RESEARCH CENTER
Nancy - Grand Est

FIELD

Activity Report 2016

Section New Results

Edition: 2017-08-25

ALGORITHMICS, PROGRAMMING, SOFTWARE AND ARCHITECTURE

APPLIED MATHEMATICS, COMPUTATION AND SIMULATION

DIGITAL HEALTH, BIOLOGY AND EARTH

NETWORKS, SYSTEMS AND SERVICES, DISTRIBUTED COMPUTING

PERCEPTION, COGNITION AND INTERACTION

CAMUS Team

7. New Results

7.1. Formal Proofs about Happens-before in Explicitly Parallel Polyhedral Programs

Participants: Éric Violard, Alain Ketterlin.

Automatic parallelization has traditionally focused on sequential programs, but the widespread availability of explicitly parallel programming languages (such as OpenMP, Cilk, X10, and others) has led researchers to consider also the optimization and re-parallelization of parallel source programs. Most of these languages have constructions for parallel loops and parallel sections, with the accompanying synchronization primitives. The X10 language is especially interesting in this respect, because it provides simple and powerful constructions. Essentially, parallelism is expressed with the help of the `async` construct, whose body is to be executed in a parallel "activity", and the `finish` construct, which acts as a container for activities (and sub-activities) and waits for their completion. These constructions are complemented with "clocks", which are essentially synchronization barriers. Clocks can be used freely, in an unstructured manner, but are best associated with `finish` constructs, where they provide an intuitive and flexible phasing mechanism. In this case, activities spawned with `async` can either inherit or hide the clock provided by the nearest enclosing `finish`.

We are focusing on polyhedral programs, where all control is based on loops whose bounds are affine combinations of the enclosing loop counters and constant parameters. There is a large body of work on optimizing and parallelizing such programs, but most of them focus on sequential loop nests. Introducing X10's parallel constructions defines the class of *explicitly parallel polyhedral programs*, which is the focus of our work. Many polyhedral analyses and optimization techniques rely on the notion of lexicographic order, which is the order of execution of the statements in the source program. For instance, a data-dependence is defined to be an ordered pair of instruction instances that use or define the same data element, such that the first executes *before* the second. The lexicographic order is a purely syntactic characteristic that can be extracted from the source program. When the source program is explicitly parallel, the execution order becomes partial, because two distinct instruction instances can be part of concurrent activities. In this case the ordering is called the *Happens-before* relation. Paul Feautrier and Tomofumi Yuki have provided the first definition of *Happens-before* for explicitly parallel polyhedral programs, which covers the case of X10 programs using `finish` and `async` but without any clock involved. Being purely syntactic, their definition opens the way to the optimization of parallel X10 `finish-async` polyhedral programs. The use of clocks, however, introduces a major difficulty. Since clocks define phases of the program, one would like to use the "phase-number" of each instruction instance as an additional dimension, and include this dimension in further analysis. Phase-numbers have analytic forms (for the class of polyhedral programs), but they belong to the class of Ehrhart's quasi-polynomials, i.e., they are outside the polyhedral (affine) model.

We have formalized the class of programs under consideration, as well as all notions pertaining to the definition of the *Happens-before* relation, in Coq, a proof assistant developed at Inria. The formalization includes minimal structures to represent explicitly parallel polyhedral programs, including `finish` and `async`, loops, and simple statements. The definition of the *Happens-before* relation is that of an inductive predicate, parametrized by the computation of phase-numbers, which is left unspecified. To make the connection between the (static) *Happens-before* relation and the (dynamic) position of instruction instances in program traces, we use a single axiom. To reinforce our confidence in this arbitrary component, we also provide a second set of axioms, which we prove is equivalent to the first. The proof is based on an operational semantics, providing the relation between programs and their executions traces. We then prove that when *Happens-before* holds between two (static) instruction instances, then any trace of the program sees the corresponding dynamic instances ordered. We also prove the converse, which makes the definition of *Happens-before* sound and complete.

The Coq source files are kept in an Inria-forge project. Since this is our first effort in formal proofs, it currently amounts to about ten thousands lines of Coq source code. It is not yet clear whether we will publish the proof by itself, or publish an informal version of it as part of our colleagues' work on the use of *Happens-before*. In any case, our short-term plan is to extend the formalization and accompanying theorems and proofs to the case of mixed-programs, where some activities ignore the clock in scope.

7.2. Loop Nests and Integer Polyhedra

Participant: Alain Ketterlin.

The polyhedral model has been found adequate to model a large number of program analyses and transformations. It has now been used for decades in automatic parallelization, locality optimization, high-level code synthesis, and other applications. Thanks to the availability of high-quality software tools, the polyhedral model is now widely used. However, we feel that some of its most fundamental operations need more thorough attention, and possibly new theoretical developments. Even though the translation of loop nests into polyhedra (or unions thereof) obviously use integers only, many algorithms still use an underlying rational (or real) domain. For instance, Fourier-Motzkin variable elimination is defined on rational domains, and its modern incarnation (the Omega test), uses convoluted and costly techniques to compensate for the mishandling of integer variables. When used for projection (for instance during code generation, i.e., turning polyhedra into loop nests), these defects lead to sub-optimal results, with programs including more control than necessary. Overall, we feel that current techniques are inadequate to capture the precise behavior of integer variables.

We have started investigating new representations for inequalities over integer variables, using a notation called "periodic numbers". This notation was invented by Eugène Ehrhart in his classical results on the number of integer points inside integer polyhedra, and rediscovered and generalized by Philippe Clauss in his work on the use of counting for locality optimization and automatic parallelization. Periodic numbers capture all sorts of integer-specific behaviors: for instance, they are especially suitable to represent the seemingly chaotic structure of discrete line intersections, or the modular intersections of parallel hyper-planes. Periodic numbers also have algebraic properties that make them easy to manipulate and combine. We have defined a generalization of affine expressions where the constant term becomes a periodic number: it turns out that this family of expressions has interesting stability properties, that make them especially suitable for variable elimination. We have shown that most problems of Fourier-Motzkin variable elimination are related to the "looseness" of affine inequalities over integer variables, and that periodic numbers can correct this defect. The result is a new representation of inequalities, that makes reasoning with inequalities sound and complete.

An immediate application of our new representation is deciding whether a given integer polyhedron contains an integer point (or: whether a given set of affine constraints on integer variables is feasible). We have developed a straightforward version of Fourier-Motzkin elimination that is always exact. An interesting aspect of this work is that the algorithm is only a slight generalization of the original Fourier-Motzkin elimination, to cover the cases where inequalities have periodic components. We have also extended the basic algorithm to produce arbitrary projections of integer polyhedra. This improves over the Omega elimination strategy in that we are able to produce a provably disjoint union. These interesting properties derive directly from the use of periodic numbers.

Periodic numbers, and periodic linear inequalities, also have applications more directly related to the compilation of affine loop nests. For instance, we have developed a fully-general unswitching transformation. Unswitching a loop containing a conditional amounts to split the loop into one or more new loops such that the conditional has a constant truth value in all loop fragments, and can therefore be removed. The transformation is general in that the resulting program contains only affine loops and periodic linear conditionals. This means that the process can be repeated until obtaining a final version of the loop nest that is completely free of conditionals. We expect this "code generation" strategy, though naive, to remove enough "divergence" to increase existing and enable new applications of vectorization, leading to more efficient code. On the theory side, producing a conditional-free code scanning an arbitrary union of polyhedra has also direct consequences on various polyhedral operations: for instance, computing extrema becomes a trivial task, and linear optimization also falls under this umbrella. We hope to be able to explore these tracks in the near future.

We have developed software making use (and illustrating) our theoretical developments. We expect to share this software with select colleagues very soon, so as to be able to assess the scope of our techniques. Publication of these results is expected in the next year, time permitting. We also expect to extend our current software base to provide a range of integer polyhedra operations (images and pre-images, projection, and linear optimization, mostly). Finally, our middle-term goal is to investigate a formal modeling of the integer polyhedra operations. All algorithms have been kept as simple as possible, favoring elaborate abstractions over complex processing, with the goal of being able to formally specify the fundamental operations.

7.3. Splitting Polyhedra to Generate More Efficient Code

Participants: Harenome Ranaivoarivony-Razanajato, Vincent Loechner, Cédric Bastoul.

Code generation in the polyhedral model takes as input a union of Z-polyhedra and produces a code scanning all of them. Modern code generation tools are heavily relying on polyhedral operations to perform this task. However, these operations are typically provided by general-purpose polyhedral libraries that are not specifically designed to address the code generation problem. In particular, (unions of) polyhedra may be represented in various mathematically equivalent ways which may have different properties with respect to code generation. We investigated this problem and tried to find the best representation of polyhedra to generate an efficient code.

We demonstrated that this problem has been largely under-estimated, showing significant control overhead deviations when using different representations of the same polyhedra. Second, we proposed an improvement to the main algorithm of the state-of-the-art code generation tool CLooG. It generates code with less tests in the inner loops, and aims at reducing control overhead and at simplifying vectorization for the compiler, at the cost of a larger code size. It is based on a smart splitting of the union of polyhedra while recursing on the dimensions.

We implemented our algorithm in CLooG/PolyLib, and compared the performance and size of the generated code to the CLooG/isl version. Our results show that there can be important performance differences between the generated versions. In some cases, our new technique may significantly improve the quality of the generated code, but in some other cases, it may not be adequate compared to the existing solution. Finding other alternatives and chosing the best one remain open problems to be investigated in the future.

7.4. Code-Bones for Fast and Flexible Runtime Code Generation

Participants: Juan Manuel Martinez Caamaño, Artiom Baloian, Philippe Clauss.

We have developed a new runtime code generation technique for speculative loop optimization and parallelization. The main benefit of this technique, compared to previous approaches, is to enable advanced optimizing loop transformations at runtime with an acceptable time overhead. The loop transformations that may be applied are those handled by the polyhedral model. The proposed code generation strategy is based on the generation of *code-bones* at compile-time, which are parametrized code snippets either dedicated to speculation management or to computations of the original target program. These code bones are then instantiated and assembled at runtime to constitute the speculatively-optimized code, as soon as an optimizing polyhedral transformation has been determined. Their granularity threshold is sufficient to apply any polyhedral transformation, while still enabling fast runtime code generation. This approach has been implemented in the speculative loop parallelizing framework Apollo, and published at the conference Euro-Par 2016 where it has been selected as best paper [13]. An extended journal version is currently under review. This is also the main contribution of Juan Manuel Martinez Caamaño's PhD thesis which was defended in September 2016 [8].

7.5. Automatic Collapsing of Non-Rectangular Loops

Participants: Philippe Clauss, Ervin Altıntaş, Matthieu Kuhn.

Loop collapsing is a well-known loop transformation which combines some loops that are perfectly nested into one single loop. It allows to take advantage of the whole amount of parallelism exhibited by the collapsed loops, and provides a perfect load balancing of iterations among the parallel threads.

However, in the current implementations of this loop optimization, as the ones of the OpenMP language, automatic loop collapsing is limited to loops with constant loop bounds that define rectangular iteration spaces, although load imbalance is a particularly crucial issue with non-rectangular loops. The OpenMP language addresses load balance mostly through dynamic runtime scheduling of the parallel threads. Nevertheless, this runtime schedule introduces some unavoidable execution-time overhead, while preventing to exploit the entire parallelism of all the parallel loops.

We propose a technique to automatically collapse any perfectly nested loops defining non-rectangular iteration spaces, whose bounds are linear functions of the loop iterators. Such spaces may be triangular, tetrahedral, trapezoidal, rhomboidal or parallelepiped. Our solution is based on original mathematical results addressing the inversion of a multi-variate polynomial that defines a ranking of the integer points contained in a convex polyhedron.

We show on a set of non-rectangular loop nests that our technique allows to generate parallel OpenMP codes that outperform the original parallel loop nests, parallelized either by using options “static” or “dynamic” of the OpenMP-schedule clause. A conference paper presenting these results, co-authored by Philippe Clauss, Ervin Altıntaş (Master student) and Matthieu Kuhn (Inria Bordeaux Sud-Ouest, team HIEPACS), is currently under review.

7.6. Efficient Data Structures for a PIC Code on SIMD Architectures

Participants: Yann Barsamian, Éric Violard.

In collaboration with Sever Adrian Hirstoaga (mathematician researcher, member of Inria team TONUS), we have developed an efficient particle simulation code. The domain of application is plasma physics, the Particle-In-Cell code simulating 2d2v Vlasov-Poisson equation on Cartesian grid with periodic boundary conditions for Landau damping test-case. We first analyzed different strategies for improving its performance on single core and then we used a standard approach for parallelizing it on many cores using hybrid OpenMP/MPI implementation. The optimization of the sequential code is mainly based on (i) a structure of arrays for the particles, (ii) an efficient data structure for the electric field and the charge density, and (iii) an appropriate code for automatic vectorization of the charge accumulation and of the positions’ update. The parallelization of the loops over the particles is performed in a simple way (without domain decomposition) by means of both distributed and share memory paradigms. Satisfactory strong and weak scaling up to 8,192 cores on GENCI’s supercomputer Curie are obtained, bounded as expected by the overhead of MPI communications. A conference paper presenting this work is currently under review.

7.7. Interactive Code Restructuring

Participants: Cédric Bastoul, Oleksandr Zinenko, Stéphane Huot.

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.

This is a new research direction opened by CAMUS which strengthens the team’s static parallelization and optimization issue. It is a joint work with two Inria teams specialized in interaction: EX-SITU at Inria Saclay (contact: Oleksandr Zinenko) and MJOLNIR at Inria Lille (contact: Stéphane Huot).

In 2016, we released the first version of our interactive tool, *Clint*, that maps direct manipulation of the visual representation to polyhedral program transformations with real-time semantics preservation feedback (https://ozinenko.com/clint). Oleksandr Zinenko also defended his thesis on the research and development on interactive code restructuring.

7.8. Automatic Generation of Adaptive Simulation Codes

Participants: Cédric Bastoul, Maxime Schmitt.

Compiler automatic optimization and parallelization techniques are well suited for some classes of simulation or signal processing applications, however they usually don't take into account neither domain-specific knowledge nor the possibility to change or to remove some computations to achieve "good enough" results. Quite differently, production simulation and signal processing codes have adaptive capabilities: they are designed to compute precise results only where it matters if the complete problem is not tractable or if the computation time must be short. In this research, we design a new way to provide adaptive capabilities to compute-intensive codes automatically, inspired by Adaptive Mesh Refinement a classical numerical analysis technique to achieve precise computation only in pertinent areas. It relies on domain-specific knowledge provided through special pragmas by the programmer in the input code and on polyhedral compilation techniques, to continuously regenerate at runtime a code that performs heavy computations only where it matters at every moment. A case study on a fluid simulation application shows that our strategy enables dramatic computation savings in the optimized portion of the application while maintaining good precision, with a minimal effort from the programmer.

This research direction started in 2015 and complements our other efforts on dynamic optimization. In 2016, we started a collaboration on this topic with Inria Nancy - Grand Est team TONUS, specialized on applied mathematics (contact: Philippe Helluy), to bring models and techniques from this field to compilers. This collaboration received the support from the excellence laboratory (LabEx) IRMIA through the funding of the thesis of Maxime Schmitt on this topic. A first paper on this new research direction has just been accepted to IMPACT 2017.

7.9. Polyhedral Compiler White-Boxing

Participants: Cédric Bastoul, Lénaïc Bagnères, Oleksandr Zinenko, Stéphane Huot.

While compilers offer a fair trade-off between productivity and executable performance in single-threaded execution, their optimizations remain fragile when addressing compute-intensive code for parallel architectures with deep memory hierarchies. Moreover, these optimizations operate as black boxes, impenetrable for the user, leaving them with no alternative to time-consuming and error-prone manual optimization in cases where an imprecise cost model or a weak analysis resulted in a bad optimization decision. To address this issue, we researched and designed a technique allowing to automatically translate an arbitrary polyhedral optimization, used internally by loop-level optimization frameworks of several modern compilers, into a sequence of comprehensible syntactic transformations as long as this optimization focuses on scheduling loop iterations. With our approach, we open the black box of the polyhedral frameworks enabling users to examine, refine, replay and even design complex optimizations semi-automatically in partnership with the compiler.

This research started in 2014 and we published our first solution in 2016. It has been conducted as a joint work between teams in compiler technologies (CAMUS and Inria Saclay's POSTALE team) and teams in interaction (EX-SITU at Inria Saclay and MJOLNIR at Inria Lille). The first paper on this has been accepted and presented in one of the top conferences on optimization techniques: CGO 2016 [10]. It is also discussed in Lénaïc Bagnèse and Oleksandr Zinenko theses. In 2016 we finally release the tool implementing this research (https://periscop.github.io/chlore).

7.10. Mapping Deviation

Participant: Cédric Bastoul.

Compilers can provide a major help by automating the optimization and parallelization work. However they are very fragile black-boxes. A compiler may take a bad optimization decision because of imprecise heuristics or may turn off an optimization because of imprecise analyses, without providing much control or feedback to the end user. To address this issue, we researched and introduced mapping deviation, a new compiler technique that aims at providing a useful feedback on the semantics of a given program restructuring. Starting from a transformation intuition a user or a compiler wants to apply, our algorithm studies its correctness and can suggest changes or conditions to make it possible rather than being limited to the classical go/no-go answer. This algorithm builds on state-of-the-art polyhedral representation of programs and provides a high flexibility. We present two example applications of this technique: improving semi-automatic optimization tools for programmers and automatically designing runtime tests to check the correctness of a transformation for compilers.

This is a mid-term research on the mathematical ground of polyhedral compilation, started back to 2012. We found a solution and published it in 2016 in one of the main conferences in compilation: Compiler Construction [11]. We plan to release the tool that implements this research during the coming year.

7.11. Combining Locking and Data Management Interfaces

Participants: Jens Gustedt, Mariem Saied, Daniel Salas.

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 [1] shows how to produce deadlock-free iterative programs that implement strong overlapping between communication, IO and computation.

An implementation (ORWL) of our ideas of combining control and data management in C has been undertaken, see 6.8 . In previous work it has demonstrated its efficiency for a large variety of platforms. In 2016, work on the ORWL model and library has gained vigor with the thesis of Mariem Saied (Inria & University of Strasbourg) and Daniel Salas (INSERM). We also now collaborate on that subject with the TADAAM project team from Inria Bordeaux, where a postdoc has been hired through Inria funding.

In 2016, a new domain specific language (DSL) has been completed that largely eases the implementation of applications with ORWL. In its first version it provides an interface for stencil codes, but extensions towards other types of applications are on their way. The approach allows to describe stencil codes quickly and efficient and leads to substantial speedups, see [14].

In addition, the framework has successfully been applied to encapsulate imaging applications that use certain pipeline patterns to describe dependencies between computational tasks, see [16]. Generally we have been able to use the knowledge of the communication structure of ORWL programs to map tasks to cores and thereby achieve interesting performance gains on multicore architectures, see [20].

In another work we have successfully applied ORWL to process Large Histopathology Images, see [15].

CARAMBA Project-Team

7. New Results

7.1. Collecting Relation for the Number Field Sieve in Medium Characteristic

Participants: Pierrick Gaudry, Laurent Grémy [contact], Marion Videau.

We study the relation collection of NFS in medium characteristic, especially in $\mathrm{GF}(p^6)$ [4]. We compare different polynomial selections that affect drastically the relation collection step, by giving the explicit formula in 3 dimensions of two functions to select the best polynomials. For the relation collection, we design new sieve algorithms in 3 dimensions and do the practical comparison of the different polynomial selections for different p. Finally, we perform the relation collection step for a field of 389 bits in 800 days, the largest computed relation collection in this type of field.

7.2. Recent Progress on the Elliptic Curve Discrete Logarithm Problem

Participant: Pierrick Gaudry [contact].

A survey on the elliptic curve discrete logarithm problem has been written in collaboration with S. Galbraith (Auckland). It appeared in a special issue of DCC [3], for the 25th birthday of the journal.

7.3. A Modified Block Lanczos Algorithm with Fewer Vectors

Participant: Emmanuel Thomé [contact].

In the context of a book project entitled “Topics in Computational Number Theory inspired by Peter L. Montgomery” (edited by Joppe W. Bos and Arjen K. Lenstra), E. Thomé contributed a chapter on “the Block Lanczos algorithm” (owed to Peter L. Montgomery [35]). This was the occasion to rework and streamline the presentation of the block Lanczos algorithm. In fact, several new characteristics of the algorithm were obtained in this process: a version adapted to homogeneous systems, an improvement on the memory footprint of the algorithm, and a heuristic justification for the success probability of the algorithm. While the collated book is still not published yet (publication is expected in 2017), the chapter is published in preprint form as [14].

7.4. Factorization of RSA-220 with CADO-NFS

Participants: Pierrick Gaudry, Emmanuel Thomé, Paul Zimmermann [contact].

In May 2016 we have completed with CADO-NFS the factorization of RSA-220 [15], which was started in December 2013. The sieving was completed in September 2014, and the first phase of the linear algebra (`krylov`) in October 2014. However we had to improve CADO-NFS to be able to run the `lingen` sub-step of the linear algebra. This was completed in January 2016, and the end of the factorization ran smoothly. This factorization is the largest one done with CADO-NFS, and the third largest one overall, after RSA-768 (232 digits) factored in December 2009, and $3^{697} + 1$ (221 digits) factored by NFS@Home in February 2015.

7.5. Linear Time Interactive Certificates for the Minimal Polynomial and the Determinant of a Sparse Matrix

Participant: Emmanuel Thomé [contact].

Following discussion with Jean-Guillaume Dumas which began in March 2015 on the topic of computing checkpoints for the `krylov` step of the block Wiedemann algorithm, we determined that a scheme very similar to this checkpointing technique (originally designed to spot data corruption errors) was able to provide a proving algorithm —in the cryptographic sense— for the computation of the minimal polynomial of a sparse matrix, or for its determinant. This led to a joint paper with Jean-Guillaume Dumas, Erich Kaltofen and Gilles Villard, published at ISSAC 2016 [8].

7.6. A Kilobit Hidden SNFS Discrete Logarithm Computation

Participants: Pierrick Gaudry, Emmanuel Thomé [contact].

In collaboration with Josh Fried and Nadia Heninger from University of Pennsylvania, we worked on discrete logarithm computation modulo primes of a special form, amenable to computation with the Special Number Field Sieve (SNFS). Our original interest in this question came from the observation that primes which are conspicuous SNFS targets *are* found in the wild, as we observed in the context of the LogJam attack in 2015. We first ran a test computation on such a prime in March ($p = 2^{784} - 2^{28} + 1027679$, found in the LibTomcrypt library. For modern cryptographic uses, such a prime qualifies undoubtedly as "not good'). Based on the computational data obtained, and on further work, we expanded to larger sizes. We crafted a prime which was chosen as a "best case" for SNFS, yet with the property that this SNFS-optimality cannot be detected. We call such primes "trapdoored primes". We showed that computing discrete logarithms modulo trapdoored primes is entirely feasible for 1024-bit primes. In the article [18], we also showed that there are primes which are found in the wild (e.g., in RFC 5114) which could plausibly be trapdoored primes, given that no justification of their origin is provided. In fact, while cryptographic best practice is to provide "rigid" choices whenever random choices are to be set publicly, the sad truth is that random data lacking a justification is found quite often.

In the context of [18], we also put into practice an improvement of the implementation of the block Wiedemann algorithm in Cado-NFS, that allowed to reduce the time for the linear algebra computation significantly.

7.7. Solving Discrete Logarithms on a 170-bit MNT Curve by Pairing Reduction

Participants: Aurore Guillevic [contact], Emmanuel Thomé [contact].

The project of computing discrete logarithms in finite fields of the form GF(p^n) for small n comes from the need to estimate precisely the security level of pairing-based cryptography. After the two record computations of 2014 and 2015 in GF(p^2) of 160 and 180 decimal digits (532 and 597 bits) we investigated GF(p^3) and took a real-life elliptic curve proposed in 2001 by Miyaji, Nakabayashi and Takano (MNT-3 curve). Thanks to a pairing computation (in few milliseconds), a discrete logarithm computation in the 170-bit MNT-3 curve, which is hard, can be done instead by a discrete logarithm computation in GF(p^3) of 508 bits, which is much faster. This computation involved Aurore Guillevic (post-doctoral fellow in 2016 at the University of Calgary, Canada), Emmanuel Thomé, and François Morain (LIX/École Polytechnique/Inria Saclay, GRACE team). The computation took 2.97 years in total: 1.81 years for the relation collection, 1.16 years for the linear algebra and 2 days for the individual discrete logarithm computation. The work was presented at the Selected Areas in Cryptography conference in Newfoundland, Canada, and published in the proceedings [11].

The next step will be to adapt the new NFS variant called Extended-Tower-NFS to attack MNT-4 and MNT-6 curves, which means computing discrete logarithms in GF(p^4) and GF(p^6). This new challenge will require the higher dimension sieve developed by Laurent Grémy.

7.8. Computing Jacobi's Theta in Quasi-linear Time

Participant: Hugo Labrande [contact].

Most of the results have been obtained in 2015. The article was accepted for publication in 2016 [5].

We study the multiprecision computation of the theta function in genus 1, *i.e.,* the Jacobi theta function. The main result is that $\theta(z, \tau)$ can be computed in time that is quasi-linear in the precision P, using an algorithm which follows the same strategy as the case of theta-constants (Dupont, 2006). A thorough analysis of the precision loss is given in order to prove correctness.

Along with this work, we have publicly released an open source implementation of the algorithm in C (using the GNU MPC library). This implementation shows this algorithm is faster than a more naive approach for precisions greater than 300,000 digits.

7.9. Computing Theta Functions in Quasi-linear Time in Genus 2 and Above

Participants: Hugo Labrande, Emmanuel Thomé [contact].

We study the multiprecision computation of the theta function in genus 2. We extend the quasi-linear algorithm for Jacobi's theta to genus 2, generalizing the approach we undertook in previous work; this required finding workarounds, most notably for the choice of signs and for being able to apply Newton's method. We also give an outline of an algorithm for the theta function in genus g, but the workarounds we found in genus 2 would need to be generalized to this case before claiming any sort of result in genus g [6].

We released along with this work a Magma implementation of our fast genus 2 algorithm, along with an implementation of a somewhat naive (but previously state-of-the-art) algorithm for genus 2. Our results show that our algorithm is faster than the naive one for precisions greater than 3,000 digits.

7.10. Computing Small Certificates of Inconsistency of Quadratic Fewnomial Systems

Participant: Pierre-Jean Spaenlehauer [contact].

This is a joint work with Jean-Charles Faugère (Inria, EPI Polsys) and Jules Svartz (Inria EPI Polsys/Ministère Éducation Nationale). Most of the results have been obtained in 2015. This work was finalized and published in 2016 [10].

We study how Gröbner bases algorithms can be adapted to compute certificates that *quadratic fewnomial systems* (*i.e.*, systems in which only a small subset of monomials occur in the equations) do not have any solution. The main results are algorithms and complexity bounds which take into account the sparsity of the monomial support of the system, under some mild genericity assumptions on the coefficients of the systems.

7.11. Critical Point Computations on Smooth Varieties: Degree and Complexity Bounds

Participant: Pierre-Jean Spaenlehauer [contact].

This is a joint work with Mohab Safey El Din (Univ. Paris 6, EPI Polsys). This work led to a publication in the proceedings of the ISSAC conference [13].

Let $V \subset \mathbb{C}^n$ be an equidimensional algebraic set and g be an n-variate polynomial with rational coefficients. Computing the critical points of the map that evaluates g at the points of V is a cornerstone of several algorithms in real algebraic geometry and optimization. Under the assumption that the critical locus is finite and that the projective closure of V is smooth, we provide sharp upper bounds on the degree of the critical locus which depend only on $\deg(g)$ and the degrees of the generic polar varieties associated to V. Using these degree bounds and an algorithm due to Bank, Giusti, Heintz, Lecerf, Matera and Solernó, we derive complexity bounds which are quadratic in the degree bounds (up to logarithmic factors) and polynomial in all the other parameters of the problem.

7.12. Constructing Sparse Polynomial Systems with Many Positive Solutions

Participant: Pierre-Jean Spaenlehauer [contact].

This is a joint work with Frédéric Bihan (Univ. de Savoie, LAMA). Most of the results have been obtained in 2015 [25]; we improved the results during 2016.

Consider a regular triangulation of the convex-hull P of a set $\mathcal{A}$ of n points in $\mathbb{R}^d$, and a real matrix C of size $d \times n$. A version of Viro's method allows to construct from these data an unmixed polynomial system with support $\mathcal{A}$ and coefficient matrix C whose number of positive solutions is bounded from below by the number of d-simplices which are positively decorated by C (a d-simplex is positively decorated by C if the $d \times (d+1)$ sub-matrix of C corresponding to the simplex has a kernel vector all coefficients of which are positive). We show that all the d-simplices of a triangulation can be positively decorated if and only if the triangulation is balanced, which in turn is equivalent to the fact that its dual graph is bipartite. This allows us to identify, among classical families, monomial supports which admit maximally positive systems, giving some evidence in favor of a conjecture due to Bihan. We also use this technique in order to construct fewnomial systems with many positive solutions.

7.13. Modular Arithmetic and ECM on the Kalray MPPA-256 Processor

Participants: Jérémie Detrey [contact], Pierrick Gaudry.

In collaboration with Masahiro Ishii from the Nara Institute of Science and Technology, Nara (Japan) we have developed a fast modular arithmetic library for the Kalray MPPA-256, which is a many-core processor with a VLIW architecture. Carefully written assembly allowed us to obtain a close to optimal use of the computing units of all the cores for the multiprecision multiplication of integers. As an application, the ECM factoring algorithm was implemented on top of our library. The performances are very interesting compared to other architectures like GPU, especially in terms of power consumption [19].

7.14. Determinism and Computational Power of Real Measurement-based Quantum Computation

Participant: Luc Sanselme [contact].

This is a joint work with Simon Perdrix (CNRS, Carte Team at Loria). This work has begun in 2014.

The starting point for this work was about a problem in «Quantum cloud computing». A person with a classical resource wants to perform a quantum computation. To do so he asks some quantum resources to perform his computation. The difficult part is that he wants to be sure that the quantum resources he asks to perform his computation don't cheat and return him the good results. This kind of «Quantum cloud computing» is called interactive proofs. The quantum resources are called the provers. Real Measurement-based quantum computing (MBQC) has been used for interactive proofs by McKague.

Measurement-based quantum computing (MBQC) is a universal model for quantum computation. The combinatorial characterization of determinism in this model, powered by measurements, and hence, fundamentally probabilistic, is the cornerstone of most of the breakthrough results in this field. To answer our question, we needed to develop some tools in this MBQC field. The most general known sufficient condition for a deterministic MBQC to be driven is that the underlying graph of the computation has a particular kind of flow called Pauli flow. The necessity of the Pauli flow was an open question. We showed that the Pauli flow is necessary for real-MBQC, and not in general providing counter-examples for (complex) MBQC. We explored the consequences of this result for real MBQC and its applications. Real MBQC and more generally real quantum computing is known to be universal for quantum computing. In the interactive proofs developed by McKague, the two-prover case corresponds to real-MBQC on bipartite graphs. While (complex) MBQC on bipartite graphs are universal, the universality of real MBQC on bipartite graphs was an open question. We showed that real bipartite MBQC is not universal: we proved that all measurements of real bipartite MBQC can be parallelized. Therefore, real bipartite MBQC leads to constant depth computations. As a consequence, McKague techniques cannot lead to two-prover interactive proofs.

7.15. Fast Integer Multiplication Using Generalized Fermat Primes

Participants: Svyatoslav Covanov [contact], Emmanuel Thomé.

The paper [17] describes an algorithm for the multiplication of two n-bit integers. It achieves the best asymptotic complexity bound $O(n \log n \cdot 4^{\log^* n})$ under a hypothesis on the distribution of generalized Fermat primes of the form $r^{2^\lambda} + 1$. This hypothesis states that there always exists a sufficiently small interval in which we can find such a prime. Experimental results give evidence in favor of this assumption. This article has been submitted to Mathematics of Computation and some corrections, that have been requested, are processed currently.

7.16. Search for Primitive Trinomials

Participant: Paul Zimmermann [contact].

This is a joint work with Richard Brent (University of Newcastle, Australia).

We have performed a search for primitive trinomials $x^r + x^s + 1$ over $\mathrm{GF}(2)$ of degree $r = 42\,643\,801$, $r = 43\,112\,609$, $r = 57\,885\,161$ and $r = 74\,207\,281$, which are the new Mersenne prime exponents found by the GIMPS project. We found respectively 5, 4, 0 and 3 primitive trinomials [16], for example the three primitive trinomials of degree $74\,207\,281$ are (with their reverse trinomials):

$$x^{74207281} + x^{9156813} + 1, \qquad x^{74207281} + x^{9999621} + 1, \qquad x^{74207281} + x^{30684570} + 1.$$

CARTE Team

6. New Results

6.1. Quantum Computing

Participants: Simon Perdrix, Quanlong Wang.

- **ZX-calculus**

  The ZX-calculus is a powerful diagrammatic language for quantum mechanics and quantum information processing. The completeness of the ZX-calculus is crucial: the language would be complete if any equation involving two diagrams representing the same quantum evolution can be derived using the rules of the language. While the language is known to be incomplete in general with no obvious way to add some new rules [75], two interesting fragments have been studied: the $\pi/2$ and the $\pi/4$-fragments, obtained by restricting the angles of diagrams to be multiples of $\pi/2$ and $\pi/4$ respectively.

  The $\pi/4$-fragment is approximatively universal for quantum mechanics, i.e. any quantum evolution can be approximated with an arbitrary accuracy using a diagram involving only angles multiple of $\pi/4$. The completeness of this fragment was one of the main open question in this domain. We have proved that this fragment is incomplete. We exhibit a fairly simple equation called supplementarity and we prove that this equation cannot be derived in the ZX-calculus. We propose as a consequence, to add supplementarity to the set of rules of the ZX-calculus. This result has been published at MFCS 2016 [20].

  The $\pi/2$-fragment is not universal, even approximatively. However it corresponds to the so-called stabiliser quantum mechanics, an interesting fragment of quantum mechanics. The $pi/2$-fragment is known to be complete for stabiliser quantum mechanics [33]. We have proved recently that the rules of the language can be simplified, leading to a simpler set of axioms. Moreover we have proved that most of the remaining rules being necessary are the completeness of the $\pi/2$-fragment. This result has been published at QPL 2016 [16].

- **Causal Graph Dynamics**

  Causal Graph Dynamics [30] extend Cellular Automata to arbitrary, bounded-degree, time-varying graphs. The whole graph evolves in discrete time steps, and this global evolution is required to have a number of physics-like symmetries: shift-invariance (it acts everywhere the same) and causality (information has a bounded speed of propagation). We add a further physics-like symmetry, namely reversibility. This result has been presented at RC 2016 [15].

6.2. Implicit Computational Complexity

Participants: Emmanuel Hainry, Romain Péchoux.

We have written a full journal paper, accepted in Information and Computation (special issue of DICE 2015), on the complexity analysis of Object Oriented programming languages based on tiered types. The corresponding type system provides sound and complete characterization of the set of polynomial time computable functions. As a consequence, the heap-space and the stack-space requirements of typed programs are also bounded polynomially. This type system is inspired by previous works on Implicit Computational Complexity, using tiering and non-interference techniques. The presented methodology has several advantages. First, it provides explicit big O polynomial upper bounds to the programmer, hence its use could allow the programmer to avoid memory errors. Second, type checking is decidable in polynomial time. Last, it has a good expressivity since it analyzes most object oriented features like inheritance, overload, override and recursion. Moreover it can deal with loops guarded by objects and can also be extended to statements that alter the control flow like break or return.

6.3. Computing with Infinite Objects

Participant: Mathieu Hoyrup.

- **Decidable properties of subrecursive functions**

  We have studied the following problem : given a subrecursive class (like the primitive recursive functions, the polynomial-time computable functions, etc.) and a sound and complete programming language for that class, what are the properties of functions that are decidable (by a Turing machine), given a program for that function in the restricted language? We give a complete characterization of these properties. We show that they can be expressed as unions of elementary properties of being compressible. If $h : \mathbb{N} \to \mathbb{N}$ is a computable increasing unbounded function (like $\log(n)$ or 2^n), we say that a function $f : \mathbb{N} \to \mathbb{N}$ is h-compressible if for each n there is a program (in the restricted language) of size at most $h(n)$ computing a function that coincides with f on entries $0, 1, ..., n$. Whether f is h-compressible is decidable given a program for f, and every decidable property can be obtained as a combination of such elementary properties.

  We also prove that such a characterization does not hold for the whole class of total recursive functions, and leave the problem open for that class.

  The results appears in an article presented at ICALP 2016 [19].

- **Baire category and computability theory**

  Baire category is a very powerful tool in mathematical analysis to prove existence of objects with prescribed properties without having to explicitly build them, but showing instead that the class of objects with these properties is large in some sense. In Computability theory one often builds objects with very specific properties, notably to separate classes, and the proofs are often very involved. We show how Baire category can be adapted in order to be applied to computability theory, to prove existence results without the need of an explicit construction. We review notions that we introduced in the last years and provide new results in an invited paper at CiE 2016 [14].

6.4. Cellular automata as a model of computation

Participant: Nazim Fatès.

The density classification problem is a simple computational problem where a distributed system composed of many cells need to find the majority state in its initial configuration. It is known that no deterministic cellular automaton can solve this problem without making errors. On the other hand, it was shown that a probabilistic mixture of the traffic rule and the majority rule solves the one-dimensional problem correctly with a probability arbitrarily close to one. We investigated the possibility of a similar approach in two dimensions and introduced a companion problem, the particle spacing problem, as an intermediary step. We showed that although this second problem does not have a cellular automaton solution, the use of randomized frameworks, via interacting particle systems, could allow us to have interesting solutions, which were analysed with a theoretical approach and with numerical simulations [18].

In the same direction of research, we studied how to coordinate a team of agents to locate a hidden source on a two-dimensional discrete grid. The challenge here is to find the position of the source with only sporadic detections. This problem arises in various situations, for instance when insects emit pheromones to attract their partners. A search mechanism named infotaxis was previously proposed to explain how agents may progressively approach the source by using only intermittent detections.

We studied the problem of doing a collective infotaxis search with agents that are almost memoryless. We presented a bio-inspired model which mixes stochastic cellular automata and reactive multi-agent systems. The model, inspired by the behaviour of the social amoeba *Dictyostelium discoideum*, relies on the use of reaction-diffusion waves to guide the agents to the source. The random emissions of waves allows the formation of a group of amoebae, which successively act as emitters of waves or listeners, according to their local perceptions. Our worked showed that the model is worth considering and may provide a simple solution to coordinate a team to perform a distributed form of infotaxis [17].

PESTO Project-Team

7. New Results

7.1. Modelling

7.1.1. New protocol and adversary models

Participants: Jannik Dreier, Steve Kremer.

Isolated Execution Environments (IEEs), such as ARM TrustZone and Intel SGX, offer the possibility to execute sensitive code in isolation from other malicious programs, running on the same machine, or a potentially corrupted OS. A key feature of IEEs is the ability to produce reports binding cryptographically a message to the program that produced it, typically ensuring that this message is the result of the given program running on an IEE. In collaboration with Jacomme (ENS Cachan) and Scerri (Univ. Bristol), Kremer presented a symbolic model for specifying and verifying applications that make use of such features. For this they introduced the SℓAPiC process calculus to reason about reports issued at given locations. They also provide tool support, extending the SAPIC/TAMARIN toolchain and demonstrate the applicability of their framework on several examples implementing secure outsourced computation (SOC), a secure licensing protocol and a one-time password protocol that all rely on such IEEs. This work has been accepted for publication at EuroS&P'17 [27].

Most security properties are modelled as *safety* properties (*"bad things do not happen"*). Another important class of properties is that of *liveness* properties (*"eventually, good things happen"*). Reasoning about the class of *liveness* properties of cryptographic protocols, has received little attention in the literature, even though this class is vital in many security-sensitive applications, such as fair exchange protocols, or security layers in industrial control systems. In collaboration with Backes and Künnemann (U. Saarland, Germany), Dreier and Kremer have designed a protocol and adversary model that are suitable for reasoning about liveness properties. Tool support is also provided by extending the *SAPIC/TAMARIN* tool chain and several case studies demonstrate the effectiveness of the approach. This work has been accepted for publication at EuroS&P'17 [20].

7.1.2. New properties

Participants: Véronique Cortier, Jannik Dreier.

Defining security properties correctly is often a challenging problem on its own: too strict definitions may lack generality and exclude systems that should be considered as secure, while relaxing definitions may lead to accepting insecure systems.

In e-voting, *verifiability* is the property meant to defend against voting devices and servers that have programming errors or are outright malicious. While the first formal definitions of verifiability were devised in the late 1980s already, new verifiability definitions are still being proposed. The definitions differ in various aspects, including the classes of protocols they capture and even their formulations of the very core of the meaning of verifiability. This is an unsatisfying state of affairs, leaving the research on the verifiability of e-voting protocols and systems in a fuzzy state. Cortier, in collaboration with Galindo (U. Birmingham, UK), Küsters, Müller (U. Trier, Germany) and Truderung (Polyas GmbH, Germany), review all formal definitions of verifiability proposed in the literature and cast them in a framework proposed by the KTV framework, yielding a uniform treatment of verifiability. This enables a detailed comparison of the various definitions of verifiability from the literature and a discussion of advantages and disadvantages, limitations and problems. Finally, a general definition of verifiability is distilled, which can be instantiated in various ways. This work has been presented at S&P'16 [26].

Industrial systems are nowadays regularly the target of cyberattacks, the most famous being Stuxnet. At the same time such systems are increasingly interconnected with other systems and insecure media such as Internet. In contrast to other IT systems, industrial systems often do not only require classical properties like data confidentiality or authentication of the communication, but have special needs due to their interaction with the physical world. For example, the reordering or deletion of some commands sent to a machine can cause the system to enter an unsafe state with potentially catastrophic effects. To prevent such attacks, the integrity of the message flow is necessary.

In joint work with Lafourcade (Université Clermont-Ferrand), Potet, and Puys (University Grenoble Alpes), Dreier developed a formal definition of Flow Integrity in the context of industrial systems. The framework is applied to two well-known industrial protocols: OPC-UA and MODBUS. Using *TAMARIN*, a cryptographic protocol verification tool, they identified several design flaws in some of the different versions of these protocols. We also discussed how to efficiently model counters and timestamps in *TAMARIN*, as they are key ingredients of the analyzed protocols. This work is currently under submission.

7.2. Analysis

7.2.1. Analysis of equivalence properties

Participants: Vincent Cheval, Véronique Cortier, Antoine Dallon, Ivan Gazeau, Steve Kremer, Christophe Ringeissen.

Automatic tools based on symbolic models have been successful in analyzing security protocols. These tools are particularly well adapted for trace properties (e.g. secrecy or authentication). However, they often fail to analyse equivalence properties. Equivalence properties can express a variety of security properties, including in particular privacy properties (vote privacy, anonymity, untraceability). Several decision procedures have already been proposed but the resulting tools are often rather limited, and lack efficiency.

In the case of a passive adversary, Ringeissen, in collaboration with Marshall (U. of Mary Washington, USA) and Erbatur (LMU, Germany) present new combination techniques for the study of deducibility and static equivalence in unions of equational theories sharing constructors. This allows us to develop new modularity results for the decidability of deducibility and static equivalence. In turn, this should allow for the security analysis of protocols which previous disjoint combination methods could not address because their axiomatization corresponds to the union of non-disjoint equational theories.

In case of an active adversary, and a bounded number of sessions, we made several advances. In [14], Cheval and Kremer, in collaboration with Chadha (U. of Missouri, USA) and Ciobâcă (U. Iasi, Romania), present the theory underlying the *Akiss* tool, a Horn clause resolution based procedure for both under- and over-approximating trace equivalence. They show partial correctness for a large class of cryptographic primitives, modelled as an arbitrary convergent equational theory that has the finite variant properties. Additionally, termination is shown for subterm convergent theories. Gazeau and Kremer, in collaboration with Baelde (LSV, ENS Cachan) and Delaune (IRISA) have extended the *Akiss* tool with support for exclusive or. They analyse unlinkability in several RFID protocols and resistance to guessing attacks of several password base protocols. Cortier and Dallon, in collaboration with Delaune (IRISA) propose a novel algorithm, based on graph planning and SAT-solving, which significantly improves the efficiency of the analysis of equivalence properties. The resulting implementation, SAT-Equiv, can analyze several sessions where most tools have to stop after one or two sessions. Finally, Cheval and Kremer propose a novel decision procedure for verifying trace equivalence. Unlike most existing tools, they support a rich class of cryptographic primitives and protocols that may use else branches. An implementation of the procedure is currently under development.

These results are currently under submission.

7.2.2. Simplification results

Participants: Véronique Cortier, Antoine Dallon, Steve Kremer.

Bounding the number of agent identies is a current practice when modeling a protocol. In 2003, it has been shown that one honest agent and one dishonest agent are indeed sufficient to find all possible attacks, for trace properties. This is no longer the case for equivalence properties, crucial to express many properties such as vote privacy or untraceability. As a first result of his PhD, Antoine Dallon has shown that it is sufficient to consider two honest agents and two dishonest agents for equivalence properties, for deterministic processes with standard primitives and without else branches. More generally, we show how to bound the number of agents for arbitrary constructor theories and for protocols with simple else branches. We show that our hypotheses are tight, providing counter-examples for non action-deterministic processes, non constructor theories, or protocols with complex else branches. This work has been presented at POST 2016 [24] and obtained the EASST best paper award of the ETAPS conference.

When verifying e-voting protocols, one of the difficulties is that they need to be secure for an arbitrary number of malicious voters. In collaboration with Arapinis (U. Edinburgh, UK), Cortier and Kremer identify a class of voting protocols for which only a small number of voters needs to be considered: if there is an attack on vote privacy, for an arbitrary number of honest and dishonest voters, then there is also an attack that involves at most 3 voters (2 honest voters and 1 dishonest voter). In the case where the protocol allows a voter to cast several votes and counts, e.g., only the last one, we also reduce the number of ballots required for an attack to 10, and under some additional hypotheses, 7 ballots. They illustrate the applicability of our results on several case studies, including different versions of Helios and Prêt-à-Voter, as well as the JCJ protocol. For some of these protocols the ProVerif tool is used to provide the first formal proofs of privacy for an unbounded number of voters. This work has been presented at ESORICS 2016 [19].

7.2.3. *Analysis of stateful security protocols*

Participants: Jannik Dreier, Charles Duménil, Steve Kremer.

In collaboration with Künnemann (U. Saarland, Germany), Kremer proposes *SAPIC* (stateful applied pi calculus), a process calculus with constructs for manipulation of a global state by processes running in parallel. They show that this language can be translated to multiset rewriting rules whilst preserving all security properties expressible in a dedicated first-order logic for security properties. The translation has been implemented in a prototype tool which uses the *TAMARIN* prover as a backend. The tool is applied to several case studies among which a simplified fragment of PKCS#11, the Yubikey security token, and an optimistic contract signing protocol. This work has been published in the Journal of Computer Security [15]. Dreier, Duménil and Kremer, in collaboration with Sasse (ETH Zurich, Switzerland) improve the underlying theory and the *TAMARIN* tool to allow for more general user-specified equational theories: the extension supports arbitrary convergent equational theories that have the finite variant property, making *TAMARIN* the first tool to support at the same time this large set of user-defined equational theories, protocols with global mutable state, an unbounded number of sessions, and complex security properties. The effectiveness of this generalization is demonstrated by analyzing several protocols that rely on blind signatures, trapdoor commitment schemes, and ciphertext prefixes that were previously out of scope. This work has been accepted for publication at POST'17.

7.2.4. *Analysis of e-voting protocols*

Participants: Véronique Cortier, Constantin-Catalin Dragan.

Cortier and Dragan provide the first machine-checked proof of privacy-related properties (including ballot privacy) for an electronic voting protocol in the computational model. They target the popular Helios family of voting protocols, for which they identify appropriate levels of abstractions to allow the simplification and convenient reuse of proof steps across many variations of the voting scheme. The resulting framework enables machine-checked security proofs for several hundred variants of Helios and should serve as a stepping stone for the analysis of further variations of the scheme.

In addition, they highlight some of the lessons learned regarding the gap between pen-and-paper and machine-checked proofs, and report on the experience with formalizing the security of protocols at this scale. This work is submitted for publication.

7.2.5. Analysis of Electrum Bitcoin wallet

Participants: Michaël Rusinowitch, Mathieu Turuani.

Electrum is a popular Bitcoin wallet. We introduce a formal modeling in ASLan++ of the two-factor authentication protocol used by the Electrum Bitcoin wallet. This allows us to perform an automatic analysis of the wallet and show that it is secure for standard scenarios in the Dolev Yao model [30]. The result could be derived thanks to some advanced features of the Cl-Atse protocol analyzer such as the possibility to specify i) new intruder deduction rules with clauses and ii) non-deducibility constraints.

7.2.6. Satisfiability Modulo Bridging Theories

Participant: Christophe Ringeissen.

Bridging theories are equational theories defining recursive functions. They are useful to handle equational theories of interest in protocol analysis, as advocated in [48], where a locality approach is promoted to solve the satisfiability problem. In collaboration with Pascal Fontaine (Veridis project-team) and Paula Chocron (IIIA-CSIC Barcelona), we investigate a combination approach for the satisfiability problem modulo this particular non-disjoint union of theories, where a source theory is connected to a target one through a bridging function. In 2016, we have prepared a new full paper unifying previous results presented respectively at CADE 2015 [4] and FroCoS 2015. In that papers, we focused on source theories admitting term-generated models. In [21], we have also explored an extension to deal with terms modulo a congruence relation. This joint work with Raphaël Berthon (ENS Rennes) allows us to consider not only trees but also data structure theories such as lists, multisets and sets.

7.2.7. Analysis of Security Properties for an Unbounded Number of Sessions

Participants: Jonathan Proietto-Stallone, Mathieu Turuani, Laurent Vigneron.

The internship of Jonathan Proietto-Stallone has permitted to study the method described in [37] for analyzing protocols without bounding the number of sessions. We have clarified the formalization of this method, including the consideration of xor and exp operators, and implemented it in *CL-AtSe*.

7.3. Design

7.3.1. E-voting protocols

Participants: Véronique Cortier, Steve Kremer, Peter Roenne.

We propose a new voting scheme, BeleniosRF, that offers both receipt-freeness and end-to-end verifiability. It is receipt-free in a strong sense, meaning that even dishonest voters cannot prove how they voted. We provide a game-based definition of receipt-freeness for voting protocols with non-interactive ballot casting, which we name strong receipt-freeness (sRF). To our knowledge, sRF is the first game-based definition of receipt-freeness in the literature, and it has the merit of being particularly concise and simple. Built upon the Helios protocol, BeleniosRF inherits its simplicity and does not require any anti-coercion strategy from the voters. We implement BeleniosRF and show its feasibility on a number of platforms, including desktop computers and smartphones. This work has been presented at CCS 2016 [26].

Another challenging problem in e-voting is to provide guarantees when the voting platform itself is corrupted. Du-Vote [45] is a recently presented remote electronic voting scheme that aims to be malware tolerant, i.e., provide security even in the case where the platform used for voting has been compromised by dedicated malware. For this it uses an additional hardware token, similar to tokens distributed in the context of online banking. Du-Vote aims at providing vote privacy as long as either the vote platform or the vote server is honest. For verifiability, the security guarantees are even higher, as even if the token's software has been changed, and the platform and the server are colluding, attempts to change the election outcome should be detected with high probability. We provide an extensive security analysis of Du-Vote and show several attacks on both privacy as well as verifiability. We also propose changes to the system that would avoid many of these attacks. This work has been presented at Euro S&P 2016 [28].

7.3.2. Designing and proving an EMV-compliant payment protocol for mobile devices

Participants: Véronique Cortier, Alicia Filipiak.

In collaboration with Gharout, Traoré and Florent (Orange Labs), we devised a payment protocol that can be securely used on mobile devices, even infected by malicious applications. Our protocol only requires a light use of Secure Elements, which significantly simplifies certification procedures and protocol maintenance. It is also fully compatible with the EMV-SDA protocol and allows off-line payments for the users. We provide a formal model and full security proofs of the protocol using the TAMARIN prover. This work has been accepted for publication at Euro S&P'17 [25].

7.3.3. Composition and design of PKIs

Participants: Vincent Cheval, Véronique Cortier.

Public Key Infrastructures (PKIs) is the backbone of public key cryptography, as it ensures that public keys can be correctly linked to identities. Their security typically relies on honest Certificate Authorities that distribute and/or generate keys to all parties. This trust assumption is a vulnerability exploited in numerous attacks. Recent proposals using public logs have succeeded in making certificate management more transparent and verifiable. However, those proposals involve a fixed set of authorities which means an oligopoly is created. Another problem with current log-based system is their heavy reliance on trusted parties that monitor the logs. Cheval, in collaboration with Ryan and Yu (U. Birmingham, UK) propose a distributed transparent key infrastructure (DTKI), which greatly reduces the oligopoly of service providers and allows verification of the behaviour of trusted parties. Their work also formalises the public log data structure and provides a formal analysis of the security that DTKI guarantees. The work has been published in The Computer Journal [17].

In protocol analysis one makes the (strong) assumption that honestly generated keys are available to all parties and that the link between identities and public keys is fixed and known to everyone. The abstraction is grounded in solid intuition but there are currently no theoretical underpinnings to justify its use. Cheval and Cortier, in collaboration with Warinschi (U. Bristol, UK), initiate a rigorous study of how to use PKIs within other protocols, securely. They first show that the abstraction outlined above is in general unsound by exhibiting a simple protocol which is secure with idealized key distribution but fails in the presence of more realistic PKI instantiation. Their main result is a generic composition theorem that identifies under which conditions protocols that require public keys can safely use any PKI protocol (which satisfies a security notion which we identify). Interestingly, unlike most existing composition results in symbolic models they do not require full tagging of the composed protocols. Furthermore, the results confirm the recommended practice that keys used in the PKI should not be used for any other cryptographic task. This work is currently under submission.

7.3.4. Physical Zero-Knowledge Proofs

Participant: Jannik Dreier.

In this work we develop physical algorithms to realize zero-knowledge proofs for Akari, Takuzu, Kakuro, and KenKen, which are logic games similar to Sudoku. The zero-knowledge proofs allow a player to show that he knows a solution without revealing it. These interactive proofs can be realized with simple office material as they only rely on cards and envelopes. They can thus be used for example for scientific outreach activities, or in teaching. Moreover, we also formalized our algorithms and proved their security. This joint work with Bultel (U. Clermont-Ferrand), Dumas (U. Grenoble Alpes), and Lafourcade (U. Clermont-Ferrand) was published at FUN 2016 [22].

7.3.5. Privacy Protection in Social Networks

Participants: Younes Abid, Abdessamad Imine, Huu Hiep Nguyen, Clément Pascutto, Michaël Rusinowitch, Laura Trivino.

Hiep Nguyen's PhD thesis addresses three privacy problems of social networks: graph anonymization, private community detection and private link exchange. The main goal is to provide new paradigms for publication of social graphs in noisy forms, private community detection over graphs as well as distributed aggregation of graphs via noisy link exchange processes. The graph anonymization problem is solved via two different semantics: uncertainty semantics and differential privacy. For uncertainty semantics, a general obfuscation model is proposed that keeps the expected node degree equal to those in the unanonymized graph. Over the last decade, a great number of algorithms for community detection have been proposed to deal with the increasingly complex networks. However, the problem of doing this in a private manner is rarely considered. We analyze the major challenges behind the problem and propose several schemes to tackle them under differential privacy from two perspectives: input perturbation and algorithm perturbation [29].

We address the problem of rapidly disclosing many friendship links using only legitimate queries (i.e., queries and tools provided by the targeted social network). Our study [18] sheds new light on the intrinsic relation between communities (usually represented as groups) and friendships between individuals. To develop an efficient attack we analysed group distributions, densities and visibility parameters from a large sample of a social network. By effectively exploring the target group network, our proposed algorithm is able to perform friendship and mutual-friend attacks along a strategy that minimizes the number of queries. Pascutto has established a state-of-the-art on inference techniques for social networks. Trivino has developed a user interface for privacy risk evaluation on social networks.

VEGAS Project-Team

6. New Results

6.1. Non-linear Computational Geometry

Participants: Laurent Dupont, Rémi Imbach, Sylvain Lazard, Guillaume Moroz, Marc Pouget.

6.1.1. Numeric and Certified Algorithm for the Topology of the Projection of a Smooth Space Curve

Let a smooth real analytic curve embedded in $\mathbb{R}^3$ be defined as the solution of real analytic equations of the form $P(x, y, z) = Q(x, y, z) = 0$ or $P(x, y, z) = \frac{\partial P}{\partial z} = 0$. Our main objective is to describe its projection $\mathcal{C}$ onto the (x, y)-plane. In general, the curve $\mathcal{C}$ is not a regular submanifold of $\mathbb{R}^2$ and describing it requires to isolate the points of its singularity locus Σ.

In previous work, we have shown how to describe the set of singularities Σ of $\mathcal{C}$ as regular solutions of a so-called ball system suitable for a numerical subdivision solver. In our current work, the space curve is first enclosed in a set of boxes with a certified path-tracker to restrict the domain where the ball system is solved. Boxes around singular points are then computed such that the correct topology of the curve inside these boxes can be deduced from the intersections of the curve with their boundaries. The tracking of the space curve is then used to connect the smooth branches to the singular points. The subdivision of the plane induced by the curve is encoded as an extended planar combinatorial map allowing point location. This work is not already published but has been presented by R. Imbach at the Summer Workshop on Interval Methods (https://swim2016.sciencesconf.org/).

The technical report [28] describes the software SubdivisionSolver (see Section 5.2) used within this project.

6.1.2. A Fast Algorithm for Computing the Truncated Resultant

Let P and Q be two polynomials in $\mathbb{K}[x, y]$ with degree at most d, where $\mathbb{K}$ is a field. Denoting by $R \in \mathbb{K}[x]$ the resultant of P and Q with respect to y, we present an algorithm to compute $R \mod x^k$ in $\widetilde{O}(kd)$ arithmetic operations in $\mathbb{K}$, where the $\widetilde{O}$ notation indicates that we omit polylogarithmic factors. This is an improvement over state-of-the-art algorithms that require to compute R in $\widetilde{O}(d^3)$ operations before computing its first k coefficients [24].

This work was done in collaboration with Éric Schost (Waterloo University, Canda).

6.1.3. Quadric Arrangement in Classifying Rigid Motions of a 3D Digital Image

Rigid motions are fundamental operations in image processing. While bijective and isometric in $\mathbb{R}^3$, they lose these properties when digitized in $\mathbb{Z}^3$. To understand how the digitization of 3D rigid motions affects the topology and geometry of a chosen image patch, we classify the rigid motions according to their effect on the image patch. This classification can be described by an arrangement of hypersurfaces in the parameter space of 3D rigid motions of dimension six. However, its high dimensionality and the existence of degenerate cases make a direct application of classical techniques, such as cylindrical algebraic decomposition or critical point method, difficult. We show that this problem can be first reduced to computing sample points in an arrangement of quadrics in the 3D parameter space of rotations. Then we recover information about the three remaining parameters of translation. We implemented an ad-hoc variant of state-of-the-art algorithms and applied it to an image patch of cardinality 7. This leads to an arrangement of 81 quadrics and we recovered the classification in less than one hour on a machine equipped with 40 cores [25].

This work was done in collaboration with Kacper Pluta (LIGM - Laboratoire d'Informatique Gaspard-Monge), Yukiko Kenmochi (LIGM - Laboratoire d'Informatique Gaspard-Monge), Pascal Romon (LAMA - Laboratoire d'Analyse et de Mathématiques Appliquées).

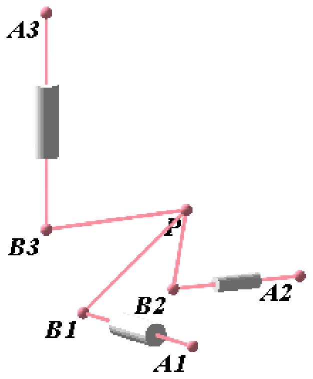

Figure 1. A configuration of the orthoglide manipulator has three orthogonal prismatic joints.

6.1.4. Influence of the Trajectory Planning on the Accuracy of the Orthoglide 5-axis manipulator

Usually, the accuracy of parallel manipulators depends on the architecture of the robot, the design parameters, the trajectory planning and the location of the path in the workspace. This paper reports the influence of static and dynamic parameters in computing the error in the pose associated with the trajectory planning made and analyzed with the Orthoglide 5-axis (Figure 1). An error model is proposed based on the joint parameters (velocity and acceleration) and experimental data coming from the Orthoglide 5-axis. Newton and Gröbner based elimination methods are used to project the joint error in the workspace to check the accuracy/error in the Cartesian space. For the analysis, five similar trajectories with different locations inside the workspace are defined using fifth order polynomial equation for the trajectory planning. It is shown that the accuracy of the robot depends on the location of the path as well as the starting and the ending posture of the manipulator due to the acceleration parameters [23].

This work was done in collaboration with Ranjan Jha (IRCCyN - Institut de Recherche en Communications et en Cybernétique de Nantes), Damien Chablat (IRCCyN - Institut de Recherche en Communications et en Cybernétique de Nantes), Fabrice Rouillier (Inria).

6.1.5. Solving Bivariate Systems and Topology of Plane Algebraic Curves

In the context of our algorithm Isotop for computing the topology of plane algebraic curves (see Section 5.1), we work on the problem of solving a system of two bivariate polynomials. We are interested in certified numerical approximations or, more precisely, isolating boxes of the solutions. But we are also interested in computing, as intermediate symbolic objects, a Rational Univariate Representation (RUR) that is, roughly speaking, a univariate polynomial and two rational functions that map the roots of the univariate polynomial to the two coordinates of the solutions of the system. RURs are relevant symbolic objects because they allow to the transformation of many queries on the system into queries on univariate polynomials. However, such representations require the computation of a separating form for the system, that is a linear combination of the variables that takes different values when evaluated at the distinct solutions of the system.

We published this year [11] results showing that, given two polynomials of degree at most d with integer coefficients of bitsize at most τ, (i) a separating form, (ii) the associated RUR, and (iii) isolating boxes of the solutions can be computed in, respectively, $\widetilde{O}_B(d^5 + d^5\tau)$, bit operations in the worst case, where $\widetilde{O}$ refers to the complexity where polylogarithmic factors are omitted and O_B refers to the bit complexity. Furthermore, we also presented probabilistic Las Vegas variants of problems (i) and (ii), which have expected bit complexity $\widetilde{O}_B(d^5 + d^4\tau)$. We also showed that these complexities are "morally" optimal in the sense of that improving them would essentially require to improve bounds on several other fundamental problems (on resultants and roots isolation of univariate polynomials) that have hold for decades. These progresses are substential since, when we started woriking on these problems, their best know complexities were in $\widetilde{O}_B(d^{12} + d^{10}\tau^2)$ (2009).

This work was done in collaboration with Yacine Bouzidi (Inria Lille), Michael Sagraloff (MPII Sarrebruken, Germany) and Fabrice Rouillier (Inria Rocquencourt).

6.1.6. *Reflection through Quadric Mirror Surfaces*

We addressed the problem of finding the reflection point on quadric mirror surfaces, especially ellipsoid, paraboloid or hyperboloid of two sheets, 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. We previously proposed a new algorithm for this problem, using a characterization of the reflection point as the tangential intersection point between the mirror and an ellipsoid with foci P_1 and P_2. The computation of this tangential intersection point is based on our algorithm for the computation of the intersection of quadrics [5], [32]. Unfortunately, our new algorithm is not yet efficient in practice. This year, we made several improvements on this algorithm. First, we decreased from 11 to 4 the degree of a critical polynomial that we need to solve and whose solutions induce the coefficients in some other polynomials appearing later in the computations. Second, we implemented Descartes' algorithm for isolating the real roots of univariate polynomials in the case where the coefficients belong to extensions of $\mathbb{Q}$ generated by at most two square roots. Furthermore, we are currently implementing the generalization of that algorithm when the coefficients belong to extensions of $\mathbb{Q}$ generated by one root of an arbitrary polynomial. We are also interested by extensions decomposable in extensions of degree 2. These undergoing improvements should allow us to compute more directly the wanted reflection point, thus avoiding problematic approximations and making the overall algorithm tractable.

6.2. Non-Euclidean Computational Geometry

Participants: Iordan Iordanov, Monique Teillaud, Gert Vegter.

6.2.1. *Closed Flat Orbifolds*

The work on Delaunay triangulations of flat d-dimensional orbifolds, started several years ago in the Geometrica project team in Sophia Antipolis, was finalized this year [13].

We give a definition of the Delaunay triangulation of a point set in a closed Euclidean d-manifold, i.e. a compact quotient space of the Euclidean space for a discrete group of isometries (a so-called Bieberbach group or crystallographic group). We describe a geometric criterion to check whether a partition of the manifold actually forms a triangulation (which subsumes that it is a simplicial complex). We provide an incremental algorithm to compute the Delaunay triangulation of the manifold defined by a given set of input points, if it exists. Otherwise, the algorithm returns the Delaunay triangulation of a finite-sheeted covering space of the manifold. The algorithm has optimal randomized worst-case time and space complexity. It extends to closed Euclidean orbifolds. To the best of our knowledge, this is the first general result on this topic.

6.2.2. *Closed Orientable Hyperbolic Surfaces*

Motivated by applications in various fields, some packages to compute periodic Delaunay triangulations in the 2D and 3D Euclidean spaces have been introduced in the CGAL library and have attracted a number of users. To the best of our knowledge, no software is available to compute periodic triangulations in a hyperbolic space, though they are also used in diverse fields, such as physics, solid modeling, cosmological models, neuromathematics.

This would be a natural extension: 2D Euclidean periodic triangulations can be seen as triangulations of the two-dimensional (flat) torus of genus one; similarly, periodic triangulations in the hyperbolic plane can be seen as triangulations of hyperbolic surfaces. A closed orientable hyperbolic surface is the quotient of the hyperbolic plane under the action of a Fuchsian group only containing hyperbolic translations. Intuition is challenged there, in particular because such groups are non-Abelian in general.

We have obtained some theoretical results on Delaunay triangulations of general closed orientable hyperbolic surfaces, and we have investigated algorithms in the specific case of the Bolza surface, a hyperbolic surface with the simplest possible topology, as it is homeomorphic to a genus-two torus [20]. We are now studying more practical aspects and we propose a first implementation of an incremental construction of Delaunay triangulations of the Bolza surface [30].

6.3. Probabilistic Analysis of Geometric Data Structures and Algorithms

Participants: Olivier Devillers, Louis Noizet.

6.3.1. Stretch Factor of Long Paths in a Planar Poisson-Delaunay Triangulation

Let $X := X_n \cup \{(0,0),(1,0)\}$, where X_n is a planar Poisson point process of intensity n. We provide a first non-trivial lower bound for the distance between the expected length of the shortest path between $(0,0)$ and $(1,0)$ in the Delaunay triangulation associated with X when the intensity of X_n goes to infinity. Experimental values indicate that the correct value is about 1.04. We also prove that the expected number of Delaunay edges crossed by the line segment $[(0,0),(1,0)]$ is equivalent to $2.16\sqrt{n}$ and that the expected length of a particular path converges to 1.18 giving an upper bound on the stretch factor [26].

This work was done in collaboration with Nicolas Chenavier (Université Littoral Côte d'Opale).

6.3.2. Walking in a Planar Poisson-Delaunay Triangulation: Shortcuts in the Voronoi Path

Let X_n be a planar Poisson point process of intensity n. We give a new proof that the expected length of the Voronoi path between $(0,0)$ and $(1,0)$ in the Delaunay triangulation associated with X_n is $\frac{4}{\pi} \simeq 1.27$ when n goes to infinity; and we also prove that the variance of this length is $O(1/\sqrt{n})$. We investigate the length of possible shortcuts in this path, and defined a shortened Voronoi path whose expected length can be expressed as an integral that is numerically evaluated to $\simeq 1.16$. The shortened Voronoi path has the property to be *locally defined*; and is shorter than the previously known locally defined path in Delaunay triangulation such as the upper path whose expected length is $35/3\pi^2 \simeq 1.18$ [27].

6.3.3. Expected Length of the Voronoi Path in a High Dimensional Poisson-Delaunay Triangulation

Let X_n be a d dimensional Poisson point process of intensity n. We prove that the expected length of the Voronoi path between two points at distance 1 in the Delaunay triangulation associated with X_n is $\sqrt{\frac{2d}{\pi}} + O(d^{-\frac{1}{2}})$ for all $n \in \mathbb{N}$ and $d \to \infty$. In any dimension, we provide a precise interval containing the exact value, in 3D the expected length is between 1.4977 and 1.50007 [31].

This work was done in collaboration with Pedro Machado Manhães De Castro (Centro de Informática da Universidade Federal de Pernambuco).

6.4. Classical Computational Geometry and Graph Drawing

Participants: Olivier Devillers, Sylvain Lazard.

6.4.1. Monotone Simultaneous Path Embeddings in $\mathbb{R}^d$

We study the following problem: Given k paths that share the same vertex set, is there a simultaneous geometric embedding of these paths such that each individual drawing is monotone in some direction? We prove that for any dimension $d \geq 2$, there is a set of $d+1$ paths that does not admit a monotone simultaneous geometric embedding [21].

This work was done in collaboration with David Bremner (U. New Brunswick), Marc Glisse (Inria Datashape), Giuseppe Liotta (U. Perugia), Tamara Mchedlidze (Karlsruhe Institute for Technology), Sue Whitesides (U. Victoria), and Stephen Wismath (U. Lethbridge).

6.4.2. Analysis of Farthest Point Sampling for Approximating Geodesics in a Graph

A standard way to approximate the distance between two vertices p and q in a graph is to compute 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 yields an efficient computation of approximate distances between any two vertices. One standard method for choosing k sources 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 $\mathcal{F}_{\text{FPS}}$ 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 showed that $\mathcal{F}_{\text{FPS}}$ can be bounded in terms of the minimal value $\mathcal{F}^*$ of the stretch factor obtained using an optimal placement of k sources as $\mathcal{F}_{\text{FPS}} \leq 2r_e^2\mathcal{F}^* + 2r_e^2 + 8r_e + 1$, where r_e is the length ratio of longest edge over the shortest edge in the graph. We further showed that the factor r_e is not an artefact of the analysis by providing a class of graphs for which $\mathcal{F}_{\text{FPS}} \geq \frac{1}{2}r_e\mathcal{F}^*$ [18].

This work was done in collaboration with Pegah Kamousi (Université Libre de Bruxelles), Anil Maheshwari (Carleton University), and Stefanie Wuhrer (Inria Grenoble Rhône-Alpes).

6.4.3. Recognizing Shrinkable Complexes is NP-complete

We say that a simplicial complex is shrinkable if there exists a sequence of admissible edge contractions that reduces the complex to a single vertex. We prove that it is NP-complete to decide whether a (three-dimensional) simplicial complex is shrinkable. Along the way, we describe examples of contractible complexes which are not shrinkable [10].

This work was done in collaboration with Dominique Attali (CNRS, Grenoble) and Marc Glisse (Inria Datashape).

VERIDIS Project-Team

7. New Results

7.1. Automated and Interactive Theorem Proving

Participants: Gabor Alági, Haniel Barbosa, Jasmin Christian Blanchette, Martin Bromberger, Simon Cruanes, Mathias Fleury, Pascal Fontaine, Marek Košta, Stephan Merz, Martin Riener, Martin Strecker, Thomas Sturm, Marco Voigt, Uwe Waldmann, Daniel Wand, Christoph Weidenbach.

7.1.1. IsaFoL: Isabelle Formalization of Logic

Joint work with Heiko Becker (MPI-SWS Saarbrücken), Peter Lammich (TU München), Andrei Popescu (Middlesex University London), Anders Schlichtkrull (DTU Copenhagen), Dmitriy Traytel (ETH Zürich), and Jørgen Villadsen (DTU Copenhagen).

Researchers in automated reasoning spend a significant portion of their work time specifying logical calculi and proving metatheorems about them. These proofs are typically carried out with pen and paper, which is error-prone and can be tedious. As proof assistants are becoming easier to use, it makes sense to employ them.

In this spirit, we started an effort, called IsaFoL (Isabelle Formalization of Logic), that aims at developing libraries and methodology for formalizing modern research in the field, using the Isabelle/HOL proof assistant.[0] Our initial emphasis is on established results about propositional and first-order logic. In particular, we are formalizing large parts of Weidenbach's forthcoming textbook, tentatively called *Automated Reasoning—The Art of Generic Problem Solving*.

The objective of formalization work is not to eliminate paper proofs, but to complement them with rich formal companions. Formalizations help catch mistakes, whether superficial or deep, in specifications and theorems; they make it easy to experiment with changes or variants of concepts; and they help clarify concepts left vague on paper.

The repository contains six completed entries and three entries that are still in development. Notably:

- Mathias Fleury formalized a SAT solver framework with learn, forget, restart, and incrementality and published the result at a leading conference, together with Jasmin Blanchette and Christoph Weidenbach [25].
- Anders Schlichtkrull, remotely co-supervised by Jasmin Blanchette, formalized unordered first-order resolution in Isabelle and presented the result at ITP 2016 [37].
- Together with an intern, Jasmin Blanchette, Uwe Waldmann, and Daniel Wand formalized a generalization for the recursive path order and the transfinite Knuth-Bendix order to higher-order terms without λ-abstractions. The result is published in the Isabelle *Archive of Formal Proofs*.

7.1.2. Combination of Satisfiability Procedures

Joint work with Christophe Ringeissen from the PESTO project-team at Inria Nancy – Grand Est, and Paula Chocron at IIIA-CSIC, Bellaterra, Catalonia, Spain.

A satisfiability problem is often expressed in a combination of theories, and a natural approach consists in solving the problem by combining the satisfiability procedures available for the component theories. This is the purpose of the combination method introduced by Nelson and Oppen. However, in its initial presentation, the Nelson-Oppen combination method requires the theories to be signature-disjoint and stably infinite (to ensure the existence of an infinite model). The design of a generic combination method for non-disjoint unions of theories is clearly a hard task, but it is worth exploring simple non-disjoint combinations that appear frequently in verification. An example is the case of shared sets, where sets are represented by unary predicates. Another example is the case of bridging functions between data structures and a target theory (e.g., a fragment of arithmetic).

[0] https://bitbucket.org/jasmin_blanchette/isafol/wiki/Home

In 2015, we defined [42] a sound and complete combination procedure à la Nelson-Oppen for the theory of absolutely free data structures (including lists and trees) connected to another theory via bridging functions. This combination procedure has also been refined for standard interpretations. The resulting theory has a nice politeness property, enabling combinations with arbitrary decidable theories of elements. We also investigated [43] other theories amenable to similar combinations: this class includes the theory of equality, the theory of absolutely free data structures, and all the theories in between.

More recently, we have been improving the framework and unified both results. A new paper is in preparation.

7.1.3. Quantifier handling in SMT

Joint work with Andrew J. Reynolds, Univ. of Iowa, USA.

SMT solvers generally rely on various instantiation techniques to handle quantifiers. We are building a unifying framework for handling quantified formulas with equality and uninterpreted functions, such that the major instantiation techniques in SMT solving can be cast in that framework. It is based on the problem of E-ground (dis)unification, a variation of the classic Rigid E-unification problem. We introduced a sound and complete calculus to solve this problem in practice: Congruence Closure with Free Variables (CCFV). Experimental evaluations of implementations of CCFV in the state-of-the-art solver CVC4 and in the solver veriT exhibit improvements in the former and makes the latter competitive with state-of-the-art solvers in several benchmark libraries stemming from verification efforts. A publication is in preparation.

7.1.4. Non-linear arithmetic in SMT

In the context of the SMArT ANR-DFG (Satisfiability Modulo Arithmetic Theories) and KANASA projects (cf. sections 9.1 and 9.3), we study the theory, design techniques, and implement software to push forward the non-linear arithmetic (NLA) reasoning capabilities in SMT. This year, we designed a framework to combine interval constraint propagation with other decision procedures for NLA, with promising results. We are also currently studying integration of these procedures into combinations of theories. The ideas are validated within the veriT solver, together with code from the raSAT solver (from JAIST). An article is in preparation.

7.1.5. Encoding Set-Theoretic Formulas in First-Order Logic

Proof obligations that arise during the verification of high-level specifications of algorithms in languages such as (Event-)B and TLA$^+$ mix theories corresponding to sets, functions, arithmetic, tuples, and records. Finding encodings of such formulas in the input languages of automatic first-order provers (superposition-based provers or SMT solvers, which are based on multi-sorted first-order logic) is paramount for obtaining satisfactory levels of automation. We describe a method, based on a combination of injection of unsorted expressions into sorted languages, simplification by rewriting, and abstraction, that is the kernel of the SMT backend of the TLA$^+$ proof system (section 6.4). A paper describing our technique was presented at ABZ 2016 [31] and an extension of that article was invited for a special issue of Science of Computer Programming.

During the internship of Matthieu Lequesne, we experimented with an adaptation of the technique for constructing models of formulas in set theory, which could be useful for understanding why proof attempts fail. A prototype generating input for the Nunchaku model finder (section 6.1) allowed us to validate the idea for a core sublanguage of TLA$^+$.

7.1.6. Modal and Description Logics for Graph Transformations

Graph transformations are a research topic that is interesting in its own right, but with many possible applications ranging from the modification of pointer structures in imperative programs, through model transformations in model-driven engineering, to schema-preserving transformations of graph databases. Our particular focus is on verifying these transformations.

Modal logics and variants (such as description logics that are the basis for the web ontology language OWL) have turned out to be suitable specification formalisms because graph structures can typically be perceived as models of modal logics, but these logics suffer from some weaknesses when reasoning about transformations. The first aim of our work was therefore to identify and define sufficiently expressive modal logics, while retaining their pleasant properties, in particular decidability [30].

Our next aim is to implement practically useful proof methods. We have first concentrated on the more natural tableau proofs, with a verification of meta-theoretic properties of the calculi (such as termination) in the Isabelle proof assistant. We now turn to an investigation of encodings as satisfiability problems that can be handled with SAT and SMT solvers, with the hope to achieve a better performance.

7.1.7. Standard Models with Virtual Substitution

Joint work with A. Dolzmann from Leibniz-Zentrum für Informatik in Saarbrücken, Germany.

Extended quantifier elimination for the reals using virtual substitution methods have been successfully applied to various problems in science and engineering. Recently they have attracted attention also as theory solvers within SMT. Such solvers typically ask also for models in the satisfiable case. Models obtained with virtual substitution are in general obtained in certain non-archimedian extension fields of the reals with a corresponding expanded signature. Consequently, the obtained values for the variables include non-standard symbols such as positive infinitesimals and infinite values.

We introduce a complete post-processing procedure to convert our models, for fixed values of parameters, into real models [15]. We furthermore demonstrate the successful application of an implementation of our method within Redlog to a number of extended quantifier elimination problems from the scientific literature including computational geometry, motion planning, bifurcation analysis for models of genetic circuits and for mass action, and sizing of electrical networks. This solves a long-standing problem with the virtual substitution method, which had been explicitly criticized in the scientific literature.

7.1.8. Decidability of Fragments of Free First-Order Logic

We introduce a new decidable fragment of first-order logic with equality, the *Separated Fragment* (SF). It strictly generalizes two already well-known decidable fragments of first-order logic: the Bernays-Schönfinkel-Ramsey (BSR) Fragment and the Monadic Fragment. The defining principle is that universally and existentially quantified variables may not occur together in atoms. Thus, our classification neither rests on restrictions of quantifier prefixes (as in the BSR case) nor on restrictions on the arity of predicate symbols (as in the monadic case).

We show that SF exhibits the finite model property and derive a non-elementary upper bound on the computing time required for deciding satisfiability of SF sentences. For the subfragment of prenex sentences with the quantifier prefix $\exists^*\forall^*\exists^*$ the satisfiability problem is shown to be NEXPTIME-complete. Furthermore, we discuss how automated reasoning procedures can take advantage of our results [34].

Continuing the work presented in the initial publication, we further investigated the computational complexity of SF satisfiability. It nicely scales across the nondeterministic standard complexity classes, depending on joint occurrences of existentially quantified variables from $\exists^*$-blocks that are separated by nonempty $\forall^+$-blocks.

In another line of work, we relaxed the definition of SF, leading to an even larger fragment for which satisfiability is still decidable. In this fragment, variables of $\exists^*$-blocks and $\forall^+$-blocks may occur together in some atom if the respective quantifiers obey a certain order.

7.1.9. Ordered resolution with dismatching constraints

The identification and algorithmic exploration of decidable logic fragments is key to the automation of logics and to obtaining push-button verification technologies. We extend a well-known decidable fragment, linear monadic shallow Horn theories, with straight dismatching constraints, preserving decidability. Furthermore, we show that the restriction to Horn clauses is not needed. The fragment has various applications in security, automata theory and theorem proving [35].

7.1.10. Undecidable combinations of first-order logic with background theories

We show that the universal fragment of Presburger arithmetic augmented with a single uninterpreted predicate (or function) symbol is already undecidable. The result has immediate consequences for verification techniques that combine uninterpreted functions or predicate symbols with (fragments of) Presburger arithmetic. For example, data structures such as arrays can be viewed as a collection of uninterpreted functions that obey certain axioms.

Our result is a sharpening of previously known results. In particular, undecidability holds for a fragment with purely universal quantification: no quantifier alternation is necessary. While in this case the set of unsatisfiable sentences is still recursively enumerable, and in fact hierarchic superposition constitutes a semi-decision procedure, allowing for one quantifier alternation ($\exists\forall$ or $\forall\exists$) leads to a fragment in which neither the satisfiable sentences nor the unsatisfiable ones form a recursively-enumerable set. Hence, there cannot be any refutationally complete calculus for such a combined theory.

7.1.11. Novel techniques for linear arithmetic constraint solving

In [26], [27], we investigate new techniques for linear arithmetic constraint solving. They are based on the linear cube transformation, which allows us to efficiently determine whether a system of linear arithmetic constraints contains a hypercube of a given edge length.

Our first findings based on this transformation are two sound tests that find integer solutions for linear arithmetic constraints. While many complete methods search along the problem surface for a solution, these tests use cubes to explore the interior of the problems. The tests are especially efficient for constraints with a large number of integer solutions, e.g., those with infinite lattice width. Inside the SMT-LIB benchmarks, we have found almost one thousand problem instances with infinite lattice width. Experimental results confirm that our tests are superior on these instances compared to several state-of-the-art SMT solvers.

We also discovered that the linear cube transformation can be used to investigate the equalities implied by a system of linear arithmetic constraints. For this purpose, we developed a method that computes a basis for all implied equalities, i.e., a finite representation of all equalities implied by the linear arithmetic constraints. The equality basis can be used to decide whether a system of linear arithmetic constraints implies a given equality.

7.2. Formal Methods for Developing and Analyzing Algorithms and Systems

Participants: Noran Azmy, Gabriel Corona, Margaux Duroeulx, Marie Duflot-Kremer, Souad Kherroubi, Dominique Méry, Stephan Merz, Nicolas Schnepf, Christoph Weidenbach.

7.2.1. Making explicit domain knowledge in formal system development

Joint work with partners of the IMPEX project.

Modeling languages are concerned with providing techniques and tool support for the design, synthesis and analysis of the models resulting from a given modeling activity, and this activity is usually part of a system development model or process. These languages quite successfully focus on the analysis of the designed system, exploiting the semantic features of the underlying modeling language. These semantics are well understood by the system designers and/or the users of the modeling language, that is why we speak of implicit semantics.

In general, modeling languages are not equipped with resources, concepts or entities handling explicitly domain engineering features and characteristics (domain knowledge) in which the modeled systems evolve.

We posit that designers should explicitly handle the knowledge resulting from an analysis of the application domain, i.e. explicit semantics. As of today, making explicit the domain knowledge inside system design models does not follow any methodological rule; instead, features of domain knowledge are introduced in an ad-hoc way through types, constraints, profiles, etc.

Our claim [11] is that ontologies are good candidates for handling explicit domain knowledge. They define domain theories and provide resources for uniquely identifying concepts of domain knowledge. Therefore, allowing models to make references to ontologies is a modular solution for models to explicitly handle domain knowledge. Overcoming the absence of explicit semantics expression in the modeling languages used to specify systems models will increase the robustness of the designed system models. Indeed, references to the axioms and theorems resulting from the ontologies can be used to strengthen the properties of the designed models. The objective is to offer rigorous mechanisms for handling domain knowledge in design models. We also show how these mechanisms are set up in the cases of formal system models, both for static and dynamic aspects.

7.2.2. Incremental Development of Systems and Algorithms

Joint work with Andriamiarina, Manamiary Bruno, with Neeraj Kumar Singh from IRIT, Toulouse, with Rosemary Monahan, NUI Maynooth, Ireland, and with Zheng Cheng, LINA, Nantes.

The development of distributed algorithms and, more generally, of distributed systems, is a complex, delicate, and challenging process. The approach based on refinement applies a design methodology that starts from the most abstract model and leads, in an incremental way, to a distributed solution. The use of a proof assistant gives a formal guarantee on the conformance of each refinement with the model preceding it.

Our main results during 2016 are:

- An extension [18] for handling the verification of concurrent programs. In a second step, we show the importance of the concept of refinement, and how it can be used to found a methodology for designing concurrent programs using the coordination paradigm.
- A fully mechanized proof [36] of correctness of self-$*$ systems along with an interesting case study related to P2P-based self-healing protocols.
- We report on our progress in implementing a software development environment that integrates two formal software engineering techniques: program refinement as supported by Event-B, and program verification as supported by the Spec# programming system. We improve the usability of formal verification tools by providing a general framework for integrating these two approaches to software verification. We show how the two approaches, based respectively on correctness by construction and on post-hoc verification, can be used in a productive way. In [32], we focus on the final steps in this process where the final concrete specification is transformed into an executable algorithm. We present EB2RC, a plug-in for the RODIN platform that reads in an Event-B model and uses the control framework introduced during its refinement to generate a graphical representation of the executable algorithm. EB2RC also generates a recursive algorithm that is easily translated into executable code. We illustrate our technique through case studies and their analysis.

7.2.3. Verification of the Pastry routing protocol

In her PhD thesis, Noran Azmy develops a formal proof in TLA$^+$ of the routing protocol used in the Pastry protocol [51] for maintaining a distributed hash table over a peer-to-peer network. In a previous thesis [47], Tianxiang Lu had found problems with all published versions of the original protocol, introduced a variant of Pastry, and given a first correctness proof of that protocol, assuming that no node ever disconnects. Due to limitations of TLAPS at that time, Lu's proof relied on many unchecked assumptions on arithmetic and on the underlying data structures, and it was later discovered that several of these assumptions were not valid.

Noran Azmy simplified the proof by introducing intermediate abstractions that allowed her to avoid low-level arithmetic reasoning in the main proof steps, and she proved lemmas corresponding to those assumptions that were actually used in the proof. As a result, she obtained a complete machine-checked proof of Lu's variant of the Pastry protocol, still under the assumption that no node leaves the network. Moreover, a close analysis of the invariant used in her simplified proof revealed that the protocol could be simplified by leaving out the final "lease exchange" protocol. The results were published at ABZ 2016 [22], and an extended article was invited for publication in Science of Computer Programming.

7.2.4. Proof of Determinacy of PharOS

Joint work with Selma Azaiez and Matthieu Lemerre (CEA Saclay), and Damien Doligez (Inria Paris).

As the main contribution of our group to the ADN4SE project funded by PIA, in cooperation with colleagues from CEA LIST, we wrote a high-level TLA$^+$ specification of the real-time operating system PharOS [46] and proved its executions to be deterministic. Roughly speaking, determinacy means that the sequence of local states of any process during a computation does not depend on the order in which processes are scheduled. The proof assumes that no deadlines are missed (which in practice is ensured by schedulability analysis of the particular applications). This property greatly simplifies the analysis and verification of programs that are executed within PharOS. The results were published at ABZ 2016 [21].

7.2.5. Formal Verification of Chains of Security Functions

Joint work with Rémi Badonnel and Abdelkader Lahmadi of the Madynes research group of Inria Nancy.

During his Master's thesis, Nicolas Schnepf studied formal techniques for the automatic verification of chains of security functions in a setting of software-defined networks (SDN). Concretely, he defined an extension of the Pyretic language [44] taking into account the data plane of SDN controllers and implemented a translation of that extension to the input languages of the nuXmv model checker and of SMT solvers. The approach and its scalability was validated over crafted security chains, and a conference paper describing the results is under preparation. Nicolas Schnepf started a PhD thesis in October 2016, jointly supervised by members of the Madynes and VeriDis groups.

7.2.6. Auditing hybrid systems for compliance

There is a huge gap in complexity between the actual analysis of a complex hybrid system and the analysis of the eventual control needed for safe operation. For example, for the combustion process of an engine there is not even a closed formal model, but the eventual control can be represented in a finite domain language. Such a language can then in particular be used for run-time control of a system through an auditor, providing the detection of faulty components or compliance violations. We have studied the consequences of such an approach if applied to the overall life time process of a technical system [29].

SPHINX Project-Team

7. New Results

7.1. Analysis, control and stabilization of heterogeneous systems

Participant: Takéo Takahashi.

In [12], T. Takahashi (with D. Maity and M. Tucsnak, both from Institut de Mathématiques de Bordeaux, France) has considered a free boundary problem modeling the motion of a piston in a viscous gas. The gas-piston system fills a cylinder with fixed extremities, which possibly allow gas from the exterior to penetrate inside the cylinder. The gas is modeled by the 1D compressible Navier-Stokes system and the piston motion is described by the second Newton law. They prove the existence and uniqueness of global in time strong solutions. The main novelty brought in is that the case of nonhomogeneous boundary conditions is considered. Moreover, even for homogeneous boundary conditions, their results require less regularity of the initial data than those obtained in previous works.

In [32], T. Takahashi (with C. Lacave from Institut Fourier, Grenoble, France) has studied the motion of a single disk moving under the influence of a 2D viscous fluid. They deal with the asymptotic as the size of the solid tends to zero. If the density of the solid is independent of the size of the solid, the energy equality is not sufficient to obtain a uniform estimate for the solid velocity. This will be achieved thanks to the optimal $L^p - L^q$ decay estimates of the semigroup associated to the fluid-rigid body system and to a fixed point argument. Next, they deduce the convergence to the solution of the Navier-Stokes equations in $\mathbb{R}^2$.

In [7], T. Takahashi (with C. Bianchini (Dimai, Florence, Italy) and A. Henrot (IECL, Nancy, France)) has tackled a model for the shape of vesicles. In order to do this, they consider a shape optimization problem associated with a Willmore type energy in the plane. More precisely, they study a *Blaschke-Santaló diagram* involving the area, the perimeter and the elastic energy of planar convex bodies. Existence, regularity and geometric properties of solutions to this shape optimization problem are shown.

We have studied the self-propelled motions of a rigid body immersed in a viscous incompressible fluid which fills the exterior domain of the rigid body. The mechanism used by the body to reach the desired motion is modeled through a distribution of velocities at its boundary.

T. Takahashi (with J. San Martín (DIM, Santiago, Chile) and M. Tucsnak (Institut de Mathématiques de Bordeaux, France)) considers in [16] a class of swimmers of low Reynolds number, of prolate spheroidal shape, which can be seen as simplified models of ciliated microorganisms. Within this model, the form of the swimmer does not change, the propelling mechanism consisting in tangential displacements of the material points of swimmer's boundary. Using explicit formulas for the solution of the Stokes equations at the exterior of a translating prolate spheroid the governing equations reduce to a system of ODE's with the control acting in some of its coefficients (bilinear control system). The main theoretical result asserts the exact controllability of the prolate spheroidal swimmer. In the same geometrical situation, they define a concept of efficiency which reduces to the classical one in the case of a spherical swimmer and they consider the optimal control problem of maximizing this efficiency during a stroke. Moreover, they analyse the sensitivity of this efficiency with respect to the eccentricity of the considered spheroid. They provide semi-explicit formulas for the Stokes equations at the exterior of a prolate spheroid, with an arbitrary tangential velocity imposed on the fluid-solid interface. Finally, they use numerical optimization tools to investigate the dependence of the efficiency on the number of inputs and on the eccentricity of the spheroid. The "best" numerical result obtained yields an efficiency of 30.66% with 13 scalar inputs. In the limiting case of a sphere their best numerically obtained efficiency is of 30.4%, whereas the best computed efficiency previously reported in the literature was of 22%.

In [10], T. Takahashi (with T. Hishida (Nagoya University, Japan) and A.L. Silvestre (IST, Lisboa, Portugal)) tackles the stationary case. The fluid motion is modeled by the stationary Navier-Stokes system coupled with two relations for the balance of forces and torques. They prove that there exists a control allowing the rigid body to move with a prescribed rigid velocity provided the velocity is small enough. They also show that since the net force exerted by the fluid to the rigid body vanishes, we have a better summability of the fluid velocity than the classical summability result for the solutions of the stationary Navier-Stokes system in exterior domains.

7.2. Inverse problems for heterogeneous systems

Participants: David Dos Santos Ferreira, Alexandre Munnier, Karim Ramdani, Julie Valein, Jean-Claude Vivalda.

Many inverse problems (IP) appearing in fluid-structure interaction and wave propagation problems have been investigated in the team.

In [14], Munnier and Ramdani consider the 2D inverse problem of recovering the positions and the velocities of slowly moving small rigid disks in a bounded cavity filled with a perfect fluid. Using an integral formulation, they first derive an asymptotic expansion of the DtN map of the problem as the diameters of the disks tend to zero. Then, combining a suitable choice of exponential type data and the DORT method (French acronym for Diagonalization of the Time Reversal Operator), a reconstruction method for the unknown positions and velocities is proposed. Let us emphasize here that this reconstruction method uses in the context of fluid-structure interaction problems a method which is usually used for waves inverse scattering (the DORT method).

In [13], Munnier and Ramdani propose a new method to tackle a geometric inverse problem related to Calderón's inverse problem. More precisely, they propose an explicit reconstruction formula for the cavity inverse problem using conformal mapping. This formula is derived by combining two ingredients: a new factorization result of the DtN map and the so-called generalized Pólia-Szegö tensors of the cavity.

In [9], P. Caro (Department of Mathematics and Statistics, Helsinki, Finland), D. Dos Santos Ferreira and Alberto Ruiz (Instituto de Ciencias Matematicas, Madrid, Spain) obtained stability estimates for potentials in a Schrödinger equation in dimension higher than 3 from the associated Dirichlet-to-Neumann map with partial data. The estimates are of log-log type and represent a quantitative version of the uniqueness result of Kenig, Sjöstrand and Uhlmann. The proof is based on a reduction to a stability estimate on the attenuated geodesic ray transform on the hypersphere.

In [15], Ramdani, Tucsnak (Institut de Mathématiques de Bordeaux, France) and Valein tackle a state estimation problem for a system of infinite dimension arising in population dynamics (a linear model for age-structured populations with spatial diffusion). Assume the initial state to be unknown, the considered inverse problem is to estimate asymptotically on time the state of the system from a locally distributed observation in both age and space. This is done by designing a Luenberger observer for the system, taking advantage of the particular spectral structure of the problem (the system has a finite number of unstable eigenvalues).

In [2], Ammar (Faculté des Sciences de Sfax, Tunisia), Massaoud (Faculté des Sciences de Sfax, Tunisia) and Vivalda characterize the globally Lipschitz continuous systems defined on $\mathbb{R}^n$ whose observability is preserved under time sampling.

7.3. Numerical analysis and simulation of heterogeneous systems

Participants: Xavier Antoine, Mohamed El Bouajaji, Karim Ramdani, Qinglin Tang, Julie Valein, Chi-Ting Wu.

In optics, metamaterials (also known as negative or left-handed materials), have known a growing interest in the last two decades. These artificial composite materials exhibit the property of having negative dielectric permittivity and magnetic permeability in a certain range of frequency, leading hence to materials with negative refractive index and super lens effects. In [8], Bunoiu (IECL, Metz, France) and Ramdani consider a complex wave system involving such materials. More precisely, they consider a periodic homogenization problem involving two isotropic materials with conductivities of different signs: a classical material and a metamaterial (or negative material). Combining the $\mathbf{T}-$coercivity approach and the unfolding method for homogenization, they prove well-posedness results for the initial and the homogenized problems and obtain a convergence result, provided that the contrast between the two conductivities is large enough (in modulus).

In [18], Tucsnak (Institut de Mathématiques de Bordeaux, France), Valein and Wu study the numerical approximation of the solutions of a class of abstract parabolic time-optimal control problems with unbounded control operator. Our main results assert that, provided that the target is a closed ball centered at the origin and of positive radius, the optimal time and the optimal controls of the approximate time optimal problems converge (in appropriate norms) to the optimal time and to the optimal controls of the original problem. In order to prove our main theorem, we provide a nonsmooth data error estimate for abstract parabolic systems.

In [4], Antoine and Lorin (School of Mathematics and Statistics, Ottawa, and CRM, Montréal, Canada) analyze the convergence of optimized Schwarz domain decomposition methods for the simulation of the time-domain Schrödinger equation with high-order local transmission conditions.

In [5], Antoine, Tang and Zhang (WPI, Austria and IRMAR, France) develop some spectral methods for computing the ground states and dynamics of space fractional Gross-Pitaevskii equations arising in the modeling of fractional Bose-Einstein equations with long-range nonlinear interactions. In addition, we also state some existence and uniqueness properties for the ground states of such equations, and prove some dynamical laws.

In [6], Bao (Department of Mathematics, Singapore), Tang and Zhang (WPI, Austria and IRMAR, France) develop a new efficient and spectrally accurate numerical for computing the ground state and dynamics of dipolar Bose-Einstein condensates. They pay a particular attention to the computation of the nonlinear nonlocal interactions through the use of the nonuniform fast Fourier transform.

In [22], Antoine, Levitt (CERMICS, France) and Tang derive a highly accurate and efficient new numerical method for computing the ground states of the fast rotating Gross-Pitaevskii equation. The method is based on a preconditioned nonlinear conjugate gradient method which leads to a high gain compared to most recent approaches.

In [26], Bao (Department of Mathematics, Singapore), Cai (Department of mathematics Purdue University, USA and CSRC, Beijing, China), Jia (Department of Mathematics, Singapore), Tang develop a uniformly accurate multiscale time integrator in conjunction with a spectral method for computing the dynamics of the nonrelativistic Dirac equation. The same authors develop and compare, in [27], some new numerical methods for the simulation of the Dirac equation when the nonrelativistic regime is considered.

The article [17] is devoted to explain how the open finite element solver GetDDM works. The mathematical methods behind GetDDM are optimized Schwarz domain decomposition methods with well-designed transmission boundary conditions. GetDDM allows to solve large scale high frequency wave problems (e.g. acoustics, electromagnetism, elasticity problems) on large clusters. This papers explains through examples and scripts how GetDDM must be used. GetDDM is a result of a long term collaboration between Xavier Antoine and Christophe Geuzaine (University of Liège).

TOSCA Project-Team

6. New Results

6.1. Probabilistic numerical methods, stochastic modelling and applications

Participants: Mireille Bossy, Nicolas Champagnat, Madalina Deaconu, Coralie Fritsch, Pascal Helson, Benoît Henry, Kouadio Jean Claude Kouaho, Antoine Lejay, Radu Maftei, Sylvain Maire, Paolo Pigato, Alexandre Richard, Denis Talay, Etienne Tanré, Milica Tomasevic, Denis Villemonais.

6.1.1. Published works and preprints

- M. Bossy with H. Quinteros (UChile) studied the rate of convergence of a symmetrized version of the Milstein scheme applied to the solution of one dimensional CEV type processes. They prove a strong rate of convergence of order one, recovering the classical result of Milstein for SDEs with smooth diffusion coefficient. In contrast with other recent results, the proof does not relies on Lamperti transformation, and it can be applied to a wide class of drift functions. Some numerical experiments and comparison with various other schemes complement the theoretical analysis that also applies for the simple projected Milstein scheme with same convergence rate ([14] accepted for publication in Bernoulli Journal).
- M. Bossy, R. Maftei, J.-P. Minier and C. Profeta worked on numerically determining the rate of convergence of the weak error for the discretised Langevin system with specular reflection conditions. The article [29] presents a discretisation scheme and offers a conjecture for the rate of convergence of the bias produced. Numerically, these conjectures are confirmed for the specular reflection scheme but also for the absorption scheme, which models perfect agglomeration. The scheme numerically follows a linear decrease. The Richardson-Romberg extrapolation is also presented with a quadratic decrease.
- M. Bossy, A. Rousseau (LEMON Inria team), JĖspina, JṀorice and C. Paris (Inria Chile) studied the computation of the wind circulation around mills, using a Lagrangian stochastic approach. They present the SDM numerical method and numerical experiments in the case of non rotating and rotating actuator disc models in [13]. First, for validation purpose they compare some numerical experiments against wind tunnel measurements. Second, they perform numerical experiments at the atmospheric scale and present some features of the numerical method, in particular the computation of the probability distribution of the wind in the wake zone, as a byproduct of the fluid particle model and the associated PDF method.
- Together with M. Baar and A. Bovier (Univ. Bonn), N. Champagnat studied the adaptive dynamics of populations under the assumptions of large population, rare and small mutations [11]. In this work, the three limits are taken simultaneously, contrary to the classical approach, where the limits of large population and rare mutations are taken first, and next the limit of small mutations [57]. We therefore obtain the precise range of parameters under which these limits can be taken, and provide explicit biological conditions for which our approximation is valid.
- N. Champagnat and J. Claisse (Ecole Polytechnique) studied the ergodic and infinite horizon controls of discrete population dynamics with almost sure extinction in finite time. This can either correspond to control problems in favor of survival or of extinction, depending on the cost function. They have proved that these two problems are related to the QSD of the processes controled by Markov controls [36].
- N. Champagnat and C. Fritsch worked with F. Campillo (Inria Sophia-Antipolis, LEMON team) on the links between a branching process and an integro-differential equation of a growth-fragmentation-death model [15]. They proved that the two representations of the model lead to the same criteria of invasion of a population in a given environment. They also studied the variations of the principal eigenvalue (resp. the survival probability) of an integro-differential equation (resp. branching process) of growth-fragmentation models with respect to an environmental parameter in [35].

- N. Champagnat and D. Villemonais consider, for general absorbed Markov processes, the notion of quasi-stationary distributions (QSD), which is a stationary distribution conditionally on non-absorbtion, and the associated Q-process, degammad as the original Markov process conditioned to never be absorbed. They prove that, under the conditions of [17], in addition to the uniform exponential convergence of conditional distributions to a unique QSD and the uniform exponential ergodicity of the Q-process, one also has the uniform convergence of the law of the process contionned to survival up to time T, when $T \to +\infty$. This allows them to obtain conditional ergodic theorems [41].
- N. Champagnat, K. Coulibaly-Pasquier (Univ. Lorraine) and D. Villemonais obtained general criteria for existence, uniqueness and exponential convergence in total variation to QSD for multi-dimensional diffusions in a domain absorbed at its boundary [37]. These results improve and simplify the existing results and methods.
- Using a new method to compute the expectation of an integral with respect to a random measure, N. Champagnat and B. Henry obtained explicit formulas for the moments of the frequency spectrum in the general branching processes known as Splitting Trees, with neutral mutations and under the infinitely-many alleles model [16]. This allows them to obtain a law of large numbers for the frequency spectrum in the limit of large time.
- N. Champagnat and D. Villemonais obtained criteria for existence, uniqueness and exponential convergence in total variation to QSD for discrete population processes with unbounded absorption rate, using a non-linear Lyapunov criterion [38]. For logistic multidimensional birth and death processes absorbed when one coordinate gets extinct, they show that their criterion covers cases stronger intra-spectific competition than inter-specific competition.
- N. Champagnat and D. Villemonais extended their work [17] to general penalized processes, including time-inhomogeneous Markov processes with absorption and Markov processes in varying environments [40]. Their method allows to improve significantly the former results of [58], [59].
- M. Deaconu worked with L. Beznea and O. Lupaşcu (Bucharest, Romania) and analyzed the description of rupture phenomena like avalanches, by using fragmentation models. The main physical properties of the model are deeply involved in this study. They obtained new results on a stochastic equation of fragmentation and branching processes related to avalanches [12].
- M. Deaconu and S. Herrmann continued and completed the study of the simulation of hitting times of given boundaries for Bessel processes. These problems are of great interest in many application fields, such as finance and neurosciences. In a previous work, the authors introduced a new method for the simulation of hitting times for Bessel processes with integer dimension. The method was based mainly on explicit formula for the distribution of the hitting times and on the connexion between the Bessel process and the Euclidean norm of the Brownian motion. The method does not apply for a non-integer dimension. In this new work they consider the simulation of the hitting time of Bessel processes with non integer dimension and provide a new algorithm by using the additivity property of the laws of squared Bessel processes. Each simulation step is splitted in two parts: one is using the integer dimension case and the other one exhibits hitting time of a Bessel process starting from zero [20].
- M. Deaconu and S. Herrmann studied the Initial-Boundary Value Problem for the heat equation and solved it by using a new algorithm based on a random walk on heat balls [44]. Even if it represents a sophisticated and challenging generalization of the Walk on Spheres (WOS) algorithm introduced to solve the Dirichlet problem for Laplace's equation, its implementation is rather easy. The definition of the random walk is based on a new mean value formula for the heat equation. The convergence results and numerical examples allow to emphasize the efficiency and accuracy of the algorithm.
- M. Deaconu, B. Dumortier and E. Vincent (EPI MULTISPEECH are working with the Venathec SAS on the acoustic control of wind farms. They constructed a new approach to control wind farms based on real-time source separation. They expressed the problem as a non-linear knapsack problem and solve it using an efficient branch-and-bound algorithm that converges asymptotically to the global

optimum. The algorithm is initialised with a greedy heuristic that iteratively downgrades the turbines with the best acoustical to electricity loss ratio. The solution is then regammad using a depth-first search strategy and a bounding stage based on a continuous relaxation problem solved with an adapted gradient algorithm. The results are evaluated using data from 28 real wind farms [46].

- C. Fritsch and B. Cloez (INRA, Montpellier) proved central limit theorems for chemostat models in finite and infinite dimensions in [42]. From these theorems, they obtianed gaussian approximations of individual-based models and made a numerical analysis for the model in finite dimension in order to discuss the validity of these approximations in different contexts.
- Together with R. Azaïs (BIGS Inria team) and A. Genadot (Univ. Bordeaux), B. Henry studied an estimation problem for a forest of size-constrained Galton-Watson trees [31]. Using the asymptotic behavior of the Harris contour process, they constructed estimators for the inverse standard deviation of the birth distribution. In addition to the theoretical convergence results obtained in this work, they used the method to study the evolution of Wikipedia webpages in order, for instance, to detect vandalism.
- In [49], B. Henry showed a central limit theorem for the population counting process of a supercritical Splitting Tree in the limit of large time. Thanks to the results of [16], he also obtained a central limit theorem for the frequency spectrum of Splitting Trees with neutral mutations and under the infinitely-many alleles model.
- In collaboration with Laure Coutin, A. Lejay have studied the sensitivity of solution of rough differential equations with respect to their parameters using a Banach space version of the implicit function theorem. This result unifies and extends all the similar results on the subject [43].
- A. Lejay have studied the parametric estimation of the bias coefficient of skew random walk, as a toy model for the problem of estimation of the parameter of the Skew Brownian motion [50].
- P. Pigato has continued with V. Bally (Univ. Marne-la-Vallée) and L. Caramellino (Univ. Roma Tor Vergata) his PhD work on the regularity of diffusions under Hörmander-type conditions [32], [33].
- A. Richard and D. Talay ended their work on the sensitivity of the first hitting time of fractional SDEs, when $H > \frac{1}{2}$ [54]. This study is being completed by the rough case $H \in (\frac{1}{4}, \frac{1}{2}]$. In relation to fractional SDEs, another short work on accurate Gaussian-like upper bounds on density of one-dimensional fractional SDEs is almost finished.
- In [21], S. Herrmann and E. Tanré propose a new algorithm to simulate the first hitting times of a deterministic continuous function by a one-dimensional Brownian motion. They give explicit rate of convergence of the algorithm.
- E. Tanré and Pierre Guiraud (Univ. of Valparaiso) have studied the synchronization in a model of neural network with noise. Using a large deviation principle, they prove the stability of the synchronized state under stochastic perturbations. They also give a lower bound on the probability of synchronization for networks which are not initially synchronized. This bound shows the robustness of the emergence of synchronization in presence of small stochastic perturbations. [48]
- V. Reutenauer and E. Tanré have worked on extensions of the exact simulation algorithm introduced by Beskos et al. [56]. They propose an unbiased algorithm to approximate the two first derivatives with respect to the initial condition x of quantities with the form $\mathbb{E}\Psi(X_T^x)$, where X is a one-dimensional diffusion process and Ψ any test-function. They also propose an efficient modification of Beskos et al. algorithm. [53]
- During his internship supervised by E. Tanré, A. Papic worked on multi scales generator of Markov processes. He presents a method to approximate such processes with an application in neuroscience for noisy Hodgkin-Huxley model [52].
- D. Villemonais worked with P. Del Moral (Univ. Sydney) on the conditional ergodicity of time inhomogeneous diffusion processes [45]. They proved that, conditionally on non extinction, an elliptic time-inhomogeneous diffusion process forgets its initial distribution exponentially fast. An interacting particle scheme to numerically approximate the conditional distribution is also provided.

- D. Villemonais worked with his Research Project student William Oçafrain (École des Mines de Nancy) on an original mean-field particle system [51]. They proved that the mean-field particle system converges in full generality toward the distribution of a conditioned Markov process, with applications to the approximation of the quasi-stationary distribution of piecewise deterministic Markov processes.

6.1.2. Other works in progress

- M. Bossy and R. Maftei are working on determining the rate of convergence of the weak error of a discretised scheme for the Langevin system with specular boundary reflection on the position. The velocity process allows for a bounded and smooth drift. In order to determine the optimal rate of convergence, the regularity of the associated PDE is required and also regularity results for the derivative of flow of the process w.r.t. the initial conditions.
- N. Champagnat and B. Henry are studying limits of small mutations in Lokta-Volterra type PDEs of population dynamics using probabilistic representations and large deviations.
- N. Champagnat, C. Fritsch and S. Billiard (Univ. Lille) are working on food web modeling.
- M. Deaconu and S. Herrmann are working on numerical approaches for hitting times of general stochastic differential equations.
- M. Deaconu, O. Lupaşcu and L. Beznea (Bucharest, Romania) worked on the numerical scheme for the simulation of an avalanche by using the fragmentation model. This work will be submitted soon.
- M. Deaconu, B. Dumortier and E. Vincent (EPI MULTISPEECH) work on handling uncertainties in the model of acoustic control of wind farms they develop, in order to design a stochastic algorithm based on filtering methods. They will submit another article to IEEE transaction on sustainable energy.
- C. Fritsch is working with F. Campillo (Inria Sophia-Antipolis, LEMON team) and O. Ovaskainen (Univ. Helsinki) about a numerical approach to determine mutant invasion fitness and evolutionary singular strategies using branching processes and integro-differential models. They illustrate this method with a mass-structured individual-based chemostat model.
- C. Fritsch is working with A. Gégout-Petit (Univ. Lorraine and sc Bigs team), B. Marçais (INRA, Nancy) and M. Grosdidier (INRA, Nancy) on a statistical analysis of a *Chalara fraxinea* model.
- B. Cloez (INRA Montpellier) and B. Henry started a work on the asymptotic behavior of splitting trees in random environment. In addition, they begin the study of scaling limits of splitting trees in varying environment.
- Together with Ernesto Mordecki (Universidad de la República, Uruguay) and Soledad Torres (Universidad de Valparaíso), A. Lejay is working on the estimation of the parameter of the Skew Brownian motion.
- A. Lejay, and P. Pigato are working on the estimation of the parameters of diffusions with discontinuous coefficients, with application to financial data.
- Together with Laure Coutin and Antoine Brault (Université Toulouse 3), A. Lejay is studying application of the Trotter-Kato theorem in the context of rough differential equations, in order to solve some Stochastic Partial Differential Equations.
- A. Lejay and H. Mardones are working on a Monte Carlo simulation of the Navier-Stokes equations which is based on a novel probabilistic representation due to F. Delbaen *et al.* [60].
- In a research visit to Chile, P. Pigato has worked with R. Rebolledo and S. Torres on the estimation of parameters of diffusions from the occupation time and the local time of the process.
- Together with Laure Coutin and Antoine Brault (Université Toulouse 3), A. Lejay is studying application of the Trotter-Kato theorem in the context of rough differential equations, in order to solve some Stochastic Partial Differential Equations.

- C. Graham (École Polytechnique) and D. Talay are polishing thesecond volume of their series on Mathematical Foundation of Stochastic Simulation to be published by Springer.
- In collaboration with J. Bion-Nadal (CNRS and École Polytechnique) D. Talay ended the first paper on an innovating calibration method for stochastic models belonging to a family of solutions to martingale problems. The methodology involves the introduction of a new Wasserstein-type distance and stochastic control problems. The manuscript is being finished.
- Motivated by the study of systems of non-linear PDE's by stochastic methods, M. Tomasevic and D. Talay studied a system of differential equations interacting through a singular kernel, depending on all the past of the solutions. They have proved the existence of a solution in the space of Lipschitz functions in short time interval and performed numerical simulations. In the same time, they studied a non-linear stochastic differential equation whose drift is given as a convolution of a singular kernel with the unknown one dimensional time marginals both in time and space. Combining probabilistic and PDE techniques, they are currently finishing the proof of the existence and uniqueness of a weak solution up to an arbitrary finite time horizon. Properties of the corresponding particle system (well-posedness and propagation of chaos) are also studied.
- A. Richard and E. Tanré's work with Patricio Orio (CINV, Chile) on the modelling and measurement of long-range dependence in neuronal spike trains is almost completed. They exhibit evidence of memory effect in genuine neuronal data and compared their fractional integrate-and-fire model with the existing Markovian models. A. Richard and E. Tanré are still working on the convergence of the statistical estimator that measures this phenomenon.
- A. Richard, E. Tanré are working with S. Torres (Universidad de Valparaíso, Chile) on a one-dimensional fractional SDE reflected on the line. The existence and uniqueness of this process is known in the case $H > \frac{1}{2}$. In addition, they have proved the existence of a penalization scheme (suited to numerical approximation) to approach this object. When $H \in (\frac{1}{4}, \frac{1}{2})$, they have proved the existence in the elliptic case and are working on the question of uniqueness and on the relaxation of ellipticity.
- During his internship supervised by E. Tanré and Romain Veltz (MATHNEURO team), Pascal Helson studied numerically and theoretically a model of spiking neurons in interaction with plasticity. He showed that a simple model without plasticity could reproduce biological phenomena such as oscillations. In order to add plasticity, he enabled synaptic weights to evolve in a probabilistic way, in agreement with biological laws. He is now studying the convergence of this model and the existence of separable time scales, which is part of his thesis.
- D. Villemonais started a collaboration with Camille Coron (Univ. Paris Sud) and Sylvie Méléard (École Polytechnioque) on the question of simultaneous/non-simultaneous extinction of traits in a structured population
- D. Villemonais currently works on the computation of lower bounds for the Wasserstein curvature of interacting particle systems.
- D. Villemonais started a collaboration with Éliane Albuisson (CHRU of Nancy), Athanase Benetos (CHRU of Nancy), Simon Toupance (CHRU of Nancy), Daphné Germain (École des Mines de Nancy) and Anne Gégout-Petit (Inria BIGS team). The aim of this collaboration is to conduct a statistical study of the time evolution of telomere's length in human cells.

6.2. Financial Mathematics

Participants: Maxime Bonelli, Mireille Bossy, Nicolas Champagnat, Madalina Deaconu, Antoine Lejay, Sylvain Maire, Khaled Salhi, Denis Talay, Etienne Tanré.

6.2.1. Published works and preprints

- K. Salhi, M. Deaconu, A. Lejay and N. Champagnat worked with N. Navet (University of Luxembourg) [28]. They construct a regime switching model for the univariate Value-at-Risk estimation. Extreme value theory (EVT) and hidden Markov models (HMM) are combined to estimate a hybrid model that takes volatility clustering into account. In the first stage, HMM is used to classify data in crisis and steady periods, while in the second stage, EVT is applied to the previously classified data to rub out the delay between regime switching and their detection. This new model is applied to prices of numerous stocks exchanged on NYSE Euronext Paris over the period 2001-2011. The relative performance of the regime switching model is benchmarked against other well-known modeling techniques, such as stable, power laws and GARCH models.
- K. Salhi wrote a survey paper about option pricing and risk management under exponential Lévy models [55]. He detailed some notions that are not well explained in the literature and he proposed new trends in the risk management of derivatives.
- In [26], D. Talay, E. Tanré, Christophe Michel (CA-CIB) and Victor Reutenauer (fotonower) have studied 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.

6.2.2. Other works in progress

- M. Bossy and M. Bonelli (Koris International) are working on the optimal portfolio investment problem under the drawdown constraint that the wealth process never falls below a fixed fraction of its running maximum. They derive optimal allocation programs by solving numerically the Hamilton-Jacobi-Bellman equation that characterizes the finite horizon expected utility maximization problem, for investors with power utility as well as S-shape utility. Using numerical experiments they show that implementing the drawdown constraint can be gainful in optimal portfolios for the power utility, for some market configurations and investment horizons. However, their study reveals different results in a prospect theory context.
- When the underlying asset price is given by a exponential Lévy model, the market is almost incomplete. Under this hypothesis, K. Salhi works on derivatives hedging under a budget constraint on the initial capital. He considers, as criterion of optimization, the CVaR of the terminal hedging risk. First, he rewrites the problem an optimisation problem on the random fraction of the payoff that permits to respect the budget constraint. Then, he approximates the problem by relaxing the constraint and considering only a specific equivalent martingale measure. This approximate problem is solved using Neyman-Pearson's Lemma and, in the case of European options, a numerical valuation of the approximated minimal CVaR based on fast Fourier transform. The article will be submitted soon.

BIGS Project-Team

7. New Results

7.1. Stochastic modeling

7.1.1. Spatial and spatio-temporal modeling

Participants: A. Gégout-Petit
External collaborators: Y. Cao, S. Li, L. Guerin-Dubrana (Inra Bordeaux)

In the framework of a collaboration with INRA Bordeaux about the esca-illness of vines, Anne Gégout-Petit with Shuxian Li developed different spatial models and spatio-temporal models for different purposes: (1) study the distribution and the dynamics of esca vines in order to tackle the aggregation and the potential spread of the illness (2) propose a spatio-temporal model in order to capture the dynamics of cases and measure the effects of environmental covariates. For purpose (1), we propose different test based on the join count statistics, a paper is accepted for publication [5]. We also developped a two-step centered autologistic model for the study of the dynamic of propagation. This work has been presented as invited paper in [20] and is in preparation for publication.

7.1.2. Modelisation of response to chemotherapy in gliomas

Participant: S. Wantz-Mézières
External collaborator: J.-M. Moureaux, Y. Gaudeau, M. Ben Abdallah, M. Ouqamra (CRAN, Université de Lorraine), L. Taillandier, M. Blonski (CHU Nancy)
The collaboration with neurologists (CHU Nancy) and automaticians (CRAN) has carried on this year and led to the PhD presentation of M. Ben Abdallah, on December 12, 2016 [17], [16]. We completed the modeling approach by a data analysis one. In the framework of a master 2 project, supervised and non supervised methods have confirmed our results on our local data base. This encourages us to continue our work in extending the data base via a collaboration with Montpellier CHU. Our perspectives are to validate multi-factor models, including biological and anatomopathological factors, and to design a decision-aid tool for praticians.

7.1.3. Time-changed extremal process as a random sup measure

Participant: Céline Lacaux
External collaborator: Gennady Samorodnistky

In extreme value theory, one of the major topics is the study of the limiting behavior of the partial maxima of a stationary sequence. When this sequence is i.i.d., the unique limiting process is well-known and called the extremal process. Considering a long memory stable sequence, the limiting process is obtained as a simple power time change extremal process. Céline Lacaux and Gennady Samorodnistky have proved that this limiting process can also be interpreted as a restriction of a self-affine random sup measure. In addition, they have established that this random measure arises as a limit of the partial maxima of the same long memory stable sequence, but in a different space. Their results open the way to propose new self-similar processes with stationary max-increments.

7.1.4. Fast and Exact synthesis of some operator scaling Gaussian random fields

Participant: Céline Lacaux
External collaborator: Hermine Biermé

Operator scaling Gaussian random fields, as anisotropic generalizations of self-similar fields, know an increasing interest in the literature. Up to now, such models were only defined through stochastic integrals, without knowing explicitly their covariance functions. In link with this misunderstanding, one of the drawbacks is that no exact method of simulation has been proposed. In view to fill this lack, Hermine Biermé and Céline Lacaux have recently exhibit explicit covariance functions, as anisotropic generalizations of fractional Brownian fields ones. This allows them to propose a fast and exact method to synthetise an operator scaling Gaussian random fields with such a covariance function. Their algorithm is based on the famous circulant embedding matrix method. This is a first piece of work to popularized operator scaling Gaussian random field in anisotropic spatial data modeling.

7.1.5. DNA sequences analysis

Participants: P. Vallois

External collaborators: A. Lagnoux and S. Mercier (Toulouse)

In an article accepted at Bioinformatics, the goal is to illustrate different results on the local score distribution assuming an i.i.d. model, especially the one based on the pair (local score,length) and the one on the local score position. We measure with statistical tests how different approximations of the local score distribution fit to simulated sequences. In particular, our simulations show that the popular Karlin & Altschul approximation is not accurate in a wide range of situations. We add to the local score the length of the segment that realises it and we study the induced changes with numerical simulations. We also study specificity and sensitivity for the different methods. We introduce a new one dimensional statistic which is a function of H_n^* and L_n^* and we test its distribution. Finally, we estimate the probability that $H_n^* = H_n$ in different settings.

7.2. Estimation and control for stochastic processes

7.2.1. Piecewise-deterministic Markov processes

Participants: Romain Azaïs, Florian Bouguet, Anne Gégout-Petit, Florine Greciet, Aurélie Muller-Gueudin

External participants: Michel Benaïm (Université de Neuchâtel), Bertrand Cloez (Inra-SupAgro MISTEA), Alexandre Genadot (Inria CQFD, Université de Bordeaux)

A piecewise-deterministic Markov process is a stochastic process whose behavior is governed by an ordinary differential equation punctuated by random jumps occurring at random times. This class of stochastic processes offers a wide range of applications, especially in biology (kinetic diatery exposure model and growth of bacteria for example). BIGS' members mainly work on statistical inference techniques for these stochastic processes [2], [29], which is an essential step to build relevant application models. We also investigate the probabilistic properties of these processes [32], [31] as well as the application in reliability to crack growth in some alloy in the industrial context of the PhD thesis of Florine Greciet with SAFRAN Aircraft Engines [33].

In a preprint recently accepted for publication in Electronic Journal of Statistics [2], we focus on the nonparametric estimation problem of the jump rate for piecewise-deterministic Markov processes observed within a long time interval under an ergodicity condition. More precisely, we introduce an uncountable class (indexed by the deterministic flow) of recursive kernel estimates of the jump rate and we establish their strong pointwise consistency as well as their asymptotic normality. In addition, we propose to choose among this class the estimator with the minimal variance, which is unfortunately unknown and thus remains to be estimated. We also discuss the choice of the bandwidth parameters by cross-validation methods. In [29], we state a new characterization of the jump rate when the transition kernel only charges a discrete subset of the state space. We deduce from this result a competitive nonparametric technique for estimating this feature of interest. We state the uniform convergence in probability of the estimator. Both the methodologies have been illustrated on numerical examples and real data.

The article [32] deals with a class of conservative growth-fragmentation equations with a deterministic viewpoint. With the help of Foster-Lyapunov criteria, we study the long-time behavior of some associated piecewise-deterministic Markov process, which represents a typical individual following the dynamics of the equation. If the growth and the fragmentation are balanced, it is possible to provide existence and unicity for the stationary distribution on the process, as well as precise bounds for its tails of distributions in the neighborhoods of both 0 and $+\infty$. Our probabilistic results are systematically compared to estimates already obtained with deterministic methods.

In [31], we are interested by the long-time behavior of inhomogeneous-time Markov chains. We put forward an original and unified approach to relate some of their asymptotic properties (stationary distribution, speed of convergence, ...) to the ones of an auxiliary homogeneous-time Markov process. Such results are close to traditional functional limit theorems, but our method differs from the standard “Tightness/Identification” argument; it is based on the notion of asymptotic pseudotrajectories on the space of probability measures. We recover classical results, such as normalized bandit algorithms converging to a piecewise-deterministic Markov process, or weighted random walks or decreasing step Euler schemes approximated with solutions of stochastic differential equations.

7.2.2. Statistics of Markov chains

Participant: Romain Azaïs

External participants: Bernard Delyon (Université Rennes 1), François Portier (Télécom ParisTech)

Suppose that a mobile sensor describes a Markovian trajectory in the ambient space. At each time the sensor measures an attribute of interest, e.g., the temperature. Using only the location history of the sensor and the associated measurements, the aim of the paper [27] is to estimate the average value of the attribute over the space. In contrast to classical probabilistic integration methods, e.g., Monte Carlo, the proposed approach does not require any knowledge on the distribution of the sensor trajectory. Probabilistic bounds on the convergence rates of the estimator are established. These rates are better than the traditional “root n”-rate, where n is the sample size, attached to other probabilistic integration methods. For finite sample sizes, the good behaviour of the procedure is demonstrated through simulations and an application to the evaluation of the average temperature of oceans is considered.

7.2.3. Realtime Tracking of the Photobleaching Trajectory during Photodynamic Therapy

Participant: T. Bastogne

Photodynamic therapy (PDT) is an alternative treatment for cancer that involves the administration of a photosensitizing agent, which is activated by light at a specific wavelength. This illumination causes after a sequence of photoreactions, the production of reactive oxygen species responsible for the death of the tumor cells but also the degradation of the photosensitizing agent, which then loose the fluorescence properties. The phenomenon is commonly known as photobleaching process and can be considered as a therapy efficiency indicator. In [8], we present the design and validation of a real time controller able to track a preset photobleaching trajectory by modulating the light impulses width during the treatment sessions. This innovative solution was validated by in vivo experiments that have shown a significantly improvement of reproducibility of the inter-individual photobleaching kinetic. We believe that this approach could lead to personalized photodynamic therapy modalities in the near future.

7.2.4. Stochastic simulation and design of numerical experiments for the prediction of nanoparticles/X-ray interactions in radiotherapy.

Participant: T. Bastogne

The increase of computational environments dedicated to the simulation of nanoparticles (NP)-X-Rays interactions has opened new perspectives in computer-aided-design of nanostructured materials for biomedical applications. Several published studies have shown a crucial need of standardization of these numerical simulations [92]. That is why, we proposed to perform a robustness multivariate analysis in [8]. A gold nanoparticle (GNP) of 100 nm diameter was selected as a standard nano-system activated by a X-ray source placed just below the NP. Two response variables were examined: the dose enhancement in seven different spatial regions of interest around the NP and the duration of the experiments. 9 factors were pre-identified as potentially critical. A Plackett-Burman design of numerical experiments was applied to estimate and test the effects of each simulation factors on the examined responses. Four factors: the working volume, the spatial resolution, the spatial cutoff and the computational mode (parallelization) do not significantly affect the dose deposition results and none except the last one may reduce the computational duration. The energy cutoff may cause significant variations of the dose enhancement in some specific regions of interest: the higher the cutoff, the closer the secondary particles will stop from the GNP. By contrast, the Auger effect as well as the choice of the physical medium and the fluence level clearly appear as critical simulation parameters. Consequently, these four factors may be compulsory examined before comparing and interpreting any simulation results coming from different simulation sessions.

In [9], we address the prediction issue of organometallic nanoparticles (NPs)-based radiosensitization enhancement. The goal was to carry out computational experiments to quickly identify efficient nanostructures and then to preferentially select the most promising ones for the subsequent in vivo studies. To this aim, this interdisciplinary article introduces a new theoretical Monte Carlo computational ranking method and tests it using 3 different organometallic NPs in terms of size and composition. While the ranking predicted in a classical theoretical scenario did not fit the reference results at all, in contrast, we showed for the first time how our accelerated in silico virtual screening method, based on basic in vitro experimental data (which takes into account the NPs cell biodistribution), was able to predict a relevant ranking in accordance with in vitro clonogenic efficiency. This corroborates the pertinence of such a prior ranking method that could speed up the preclinical development of NPs in radiation therapy.

This in-silico approach was tested in [25] to screen radiosensitizing nanoparticles and the results have been validated by in vitro assays.

7.2.5. *Complexity analysis of Policy Iteration*

Participant: Bruno Scherrer

Given a Markov Decision Process (MDP) with n states and a total number m of actions, we study in [10] the number of iterations needed by Policy Iteration (PI) algorithms to converge to the optimal γ-discounted 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 $O\left(\frac{m}{1-\gamma}\log\left(\frac{1}{1-\gamma}\right)\right)$ iterations, improving by a factor $O(\log n)$ a result by Hansen et al., while Simplex-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 Ye. Under some structural properties of the MDP, we then consider bounds that are independent of the discount factor γ: quantities of interest are bounds τ_t and τ_r—uniform on all states and policies—respectively on the *expected time spent in transient states* and *the inverse of the frequency of visits in recurrent states* given that the process starts from the uniform distribution. Indeed, we show that Simplex-PI terminates after at most $\widetilde{O}\left(n^3m^2\tau_t\tau_r\right)$ iterations. This extends a recent result for deterministic MDPs by Post & Ye, in which $\tau_t \leq 1$ and $\tau_r \leq n$; in particular it shows that Simplex-PI is strongly polynomial for a much larger class of MDPs. 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 both Howard's PI and Simplex-PI terminate after at most $\widetilde{O}(m(n^2\tau_t + n\tau_r))$ iterations.

7.2.6. *Approximate Dynamic Programming for Markov Games*

Participant: Bruno Scherrer

We have made two contributions to the analysis of Approximate Dynamic Programming algorithms for Markov Games.

First, we extend in [21] several non-stationary Reinforcement Learning (RL) algorithms and their theoretical guarantees to the case of discounted zero-sum Markov Games (MGs). As in the case of Markov Decision Processes (MDPs), non-stationary algorithms are shown to exhibit better performance bounds compared to their stationary counterparts. The obtained bounds are generically composed of three terms: 1) a dependency over gamma (discount factor), 2) a concentrability coefficient and 3) a propagation error term. This error, depending on the algorithm, can be caused by a regression step, a policy evaluation step or a best-response evaluation step. As a second contribution, we empirically demonstrate, on generic MGs (called Garnets), that non-stationary algorithms outperform their stationary counterparts. In addition, it is shown that their performance mostly depends on the nature of the propagation error. Indeed, algorithms where the error is due to the evaluation of a best-response are penalized (even if they exhibit better concentrability coefficients and dependencies on gamma) compared to those suffering from a regression error.

Furthermore, we report in [22] theoretical and empirical investigations on the use of quasi-Newton methods to minimize the Optimal Bellman Residual (OBR) of zero-sum two-player Markov Games. First, it reveals that state-of-the-art algorithms can be derived by the direct application of Newton's method to different norms of the OBR. More precisely, when applied to the norm of the OBR, Newton's method results in the Bellman Residual Minimization Policy Iteration (BRMPI) and, when applied to the norm of the Projected OBR (POBR), it results into the standard Least Squares Policy Iteration (LSPI) algorithm. Consequently, new algorithms are proposed, making use of quasi-Newton methods to minimize the OBR and the POBR so as to take benefit of enhanced empirical performances at low cost. Indeed, using a quasi-Newton method approach introduces slight modifications in term of coding of LSPI and BRMPI but improves significantly both the stability and the performance of those algorithms. These phenomena are illustrated on an experiment conducted on artificially constructed games called Garnets.

7.3. Algorithms and estimation for graph data

7.3.1. Modelisation of networks of multiagent systems

Participants: Aurélie Muller-Gueudin

We relate here a collaboration with researchers in Automatic in Nancy (CRAN).

We consider here networks, modeled as a graph with nodes and edges representing the agents and their interconnections, respectively. The connectivity of the network, persistence of links and interactions reciprocity influence the convergence speed towards a consensus.

The problem of consensus or synchronization is motivated by different applications as communication networks, power and transport grids, decentralized computing networks, and social or biological networks.

We then consider networks of interconnected dynamical systems, called agents, that are partitioned into several clusters. Most of the agents can only update their state in a continuous way using only inner-cluster agent states. On top of this, few agents also have the peculiarity to rarely update their states in a discrete way by reseting it using states from agents outside their clusters. In social networks, the opinion of each individual evolves by taking into account the opinions of the members belonging to its community. Nevertheless, one or several individuals can change its opinion by interacting with individuals outside its community. These inter-cluster interactions can be seen as resets of the opinions. This leads us to a network dynamics that is expressed in term of reset systems. We suppose that the reset instants arrive stochastically following a Poisson renewal process.

We have an accepted paper in the journal IEEE Transactions on Automatic Control [6].

7.3.2. Compression and analysis of trees

Participant: Romain Azaïs

External participants: Jean-Baptiste Durand (ENSIMAG, Inria MISTIS), Christophe Godin (Inria Virtual Plants), Benoît Henry (Inria TOSCA puis Madynes), Alexandre Genadot (Université de Bordeaux, Inria CQFD)

Tree-structured data naturally appear in various fields, particularly in biology where plants and blood vessels may be described by trees, but also in computer science because XML documents form a tree structure. Among trees, the class of self-nested trees presents remarkable compression properties because of the systematic repetition of subtrees in their structure. In a recent preprint [28], we provide a better combinatorial characterization of this specific family of trees. We show that self-nested trees may be considered as a good approximation class of unordered trees. In addition, we compare our approximation algorithms with a competitive approach of the literature on a simulated dataset. On the other hand, the paper [30] is devoted to the estimation of the relative scale of ordered trees that share the same layout. The theoretical study is achieved for the stochastic model of conditioned Galton-Watson trees. New estimators are introduced and their consistency is stated. A comparison is made with an existing approach of the literature. A simulation study shows the good behavior of our procedure on finite-sample sizes. An application to the analysis of revisions of Wikipedia articles is also considered through real data.

7.4. Regression and machine learning

7.4.1. Aggregated methods for covariates selection in high-dimensional data under dependence

Participants: A. Gégout-Petit, A. Muller-Gueudin, Y. Shi
External collaborators: B. Bastien (Transgene, Strasbourg)

In the purpose to select factors linked to the efficiency of a treatment in the context of high dimension (about 100.000 covariates), we have developed a new methodology to select and rank covariates associated to a variable of interest in a context of high-dimensional data under dependence but few observations. The methodology imbricates successively rough selection, clustering of variables, decorrelation of variables using Factor Latent Analysis, selection using aggregation of adapted methods and finally ranking through bootstrap replications. Simulations study shows the interest of the decorrelation inside the different clusters of covariates. The methodology was applied to select covariates among genomics, proteomics covariates linked to the success of a immunotherapy treatment for the lung cancer. A paper on the subject is in preparation.

7.4.2. Clustering of the values of a response variable and simultaneous covariate selection using a stepwise algorithm

Participant: J.-M. Monnez
External collaborator: O. Collignon (LIH Luxembourg)
In supervised learning the number of values of a response variable to predict can be very high. Grouping these values in a few clusters can be useful to perform accurate supervised classification analyses. On the other hand selecting relevant covariates is a crucial step to build robust and efficient prediction models. We propose in this paper an algorithm that simultaneously groups the values of a response variable into a limited number of clusters and selects stepwise the best covariates that discriminate this clustering. These objectives are achieved by alternate optimization of a user-defined selection criterion. This process extends a former version of the algorithm to a more general framework. Moreover possible further developments are discussed in detail [3].

7.4.3. Death or hospitalization scoring for heart failure patients

Participant: J.-M. Monnez, K. Duarte
External collaborator: E. Albuisson (CHU, Nancy)
The purpose of this study was to define a short term event (death or hospitalization) score for heart failure patients based on the observation of biological, clinical and medical historical variables. Some of them were transformed or winsorized. Two methods of statistical learning were performed, logistic regression and linear discriminant analysis, different variable selection methods were used, on bootstrap samples. Aggregation of classifiers and out-of-bag validation were used. Finally a score taking values between 0 and 100 was established and an odds-ratio was defined in order to support medical decision (writing in progress).

7.4.4. Sequential linear regression with online standardized data

Participant: J.-M. Monnez, K. Duarte
External collaborator: E. Albuisson
We consider the problem of sequential least square multidimensional linear regression using a stochastic approximation process. The choice of the stepsize may be crucial in this type of process. In order to avoid the risk of numerical explosion which can be encountered, we define three processes with a variable or a constant stepsize and establish their convergence. Finally these processes are compared to classic processes on 11 datasets, 6 with a continuous output and 5 with a binary output, for a fixed total number of observations used and then for a fixed processing time. It appears that the third-defined process with a very simple choice of the stepsize gives usually the best results (paper to be submitted).

7.4.5. Mixed-effects ARX Model Identification of Dynamical Biological Systems

Participants: T. Bastogne, L. Batista

System identification is a data-driven modeling approach more and more used in biology and biomedicine [26]. In this application context, each assay is always repeated to estimate the response variability. The inference of the modeling conclusions to the whole population requires to account for the inter-individual variability within the modeling procedure. One solution consists in using mixed effects models but up to now no similar approach exists in the field of dynamical system identification. In [23], we propose a new solution based on an ARX (Auto Regressive model with eXternal inputs) structure using the EM (Expectation-Maximisation) algorithm for the estimation of the model parameters. Simulations show the relevance of this solution compared with a classical procedure of system identification repeated for each subject.

In [24], we propose a solution to firstly estimate the Fisher information matrix using the Louis' method and secondly to determine the parameters confidence intervals of an ARX model structure. We show relevance of the proposed solution in simulation and using real in-vitro data coming from realtime cell impedance measurements.

In parallel, we applied the mixed-effect modeling approach to the analysis in vivo responses in order to identify pronostic biomarkers of tumor regrowth after photodynamic therapy [11]. This application corroborated the practical relevance of our model-based approach.

7.4.6. Uniform asymptotic certainty bands for the conditional cumulative distribution function

Participants: S.Ferrigno, A. Muller-Gueudin, M. Maumy-Bertrand (IRMA, Strasbourg)

In this work, we study the conditional cumulative distribution function and a nonparametric estimator associated to this function. The conditional cumulative distribution function has the advantages of completely characterizing the law of the random considered variable, allowing to obtain the regression function, the density function, the moments and the conditional quantile function. As a nonparametric estimator of this function, we focus on local polynomial techniques described in Fan and Gijbels [ref]. In particular, we use the local linear estimation of the conditional cumulative distribution function.

The objective of this work is to establish uniform asymptotic certainty bands for the conditional cumulative distribution function. To this aim, we give exact rate of strong uniform consistency for the local linear estimator of this function (writing in progress).

7.4.7. Omnibus tests for regression models

Participants: R.Azaïs, S.Ferrigno, M-J Martinez Marcoux (LJK, Grenoble)

The aim of this collaboration begins is to compare, through simulations, several methods to test the validity of a regression model. These tests can be "directional" in that they are designed to detect departures from mainly one given assumption of the model (for example the regression function, the variance or the error) or global (for example the conditional distribution function). The establishment of such statistical tests require the use of nonparametric estimators various functions (regression, variance, cumulative distribution function). The idea would then be able to build a tool (package R) that allows a user to test the validity of the model it uses through different methods and varying parameters associated with modeling. This work is currently in progress.

CAPSID Project-Team

7. New Results

7.1. Correlating Adverse Drug Side Effects

It is well known that many therapeutic drug molecules can have adverse side effects. However, when patients take several combinations of drugs it can be difficult to determine which drug is responsible for which side effect. In collaboration with Prof. Michel Dumontier of the Biomedical Informatics Research Laboratory, Stanford, we developed an approach which combines multiple ontologies such as the Anatomical Therapeutical Classification of Drugs, the ICD-9 classification of diseases, and the SNOMED-CT medical vocabulary together with the use of Pattern Structures (an extension of Formal Concept Analysis) in order to extract association rules to analyse the co-occurrence of adverse drug effects in patient records [26], [27]. A paper describing this work has been submitted to the Journal of Biomedical Semantics.

7.2. Docking Symmetrical Protein Structures

Many proteins form symmetrical complexes in which each structure contains two or more identical copies of the same sub-unit. We recently developed a novel polar Fourier docking algorithm called “Sam” for automatically assembling symmetrical protein complexes. A journal article describing the Sam algorithm has been published [19]. An article describing the results obtained when using Sam to dock several symmetrical protein complexes from the “CAPRI” docking experiment has also been published [13].

7.3. Multiple Flexible Protein Structure Alignments

Comparing two or more proteins by optimally aligning and superposing their backbone structures provides a way to detect evolutionary relationships between proteins that cannot be detected by comparing only their primary amino-acid sequences. We have recently extended our “Kpax” protein structure alignment algorithm to flexibly align pairs of structures that cannot be completely superposed by a single rigid-body transformation, and to calculate multiple alignments of several similar structures flexibly. A journal article describing the approach has been published [20].

7.4. Annotating 3D Protein Domains

Many protein chains in the Protein Data Bank (PDB) are cross-referenced with EC numbers and Pfam domains. However, these annotations do not explicitly indicate any relation between EC numbers and Pfam domains. In order to address this limitation, we developed EC-DomainMiner, a recommender-based approach for associating EC (Enzyme Commission) numbers with Pfam domains [29]. EC-DomainMiner is able to infer automatically 20,179 associations between EC numbers and Pfam domains from existing EC-chain/Pfam-chain associations from the SIFTS database as well as EC-sequence/Pfam-sequence associations from UniProt databases. A manuscript describing this work has been provisionally accepted by the journal *BMC-Bioinformatics*.

7.5. Identifying New Anti-Fungal Agents

In this collaboration with several Brasilian laboratories (at University of Mato Grosso State, University of Maringá, Embrapa, and University of Brasilia), we identified several novel small-molecule drug leads against *Trypanosoma cruzi*, a parasite responsible for Chagas disease [21]. We also proposed several small-molecule inhibitors against *Fusarium graminearum*, a fungal threat to global wheat production [15], [12].

MIMESIS Team

5. New Results

5.1. Augmented Reality for Hepatic Surgery

Participants: Rosalie Plantefève, Bruno Marques, Frederick Roy, Nazim Haouchine, Igor Peterlik, Stéphane Cotin.

Liver cancer is the 2nd most common cause of cancer death worldwide, with more than 745,000 deaths from liver cancer in 2012. When including deaths from liver cirrhosis, the toll reaches nearly 2 million people worldwide. Today, surgical tumor ablation remains the best treatment for liver cancer.To localize the hepatic tumors and to define the resection planes, clinicians rely on pre-operative medical images (obtained with computed tomography scanner or magnetic resonance imaging). However, the liver lesions and vascular system are difficult to localize during surgery. This may lead to incomplete tumor resection or haemorrhage.

We provide surgeons with an augmented view of the liver and its internal structures during surgery to help them to optimally resect the tumors while limiting the risk of vascular lesion. Therefore, an elastic registration method to align the pre-operative and intra-operative data has been developed [26]. This method, which uses a biomechanical model and anatomical landmarks, was designed to limit its impact on the clinical workflow and reaches a registration accuracy below the resection margin even when the liver is strongly deformed between its pre-operative and intra-operative state. This registration algorithm has been integrated into a software, SOFA-OR, to conduct the first clinical tests.

5.2. Augmented Reality for Mini-Invasive Surgery

Participants: Nazim Haouchine, Lionel Untereiner, Frederick Roy, Igor Peterlik, Stéphane Cotin.

We have addressed the ill-posed problem of initial alignment of pre-operative to intra-operative data for augmented reality during minimally invasive hepatic surgery. This problem consists in finding the rigid transformation that relates the scanning reference and the endoscopic camera pose, and the non-rigid transformation undergone by the liver with respect to its scanned state. Most of the state-of-the-art methods assume a known initial registration.

We have proposed in [16] a method that permits to recover the deformation undergone by the liver while simultaneously finding the rotational and translational parts of the transformation. Our formulation considers the boundaries of the liver with its surrounding tissues as hard constraints directly encoded in an energy minimization process. We performed experiments on real in-vivo data of human hepatic surgery and synthetic data, and compared our method with related works (Figure 7).

5.3. Detecting topological changes during non-rigid registration

Participants: Christoph Paulus, David Cazier, Stéphane Cotin.

Augmented reality has shown significant promise in overcoming certain visualization and interaction challenges in various domains such as medicine, construction, advertising, manufacturing, and gaming. Despite the promise of augmented reality and its successful application to many domains, significant research challenges remain. Among these challenges is the augmentation of non-rigid structures that can undergo topological changes, such as fracture, tearing or cutting. This is for instance the case in minimally invasive surgery, which has gained popularity and became a well-established procedure thanks to its benefits for the patient, in particular with shortened recovery times.

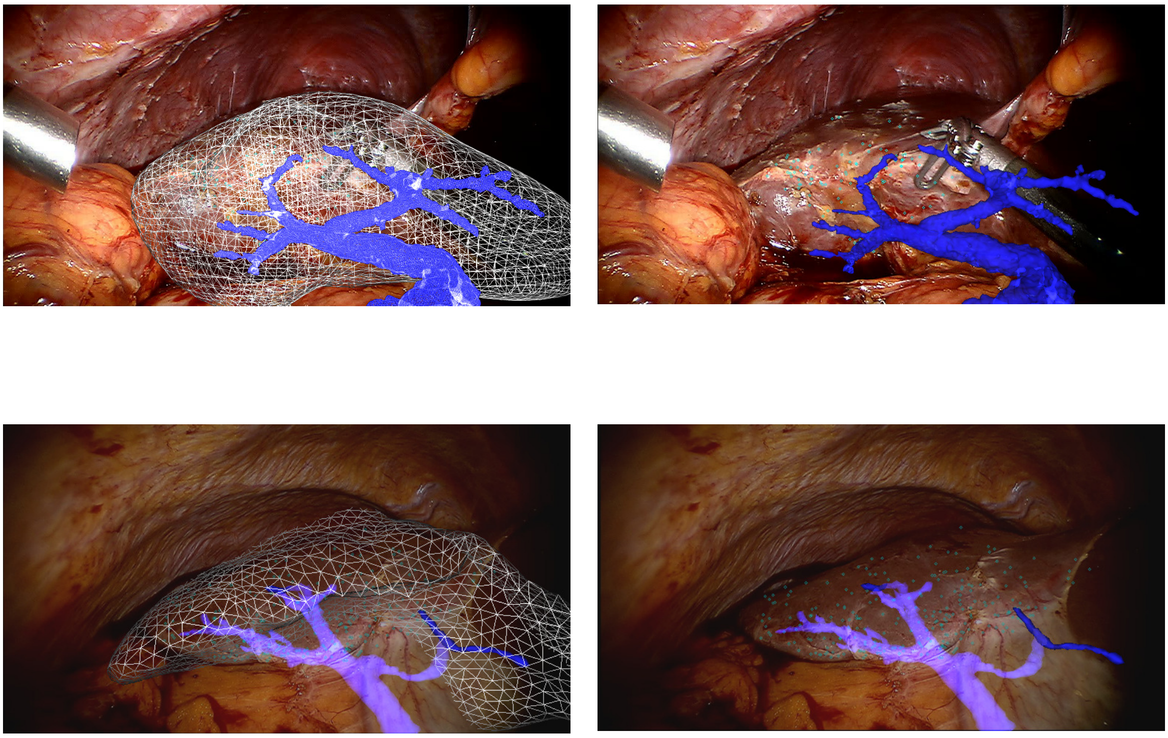

Figure 6. Non-rigid registration between intra-operative and pre-operative data. The overlay of the liver and its vascular network help the surgeon during the operation.

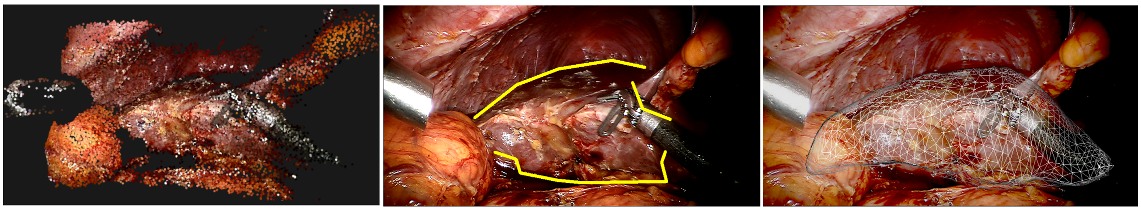

Figure 7. Left: a 3D map is reconstructed from the intra-operative view. Middle: The contours of the liver are extracted. Right: They are used as constraint to pilot a biomechanical model.

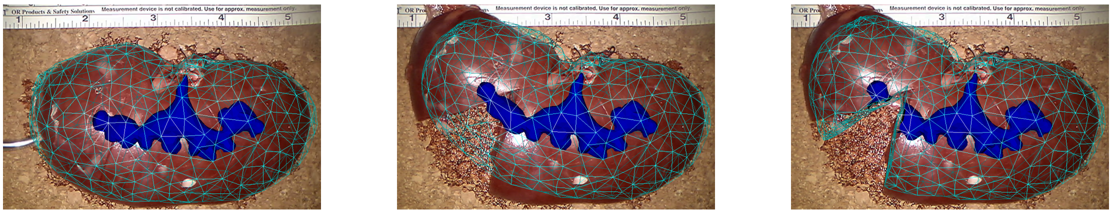

Figure 8. Left: A kidney whose internal structures have been scanned and segmented is cut and deformed. Middle: Standart methods do not detect the cut. Right: Our method detects the cut and applies it to the virtual model.

Current methods dealing with non-rigid augmented reality only provide an augmented view when the topology of the tracked object is not modified, which is an important limitation. We solve this shortcoming by introducing a method for physics-based non-rigid augmented reality [11]. Singularities caused by topological changes are detected by analyzing the displacement field of the underlying deformable model. These topological changes are then applied to the physics-based model to approximate the real cut. All these steps, from deformation to cutting simulation, are performed in real-time. This significantly improves the coherence between the actual view and the model, and provides added value.

5.4. Augmented Reality for Vascular Surgery

Participants: Raffaella Trivisonne, Igor Peterlik, Hadrien Courtecuisse, Stéphane Cotin.

Significant changes have taken place over the past 20 years in medicine with the development of minimally invasive procedures. While surgery evolved towards laparoscopy for instance, interventional radiology has become another alternative for many pathologies. Regarding catheter-based interventions, the lack of depth perception in projective grey-scale images, and the extensive use of X-ray imaging to visualize the instrument and the anatomy through which it must be inserted, are among the main issues. We propose to address these different problems by developing an advanced navigation system which relies on a combination of real-time simulation and information extracted from intra-operative images to assess the current position of the catheter. Such a method would have direct applications in endovascular procedures allowing for an enhanced view of the operating field, both in term of 3D perception and quality of the images. Our approach combines advanced modeling of the device, 2D-3D registration and constraint-based simulation.

We have developed a method [18] based on constraint-based simulation allowing for the enhancement of fluoroscopic images with a 3D real-time catheter insertion and 3D vessel visualization. Our method relies mainly on image features, without the need of any information about the surrounding 3D vasculature, nor does it require any tracking device (Figure 9).

5.5. Image analysis for the characterization of cell mobility

Participant: Igor Peterlik.

The complex behaviour of motile cells plays a crucial role in biological processes such as tissue growth and tumorigenesis. Biomedical research that focuses on understanding the mechanisms of cell motility generates large amounts of multidimensional image data acquired by fully automated optical microscopes. Manual analysis of such data is extremely laborious and therefore, it is necessary to develop reliable automatic methods of image analysis. However, evaluation and assessment of such methods remains a challenging task, since in the case of real data, no ground truth is available to establish simple and robust metrics. Therefore, an important task in development of automatic methods of image analysis is the synthetic generation of realistic images allowing for quantitative assessment based on the ground truth.

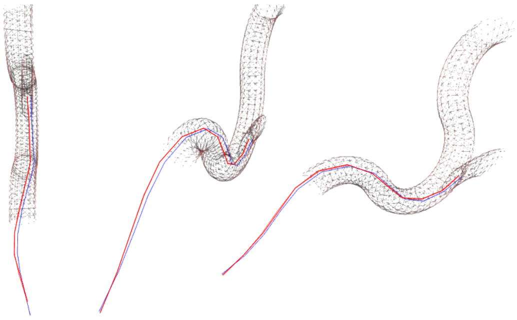

Figure 9. A 3D catheter reconstruction (red) and the real catheter (blue).

We collaborate with the Centre of Biomedical Image Analysis (CBIA) at Masaryk University, Czech Republic on the development of reliable image analysis methods for quantitative characterization of cell motility driven by cellular protrusions at the leading edge of crawling cells. In particular, we develop physics-based models of living cells which are used to generate synthetic time-lapse 3D image series that realistically mimic the motile cells with protrusions (Figure 10). Although modeling of living cells has many specificities, we successfully exploit the modeling algorithms originally designed and developed for the simulation soft tissues. We have already demonstrated that realistic simulation of living cells can be achieved using SOFA and are working toward more complex models and scenarios, involving interactions among the cells and mitosis.

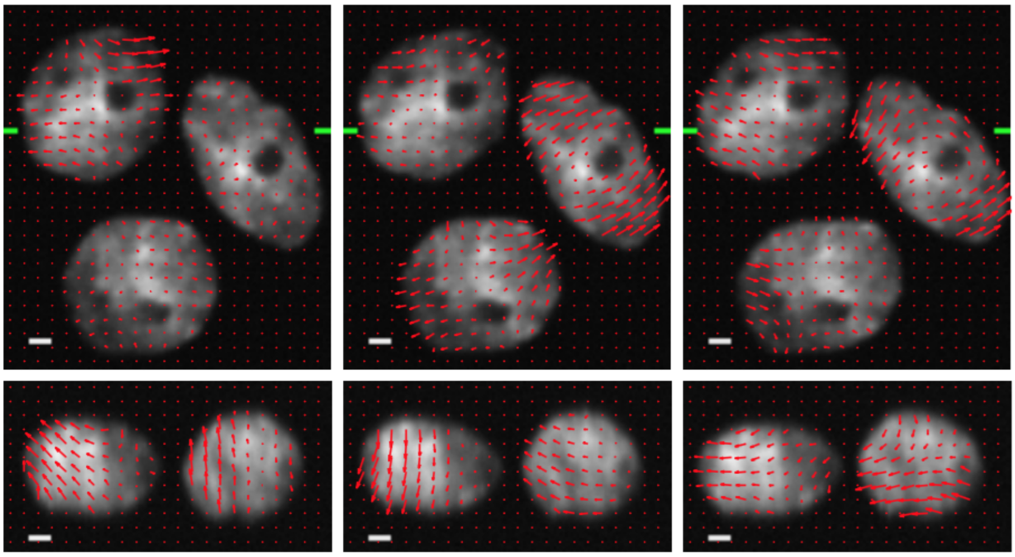

Figure 10. Sample synthetic nuclei generated with our method.

5.6. Training for retina surgery

Participants: Rémi Bessard Duparc, Stéphane Cotin.

Retina surgery is an increasingly performed procedure for the treatment of a wide spectrum of retinal pathologies. Yet, as most micro-surgical techniques, it requires long training periods before being mastered. To properly answer requests from clinicians for highly realistic training on one hand, and new requirements from accreditation or recertification from surgical societies on the other hand, we are developing a high-fidelity training system for retinal surgery.

This simulator is built upon our strong scientific expertise in the field of real-time simulation and a success story for technology transfer in the field of cataract surgery simulation. The simulation system is based on the Open Source simulation platform SOFA, and relies on expertise from our partners to ensure clinical and industrial relevance (this work is funded through the ANR project RESET). A first version of the training system has been developed and demonstrated in different ophthalmology conferences.

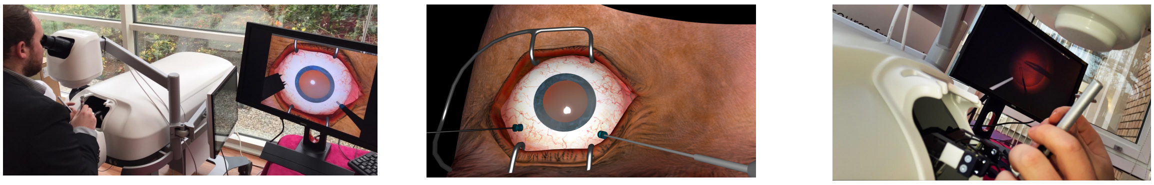

Figure 11. Left: the simulation is performed on a dedicated hardware including a microscope and instruments. Middle: The instruments are inserted in the eye. Right: The epiretinal membrane is removed.

5.7. Robotic control of flexible needle insertion

Participants: Yinoussa Adagolodjo, Hadrien Courtecuisse.

We introduce a new method for automatic robotic needle steering in deformable tissues [13]. It uses an inverse Finite Element (FE) simulation to control an articulated robot interacting with deformable structures. We consider a flexible needle, embedded in the end effector of a 6 arm Mitsubishi RV1A robot, and its insertion into a silicone phantom. Given a trajectory on the rest configuration of the silicone phantom, our method provides in real-time the displacements of the articulated robot which guarantee the permanence of the needle within the predefined path, taking into account any undergoing deformation on both the needle and the trajectory itself. A forward simulation combines i) a kinematic model of the robot, ii) FE models of the needle and phantom gel iii) an interaction model allowing the simulation of friction and puncture force. A Newton-type method is then used to provide the displacement of the robot to minimize the distance between the needle's tip and the desired trajectory. We validate our approach with a simulation in which a virtual robot can successfully perform the insertion while both the needle and the trajectory undergo significant deformations.

5.8. Compensation of brain shift in brain tumor surgery

Participant: Hadrien Courtecuisse.

During brain tumor surgery, planning and guidance are based on pre-operative images which do not account for brain-shift. However, this shift is a major source of error in neuro-navigation systems and affects the accuracy of the procedure. The vascular tree is extracted from pre-operative Magnetic Resonance Angiography and from intra-operative Doppler ultrasound images, which provides sparse information on brain deformations. The pre-operative images are then updated based on an elastic registration of the blood vessels, driven by a patient-specific biomechanical model. We develop a biomechanical model [17] to extrapolate the deformation to the surrounding soft tissues. Our method has proved to efficiently compensate for brain deformation while being compatible with a surgical process.

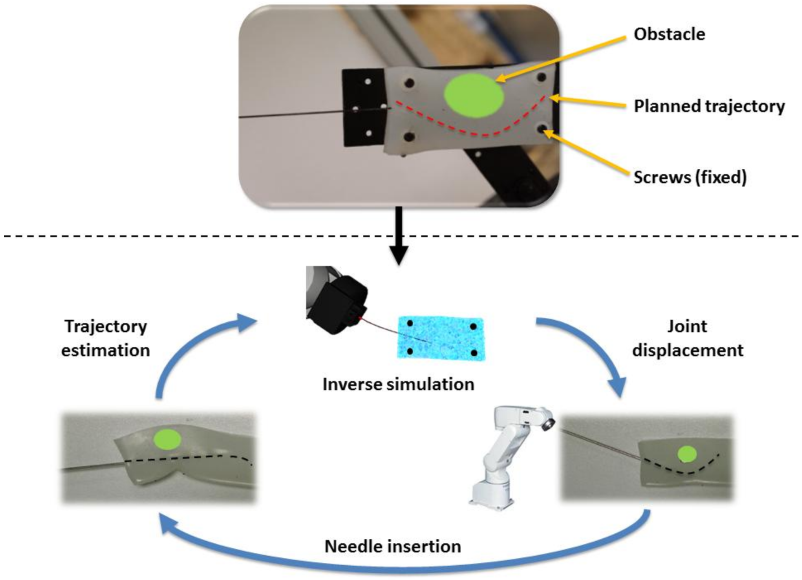

Figure 12. Automatic robotic needle steering in deformable tissues.

5.9. Regional anaesthesia

Participants: Rémi Bessard Duparc, Stéphane Cotin.

The **RASimAs** project (Regional Anaesthesia Simulator and Assistant) is a European research project funded by the European Union's 7th Framework Program. It aims at providing a virtual reality simulator and assistant to doctors performing regional anaesthesia by developing the patient-specific Virtual Physiological Human models. Our work lead to the following journal article (submitted in Sept 2016) : *Real-time error controlled adaptive mesh refinement: Application to needle insertion simulation*.

This paper presents the first real-time discretization-error-driven adaptive finite element approach for corotational elasticity problems involving strain localization. We propose a hexahedron-based finite element method, combined with a posteriori error estimation driven local h-refinement, for simulating soft tissue deformation. This enables to control the local error and global error level in the mechanical fields (e.g. displacement or gradient) during the simulation. The local error level is used to refine the mesh only where it is needed, while maintaining a coarser mesh elsewhere. We investigate the convergence of the algorithm on academic examples, and demonstrate its practical usability on a percutaneous procedure involving needle insertion in soft tissues.

2016 was the third year of the project during which we developed new models of the biomechanics of the leg and arm, as well as the simulation of the insertion of the anaesthesiology needle.

See the RASimAs web site for more details.

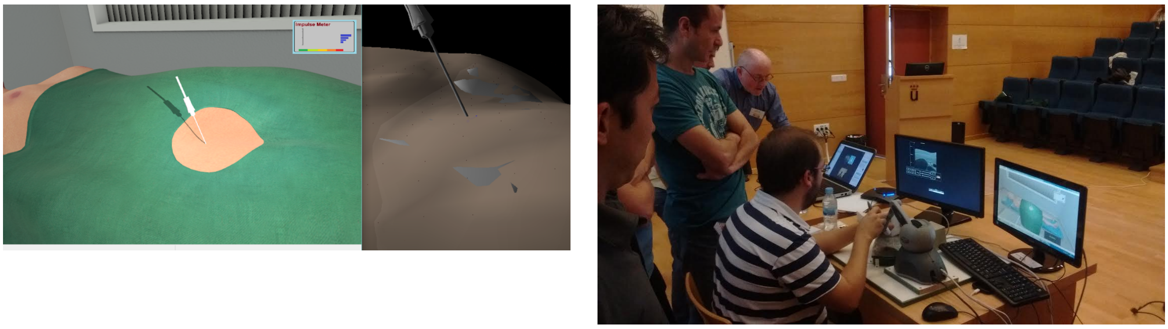

Figure 13. Left: Interface of the RASimAs simulator during femoral nerve block. Right: The RASimas developer team at the General Assembly.

NEUROSYS Project-Team

7. New Results

7.1. From the microscopic to the mesoscopic scale

Participants: Laure Buhry, Francesco Giovannini
In collaboration with Beate Knauer and Motoharu Yoshida (Ruhr University) and LieJune Shiau (University of Houston)

7.1.1. Memory and Anaesthesia

7.1.1.1. The CAN-In model of hippocampal theta oscillations

During working memory tasks, the hippocampus exhibits synchronous theta-band activity, which is thought to be correlated with the short-term memory maintenance of salient stimuli. Recent studies indicate that the hippocampus contains the necessary circuitry allowing it to generate and sustain theta oscillations without the need of extrinsic drive. However, the cellular and network mechanisms supporting synchronous rhythmic activity are far from being fully understood. Based on electrophysiological recordings from hippocampal pyramidal CA1 cells, we have presented a possible mechanism for the maintenance of such rhythmic theta-band activity in the isolated hippocampus [3]. Our model network, based on the Hodgkin-Huxley formalism, comprising pyramidal neurons equipped with calcium-activated non-specific cationic (CAN) ion channels, is able to generate and maintain synchronized theta oscillations ($4-12\,Hz$), following a transient stimulation. The synchronous network activity is maintained by an intrinsic CAN current (I_{CAN}), in the absence of constant external input. The analysis of the dynamics of model networks of pyramidal-CAN and interneurons (CAN-In) reveals that feedback inhibition improves the robustness of fast theta oscillations, by tightening the synchronisation of the pyramidal CAN neurons. The frequency and power of the theta oscillations are both modulated by the intensity of the I_{CAN}, which allows for a wide range of oscillation rates within the theta band.

This biologically plausible mechanism for the maintenance of synchronous theta oscillations in the hippocampus aims at extending the traditional models of septum-driven hippocampal rhythmic activity.

7.1.1.2. Generation of gamma oscillations in a network of adaptive exponential integrate and fire neurons

Fast neuronal oscillations in the Gamma rhythm (20-80 Hz) are observed in the neocortex and hippocampus during behavioral arousal. Through a conductance-based, four-dimensional Hodgkin-Huxley type neuronal model, Wang and Buzsáki have numerically demonstrated that such rhythmic activity can emerge from a random network of GABAergic interneurons when their intrinsic neuronal characters and network structure act as the main drive of the rhythm. We investigate Gamma oscillations through a randomly connected network model comprising low complexity, two-dimensional adaptive exponential integrate-and-fire (AdEx) neurons that have subthreshold and spike-triggered adaptation mechanisms. Despite the simplicity of our network model, it shares two important results with the previous biophysical model: the minimal number of necessary synaptic inputs to generate coherent Gamma-band rhythms remains the same, and this number is weakly-dependant on the network size. Using AdEx model, we also investigate the necessary neuronal, synaptic and connectivity properties that lead to random network synchrony with Gamma rhythms. These findings suggest a computationally more tractable framework for studying sparse and random networks inducing cortical rhythms in the Gamma band (Laure Buhry submitted an article to Journal of Computational Neuroscience, currently under major revision).

7.2. From the Mesoscopic to the Macroscopic Scale

Participants: Laurent Bougrain, Axel Hutt, Tamara Tošić, Mariia Fedotenkova, Meysam Hashemi, Cecilia Lindig-Leon, Jimmy, Nex, Sébastien Rimbert.

In collaboration with Stéphanie Fleck (Univ. Lorraine), Nathalie Gayraud (Inria Sophia Antipolis) and Maureen Clerc (Inria Sophia Antipolis)

7.2.1. Level of Consciousness

Participants: Axel Hutt, Meysam Hashemi

Meysam Hashemi defended his thesis about analytical and numerical studies of thalamo-cortical neural population models during general anesthesia. The findings of this thesis provide new insights into the mechanisms responsible for the specific changes in EEG patterns that are observed during propofol-induced sedation. Our results indicate that depending on the mean potential values of the system resting states, an increase or decrease in the thalamo-cortical gain functions results in an increase or decrease in the alpha power, respectively. In contrast, the evolution of the delta power is rather independent of the system resting states; the enhancement of spectral power in delta band results from the increased synaptic or extra-synaptic GABAergic inhibition. Furthermore, we aim to identify the parameters of a thalamo-cortical model by fitting the model power spectrum to the EEG recordings. To this end, we address the task of parameter estimation in the models that are described by a set of stochastic ordinary or delay differential equations [2].

7.2.2. Motor system

Participants: Laurent Bougrain, Cecilia Lindig-Leon, Jimmy, Nex, Sébastien Rimbert.

In collaboration with Stéphanie Fleck (Univ. Lorraine), Nathalie Gayraud (Inria Sophia Antipolis) and Maureen Clerc (Inria Sophia Antipolis)

7.2.2.1. Incremental motor imagery learning for rehabilitation after stroke

After a stroke, Brain-Computer Interfaces (BCI) allows improving rehabilitation of the motor cortex to recover the autonomy of the patient. The design of BCIs has to be done with an in-depth analysis concerning user's conditions during the learning of BCI. Since strokes affect mainly senior citizens, it is very important to guide the design of BCIs to make it usable. We propose to improve the experimental conditions through a new BCI protocol including an incremental motor imagery learning [21].

7.2.2.2. Motor neuroprostheses

We wrote a review that aims to position current neuroprosthetics research between reality and fiction, expectations of persons under a disability, fantasies of the augmented Man and scientific difficulties. Beyond the buzz effect to get the attention of the public and funders, and enthusiasm by journalists for novelty what are the expectations of potential users, the disappointments and the satisfactions of patients, how many persons are equipped, what are the price and the opportunities to use such devices outside of laboratories [5].

7.2.2.3. Classification of Motor patterns

In order to build systems that are able to detect several motor patterns, multiclass schemes need to be applied. We compared a series of multiclass approaches to assert the benefits of hierarchical classification. The compared methods are based on two effective techniques for MI-discrimination, namely, Common Spatial Patterns (CSP) and Riemannian geometry, for which the hierarchical and non-hierarchical approaches have been considered. We include the CSP by Joint Diagonalization method, which corresponds with a non-hierarchical approach; and its hierarchical counterpart, namely, Binary CSP. In addition, the non-hierarchical Minimum Distance to Riemannian Mean method (MDRM) is also evaluated, together with its analogous hierarchical approach; a contribution of the present work called Hierarchical MDRM algorithm (HMDRM). All these methods have been applied on dataset 2a of the BCI competition IV to facilitate their comparison. The highest accuracies were reached by the BCSP and HMDRM methods, confirming the effectiveness of hierarchical algorithms [7].

7.2.2.4. Discrete Motor Imageries for a Faster Detection

We are investigating differences between continuous MIs and discrete MIs corresponding to a 2s MI. Results show that both discrete and continuous MIs modulate ERD and ERS components. Both ERSs are different but ERDs are close in term of power of (de)synchronization. These results show that discrete motor imageries may be preferable for BCI systems design in order to faster detect MIs and reduce user fatigue. [8]

7.2.3. Pain under General Anaesthesia

Participants : Mariia Fedotenkova, Axel Hutt, Tamara Tošić
In collaboration with Peter beim Graben and James W. Sleigh.

7.2.3.1. Detection of EEG-signal Features for Pain under General Anaesthesia

Mariia Fedotenkova defended her thesis about extraction of multivariate components in brain signals obtained during general anesthesia. We studied analgesia effect of general anesthesia, more specifically, on patients reaction to nociceptive stimuli. We also study differences in the reaction between different anesthetic drugs. The study was conducted on a dataset consisting of 230 EEG signals: pre- and post-incision recordings obtained from 115 patients, who received desflurane and propofol. Combining features obtained with power spectral analysis and recurrence symbolic analysis [22], [6], [23], classification was carried out on a two-class problem, distinguishing between pre-/post-incision EEG signals, as well as between two different anesthetic drugs, desflurane and propofol [1].

TONUS Team

6. New Results

6.1. Time scheme for finite elements code for fluids models

Participants: Emmanuel Franck, Philippe Helluy, David Coulette, Ahmed Ratnani, Eric Sonnendrücker.

The finite element code JOREK use currently a classical implicit solver for reduced MHD model coupled with a block Jacobi preconditioning. For the future full MHD code we propose to change the solver in time to reduce the memory consumption and improve the robustness. During this year two directions have been followed. The first one is based on the classical physics-based preconditioning proposed by L. Chacon. Firstly, we have generalized this method by rewriting the preconditioning as a splitting scheme which separates the advection terms and the acoustic part and by generalizing the splitting algorithm. We obtain different solutions with different advantages. These different splitting schemes have been tested on simplified models and are currently tested on the Euler equations. The second direction is to use a relaxation scheme which allows to rewrite a nonlinear system as a linear hyperbolic system (larger that the previous one) and a nonlinear local source term. Using a splitting scheme we obtain a very simple method where in the first step we solve independent linear transport problems and in a second step we have some nonlinear projections. With a good parallelism and good solver for the transport subproblems the algorithm is very efficient compared to the classical one.

6.2. Preconditioning for elliptic solvers

Participants: Emmanuel Franck, Mariarosa Mazza, Ahmed Ratnani, Eric Sonnendrücker, Stefano Serra-Capizzano.

The different algorithms to discretize in time the MHD or to design preconditioning use solvers for a lot of elliptic operators like Laplacian. For high order finite elements like B-Splines the classical multi-grid methods are not very efficient. Indeed the number of iterations to converge increases strongly when the polynomial order increases. Using a theory called GLT, proposed by S. Serra-Capizzano, we have implemented and validated a smoother for multi-grid, able to obtain the convergence quasi independent of the polynomial degree. This method is also efficient as a preconditioning for mass matrices. We obtain at the end, very robust solvers for these simple problems and allows to perform the time algorithm for fluid models. The next step is to extend this method for more complex problems like vectorial elliptic problems.

6.3. Implicit Lattice Boltzmann scheme for fluid models

Participants: Emmanuel Franck, Philippe Helluy, David Coulette, Conrad Hillairet.

Many systems of conservation laws can be written under a lattice-kinetic form. A lattice-kinetic model is made of a finite set of transport equations coupled through a relaxation source term. Such representation is very useful:

- easy stability analysis, possibility to add second order terms in a natural way;
- can be solved by a splitting strategy;
- easy-to-implement implicit schemes, avoiding CFL constraint;
- high parallelism.

We have started to work on such approaches for solving the MHD equation inside a tokamak (postdoc of David Coulette). We have programmed a generic parallel lattice-kinetic solver in Kirsch, using the StarPU runtime. It presents a very good parallel efficiency. We have also started studying more theoretical aspects: stability of kinetic models, higher order time-integration, viscous terms modeling.

6.4. Hybrid computing

Participants: Philippe Helluy, Nhung Pham, Michel Massaro, Pierre Gerhard, David Coulette, Laura Mendoza, Conrad Hillairet.

In order to harness hybrid computers architecture, we have developed software and algorithms that are well adapted to CPU/GPU computing. For instance we have applied a task-graph approach for computing electromagnetic waves (https://hal.archives-ouvertes.fr/hal-01134222). We have also used an OpenCL-based GPU version of schnaps for computing a drift-kinetic plasma model (Nhung Pham's PhD). Recently, we have also developed a new implementation of the Discontinuous Galerkin solver into schnaps. We now use the StarPU runtime (http://starpu.gforge.inria.fr) for addressing automatically CPUs or GPUs available on the computational node. This development has been applied to the MHD equations (thesis of Michel Massaro). The new development will now be applied to kinetic acoustic simulations (Pierre Gerhard's PhD), gyrokinetic plasma simulations (Laura Mendoza's Postdoc) and implicit MHD simulations (Conrad Hillairet's PhD).

6.5. DG scheme for Drift-Kinetic equation

Participants: Laurent Navoret [correspondent], Philippe Helluy, Nhung Pham.

Using the discontinuous Galerkin solver of Schnaps, we have implemented a numerical scheme for the drift-kinetic model (in a cylinder geometry). The equation is written as an hyperbolic system after reduction in velocity (using spectral finite element). The code is parallelized on a multi-CPU or GPU architecture using OpenCL instructions. To solve the quasineutral equation (for the electric potential), the elliptic solver (already present in Schnaps) has been extended to be used slice by slice (of the cylinder). We have started by validating the code on the 2D guiding-center model and the diocotron instability test-case: we observe that the geometry approximation of the computational domain has a major impact on the precision of the numerical simulations.

6.6. Quasi-neutrality equation in a polar mesh

Participants: Michel Mehrenberger, Philippe Helluy, Guillaume Latu, Nicolas Crouseilles, Christophe Steiner.

In the quasi-neutrality equation in GYSELA, we are now able to treat correctly the inner radius thanks to a simple trick by taking the inner radius $\frac{\Delta r}{2}$. We also continue working on the gyro-average approximation. The new Padé method depends on a parameter ε. When setting ε to a large value, the solution is very similar to the classical Padé one, while taking small value for ε leads to a solution very near to the one obtained using the interpolation method (which approximates better the exact operator, but which can however lead to unstable results as it does not damp high modes). We can then prevent the scheme from instability, by setting large ε, but not too large in order to be more accurate than the classical Padé approximation. Further study in GYSELA is under discussion.

6.7. PICSL: Particle in Cell and Semi-Lagrangian schemes for two species plasma simulations

Participants: Michel Mehrenberger [correspondent], Sever Hirstoaga, Joackim Bernier, Yann Barsamian.

We have worked at CEMRACS 2016 on an algorithm that handles both the Particle in Cell method and the Semi-Lagrangian method in the context of a $2D \times 2D$ to handle the different scales associated with the ions and the electrons in Vlasov-Poisson simulation. Using PIC methods for the electrons allows to use easily specific numerical methods for fast dynamic. Numerical results are in accordance with the dispersion relation.

6.8. TARGET: TArgeting Realistic GEometry in Tokamak code gysela

Participants: Michel Mehrenberger, Nicolas Bouzat, Guillaume Latu, Camilla Bressan, Virginie Grandgirard.

We have worked at CEMRACS2016 on a new variant for the interpolation method to handle both mesh singularity at the origin and non circular geometry. It is based on a non uniform number of points for each closed flux line (intersection of the flux surfaces with the poloidal plane), which are concentric circles in the case of the circular geometry. This strategy, following previous works on curvilinear geometry and hexagonal meshes, should allow to generalize the work in [14] to non circular tokamaks.

6.9. Field aligned interpolation for gyrokinetics

Participants: Michel Mehrenberger, Maurizio Ottaviani, Yaman Güclü, Guillaume Latu, Eric Sonnendrücker.

A theoretical justification of the field align method is provided in the simplified context of constant advection on a 2D periodic domain: unconditional stability is proven, and error estimates are given which highlight the advantages of field-aligned interpolation. The same methodology is successfully applied to the solution of the gyrokinetic Vlasov equation, for which we present the ion temperature gradient (ITG) instability as a classical test-case: first we solve this in cylindrical geometry (screw-pinch), and next in toroidal geometry (circular Tokamak). A paper has been submitted [14].

6.10. High order implicit time splitting schemes for the BGK model

Participants: Michel Mehrenberger, Philippe Helluy, Laurent Navoret, David Coulette, Emmanuel Franck.

In the context of the Lattice Boltzmann or relaxation methods (6.1 -6.3), it is interesting to obtain a very high order implicit splitting. For this, we have considered a time splitting discretization of the BGK model with 3 velocities. First and second order schemes are studied before using Strang splitting coupled with a Semi Lagrangian or a Cranck-Nicholson DG scheme. Using complex time steps and composition methods, we obtain 4th order time step, unconditionally stable for the discrete BGK models. These results could be used with the Lattice Boltzmann method, the relaxation method and also the kinetic model.

6.11. Particle-In-Cell simulations for Vlasov-Poisson equations

Participants: Sever Hirstoaga, Yann Barsamian.

In the work [3], we implement in Selalib an efficient, regarding the memory access, Particle-In-Cell method which enables simulations with a large number of particles. Numerical results for classical one-dimensional Landau damping and two-dimensional Kelvin-Helmholtz test cases are exposed. The implementation also relies on a standard hybrid MPI/OpenMP parallelization. Code performance is assessed by the observed speedup and attained memory bandwidth. A convergence result is also illustrated by comparing the numerical solution of a four-dimensional Vlasov-Poisson system against the one for the guiding center model.

Then, we continued to optimize the code by analyzing different data structures for the particles (structure of arrays vs. arrays of structure) and for the grid fields (using space-filling curves like Morton, Hilbert etc.) with the aim of improving the cache reuse. In addition, we added the functionality of vectorization from the compiler and we obtained significant gain by testing the different data structures. We thus achieved to run PIC simulations processing 65 million particles/second on an Intel Haswell architecture, without hyper-threading. The hybrid parallelization through OpenMP/MPI gave satisfactory strong and weak scaling up to 8192 cores on GENCI's supercomputer Curie.

6.12. Kinetic modeling and simulation of edge tokamak plasmas and plasma-wall interactions

Participants: Sever Hirstoaga, David Coulette, Giovanni Manfredi.

We performed a full parallelization (over species and using 4D domain decomposition) of the 1D3V Multi-species Vlasov-Poisson finite-volumes code. The 4D code was then used to perform, by means of parametric studies, an analysis of the structure of the multi-scale boundary layer (the so-called Debye sheath and various pre-sheaths) for a magnetized-plasma in contact with an absorbing wall. This study allowed us to show, notably, that when the strong confining magnetic field is close to grazing incidence with respect to the absorbing surface, the boundary layer extends further into the plasma and as a result the magnitude of the electric field is lessened.

A second study was devoted to the dynamics of the propagation of the so-called "ELMs" (Edge-Localized-Modes) at the edge of Tokamak devices. The $1D1V$ collisionless model used in previous studies was extended by coupling a $1D1V$ kinetic model for the fast parallel propagation of the plasma disturbance along magnetic field lines with a fluid model in the directions perpendicular to the magnetic field. The coupling occurs by means of collision operators allowing for energy transfer between the parallel and perpendicular degrees of freedom. The initial asymptotic preserving scheme was extended to allow for adaptive time-stepping due to the introduction of the fluid transport equation. Using simulation results for various realistic collision rates we showed that collisional isotropization of the electronic population have a significant impact on the heat flux impacting the devices wall. The results were presented to the magnetic fusion community at the EPS conference in Leuven [9].

COAST Project-Team

5. New Results

5.1. Evaluation and Design of Consistency Maintenance Algorithms for Complex Data

Participants: Luc André, Quang Vinh Dang, Claudia-Lavinia Ignat, Gérald Oster, Pascal Urso.

Since the Web 2.0 era, the Internet is a huge content editing place on which users collaborate. 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 amounts 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. We designed new optimistic replication algorithms for maintaining consistency for complex data such as wikis and strings and we evaluated existing algorithms in large scale settings.

Wikis are one of the most important tools of Web 2.0 allowing users to easily edit shared data. However, wikis offer limited support for merging concurrent contributions on the same pages. Users have to manually merge concurrent changes and there is no support for an automatic merging. Real-time collaborative editing reduces the number of conflicts as the time frame for concurrent work is very short. We proposed extending wiki systems with real-time collaboration and designed an automatic merging solution adapted for rich content wikis [5]. Our merging solution is based on an operational transformation approach for which we defined operations with high-level semantics capturing user intentions when editing wiki content such as move, merge and split. Our solution is the first one that deals with high level operations, existing approaches being limited to operations of insert, delete and update on textual documents.

Over the last years we designed a CRDT-based consistency maintenance algorithm for strings [20] for peer-to-peer large scale collaboration that is used by our MUTE collaborative editor which will be integrated in the virtual desktop of the OpenPaaS::NG project. This algorithm called LogootSplit can be seen as an extension for variable-sized elements (e.g. strings) of one of the first basic CRDT algorithms for unit elements (e.g. characters) proposed by our team called Logoot [32]. Its principles are general and can be applied to other basic CRDT algorithms. This year we proposed another algorithm for strings based on the RGA algorithm [9].

By means of simulations we measured the delays in popular real-time collaborative editing systems such as GoogleDocs and Etherpad [12] in terms of the number of users that edit a shared document and their typing frequency. Delays exist between the execution of one user's modification and the visibility of this modification to the other users. Such delays are in part fundamental to the network, as well as arising from the consistency maintenance algorithms and underlying architecture of collaborative editors. Results of this study support our team assertion that delay associated with conventional consistency maintenance algorithms will impede group performance.

5.2. Probabilistic Partial Orderings

Participants: Jordi Martori Adrian, Pascal Urso.

Ensuring reliable and ordered communication between computers usually requires acknowledgment messages. In systems with a high rate of broadcast communication, the cost of such acknowledgment messages can be large. We propose to use the causal ordering information required by some applications to detect and request missing messages. To circumscribe the number of unnecessary requests we combine local awareness and probabilistic methods. Our model allows us to obtain reliable communication within a latency equivalent to unordered communication and lower network usage than acknowledgment systems [18].

5.3. Computational Trust based on User Behavior

Participants: Quang Vinh Dang, Claudia-Lavinia Ignat.

We continued our investigation on computing a trust score for each user according to their behaviour during a collaborative task. Previously we proposed a contract-based collaboration model [31] where trust in users is established and adjusted based on their compliance to the contracts specified by the data owners when they share the data.

We continued this work by proposing an experimental design for testing the proposed trust-based collaboration model. We studied the trust game, a money exchange game that has been widely used in behavioural economics for studying trust and collaboration between humans. In this game, exchange of money is entirely attributable to the existence of trust between users. In the context of the trust game we proposed a trust metric that reflects user behaviours during the collaboration [10]. This metric is robust against fluctuating user behaviour. Our trust metric is the first one that was proposed in the context of the trust game in order to predict user behaviour.

In order to compute the trust score of users according to their contributions during a collaborative editing task, we need to evaluate the quality of the document content. As an initial work in this direction we investigated how to automatically assess the quality of Wikipedia articles in order to guide readers towards high quality articles and to suggest to authors which articles need to be improved. In this context we proposed two automatic assessment methods of the quality of Wikipedia articles. In the first approach we introduced readability features for a better prediction of quality [11]. The second approach is based on a deep-learning mechanism that automatically learns features from document contents rather than manually defining them [13], [4].

5.4. A model to secure collaborative resources within Enterprise Social Networks

Participants: Ahmed Bouchami, Olivier Perrin.

Enterprise social networks (ESN) are collaborative environments that raise major challenges to secure them. In his thesis [2], Ahmed Bouchami addressed the problem of authentication of digital identities within collaborative communities. He proposed an interoperable architecture for managing federated authentication, thus allowing each enterprise to preserve its (own) authentication mechanism and each principal to perform a single sign on authentication regarding different enterprises. He also proposed access control management. His flexible access control model is based on a set of identity attributes, and a formal language based on temporal logic. This model allows for checking the consistency of the policies defined. with the model.

Last, the access control system offers the ability to control the user-centric sharing policies through policies based on a risk management mechanism, which makes the access control mechanism dynamic. The risk mechanism is based on the NIST's risk definition with an alignment with a set of parameters that include access control in the ESN context. More precisely, the dynamic risk management includes, the collaborative resource's importance, the authentication system's vulnerabilities and trust level reflected through the behavior of each collaborative actor. On this latter aspect of trust, a reputation score is computed using the history of collaborative interactions of each subject of the collaborative environment. Finally, a prototype is available and was demonstrated within the OpenPaaS ESN project.

5.5. Risk management for the deployment of a business process in a multi-cloud context

Participants: Amina Ahmed Nacer, Claude Godart, Elio Goettelmann, Samir Youcef.

The lack of trust in cloud organizations is often seen as obstacle to SaaS developments. This work proposes an approach which supports a trust model and a business process model in order to allow the orchestration of trusted business process components in the cloud.

The contribution is threefold and consists in a method, a model and a framework. The method categorizes techniques to transform an existing business process into a risk-aware process model that takes into account security risks related to cloud environments. These techniques are partially described in the form of constraints to automatically support process transformation. The model formalizes the relations and the responsibilities between the different actors of the cloud. This allows to identify the different information required to assess and quantify security risks in cloud environments.

The framework is a comprehensive approach that decomposes a business process into fragments that can automatically be deployed on multiple clouds. The framework also integrates a selection algorithm that combines the security information of cloud offers and of the process with other quality of service criteria to generate an optimized configuration. It is implemented in a tool to assess cloud providers and decompose processes.

Rooted in past years work, we are contributing this year at the methodological and framework levels in two directions:

- At the methodological level, while our risk computing model rested previously only on data provided by cloud providers (provider-side risk model), we are developing a risk model integrating client-side knowledge (client-side risk model).
- At the framework level, we have integrated the ability to integrate fake BP fragments in the objective to increase the obfuscation of a deployed BP logic [15].

5.6. Cloud Provisioning for Elastic BPM

Participants: François Charoy, Samir Youcef, Guillaume Rosinosky.

Even though the cloud computing paradigm has proven benefits, it faces a serious problem that can compromise its commercial success. It concerns the lack of an efficient approach for using optimally the available resources. For this, several approaches have been proposed [29]. However, they suffer from several shortcomings. Often only one objective is taken into account, expressing all operations in terms of cost. Furthermore, business processes should be insured with elasticity and multi-tenancy mechanism while adjusting the available resources to the dynamic load distribution. We proposed to optimize two conflicting objectives, namely the number of migrations of tenants and the cost incurred using a set of resources. Our approach allows to take into account the multi-tenancy property and the Cloud computing elasticity, and is efficient as shown by an extensive experimentation based on real data from Bonita BPM customers [16]. In order to secure the scientific value of our findings we have set up a experimentation infrastructure for making repeatable experiments on the Cloud [17]

5.7. Orchestration of crowdsourcing activities

Participants: François Charoy, Kahina Bessai.

Crowdsourcing is an important paradigm in human problem solving using the Web. When they face a workload outburst, businesses may choose to outsource some or all of their process tasks to the crowd in order to maintain the quality of service promised for their customers. This may occur in situations like crisis management, when organizations are overloaded by a sudden event breakout. These tasks are generally difficult to implement as solution based on software service only. So, the use of crowdsourcing platform seems enticing. To ensure efficient and wise use of resources, methods assisting decision making need to be developed whose aim is to assist businesses in choosing the most knowledgeable workers. We addressed the resource allocation problem in crisis context by defining a delegation approach based on crowdsourcing as resource provider. We introduce a mathematical model for business process execution in crowd-sourcing context and an exact optimization algorithm. As the problem addressed is NP-complete, we proposed a more efficient algorithm that we validated through simulation [7]. Furthermore, to overcome the limitations of existing works we take into account the fact that business process tasks are ordered while optimizing the overall execution time of a given business process instance under budget constraint. We used a synthetic crowd model or valitation. We have also defined a model to validate our work for geo-crowdsourcing activities [8].

MADYNES Project-Team

6. New Results

6.1. Monitoring

6.1.1. Quality of Experience Monitoring

Participants: Isabelle Chrisment [contact], Thibault Cholez, Vassili Rivron.

We have pursued our work on smartphone usage monitoring. In [26], we presented an exploratory smartphone usage study with logs collected from users in the wild, combined with the sociodemographic, technological and cultural information provided by them. We have shown that application usage among users is highly diverse. However when the applications are grouped as services, interesting relations appear between user profiles and types of services used. We found significant correlations between service usage and socio-demographic profile. We have proposed several possible use cases of how sociological information can be used to renew the official statistics, to recommend suitable applications to potential users.

6.1.2. Active Monitoring

Participants: Abdelkader Lahmadi [contact], Jérôme François, Frédéric Beck [LHS], Loic Rouch [LHS].

Following preliminary work in 2015, we pursued our assessment of industrial system exposition in the Internet. Industrial systems are composed of multiple components whose security has not been addressed for a while. Even if recent propositions target to improve it, they are still often exposed to vulnerabilities, since their components are hard to update or replace. In parallel, they tend to be more and more exposed in the public Internet for convenience. Although awareness of such a problem has been raised, there is no precise evaluation of such a risk. We thus defined a methodology to measure the exposure of industrial systems through Internet. In particular, a carefully designed scanning approach and software with a low footprint, named WiScan, consists in optimizing the distance between consecutively scanned IP addresses but being fast to compute. It has been applied on the entire IPv4 address space, by targeting specific SCADA ports. This work is reported in [20].

During the year 2016, we are also working with the regional PME TracIP http://www.tracip.fr on the development of attack assessment and forensics platform dedicated to industrial control system. The platform involves multiple PLC from different manufactures and real devices of factory automation systems.

6.1.3. SDN enhanced monitoring

Participants: Jérôme François [contact], Lautaro Dolberg [University of Luxembourg].

Software-Defined Networking (SDN) provides a highly flexible flow management platform through a logically centralized controller that exposes network capabilities to the applications. However, most applications do not natively use SDN. An external entity is thus responsible for defining the corresponding flow management policies. This is mainly the role of the network administrator, which also prefers to keep the control of its network rather than fully let the control to users or applications.

Usually network operators prefer to control the flow management policies, rather than granting full control to the applications. Although IP addresses and port numbers can suffice to identify users and applications in ISP networks and determine the policies applicable to their flows, such an assumption does not hold strongly in cloud environments. IP addresses are allocated dynamically to the users, while port numbers can be freely chosen by users or cloud-based applications. These applications, like computing or storage frameworks, use diverse port numbers which amplifies this phenomenon. We have proposed higher-level abstractions for defining user- and application-specific policies. In this scope, our framework transparently maps application-level policies (involving application and user names) to OpenFlow rules (IP addresses, protocols and port numbers), which alleviates the necessity for the control applications (those interacting with the Northbound interface of the controller) to keep track of the network characteristics (like location) of users and applications themselves. To achieve this end, application-level information is retrieved in real-time through local remote system agents, which can be easily deployed in a cloud platform where both network and computational infrastructure are hosted by the same entity.

Thus our work enables the association of flows with applications and users. It led to a publication [19].

6.1.4. Service-level Monitoring of HTTPS traffic

Participants: Thibault Cholez [contact], Shbair Wazen, Jérôme François, Isabelle Chrisment.

We previously investigated the latest technique for HTTPS traffic filtering that is based on the Server Name Indication (SNI) field of TLS and which has been recently implemented in many firewall solutions. We showed that SNI has two weaknesses, regarding (1) backward compatibility and (2) multiple services using a single certificate. On the other side, HTTPS proxy suffers from privacy issues by decrypting users' sensitive traffic. This led us to the development of new reliable methods to investigate the increasing number of HTTPS traffic with a proper level of identification (service-level) that allows the management of the traffic while other methods are either too broad (protocol-lvl identification) or too precise (page-level identification).

We proposed to improve HTTPS traffic monitoring based on SNI. Our investigation shows that 92% of the HTTPS websites surveyed can be accessed with fake-SNI. Our approach verifies the coherence between the real destination server and the claimed value of SNI by relying on a trusted DNS service. Experimental results show the ability to overcome the shortage of SNI-based monitoring by detecting forged SNI values while having a very small false positive rate (1.7%). The overhead of our solution only adds negligible delays to access HTTPS websites. The proposed method opens the door to improve global HTTPS monitoring and firewall systems and was published in the IEEE STAM workshop [31].

We proposed an alternative technique to investigate HTTPS traffic which aims to be robust, privacy-preserving and practical with a service-level identification of HTTPS connections, i.e. to name the services, without relying on specific header fields that can be easily altered. We have defined dedicated features for HTTPS traffic that are used as input for a multi-level identification framework based on machine learning algorithms processing full TLS sessions. Our evaluation based on real traffic shows that we can identify encrypted web services with a high accuracy. This work was published in IFIP/IEEE NOMS [30] and is now extended in the frame of the CNRS PEPS NEFAE project to address the challenge of real-time monitoring of HTTPS. We extract statistical features on TLS handshake packets and progressively on application data packets, so that we can identify HTTPS services very early in the session. Extensive experiments performed over a significant and open dataset show that our method offers a good accuracy and a prototype implementation confirms that the real-time requirement of monitoring HTTPS services is satisfied.

6.1.5. Sensor networks monitoring

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

This year, we have pursued our work on IoT security monitoring, based on our distributed architecture specified in [24]. This one exploits the multi-instance mechanisms of the RPL protocol, to build a monitoring plane using high-order nodes, in the context of Advanced Metering Infrastructures (AMI). It permits to preserve more constrained node resources, by passively monitoring the network. We have shown in [23] its benefits for detecting version number attacks. A DODAG versioning system is incorporated into the RPL protocol, in order to ensure an optimized topology. However, an attacker can exploit this mechanism to damage the network and reduce its lifetime. We have therefore proposed a detection strategy with a set of algorithms capable of identifying malicious nodes performing such attacks. We have evaluated our solution through experiments and have analyzed the performance according to defined metrics. We have shown that false positive rates can be reduced by a strategic monitoring node placement. In particular, we have addressed scalability considerations, as an optimization problem which can be easily adapted to different topologies. By resolving this problem, we were able to quantify the number of monitoring nodes required to ensure an acceptable false positive rate for different topologies.

Our taxonomy on security attacks in these networks has also been published in [2]. The RPL protocol is exposed to a large variety of attacks, whose consequences can be quite significant in terms of network performance and resources. The attacks against resources reduce network lifetime through the generation of fake control messages or the building of loops. The attacks against the topology make the network converge to a sub-optimal configuration or isolated nodes. Attacks against network traffic let a malicious node capture and analyse large part of the traffic. This classification serves as a support to prioritize attacks depending on the damages they may cause to the network, and can be exploited for risk management purposes in order to select counter-measures.

6.2. Security

6.2.1. Security analytics

Participants: Jérôme François [contact], Abdelkader Lahmadi, Giulia de Santis, Marc Coudriau, Olivier Festor.

During 2016, active collaboration with the High Security Lab in Nancy continues especially in the context of the FUI HuMa project. First we developed a method to automatically analyze darknet data. A darknet or telescope is a whole subnetwork, which is announced over Internet such that packets sent to the IP addresses are properly routed over but not replied to. In our case, the darknet is a /20 network meaning that we monitor 2^{12} addresses. The main challenge we faced was to cope with the volume of data in order to extract intertwined phenomena characterized by groups of packets. We proposed a clustering and visualisation method derived from the Mapper algorithm that has been developed in the field of Topological Data Analysis (TDA). The developed method and its associated tool are able to analyze a large number of IP packets in order to make malicious activity patterns easily observable by security analysts. The results show that our method is able to exhibit observable patterns which have been missed by Suricata, a widely used State-of-the-Art IDS https://hal.inria.fr/hal-01403950/document.

Second scannings have been particularly studied as they represent the first phase of recognition in advanced persistent threats. While it is known that every exposed systems is always being actively scanned from multiple sources, it is still challenging to fingerprint them, in particular to identify what are the distributed sources of a single synchronized scan and what is the tool used to generate it. As a first step, we proposed a methodology based on Hidden Markov Models (HMMs) to model scanning activities monitored by a darknet [18]. The HMMs of scanning activities are built on the basis of the number of scanned IP addresses within a time window and fitted using mixtures of Poisson distributions.

We are also still maintaining an IRTF draft [50] to promote a standardization effort towards the extension of IP Flow-based monitoring with geographic information. Associating Flow information with their measurement points geographic locations will enable security applications to detect anomalous activities. In the case of mobile devices, the characterization of communication patterns using only time and volume is not enough to detect unusual location-related communication patterns. The draft went through an IRSG review and a feedback is still required from the OPSWAG IETF working group.

6.2.2. DDoS Signaling

Participants: Jérôme François [contact], Abdelkader Lahmadi, Giovane Moura [SIDN Labs, Netherland], Marco Davids [SIDN Labs, Netherlands].

A distributed denial-of-service (DDoS) attack aims at rendering machines or network resources unavailable. These attacks have grown in frequency, intensity and target diversity. In the context of Flamingo, Madynes contributed to the definition of an opportunistic signaling protocol in cooperation with SIDN Labs in Netherlands. The goal is to provide an efficient mechanism where nodes in an IPv6 network facing a DDoS attack can deliver a DOTS (DDoS Open Threat Signaling) signal message sent by a DOTS client to the DOTS server. The specified mechanism does not generate transport packets to carry the DOTS signal message but it only relies on existing IPv6 packets in the network to include within them a hop-by-hop extension header which contains an encoded DOTS signal message.

This work is done under the umbrella of our standardization activities especially within the IETF DOTS working group [45] and was presented during IETF 96 in Berlin.

6.2.3. NDN Security

Participants: Thibault Cholez [contact], Xavier Marchal, Olivier Festor.

Named-Data Networking (NDN) is one of the most advanced ICN architecture but the security of NDN or NFD (NDN Forwarding Deamin) is still in the early stages and not ready for real deployment. In the context of the ANR Doctor project, we investigate NDN security in order to unveil issues and propose remediations.

First, we discovered a new vulnerability of NDN which is easy to exploit and can lead to very serious attacks, badly affecting the network. This vulnerability is due to an absence of control at the precise moment when NFD receives an incoming Data. In fact, NFD only checks two points: if the Data belongs to the localhost scope, or if it matches an existing PIT entry, but not if the Data comes from a valid Face. This is a critical shortage because it allows malicious users to directly send Data to perform attacks like DoS and cache poisoning without having to register a prefix in the router's FIB beforehand to receive legitimate Interests. After these checks, NFD continues to process the Data packet. The NDN protocol makes the hypothesis that a node cannot send a Data packet without having previously received the corresponding Interest (receiver driven communication). However, NFD should consider malicious nodes that decide to not follow the standard way to proceed with NDN communications and send Data unexpectedly. We further described two serious attack scenarios exploiting this vulnerability based on the fact that malicious nodes can send unexpected Data that can consume legitimate PIT entries. We also propose two ways to prevent it with minor modifications in NFD. This work was published and demonstrated at the ACM-ICN conference [46].

Second, we addressed the Content Poisoning Attack (CPA), known to be one of the major threats in NDN. So far, existing works in that area have fallen into the pit of coupling a biased and partial phenomenon analysis with a proposed solution, hence lacking a comprehensive understanding of the attack's feasibility and impact in a real network. In the context of the ANR Doctor Project, and in collaboration with UTT, we demonstrated through an experimental measurement campaign that CPA can easily and widely affect NDN. We proposed three realistic attack scenarios relying on both protocol design and implementation weaknesses and presented their implementation and evaluation in a testbed based on the latest NFD version. We analyzed their impact on the different ICN nodes composing a realistic topology (clients, access and core routers, content provider) in order to fully characterize the CPA. This work has been accepted and will be published in IFIP/IEEE IM 2017 conference.

6.2.4. Configuration security automation

Participants: Rémi Badonnel [contact], Abdelkader Lahmadi, Olivier Festor, Nicolas Schnepf, Maxime Compastie.

We have pursued during year 2016 our efforts on the orchestration of security functions in the context of mobile smart environments, with a joint work with Stephan Merz of the VeriDis project-team at Inria Nancy. In particular, Nicolas Schnepf studied during his Master thesis formal techniques for the automatic verification of chains of security functions in a setting of software-defined networks (SDN). Concretely, he defined an extension of the Pyretic language [51] which takes into account the data plane of SDN controllers and implemented a translation of that extension to the input languages of the nuXmv model checker and of SMT solvers. The approach and its scalability were validated over crafted security chains, and a conference paper describing the results is going to be submitted shortly. Nicolas Schnepf started a PhD thesis on the same topic in October 2016 with joint supervision by members of the Madynes and VeriDis Inria project-teams.

In addition, we have analyzed and evaluated the usage of OpenFlow messages for security applications [29], jointly with Bundeswehr University of Munich. The purpose was to quantify the performances of security solutions that are built on top of software-defined networking infrastructures. We have considered overloading attacks and information gathering attacks, that are quite common in these environments, and have detailed regular and sdn-based mitigation mechanisms that have been designed for tackling them. We have then analyzed for each category the dependencies of these mechanisms to the OpenFlow protocol commonly supporting the communications between sdn controllers and switches. These dependencies have been identified through the mapping of OpenFlow messages to security functionalities in that context. Based on this analysis, we performed series of experiments on two different testbeds for comparing and evaluating the accuracy and reliability that can be expected with respect to these messages.

We have also investigated in [16] a software- defined security framework, for supporting the enforcement of security policies in distributed cloud environments. These latter require security mechanisms able to address their multi-tenancy and multi-cloud properties. This framework relies on the autonomic paradigm to dynamically configure and adjust these mechanisms to distributed cloud constraints, and exploit the software-defined logic to express and propagate security policies to the considered cloud resources. It exploits a security orchestrator, policy decision points (PDP) and policy enforcement point (PEP) interacting according to a dedicated set of protocols, and will take advantage of facilities offered by unikernel and micro-services techniques to reduce the security exposure of cloud resources. The proposed framework has been evaluated so far through a set of validation scenarios corresponding to a realistic use cases including cloud resource allocation/deallocation, cloud resource state change, and dynamic access control.

6.3. Experimentation, Emulation, Reproducible Research

This section covers our work on experimentation on testbeds (mainly Grid'5000), on emulation (mainly on Distem), and on Reproducible Research.

6.3.1. Grid'5000 design and evolutions

Participants: Jérémie Gaidamour, Arthur Garnier, Lucas Nussbaum [contact], Clément Parisot, Florent Didier.

The team was again heavily involved in the evolutions and the governance of the Grid'5000 testbed.

First, we finished the installation and setup of several new clusters in the Nancy site, which brought several new local users, from various teams, to the testbed.

In the context of ADT LAPLACE, Jérémie Gaidamour added support for the control of CPU parameters such as Hyperthreading, Turboboost, P-states and C-states. It is expected that this work will enable interesting usages in the areas of HPC runtimes and energy-aware computing.

Finally, in the context of his roles in the *bureau*, *comité d'architectes* and *comité des responsables de sites* of Grid'5000, Lucas Nussbaum managed the purchase of the new clusters at Nancy mentioned above, and gave several presentations about the testbed, at the *Grid'5000 School* [5] [38], at a GENI-FIRE collaboration workshop [9], [8], [6], [7].

6.3.2. Emulation with Distem

Participants: Emmanuel Jeanvoine, Lucas Nussbaum [contact], Cristian Ruiz.

Several improvements have been made around Distem, mostly in the context of ADT COSETTE.

A paper demonstrating the use of Distem to evaluate fault tolerance and load balancing strategies implemented in Charm++ was accepted at CCGrid'2016 [28].

We continued our work on using Distem to experiment on NDN infrastructures. We obtained promising results, especially in terms of scale. This work is still pending publication.

Finally, we also evaluated the porting of Distem to other testbeds (ChameleonCloud and CloudLab), which was interesting for Distem specifically, but also to understand differences between those testbeds [43].

6.3.3. Management of experiments

Participants: Tomasz Buchert, Emmanuel Jeanvoine, Lucas Nussbaum [contact], Cristian Ruiz.

We continued work on Ruby-Cute, a library that aggregates various useful functionality in the context of such tools. Several releases were made in 2016. We hope that it will be useful as a basis for future tools, and ease testing of new ideas in that field. The library is available on http://ruby-cute.github.io/.

Tomasz Buchert defended his PhD thesis, entitled *Managing large-scale, distributed systems research experiments with control-flows*, in January 2016 [1].

6.3.4. Experimentation methodologies on Big Data

Participants: Abdulqawi Saif, Lucas Nussbaum [contact], Ye-Qiong Song [contact].

Abdulqawi Saif started his PhD on experimentation methodologies for Big Data at the end of 2015. His first work [35] is a multi-criteria analysis of NFS performance using statistical Design of Experiments techniques.

6.4. Routing

6.4.1. Probabilistic Energy-Aware Routing for Wireless Sensor Networks

Participants: Evangelia Tsiontsiou, Bernardetta Addis, Alberto Ceselli [Universita degli Studi di Milano], Ye-Qiong Song [contact].

Healthcare applications are considered as promising fields for Wireless Sensor Networks (WSNs) and globally IoT. Thanks to WSNs, patients can be monitored in hospitals or smart home environments, providing health improvement, or emergency care. Network lifetime is still the key issue when we deploy wireless sensor networks and IoT solutions in real-world applications. Current WSN research trends include duty-cycling at MAC layer and energy efficient routing at network layer, among others. We proposed an Optimal Probabilistic Energy-Aware Routing Protocol (OPEAR) for duty-cycled WSNs which aims at maximizing the network lifetime by keeping low energy consumption and balancing network traffic between nodes. Our experimental campaign reveals that our OPEAR protocol outperforms the popular Energy Aware Routing Protocol (EAR) from the literature, proving to be more effective in extending the network lifetime [33]. It is part of Lorraine AME Satelor project granted by Lorraine Region.

6.4.2. NDN router with P4

Participants: Salvatore Signorello [University of Luxembourg], Olivier Festor [contact], Radu State [University of Luxembourg], Jérôme François.

Although content-awareness at the network level is becoming more and more needed, Information-Centric Networking (ICN)-based solutions struggle to emerge. Research on ICN has already produced insightful outputs, nevertheless architecture-tied designs of ICN devices cannot be easily deployed and tested in operational networks; further those designs are hard to share. In the meantime, the vision of Software-Defined Networking has grown and taken new shapes. Network players desire to change devices' behavior often and drastically, even though performances are still crucial to operate at line-speed. This has been leading to a rethink of network devices designs with the aim to offer full-programmability through high-level programming languages for packet processors, like P4. It is a programming language to describe the forwarding plane of network devices. The language abstracts how packets are processed by different devices in target- independent programs. Then, compilers map those programs to different forwarding devices with as final goal a single specification which can be automatically mapped to hardware or software implementations. Although high-level protocols like ICN with advanced parsing mechanisms are usually handled by software switch with standard programming capacity, P4 would allow more efficient implementation on specific platform. Our preliminary implementation strives to implement many features of the NDN routing by using native P4 language constructs only [32].

6.4.3. NDN/HTTP cohabitation

Participants: Thibault Cholez [contact], Xavier Marchal, Olivier Festor.

Network operators are reluctant to deploy globally Named Data Networking (NDN) because of the huge investment costs required and the uncertainty about the security and the manageability of such disruptive network protocols when deployed in production, while the return of investment is also uncertain. Meanwhile, Network Functions Virtualization (NFV) greatly facilitates the deployment of novel networking architectures by reducing the costs thanks to the usage of commodity hardware in place of dedicated equipments. Consequently, leveraging NFV to ease the deployment of NDN infrastructures appears as a strong mean to incite network operators to adopt this technology. In this context, the challenge we address in the ANR DOCTOR project is to fulfil the requirements needed to move NDN from a solution restricted to labs or tesbeds to a fully operational one by developing NDN-specific Virtual Network Functions (VNF).

In this effort, one of the main first questions which arise is about the integration of NDN into the existing Internet, and particularly the collocation of NDN with IP and HTTP. We think that a good way to deploy NDN consists in creating virtualized NDN island that can be crossed by specific content-related traffic, such as HTTP, and thus benefit from NDN properties (caching, aggregation, etc.). We proposed and developed an early version of a fully-capable NDN/HTTP gateway that can seamlessly connect a NDN network to the rest of the World Wide Web. This work was published and demonstrated at the ACM-ICN conference [47].

6.5. Multi-modeling and co-simulation

Participants: Laurent Ciarletta [contact], Olivier Festor, Ye-Qiong Song, Yannick Presse, Julien Vaubourg, Alexandre Tan, Benjamin Segault, Thomas Paris.

Vincent Chevrier (former Maia team, Dep 5, LORIA) is a collaborator and the correspondant for the MS4SG/MECSYCO project, Benjamin Camus, and Christine Bourjot (former MAIA team, Dep 5, LORIA) are collaborators for AA4MM/MECSYCO. Julien Vaubourg and Thomas Paris's PhDs are under the co-direction of V. Chevrier and L. Ciarletta.

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.

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 proposed the AA4MM meta-model [52] that solves the core challenges of multimodeling 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. In the MECSYCO-NG (formerly MS4SG, Multi Simulation for Smart Grids) projet which involves some members of the former MAIA team, Madynes and EDF R&D on smart-grid simulation, we developed a proof of concepts for a smart-appartment case that serves as a basis for building up use cases, and we have worked on some specific cases provided by our industrial partner.

In 2016 we worked on the following research topics:

- Assessment and evaluation of complex systems.
- Cyber Physical Systems.

  We have pursued the design and implementation of the Aetournos platform at Loria. The collective movements of a flock of flying communicating robots / UAVs, evolving in potentially perturbed environment constitute a good example of a Cyber Physical System.

We have maintained thanks to the ADT UASS a set of tools: multi-simulation behavior / network / physics and generic software development using ROS (Robot Operating System). The UAVs carry a set of sensors for location awareness, their own computing capabilities and several wireless networks.

- MS4SG / MECSYCO-NG opportunity to link simulations tools with a strong focus on FMI (Functional Mockup Interface) and network simulators (NS3/Omnet++) thanks to our MECSYCO (formerly AA4MM) framework. We have so far successfully applied our solution to the simulation of smart apartment complex and to combine the electrical and networking part of a Smart Grid. The AA4MM software is now MECSYCO and has seen major improvements in 2016 thanks to the ressources provided by the MECSYCO-NG project in collaboration with EDF R&D (http://www.mecsyco.com).

  Starting from domain specific and heterogenous models and simulators, the MECSYCO suite allows for multi *systems* integration at several levels: conceptual, formal and software. A couple of visualization tools have been developed as proof of concepts both at run-time and post-mortem.

  We have developed software components and plugins that interconnects within MECSYCO heterogeneous simulators from different domains: FMU (working with the 1.0 and 2.0 FMI standard for CoSimulation) ou non-FMU such as NS3 or Omnet++.

  Several EDF oriented advanced use cases have demonstrated multi-simulations.

In addition to technical reports [41], several publications have been accepted in 2016 on these subjects [25], [13] and [34].

6.6. Pervasive or Ubiquious Computing

Participants: Laurent Ciarletta [contact], Olivier Festor, Ye-Qiong Song, Emmanuel Nataf, Thomas Paris, Benjamin Segault, Antoine Richard, Petro Aksonenko.

P. Aksonenko PhD is under the co-direction of L. Ciarletta and Patrick Henaff from Loria Dep 5. Thomas Gurriet, now PhD student at Georgia Tech under the supervision of Prs Eric Feron and Aaron Ames is contributing to the topic of CPS safety.

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.

These systems, increasingly numerous and heterogeneous, are embedded in the fabric of our daily lives. Our initial subject of interest is to study them with regards to their complexity: Those 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 their surroundings and the environment. Secondly, the potential multiplicity and heterogeneity of devices, services, communication protocols, and the constant mobility and reorganization also need to be addressed. Thirdly we are aking into account their dynamcity, with regards to their mobility and evolving context.

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.

In 2016 we mainly worked on the Cyber Physical Systems.

We maintained the Aetournos platform at Loria in collaboration with 6PO and the support of ADT UASS. We are studying the collective movements of a flock of flying communicating robots / UAVs, evolving in potentially perturbed environment constitute a good example of a Cyber Physical System.

The effort put in the UAVs gathers academic and research ressources from the Aetournos platform, the Inria ADT R2D2 and the 6PO project, while applied, industrial and more R&D projects have been pursued this year (Medical Express / Outback Joe Search and Rescue Challenge, Alerion, Hydradrone, and a CIFRE PhD with Thales for example) .

This also led to two new accepted projects:

- one Interreg “Grone”, a generic project about drones in industrial and agricultural environments, started in October 2016
- and one FUI22 “CEOS”, about insuring safety in UAVs at the system level that will start in 2017

  One of the emerging topic in this area is the safety of Mobile IoT / CPS with regards to their environment and users. This gave first results on how to design the internal communication system [21], the overal system [15], specific safety solutions [14] and a US Patent has been filled on a termination system led by Georgia Tech [Optimal Emergency Termination System for Unmanned Aerial Vehicles by Destructive Rotor Surface Reduction, Application No.: 62/378,923].
- Smart * (MECSYCO)

  We have studied scientific problems around models and simulators composition. We have also looked into practical and implementation issues in the frame of our MECSYCO /AA4MM solutions. We have added to our Smart Grid scenarios a smart appartment complex use case.
- (Very Serious) Gaming: Starburst Gaming. During some exploratory work, we have seen the potential of these Pervasive Computing ressources in the (Very Serious) Gaming area.

6.7. Quality-of-Service

6.7.1. Self-adaptive MAC protocol for both QoS and energy efficiency

Participants: Kévin Roussel, Shuguo Zhuo, Olivier Zendra, Ye-Qiong Song [contact].

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 at light traffic, but also high throughput with self-adaptation to dynamic traffic bursts.

We have mainly contributed to enhancing the implementation of the high efficient traffic self-adaptive MAC protocols. As part of RIOT ADT project, we have improved and implemented a fully functional iQueue-MAC which provides not only the unique feature of high traffic self-adaptivity, but also the robustness by using two control channels (https://github.com/RIOT-OS/RIOT/pull/5618).

As part of LAR project, we were interested by using the Cooja/MSPSim network simulation framework for RIOT OS based platforms. We have showed that Cooja is not limited only to the simulation of the Contiki OS based systems and networks, but can also be extended to perform simulation experiments of other OS based platforms, especially that with RIOT OS. Moreover, when performing our own simulations with Cooja and MSPSim, we observed timing inconsistencies with identical experimentations made on actual hardware. Such inaccuracies clearly impair the use of the Cooja/MSPSim framework as a performance evaluation tool, at least for time-related performance parameters. The detailed results of our investigations on the inaccuracy problems, as well as the consequences of this issue, and possible ways to fix or avoid it are available in [27].

6.7.2. QoS and fault-tolerance in distributed real-time systems

Participants: Florian Greff, Laurent Ciarletta, Arnauld Samama [Thales TRT], Eric Dujardin [Thales TRT], Ye-Qiong Song [contact].

The QoS must be guaranteed when dealing with real-time distributed systems interconnected by a network. Not only task schedulability in processors, but also message schedulability in networks should be analyzed for validating the system design. Fault-tolerance is another critical issue that one must take into account. In collaboration with Thales TRT industrial partner as part of a CIFRE PhD work, we started a study on the real-time dependability of distributed multi-criticity systems interconnected by an embedded mesh network (RapidIO). For easing the QoS specification at the higher level, DDS middleware is used. We postulate that enhancing QoS for real-time applications entails the development of a cross-layer support of high-level requirements, thus requiring a deep knowledge of the underlying networks. This year, we proposed and implemented a new simulation/emulation/experimentation framework called ERICA, for designing such a feature. ERICA integrates both a network simulator (Ptolemy) and an actual hardware network to allow implementation and evaluation of different QoS-guaranteeing mechanisms. It also supports real-software-in-the-loop, i.e. running of real applications and middleware over these networks [21].

We have also dealt with mesh networking of embedded components. Our approach is to allow applications to make online real-time flow resource requests and consequently dynamically allot network resources according to these requirements. To this end, additional mechanisms must be provided in order to meet the real-time constraints while the platform remains as dynamic as possible. We gather these mechanisms into a Software-Defined Real-time Network (SDRN) paradigm. The online admission control and pathfinding algorithms have been developed allowing the controller to dynamically configure the real-time network nodes. We have evaluated several pathfinding algorithms.

6.7.3. Wireless sensor and actuator networks

Participants: Lei Mo, Adrian Guenard, Yifei Qi [Zhejiang University], Jiming Chen [Zhejiang University], Ye-Qiong Song [contact].

Wireless sensor and actuator networks provide a key technology for fully interacting within a CPS (Cyber-Physical System). However, the introduction of the mobile actuator nodes in a network rises some new challenging issues. In this context, we addressed two important issues: the multiple target tracking using both fixed and mobile sensors and the optimal scheduling of mobile wireless energy chargers (actuators) for fixed sensor nodes.

In the low-cost and large-scale deployment of mobile sensor nodes for target tracking, due to the constraints of limited sensing range, it is of great importance to design node coordination mechanism for reliable tracking so that at least the target can always be detected with a high probability, while the total network energy cost can be reduced for longer network lifetime. In [3], we dealt with this problem considering both the unreliable wireless channel and the network energy constraint. We transfer the original problem into a dynamic coverage problem and decompose it into two subproblems. By exploiting the online estimate of target location, we first decide the locations where the mobile nodes should move into so that the reliable tracking can be guaranteed. Then, we assign different mobile nodes to each location in order that the total energy cost in terms of moving distance can be minimized. Extensive simulations under various system settings have shown the effectiveness of our solution.

We also investigated the multiple mobile chargers coordination problem that is minimizing the energy expenditure of the mobile chargers while guaranteeing the perpetual operation of the wireless sensor network. We extended our previous result (published in IPCCC2015) by taking into account mobile charger's charging ability. We formulated this problem as a mixed-integer linear program (MILP), and proposed a novel decentralized method which is based on Benders decomposition. The convergence of proposed method is analyzed theoretically. Simulation results demonstrate the effectiveness and scalability of the proposed method.

6.7.4. NDN performance evaluation

Participants: Thibault Cholez [contact], Xavier Marchal, Olivier Festor.

NDN (Named Data Networking) is a promising protocol that can help to reduce congestion at Internet scale by putting content at the center of communications instead of hosts. NDN can also natively authenticate transmitted content with a mechanism similar to website certificates that allows clients to assess the original provider. But this security feature comes at a high cost, as it relies heavily on asymmetric cryptography which affects server performance when NDN Data are generated. This is particularly critical for many services dealing with real-time data (VOIP, live streaming, etc.), but current tools are not adapted for a realistic server-side performance evaluation of NDN traffic generation when digital signature is used. We propose a new tool, NDNperf, to perform this evaluation and show that creating NDN packets is a major bottleneck of application performances. On our testbed, 14 server cores only generate $\sim$400 Mbps of new NDN Data with default packet settings. We gave recommendation about the configuration of NDN (packet size, cryptographic function) and proposed practical improvements to the NDN library that all combined can vastly increase the performance of server-side NDN Data generation (x8,5). This work was published in the ACM-ICN conference [22].

ALICE Project-Team

7. New Results

7.1. Hexahedral-dominant Remeshing

Participants: Dmitry Sokolov, Nicolas Ray, Bruno Lévy, Maxence Reberol

Representing the geometry of complex objects in a computer is usually achieved by a mesh: the object is decomposed in cells that have a simple geometry. Each cell is defined by a set of facets. The simplest choice is to use meshes with tetrahedral cells that are relatively easy to produce and to work with. However, some applications involving numerical simulations better work with hexahedral cells. Such hexahedral meshes are very difficult to produce, even when it is completely done by a designer. Our objective is to relax the intrinsic difficulties of full hexahedral remeshing by allowing the process to generate a few tetrahedra in the hexahedral mesh (hexahedral-dominant meshes). Our approach is to produce as many hexahedra as possible by filling most of the volume with a deformed 3D grid, and to rely on more classic meshing techniques everywhere else. We also develop tools to evaluate how our remeshing impacts results of FEM simulations.

7.1.1. Generation of Hexahedral-dominant Meshes

The traditional approach to produce hexahedral dominant meshes is by advancing front: first hexahedra are produced near the object boundary, then additionals hexahedra are attached to them. An alternative solution is to consider an hexahedral mesh as a deformed 3D grid: the hexahedral remeshing problem is then restated as finding the (geometric) deformation that will transform the hexahedral mesh into the regular grid. This approach is able to generate very good hexhaderal meshes, but it is often impossible to entirely remesh the input object.

Our objective is to produce hexahedra from the mapping approach, then complete the mesh with traditional approaches that may leave some tetrahedra. We proposed a first solution [9]: we compute a mapping, extract the vertices of the deformed 3D grid, generate a tetrahedral mesh having these vertices, then merge sets of tetrahedra into hexahedra with an extension of [25]. Using the mapping as a heuristic made this solution very competitive with other hexahedral dominant methods. We are now developing a software pipeline that makes it easy for different algorithms (frame field, mapping and classic remeshing) to work together. With a simple implementation of each step, we already observe better performances than previous works, and we foresee many opportunities to improve it.

7.1.2. Impact on FEM Performance

It is admitted by our scientific community that hexahedral meshes are better than tetrahedral meshes for some FEM simulation. We would like to demonstrate evidence of this belief, including fair comparisons with equal running time and/or result accuracy, with the best function basis for each case. For hexahedral dominant meshes, we have developed a new specific function basis devoted to properly link tetrahedral and hexahedral elements. Using a combination of tri-linear and quadratic hexahedra, we can build an approximation space made of continuous functions, even at non-conforming interfaces between hexahedra and tetrahedra. But in practice, hexahedral-dominant meshes are mainly useful to mesh complicated 3D domains. In such cases, there are no analytical solutions of partial differential equations and thus it is not straightforward to evaluate the accuracy of a new numerical method. To measure the differences between finite element solutions defined on different meshes of the same 3D model, we are developing a fast and efficient sampling method which exploits GPU hardware. These topics are addressed in the (ongoing) Ph.D. thesis of Maxence Reberol.

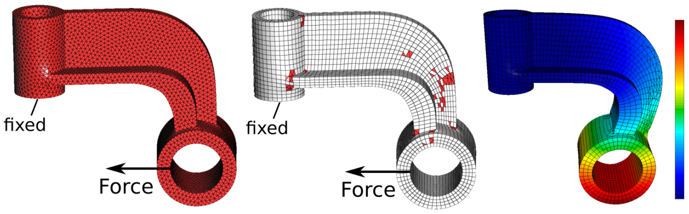

Figure 2. Mechanical problem on the Hanger 3D model. (left) Sandard tetrahedral mesh. (center) Our hex-dominant mesh, hex in gray and tet in red. (right) Solution of the problem with mixed hexahedral-tetrahedral finite elements, color is the amplitude of the displacement.

7.2. Optimal transport

Participant: Bruno Lévy

7.2.1. Optimal transport:

Optimal Transport is not only a fundamental problem with a rich structure, but also a new computational tool, with many possible applications. To name but a few, applications of Optimal Transport comprise image registration, reflector and refractor design, histogram interpolation, artificial intelligence. In astrophysics, it is used by Early Universe Reconstruction, a difficult inverse problem that reconstructs the time evolution of the universe from the observed current state. It can be also used in meteorology, to simulate certain phenomena (semi-geostrophic currents). It is also the main component of solvers for certain equations, based on a variational formulation that leads to a gradient flow. All these applications and future developments depend on a single component: an efficient solver for the Monge-Ampère equation. We developed a new algorithm that overcome by several order of magnitude the speed of the classical "auction algorithm" (that solves in $O(n\log(n))$ a discrete version of the problem). The *semi-discrete* version of the problem that we study can be solved by extremizing a smooth objective function, thus a significantly faster speed is obtained as compared to the previous combinatorial algorithm. This year we improved our Quasi-Newton solver and replaced it with a Full-Newton solver, that gains one additional order of magnitude in speed, and we can solve semi-discrete problems with 1 million Dirac masses in a matter of minutes. We also experimented with applications of this solver to fluid simulation. Last winter (December 2015) Wenping Wang visited Nancy, and we discussed several ideas on Optimal Transport. We proposed together this year (2016) a new method to sample a surface with a power diagram [31]. The positions of the samples are optimized by a criterion similar to centroidal Voronoi tessellations, and the associated weights are used to control the areas of the power cells with prescribed values. We give the expressions of the derivatives of the combined objective function, and propose a quasi-Newton algorithm to optimize it. We describe several applications of the algorithm.

7.3. 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 that clusters

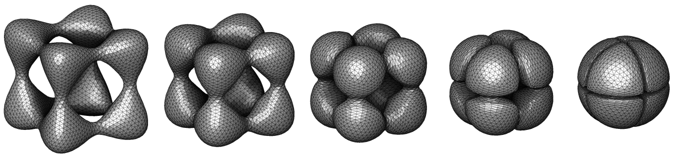

Figure 3. Semi-discrete optimal transport between a shape and a sphere, computed by our algorithm

a point cloud into elementary plant units such as internodes, petioles and leaves. The algorithm creates a graph (points + edges) to recover plausible neighboring relationships between the points and embeds this graph in a spectral space in order to segment the point-cloud into meaningful elementary plant units. This work has been published in the International Journal of Remote Sensing [6].

7.4. Surface Reconstruction From 3D Point Clouds

Participants: Dobrina Boltcheva, Bruno Lévy

We have developed a practical reconstruction algorithm that generates a surface triangulation from an input pointset. In the result, the input points appear as vertices of the generated triangulation. The algorithm has several desirable properties: it is very simple to implement, it is time and memory efficient, and it is trivially parallelized. On a standard hardware (core i7, 16Gb) it takes less than 10 seconds to reconstruct a surface from 1 million points, and scales-up to 36 million points (then it takes 350 seconds). On a smartphone (ARMV7 Neon, quad core), it takes 55 seconds to reconstruct a surface from 900K points. The algorithm computes the Delaunay triangulation of the input pointset restricted to a "thickening" of the pointset (similarly to several existing methods, like alpha-shapes, crust and co-cone). By considering the problem from the Voronoi point of view (rather than Delaunay), we use a simple observation (radius of security) that makes the problem simpler. The Delaunay triangulation data structure and associated algorithms are replaced by simpler ones (KD-Tree and convex clipping) while the same set of triangles is provably obtained. The restricted Delaunay triangulation can thus be computed by an algorithm that is not longer than 200 lines of code, memory efficient and parallel. The so-computed restricted Delaunay triangulation is finally post-processed to remove the non-manifold triangles that appear in regions where the sampling was not regular/dense enough. Sensitivity to outliers and noise is not addressed here. Noisy inputs need to be pre-processed with a pointset filtering method. In the presented experimental results, we are using two iterations of projection onto the best approximating plane of the 30 nearest neighbors (more sophisticated ones may be used if the input pointset has many outliers).

This work has been published in the Research Report [13] and is currently in revision for Eurographics 2017.

7.5. Microstructures for additive manufacturing

Participants: Jonas Martinez, Sylvain Lefebvre

Nowadays, there is a big interest in the functional optimization of microstructures for additive manufacturing, as reflected by the high number of recent publications on the subject. This also comes not only from research but also industry, as controlling the macroscopic elasticity of materials has a wide range of industrial applications. For instance, to fabricate flexible prosthetic body parts, or to produce rigid but porous prosthetics for surgery. In particular, controlling material elasticity will enable the design of lightweight and resistant materials, and in turn, reduce material consumption.

Most of the existing software either optimize for periodic tilings of microstructures, or generate random microstructures without precise control of their functionality. We recently introduced a method [7] to generate stochastic structures (figure 4) while having unique computational advantages, and precisely controlling their functionality. Our optimization approach of stochastic porous structures deviates significantly from both the periodic tiling of microstructures and the optimization of macrostructures, by making a link between microstructures, and procedural solid textures with controlled statistics in Computer Graphics. We believe there are many other such structures left to be discovered, and hope our work will spark further interest in procedurally generated, stochastic microstructures.

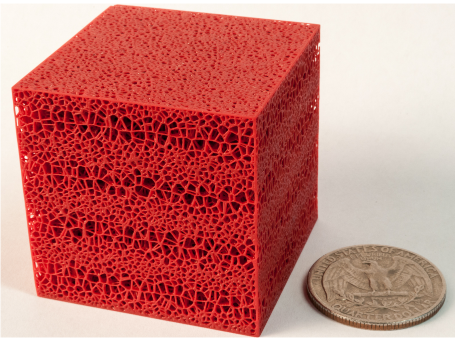

Figure 4. Anisotric microstructures

7.6. Towards Zero-Waste Furniture Design

Participants: Bongjin Koo, Jean Hergel, Sylvain Lefebvre, Niloy J. Mitra.

This project considered the optimization of parametric models of furniture to reduce the wastage of material used to fabricate the model. Our approach uses a 2D packing algorithm to pack the different parts of the furniture in a wooden plank. Then we optimize locally the wastage by editing smoothly the parameters with only moving smoothly the parts in the packing space. We produced full size objects with laser cutter to prove the efficiency of our method. This work has been accepted in Transaction on Visualization and Computer Graphics.

7.7. Anti-aliasing for fused filament deposition

Participants: Hai-Chuan Song, Nicolas Ray, Dmitry Sokolov, Sylvain Lefebvre

Layered manufacturing inherently suffers from staircase defects along surfaces that are gently sloped with respect to the build direction. Reducing the slice thickness improves the situation but never resolves it completely as flat layers remain a poor approximation of the true surface in these regions. In addition, reducing the slice thickness largely increases the print time. In this project we focus on a simple yet effective technique to improve the print accuracy for layered manufacturing by filament deposition. Our method [16] works with standard three-axis 3D filament printers (e.g. the typical, widely available 3D printers), using standard extrusion nozzles. It better reproduces the geometry of sloped surfaces without increasing the print time. Our key idea is to perform a local anti-aliasing, working at a sub-layer accuracy to produce slightly curved deposition paths and reduce approximation errors. We show that the necessary deviation in height compared to standard slicing is bounded by half the layer thickness. Therefore, the height changes remain small and plastic deposition remains reliable. We further split and order paths to minimize defects due to the extruder nozzle shape, avoiding any change in the existing hardware. We apply and analyze our approach on 3D printed examples, showing that our technique greatly improves surface accuracy and silhouette quality while keeping the print time nearly identical.

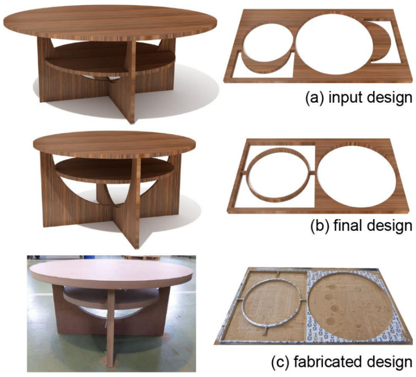

Figure 5. Our technique modifies the parameters of the input design (a) to improve the packing and waste less material (b). The produced furniture is shown in (c).

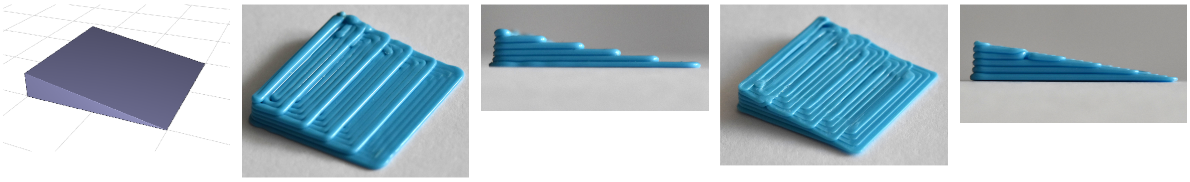

Figure 6. Printing a wedge model clearly reveals the staircase defects that plague 3D printing. (a) Input 3D model; the bottom edge length is 20mm and the angle of the incline plane is 10. (b) Global view and (c) side view of a standard, flat layer printed result. (d) Global view and (e) side view of our anti-aliased printed result, revealing the improvement in surface accuracy and silhouette smoothness

LARSEN Team

7. New Results

7.1. Lifelong Autonomy

7.1.1. PsyPhINe: Cogito Ergo Es

Participant: Amine Boumaza.

PsyPhINe is an interdisciplinary and exploratory project (see 8.1.1) between philosophers, psychologists and computer scientists. The goal of the project is related to cognition and behavior. Cognition is a set of processes that are difficult to unite in a general definition. The project aims to explore the idea of assignments of intelligence or intentionality, assuming that our intersubjectivity and our natural tendency to anthropomorphize play a central role: we project onto others parts of our own cognition. To test these hypotheses, our aim is to design a "non-verbal" Turing Test, which satisfies the definitions of our various fields (psychology, philosophy, neuroscience and computer science) using a robotic prototype. Some of the questions that we aim to answer are: is it possible to give the illusion of cognition and/or intelligence through such a technical device? How elaborate must be the control algorithms or "behaviors" of such a device so as to fool test subjects? How many degrees of freedom must it have?

Last year, an experimental robotic device was designed and built, and an experimental campaign with human subject was conducted. The experiments consisted in recording the interactions of the subjects with the robot when realizing a task. The results of the experiments are under analysis and will partly be presented at the second edition of the PsyPhINe workshop organized by the group, gathering top researchers from philosophy, anthropology, psychology and computer science to discuss and exchange on our methodology (see 9.1.1.1).

7.1.2. Localisation of robots on load-sensing floor

Participants: François Charpillet, Francis Colas, Vincent Thomas.

The use of floor-sensors in ambient intelligence contexts began in the late 1990's. We designed such a sensing floor in Nancy in collaboration with the Hikob company (http://www.hikob.com) and Inria SED. This is a load-sensing floor which is composed of square tiles, each equipped with two ARM processors (Cortex m3 and a8), 4 load cells, and a wired connection to the four neighboring cells. Ninety tiles cover the floor of our experimental platform (HIS).

This year, with Alexis Grall (master student from Enseirb-Matmeca), we have focused on identifying localisation and tracking scenarios involving several robots and on collecting data corresponding to instantiation of these scenarios. These data originated from the sensing tiles but also from Qualisys motion capture system in order to have information about ground-truth. We have also focused on basic algorithms (for instance, Kalman filter) to tackle the issue of tracking targets, but we plan to investigate more elaborate strategies for dealing with sensor discontinuity (for example, when the robot leaves or enters a tile) and multi-traget tracking (Joint Probability Data Association Filter algorithm [52]).

With Mohammad Rami Koujan, we also started to apply deep-learning techniques on those sequential data in order to compare model-based and model-free approaches. This work included some long-term data collection with a randomized behavior in order to have enough training data.

7.1.3. Active sensing and multi-camera tracking

Participants: Olivier Buffet, François Charpillet, Vincent Thomas.

The problem of active sensing is of paramount interest for building self awareness in robotic systems. It consists of a system to make decisions in order to gather information (measured through the entropy of the probability distribution over unknown variables) in an optimal way.

This problem we are focusing on consists of following the trajectories of persons with the help of several controllable cameras in the smart environment. This is a difficult problem since the set of cameras cannot simultaneously cover the whole environment, some persons can be hidden by obstacles or by other persons, and 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 probabilistic decision processes in partial observability (POMDP - Partially Observable Markov Decision Processes) and particle filters. In the past, we have proposed an original formalism rho*-POMDP* and new algorithms for representing and solving active sensing problems [38] by tracking several persons with fixed camera based on particle filters and Simultaneous Tracking and Activity Recognition approach [45].

This year, we have focused on investigating the issue of solving the active sensing problem with controllable cameras. Approaches based on Monte-Carlo Tree Search algorithms (MCTS) like POMCP [54] are currently investigated for adressing the combinatorial explosion of the state space to consider (which is the space of probability distributions over all the possible states of the system).

7.1.4. Audio Source Localization

Participants: François Charpillet, Francis Colas, Van Quan Nguyen.

We collaborate on this subject with Emmanuel Vincent from the Multispeech team (Inria Nancy - Grand Est).

We considered, here, the task of audio source localization using a microphone array on a mobile robot. Active localization algorithms have been proposed in the literature that can estimate the 3D position of a source by fusing the measurements taken for different poses of the robot. A typical implicit assumption in the literature is that the sound source is active, but a lot of real sound sources are actually intermittent. Systems of activity detection exist but cannot reach perfect accuracy. In this work, we propose a new mixture Kalman filter that explicitly includes the discrete activity of the source in the estimated state vector, alongside the continuous states such as the position of the robot or the sound source. We take into account the imperfection of activity detection systems in order to show that we have better accuracy than the state of the art [26].

This work is led through the PhD Thesis of Van Quan Nguyen under the supervision of Emmanuel Vincent and Francis Colas.

7.1.5. Learning for damage recovery

Participants: Jean-Baptiste Mouret, Konstantinos Chatzilygeroudis, Vassilis Vassiliades, Dorian Goepp.

In 2015, we introduced a novel algorithm that allows robots to learn by trial-and-error when they are damaged [42]. In 2016, we extended this algorithm to make it easier to deploy it in real-life situations and real systems:

- We added “safety constraints” so that the learning algorithm both maximizes the post-damage performance and minimizes the probability of breaking the robot during the learning process; we demonstrated this extension with a simulation of the iCub robot, which is a fragile and expensive robot (around 250,000 euros) for which we would like to use our learning algorithms [33].
- We proposed a novel algorithm that does not require to reset the robot to its starting position between each trial [40], which allows the damaged robots to “learn while doing”. We demonstrated this algorithm on our 6-legged walking robot.
- We extended the MAP-Elites algorithm, that is, the evolutionary algorithm that we use to generate prior probability distributions for our online learning algorithm, to scale-up to high-dimensional search spaces [59]. The algorithm is based on central Voronoi tesselations (CVT). In addition, we investigated the influence of the encoding (representation of the controller) on the performance of MAP-Elites [30].

7.1.6. Interactions with biology

Participant: Jean-Baptiste Mouret.

We continued our on-going collaborations with biologists.

- *The Evolutionary Origins of Hierarchy.* Hierarchical organization—the recursive composition of sub-modules—is ubiquitous in biological networks, including neural, metabolic, ecological, and genetic regulatory networks, and in man-made systems such as large organizations and the Internet. In this contribution, we showed that the pressure to minimize the connection costs in network can explain the evolution of hierarchical and modular biological networks [21]; this result extends our previous work on the evolutionary origins of modularity in biological networks [41]. (Collaboration with Jeff Clune, University of Wyoming, USA).
- *Animal-robot interaction.* We worked with a team based in Rennes to perform preliminary experiments about animal-robot attachment (here with a gallinaceous bird) [16].

7.1.7. Learning for whole-body motions

Participants: Serena Ivaldi, Valerio Modugno.

Within the European project CoDyCo, we studied how to combine learning, dynamics, and control for redundant robots. In [25], we proposed a framework to automatically optimize the evolution in time of soft task priorities for multi-task controllers. The motivation of the work was to propose a way to automatate the manual optimization procedure of task priorities and weights, that is classically done by control experts and is time consuming. In [24], we improved the framework by using constrained stochastic optimization algorithms to optimize the task priorities while ensuring that the system constraints (robot and problem setting) are never violated. We showed the results on our robot iCub. Our master student Ugo Chervet contributed to the simulations of this paper.

7.2. Natural Interaction with Robotic Systems

7.2.1. Human Activity recognition on load-sensing floor

Participant: François Charpillet.

In the framework of a collaboration with Lebanese University and CRIStAL laboratory, Lille, we have evaluated this year the capability of the load-sensing floor that we have designed in Nancy, to adress fall detection and activity recognition for elderly people living alone at Home.

The Inria-Nancy sensing floor consists of 104 tiles (60*60 cm). Each tile is equipped with a 3-axis accelerometer in the center of the tile, and four force sensors (strain gauge load cells) positioned at each corner.

The pressure sensors measure the load forces exerted on the floor that can be used to determine, for example, the center of pressure of objects, robots or human beeing on the floor.

This year we have demonstrated that we can also determine the posture or activiy of the monitored person (walking, sitting, standing, falling, etc.) by combining the pressure amount, the pressure duration on a tile, the 3-axis acceleration using a relatively simple algorithm [10], [11].

7.2.2. Human Activity recognition with depth camera

Participants: François Charpillet, Xuan Son Nguyen.

This year, we proposed a new local descriptor for action recognition in depth images. The proposed descriptor relies on surface normals in 4D space of depth, time, spatial coordinates and higher-order partial derivatives of depth values along spatial coordinates. In order to classify actions, we follow the traditional Bag-of-words (BoW) approach, and propose two encoding methods termed Multi-Scale Fisher Vector (MSFV) and Temporal Sparse Coding based Fisher Vector Coding (TSCFVC) to form global representations of depth sequences. The high- dimensional action descriptors resulted from the two encoding methods are fed to a linear SVM for efficient action classification. Our proposed methods are evaluated on two public benchmark datasets, MSRAction3D and MSRGesture3D. The experimental result shows the effectiveness of the proposed methods on both the datasets.

7.2.3. Human Posture Recognition

Participants: François Charpillet, Abdallah Dib, Alain Filbois, Thomas Moinel.

Human pose estimation in realistic world conditions raises multiple challenges such as foreground extraction, background update and occlusion by scene objects. Most of existing approaches were demonstrated in controlled environments. In this work, we propose a framework to improve the performance of existing tracking methods to cope with these problems. To this end, a robust and scalable framework is provided composed of three main stages. In the first one, a probabilistic occupancy grid updated with a Hidden Markov Model used to maintain an up-to-date background and to extract moving persons. The second stage uses component labelling to identify and track persons in the scene. The last stage uses a hierarchical particle filter to estimate the body pose for each moving person. Occlusions are handled by querying the occupancy grid to identify hidden body parts so that they can be discarded from the pose estimation process. We provide a parallel implementation that runs on CPU and GPU at 4 frames per second. We also validate the approach on our own dataset that consists of synchronized motion capture with a single RGB-D camera data of a person performing actions in challenging situations with severe occlusions generated by scene objects. We make this dataset available online (http://www0.cs.ucl.ac.uk/staff/M.Firman/RGBDdatasets/).

7.2.4. Evaluation of control interfaces by non-experts

Participants: Serena Ivaldi, François Charpillet.

In this work, we address the question of user preference for a robotic interface by non-experts (or naive users without training in robotics), after one single evaluation of such an interface on a simple task. This refers to situations when non-experts face the decision of adopting a robot for episodic use (i.e., not a regular continuous use as workers in factories): the ease of use of an interface is crucial for the robot acceptance. We also probe the possible relation between user performance and individual factors. After a focus group study, we chose to compare the robotic arm joystick and a graphical user interface. Then, we studied the user performance and subjective evaluation of the interfaces during an experiment with the robot arm Jaco and 40 healthy adults. Our results show that the user preference for a particular interface does not seem to depend on their performance in using it: for example, many users express their preference for the joystick while they are better performing with the graphical interface. Contrary to our expectations, this result does not seem to relate to the user's individual factors that we evaluate, namely desire for control and negative attitude towards robots.

The preliminary results of this work are published in [23]. A journal paper with the complete results is in preparation. The work was conducted with the master students Sebastian Marichal and Adrien Malaisé.

7.2.5. Robot acceptance and trust

Participant: Serena Ivaldi.

We continued our collaboration with psychologists.

- *Trust as a measure of robot acceptance*: together with the research group of Elisabetta Zibetti (Université de Paris 8), we proposed trust as a main indicator of acceptance in decision-making tasks characterized by perceptual uncertainty (e.g., evaluating the weight of two objects) and socio-cognitive uncertainty (e.g., evaluating which is the most suitable item in a specific context). We measured trust by the participants' conformation to the iCub's answers to specific questions. We found that participants conformed more to the iCub's answers when their decisions were about functional issues than when they were about social issues. Moreover, the few participants conforming to the iCub's answers for social issues also conformed less for functional issues. Trust in the robot's functional knowledge does not thus seem to be a pre-requisite for trust in its social knowledge. Finally, desire for control, attitude towards social influence of robots and type of interaction scenario did not influence the trust in iCub. The results have been published in [13].
- *Acceptance of assistance robots in EHPADs by professional caregivers*: together with Sophie Nertomb (Université de Lorraine), we started a dialogue with professional caregivers to probe their acceptance and positive/negative attitude towards an assistance robot as a collaborator in an EHPAD.

From the first focus group, we found that caregivers are rather positive in adopting a robot to get assistance in some daily tasks with the patients, and they would prefer a social robot such as Pepper rather than a functional robot arm, because they believe it could be more useful and would be better accepted by patients. The results of our preliminary investigation were presented in [22].

7.2.6. *Individual factors and social/physical signals*

Participant: Serena Ivaldi.

We finalized our study about the influence of individual factors in the production of social signals during human-humanoid interaction on a collaborative assembly task. We found that the more people are extrovert, the more and longer they tend to talk with the robot, and the more people have a negative attitude towards robots, the less they will look at the robot face and the more they will look at the robot hands where the assembly and the contacts occur. Our results confirm and provide evidence that the engagement models classically used in human-robot interaction should take into account attitudes and personality traits. The results are published in [15].

We started to study the influence of individual factors on physical signals and collaborative movement. We made interesting observations, for example the influence of age and negative attitude towards robots in the amount of exchanged forces. Part of the analysis was performed by the master student Anthony Voilqué. A paper describing our findings is in preparation.

7.2.7. *Learning gait models with cheap sensors for applications in EHPADs*

Participants: Serena Ivaldi, François Charpillet, Olivier Rochel.

Thanks to the MITACS-Inria grant, we started a collaboration with Prof. Dana Kulic in University of Waterloo on the topic of learning gait models with cheap sensors. Jamie Waugh, master student, visited us for 3 months to start a data collection protocol where several sensors are used to monitor the human gait under different conditions. The aim is to learn gait parameters with different sensors, such as IMUs and Kinect cameras, and to provide quantitative comparison of the accuracy of the estimation provided by the different sensors. As ground truth, the Qualisys motion capture and the Gaitrite walking mat are used. The final goal of the project is to be able to deliver algorithms for estimating gait based on cheap sensors that could be used on a daily basis in healthcare facilities such as EHPADs.

MAGRIT Project-Team

6. New Results

6.1. Matching and localization

Participants: Marie-Odile Berger, Antoine Fond, Pierre Rolin, Gilles Simon, Frédéric Sur.

Pose initialization

Estimating the pose of a camera from a model of the scene is a challenging problem when the camera is in a position not covered by the views used to build the model, because feature matching is difficult in such a situation. Several viewpoint simulation techniques have been recently proposed in this context. They generally come with a high computational cost, are limited to specific scenes such as urban environments or object-centered scenes, or need an initial guess for the pose. In [24], we have proposed a viewpoint simulation method well suited to most scenes and query views. Two major problems have been addressed: the positioning of the virtual viewpoints with respect to the scene, and the synthesis of geometrically consistent patches. Experimental results showed that patch synthesis dramatically improves the accuracy of the pose in case of difficult registration, with a limited computational cost.

Facade detection and matching

Planar building facades are semantically meaningful city-scale landmarks. Such landmarks are essential for localization and guidance tasks in GPS-denied areas which are common in urban environments. Detection of facades is also key in augmented reality systems that allow for the annotation of prominent features in the user's view. We introduced several "facadeness" measures of image regions and showed how to combine them to generate building facade proposals in images of urban environments [26]. We demonstrated the interest of this procedure through two applications. First, a convolutional neural network (CNN) was proposed to detect facades from a restricted list of facade proposals. We showed that this method outperforms the state-of-the-art techniques in term of adequation of the detected facades with a ground truth. In addition, the computational time is compatible with the navigation requirements. Second, we investigated image matching based on facade proposals. Considering a large set of data extracted from Google Street View, we showed that matching based on Euclidean distances between CNN descriptors outperforms the classical SIFT matching based on RANSAC-homography calculation. This work has been submitted to IEEE ICRA'2017.

A preliminary step in facade detection is the image rectification process. For that purpose, we introduced a simple and effective method to detect orthogonal vanishing points in Manhattan scenes. A key element of this approach is to explicitly detect the horizon line *before* detecting the vanishing points, which is done by exploiting accumulations of oriented segments around the horizon line. This results in a significant reduction in computation times, while keeping an accuracy comparable or superior to more complex approaches. A paper reporting on this work was published and an oral presentation was made at Eurographics'2016 [25].

6.2. Handling non-rigid deformations

Participants: Marie-Odile Berger, Jaime Garcia Guevara, Pierre-Frédéric Villard.

Simultaneous pose estimation and augmentation of elastic surface

We have proposed an original method to estimate the pose of a monocular camera while simultaneously modeling and capturing the elastic deformation of the object to be augmented [22]. Our method tackles a challenging problem where ambiguities between rigid motion and non-rigid deformation are present. This issue represents a major barrier for the establishment of an efficient surgical augmented reality where the endoscopic camera moves and organs deform. Using an underlying physical model to estimate the low stressed regions our algorithm separates the rigid body motion from the elastic deformations using polar decomposition of the strain tensor. Following this decomposition, a constrained minimization, that encodes both the optical and the physical constraints, is resolved at each frame. Results on real and simulated data proved the effectiveness of our approach.

Fusing US and CT data
3D ultrasound (3D US) is an ideal imaging modality for hepatic image-guided interventions. Yet, its limited field of view and poor in-depth image quality reduce its usefulness. Within J. Guevara's PhD thesis, we propose to reduce these limitations by augmenting the intraoperative 3D US view with a preoperative image. Our approach is automatic and does not require manual initialization or a tracking device for the 3D US probe. Moreover, by using an underlying biomechanical model, the proposed method handles significant liver deformation, even when it occurs outside the 3D US field of view. The method relies on the segmentation of a vascular tree from the preoperative and intraoperative images, and their transformation into graphs. The preoperative and partial intraoperative graphs are then matched using an algorithm based on a combined Gaussian Process regression approach and biomechanical model. The model is used to robustly select a correct match from several hypotheses generated by the Gaussian Process. Once the two graphs are matched, a deformation of the preoperative liver is driven by the local displacement field computed from the partial graph match.

Individual-specific heart valve modeling
We developed a method to semi-automatically build a mitral valve computational model from micro CT (computed tomography) scans: after manually picking fiducial points on the chordae, the leaflets were segmented and the boundary conditions as well as the loading conditions were automatically defined. Fast Finite Element Method (FEM) simulation was carried out using Simulation Open Framework Architecture (SOFA) to reproduce leaflet closure at peak systole. We developed three metrics to evaluate simulation results. We validated our method on three explanted porcine hearts and showed that our model performs well. We evaluated the sensitivity of our model to changes in various parameters. We also measured the influence of the positions of the chordae tendineae on simulation results.

6.3. Interventional neuroradiology

Participants: Marie-Odile Berger, Charlotte Delmas, Erwan Kerrien, Raffaella Trivisonne.

Tools reconstruction for 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 any brain tissue except the vasculature. In particular, since at most only two projective fluoroscopic views are available, containing absolutely no depth hint, the 3D shape of the micro-tool (guidewire, micro-catheter or micro-coil) can be very difficult, if not impossible to infer, which may have an impact on the clinical outcome of the procedure.

In collaboration with GE Healthcare, we aim at devising ways to reconstruct the micro-tools in 3D from fluoroscopy images. Charlotte Delmas has been working as a PhD CIFRE student on this subject since April 2013. A setup was designed in a view to reconstruct in 3D a deploying coil in as little X-ray dose and time as possible. It combines a fast rotation of both X-ray planes around the patient's head and a tomographic reconstruction combining an l_1-constraint to promote sparsity together with diffusion filters that promote the curvilinear nature of the coil. During this final year of her PhD thesis, various acquisition strategies and diffusion filters were evaluated [20].

Image driven simulation We consider image-driven simulation, applied to interventional neuroradiology as a coupled system of interactive computer-based simulation (interventional devices in blood vessels) and on-line medical image acquisitions (X-ray fluoroscopy). The main idea is to use the live X-ray images as references to continuously refine the parameters used to simulate the blood vessels and the interventional devices (micro-guide, micro-catheter, coil).

Raffaella Trivisonne started her PhD thesis in November 2015 (co-supervised by Stéphane Cotin, from MIMESIS team in Strasbourg) to address this research topic. Both projective and mechanical constraints were integrated in an augmented Lagrangian framework to solve the dynamical system. Experiments based on synthetic and phantom data were indicative that the shape from template problem could be solved without the need for considering collisions with the vessel surface, if an efficient tracking of the catheter in the X-ray images is available. These results were submitted for publication at a conference.

6.4. Assessing metrological performances in experimental mechanics

Participant: Frédéric Sur.

Progress was made during this year on several aspects of our collaboration with Institut Pascal on experimental mechanics. As mentioned in Section 4.3, the surface of the specimens under study are marked either by a regular grid, or by a random speckle. Displacement and strain maps are estimated by comparing images taken before and after deformation: through spectral methods (named here "the grid method") in the first case and through digital image correlation (DIC) in the latter.

Our contributions to the grid method are twofolds. First, we carefully analyzed the effect of digital sampling which causes aliasing [17]. We have proposed simple guidelines to minimize the effect of aliasing on strain maps. Second, we have mathematically characterized the properties of the analysis windows commonly used for processing grid images through the grid method [18]. It turns out that a Gaussian window has to be used, mainly because of its good concentration in both spatial and spectral domains in the sense of the Wigner-Ville transform. We eventually published a comprehensive review paper on the use of grid methods in experimental mechanics [15]

We also contributed to DIC-based methods. We have proposed new predictive formulas for the resolution of the displacement maps provided by DIC, which is mainly limited by sensor noise. These formulas take interpolation into account [12]. Indeed, displacement amplitude being often much smaller than one pixel, it is crucial to analyze the effect of the interpolation scheme. We have also proposed an experimental validation of these formula. This requires to take into account the heteroscedastic nature of sensor noise and rigid body motions caused by unavoidable vibrations [13].

MULTISPEECH Project-Team

7. New Results

7.1. Explicit Modeling of Speech Production and Perception

Participants: Yves Laprie, Slim Ouni, Vincent Colotte, Anne Bonneau, Agnès Piquard-Kipffer, Denis Jouvet, Odile Mella, Dominique Fohr, Benjamin Elie, Sucheta Ghosh, Anastasiia Tsukanova, Yang Liu, Sara Dahmani, Valérian Girard, Aghilas Sini.

7.1.1. Articulatory modeling

7.1.1.1. Acoustic simulations

The acoustic simulations play a central role in articulatory synthesis and should enable the production of all classes of sounds in a realistic manner. The production of voiced fricatives relies on a partial closure of the glottis which simultaneously creates an airflow which generates turbulence downwards from the constriction and the vibration of the vocal folds. Our acoustic simulation framework [14] has been extended to incorporate a glottal chink [29] in a self-oscillating vocal fold model. The glottis is then made up of two main separated components: a self-oscillating part and a constantly open chink. This feature allows the simulation of voiced fricatives, thanks to a self-oscillating model of the vocal folds to generate the voiced source, and the glottal opening that is necessary to generate the frication noise.

The acoustic propagation paradigm is appropriately chosen so that it can deal with complex geometries and a time-varying length of the vocal tract. Temporal scenarios for the dynamic shapes of the vocal tract and the glottal configurations were derived from the simultaneous acquisition of X-ray or MRI images and audio recording. Copy synthesis of a few French sentences [30], [31], [53] shows the accuracy of the simulation framework to reproduce acoustic cues of phrase-level utterances containing most of French phone (sound) classes while considering the real geometric shape of the speaker. For this purpose the articulatory model has been extended to offer a better precision of the epiglottis and of lips.

7.1.1.2. Acquisition of articulatory data

The acquisition of dynamic data is a key objective since speech production gestures involve the anticipation of the articulatory targets of the coming sounds. Cine-MRI represents an invaluable tool since it can image the whole vocal tract. However, speech requires a sampling frequency above 30 Hz to capture interesting information. Compressive sampling relies on partially collecting data in the Fourier space of the images acquired via MRI. The combination of compressed sensing technique, along with homodyne reconstruction, enables the missing data to be recovered [32]. The good reconstruction is guaranteed by an appropriate design of the sampling pattern. It is based on a pseudo-random Cartesian scheme, where each line is partially acquired for use of the homodyne reconstruction, and where the lines are pseudo-randomly sampled: central lines are constantly acquired and the sampling density decreases as the lines are far from the center.

7.1.1.3. Markerless articulatory acquisition techniques

With the spread of depth cameras (kinect-like systems), many researchers consider using these systems to track the movement of some speech articulators as lips and jaw. We are considering using this kind of system if it is suitable for speech production studies. For this reason, we have assessed the precision of markerless acquisition techniques when used to acquire articulatory data for speech production studies [19]. Two different markerless systems have been evaluated and compared to a marker-based one. The main finding is that both markerless systems provide reasonable results during normal speech and the quality is uneven during fast articulated speech. The quality of the data is dependent on the temporal resolution of the markerless system.

7.1.2. Expressive acoustic-visual synthesis

7.1.2.1. Expressive speech

A comparison between emotional and neutral speech was conducted using a small database containing utterances recorded in six emotional types (anger, fear, sadness, disgust, surprise and joy) as well as in a neutral pronunciation. The prosodic analysis focused on the main prosodic parameters such as vowel duration, energy and fundamental frequency (F0) level, and pause occurrences. The values of prosodic parameters were compared among the various emotional styles, as well as between emotional style and neutral style utterances. Moreover, the structuration of the sentences, in the various emotional styles, was particularly studied through a detailed analysis of pause occurrences and their length, and of the length of prosodic groups [23].

7.1.2.2. Expressive acoustic and visual speech

Concerning expressive audiovisual speech synthesis, a case study of a semi-professional actor who uttered a set of sentences for 6 different emotions in addition to neutral speech was conducted. Our purpose is to identify the main characteristics of audiovisual expressions that need to be integrated during synthesis to provide believable emotions to the virtual 3D talking head. We have recorded concurrently audio and motion capture data. The acoustic and the visual data have been analyzed. The main finding is that although some expressions are not well identified, some expressions were well characterized and tied in both acoustic and visual space [40]. The acquisition of the corpus was done with the platform software PLAVIS (cf. 9.2.12).

7.1.3. Categorization of sounds and prosody for native and non-native speech

7.1.3.1. Categorization of sounds for native speech

We examined the schooling experiences of 166 young people with disabilities, aged from 6 to 20 years old. These children and teenagers had specific language impairment : SLI (severe language impairment), dyslexia, dysorthographia. The phonemic discrimination, phonological and phonemic analysis difficulties faced in their childhoods had raised reading difficulties which constituted a major obstacle, which the pupils did not overcome. Consequently, this led them to repeat one or more grades. This rate is 18 times higher than the French average. The importance of this cycle of learning can be better understood through this data, which could also enable, if not overcoming the handicap, to at least improving their learning possibilities [64].

7.1.3.2. Digital books for language impaired children

Three digital albums for language impaired children were designed within the Handicom (ADT funded by Inria). These three prototypes focus on the importance of multimodal speech combining written words and visual clues: a 3D avatar telling the stories and coding oral language in LPC (french cued speech) for hearing impaired children. Eight speech and language therapists used one of these albums (the digital prototype *Nina fête son anniversaire* !) with 8 children who are aged 5 years: 4 hearing impaired children, 2 children with SLI and 2 children with autism. The training they experienced with these children showed that the use of the digital book can foster some capacities involved in language learning [41].

7.1.3.3. Analysis of non-native pronunciations

The IFCASL corpus is a French-German bilingual phonetic learner corpus designed, recorded and annotated in the IFCASL project (cf. 9.2.6). It incorporates data for a language pair in both directions, i.e. in our case French learners of German, and German learners of French. In addition, the corpus is complemented by two sub-corpora of native speech by the same speakers. The corpus has been finalized, and provides spoken data by about 100 speakers with comparable productions, annotated and segmented at the word and phone levels, with more than 50% of manually checked and corrected data [51].

We investigated the correct placement of lexical (German) or post-lexical (French) accents [52]. French and German differ with respect to the representation and implementation of prominence. French can be assumed to have no prominence represented in the mental lexicon and accents are regularly assigned post-lexically on the last full vowel of an accentual group. In German, prominence is considered to be represented lexically. This difference may give rise to interferences when German speakers learn French and French speakers learn German. Results of a judgment task (conducted with 3 trained phoneticians) of native and nonnative productions of French learners of German and German learners of French, all of them beginners, show that both groups have not completely acquired the correct suprasegmental structures in the respective L2 [0], since both groups are worse concerning the correct placement of prominence than the native speakers. Furthermore, the results suggest that the native pattern is one of the most important factors for wrong prominence placements in the foreign language, e.g., if the prominence placement of L1 and L2 coincide, speakers produce the smallest amount of errors. Finally, results indicate that visual display of accented syllables increases the likelihood of a correct accent placement.

7.1.3.4. Implementation of acoustic feedback for devoicing of final fricatives

In view of implementing acoustic feedback in foreign language learning we analyzed acoustic cues which could explain that final fricatives are perceived as voiced or unvoiced. The ratio of unvoiced frames in the consonantal segment and also the ratio between consonantal duration and vowel duration were measured. As expected, we found that beginners face more difficulties to produce voiced fricatives than advanced learners. Also, the production becomes easier for the learners, especially for beginners, if they practice repetition after a native speaker. We use these findings to design and develop feedback via speech analysis/synthesis technique TD-PSOLA using the learner's own voice and voiced fricatives uttered by French speakers [36]. We selected fully voiced exemplars and evaluated whether the presence of an additional schwa fosters the perception of voicing by native French speakers.

7.2. Statistical Modeling of Speech

Participants: Antoine Liutkus, Emmanuel Vincent, Irène Illina, Dominique Fohr, Denis Jouvet, Vincent Colotte, Ken Deguernel, Mathieu Fontaine, Amal Houidhek, Aditya Nugraha, Imran Sheikh, Imene Zangar, Mohamed Bouallegue, Sunit Sivasankaran.

7.2.1. Source separation

7.2.1.1. Deep neural models for source separation

We pursued our research on the use of deep learning for multichannel source separation [18]. Our technique exploits both the spatial properties of the sources as modeled by their spatial covariance matrices and their spectral properties as modeled by a deep neural network. The model parameters are alternately estimated in an expectation-maximization (EM) fashion. We used this technique for music separation in the context of the 2016 Signal Separation Evaluation Campaign (SiSEC) [39]. We also used deep learning to address the fusion of multiple source separation techniques and found it to perform much better than the variational Bayesian model averaging techniques previously investigated [17].

We wrote an article about music source separation for the general public [59].

7.2.1.2. α-stable modeling of audio signals

The alpha-harmonizable model has recently been proposed by A. Liutkus et al. [66] as the only available probabilistic framework to account for signal processing methods manipulating fractional spectrograms instead of more traditional power spectrograms. Indeed, they generalize the classical Gaussian formulation and permit to handle large uncertainties or signal dynamics, which are both common in audio.

Our work on this topic this year has notably focused on its extension to the multichannel setting, which is important for music processing and source localization. Since inference in multivariate alpha-stable distribution is a very intricate issue, the approach undertaken has focused on analysing the multichannel signals through the joint analysis of multiple scalar projections on the real line. This results in an original algorithm called PROJET that combines computational tractability with the inherent robustness of alpha-stable models [15], [34].

[0] L2 indicates the non-native language, whereas L1 indicates the native language

7.2.2. Acoustic modeling

7.2.2.1. Noise-robust acoustic modeling

In many real-world conditions, the target speech signal is reverberated and noisy. In order to motivate further work by the community, we created an international evaluation campaign on that topic in 2011: the CHiME Speech Separation and Recognition Challenge. After three successful editions [11], [55], we organized the fourth edition in 2016. We also summarized the speech distortion conditions in real scenarios for speech processing applications [42] and collected a French corpus for distant-microphone speech processing in real homes [24].

Speech enhancement and automatic speech recognition (ASR) are most often evaluated in matched (or multi-condition) settings where the acoustic conditions of the training data match (or cover) those of the test data. We conducted a systematic assessment of the impact of acoustic mismatches (noise environment, microphone response, data simulation) between training and test data on the performance of recent DNN-based speech enhancement and ASR techniques [21]. The results show that most algorithms perform consistently on real and simulated data and are barely affected by training on different noise environments. This suggests that DNNs generalize more easily than previously thought.

7.2.2.2. Environmental sounds

We explored acoustic modeling for the classification of environmental sound events and sound scenes and submitted our system to the DCASE 2016 Challenge [33].

7.2.3. Linguistic modeling

7.2.3.1. Out-of-vocabulary proper name retrieval

The diachronic nature of broadcast news causes frequent variations in the linguistic content and vocabulary, leading to the problem of Out-Of-Vocabulary (OOV) words in automatic speech recognition. Most of the OOV words are found to be proper names whereas proper names are important for automatic indexing of audio-video content as well as for obtaining reliable automatic transcriptions. New proper names missed by the speech recognition system can be recovered by a dynamic vocabulary multi-pass recognition approach in which new proper names are added to the speech recognition vocabulary based on the context of the spoken content [47]. The goal of this work is to model the semantic and topical context of new proper names in order to retrieve OOV words which are relevant to the spoken content in the audio document. Probabilistic topic models [44] and word embeddings from neural network models are explored for the task of retrieval of relevant proper names. Neural network context models trained with an objective to maximise the retrieval performance are proposed. A Neural Bag-of-Words (NBOW) model trained to learn context vector representations at a document level is shown to outperform the generic representations. The proposed Neural Bag-of-Weighted-Words (NBOW2) model learns to assign a degree of importance to input words and has the ability to capture task specific key-words [46] [45]. Experiments on automatic speech recognition of French broadcast news videos demonstrate the effectiveness of the proposed models. Further evaluation of the NBOW2 model on standard text classification tasks, including movie review sentiment classification and newsgroup topic classification, shows that it learns interesting information about the task and gives the best classification accuracies among the bag-of-words models.

7.2.3.2. Adding words in a language model

Out-of-vocabulary (OOV) words can pose a particular problem for automatic speech recognition of broadcast news. The language models (LMs) of ASR systems are typically trained on static corpora, whereas new words (particularly new proper nouns) are continually introduced in the media. Additionally, such OOVs are often content-rich proper nouns that are vital to understanding the topic. We explore methods for dynamically adding OOVs to language models by adapting the n-gram language model used in our ASR system. We propose two strategies: the first one relies on finding in-vocabulary (IV) words similar to the OOVs, where word embeddings are used to define similarity. Our second strategy leverages a small contemporary corpus to estimate OOV probabilities. The models we propose yield improvements in perplexity over the baseline; in addition, the corpus-based approach leads to a significant decrease in proper noun error rate over the baseline in recognition experiments [26].

7.2.3.3. 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 published two articles that summarize our work on the System & Contrast model for the characterization of the mid-term and long-term structure of music [12] and on the structural segmentation of popular music pieces using a regularity constraint that naturally stems from this model [20], [58]. We also proposed a new model for automatic music improvisation that combines a multi-dimensional probabilistic model encoding the musical experience of the system and a factor oracle encoding the local context of the improvisation [27].

7.2.4. Speech generation by statistical methods

Work on HMM-based Arabic speech synthesis was carried out within a CMCU PHC project with ENIT (Engineer school at Tunis-Tunisia; cf. 9.4.2.2). A first version of the system, based on the HTS toolkit (HMM-based Speech Synthesis System), is now working; and the study of the impact of some parameters is ongoing.

In parallel, the HTS system is also applied to the French language.

7.3. Uncertainty Estimation and Exploitation in Speech Processing

Participants: Emmanuel Vincent, Odile Mella, Dominique Fohr, Denis Jouvet, Baldwin Dumortier, Juan Andres Morales Cordovilla, Karan Nathwani, Ismaël Bada.

7.3.1. Uncertainty and acoustic modeling

7.3.1.1. Uncertainty in noise-robust speech and speaker recognition

In many real-world conditions, the target speech signal overlaps with noise and some distortion remains after speech enhancement. The framework of uncertainty decoding assumes that this distortion has a Gaussian distribution and seeks to estimate its covariance matrix in order to exploit it for subsequent feature extraction and decoding. A number of uncertainty estimators have been proposed in the literature, which are typically based on fixed mathematical approximations or heuristics. We finalized our work on a principled variational Bayesian approach to uncertainty estimation and showed its benefit w.r.t. other estimators for speech and speaker recognition [9]. We also pursued our work on the propagation of uncertainty in deep neural network acoustic models.

7.3.1.2. Uncertainty in other applications

Besides the above applications, we pursued our exploration of uncertainty modeling for robot audition and wind turbine control. In the first context, uncertainty arises about the location of acoustic sources and the robot is controlled to locate the sources as quickly as possible [38]. In the second context, uncertainty arises about the noise intensity of each wind turbine and the turbines are controlled to maximize electrical production under a maximum noise threshold [62].

7.3.2. Uncertainty and phonetic segmentation

7.3.2.1. Speech-text alignment

We have continued our work on determining more accurate phonetic boundaries with two new approaches based on DNN. The first approach proposes to find phonetic boundaries directly from the parameterized speech signal using an LSTM (Long Short-Term Memory) neural network. The aim of the second approach is twofold: provide confidence measures for evaluating speech-text alignment outputs and refine these outputs. One of these studies was done with the Synalp team of LORIA in the framework of the project ORFEO (cf. 9.2.5). The achieved confidence measure outperforms a confidence score (based on acoustic posterior probability) derived from a state-of-the-art text-to-speech aligner [43].

Within the IFCASL project (cf. 9.2.6), we have also developed a speech-text alignment system for German which will be integrated into the ASTALI software.

7.3.3. Uncertainty and prosody

The study of discourse particles that was initiated last year, has continued in the framework of the CPER LCHN (cf. 9.1.2). A larger set of words and expressions that can be used either as normal lexical words or as discourse particles (as for example *quoi* (what), *voilà* (there it is), ...) has been considered. For each of these words/expressions and for each speech corpus that was aligned in the ORFEO project (cf. 9.2.5), a subset of about one hundred occurrences were selected. Thanks to the CPER LCHN support, a part of these occurrences have been annotated as "discourse particle" or "non discourse particle". Detailed analysis is in progress, with respect to the function (discourse particle or not), the type of speech corpus, and the associated prosodic features.

The fundamental frequency is one of the prosodic features. Numerous approaches exist for the computation of F0. Most of them lead to good performance on good quality speech. The performance degradation with respect to noise level has been studied on reference databases, for several (about ten) F0 detection approaches. It was observed that for each algorithm, a large part of the errors are due to incorrect voiced/unvoiced decision. Studies have also been initiated for computing a confidence measure on the estimated F0 values through the use of neural network approaches.

ORPAILLEUR Project-Team

7. New Results

7.1. The Mining of Complex Data

Participants: Quentin Brabant, Miguel Couceiro, Adrien Coulet, Esther Galbrun, Nicolas Jay, Nyoman Juniarta, Florence Le Ber, Joël Legrand, Pierre Monnin, Amedeo Napoli, Justine Reynaud, Chedy Raïssi, Mohsen Sayed, My Thao Tang, Yannick Toussaint.

Keywords: formal concept analysis, relational concept analysis, pattern structures, pattern mining, association rule, redescription mining, graph mining, sequence mining, biclustering, aggregation

Pattern mining and Formal Concept Analysis are suitable symbolic methods for KDDK, that may be used for real-sized applications. Global improvements are carried out 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 complex data (e.g. textual documents, biological, chemical or medical data), involving objects with multi-valued attributes (e.g. domains or intervals), n-ary relations, sequences, trees and graphs.

7.1.1. FCA and Variations: RCA, Pattern Structures and Biclustering

Advances in data and knowledge engineering have emphasized the needs for pattern mining tools working on complex data. In particular, FCA, which usually applies to binary data-tables, can be adapted to work on more complex data. In this way, we have contributed to two main extensions of FCA, namely Pattern Structures and Relational Concept Analysis. Pattern Structures (PS [79]) allow building a concept lattice from complex data, e.g. numbers, sequences, trees and graphs. Relational Concept Analysis (RCA) is able to analyze objects described both by binary and relational attributes [90] and can play an important role in text classification and text mining.

Many developments were carried out in pattern mining and FCA for improving data mining algorithms and their applicability, and for solving some specific problems such as information retrieval, discovery of functional dependencies and biclustering. We designed new information retrieval methods based on FCA [72], text classification and heterogeneous pattern structures [71], pattern structures for structured attribute sets [67], and also a quasi-polynomial algorithm for mining top patterns w.r.t. measures satisfying special properties in a FCA framework [70]. We developed also a whole line of work on pattern structures for the discovery of functional dependencies [33], text classification and heterogeneous pattern structures [71], and fuzzy FCA as well [31]. Finally, we also proposed new visualization techniques and tools able to display important and useful information (e.g. stable concepts) from large concept lattices [28].

7.1.2. Text Mining

The thesis work of My Thao Tang [11] proposes a process where software and humans agents cooperate in knowledge discovery from different source textual types for extending a knowledge base. One challenge is that, on the one hand, knowledge discovery methods (software agents) can be run in accordance with background knowledge (or expert knowledge), at any step of the KDD process. On the other hand, human agents should be able to correct or to extend the current knowledge base. FCA is used for discovering a “class schema” (or “representation model”) within textual resources which can be either a set of attribute implications or a concept lattice. However, such a schema does not necessarily fit the point of view of a domain expert for different reasons, e.g. noise, errors or exceptions in the data. Thus, a bridge filling the possible gap between the representation model based on a concept lattice and the representation model of a domain expert is studied in [44]. The background knowledge is encoded as a set of attribute dependencies or constraints which is “aligned” with the set of implications associated with the concept lattice. Such an alignment may lead to modifications in the original concept lattice. This method can be generalized for generating lattices satisfying some constraints based on attribute dependencies in using the so-called “extensional projections”. It also allows experts to keep a trace of the changes occurring in the original lattice and the revised version, and to assess how concepts in practice are related to concepts discovered in the data.

In the framework of the Hybride ANR project (see 8.2.1.1), Mohsen Sayed proposes an original machine learning approach for identifying in literature disease phenotypes that are not yet represented within existing ontologies. The process is based on graph patterns extracted from sentences represented as dependency graphs. Phenotypes are usually expressed by complex noun phrases while traditional gazetteers recognize them only partially. The strength of graph patterns is to preserve the linguistic component bounds and to enable the identification of the complete phenotype formulation. A specific publication is currently in preparation.

7.1.3. Mining Sequences and Trajectories

Nowadays data sets are available in very complex and heterogeneous ways. Mining of such data collections is essential to support many real-world applications ranging from healthcare to marketing. This year, we completed a research work on the analysis of "complex sequential data" by means of interesting sequential patterns [13]. We approach the problem using FCA and pattern structures, where the subsumption relation ordering patterns is defined w.r.t. the partial order on sequences.

7.1.4. Redescription Mining

Among the mining methods developed in the team is redescription mining. Redescription mining aims to find distinct common characterizations of the same objects and, vice versa, to identify sets of objects that admit multiple shared descriptions [89]. It is motivated by the idea that in scientific investigations data oftentimes have different nature. For instance, they might originate from distinct sources or be cast over separate terminologies. In order to gain insight into the phenomenon of interest, a natural task is to identify the correspondences that exist between these different aspects.

A practical example in biology consists in finding geographical areas that admit two characterizations, one in terms of their climatic profile and one in terms of the occupying species. Discovering such redescriptions can contribute to better our understanding of the influence of climate over species distribution. Besides biology, applications of redescription mining can be envisaged in medicine or sociology, among other fields.

In recent work [40], we focused on the problem of pattern selection, developing a method for filtering a set of redescription to identify a non-redundant, interesting subset to present to the analyst. Also, we showcased the usability of redescription mining on an application in the political domain [50]. More specifically, we applied redescription mining to the exploratory analysis of the profiles and opinions of candidates to the parliamentary elections in Finland in 2011 and 2015.

We presented an introductory tutorial on redescription mining at ECML-PKDD in September 2016 to help foster the research on these techniques and widen their use (http://siren.mpi-inf.mpg.de/tutorial/main/).

7.1.5. E-sports analytics and subgroup discovery based on a single-player game

Discovering patterns that strongly distinguish one class label from another is a challenging data-mining task. The unsupervised discovery of such patterns would enable the construction of intelligible classifiers and to elicit interesting hypotheses from the data. Subgroup Discovery (SD) [87] is one framework that formally defines this pattern mining task. However, SD still faces two major issues: (i) how to define appropriate quality measures to characterize the uniqueness of a pattern; (ii) how to select an accurate heuristic search technique when exhaustive enumeration of the pattern space is unfeasible. The first issue has been tackled by the Exceptional Model Mining (EMM) framework [77]. This general framework aims to find patterns that cover tuples that locally induce a model that substantially differs from the model of the whole dataset. The second issue has been studied in SD and EMM mainly with the use of beam-search strategies and genetic algorithms for discovering a pattern set that is non-redundant, diverse and of high quality. In [58], we argue that the greedy nature of most of these approaches produce pattern sets that lack of diversity. Consequently, we proposed to formally define pattern mining as a single-player game, as in a puzzle, and to solve it with a Monte Carlo Tree Search (MCTS), a recent technique mainly used for artificial intelligence and planning problems. The exploitation/exploration trade-off and the power of random search of MCTS lead to an any-time mining approach, in which a solution is always available, and which tends towards an exhaustive search if given enough time and memory. Given a reasonable time and memory budget, MCTS quickly drives the search towards a diverse pattern set of high quality. MCTS does not need any knowledge of the pattern quality measure, and we show to what extent it is agnostic to the pattern language.

7.1.6. Data Privacy: Online link disclosure strategies for social networks

Online social networks are transforming our culture and world. While online social networks have become an important channel for social interactions, they also raise ethical and privacy issues. A well known fact is that social networks leak information, that may be sensitive, about users. However, performing accurate real world online privacy attacks in a reasonable time frame remains a challenging task. In [57], [26] (this work is done in cooperation with the Pesto Inria Team), we address the problem of rapidly disclosing many friendship links using only legitimate queries (i.e., queries and tools provided by the targeted social network). Our study sheds new light on the intrinsic relation between communities (usually represented as groups) and friendships between individuals. To develop an efficient attack we analyzed group distributions, densities and visibility parameters from a large sample of a social network. By effectively exploring the target group network, our proposed algorithm is able to perform friendship and mutual-friend attacks along a strategy that minimizes the number of queries. The results of attacks performed on a major social network profiles show that 5 different friendship links are disclosed in average for each single legitimate query in the best cases.

7.1.7. Aggregation

Aggregation theory is the study of processes dealing with the problem of merging or fusing several objects, e.g., numerical or qualitative data, preferences or other relational structures, into a single or several objects of similar type and that best represents them in some way. Such processes are modeled by so-called aggregation or consensus functions [82]. The need to aggregate objects in a meaningful way appeared naturally in classical topics such as mathematics, statistics, physics and computer science, but it became increasingly emergent in applied areas such as social and decision sciences, artificial intelligence and machine learning, biology and medicine.

We are working on a theoretical basis of a unified theory of consensus and to set up a general machinery for the choice and use of aggregation functions. This choice depends on properties specified by users or decision makers, the nature of the objects to aggregate as well as computational limitations due to prohibitive algorithmic complexity. This problem demands an exhaustive study of aggregation functions that requires an axiomatic treatment and classification of aggregation procedures as well as a deep understanding of their structural behavior. It also requires a representation formalism for knowledge, in our case decision rules, as well as methods for extracting them. Typical approaches include rough-set and FCA approaches, that we aim to extend in order to increase expressivity, applicability and readability of results. Direct applications of these efforts are expected in the context of two multidisciplinary projects, namely the “Fight Heart Failure” and the European H2020 “CrossCult” project.

In our recent work, we mainly focused on the utility-based preference model in which preferences are represented as an aggregation of preferences over different attributes, structured or not, both in the numerical and qualitative settings. In the latter case, we provided axiomatizations of noteworthy classes of lattice-based aggregation functions, which were then used to model preferences and to provide their logical description [14]. In this qualitative setting, we also tackled the problem of computing version spaces (with explicit descriptions of all models compatible with a given dataset) and proved a dichotomy theorem showing that the problem is NP-complete for preferences over at least 4 attributes whereas it is solvable in polynomial time otherwise [61].

Finding consensual structures among different classifications or metrics is again a challenging task, especially, for large and multi-source data, and its importance becomes apparent since algorithmic approaches are often heuristic on such datasets and they rarely produce the same output. The difficulty in extracting such consensual structures is then to find appropriate and meaningful aggregation rules, and their impossibility is often revealed by Arrow type impossibility results. In the current year, we focused on median structures [19], [21] that include several relational structures (trees, graphs, lattices) and allow several consensus procedures.

7.2. Knowledge Discovery in Healthcare and Life Sciences

Participants: Miguel Couceiro, Adrien Coulet, Kévin Dalleau, Joël Legrand, Pierre Monnin, Amedeo Napoli, Chedy Raïssi, Mohsen Sayed, Malika Smaïl-Tabbone, Yannick Toussaint.

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 healthcare, 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 Life Sciences is in concern with mining biological data, data integration, information retrieval, and use of bio-ontologies and linked data for resource annotation.

7.2.1. Ontology-based Clustering of Biological Linked Open Data

Increasing amounts of biomedical data provided as Linked Open Data (LOD) offer novel opportunities for knowledge discovery in bio-medicine. We proposed an approach for selecting, integrating, and mining LOD with the goal of discovering genes responsible for a disease [88]. We are currently working on the integration of LOD about known phenotypes and genes responsible for diseases along with relevant bio-ontologies. We are also defining a corpus-based semantic distance. One possible application of this work is to build and compare possible diseaseomes, i.e. global graphs representing all diseases connected according to their pairwise similarity values.

7.2.2. Biological Data Aggregation for Knowledge Discovery

Two multi-disciplinary projects were initiated in 2016, in collaboration with the Capsid Team, with a group of clinicians from the Regional University Hospital (CHU Nancy) and bio-statisticians from the Maths Lab (IECL). The first project is entitled ITM2P [0] and depends on the so-called CPER 2015–2020 framework. We are involved in the design of the SMEC platform as a support for “Simulation, Modeling and Knowledge Extraction from Bio-Medical Data”.

The second project is a RHU [0] project entitled *Fight Heart Failure* (FHF), where we are in charge of a workpackage about “data aggregation” mechanisms. Accordingly, we are working on the definition of multidimensional similarity measure for comparing and clustering sets of patients. Each cluster should correspond to a bioprofile, i.e. a subgroup of patients sharing the same form of the disease and thus the same diagnosis and care strategy.

The first results were presented at the International Symposium on Aggregation and Structures (ISAS 2016) [36]. We propose the GABS for “Graph Aggregation Based Similarity” approach for complex graph aggregation resulting in a similarity graph between a subset of nodes. Indeed the initial graph contains two types of nodes, i.e. individuals and attributes. The pairwise similarity between individuals is derived from the various paths in the initial graph. This setting allows the integration of domain knowledge in the initial graph (corresponding to domain ontologies, norms...). Another advantage of the GABS approach is to generate a similarity graph which can be used as input for various clustering algorithms (graph-based ones as well as those working on similarity/distance matrix).

The next question will be to build a prediction model for each bioprofile/subgroup (once validated by the clinicians) for a decision support system. Thus, we are investigating SRL (“Statistical Relational Learning”) methods which combine symbolic and probabilistic methods for improving expressivity (through logical or relational languages) and for dealing with uncertainty.

7.2.3. Suggesting Valid Pharmacogenes by Mining Linked Open Data and Electronic Health Records

A standard task in pharmacogenomics research is identifying genes that may be involved in drug response variability and called “pharmacogenes”. As genomic experiments in this domain tend to generate many false positives, computational approaches based on background knowledge may generate more valuable results. Until now, the later have only used molecular networks databases or biomedical literature. We are

[0] “Innovations Technologiques, Modélisation et Médecine Personnalisée”

[0] “Recherche Hospitalo-Universitaire”

studying a new method taking advantage of various linked data sources to validate uncertain drug-gene relationships, i.e. pharmacogenes [75]. One advantage relies on the standard implementation of linked data that facilitates the joint use of various sources and makes easier the consideration of features of various origins. Accordingly, we selected, formatted, interconnected and published an initial set of linked data sources relevant to pharmacogenomics. We applied numerical classification methods for extracting drug-gene pairs that can become validated pharmacogene candidates.

The ANR project "PractiKPharma" initiated in 2016 relies on similar ideas, having the motivation of validating state-of-the-art knowledge in pharmacogenomics (http://practikpharma.loria.fr/). The originality of "PractiKPharma" is to use Electronic Health Records (EHRs) to constitute cohorts of patients that can be mined for validating extracted pharmacogenomics knowledge units.

7.2.4. *Analysis of biomedical data annotated with ontologies*

In the context of the Snowflake Inria Associate team, Gabin Personeni, who is a PhD student co-supervised by Marie-Dominique Devignes (Capsid EPI) and Adrien Coulet (Orpailleur EPI) spent four months at the Stanford University in 2016. After this internship, we developed an approach based on pattern structures to identify frequently associated ADRs (Adverse Drug Reactions) from patient data either in the form of EHR or ADR spontaneous reports [51], [49]. In this case, pattern structures provide an expressive representation of ADR, taking into account the multiplicity of drugs and phenotypes involved in such reactions. Additionally, pattern structures allow considering diverse biomedical ontologies used to represent or annotate patient data, enabling a "semantic" comparison of ADRs. Up to now, this is the first research work considering such representations to mine rules between frequently associated ADRs. We illustrated the generality of the approach on two distinct patient datasets, each of them linked to distinct biomedical ontologies. The first dataset corresponds to anonymized EHRs, extracted from "STRIDE", the EHR data warehouse of Stanford Hospital and Clinics. The second dataset is extracted from the U.S. FDA (for Food & Drug Administration) Adverse Event Reporting System (FAERS). Several significant association rules have been extracted and analyzed and may be used as a basis of a recommendation system.

7.3. Knowledge Engineering and Web of Data

Participants: Emmanuelle Gaillard, Nicolas Jay, Florence Le Ber, Jean Lieber, Amedeo Napoli, Emmanuel Nauer, Justine Reynaud.

Keywords: knowledge engineering, web of data, definition mining, classification-based reasoning, case-based reasoning, belief revision, semantic web

7.3.1. *Around the Taaable Research Project*

The Taaable project was originally created as a challenger of the Computer Cooking Contest (ICCBR Conference) [73]. Beyond its participation to the CCC challenges, the Taaable project aims at federating various research themes: case-based reasoning (CBR), information retrieval, knowledge acquisition and extraction, knowledge representation, belief change theory, ontology engineering, semantic wikis, text-mining, etc. CBR performs adaptation of recipes w.r.t. user constraints. The reasoning process is based on a cooking domain ontology (especially hierarchies of classes) and adaptation rules. The knowledge base is encoded within a semantic wiki containing the recipes, the domain ontology and adaptation rules.

As acquiring knowledge from experts is costly, a new approach was proposed to allow a CBR system using partially reliable, non expert, knowledge from the web for reasoning. This approach is based on notions such as belief, trust, reputation and quality, as well as their relationships and rules to manage the 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. Performing CBR with knowledge resulting from an e-community is improved by taking into account the knowledge reliability [10]. In the same way, another study shows how the case retrieval of a CBR system can be improved using typicality. Typicality discriminates subclasses of a class in the domain ontology depending of how a subclass is a good example for its class. An approach has been proposed to partition the subclasses of some classes into atypical, normal and typical subclasses in order to refine the domain ontology. The refined ontology allows a finer-grained generalization of the query during the retrieval process, improving at the same time the final results of the CBR system.

The Taaable system also includes a module for adapting textual preparations (from a source recipe text to an adapted recipe text, through a formal representation in the qualitative algebra INDU). The evaluation of this module as a whole thanks to users has been carried out and has shown its efficiency (w.r.t. text quality and recipe quality), when compared with another approach to textual adaptation [76].

FCA allows the classification of objects according to the properties they share into a concept lattice. A lattice has been built on a large set a cooking recipes according to the ingredients they use, producing a hierarchy of ingredient combinations. When a recipe R has to be adapted, this lattice can be used to search the best ingredient combinations in the concepts that are the closest to the concept representing R.

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 to adjust the ingredient quantities using specific inference engines.

Another approach to adaptation based on the principles of analogical transfer applied to the formalism RDFS has been developed [41]. It is based on the problem-solution dependency represented as an RDFS graph: this dependency within the source case is modified so that it fits the context of the target problem. The application problem that has guided this research addresses the issue of cocktail name adaptation: given a cocktail recipe, the name of this cocktail and the ingredient substitution that produces a new cocktail, how could the new cocktail be called?

7.3.2. Exploring and Classifying the Web of Data

A part of the research work in Knowledge Engineering is oriented towards knowledge discovery in the web of data, as, with the increased interest in machine processable data, more and more data is now published in RDF (Resource Description Framework) format. The popularization and quick growth of Linked Open Data (LOD) has led to challenging aspects regarding quality assessment and data exploration of the RDF triples that shape the LOD cloud. Particularly, we are interested in the completeness of the data and the their potential to provide concept definitions in terms of necessary and sufficient conditions [66]. We have proposed a novel technique based on Formal Concept Analysis which organizes subsets of RDF data into a concept lattice [43]. This allows data exploration as well as the discovery of implication rules which are used to automatically detect missing information and then to complete RDF data and to provide definitions. Moreover, this is also a way of reconciling syntax and semantics in the LOD cloud. Experiments on the DBpedia knowledge base shows that this kind of approach is well-founded and effective.

7.4. Advances in Graph Theory

Participants: Aurore Alcolei, Rémi de Joannis de Verclos, François Pirot, Jean-Sébastien Sereni.

Keywords: graph theory, graph coloring, extremal graph theory, chromatic number, two-mode data networks

Motivated by notions brought forward by sociology, we confirm a conjecture by Everett, Sinclair, and Dankelmann [Some Centrality results new and old, J. Math. Sociology 28 (2004), 215–227] regarding the problem of maximizing closeness centralization in two-mode data, where the number of data of each type is fixed. Intuitively, our result states that among all networks obtainable via two-mode data, the largest closeness is achieved by simply locally maximizing the closeness of a node. Mathematically, our study concerns bipartite graphs with fixed size bipartitions, and we show that the extremal configuration is a rooted tree of depth 2, where neighbors of the root have an equal or almost equal number of children [24].

Using recently introduced techniques based on entropy compression, we proved that the acyclic chromatic number of a graph with maximum degree Δ is less than $2.835\Delta^{4/3} + \Delta$. This improved the previous upper bound, which was $50\Delta^{4/3}$ (see [91] which is now published in Journal of Combinatorics, 7(4):725–737, 2016).

SEMAGRAMME Project-Team

6. New Results

6.1. Syntax-semantics interface

Participants: Philippe de Groote, Sylvain Pogodalla.

6.1.1. Lambek categorial grammar as abstract categorial grammars

Abstract Categorial Grammars (ACG, for short) differ from classical categorial grammars in an essential way: the ACG type system is based on a commutative logic (namely, the implicative fragment of multiplicative linear logic). For this reason, it has been argued that the way of encoding wh-extraction in an ACG corresponds to an uncontrolled form of extraction, which results in syntactic overgeneration. In particular, an ACG could not accomodate left and right peripheral extractions like a Lambek categorial grammar (LG, for short) does. In order to challenge this claim, we have shown how LG may be encoded as ACG [14].

6.1.2. Lexical Semantics

The interpretation of natural language utterances relies on two complementary elements of natural language modeling. On the one hand, the description of the combinatorics of natural language expresses how elementary units, or *lexical units* (typically the word), combine in order to build more complex elements, such as sentences or discourses. On the other hand, the description of these elementary units specifies how they contribute to the meaning of the whole by their *lexical meaning*. This specification should also take into account how the different parts of the lexical meanings combine during the *composition* process and how they relate to their underlying meaning concepts. For instance, the verbs *buy* and *sell* should refer to a common conceptual representation. However, their syntactic arguments (e.g., the subject) play a different (semantic) role with respect to the *transaction* concept that they share.

The modeling of these concepts and how they relate to each other gave rise to Frames Semantics as a representation format of conceptual and lexical knowledge [37], [30], [25], [45]. Frames consists of directed graphs where nodes correspond to entities (individuals, events, ...) and edges correspond to (functional or non-functional) relations between these entities. Providing a fine-grained representation of the internal concept structure allows both for a *decomposition* of the lexical meaning and for a precise description of the sub-structural interactions in the semantic composition process [44].

Following up on our previous work based on Hybrid Logic (HL) [26], [24] on linking Frames and truth-logical semantics, with a specific focus on explicit quantification over entities or events that are lexically triggered, we extended our model to the interaction between bounded events and *for*-adverbials. This interaction turns bounded events (*John biked to the office*) to iterated events (*John biked to the office for three months*), when the bounded events themselves result from coercing a progression (*John biked*) by addition of a prepositional phrase (*to the office*). We also proposed a modeling taking into account the respective scopes of the quantifiers induced by *for*-adverbials (over events) and quantification introduced by indefinites (over entities) [17]. Finally, we used the flexibility of the approach to model semantic coercion as induced by verbs such as *read* that can syntactically have an entity as argument (*John began a book*) while it semantically relates to an event (e.g., *reading*, *writing*, etc.) [21].

6.2. Discourse dynamics

Participants: Philippe de Groote, Sylvain Pogodalla, Maxime Amblard, Jirka Maršík, Aleksandre Maskharashvili.

6.2.1. Effects and Handlers in Natural Language

In formal semantics, logical meanings are assigned to natural language utterances. This process is guided by the principle of compositionality: the meaning of an expression is a function of the meanings of its parts. These functions are often formalized using the λ-calculus. However, there are areas of language which challenge the notion of compositionality, e.g. anaphoric pronouns or presupposition triggers. These force one to either abandon compositionality or adjust the structure of meanings. In the first case, meanings are derived by processes that no longer correspond to pure mathematical functions but rather to context-sensitive procedures, much like the functions of a programming language that manipulate their context with side effects. In the second case, when the structure of meanings is adjusted, the new meanings tend to be instances of the same mathematical structure, the monad. Monads themselves being widely used in functional programming to encode side effects, the common theme that emerges in both approaches is the introduction of side effects. Furthermore, different problems in semantics lead to different theories which are challenging to unite. We claim that by looking at these theories as theories of side effects, we can reuse results from programming language research to combine them.

Our work extends the λ-calculus with a monad of computations. The monad implements effects and handlers, a recent technique in the study of programming language side effects. We have proven some of the fundamental properties of our extended calculus: subject reduction, confluence and termination. We have then demonstrated how to use our calculus to implement treatments of several linguistic phenomena: deixis, quantification, conventional implicature, anaphora and presupposition.

6.2.2. Discourse Modeling with Abstract Categorial Grammars

We have studied several TAG-based grammatical formalisms for discourse analysis (D-LTAG [38], G-TAG [34], and D-STAG [33]), and we have proposed an ACG encodings of them. G-TAG is a formalism introduced for generating natural language texts out of conceptual (semantic) representation inputs. D-STAG is a synchronous formalism for modeling the syntax-semantics interface for discourse. It was introduced for discourse analysis (parsing). The ACG encodings of G-TAG and D-STAG shed light on the problem of clause-medial connectives that TAG-based formalisms do not account for. To deal with a discourse that contains clause-medial connectives, D-LTAG, G-TAG, and D-STAG, all make use of an extra grammatical step. In contrast, the ACG encodings of G-TAG and D-STAG offer a purely grammatical approach to discourse connectives occupying clause-medial positions. The method we propose is a generic one and can serve as a solution for encoding clause-medial connectives with the formalisms based on TAGs. The ACG encodings of G-TAG and D-STAG that we propose are second-order. Importantly, the class of second-order ACGs consists of intrinsically reversible grammars. Grammars of this class use the same polynomial algorithm to build parse structures both for strings and for logical formulas. Thus, second-order ACGs can be used both for parsing and generation. Therefore, the problems of parsing and generation with the ACG encodings of G-TAG and D-STAG are of polynomial complexity.

6.3. Common basic resources

Participants: Bruno Guillaume, Guy Perrier, Nicolas Lefebvre.

6.3.1. Crowdsourcing Complex Language Resources

This work [15] presents the results we obtained on a complex annotation task (that of dependency syntax) using a specifically designed Game with a Purpose, ZombiLingo. [0] The design of the game has to deal with the fact that the task is complex and does not directly rely on human intuition. We show that with suitable mechanisms (decomposition of the task, training of the players and regular control of the annotation quality during the game), it is possible to obtain annotations whose quality is significantly higher than that obtainable with a parser, provided that enough players participate. The source code of the game and the resulting annotated corpora (for French) are freely available.

[0] See: http://zombilingo.org/.

6.3.2. Universal Dependencies

We participated to development of new versions of the French part of the Universal Dependencies project (http://universaldependencies.org/).

The version 1.3 [52] was released in May. In this version, the lemmatization and the morphological annotation were added automatically when possible and with manual verification for ambiguous occurrences.

The version 1.4 [51] was released in November. This version contains a large number of annotation corrections. The Grew software was used to explore, to check consistency and to correct systematically the data. For instance, all copula annotations where checked manually.