations, for example dynamic speculative parallelization. It is based on the prototype VMAD developed previously by the team between 2009 and 2012.

APOLLO includes a modified LLVM compiler and a runtime system. The program binary files are first generated by our compiler to include necessary data, instrumentation instructions, parallel code skeletons, and callbacks to the runtime system which is implemented as a dynamic library. External modules associated to specific analyses and transformations are dynamically loaded when required at runtime.

APOLLO uses sampling and multi-versioning to limit the runtime overhead (profiling, analysis, and code generation). At runtime, targeted codes are launched by successive chunks that can be either original, instrumented or optimized/parallelized versions. After each chunk execution, decisions can be taken relatively to the current optimization strategy. APOLLO is handling advanced memory access profiling [26], [17] through linear interpolation of the addresses, dynamic dependence analysis [18], version selection [26] and speculative polyhedral parallelization [22], [17].

Alexandra Jimborean defended her PhD thesis on this topic in 2012 [25].

In 2012, Aravind Sukumaran-Rajam started his PhD in our team to extend this work in order to handle more general programs which do not exhibit a pure polyhedral memory behavior. The investigated approach will explore approximative modelling of dependences still allowing advanced optimizing transformations of loop nests. A main issue concerns speculation verification when using approximative modelling.

Juan Manuel Martinez started his PhD in our team in 2013, with the goal of improving the flexibility of the parallel code generation phase inside Apollo. Indeed, although code skeletons are a good solution to fast dynamic parallel code generation, their shapes limit the kind of optimizing transformations that may be applied at runtime. Juan Manuel's work consists in defining elementary code skeletons that may be assembled at runtime to form a large panel of possible codes. These elementary skeletons will be defined as the objects forming the Apollo specific intermediate representation. Juan Manuel Martinez is a former master student of the University of Buenos Aires, Argentina (associate team EA-Ancome), and has already been working on VMAD to make the code generation support tiling. He defended his master thesis on this subject in October 2013 at the University of Buenos Aires.

Jean-Fran cois Dollinger will extend the framework to handle heterogeneous architectures (GPGPUs) in 2014. Willy Wolff, a master student from the University of Strasbourg, joined the APOLLO group in September 2013. His work is to implement just-in-time compilation in the APOLLO framework.

6.2. The Multifor programming construct

We have proposed a new programming control structure called "multifor", allowing to take advantage of optimization and parallelization opportunities that are not easily attainable using the standard programming structures.

In a multifor-loop, several loops whose bodies are run in interleaved fashion can be defined. Respective iteration domains are mapped onto each other according to a run frequency – the grain – and a relative position – the offset. Imen Fassi developed a source-to-source compiler called IBB (Iterate-But-Better) which is automatically translating any C source code containing multifor-loops into an equivalent source code where multifor-loops have been transformed into equivalent for-loops. Traditional polyhedral software tools, and particularly CLooG [21], are used to generate the corresponding code. Additionally, a promising perspective related to non-linear mapping of iteration spaces has also been developed, yielding to run a loop nest inside any other one by solving the problem of inverting "ranking Ehrhart polynomials".

This work is the PhD work of Imen Fassi, who started her work in 2013 and who is co-advised by Yosr Slama, Assistant Professor at the University El Manar in Tunis, Tunisia, and Philippe Clauss. A first paper [15] on this topic has been published at the IMPACT workshop that was held in conjunction with the HIPEAC conference in Berlin, Germany, in January 2013. Another paper describing the IBB compiler and showing the efficiency of multifor codes has been submitted to an international conference.

Obviously, reasoning on such a syntactic sugar suppose an associated precise and unambiguous meaning. Therefore a denotational semantics has been defined that resolves all such semantic issues and that is well-suited to prove code transformations. It has been presented to the French community of Compilation during the sixth meeting in Annecy [8].

6.3. CPU+GPU adaptive computation

In this work, we aim to automatically use CPU and GPU to jointly execute a parallel code. To ensure load balance between different PUs, thus to preserve performance, it is necessary to consider the underlying hardware and the program parameters. Compiler optimizations, execution context, hardware availability and specification make it difficult to determine execution times statically. To overcome this hurdle we rely on a portable and automatic method for predicting execution times of statically generated codes on multicore CPUs and on CUDA GPUs. This approach relies on three stages: automatic code generation, offline profiling and online prediction.

This is the latest result of PhD student Jean-François Dollinger, advised by Vincent Loechner since 2011. Preliminary results, a "fastest-wins" algorithm between a multicore CPU and the best predicted GPU code version, was published in 2013 in ICPP [14]. We are currently writing a conference paper presenting the latest advances, and preparing a journal paper to be submitted in 2014, before Jean-François Dollinger's PhD defense by the end of the year.

6.4. Minimizing the synchronization overhead of X10 programs

The CAMUS team has for long focused on compiling, optimizing, and parallelizing *sequential* programs. The project described in this section is somewhat unusual in this context, in that it targets programs written in an explicitly parallel language, and applies polyhedral modeling techniques to reschedule computations, effectively introducing parallel-to-parallel program transformations. This work has been done in collaboration with the Inria COMPSYS team at ENS Lyon, and first results will be presented at the *Compiler Construction* conference (CC'14) in April 2014.

The need to leverage the computing power of multi-core processors (and distributed computers) has lead to the design of explicitly parallel programming languages. Such languages often employ a fork/join model, and include syntax to launch and synchronize tasks (also called activities) with well-defined semantics. This brings parallel constructions under the control of the compiler, and introduces new optimization opportunities. Our work has focused on the various synchronization primitives available to the programmer, and more specifically on how one type of synchronization can be replaced with another for specific classes of programs, the goal being to minimize the synchronization overhead. We have demonstrated significant speedups on programs written using the X10 programming language, and have obtained similar results on equivalent Habanero-Java programs.

More specifically, our proposed optimization works by eliminating the use of clocks in X10 programs whose activities can be characterized with a polyhedral time-domain. The X10 language basically has two activity synchronization primitives: one is the explicit use of "clocks" (synchronization barriers) during activity execution, the other is the implicit use of activity containers that synchronize only on the end of activities. Under reasonable conditions on the patterns of activity creation and control, we have shown that long-running activities using clocks can be replaced by short-lived activities synchronized only on the end of their containers, and that this transformation provides a significant gain at run time. This work has two main contributions. First, it extends a known transformation framework to the case where the original program is already parallel.

---

[8] http://compilation.gforge.inria.fr/2013_04_Annecy

Second, it shows that the polyhedral model has applications far beyond its current use in data dependence and memory locality analyzes. This work also opens up new research directions. First, it turns out that our transformation is far more general than the use we currently make of it, and therefore that it provides a solid basis for other optimizations of parallel programs. Second, the polyhedral model we have developed provides an immediate cost model for synchronization primitives, which is not used in our current work, but may provide sound heuristics to adapt the optimization phase to the characteristics of specific run time components. We plan to explore these aspects in the near future.

This work has been done in collaboration with Paul Feautrier, member of the COMPSYS Inria team, in ENS Lyon. The CAMUS team has invited Paul Featrier for one week in June 2013 in Strasbourg. We are currently seeking funding to organize more frequent stays at either Lyon or Strasbourg.

This work has been invited for presentation at the LCPC workshop held in Lyon in July 2013 (http://labexcompilation.ens-lyon.fr/cpc2013). An extended version of this work has been accepted for publication at the *Compiler Construction* conference, to be held in April 2014.

6.5. Switcheable scheduling

Parallel applications used to be executed alone until their termination on partitions of supercomputers. The recent shift to multicore architectures for desktop and embedded systems is raising the problem of the coexistence of several parallel programs. Operating systems already take into account the *affinity* mechanism to ensure a thread will run only onto a subset of available processors (e.g., to reuse data remaining in the cache since its previous execution). But this is not enough, as demonstrated by the large performance gaps between executions of a given parallel program on desktop computers running several processes. To support many parallel applications, advances must be made on the system side (scheduling policies, runtimes, memory management...). However, automatic optimization and parallelization can play a significant role by generating programs with dynamic-auto-tuning capabilities to adapt themselves to the complete execution context, including the system load.

Our approach is to design at compile-time programs that can adapt at run-time to the execution context. The originality of our solution is to rely on *switcheable scheduling*, a selected set of program restructuring which allows to swap between program versions at some meeting points without backtracking. A first step selects pertinent versions according to their performance behavior on some execution contexts. The second step builds the auto-adaptive program with the various versions. Then at runtime the program selects the best version by a low overhead sampling and profiling of the versions, ensuring every computation is useful.

This work is an addition to the research directions of CAMUS related to dynamic optimization. It has been started at Paris-Sud University by Cédric Bastoul before he joined CAMUS during this year. This is an ongoing work with the PhD student Lénaïc Bagnères (GRAND-LARGE Team at Inria Saclay-Île-de-France, co-advised by Christine Eisenbeis and Cédric Bastoul). The first results have been presented in 2013 at the HiPEAC Computing System Week [9] and at the Rencontres Françaises de Compilation [10].

6.6. Interactive Code Restructuring

This work falls within the exploration and development of semi-automatic programs optimization techniques. It consists in designing and evaluating new visualization and interaction techniques for code restructuring, by defining and taking advantage of visual representations of the underlying mathematical model. The main goal is to assist programmers during program optimization tasks in a safe and efficient way, even if they neither have expertise into code restructuring nor knowledge of the underlying theories. This project is an important step for the efficient use and wider acceptance of semi-automatic optimization techniques, which are still tedious to use and incomprehensible for most programmers. More generally, this research is also investigating new presentation and manipulation techniques for code, algorithms and programs, which could lead to many practical applications: collaboration, tracking and verification of changes, visual search in large amount of code, teaching, etc.

---

[9] http://www.hipeac.net/thematic-session/let-us-push-thread-level-speculation
[10] http://compil13.cri.mines-paristech.fr

This is a rather new research direction which strengthen CAMUS's static parallelization and optimization issue. It has been initiated at Paris-Sud University as a collaboration between Compilation, represented by Cédric Bastoul before he joined CAMUS during this year, and Human-Machine Interaction, represented by Stéphane Huot from the IN-SITU Team at Inria Saclay-Île-de-France. This work is essentially the PhD topic of Alexander Zinenko (IN-SITU Team at Inria Saclay-Île-de-France, co-advised by Stéphane Huot and Cédric Bastoul, CORDI Grant) which started in 2013.

<p style="text-align:center; color:red">CARAMEL Project-Team</p>

6. New Results

6.1. Computation of Discrete Logarithms in $\mathrm{GF}(2^{809})$

Participants: Razvan Barbulescu, Cyril Bouvier, Jérémie Detrey, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé [contact], Marion Videau, Paul Zimmermann.

In the context of the CATREL ANR project, most team members contributed to the achievement of a new record computation for discrete logarithms in $\mathrm{GF}(2^{809})$, with the Function Field Sieve (FFS) algorithm. This is, to date, the largest computation in a binary field of prime extension degree. Beyond the experimental data and the improvements related to "what it takes" to beat such a record, this work provides very useful basis information towards the assessment of the cut-off with the novel quasi-polynomial algorithm discussed below.

This work has been reported in the article [15], accepted for publication in the conference PKC 2014 (Public Key Cryptography). It was the occasion to illustrate several contributions of members of the teams to various phases of the algorithm: Răzvan Bărbulescu [21] analyzed the polynomial selection step for FFS; Jérémie Detrey, Pierrick Gaudry and Marion Videau [17] improved the practical implementation of the relation collection; Cyril Bouvier [23] studied the filtering step; and Hamza Jeljeli [28] proposed to use the Residue Number System representation for the linear algebra step on GPU and CPU.

6.2. A Quasi-polynomial Algorithm for the Computation of Discrete Logarithms in Finite Fields of Small Characteristic

Participants: Razvan Barbulescu, Pierrick Gaudry, Emmanuel Thomé [contact].

In collaboration with Antoine Joux (Université Pierre et Marie Curie), Răzvan Bărbulescu, Pierrick Gaudry, and Emmanuel Thomé designed a new algorithm of quasi-polynomial complexity for computing discrete logarithms in finite fields $\mathrm{GF}(p^n)$, under the constraint that the characteristic p is small: it must not grow faster than a polynomial in the input size $n \log p$. This constraint accomodates for instance the cryptographically relevant case of finite fields of fixed characteristic $\mathrm{GF}(2^n)$ and $\mathrm{GF}(3^n)$.

This new algorithm dramatically changes the complexity landscape of the computation of discrete logarithms in finite fields. This has in particular an immense impact on the small characteristic pairing-based cryptography proposals. As it turns out, the field of definition of the Weil pairing for curves over small characteristic fields lends itself incredibly well to the new algorithm, to the point that the key sizes which are necessary to claim a sufficient security suddenly become unacceptably large. The newly proposed algorithm practically kills such cryptosystems.

This work has been published in preprint form in June 2013 [22] and was immediately acclaimed as a breakthrough, receiving also some external publicity. Pending the submission outcome, a first publication is expected in 2014.

6.3. Computation of CM Class Polynomials for Genus 2 Jacobians

Participant: Emmanuel Thomé [contact].

In collaboration with Andreas Enge, Emmanuel Thomé has developed software for computing class polynomials, in the context of complex multiplication theory in genus 2. The current computations set new records which are well above the previous state of the art, as Igusa class polynomials for class number above 20,000 have been computed in december 2013 using this software. An article describing this work has been accepted for publication in *Experimental Mathematics* [11].

Using similar underlying tools and theory, and based on work by Sorina Ionica [13], Sorina Ionica and Emmanuel Thomé have worked on the analysis of isogeny graphs in genus 2, when certain properties of the endomorphism ring are satisfied. A publication is being worked on, and is expected to be submitted in early 2014.

6.4. Binary to Decimal Conversion

Participants: Cyril Bouvier, Paul Zimmermann.

Cyril Bouvier and Paul Zimmermann designed a new algorithm to convert a large binary integer to decimal (or more generally any non-power-of-two radix). Compared to the reference implementation in GNU MP, this algorithm replaces divisions by multiplications, and exhibits a speedup of up to a factor of two (or more) in some cases [24].

6.5. Fast Change of Ordering for Gröbner Bases

Participant: Pierrick Gaudry.

When solving polynomial systems, the usual approach is to compute a Gröbner basis for a monomial order that is compatible with the degree with the F4 or F5 algorithm, and then compute a Gröbner basis for the lexicographical order using the FGLM algorithm. In collaboration with Jean-Charles Faugère, Louise Huot and Guénaël Renault, Pierrick Gaudry designed another approach [27] for this second step, leading to a better asymptotic complexity: the cubic complexity is replaced by the complexity of the linear algebra where the exponent can theoretically be as small as 2.37.

<h1 style="text-align:center; color:red">CARTE Project-Team</h1>

6. New Results

6.1. Computation and Dynamical Systems

In [12], we analyzed the power of dynamical system that are robust to infinitesimal perturbations. While previous works on this question were limited to very specific kinds of systems such as piecewise constant derivative systems, we obtained results for a quite general class of systems: the main hypothesis being smoothness (which is already a prerequisite in systems that perform analog computation). We show that if a system is robust, then the language it recognizes is computable, and the converse: all computable languages can be recognized by a robust smooth system. Those results are true for discrete-time as well as continuous-time dynamical systems on bounded or unbounded domains.

We investigated in [23], [15], [33] the isomorphism (conjugacy) problem for dynamical systems. While the decidability in the one-dimensional case is a long-standing open problem, we characterize its exact complexity [23] in higher dimensions. Our result suggest that the isomorphism problem is easier than the factoring and embedding problem (decide if one dynamical system is a subsystem of another). A traditional approach to prove two dynamical systems are not isomorphic is to prove that they have different dynamical invariants. We characterised in terms of complexity and computability classes different well known dynamic invariants (periodic points, Turing degrees) in [23], [33].

While Turing machines are usually used for computing, it is an interesting model of dynamical systems, which looks very much like two-dimensional piecewise-affine maps. We investigated dynmacial invariants (entropy and Lyapunov exponents) for Turing machines, and proved quite surprisingly that they are computable. Essentially this means that Turing machines that do interesting computations must do it so slowly that this cannot be seen in their dynamics. This work will be presented in STACS 2014

6.2. Computability, Complexity and Topology

6.2.1. *Complexity of real functionals*

Computability and topology are closely related as computability assumptions impose topological restrictions: on a topological space, computable functions are continuous and continuous functions are computable relative to some oracle. In the same way, complexity assumptions as bounds on the computation time impose analytical restrictions, but in a way that is not understood yet. For functions from the real numbers to the real numbers, it is known that polynomial-time computable functions correspond to functions with a polynomial modulus of continuity. However for functions on other spaces no such correspondence is known. We investigate the particular case of norms on the space of continuous real functions defined on the unit interval. We introduce analytical characteristics of a norm, namely its dependency on points and the concept of *relevant points*, and use them to characterize the polynomial-time computable norms. This work was presented at LICS 2013 [19]. A full version including other results on non-deterministic complexity classes is currently submitted [28].

6.2.2. *Higher-order complexity*

While computability theory is well-developed and understood on large classes of topological spaces, complexity theory in analysis is still in its infancy. We argue that the usual way of representing mathematical objects by functions from finite strings to finite strings (order 1 functions) is not appropriate for general spaces. We show that as soon as the space becomes large in a topological sense, it cannot be represented by order 1 functions in a way that respects complexity notions, so we propose to represent objects using higher order functions over finite strings. However higher order complexity theory is not well-understood. The only known class to date is BFF, the class of Basic Feasible Functionals, which does not enjoy nice properties: some intuitively feasible functionals do not belong to the class. We develop a new way of carrying out complexity theory at higher order types, using an adaptation of game semantics. A preliminary version of this work was presented at CCA 2013 [26].

6.2.3. Irreversible computable functions

As mentioned before, computable functions must be continuous. It gives a simple way of proving that some operator is not computable by showing that it is discontinuous. We recall that a function f is computable if there is a *single* oracle Turing machine M that on each x given by an oracle, computes $f(x)$. The following weaker notion is also interesting: a function *f preserves computability* if for each computable x, $f(x)$ is computable. Preservation of computability no more implies continuity, so there is no topological argument to show that some operator does not preserve computability. We develop a strong notion of discontinuity and prove a general result stating that this notion of discontinuity prevents preservation of computability. We apply this result to solve an open problem about the non-computability of the ergodic decomposition. We show that many classical constructions in computability theory are instances of our result. Hence we exhibit deeper connections between computability and topology. The work has been accepted at STACS 2014 [22]. A partial result was published in [13].

6.3. Implicit Computational Complexity

In the setting of non-interference and implicit computational complexity, Emmanuel Hainry, Jean-Yves Marion, and Romain Péchoux presented a characterization of FPSPACE in a language with a fork/wait mechanism [20]. The language used in this work is a classical imperative language with while loops complemented with a mechanism to launch new processes through forks. The fork instruction is heavily inspired by C's fork/wait construction for Unix operating systems, which anchors this work in a down-to-earth setting. Using a type system that enforces a data-ramification on variables, they show that all programs that can be typed and are terminating compute an FPSPACE function, that with a natural evaluation strategy, they indeed use only polynomial space, and conversely that this type system is complete as all FPSPACE functions can be implemented in this language in a typable way.

Emmanuel Hainry and Romain Péchoux also used data-ramification combined with non-interference principles to effectively bound the memory used by object oriented languages in [21]. This work introduces a type system for an object oriented language (derived from java). This type system allows to compute polynomial bounds on the heap and stack used by a typable program, ensuring that if the program halts, it will only use memory under this explicit bound. As the typing procedure is doable in time polynomial in the size of the program, those bounds are easy to obtain, though not tight. Interesting features of this work include inheritance (with overloading and overriding) and, the ability to analyze programs with flow statements controled by objects, contrary to most other works in implicit computational complexity. In [24], Romain Péchoux has shown that the notion of (polynomial) interpretation over term rewrite systems can be adapted on a process language, a variant of the pi-calculus with process recursive definitions. This work shows that the order induced by simulation can be used wrt a given process semantics to infer time and space upper bounds on process resource usage (reduction length, size of sent values, ...).

6.4. Computer Virology

The study on behavioural malware detection has been continued. Guillaume Bonfante, Isabelle Gnaedig and Jean-Yves Marion have been developing an approach detecting suspicious schemes on an abstract representation of the behavior of a program, by abstracting program traces, rewriting given subtraces into abstract symbols representing their functionality. Considering abstract behaviors allows us to be implementation-independent and robust to variants and mutations of malware. Suspicious behaviors are then detected by comparing trace abstractions to reference malicious behaviors.

Model checking is a strong point of our approach: the predefined behavior patterns, used to abstract program traces, are defined by first order temporal logic formulas, as well as the reference suspicious behaviors, given in a signature. The infection problem can then be seen as the satisfaction problem of the formula of the signature by an abstracted trace of the program, which can be checked using existing model checking techniques

The previous work by the team involved abstracting trace automata by rewriting them with respect to a set of predefined behavior patterns defined as a regular language described by a string rewriting system [37], and then, by a term rewriting system [38], which allows to detect information leak.

This work has been finished this year by designing a probabilistic generalization of our approach. Introducing probabilities in our technique allows to express a pertinence degree of detection when analysis of the program results in an incomplete or uncertain program dataflow, or when abstraction cannot be performed reliably. Proposing malware detection with a probabilistic rate is finer and more realistic in practice than giving the binary answer of whether a program is infected or not.

Using a tropical semiring over the reals, they have presented a formalism relying on a weighted term rewriting mechanism, where a weight w, naturally associated to a probability p by the formula: $w = -log(p)$, represents the probability that the realized abstraction be right.

Detection of an abstract behavior has then be defined with respect to a threshold, and a program P exhibits an abstract behavior M if and only if one of its traces admits an abstract form realizing M with a weight not exceeding this threshold.

The weighted abstraction formalism has the advantage of providing a detection algorithm with the same complexity as in the unweighted case, that is linear in the size of the trace automaton [27].

6.5. Graph rewriting

Guillaume Bonfante and Bruno Guillaume provide a new graph rewriting framework adapted to Natural Language Processing. It involves a new form of edge transformation. A new termination technique is also described. The extended paper [17] is accepted for publication in Mathematical Structure in Computer Science.

CASSIS Project-Team

6. New Results

6.1. Automated Deduction

We develop general techniques which allow us to re-use available tools in order to build a new generation of solvers offering a good trade-off between expressiveness, flexibility, and scalability. We focus on the careful integration of combination techniques and rewriting techniques to design decision procedures for a wide range of verification problems.

6.1.1. *Building and verifying decision procedures*

Participants: Alain Giorgetti, Olga Kouchnarenko, Christophe Ringeissen, Elena Tushkanova.

We have developed a methodology to build decision procedures by using superposition calculi which are at the core of equational theorem provers. In [14], we have developed automated deduction techniques to prove properties about these superposition-based decision procedures. To this aim, we have further investigated the use of schematic superposition, to check the termination and the combinability of superposition-based procedures. We have worked on the development of a framework for specifying and verifying superposition-based procedures. We have designed an implementation in Maude of the schematic superposition calculus. Thanks to this implementation we automatically derive termination of superposition for a couple of theories of interest in verification.

Until now, schematic superposition was only studied for standard superposition. In [53], [55], we introduce a schematic superposition calculus modulo a fragment of arithmetics, namely the theory of Integer Offsets. This new schematic calculus is used to prove the decidability of the satisfiability problem for some theories extending Integer Offsets. We illustrate our theoretical contribution on theories representing extensions of classical data structures, e.g., lists and records. Our Maude-based implementation has been extended to incorporate this new schematic superposition calculus modulo Integer Offsets. It enables automatic decidability proofs for theories of practical use.

6.1.2. *Hierarchical combination of unification procedures*

Participant: Christophe Ringeissen.

In [45], [54], a novel approach is described for the combination of unification algorithms for two equational theories which share function symbols. We are able to identify a set of restrictions and a combination method such that if the restrictions are satisfied the method produces a unification algorithm for the union of non-disjoint equational theories. Furthermore, we identify a class of theories satisfying the restrictions. The critical characteristics of the class is the hierarchical organization and the shared symbols being restricted to "inner constructors". Our approach can be applied to theories used for the analysis of protocols. The property of having an inner constructor in one side of an equality is common in the use of exponentiation in Diffie-Hellman inspired key agreement protocols. We are working on considering additional hierarchical theories. A possible candidate theory is a partial theory of Cipher Block Chaining.

6.1.3. *Unification modulo equational theories of cryptographic primitives*

Participant: Michaël Rusinowitch.

Some attacks exploit in a clever way the interaction between protocol rules and algebraic properties of cryptographic operators. In [74], we provide a list of such properties and attacks as well as existing formal approaches for analyzing cryptographic protocols under algebraic properties.

We have further investigated unification problems related to the Cipher Block Chaining (CBC) mode of encryption. We first model chaining in terms of a simple, convergent, rewrite system over a signature with two disjoint sorts: list and element. The 2-sorted convergent rewrite system is then extended into one that captures a block chaining encryption-decryption mode at an abstract level, (using no AC-symbols); unification modulo this extended system is shown to be decidable [15].

6.2. Security Protocol Verification

The design of cryptographic protocols is error-prone. Without a careful analysis, subtle flaws may be discovered several years after the publication of a protocol, yielding potential harmful attacks. In this context, formal methods have proved their interest for obtaining good security guarantees. Many analysis techniques have been proposed in the literature [70]. We have edited a book [62] where each chapter presents an important and now standard analysis technique. We develop new techniques for richer primitives, wider classes of protocols and higher security guarantees. In Section 6.4.3 we consider derived testing techniques for verifying protocol implementations.

6.2.1. *Voting protocols*

Participants: Véronique Cortier, David Galindo-Chacon, Stéphane Glondu, Malika Izabachene, Steve Kremer, Cyrille Wiedling.

Voting is a cornerstone of democracy and many voting systems have been proposed so far, from old paper ballot systems to purely electronic voting schemes. Although many works have been dedicated to standard protocols, very few address the challenging class of voting protocols. We have studied several protocols that are currently in use:

- Helios is an open-source web-based end-to-end verifiable electronic voting system, used e.g. by UCL and the IACR association in real elections. One main advantage of Helios is its verifiability, up-to the ballot box (a dishonest ballot box may add ballots). We have defined a variant of Helios, named Belenios, that prevents from ballot stuffing, even against a dishonest ballot box. Our approach consists in introducing an additional authorities that provides credentials that the ballot box can verify but not forge. This new version has been implemented by Stéphane Glondu and has been tested in a mock election in the teams Cassis and Caramel.
  We have proved computational security for both ballot secrecy and full verifiability (due to our credentials). Helios, as well as Belenios, makes use of threshold decryption, to ensure that decryption keys are distributed among several authorities, yet allowing decryption even some of the authorities are missing. We have provided a fully distributed (with no dealer) threshold cryptosystem suitable for the Helios voting system (in particular, suitable to partial decryption), and prove it secure under the Decisional Diffie-Hellman assumption [40]. Ballot privacy of Belenios then follows from ballot privacy of Helios. For full verifiability, we had first to adapt existing definitions of verifiability in the case of a corrupted ballot box and then prove verifiability of Helios [60].
- The Section 07 of CNRS (now split into Section 06 and Section 07) has proposed a voting protocol for Face-to-Face meetings to enhanced the verifiability of an election run through electronic devices. We have formally modeled this protocol and proved both ballot secrecy and verifiability [32].

Security based on cryptography relies on the fact that certain operations (such as decrypting) are computationally infeasible. However, e-voting protocols should also guarantee privacy in the future, when computers will have an increased computational power and will be able e.g. to break nowadays keys. Such privacy in the future is called *everlasting privacy* and we have proposed a definition of *practical everlasting privacy* [31]. As an illustration, we show that several variants of Helios (including Helios with Pedersen commitments) and a protocol by Moran and Naor achieve practical everlasting privacy, using the ProVerif and the AKiSs tools, which we had to adapt to cope with everlasting privacy.

We have written a popularization science paper on e-voting in Interstices[4].

---

[4]https://interstices.info/jcms/int_68258/vote-par-internet

6.2.2. *Other families of protocols*

Participants: Véronique Cortier, Steve Kremer, Robert Künnemann, Cyrille Wiedling.

Securing routing Protocols. The goal of routing protocols is to construct valid routes between distant nodes in the network. If no security is used, it is possible for an attacker to disorganize the network by maliciously interacting with the routing protocols, yielding invalid routes to be built. We have proposed a new model and an associated decision procedure to check whether a routing protocol can ensure that honest nodes only accept valid routes, even if one of the nodes of the network is compromised. This result has been obtained for a bounded number of sessions, adapting constraint solving techniques to node topologies as well as some families of recursive tests, used in routing protocols [16].

Security APIs. In some systems, it is not possible to trust the host machine on which sensitive codes are executed. In that case, security-critical fragments of a program should be executed on some tamper resistant device (TRD), such as a smartcard, USB security token or hardware security module (HSM). The exchanges between the trusted and the untrusted infrastructures are ensured by special kind of API (Application Programming Interface), that are called *security APIs*. We have designed a generic API for key-management based on key hierarchy [23], that can self-recover from corruption of arbitrary keys, provided the number of corrupted, active keys is smaller than some threshold. In [50], we propose a universally composable key management functionality and show how to achieve a secure, distributed implementation on TRDs. We are currently also working on automated verification of security APIs (and more generally protocols that require global mutable state). A tool implementation using the tamarin prover as a backend is currently in progress.

6.2.3. *Automated verification of indistinguishability properties.*

Participants: Rémy Chrétien, Véronique Cortier, Stéphane Glondu, Steve Kremer.

New emerging classes of protocols such as voting protocols often require to model less classical security properties, such as anonymity properties, strong versions of confidentiality and resistance to offline guessing attacks. Many of these properties can be modelled using the notion of indistinguishability by an adversary, which can be conveniently modeled using process equivalences.

Static case. The YAPA tool [17] can check static equivalence for convergent equational theories. It is proved to terminate for a wide class of equational theories that includes subterm convergent theories (e.g. encryption, signatures, pairing and hash) and layered convergent theories (e.g. blind signatures). The procedure is generic in the sense that it remains sound and complete (but may not terminate) for any convergent theory. It has been implemented in the YAPA tool[5].

Active case. We have shown that, for arbitrary equational theories, verifying indistinguishability properties such as trace equivalence in security protocols amounts to deciding the equivalence of constraint systems, i.e., checking whether they have the same set of solutions [20]. When considering the equational theory corresponding to the standard primitives, Vincent Cheval has proposed a decision procedure for checking equivalence of set constraints, which yields a procedure for checking trace equivalence [73]. We have extended this decision procedure to the case where the attacker can observe the *length* of messages [37]. This yields the discovery of a new attack on the biometric passport. This attack has been implemented and successfully tested on a small set of passports. This attack is explained in details in a webpage[6] and has obtained some press coverage.

Active case, unbounded number of sessions. Rémy Chrétien has started a PhD on deciding trace equivalence for an unbounded number of sessions. He has shown that for some classes of protocols, decidability of trace equivalence can be reduced to equivalence of deterministic pushdown automata [38]. Equivalence of deterministic pushdown automata is decidable [81] and the corresponding decision procedure is currently implemented by Géraud Senizergues. Based on his tool, we are developing a tool for automatically checking equivalence, for an unbounded number of sessions.

---

[5]http://www.lsv.ens-cachan.fr/~baudet/yapa/
[6]http://www.loria.fr/ glondu/epassport/attack-lengths.html

6.2.4. *Securely Composing Protocols*

Participants: Véronique Cortier, Steve Kremer, Éric Le Morvan.

Protocols are often built in a modular way. For example, authentication protocols may assume pre-distributed keys or may assume secure channel. However, when an authentication protocol has been proved secure assuming pre-distributed keys, there is absolutely no guarantee that it remains secure when executing a real protocol for distributing the keys. How the security of these protocols can be combined is an important issue that is studied in the PhD thesis recently started by Éric Le Morvan.

A related problem arises when several protocols use the same secrets, e.g. the same keys. While each protocol may be proved secure in isolation, the protocols may become insecure when executed in parallel. In [21] we study whether password protocols can be safely composed, even when a same password is reused. It seems indeed unrealistic to suppose that users do not re-use the same password for different applications. More precisely, we present a transformation which maps a password protocol that is secure for a single protocol session (a decidable problem) to a protocol that is secure for an unbounded number of sessions. Our result provides an effective strategy to design secure password protocols: (i) design a protocol intended to be secure for one protocol session; (ii) apply our transformation and obtain a protocol which is secure for an unbounded number of sessions. Our technique also applies to compose different password protocols allowing us to obtain both inter-protocol and inter-session composition.

6.2.5. *Soundness of the Dolev-Yao Model*

Participants: Véronique Cortier, Guillaume Scerri.

All the previous results rely on symbolic models of protocol executions in which cryptographic primitives are abstracted by symbolic expressions. This approach enables significantly simple and often automated proofs. However, the guarantees that it offers have been quite unclear compared to cryptographic models that consider issues of complexity and probability. A somewhat recent line of research consists in identifying cases where it is possible to obtain the best of both cryptographic and formal worlds: fully automated proofs and strong, clear security guarantees.

A first approach consists in proving that symbolic models (as the ones studied on the previous sections) are actually *sound* w.r.t. cryptographic models, provided the primitives satisfy some (strong) security properties. Soundness result are usually established for some set of cryptographic primitives and extending the result to encompass new primitives typically requires redoing most of the work. In [35], we propose a notion of computational soundness, amenable to modular extensions. Specifically, we prove that a deduction sound implementation of some arbitrary primitives can be extended to include all standard primitives (asymmetric ans symmetric encryption, public data-structures - e.g. pairings or list, signatures, MACs, and hashes) without repeating the original proof effort. Furthermore, our notion of soundness concerns cryptographic primitives in a way that is independent of any protocol specification language.

Such soundness results require however strong hypotheses on the implementation. For example, primitives must be tagged to avoid confusion between e.g. pairs and encryption. Gergei Bana and Hubert Comon have proposed a new framework [67] where the symbolic model now specifies what an attacker *cannot* do instead of specifying what it can do. Checking protocols security can then be reduced to checking inconsistency of some set of first order formula. During his PhD, Guillaume Scerri studies how to develop a (polynomial) decision procedure for deciding consistency of sets of formulas, for some class of formulas corresponding to security protocols [39].

6.3. Model-based Verification

We have investigated extensions of regular model-checking to new classes of rewrite relations on trees. We have studied specification and proof of modular imperative programs.

6.3.1. *Verification of Linear Temporal Patterns over Finite and Infinite Traces*

Participants: Pierre-Cyrille Héam, Vincent Hugot, Olga Kouchnarenko.

In the regular model-checking framework, reachability analysis can be guided by temporal logic properties, for instance to achieve the counter example guided abstraction refinement (CEGAR) objectives. A way to perform this analysis is to translate a temporal logic formula expressed on maximal rewriting words into a "rewrite proposition" – a propositional formula whose atoms are language comparisons, and then to generate semi-decision procedures based on (approximations of) the rewrite proposition. In [13] we have investigated suitable semantics for LTL on maximal rewriting words and their influence on the feasibility of a translation, and we have proposed a general scheme providing exact results for a fragment of LTL corresponding mainly to safety formulæ, and approximations for a larger fragment.

6.3.2. *Approximations Techniques for Regular Model-Checking*
Participants: Aloïs Dreyfus, Pierre-Cyrille Héam, Olga Kouchnarenko.

We address the following general problem of regular model-checking: decide whether $R^*(L) \cap L_p = \varnothing$ where R^* is the reflexive and transitive closure of a successor relation R, and L and L_p are both regular tree languages. Considering a relation R on finite words and a regular language L encoding the initial configurations of a system, the set $R^*(L)$ of accessible words is not necessarily regular. Therefore, a way to verify safety properties is to over-approximate the set of reachable words by a regular language. In [42], we develop new efficient approximation techniques based on syntactic criteria. When these syntactic over-approximations are too coarse, we propose CEGAR-like techniques to refine them using counter-examples. The approach has been successfully applied to verify mutual exclusion protocols.

6.4. Model-based Testing

Our research in Model-Based Testing (MBT) aims to extend the coverage of tests. The coverage refers to several artefacts: model, test scenario/property, and code of the program under test. The test generation uses various underlying techniques such as symbolic animation of models [75], or symbolic execution of programs by means of dedicated constraints, SMT solvers, or model-checkers.

6.4.1. *Automated Test Generation from Behavioral Models*
Participants: Fabrice Bouquet, Kalou Cabrera, Jérome Cantenot, Frédéric Dadeau, Jean-Marie Gauthier, Julien Lorrain.

We have developed an original model-based testing approach that takes a behavioural view (modelled in UML) of the system under test and automatically generates test cases and executable test scripts according to model coverage criteria. We continue to extend this result to SysML specifications for validating embedded systems [30]. To allow the test generation from SysML models, in [47] we study the transformation into a low level language suitable for hardware specification.

In the context of software evolution, we have worked on exploiting the evolution of requirements in order to classify test sequences, and precisely target the parts of the system impacted by this evolution. We have proposed to define the life cycle of a test via three test classes: (i) Regression, used to validate that unimpacted parts of the system did not change, (ii) Evolution, used to validate that impacted parts of the system correctly evolved, and (iii) Stagnation, used to validate that impacted parts of the system did actually evolve. The associated algorithms are under implementation in a dedicated prototype already used in the SecureChange European project.

6.4.2. *Scenario-Based Verification and Validation*
Participants: Fabrice Bouquet, Kalou Cabrera, Frédéric Dadeau.

Test scenarios represent an abstract test case specification that aims at guiding the model animation in order to produce relevant test cases. Contrary to the previous section, this technique is not fully automated since it requires the user to design the scenario, in addition to the model.

We have designed a scenario based testing language for UML/OCL that can be either connected to a model animation engine or to a symbolic animation engine, based on a set-theoretical constraint solver [75]. In the context of the ANR TASCCC project, we investigated the automation of test generation from Security Functional Requirements (SFR), as defined in the Common Criteria terminology. To achieve that, we worked on the definition of description patterns for security properties, to which a given set of SFRs can be related. These properties are used to automatically generate test scenarios that produce model based test cases. The traceability, ensured all along the testing process, makes it possible to provide evidences of the coverage of the SFR by the tests, required by the Common Criteria to reach the highest Evaluation Assurance Levels.

We have proposed a dedicated formalism to express test properties. translated into a finite state automaton which describes a monitor of its behaviors [36]. We have proposed dedicated property coverage criteria that can be used either to measure the property coverage of a given test suite, or to generate test cases, exercising nominal or robustness aspects of the property. This process has been fully tool-supported into an integrated software prototype[7] [41].

In the context of the SecureChange project, we have also investigatde the evolution of test scenarios. As the system evolves, the model evolves, and the associated test scenarios may also evolve. We are currently extending the test generation and management of system evolutions to ensure the preservation of the security.

6.4.3. *Mutation-based Testing of Security Protocols*
Participants: Frédéric Dadeau, Pierre-Cyrille Héam, Ghazi Maatoug, Michaël Rusinowitch.

Verification of security protocols models is an important issue. Nevertheless, the verification reasons on a model of the protocol, and does not consider its concrete implementation. While representing a safe model, the protocol may be incorrectly implemented, leading to security flaws when it is deployed. We have proposed a model-based penetration testing approach for security protocols [9]. This technique relies on the use of mutations of an original protocol, proved to be correct, for injecting realistic errors that may occur during the protocol implementation (e.g. re-use of existing keys, partial checking of received messages, incorrect formatting of sent messages, use of exponential/xor encryption, etc.). Mutations that lead to security flaws are used to build test cases, which are defined as a sequence of messages representing the behavior of the intruder. secret. We have applied our technique on protocols designed in HLPSL, and implemented a protocol mutation tool that performs the mutations. The mutants are then analyzed by the CL-Atse [82] front-end of the AVISPA toolset [64]. We have experimented our approach on a set of protocols, and we have shown the relevance of the proposed mutation operators and the efficiency of the CL-Atse tool to conclude on the vulnerability of a protocol and produce an attack trace that can be used as a test case for implementations. We applied our approach on the Paypal Express protocol, and we were able to retrieve an existing attack trace on this protocol[8]. We are now investigating the transformation of an attack trace into executable tests scripts. To achieve that, we propose to automatically generate skeletons of Java test programs that the validation engineer only has to fill in order to concretize the steps of the test. A first experience in this direction has been described in [48].

6.4.4. *Rewriting-based Mathematical Model Transformations*
Participants: Walid Belkhir, Alain Giorgetti.

Since 2011 we collaborate with the Department "Temps-Fréquence" of the FEMTO-ST institute (Franche-Comté Electronique Mécanique Thermique et Optique - Sciences et Technologies, CNRS UMR 6174) on the formalization of asymptotic methods (based on two-scale convergence).The goal is to design a software, called *MEMSALab*, for the automatic derivation of multiscale models of arrays of micro- and nanosystems. In this domain a model is a partial differential equation. Multiscale methods approximate it by another partial differential equation which can be numerically simulated in a reasonable time. The challenge consists in taking into account a wide range of geometries combining thin and periodic structures with the possibility of multiple nested scales. We have designed a transformation language facilitating the design of MEMSALab [18]. It

---

[7]A video of the prototype is available at: http://vimeo.com/53210102
[8]http://www.nbs-system.com/blog/faille-securite-magento-paypal.html

is proposed as a Maple^{TM} package for rule-based programming, rewriting strategies and their combination with standard Maple^{TM} code. We illustrate the practical interest of this language by using it to encode two examples of multiscale derivations, namely the two-scale limit of the derivative operator and the two-scale model of the stationary heat equation. A more general framework for the derivation of the multi-scale models was established in [26].

6.4.5. *Code-related Test Generation and Static Analysis*

Participants: Fabrice Bouquet, Frédéric Dadeau, Ivan Enderlin, Alain Giorgetti.

We have designed a new annotation language for PHP, named PRASPEL (for *PHP Realistic Annotation SPEcification Language*). This language relies on *realistic domains* which serve two purposes. First, they assign to a data a domain that is supposed to be specific w.r.t. a context in which it is employed. Second, they provide two features that are used for test generation: (i) *samplability* makes it possible to automatically generate a value that belongs to the realistic domain so as to generate test data, (ii) *predicability* makes it possible to check if the value belongs to a realistic domain. This approach is tool-supported in a dedicated framework for PHP which makes it possible to produce unit test cases using random data generators, execute the test cases on an instrumented implementation, and decide the conformance of the code w.r.t. the annotations by runtime assertion checking. This principle has been extended to generate grammar-based textual data based on various strategies, namely uniform random generation, bounded exhaustive generation and rule-coverage-based test generation. In a recent work, we have proposed a dedicated constraint solver for PHP arrays [44] aiming to avoid rejection during the generation of array structures.

6.4.6. *Random Testing*

Participants: Aloïs Dreyfus, Pierre-Cyrille Héam, Olga Kouchnarenko.

The random testing paradigm represents a quite simple and tractable software assessment method for various testing approaches. When performing random testing, the random sampler is supposed to be independent of tester choices or convictions: a solution is to exploit uniform random generators.

In [78] a method is proposed for drawing paths in finite graphs uniformly, and it is explained how to use these techniques for testing C programs within a control flow graph based approach. Nevertheless, as finite graphs often provide strong abstractions of the systems under test, many abstract tests generated by the approach cannot be played on the implementation. In [79], we have proposed a new approach, extending [78], to manage stack-call during the random test generation while preserving uniformity. In [61], we go further by investigating a way to bias the random testing, in order to optimize the probability to fulfil a coverage criterion. The new approaches have been implemented in a prototype and experimented on several examples. A similar approach for grammar based testing is developed in [43]: we show how to hedge the random generation of execution trees to optimize the probability of covering either all rules or all non terminal symbols.

6.5. Verification of Collaborative Systems

We investigate security problems occurring in decentralized systems. We develop general techniques to enforce read and update policies for controlling access to XML documents based on recursive DTDs (Document Type Definition). Moreover, we provide a necessary and sufficient condition for undoing safely replicated objects in order to enforce access control policies in an optimistic way.

6.5.1. *Automatic Analysis of Web Services Security*

Participants: Walid Belkhir, Michaël Rusinowitch, Mathieu Turuani, Laurent Vigneron.

Automatic composition of web services is a challenging task. Many works have considered simplified automata models that abstract away from the structure of messages exchanged by the services. For the domain of secured services (using e.g. digital signing or timestamping) we propose a novel approach to automated orchestration of services under security constraints. Given a community of services and a goal service, we reduce the problem of generating a mediator between a client and a service community to a security problem where an intruder should intercept and redirect messages from the service community and a client service till reaching a satisfying state. This orchestration specification is expressed in ASLan language, a formal language designed for modeling Web Services tied with security policies that was developed in AVANTSSAR project. The AVANTSSAR Orchestrator (presented in [28]) generates an attack trace describing the execution of a the mediator and translates it into ASLan. Then we can check with automatic tools that this ASLan specification verifies required security properties such as secrecy and authentication. If no flaw is found, we can compile the ASLan specification into a Java servlet that can be used to execute the orchestration.

In [34] we introduce an alternative approach based on *fresh-variable automata*, a natural extension of finite-state automata over infinite alphabet. In this model the transitions are labeled with constants or variables that can be refreshed in some specified states. We prove several closure properties for this class of automata and study their decision problems. We show the applicability of our model to Web services handling data from an infinite domain. We introduce a notion of simulation that enables us to reduce the Web service composition problem to the construction of a simulation of a target service by the asynchronous product of existing services, and prove that this construction is computable. We now work on synthesizing composed services that satisfy required security policies.

6.5.2. *Secure Querying and Updating of XML Data*

Participants: Abdessamad Imine, Houari Mahfoud, Michaël Rusinowitch.

It is increasingly common to find XML views used to enforce access control as found in many applications and commercial database systems. To overcome the overhead of view materialization and maintenance, XML views are necessarily virtual. With this comes the need for answering XML queries posed over virtual views, by rewriting them into equivalent queries on the underlying documents. A major concern here is that query rewriting for recursive XML views is still an open problem, and proposed approaches deal only with non-recursive XML views. Moreover, a small number of works have studied the access rights for updates. In [51], we present SVMAX (Secure and Valid MAnipulation of XML), the first system that supports specification and enforcement of both read and update access policies over arbitrary XML views (recursive or non). SVMAX defines general and expressive models for controlling access to XML data using significant class of XPath queries and in the presence of the update primitives of W3C XQuery Update Facility. Furthermore, SVMAX features an additional module enabling efficient validation of XML documents after primitive updates of XQuery. The wide use of W3C standards makes of SVMAX a useful system that can be easily integrated within commercial database systems as we will show. We give extensive experimental results, based on real-life DTDs, that show the efficiency and scalability of our system.

We introduce in [49] an extension of hedge automata called bidimensional context-free hedge automata, proposing a new uniform representation of vertical and horizontal computation steps in unranked ordered trees. We also extend the parameterized rewriting rules used for modeling the W3C XQuery Update Facility in previous works, by the possibility to insert a new parent node above a given node. Since the rewrite closure of hedge automata languages with these extended rewriting systems is a computable context-free hedge language we can perform some static typechecking on these XML transformations.

6.5.3. *On Adding Friends Problem in Social Networks*

Participants: Bao Thien Hoang, Abdessamad Imine.

Online social networks are currently experiencing a peak and they resemble real platforms of social conversion and content delivery. Indeed, they are exploited in many ways: from conducting public opinion polls about any political issue to planning big social events for a large public. To securely perform these large-scale computations, current protocols use a simple secret sharing scheme which enables users to obfuscate their

inputs. However, these protocols require a minimum number of friends, i.e. the minimum degree of the social graph should be not smaller than a given threshold. Often this condition is not satisfied by all social graphs. Yet we can reuse these graphs after some structural modifications consisting in adding new friendship relations. In this paper, we provide the first definition and theoretical analysis of the "*adding friends*" problem. We formally describe this problem that, given a graph G and parameter c, asks for the graph satisfying the threshold c that results from G with the minimum of edge-addition operations. We present algorithms for solving this problem in centralized social networks [33]. An experimental evaluation on real-world social graphs demonstrates that our protocols are accurate and inside the theoretical bounds.

6.5.4. *Access Control Models for Collaborative Applications*

Participants: Fabrice Bouquet, Abdessamad Imine, Michaël Rusinowitch.

The importance of collaborative systems in real-world applications has grown significantly over the recent years. The most of new applications are designed in a distributed fashion to meet collaborative work requirements. Among these applications, we focus on Real-Time Collaborative Editors (RCE) that provide computer support for modifying simultaneously shared documents, such as articles, wiki pages and programming source code by dispersed users. Although such applications are more and more used into many fields, the lack of an adequate access control concept is still limiting their full potential. In fact, controlling access in a decentralized fashion in such systems is a challenging problem, as they need dynamic access changes and low latency access to shared documents. In [19], we propose a generic access control model based on replicating the shared document and its authorization policy at the local memory of each user. We consider the propagation of authorizations and their interactions. We propose an optimistic approach to enforce access control in existing collaborative editing solutions in the sense that the access control policy can be temporarily violated. To enforce the policy, we resort to the selective undo approach in order to eliminate the effect of illegal document updates. Since, the safe undo is an open issue in collaborative applications. We investigate a theoretical study of the undo problem and propose a generic solution for selectively undoing operations. Finally, we apply our framework on a collaboration prototype and measure its performance in the distributed grid GRID'5000 to highlight the scalability of our solution.

However, verifying whether the combination of access control and coordination protocols preserves the data consistency is a hard task since it requires examining a large number of situations. In [52], we specify this access control protocol in the first-order relational logic with Alloy, and we verify that it preserves the correctness of the system on which it is deployed, namely that the access control policy is enforced identically at all participating user sites and, accordingly, the data consistency remains still maintained.

PAREO Project-Team

6. New Results

6.1. Static analysis

Participant: Sergueï Lenglet.

6.1.1. *Static analysis for control operators*

Control operators allow programs to have access and manipulate their execution context. Abortive control operators, such as *call/cc* in Scheme or SML, capture the entire execution context (also called continuation), while delimited-control operators, such as *shift* and *reset* captures only a part of the continuation (delimited by reset). We want to prove properties (like equivalences between terms or termination) for languages with these operators, using static analysis.

In [9], [16], we study the behavioral theory of a language with delimited control. More precisely, we define environmental bisimilarities for the delimited-control operators shift and reset. We consider two different notions of contextual equivalence: one that does not require the presence of a top-level control delimiter when executing tested terms, and another one, fully compatible with the original CPS semantics of shift and reset, that does. For each of them, we develop sound and complete environmental bisimilarities, and we discuss up-to techniques.

In [8], we present new proofs of termination of evaluation in reduction semantics (i.e., a small-step operational semantics with explicit representation of evaluation contexts) for System F with control operators. We introduce a modified version of Girard's proof method based on reducibility candidates, where the reducibility predicates are defined on values and on evaluation contexts as prescribed by the reduction semantics format. We address both abortive control operators (*callcc*) and delimited-control operators (*shift* and *reset*) for which we introduce novel polymorphic type systems, and we consider both the call-by-value and call-by-name evaluation strategies.

6.1.2. *Polymorphism and higher-order functions for XML*

In [11], we define a calculus with higher-order polymorphic functions, recursive types with arrow and product type constructors and set-theoretic type connectives (union, intersection, and negation). We study the explicitly-typed version of the calculus in which type instantiation is driven by explicit instantiation annotations. In particular, we define an explicitly-typed λ-calculus with intersection types and an efficient evaluation model for it. In a companion paper [21], we define a local type inference system that allows the programmer to omit explicit instantiation annotations, and a type reconstruction system that allows the programmer to omit explicit type annotations. The work presented in the two articles provides the theoretical foundations and technical machinery needed to design and implement higher-order polymorphic functional languages for semi-structured data.

6.2. Model Transformations

Participants: Jean-Christophe Bach, Pierre-Etienne Moreau.

Model Driven Engineering is a technique that has been applied quite successfully for the design of complex systems. Such systems cannot be released and embedded without complying with the certification required by the application domain: EN 50128 for railways, DO-178C for aeronautics, or ISO 26262 for automotive for instance.

Recently we have developed an extension of *Tom* to support the development of Model Transformations and the generation of traces which are needed to give confidence in the quality of the implemented transformation.

In [12], we present a method, a language and dedicated tooling to ease and to speed up software development based on models transformations. Our approach aims to bridge the gap between general purpose languages and domain specific ones in order to take benefit from both of the two worlds, and to increase software quality. Our approach uses the Tom language which is a shallow extension of general purpose languages. Our proposal allows to write modular transformations whose code is reusable, and which are traceable.

6.3. Property based testing

Participants: Horatiu Cirstea, Pierre-Etienne Moreau, Cosay Topaktas.

Quality is crucial for software systems and several aspects should be taken into account. Formal verification techniques like model checking and automated theorem proving can be used to guarantee the correctness of finite or infinite systems. While these approaches provide a high level of confidence they are sometimes difficult and expensive to apply. Software testing is another approach and although it cannot guarantee correctness it can be very efficient in finding errors.

We have proposed a property based testing framework for the *Tom* language inspired from the ones prosed in the context of functional programming. In the current version relatively simple properties can be already expressed and tested on *Tom* programs. It consists of an exhaustive approach testing all possible input values and guaranteeing that the discovered counter-examples are the smallest ones (the size of the inputs is clearly limited by the execution time) and a random approach where inputs of bigger size could be tested but the minimal counter-example is not guaranteed. A relatively simple shrinking method which searches a smaller counter-example starting from an initial relatively complex one has been also proposed. There is ongoing work on the expressiveness of the property language and the efficiency of the shrinking method. The library is available at http://gforge.inria.fr/projects/tom.

6.4. Nominal Theory

Participant: Christophe Calvès.

Nominal unification is proven to be quadratic in time and space. It was so by two different approaches, both inspired by the Paterson-Wegman linear unification algorithm, but dramatically different in the way nominal and first-order constraints are dealt with.

To handle nominal constraints, Levy and Villaret introduced the notion of replacing while Calvès and Fernández use permutations and sets of atoms. To deal with structural constraints, the former use multi-equation in a way similar to the Martelli-Montanari algorithm while the later mimic Paterson-Wegman.

In [10] we abstract over these two approaches and genralize them into the notion of modality, highlighting the general ideas behind nominal unification. We show that replacings and environments are in fact isomorphic. This isomorphism is of prime importance to prove intricate properties on both sides and a step further to the real complexity of nominal unification.

TRIO Team

6. New Results

6.1. Probabilistic real-time systems

Participants: Liliana Cucu-Grosjean, Adriana Gogonel, Codé Lo, Dorin Maxim and Cristian Maxim.

The arrival of complex hardware responding to the increasing demand for computing power in next generation systems exacerbates some of the limitations of static timing analysis for the estimation of the worst-case execution time (WCET) estimation. In particular, the effort of acquiring (1) detail information on the hardware to develop an accurate model of its execution latency as well as (2) knowledge of the timing behaviour of the program in the presence of varying hardware conditions, such as those dependent on the history of previously executed instructions. These problems are also known as the timing analysis walls. The probabilistic timing analysis, a novel approach to the analysis of the timing behaviour of next-generation real-time embedded systems, provides answers to timing analysis walls. In [7], [13], [11] timing analysis attacks the timing analysis walls. We have also presented experimental evidence that shows how probabilistic timing analysis reduces the extent of knowledge about the execution platform required to produce probabilistically-safe and tight WCET estimations.

Based on existing estimations of WCET or minimal inter-arrival time [16], we may propose different probabilistic schedulability analyses [6], [12].

2013 was also the year when through several invited talks [8], [10], [9], we had the opportunity to underline historical misunderstandings on probabilistic real-time systems. The most common is related to the notion of independence that is used with a wrong meaning by different papers.

<div align="center">

VEGAS Project-Team

</div>

5. New Results

5.1. Classical and probabilistic computational geometry

Participants: Xavier Goaoc, Guillaume Moroz, Sylvain Lazard, Marc Pouget.

5.1.1. *Probabilistic complexity analysis of random geometric structures*

Average-case analysis of data-structures or algorithms is commonly used in computational geometry when the more classical worst-case analysis is deemed overly pessimistic. Since these analyses are often intricate, the models of random geometric data that can be handled are often simplistic and far from "realistic inputs".

Complexity analysis of random geometric structures made simpler. In a joint work with Olivier Devillers and Marc Glisse (Inria Geometrica), we presented a new simple scheme for the analysis of geometric structures. While this scheme only produces results up to a polylog factor, it is much simpler to apply than the classical techniques and therefore succeeds in analyzing new input distributions related to smoothed complexity analysis. We illustrated our method on two classical structures: convex hulls and Delaunay triangulations. Specifically, we gave short and elementary proofs of the classical results that n points uniformly distributed in a ball in R^d have a convex hull and a Delaunay triangulation of respective expected complexities $\widetilde{\Theta}(n^{((d+1)/(d-1))})$ and $\widetilde{\Theta}(n)$. We then prove that if we start with n points well-spread on a sphere, e.g. an (ϵ, κ)-sample of that sphere, and perturb that sample by moving each point randomly and uniformly within distance at most δ of its initial position, then the expected complexity of the convex hull of the resulting point set is $\widetilde{\Theta}(\sqrt{(n)}^{(1-1/d)}\delta^{-(d-1)/(4d)})$. We presented these results in the *Symposium on Computational Geometry* 2013 [20].

Monotonicity of the number of facets of random polytopes. We also proved a result on the size of the convex hull K_n of n points sampled uniformly in a convex set K. More precisely, let $u_n^{K,i}$ be the expected number of facets of dimension i of the convex hull. We proved that, in the plane, $u_n^{K,0}$ is an increasing sequence. In higher dimension, if K is a convex, smooth, compact body, then we showed that the sequence $u_n^{K,d-1}$ is asymptotically increasing. This result, published in the *Electronic Communications in Probability* [13], was obtained in collaboration with Olivier Devillers and Marc Glisse (Inria Geometrica) and Matthias Reitzner (Osnabruck Univ.).

Worst-case silhouette size of random polytopes. Finally, we studied from a probabilistic point of view the size of the silhouette of a polyhedron. While the silhouette size of a polyhedron with n vertices may be linear for some view points, several experimental and theoretical studies show a sublinear behavior for a wide range of constraints. The latest result on the subject proves a bound in $\Theta(\sqrt{n})$ on the size of the silhouette from a random view point of polyhedra of size n approximating non-convex surfaces in a reasonable way [9]. This result considers the polyhedron given and average the sizes of the silhouettes over all view points. This year, we addressed the problem of bounding the worst-case size of the silhouette where the average is taken over a set of polyhedra. Namely, we consider random polytopes defined as the convex hull of a Poisson point process on a sphere in $\mathbb{R}^3$ such that its average number of points is n. We show that the expectation over all such random polytopes of the maximum size of their silhouettes viewed from infinity is $\Theta(\sqrt{n})$. This work was done in collaboration with Marc Glisse (Inria Geometrica) and Julien Michel (Université de Poitiers) [24].

5.1.2. *Embedding geometric structures*

We continued working this year on the problem of embedding geometric objects on a grid of $\mathbb{R}^3$. Essentially all industrial applications take, as input, models defined with a fixed-precision floating-point arithmetic, typically doubles. As a consequence, geometric objects constructed using exact arithmetic must be embedded on a fixed-precision grid before they can be used as input in other software. More precisely, the problem is, given a geometric object, to find a similar object representable with fixed-precision floating-point arithmetic, where similar means topologically equivalent, close according to some distance function, etc. We are working on the problem of rounding polyhedral subdivisions on a grid of $\mathbb{R}^3$, where the only known method, due to Fortune in 1999, considers a grid whose refinement depends on the combinatorial complexity of the input, which does not solve the problem at hand. This project is joint work with Olivier Devillers (Inria Geometrica) and William Lenhart (Williams College, USA).

5.1.3. *Bounded-Curvature Shortest Paths*

We considered the problem of computing shortest paths having curvature at most one almost everywhere and visiting a sequence of n points in the plane in a given order. This problem is a sub-problem of the Dubins Traveling Salesman Problem and also arises naturally in path planning for point car-like robots in the presence of polygonal obstacles. We showed that when consecutive waypoints are distance at least four apart, this question reduces to a family of convex optimization problems over polyhedra in $\mathbb{R}^n$. This result, done in collaboration with Hyo-Sil Kim (KAIST) was published in the *SIAM Journal on Computing* [15].

5.1.4. *Approximating Geodesics in Meshes*

A standard way to approximate the distance between any two vertices p and q on a mesh is to compute, in the associated graph, a shortest path from p to q that goes through one of k sources, which are well-chosen vertices. Precomputing the distance between each of the k sources to all vertices of the graph yields an efficient computation of approximate distances between any two vertices. One standard method for choosing k sources, which has been used extensively and successfully for isometry-invariant surface processing, is the so-called *Farthest Point Sampling* (FPS), which starts with a random vertex as the first source, and iteratively selects the farthest vertex from the already selected sources.

We analyzed the stretch factor $\mathcal{F}_{FPS}$ of approximate geodesics computed using FPS, which is the maximum, over all pairs of distinct vertices, of their approximated distance over their geodesic distance in the graph. We show that $\mathcal{F}_{FPS}$ can be bounded in terms of the minimal value $\mathcal{F}^*$ of the stretch factor obtained using an optimal placement of k sources as $\mathcal{F}_{FPS} \leq 2r_e^2\mathcal{F}^* + 2r_e^2 + 8r_e + 1$, where r_e is the ratio of the lengths of the longest and the shortest edges of the graph. This provides some evidence explaining why farthest point sampling has been used successfully for isometry-invariant shape processing. Furthermore, we showed that it is NP-complete to find k sources that minimize the stretch factor [25].

5.1.5. *On Point-sets that Support Planar Graphs*

A set of points is said universal if it supports a crossing-free drawing of any planar graph. For a planar graph with n vertices, if bends on edges of the drawing are permitted, universal point-sets of size n are known, but only if the bend-points are in arbitrary positions. If the locations of the bend-points must also be specified as part of the point-set, no result was known, and we prove that any planar graph with n vertices can be drawn on a universal set $\mathcal{S}$ of $O(n^2/\log n)$ points with at most one bend per edge and with the vertices and the bend points in $\mathcal{S}$. If two bends per edge are allowed, we show that $O(n \log n)$ points are sufficient, and if three bends per edge are allowed, $\Theta(n)$ points are sufficient. When no bends on edges are permitted, no universal point-set of size $o(n^2)$ is known for the class of planar graphs. We show that a set of n points in balanced biconvex position supports the class of maximum-degree-3 series-parallel lattices. These results were published this year in the journal *Computational Geometry: Theory and Application* [14].

We also considered the setting in which graphs are drawn with curved edges. We proved that, surprisingly, there exists a universal set of n points in the plane for which every n-vertex planar graph admits a planar drawing in which the edges are drawn as a circular arc. This result was presented in the *Canadian Conference on Computational Geometry* [17].

5.2. Non-linear computational geometry

Participants: Guillaume Moroz, Sylvain Lazard, Marc Pouget, Yacine Bouzidi, Laurent Dupont.

5.2.1. *Solving bivariate systems and topology of algebraic curves*

In the context of our algorithm Isotop for computing the topology of algebraic curves [4], we work on the problem of solving a system of two bivariate polynomials. We focus on the problem of computing a Rational Univariate Representation (RUR) of the solutions, that is, roughly speaking, a univariate polynomial and two rational functions which map the roots of the polynomial to the two coordinates of the solutions of the system.

Separating linear forms. We first presented an algorithm for computing a separating linear form of a system of bivariate polynomials with integer coefficients, that is a linear combination of the variables that takes different values when evaluated at distinct (complex) solutions of the system. In other words, a separating linear form defines a shear of the coordinate system that sends the algebraic system in generic position, in the sense that no two distinct solutions are vertically aligned. The computation of such linear forms is at the core of most algorithms that solve algebraic systems by computing rational parameterizations of the solutions and, moreover, the computation of a separating linear form is the bottleneck of these algorithms, in terms of worst-case bit complexity. Given two bivariate polynomials of total degree at most d with integer coefficients of bitsize at most τ, our algorithm computes a separating linear form in $\widetilde{O}_B(d^8 + d^7\tau)$ bit operations in the worst case, which decreases by a factor d^2 the best known complexity for this problem ($\widetilde{O}_B$ refers to the complexity where polylogarithmic factors are omitted and O_B refers to the bit complexity). This result was presented at the *International Symposium on Symbolic and Algebraic Computation* in 2013 [19] and submitted to a journal [23].

Solving bivariate systems & RURs. Given such a separating linear form, we also presented an algorithm for computing a RUR with worst-case bit complexity in $\widetilde{O}_B(d^7 + d^6\tau)$ and a bound on the bitsize of its coefficients in $\widetilde{O}(d^2 + d\tau)$. We showed in addition that isolating boxes of the solutions of the system can be computed from the RUR with $\widetilde{O}_B(d^8 + d^7\tau)$ bit operations. Finally, we showed how a RUR can be used to evaluate the sign of a bivariate polynomial (of degree at most d and bitsize at most τ) at one real solution of the system in $\widetilde{O}_B(d^8 + d^7\tau)$ bit operations and at all the $\Theta(d^2)$ real solutions in only $O(d)$ times that for one solution. These results were also presented at the *International Symposium on Symbolic and Algebraic Computation* in 2013 [18] and submitted to a journal [22].

This work is done in collaboration with Fabrice Rouillier (project-team Ouragan at Inria Paris-Rocquencourt).

5.2.2. *Reflection through quadric mirror surfaces*

We addressed the problem of finding the reflection point on a quadric mirror surfaces of a light ray emanating from a 3D point source P_1 and going through another 3D point P_2, the camera center of projection. This is a classical problem known as Alhazen's problem dating from around 1000 A.D. and based on the work of Ptolomy around 150 A.D. [31], [33]. We proposed a new algorithm for this problem based on our algorithm for the computation of the intersection of quadrics [7], [30] and using a characterization the reflection point as the tangential intersection point between the mirror and an ellipsoid with foci P_1 and P_2. The implementation is in progress. This work is done in collaboration with Nuno Gonçalves, University of Coimbra (Portugal).

5.2.3. *Fast polynomial evaluation and composition*

Evaluating a polynomial can be done with different evaluation schemes. The Hörner scheme for example allows to evaluate a polynomial of degree n in $O(n)$ arithmetic operations. When the cost of the arithmetic operations is constant, such as in floating point arithmetic, this leads to $O(n)$ binary operations. However, with integers, the size of the elements grows linearly after each multiplication and this may lead to $O(n^2)$ binary operations. This problem arises also with polynomial composition.

The best way to handle these cases is to use divide-and-conquer algorithms to keep a linear complexity in the degree up to logarithmic factors. State-of-the-art algorithms split at the highest pure power of 2 lower or equal to $\frac{n}{2}$. However when n is not a pure power of 2, this strategy might not be optimal.

We developed the library *fast_polynomial* to explore different divide-and-conquer schemes and observed notably that splitting at $\lfloor \frac{n}{2} \rfloor$ is more efficient in some cases. In particular, this evaluation scheme does not suffer the staircase effect observed in state-of-the-art evaluations. Experimentally, it is always faster than our own implementation of the classical divide-and-conquer scheme, and faster than the state of the art library *Flint 2* when the degree of the input polynomial is between 2^k and $2^k + 2^{k-1}$. These results are presented in the technical report [26].

5.3. Combinatorics and combinatorial geometry

Participant: Xavier Goaoc.

5.3.1. *Simplifying inclusion-exclusion formulas*

In a joint work with Jiří Matoušek, Pavel Paták, Zuzana Safernová, Martin Tancer (Charles University, Prague, Czech republic), we worked on computing simplified inclusion-exclusion formulas. Let $\mathcal{F} = \{F_1, F_2, ..., F_n\}$ be a family of n sets on a ground set S, such as a family of balls in $\mathbb{R}^d$. For every finite measure μ on S, such that the sets of $\mathcal{F}$ are measurable, the classical *inclusion-exclusion formula* asserts that $\mu(F_1 \cup F_2 \cup \cdots \cup F_n) = \sum_{I:\varnothing \neq I \subseteq [n]} (-1)^{|I|+1} \mu \left(\bigcap_{i \in I} F_i \right)$; that is, the measure of the union is expressed using measures of various intersections. The number of terms in this formula is exponential in n, and a significant amount of research, originating in applied areas, has been devoted to constructing simpler formulas for particular families $\mathcal{F}$. We provide an upper bound valid for an arbitrary $\mathcal{F}$: we show that every system $\mathcal{F}$ of n sets with m nonempty fields in the Venn diagram admits an inclusion-exclusion formula with $m^{O(\log^2 n)}$ terms and with ± 1 coefficients, and that such a formula can be computed in $m^{O(\log^2 n)}$ expected time. We also construct systems of n sets on n points for which every valid inclusion-exclusion formula has the sum of absolute values of the coefficients at least $\Omega(n^{3/2})$. This work was presented at the EUROCOMB conference [21] in September 2013.

5.3.2. *Helly numbers of acyclic families*

In a joint work with Éric Colin de Verdière (CNRS-ENS) and Grégory Ginot (IMJ-UPMC), we worked on applications of algebraic topology to combinatorial geometry, and more precisely on extending classical results on nerve complexes. The nerve complex of a family is an abstract simplicial complex that encode its intersection patterns. Nerves are widely used in computational geometry and topology, in particular in reconstruction problems where one aims at inferring the geometry of an object from a point sample while guaranteeing that the topology is correct. Indeed, the *nerve theorem* ensures that the nerve of a family of geometric objects has the same "topology" (formally: homotopy type) as the union of the objects whenever they form a "good cover", that is, when any subset of the objects has an empty or contractible intersection. We relaxed this "good cover" condition to allow for families of non-connected sets. We defined an analogue of the nerve, called the *multinerve*, that is suitable for general acyclic families, and we proved that this combinatorial structure enjoys an analogue of the nerve theorem. Using multinerve, we could derive a new *topological Helly-type theorem* for acyclic families that generalizes previous results of Amenta, Kalai and Meshulam, and Matoušek. We finally used this new Helly-type theorem to (re)prove, in a unified way, bounds on transversal Helly numbers in *geometric transversal theory*. This article was submitted to the journal *Advances in mathematics* in 2012; it was accepted in 2013 and will appear in 2014 [16].

5.3.3. *Set systems and families of permutations with small traces*

In a joint work with Otfried Cheong (KAIST, South Korea) and Cyril Nicaud (Univ. Marne-La-Vallée), we studied two problems of the following flavor: how large can a family of combinatorial objects defined on a finite set be if its number of distinct "projections" on any small subset is bounded? We first consider set systems, where the "projections" is the standard notion of trace, and for which we generalized Sauer's Lemma on the size of set systems with bounded VC-dimension. We then studied families of permutations, where the "projections" corresponds to the notion of containment used in the study of permutations with excluded patterns, and for which we delineated the main growth rates ensured by projection conditions. One of our motivations for considering these questions is the "geometric permutation problem" in geometric transversal

theory, a question that has been open for two decades. This work was submitted to the European Journal of Combinatorics in 2012 and published in 2013 [12].

VERIDIS Project-Team

6. New Results

6.1. Automated and Interactive Theorem Proving

6.1.1. *Using symmetries in SMT*

Participants: David Déharbe, Pascal Fontaine, Stephan Merz.

Joint work with Carlos Areces, Raúl Fervari, Guillaume Hoffmann, and Ezequiel Orbe at Universidad Nacional de Córdoba (see also section 8.2).

Methods exploiting problem symmetries have been very successful in several areas including constraint programming and SAT solving. We proposed similar techniques for enhancing the performance of SMT-solvers by detecting symmetries in the input formulas and using them to prune the search space of the SMT algorithm. These techniques are based on the concept of (syntactic) invariance by permutation of symbols. In 2011, we presented a technique restricted to constants but which exhibited impressive results for some categories of formulas [4]; this technique was quickly implemented in major SMT solvers, including CVC4 and Z3.

In 2013, we proposed, together with our colleagues at the University of Córdoba, Argentina, a more general approach to detect symmetries in an SMT context. These techniques are based on graph isomorphisms, and the Schreier-Sims algorithm for improving the presentation of the symmetries. This work was published at the SMT workshop 2013 [21].

6.1.2. *Computing minimal models (prime implicants)*

Participants: David Déharbe, Pascal Fontaine.

Joint work with Daniel Le Berre and Bertrand Mazure from the CRIL laboratory in Lens, France.

Model checking and counter-example guided abstraction refinement are examples of applications of SAT solving that require the production of models for satisfiable formulas. Instead of giving a truth value to every variable, it is usually preferable to provide an implicant, i.e. a partial assignment of the variables such that every full extension is a model for the formula. An implicant is *prime* if every assignment is necessary. Since prime implicants contain no literal irrelevant for the satisfiability of the formula, they are considered as highly refined information.

In 2013, we proposed a novel algorithm that uses data structures found in modern CDCL SAT solvers for efficiently computing prime implicants starting from an existing model. The original aspects are (1) the algorithm is based on watched literals and a form of propagation of required literals, adapted to CDCL solvers, (2) the algorithm works not only on clauses, but also on generalized constraints, and (3) for clauses (and more generally, for cardinality constraints) the complexity of the algorithm is linear in the size of the constraints. We implemented and evaluated the algorithm with the Sat4j library. This work gave rise to a publication at the FMCAD 2013 international conference [13].

6.1.3. *Encoding TLA+ proof obligations for SMT solvers*

Participants: Stephan Merz, Hernán Vanzetto.

The TLA$^+$ proof system TLAPS (see section 5.2) is being developed within a project at the MSR-Inria Joint Centre to which we contribute. Typical proof obligations that arise during the verification of TLA$^+$ specifications mix reasoning about sets, functions, arithmetic, tuples, and records. In previous work [47], we have developed translations from TLA$^+$ set theory to SMT-Lib, the standard input language of SMT solvers. The main challenge has been to design a sound translation from untyped TLA$^+$ to the multi-sorted first-order logic that underlies SMT-Lib. Our solution is based on an incomplete type inference based on "typing hypotheses" present in TLA$^+$ proof obligations. When type inference fails, we fall back to an "untyped" encoding where interpreted sorts such as integers are injected into a designated sort of TLA$^+$ values, and proof obligations corresponding to well-sortedness conditions must be discharged during the proof.

In 2013, we have stabilized and extended the type inference, based on a more expressive type system that includes dependent types, predicate types, and subtyping. The new type system is able to solve many more typing conditions during the translation of proof obligations and thus improves both the scope and the efficiency of the SMT backend. It has been implemented as part of the SMT backend of TLAPS, and an article describing the type system has been submitted. A full description will appear in the PhD thesis of Hernán Vanzetto, expected to be defended in early 2014.

6.1.4. *Formalization of stuttering invariance in temporal logic*
Participant: Stephan Merz.

Extending our previous formalization in the interactive proof assistant Isabelle/HOL of the concept of stuttering invariance, we formally proved that a property expressible in propositional temporal logic is stuttering invariant if and only if it is equivalent to a formula using only the *until* temporal operator (and in particular not the *next-time* operator). The formalization follows the proof in the classical paper by Peled and Wilke [49]. It allowed us to uncover and correct an error in the proof that had previously not been known. The corresponding extended version of the Isabelle proof development has been accepted at the Archive of Formal Proofs.

6.1.5. *Superposition modulo theories*
Participants: Noran Azmy, Christoph Weidenbach.

We are currently in a transition phase moving SPASS from a first-order logic prover to a first-order logic prover over theories SPASS(T), in particular arithmetic. Our experience in combining SPASS with interactive verification systems such as TLAPS or Isabelle shows that this is a mandatory step in improving automation [46], [34]. Meanwhile we have built the theoretical foundations [41], [40], [43] for combining superposition with theories which we now turn into algorithmic solutions. This makes an overall reimplementation of SPASS necessary. As a first step we reimplemented and improved our clause normal form transformation [11].

In particular, we want to support integer theories and modulo reasoning [15], as it is often used in distributed algorithms [46]. We have built first implementations of arithmetic modules which we want to combine in 2014 to a first version of SPASS(T).

6.1.6. *Presburger Arithmetic in Compiler Optimization*
Participants: Marek Košta, Thomas Sturm.

One of our focuses in 2013 was the application of SMT-solvers in new and different problem areas. We started a fruitful cooperation with the Compiler Lab at the Saarland University, Germany on compilation of data-parallel languages.

Data-parallel languages like OpenCL and CUDA are an important means to exploit the parallel computational capabilities of today's computing devices. However, the historical development of data-parallel languages stemming from GPUs plays a crucial role when compiling them for a SIMD (Single Instruction Multiple Data) CPU: on the CPU, one has to emulate dynamic features that on GPU are implemented in the hardware. This difference gives rise to several problems that have to be dealt with during the compilation process.

Our work [15] considers compilation of OpenCL programs for CPUs with SIMD instruction sets. It turns out that SMT-solvers can be used to generate more efficient CPU code. The lack of some dynamic features on CPU implies that one wants to statically decide whether or not certain memory operations access consecutive addresses. Our approach formalizes the notion of consecutivity and algorithmically reduces the static decision to satisfiability problems in Presburger Arithmetic. This is where SMT-solvers come into play. To make an application of an off-the-shelf SMT solver feasible, a preprocessing technique on the SMT problems was introduced. Combining three different systems (computer algebra system REDLOG, SMT-solver Z3, and an OpenCL driver developed in the Compiler Lab), a proof-of-concept system based on our approach was developed. The system generated more efficient code than any other state-of-the-art OpenCL compiler.

Further development is needed to turn the proof-of-concept system mentioned above into one integrated software system. To achieve this, the redundant combination of three heterogeneous systems needs to be replaced by a coherent library offering the same functionality. The work [23] presents the development of such a novel library. The library provides functions to fully automatize the approach proposed in the previous work. It is capable of parallel computations by means of threads and processes and uses an SMT-solver library to carry out the needed computations. To create the final system, the integration of the library with the OpenCL driver needs to be done. This final step is left for future work.

6.1.7. *Non-Linear SMT-Solving*

Participants: Marek Košta, Thomas Sturm.

In [42] de Moura and Jovanović give a novel satisfiability procedure for the theory of the reals. The procedure uses DPLL-style techniques to search for a satisfying assignment. In case of a conflict, cylindrical algebraic decomposition (CAD) [38] is used to guide the search away from the conflicting state: on the basis of one conflicting point, the procedure learns to avoid in the future an entire CAD cell containing the point. The function realizing this learning is the crucial ingredient that makes the DPLL-style search possible at all. Unfortunately, it is the main computational bottleneck of the whole procedure.

The work of Brown [35] develops a more efficient learning function for the case when the cell to-be learned is full-dimensional. In collaboration with Prof. Brown (United States Naval Academy, USA), we extend this to the general case. While restricting to one cell is quite straightforward for the base and lifting phases of a CAD algorithm, our approach is able to optimize the projection phase as well. This requires a thorough analysis of available geometric infomation and properties of the involved projection operator. Our cell construction algorithm is able to produce bigger cells and it is faster than the approach used in [42]. Both of these are benefits, because a bigger cell means a better generalization of the conflicting assignment. Prototypical implementation of our cell construction algorithm gives very promising results on various kinds of problems. Its elaborate implementation and integration with an DPLL engine within the computer algebra system REDLOG is left for future work. A publication has been submitted to the Journal of Symbolic Computation.

6.1.8. *Towards Tropical Decision for NLA*

Participant: Thomas Sturm.

Inspired by problems related to stability analysis of chemical reaction networks we have developed an incomplete decision procedure for satisfiability in nonlinear real arithmetic. A first implemented version focuses on specific situations where all variables are known to be strictly positive, which naturally occurs in many scientific contexts. Furthermore, only one single equation is considered. The principal *tropical* approach is, after reducing the problem to finding a point with positive value for f in the considered equation $f = 0$, to consider instead of f only the exponent tuples of the contained summands as points in $\mathbb{Z}^n$. On that basis dominating summands can be identified using LP techniques.

In our particular application discussed in [14], we were able to solve problems, which are intractable even by numerical methods: Typical input equations had around 6000 summands and up to seven variables of degrees between 4 and 9. The methods failed in only 3 percent of the 496 considered input problems.

We are currently generalizing the approach to the general case where variables can have arbitrary values. Furthermore, as it is well known that every existential decision problems over the reals can be equi-satisfiably encoded into one equation, we are aiming at a corresponding general procedure as a long-term research goal.

6.1.9. *Hierarchical superposition for arithmetic*

Participant: Uwe Waldmann.

Many applications of automated deduction require reasoning in first-order logic modulo background theories, in particular some form of integer arithmetic. A major unsolved research challenge is to design theorem provers that are "reasonably complete" even in the presence of free function symbols ranging into a background theory sort. The hierarchic superposition calculus of Bachmair, Ganzinger, and Waldmann already supports such symbols, but not optimally. We have introduced a novel form of clause abstraction, a core component in the hierarchic superposition calculus for transforming clauses into a form needed for internal operation. We have also demonstrated that hierarchic superposition is refutationally complete for linear integer or rational arithmetic, even if one considers the standard model semantics rather than the first-order semantics, provided that all background-sorted terms in the input are either ground or variables (variables with integer offsets can be permitted in certain positions).

6.2. Proved development of algorithms and systems

6.2.1. *Incremental development of distributed algorithms*

Participants: Dominique Méry, Manamiary Andriamiarina.

Joint work with Mohammed Mosbah and Mohammed Tounsi from the LABRI laboratory in Bordeaux, France.

The development of distributed algorithms and, more generally, of distributed systems, is a complex, delicate, and challenging process. The approach based on refinement helps to gain formality by using a proof assistant, and proposes to apply a design methodology that starts from the most abstract model and leads, in an incremental way, to the most concrete model, for producing a distributed solution. Our work helps formalizing pre-existing algorithms, developing new algorithms, as well as developing models for distributed systems.

Our research was initially supported by the ANR project RIMEL (see http://rimel.loria.fr). More concretely, we aim at an integration of the correct-by-construction refinement-based approach into the *local computation* programming model. The team of LABRI develops an environment called VISIDIA (http://visidia.labri.fr) that provides a toolset for developing distributed algorithms expressed as a set of rewriting rules of graph structures. The simulation of rewriting rules is based on synchronization algorithms, and we have developed these algorithms by refinement [20].

In particular, we show how state-based models can be developed for specific problems and how they can be simply reused by controlling the composition of state-based models through the refinement relationship. Traditionally, distributed algorithms are supposed to run on a fixed network, whereas we consider a network with a changing topology.

The contribution is related to the development of proof-based patterns providing effective help to the developer of formal models of applications [10]. Our patterns simplify the development of distributed systems using refinement and temporal logic. Moreover, we have especially evaluated the extension of the scope of Event B by proposing a technique for integrating fairness in the development of distributed algorithms [17].

6.2.2. *Modeling Medical Devices*

Participant: Dominique Méry.

Formal modelling techniques and tools have attained sufficient maturity for formalizing highly critical systems in view of improving their quality and reliability, and the development of such methods has attracted the interest of industrial partners and academic research institutions. Building high quality and zero-defect medical software-based devices is a particular domain where formal modelling techniques can be applied effectively. Medical devices are very prone to showing unexpected system behaviour in operation when traditional methods are used for system testing. Device-related problems have been responsible for a large number of serious injuries. Officials of the US Food and Drug Administration (FDA) found that many deaths and injuries related to these devices are caused by flaws in product design and engineering. Cardiac pacemakers and implantable cardioverter-defibrillators (ICDs) are among the most critical medical devices and require closed-loop modelling (integrated system and environment modelling) for verification purposes before obtaining a certificate from the certification bodies.

Clinical guidelines systematically assist practitioners in providing appropriate health care in specific clinical circumstances. Today, a significant number of guidelines and protocols are lacking in quality. Indeed, ambiguity and incompleteness are likely anomalies in medical practice. The analysis of guidelines using formal methods is a promising approach for improving them.

In [9], we propose a refinement-based methodology for complex medical systems design, which possesses all the required key features. A refinement-based combined approach of formal verification, model validation using a model-checker and refinement chart is proposed in this methodology for designing a high-confidence medical device. Furthermore, we show the effectiveness of this methodology for the design of a cardiac pacemaker system.

Inappropriate mode transitions can be a common cause of mishaps in complex health-care systems. In [19], we present an approach for formalizing and reasoning about optimal mode transition in a health-care system that uses several operating modes in various operating states. Modes are formalized and their relation to a state-based formalism is established through a refinement approach. The efficiency of this approach is presented by formalizing an ideal operating mode transition of a cardiac pacemaker case study. An incremental approach is used to develop the system and its detailed design is verified through a series of refinements. In this way, we show how to improve system structuring, elicitation of system assumptions and expected functionality, as well as requirement traceability using modes in state-based modeling. Models are expressed in the Event B [25] modeling language, and they are validated by the model checker ProB.

Finally, in a joint work with colleagues of the CRAN laboratory in Nancy, we have completed a joint project with Airbus on the integration of physiological features in the development of systems like maintenance systems.

6.2.3. *Analysis of real-time Java programs*
Participants: Jingshu Chen, Marie Duflot-Kremer, Pascal Fontaine, Stephan Merz.

Joint work with Nadezhda Baklanova, Jan-Georg Smaus, Wilmer Ricciotti, and Martin Strecker at IRIT Toulouse, France, funded by EADS Foundation (see also section 7.1).

We investigate techniques for the formal verification of programs written in a dialect of Java that includes real-time annotations. Inspired by Safety-Critical Java [36], our partners in Toulouse developed a formal semantics for that dialect in Isabelle/HOL. In joint work, we have designed translations of programs to respectively timed automata and to SMT-Lib for analysis with the Uppaal model checker and with SMT solvers. We are evaluating the features and the scalability of the two approaches, and also plan to formally prove the soundness of the translations based on the semantics formalized in Isabelle.

6.2.4. *Fundamentals of Network Calculus in Isabelle/HOL*
Participant: Stephan Merz.

Joint work with Marc Boyer from ONERA (Toulouse, France) and Loïc Fejoz, Etienne Mabille and Nicolas Navet from RealTime at Work (RTaW, Nancy).

Network Calculus [45] is a well-established theory for the design and analysis of embedded networks. Based on the $(\min, +)$ dioid, it allows a network designer to compute upper bounds for delay and buffer sizes in networks. The theory is supported by several commercial and open-source tools and has been used in major industrial applications, such as the design and certification of the Airbus A380 AFDX backbone. Nevertheless, it is difficult for certification authorities to assess the correctness of the computations carried out by the tools supporting Network Calculus, and we propose the use of *result certification* techniques for increasing the confidence in the Network Calculus toolchain. We have formalized parts of the theory underlying Network Calculus in the proof assistant Isabelle/HOL. We have also developed a prototype analyzer that outputs traces of its computations so that they can be certified using Isabelle. Our work has been published at the conferences EUCASS and ITP [16], [24], and we have submitted a project proposal to ANR together with ONERA, RTaW, Kalray, Eurocopter, and Astrium. Unfortunately, the project was not granted, and future work on this promising subject is on hold.

6.2.5. *Modeling and verifying the Pastry routing protocol*

Participants: Tianxiang Lu, Stephan Merz, Christoph Weidenbach.

As a significant case study for the techniques that we are developing within VeriDis, we are modeling and verifying the routing protocol of the Pastry algorithm [37] for maintaining a distributed hash table in a peer-to-peer network. As part of his PhD work, Tianxiang Lu developed a TLA$^+$ model of the Pastry routing protocol, and has uncovered several problems in the existing presentations of the protocol in the literature that could lead to network partitioning.

He proposed a novel variant of the protocol and proved its correctness under the strong assumption that no nodes leave the network, using TLAPS (see section 5.2). He also demonstrated that the protocol could not work if arbitrary nodes are allowed to leave; it is not clear at this point under what reasonable assumptions the protocol can be made to work. The correctness proofs contain almost 15000 interactions and constitutes the largest case study carried out so far using TLAPS. Tianxiang Lu defended his thesis at the end of November 2013; a journal publication describing this work is in preparation.

6.2.6. *Bounding message length in attacks against security protocols*

Participant: Marie Duflot-Kremer.

Joint work with Myrto Arapinis from the University of Birmingham, UK.

Security protocols are short programs that describe communication between two or more parties in order to achieve security goals. Despite the apparent simplicity of such protocols, their verification is a difficult problem and has been shown to be undecidable in general. This undecidability comes from the fact that the set of executions to be considered is of infinite depth (an infinite number of protocol sessions can be run) and infinitely branching (the intruder can generate an unbounded number of distinct messages). Several attempts have been made to tackle each of these sources of undecidability. We have shown [30] that, under a syntactic and reasonable condition of "well-formedness" on the protocol, we can get rid of the infinitely branching part. Following this conference publication, we have submitted a journal version of this result extending the set of security properties to which the result is applicable, in particular including authentication properties.

6.2.7. *Evaluating and verifying probabilistic systems*

Participant: Marie Duflot-Kremer.

Joint work with colleagues at ENS Cachan and University Paris Est Créteil.

Since its introduction in the 1980s, model checking has become a prominent technique for the verification of complex systems. The aim was to decide whether or not a system was fulfilling its specification. With the rise of probabilistic systems, new techniques have been designed to verify this new type of systems, and appropriate logics have been proposed to describe more subtle properties to be verified. However, some characteristics of such systems cannot fall in the field of model checking. The aim is thus not to tell wether a property is satisfied but how well the system performs with respect to a certain measure. We have designed a statistical tool for tackling both performance and verification issues. Following several conference talks, two journal papers have been written. The first one presents the approach in details with a few illustrative applications. The second one focuses on biological application, and more precisely the use of statistical model checking to detect and measure several indicators of oscillating biological systems.

CALVI Project-Team

6. New Results

6.1. Software development

6.1.1. New methods in Selalib

The Selalib library has seen important developments during the year 2013 as we move towards a release in 2014. Several existing modules were improved in terms of their interfaces or implementations, while many other modules were added. Notably, we have improved our interaction with external software (Pigasus, developed by Dr. Ahmed Ratnani) capable of producing NURBS-based coordinate transformations and introduced a general elliptic PDE solver based on finite elements and arbitrary degree splines that can be used as a field solver in domains deformed by an arbitrary coordinate transformation. Preliminary results of these developments have been published [2]. In addition, we have included new abstractions to facilitate the development of parallel codes using domain decomposition methods. Modules like these have been already used in some of the multiple pre-packaged simulations also included during this period. For instance, it allows us to implement a new Vlasov-Poisson solver by the Eulerian reduced approach, with applications to four-dimensional Landau-Damping. The latest simulations also use newly developed interfaces related with the semi-lagrangian methodology, such as generic interfaces for advections and calculation of characteristics. At the end of 2013 virtually all conceivable abstractions related with the semi-lagrangian methodology have a natural place to live within the library.

Many new and classical methods and models have been cleanly incorporated into our software Selalib:

- Vlasov-Poisson solver by the Eulerian reduced approach. Application to 4D Landau-Damping.
- cartesian semi-Lagrangian 2D guiding center sequential simulation tested on periodic Kelvin Helmholtz instability
- polar semi-Lagrangian 2D guiding center sequential simulation tested on diocotron instability
- general curvilinear semi-Lagrangian 2D guiding center sequential simulation; first results, still in progress
- cartesian semi-Lagrangian 2D Vlasov-Poisson parallel simulation with high order splitting tested on Landau damping, bump on tail, two stream instability and beam
- cartesian semi-Lagrangian 2D Vlasov-Poisson sequential simulation without splitting tested on beam
- cartesian semi-Lagrangian 4D Vlasov-Poisson parallel simulation on cartesian grid with high order splitting tested on Landau-Damping
- polar semi-Lagrangian 4D drift kinetic parallel simulation tested on a simple ITG instability
- general curvilinear semi-Lagrangian 4D drift kinetic parallel simulation (in development)

6.1.2. New developments in CLAC

CLAC is a generic DG solver for hyperbolic conservation laws. It is optimized for running efficiently on GPU clusters. We have reorganized the software conception in order to accelerate the computations. A first point is to group the finite-elements into uniform zones in order to get optimized kernels for SIMD architectures. A second point is to manage efficiently the data transfers between the zone. An important last point is to consider a non blocking parallel task management. This is achieved through a coupling between the event mechanisms of OpenCL and MPI. Some ideas and results are presented in [44]. In addition to these developments, we have started to test some parallel programming approaches in order to achieve good efficiency on multicore processors. These ideas have been tested on fluid models [27] and the MHD model [47]. They are very efficient and will be incorparated into CLAC later on.

---

[2] A. Back, E. Chacon-Golcher, V. Grandgirard, A. Ratnani, E. Sonnendrücker, A 4D semi-Lagrangian Vlasov solver based on an arbitrary curvilinear grid in physical space, poster at Vlasovia, 25-28 November 2013, Nancy

6.2. Mathematical analysis of kinetic models

Participants: N. Besse, M. Bostan.

Contribution [13] concerns a one-dimensional version of the Vlasov equation dubbed the Vlasov-Dirac-Benney equation (in short V-D-B) where the self interacting potential is replaced by a Dirac mass. Emphasis is put on the relations between the linearized version, the full nonlinear problem and equations of fluids. In particular the connection with the so-called Benney equation leads to new stability results. Eventually the V-D-B appears to be at the cross road of several problems of mathematical physics which have as far as stability is concerned very similar properties.

The subject matter of paper [3] concerns anisotropic diffusion equations: we consider heat equations whose diffusion matrices have disparate eigenvalues. We determine first and second order approximations, we study their well-posedness and then, we establish convergence results. The analysis relies on averaging techniques, which have been used previously for studying transport equations whose advection fields have disparate components.

In [4] we perform an asymptotic analysis of general particle systems arising in collective behavior in the limit of large self-propulsion and friction forces. These asymptotics impose a fixed speed in the limit, and thus a reduction of the dynamics to a sphere in the velocity variables. The limit models are obtained by averaging with respect to the fast dynamics. We can include all typical effects in the applications: short-range repulsion, long-range attraction, and alignment. For instance, we can rigorously show that the Cucker-Smale model is reduced to the Vicsek model without noise in this asymptotic limit. Finally, a formal expansion based on the reduced dynamics allows us to treat the case of diffusion. This technique follows closely the gyroaverage method used when studying the magnetic confinement of charged particles. The main new mathematical difficulty is to deal with measure solutions in this expansion procedure.

6.2.1. Gyrokinetic approximation

Participants: E. Frénod, M. Lutz.

Considering a Hamiltonian Dynamical System describing the motion of charged particle in a Tokamak or a Stellarator, we build in [42] a change of coordinates to reduce its dimension. This change of coordinates is in fact an intricate succession of mappings that are built using Hyperbolic Partial Differential Equations, Differential Geometry, Hamiltonian Dynamical System Theory and Symplectic Geometry, Lie Transforms and a new tool which is here introduced : Partial Lie Sums.

6.3. Development of semi-Lagrangian methods

Participants: N. Crouseilles, P. Glanc, A. Hamiaz, S. Hirstoaga, M. Mehrenberger, J. Petri, E. Sonnendrücker, C. Steiner.

The development of numerical methods - here semi-Lagrangian schemes for plasma physic applications- is continued and strengthened in the context of the on-going library Selalib. We intend to improve the robustness of the numerical tools in order to be prepared for future more realistic test problems.

6.3.1. Vlasov-Poisson simulations on cartesian grids

We have developed a 1D x 1D Vlasov-Poisson solver on GPU using optimized FFT of CUDA and applied it on KEEN waves test case, which needs a fine resolution in velocity [46]. An efficiency of 100 Gflops on 4096x4096 grid is obtained while using single precision, and about 30 GFlops on a 2048x3048 grid using double precision. The approach is valid: implementation effort is reduced, because we rely on external optimizations and the speed-up is quite impressive (only 1 or 2 GFlops were obtained using CPU). We emphasize that FFT is used for the implementation but not (necessarily) for the numerical method. Classical methods like splines or arbitrary high order odd Lagrange interpolation are used, as they can be fitted in

---

[3]M. Bostan, Strongly anisotropic diffusion problems; asymptotic analysis, in *J. Differential Equations*, vol. 256 pp. 1043-1092 (2013)

[4]M. Bostan, J.-A. Carrillo, Asymptotic fixed speed reduced dynamics for kinetic equations in swarming, *Math. Models Methods Appl. Sci.*, Vol.23, No. 13 pp. 2353-2393 (2013)

this framework. In order to reduce mass conservation issues while using single precision, a delta-f method is validated. The limitation is here the grid size; we were not able to run the code for bigger sizes. We then developed other strategies based on non uniform grids in velocity with cubic splines and two grid strategies [5] and with the semi-Lagrangian discontinuous Galerkin (SLDG) scheme [6]. Integration of the code in Selalib with upgraded interface to deal with non uniform grids has been thought but remains to be done. Thanks to the MPI Parallelization of the Selalib code, we should be able to run the code for more interesting physical parameters, in particular, when the drive amplitude goes to zero, which leads to even more localized delta-f function in velocity.

Considering the SLDG scheme, we were able to prove a super convergence property in the case of constant linear advection [48].

6.3.2. *Guiding-center based simulations on polar grids*

We continue our work on polar grids, which are intermediate, between cartesian and general curvilinear grids. We have revisited a diocotron simulation previously done with the PIC method [75] by using a (classical) semi-Lagrangian approach. A detailed study of boundary conditions, energy and mass conservation as well as linear growth rates is performed and validated with teh code [33]. We then have extended the code to a first drift kinetic simulation [7] using at first the classical cubic splines method and then a new 2D conservative method, called CSL2D (conservative semi-Lagrangian 2D), based on mesh intersections and displacement of volumes [11]. For the latter method to work, we had to take care of the Jacobian and we used a delta-f method, in order to treat more easily non zero boundary conditions. We have benefitted from previous experience on the FSL2D (forward semi-Lagrangian) method. Again, the integration in Selalib is under development. Linear growth rate is here validated, by solving numerically the dispersion relation using recent results of [21].

6.3.3. *Guiding-center simulations on general curvilinear grids*

In order to deal with more complex geometries or to consider field aligned coordinates, we work on generalizing existing methods for curvilinear grids. Guiding center simulations have been successfully performed with the classical cubic splines method and a finite element solver for the Poisson equation developed by A. Back [32]. Further works concern integration in Selalib, in a more modular way. This should help the comparison with other methods as for example the recent CSL2D method [11] but also the previous CSL1D method [5].

6.4. Development of reduced Eulerian methods

Participants: E. Chacon Golcher, P. Helluy, L. Navoret, N. Pham.

6.4.1. *Eulerian methods in the physical phase-space*

Kinetic plasmas computer simulations are very intensive, because of the gyrokinetic turbulence. In some situations, it is possible to make assumptions on the shape of the distribution function that simplify the model. We obtain in this way a family of fluid or reduced models.If the distribution function has a Maxwellian shape (strong collisions), we obtain the MagnetoHydroDynamic (MHD) model. Even without collisions, the plasma may still relax to an equilibrium state over sufficiently long time scales (Landau damping effect). This indicates that the approximation of the distribution function could require fewer data while still achieving a good representation, even in the collisionless regime. In what follows we call this the "reduced model" approach. A reduced model is a model where the explicit dependence on the velocity variable is suppressed. In a more mathematical way, we consider that in some regions of the plasma, it is possible to exhibit a (preferably small) set of parameters α that allows us to describe the main properties of the plasma with a generalized

---

[5]M. Mehrenberger, N. Crouseilles, E. Sonnendrücker, B. Afeyan High-Order Numerical Methods for KEEN Wave Vlasov-Poisson Simulations, Poster at PPPS, 16-21 June 2013, San Francisco

[6]C. Steiner, M. Mehrenberger, A semi-Lagrangian discontinuous Galerkin scheme for Vlasov-Poisson equation, poster at Vlasovia, 25-28 November 2013, Nancy

[7]N. Crouseilles, P. Glanc, S. Hirstoaga, E. Madaule, M. Mehrenberger, J. Pétri, Semi-Lagrangian simulations on polar grids: from diocotron instability to ITG turbulence, poster at Vlasovia, 25-28 November 2013, Nancy

"Maxwellian" M . Then $f(x, v, t) = M(\alpha(x, t), v)$. In this case it is sufficient to solve for $\alpha(x, t)$. Generally, the vector α is solution of a first order hyperbolic system.

Several approaches are possible that we have started to study theoretically and numerically: waterbag approximations, velocity space transforms, etc.

It is also possible to construct in this way intermediate models between the kinetic and the fluid models by truncating the velocity expansion. The unknowns α of the problem become the coefficients of the expansion, which depend only on space and time. They obey a first order hyperbolic PDE system. And then it is possible to capitalize on the large theoretical and numerical machinery developed for such PDEs.

A first step is to develop the one-dimensional models in order to test several numerical methods. The chosen approach is the high order Discontinuous Galerkin (DG) family of methods for solving the hyperbolic system. We compare the reduced Eulerian model with semi-Lagrangian or PIC methods on classical test cases: Landau damping, two-stream instability [28].

6.4.2. Eulerian method in the Fourier transformed phase-space

An experiment made in the 60's [8] exhibits in a spectacular way the reversible nature of the Vlasov equations. When two perturbations are applied to a plasma at different times, at first the plasma seems to damp and reach an equilibrium. But the information of the perturbations is still here and "hidden" in the high frequency microscopic oscillations of the distribution function. At a later time a resonance occurs and the plasma produces an echo. The time at which the echo occurs can be computed (see Villani[9], page 74). The fine mathematical study of this phenomenon allowed C. Villani and C. Mouhot to prove their famous result on the rigorous nonlinear Landau damping[10].

More practically, this experiment and its theoretical framework show that it is interesting to represent the distribution function by an truncated expansion on an orthonormal basis of oscillating functions in the velocity variables. This representation allows a better control of the energy transfer between the low frequencies and the high frequencies in the velocity direction, and thus provides more relevant numerical methods. This kind of approach is studied for instance by Eliasson [11].

We have started to study such kind of approaches in [43]. An interesting point is that the truncated reduced model is also an hyperbolic system in the space direction only. This allows the classical methods for hyperbolic systems to be reused.

6.5. Two-Scale numerical methods

Participant: E. Frénod.

In note [39] a classification of Homogenization-Based Numerical Methods and (in particular) of Numerical Methods that are based on the Two-Scale Convergence is done. In this classification stand: Direct Homogenization-Based Numerical Methods, H-Measure-Based Numerical Methods, Two-Scale Numerical Methods and TSAPS (Two-Scale Asymptotic Preserving Schemes).

In [34] we develop and we explain the two-scale convergence in the covariant formalism, i.e. using differential forms on a Riemannian manifold. For that purpose, we consider two manifolds M and Y, the first one contains the positions and the second one the oscillations. We establish some convergence results working on geodesics on a manifold. Then, we apply this framework on examples.

6.6. Spline Discrete Differential Forms and applications

Participant: E. Sonnendrücker.

---

[8]Malmberg, J. and Wharton, C. Collisionless damping of electrostatic plasma waves. Phys. Rev. Lett. 13, 6 (1964), 184–186.

[9]Villani, C. Landau damping. CEMRACS 2010 lectures.

[10]Mouhot, C. ; Villani, C. On Landau damping, Acta Mathematica 207 (September 2011), 29-201.

[11]Eliasson, B. Outflow boundary conditions for the Fourier transformed one-dimensional Vlasov-Poisson system. J. Sci. Comput. 16 (2001), no. 1, 1–28.

In [36] we construct a new set of discrete differential forms based on B-splines of arbitrary degree as well as an associated Hodge operator. The theory is first developed in 1D and then extended to multi-dimension using tensor products. We link our discrete differential forms with the theory of chains and cochains. The spline discrete differential forms are then applied to the numerical solution of Maxwell's equations.

The notion of B-spline based discrete differential forms is recalled and along with a Finite Element Hodge operator, it is used in [35] to design new numerical methods for solving the Vlasov-Poisson equations.

6.7. Simulations of highly oscillatory Vlasov-Poisson system

Participants: E. Frénod, S. Hirstoaga, M. Lutz, E. Sonnendrücker.

In paper [45] a Lie Transform method is applied for a charged beam under the action of a radial external electric field. The aim of the Lie transform method that is used here is to construct a change of variable which transforms the 2D kinetic problem into a 1D problem. This reduces the dimensionality of the problem and make it easier to solve numerically.

In paper [41], in the framework of a Particle-In-Cell scheme for some 1D Vlasov-Poisson system depending on a small parameter, we propose a time-stepping method which is numerically uniformly accurate when the parameter goes to zero. Based on an exponential time differencing approach, the scheme is able to use large time steps with respect to the typical size of the fast oscillations of the solution.

6.8. Waterbag models: analysis and simulations

Participant: N. Besse.

Ion temperature gradient instabilities play a major role in the understanding of anomalous transport in core fusion plasmas. In the considered cylindrical geometry, ion dynamics is described in [20] using a drift-kinetic multi-water-bag model for the parallel velocity dependency of the ion distribution function. In a first stage, global linear stability analysis is performed. From the obtained normal modes, parametric dependencies of the main spectral characteristics of the instability are then examined. Comparison of the multi-water-bag results with a reference continuous Maxwellian case allows us to evaluate the effects of discrete parallel velocity sampling induced by the Multi-Water-Bag model. Differences between the global model and local models considered in previous works are discussed. Using results from linear, quasilinear, and nonlinear numerical simulations, an analysis of the first stage saturation dynamics of the instability is proposed, where the divergence between the three models is examined.

In paper [21] we present two new codes devoted to the study of ion temperature gradient (ITG) driven plasma turbulence in cylindrical geometry using a drift-kinetic multi-water- bag model for ion dynamics. Both codes were developed to complement the Runge–Kutta semi-lagrangian multi-water-bag code GMWB3D-SLC described in [1]. The CYLGYR code is an eigenvalue solver performing linear stability analysis from given mean radial profiles. It features three resolution schemes and three parallel velocity response models (fluid, multi-water-bag, continuous Maxwellian). The QUALIMUWABA quasilinear code is an initial value code allowing the study of zonal flow influence on drift-waves dynamics. Cross-validation test performed between the three codes show good agreement on both temporal and spatial characteristics of unstable modes in the linear growth phase.

6.9. Full wave modeling of lower hybrid current drive in tokamaks

Participants: Takashi Hattori, Simon Labrunie, Jean R. Roche.

This work is performed in collaboration with Yves Peysson (DRFC, CEA Cadarrache). Since September 2012 this work is included in the ANR CHROME.

The aim of this project is to develop a finite element numerical method for the full-wave simulation of electromagnetic wave propagation in plasma. Full-wave calculations of the LH wave propagation is a challenging issue because of the short wave length with respect to the machine size. In the continuation of the works led in cylindrical geometry , a full toroidal description for an arbitrary poloidal cross-section of the plasma has been developed.

Since its wavelength λ at the LH frequency is very small as compared to the machine size R, a conventional full wave description represents a considerable numerical effort.Therefore, the problem is addressed by an appropriate mathematical finite element technique, which incorporates naturally parallel processing capabilities. It is based on a mixed augmented variational (weak) formulation taking account of the divergence constraint and essential boundary conditions, which provides an original and efficient scheme to describe in a global manner both propagation and absorption of electromagnetic waves in plasmas.

With such a description, usual limitations of the conventional ray tracing related to the approximation $\lambda \ll \phi_B \ll R$, where ϕ_B is the size of the beam transverse to the rf power flow direction, may be overcome. Since conditions are corresponding to $\lambda \ll \phi_B \sim R$, the code under development may be considered as a WKB full wave, dielectric properties being local.

This formulation provides a natural implementation for parallel processing, a particularly important aspect when simulations for plasmas of large size must be considered.

The domain considered is as near as possible of the cavity fill by a tokomak plasma. Toroidal coordinates are introduced. In our approach we consider Fourier decomposition in the angular coordinate to obtain stationary Maxwell equations in a cross-section of the tokamak cavity.

A finite element method is proposed for the simulation of time-harmonic electromagnetic waves in a plasma, which is an anisotropic medium. The approach chosen here is sometimes referred to as *full-wave modeling* in the literature: the original Maxwell's equations are used to obtain a second order equation for the time-harmonic electric field. These are written in a weak form using a augmented variational formulation (AVF), which takes into account the divergence. The variational formulation is then discretized using modified Taylor-Hood (nodal) elements.

The analyze of the model considered, existence and unicity of solution, equivalence of the formulation for the domain decomposition formulation was completed in the frame of Takashi Hattori Phd thesis.

During 2013 we continue to develop the domain decomposition method introduced in 2012 and a new preconditioned system was considered in the code "FullWaveFEM", [31].

6.10. Eulerian simulations of parallel transport in the SOL

Participants: S. Hirstoaga, G. Manfredi.

During the year 2013, we have progressed in the implementation of an asymptotic preserving (AP) Eulerian Vlasov code (VESPA: Vlasov Eulerian Simulator of PArallel transport) for the study of parallel transport in the scrape-off layer of tokamaks. An AP Vlasov-Poisson code had already been partially developed for the quasi-neutral regime. In this case the small parameter is the Debye length λ (normalized to the parallel connection length). The Poisson equation becomes singular when $\lambda \to 0$: the AP solution consists in reformulating Poisson's equation in a way that is no longer singular in this limit. In theory, any value of λ can be used, including $\lambda = 0$, without numerical instability and without any constraint on the grid spacing and time-step. In practice, we have observed a CFL stability condition (although not very restrictive) and a limit on the smallness of λ. During the past year, we have performed systematic tests on the code, which is now capable of attaining very small values of λ, down to 10^{-4} or even lower. Meaningful results can be obtained with just 1-2 hours of computation on a standard desktop computer (see for example [29]).

The next upgrade of the VESPA code concerns the modelling of collisions, which have been implemented through a relaxation (BGK) term that also retains the possibility to include ionization and recombination in the model. The BGK term has been tested and validated against analytical results. In particular, the AP scheme had to be modified in order to correctly treat the BGK term. These upgrades are now fully integrated into the VESPA code.

Using the VESPA code, we have studied the dynamical response of a stationary sheath-presheath system to an external perturbation, which takes the form of a small density disturbance in the central region of the plasma, far from the sheaths. The numerical results suggest that, for most regimes of physical interest, the perturbation is damped away before it reaches the wall and does not have a significant impact on the structure of the sheath. This scenario has been studied for different temperatures and density profiles of the disturbance.

We have started to look at the impact of secondary electrons (SE) on the structure and the formation of the sheath. SEs were neglected in previous versions of the code but can play a significant role on the wall potential. In the VESPA code, they are now modelled as a Maxwellian electron source located near the wall. First results indicate that a large yield rate of SEs reduces the potential drop between the plasma bulk and the wall.

6.11. Other application domains

6.11.1. Applications of Two-Scale numerical methods
Participant: E. Frénod.

In paper [37] we consider a model for short term dynamics of dunes in tidal area. We construct a Two-Scale Numerical Method based on the fact that the solution of the equation which has oscillations Two-Scale converges to the solution of a well-posed problem. This numerical method uses on Fourier series.

In [18] we present Chapman–Enskog and Hilbert expansions applied to the $O(v/c)$ Boltzmann equation for the radiative transfer of neutrinos in core-collapse supernovae. Based on the Legendre expansion of the scattering kernel for the collision integral truncated after the second term, we derive the diffusion limit for the Boltzmann equation by truncation of Chapman–Enskog or Hilbert expansions with reaction and collision scaling. We also give asymptotically sharp results obtained by the use of an additional time scaling. The diffusion limit determines the diffusion source in the *Isotropic Diffusion Source Approximation (IDSA)* of Boltzmann's equation for which the free streaming limit and the reaction limit serve as limiters. Here, we derive the reaction limit as well as the free streaming limit by truncation of Chapman–Enskog or Hilbert expansions using reaction and collision scaling as well as time scaling, respectively. Finally, we motivate why limiters are a good choice for the definition of the source term in the IDSA.

6.11.2. Inverse problem governed by Maxwell equations
Participant: Jean R. Roche.

This work is performed in collaboration with José Herskovits Norman of UFRJ, Rio de Janeiro, Antonio André Novotny from the LNCC, Petropolis, both from Brazil and Alfredo Canelas from the University of the Republic, Montevideo, Uruguay.

The industrial technique of electromagnetic casting allows for contactless heating, shaping and controlling of chemical aggressive, hot melts. The main advantage over the conventional crucible shape forming is that the liquid metal does not come into contact with the crucible wall, so there is no danger of contamination. This is very important in the preparation of very pure specimens in metallurgical experiments, as even small traces of impurities, such as carbon and sulphur, can affect the physical properties of the sample. Industrial applications are, for example, electromagnetic shaping of aluminum ingots using soft-contact confinement of the liquid metal, electromagnetic shaping of components of aeronautical engines made of superalloy materials (Ni,Ti, etc.), control of the structure solidification.

The electromagnetic casting is based on the repulsive forces that an electromagnetic field produces on the surface of a mass of liquid metal. In the presence of an induced electromagnetic field, the liquid metal changes its shape until an equilibrium relation between the electromagnetic pressure and the surface tension is satisfied. The direct problem in electromagnetic casting consists in determining the equilibrium shape of the liquid metal. In general, this problem can be solved either directly studying the equilibrium equation defined on the surface of the liquid metal, or minimizing an appropriate energy functional. The main advantage of this last method is that the resulting shapes are mechanically stable.

The inverse problem consists in determining the electric currents and the induced exterior field for which the liquid metal takes on a given desired shape. This is a very important problem that one needs to solve in order to define a process of electromagnetic liquid metal forming.

In a previous work we studied the inverse electromagnetic casting problem considering the case where the inductors are made of single solid-core wires with a negligible area of the cross-section. In a second paper we considered the more realistic case where each inductor is a set of bundled insulated strands. In both cases the number of inductors was fixed in advance, see [61]. In order to look for configurations of inductors considering different topologies we introduce a new formulation for the inverse problem using a shape functional based on the Kohn-Vogelius criterion. A topology optimization procedure is defined by means of topological derivatives, a new method that simplifies computation issues was considered, see [60] and [49].

During 2013 we rewrite the inverse electromagnetic casting model in order to have a quadratic programming problem, this simplified the numerical solution and simulation [19].

<h1 style="text-align:center; color:red;">CORIDA Project-Team</h1>

5. New Results

5.1. Analysis and control of fluids and of fluid-structure interactions

In [47], we analyze the system fluid-rigid body in the case of where the rigid body is a ball of "small radius". More precisely, we consider the limit system as the radius goes to zero. We recover the Navier-Stokes system with a particle following the the velocity of the fluid. We consider in [45] a model of vesicle moving into a viscous incompressible fluid. Such a model, based on a phase-field approach was derived by researchers in Physics, and is quite difficult to study. By considering some approximation, we prove some result of existence of solutions for such a system.

By acting on a part of the fluid domain or on a part of the exterior boundary, we aim at controlling the fluid velocity, the rigid velocity and the position of the rigid body. It can be a control in open loop or in closed loop. We have studied both problems in the 1D case. In this case, the study benefits some simplifications, but can also be more difficult since the fluid domain is no more connected. As a consequence, if one wants to control by using only one input, on one part of the fluid domain, the fluid on the other side of the particle is only controlled by the motion of the structure.

We introduce a new method for controllability of nonlinear parabolic system allowing to deal with this problem and we solve it in ([24]). We also obtain the local stabilization of such system around a stationary state in [41].

We study the Cauchy problem corresponding to a similar 1D system without viscosity in [40]. In that case, we have to deal with the interaction between the particle and shock waves or relaxation waves. In [44], we analyze a numerical scheme for the method of observers used to reconstruct the initial data of hyperbolic systems such as wave equation. We add some numerical viscosity in the scheme in order to have a uniform decay of the error between the reconstructed solution and the real one.

In [30], a Lagrange-Galerkin method is introduced to approximate a two dimensional fluid-structure interaction problem for deformable solids. The new numerical scheme we present is based on a characteristics function mapping the approximate deformable body at the discrete time level t_{k+1} into the approximate body at time t_k.

The aim of [25] is to tackle the time optimal controllability of an $(n+1)$-dimensional nonholonomic integrator with state constraints. A full description of an optimal control together with the corresponding optimal trajectories are explicitly obtained. The optimal trajectories we construct, are composed of arcs of circle lying in a 2-dimensional plane.

In [26], controllability results are obtained for a low Reynolds number swimmer composed by a spherical object which is undergoing radial and axi-symmetric deformations in order to propel itself in a viscous fluid governed by the Stokes equations. A time optimal control problem is also solved for a simplified model and explicit optimal solutions are constructed.

5.2. Frequency domain methods for the analysis and control of systems governed by PDE's

With a numerical viscosity terms in the approximation scheme of second order evolution equations, we show in [11] the exponential or polynomial decay of the discrete scheme when the continuous problem has such a decay and when the spectrum of the spatial operator associated with the undamped problem satisfies the generalized gap condition. We further show the convergence of the discrete solution to the continuous one.

In [19], we propose a strategy to determine the Dirichlet-to-Neumann (DtN) operator for infinite, lossy and locally perturbed hexagonal periodic media, using a factorization of this operator involving two non local operators. The first one is a DtN type operator and corresponds to a half-space problem, while the second one is a Dirichlet-to-Dirichlet (DtD) type operator related to the symmetry properties of the problem.

In [22], we generalize to the case of acoustic penetrable scatterers the results derived by Hazard and Ramdani [54] for sound hard scatterers. In particular, we provide a justification of the DORT method in this case and we show that each small inhomogeneity gives rise to $3d + 1$ eigenvalues of the time reversal operator. The selective focusing of the corresponding eigenfunctions is also proved.

In [17], we consider the inverse problem of determining the potential in the dynamical Schrödinger equation on the interval by the measurement on the boundary. We use the Boundary Control Method to recover the spectrum of the problem from the observation at either left or right end points. Using the specificity of the one-dimensional situation we recover the spectral function, reducing the problem to the classical one which could be treated by known methods. We also consider the case where only a finite number (N) of eigenvalues are available and we prove the convergence of the reconstruction method as N tends to infinity.

We give some spectral and condition number estimates of the acoustic single-layer operator for low-frequency multiple scattering in dense [15] and dilute [16] media.

5.3. Use of geometric techniques for the control of finite and infinite dimensional systems

The paper [31] deals with the design of high gain observers for a class of continuous dynamical systems with discrete-time measurements. The new idea of the this work is to synthesize an observer requiring the less knowledge as possible from the output measurements. This is done by using an updated sampling time observer.

In [12], it is shown that, for a bilinear system, the property of observability is preserved after sampling provided that the controls take their values in a compact space and do not vary too quickly.

In the note [18] two notions of controllability are studied, called respectively radial controllability and directional controllability. It is proven that for families of linear vector fields, the two notions are actually equivalent.

We used operators theory to obtain some new estimates of the energy of an infinite dimensional bilinear quantum systems. These results were presented in [34].

Robust control of bilinear Schrödinger equation was investigated in [35]. The use of sharp finite dimensional energy estimates (in the spirit of [34]) allows to obtain the first approximate ensemble controllability results for infinite dimensional quantum systems, also in presence of mixed spectrum for the free Hamiltonian.

The above energy questions, together with a their relation with some open question in the control of bilinear quantum systems, were gathered in the survey [32].

Our team is heavily involved in the optimization of driving strategy, and especially in the effective implementation in the prototype build in ESSTIN. MPC related methods have been tested and successfully improved as described in [37].

TOSCA Project-Team

6. New Results

6.1. Probabilistic numerical methods, stochastic modelling and applications

Participants: Mireille Bossy, Nicolas Champagnat, Julien Claisse, Madalina Deaconu, Samuel Herrmann, James Inglis, Antoine Lejay, Sylvain Maire, Sebastian Niklitschek Soto, Denis Talay, Etienne Tanré, Denis Villemonais, Laurent Violeau.

6.1.1. Published works and preprints

- M. Bossy and J-F. Jabir (University of Valparaíso) [29], have proved the well-posedness of a conditional McKean Lagrangian stochastic model, endowed with the specular boundary condition, and further the mean no-permeability condition, in a smooth bounded confinement domain $\mathcal{D}$. This result extends their previous work [48], where the confinement domain was the upper-half plane. The extension of the construction to more general confinement domain exhibits difficulties that we handle by combining stochastic calculus and the analysis of kinetic equations. As a prerequisite for the study of the nonlinear case, we construct a Langevin process confined in $\overline{\mathcal{D}}$ and satisfying the specular boundary condition. We then use PDE techniques to construct the time-marginal densities of the nonlinear process from which we are able to exhibit the conditional McKean Lagrangian stochastic model.

- N. Champagnat studied in collaboration with S. Méléard (Ecole Polytechnique, Palaiseau) and P.-E. Jabin (Univ. of Maryland) adaptive dynamics and evolutionary branching in individual-based models of populations competing for resources, where resources consumption is modelled similarly as for chemostat systems of ODEs [13].

- M. Deaconu and S. Herrmann constructed a new procedure for the simulation of the hitting times of nonlinear boundaries for Bessel processes. This method, called the random walk on moving spheres algorithm, is based on two key properties: first, the explicit distribution of the first hitting time of a particular boundary for the Bessel process; second, the connexion between the Bessel process and the Euclidean norm of a Brownian motion having the same dimension. This result can be applied for the hitting time of a given level for the Cox-Ingersoll-Ross process and thus be used in models arising from finance and neurosciences [15].

- J. Inglis and E. Tanré completed their study with F. Delarue and S. Rubenthaler (Univ. Nice – Sophia Antipolis) on the global solvability of a networked system of integrate-and-fire neurons proposed in the neuroscience literature. To do this it was necessary to obtain some general estimates of the first hitting times of barriers by non-homogeneous processes, which have been collected together separately in [40], http://hal.inria.fr/hal-00870991.

- J. Inglis, in collaboration with O. Faugeras (EPI NEUROMATHCOMP), studied the well-posedness of stochastic neural field equations within a rigorous framework. The deterministic versions of these equations have been used to great success for the macroscopic modeling of brain activity. Their stochastic counterparts are non-trivial SPDEs, due to the presence of a nonlocal operator [26], http://hal.inria.fr/hal-00907555.

- A. Lejay and L. Coutin (Université de Toulouse) have continued their work on the sensitivity of the Itô's map in the context of rough paths [37].

- With L. Coutin (Université de Toulouse), A. Lejay has provided a framework for considering linear rough differential equations [49].

- With A. Kohatsu-Higa (Ritsumeikan University) and K. Yasuda (Hosei University), A. Lejay provided bounds on the weak rate of convergence of the Euler scheme when the drift term is discontinuous [41].

- S. Maire and G. Nguyen have developed a Monte Carlo method to deal with Robin and transmission conditions for elliptic diffusion equations in stratified media. It combines walk on spheres techniques and finite differences [44].

- D. Villemonais worked on the empirical distribution of Fleming-Viot type particle systems. Using couplings with reflected diffusion processes, he proved the uniform tightness of such empirical distributions and deduced the non-degeneracy of the law of diffusion processes conditioned not to hit a boundary [19].

- D. Villemonais proved in [18] a general approximation method for Markov processes conditioned not be killed. The method is based on a mean field interacting particles system which is easy to simulate. The study also details the particular case of time/environment dependent diffusion processes.

6.1.2. Other works in progress

- N. Champagnat and B. Henry work on the long-time behaviour of the frequency spectrum for the Splitting Tree models under the infinitly-many alleles model. Specificaly, they want to study the asymptotic behavior of the largests families in the "supercritical clonal" case. Such results could be applied to design statistical methods to detect positive selection of a gene in a growing population.

- N. Champagnat, D. Ritchie (ORPAILLEUR team, Inria Nancy) and B. Henry work on the design of a stochastic model for the evolution of 3D structures of proteins. Using Kpax algorithm [52], which allow to quantify the evolutionary distance between proteins, their goal is to design a statistical method to infer phylogenetic trees with particle systems methods.

- N. Champagnat and D. Villemonais obtained criterions for existence and uniqueness of quasi-stationary distributions and Q-processes for general absorbed Markov processes. A quasi-stationary distribution is a stationary distribution conditionnally on non-absorbtion, and the Q-process is defined as the original Markov process conditionned to never be absorbed. The criterion that they obtain ensures exponential convergence of the conditionned t-marginal of the process conditionned not to be absorbed at time t, to the quasi-stationary distribution and also the exponential ergodicity of the Q-process. This work is currently being written.

- J. Claisse continued his PhD. under the supervision of N. Champagnat and D. Talay on stochastic control of population dynamics. He completed a finite-horizon optimal control problem on branching–diffusion processes. He also created and studied a hybrid model of tumor growth emphasizing the role of acidity. Key therapeutic targets appear in the model to allow investigation of optimal treatment problems.

- M. Deaconu and S. Herrmann are developing a new algorithm for the simulation of Bessel processes hitting times for non-integer dimensions. The idea is to decompose the dimension into its integer part and its fractional part and use the additivity property for squared Bessel processes. Each simulation step is splitted in two parts: one uses the integer dimension case and the other one considers hitting times of a Bessel process starting from zero.

- M. Deaconu in collaboration with L. Beznea (IMAR Bucarest) and O. Lupaşcu (Université Paris 13 and IMAR Bucarest) studies the connexion between the coagulation/fragmentation phenomena and branching processes.

- J. Inglis and D. Talay are developing a mean-field model of a network of neurons, that contains both a spatial element describing the transmission of a signal along dendrites, as well as non-homogenous weights that represent the strength of the synaptic connections. More generally, this leads to the study of the limiting behavior of non-exchangeable mean-field particle systems.

- J. Inglis and E. Tanré are continuing their collaboration with F. Delarue (Univ. Nice – Sophia Antipolis) by developing approximations to a limiting equation describing the behavior of a large network of neurons all behaving according to the integrate-and-fire model. Both a particle system approximation and an approximation involving delays are considered.

- S. Larnier and A. Lejay have worked on nearshore wave analysis and bathymetry identification through the use of a video installed on the shore [42], [43].

- A. Lejay has continued his work with R. Rebolledo (Pontificia Universidad Católica), S. Torres (Universidad de Valparaíso) and E. Mordecki (Universidad de la República) on the parametric estimation of coefficients of diffusion with discontinuous coefficients.

- S. Maire and I. Dimov (Bulgarian academy of sciences) have introduced a new Monte Carlo method to solve real or complex linear systems of equations. Coupled with sequential Monte Carlo this walk on equations method shows a very fast convergence. A similar method is in progress to solve linear integral equations.

- S. Niklitschek Soto and D. Talay have set up and solved a new martingale problem which has allowed them to get a new stochastic representation for solutions of multi-dimensional diffraction parabolic PDEs with general discontinuous coefficients. One of the main difficulties to overcome has been to identify the proper weighted local time process involved in the stochastic dynamics. This work opens the way to innovating Monte Carlo methods for this class of PDEs.

- P. Guiraud (University of Valparaíso) and E. Tanré study the effect of noise in the phenomenon of spontaneous synchronisation in a network of full connected integrate- and-fire neurons. They detail cases in which the phenomenon of synchronization persists in a noisy environment, cases in which noise permits to accelerate synchronization, and cases in which noise permits to observe synchronization while the noiseless model does not show synchronization. (Math Amsud program SIN)

- L. Capietto worked during his internship under the supervision of O. Faugeras (EPI NEUROMATH-COMP) and E. Tanré on extension of [51], in a context with several populations of homogeneous neurons. They study the limit mean field equation of the membrane potential as the number of neurons increase in a network with correlated synaptic weights.

- E. Tanré, in collaboration with O. Faugeras (EPI NEUROMATHCOMP) and the team Inference and Visual Behavior (IViBe) of Institut de Neurosciences de la Timone (INT), studied the motion of eyes, the phenomena of sacades and micro-saccades when monkeys or humans have to fix the center of a picture during a few minutes. They introduce a stochastic model to describe the typical path of the eyes on the picture and evaluate the link between the characteristics of the artificial pictures and the coefficients of the stochastic model.

- L. Violeau continued his PhD. on *Stochastic Lagrangian Models and Applications to Downscaling in Fluid Dynamics* under the supervision of M. Bossy and A. Rousseau (LEMON team, Inria Sophia Antipolis - Méditerranée). Laurent Violeau has obtained a theoretical rate of convergence of the particle approximation of kinetic conditional McKean-Vlasov stochastic models. This result is the first that explicits the complex relationship between the two sources of spacial errors in such kind of algorithm: the smoothing parameter for the conditional expectation estimator and the number of interacting particles. This theoretical convergence rate was confronted with numerical tests in the case of simplified Lagrangian models that confirm the pertinence of the theoretical bound for the error.

- C. Graham and D. Talay are writing the second volume of their series published by Springer on the Mathematical Foundations of Stochastic Simulations.

- In collaboration with N. Touzi (Ecole Polytechnique), D. Talay is studying stochastic differential equations involving local times with stochastic weights, and extensions of classical notions of viscosity solutions to PDEs whose differential operator has discontinuous coefficients and transmission boundary conditions.

6.2. Financial Mathematics

Participants: Mireille Bossy, Nicolas Champagnat, Paul Charton, Madalina Deaconu, Dalia Ibrahim, Antoine Lejay, Khaled Salhi, Denis Talay, Etienne Tanré.

6.2.1. Published works and preprints

- In collaboration with N. Maïzi (CMA - Mines Paristech) and O. Pourtallier (COPRIN team, Inria Sophia Antipolis - Méditerranée), M. Bossy studied the existence result of a Nash equilibrium between electricity producers selling their production on an electricity market and buying CO2 emission allowances on an auction carbon market. The producers' strategies integrate the coupling of the two markets via the cost functions of the electricity production. The authors set out a clear Nash equilibrium that can be used to compute equilibrium prices on both markets as well as the related electricity produced and CO2 emissions covered [30]

- In addition to the internship of K. Salhi, N. Champagnat, M. Deaconu, and A. Lejay have worked on the use of power law to predict risk in financial markets using data from Euronext NSYE stocks exchanges [33].

- P. Charton submitted an article [35] on the optimal operation of a windfarm equipped with a storage unit.

6.2.2. Other works in progress

- D. Ibrahim, D. Talay and E. Tanré worked on a model coming from technical analysis in finance. They study the Bollinger Bands indicator to detect jumps in the volatility in an extension of classical Black and Scholes models. They evaluate the efficiency of such indicators to detect the random time at which the volatility jump from a *small* value to a *large* one. A paper is being written.

- In collaboration with Victor Reutenauer and Christophe Michel (CA-CIB), D. Talay and E. Tanré worked on a model in financial mathematics including bid-ask spread cost. They study the optimal strategy to hedge an interest rate swap that pays a fixed rate against a floating rate. They present a methodology using a stochastic gradient algorithm to optimize strategies. A paper is being submitted.

- In collaboration with J. Bion-Nadal (Ecole Polytechnique and CNRS), D. Talay introduced a new calibration method based on dynamical risk measures and stochastic control PDEs. A paper is being written.

6.3. Stochastic Analysis

Participants: Nicolas Champagnat, Julien Claisse, Denis Talay.

- N. Champagnat studied in collaboration with P.-E. Jabin (Univ. of Maryland) strong existence and pathwise uniqueness for stochastic differential equations driven by a Brownian motion and with rough coefficients [34]. The method is an extension of the one of [50], which studies well-posedness for deterministic dynamical system. Strong existence and pathwise uniqueness can be proved for example if the drift vector is $L^1(W^{1,1})$ and the diffusion matrix is uniformly elliptic and $L^q(W^{1,p})$ with $2/q + d/p = 1$. This improves the previous conditions of [53].

- J. Claisse and D. Talay studied in collaboration with X. Tan (Univ. of Paris Dauphine) a conditioning argument which is often used to prove the dynamic programming principle [36]. Their study of the literature revealed that previous proofs of this argument are incorrect or incomplete. They provided a rigorous and detailed proof by setting up martingale controlled problems in a original way.

CORTEX Team

6. New Results

6.1. Understanding embodied neural systems

Participants: Dominique Martinez, Carlos Carvajal-Gallardo, Georgios Detorakis.

6.1.1. Bio-physical modeling and embodied olfaction

Our understanding of the computations that take place in the human brain is limited by the extreme complexity of the cortex, and by the difficulty of experimentally recording neural activities, for practical and ethical reasons. The Human Genome Project was preceded by the sequencing of smaller but complete genomes. Similarly, it is likely that future breakthroughs in neuroscience will result from the study of smaller but complete nervous systems, such as the insect brain or the rat olfactory bulb. These relatively small nervous systems exhibit general properties that are also present in humans, such as neural synchronization and network oscillations. Our goal has been therefore to understand the role of these phenomena by combining biophysical modelling and experimental recordings, before applying this knowledge to humans. In the last year, we have extended our neuronal model of the insect olfactory system. This model is capable of reproducing and explaining the stereotyped multiphasic firing pattern observed in pheromone sensitive antennal lobe neurons [10].

Using this model in robotic experiments and insect antennae as olfactory sensors, we related these multiphasic responses to action selection. The efficiency of the model for olfactory searches was demonstrated in driving the robot toward a source of pheromones. Two different classes of strategies are possible for olfactory searches, those based on a spatial map, e.g. Infotaxis, and those where the casting-and-zigzagging behaviour observed in insects is purely reactive, without any need for an internal memory, representation of the environment, or inference [15]. Our goal was to investigate this question by implementing infotactic and reactive search strategies in a robot and test them in real environmental conditions. We previously showed that robot Infotaxis produces trajectories that feature zigzagging and casting behaviours similar to those of moths, is robust and allows for rapid and reliable search processes. We have implemented infotactic and reactive search strategies in a cyborg using the antennae of a tethered moth as sensors, since no articial sensor for pheromone molecules is presently known [10].

6.1.2. Somato-sensory cortex

In a joint work with the Mnemosyne team, we have investigated the formation and maintenance of ordered topographic maps in the primary somatosensory cortex as well as the reorganization of representations after sensory deprivation or cortical lesion. We consider both the critical period (postnatal) where representations are shaped and the post-critical period where representations are maintained and possibly reorganized. We hypothesize that feed-forward thalamocortical connections are an adequate site of plasticity while cortico-cortical connections are believed to drive a competitive mechanism that is critical for learning. We model a small skin patch located on the distal phalangeal surface of a digit as a set of 256 Merkel ending complexes (MEC) that feed a computational model of the primary somatosensory cortex (area 3b). This model is a two-dimensional neural field where spatially localized solutions (a.k.a. bumps) drive cortical plasticity through a Hebbian-like learning rule. Simulations explain the initial formation of ordered representations following repetitive and random stimulations of the skin patch. Skin lesions as well as cortical lesions are also studied and results confirm the possibility to reorganize representations using the same learning rule and depending on the type of the lesion. For severe lesions, the model suggests that cortico-cortical connections may play an important role in complete recovery [11], [19], [7].

6.1.3. K-cells in visuomotor tasks

In another joint work with the Mnemosyne team, we have explored the role of the thalamus in visuomotor tasks implicating non-standard ganglion cells. Such cells in the retina have specific loci of projection in the visuomotor systems and particularly in the thalamus and the superior colliculus. In the thalamus, they feed the konio pathway of the LGN. Exploring the specificities of that pathway, we discovered it could be associated to the matrix system of thalamo-cortical projections, known to allow for diffuse patterns of connectivity and to play a major role in the synchronization of cortical regions by the thalamus. An early model led to the design of the corresponding information flows in the thalamo-cortical system, that we expanded, in the framework of the Keops project, to be applied to real visuomotor tasks [13].

We proposed to implement the computational principles raised by the study on the K-cells of the retina using a variational specification of the visual front-end, with an important consequence. In such a framework, the GC are not to be considered individually, but as a network, yielding a mesoscopic view of the retinal process. Given natural image sequences, fast event-detection properties appear to be exhibited by the mesoscopic collective non-standard behavior of a subclass of the so-called dorsal and ventral konio-cells (K-cells) that correspond to specific retinal output. We considered this visual event detection mechanism to be based on image segmentation and specific natural statistical recognition, including temporal pattern recognition, yielding fast region categorization. We discussed how such sophisticated functionalities could be implemented in the biological tissues as a unique generic two-layered non-linear filtering mechanism with feedback. We used computer vision methods to propose an effective link between the observed functions and their possible implementation in the retinal network. The available computational architecture is a two-layers network with non-separable local spatio-temporal convolution as input, and recurrent connections performing non-linear diffusion before prototype based visual event detection [17].

6.2. Neuro-inspired computational models

Participants: Yann Boniface, Benoît Chappet de Vangel, Bernard Girau, Patrick Hénaff.

6.2.1. Motion detection

We develop bio-inspired neural architectures to extract and segment the direction and speed components of the optical flow from sequences of images. Following this line, we have built additional models to code and distinguish different visual sequences. The structure of these models takes inspiration from the course of visual movement processing in the human brain, such as in area MT (middle temporal) that detects patterns of movement, or area FBA where neurons have been found to be sensitive to single spatio-temporal patterns. This work has been extended to complex movements: to fight, to wave, to clap, using real-world video databases [9].

6.2.2. Multimodal learning through joint dynamic neural fields

We have developed a coherent multimodal learning for a system with multiple sensory inputs. To this aim, we modified the BCM synaptic rule, a local learning rule, to obtain the self organization of our neuronal inputs maps and we used a CNFT based competition to drive the BCM rule. In practice, we introduced a feedback modulation of the learning rule, representing multimodal constraints of the environment. We also introduced an unlearning term in the BCM equation to solve the problem of the different temporalities between the raise of the activity within modal maps and the multimodal learning of the organization of the maps [12].

6.2.3. Adaptive sensori-motor loop

We develop bio-inspired neural controllers to control humanoids robot when they interact physically (or socially) with the human. We focus on the role of rythmicity in the interaction: how the phenomena of coupling, synchrony or others are involved in the interaction between humans? what models of neural structures can incorporate rythmicity intrinsically, and can include learning or adaptive mechanisms of the rythmicity.

6.2.4. Randomly spiking dynamic neural fields

We have defined a new kind of spiking neural field that is able to use only local links while transmitting spikes through the map by succesive random propagations. Such a model is able to be mapped onto FPGAs, while maintaining most properties of neural fields. This model has been validated from a behavioral point of view, and a fully scalable hardware implementation has been designed with several thousands of neurons on-chip. These first results are the object of an article that is currently reviewed after requested revisions.

BIGS Project-Team

6. New Results

6.1. Modern methods of data analysis

Participants: R. Bar, S. Ferrigno, B. Lalloué, J-M. Monnez, A. Muller-Gueudin, S. Tindel

6.1.1. Help to medical decision and telemedecine in the monitoring of heart failure

We describe here a project started in 2013, for which we expect some concrete output in 2014. This project fits in the general framework of telemedecine and more precisely in the monitoring of heart failure patients. From measurements performed automatically and daily on a patient at home through a new process under development at the Pluri-Thematic Clinical Investigation Center of the University Hospital of Nancy, the aim is to propose therapeutic adjustments to improve the prognosis of patient in order to increase his chances of survival or to avoid his rehospitalization.

The patient's condition and its evolution are determined by the initial values of his biological or clinical parameters as well as those collected throughout his follow-up. The treatments are intended to stabilize or change the values of parameters in order to avoid the occurrence of adverse events, in particular the death of the patient. This is why the first part of the study will consist in building survival scores or rehospitalization scores according to the values of biological or clinical parameters.

In a second part, we will seek to build models of the evolution of the values of biological or clinical parameters depending on treatments (average or cumulative drug doses, drug combinations) and patients' characteristics. This will allow to predict the potential effect of an adjustment proposal or modification of treatment and then predict a new survival score to conclude the relevance or not of the proposed medication.The physician will have this help to confirm or change his decision which belongs finally to him.

We will use to carry out this study a wide range of classic and recent methods of data analysis, in particular discriminant analysis, without a priori: several methods will be used, compared and selected according to their performance in the treated applications.

6.1.2. Online factorial data analysis methods

Nowadays data analysts are often faced with the problem of dealing with a rapid and infinite flow of data. Examples include web, telecommunications, process control or financial data. We made first the assumption that the data are generated at random according to a stationary distribution, but in many cases this assumption does not hold true. We developed in [13] the online adaptation of principal component analysis and other dimension reduction statistical algorithms by using stochastic approximation. An R package was developed by Romain Bar.

6.1.3. Data analysis techniques and Bayesian models applied to the context of social inequalities and environmental exposures

The aim of [10] is to improve the knowledge about and apply data mining techniques and some Bayesian model in the field of social and environmental health inequalities. The health event considered is infant mortality. We try to explain its risk with socio-economic data retrieved from the national census and environmental exposures such as air pollution, noise, proximity to traffic, green spaces and industries. The data mining part details the development of a procedure of creation of multi-dimensional socio-economic indices and of an R package that implements it.

6.1.4. *A simultaneous stepwise variable selection and clustering algorithm to discriminate a class variable with numerous levels*

In supervised learning the number of levels of a categorical variable to explain can be high. When some of its levels are of low frequency, clustering them in order to reduce the number of classes can be useful to perform relevant discriminant analyses. On the other hand selecting relevant predictors is a crucial step to build robust and efficient classification rules, especially when too many variables are available in regard to the overall sample size. We are currently carrying out an extension of an algorithm we had devised to solve both these problems using an alternate minimization of Wilks' Lambda. We show through simulations the interest of adding Akaike Information Criterion as another optimality criterion. We also moved forward to stepwise selection and applied this new version of our algorithm to real allergology datasets.

6.1.5. *Local polynomial regression. Application to the estimation of the fetal growth.*

This topic is an ongoing collaboration with M. Maumy-Bertrand, for which we expect a publication in 2014. We have established exact rate of strong uniform consistency for the local linear estimator of the conditional distribution function. We want to extend our results to obtain exact rates of strong uniform consistency for the local linear estimator of other conditional quantities: the conditional mean $\mathbb{E}(Y|X)$, and the conditional quantiles $q_\alpha(x) = \inf\{y : F(y|x) \geq \alpha\}$, for $\alpha \in (0,1)$.

Another crucial problem with the non parametric regression methods is the choice of the bandwidth parameter h. It is common in practice to choose $h > 0$ so to minimize asymptotically the mean square error (MSE) or the mean integrated square error (MISE). This minimization leads to an optimal choice of h of the form $h_n = C(X_1, ..., X_n)n^{-1/5}$, where n is the sample size, and $X_1, ..., X_n$ are the n independent copies of the random variable X. This bandwidth is called a *data-driven bandwidth* to enhance its dependence to the data. Our current project in this direction consists in establishing the consistency of the local linear estimator when the bandwidth h is allowed to range in a small interval which may decrease in length with the sample size. Such a result would be immediately applicable to prove uniform consistency of the local linear estimator when the bandwidth is a data-driven bandwidth $h_n = C(X_1, ..., X_n)n^{-1/5}$.

Turning to applications, note that we have a contact with Professor Bernard Foliguet at the Maternité Régionale de Nancy. We will continue to collaborate with him, to estimate growing curves of the fetal weight, and other fetal quantities thanks to the techniques mentioned above.

6.1.6. *Cohort analysis*

In an ongoing work with the INSERM team of P. Guéant, we aim at describing the complex interactions between genetic, phenotypic and biologic variables that are available in medical cohorts, in different contexts (cognitive decline; inflammatory intestinal diseases; liver cancer).

A firt step in our analysis, which should be finished in 2014, consists in giving an overview of the existing methods given in the literature, for the analysis of qualitative and quantitative data. Indeed, we have to describe links between qualitative and quantitative data:

1. with exploratory methods, or factorial models,
2. with regression models to predict qualitative variable by the use of qualitative or quantitative factors.

In the sequel, we will test non association or independence between the variables. The objective is to develop new methods, adapted to the studied cohorts (matching cases/controls, high number of individuals, high number of explicative variables, missing data problem). The particularity of our work is to combine statistical and symbolical methods.

After having identified and choice the relevant variables, we will have to give a model for classifying the data. The proposed models will allow us to identify subgroups of invidious, with common genetic, biologic and phenotypic characteristics.

6.1.7. Local polynomial estimation and goodness-of-fit tests

We describe here an ongoing work with Marie-José Martinez, assistant professor at the IUT of Grenoble and member of the Inria MISTIS team. A related publication should be finished at the end of 2014. Many clinical trials and other medical studies involve responses that might be considered to have a normal distribution. However, this is not invariably the case and models based on this distribution are often indiscriminately applied to data which might be better handled otherwise. This is especially true for discrete data. An approach which may yields models that are more biologically reasonable in many situations is to use generalized linear models (GLM).

In statistical theory, generalized linear models were formulated by John Nelder and Robert Wedderburn (1972) as a way of unifying various other statistical models including for examples linear regression, logistic regression and poisson regression. Such a technique was developed by McCullagh and Nelder (1989). It is an extension of the linear model, in the sense that its satisfies a relation of the form $Y = g(X) + \epsilon$ where:

- The stochastic component ϵ follows other distributions than the Gaussian.
- The function g can be non linear.

Notice that those models are well-suited to analyze dependences between variables following distributions in the so-called exponential family, like Poisson, Binomial and Gamma distributions. In practice, link functions are chosen such that the inverse link, $\mu = g^{-1}(\eta)$ is easily computed. For instance, for binomial data, logit and probit link functions are commonly used.

Our aim in this project is to use generalized linear models in order to extend our global test of goodness-of-fit to a wide range of models used in biological and medical applications. We wish to use the cumulative conditional distribution $F(y|X = x)$ again, which embodies all the information about the joint behavior of two random variables. The expected outcome is a global goodness of fit test for the relationship between two random variables in the exponential family. The test will compare a nonparametric estimator of the cumulative distribution function with the value of the cumulative distribution function under the null hypothesis.

6.1.8. Model selection for SVM

Support vector machines provide a very powerful method of data classification, for which model selection is one of the key issues. For a support vector machine, model selection consists in selecting the kernel function, the values of its parameters, and the amount of regularization. To set the value of the regularization parameter, one can minimize an appropriate objective function over the regularization path. A priori, this requires the availability of two elements: the objective function and an algorithm computing the regularization path at a reduced cost. The literature provides us with several upper bounds and estimates for the leave-one-out cross-validation error of the ℓ_2-SVM. However, no algorithm was available so far for fitting the entire regularization path of this machine. In our contribution [3], we introduce the first algorithm of this kind. It is involved in the specification of new methods to tune the corresponding penalization coefficient, whose objective function is a leave-one-out error bound or estimate. From a computational point of view, these methods appear especially appropriate when the Gram matrix is of low rank. A comparative study involving state-of-the-art alternatives provides us with an empirical confirmation of this advantage.

6.2. Estimation for complex and biological systems

Participants: T. Bastogne, C. Lacaux, S. Mézières, S. Tindel, P. Vallois

6.2.1. Tumor growth modeling

This project is an extension of our article [15], which will be written in 2014. A cancer tumor can be represented for simplicity as an aggregate of cancer cells, each cell behaving according to the same discrete model and independently of the others. Therefore to measure its size evolution, it seems natural to use tools coming from dynamics of population, for instance the logistic model. This deterministic framework is well-known but the stochastic one is worthy of interest. We are currently working on a model in which we suppose that the size V_t at time t of the tumor is a diffusion process of the type :

$$\begin{cases} dV_t = r\, V_t \left(1 - \frac{V_t}{\kappa}\right) - c\, V_t + \beta\, V_t\, dB_t \\ V_0 = v > 0 \end{cases} \tag{1}$$

where $(B_t)_{t \geq 0}$ is a standard brownian motion starting from zero.Then (i) We define a family of time continuous Markov chains which models the evolution of the rate of malignant cells and approximate (under some conditions) the diffusion process (V_t). (ii) We study in depth the solution to equation (1). This diffusion process lives between two frontiers : 0 and κ. In this stochastic setting, the role of κ is not so clear and we contribute to understand it. We describe the asymptotic behavior of the diffusion according to the values of the parameters. The tools we resort to are boundary classification criteria and Laplace transform of the hitting time to biological worthwhile level. We believe we are able in particular to express the mean of the hitting time.

The next step in this project can be summarized as follows: at this point in our investigations on tumor growth modelization, we have identified a pertinent and consistent model. Nevertheless our study remains theoretical. A statistical estimation of the parameters $r, \kappa, c\beta$ is thus in order. This would permit to apply our model to real data. A further objective could be to consider a more complex form for the logistic term, see e.g. Schurtz (2007).

6.2.2. *Local score associated with long biological sequences*

Statistical properties of the distribution of the local score is largely used by molecular biologists to extract important features in biological sequences and in particular to determine the most significant one among a collection of biological sequences. The probabilistic model which is commonly used is the following. Associated with a sequence $(\epsilon_i)_{i \geq 1}$ of independent, centered and reduced random variables, consider $S_n = \epsilon_1 + \cdots + \epsilon_n$ and

$$\underline{S}_n = \min_{0 \leq i \leq n} S_i, \quad U_n = S_n - \underline{S}_n = S_n - \min_{i \leq n} S_i \quad n \geq 0.$$

In biological sequence analysis, (ϵ_i) can for example correspond to the physical or chemical properties of the i-th amino acid or nucleotid of the sequence ; it can also reflect the similarity between components of two sequences. The local score $\overline{U}_n$ is the supremum of (U_n) up to time n. Molecular biologists are interested by this supremum as it highlights the best part of the studied sequence, the eventual segment of DNA transmitted by a common ancestor for sequence comparison or the best hydrophobic segment of a protein that would thus naturally move in a transmembrane place. It is clear that the trajectory of (U_n) can be decomposed in a succession of 0 and excursions above 0. These excursions have an important biological interpretation and in particular the highest one corresponds to the best segment due to the physico chemical property or similarity scores that have been chosen. Note that the local score $\overline{U}_n$ can be viewed as the maximum of the heights of all the excursions up to time n. In the article [22], we are interested in complete excursions up to a fixed time. This leads us to introduce the maximum U_n^* of the heights of all the excursions up to time n. The second variable which will play an important role is θ_n^* the time necessary to reach its maximal height U_n^*.
We believe that the knowledge of the joint distribution of the pair (U_n^*, θ_n^*) would permit to get more efficient statistical tests than the ones only based on the local score. This point should be developed in a forthcoming paper.

However, it seems difficult to determine explicitly the law of (U_n^*, θ_n^*) for a fixed n. This difficulty can be overcome considering biological sequences which have a large number of bases and approximating the initial random walk (S_n) by a Brownian motion (B_t) started at 0. Using the functional theorem of convergence of Donsker, the process (U_k) can be compared to

$$\widehat{U}(t) := B(t) - \inf_{0 \leq s \leq t} B(s), \quad t \geq 0. \tag{2}$$

This leads us to consider:

1. the local score $\overline{U}(t)$ which is the maximum of the heights of all the excursions of $U(s)$ up to time t,

2. the maximum $U^*(t)$ of the heights of all the complete excursions up to time t,

3. the time $\theta^*(t)$ taken by $U(s)$ starting from the beginning of the largest excursion to hit the maximal level $U^*(t)$.

The approximation of (U_n) by $(\widehat{U}_t)$ permits to prove that the asymptotic distribution of $\left(\dfrac{U_n^*}{\sqrt{n}},\ \dfrac{\theta_n^*}{n} \right)$ as $n \to \infty$ is the one of $(U^*(1), \theta^*(1))$. Consequently, our initial problem in the discrete setting reduces to determine the joint law of $(U^*(t), \theta^*(t))$, where $t > 0$ is given. We determine in [22] the distribution and the density functions of $(U^*(t), \theta^*(t))$.

6.2.3. *Bacteriophage therapies*

In the last years Bacteriophage therapies are attracting the attention of several scientific studies. They can be a new and powerful tool to treat bacterial infections or to prevent them applying the treatment to animals such as poultry or swine. Very roughly speaking, they consist in inoculating a (benign) virus in order to kill the bacteria known to be responsible of a certain disease. This kind of treatment is known since the beginning of the 20th century, but has been in disuse in the Western world, erased by antibiotic therapies. However, a small activity in this domain has survived in the USSR, and it is now re-emerging (at least at an experimental level). Among the reasons of this re-emersion we can find the progressive slowdown in antibiotic efficiency (antibiotic resistance). Reported recent experiments include animal diseases like hemorrhagic septicemia in cattle or atrophic rhinitis in swine, and a need for suitable mathematical models is now expressed by the community.

At a mathematical level, whenever the mobility of the different biological actors is high enough, bacteriophage systems can be modeled by a kind of predator-prey equation. Namely, set S_t (resp. Q_t) for the bacteria (resp. bacteriophages) concentration at time t. Then a model for the evolution of the couple (S, Q) is as follows:

$$\begin{cases} \mathrm{d}S_t & = [\alpha - k\,Q_t]\,S_t \mathrm{d}t + \varepsilon\,S_t\,\mathrm{d}W_t^1 \\ \mathrm{d}Q_t & = \left[d - mQ_t - k\,Q_t\,S_t + k\,b\,e^{-\mu\zeta}\,Q_{t-\zeta}\,S_{t-\zeta}\right] \mathrm{d}t + \varepsilon\,Q_t\,\mathrm{d}W_t^2, \end{cases} \tag{3}$$

where α is the reproducing rate of the bacteria and k is the adsorption rate. In equation (3), d also stands for the quantity of bacteriophages inoculated per unit of time, m is their death rate, we denote by b the number of bacteriophages which is released after replication within the bacteria cell, ζ is the delay necessary to the reproduction of bacteriophages (called latency time) and the coefficient $e^{-\mu\zeta}$ represents an attenuation in the release of bacteriophages (given by the expected number of bacteria cell's deaths during the latency time, where μ is the bacteria's death rate). A given initial condition (S_0, Q_0) is also specified, and the term $\varepsilon\,\mathrm{d}W_t$ takes into account a small external noise standing for both uncertainties on the measures and the experiment conditions. One should be aware of the fact that the latency time ζ (which can be seen as the reproduction time of the bacteriophages within the bacteria) cannot be neglected, and is generally of the same order (about 20mn) as the experiment length (about 60mn).

With this model in hand, our main results in this direction (see [1]) have been the following:

- Quantification of the exponential convergence to a bacteria-free equilibrium of equation (3) when d is large enough.

- Use of the previous result plus concentration inequalities in order to study the convergence of the noisy system to equilibrium in a reasonable time range.

- Simulation of the stochastic processes at stake in order to observe the convergence to equilibrium.

6.2.4. Light transport in tissues with probabilistic methods

Photodynamic therapy (PDT) is a type of phototherapy used for treating several diseases such as acne, bacterial infection, viruses and some cancers. The aim of this treatment is to kill pathological cells with a photosensitive drug that is absorbed by the target cells and that is then activated by light. For appropriate wavelength and power, the light beam makes the photosensitizer produce singlet oxygen at high doses and induces the apoptosis and necrosis of the malignant cells. Our project focuses on an innovative application: the interstitial PDT for the treatment of high-grade brain tumors. This strategy requires the installation of optical fibers to deliver the light directly into the tumor tissue to be treated, while nanoparticles are used to carry the photosensitizer into the cancer cells. In order to optimize the intra-cerebral position of our optical fiber, two fundamental questions have to be answered:

1. What is the optimal shape and position of the light source in order to optimize the damage on malignant cells?
2. Is there a way to identify the physical parameters of the tissue which drive the light propagation?

Notice that we are obviously not the first ones to address these issues, and there is nowadays a consensus in favor of the algorithm proposed by L. Wang and S. L. Jacques for the simulation of light transport in biological tissues. However, our starting point is the observation that the usual methods slightly lack of formalism and miss formal representations that answer the questions of identifiability. In [25], in the framework of homogeneous biological tissues, we propose an alternative MC method to Wang's algorithm. Then we also propose a variance reduction method. Interestingly enough, our formulation also allows us to design quite easily a Markov chain Monte Carlo (MCMC) method based on Metropolis-Hastings algorithm and to handle the inverse problem (of crucial importance for practitioners), consisting in estimating the optical coefficients of the tissue according to a series of measurements. We have compared the proposed MC and MCMC method and Wang's algorithm: we see that our MC method is much more consistent. However, MCMC methods induce quick mutations, which paves the way to very promising algorithms in the inhomogenous case. To handle the inverse problem, we derive a probabilistic representation of the variation of the fluence with respect to the absorption and scattering coefficients. This leads us to the implementation of a Levenberg-Marquardt type algorithm that gives an approximate solution to the inverse problem.

6.2.5. System identification of gap junctional intercellular communication channels of two cancer cell lines.

The main challenge addressed in this work [12], [14] was to assess the relevance of a proposed model-based approach to detect differences between gap junctional intercellular communication channels of two cancer cell lines. To that aim, KB and FaDu, two human head and neck carcinoma cell lines, were used. The former expresses connexin proteins (positive line) while the latter does not (negative line). Moreover, each cell line was tested on spheroid (3-D) and monolayer (2-D) slices and *in vitro* assays were repeated six times. Continuous-time system identification algorithms of the Matlab System Identification and CONTSID toolboxes are tested and applied to a set of *in vitro* data. Results firstly show an acceptable fit of the biological responses but they mainly emphasize the possibility to use several model parameters as statistics to discriminate different cancer cell lines. So, this study exemplifies the potential contribution of dynamic system identification methods and tools to the discovery of new diagnostic biomarkers in systems biology.

6.2.6. Photodynamic therapy modeling and control.

We have also carried on the development of methodological and technological innovations for the realtime control of the therapeutic efficiency in photodynamic therapy (Tylcz:2013). One part of the innovation has been protected by a patent submitted in 2012 (No.1261339, INPI) and extended in 2013. A demonstration platform is currently in development.

6.2.7. Bio-inspired system reliability method.

Based on previously developed works (Keinj, 2011, 2012), we have also proposed in [15] an extension of the target theory in biology applied to system reliability. In this development, we consider rough products

produced by a factory. Each product coming from the plant has m vital elements and some elements can be damaged. To obtain a perfect product (i.e. all the constitutive m elements are safe) all the damaged elements are repaired and a test phase follows. The result of this two-steps procedure is random. We suppose that the number Z_k of non-damaged elements is a Markov chain valued in the set $\{0, 1, \cdots, m\}$, where k is the number of applied repairing-test phases. We have a qualitative result which says that if the repair phase is efficient then $P(Z_k = m)$ is close to 1. As for production of a large number n of products, the former result allows us to give conditions under which either the n elements or a fraction of these n elements are (is) safe after the application of k previous maintenance phases.

6.2.8. *Dynamical Global Sensitivity Analysis as an Early Warning for System's Critical Transition.*

In biology, systems with bifurcations may experience abrupt irreversible and often unwanted shifts in their performance, called critical transitions. For many systems like climate, economy, ecosystems it is highly desirable to identify indicators serving as early warnings of such regime shifts. Several statistical measures were recently proposed as early warnings of critical transitions including increased variance, autocorrelation and skewness of experimental or model-generated data. The lack of automatized tool for model-based prediction of critical transitions led to designing DyGloSA, a Matlab toolbox for dynamical global parameter sensitivity analysis (GPSA) of ordinary differential equations models. One part of our research activity in 2013 was focused on the implementation of a global sensitivity analysis method developed in (Dobre, 2011, 2012) into DyGloSA for dynamical global parameter sensitivity analysis (GPSA) of ordinary differential equations models. This work has been carried out in the context of a collaboration with the University of Luxembourg and more precisely the Thomas Sauter's team. We have shown in [2] that tools developed in this toolbox are efficient to analyze several models with bifurcations and predict the time periods when systems can still avoid going to a critical transition by manipulating certain parameter values, which is not detectable with the existing SA techniques.

6.3. Inference for gaussian systems

Participants: C. Lacaux, S. Tindel

6.3.1. *Inference for dynamical systems driven by Gaussian noises.*

As mentioned at the *Scientific Foundations* Section, the problem of estimating the coefficients of a general differential equation driven by a Gaussian process is still largely unsolved. To be more specific, the most general ($\mathbb{R}$-valued) equation handled up to now as far as parameter estimation is concerned is of the form:

$$X_t^\theta = a + \theta \int_0^t b(X_u)\, du + B_t,$$

where θ is the unknown parameter, b is a smooth enough coefficient and B is a one-dimensional fractional Brownian motion. In contrast with this simple situation, our applications of interest (see the *Application Domains* Section) require the analysis of the following $\mathbb{R}^n$-valued equation:

$$X_t^\theta = a + \int_0^t b(\theta; X_u)\, du + \int_0^t \sigma(\theta; X_u)\, dB_t, \tag{4}$$

where θ enters non linearly in the coefficient, where σ is a non-trivial diffusion term and B is a d-dimensional fractional Brownian motion. We have thus decided to tackle this important scientific challenge first.

To this aim, here are the steps we have focused on in 2013:

- A better understanding of the underlying rough path structure for equation (4), carried out in [6]. This step allows a proper definition of stochastic integrals with respect to fractional Brownian motion in a wide range of contexts.

- Extension of pathwise stochastic integration to processes indexed by the plane in [19], which helps to the definition of noisy systems such as partial differential equations.

- Gaussian type bounds for equations driven by a fractional Brownian motion, obtained in [18], [7]. This is an important preliminary step for likelihood estimates for stochastic processes. Also notice the interesting central limit theorems exhibited in [24], in a context which is similar to our equation of interest.

- Numerical aspects of a maximum likelihood type procedure for an equation of the form (4), expressed in terms of Malliavin calculus tools (see [4]).

6.3.2. LAN property for fractional Brownian motion

We have first focused on an important statistical property of fractional Brownian paths on their own. Indeed, the local asymptotic normality (LAN) property is a fundamental concept in asymptotic statistics, which gives the asymptotic normality of certain estimators such as the maximum likelihood estimator for instance. In [5], we focus on the LAN property for the model where we observe a sample of n observations $\mathbf{X_n} = (X_1, ..., X_n)$ of a Gaussian stationary sequence. The sequence $(X_n)_{n \in \mathbb{N}}$, whose spectral density f_θ is indexed by a parameter θ, can admit antipersistence, long memory or short memory and be noninvertible. To be more specific, our main assumption is:

$$f_\theta(x) \sim_{x \to 0} |x|^{-\alpha(\theta)} L_\theta(x)$$

with L_θ a slowly varying function and $\alpha(\theta) \in (-\infty, 1)$. We prove the LAN property by studying an asymptotic expansion of the log likelihood and using some results on Toeplitz matrices. In particular, our assumptions are fulfilled by fractional Gaussian noises and autoregressive fractionally integrated moving average processes (ARFIMA(p, d, q)). We also obtain the LAN property for fractional Brownian motion.

6.3.3. Self-similarity properties and stable or Gaussian random fields

In 2009, C. Lacaux and H. Biermé carried on the study of some sample paths properties for an important class of anisotropic random fields called operator scaling random fields, which had been previously introduced by H. Biermé, M. Meerschaert and P. Scheffler (2007). To be more specific, the classical self-similarity property is replaced by the following operator scaling property:

$$\forall c > 0, \ \left(X(c^E x) \right)_{x \in \mathbb{R}^d} \stackrel{(d)}{=} c \left(X(x) \right)_{x \in \mathbb{R}^d}, \tag{5}$$

where $c^E := \exp(E \ln(c))$. In particular, the Hölder regularity properties of operator scaling Gaussian or stable harmonizable random fields have been expressed in terms of the matrix E. The method they used can be applied to study the modulus of continuity of many stable or Gaussian random fields. As example in 2011, with P. Scheffler, they have followed it to study multi-operator harmonizable stable random fields, which satisfy a local version of the operator scaling property and enjoy a regularity which may vary along the trajectories. In [20], it has been developed in the more general framework of conditionally sub-Gaussian random series. This allows to also study for example some multistable random fields, which have been introduced in (Falconer & al, 2009); for such a field X, the marginal $X(x)$ is a stable random variable whose index of stability can depend on x. In this paper, some conditions have been proposed to establish the uniform convergence of the series (on an eventually random ball), an upper bound for the modulus of continuity of its limit, an uniform control of the partial series ones and an explicit rate of convergence. Focusing on LePage random series, upper bounds of the modulus of continuity of some harmonizable stable or multistable random fields are provided. In the conference paper [11], [20] has then been applied to study the class of linear multifractional multistable

motions. In particular, the upper bound obtained for the modulus of linear multifractional stable motion is the sharpest available.

We are also interested in self-similar processes indexed by manifolds in [8]. This study is motivated by the fact various spatial data are indexed by a manifold and not by the Euclidean space $\mathbb{R}^d$ in practical situations such as image analysis.

<p style="text-align:center">**MASAIE Project-Team**</p>

5. New Results

5.1. Release of Wolbachia as a preventive action against dengue

We have designed a model of infection by *Wolbachia* of a *Aedes aegypti* population, to take into account the biology of this infection and also the data that can be obtained. The objective is to use this model for predicting the sustainable introduction of this bacteria. We provide a complete mathematical analysis of the model proposed and give the basic reproduction ratio $\mathcal{R}_0$ for *Wolbachia* . We observe a bistability phenomenon. Two equilibria are asymptotically stable : an equilibrium where all the population is uninfected and an equilibria where all the population is infected. A third unstable equilibrium exists. We are in a backward bifurcation situation. The bistable situations occurs with natural biological values for the parameters. Our model is an example of an epidemiological model with only vertical transmission.

This infection model is then connected with a classical dengue model. We prove that for the complete model the equilibrium with *Wolbachia* for the mosquitoes and without dengue for the human is asymptotically stable. We prove that, if a sufficiently great population of infected mosquitoes is introduced, dengue will disappear.

We use the data of a real trial of releases of infected mosquitoes in Cairns (Australia) to calibrate our model. Our model behave remarkably well versus the observed data. We use then the calibrated model to simulate different scenarii of appearance of dengue. We use a pessimistic situation where the basic reproduction ratio $\mathcal{R}_0$ of dengue is 24.5. The simulations confirm our findings, dengue epidemics does not occur, and show that the introduction of *Wolbachia* is a promising way of control dengue.

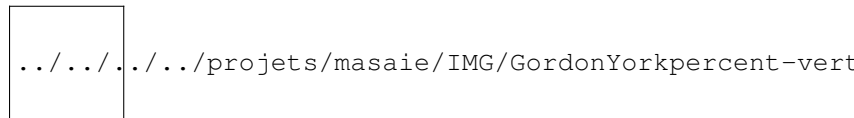`../../../../projets/masaie/IMG/GordonYorkpercent-vert`

Figure 1. Frequencies observed and predicted. The red squares are the frequencies of infection given by the model. The blue circles are the frequencies observed
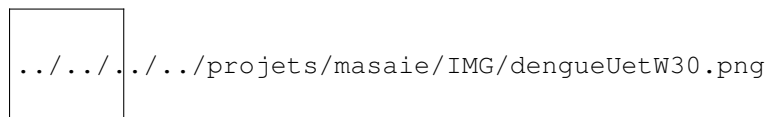
`../../../../projets/masaie/IMG/dengueUetW30.png`

Figure 2. In green the infected human with Wolbachia present. In blue when mosquitoes have not been infected by Wolbachia.

5.2. Arboviruses on urban environments

We investigate the influence of *human movement* for the onset of an arboviral (mosquito-borne) epidemics (such as Dengue, Chikungunya, West Nile or Yellow fever) on an urban environment. The metapopulation

model has a standard SIR (human)/SI (mosquito) model as the basic dynamics on the patches. The nodes consist of notification districts used by public health authorities. The subsystems are coupled by human movement. Our main result provides quantitative relations between three reproduction numbers: *local* - at each isolated subsystem, *uniform* or *mixing* - aggregating the data of the whole region, and the *network* reproduction number - for the coupled dynamics. We observe that the epidemics can spread among the patches as a consequence solely of human movement: while all nodes may have, if isolated, local reproduction ratio less than one and, moreover, the uniform reproduction number being also less than one, however, the network reproduction number can be greater than one. An estimate is provided on the overall effect of vector control on a chosen patch [13].

5.3. Analysis of the dynamics of some models for vector-borne diseases with host circulation

In this work we study the dynamics of a vector borne disease on a metapopulation model that accounts for host circulation. For such models, the movement network topology gives rise to a contact network topology, corresponding to a bipartite graph. Under the assumption that the contact network is strongly connected, we can define the basic reproductive number R_0 and show that this system has only two equilibria: the so called disease free equilibrium (DFE); and a unique interior equilibrium that exists if, and only if, the basic reproduction number, R_0, is greater that unity. We are also able to show that the DFE is globally asymptotically stable, if $R_0 \leq 1$. If $R_0 > 1$, the dynamics is uniformly persistent and, with further assumptions on the contact network structure, we also show that the endemic equilibrium (EE) is globally asymptotically stable [17].

5.4. Analysis and observer design for a schistosomiasis model

Human schistosomiasis is a behavioral and occupational disease associated with poor human hygiene, insanitary animal husbandry and economic activities. Among human parasitic diseases, schistosomiasis ranks second behind malaria as far as the socio-economic and public health importance in tropical and subtropical areas are concerned. The spread and persistence of schistosomiasis have made of it one of the most complex host-parasite process to model mathematically because of the different steps of growth of larvae assumed by the parasite and the requirement of two host elements (definitive human host and intermediate snail hosts) during their life cycle.

An efficient method to control the schistosomiasis infection that may require relatively little funding is a biological control. Particularly, trematode parasites or competitive snails of the intermediate snail hosts have been proved to be effective in controlling schistosomiasis in the Caribbean area.

We have studied a schistosomiasis infection model that involves human and intermediate snail hosts as well as an additional mammalian host and a competitor snail species. This mathematical analysis of the model gives insight about the epidemiological consequences of the introduction of a competitor resistant snail species [15].

We have also proposed a solution to the state estimation problem for a schistosomiasis infection dynamical model described by a continuous non linear system when only the infected human population is measured. We have constructed an estimator that is able to give dynamical estimates of the variables that can not be measured [14].

6. New Results

6.1. From the microscopic to the mesoscopic scale

Participants: Axel Hutt, Laure Buhry, Meysam Hashemi, Pedro Garcia Rodriguez, Peter beim Graben, James Wallace Sleigh.

Several previous studies focus on the derivation of neural population models. However most of these studies do not consider explicitly the microscopic properties of neurons, such as synaptic receptor dynamics or ion-channel distributions, although they may be implicit. The resulting models in some previous studies are poorly tractable analytically due to their complexity. Moreover, the complexity of previous models makes it difficult to discover those elements in the model that induce certain dynamical features as observed in experiments. Essentially most of previous studies do not consider the spatial interactions of neurons and, importantly, neglect delays present in biological networks. We aim to improve some previous models and a first step to a new statistical approach has been developed [11], [18], [17], [22] to bridge the scales between the network activity of coupled spiking single neurons and statistical quantities of populations, e.g., the mean membrane potential in the network and the networks population firing rate. Our work considers the specific effect of anaesthetics and takes into account the physiological effects of extra-synaptic $GABA_A$-receptors at single neurons, which are highly sensitive to anaesthetic drugs, such as propofol. We find numerically by simulation of a spiking neural network that propofol on single neuron level diminishes the network oscillation power in the $\alpha-$frequency band and affects strongly the spike coherence in the population. Such effects have been shown in previous experimental data obtained during propofol anaesthesia demonstrating the importance of extra-synaptic receptor dynamics in the understanding of experimental phenomena in anaesthesia.

The neural origin of generation and planning of motor action in humans is still unknown. In this context, psychophysical experiments and the neural modeling of the gained results may lead to further insight. We have participated in an experimental and theoretical study [8] to reveal the effect of temporal attention on non-conscious prime processing. Our stochastic accumulator model improves extensively the standard accumulator model for reaction time by involving additional stochastic neural accumulators, which permits an almost perfect fit to experimental data. The model indicates that motor action, which is generated on a population level, obeys a stochastic accumulation of activity of single neuron activity.

6.2. From the mesoscopic to the behavior scale

Participants: Axel Hutt, Laurent Bougrain, Eric Nichols, Maxime Rio, Carolina Saavedra, Louis Korczkovsky, Alexandre Martin, Pierre-Jean Morieux.

To link neural population activity to behavior, it is necessary to understand well the dynamic properties of population models which we have studied in general models [5], [14], [15], [16], [24]. To this end, we have analyzed a neural mass model [4] describing the neural population activity subject to synaptic anaesthetic action to explain characteristic signal features in measured EEG. The model explains the gain of power in the $\alpha-$ and $\delta-$frequency observed experimentally by a dynamic oscillatory instability (Hopf instability). The model considers a cortical population only and hence the result indicates that the experimental feature observed may originate in the cortex.

An extended population model considers not only the cortex but a feedback-loop to the thalamus. This model involves a delayed interaction. At first, we have studied the dynamics of delayed dynamical systems subject to additive stimuli [23], [7], [6] to learn more about the expected activity. Our first study of a linear thalamo-cortical feedback model [21], [20] reveals the descriptive power of neural mass models to describe EEG under anaesthesia.

In order to learn more about the effect of anaesthetics on neural populations, we have participated in the data analysis of an experimental study on anaesthesia in animals [9]. Moreover we have started developing new data analysis techniques to extract novel features from EEG. In his doctoral thesis, Maxime Rio has developed a new method to detect transient amplitude synchronization in multi-variate time series in a subset of time series [1]. Carolina Saavedra has conducted wavelet analysis in her thesis to improve the denoising in BCI-relevant measured signals [2]. Another study [3] proposes a new recurrence plot-technique based on symbolic dynamics. It extracts spatio-temporally recurrence patterns in a multivariate dataset which reflect underlying neural recurrent dynamics.

The event-related potentials (ERP) in EEG are important markers of cognitive processes in the brain and serve as features to control interfaces in BCI. We have performed advanced studies to improve the detection of ERP [13], [12].

6. New Results

6.1. Electrophysiology

Cardiac arrhythmia is a very frequent pathology that comes from an abnormal electrical activity in the myocardium. This work aims at developing a training simulator for interventional radiology and thermo-ablation of these arrhythmias. After tackling the issue of fast electrophysiology, a first version of our training simulator was proposed.

../../../../projets/shacra/IMG/Electrophysiology.png

Figure 3. Cardiac electrophysiology computed on a patient-specific geometry

The first main contribution of this work is the interactive catheter navigation inside a moving venous system and a beating heart. The virtual catheterization reproduces navigation issues that can be solved using a bending catheter. Second, our real-time GPU electrophysiology model allows interactions during the simulation such as extra-cellular potential measurement, RF ablation, and electrical stimulation. An innovative management of the computational units based on multithreading offers performances close to real-time. This framework is therefore a substantial step towards realistic and highly efficient virtual training systems in cardiology. As future work, we intend to use patient-specific data in our framework so that cardiologists could quantitatively assess the realism of our virtual training.
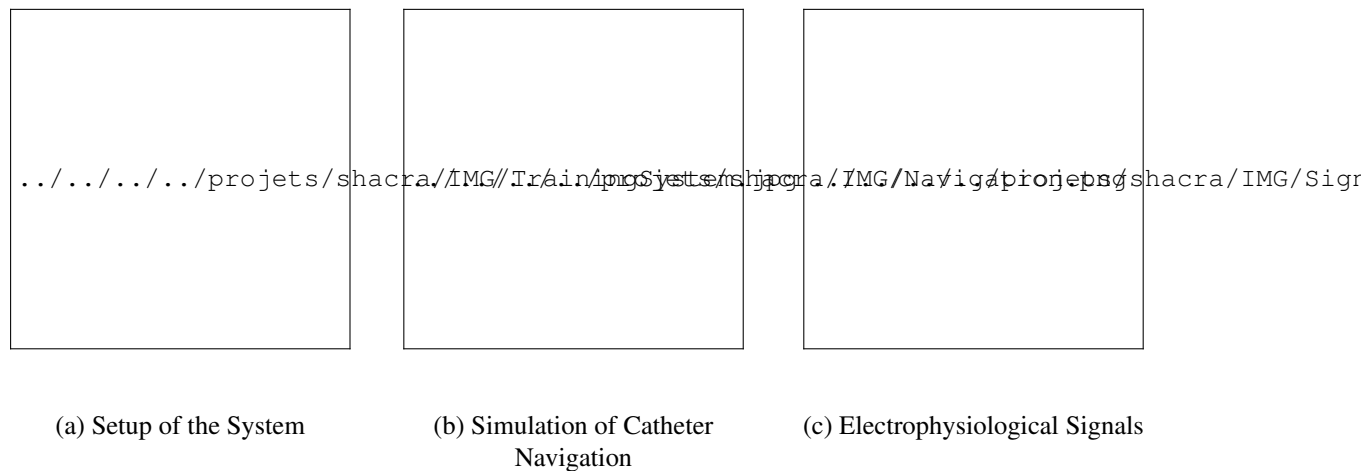
../../../../projets/shacra/IMG/Train.jpg ../../../../projets/shacra/IMG/Naviga ../../../../projets/shacra/IMG/Sign

(a) Setup of the System   (b) Simulation of Catheter   (c) Electrophysiological Signals
                                      Navigation

Figure 4. The first simulation dedicated to electrocardiology training

6.2. Cryoablation

A new project started this year around cryotherapy. This technique consists in inserting needles that freezing the surrounding tissues, thus immediately leading to cellular death of the tissues. Cryoablation procedure is used in many medical fields for tumor ablation, and even starts being used in cardiology. In this scope, we build a simulator able to place the cryoprobes and run a simulation representing the evolution of iceballs in living tissues.
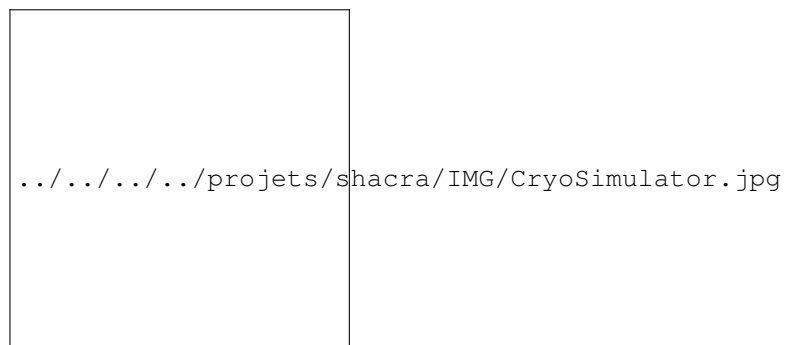
../../../../projets/shacra/IMG/CryoSimulator.jpg

Figure 5. Simulation framework for cryoablation planning

6.3. Stapedotomy

Stapedotomy is a challenging procedure of the middle ear microsurgery, since the surgeons is in direct contact with sensitive structures such as the ossicular chain. This procedures is taught and performed in the last phase of the surgical apprenticeship. To improve surgical teaching, we propose to use a virtual surgical simulator based on a finite element model of the middle ear. The static and dynamic behavior of the developed finite element model was successfully compared to published data on human temporal bones specimens. A semi-automatic algorithm was developed to perform a quick and accurate registration of our validated mechanical

atlas to match the patient dataset. This method avoids a time-consuming work of manual segmentation, parameterization, and evaluation. A registration is obtained in less than 260 seconds with an accuracy close to a manual process and within the imagery resolution. The computation algorithms, allowing carving, deformation of soft and hard tissus, and collision response, are compatible with a real-time interactive simulation of a middle ear procedure. As a future work, we propose to investigate new robotized procedures of the middle ear surgery in order to develop new applications for the RobOtol device and to provide a training tool for the surgeons.

../../../../projets/shacra/IMG/ENT.png

Figure 6. Simulation of the stapedotomy procedure.

6.4. Radiotherapy planning

The main challenge of radiotherapy treatment is to irradiate the tumor while sparing the surrounding healthy tissues. In the case of throat cancer, the complexity of the therapy treatment is due to the proximity of organs at risk such as the two parotide glands. The parotide glands are the main salivary glands. An overdose of radiation in these glands may cause xerostomia, which is a medical term for the symptom of dryness in the mouth, or in other words, a lack of saliva. This disease affect significantly the life of the patient: difficulty talking, tasting, chewing, swallowing, excessive thirst, constant pain in the throat etcetera. A radiation therapy treatment of throat cancer takes from 5 to 7 weeks. The treatment is planned several days before the therapy. The planning consist in contouring each organ of the area on CT-scan images and defining the dose of radiation to deliver to each of these organs. This stage is lengthy and takes around two hours per patient. Yet, some anatomical variations occur in the course of the treatment, mainly due to the weight loss of the patients. These variations compromise the safety of the healthy tissues, because the planned treatments is no more up to date. For now, the physicians have no solution goog enough to handle these changes. Xerostomia affects around 20 per-cent of the patients suffering from throat cancer.

The main idea of this work is to create an interface that the physicians could use to redo the planning when it is needed, when the anatomical changes are significant. The purpose is to give to them the possibility to use what they see on images, to recreate the right shape of the contours without recontouring each images, and in a reasonable time. This interface will use their knowledge to determine the new shape of the organs. The work does not aim at providing a fully automatic method because it would reduce its acceptation by the physicians. As the method is based on the input of the physician, they can control the deformation based on images but also on their knowledge.

6.5. Image-based diagnoses

In the context of the female pelvic medicine, image-based diagnoses of pelvic floor disorders like prolapse or endometriosis rely on mechanical indicators, such as mobilities of organs and shear displacements between
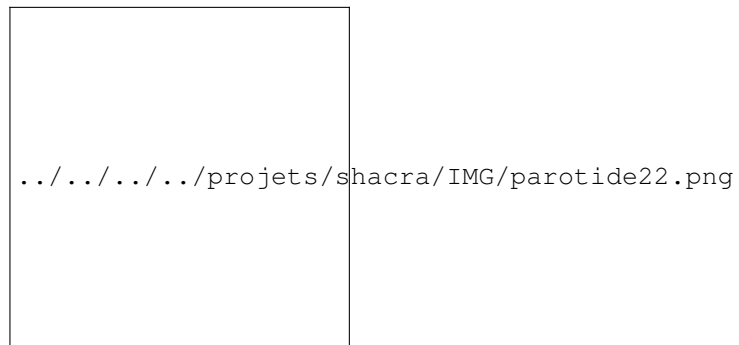
Figure 7. Screenshot of our radotherapy planning tool.

organs. This information would be useful for both precise diagnoses and planning of surgical procedure. Involving numerical tools for diagnoses and surgery planing becomes increasingly interesting for physicians in clinical uses. The advantages of numerical models are not only in visualization, but also in quantitative measurements on a group of organs, such as their shapes and their relative movements. The processing pipeline includes patient data retrieval, image analysis, patient-specific modeling and biomechanical simulation. Our work consists in proposing new methods and algorithms for modeling the 3D anatomy of specific patients based on image data. This model should be compatible with the requirements of a biomechanical simulation. Moreover, we aim at developing new image processing tools for analyzing 2D dynamic MRI (to assess the mobilities of the pelvic system by extracting certain mechanical indicators from images) and for comparison with simulations.

Registration between geometric models and images remains a major challenge in these applications. We proposed a new model-to-image registration approach which was developed and tested for segmentation of organs in 2D images and for tracking the motion of pelvic organs from 2D dynamic MRI. Thanks to this technique, evaluation of the level of shear strain that is encountered by the fascias (connective tissues between organs) during the motion became possible. This tool could help in early diagnostic of prolapse. In the next step, our objective is to extend this method for adapting it to 3D reconstruction (with 3D geometric models and 3D MR images) and for the comparison of 3D simulations with deformable images.

6.6. Dynamic Deformations Simulated at Different Frequencies

The dynamic response of deformable bodies varies significantly in dependence on mechanical properties of the objects: while the dynamics of a stiff and light object (e. g. wire or needle) involves high-frequency phenomena such as vibrations, much lower frequencies are sufficient for capturing dynamic response of an object composed of a soft tissue. Yet, when simulating mechanical interactions between soft and stiff deformable models, a single time-step is usually employed to compute the time integration of dynamics of both objects. However, this can be a serious issue when haptic rendering of complex scenes composed of various bodies is considered. In this work, we present a novel method allowing for dynamic simulation of a scene composed of colliding objects modelled at different frequencies: typically, the dynamics of soft objects are calculated at frequency about 50 Hz, while the dynamics of stiff object is modeled at 1 kHz, being directly connected to the computation of haptic force feedback. The collision response is performed at both low and high frequencies employing data structures which describe the actual constraints and are shared between the high and low frequency loops. During the simulation, the realistic behaviour of the objects according to the mechanical principles (such as non-interpenetration and action-reaction principle) is guaranteed. We have shown several scenarios involving different bodies in interaction, demonstrating the benefits of the proposed method. This research has been published at IROS 2013.

6.7. Simulation of Lipofilling Reconstructive Surgery

We have developed a method to simulate the outcome of reconstructive facial surgery based on fat-filling. Facial anatomy is complex: the fat is constrained between layers of tissues which behave as walls along the face; in addition, connective tissues that are present between these different layers also influence the fat-filling procedure. To simulate the end result, we have proposed a method which couples a 2.5D Eulerian fluid model for the fat and a finite element model for the soft tissues. The two models are coupled using the computation of the mechanical compliance matrix. We had two contributions: a solver for fluids which couples properties of solid tissues and fluid pressure, and an application of this solver to fat-filling surgery procedure simulation. This research has been published at MICCAI 2013.

6.8. Real-time simulation of contact and cutting of heterogeneous soft-tissues

We have developed a new numerical method for interactive (real-time) simulations, which considerably improves the accuracy of the response of heterogeneous soft-tissue models undergoing contact, cutting and other topological changes. It provides an integrated methodology able to deal both with the ill-conditioning issues associated with material heterogeneities, contact boundary conditions which are one of the main sources of inaccuracies, and cutting which is one of the most challenging issues in interactive simulations. Our approach is based on an implicit time integration of a non-linear finite element model. To enable real-time computations, we propose a new preconditioning technique, based on an asynchronous update at low frequency. The preconditioner is not only used to improve the computation of the deformation of the tissues, but also to simulate the contact response of homogeneous and heterogeneous bodies with the same accuracy. We also address the problem of cutting the heterogeneous structures and propose a method to update the preconditioner according to the topological modifications. Finally, we have applied our approach to three challenging demonstrators: i) a simulation of cataract surgery ii) a simulation of laparoscopic hepatectomy iii) a brain tumor surgery. This research was done in collaboration with the University of Cardiff and has been published in the journal Media this year.

6.9. Control of Elastic Soft Robots

In this work, we present a new method for the control of soft robots with elastic behavior, piloted by several actuators. The central contribution of this work is the use of the Finite Element Method (FEM), computed in real-time, in the control algorithm. The FEM based simulation computes the nonlinear deformations of the robots at interactive rates. The model is completed by Lagrange multipliers at the actuation zones and at the end-effector position. A reduced compliance matrix is built in order to deal with the necessary inversion of the model. Then, an iterative algorithm uses this compliance matrix to find the contribution of the actuators (force and/or position) that will deform the structure so that the terminal end of the robot follows a given position. Additional constraints, like rigid or deformable obstacles, or the internal characteristics of the actuators are integrated in the control algorithm. We illustrate our method using simulated examples of both serial and parallel structures and we validate it on a real 3D soft robot made of silicone.

<p align="center" style="color:red">ALGORILLE Project-Team</p>

6. New Results

6.1. Structuring applications for scalability

In this domain we have been active on several research subjects: efficient locking interfaces, data management, asynchronism, algorithms for large scale discrete structures and the use of accelerators, namely GPU.

In addition to these direct contributions within our own domain, numerous collaborations have permitted us to test our algorithmic ideas in connection with academics of different application domains and through our association with SUPÉLEC with some industrial partners: physics and geology, biology and medicine, machine learning or finance.

6.1.1. Efficient linear algebra on accelerators.

Participants: Sylvain Contassot-Vivier, Thomas Jost.

The PhD thesis of Thomas Jost, co-supervised by S. Contassot-Vivier and Bruno Lévy (Alice INRIA team) since January 2010, dealt with specific algorithms for GPUs, in particular linear solvers [32]. He also worked on the use of GPUs within clusters of workstations via the study of a solver of non-linear problems [30], [33], [29]. The defense of this thesis was initially planned in January 2013 but Thomas decided at the end of 2012 to stop his PhD and to leave for industry.

6.1.2. Development methodologies for parallel programming of clusters.

Participants: Sylvain Contassot-Vivier, Jens Gustedt, Stéphane Vialle.

We have conducted a particular effort in merging and synthesizing our respective experiences of parallel programming of clusters (homogeneous, heterogeneous, hybrid). This has lead to two book chapters [19] and [34] (to appear).

6.1.3. Combining locking and data management interfaces.

Participants: Jens Gustedt, Stéphane Vialle, Soumeya Leila Hernane, Rodrigo Campos-Catelin.

Handling data consistency in parallel and distributed settings is a challenging task, in particular if we want to allow for an easy to handle asynchronism between tasks. Our publication [4] shows how to produce deadlock-free iterative programs that implement strong overlapping between communication, IO and computation. The thesis of Soumeya Hernane [12] has been defended in 2013. It extends distributed lock mechanisms and combines them with implicit data management.

A new implementation (ORWL) of our ideas of combining control and data management in C has been undertaken, see 5.2.1 . In 2013, work has demonstrated its efficiency for a large variety of platforms, see [22]. By using the example of dense matrix multiplication, we show that ORWL permits to reuse existing code for the target architecture, namely open source library ATLAS, Intel's compiler specific MKL library or NVidia's CUBLAS library for GPUs. ORWL assembles local calls into these libraries into efficient functional code, that combines computation on distributed nodes with efficient multi-core and accelerator parallelism.

Additionally, during the internship of Rodrigo Campos-Catelin, a detailed instrumentation of the ORWL library has been undertaken, and a new, less expensive strategy for cyclic FIFOs has been tested. This work will be continued with a master thesis at the university of Buenos Aires that will summarize and extend the results that were achieved during the internship.

Our next efforts will concentrate on the continuation of an implementation of a complete application (an American Option Pricer) that was chosen because it presents a non-trivial data transfer and control between different compute nodes and their GPU. ORWL is able to handle such an application seamlessly and efficiently, a real alternative to home made interactions between MPI and CUDA.

6.1.4. Discrete and continuous dynamical systems.

Participants: Sylvain Contassot-Vivier, Marion Guthmuller.

The continuous aspect of dynamical systems has been intensively studied through the development of asynchronous algorithms for solving PDE problems. In past years, we have focused our studies on the interest of GPUs in asynchronous algorithms [29]. Also, we have investigated the possibility to insert periodic synchronous iterations inside the asynchronous scheme in order to improve the convergence detection delay. This is especially interesting on small/middle sized clusters with efficient networks. The SimGrid environment has been used to validate and evaluate load balancing strategies in parallel iterative algorithms on large scale systems [28].

In 2011, the PhD thesis of Marion Guthmuller, supervised by M. Quinson and S. Contassot-Vivier, has started on the subject of model-checking distributed applications inside the SimGrid simulator [31]. The expected results of that work may provide a very interesting tool for studying dynamical systems expressed under the form of a distributed application.

6.2. Transparent Resource Management for Clouds

Participants: Julien Gossa, Rajni Aron, Stéphane Genaud, Étienne Michon, Marc-Eduard Frîncu.

6.2.1. Provisioning strategies.

Our main achievement was the design of one comprehensive provisioning meta-strategy. This meta-strategy only use one parameter as a deadline given by the user. Contrary to other deadline-based provisioning strategies, our meta-strategy is able to combine any provisioning strategy in order to optimize the cost while meeting the deadline. This is achieved through simulation of cost and makespan of every available strategy thanks to SCHIaaS5.4.3 . It allows to apply the most inexpensive strategy as long as possible, before progressively switching to more expensive strategy when the deadline becomes closer.

The next step is to asses this meta-strategy among an important set of applications and platforms, both in real environments and simulation. The data are currently gathered and analyzed, and we should be able to draw conclusions soon.

6.2.2. User workload analysis.

We have conducted one broad study about workflows execution on the cloud, from both the theoretical and experimental point of view. In this study, we tried to discover causalities between the characteristics of workflows and the performances of provisioning strategies. We concluded that, except very peculiar cases, no causality can be identified. That is why we decided to make use of simulation to predict the strategies performances.

This predictive process is now integrated as a module of our cloud broker. It can be invoked by a user to help him decide which strategy should be used before any actual resource leasing.

We are now convinced that workload analysis is not a suitable approach because of its lack of generality.

6.2.3. Experimentations.

Given the very large consumption of CPU hours, the above work was supported mostly by simulation. We have assessed the gap between the performances of real executions on a private cloud and simulation. The latter proved to be very accurate, predicting almost perfectly the cost and makespan of every strategy on a wide range of workloads.

However, we have also shown that the simulation can be very sensitive to user defined input parameters (such as task runtimes) and may be mislead in borderline cases. Identifying the pitfalls and limitations of the simulation is very important and should end up in recommendations for a wise interpretation of simulation results.

We have also extended the range of experimentations to assess our simulator. First, we have extended the set of simulations with new applications, mostly workflows that are both generated and real applications (i.e. Montage). Second, we have conducted intensive experimentations on new platforms (i.e. Bonfire). The experimental data we have recently gathered in both cases is to be analyzed to further validate our approach.

6.3. Experimental methodologies for the evaluation of distributed systems

This year, M. Quinson defended his Habilitation on the experimental methodologies of distributed systems [13]. This concludes 10 years of research on this topic (including the elements presented in this section), and paves the road of future research.

6.3.1. Simulation and dynamic verification

6.3.1.1. MPI simulation
Participants: Martin Quinson, Paul Bédaride, Marion Guthmuller.

We continued our long-term effort toward the simulation of HPC application within SimGrid. We slightly increased the API coverage of our reimplementation of MPI on top of SimGrid, and proposed a new model of the network performance for MPI applications on top of Ethernet TCP networks. This model combines the advantages of flow-based networks for large data transfers as previous SimGrid network models, but also leverage algorithmic performance models extending the classical LogP models. As shown in [16], these models greatly improve the realism of MPI simulations, enabling the prediction of the performance of a non-trivial application in great details.

6.3.1.2. Dynamic verification and SimGrid
Participants: Marion Guthmuller, Martin Quinson, Gabriel Corona.

This year, our work toward the verification of liveness properties within SimGrid became fully functional thanks to the PhD work of M. Guthmuller. This relies on a system-level introspection mechanism allowing the model checker to finely explore the state of the verified programs. This is mandatory to detect the execution cycles that constitute the counter examples to liveness properties. This introspection mechanism is also used to implement a new reduction mechanism that can mitigate the state space explosion problem. A publication presenting these results is currently under review.

6.3.1.3. SimGrid framework improvement
Participants: Paul Bédaride, Martin Quinson, Gabriel Corona.

We rolled out a new major version of the SimGrid framework to our users. It contains both the HPC network models used to improve the prediction of MPI applications and all of our developments toward the dynamic verification of distributed applications. We also improved further the usability of our framework, that is now properly integrated within the Debian Linux distribution.

The next release is already underway, with a proper integration of the work from our partners on virtual machines and with a full reimplementation of the simulation kernel in C++ for a better modularity.

6.3.1.4. Formal Verification of Distributed Algorithms
Participants: Esteban Campostrini, Martin Quinson, Stephan Merz.

M. Quinson co-advised an internship with S. Merz (project-team Veridis) on the formal verification of distributed algorithm. The goal was to push further the PlusCal algorithmic language and its compiler to TLA$^+$ on which we are working since several years within the Veridis team.

We wanted to explore some hard problem raised by the verification of distributed protocol, such as how to represent timeout errors in verification settings where the time is not present. We think that this could be modeled somehow similarly to fairness properties, but more work is needed in this topic for a definitive answer.

6.3.2. Experimentation on testbeds and production facilities, emulation

6.3.2.1. Distem improvements: scalability and matrix-based inter-nodes latencies
Participants: Ahmed Bessifi, Emmanuel Jeanvoine, Lucas Nussbaum.

(For context, see sections 3.3 and 5.3 .)

Following our PDP'13 publication[18], we focused on improving Distem's scalability. First, on the Distem engine side, we parallelized the startup of physical nodes and virtual nodes, and added support for BTRFS snapshots to enable starting a very large number of virtual nodes with their own filesystems. Second, during the internship of Ahmed Bessifi we investigated several networking issues causing problems with large-scale experiments (over 4000 virtual nodes). The resulting improvements to ARP parameters tunings were integrated in Distem 0.8, and enabled network-intensive experiments with up to 8000 virtual nodes. We plan to publish those results in early 2014.

In the context of the AEN HEMERA project, we worked with Trong-Tuan Vu (EPI DOLPHIN, Inria Lille Nord Europe) to add support for specifying inter-nodes latencies using a matrix. This is especially useful for experiments on load-balancing and locality.

6.3.2.2. Evaluating load balancing HPC runtimes with Distem
Participants: Joseph Emeras, Emmanuel Jeanvoine, Lucas Nussbaum.

(For context, see sections 3.3 and 5.3 .)

We aim at demonstrating the suitability of Distem to evaluate Exascale and Cloud runtime environments providing load balancing and fault tolerance features. In that context, we reproduced some experiments published at CCGrid'2013 on Charm++ load balancers. Preliminary results are promising, and we hope that this will lead to collaborations with runtime developers.

A publication presenting how Distem to test HPC runtimes (scalability, fault tolerance and load balancing capabilities) is in the works.

6.3.2.3. Further improvements to XPFlow
Participants: Tomasz Buchert, Lucas Nussbaum, Jens Gustedt.

(For context, see sections 3.3 and 5.6 .)

We strengthened our XPFlow experiment control system using several sets of experiments, including experiments on the OpenStack IaaS Cloud stack on hundreds of Grid'5000 nodes.

A publication describing XPFlow was submitted to CCGrid'2014[21].

6.3.2.4. Further improvements to Kadeploy
Participants: Luc Sarzyniec, Emmanuel Jeanvoine, Lucas Nussbaum.

(For context, see sections 3.3 and 5.5 .)

We continued the development of Kadeploy:

- The support for multi-partition images was added;
- The communication interface between the Kadeploy server and the Kadeploy client was completely rewritten to use a REST API;
- A test framework, integrated with Inria's Continuous Integration facility, was added.

Two new Kadeploy releases were published during 2013, including those changes.

6.3.2.5. Grid'5000
Participants: Sébastien Badia, Luc Sarzyniec, Émile Morel, Lucas Nussbaum.

(For context, see sections 3.3 and 5.7 .)

The team continued to support Grid'5000. Highlights of 2013 include:

- Lucas Nussbaum is now a member of the *Bureau* and *Comité d'Architectes* of GIS Grid'5000. In the context of the *Comité d'Architectes*, he led the writing on several internal documents (on possible evolutions of the testbed).

- An article describing Grid'5000's support for experiments on IaaS Clouds[15] was published at the *Testing The Cloud* workshop.

- A new cluster, *graphite*, was installed in Nancy.

6.3.3. Convergence and co-design of experimental methodologies

6.3.3.1. Practical study on combining experimental methodologies

Participants: Maximiliano Geier, Lucas Nussbaum, Martin Quinson.

During an internship, we explored how simulation, emulation and experimentation on Grid'5000 could be combined in practice. Starting with a simple question on a particular system, we used a representative framework for each methodology: SimGrid for simulation, Distem for emulation and Grid'5000 for experimentation, and described our experiments using the workflow logic provided by the XPFlow tool. We identified a set of pitfalls in each paradigm that experimenters may encounter regarding models, platform descriptions and others. We proposed a set of general guidelines to avoid these pitfalls. We showed these guidelines may lead to accurate simulation results. Finally, we provided some insight to framework developers in order to improve the tools and thus facilitate this convergence.

The results of this work were published at the *WATERS* workshop[17].

6.3.3.2. Organization of an event on reproducible research

Participant: Lucas Nussbaum.

We organized Realis, an event aiming at testing the experimental reproducibility of papers submitted to Compas'2013. Associated to the Compas'13 conference, this workshop aimed at providing a place to discuss the reproducibility of the experiments underlying the publications submitted to the main conference. We hope that this kind of venue will motivate the researchers to further detail their experimental methodology, ultimately allowing others to reproduce their experiments.

<p style="text-align:center;color:red;font-weight:bold">MADYNES Project-Team</p>

6. New Results

6.1. Android Security

Participants: Olivier Festor, Abdelkader Lahmadi [contact], Eric Finickel.

Android-based devices include smart phones and tablets that are now widely adopted by users because they offer a huge set of services via a wide range of access networks (WiFi, GPRS/EDGE, 3G/4G). Android provides the core platform for developing and running applications. Those applications are available to the users over numerous online marketplaces. These applications are posted by developers, with little or no review process in place, leaving the market self-regulated by users. This policy generates a side-effect where users are becoming targets of different malicious applications which the goal is to steal their private information, collect all kind of sensitive data via sensors or abusing granted permissions to make surtaxed calls or messages. To address this security issue, monitoring the behaviour of running applications is a key technique enabling the identification of malicious activities.

During 2013, we have designed and extended a monitoring framework integrating observed network and system activities of running Android applications. We extended and enhanced our modular NetFlow probe [48] running on android devices to export observed network flow records to a collection point for their processing and analysis. Our embedded probe includes a new set of IPFIX information elements that we have designed [41] to encapsulate geographic location information within exported flows. This work was done in collaboration with the Univerisity of Twente, where they developed the flow collector and the analysis application.

We have also developed an embedded logging probe that exports available logs generated by an Android device to a big data enabled store [25]. We have analyzed the collected logs using TreeMapping visualization technique [46] to display behavioral graphs of Android applications. The generated graphs are able to provide an aggregated view of the different components of a running application. This view is useful to improve the understanding of the behaviour of an application.

6.2. Sensor networks monitoring

Participants: Rémi Badonnel, Alexandre Boeglin, Isabelle Chrisment, Olivier Festor, Abdelkader Lahmadi [contact], Anthea Mayzaud, Bilel Saadallah.

Low Power and Lossy Networks (LLNs) are made of interconnected wireless devices with limited resources in terms of energy, computing and communication. The communication channels are low-bandwidth, high loss rate and volatile wireless links subject to failure over time. They are dynamic and the connectivity is limited and fluctuant over time. Each node may loss frequently its connectivity with its neighborhood nodes. In addition, link layer frames have high constrains on their size and throughput is limited. These networks are used for many different applications including industrial automation, smart metering, environmental monitoring, homeland security, weather and climate analysis and prediction. The main issue in those networks is optimal operation combined with strong energy preservation. Monitoring, i.e the process of measuring sampled properties of nodes and links in a network, is a key technique in operational LLNs where devices need to be constantly or temporally monitored to assure their functioning and detect relevant problems which will result in an alarm being for- warded to the enterprise network for analysis and remediation.

We developed and designed a novel algorithm and a supporting framework [16] that improves a distributed poller-pollee based monitoring architecture. We empower the poller-pollee placement decision process and operation by exploiting available routing data to monitor nodes status. In addition, monitoring data is efficiently embedded in any messages flowing through the network, drastically reducing monitoring overhead. Our approach is validated through both simulation, implementation and deployment on a 6LoWPAN-enabled network. Results demonstrate that our approach is less aggressive and less resource consuming than its competitors.

In a previous work, we developed a first fully operational content centric networking protocol stack (CCNx) dedicated to a wireless sensor network. During this year, we have extended this implementation and designed a novel monitoring service [32] to efficiently aggregate data in a WSN. The developed solution has been implemented in the Contiki operating system and evaluated using the Cooja simulator. We have compared the performance of our proposed solution with the SPIN protocol in terms of the number of exchanged messages and response times. Our results show that our solution provides better performance for collecting and aggregating data inside the network using operators such as maximum or average.

This year, we also analyzed security attacks against LLN networks, and more specifically those targeting the RPL routing protocol. In that context, we introduced a taxonomy in order to classify these attacks into three main categories. The attacks against resources, such as DIS flooding attacks and increased rank attacks, permit to reduce the network lifetime through the generation of fake control messages or the building of RPL loops. The attacks against the topology, such as wormhole attacks or DAO inconsistency attacks, permit the network to converge to a sub-optimal configuration or to isolate one or several nodes. Finally, attacks against network traffic, such as eaves-dropping attacks and decreased rank attacks, permit to capture and analyse large part of the RPL traffic.

Based on this taxonomy, we compared the properties of attacks and discussed methods and techniques for monitoring them. In particular, we are investigating efficient solutions for supporting security monitoring in these resource-constrained environments [17]. We considered DODAG inconsistency attacks as a first case study. Scenarios were constructed to evaluate the performance of the RPL network when such attacks are carried out. Via an implementation in Contiki, it was identified that the internal mechanism proposed by RPL, which involves ignoring packets with the appropriate IPv6 header after a fixed threshold is reached, uses an arbitrary value for the threshold. A new function that dynamically scales this threshold was developed to improve performance of the network while under attack. In addition, a comparative study between the (1) no threshold, (2) fixed threshold and (3) dynamic threshold scenarios has been performed.

6.3. Monitoring of anonymous networks

Participants: Isabelle Chrisment [contact], Olivier Festor, Juan Pablo Timpanaro.

Anonymous networks have emerged to protect the privacy of network users and to secure the data exchange over the Internet. Nevertheless, the monitoring of these networks has not been investigated very much and only few networks have been studied. Large scale monitoring on these systems allows us to understand how they behave and which type of data which is shared among users.

In 2013, we continued our research about anonymous systems, with a special focus on the I2P network [3]. The I2P network provides an abstraction layer to permit two parties to communicate in an anonymous and secure manner. This network is optimized for anonymous web hosting and anonymous file-sharing. I2P's file-sharing community is highly active, where users deploy their file-sharing applications on top of the network. I2P uses a variation of Onion routing, thus assuring the unlinkability between a user and its file-sharing application.

Current statistics service for the I2P network do not provide values about the type of applications deployed in the network nor the geographical localization of users. We conducted the first large-sale monitoring on the I2P anonymous system, characterizing users and services running on top of the network. We first designed and implemented a distributed monitoring architecture based on probes placed in the I2P's distributed hash table (I2P's netDB), which allows us to collect a vast amount of network metadata. So, our distributed monitoring architecture provides us with different insights about the I2P network.

We were able to detect the behavior of particular applications, notably their period of activity. By considering the behavior of a particular anonymous service along with a particular set of I2P users, we determined in which measure this set of users was responsible for the activity of the anonymous service. We thus conducted a correlation analysis between the behavior of I2P users from two top cities along with the behavior of anonymous file-sharing clients (I2PSnark clients) throughout a particular period of time. By applying

---

[3]http://i2p2.de

Pearson's correlation coefficient, we achieved a group-based characterization and we determined that the activity of users from those cities explained 38% of all detected file-sharing activity [22], [2].

Starting from our limitations to de-anonymise a particular I2P user, we studied I2P's unidirectional tunnels and the mechanism used to create these tunnels. We discovered a vulnerability in this mechanism, vulnerability which allows an attacker to detect whether a user is the last participant in an inbound tunnel. With this knowledge, we showed that it would be possible to attack an I2P's eepsite in order to de-anonymise the eepsite's operator [39].

6.4. Configuration security automation

Participants: Rémi Badonnel [contact], Martin Barrere, Olivier Festor.

The main research challenge addressed in this work is focused on enabling configuration security automation in autonomic networks and services. In particular our objective is to increase vulnerability awareness in the autonomic management plane in order to prevent configuration vulnerabilities. The continuous growth of networking significantly increases the complexity of management. It requires autonomic networks and services that are capable of taking in charge their own management by optimizing their parameters, adapting their configurations and ensuring their protection against security attacks. However, the operations and changes executed during these self-management activities may generate vulnerable configurations.

A first part of our work in the year 2013 has been dedicated to the issue of past hidden vulnerable states [8]. Even though a known vulnerability may not be present on a current system, it could have been unknowingly active in the past providing an entry point for attacks that may still constitute a potential security threat in the present. Indeed, vulnerabilities can survive within active systems for a long period of time without being known. During this period, attackers may perform well-planned and clean attacks (e.g., stealing information) without being noticed by security entities (e.g., system administrators, intrusion detection systems, self-protection modules). Changes on the system or even its normal activity can alter or erase the remaining evidence on the current configuration. In that context, we have defined a new strategy for assessing past hidden vulnerable states. This solution is based on a mathematical model for describing and detecting unknown past security exposures and on an OVAL-based framework able to autonomously build and monitor the evolution of network devices and to outsource the assessment of their exposure in an automatic manner. We also have developed an implementation prototype that efficiently performs assessment activities over an SVN repository of IOS system images. Experimental results have confirmed the feasibility and scalability of our solution.

A second part aimed at light-weighting the vulnerability assessment process in the context of mobile devices [9]. Security activities imply a consumption of resources that should be taken to a minimum in order to maximize the performance and responsiveness of such critical environments. Sometimes users may prefer to deactivate security processes such as antivirus software instead of having a short battery lifetime. The proposed approach centralizes main logistic vulnerability assessment aspects as a service while mobile clients only need to provide the server with required data to analyze known vulnerabilities described with the OVAL language. By configuring the analysis frequency as well as the percentage of vulnerabilities to evaluate at each security assessment, our probabilistic solution permits to bound client resource allocation and also to outsource the assessment process. The strategy consists in distributing evaluation activities across time thus alleviating the workload on mobile devices, and simultaneously ensuring a complete and accurate coverage of the vulnerability dataset. This technique results in a faster assessment process, typically done in the cloud, and considerably reduces the resource allocation on the client side. A prototype of our vulnerability assessment framework for Android has been selected and presented during the demonstration session of the IEEE/IFIP IM'2013 international conference [10].

We are currently investigating new methods for remediating known vulnerabilities, formalizing the change decision problem as a satisfiability or SAT problem [27]. By specifying our vulnerability knowledge source as a logical formula, fixing those system properties we can not change and freeing those variables for which changes are available, our objective is to use a SAT solving engine for determining what changes have to be made so as to secure the system. In order to provide proactive and reactive solutions, we are interested in the concept of future state descriptions to specify how a system will look like after applying a specific change.

6.5. Cache Management in CCN

Participants: Thomas Silverston [contact], César Bernardini, Olivier Festor.

The Internet is currently mostly used for accessing content. Indeed, ranging from P2P file sharing to current video streaming services such as Youtube, it is expected that content will count for approximately 86% of the global consumer traffic by 2016.

While the Internet was designed for -and still focuses on- host-to-host communication (IP), users are only interested in actual content rather than source location. Hence, new Information-Centric Networking architectures (ICN) such as CCN, NetInf, Pursuit have been proposed giving high priority to efficient content distribution at large scale. Among all these new architectures, Content Centric Networking (CCN) has attracted considerable attention from the research community [4].

CCN is a network architecture based on named data where a packet address names content, not location. The notion of host as defined into IP does not exist anymore. In CCN, the content is not retrieved from a dedicated server, as it is the case for the current Internet. The premise is that content delivery can be enhanced by including per-node-caching as content traverses the network. Content is therefore replicated and located at different points of the network, increasing availability for incoming requests.

As content is cached along the path, it is crucial to investigate the caching strategy for CCN Networks and to propose new schemes adapted to CCN. We therefore designed *Most Popular Content* (MPC), a new caching strategy for CCN network [12], [11].

Instead of storing all the content at every nodes on the path, MPC strategy caches only popular content. With MPC, each node counts all the requests for a content and when it has been requested a large amount of time, the content will be cached at each node along the path. Otherwise, the content is not popular; it is transmitted but it is not cached into the network.

We implemented MPC into the ccnSim simulator and evaluate it through extensive simulations.

Our results demonstrate that using MPC strategy allow to achieve a higher Cache Hit in CCN networks and still reduces drastically the number of replicas. By caching only popular content, MPC helps at reducing the cache load at each node and the network resource consumption.

We expect that our strategy could serve as a base for studying name-based routing protocols. Being a suggestion based mechanism, it is feasible to adapt it to manage content among nodes, to predict popularity and to route content to destination. In addition, we are currently investigating the social relationship between users to improve our caching strategy for CCN networks.

Besides, Online Social Networks (OSN) have gained tremendous popularity on the Internet. Millions of users interact with each other through OSN such as Facebook or Twitter. New ubiquitous devices (smartphones, tablets) appeared and include functionalities to instantaneously share information through OSN. As a central component of CCN is in-network caching, the content's availability depends on several criteria such as cache strategies and replacement policies, cache size or content popularity. OSN carry extremely valuable information about users and their relationships. This knowledge can help to drastically improve the efficiency of Content Centric Networks. Thus, we propose to include social information in the design of a new caching strategy for Content Centric Networking. We designed *SACS*, a novel caching strategy for CCN based on the social information of users [28]. Our socially-aware caching strategy gives priority to content issued by Influential users and cache it pro-actively into the CCN network. We performed simulations of our caching strategy and show its ability to improve the cache performances of CCN. In addition, we implemented a prototype on PlanetLab and performed large-scale experiments. Our solution improves the caching performances of CCN by 2.5 times on real testbed.

6.6. QoS in Wireless Sensor Networks

Participants: François Despaux, Abdelkader Lahmadi, Evangelia Tsiontsiou, Kévin Roussel, Moutie Chehaider, Ye-Qiong Song [contact].

---

[4]http://www.ccnx.org

WSN research focus has progressively been moved from the energy issue to the QoS issue. Typical example is the MAC protocol design, which cares about not only low duty-cycle, but also high throughput with self-adaptation to dynamic traffic changes. Our research on WSN QoS is thoroughly organized in four topics:

- self-adaptive MAC protocol for both QoS and energy efficiency

  By combining our two previous MAC protocols called Queue-MAC and CoSenS, we extended Queue-MAC to iQueue-MAC to support multi-hop transmission [23], [6]. iQueue-MAC provides immediate yet energy-efficient throughput enhancement for dealing with burst or heavy traffic. Combined with CSMA/CA, iQueue-MAC makes use of queue length of each sensor node and allocates suitable TDMA slots to them for packets transmission. During light traffic period, no extra slots will be allocated; iQueue-MAC acts like other low duty-cycle MACs to conserve power. While in burst or heavy traffic period, iQueue-MAC senses the build up of packet queues and dynamically schedules adequate number of slots for packet transmission. Within ANR QUASIMODO project, we have implemented iQueue-MAC on STM32W108 chips that offer IEEE 802.15.4 standard communication. We set up several real-world experimental scenarios, including a 46 nodes multi-hop test-bed for simulating a general application, and conducted numerous experiments to evaluate iQueue-MAC, in comparison with other traffic adaptive duty-cycle protocols, such as multi- channel version RI-MAC and CoSenS. Results clearly show that iQueue-MAC outperforms multi-channel version of RI-MAC and CoSenS in terms of packet delay and throughput.

- QoS routing

  For supporting different QoS requirements, routing in WSN must simultaneously consider several criteria (e.g., minimizing energy consumption, hop counts or delay, packet loss probability, etc.). When multiple routing metrics are considered, the problem becomes a multi-constrained optimal path problem (MCOP), which is known as NP-complete. In practice, the complexity of the existing routing algorithms is too high to be implemented on the low cost and power constrained sensor nodes. Recently, Operator calculus (OC) has been developed by Schott and Staples with whom we collaborate. OC can be applied to solving MCOP problem with lower complexity and can deal with dynamic topology changes (which is the case in duty-cycled WSN). Through intensive numerical experiments, we have shown that OC has much less complexity compared with SAMCRA, known as one of the best existing algorithms. Sub-optimal paths can be obtained with a distributed version of OC, and following this principle, a first OC-based routing protocol is implemented over Contiki rime stack on TelosB motes. Its improvement and performance evaluation, as well as its integration to uIP/RPL stack is our ongoing work.

- Systems and middleware for supporting QoS in wireless sensor networks

  For supporting new protocols implementation which require to interact with low level services (MAC, Radio drivers, hardware timers) and integration to the Internet of Things approach, we focused on the OS for WSN. Several contributions have been made available for both ContikiOS (https://github.com/contiki-os/contiki/pull/519) and RiotOS (https://github.com/RIOT-OS/RIOT/pull/408, https://github.com/RIOT-OS/RIOT/pull/459). This allows to preparing for the next step towards the implementation of iQueue-MAC on both ContikiOS and RiotOS and compare experimentally with other protocols. In parallel and as part of LAR project, we also investigated the integration of different types of WSN using a gateway to make the data access transparent following RESTful webservice through CoAP/UPD/6loWPAN [24].

- End-to-end performance in multi-hop networks

  Probabilistic end-to-end performance guarantee may be required when dealing with real-time applications. As part of ANR QUASIMODO project, we are dealing with Markov modeling of multi-hop networks running slotted CSMA/CA (beacon enabled mode of IEEE 802.15.4). One of the problem of the existing models resides in their strong assumptions that may not be directly used to assess the end-to-end delay in practice. In particular, realistic radio channel, capture effect and OS-related implementation factors are not taken into account [15], [14]. We proposed to explore a new

approach which is based on process mining to extract the Markov chain model from the execution of the protocol code.

6.7. Routing in Wireless Sensor Networks

Participants: Emmanuel Nataf [contact], Patrick-Olivier Kamgueu.

Our work on the estimation of the remaining energy inside a sensor is published in [18]. We have integrated this model in the standard routing protocol for wireless sensors networks (RPL) and compared our energy based routing against a routing plane based on the quality of transmission between sensors [30].

We have built a new model to combine together several criteria, as the remaining energy, the expected transmission rate and the hop count into one quality indicator. To achieve this, we propose to use fuzzy logic either because it is a recognized mathematical tool for combining heterogeneous data and because it can be implemented with a small memory footprint. Our work is fully integrated in the standard protocol and does not need additional messages or new protocol states.

We bought 35 sensors and deployed them in the Loria building. The goal of this deployment is manyfold :

- to build and observe a real network in a real environment;
- to provide the team with a demonstrative tool to help the understanding of our work;
- to provide the team with a testbed for other works on IoT, like the security monitoring or the QoS.

6.8. Online Risk Management

Participants: Rémi Badonnel [contact], Oussema Dabbebi, Olivier Festor.

Telephony over IP has known a large scale deployment and has been supported by the standardization of dedicated signaling protocols. This service is however exposed to multiple attacks due to a lower confinement in comparison to traditional PSTN networks. While a large variety of methods and techniques has been proposed for protecting VoIP networks, their activation may seriously impact on the quality of such a critical service. Risk management provides new opportunities for addressing this challenge. In particular our work aims at performing online risk management for VoIP networks and services. The objective is to dynamically adapt the service exposure with respect to the threat potentiality, while maintaining a low security overhead.

In the year 2013, these efforts on VoIP risk management have led the PhD defense of Oussema Dabbebi. This work has been structured into three axes [1]. The first axis concerns the automation of the risk management process in VoIP enterprise network. In this context, we have developed a mathematical model for assessing risk, a set of progressive countermeasures to counter attackers and mitigation algorithms that evaluate the risk level and takes the decision to activate a subset of countermeasures [4]. To improve our strategy, we have coupled it with an anomaly detection system based on SVM and a self-configuration mechanism which provides feedback about countermeasure efficiency. The second axis deals with the extension of our adaptive risk strategy to P2PSIP infrastructures. We have implemented a specific risk model and a dedicated set of countermeasures with respect to its peer-to-peer nature. For that, we have identified attack sources and established different threat scenarios. We have analysed the RELOAD framework and proposed trust mechanisms to address its residual attacks. Finally, the third axis focuses on VoIP services in the cloud where we have proposed a risk strategy and several strategies to deploy and apply countermeasures [5].

6.9. Pervasive Computing

Participants: Laurent Ciarletta [contact], Olivier Festor, Ye-Qiong Song, Yannick Presse, Emmanuel Nataf.

Vincent Chevrier, Thomas Navarrete Gutierrez and Julien Vaubourg (MAIA team) did contribute to part of this activity.

In Pervasive or Ubiquitous Computing, a growing number of communicating/computing devices are collaborating to provide users with enhanced and ubiquitous services in a seamless way. In a related field, Cyber Physical Systems also are technological systems that have to be considered within a physical world and its contraints. They are complex systems where several inter-related phenomena have to be considered. In order to be studied, modeled and evaluated, we propose the use of co-simulation and multimodeling.

Pervasive Computing is about interconnected and situated computing resources providing us(ers) with contextual services. These systems, embedded in the fabric of our daily lives, are complex: numerous interconnected and heterogeneous entities are exhibiting a global behavior impossible to forecast by merely observing individual properties. Firstly, users physical interactions and behaviors have to be considered. They are influenced and influence the environment. Secondly, the potential multiplicity and heterogeneity of devices, services, communication protocols, and the constant mobility and reorganization also need to be addressed. Our research on this field is going towards both closing the loop between humans and systems, physical and computing systems, and taming the complexity, using multi-modeling (to combine the best of each domain specific model) and co-simulation (to design, develop and evaluate) as part of a global conceptual and practical toolbox. We're applying this work on UAvs, dynamic networks (adhoc, mesh, P2P, wireless sensors and actuators), energy-constrained / location aware services, smart grids etc.

Such systems can be seen as complex and are present everywhere in our environment: internet, electricity distribution networks, transport networks. This systems have as characteristics: a large number of autonomous entities, dynamic structures, different time and space scales and emergent phenomena.

Application domains such as Smart Spaces, Smart Cities, Smart Trasportation Systems and Smart Grid makes us sometimes use Smart* or SmartX as a generic word. Madynes is focusing on the networking aspects of such systems and on the tools to develop and assess them. We cooperate with other teams and most notably the Maia team to be able to encompass issues and research questions that combine both networking and cognitive aspects.

In 2013 we worked on the following research topics :

- Assessment and evaluation of complex systems. Continuing the work on multi-modeling and co-simulation, we have participated with the MAIA team on the development of an architecture for the control of complex systems based on multi-agent simulation, a CPS co-simulation (next item) and a Smart grid simulation tool (last item), and continue working on the AA4MM framework (Agents and artefacts for Multiple heterogeneous Models).

  A control architecture has been proposed by Tomas Navarrete, based on an "equation-free" approach. We use a multi-agent model to evaluate the global impact of local control actions before applying the most pertinent set of actions. Associated to our architecture, an experimental platform has been developed to confront the basic ideas or the architecture within the context of simulated "free-riding" phenomenon in peer to peer file exchange networks. We have demonstrated that our approach allows to drive the system to a state where most peers share files, despite given initial conditions that are supposed to drive the system to a state where no peer shares. We have also executed experiments with different configurations of the architecture to identify the different means to improve the performance of the architecture.

  This work helped us to identify [13] the key issues related to the usage of the multi-agent paradigm in the context of control of complex systems.

- In Cyper Physical Systems, we have lead the design and implementation of the Aetournos (Airborne Embedded auTonomOUs Robust Network of Objects and Sensors) platform at Loria. The idea of AETOURNOS is to build a platform which can be at the same time a demonstrator of scientific realizations and an evaluation environment for research works of various teams of our laboratory. It is also its own research domain : building a completely autonomous and robust flock of collaborating UAVs.

  In Madynes, we focus on the CPS and their networks and applications. Those systems consist of numerous autonomous elements in sharp interaction which functioning require a tight coupling be-

tween software implementations and technical devices. The collective movements of a flock of flying communicating robots / UAVs, evolving in potentially perturbed environment constitute a good example of such a system. Indeed, if we look at the level of each of the elements playing a role into this system, a certain number of challenges and scientific questions can be studied: respect of real-time constraints of calculations for every autonomous UAV and for the communication between the robots, conception of individual, embedded, distributed or global management systems, development of self-adaptative mechanisms, conception of algorithms of collective movement etc... Furthermore, the answers to each of these questions have to finally contribute to the global functioning of the system. Applying co-simulation technique we plan to develop a hybrid "network-aware flocking behavior" / "behavior aware routing protocol". The platform is composed of several high-grade research UAVs (Pelican quadcopters and Firefly hexacopters) and lighter models (AR.Drone quacopters). We have provided a working set of tools : multi-simulation behavior / network / physics and generic software development using ROS (Robot Operating System). The UAVs carry a set of sensor for location awareness, their own computing capabilities and several wireless networks.

This work is discribed in a position paper where a first implementation of a formation flight is detailed [29].

- Smart grids and Smart spaces are another application domain. MS4SG (cf. has given us the opportunity to link multi-simulations tools such as HLA (High Level Architecture) and FMI (Functional Mockup Interface) thanks to our AA4MM framework. We've so far successfully applied our solution to the simulation of smart appartment complex and to combining the electrical and networking part of a Smart Grid (first deliverable and first workshop with EDF R&D, Supélec and SIANI were in september 2013). A paper has also been accepted to Simutools 2014. In 2014, we will continue working on the hybrid protocols and on the UAV platform, and apply our co-simulation work to Smart Grids and other Smart* [13].

6.10. SCADA Systems Security

Participants: Olivier Festor, Abdelkader Lahmadi [contact], Bilel Saadallah.

SCADA is a term used in several industries and it stands for *Supervisory Control and Data Acquisitions*. It refers to a centralized control and monitoring system for a variety of machinery and equipment involved with many industrial activities including: power generation and distribution, transportation, nuclear plants, manufacturing processes, etc. SCADA systems use a family of network protocols (PROFINET, MODBUS, DNP3) to monitor and control these industrial activities or even our homes. SCADA systems are becoming target to different attacks exploiting traditional IT vulnerabilities, e.g. buffer overflows, script crossing, crafted network packets, or specific vulnerabilities related to control and estimation algorithms employed by control processes. Several of them are daily discovered and disclosed or remain still unknown. The most threaten accidents in SCADA networks are caused by targeted attacks, where adversaries exploit those vulnerabilities available in software or network protocols components to disturb and make damage to the physical process. Therefore, it is important to provide new methods and tools for protecting SCADA network from malicious cyber attacks targeting physical processes and infrastructures.

During the year 2013, we have firstly designed and setup a SCADA test bed [31] to be able to analyze and develop security methods for several controlled physical systems. The testbed uses a Profinet based network to control experimental real-time simulated physical processes through hardware programmable logic controllers (PLCs). Secondly, we have developed a novel methodology to automatically discover a pattern of behaviour of a running controlled system through the analysis of communication messages traveling in its control loop network. The method applies process mining techniques on the exchanged communication packets between control and feedback devices to infer a model of the controlled running system. The extracted model will be then used to build a tailored anomaly-based intrusion detection module for the studied system.

6.11. Dynamic resource allocation for network virtualization

Participants: Said Seddiki, Bilel Nefzi, Mounir Frikha, Ye-Qiong Song [contact].

The objective of this research topic is to develop different resource allocation mechanisms in Network Virtualization, for creating multiple virtual networks (VNs) from a single physical network. It is accomplished by logical segmentation of the network nodes and their physical links. Sharing resources and improving utilization are the main idea of virtualization. Finding effective solutions for the needs expressed by users without deteriorating the performance of different VNs is a research challenge. In addition, solutions should meet different performance criteria required by network infrastructure.

We proposed several approaches that aim to select substrate nodes [21] with sufficient CPU, disk, and other resources, as well as substrate links with enough spare bandwidth [19], [20]. These dynamic approaches, where online monitoring of the VN is required, allow adaptively changing the resource allocations. We have shown through simulations that the proposed approaches offer higher utilization of physical network and better managing the satisfaction of virtual networks by minimizing the packet delays inside the physical node. They also provide a fair and efficient allocation of link capacity and avoid bottlenecks. The next step is the implementation of these propositions using OPENFLOW in a software defined network.

6.12. Crowdsourcing Services

Participants: Thomas Silverston [contact], Olivier Festor, Abdelkader Lahmadi, Elian Aubry.

Nowadays cities invest more in their public services, and particularly digital ones, to improve their resident's quality of life and attract more people. Thus, new crowdsourcing services appear and they are based on contributions made by mobile users equipped with smartphones. For example, the respect of the traffic code is essential to ensure citizens' security and welfare in their city. We therefore designed CrowdOut, a new mobile crowdsourcing service for improving road safety in cities. CrowdOut allows users to report traffic offense they witness in real time and to map them on a city plan. CrowdOut has been implemented and experiments and demonstrations have been performed in the urban environment of the Grand Nancy, in France. This service allows users appropriating their urban environment with an active participation regarding the collectivity. This service also represents a tool for city administrators to help for decisions and improve their urbanization policy, or to check the impact of their policy in the city environment.

<p style="text-align:center">**SCORE Team**</p>

5. New Results

5.1. Evaluation and Design of Collaborative Editing Algorithms

Participants: Mehdi Ahmed-Nacer, Luc André, Claudia-Lavinia Ignat, Stéphane Martin, Gérald Oster, Pascal Urso.

Since the Web 2.0 era, the Internet is a huge content editing place in which users contribute to the content they browse. Users do not just edit the content but they collaborate on this content. Such shared content can be edited by thousands of people. However, current consistency maintenance algorithms seem not to be adapted to massive collaborative updating involving large amount of contributors and a high velocity of changes. This year we continued our work on the evaluation of existing collaborative editing approaches and on the design of new algorithms that overcome limitations of state of the art ones. Moreover, we started to work on experimental user studies for understanding the real-time requirements for collaborative editing and grounding a theory for the effect of real-time constraints in collaborative work [26].

We also run experiments to compare the merge automatically obtained by collaborative editing algorithms – CRDTs, OTs and the world-wide used diff3 – to the merge validated by the user. We obtain automatically such results exploiting the massively available distributed version control systems histories of open-source software. We use these results to improve an existing collaborative editing algorithm and obtain result statistically better than the existing ones (including diff3 used in major DVCS systems) [9].

In existing collaborative editing algorithms shared data is usually fragmented into fixed granularity atomic elements that can only be added or removed. Coarse-grained data leads to the possibility of conflicting updates while fine-grained data requires more metadata. In [11] we offer a solution for handling an adaptable granularity for shared data that overcomes the limitations of fixed-grained data approaches. Our solution relies on a novel commutative replicated data type (CRDT) for sequences of text that assigns unique identifiers to substrings of variable length contrary to existing CRDTs that assign unique identifiers to fixed size elements of the text (i.e. characters or lines). This offers the possibility to define coarse grained elements when they are created and refine them when needed. This greatly reduces the memory consumption since a smaller memory overhead is needed to store metadata (identifiers). Moreover, we show using simulations that overall performances of our algorithms are superior to existing ones.

We proposed a new concurrency control algorithm, based on conflict-free data types. It is built on the ideas previously developed for synchronous collaboration, extending them to support asynchronous collaboration. Our solution also includes the necessary information for providing comprehensive awareness information to users. The evaluation of our algorithm shows that comparing our solution with traditional solutions in collaborative editing, the conflict resolution strategy proposed in this paper leads to results closer to the ones expected by users [10].

5.2. Decentralized monitoring of orchestration execution

Participants: Mohamed Aymen Baouab, Olivier Perrin, Claude Godart.

Cross-organizational service-based processes are increasingly adopted by different companies when they cannot achieve goals on their own. The dynamic nature of these processes poses various challenges to their successful execution. In order to guarantee that all involved partners are informed about errors that may happen in the collaboration, it is necessary to monitor the execution process by continuously observing and checking message exchanges during runtime. This allows a global process tracking and evaluation of process metrics. Complex event processing can address this concern by analysing and evaluating message exchange events, to the aim of checking if the actual behaviour of the interacting entities effectively adheres to the modelled business constraints. In our recent work (Aymen Baouab thesis [1]), we presented an approach for

decentralized monitoring of cross-organizational choreographies. We have defined a hierarchical propagation model for exchanging external notifications between the collaborating parties. We also proposed a runtime event-based approach to deal with the problem of monitoring conformance of interaction sequences. Our approach allows for an automatic and optimized generation of rules. After parsing the choreography graph into a hierarchy of canonical blocks, tagging each event by its block ascendancy, an optimized set of monitoring queries is generated. We evaluate the concepts based on a scenario showing how much the number of queries can be significantly reduced [12].

5.3. Optimization and security of business processes in SaaS contexts

Participants: Claude Godart, Elio Goettelmann, Samir Youcef.

Globalization and the increase of competitive pressures created the need for agility in business processes, including the ability to outsource, offshore, or otherwise distribute its once-centralized business processes or parts thereof. While hampered thus far by limited infrastructure capabilities, the increase in bandwidth and connectivity and decrease in communication cost have removed these limits. This is even more true with the advent of cloud, particularly in its "Service as a software" dimension. To adapt to such a context, there is a growing need for the ability to fragment one's business processes in an agile manner, and be able to distribute and wire these fragments so that their combined execution recreates the function of the original process. Our work focuses on solving some of the core challenges resulting from the need to dynamically restructure enterprise interactions. Restructuring such interactions corresponds to the fragmentation of intra and inter enterprise business process models. It describes how to identify, create, and execute process fragments without loosing the operational semantics of the original process models. In addition, this fragmentation is complicated by the constraints of quality of service, in particular the execution time and the cost, and of security, especially privacy. During the year, we consider this problem at two levels: the design of privacy-aware process models, and the process scheduling optimization. We developed a methodology to integrate privacy concerns in the design of a business process before distribution in the cloud. Based on a risk analysis, the result of the design is a set of process (re-)modelling actions, a set of constraints on process fragments assignments to clouds, and a set of constraints for cloud selection based on cloud properties [19]. We developed bi-criteria strategies for business processes scheduling in cloud environments with execution time and cost constraints, augmented with fairness metrics, and taking into account the availability of human resources, a critical point in business processes [14], [15], [3].

5.4. Large Scale Coordination of Crowdsourcing Activities

Participants: François Charoy, Karim Benouaret, Raman Valliyur-Ramalingam, Alexandre Roux d Anzi.

As a follow-up of our work on coordination of large scale processes that we have investigated in the domain of crisis management [4], [5], we have studied a new application domain for BPM, crowdsourcing. In order to make cities smarter, it would be interesting to design a platform where citizens are given an opportunity to be effectively connected to the governing bodies in their location and to contribute to the general well being. We have developed CrowdSC, a crowdsourcing framework designed for smarter cities. We have shown that it is possible to combine data collection, data selection and data assessment crowdsourcing activities in a crowdsourcing process to achieve sophisticated goals in a predefined context. Depending on the executing strategy of this process, different kinds of outcomes can be produced. We have conducted an experimental study that evaluates these process outcomes depending on different execution strategies [2], [13].

ALICE Project-Team

5. New Results

5.1. Geometry Processing

5.1.1. Fitting Polynomial Volumes to Surface Meshes with Voronoi Squared Distance Minimization

Participants: Gilles-Philippe Paillé, Bruno Lévy.

We propose a method for mapping polynomial volumes. Given a closed surface and an initial template volume grid, our method deforms the template grid by fitting its boundary to the input surface while minimizing a volume distortion criterion. The result is a point-to-point map distorting linear cells into curved ones. Our method is based on several extensions of Voronoi Squared Distance Minimization (VSDM) combined with a higher-order finite element formulation of the deformation energy. This allows us to globally optimize the mapping without prior parameterization. The anisotropic VSDM formulation allows for sharp and semi-sharp features to be implicitly preserved without tagging. We use a hierarchical finite element function basis that selectively adapts to the geometric details. This makes both the method more efficient and the representation more compact. We apply our method to geometric modeling applications in computer-aided design and computer graphics, including mixed-element meshing, mesh optimization, subdivision volume fitting, and shell meshing.

This work was presented at the "ACM Symposium on Geometry Processing" and published in the "Computer Graphics Forum" journal [16].

5.1.2. Particle-Based Anisotropic Surface Meshing

Participant: Bruno Lévy.

This paper introduces a particle-based approach for anisotropic surface meshing. Given an input polygonal mesh endowed with a Riemannian metric and a specified number of vertices, the method generates a metric-adapted mesh. The main idea consists of mapping the anisotropic space into a higher dimensional isotropic one, called "embedding space". The vertices of the mesh are generated by uniformly sampling the surface in this higher dimensional embedding space, and the sampling is further regularized by optimizing an energy function with a quasi-Newton algorithm. All the computations can be re-expressed in terms of the dot product in the embedding space, and the Jacobian matrices of the mappings that connect different spaces. This transform makes it unnecessary to explicitly represent the coordinates in the embedding space, and also provides all necessary expressions of energy and forces for efficient computations. Through energy optimization, it naturally leads to the desired anisotropic particle distributions in the original space. The triangles are then generated by computing the Restricted Anisotropic Voronoi Diagram and its dual Delaunay triangulation. We compare our results qualitatively and quantitatively with the state-of-the-art in anisotropic surface meshing on several examples, using the standard measurement criteria. This work was published in the "ACM Transactions on Graphics" journal (SIGGRAPH conference proceedings) [19].

5.1.3. Approximating Functions on a Mesh with Restricted Voronoi Diagrams

Participant: Bruno Lévy.
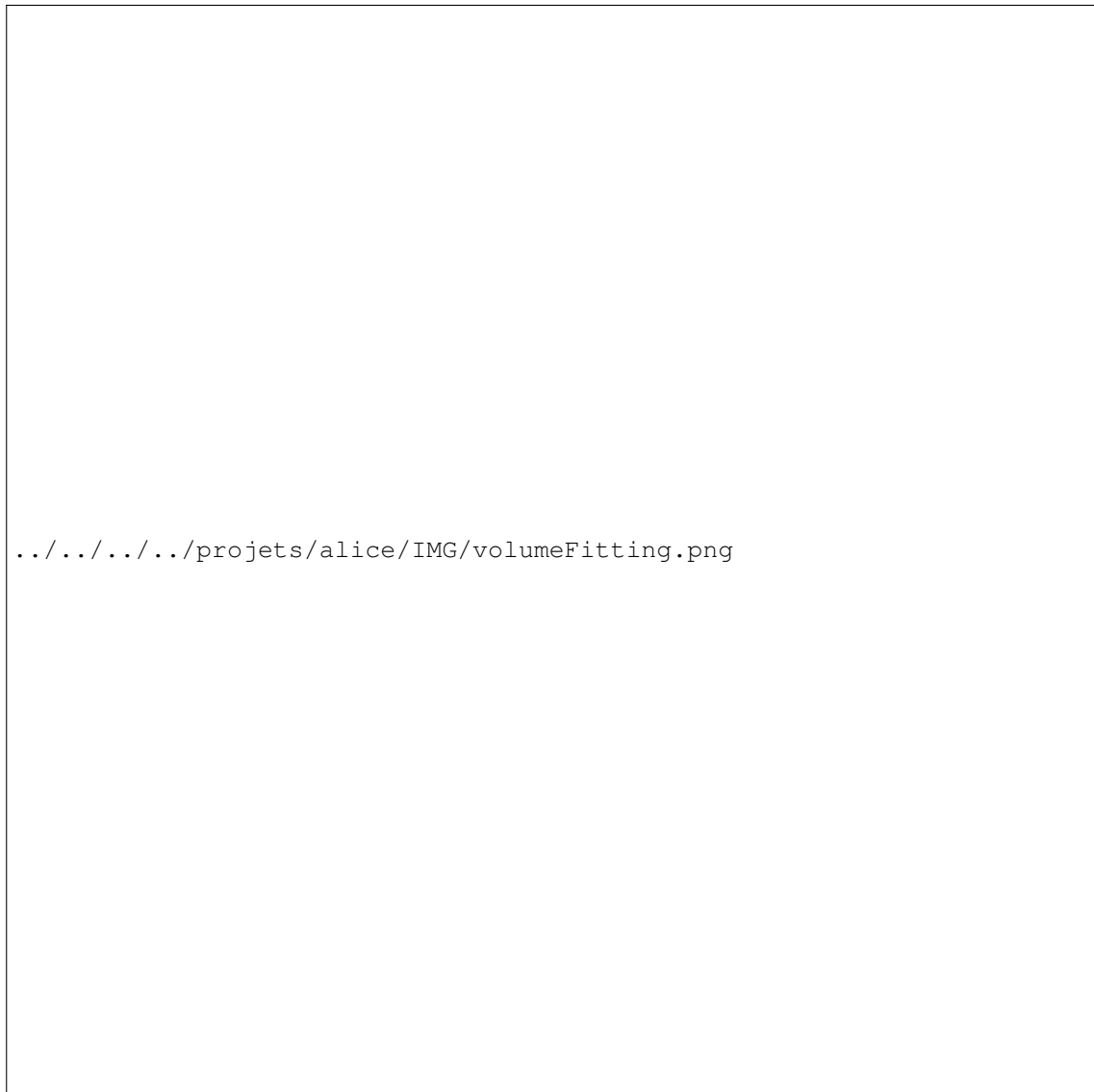
../../../../projets/alice/IMG/volumeFitting.png

Figure 2. Fitting Polynomial Volumes to Surface Meshes with Voronoi Squared Distance Minimization

We propose a method that computes a piecewise constant approximation of a function defined on a mesh. The approximation is associated with the cells of a restricted Voronoi diagram. Our method optimizes an objective function measuring the quality of the approximation. This objective function depends on the placement of the samples that define the restricted Voronoi diagram and their associated function values. We study the continuity of the objective function, derive the closed-form expression of its derivatives and use them to design a numerical solution mechanism. The method can be applied to a function that has discontinuities, and the result aligns the boundaries of the Voronoi cells with the discontinuities. Some examples are shown, suggesting potential applications in image vectorization and compact representation of lighting. This work was presented at the "ACM Symposium on Geometry Processing" and published in the "Computer Graphics Forum" journal [15].
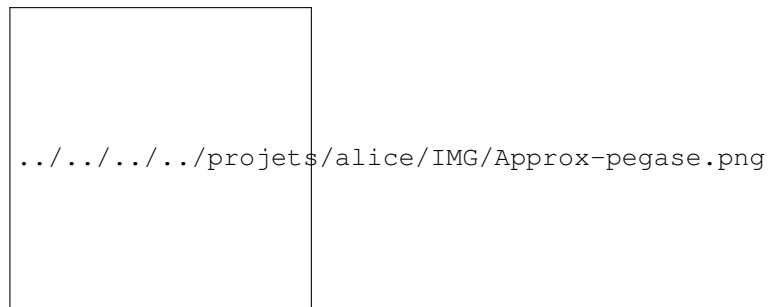

Figure 3. Approximating Functions on a Mesh with Restricted Voronoi Diagrams

5.1.4. *Spectral Clustering of Plant Units From 3D Point Clouds*

Participant: Dobrina Boltcheva.

High-resolution terrestrial Light Detection And Ranging (tLiDAR), a 3-D remote sensing technique, has recently been applied for measuring the 3-D characteristics of vegetation from grass to forest plant species. The resulting data are known as a point cloud which shows the 3-D position of all the hits by the laser beam giving a raw sketch of the spatial distribution of plant elements in 3-D, but without explicit information on their geometry and connectivity.

We have developed a new approach based on a delineation algorithm (Fig. 4) that clusters a point cloud into elementary plant units such as internodes, petioles and leaves. The algorithm creates a graph (points + edges) to recover plausible neighbouring relationships between the points and embeds this graph in a spectral space in order to segment the point-cloud into meaningful elementary plant units.

We have presented this work at the 7th International Conference on Functional—Structural Plant Models (FSPM) which took place in Finland this summer [21].

5.1.5. *Fixing Normal Constraints for Generation of Polycubes*

Participants: Nicolas Ray, Dmitry Sokolov.

A polycube is a piecewise linearly defined surface where all faces are squares that are perpendicular to an axis of a global basis. Deforming triangulated surfaces to polycubes provides maps (form the original surface to the polycube) that can be used for a number of applications including hex-meshing. To define such a deformation, it is necessary to determine, for each point of the original surface, what will be its orientation (global axis) in the polycube.
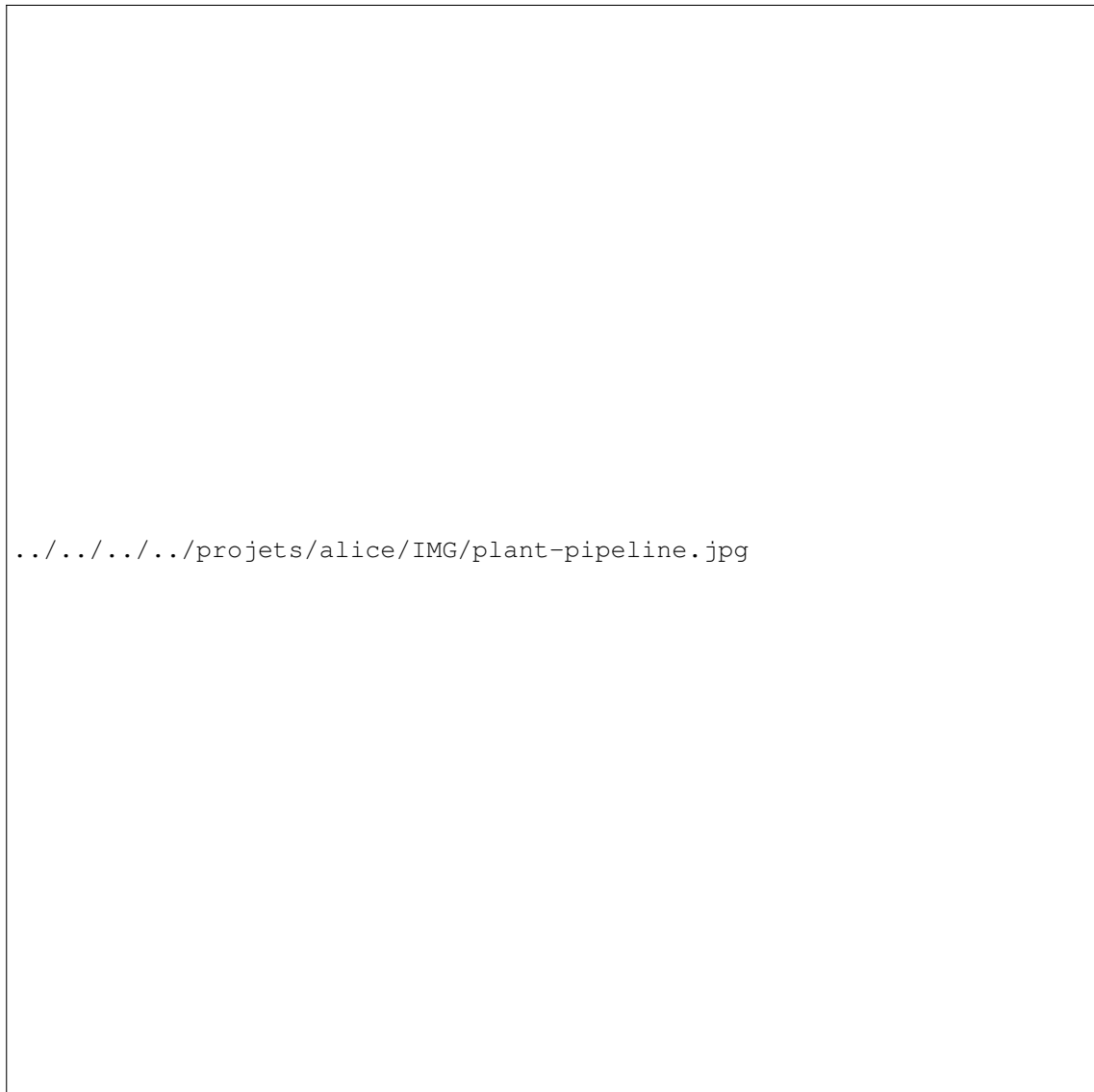
../../../../projets/alice/IMG/plant-pipeline.jpg

Figure 4. From a point cloud scan of a plant to a segmentation of its leaves.

This problem is actually tackled by heuristics that basically affect the closest global axis to the surface normal. Coupled with a mesh deformation as pre-processing and some fixing rules as a post-processing, it is able to provide nice results for a number of surfaces. However, nothing ensures that the surface can be deformed to a polycube having these desired face orientations.

We have worked on a method able to determine if there exists a deformation of the surface that respects a given orientation constraint on each point. We have also designed an automatic solution that can fix constraints that would prevent the existence of a deformation into a polycube (Figure 5).

This study has highlighted that the constraints on desired orientation are global and requires constrained optimization methods to be solved. Our current solution is able to manage many cases where previous works would fail, but we can still produce some complex cases where interactions between dimension may lead to deadlocks.

../../../../projets/alice/IMG/polycube.png

*Figure 5. **Upper row:** the surface is deformed to make its normals closer to major axis, but to reach an equality, we need to have a coherent "wished orientation" of the faces. **Middle row:** we define a valid deformation into a polycube by editing the "wished orientation". **Lower row:** the resolution is performed a dimension at a time.*

5.1.6. Some Basic Geometric Considerations in Variational Multiview Stereo
Participant: Rhaleb Zayer.

We developed a technique for processing correspondences originating from dense variational matching in the context of multiview stereo. Such data tends to be very large and can easily encompass tens or hundreds of millions of points, these figures keep growing as high resolution images are becoming mainstream. Inspired by Lambert's cosine law, we regard the matching as sequences of planar maps across neighboring views, and show how to take advantage of geometric properties of such maps to favor image areas where the cosine angle between the surface normal and the line of sight is maximal. As the approach operates in the planar domain on smaller subsets of neighboring views, it is computationally efficient and has a low memory footprint. A preprint is in preparation.

5.1.7. *Multi-frontal Propagation Based Matching*

Participants: Rhaleb Zayer, Patricio Galindo.

We consider the propagation-based matching problem, which deals with expanding a limited set of correspondences towards a quasi-dense map across two views. Two issues which have not received much interest in earlier work are raised here. The traversal of weakly textured regions is shown to negatively impact the quality of subsequent correspondences. Analysis of the propagation results using the commonly adopted global best-fit strategy reveals that only a small subset of the input seeds contributes effectively to the propagation, which is probably not optimal since the quality of the matches may deteriorate as the propagation region becomes significantly large as shown in figure 7 -bottom. This research extends existing propagation techniques in two ways: (i) The selection of reliable expansion regions is automatized and adapted to the propagation by categorizing the image into three regions, no-propagation regions, safe-propagation regions and buffer-regions where seeds can propagate but cannot generate new seeds. (ii) A multi-frontal propagation approach is proposed with emphasis on the balance between the greedy nature of the original algorithm and the contribution of the seeds. A preprint is in preparation.

5.1.8. *Large Deformations of Slender Objects*

Participant: Rhaleb Zayer.

We studied the problem of large spatial deformation in the context of interactive editing of slender curve-like objects. The deformation is analyzed in the local frame of the individual curve segments (beams) and the rigid motion of the local frame is updated using a total Lagrangian approach. Analysis of the virtual work in the light of this decoupling allows formulating the Hessian of the deformation in a simple but principled manner. The resulting representation is sparser than existing derivations and can handle the simultaneous action of torques, and forces, efficiently, so as to reproduce a natural behavior in such path dependent situations. The proposed approach is conceptually simple, easy to implement, and suitable for object editing. The numerical solution is carried out using an efficient iterative scheme which allows stable convergence. A preprint is in preparation.

5.2. Computer Graphics

5.2.1. *By-example Synthesis of Curvilinear Structured Patterns*

Participants: Anass Lasram, Sylvain Lefebvre.

Many algorithms in Computer Graphics require to synthesize a pattern along a curve. This is for instance the case with line stylization, to decorate objects with elaborate patterns (chains, laces, scratches), or to synthesize curvilinear features such as mountain ridges, rivers or roads. We describe a simple yet effective method for this problem. Our method addresses the main challenge of maintaining the continuity of the pattern while following the curve. It allows some freedom to the synthesized pattern: It may locally diverge from the curve so as to allow for a more natural global result. This also lets the pattern escape areas of overlaps or fold-overs. This makes our method particularly well suited to structured, detailed patterns following complex curves. Our synthesizer copies tilted pieces of the exemplar along the curve, following its orientation. The result is optimized through a shortest path search, with dynamic programming. We speed up the process by an efficient parallel implementation. Finally, since discontinuities may always remain we propose an optional post-processing step optimally deforming neighboring pieces to smooth the transitions.

../../../../projets/alice/IMG/ft0001.jpg ../../../../projets/alice/IMG/ft0005.jpg ../../../../projets/alice/IMG/ft0008

../../../../projets/alice/IMG/ft2y.jpg ../../../../projets/alice/IMG/ft6y.jpg ../../../../projets/alice/IMG/ft9.jp

../../../../projets/alice/IMG/ftres.jpg ../../../../projets/alice/IMG/ftresbom3.jpg ../../../../projets/alice/IMG/ftres
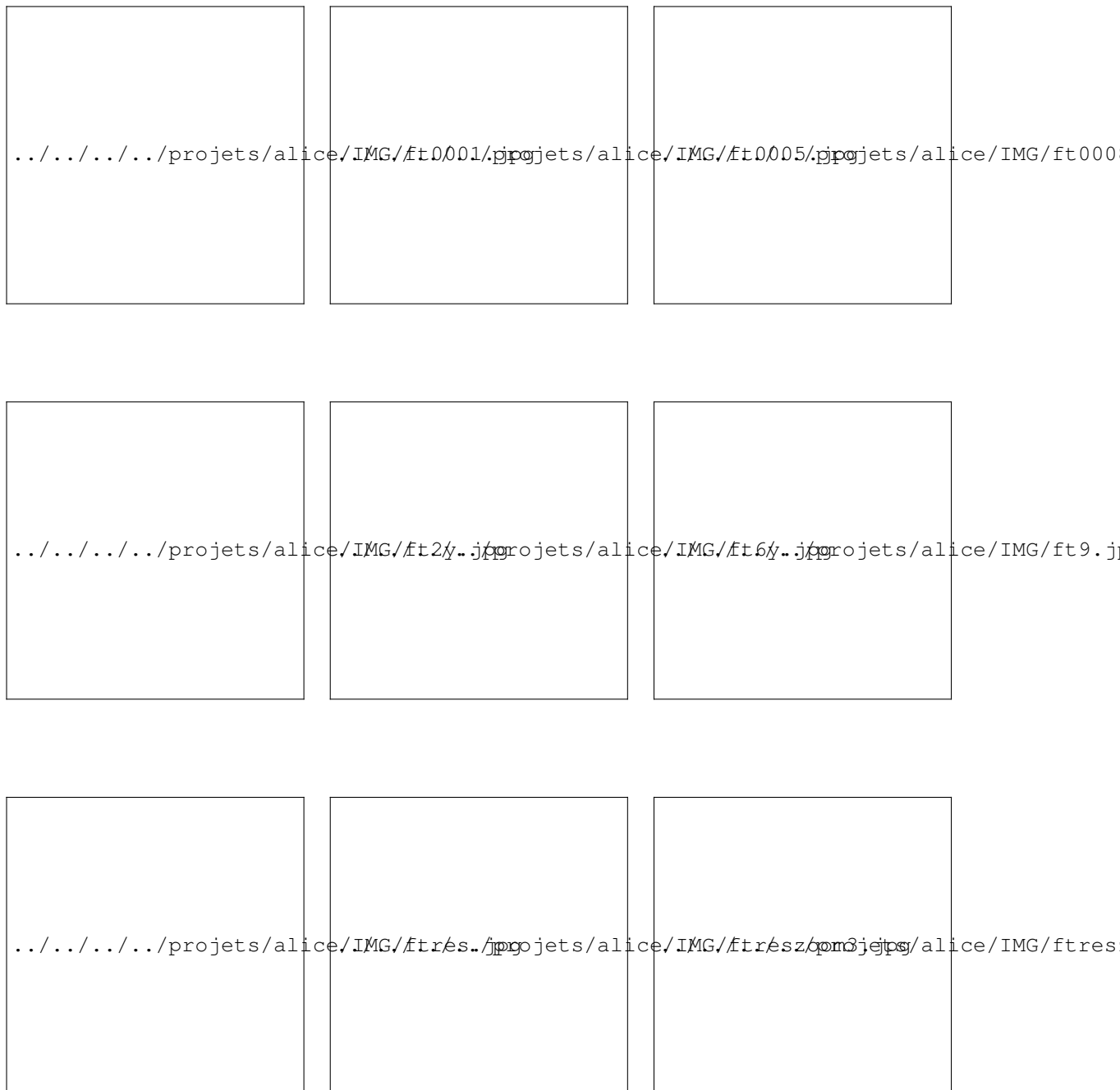
Figure 6. Processing best viewed regions in the Fountain data set (top). Each view represents the central image of a triplet (other two images not shown). The red-colored regions (middle) represent areas best viewed in the triplet. Yellow-marked regions represent regions which are only visible in the triplet and therefore are included even if they do not comply with the best view requirement. The resulting reconstruction (bottom) shows an almost outlier free point cloud.

Figure 7. Typical result of our approach (top), compared to a best-first strategy (bottom). In both experiments, the same initial seeds were used (≈ 40 seeds). The descendants of each initial seed are uniquely colored. Our approach clearly allows all seeds to contribute, whereas the greedy approach marginalize a majority of them.
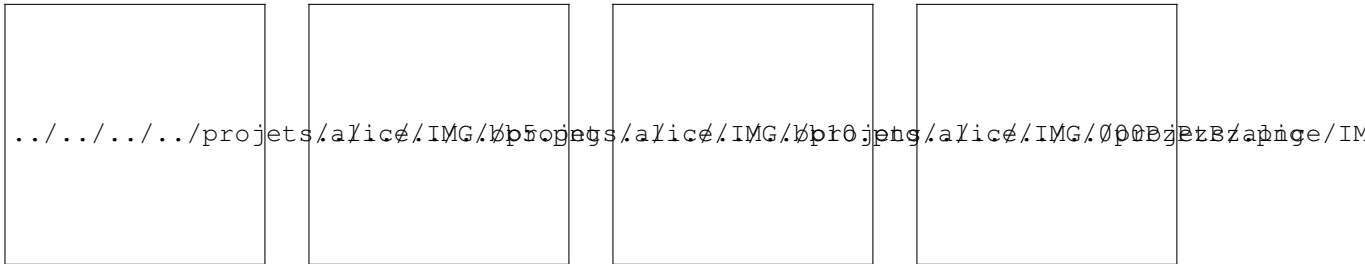
../../../../projets/alice/IMG/bprojets/alice/IMG/bprojets/alice/IMG/0projetB/apnge/IM

Figure 8. Typical editing examples of slender objects under various constraint, the faded snapshots shows initial or intermediate configurations.

This work was presented at the Eurographics conference and published in the "Computer Graphics Forum" journal [20].

5.2.2. *Game Level Layout*

Participant: Sylvain Lefebvre.

This work is a collaboration with the University of British Columbia. We consider a long standing problem in the video game industry: How to automatically generate game levels. Most procedural game levels tend to exhibit a random organization, reducing their interest. Instead, our approach lets a professional game designer describe the global organization of the level through a planar graph, capturing the connectivity and sequencing of different level 'rooms'. Our approach then automatically generates multiple level geometries that correspond to this high-level description.

The work will be presented at *Eurographics 2014* [13].

5.2.3. *Dynamic Element Textures*

Participant: Sylvain Lefebvre.

This work is a collaboration with Microsoft Research Asia. We consider the problem of synthesizing animated details from an example. We first define the notion of a 'textured' animation and extract details from the example animation. Intuitively, these are small scale repetitive motions found for instance for leaves in the wind or in swarms. We then propagate these motions to a coarse scale animation. Our techniques work on 1D, 2D and 3D objects.

We published this work in *ACM Transactions on Graphics (SIGGRAPH proceedings)* [14].

5.2.4. *Make It Stand: Balancing Shapes for 3D Fabrication*

Participant: Sylvain Lefebvre.

This work is a collaboration with ETH Zurich. We consider the problem of balancing 3D models so that they stand in static equilibrium on their base of support after printing. We formulate the problem as the joint optimization of a voxel selection inside the model and a continuous detail preserving deformation of the outter surface.

The work has been published in *ACM Transactions on Graphics (SIGGRAPH proceedings)* [18].

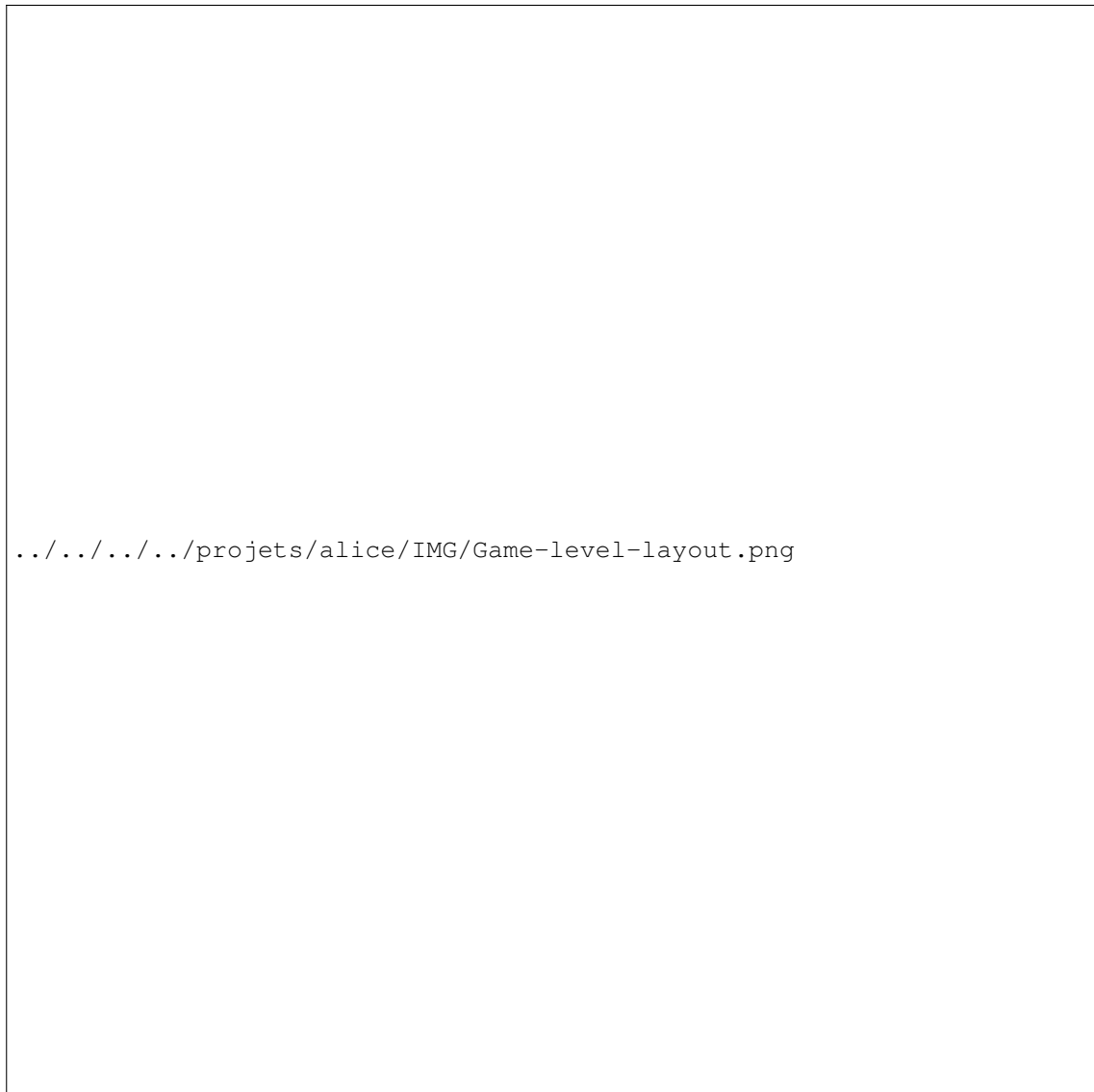### 5.2.5. *Clean Colors*

Participants: Jean Hergel, Sylvain Lefebvre.

../../../../projets/alice/IMG/Game-level-layout.png

Figure 9. Game Level Layout

../../../../projets/alice/IMG/Dynamic-element-texture.jpg

Figure 10. Dynamic Element Textures

In this work we consider the problem of tool path planning for low-cost FDM (Fused Deposition Modeling) printers when using multiple filaments. Our method is based on three components which together reduce most of the defects found in such prints. Our algorithm first optimizes the orientation (azimuth angle) of the print so as to minimize defects. It then builds a rampart in close proximity of the model. This captures most of the strings of plastic oozing from idle extruders. Finally, we optimize for navigation paths minimizing the apparition of defects.

The work will be presented at *Eurographics 2014* [22].

5.2.6. *Fast Fragment Sorting on the GPU*

Participants: Sylvain Lefebvre, Samuel Hornus.

In this work, we build upon our result on "hashing on the GPU" from 2011 [1] to develop new techniques for sorting per-pixel lists of fragments as the latter are rasterized. We can then obtain, for each pixel, the list of surface elements visible through that pixel, sorted according to their distance to the viewpoint. The lists are obtained in a single rasterization pass instead of two for some earlier work; this is a clear win for bandwidth usage and processing time. Two important applications are the possibility to correctly visualize transparent objects and to directly display constructive-solid-geometry models without having to compute their boundary first (the boolean operations are performed on the fly, per pixel).

Our initial work has been published as a research report [25]. It has then been extended into a book chapter [24].

The techniques developed in this work are extensively used in our 3D printing sotfware IceSL (see section 4.2).

5.2.7. *Techniques for Shooting Highly Coherent Rays*

Participant: Samuel Hornus.

This work explores novels ways to exploit the coherence of some set of rays used in the ray-tracing and other realistic image synthesis techniques. We propose new ways to traverse the usual data-structure for 3D indexes and leverage optimized and exact geometric predicates. Our first results give a faster ray shooting technique for pinhole camera rays and exhibit a remarkable increase in efficiency as the number of rays rises. A manuscript was submitted but not accepted to Eurographics.

5.3. Algorithms and analysis

Participant: Laurent Alonso.

5.3.1. *The Majority Problem*

Given a set of n elements each of which is either red or blue, Boyer and Moore's algorithm uses pairwise equal/not equal color comparisons to determine the majority color. We analyze the average behavior of their algorithm, proving that if all 2^n possible inputs are equally likely, the average number of color comparisons used is $n - \sqrt{2n/\pi} + O(1)$ and has variance $\frac{\pi-2}{\pi}n - \frac{\sqrt{2\,n}}{\sqrt{\pi}} + O(1)$. This joint work with Edward M. Reingold was published in the IPL journal [8].

5.3.2. *The $X + Y$ Sorting Problem*

Some combinatorial approaches were taken to try to find bounds on the $X + Y$ problem: Given two lists: $X = (x_1, ..., x_n), Y = (y_1, ..., y_m)$, determine the ordering of the values $x_i + y_j$ for $i \in [1, n], j \in [1, m]$.

5.4. Fractal Geometry

Participant: Dmitry Sokolov.

Fractal geometry is a relatively new branch of mathematics that studies complex objects of non-integer dimensions. It finds applications in many branches of science as objects of such complex structure often exhibit interesting properties.

In 1988 Barnsley presented the Iterative Function System (IFS) model that allows modelling complex fractal shapes with only a limited set of contractive transformations. Later many other models were based on the IFS model such as Language-Restricted IFS, Projective IFS, Controlled IFS and Boundary Controlled IFS. The latter allows modeling complex shapes with control points and specific topology. These models cover classical geometric models such as B-splines and subdivision surfaces as well as fractal shapes.

This year we focused on the analysis of the differential behaviour of the shapes described with Controlled IFS and Boundary Controlled IFS. We derive the necessary and sufficient conditions for differentiability for everywhere dense sets of points. Our study is based on the study of the eigenvalues and eigenvectors of the transformations composing the IFS.

We apply the obtained conditions to modeling curves in surfaces. We describe different examples of differential behaviour presented in shapes modeled with Controlled IFS and Boundary Controlled IFS. We also use the Boundary Controlled IFS to solve the problem of connecting different subdivision schemes. We construct a junction between Doo-Sabin and Catmull-Clark subdivision surfaces and analyse the differential behaviour of the intermediate surface.

An article about this work is in the publication process in LNCS.

5.5. Scientific Computing for Linear and Nonlinear Wave Problems

Participant: Xavier Antoine.

We consider the Backward Euler SPectral (BESP) scheme that was proposed for computing the stationary states of Bose-Einstein Condensates (BECs) through the Gross-Pitaevskii equation. We show that the fixed point approach introduced earlier fails to converge for fast rotating BECs. A simple alternative approach based on Krylov subspace solvers with a Laplace or Thomas-Fermi preconditioner is given. Numerical simulations (obtained with the associated freely available Matlab toolbox GPELab) for complex configurations show that the method is accurate, fast and robust for 2D/3D problems and multi-components BECs.

This work was published in the journal "Journal of Computational Physics" [9].

5.6. Accelerating Structural Biology Software

Participant: Xavier Cavin.

This work is a collaboration with Dave Ritchie (team ORPAILLEUR, Nancy). The aim of this project is to leverage parallelism, multi-core computing and GPU in order to speed-up costly computations in cryo-electron microscopy. Several tools have been developped. Two of those "gEM tools" have been the subject of two articles were published in 2013 in "Journal of Structural Biology" [10] and "BMC Structural Biology" [11].

MAGRIT Project-Team

6. New Results

6.1. Motion, Scene and Camera Reconstruction

Participants: Marie-Odile Berger, Srikrishna Bhat, Pierre Rolin, Gilles Simon, Frédéric Sur.

- **Metrological performance enhancement and resolution assessment for experimental solid mechanics**

  This work is motivated by image processing problems from experimental solid mechanics. One of the problem in this field is to measure heterogeneous strains on the surface of specimens subjected to mechanical tests, through an imaging device. Among full-field measurement techniques, the grid method consists in transferring a regular grid on the surface of the specimen and in taking images of the grid before and after deformation. Windowed Fourier analysis then gives an estimation of the surface displacement and strain components. In a collaboration with Institut Pascal (Université Blaise Pascal, Clermont Ferrand), we have shown that the estimations obtained by this technique are a first-order approximation of the convolution of the actual values with the analysis window. We have also characterized how the noise in the grid image impairs the displacement and strain maps [3]. This study has allowed us to improve the metrological performance of the grid method with deconvolution algorithms. A numerical and experimental study can be found in [10], [16], [21]. As any contactless measurement method, the resolution of the grid method is limited by the noise impairing the sensor. We have also characterized this resolution within a Poisson-Gaussian noise model, which is known to be realistic for CCD or CMOS sensors [4].

- **Matching in difficult conditions**

  Visual vocabularies are emerging as a new tool for building point correspondences for pose estimation. Within S. Bhat's PhD thesis [9] we have proposed several methods for visual word construction dedicated to point matching, with structure from motion and pose estimation applications in view. The three dimensional geometry of a scene is first extracted with bundle adjustment techniques based on keypoint correspondences. These correspondences are obtained by grouping the set of all SIFT descriptors from the training images into visual words. We obtain a more accurate 3D geometry than with classical image-to-image point matching. In a second on-line step, these visual words serve as 3D point descriptors that are robust to viewpoint change, and are used for building 2D-3D correspondences on-line during application, yielding the pose of the camera by solving the PnP problem. Several visual word formation techniques have been compared with respect to robustness to viewpoint change between learning and the test images.

  The PhD thesis of P. Rolin comes within the scope of camera pose estimation from an unstructured 3D point dataset, endowed with image descriptors. His work focuses on improving pose estimation with respect to strong viewpoint changes. 2D-3D correspondences are actually difficult to establish if there are too large viewpoint changes between the image whose pose is sought and the images that gave the 3D point dataset. P. Rolin currently assesses viewpoint simulation techniques in order to enhance the description of the 3D points with information from different viewpoints.

- **Acquisition of 3D calibrated data**

---

[3] F. Sur, M. Grédiac. Towards deconvolution to enhance the grid method for in-plane strain measurement. To appear in AIMS Inverse Problems and Imaging, American Institute of Mathematical Sciences, 2014.

[4] M. Grédiac, F. Sur. Effect of sensor noise on the resolution and spatial resolution of displacement and strain maps estimated with the grid method. To appear in Strain, Wiley, 2014.

In situ modeling is generating increasing interest in the community as it makes it possible to build AR applications in unprepared environments. In [19], we present a new method for interactive modeling of polygonal scenes, using a tablet PC, a laser rangefinder, an inertial measurement unit (IMU) and a camera. A well-founded calibration method is used to determine the orientation of the IMU and the origin and direction of the laser beam in the camera coordinate system. A new hybrid, driftless orientation tracking method is proposed, inspired by the tracking-by-synthesis algorithm adapted to 3-degree-of-freedom camera motions. Visual hints are provided during the tracking-and-modeling process in order to help the user get the best possible accuracy. These visual hints are based on a PCA analysis of the reconstructed laser point clouds and statistical measurements of the camera tracking accuracy.

6.2. Medical Imaging

Participants: René Anxionnat, Marie-Odile Berger, Nazim Haouchine, Erwan Kerrien, Matthieu Loosvelt, Pierre-Frédéric Villard, Brigitte Wrobel-Dautcourt, Ahmed Yureidini.

- **Interventional neuro radiology**
  Minimally invasive techniques impact surgery in such ways that, in particular, an imaging modality is required to maintain a visual feedback. Live X-ray imaging, called fluoroscopy, is used in interventional neuroradiology. Such images are very noisy, and cannot show but the vasculature and no other brain tissue. Most of all, and despite recent progress on the sensors, X-rays are bad for the patient's health and X-ray images are 2D projections deprived of any depth hint such as occlusions or shading. To quote a fellow physician: "it is rather uncanny to use 2D images to perform a gesture that is, by nature, 3D". Two of our long term aims in interventional neuroradiology are to reduce the operation time, and provide the interventional radiologists with a real-time visual feedback in 3D.

  All our research activity in this field is led in collaboration with the Department of Interventional Neuroradiology from Nancy University Hospital. This year was pivotal in this activity where some projects ended and other new projects started.

  We've been collaborating with Shacra Inria project-team (Lille-Nord Europe) in the context of the SOFA-InterMedS Inria Large-Scale Initiative for 4 years. Ahmed Yureidini is on the verge of defending his PhD thesis and the last step of his work consisted in validating the model he devised for the blood vasculature as a tree of local implicit surfaces [8]. Comparisons were made against simulations using triangular meshes against our implicit model and they showed a reduction by 2 orders of magnitude in computing time while numerical instabilities encountered with meshes (jaggy motions, unrealistic sticking of the catheter tip on the vessel surface, ...) were not observed with our implicit model. Publication of these results is under way.

  We also collaborate with Shacra team within the ANR IDeaS project. Computer simulations are very sensitive to inaccuracies in the various mechanical parameters or geometrical boundary conditions. Such inaccuracies are ubiquitous when dealing with patient-based data. We aim at developing Image-Driven Simulation to add the live X-ray images as new constraints to make the simulated surgical tool virtual visualization fit their position seen in the actual images. This year, a sensor was designed and tested to capture the motion of the line-shaped micro-tools (catheters, guidewires, etc...) and progress was made to design Kalman-like filters compliant with Sofa simulation platform.

  Our long-term collaboration with GE Healthcare took a new step this year with the arrival of Charlotte Delmas as a PhD student. She will work towards devising algorithms to reconstruct the micro-tools in 3D from fluoroscopy images.

- **Designing respiration models for patient based simulators**
  Respiration models are useful in many ways. They can be used in: 1) pulmonary radiotherapy, where the tumor displacement should be accurately known to be targeted by ionizing radiation, 2) thoracic surgery simulators, where breathing motion increases the realism of virtual patients, 3) interventional radiology, where augmented medical imaging that incorporates breathing motion can be used during treatment.

However building and parameterizing a fast and accurate respiration model is still an open problem. We continue this year to work on evolutionary methods to estimate the parameters of a complex 15-D respiration model on 5 patients [23]. A compound fitness function has been designed to take into account various quantities that have to be minimized.

The optimized parameters have been applied to an interventional radiology simulator that takes into account the respiration [14]. It also includes: segmentation, physically based modeling, haptics rendering, pseudo-ultrasound generation and the concept of a physical mannequin. It is the result of a close collaboration between different universities (Liverpool, Manchester, Imperial College, Banghor, Leeds, Hull) involving computer scientists, clinicians, clinical engineers and occupational psychologists.

- **Realistic simulation of organ dissection** Whilst laparoscopic surgical simulators are becoming increasingly realistic they can not, as yet, fully replicate the experience of live surgery. In particular tissue dissection is one task that is particularly challenging to replicate. Limitation of current attempts to simulate tissue dissection include: poor visual rendering; over simplification of the task and; unrealistic tissue properties. In an effort to generate a more realistic model of tissue dissection in laparoscopic surgery we worked on a novel method based on task analysis. Initially we have chosen to model only the basic geometrics of this task rather than a whole laparoscopic procedure. This year preliminary work has led to the development of a real time simulator performing organ dissection with a haptic thread at 1000Hz. 2D soft-tissue models replicate the process of tissue cutting.

- **Physics-based augmented reality**
  The development of AR systems for use in the medical field faces one major challenge: the correct superposition of pre-operative data onto intraoperative images. This task is especially difficult when laparospic surgery is considered since superposition must be achieved on deformable organs. Most existing AR systems only consider rigid registration between the pre and intraoperative data and the transformation is often computed interactively or from markers attached to the patient's body.

  In cooperation with the Shacra team, we have proposed in [17], [18] a framework for real-time augmentation of the vascular network and tumors during minimally invasive liver surgery. Internal structures computed from pre-operative CT scans can be overlaid onto the laparoscopic view for surgery guidance. Compared to state-of-the-art methods, our method uses a real-time biomechanical model to compute a volumetric displacement field from partial three-dimensional liver surface motion.

  The main contributions of this work are threefold: a) the use of a biomechanical model of liver deformation allows us to account for heterogeneity and anisotropy due to veins and arteries. In addition, the physical model is used as regularizer for the unreliable measurement of the visual tracking and as motion compensation in poorly textured areas; b) a real-time implementation of this virtual liver model has been proposed c) appropriate boundary conditions and external force have been defined which guide the biomechanical model using partial 3D motion estimated at the liver surface from a stereo video stream.

  Thanks to this framework, we are able to estimate, in real-time, relevant positions of internal structures of the liver (vessels and tumors) taking into account liver deformations and tissue heterogeneity.

MAIA Project-Team

6. New Results

6.1. Decision Making

6.1.1. Searching for Information with MDPs

Participants: Mauricio Araya, Olivier Buffet, Vincent Thomas, François Charpillet.

In the context of Mauricio Araya's PhD and PostDoc, we are working on how MDPs – or related models – can search for information. This has led to various research directions, such as extending POMDPs so as to optimize information-based rewards, or actively learning MDP models. This year has begun with the defense of Mauricio's PhD thesis in February. Since then, we have kept extending Mauricio's work and are preparing journal submissions.

While we have done some progress in this field, there are no concrete outcomes to present concerning optimistic approaches for model-based Bayesian Reinforcement Learning. Concerning POMDPs with information-based rewards, Mauricio's PhD thesis presents strong theoretical results that allow – in principle – deriving efficient algorithms from state-of-the-art "point-based" POMDP solvers. This year we have put this idea into practice, implementing variants of PBVI, PERSEUS and HSVI.

Preliminary results have been published (in French) in JFPDA'13 [32]. A journal paper with complete theoretical and empirical results is under preparation.

6.1.2. Adaptive Management with POMDPs

Participant: Olivier Buffet.

Samuel Nicol, Iadine Chadès (CSIRO), Takuya Iwamura (Stanford University) are external collaborators.

In the field of conservation biology, adaptive management is about managing a system, e.g., performing actions so as to protect some endangered species, while learning how it behaves. This is a typical reinforcement learning task that could for example be addressed through Bayesian Reinforcement Learning.

This year, we have worked in the context of bird migratory pathways, in particular the East Asian-Australasian (EAA) flyway, which is modeled as a network whose nodes are land areas where birds need to stay for some time. An issue is that these land areas are threatened due to sea level rise. The adaptive management problem at hand is that of deciding in the protection of which land areas to invest money so as to preserve the migratory pathways as efficiently as possible.

The outcome of this work is a data challenge paper published at IJCAI'13 [27], which presents the problem at hand, describes its POMDP model, gives empirical results obtained with state-of-the-art solvers, and challenges POMDP practitioners to find better solution techniques.

6.1.3. Solving decentralized stochastic control problems as continuous-state MDPs

Participants: Jilles Dibangoye, Olivier Buffet, François Charpillet.

External collaborators: Christopher Amato (MIT), Arnaud Doniec (EMD), Charles Bessonnet (Telecom Nancy), Joni Pajarinen (Aalto University).

Decentralized partially observable Markov decision processes (DEC-POMDPs) are rich models for cooperative decision-making under uncertainty, but are often intractable to solve optimally (NEXP-complete), even using efficient heuristic search algorithms. In this work, we present an efficient methodology to solving decentralized stochastic control problems formalized as a DEC-POMDP or its subclasses. This methodology is three-fold: (1) it converts the original decentralized problem into a centralized problem from the perspective of a solution method that can take advantage of the total data about the original problem that is available during the online execution phase; (2) it shows that the original and transformed problems are equivalent; (3) it solves the transformed problem using a centralized method and transfers the solution back to the original problem. We applied this methodology in various different decentralized stochastic control problems.

Our results include the application of this methodology over DEC-POMDPs [20], [33]. We recast them into deterministic continuous-state MDPs, where states — called *occupancy states* — are probability distributions over states and action-observation histories of the original DEC-POMDPs. We also demonstrate the occupancy state is a sufficient statistic for optimally solving DEC-POMDPs. We further show the optimal value function is a piecewise-linear and convex function of the occupancy states. With these results as a background, we prove for the first time that POMDP (and more generally continuous-state MDP) solution methods can, at least in principle, apply in DEC-POMDPs. This work has been presented at IJCAI'2013 [20] and (in French) at JFPDA'2013 [33], and an in-depth journal article is currently under preparation. We have already extended the results we obtained for general DEC-POMDPs in the case of transition- and observation-independent DEC-MDPs. Of particular interest, we demonstrated that the occupancy states can be further compressed into a probability distribution over the states — the first sufficient statistic in decentralized stochastic control problems that is invariant with time. This work has been presented at AAMAS'2013 [21], and an in-depth journal article is currently under preparation.

We believe our methodology lays the foundation for further work on optimal as well as approximate solution methods for decentralized stochastic control problems in particular, and stochastic control problems in general.

6.1.4. *Abstraction Pathologies in Markov Decision Processes*
Participants: Manel Tagorti, Bruno Scherrer, Olivier Buffet.

Jörg Hoffmann, former member of MAIA, is an external collaborator (from Saarland University).

Abstraction is a common method to compute lower bounds in classical planning, imposing an equivalence relation on the state space and deriving the lower bound from the quotient system. It is a trivial and well-known fact that refined abstractions can only improve the lower bound. Thus, when we embarked on applying the same technique in the probabilistic setting, our firm belief was to find the same behavior there. We were wrong. Indeed, there are cases where every direct refinement step (splitting one equivalence class into two) yields strictly worse bounds. We give a comprehensive account of the issues involved, for two wide-spread methods to define and use abstract MDPs.

This work has been presented and published in the ICAPS-13 workshop on Heuristics and Search for Domain-Independent Planning (HSDIP) [29] and (in French) in JFPDA-13 [37].

6.1.5. *Evolutionary programming for Policies Space exploration*
Participants: Amine Boumaza, Vincent Thomas.

Evolutionary Programming proposed by Fogel (initially introduced in 1966) is an approach to build an automaton optimizing a fitness function. Like other evolutionary algorithms, an initial population of automata is given, and the evolutionary programming algorithm will make this population evolve by progressively modifying automata (mutations) and keeping the most efficient ones in the next generation.

This process is close to the progressive construction by a policy iteration algorithm in a POMDP and we are currently investigating the links between these approaches.

This work has begun this year through an internship (Benjamin Bibler) and preliminary development has been made to solve the Santa Fe trail problem proposed by Koza (1992) which has become a benchmark to compare genetic and evolutionary programming approaches.

6.1.6. *Evolutionary Learning of Tetris Policies*
Participant: Amine Boumaza.

Learning Tetris controllers is an interesting and challenging problem due to the fact of the size of its search space where traditional machine learning methods do not work and the use of approximate methods is necessary (see 6.1.10). In this work we study the performance of a direct policy search algorithm namely the Covariance Matrix Adaptation Evolution Strategy (CMAES). We also proposed different techniques to reduce the learning time, one of which is racing. This approach concentrates the computation effort on promising policies and quickly disregards bad ones in order do reduce the computation time. This approach allowed to

obtain policies of the same performance as those obtained without but at the fifth of the computation cost. The learned strategies are among the best performing players at this time scoring several millions of lines on average.

6.1.7. *Evolutionary behavior learning*

Participants: Amine Boumaza, François Charpillet, Iñaki Fernandèz.

Evolutionary Robotics (ER) deals with the design of agent behaviors using artificial evolution. Within this framework, the problem of learning optimal policies (or controllers) is treated as a policy search problem in the parameterized space of candidate policies. The search for the optimal policies in this context is driven by a fitness function that associates a value to the candidate policy by measuring its performance on the given task.

The work shown here describes the results of the master's thesis of Inãki Fernandèz which will be extended during a Ph.D. thesis started on october 2014.

- **Incremental policy learning with shaping**. Several methods have been proposed to accelerate the search for optimal policy in evolutionary robotics. In this work, we investigated the use of incremental learning and, more precisely, shaping, a well-known technique in behavioral psychology. The main idea is to learn to solve simple tasks and then exploit the learned behaviors to tackle increasingly harder tasks.

  Our preliminary results show that the best performances are obtained either in the setups with shaping or in the control experiment where the task difficulty is maximal. Nevertheless, a closer look at the results indicates that the best controllers for the shaping setups are not obtained at the end of the evolution, but rather at an earlier stage. This means that, for these shaping techniques, the best controllers have learned to solve the task when its difficulty was at an easy level and their performance is maintained later when the task difficulty increases. Although this was unforeseen, the results seem promising and deserve further investigation.

- **Online evolutionary learning**. As opposed to traditional evolutionary robotics which treat the learning problem as an off-line, centralized process, online onboard distributed evolutionary algorithms [67], [55] consider the learning process as executed at the agent level in a decentralized way. In this sense, each agent has its own controller or genome which is locally broadcasted from agent to agent and the best performing ones survive and spread. This gene-centered view of evolution is inspired from the theory introduced by Richard Dawkins: The selfish gene.

  The online aspect of the algorithms means that the agents are learning at the same time they are performing the task at hand. Another property that derives is that the agents are continuously learning which allows them to adapt to dynamically changing conditions and tasks. This is in opposition to the traditional view of evolutionary robotics (offline) where the outcome of evolution is tailored toward single task. Many challenging problems are raised in this framework and this thesis will address the problem of defining fitness functions that drive a swarm of agents to learn to solve a task. One other question is to study the dynamics of these algorithms both experimentally and theoretically using tools from distributed systems. Some promising work in this direction has been proposed [54].

6.1.8. *Learning Bad Actions*

Participant: Olivier Buffet.

Jörg Hoffmann, former member of MAIA, and Michal Krajňanský are external collaborators from Saarland University.

In classical planning, a key problem is to exploit heuristic knowledge to efficiently guide the search for a sequence of actions leading to a goal state.

In some settings, one may have the opportunity to solve multiple small instances of a problem before solving larger instances, e.g., trying to handle a logistics problem with small numbers of trucks, depots and items before moving to (much) larger numbers. Then, the small instances may allow to extract knowledge that could be reused when facing larger instances. Previous work shows that it is difficult to directly learn rules specifying which action to pick in a given situation. Instead, we look for rules telling which actions should not be considered, so as to reduce the search space. But this approach requires considering multiple questions: What are examples of bad (or non-bad) actions? How to obtain them? Which learning algorithm to use?

This research work is conducted as part of Michal Krajňanský's master of science (to be defended in early 2014). Early experiments show encouraging results, and we consider participating in the learning track of the international planning competition in 2014.

6.1.9. Complexity of the Policy Iteration algorithm
Participant: Bruno Scherrer.

We have this year improved the state-of-the-art upper bounds for the complexity of a standard algorithm for solving Markov Decision Processes: Policy Iteration.

Given a Markov Decision Process with n states and m actions per state, we study the number of iterations needed by Policy Iteration (PI) algorithms to converge to the optimal γ-discounted optimal policy. We consider two variations of PI: Howard's PI that changes the actions in all states with a positive advantage, and Simplex-PI that only changes the action in the state with maximal advantage. We show that Howard's PI terminates after at most $O\left(\frac{nm}{1-\gamma} \log\left(\frac{1}{1-\gamma}\right)\right)$ iterations, improving by a factor $O(\log n)$ a result by Hansen et al. (2013), while Simplex-PI terminates after at most $O\left(\frac{n^2 m}{1-\gamma} \log\left(\frac{1}{1-\gamma}\right)\right)$ iterations, improving by a factor $O(\log n)$ a result by Ye (2011). Under some structural assumptions of the MDP, we then consider bounds that are independent of the discount factor γ: given a measure of the maximal transient time τ_t and the maximal time τ_r to revisit states in recurrent classes under all policies, we show that Simplex-PI terminates after at most $\widetilde{O}\left(n^3 m^2 \tau_t \tau_r\right)$ iterations. This generalizes a recent result for deterministic MDPs by Post & Ye (2012), in which $\tau_t \leq n$ and $\tau_r \leq n$. We explain why similar results seem hard to derive for Howard's PI. Finally, under the additional (restrictive) assumption that the state space is partitioned in two sets, respectively states that are transient and recurrent for all policies, we show that Simplex-PI and Howard's PI terminate after at most $\widetilde{O}(nm(\tau_t + \tau_r))$ iterations.

These results were presented at the JFPDA national workshop [36] and at the NIPS 2013 international conference [28].

6.1.10. Approximate Dynamic Programming and Application to the Game of Tetris
Participant: Bruno Scherrer.

Victor Gabillon and Mohammad Ghavamzadeh are external collaborators (from the Inria Sequel EPI). Matthieu Geist is an external collaborator (from Supélec Metz).

We present here three results: the first is a unified review of algorithms that are used to estimate a linear approximation of the value of some policy in a Markov Decision Process; the second concerns the analysis of a class of approximate dynamic algorithms for large scale Markov Decision Processes; the last is the successful application of similar dynamic programming algorithms on the Tetris domain.

In the framework of Markov Decision Processes, we have considered linear *off-policy* learning, that is the problem of learning a linear approximation of the value function of some fixed policy from one trajectory possibly generated by some other policy. We have made a review of *on-policy* learning algorithms of the literature (gradient-based and least-squares-based), adopting a unified algorithmic view. We have highlighted a systematic approach for adapting them to *off-policy* learning *with eligibility traces*. This lead to some known algorithms and suggested new extensions. This work has recently been accepted to JMLR and should be published at the beginning of 2014 [6].

We have revisited the work of Bertsekas and Ioffe (1996), that introduced λ policy iteration-a family of algorithms parametrized by a parameter λ-that generalizes the standard algorithms value and policy iteration, and has some deep connections with the temporal-difference algorithms described by Sutton and Barto (1998). We deepen the original theory developed by the authors by providing convergence rate bounds which generalize standard bounds for value iteration. We develop the theory of this algorithm when it is used in an approximate form. This work was published in JMLR [7].

Tetris is a video game that has been widely used as a benchmark for various optimization techniques including approximate dynamic programming (ADP) algorithms. A look at the literature of this game shows that while ADP algorithms that have been (almost) entirely based on approximating the value function (value function based) have performed poorly in Tetris, the methods that search directly in the space of policies by learning the policy parameters using an optimization black box, such as the cross entropy (CE) method, have achieved the best reported results. We have applied an algorithm we proposed in the past, called classification-based modified policy iteration (CBMPI), to the game of Tetris. Our experimental results show that for the first time an ADP algorithm, namely CBMPI, obtains the best results reported in the literature for Tetris in both small 10×10 and large 10×20 boards. Although the CBMPI's results are similar to those of the CE method in the large board, CBMPI uses considerably fewer (almost 1/6) samples (calls to the generative model) than CE. This work was presented at NIPS 2013 [26].

6.2. Ambiant Intelligence And Robotic Systems

6.2.1. *Robotic systems : autonomy, cooperation, exploration, robustness, assistance*

6.2.1.1. *Local control based platooning*
Participants: Jano Yazbeck, François Charpillet, Alexis Scheuer.

We consider decentralized control methods to operate autonomous vehicles at close spacings to form a platoon. We study models inspired by the flocking approach, where each vehicle computes its control from its local perceptions. We investigate different decentralized models in order to provide robust and callable solutions. Open questions concern collision avoidance, stability and multi-platoon navigation.

In order to reduce the tracking error (*i.e.* the distance between each follower's path and the path of its predecessor), we developed both an innovative approach [68] and a new lateral control law. This lateral control law reduces the tracking error faster than other existing control laws. An article, presenting this control law, its integration with a previously defined secure longitudinal control law [64] and the experimental results obtained with it, has been accepted to 2014 IEEE International Conference on Robotics and Automation.

6.2.1.2. *Map Matching*
Participants: François Charpillet, Maan El-Badaoui-El-Najjar.

We addressed an important issue for intelligent transportation system, namely the ability of vehicles to safely and reliably localize themselves within an a priori known road map network. For this purpose, we proposed an approach based on hybrid dynamic bayesian networks enabling to implement in a unified framework two of the most successful families of probabilistic model commonly used for localization: linear Kalman filters and Hidden Markov Models. The combination of these two models enables to manage and manipulate multi-hypotheses and multi-modality of observations characterizing Map Matching problems and it improves integrity approach. Another contribution is a chained-form state space representation of vehicle evolution which permits to deal with non-linearity of the used odometry model. Experimental results, using data from encoders' sensors, a DGPS receiver and an accurate digital roadmap, illustrate the performance of this approach, especially in ambiguous situations [8].

6.2.1.3. *Adaptation of autonomous vehicle traffic to perturbations*
Participants: Mohamed Tlig, Olivier Simonin, Olivier Buffet.

The aim of the European project InTraDE is to propose more efficient ways to handle containers in seaports through the use of IAVs (Intelligent Autonomous Vehicles).

In his PhD thesis, Mohamed Tlig considers the displacements of numerous such IAVs whose routes are a priori planned by a supervisor. However, in such a large and complex system, different unexpected events can arise and degrade the traffic: failure of a vehicle, human mistake while driving, obstacle on roads, local re-planning, and so on.

After working on a simple decentralized strategy to allow two queues of vehicles to share a single lane (presented in 2012, and this year in AATMO-13 [30]), we have started looking at improving vehicle flows in complete road networks. In particular, we have proposed an approach that allows multiple flows of vehicles to cross an intersection without stopping, allowing to reduce delays as well as energy consumption. Preliminary results have been presented (in French) at RJCIA-13 [38], and more advanced work is under submission.

The next step is to coordinate the controller agents located in each of the network's intersections so as to create "green waves" that would improve the flows not just locally, but globally.

6.2.1.4. Living assistant Robot
Participants: François Charpillet, Antoine Bautin, Abdallah Dib, Olivier Simonin.

With LAR (**living AssistanT Robot**), a PIA projet which started in March, Abdallah Dib joined our team for a PhD. His work is about the development of a low cost navigation system for a robot evolving in an indoor environment. The main issue of his work is to design a Simultaneous Localisation and Mapping algorithm working in a dynamic environment in which people are moving. This is very challenging if we restrict the sensing capabilities of the robot with low cost sensors such as RGB-D camera. An important service we expect the robot to achieve, is realizing similar services as the one we described below: fall detection, activity recognition.

6.2.1.5. Exploring an unknown environment with a team of mobile robots
Participants: François Charpillet, Olivier Simonin, Antoine Bautin, Nassim Kaldé.

This work has been realized during the ANR Cart-O-matic project. Antoine Bautin has been hired by the Maia team for this project for a PhD. The main objective of the project was to design and build a multi-robot system able to autonomously map an unknown building. This work has been done in the framework of a French robotics contest called Defi CAROTTE organized by the General Delegation for Armaments (DGA) and the French National Research Agency (ANR). The scientific issues of this project deal with Simultaneous Localization And Mapping (SLAM), multi-robot collaboration and object recognition. The Maia Team has been mainly involved in multi-robot collaboration and navigation [13], [1], [11].

Nassim Kaldé, a new PhD student started last year in order to carry out the work done by Antoine Bautin. The new directtion aims at addressing similar problems as the one we addressed in Cart-O-matic project but with dynamical environment, i.e. environment in which people are evolving with robots. An other point that Nassim Kaldé will address is social navigation, which is important for robot and human to coexist in a smart manner.

6.2.1.6. Features extraction for the control of redundant system with continuous sensori-motor space
Participants: Alain Dutech, Thomas Moinel.

Yann Boniface (CORTEX Team, Loria) is an external collaborator

In collaboration with the CORTEX team and supported by a M2R internship, many questions related to learning the control of a complex (mono)-agent system with a continuous sensori-motor space are explored. For several reasons, the classical framework of Reinforcement Learning is not easily used in that context:

- the value function to be learned has to be encoded using features that are not known at start,

- because of the richness of the sensori-motor space, a random exploration scheme is unlikely to find the rewarded states that are needed by the learning process,

- exploiting what is learned is difficult as one would need to find the maximum of the value function *while* it is learned.

../../../../projets/maia/IMG/bras6muscles_eng.png

Figure 1. Model of 2-joint human arm with 6 muscles.

Our work is focused on a planar model of the human arm with 2 joints and 6 muscles (see figure 1). Control signals are the activity of the motor-neurons that alter the length of the muscles, and thus the forces applied on the joints. This system is redundant but also highly non linear as many aspects of the model are described by non-linear differential equations (our model is a slight improvement over the one of Li [59]). The task to learn is to reach different positions from given starting points.

We have studied a developmental learning process with a simple muscle activation pattern. The idea is to start the learning process in an artificially reduced sensori-motor space (using rough perception and motor capacities) and slowly increase the size and complexity of this space when interesting behaviors are learned. Our approach [60] gives results comparable to other developmental techniques and raises several important research questions. Our work showed that we need an abstraction mechanism in order to define or refine the features used in actions but also in perceptions. This is a very difficult challenge that is one of the keys to the understanding (and design) of cognition. There is also a need for stronger generalization capabilities in the function approximation used in the process.

In parallel, we are taking inspiration from the field of neurosciences, and particularly on the coupling between the cortex and the cerebellum in motor control. Models based on the work of Kaladjian [58] should help us understand what control signals are used by the brain apparatus and how the learning of gestures is organized between these two regions. Our long term goal is to design mechanisms for learning features abstraction in the sensori-motor space while being guided by the improvement in behavior performances.

6.2.2. *Ambiant intelligence*

6.2.2.1. *Personnaly Assisted Living*
Participants: François Charpillet, Amandine Dubois, Olivier Simonin.

This action is supported by the Inria IPL Personally Assisted Living (PAL) which gathers 9 Inria teams associated with 6 research partners (technological, medical or social) which work together on three main issue guidelines: mobility assistance, assessing the degree of frailty of the persons, home activities analysis. The MAIA team is currently mainly involved in the 2 later topics, plus fall detection.

- **Evaluation of the degree of frailty of the elderly.** As argued in the famous paper of Fried *et al* [56] the estimation of frailty is highly significant to evaluate the risk of falls, disability, hospitalization and mortality. This issue is considered in Maia Team with different sensing devices: single RGB-D cameras [34], network of RGB-D cameras, sensing intelligent floor. One simple idea which is currently developed in the team is to determine either the center of mass of a person using one or several kinects, or the center of pressure and footsteps localization using an intelligent floor. The idea is to induce from these simple measures, the walking speed, the length of the steps and the position of the monitored persons.

- **People activity analysis.** The follow-up of the activity of elderly people over long period of time can be a good indicator of their well-being, but the evalution of the behavior of a person at home is an open challenge.

  To address this issue, we proposed this year a HMM based model capable of following simple activities such as sitting, walking, etc. An evaluation of this model has been conducted within a real smart environment with 26 subjects which were performing any of eight activities (sitting, walking, going up, squatting, lying on a couch, falling, bending and lying down). Seven out of these eight activities were correctly detected among which falling which was detected without false positives [24].

- **Fall detection.** Elderly fall is one of the major health issues affecting elderly people, especially at home. One of the objectives of the PhD work of Amandine Dubois is to design an automatic system to detect fall at home, which in its final version will be made up of a network of RGB-D sensors. A simple and robust method based on the identification and tracking of the center of mass of people evolving in an indoor environment has been developed. Using a simple Hidden Markov Model whose observations are the position of the center of mass, its velocity and the general shape of the body, we

can surprisingly monitor the activity of a person with high accuracy and thus detect falls with very good accuracy without false positives [22], [23]. An experimental study, that is reported here, has been driven in our smart apartment lab. 26 subjects were asked to perform a predefined scenario in which they realized a set of eight postures. 2 hours of video (216 000 frames) were recorded for the evaluation, half of it being used for the training of the model. The system detected the falls without false positives. This result encourages us to use this system in real situation for a better study of its efficiency.

6.2.2.2. Interconnected intelligent tiles
Participants: Mihai Andries, François Charpillet, Olivier Simonin.

We are also involved in the development of a new innovative sensing device: a Pressure-Sensing Floor with LED lighting making possible to provide a new way for people to interact with their environment. Sensitive or intelligent floors have attracted a lot of attention during the last two decades for different applications going from interaction capture in immersive virtual environments to robotics or human tracking, fall detection or activity recognition. Different technologies have been proposed so far either based on optical fiber sensing, pressure sensing or electrical near field. In the Maia Team, we have developed a more sophisticate approach in which both computation and sensing is distributed within the floor. This floor is made up of interconnected intelligent titles with can communicate with each other, have internal computation power, sense the environment activity (through four weight sensors, an accelerometer and a magnetometer) and can interact with users, robots or other sensor networks either by wireless/wire communication or through visual communication (each tile being equipped with 16 leds).

Several scientific challenges are open to us in the fields of decentralized spatial computing and in designing real application for assisting people suffering from loss of autonomy.

Some of these issues have been addressed this year. Mihai Andries, a PhD student, proposed two contributions demonstrating the relevancy of an intelligent floor such as the one we have developed. First contribution is about controlling a mobile robot through its interactions throughout the floor [10]. The second, least developed is about activity recognition of a person through its physical interaction on the floor. This approach has an important advantage compared to video based activity recognition: the privacy of people is without any doubt guaranteed. Let us mention too, the work of an internship student who developed a gait evaluation algorithm using the variation over time of the center of pressure that is sensed by the floor when one or several person walk over the floor.

6.2.2.3. Multi-Camera Tracking in Partially Observable Environment
Participants: Arsène Fansi Tchango, Olivier Buffet, Vincent Thomas, Alain Dutech.

Fabien Flacher (Thales THERESIS) is an external collaborator.

In collaboration with Thales ThereSIS - SE&SIM Team (Synthetic Environment & Simulation), we focus on the problem of following the trajectories of several persons with the help of several controllable cameras. This problem is difficult since the set of cameras cannot cover simultaneously the whole environment, since some persons can be hidden by obstacles or by other persons, and since the behavior of each person is governed by internal variables which can only be inferred (such as his motivation or his hunger).

The approach we are working on is based on (1) POMDP formalisms to represent the state of the system (person and their internal states) and possible actions for the cameras, (2) a simulator provided and developed by Thales ThereSIS and (3) particle filtering approaches based on this simulator.

From a theoretical point of view, we are currently investigating how to use a deterministic simulator and to generate new particles in order to keep a good approximation of the posterior distribution.

6.3. Understanding and mastering complex systems

6.3.1. *Robustness of Cellular Automata and Reactive Multi-Agent Systems*
Participants: Olivier Bouré, Vincent Chevrier, Nazim Fatès.

Our research on emergent collective behavior focuses on the analysis of the robustness of discrete models of complex systems. We ask to which extent systems may resist to various perturbations in their definitions. We progressed in the knowledge of how to tackle this issue in the case of cellular automata (CA) and multi-agent systems (MAS).

We proposed new definitions of asynchronism in lattice-gas cellular automata [3]. An experimental work was carried out and it was shown that the observation of an asynchronous version of a discrete model of swarm formation could help us gain insight on this well-studied model. The PhD thesis of O. Bouré [2] provides a detailed view of this work.

A study on the density classification problem, a well-studied problem of consensus in cellular automata, was carried out for infinite systems in 1D and 2D and for infinite trees [5], [4]. Positive results were provided and important conjectures were raised.

We proposed a survey on asynchronous cellular automata [25] and explained some of the difficulties in the classification of these objects [9].

In collaboration with colleagues from India, we proposed a complete characterisation of the reversibility of the set of the 256 Elementary Cellular Automata, which are known to be diffcult to study in all generality [53]. We also proposed a mathematical analysis of the second-order phase transitions that are observed in the most simple asynchronous cellular automata [48]. We also coordinated a special issue on asynchronous cellular automata in the *Natural Computing* journal [41].

6.3.2. *Adaptive control of a complex system based on its multi-agent model*

Participants: Vincent Chevrier, Tomas Navarrete.

Laurent Ciarletta (Madynes team, LORIA) is an external collaborator.

Complex systems are present everywhere in our environment: internet, electricity distribution networks, transport networks. These systems have as characteristics: a large number of autonomous entities, dynamic structures, different time and space scales and emergent phenomena. The thesis work of Tomas Navarrete is centered on the problem of control of such systems. The problem is defined as the need to determine, based on a partial perception of the system state, which actions to execute in order to avoid or favor certain global states of the system. This problem comprises several difficult questions: how to evaluate the impact at the global level of actions applied at a global level, how to model the dynamics of a heterogeneous system (different behaviors arise from different levels of interactions), how to evaluate the quality of the estimations obtained trhough the modeling of the system dynamics.

We propose a control architecture based on an "equation-free" approach. We use a multi-agent model to evaluate the global impact of local control actions before applying the most pertinent set of actions.

Our architecture has been prototypically implemented in order to confront the basic ideas of the architecture within the context of simulated "free-riding" phenomenon in peer to peer file exchange networks. We have demonstrated that our approach allows to drive the system to a state where most peers share files, even when the initial conditions are supposed to drive the system to a state where no peer shares. We have also performed experiments with different configurations of the architecture to identify the different means to improve the performance of the architecture.

This work helped us to better identify [16] the key questions that rise when using the multi-agent paradigm in the context of control of complex systems, concerning the relationship between the model entities and the target system entities.

6.3.3. *Multi-Modeling and multi-simulation*

Participants: Vincent Chevrier, Christine Bourjot, Benjamin Camus, Julien Vaubourg.

Laurent Ciarletta and Yannick Presse (Madynes team, LORIA) are external collaborators.

Laurent Ciarletta is the co-advisor of the thesis of Julien Vaubourg.

Models of Complex systems generally require different points of view (abstraction levels) at the same time in order to capture and to understand all the dynamics and the complexity. Consisting of different interacting parts, a model of a complex system also requires the joint and simultaneous use of modeling and simulation tools from different scientific fields.

We proposed the AA4MM meta-model [65] that solves the core challenges of multi-modelling and simulation coupling in an homogeneous perspective. In AA4MM, we chose a multi-agent point of view: a multi-model is a society of models; each model corresponds to an agent and coupling relationships correspond to interaction between agents.

This year we have made progress in the definition of multi-level modeling [15], [42]. We identified several facets of multi-level modeling and implemented them as different kinds of interactions in the AA4MM framework. A demonstration of these different multi-level couplings has been developed on a collective motion phenomenon.

In February started the MS4SG projet which involes MAIA, Madynes and EDF R&D on smart-grid simulation. A Phd thesis started on october 2013 by Julien Vaubourg in the MAIA team on the confrontation of the AA4MM principles against the specificities of smart-grid domain as a kind of complex system.

<div align="center" style="color:red">**ORPAILLEUR Project-Team**</div>

6. New Results

6.1. The Mining of Complex Data

Participants: Mehwish Alam, Aleksey Buzmakov, Melisachew Chekol, Victor Codocedo, Adrien Coulet, Elias Egho, Nicolas Jay, Florence Le Ber, Ioanna Lykourentzou, Luis-Felipe Melo, Amedeo Napoli, Chedy Raïssi, Mohsen Sayed, My Thao Tang, Mohsen Sayed, Yannick Toussaint.

> **Keywords:** formal concept analysis, relational concept analysis, pattern structures, frequent itemset, association rule, graph mining, sequence mining, skyline

Formal Concept Analysis, together with itemset search and association rule extraction, are suitable symbolic methods for KDDK, that may be used for real-sized applications. Global improvements are carried on the scope of applicability, the ease of use, the efficiency of the methods, and on the ability to fit evolving situations. Accordingly, the team is extending these symbolic data mining methods for working on biological or chemical data or textual documents, involving objects with multi-valued attributes (e.g. domains or intervals), n-ary relations, sequences, trees and graphs.

6.1.1. FCA and variations: RCA and Pattern Structures

There are a few extensions of FCA for handling contexts involving complex data formats, e.g. graphs or relational data. Among them, Relational Concept Analysis (RCA) is a process for analyzing objects described both by binary and relational attributes [10]. The RCA process takes as input a collection of contexts and of inter-context relations, and yields a set of lattices, one per context, whose concepts are linked by relations. RCA has an important role in KDDK, especially in text mining [86], [85].

Another extension of FCA is based on Pattern Structures (PS) [92], which allows to build a concept lattice from complex data, e.g. nominal, numerical, and interval data. In [100], pattern structures are used for building a concept lattice from interval data. Since then, we worked on a some experiments involving pattern structures, namely sequence mining [41], information retrieval [48] and functional dependencies [38]. one of the next step is the adaptation of pattern structures to graph mining. Moreover, the notion of similarity between objects is also closely related to pattern structures [99]: two objects are similar as soon as they share the same attributes (binary case) or attributes with similar values or the same description (at least in part). Combination of similarity and pattern structures is also under study, in particular for solving information retrieval and annotation problems.

Finally, there is also an on-going work relating FCA and semantic web. This work focuses on the classification within a concept lattice of the answers returned by SPARQL queries [37], [47], [46], [44]. The concept lattice is then used as an index for navigating and ranking the answers w.r.t. their content and interest for a given objective.

6.1.2. Advances in mining complex data: sequences and healthcare trajectories

Sequence data is widely used in many applications. Consequently, mining sequential patterns and other types of knowledge from sequence data has become an important data mining task. The main emphasis has been on developing efficient mining algorithms and effective pattern representation. The most frequent sequences generally provide a trivial information. When analyzing the set of frequent sequences with a low minimum support, the user is overwhelmed by millions of patterns. In our recent work, the general idea is to extract patterns whose characteristic on a given measure such as the support strongly deviates from its expected value under a null model. The frequency of a pattern is considered as a random variable, whose distribution under the null model has to be calculated or approximated. Then, the significance of the pattern is assessed through a statistical test that compares the expected frequency under the null model to the observed frequency. One of

the key-points of this family of approaches is to choose an appropriate null model. It will ideally be a trade-off between adjustment to the data and simplicity: the model should capture some characteristics of the data, to integrate prior knowledge, without overfitting, to allow for relevant patterns discovery. We introduced a rigorous and efficient approach to mine statistically significant, unexpected patterns in sequences of itemsets. Experiments on sequences of replays of a video game demonstrated the scalability and the efficiency of the method to discover unexpected game strategies. This work was successfully published as an international conference paper [8].

Other work on sequences is in concern with patient trajectories, i.e. the "path" of a patient during its illness. With the increasing burden of chronic illnesses, administrative health care databases hold valuable information that could be used to monitor and assess the processes shaping the trajectory of care of chronic patients. In this context, temporal data mining methods are promising tools, though lacking flexibility in addressing the complex nature of medical events. In a set of recent works with Elias Egho, a PhD candidate, we present new algorithms to extract patient trajectory patterns with different levels of granularity by relying on external taxonomies [52]. Our algorithms rely on the general FCA framework to formalize the general notion of multidimensional healthcare trajectories. We also continued working on the complex notion of sequences or trajectory similarity measures. We show the interest of our approaches with the analysis of trajectories of care for colorectal cancer using data from the French healthcare information system (see also [41]).

6.1.3. KDDK in Text Mining

Ontologies help software and human agents to communicate by providing shared and common domain knowledge, and by supporting various tasks, e.g. problem-solving and information retrieval. In practice, building an ontology depends on a number of "ontological resources" having different types: thesaurus, dictionaries, texts, databases, and ontologies themselves. We are currently working on the design of a methodology and the implementation of a system for ontology engineering from heterogeneous ontological resources [58]. This methodology is based on both FCA and RCA, and was previously successfully applied in contexts such as astronomy and biology. In the framework of the ANR Hybride project (see 8.2.1.2), an engineer is implementing a robust system based on these previous research results, for preparing the way to new research directions involving trees and graphs.

6.2. KDDK in Life Sciences

Participants: Yasmine Assess, Emmanuel Bresso, Adrien Coulet, Marie-Dominique Devignes, Anisah Ghoorah, Bernard Maigret, Amedeo Napoli, Gabin Personeni, David Ritchie, Mohsen Sayed, Malika Smaïl-Tabbone, My Thao Tang, Mohsen Sayed, Yannick Toussaint.

The Life Sciences constitute a challenging domain for KDDK. Biological data are complex from many points of views, e.g. voluminous, high-dimensional and deeply inter-connected. Analyzing such data is a crucial issue in health care, environment and agronomy. Besides, many bio-ontologies are available and can be used to enhance the knowledge discovery process. Accordingly, the research work of the Orpailleur team in KDDK applied to the Life Sciences is developed in one main direction which is in concern with the use of bio-ontologies to improve KDDK but also information retrieval, access to the so-called "Linked Open Data" and data integration.

6.2.1. Using ILP for the characterization and prediction of drug side-effect profiles

Inductive Logic Programming (ILP) is a learning method which allows expressive representation of the data and produces explicit first-order logic rules [89]. We applied ILP for understanding drug side-effets. Indeed, late appearance of adverse side effets during clinical trials constitute the main reason for stopping the drug development process which is very costly [1]. Improving our ability to understand drug side effects is necessary to reduce this inconvenience. Moreover, it can contribute to design safer drugs and anticipate the appearance of yet unreported side effects of approved drugs. Today, most investigations deal with prediction of single side effects and overlook possible combinations.

In our study, drug annotations are collected from the SIDER and DrugBank databases. Terms describing individual side effects reported in SIDER are clustered with the IntelliGO semantic similarity measure into term clusters (TCs) [83]. Maximal frequent itemsets are extracted from the resulting $drug \times TC$ binary table, leading to the identification of what we call side-effect profiles (SEPs). A SEP is defined as the longest combination of TCs which are shared by a significant number of drugs. Frequent SEPs are explored on the basis of integrated drug and target descriptors using two machine learning methods: decision-trees and ILP. Learning efficiency is evaluated by cross-validation and direct testing with new molecules. Comparison of the two methods shows that the ILP displays a greater sensitivity than decision trees. Although both methods yield explicit models, ILP is able to exploit not only drug properties but also background knowledge, thereby producing rich and expressive rules.

6.2.2. Functional classification of genes

The IntelliGO measure computes semantic similarity between genes in taking into account domain knowledge in Gene Ontology (GO) [83]. IntelliGO is used for functional clustering of a set of genes, i.e. based on functional annotations of these genes. For example, a gene set of interest may include genes showing the same expression profile.

A functional clustering method based on IntelliGO was tested on four benchmarking datasets consisting of biological pathways (KEGG database) and functional domains (Pfam database) [90]. A follow-up of this study was motivated by the fact that the IntelliGO measure, like most of the biological similarity measures, does not verify "triangle inequality" and thus is not a mathematical distance. Interestingly, specific spectral clustering techniques can be used for improving the clustering of the objects for which exists a pairwise (dis-)similarity matrix [115], [125]. Spectral clustering techniques make use of the eigenvalues of this (dis-)similarity matrix to perform dimension reduction before clustering in fewer dimensions. We have conducted a comparative and large-scale gene clustering evaluation using the IntelliGO measure and reference sets. Our results showed an improvement of the clustering quality with "constant-shift spectral clustering" [63].

6.2.3. Analysis of biomedical data annotated with ontologies

Annotating data with concepts of an ontology is a common practice in the biomedical domain. Resulting annotations define links between data and ontologies that are key for data exchange, data integration and data analysis. Since 2011, we collaborate with the National Center for Biomedical Ontologies (NCBO) to develop a large repository of annotations named the NCBO Resource Index [98]. This repository contains annotations of 36 biomedical databases annotated with concepts of more than 200 ontologies of the BioPortal [3]. In 2012, we compared the annotations of a database of biomedical publications (Medline) with two databases of scientific funding (Crisp and ResearchCrossroads) to profile disease research [105]. One main challenge remains to develop a knowledge discovery approach able to mine correlations between annotations based on BioPortal ontologies, i.e. is it possible to discover interesting knowledge units within these annotations?

In 2013, we proposed an adaptation of FCA techniques, namely pattern structures, to explore the annotations of biomedical databases [2]. We considered documents of biomedical databases annotated with sets of ontological concepts as objects in a pattern structure. Corresponding annotations have been classified according to several dimensions, where a dimension is related to a particular aspect of domain knowledge. Then, the pattern structure formalism was applied to classify these annotations, allowing to discover correlations between annotations but also lacks of completion in the annotations that could be fixed afterward. This adaptation of pattern structures opens many perspectives in term of ontology reengineering and knowledge discovery.

In another context, a related work was carried out in the Kolflow project (see 8.2.1.4). We proposed an interactive environment based on Formal Concept Analysis which makes possible a simultaneous enrichment of semantic annotations of medical texts and of the ontology of medical domain [66], [59].

6.2.4. Analysis and interpretation of sequential patterns with Linked Open Data

---

[3]http://bioportal.bioontology.org/

Linked Data is a set of principles and technologies that rely on the architecture of the Web (URIs and links) to share, model and integrate data. The basic idea is that data objects (e.g., a surgical procedure) are identified by web addresses (URIs), and the information attached to these objects are represented through links to values or other URIs representing other objects.

Considering the potential development and availability of biomedical Linked Data, we investigated it as a source of additional information to support the interpretation of the results of a data mining process, such as sequential pattern discovery. We developed a system using several linked data endpoints to collect descriptive dimensions about the items that constitute sequential patterns. These dimensions are used to automatically classify with Formal Concept Analysis the extracted patterns, thus generating a structure that can support exploration and navigation into the results of the data mining step [55].

6.3. Structural Systems Biology

Participants: Marie-Dominique Devignes, Anisah Ghoorah, Van-Thai Hoang, Bernard Maigret, David Ritchie, Malika Smaïl-Tabbone.

Keywords: bioinformatics, chemistry, docking, knowledge discovery, screening, systems biology

Structural systems biology aims to describe and analyze the many components and interactions within living cells in terms of their three-dimensional (3D) molecular structures. We are currently developing advanced computing techniques for molecular shape representation, protein-protein docking, protein-ligand docking, high-throughput virtual drug screening, and knowledge discovery in databases dedicated to protein-protein interactions.

6.3.1. Accelerating protein docking calculations using graphics processors

We have recently adapted the *Hex* protein docking software [113] to use modern graphics processors (GPUs) to carry out the expensive FFT part of a docking calculation [114]. Compared to using a single conventional central processor (CPU), a high-end GPU gives a speed-up of 45 or more. This software is publicly available at http://hex.loria.fr. A public GPU-powered server has also been created (http://hexserver.loria.fr) [106]. The docking server has performed some 14,000 docking runs during 2013.

Our docking work has facilitated further developments on modeling the assembly of multi-component molecular structures using a particle swarm optimization technique [123], and on modeling protein flexibility during docking [122]. In 2013, in collaboration with the Nano-D team at Inria Grenoble, we developed a new docking algorithm called "DockTrina" [31], which can rapidly model trimers of protein structures by combining multiple pair-wise docking results from *Hex*. We also used *Hex* successfully to model a challenging protein complex containing water molecules at the protein-protein interface [29].

6.3.2. KBDOCK: Protein docking using Knowledge-Based approaches

In order to explore the possibilities of using structural knowledge of protein-protein interactions, Anisah Ghoorah recently developed the KBDOCK system as part of her doctoral thesis project [95]. KBDOCK is available at http://kbdock.loria.fr. KBDOCK combines coordinate data from the Protein Data Bank [87] with the Pfam protein domain family classification [91] in order to describe and analyze all known protein-protein interactions for which the 3D structures are available. We have demonstrated the utility of KBDOCK [94] for template-based docking using 73 complexes from the Protein Docking Benchmark [97]. We recently presented results obtained using KBDOCK at the CAPRI conference on protein docking in Utrecht [21]. In 2013, we updated KBDOCK with the latest data from Pfam and the Protein Data Bank. An article describing the new version of KBDOCK was accepted by the Database Issue of Nucleic Acids Research [6].

6.3.3. Kpax: A new algorithm for protein structure alignment

We have developed a new protein structure alignment approach called Kpax [112]. The approach exploits the fact that each amino acid residue has a carbon atom with a highly predictable tetrahedral geometry. This allows the local environment of each residue to be transformed into a canonical orientation, thus allowing easy comparison between the canonical orientations of residues within pairs of proteins using a novel scoring function based on Gaussian overlaps. The overall approach is two or three orders of magnitude faster than most contemporary protein structure alignment algorithms, while still being almost as accurate as the state-of-the-art TM-Align approach [124]. The Kpax program is available at http://kpax.loria.fr/. The Kpax program is now used heavily behind the scenes in the new KBDOCK web server [6] to find structural templates for docking which might be beyond the reach of sequence-based homology modeling approaches.

6.3.4. gEMpicker and gEMfitter: GPU-accelerated tools for cryo-electron microscopy

Solving the structures of large protein assemblies is a difficult and computationally intensive task. Multiple two-dimensional (2D) images must be processed and classified to identify protein particles in different orientations. These images may then be averaged and stacked to deduce the three-dimensional (3D) structure of a protein. In order to help accelerate the first of these tasks we have recently developed a novel and highly parallel algorithm called "gEMpicker" which uses multiple graphics processors to detecting 2D particles in cryo-electron microscopy images [112]. We have also developed a 3D shape matching algorithm called "gEMfitter" which also exploits graphics processors, and which will provide a useful tool for the final 3D assembly step [112]. Both programs have been made publicly available at http://gem.loria.fr/.

6.3.5. DOVSA: Developing new algorithms for virtual screening

In 2010, Violeta Pérez-Nueno joined the Orpailleur team thanks to a Marie Curie Intra-European Fellowship (IEF) award to develop new virtual screening algorithms (DOVSA). The aim of this project was to advance the state of the art in computational virtual drug screening by developing a novel consensus shape clustering approach based on spherical harmonic (SH) shape representations [110]. As a continuation of this project, and in collaboration with colleagues from the University of Bari in Italy, we recently published a review on drug discovery relating to the GPCR receptor proteins [15]. We also published a book chapter describing the ParaFit program for fast spherical harmonic shape matching [70].

6.4. Around the Taaable research project

Participants: Valmi Dufour-Lussier, Emmanuelle Gaillard, Laura Infante Blanco, Florence Le Ber, Jean Lieber, Amedeo Napoli, Emmanuel Nauer.

> **Keywords:** knowledge representation, description logics, classification-based reasoning, case-based reasoning, belief revision, semantic web

The Taaable project [69] (http://taaable.fr) has been originally created as a challenger of the Computer Cooking Contest (ICCBR Conference). A candidate to this contest is a system whose goal is to solve cooking problems on the basis of a recipe book (common to all candidates), where each recipe is a shallow XML document with an important plain text part. The size of the recipe book (about 1500 recipes) prevents from a manual indexing of recipes: this indexing is performed using semi-automatic techniques.

Beyond its participation to the CCCs, the Taaable project aims at federating various research themes: case-based reasoning (CBR), information retrieval, knowledge acquisition and extraction, knowledge representation, minimal change theory, ontology engineering, semantic wikis, text-mining, etc. CBR is used to perform adaptation of recipe to user constraints. The reasoning process uses a cooking domain ontology (especially hierarchies of classes) and adaptation rules. The knowledge base used by the inference engine is encoded within a semantic wiki, which contains the recipes, the domain ontology, and adaptation rules.

Minimal change theory and belief revision can be used as tools to support adaptation in CBR, i.e. the source case is modified to be consistent with the target problem using a revision operator. Belief revision was applied to Taaable for the adaptation of recipe preparations [3], using one of the engines included in the library Revisor (cf. § 5.4.5).

As acquiring knowledge from experts is costly, a new approach was proposed to allow a CBR system to use partially reliable, non expert, knowledge from the Web for reasoning [68] [5]. This approach is based on a meta-knowledge model to manage knowledge reliability. This model represents notions such as belief, trust, reputation and quality, as well as their relationships and rules to evaluate knowledge reliability. The reliability estimation is used to filter knowledge with high reliability as well as to rank the results produced by the CBR system, ensuring the quality of results.

6.5. Some results in graph theory

Participants: Amedeo Napoli, Chedy Raïssi, Jean-Sébastien Sereni, Mario Valencia.

Keywords: graph theory, extremal graph theory, coloring, clustering

6.5.1. *Structural and extremal graph theory*

Regarding graph coloring, a conjecture of Gera, Okamoto, Rasmussen and Zhang on set coloring was solved. A *set coloring* of a graph $G = (V, E)$ is a function $c : V \to \{1, ..., k\}$ such that whenever u and v are adjacent vertices, it holds that $\{c(x) : x \text{ neighbor of } u\} \neq \{c(x) : x \text{ neighbor of } v\}$. In other words, there must be at least one neighbor of u that has a color not assigned to a neighbor of v, or *vice-versa*. The smallest k such that G admits a set coloring is the *set coloring number* $\chi_s(G)$. We confirmed the conjecture by proving that $\chi_s(G) \geq \lceil \log_2 \chi(G) \rceil + 1$, where $\chi(G)$ is the (usual) chromatic number of G. This bound is tight.

Works have been started on a 12-year-old conjecture by Heckman and Thomas about the fractional chromatic number of graphs with no triangles and maximum degree at most 3. This conjecture is actually a natural generalization of a fact established by Staton in 1979. Heckman and Thomas posits that in every graph with no triangles, maximum degree at most 3 and arbitrary weights on the vertices, there exists an independent set of weight at least $5/14$ times the total weight of the graph.

Regarding extremal graph theory, two results have been obtained. The first one deals with permutation snarks, while the second one reads as follows.
For every 3-coloring of the edges of the complete graph on n vertices, there is a color c and a set X of 4-vertices such that at least $2n/3$ vertices are linked to a vertex in X by an edge of color c.
This theorem is motivated by a conjecture of Erdős, Faudree, Gould, Gyárfás, Rousseau and Schelp from 1989, which asserts that X can be of size 3 only. However, they were only able to prove that X can be of size 22. Recently, Rahil Baber and John Talbot managed to build upon our work in a very nice article: adding a new idea to our argument, they managed to confirm the conjecture.

6.5.2. *Graph theory and other fields*

Interactions of graph theory with other topics (theoretical computer science, number theory, group theory, sociology and chemistry) have been considered. Most of them are still in progress and some are published. For instance, regarding distributed computing, the purpose of our work was to question the global knowledge each node is assumed to start with in many distributed algorithms (both deterministic and randomized). More precisely, numerous sophisticated local algorithm were suggested in the literature for various fundamental problems. Noticeable examples are the MIS algorithms and the $(\Delta + 1)$-coloring algorithms. Unfortunately, most known local algorithms are *non-uniform*, that is, they assume that all nodes know good estimations of one or more global parameters of the network, e.g., the number of nodes n. Our work provides a rather general method for transforming a non-uniform local algorithm into a uniform one. Furthermore, the resulting algorithm enjoys the same asymptotic running time as the original non-uniform algorithm. Our method applies to a wide family of both deterministic and randomized algorithms. Specifically, it applies to almost all of the state of the art non-uniform algorithms regarding MIS and Maximal Matching, as well as to many results concerning the coloring problem.

6.5.3. *Other aspects on graph coloring and clustering*

Since September 2013, Mario Valencia has obtained a one year invitation (namely Inria "Délégation") for working at Inria Nancy – Grand Est, in the Orpailleur team, on graph theoretical aspects and data clustering. This research work consists in studying the modular decomposition techniques on the threshold graphs issues of the clustering process. More precisely, this study relies on families of graphs having a "good" decomposition as cographs and chordal graphs, and then, and on the analysis of the adaptation of these two families of graphs within a clustering activity.

Other research dimensions are dealing with algorithmic aspects of some variations of the classical graph coloring problem.

- Packing colorings of graphs where we need to color the vertices of a graph in such a way that vertices having a same color c should be at a distance at least equal to $c + 1$ in the graph. With P. Torres, a postdoc student, we have obtained some upper bounds for the packing chromatic number of hypercubes graphs of dimension n, denoted by Q_n, and we have computed exactly this parameter for this family of graph for $n = 6, 7, 8$, extending previous results known for $n = 2, 3, 4, 5$ [35].

- (k, i)-coloring of graphs, which is a generalization of a k-tuple coloring of graphs: given positive integers k and i, we want to affect to each vertex a k-set of colors such that the intersection of the k-sets affected to adjacent vertices has cardinality at most equal to i. With F. Bonomo, I. Koch, and G. Duran, we have found a linear time algorithm for this problem on cycles and cacti graphs. Moreover, we have obtained an interesting equivalence between this problem on complete graphs and a problem on weighted binary codes.

- b-coloring of graphs, where we need to color the vertices of a graph in such a way that in each color class j there exists at least one vertex x_j adjacent to at least one vertex in all the other color classes. The goal of this problem is to maximize the number of colors under such a constraint (i.e. the b-chromatic number of a graph). With F. Bonomo, O. Schaudt and M. Stein, we have shown that b-coloring is NP-hard on co-bipartite graphs and polytime solvable on tree-cographs [77].

PAROLE Project-Team

6. New Results

6.1. Speech analysis and synthesis

Participants: Anne Bonneau, Vincent Colotte, Dominique Fohr, Yves Laprie, Joseph Di Martino, Slim Ouni, Agnès Piquard-Kipffer, Emmanuel Vincent, Utpala Musti.

Signal processing, phonetics, health, perception, articulatory models, speech production, learning language, hearing help, speech analysis, acoustic cues, speech synthesis

6.1.1. *Acoustic-to-articulatory inversion*

The acoustic-to-articulatory inversion from cepstral data has been evaluated on the X-ray database, i.e. X-ray films recorded with the original speech signal. A codebook is used to represent the forward articulatory to acoustic mapping and we designed a loose matching algorithm using spectral peaks to access it. This algorithm, based on dynamic programming, allows some peaks in either synthetic spectra (stored in the codebook) or natural spectra (to be inverted) to be omitted. Quadratic programming is used to improve the acoustic proximity near each good candidate found during codebook exploration. The inversion [40], [10] has been tested on speech signals corresponding to the X-ray films. It achieves a very good geometric precision of 1.5 mm over the whole tongue shape unlike similar works which limit the error evaluation at 3 or 4 points corresponding to sensors located at the front of the tongue.

6.1.1.1. Construction of articulatory models

Articulatory models are intended to approximate the vocal tract geometry with a small number of parameters controlling linear deformation modes. Most of the models have been designed on images of vowels and thus offer a good coverage for vowels but are unable to provide a good approximation for consonants, especially in the region of the constriction. The first problem is related to the nature of contours used to derive linear components. When dealing with vowels there is no contact between the tongue and other fixed articulators (palate, teeth). Factor analysis used to determine linear modes of deformation of the tongue only takes into account the influence of the tongue muscles. This is no longer the case with consonants, since a contact is realized between the tongue and the palate, alveolar ridge or teeth for stops /k, g, t, d/ and the sonorant /l/ in French. The deformation factors thus incorporate the "clipping" effect of the palate. Following the idea of using virtual articulatory targets that lie beyond the positions that can be reached, here the palate, we edited delineated tongue contours presenting a contact with the palate. We chose a conservative solution which consists of keeping the tongue contour up to the contact point and extending it while guaranteeing a "natural shape". These new contours do not cross the palate for more than 10 mm. As such, this modification alone is not sufficient, because the number of images corresponding to consonants is small even if the corpus used in this work is phonetically balanced. We thus duplicated a number of consonant X-ray images in order to increase the weight of deformation factors corresponding to the tongue tip which is essential for some consonants, /l/ for instance. This approach provides a very good fitting with original tongue contours, i.e. 0.83 mm in average with 6 components over the whole tongue contour and only 0.56 mm in the region of the main place of articulation, which is important with a view of synthesizing speech.

6.1.1.2. Articulatory copy synthesis

Acoustic features and articulatory gestures have always been studied separately. Articulatory synthesis could offer a nice solution to study both domains simultaneously provided that relevant information can be fed into the acoustic simulation. The first step consisted of connecting the 2D geometry given by mediosagittal images of the vocal tract with the acoustic simulation. Last year we thus developed an algorithm to compute the centerline of the vocal tract, i.e. a line which is approximately perpendicular to the wave front. The centerline is then used to segment the vocal tract into elementary tubes whose acoustic equivalents are fed into the acoustic simulation. A new version of the centerline algorithm [53] has been developed in order to approximate the propagation of a plane wave more correctly.

The work on the development of time patterns used to pilot the acoustic simulation has been continued by improving the choice of relevant X-ray images and the temporal transitions from one image to the following. This procedure has been applied successfully to copy sentences and VCV for four X-ray films of the DOCVACIM database[52]. More difficult transitions, i.e. those corresponding to consonant clusters, will be investigated this year.

In addition to the control of the acoustic simulation we started an informal cooperation with the IADI laboratory www.iadi-nancy.fr in order to record better static images of the vocal tract, and cineMRI, i.e. films, for a number of sentences.

6.1.2. *Using articulography for speech animation*

We are continuously working on the acquisition and analysis of the articulatory data using electromagnetic articulography (EMA).This year, we have conducted research to use EMA as motion capture data and we showed that it is possible to use it for audiovisual speech animation. In fact, as EMA captures the position and orientation of a number of markers, attached to the articulators, during speech, it performs the same function for speech that conventional motion capture does for full-body movements acquired with optical modalities, a long-time staple technique of the animation industry. We have processed EMA data from a motion-capture perspective and applied to the visualization of an existing multimodal corpus of articulatory data, creating a kinematic 3D model of the tongue and teeth by adapting a conventional motion capture based animation paradigm. Such an animated model can then be easily integrated into multimedia applications as a digital asset, allowing the analysis of speech production in an intuitive and accessible manner. In this work [61], we have addressed the processing of the EMA data, its co-registration with 3D data from vocal tract magnetic resonance imaging (MRI) and dental scans, and the modeling workflow. We will continue our effort in the future to improve this technique.

6.1.3. *Acoustic analyses of non-native speech*

Within the framework of the project IFCASL, we designed a corpus for the study of French and German, with both languages pronounced by French and German speakers, so as to put into light L1/L2 interferences. The corpus was constructed to control for several segmental and suprasegmental phenomena. German and French, for instance, show different kinds of voicing patterns. Whereas in French, the voicing opposition of stops is realized as voiced versus unvoiced, in German, the same difference is realized mostly as unaspirated versus aspirated. Furthermore, differences between the two language groups are expected with respect to the production of nasal vowels (absent in German), the realization of /h/ (not present in French, but in German). On the suprasegmental level, word stress and focus intonation are central to our investigation. Speakers produce both native and non-native speech, which allows for a parallel investigation of both languages.

We have conducted a pilot study on the realization of obstruents in word-final position -a typical example of L1-L2 interference on the segmental level-, which are subject to devoicing in German, but not in French. First results showed that German learners (beginners) had difficulties to voice French obstruents in this context, and, when listening to French realizations, tend to add a final schwa to achieve the expected realization.

6.1.4. *Speech synthesis*

We recall that within the framework of the ViSAC project we have developed bimodal acoustic-visual synthesis technique that concurrently generates the acoustic speech signal and a 3D animation of the speaker's outer face. This is done by concatenating bimodal diphone units that consist of both acoustic and visual information. In the visual domain, we mainly focus on the dynamics of the face rather than on rendering. The proposed technique overcomes the problems of asynchrony and incoherence inherent in classic approaches to audiovisual synthesis. The different synthesis steps are similar to typical concatenative speech synthesis but are generalized to the acoustic-visual domain. This year we have performed an extensive evaluation of the synthesis system using perceptual and subjective evaluations. The overall outcome of the evaluation indicates that the proposed bimodal acoustic-visual synthesis technique provides intelligible speech in both acoustic and visual channels [22]. For testing purposes we have also added a simple tongue model that is controlled by the generated phonemes. The purpose is to improve the quality of the audiovisual speech intelligibility.

Morover, we perform feature selection and weight tuning for a given unit-selection corpus to make the ranking given by the target cost function consistent with the ordering given by an objective dissimilarity measure. To find an objective metric highly correlated to perception we analyzed correlation between objective and subjective evaluation results. It shows interesting patterns which might help in designing better tuning metrics and objective evaluation techniques [55].

6.1.5. Phonemic discrimination evaluation in language acquisition and in dyslexia and dysphasia

We keep working on a project concerning identification of early predictors of reading, reading acquisition and language difficulties, more precisely in the field of specific developmental disabilities : dyslexia and dysphasia. A fair proportion of those children show a weakness in phonological skills, particularly in phonemic discrimination. However, the precise nature and the origin of the phonological deficits remain unspecified. In the field of dyslexia and normal acquisition of reading, our first goal was to contribute to identify early indicators of the future reading level of children. We based our work on the longitudinal study - with 85 French children - of [90], [91] which indicates that phonemic discrimination at the beginning of kindergarten is strongly linked to success and specific failure in reading acquisition. We study now the link between oral discrimination both with oral comprehension and written comprehension. Our analyses are based on the follow up of a hundred children for 4 years from kindergarten to end of grade 2 (from age 4 to age 8) [98].

6.1.6. Enhancement of esophageal voice

6.1.6.1. Pitch detection

Over the last two years, we have proposed two new real time pitch detection algorithms (PDAs) based on the circular autocorrelation of the glottal excitation, weighted by temporal functions, derived from the CATE [85] original algorithm (Circular Autocorrelation of the Temporal Excitation), proposed initially by J. Di Martino and Y. Laprie. In fact, this latter algorithm is not constructively real time because it uses a post-processing technique for the Voiced/Unvoiced (V/UV) decision. The first algorithm we developed is the eCATE algorithm (enhanced CATE) that uses a simple V/UV decision less robust than the one proposed later in the eCATE+ algorithm. We propose a recent modified version called the eCATE++ algorithm which focuses especially on the detection of the F0, the tracking of the pitch and the voicing decision in real time. The objective of the eCATE++ algorithm consists in providing low classification errors in order to obtain a perfect alignment with the pitch contours extracted from the Bagshaw or Keele databases by using robust voicing decision techniques. This algorithm has been published in Signal, Image and Video Processing, [14].

6.1.6.2. Real-time pitch detection for application to pathological voices

The work first rested on the CATE algorithm developed by Joseph Di Martino and Yves Laprie, in Nancy, 1999.The CATE (Circular Autocorrelation of the Temporal Excitation) algorithm is based on the computation of the autocorrelation of the temporal excitation signal which is extracted from the speech log-spectrum. We tested the performance of the parameters using Bagshaw database, which is constituted of fifty sentences, pronounced by a male and a female speaker. The reference signal is recorded simultaneously with a microphone and a laryngograph in an acoustically isolated room. These data are used for the calculation of the contour of the pitch reference. When the new optimal parameters from the CATE algorithm were calculated, we carried out statistical tests with the C functions provided by Paul BAGSHAW. The results obtained were very satisfactory and a first publication relative to this work was accepted and presented at the ISIVC 2010 conference [79]. At the same time, we improved the voiced / unvoiced decision by using a clever majority vote algorithm electing the actual F0 index candidate. Recently Fadoua Bahja developed a new algorithm based on wavelet transforms applied to the cepstrum excitation. The preliminary results obtained were satisfactory and a complete description of this latter study is under a submission process in an international journal.

6.1.6.3. Voice conversion techniques applied to pathological voice repair

Voice conversion is a technique that modifies a source speaker's speech to be perceived as if a target speaker had spoken it. One of the most commonly used techniques is the conversion by GMM (Gaussian Mixture Model). This model, proposed by Stylianou, allows for efficient statistical modeling of the acoustic space of a

speaker. Let "x" be a sequence of vectors characterizing a spectral sentence pronounced by the source speaker and "y" be a sequence of vectors describing the same sentence pronounced by the target speaker. The goal is to estimate a function F that can transform each source vector as nearest as possible of the corresponding target vector. In the literature, two methods using GMM models have been developed: In the first method (stylianou,98), the GMM parameters are determined by minimizing a mean squared distance between the transformed vectors and target vectors. In the second method (kain,98), source and target vectors are combined in a single vector "z". Then, the joint distribution parameters of source and target speakers is estimated using the EM optimization technique. Contrary to these two well known techniques, the transform function F, in our laboratory, is statistically computed directly from the data: no needs of EM or LSM techniques are necessary. On the other hand, F is refined by an iterative process. The consequence of this strategy is that the estimation of F is robust and is obtained in a reasonable lapse of time. Recently, we realized that one of the most important problems in speech conversion is the prediction of the excitation. In order to solve this problem we developed a new strategy based on the prediction of the cepstrum excitation pulses. Another very important problem in voice conversion concerns the prediction of the phase spectra. This study is under progress in the framework of an Inria ADT which began in September 2013.

6.1.6.4. Signal reconstruction from short-time Fourier transform magnitude spectra

Joseph Di Martino and Laurent Pierron developed in 2010 an algorithm for real-time signal reconstruction from short-time Fourier magnitude spectra [86]. Such an algorithm has been designed in order to enable voice conversion techniques we are developing in Nancy for pathological voice repair. Recently Mouhcine Chami, an assistant-professor of the INPT institute at Rabat (Morocco) proposed a hardware implementation of this algorithm using FPGAs. This implementation has been published in the SIIE 2012 conference [81]. Maryem Immassi, a PhD student of Mouhcine Chami, is comparing this algorithm with the state of the art RTISI-LA algorithm in the framework of a hardware implementation.

6.1.7. Audio source separation

Audio source separation is the task of extracting one or more target source signals from a given mixture signal. It is an inverse problem, which requires the user to guide the separation process using prior models for the source signals and the mixing filters or for the source spectra and their spatial covariance matrices. We studied the impact of sparsity penalties over the mixing filters [38] and we defined probabilistic priors [20] and deterministic subspace constraints [45] over the spatial covariance matrices. We also wrote a review paper about guided audio source separation for *IEEE Signal Processing Magazine* [28].

This paper highlighted that many guided separation techniques now exist that are closer than ever to successful industrial applications, as exemplified by the ongoing industrial collaborations of the team. In order to exploit our know-how for these real-world applications, we investigated issues such as the impact of audio coding [59], artifact reduction [21], real-time implementation [62], and latency [70]. Two patents have been filed [77], [76]. We also started a new research track on the fusion of multiple source separation techniques [46].

Finally, we pursued our long-lasting efforts on the evaluation of audio source separation by collecting the first-ever publicly available dataset of multichannel real-world noise recordings [71] and by conducting an experimental comparison of the two main families of techniques used for source separation [63].

6.2. Automatic speech recognition

Participants: Dominique Fohr, Jean-Paul Haton, Irina Illina, Denis Jouvet, Odile Mella, Emmanuel Vincent, Arseniy Gorin, Luiza Orosanu, Dung Tran.

stochastic models, acoustic models, language models, automatic speech recognition, speech transcription, training, robustness

6.2.1. Detailed acoustic modeling

Acoustic models aim at representing the acoustic features that are observed for the sounds of the language, as well as for non-speech events (silence, noise, ...). Currently context-dependent hidden Markov models (CD-HMM) constitute the state of the art for speech recognition. However, for text-speech alignment, simpler context-independent models are used as they provide better performance.

The use of larger speech training corpora allows us increasing the size of the acoustic models (more parameters through more Gaussians components per density, and more shared densities) and this leads to improved performance. However, in such approaches, Gaussian components are estimated independently for each density. Thus, after having investigated last year the usage of multiple modeling approaches for better constraining the acoustic decoding space, recent studies have focused on enriching the acoustic models themselves in view of handling trajectory and speaker consistency in decoding.

This year a new modeling approach was developed that takes benefit of the multiple modeling ideas and involves a sharing of parameters. The idea is to use the multiple modeling approach to partition the acoustic space according to classes (manual classes or automatic classification). Then, for each density, some Gaussian components are estimated on the data of each class. These class-based Gaussian components are then pooled to provide the set of Gaussian components of the density. Finally class dependent mixture weights are estimated for each density. The method allows us to better parameterize GMM-HMM without increasing significantly the number of model parameters. The experiments on French radio broadcast news data demonstrate the improvement of the accuracy with such parameterization compared to the models with similar, or even larger number of parameters [43].

Current experiments deal with stranded HMM. The objective of such an approach is to introduce in the GMM-HMM modeling some extra parameters to take into account the transition between the Gaussian components when moving from one frame to the next.

6.2.2. *Noise-robust speech recognition*

In many real-world conditions, the speech signal is overlapped with noise, including environmental sounds, music, or undesired extra speech. Source separation may then be used as a pre-processing stage to enhance the desired speech signal [64]. In practice, the enhanced signal always includes some distortions compared to the original clean signal. It is important to quantify which parts of the enhanced signal are reliable in order not to propagate these distortions to the subsequent feature extraction and decoding stages. A number of heuristic statistical uncertainty estimators and propagators have been proposed to this aim. We started some work aiming to improve the accuracy of these estimators and propagators. We also showed how to exploit uncertainty in order to train unbiased acoustic models directly from noisy data [24].

In order to motivate further work by the community, we created a new international evaluation campaign on that topic in 2011: the CHiME Speech Separation and Recognition Challenge. This challenge aims to recognize small or medium-vocabulary speech mixed with noise recorded in a real family home over the course of several weeks. We analyzed the outcomes of the first edition [16] which led to a special issue of *Computer Speech and Language* [15] and we organized a second edition in 2013 [66] which illustrated the progress made in two years over small-vocabulary speech and the remaining challenges towards robust recognition of medium-vocabulary speech [65].

6.2.3. *Linguistic modeling*

Usually the lexicon used by a speech recognition system refers to word entries, where each entry in the pronunciation lexicon specifies a possible pronunciation of a word, and the associated language model specifies the probability of a word knowing preceding words. However, whatever the size of the lexicon is, the size is always finite, and the speech recognition system cannot recognize properly words that are not present in the lexicon. In such cases, the unknown word is typically replaced by a sequence of short words which is acoustically similar to the unknown speech portion.

6.2.3.1. *Random indexing*

This year we studied the introduction of semantic information through the Random Indexing paradigm (RI) in statistical language models used in speech recognition. Random Indexing is a scalable alternative to LSA (Latent Semantic Analysis) for analyzing relationships between a set of documents and the terms they contain. We determined the best methods and parameters by minimizing the perplexity of a realistic corpus of 290000 words. We investigated 4 methods for training RI matrices, 4 weighting functions, several matrix sizes and how balancing the 4-gram and RI language model. We only obtained a relative gain of 3% [42].

6.2.3.2. Continuous language models

Language modeling plays an important role in automatic speech recognition because it constrains the decoder to search the most likely sequences of words according to a given language and a given task. A limitation of N-grams models is that they represent the words in a discrete space. It would be interesting to represent words in a continuous space where semantically close words would be projected in the same region of space. This projection can be achieved by recurrent neural networks. Moreover they are able to learn long-term dependencies with the recurrent layer that can store a record of the past. During his master internship, Othman Zennaki integrated this new language model in our speech recognition system ANTS.

6.2.3.3. Linguistic units for embedded systems

In the framework of the RAPSODIE project, speech recognition is to be used to help communication with hard of hearing people. Because of requirements on memory and CPU (almost real time processing), various modeling approaches have been investigated with respect to linguistic units. The first approach has focused on analyzing the achieved phonetic decoding performance of various linguistic units (phonemes, syllables, words). Best phonetic decoding performance is achieved using word units and associated tri-gram language model, but at the expense of large CPU and memory requirements. Using directly phoneme units leads to the smallest models and requires little CPU, however, this also leads to the worst performance. The proposed approach relying on syllable units provides results which are rather close to the word based approach, but requires much less CPU [58], [57].

Further experiments are now focusing on combining word and syllable units, in view of having frequent words covered by the word units, and using syllables for decoding unknown words.

6.2.3.4. OOV proper name retrieval

Proper name recognition is a challenging task in information retrieval in large audio/video databases. Proper names are semantically rich and are usually key to understanding the information contained in a document.

In the framework of the ContNomina project, we focus on increasing the vocabulary coverage of a speech transcription system by automatically retrieving proper names from contemporary diachronic text documents. We proposed methods that dynamically augment the automatic speech recognition system vocabulary, using lexical and temporal features in diachronic documents. We also studied different metrics for proper name selection in order to limit the vocabulary augmentation and therefore the impact on the ASR performances. Recognition results show a significant reduction of the word error rate using augmented vocabulary [56].

6.2.4. Speech transcription

The first complete version of the speech transcription system ANTS (see section 5.5) has been initially developed in the framework of the Technolangue project ESTER, and since then, the system has been regularly enriched through the integration of research results. The latest version can handle either HTK-based acoustic models through the Julius decoder, or Sphinx-based acoustic models with the CMU Sphinx decoders. In the last version, a Perl script encapsulates all the calls to the various tools used for diarization, model adaptation and speech recognition, and takes benefit of the multiple CPU available on the computer for parallelizing the different tasks as much as possible.

6.2.4.1. Combining recognizers

Last year in the context of the ETAPE speech transcription evaluation campaign, the Sphinx-based and Julius-based decoders have been further improved, and it was observed that combining the recognition outputs of several Sphinx-based and Julius-based decoder lead to a significant word error rate reduction compared to the best individual system.

More controlled experiments have then been performed to understand what was the main reason of the large performance improvement observed when combining Julius-based and Sphinx-based transcription system results. The Sphinx decoder processes the speech data in a forward pass, whereas the Julius decoder ends its decoding process by a backward pass. The Sphinx training and decoding scripts have been modified to process the speech material in a reverse time order; and various systems were developed by using different

sets of acoustic features and different sets of acoustic units. It was then observed that combining several Sphinx-forward and several Sphinx-reverse decoders lead to much better results than combining the same amount of only Sphinx-forward decoders or only Sphinx-reverse decoders; and the achieved word error rate was consistent with the one obtained by combining the Sphinx-based (forward) and Julius-based (backward) decoders [49]. Hence, the improvement is mainly due to the fact that forward-based and backward-based processing are combined. Because heuristics are applied during decoding to limit the acoustic space that is explored, some hypotheses might be wrongly pruned when processing the data one way, and may be kept in the active beam search when processing the other way. This is corroborated by the analysis of the word graph which show a large dissimilarity in the distribution of the number of words starting and ending in each frame [48].

Experiments have also shown that when the forward and backward decoders yield the same word hypothesis, this word is likely to be a correct answer. Recent experiments are investigating how far such behavior could help for unsupervised learning of acoustic models.

6.2.4.2. Spontaneous speech

During his master intership, Bruno Andriamiarina focuses on the new challenges brought by this spontaneity of the speech, making it difficult to be transcribed by the existing automatic speech recognition systems. He studied how to improve global performance of automatic speech recognition systems when dealing with spontaneous speech by adapting language model and pronunciation dictionary to this particular type of speech. He also studied the detection of disfluent speech portions (produced by spontaneous speech) in speech signal using a Gaussian Mixture Model (GMM)-based classifier trained on prosodic features covering the main prosodic characteristics (duration, fundamental frequency and energy).

6.2.4.3. Towards a structured output

The automatic detection of the prosodic structure of speech utterances has been investigated. The algorithm relies on a hierarchical representation of the prosodic organization of the speech utterances, and detects prosodic boundaries whether they are followed or not by pause. The detection of the prosodic boundaries and of the prosodic structures is based on an approach that integrates little linguistic knowledge and mainly uses the amplitude of the F0 slopes and the inversion of the F0 slopes as well as phone durations. The approach was applied on a corpus of radio French broadcast news and also on radio and TV shows which are more spontaneous speech data. The automatic prosodic segmentation results were then compared to a manual prosodic segmentation made by an expert phonetician [37].

Further work has focused on analyzing the links between manually set punctuation marks and this automatically detected prosodic structure, in view of using the prosodic structure for helping an automatic punctuation process.

6.2.5. Speech/text alignment

6.2.5.1. Alignment with non-native speech

Non-native speech alignment with text is one critical step in computer assisted foreign language learning. The alignment is necessary to analyze the learner's utterance, in view of providing some prosody feedback (as for example bad duration of some syllables - too short or too long -). However, non-native speech alignment with text is much more complicated than native speech alignment. This is due to the pronunciation deviations observed on non-native speech, as for example the replacement of some target language phonemes by phonemes of the mother tongue, as well as errors in the pronunciations.

In the case of French speakers learning English, we conducted a detailed analysis that has showed the benefit of taking into account non-native variants, and lead to determining the classes of phonemes whose temporal boundaries are the most accurate and which should be favored in the design of exercises for language learning[18].

In the framework of the IFCASL project, we proposed to use a two-step approach for automatic phone segmentation. The first step consists in determining the phone sequence that best explains the learner's utterance. This is achieved by force aligning the learner's speech utterance with a model representing the various possible pronunciation variants of the current sentence (both native and non-native variants need to be considered). In this step detailed acoustic Hidden Markov Models (HMMs) are used, with a rather large number of Gaussian components per mixture density. This kind of detailed acoustic models is the one that provides the best performance in automatic speech recognition. The second step consists in determining the phone boundaries. This is also achieved through a forced alignment process, but this time, the sequence of phones is known (as determined in the first step), and phone acoustic models with only a few Gaussians components per mixture density are used because it has been shown that they provide better temporal precision than detailed acoustic models. For the training of the models used for both forced alignment steps, the speech of native and non-native speakers could be used, either directly or by MLLR (Maximum Likelihood Linear Regression) adaptation.

6.2.5.2. Alignment with spontaneous speech

In the framework of the ANR ORFEO, we addressed the problem of the alignment of spontaneous speech. The ORFEO audio files were recorded under various conditions with a large SNR range and contain extra speech phenomena and overlapping speech. As regards overlapping speech, the orthographic transcription of the audio files only provides a rather imprecise time information of the overlapping speech segment. As a first approach, among the different orthographic transcripts corresponding to the overlapping area, we determined as the main transcript the one that best matches the audio signal, the others are kept in other tiers with the same time boundaries.

6.3. Machine translation and language modeling

Participants: Kamel Smaïli, David Langlois, Denis Jouvet, Emmanuel Vincent, Motaz Saad, Cyrine Nasri.

machine translation, statistical models

6.3.1. Language modeling

6.3.1.1. Vocabulary selection

In the framework of the ETAPE evaluation campaign a new machine learning based process was developed to select the most relevant lexicon to be used for the transcription of the speech data (radio and TV shows). The approach relies on a neural network trained to distinguish between words that are relevant for the task and those that are not. After training, the neural network (NN) is applied to each possible word (text tokens extracted from a very large text corpus). Then the words that have the largest NN output score are selected for creating the speech recognition lexicon. Such an approach can handle counts of occurrences of the words in various data subsets, as well as other complementary information, and thus offer more perspectives than the traditional unigram-based selection procedures [50].

6.3.1.2. Music language modeling

Similarly to speech, music involves several levels of information, from the acoustic signal up to cognitive quantities such as composer style or key, through mid-level quantities such as a musical score or a sequence of chords. The dependencies between mid-level and lower- or higher-level information can be represented through acoustic models and language models, respectively. We pursued our pioneering work on music language modeling, with a particular focus on log-linear interpolation of multiple conditional distributions. We applied it to the joint modeling of "horizontal" (sequential) and "vertical" (simultaneous) dependencies between notes for polyphonic pitch estimation [26] and to the joint modeling of melody, key and chords for automatic melody harmonization [25]. We also proposed a new Bayesian n-gram topic modeling and estimation technique, which we applied to genre-dependent modeling of chord sequences and to music genre classification [74].

6.3.2. *Quality estimation of machine translation*

In the scope of Confidence Measures, we participated to the World Machine Translation evaluation campaign for the second year (WMT2013 http://www.statmt.org/wmt13/quality-estimation-task.html). More precisely, we proposed a Quality Estimation system to the Quality Estimation shared task. The goal was to predict the quality of translations generated by an automatic system. Each translated sentence is given a score between 0 and 1. The score is obtained by using several numerical or boolean features calculated according to the source and target sentences. We performed a linear regression of the feature space against scores in the range [0 ;1], to this end, we use a Support Vector Machine with 66 features. In this new participation, we proposed to increase the size of the training corpus. For that, we decided to use the post-edited and reference corpora in the training step after assigning a score to each sentence of these corpora. Then, we tune these scores on a development corpus. This leads to an improvement of 10.5% on the development corpus, in terms of Mean Average Error (average difference between reference and predicted scores), but achieves only a slight improvement on the test corpus. This work has been published in [51].

6.3.3. *Comparable corpora and multilingual sentiment analysis*

In the PhD Thesis of Motaz Saad, we work on collecting comparable corpora. For that purpose we presented a method which extracts and aligns comparable corpora at the article level from Wikipedia encyclopedia based on interlanguage links. To evaluate the closeness of corpora we proposed several comparability measures. Our evaluations show that the proposed comparability measures are able to capture the comparability degree of any comparable corpora [60]. We go further on the comparability of multilingual corpora by studying their comparability in terms of sentiment. The final objective is to propose a multilingual press review concerning a given topic. This review should use several multilingual resources (electronic newspapers), and should class resources according to the including sentiments (fear, joy...about the subject), polarity (against or not to the subject)...This conducts to study opinions across different languages by comparing the underlying messages written by different people having different opinions. We propose "Sentiment based Comparability Measures" to compare opinions in multilingual comparable articles without translating source/target into the same language [27].

6.3.4. *Machine translation of arabic dialect*

The translation of Arabic dialect constitutes a real challenge since it is an under-resourced language. In fact, Modern Standard Arabic is as any other evoluated language, it means it could be processed by the available tools but unfortunately in Arabic countries people speak an Arabic language which is inspired from the standard one but is different. Our objective is then to propose a speech to speech system converting modern standard Arabic to Algerian dialect. After collecting corpus, we decided to propose a method allowing to diacritize dialects in order to be able in the following to develop an acoustic model. For that, we considered the issue of diacritization as a machine translation issue, and we have developed a statistical machine translation which learns to transform an undiacritized corpus into a diacritized one [44].

SÉMAGRAMME Project-Team

6. New Results

6.1. Syntax-Semantics Interface

6.1.1. TAG, Dependency Grammars, and ACG

Aleksandre Maskharashvili and Sylvain Pogodalla gave an ACG account of [41]'s process of transformation of the derivation trees of Tree Adjoining Grammar (TAG) into dependency trees. They made explicit how the requirement of keeping a direct interpretation of dependency trees into strings results into lexical ambiguity. Since the ACG framework has already been used to provide a logical semantics from TAG derivation trees, it results in a unified picture where derivation trees and dependency trees are related but independent equivalent ways to account for the same surface–meaning relation. This result has been published in [15].

6.1.2. Semantics of Neg-Raising Predicates in TAG

Laurence Danlos, Philippe de Groote, and Sylvain Pogodalla proposed a lexical semantic interpretation of Neg-Raising (NR) predicates that heavily relies on a Montague-like semantics for TAG and on higher-order types. NR verbs form a class of verbs with a clausal complement that show the following behavior: when a negation syntactically attaches to the ma- trix predicate, it can semantically attach to the embedded predicate, as the implication of (2) by (1) shows. This corresponds to the NR reading of this predicate.

- *Marie ne pense pas que Pierre partira.*
- *Marie pense que Pierre ne partira pas.*

As a base case, the approach lexically provides both NR and non-NR readings to NR predicates. The proposal is implemented in the ACG framework as it offers a fairly standard interface to logical formal semantics for TAG. This result has been published in [13].

6.1.3. Intensionalization

Makoto Kanazawa and Philippe de Groote have defined a general intensionalization procedure that turns an extensional semantics for a language into an intensionalized one that is capable of accommodating truly intensional lexical items without changing the compositional semantic rules [10]. They have proved some formal properties of this procedure and have clarified its relation to the procedure implicit in Montague's PTQ.

6.2. Lexical Disambiguation

Guy Perrier adapted the methods of lexical disambiguation presented in Mathieu Morey's PhD thesis [49] to the formalism of Tree Adjoining Grammar (TAG) in a common work with Claire Gardent, Yannick Parmentier and Sylvain Schmitz [24].

More precisely, the algorithm of lexical disambiguation for TAG uses the one-to-one relations between substitution nodes and roots of elementary tress in the parsing process and it takes also into account the position of the subsitution nodes with respect to the anchors in elementary trees, to discard lexical selections that do not respect some constraints. These constraints are implemented through a polarization of the elementary trees and for sake of efficiency, the lexical selections are represented in a compact way with automata.

A major default of the methods of lexical disambiguation presented in Mathieu Morey's PhD thesis is that they ignore local contexts. To overcome this default, Guy Perrier proposed an algorithm to foresee the elementary structures of the grammar that can be inserted between two words that will interact in the parsing process [20]. This algorithm applies to lexicalized grammars, in which the elementary structures are trees.

6.3. Linguistic Resources

6.3.1. *Large Scale Grammatical Resources*

Guy Perrier and Bruno Guillaume continued to develop FRIGRAM [2] a French grammar with a large coverage, written in the formalism of Interaction Grammars [16].

A major challenge in this task is to guarantee and to maintain the consistency of the grammar while aiming at the largest coverage. For this, they resorted an original property coming from the polarization of the elementary structures of an interaction grammar : the *companion property*. It is possible to determine all elementary structures (the *companions*) that are able to interact with a given elementary structure, in a static computation on the whole non anchored grammar, using the systeme of polarities. The knowledge of the companions of every elementary structure is very useful to check the linguistic consistency of a grammar.

Guy Perrier wrote a detailed documentation on FRIGRAM illustrated with a lot of examples [26].

6.3.2. *Deep Syntax Annotation of the Sequoia French Treebank*

Marie Candito, Guy Perrier, Bruno Guillaume, Corentin Ribeyre, Karën Fort, Djamé Seddah and Eric de la Clergerie started a project of annotating the Sequoia French Treebank with deep syntax dependencies.

The Sequoia French Treebank [33] is a 3 200 sentence treebank covering several domains (news, medical, europarl and fr-wikipedia). It is freely available and has already been annotated with surface dependency representations.

The participants in the project have defined a deep syntactic representation scheme for French, which abstracts away from surface syntactic variation and diathesis alternations. The goal is to obtain a freely available corpus, which will be useful for corpus linguistics studies and for training deep analyzers to prepare semantic analysis.

The different steps of the annotation process were conducted in a collaborative way. As the members of the project are located in two different French towns (Paris and Nancy), they decided to produce a complete annotation of the TreeBank in both towns and to collaboratively adjudicate the two results. In Nancy, Line Heckler, Mathilde Huguin and Alice Kneip produced a double annotation of the corpus and Guy Perrier was in charge of the adjudication.

At the beginning of the project, a mini reference was selected randomly, composed of 250 sentences from the Sequoia Corpus. Its annotation was conducted in parallel to the production of the annotation guide, in order to get feedback for the guide. Each team separately produced an initial annotated version of the mini reference. The final version, resulting from several iterations and adjudications, is already available [3].

The full version of the Sequoia French Treebank with deep syntax dependencies and its annotation guide will be released during Spring 2014.

6.3.3. *Agile Annotation*

In [19], Bruno Guillaume and Karën Fort present a methodology, inspired from the agile development paradigm, that helps preparing an annotation campaign. The idea behind the methodology is to formalize as much as possible the instructions given in the guidelines, in order to automatically check the consistency of the corpus being annotated with the guidelines, as they are being written. To formalize the guidelines, the authors use a graph rewriting tool, that allows to use a rich language to describe the instructions. This formalization allows to spot the rightfully annotated constructions and, by contrast, those that are not consistent with the guidelines. In case of inconsistency, an expert can either correct the annotation or update the guidelines and rerun the process.

---

[2]http://wikilligramme.loria.fr/doku.php?id=frigram:frigram
[3]http://talc2.loria.fr/mini_sequoia/

6.3.4. Integration of Multiple Constraints in ACG

In [14], Jiri Marsik and Maxime Amblard present a first step toward the integration of multiple constraints in ACG. However, all of the known treatments only consider tiny fragments of languages. We are interested in building a wide-coverage grammar which integrates and reconciles the existing formal treatments of discourse and allows us to study their interactions and to build discourse representations automatically.

This proposal is a first step towards a wide-coverage Abstract Categorial Grammar (ACG) that could be used to automatically build discourse-level representations. We focus on the challenge of integrating the treatment of disparate linguistic constraints in a single ACG and propose a generalization of the formalism: Graphical Abstract Categorial Grammars.

6.4. Graph Rewriting

Guillaume Bonfante and Bruno Guillaume studied formal properties of the Graph Rewriting in [12]. It is well-known that some linguistic phenomena do not cope properly with trees as the core mathematical structure to represent linguistic informations. In a former paper, the authors showed the benefit of encoding linguistic structures by graphs and of using graph rewriting rules to compute on those structures.

The Graph Rewriting formalism they consider is a formalization of the system which is implemented in the Grew software. Justified by some linguistic considerations, this Graph Rewriting formalization is characterized by two features: first, there is no node creation along computations and second, there are non-local edge modifications. Under these hypotheses, the article shows that uniform termination is undecidable and that non-uniform termination is decidable. Two termination techniques based on weights are described and a complexity bound on the derivation length for these rewriting systems is given.

6.5. Discourse in Pathological context

Maxime Amblard, Manuel Rebuschi and Michel Musiol continue to analyze in fine details pathological dialogues from the SLAM project. They present all theses results in [22] [21] and [11]. Schizophrenia is well-known among mental illnesses for the severity of the thought disorders it involves, and for their widespread and spectacular manifestations: from deviant social behavior to delusion, not to mention affective and sensitive distortions. The goal of our interdisciplinary work is to (i) analyze linguistic troubles in conversational contexts in which one of the speakers is schizophrenic, (ii) construe how the concept of rationality and logicality may apply to them, and (iii) propose a formal representation about this specific manifestation.