RESEARCH CENTER
Nancy - Grand Est

FIELD

Activity Report 2014

Section New Results

Edition: 2015-03-24

1. ALGORILLE Project-Team 4
2. ALICE Project-Team 8
3. BIGS Project-Team 9
4. CAMUS Team 16
5. CARAMEL Project-Team 21
6. CARTE Project-Team 23
7. CASSIS Project-Team 26
8. COAST Team 37
9. CORIDA Team 39
10. MADYNES Project-Team 42
11. MAGRIT Project-Team 51
12. MAIA Project-Team 55
13. MASAIE Project-Team 65
14. MULTISPEECH Team 67
15. NEUROSYS Team 75
16. ORPAILLEUR Project-Team 78
17. PAREO Project-Team 85
18. SEMAGRAMME Project-Team 87
19. SHACRA Project-Team 91
20. TONUS Team 102
21. TOSCA Project-Team 105
22. VEGAS Project-Team 110
23. VERIDIS Project-Team 112

ALGORILLE Project-Team

6. New Results

6.1. Structuring applications for scalability

6.1.1. Combining locking and data management interfaces

Participants: Jens Gustedt, Mariem Saied.

Handling data consistency in parallel and distributed settings is a challenging task, in particular if we want to allow for an easy to handle asynchronism between tasks. Our publication [4] shows how to produce deadlock-free iterative programs that implement strong overlapping between communication, IO and computation.

A new implementation (ORWL) of our ideas of combining control and data management in C has been undertaken, see 5.2.1 . In 2014, work has demonstrated its efficiency for a large variety of platforms, see [20]. By using the example of dense matrix multiplication, we show that ORWL permits to reuse existing code for the target architecture, namely open source library ATLAS, Intel's compiler specific MKL library or NVidia's CUBLAS library for GPUs. ORWL assembles local calls into these libraries into efficient functional code, that combines computation on distributed nodes with efficient multi-core and accelerator parallelism.

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

6.2. Experimental methodologies for the evaluation of distributed systems

6.2.1. Simulation and dynamic verification

6.2.1.1. SimGrid framework improvement

Participants: Paul Bédaride, Martin Quinson, Gabriel Corona.

On the technical side, we kept up with our regular releases of the SimGrid framework, integrating the work of our partners in the SONGS ANR project. This year, we reimplemented the simulation kernel in C++. This modularity improvement will ease the addition of performance models by external contributors. This work thus contributes to our overall goal of constituting a user community focused on this first-class tool.

[11] is a long awaited paper describing the current state of the project and its future roadmap. This constitutes the new reference paper on the SimGrid project (the previous article, a short paper from 2008, was cited over 350 times since its publication). We show that despite the common beliefs, the tool specialization is not necessarily a warrant for performance and correctness.

We also continued our animation of our scientific community, for example through our participation to the Joint Laboratory for Petascale Computing (Inria/ANL/UIUC/BSC). We co-organized a summer school on Performance Metrics, Modeling and Simulation of Large HPC Systems in June, to push our tools toward PhD students that need to assess their HPC applications.

6.2.1.2. Dynamic verification and SimGrid

Participants: Marion Guthmuller, Martin Quinson, Gabriel Corona.

This year, the PhD thesis of M. Guthmuller went into its third year. The proposed methodology maturated into a usable tool: we can now verify small-size real HPC applications using MPI in C/C++/Fortran. This relies on a heuristic exploration of the applicative state at the system level that was presented in [21], [22].

Also, we finally added the ability to dynamically verify some CTL properties over MPI implementations. SimGrid was one of the rare framework able to verify LTL liveness properties over real implementations. To the best of our knowledge, it becomes the very first tool verifying CTL properties on real C/C++/Fortran applications. The targeted properties quantify the stability of the applicative communication pattern. The applications that respect these properties can benefit from specific, more efficient, fault tolerance algorithms. Verifying these properties is thus of a major practical interest. A publication is in preparation, as well as the PhD manuscript of M. Guthmuller who will defend by 2015 Q1.

6.2.2. Experimentation on testbeds and production facilities, emulation

6.2.2.1. Evaluating load balancing and fault tolerance strategies on Distem

Participants: Joseph Emeras, Emmanuel Jeanvoine, Lucas Nussbaum.

(For context, see sections 3.3 and 5.4 .)

We extended our work [27] to enable the study of load balancing and fault tolerance strategies on Distem. Distem now supports the introduction of changing heterogeneity and imbalance among virtual nodes, as well as the introduction of failures. Two HPC runtimes targeting Exascale (Charm++ and OpenMPI) were used as target applications. This work was presented at the Joint Laboratory for Extreme-Scale Computing in June, and at the Grid'5000 Spring School. However, those results still have to be properly published.

6.2.2.2. Distem improvements: VXLAN, release and tutorial

Participants: Emmanuel Jeanvoine, Tomasz Buchert, Lucas Nussbaum.

(For context, see sections 3.3 and 5.4 .)

The scalability of Distem's networking layer was improved by adding support for VXLAN networks. This enabled experiments with up to 40,000 virtual nodes, presented at the CCGrid'2014 SCALE challenge (where we were selected as finalist) [17]. Version 1.0 of Distem was also released in March 2014, and featured in a tutorial at the Grid'5000 Spring School.

6.2.2.3. Kadeploy improvements: REST API, new image broadcast mechanism

Participants: Luc Sarzyniec, Stéphane Martin, Emmanuel Jeanvoine, Lucas Nussbaum.

(For context, see sections 3.3 and 5.4 .)

Kadeploy 3.2 was released in March 2014. Among many other changes, that release included a new REST API to interact with Kadeploy, replacing the old Ruby-specific RPC mechanism, and easing the automation of experiments by providing a way to call Kadeploy from scripts.

Kadeploy 3.3 was released in November 2014. This release is mostly a bug-fix release, with many bug fixes in the internal cache system, the shell runner, and others.

We also implemented an improved mechanism to broadcast machine images to nodes. The new tool, called Kascade, is fault tolerant, and its performance has been thoroughly tested. It was described in a publication accepted at HPDIC'2014 [24], included in Kadeploy 3.2, and used as the default method for environment broadcast since Kadeploy 3.3.

6.2.2.4. XPFlow

Participants: Tomasz Buchert, Stéphane Martin, Emmanuel Jeanvoine, Lucas Nussbaum, Jens Gustedt.

(For context, see sections 3.3 and 5.7 .)

A publication focusing on XPFlow was accepted at CCGrid'2014 [18], and XPFlow was also featured in a tutorial at Grid'5000 Spring School. Our ongoing work focuses on improved support for collecting provenance in XPFlow.

6.2.2.5. Survey of Experiment Management tools

Participants: Tomasz Buchert, Cristian Ruiz, Lucas Nussbaum.

We produced a survey of Experiment Management tools for distributed systems, published in Future Generation Computer Systems [10]. This survey provides an extensive list of features offered by general-purpose experiment management tools dedicated to distributed systems research on real platforms. It then uses it to assess existing solutions and compare them, outlining possible future paths for improvements.

6.2.2.6. Grid'5000

Participants: Émile Morel, Luc Sarzyniec, Lucas Nussbaum.

(For context, see sections 3.3 and 5.8 .)

The work on resources description, selection, reservation and verification was wrapped-up in a TridentCom'2014 paper [23].

As a member of the Grid'5000 architects committee, Lucas Nussbaum was involved in the submission (and acceptance) of ADT Laplace.

Lucas Nussbaum also presented a talk [12] on Reproducible Research and Grid'5000 at the Grid'5000 evaluation by the Scientific Committee, during the Spring School.

6.2.3. Convergence and co-design of experimental methodologies

6.2.3.1. Realis'2014

Participant: Lucas Nussbaum.

Lucas Nussbaum organized (with Olivier Richard) the second edition of the Realis event [14]. Associated to the Compas'14 conference, this workshop aimed at providing a place to discuss the reproducibility of the experiments underlying the publications submitted to the main conference. We hope that this kind of venue will motivate the researchers to further detail their experimental methodology, ultimately allowing others to reproduce their experiments.

6.2.3.2. Reproducible Research working group at Inria Nancy – Grand Est

Participant: Lucas Nussbaum.

Lucas Nussbaum is organizing a working group on Reproducible Research at Inria Nancy – Grand Est since May 2014. Meetings involve a dozen of members from many different teams, and discussion topics have so far covered online platforms to test algorithms and applications, and evaluation contests organized together with conferences and workshops.

Lucas Nussbaum has also been invited to participate in the Inria national initiative on reproducible research.

6.2.3.3. Organization of Reppar

Participant: Lucas Nussbaum.

Lucas Nussbaum co-organized the first edition of the Reppar workshop, held during Europar'2014, with a focus on experimental practices in parallel computing research.

6.3. Algorithmic schemes for efficient use of parallel devices in clusters

Participants: Sylvain Contassot-Vivier, Stéphane Vialle [External collaborator, SUPELEC].

During the year 2014, we have continued our studies about the design and implementation of efficient algorithmic schemes to fully exploit all the available computational resources inside a parallel system. In particular, we have proposed general schemes that optimize the use of GPUs in clusters [26]. This is achieved by performing two kinds of overlappings. The former corresponds to computation/communication overlappings, either for the communications between machines but also for the data transfers between central RAM and GPUs inside each machine. The latter is the computation/computation overlapping that consists in executing computations on the GPUs in parallel of some computations on the central CPUs. Moreover, in this work we have paid a particular attention to some important aspects of software engineering that are the development and maintenance costs. Those aspects are essential as they directly determine the practical usability of the schemes, especially in the industry where there is a permanent vigilance to minimize the associated costs.

6.4. Parallel schemes for the resolution of the RTE with finite volumes method

Participant: Sylvain Contassot-Vivier.

In the context of our collaboration with the Lemta laboratory (Fatmir Asllanaj), about the design and implementation of an efficient and high accuracy algorithm for solving the Radiative Transfer Equation (RTE), we have reached our second objective that consisted in the realization of a multi-threaded parallel version of the software. That new version is based on the optimized sequential version produced as a first objective. It makes use of the OpenMP library to exploit all the cores inside one machine. The results are very satisfying as our algorithm obtains very good speed up and efficiency (around 90% and above) in realistic contexts. Moreover, besides this work over performance, we focus also on the high quality (accuracy) of the results of our software by making a permanent effort to track any possible enhancement of our numerical scheme. Then, the actual implementation of each of these possible enhancements is considered according to its potential costs, either in performance degradation as well as in additional resource consumptions (CPUs, GPUs and RAM). Confrontations to other existing computational schemes to solve the RTE are regularly realized to corroborate the validity preservation of our software [9], [15].

6.5. Study of binary multiplication and dynamical approaches to the integer factorization

Participants: Sylvain Contassot-Vivier, Nazim Fatès.

In the context of a collaboration with Nazim Fatès over dynamical systems we have co-supervised the internship of Raphaël Rieu-Helft (student at the ENS Paris), during June and July 2014. The goal of this internship was to study the relevance of the dynamical systems formalism as an efficient way to express and solve two specific problems. The former one was the queens problem on chessboards of arbitrary size. This goal was to express a solving algorithm of the queens problem under the form of a cellular automaton. The second step was to extend the results obtained for the queens problem to a more complex and computationally expensive problem that is the integer factorization. Two dynamical systems (cellular automata) have been obtained for both problems and their respective efficiencies, either in terms of convergence speed or speed of solution reaching, have been experimentally evaluated.

ALICE Project-Team

6. New Results

6.1. Highlights of the Year

Fabrication: We proposed a novel technique to automatically generate support structures for additive manufacturing with filament based processes. The deposited filament has to be properly supported at all times, which complicates printing of overhanging shapes: a disposable support has to be generated to temporarily hold the filament deposited above. Existing techniques either generate large structures, wasting material, or generate very thin structures that are hard to print and prone to failure. In contrast, our technique optimizes a scaffolding which is made of vertical pillars and horizontal bridges – such horizontal bridges print properly as long and the filament is deposited in straight line from one pilar to the next. We showed how to formulate scaffolding generation as a minimization problem and proposed a heuristic algorithm based on an efficient plane sweeping approach. The work was published [9] in ACM Transactions on Graphics in 2014 (proceedings of SIGGRAPH 2014). It is integrated within our 3D modeler for additive manufacturing, IceSL.

Optimal transport: this is an active research topics in the mathematics community. Given two measures μ and ν, optimal transport defines a distance between μ and ν, as the minimum cost of “morphing” μ into ν. This distance (called the *Wasserstein distance*) structures the space of measures and offers new ways of solving some highly non-linear PDEs (Monge-Ampere, Fokker-Plank ...). This requires a numerical way of computing the Wasserstein distance and its gradients. We studied a semi-discrete technique [21] submitted to ESAIM J. M2AN), that optimizes power diagrams. This is to our knowledge the first numerical implementation of optimal transport for volumetric densities (computes the Wasserstein distance between a sum of Dirac masses and a piece-wise linear density supported on a tetrahedral mesh).

6.2. New results

This year, we obtained new results in fabrication, in geometry processing and in multi-view reconstruction.

We investigated software solutions for printing with low cost (filament) 3D printers. We proposed a solution to automatically define temporary structures that will supports the object during its creation [9]. We also strongly reduce the artefacts that are produced by multi-material printing [17]. These works allow to better understand the physics of these printers, and to come up with efficient software solutions to common drawbacks of this technology. Other contributions in fabrication are more related to the design of the printable objects, that is developed in our software IceSL. To achieve real-time rendering of CSG models, we developed a new GPU approach for single pass A-Buffer [23]. This technique is also a simple solution to handle complex rendering problems such as transparency. We also proposed [11] an efficient method for performing dilatation and erosion directly on the same representation of volume by sequence of dilatation and erosions on segments.

In geometry processing, we proposed an algorithm to compute the intersection of Voronoi cells and a simplicial complex [25]. This algorithm is fast in dimension up to $10D$ because it doesn’t require to explicit the Voronoi diagram. It comes with exact predicates and symbolic perturbation to ensure its robustness. We have also developed an algorithm [13] able to trace streamlines on triangulated surfaces in such a way that two such streamlines cannot cross or merge. This property seems obvious in the continuous case, but was very difficult to enforce with the discrete representations (triangulated surface, and floating points) manipulated by the computer. We did also revisit the Optimal Delaunay triangulation in the case of graded mesh generation [14], and we adapted our remeshing methods to Geologic applications [27].

We obtained some new results in multi-view reconstruction: a new method that expands a limited set of correspondences towards a quasi-dense map across two views [15], and an improvement of variational multi-view reconstruction obtained thanks to a simple characterization of geometric deformations [16].

BIGS Project-Team

5. New Results

5.1. Analysis of high dimensional data

Participants: K. Duarte, S. Ferrigno, J.-M. Monnez, A. Muller-Gueudin, S. Tindel

5.1.1. Online partial principal component analysis of a data stream

Consider a data stream and suppose that each data vector is a realization of a random vector whose expectation varies with time, the law of the centered data vector being stationary. Consider the principal component analysis (PCA) of this centered vector called partial PCA. In this study are defined online estimations of the first principal axes by stochastic approximation processes using a data batch at each step of the process or all the data until the current step. This extends a former result obtained by J.-M. Monnez by using one data vector at each step. This is applied to partial generalized canonical correlation analysis by defining a stochastic approximation process of the metric involved in this case using all the data until the current step. If the expectation of the data vector varies according to a linear model, a stochastic approximation process of the model parameters is used. All these processes can be performed in parallel. A forthcoming preprint by R. Bar and J.-M. Monnez will discuss those aspects.

5.1.2. Data analysis for cumulative exposure Index

Everyone is subject to environmental exposures from various sources, with negative health impacts (air, water and soil contamination, noise ...) or with positive effects (e.g., green space). Studies considering such complex environmental settings in a global manner are rare. In [5] we propose to use statistical factor and cluster analyses to create a composite exposure index with a data-driven approach, in view to assess the environmental burden experienced by populations. The study was carried out in the Great Lyon area (France, 1.2M inhabitants) at the census block group (BG) scale. We used as environmental indicators ambient air NO2 annual concentrations, noise levels, proximity to green spaces, to industrial plants, to polluted sites and to road traffic. Although it cannot be applied directly for risk or health effect assessment, the resulting index can help to identify hot spots of cumulative exposure, to prioritize urban policies or to compare the environmental burden across study areas in an epidemiological framework.

5.1.3. A simultaneous stepwise covariate selection

In supervised learning the number of values of a response variable to predict can be high. Also clustering them in a few clusters can be useful to perform relevant supervised classification analysis. On the other hand selecting relevant covariates is a crucial step to build robust and efficient prediction models, especially when too many covariates are available in regard to the overall sample size. As a first attempt to solve these problems, we had already devised in a previous study an algorithm that simultaneously clusters the levels of a categorical response variable in a limited number of clusters and selects forward the best covariates by alternate minimization of Wilks's Lambda. In the project carried out this year, we first extend the former version of the algorithm to a more general framework where Wilks's Lambda can be replaced by any model selection criterion. We also turned forward selection into stepwise selection in order to remove covariates in real time if necessary. Finally an application of our algorithm to real datasets from peanut allergy studies allowed to get confirmation of some previously published results and suggested new discoveries. The possibilities of this algorithm are promising and it is hoped to be useful for many practitioners.

5.1.4. Prognostic value of the Strauss estimated plasma

We describe here an application oriented study lead jointly by J.-M. Monnez and a medical team under the supervision of E. Albuisson at CHU Brabois. The objective is to assess the prognostic value of estimations of volemia, or of their variations, beyond clinical examination in a post-hoc analysis of the Eplerenone Post-Acute Myocardial Infarction (AMI) Heart Failure (HF) Efficacy and Survival Study (EPHESUS). Assessing congestion post-discharge is indeed challenging but of paramount importance to optimize patient management and prevent hospital readmissions. The analysis was performed in a subset on 4957 patients with available data (within a full dataset of 6632 patients). Study endpoint was cardiovascular death and/or hospitalization for HF between month 1 and month 3 after post-AMI HF. Estimated plasma volume variations between baseline and month 1 were estimated by the Strauss formula, which includes hemoglobin and hematocrit ratios. Other potential predictors including congestion surrogates, hemodynamic and renal variables, and medical history variables were tested. An instantaneous estimation of plasma volume at month 1, ePVS M1, was defined and also tested. Multivariate analysis was performed using stepwise logistic regression and linear discriminant analysis. In HF complicating MI, congestion assessed by the Strauss formula and an instantaneous derived measurement of plasma volume displayed an added predictive value of early cardiovascular events, beyond routine clinical assessment. Trials assessing congestion management guided by this simple tool to monitor plasma volume are warranted.

5.1.5. Non parametric estimation of the conditional cumulative distribution function

This project fits into the global aim of improving local regression techniques. Indeed, we propose in [21] to study the local linear estimator of the conditional distribution function. Namely, having an i.i.d. sample $(X_i, Y_i)_{1\leq i\leq n}$, we estimate the conditional distribution function $F(t|x) = \mathbb{P}(Y \leq t|X = x)$ by:

$$\widehat{F}_n^{(1)}(t, h_n|x) = \frac{\widehat{f}_{n,2}(x, h_n)\widehat{r}_{n,0}(x, t, h_n) - \widehat{f}_{n,1}(x, h_n)\widehat{r}_{n,1}(x, t, h_n)}{\widehat{f}_{n,0}(x, h_n)\widehat{f}_{n,2}(x, h_n) - \left(\widehat{f}_{n,1}(x, h_n)\right)^2} \tag{1}$$

where $^{(1)}$ denotes the order 1 of the local polynomial estimator, $\widehat{f}_{n,j}$ stands for a kernel estimator with order j of the probability density function f_X of X, $\widehat{r}_{n,j}$ estimates the distribution of the couple (X, Y) and h_n is a bandwidth parameter.

This estimator is a particular case of the local polynomial estimators. It is the local polynomial estimator of order $p = 1$. Another simpler estimator, with order $p = 0$, is well known as the Nadaraya-Watson estimator.

We are interested in showing the advantage of this estimator over the Nadaraya-Watson estimator. We show asymptotic results for our estimator (exact rate of uniform consistency), and establish also uniform asymptotic certainty bands for the conditional cumulative distribution function.

We obtain the following result under some assumptions on the cumulative distribution F, f_X, the kernel K and the bandwidth h_n,

$$\sup_{t\in\mathbb{R}}\sup_{x\in I}\sqrt{\frac{nh_n}{\log(h_n^{-1})}}\left|\widehat{F}_n^{(1)}(t, h_n|x) - \widehat{\mathbb{E}}\left(\widehat{F}_n^{(1)}(t, h_n|x)\right)\right| \underset{n\to+\infty}{\overset{\mathbb{P}}{\to}} \sigma_F(I) \tag{2}$$

where

$$\sigma_F^2(I) = \frac{||K||_2^2}{2\inf\limits_{x\in I} f_X(x)}.$$

As corollaries of this result, we extend our results to other statistical functions, such as the quantiles and the regression function.

We illustrate our results with simulations and an application on foetopathologic data.

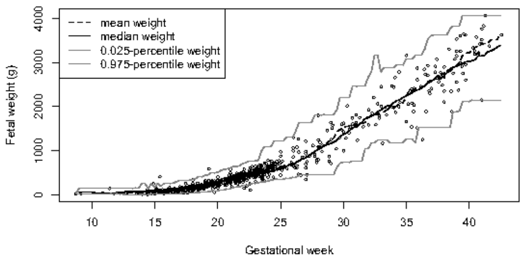


Figure 5. Fetal weight during the pregnancy: estimation of mean and quantiles from our local polynomial regression method.

We have also started a study about the regression function in the application on foetopathologic data. We consider the nonparametric model

$$Y = m(X) + \epsilon,$$

where Y is the fetal weight , X are the gestational weeks, m is a smooth unknown function and ϵ the error. The goal is to provide a test to detect significant features (or change points) of this regression curve. The regression curve is estimated using local polynomial kernel smoothers.

5.2. Stochastic modeling for complex and biological systems

Participants: R. Azaïs, T. Bastogne, C. Lacaux, A. Muller-Gueudin, S. Tindel, P. Vallois, S. Wantz-Mézières

5.2.1. Modelisation of networks of multiagent systems

We relate here the beginning of collaboration between A. Gueudin, R. Azaïs and some automatic control researchers in Nancy.

We consider 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 resetting 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.

5.2.2. Tumor growth modeling

A cancer tumor can be represented for simplicity as an aggregate of cancer cells, each cell behaving according to the same discrete model and independently of the others. Therefore to measure its size evolution, it seems natural to use tools coming from dynamics of population, for instance the logistic model. This deterministic framework is well-known but the stochastic one is worthy of interest. We are currently studying in [22] a model in which we suppose that the size V_t at time t of the tumor is a diffusion process of the type :

$$\begin{cases} dV_t = r\,V_t\,\left(1 - \frac{V_t}{\kappa}\right) - c\,V_t + \beta\,V_t\,dB_t \\ V_0 = v > 0 \end{cases} \tag{3}$$

where $(B_t)_{t\geq 0}$ is a standard brownian motion starting from zero.Then (i) We define a family of time continuous Markov chains which models the evolution of the rate of malignant cells and approximate (under some conditions) the diffusion process (V_t). (ii) We study in depth the solution to equation (3). This diffusion process lives in a domain delimited by two boundaries: 0 and $\kappa > 0$. In this stochastic setting, the role of κ is not so clear and we contribute to understand it. We describe the asymptotic behavior of the diffusion according to the values of the parameters. The tools we resort to are boundary classification criteria and Laplace transform of the hitting time to biological worthwhile level. We are able in particular to express the mean of the hitting time.

5.2.3. Anisotropic random fields

Hermine Biermé (Tours) and Céline Lacaux follow in [19] their collaboration in the study of anisotropic random fields. They have extended their previous works in the framework of conditionally sub-Gaussian random series. For such anisotropic fields, they have obtained a modulus of continuity and a rate of uniform convergence. Their framework allows to study e.g., Gaussian fields, stable random fields and multi-stable random fields.

5.2.4. Inference for dynamical systems driven by Gaussian noises.

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

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

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

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

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

To this aim, here are the steps we have focused on in 2014:

- A better understanding of the underlying rough path structure for equation (4). This includes two studies on differential systems driven by some general Gaussian noises in infinite dimensions: [17] on the Parabolic Anderson model, and [16] about viscosity solutions in the rough paths setting.
- Study of densities for general systems driven by Gaussian noises as in [18] and [15].
- Ergodic aspects, which are another important ingredient for estimation procedures for stochastic differential equations, are handled in [3].

5.2.5. Extremal process

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 in [23] 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.

5.2.6. Self-nested structure of plants

In a recent work, Godin and Ferraro designed a method to compress tree structures and to quantify their degree of self-nestedness. This method is based on the detection of isomorphic subtrees in a given tree and on the construction of a DAG, equivalent to the original tree, where a given subtree class is represented only once (compression is based on the suppression of structural redundancies in the original tree). In the compressed graph, every node representing a particular subtree in the original tree has exactly the same height as its corresponding node in the original tree.

The degree of self-nestedness is defined as the edit-distance between the considered tree structure and its nearest embedded self-nested version. Indeed, finding the nearest self-nested tree of a structure without more assumptions is conjectured to be an NP-complete or NP-hard problem. We thus design a heuristic method based on interacting simulated annealing algorithms to tackle this difficult question. This procedure is also a keystone in a new topological clustering algorithm for trees that we propose in this work. In addition, we obtain new theoretical results on the combinatorics of self-nested structures. For instance, we have shown that the number $C_{\leq H}(m)$ of self-nested trees with maximal height H and a ramification number for each vertex less than m satisfies the following formula,

$$C_{\leq H}(m) = \sum_{h=1}^{H} \prod_{i=1}^{h} \binom{m+h-i}{h-i+1}.$$

In particular, the cardinality $C_{=h}(m)$ of self-nested trees with exact height h evolves according to

$$\log C_{=h}(m) \sim \frac{(m+h)^2}{2} \log{(m+h)} - \frac{h^2}{2} \log h - \frac{m^2}{2} \log m - mh \log m,$$

when m and h simultaneously go to infinity. The redaction of an article is currently in progress.

5.2.7. Semi-parametric inference for a growth-fragmentation model

Statistical inference for piecewise-deterministic Markov processes has been extensively investigated for a few years under some ergodicity conditions. Our paper [2] is dedicated to a statistical approach for a particular non ergodic growth-fragmentation model for which the set $[0, 1]$ is absorbing. This kind of stochastic process may model the dynamic of a malthusian population for which there exists an extinction threshold. We focus on the estimation of the extinction probability and of the distribution of the extinction time from only one path of the model within a long time interval.

We establish that the absorption probability p is the unique solution in an appropriate space of a Fredholm equation of the second kind whose parameters are unknown,

$$p - Kp = s,$$

where K is an integral operator depending explicitly on the main features of the model. From n data, we estimate this important characteristic of the underlying process by solving numerically the estimated Fredholm equation. Indeed, $\widehat{p}_{n,m}$ is defined as the approximated solution of the equation $p - \widehat{K}_n p = \widehat{s}_n$ after m steps of the algorithm. Fortunately, this procedure allows us to estimate also the extinction time.

We have shown the convergence in probability of the proposed estimators under some usual asymptotic conditions. In particular, we have,

$$\forall\, \varepsilon > 0,\ \mathbf{P}\left(\|p - \widehat{p}_{n,m}\|_1 > \varepsilon\right) \to 0,$$

when n and m simultaneously go to infinity. The good behavior of our estimates on finite sample sizes is presented in Figure 6 . In future works, we plan to apply this methodology to more intricate situations, in particular for the pharmacokinetics and pharmacodynamics stochastic models recently introduced in the literature.

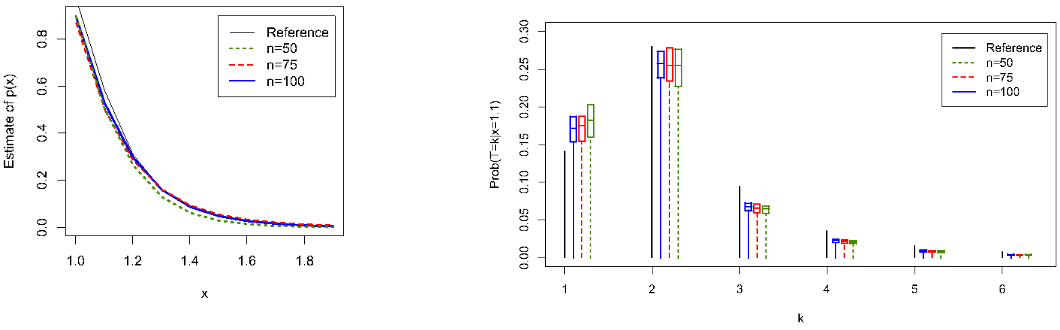


Figure 6. Probability of extinction $p(x)$ and its estimates for a trajectory starting from the initial population $1 \leq x \leq 2$ (left) and distribution of the extinction time and its estimates for a trajectory starting from $x = 1.1$ (right).

5.2.8. A Model-based Pharmacokinetics Characterization Method of Engineered Nanoparticles for Pilot Studies

Recent developments on engineered multifunctional nanomaterials have opened new perspectives in oncology. But assessment of both quality and safety in nanomedicine requires new methods for their biological characterization. We have recently proposed a new model-based approach for the pre-characterization of multifunctional nanomaterials pharmacokinetics in small scale in vivo studies. Two multifunctional nanoparticles, with and without active targeting, designed for photodynamic therapy guided by magnetic resonance imaging are used to exemplify the presented method. It allows the experimenter to rapidly test and select the most relevant pharmacokinetic (PK in the sequel) model structure planned to be used in the subsequent explanatory studies. We also show that the model parameters estimated from the in vivo responses provide relevant preliminary information about the tumor uptake, the elimination rate and the residual storage. For some parameters, the accuracy of the estimates is good enough to compare and draw significant pre-conclusions. A third advantage of this approach is the possibility to optimally refine the in vivo protocol for the subsequent explanatory and confirmatory studies complying with the 3Rs (reduction, refinement, replacement) ethical recommendations. More precisely, we show that the identified model may be used to select the appropriate duration of the magnetic resonance imaging sessions planned for the subsequent studies. The proposed methodology integrates magnetic resonance image processing, continuous-time system identification algorithms and statistical analysis. Except, the choice of the model parameters to be compared and interpreted, most of the processing procedure may be automated to speed up the PK characterization process at an early stage of experimentation.

More specifically, our efforts have been split into the following tasks:

- The article [6] gives an application of statistical methods for the design of experiments to optimize the formulation of a composite molecule in photodynamic therapy. The associated know-how has been transferred to the start-up CYBERnano to be generalized to the rational design of engineered nanoparticles. Collaboration with CRAN and LRGP (Nancy) and UNINE (Neuchâtel, Suisse).
- In [12], in vivo application of photodynamic therapy, a mathematical model and computational simulations of the light propagation in biological tissues were developed to help biologists to determine *a priori* some parameters of the experimental protocol. More precisely, the numerical results were used to select the most suited position of the optical fiber to be implemented within the animal brain. This equipment is required to bring the light and thus activate the molecule within the tumor. The therapeutical objective was to maximize the homogeneity of light intensity within the tumor volume.
- Obstacles and challenges to the clinical use of the photodynamic therapy (PDT) are numerous: large inter-individual variability, heterogeneity of therapeutic predictability, lack of in vivo monitoring concerning the reactive oxygen species (ROS) production, etc. All of these factors affect in their ways the therapeutic response of the treatment and can lead to a wild uncertainty on its efficiency. To deal with these variability sources, we have designed and developed an innovative technology able to adapt in realtime the width of light impulses during the photodynamic therapy. The first objective is to accurately control the photobleaching trajectory of the photosensitizer during the treatment with a subsequent goal to improve the efficacy and reproducibility of this therapy. In this approach, the physician a priori defines the expected trajectory to be tracked by the photosensitizer photobleaching during the treatment. The photobleaching state of the PS is regularly measured during the treatment session and is used to change in real-time the illumination signal. This adaptive scheme of the photodynamic therapy has been implemented, tested and validated during in vitro tests. These tests show that controlling the photobleaching trajectory is possible, confirming the technical feasibility of such an approach to deal with inter-individual variabilities in PDT. These results, contained in [13], open new perspectives since the illumination signal can be different from a patient to another according to his individual response. This study has proven its interest by showing promising results in an in vitro context, which has to be confirmed by the current in vivo experiments. However, it is fair to say that in a near future, the proposed solution could lead, in fine, to an optimized and personalized PDT. A patent was deposited subsequently. Collaboration with CRAN (Nancy).
- The communications [8], [9] and [10] present successful applications of a model-based design of nanoparticles. This approach is based on statistical design of experiments and black-box modeling in cell biology. The associated know-how has been transferred to the start-up CYBERnano. Collaboration with CEA LETI and INSERM (Grenoble).

CAMUS Team

6. New Results

6.1. Highlights of the Year

One of Philippe Clauss' early papers on Ehrhart polynomials has been celebrated, 18 years later, in a selection of papers for the International Conference on Supercomputing (ICS) 25th anniversary retrospective [13]. 35 papers have been selected among roughly 1800 papers published between 1987 and 2011. The paper is:

"Counting Solutions to Linear and Nonlinear Constraints Through Ehrhart Polynomials: Applications to Analyze and Transform Scientific Programs", by Philippe Clauss, ICS'96, which introduced Ehrhart polynomials in the field of program analysis and optimization.

Philippe Clauss wrote an additional retrospective [12] related to this research which complements the paper in the ICS special issue.

6.2. APOLLO (Automatic speculative POLyhedral Loop Optimizer)

The goal of the APOLLO project is to provide a set of annotations (pragmas) that the user can insert in the source code to perform advanced analyses and optimizations, for example dynamic speculative parallelization. It is based on the prototype named VMAD which was developed previously by the team between 2009 and 2012. Alexandra Jimborean defended her PhD thesis on this topic in 2012 [30].

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

APOLLO uses sampling, multi-versioning and code skeletons to limit the runtime overhead (profiling, analysis, and code generation). At runtime, targeted codes are launched by successive chunks that can be either original, instrumented or optimized/parallelized versions. These latter versions are generated on-the-fly through fast instantiation of the code skeletons. After each chunk execution, decisions can be taken relatively to the current optimization strategy. APOLLO is handling advanced memory access profiling through linear interpolation of the addresses, dynamic dependence analysis, version selection and speculative polyhedral parallelization [9].

Several extensions and improvements have been implemented inside Apollo in 2014:

- the scheduler of the polyhedral compiler Pluto has been integrated inside the framework. Thus, the runtime decision regarding what optimizing and parallelizing transformation is now entirely depending on Pluto, whose input is generated by the instrumentation and interpolation phase of Apollo [20].
- the static compilation phase of Apollo has been significantly enforced. Linear dependencies between values of scalars and memory addresses are identified in order to alleviate the cost of the instrumented code version. Additionally, memory reference functions that can be disambiguated at compile-time are now fully handled. These improvements are using analysis passes of the LLVM compiler, as well as passes that were specifically developed.
- Apollo is now using the LLVM JIT compiler to further optimize the instantiated code skeletons. Previously, code skeletons were generated as binary executable at compile-time with global variables instantiated at runtime. This approach yielded sub-optimal code including unnecessary or invariant computations. Code skeletons are now kept in LLVM intermediate form until being instantiated and compiled at runtime using the LLVM JIT compiler, thus resulting in faster optimized codes.

- Other memory behavior modeling approaches are now being studied and implemented, in order to allow Apollo handling codes that do not have a completely linear behavior. Three main cases are addressed:
  - quasi-linear behavior in which memory accesses which do not fit the linear prediction are checked on-the-fly, i.e., if these delinquent accesses do not invalidate the current parallel schedule.
  - linear regression behavior in which memory accesses are staying inside a “tube” bordered by linear functions.
  - behavior in which memory accesses are staying inside disjointed address ranges.

6.3. The XFOR programming structure

We have proposed a new programming control structure called “xfor” or “multifor”, providing users a way to schedule explicitly the statements of a loop nest, and take advantage of optimization and parallelization opportunities that are not easily attainable using the standard programming structures. This work is the PhD work of Imen Fassi, who started her work in 2013 and who is co-advised by Yosr Slama, Assistant Professor at the University El Manar in Tunis, Tunisia, and Philippe Clauss.

Data locality optimization is a well-known goal when handling programs that must run as fast as possible or use a minimum amount of energy. However, usual techniques never address the significant impact of numerous stalled processor cycles that may occur when consecutive load and store instructions are accessing the same memory location. In [15], we show that two versions of the same program may exhibit similar memory performance, while performing very differently regarding their execution times because of the stalled processor cycles generated by many pipeline hazards. The xfor structure enables the explicit control of the way data locality is optimized in a program and thus, to control the amount of stalled processor cycles. In [15], we also show the benefits of xfor regarding execution time and energy saving.

While many advanced and fully automatic program analysis and optimization techniques have been developed thanks to the accuracy and expressiveness of the polyhedral model, these techniques may fail in producing efficient codes in some circumstances. The xfor structure eases the manual application of optimizing transformations on loop nests for expert programmers and allows to generate executable codes that may be significantly faster than those generated automatically using well-established polyhedral strategies. we highlight five main gaps regarding these strategies and discuss some ideas on how to bridge them in [14].

6.4. CPU+GPU adaptive computation

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

This is mainly the work of PhD student Jean-François Dollinger, advised by Vincent Loechner since 2011. Preliminary results, a "fastest-wins" algorithm between a multicore CPU and the best predicted GPU code version, was published in 2013 in ICPP. Our latest advances, load balancing code between multiple cores CPUs and multiple GPUs will be presented at the IMPACT 2015 workshop [25] in conjunction with the HiPEAC conference. We are currently preparing an extended journal paper to present this work, and Jean-François Dollinger will defend his PhD in 2015.

6.5. Minimizing the synchronization overhead of X10 programs

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

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

More specifically, our work focused on synchronization primitives of X10. The X10 language basically has two activity synchronization primitives: one is the explicit use of "clocks" (synchronization barriers) during activity execution, the other is the implicit use of activity containers that synchronize only on the end of activities. Under reasonable conditions on the patterns of activity creation and control, we showed that long-running activities using clocks can be replaced by short-lived activities synchronized only on the end of their containers, and that this transformation provides a significant gain at run time.

We have studied the converse transformation, i.e. starting with an unclocked X10 program, obtaining a system of sequential threads executing in parallel and synchronizing with clocks. This transformation is interesting since it yields to further optimization opportunities. We have elaborated a system of rules to execute the transformation. Applying these rules to "regular" programs gives good results, but fails on some paradigmatic X10 codes. For irregular programs, some parallelism may be lost. We now are investigating a new set of rules to give a correct result for arbitrary X10 programs. A main difficulty is bringing the proof that the set of upgraded rules will give a correct result.

This work has been done in collaboration with Paul Feautrier, member of the COMPSYS Inria team, in ENS Lyon. The CAMUS team has invited Paul Feautrier one more time for one week in June 2014 in Strasbourg.

6.6. Hardware/Software helper thread prefetching

Heterogeneous Many Cores (HMC) architectures that mix many simple/small cores with a few complex/large cores are emerging as a design alternative that can provide both fast sequential performance for single threaded workloads and power-efficient execution for through-put oriented parallel workloads. The availability of many small cores in a HMC presents an opportunity to utilize them as low-power helper cores to accelerate memory-intensive sequential programs mapped to a large core. However, the latency overhead of accessing small cores in a loosely coupled system limits their utility as helper cores. Also, it is not clear if small cores can execute helper threads sufficiently in advance to benefit applications running on a larger, much powerful, core.

In this project, we designed a hardware/software framework called core-tethering to support efficient helper threading on heterogeneous manycores. Core-tethering provides a co-processor like interface to the small cores that (a) enables a large core to directly initiate and control helper execution on the helper core and (b) allows efficient transfer of execution context between the cores, thereby reducing the performance overhead of accessing small cores for helper execution. Our evaluation on a set of memory intensive programs chosen from the standard benchmark suites shows that helper threads using moderately sized small cores can significantly accelerate a larger core compared to using a hardware prefetcher alone. We find that a small core provides a good trade-off against using an equivalent large core to run helper threads in a HMC. Additionally, helper prefetching on small cores when used along with hardware prefetching, can provide an alternate design point to growing instruction window size for achieving higher sequential performance on memory intensive applications.

This work is a collaboration between the ALF team in Rennes and CAMUS in Strasbourg. Our contribution is mainly on the generation of helper thread code (as a followup to our work on program skeletonization). The result of the work has been published in October 2014 in the Proceedings of the SBAC-PAD conference [17].

6.7. Loop-based Modeling of Parallel Communication Traces

Parallel communication traces are traces of the various actions performed by parallel programs (typically written using MPI or some such library). The traces usually contain actions like message sending and receiving, and entering and exiting collective operations. The goal of this project is to build a model of the parallel program from the traces of the various processes that form the program. Consolidating on our previous work on sequential traces, we have developed an algorithm that takes the traces of the individual processes and merges them into a global model.

The main characteristics of our algorithm is that the result takes the form of loops enclosing various parallel constructs and communication actions. The driving goal of this work is to use the model for various analyzes, mainly to draw qualitative conclusions on the program (like the affinity of the various processes involved), but also to extract quantitative information (like communication matrices). A long term goal is to use the parallel loops to suggest program optimizations.

As of today, our algorithm has been evaluated on several applications. The most obvious is trace compression, with spectacular results because of the underlying loop-nest model (as was already the case for our sequential trace analysis algorithm). Another application is replay, where the program's (actual, i.e., traced) behavior can be simulated on a different parallel architecture. The last application is to build a lightweight model from a subset of trace data, and use the model to index into potentially massive quantitative data associated to the various events.

It turns out that it is difficult to publish such algorithms without evaluating them in "realistic" settings, on applications running on massively parallel hardware, something we don't have easy access to. Also, there are currently a few algorithms that provide similar solutions to practitioners, in a way that we think are fundamentally inferior to our proposition but that seem to be good enough for their current use. Waiting for better opportunities to illustrate the power of our method, we have published a research report summarizing our work [26].

6.8. Switcheable scheduling

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

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

This is an ongoing work with the PhD student Lénaïc Bagnères (POSTALE Team at Inria Saclay-Île-de-France, co-advised by Christine Eisenbeis and Cédric Bastoul). The first results have been presented in 2014 at the Euro-Par International Conference [11].

6.9. Interactive Code Restructuring

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

This is a rather new research direction which strengthen CAMUS's static parallelization and optimization issue. It has been initiated at Paris-Sud University as a collaboration between Compilation, represented by Cédric Bastoul before he joined CAMUS, and Human-Machine Interaction, represented by Stéphane Huot from the IN-SITU Team at Inria Saclay-Île-de-France. This work is essentially the PhD topic of Alexander Zinenko (IN-SITU Team at Inria Saclay-Île-de-France, co-advised by Stéphane Huot and Cédric Bastoul, CORDI Grant) which started in 2013. The first results have been presented in 2014 to the IEEE VL/HCC Conference [22]. Moreover, another paper on the topic has been accepted to the International IMPACT 2015 Workshop to be held in conjunction with the HiPEAC International Conference.

CARAMEL Project-Team

6. New Results

6.1. Highlights of the Year

Razvan Barbulescu, ex-PhD student in the team, has received the award “Prix Le Monde de la recherche universitaire”, as one of the top-5 PhD thesis in exact science in 2014.

Emmanuel Thomé has received the “Prix Régional du Chercheur” of the Région Lorraine.

Emmanuel Thomé has received the “Prix de l’Association des Amis de l’Université de Lorraine”.
BEST PAPER AWARD :
[17] **Eurocrypt 2014**. R. BARBULESCU, P. GAUDRY, A. JOUX, E. THOMÉ.

6.2. Discrete logarithm computation in a prime finite field of 180 decimal digits

Participants: Cyril Bouvier, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé [contact].

In the context of the CATREL ANR project, we performed a new computation of a discrete logarithm modulo a 180 digit (596-bit) prime using the number field sieve algorithm. Previous records were 135-digit (448 bits, done in 2006) and 160-digit (530-bit, done in 2007) primes. This is, to date, the largest computation in a prime field. In total, this took the equivalent of 130 years on one CPU core.

6.3. Discrete logarithm in finite fields of small extension degree

Participant: Pierrick Gaudry [contact].

Together with Razvan Barbulescu (CNRS, IMJ-PRG), Aurore Guillevic and François Morain (GRACE project-team), we investigated the discrete logarithm problem in the case of finite fields of the form $\mathbb{F}_{p^n}$, where $n > 1$ is a small integer. We proposed in a preprint — a part of which was accepted to Eurocrypt 2015 — various theoretical and practical improvements [25]:

- new methods for selecting polynomials,
- better (heuristic) asymptotic complexity in the case where $n \approx \log p$, and
- use of algebraic number theory to show that in some cases we can skip the Schirokauer maps.

We have adapted CADO-NFS in order to perform a record computation in a field of the form $\mathbb{F}_{p^2}$, where p^2 has 180 digits. To our knowledge, this is the first time that the number field sieve algorithm is used in practice for record-size computations in this type of fields.

6.4. Igusa class polynomials computation for class number 20,016

Participant: Emmanuel Thomé [contact].

In collaboration with the LFANT project-team, Emmanuel Thomé and Andreas Enge completed the computation of Igusa class polynomials for a quartic CM field whose Igusa class number is 20,016. That is more than 20 times more than the previous state of the art. This has been made possible with the CMH software, which corresponds to the article [10].

6.5. Isogeny graphs for curves with maximal real multiplication

Participant: Emmanuel Thomé [contact].

Emmanuel Thomé and Sorina Ionica (currently with the LFANT project-team) worked on a new algorithm for computing isogeny graphs for Jacobians of curves having the special property that the intersection of their endomorphism ring with its real subfield is maximal. The resulting algorithm is the first depth-first algorithm for this task. This work has been submitted [29].

6.6. Polynomial selection for the Number Field Sieve

Participants: Cyril Bouvier, Nicholas Coxon, Alexander Kruppa, Paul Zimmermann [contact].

A new polynomial selection algorithm for GNFS (General Number Field Sieve) has been described in a preprint [24] and implemented in CADO-NFS. We demonstrate the efficiency of this algorithm by exhibiting a better polynomial than the one used for the factorization of RSA-768, and a polynomial for RSA-1024 that outperforms the best published one.

Montgomery's method of polynomial selection for GNFS has been analysed in a preprint [27]. Criteria for the selection of good parameters for Montgomery's method are given, and the existence of the modular geometric progressions used in the method is considered.

6.7. Beyond double precision

Participant: Paul Zimmermann [contact].

A project entitled "Beyond Double Precision" (BeDoP) has been submitted to the European Research Council (ERC) for funding (advanced grant category). The BeDoP project will (i) demonstrate the limits of double precision on large-scale applications, (ii) make multiple-precision tools easier to use in modern computer languages, and (iii) improve the efficiency and robustness of those tools, in particular by using formal proof techniques. Our dream with the BeDoP project is that scientific computations on exascale computers will no longer give very fast and very wrong results, but instead give very fast and very accurate results.

6.8. Gröbner bases for sparse algebraic systems

Participant: Pierre-Jean Spaenlehauer [contact].

In collaboration with Jean-Charles Faugère and Jules Svartz (POLSYS project-team), new Gröbner bases algorithms have been proposed in [20] to solve efficiently sparse systems of multivariate polynomial equations. Moreover, new complexity bounds have also been proved; they extend in a unified way previous bounds known for solving multi-homogeneous systems with Gröbner bases. For such systems, a proof-of-concept prototype implementation of these algorithms achieves large speed-ups compared to state-of-the-art optimized Gröbner bases algorithms.

6.9. Faster index calculus in algebraic curves

Participant: Maike Massierer [contact].

A possible application of the new ideas speeding up the function field sieve algorithm to index calculus in Jacobians of algebraic curves of large genus has been studied in [30]. Based on a number of practical experiments as well as theoretical considerations, a conjecture has been formulated. It implies that the new ideas only apply to curves which are not interesting in the context of the discrete logarithm problem.

6.10. FFS factory

Participant: Jérémie Detrey [contact].

An extension of Coppersmith's "factorization factory" and Barbulescu's "discrete logarithm factory" to the Function Field Sieve was proposed, dubbed the "FFS factory" [28]. The idea is to batch discrete logarithm computations in finite fields of different extension degrees, sharing the sieving step on the algebraic side between all these finite fields. A careful analysis proved that this approach can be used to lower the overall asymptotic complexity. This was also illustrated with a practical experiment in which the discrete logarithm problem was solved for all of the 50 binary fields of the form $\mathbb{F}_{2^n}$ with n odd ranging from 601 to 699.

CARTE Project-Team

6. New Results

6.1. Highlights of the Year

Our team made remarkable progress into the understanding of complexity of higher-order functionals. While a robust class of computable functionals exists at any finite type built from $\mathbb{N}$ and $\rightarrow$ (the Kleene-Kreisel functionals), no satisfying complexity classes had been defined so far, except the class BFF of Basic Feasible Functionals. However that class is not a complexity class in the usual sense and does not offer the possibility to define space complexity or non-deterministic time complexity. In his PhD Hugo Férée has developed a non-trivial notion of size for higher-order functionals using game semantics and he has defined a notion of polynomial-time computable functional including BFF but behaving more satisfactorily in several ways. A paper in preparation will gather these results.

6.2. Malware Detection and Program Analysis

- **Complexity Information Flow in a Multi-threaded Imperative Language.** Program resource analysis using tiering based type system has been extended to analyze the time consumed by multi-threaded imperative programs with a shared global memory, which delineates a class of safe multi-threaded programs. In this work presented at TAMC'14 (Theory and Applications of Models of Computation) [22] Jean-Yves Marion and Romain Péchoux have demonstrated that a safe multi-threaded program runs in polynomial time if (i) it is strongly terminating w.r.t. a non-deterministic scheduling policy or (ii) it terminates w.r.t. a deterministic and quiet scheduling policy. As a consequence, we obtain a characterization of the set of polynomial time functions. As far as we know,this is the first characterization by a type system of polynomial time multi-threaded programs
- **A Categorical Treatment of Malicious Behavioral Obfuscation.** In this work presented at TAMC'14 (Theory and Applications of Models of Computation) [23] Romain Péchoux and Thanh Dinh Ta consider malicious behavioral obfuscation through the use of a new abstract model for process and kernel interactions based on monoidal categories. In this model, program observations are considered to be finite lists of system call invocations. In a first step, the authors have shown how malicious behaviors can be obfuscated by simulating the observations of benign programs. In a second step, they have shown how to generate such malicious behaviors through a technique called path replaying and they have extended the class of captured malwares by using some algorithmic transformations on morphisms graphical representation.
- **Malware Message Classification by Dynamic Analysis.** Guillaume Bonfante, Jean-Yves Marion and Thanh Dinh Ta presented to FPS in 2014 a new approach in malware retro-engineering. Usually, either communications, or code is analyzed. Here, the authors take a hybrid perspective. They showed how malware communication can be seen under a language perspective. They tested their idea on real malware and, for instance, showed that the botnet Zeus uses FTP as an underlying network support.
- **Supertagging with Constraints.** The parsing in Natural Language Processing is usually done by statistical analysis. Formal approaches are much more challenging, usually involving hard problems. Guillaume Bonfante, Bruno Guillaume, Mathieu Morey, and Guy Perrier [24] propose a new stream algorithm which discriminates tags in sentences.

6.3. Computability and Complexity

- **Genericity of semi-computable objects.** One of the main goals of computability theory is to understand and classify the algorithmic content of infinite objects, which can be expressed as the difficulty of computing them or as their ability to help solving problems. In establishing this classification one is often led to separate classes of algorithmic complexity and the construction of counter-examples is usually a hard task that requires the use of advanced technics (among which the so-called priority method with finite injury). The difficulty in such a construction is that the constructed object should satisfy two types of requirements going in opposite directions: it should lack algorithmic content but at the same time should be constructible in some way. In other words, these objects live somewhere between *generic* objects (objects with no structure) and *computable* objects (the most constructible objects). While computability theory provides formal notions of genericity, these ones are always incompatible with computability.

  We introduce a new notion of genericity which has two advantages: it is close to plain genericity, and we prove that it is compatible with semi-computability (for a property, being semi-decidable is a semi-computability notion while being decidable is a plain computability notion). The latter result has important consequences: many ad hoc existing constructions are subsumed by this result and then unified, new results can be obtained whenever the new notion of genericity captures the sought properties, and the result clarifies the role of topology in computability theory.

  This work is the sequel of the STACS 2013 paper [19] and is currently submitted [26].

- **Analytical properties of resource-bounded real functionals.** In [14] Hugo Férée, Walid Gomaa and Mathieu Hoyrup extend the results of [52] to non-deterministic complexity. More precisely, we introduce the analytical concepts of essential point and sufficient set for norms over continuous functions and use them to characterize the class of norms that are computable in non-deterministic polynomial time.

- **Call-by-value, call-by-name and the vectorial behaviour of the algebraic λ-calculus.** In this article published in LMCS (Logical Methods in Computer Science) [12], Ali Assaf, Alejandro Díaz-Caro, Simon Perdrix, Christine Tasson and Benoît Valiron examine the relationship between the algebraic lambda-calculus, a fragment of the differential lambda-calculus and the linear-algebraic lambda-calculus, a candidate lambda-calculus for quantum computation. Both calculi are algebraic: each one is equipped with an additive and a scalar-multiplicative structure, and their set of terms is closed under linear combinations. However, the two languages were built using different approaches: the former is a call-by-name language whereas the latter is call-by-value; the former considers algebraic equalities whereas the latter approaches them through rewrite rules. In this paper, they analyse how these different approaches relate to one another. To this end, four canonical languages based on each of the possible choices are proposed: call-by-name versus call-by-value, algebraic equality versus algebraic rewriting. The various languages are simulating each other. Due to subtle interaction between beta-reduction and algebraic rewriting, to make the languages consistent some additional hypotheses such as confluence or normalisation might be required.

- **Real or Natural numbers interpretations and their effect on complexity.** Guillaume Bonfante, Florian Deloup and Antoine Henrot [13] have shown how deep results in algebraic geometry may be read in a complexity perspective. They show that real numbers though they are not well founded can be used as natural numbers are for program interpretations. The argument is based on Positivstellensatz, a major result proved by Stengle.

- **Information carried by programs about the objects they compute.** In computability theory and computable analysis, finite programs can compute infinite objects. Presenting a computable object via any program for it, provides at least as much information as presenting the object itself, written on an infinite tape. What additional information do programs provide? We characterize this additional information to be any upper bound on the Kolmogorov complexity of the object, i.e., it gives an upper bound on size of a shortest program computing the object.

  This problem can be formalized using the two classical models of computation of Markov-computability [61] and Type-2 computability [74], which are the most famous and studied ways of computing with infinite objects. Many celebrated results comparing these models have been developed in the 50's (theorems by Rice, Rice-Shapiro, Kreisel-Lacombe-Schoenfiled/Ceitin, Friedberg) but a complete understanding of their precise relationship has never been obtained. Our results fill this void, identifying the exact relationship between the two models. In particular this relationship enables us to obtain several results characterizing the computational and topological structure of Markov-semidecidable properties.

This work, made in collaboration with Cristóbal Rojas (Santiago) during his visit as an Inria "Chercheur Invité", has been accepted in STACS 2015 [20].

- **Causal Graph Dynamics.** Causal Graph Dynamics extend Cellular Automata to arbitrary, bounded-degree, time-varying graphs. The whole graph evolves in discrete time steps, and this global evolution is required to have a number of physics-like symmetries: shift-invariance (it acts everywhere the same) and causality (information has a bounded speed of propagation). Pablo Arrighi, Emmanuel Jeandel, Simon Martiel (I3S, Univ. Nice-Sophia Antipolis), and Simon Perdrix are investigating the properties of this model. In particular a work on the reversibility of causal graph dynamics has just been submitted in January 2015.
- **The Parameterized Complexity of Domination-type Problems and Application to Linear Codes.** In this article presented at TAMC'14 (Theory and Applications of Models of Computation) [17], David Cattanéo and Simon Perdrix study the parameterized complexity of domination-type problems. (σ, ρ)-domination is a general and unifying framework introduced by Telle: given $\sigma, \rho \subseteq \mathbb{N}$, a set D of vertices of a graph G is (σ, ρ)-dominating if for any $v \in D$, $|N(v) \cap D| \in \sigma$ and for any $v \notin D$, $|N(v) \cap D| \in \rho$. The main result is that for any σ and ρ recursive sets, deciding whether there exists a (σ, ρ)-dominating set of size k, or of size at most k, are both in W[2]. This general statement is optimal in the sense that several particular instances of (σ, ρ)-domination are W[2]-complete (e.g., DOMINATING SET). This result is also extended to a class of domination-type problems which do not fall into the (σ, ρ)-domination framework, including CONNECTED DOMINATING SET and the problem of the minimal distance of a linear code over a finite field.

  To prove the W[2]-membership of the domination-type problems the authors extend the Turing-way to parameterized complexity by introducing a new kind of non-deterministic Turing machine with the ability to perform 'blind' transitions, i.e., transitions which do not depend on the content of the tapes.
- **Quantum Circuits for the Unitary Permutation Problem**. In this paper [18] presented at DCM'14 (New Development in Computational models) and at the Workshop on Quantum Metrology, Interaction, and Causal Structure 2014 (invited talk), Stefano Facchni and Simon Perdrix consider the *Unitary Permutation* problem which consists, given n quantum gates $U_1, ..., U_n$ and a permutation σ of $\{1, ..., n\}$, in applying the quantum gates in the order specified by σ, i.e., in performing $U_{\sigma(n)} \circ ... \circ U_{\sigma(1)}$.

  This problem has been introduced and investigated in [40] where two models of computations are considered. The first is the (standard) model of query complexity: the complexity measure is the number of calls to any of the quantum gates U_i in a quantum circuit which solves the problem. The second model is roughly speaking a model for higher order quantum computation, where quantum gates can be treated as objects of second order. In both model the existing bounds are improved, in particular the upper and lower bounds for the standard quantum circuit model are established by pointing out connections with the *permutation as substring* problem introduced by Karp.

CASSIS Project-Team

6. New Results

6.1. Highlights of the Year

Véronique Cortier was one of the two FLoC plenary speakers during the Vienna Summer of Logic [31].

Steve Kremer and Robert Künnemann got a paper accepted at the 35th IEEE symposium on Security and Privacy [45].

The ANR project SEQUOIA has been accepted.

BEST PAPERS AWARDS :

[43] **Software Security and Reliability (SERE)**. E. FOURNERET, J. CANTENOT, F. BOUQUET, B. LEGEARD, J. BOTELLA.

[47] **The 7th International Symposium on Foundations & Practice of Security FPS'2014**. H. H. NGUYEN, A. IMINE, M. RUSINOWITCH.

6.2. Automated Deduction

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

6.2.1. Combination of Satisfiability Procedures

Participant: Christophe Ringeissen.

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 guarantee the existence of an infinite model). The design of a 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). In collaboration with Paula Chocron (U. Buenos Aires, former intern in Cassis) and Pascal Fontaine (project-team Veridis), we have investigated both cases.

The notion of gentle theory has been introduced in the last few years as one solution to go beyond the restriction of stable infiniteness, but in the case of disjoint theories. In [36], [59], we adapt the notion of gentle theory to the non-disjoint combination of theories sharing only unary predicates (plus constants and the equality). Like in the disjoint case, combining two theories, one of them being gentle, requires some minor assumptions on the other one. We show that major classes of theories, i.e., Loewenheim and Bernays-Schoenfinkel-Ramsey, satisfy the appropriate notion of gentleness introduced for this particular non-disjoint combination framework.

We have also considered particular non-disjoint unions of theories connected via bridging functions [37]. We present a combination procedure which is proved correct for the theory of absolutely free data structures. We consider the problem of adapting the combination procedure to get a satisfiability procedure for the standard interpretations of the data structure.

6.2.2. Unification Modulo Equational Theories of Cryptographic Primitives

Participants: Christophe Ringeissen, Michaël Rusinowitch.

Asymmetric unification is a new paradigm for unification modulo theories that introduces irreducibility constraints on one side of a unification problem. It has important applications in symbolic cryptographic protocol analysis, for which it is often necessary to put irreducibility constraints on portions of a state. However many facets of asymmetric unification that are of particular interest, including its behavior under combinations of disjoint theories, remain poorly understood. In [42], [63] we give a new formulation of the method for unification in the combination of disjoint equational theories developed by Baader and Schulz that both gives additional insights into the disjoint combination problem in general, and furthermore allows us to extend the method to asymmetric unification, giving the first unification method for asymmetric unification in the combination of disjoint theories.

Some attacks exploit in a clever way the interaction between protocol rules and algebraic properties of cryptographic operators. In [79], we provide a list of such properties and attacks as well as existing formal approaches for analyzing cryptographic protocols under algebraic properties.

We have further investigated unification problems related to the Cipher Block Chaining (CBC) mode of encryption. We first model chaining in terms of a simple, convergent, rewrite system over a signature with two disjoint sorts: list and element. The 2-sorted convergent rewrite system is then extended into one that captures a block chaining encryption-decryption mode at an abstract level, (using no AC-symbols); unification modulo this extended system is shown to be decidable [13].

6.2.3. Enumeration of Planar Proof Terms

Participant: Alain Giorgetti.

By the Curry-Howard isomorphism, simply typed lambda terms correspond to natural deduction proofs in minimal logic. Abramsky has introduced a notion of planarity for proof terms, from a graphical representation of proofs. Noam Zeilberger and Alain Giorgetti have initiated an enumerative study of normal planar lambda terms. At the MAP 2014 workshop in Paris, Noam Zeilberger conjectured that the sequence counting the number of closed normal planar lambda terms by increasing size may coincide with the one counting the number of rooted planar maps by number of edges. Zeilberger and Giorgetti started discussing this curious coincidence at the workshop and found a proof that both families are in size-preserving bijection [70]. Although the formal aspect is not emphasized in the paper, the use of formal representations of both normal planar lambda terms and rooted planar maps, of logic programming and a proof assistant software helped much in more quickly finding the bijection. Moreover the result puts a new light on the structure of proofs in minimal logic.

6.3. Security Protocol Verification

The design of cryptographic protocols is error-prone. Without a careful analysis, subtle flaws may be discovered several years after the publication of a protocol, yielding potential harmful attacks. In this context, formal methods have proved their interest for obtaining good security guarantees. Many analysis techniques have been proposed in the literature [76]. We have edited a book [71] where each chapter presents an important and now standard analysis technique. This year, we have written a tutorial that may serve when teaching formal analysis of security protocols [26]. We develop new techniques for richer primitives, wider classes of protocols and higher security guarantees. In Section 6.5.3 we consider derived testing techniques for verifying protocol implementations.

6.3.1. Voting Protocols

Participants: Véronique Cortier, David Galindo-Chacon, Stéphane Glondu, Steve Kremer.

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

One famous e-voting protocol is Helios, an open-source web-based end-to-end verifiable electronic voting system, used e.g., by UCL and the IACR association in real elections. One main advantage of Helios is its verifiability, up-to the ballot box (a dishonest ballot box may add ballots). We have defined a variant of Helios, named Belenios, that prevents from ballot stuffing, even against a dishonest ballot box. Our approach consists in introducing an additional authority that provides credentials that the ballot box can verify but not forge. Ballot privacy of Belenios then follows from ballot privacy of Helios. For full verifiability, we had first to adapt existing definitions of verifiability in the case of a corrupted ballot box and then prove verifiability of Helios [40], [61].

This new version has been implemented by Stéphane Glondu and has been tested in an election that involved the members of the Inria Nancy-Grand Est center and the LORIA lab (about 500 people that had to chose the best LORIA pictures).

Even a basic property like ballot secrecy is difficult to define formally and several definitions co-exist. We studied all game-based privacy definitions of the literature and discovered that none of them was satisfactory: they were either limited (not fully modeling e-voting protocols), or too strong (incompatible with verifiability), or even flawed for a few of them. Based on our findings, we have proposed a new game-based privacy definition BPRIV, proved that it implies simulation-based privacy and showed that it is realized by the Helios protocol.

Existing automated analysis techniques are inadequate to deal with commonly used cryptographic primitives, such as homomorphic encryption and mix-nets, as well as some fundamental security properties, such as verifiability. In collaboration with Matteo Maffei and Fabienne Eigner (Saarland University) we propose a novel approach based on refinement type systems for the automated analysis of two fundamental properties of e-voting protocols, namely, vote privacy and verifiability. We demonstrate the effectiveness of our approach by developing the first automated analysis of Helios using an off-the-shelf type-checker.

We have presented some of our results on e-voting as plenary speaker of FLOC 2014 [31].

6.3.2. Other Families of Protocols

Participants: Véronique Cortier, Steve Kremer, Cyrille Wiedling.

Securing routing Protocols. The goal of routing protocols is to construct valid routes between distant nodes in the network. If no security is used, it is possible for an attacker to disorganize the network by maliciously interacting with the routing protocols, yielding invalid routes to be built. We have proposed a new model and an associated decision procedure to check whether a routing protocol can ensure that honest nodes only accept valid routes, even if one of the nodes of the network is compromised. This result has been obtained for a bounded number of sessions, adapting constraint solving techniques to node topologies as well as some families of recursive tests, used in routing protocols [15].

Security APIs. In some systems, it is not possible to trust the host machine on which sensitive codes are executed. In that case, security-critical fragments of a program should be executed on some tamper resistant device (TRD), such as a smartcard, USB security token or hardware security module (HSM). The exchanges between the trusted and the untrusted infrastructures are ensured by special kind of API (Application Programming Interface), that are called *security APIs*. We have designed a generic API for key-management based on key hierarchy [20], that can self-recover from corruption of arbitrary keys, provided the number of corrupted, active keys is smaller than some threshold.

Security APIs, key servers and protocols that need to keep the status of transactions, require to maintain a global, non-monotonic state, e.g., in the form of a database or register. However, most existing automated verification tools do not support the analysis of such stateful security protocols - sometimes because of fundamental reasons, such as the encoding of the protocol as Horn clauses, which are inherently monotonic. A notable exception is the recent tamarin prover which allows specifying protocols as multiset rewrite (MSR) rules, a formalism expressive enough to encode states. As multiset rewriting is a “low-level” specification language with no direct support for concurrent message passing, encoding protocols correctly is a difficult and error-prone process. In [45] we propose a process calculus with constructs for manipulation of a global state by processes running in parallel. We show that this language can be translated to MSR 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. We apply the tool to several case studies among which a simplified fragment of PKCS#11, the Yubikey security token, and an optimistic contract signing protocol.

6.3.3. Automated Verification of Indistinguishability Properties

Participants: Vincent Cheval, Rémy Chrétien, Véronique Cortier, Steve Kremer.

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

Active case, unbounded number of sessions. We have studied how to reduce the search space for attacks on equivalence-based properties, for an unbounded number of sessions. Specifically, we have shown [38], [60] that if there is an attack then there is one that is well-typed. Our result holds for a large class of typing systems and a large class of *determinate* security protocols. Assuming finitely many nonces and keys, we can derive from this result that trace equivalence is decidable for an unbounded number of sessions for a class of tagged protocols, yielding one of the first decidability results for the unbounded case. As an intermediate result, we also provide a novel decision procedure in the case of a bounded number of sessions.

Active case, bounded number of sessions. We previously proposed a procedure for approximating trace equivalence in the case of a bounded number of sessions, i.e., for a replication free fragment of a cryptographic process calculus. The procedure is implemented in the *Akiss* tool. While we proved soundness and correctness for any convergent rewrite system that has the finite variant property, termination of the procedure was still an open question. We have recently shown that the procedure indeed terminates for the class of subterm convergent rewrite systems. The submission of this result is in preparation.

6.3.4. Securely Composing Protocols

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

Protocols may interact with an arbitrary attacker which yields a verification problem that has several sources of unboundedness (size of messages, number of sessions, etc.). In [14], we characterise a class of protocols for which deciding security for an unbounded number of sessions is decidable, by the means of a composition result. More precisely, we present a simple transformation which maps a protocol that is secure for a bounded number of protocol sessions (a decidable problem) to a protocol that is secure for an unbounded number of sessions. The precise number of sessions that need to be considered is a function of the security property and we show that for several classical security properties a single session is sufficient. Therefore, in many cases our result yields a design strategy for security protocols: (i) design a protocol intended to be secure for a single session; and (ii) apply our transformation to obtain a protocol which is secure for an unbounded number of sessions.

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

6.3.5. Soundness of the Dolev-Yao Model

Participants: Véronique Cortier, Guillaume Scerri.

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

Gergei Bana and Hubert Comon have proposed a new framework [73] where the symbolic model now specifies what an attacker *cannot* do instead of specifying what it can do. Checking protocols security can then be reduced to checking inconsistency of some set of first order formula. During his PhD, Guillaume Scerri studies how to develop a (polynomial) decision procedure for deciding consistency of sets of formulas, for some class of formulas corresponding to security protocols. This procedure has been extended and implemented, yielding the tool SCARY that can successfully analyse several protocols of the literature [52].

6.3.6. Advanced Cryptographic Models

Participant: David Galindo-Chacon.

A classical approach in cryptographic research consists in weakening the assumptions cryptographic primitives are built upon. The following works belong to this research line.

We generalize the decisional problem that was used to prove the security of a well-known hierarchical identity-based encryption scheme by Boneh, Boyen and Goh. We argue that our new problem is strictly harder than the original problem, and thus the security of the aforementioned cryptographic primitive is laid on even stronger foundations [24].

It is known how to transform certain canonical three-pass identification schemes into signature schemes via the Fiat-Shamir transform. Pointcheval and Stern showed that those schemes are existentially unforgeable in the random-oracle model leveraging the, at that time, novel forking lemma. Recently, a number of 5-pass identification protocols have been proposed. Extending the above technique to capture 5-pass identification schemes would allow to obtain novel unforgeable signature schemes. In this paper, we provide an extension of the forking lemma (and the Fiat-Shamir transform) in order to assess the security of what we call n-generic signature schemes. These include signature schemes that are derived from certain $(2n+1)$-pass identification schemes. In doing so, we put forward a generic methodology for proving the security of a number of signature schemes derived from $(2n+1)$-pass identification schemes for $n \geq 2$. As an application of this methodology, we obtain two new code-based existentially-unforgeable signature schemes, along with a security reduction. In particular, we solve an open problem in multivariate cryptography posed by Sakumoto, Shirai and Hiwatari at CRYPTO 2011 [22].

Traditionally, symbolic and computational models for cryptographic protocols do not take into account the data leaked due to the physical nature of the cryptographic computations. Recently, the research area of leakage-resilient cryptography has emerged in order to cope with this source of attacks in the computational model. We have studied a conjecture that states that an ElGamal-based public-key encryption scheme with stateful decryption resists lunch-time chosen ciphertext and leakage attacks in the only computation leaks information model. We have given a non-trivial upper bound on the amount of leakage tolerated by this conjecture. More precisely, we prove that the conjecture does not hold if more than a $(\frac{3}{8}+o(1))$ fraction of the bits are leaked at every decryption step, by showing a lunch-time attack that recovers the full secret key. The attack uses a new variant of the Hidden Number Problem, that we call Hidden Shares - Hidden Number Problem, which is of independent interest [25].

6.4. Model-based Verification

We have investigated extensions of regular model-checking to new classes of rewrite relations on terms. We have studied specification and proof of modular imperative programs, as well as of modal workflows.

6.4.1. Tree Automata with Constraints

Participants: Pierre-Cyrille Héam, Olga Kouchnarenko.

Tree automata with constraints are widely used to tackle data base algorithmic problems, particularly to analyse queries over XML documents. The model of Tree Automata with Global Constraints (TAGED) is a model introduced in 2009 for these purposes. The membership problem for TAGED is known to be NP-complete. The emptiness problem for TAGED is known to be decidable and the best known algorithm in the general case is non elementary. In collaboration with Vincent Hugot, we show that if there is at least one negative constraint, the problem is already NP-hard [64]. In the future, we plan to investigate upper bounds for the emptiness problem with a unique negative constraint. We also plan to study the complexity of the universality problem with a single constraint.

6.4.2. Random Generation of Finite Automata

Participant: Pierre-Cyrille Héam.

Developing new algorithms and heuristics raises crucial evaluation issues, as improved worst-case complexity upper-bounds do not always transcribe into clear practical gains. A suite for software performance evaluation can usually gather three types of entries: benchmarks, hard instance and random inputs, that deliver average complexity estimations, for which the catch resides in obtaining a meaningful random distribution (for instance a uniform random distribution).

In collaboration with Jean-Luc Joly, we investigate the problem of randomly and uniformly generating deterministic pushdown automata [65]. Based on a recursive counting approach, we propose a polynomial time algorithm for this purpose. The influence of the accepting condition on the generated automata is also experimentally studied.

Partially ordered automata are finite automata where simple loops have length one. They appear in several verification techniques, such as computing closures under semi-commutation relations or studying FIFO systems. In [68], we use a Markov chain based approach to randomly - and uniformly - generate deterministic partially ordered automata. The advantage of such a technique is its flexibility, allowing for instance to easily bound the number of loops. Experiments show that the mixing time seems to be polynomial, providing a tractable approach.

6.4.3. Verification of Linear Temporal Patterns over Finite and Infinite Traces

Participants: Pierre-Cyrille Héam, Olga Kouchnarenko.

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

6.4.4. Machine-Learning Techniques for Regular Model-Checking

Participants: Maxime Bride, Pierre-Cyrille Héam.

Using a machine-learning approach, we address the general problem of regular model-checking of computing $R^*(L)$, when L is a regular language and R a relation. Rather than developing specific algorithms to compute $R^*(L)$, it consists in using Angluin style's algorithms. In [58], we focus on the generation of examples, counter-examples and on the design of an oracle for the specific case of semi-commutation relations. Experiments are promising, particularly for the sizes of the obtained automata, which are quite smaller than with dedicated algorithms.

6.4.5. Constraint Solving for Verifying Modal Workflow Specifications

Participants: Hadrien Bride, Olga Kouchnarenko.

Workflow Petri nets are well suited for modelling and analysing discrete event systems exhibiting behaviours such as concurrency, conflict, and causal dependency between events. They represent finite or infinite-state processes, and several important verification problems, like reachability or soundness, are known to be decidable. Modal specifications introduced in [84] allow loose or partial specifications in a framework based on process algebras.

Our work in [34] focuses on the verification of modal workflow specifications using constraint solving as a computational tool. Its main contribution consists of a formal framework based on constraint systems to model executions of workflow Petri nets and their structural properties, as well as to verify their modal specifications. An implementation and promising experimental results obtained within the proposed approach constitute a practical contribution. In particular, a business process example from the IT domain enables to successfully assess the reliability of our contributions.

6.4.6. Rewriting-based Mathematical Model Transformations

Participants: Walid Belkhir, Alain Giorgetti.

Since 2011 we collaborate with the Department "Temps-Fréquence" of the FEMTO-ST institute (Franche-Comté Electronique Mécanique Thermique et Optique - Sciences et Technologies, CNRS UMR 6174) on the formalization of asymptotic methods (based on two-scale convergence). The goal is to design a software, called *MEMSALab*, for the automatic derivation of multiscale models of arrays of micro- and nanosystems. In this domain a model is a partial differential equation. Multiscale methods approximate it by another partial differential equation which can be numerically simulated in a reasonable time. The challenge consists in taking into account a wide range of geometries combining thin and periodic structures with the possibility of multiple nested scales. We have designed a transformation language facilitating the design of MEMSALab [17]. It is proposed as a Maple^{TM} package for rule-based programming, rewriting strategies and their combination with standard Maple^{TM} code. We illustrate the practical interest of this language by using it to encode two examples of multiscale derivations, namely the two-scale limit of the derivative operator and the two-scale model of the stationary heat equation. A more general framework for the derivation of the multi-scale models was established in [29].

6.5. Model-based Testing

Our research in Model-Based Testing (MBT) aims to extend the coverage of tests. The coverage refers to several artefacts: model, test scenario/property, and code of the program under test [55]. The test generation uses various underlying techniques such as symbolic animation of models [80], or symbolic execution of programs by means of dedicated constraints, SMT solvers, or model-checkers.

6.5.1. Automated Test Generation from Behavioral Models

Participants: Fabrice Bouquet, Kalou Cabrera, Jérome Cantenot, Frédéric Dadeau, Jean-Marie Gauthier, Julien Lorrain, Alexandre Vernotte.

We have developed an original model-based testing approach that takes a behavioral view (modelled in UML) of the system under test and automatically generates test cases and executable test scripts according to model coverage criteria [18]. We continue to extend this result to SysML specifications for validating embedded systems. We apply this method on smartSurface [44].

In the context of the FSN DAST project on Dynamic Application Security Testing, we investigated the use of a model-based testing approach for vulnerability testing in web applications. We designed a process based on two artefacts. First, a generic UML model, that is used to represent the web application entities (pages, forms, etc.), coupled with OCL constraints that describe the business logics of the application. Second, a set of test purposes, that will look for specific vulnerabilities (cross-site scripting, SQL injections, etc.). We have implemented a research prototype and applied it on several case studies. It has shown its effectiveness to detect vulnerabilities on already deployed web applications [50].

6.5.2. Scenario-Based Verification and Validation

Participants: Fabrice Bouquet, Kalou Cabrera, Frédéric Dadeau.

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

We have proposed a dedicated formalism to express test properties. A test property is first translated into a finite state automaton which describes a monitor of its behaviors. We have also proposed dedicated property coverage criteria that can be used either to measure the property coverage of a given test suite, or to generate test cases, exercising nominal or robustness aspects of the property [41]. This process has been fully tool-supported into an integrated software prototype[0]. This process has been designed during the ANR TASCCC project (2009-2012) and was continued during the ANR ASTRID OSEP project (2012-2013). The industrialization of this approach, and its integration within commercial test generation tools has started with the ANR ASTRID Maturation MBT_Sec project (2014-2015).

In the context of the SecureChange project, we have also investigated the evolution of test scenarios. As the system evolves, the model evolves, and the associated test scenarios may also evolve. We are currently extending the test generation and management of system evolutions to ensure the preservation of the security [43].

6.5.3. Mutation-based Testing of Security Protocols

Participants: Frédéric Dadeau, Pierre-Cyrille Héam, Ghazi Maatoug, Michaël Rusinowitch.

We have proposed a model-based penetration testing approach for security protocols [41]. This technique relies on the use of mutations of an original protocol, proved to be correct, for injecting realistic errors that may occur during the protocol implementation (e.g., re-use of existing keys, partial checking of received messages, incorrect formatting of sent messages, use of exponential/xor encryption, etc.). Mutations that lead to security flaws are used to build test cases, which are defined as a sequence of messages representing the behavior of the intruder. We have applied our technique on protocols designed in HLPSL, and implemented the protocol mutation tool jMuHLPSL that performs the mutations. The mutants are then analyzed by *CL-AtSe*. We have experimented our approach on a set of protocols, and we have shown the relevance of the proposed mutation operators and the efficiency of the *CL-AtSe* to conclude on the vulnerability of a protocol and produce an attack trace that can be used as a test case for implementations. We applied our approach on the Paypal Express protocol, and we were able to retrieve an existing attack trace on this protocol[0]. We also investigated the transformation of an attack trace into executable tests scripts. To achieve that, we have proposed to automatically generate skeletons of Java test programs that the validation engineer only has to fill in order to concretize the steps of the test. Experimentations on these principles have been described in [53].

6.5.4. Code and Contract-based Test Generation and Static Analysis

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

With the CEA we have developed a test generation technique based on C code and formal specifications, to facilitate deductive verification, in a new tool named StaDy [67], [49], [51]. The tool integrates the concolic test generator PathCrawler within the static analysis platform Frama-C. StaDy is able to handle the ANSI C Specification Language (ACSL) of the framework and other Frama-C plug-ins are able to reuse results from the test generator. This tool is designed to be the foundation stone of modular static and dynamic analysis combinations in the Frama-C platform.

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

[0] A video of the prototype is available at: http://vimeo.com/53210102

[0] http://www.nbs-system.com/blog/faille-securite-magento-paypal.html

on various strategies, namely uniform random generation, bounded exhaustive generation and rule-coverage-based test generation. In a recent work, we have proposed a dedicated constraint solver for PHP arrays aiming to avoid rejection during the generation of array structures. Finally, we have proposed dedicated specification coverage criteria to drive the test generation process. These coverage criteria focus on the selection of a subset of a method's contract, or the selection of specific predicates or realistic domains inside the contract. The whole approach has been implemented into a dedicated framework [62] integrated with state-of-the-practice test execution environments, such as atoum.

6.5.5. Random Testing

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

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

In [82] a method is proposed for drawing paths in finite graphs uniformly, and it is explained how to use these techniques for testing C programs within a control flow graph based approach. Nevertheless, as finite graphs often provide strong abstractions of the systems under test, many abstract tests generated by the approach cannot be played on the implementation. In [83], we have proposed a new approach, extending [82], to manage stack-call during the random test generation while preserving uniformity. In [23], we go further by investigating a way to biase the random testing, in order to optimize the probability to fulfil a coverage criterion. The new approaches have been implemented in a prototype and experimented on several examples.

6.6. Verification of Collaborative Systems

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

6.6.1. Automatic Analysis of Web Services Security

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

Automatic composition of web services is a challenging task. Many works have considered simplified automata models that abstract away from the structure of messages exchanged by the services. For the domain of secured services (using e.g., digital signing or timestamping) we propose a novel approach to automated orchestration of services under security constraints. Given a community of services and a goal service, we reduce the problem of generating a mediator between a client and a service community to a security problem where an intruder should intercept and redirect messages from the service community and a client service till reaching a satisfying state. This orchestration specification is expressed in ASLan language, a formal language designed for modeling Web Services tied with security policies that was developed in AVANTSSAR project. The AVANTSSAR Orchestrator (presented in [56]) generates an attack trace describing the execution of the mediator and translates it into ASLan. Then we can check with automatic tools that this ASLan specification verifies required security properties such as secrecy and authentication. If no flaw is found, we can compile the ASLan specification into a Java servlet that can be used to execute the orchestration.

In [16] we develop our alternative approach based on *parametrized automata*, a natural extension of finite-state automata over infinite alphabet. In this model the transitions are labeled with constants or variables that can be refreshed in some specified states. We prove several closure properties for this class of automata and study their decision problems. We show the applicability of our model to Web services handling data from an infinite domain. We introduce a notion of simulation that enables us to reduce the Web service composition problem to the construction of a simulation of a target service by the asynchronous product of existing services, and prove that this construction is computable. The existence of a service orchestrator solving a service composition problem can alternatively be reduced to the satisfiability of formula in parametrized propositional dynamic logic, and the latter was shown decidable in [33].

We now work on synthesizing composed services that satisfy required security policies.

6.6.2. Secure Querying and Updating of XML Data

Participants: Abdessamad Imine, Houari Mahfoud, Michaël Rusinowitch.

It is increasingly common to find XML views used to enforce access control as found in many applications and commercial database systems. To overcome the overhead of view materialization and maintenance, XML views are necessarily virtual. With this comes the need for answering XML queries posed over virtual views, by rewriting them into equivalent queries on the underlying documents. A major concern here is that query rewriting for recursive XML views is still an open problem, and proposed approaches deal only with non-recursive XML views. Moreover, a small number of works have studied the access rights for updates. In [11], we present SVMAX (Secure and Valid MAnipulation of XML), the first system that supports specification and enforcement of both read and update access policies over arbitrary XML views (recursive or non). SVMAX defines general and expressive models for controlling access to XML data using significant class of XPath queries and in the presence of the update primitives of W3C XQuery Update Facility. Furthermore, SVMAX features an additional module enabling efficient validation of XML documents after primitive updates of XQuery. The wide use of W3C standards makes of SVMAX a useful system that can be easily integrated within commercial database systems. We give extensive experimental results, based on real-life DTDs, that show the efficiency and scalability of our system.

6.6.3. Secure Computation in Social Networks

Participants: Bao Thien Hoang, Abdessamad Imine, Huu Hiep Nguyen, Michaël Rusinowitch.

Online social networks are currently experiencing a peak and they resemble real platforms of social conversion and content delivery. Indeed, they are exploited in many ways: from conducting public opinion polls about any political issue to publish social graph data for achieving in-depth studies. To securely perform these large-scale computations, we need the design of reliable protocols to ensure the data privacy. To address the polling problem in social networks (where the privacy of exchanged information and user reputation are very critical), we provide a simple decentralized polling protocol that relies on the current state of social graphs. More explicitly, we define one family of social graphs that satisfy what we call the m-broadcasting property (where m is less than or equal to a minimum node degree). We show their structures enable low communication cost and constitute necessary and sufficient condition to ensure vote privacy and limit the impact of dishonest users on the accuracy of the polling output. To securely publish social graph data, we focus on the problem of anonymizing a deterministic graph by converting it into an uncertain form [48], [47]. We first analyze drawbacks in a recent uncertainty-based anonymization scheme and then propose Maximum Variance, a novel approach that gains better tradeoff between privacy and utility. Towards a fair comparison between the anonymization schemes on graphs, the second contribution of our work is to describe a quantifying framework for graph anonymization by assessing privacy and utility scores of typical schemes in a unified space.

6.6.4. Safe and Secure Protocols for Collaborative Applications

Participants: Abdessamad Imine, Michaël Rusinowitch.

The Operational Transformation (OT) approach, used in many collaborative editors, allows a group of users to concurrently update replicas of a shared object and exchange their updates in any order. The basic idea is to transform any received update operation before its execution on a replica of the object. Designing transformation functions for achieving convergence of object replicas is a critical and challenging issue. In this work, we investigate the existence of transformation functions [27]. From the theoretical point of view, two properties, named TP1 and TP2, are necessary and sufficient to ensure convergence. Using controller synthesis technique, we show that there are some transformation functions, which satisfy TP1 for the basic signatures of insert and delete operations. But, there is no transformation function, which satisfies both TP1 and TP2. Consequently, a transformation function which satisfies both TP1 and TP2 must necessarily have additional parameters in the signatures of some update operations. Accordingly, we provide a new transformation function and show formally that it ensures convergence.

In [19], we propose a generic access control model based on replicating the shared document and its authorization policy at the local memory of each user. We consider the propagation of authorizations and their interactions. We use an optimistic approach to enforce access control in existing collaborative editing solutions in the sense that the access control policy can be temporarily violated. To enforce the policy, we resort to the selective undo approach in order to eliminate the effect of illegal document updates. To validate our approach, we implement an optimistic access control on the top of a collaboration prototype and measure its performance in the distributed grid GRID’5000 to highlight the scalability of our solution.

However, verifying whether the combination of access control and coordination protocols preserves the data consistency is a hard task since it requires examining a large number of situations. In [30], we specify this access control protocol in the first-order relational logic with Alloy, and we verify that it preserves the correctness of the system on which it is deployed, namely that the access control policy is enforced identically at all participating user sites and, accordingly, the data consistency remains still maintained.

COAST Team

5. New Results

5.1. An authentication/authorization framework for federated environments

Participants: Ahmed Bouchami, Olivier Perrin.

Collaborative environments have put an enormous challenge on the security of information processing systems used to manage them. In the context of the Open PaaS project, we worked on a decentralised hybrid framework for managing access control designed for support of these environments. In our proposal, we manage thress dimensions: the authentication, the access control, and the governance of the security.

Our authentication framework supports an interoperable authentication, a combination of RBAC, XACML for decentralized multiple administration (authorization). Both identities and resources are federated: the former are controlled by PaaS Federated Security Modules, while the later are by a PaaS Federated Security Modules. This work has been presented in the I-ESA conference ([10]).

We have also proposed a formal cloud-based authorization framework. We have considered trust to be a dynamic attribute to facilitate authorization decisions and have proposed models to handle different qualitative, quantitative and periodicity based temporal constraints. Further, we have presented an architecture for policies evaluation in the cloud. We presented our model in the CollaborateCom conference [17]. The model relies on a formal event-calculus based approach. We have introduced an architecture that considers different levels at which authorization policies can be specified and decisions can be taken and combines user level policies with the enterprise policies, and it considers real-time and dynamic environment changes (context), supports timed delegation, and the computation and specification of attributes based on trust. An implementation has been integrated in the Open PaaS platform.

A third aspect deals with the governance of the security aspects (mainly authorization). In this part, we have proposed to audit the various accesses to the resources, and we have proposed a model which is able to lower/raise the trust level of a member of the federated community.

During this year, we have also implemented and integrated the framework in the Open PaaS prototype, and all the code is now accessible in the repository of the project. The integration is done, and the other components of the project are now using the authentication/authorization component.

5.2. Experimental user studies for collaborative editing

Participants: Mehdi Ahmed-Nacer, François Charoy, Claudia-Lavinia Ignat, Gérald Oster, Pascal Urso.

With several tools to support collaborative editing such as Google Drive and Etherpad, the practice of colaborative editing is increasingly common, e.g., group note taking during meetings and conferences, and brainstorming activities. While collaborative editing tools meet technical goals, the requirements for group performance are unclear. One system property of general interest is delay between a modification of a user is performed and this modification is visible to the other users. This delay can be caused by different reasons such as network delay due to physical communication technology, the complexity of various algorithms for ensuring consistency and the type of underlying architectures. No prior work questioned the maximum acceptable delay for real-time collaboration or the efficacy of compensatory strategies.

In [14] we studied the effect of delay on group performance on an artificial collaborative editing task where a group of four participants located the release dates for an alphabetized list of movies and re-sorted the list in chronological order. The experiment was performed with eighty users. We measured sorting accuracy based on the insertion sort algorithm, average time per entry, strategies (tightly coupled or loosely coupled task decomposition of the task) and chat behavior between users. We found out that delay slows down participants which decrements the outcome metric of sorting accuracy. Tightly coupled task decomposition enhances outcome at minimal delay, but participants slow down with higher delays. A loosely coupled task decomposition at the beginning leaves a poorly coordinated tightly coupled sorting at the end, requiring more coordination as delay increases.

In asynchronous collaborative editing, such as version control, the main feature to allow collaboration is the merge feature. However, software merging is a time-consuming and error-prone activity, and if a merge feature return results with too many conflicts and errors, this activity becomes even more difficult. To help developers, several algorithms have been proposed to improve the automation of merge tools. These algorithms aim at minimising conflict situations and therefore improving the productivity of the development team, however no general framework is proposed to evaluated and compare their result.

In [9] we propose a methodology to measure the effort required to use the result of a given merge tool. We employ the large number of publicly available open-source development histories to automatically compute this measure and evaluate the quality of the merging tools results. We use the simple idea that these histories contains both the concurrent modifications and their merge results as approved by the developers. Through a study of six open-source repositories totalling more than 2.5 millions lines of code, we show meaningful comparison results between merge algorithms and how to use the results to improve them.

5.3. Optimization and security of business processes in SaaS contexts

Participants: Claude Godart, Elio Goettelmann, Samir Youcef.

Globalization and the increase of competitive pressures created the need for agility in business processes, including the ability to outsource, offshore, to take opportunity of the cloud, or otherwise distribute its once-centralized business processes or parts thereof. While hampered thus far by limited infrastructure capabilities, the increase in bandwidth and connectivity and decrease in communication cost have removed these limits. This is even more true with the advent of cloud, particularly in its “Service as a software” dimension. To adapt to such a context, there is a growing need for the ability to fragment one’s business processes in an agile manner, and be able to distribute and wire these fragments so that their combined execution recreates the function of the original process. Our work is focused on solving some of the core challenges resulting from the need to dynamically restructure enterprise interactions. Restructuring such interactions corresponds to the fragmentation of intra- and inter-enterprise business process models. It describes how to identify, create, and execute process fragments without loosing the operational semantics of the original process models. In addition, this fragmentation is complicated by the constraints of quality of service, in particular the execution time and the cost, and of security, especially privacy. During the year, we consider this problem at two levels: the design of privacy-aware process models, and the optimization of process schedules. We developed a methodology to integrate privacy concerns in the design of a business process before distribution in the cloud [11]. Based on a risk analysis, the result of the design is a set of process (re)modeling actions, a set of constraints on process fragments assignments to clouds, and a set of constraints for cloud selection based on cloud properties [12].

CORIDA Team

6. New Results

6.1. Highlights of the Year

The CORIDA team organized two scientific meetings in 2014.

The first workshop, “Observers for finite and infinite dimensional systems” in April 2014, gathered people working in the field of control theory for finite and infinite dimensional systems.

Ten speakers from France, India, Portugal and Germany were invited for the second workshop, “Workshop in Mathematical Fluid Dynamics", in November 2014.

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

In [42], we consider a two dimensional collision problem for a rigid solid immersed in a cavity filled with a perfect fluid. we investigate the asymptotic behavior of the Dirichlet energy associated to the solution of a Laplace Neumann problem as the distance between the solid and the cavity’s bottom tends to zero. We prove that the solid always reaches the cavity in finite time. The contact occurs with non zero (real shock) or null velocity velocity (smooth landing), depending on the tangency exponent at the contact point. The proof is based on a suitable change of variables sending to infinity the cusp singularity at the contact. More precisely, the initial Laplace Neumann problem is transformed into a generalized Neumann problem set on a domain containing a horizontal strip, whose length goes to infinity as the the solid gets closer to the the cavity’s bottom.

In [43], we investigate the geometric inverse problem of determining, from the knowledge of the DtN operator of the problem, the positions and the velocities of moving rigid solids in a bounded cavity filled with a perfect fluid. We assume that the solids are small disks moving slowly. Using an integral formulation, we first derive the asymptotic expansion of the DtN map as the diameters of the disks tend to zero. Then, combining a suitable choice of exponential type data and the DORT technique (which is usually used in inverse scattering for the detection of point-like scatterers), we propose a reconstruction method for the unknown positions and velocities.

In [22], Ana Leonor Silvestre (Lisbon, Portugal) and Takéo Takahashi analyze the system fluid-rigid body in the case of where the rigid body is a ball of “small radius”. More precisely, they consider the limit system as the radius goes to zero. They recover the Navier-Stokes system with a particle following the the velocity of the fluid.

In [14], Mehdi Badra (University of Pau) and Takéo Takahashi study the feedback stabilization of a system composed by an incompressible viscous fluid and a rigid body. They stabilize the position and the velocity of the rigid body and the velocity of the fluid around a stationary state by means of a Dirichlet control, localized on the exterior boundary of the fluid domain and with values in a finite dimensional space. The first result concerns weak solutions in the two-dimensional case, for initial data close to the stationary state. The method is based on general arguments for stabilization of nonlinear parabolic systems combined with a change of variables to handle the fact that the fluid domain of the stationary state and of the stabilized solution are different. This additional difficulty leads to the assumption that the initial position of the rigid body is the position associated to the stationary state. Without this hypothesis, they work with strong solutions, and to deal with compatibility conditions at the initial time, they use finite dimensional dynamical controls. They prove again that for initial data close to the stationary state, they can stabilize the position and the velocity of the rigid body and the velocity of the fluid.

In [15], Mehdi Badra (University of Pau) and Takéo Takahashi use the Fattorini criterion (more known as the Hautus criterion) to obtain the feedback stabilizability of general linear and nonlinear parabolic systems. They then consider flow systems described by coupled Navier-Stokes type equations (such as MHD system or micropolar fluid system) to obtain the stabilizability by only considering a unique continuation property of a stationary Stokes system.

In [36], we use geometric control theory to investigate the existence and the design of optimal strokes for swimmers in Stokes of potential flows.

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

In [20], we use microlocal analysis techniques to build artificial boundary conditions for reltivistic quantum dynamics.

In [11], we give a complete analysis of some new domain decomposition techniques and investigate their approximations for application in quantum physics.

In the chapter [28], we give an introduction to the modeling and the simulation of equilibrium states of Gross-Pitaevskii equations modeling Bose-Einstein condensates.

In [17], we give the basic methodology to use the software 3D GPELab for the simulation of Bose-Einstein condensates.

In [10], we develop a pseudo-spectral iterative method to compute equilibrium state of fast rotating Gross-Pitaevskii equations.

In [18], we develop a new approximation and implementation of a Magnetic-to-Electric operator for 3D-Maxwell equations.

In [13], we consider the inverse problem of determining the potential in the dynamical Schrödinger equation on the interval by the measurement on the boundary. Using the Boundary Control Method we first recover the spectrum of the problem from the observation at either left or right end points. Taking advantage of the one-dimensional configuration, we recover then the spectral function, reducing the problem to the classical one of determining the potential from the spectral function. This can be done by known methods. In order to handle more realistic situations, we also consider the case where only a finite number of eigenvalues are available and we prove the convergence of the reconstruction method as this number tends to infinity.

6.4. Observality, controllability and stabilization in the time domain

In [27], we dealt with the problem of the stabilization of a switched linear system, the feedback law being based on the optimization of a quadratic criterion. The Lyapunov function used for the design of this law defines a tight upper bound of the value of the cost for a quadratic optimization problem related to the system. Thus the obtained control law is sub-optimal.

In [19] we deal with the problem of the output stabilization of linear impulsive systems. These system are a mix of continuous and discrete-time system. An observer is synthesized and the stabilization is ensured through a feedback law which depends on the estimated state provided by the observer.

In [29], we consider the design an high gain observers for a class of continuous dynamical systems with discrete-time measurements. In this work, the measurement sampling time is considered to be variable. Moreover, the new idea of the proposed work is to synthesize an observer requiring the less knowledge as possible from the output measurements. This is done by using an updated sampling time observer. Under the global Lipschitz assumption, the asymptotic convergence of the observation error is established. As an application of this approach, an state estimation problem of an academic bioprocess is studied, and its simulation results are discussed.

In [26], we propose an MPC control scheme for a linear system with real-time constraints.

In [25] and [12], we use precise energy estimates to provide an upper bound on the error made when replacing the dynamics of an infinite dimensional conservative quantum system by a finite dimensional projection.

In [34], we give a set of sufficient conditions for approximate controllability of closed quantum systems when the dipolar approximation has to be replaced by a more realistic quadratic modeling.

In [35], we investigate the regularity of propagators of bilinear control systems and extend a celebrated negative result of Ball, Marsden and Slemrod.

In [16], we consider an infinite dimensional system modelling a boost converter connected to a load via a transmission line. The governing equations form a system coupling the telegraph partial differential equation with the ordinary differential equations modeling the converter. The coupling is given by the boundary conditions and the nonlinear controller we introduce. We design a nonlinear saturating control law using a Lyapunov function for the averaged model of the system. The main results give the well-posedness and stability properties of the obtained closed loop system.

MADYNES Project-Team

6. New Results

6.1. Highlights of the Year

The following points of 2014 deserves to be highlighted:

- One new permanent member joined the MADYNES team: Jérôme François as Inria researcher.
- An IBM Faculty Award has been received by a team member (Rémi Badonnel, TELECOM Nancy) for his work on security and cloud computing.

BEST PAPER AWARD :
[21] **8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2014**. A. MAYZAUD, A. SEHGAL, R. BADONNEL, I. CHRISMENT, J. SCHÖNWÄLDER.

6.2. Monitoring

6.2.1. P2P network monitoring

Participants: Thibault Cholez [contact], Isabelle Chrisment, Olivier Festor.

Finishing a work started several years ago with our colleagues from the team Complex Network [0] at the LIP6, we published a final result on the comparison of paedophile activity in different P2P systems [5]. We designed a methodology for comparing KAD and eDonkey, two P2P systems among the most prominent ones and with different anonymity levels. We have detected paedophile-related queries with a previously validated tool and we proposed, for the first time, a large-scale comparison of paedophile activity in two different P2P systems.

We are also glad to have contributed to a book chapter in french on the uses and misuses of digital identities on the Internet [33]. It summarizes several years of work of the team, fighting against the Sybil attack in P2P networks in order to improve their security and quality of service.

6.2.2. Anonymous networks monitoring

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

Anonymous networks have emerged to protect the privacy of network users. Large scale monitoring on these systems allows us to understand how they behave and which type of data is shared among users.

In 2014, we continued our research about the I2P anonymous network [0]. This network is optimized for anonymous web hosting and anonymous file-sharing. I2P's file-sharing community is highly active with users deploying their file-sharing applications on top of the network. I2P uses a variation of Onion routing, thus assuring the unlinkability between a user and its file-sharing application. In [26] we took the first step towards the linkability of users and applications in the I2P network. We conducted a group-based characterization, where we determine to what extent a group of users is responsible for the overall I2P's file-sharing activity. We used Pearson's coefficient to correlate users from two cities and the most used anonymous file-sharing application.

6.2.3. Smartphone usage monitoring

Participants: Vassili Rivron [contact], Mohammad Irfan Khan, Simon Charneau [Inria], Isabelle Chrisment.

Over the last few years the number of smartphone applications has increased enormously. In 2014, we passively collected smartphones usage logs in the wild by inviting the crowd to participate in the PRACTIC [0] contest and install our crowdsensing application to contribute anonymous smartphone usage logs, voluntarily and in the most natural settings (their own phone, own pricing plan) .

[0] http://www.complexnetworks.fr/
[0] http://i2p2.de
[0] http://beta.apisense.fr/practic

Complementary to sensing we also collected contextual information (social, demographic, professional) and information about users'perception via survey questionnaires built in the application or on the web.

This experiment used a crowd sensing platform called APISENSE ®[0] and developed by the Inria Spirals Team. It was carried out in the context of building a country-wide Internet observation platform in France, called Metroscope [0].

6.3. Security

6.3.1. Security Automation

Participants: Rémi Badonnel [contact], Martin Barrere, Gaëtan Hurel, Abdelkader Lahmadi, Olivier Festor.

The main research challenge addressed in this work is focused on enabling configuration security automation in dynamic networks and services.

A first part of our work in the year 2014 was centered on a strategy for remediating known vulnerabilities, formalizing the correction decision problem as a satisfiability or SAT problem [10]. From a proactive perspective, it should be able to decide which potential states could be dangerous. By specifying our vulnerability knowledge source (OVAL repository) as a propositional logical formula, we have fixed system properties that we cannot change and free those variables for which changes are available. We have introduced the X2CCDF language, built on top of XCCDF and OVAL, that allows us to express the impact of these changes over target systems. These descriptions can be used for analyzing the security impact of changes without actually changing the system. When this information is not available, we have considered the NETCONF protocol and its notion of candidate state where changes can be applied, analyzed and rolled back if necessary.

A second part of our work has been dedicated to the orchestration of security functions in the context of mobile smart environments [19]. Most of current security approaches for these environments are provided in the form of applications or packages to be directly installed on the devices themselves inducing local resource consumption. In that context, we have investigated a new approach for outsourcing mobile security functions as cloud-based services for smartphones and tablets [32]. The outsourced functions are dynamically activated, configured and orchestrated using software-defined networking and virtualization techniques. We consider the use of security compositions in order to dynamically fit the security requirements of mobile devices according to their current contexts. This approach is based on different traversal schemes (sequential, conditional, and concurrent). The solution has been prototyped based on the mininet software-defined networking emulator, jointly with mobile devices using the android operating system.

6.3.2. SDN-based security

Participants: Jérôme François [contact], Lautaro Dolberg [University of Luxembourg], Olivier Festor, Thomas Engel [University of Luxembourg].

By decoupling the data and control plane, Software-Defined Networking allows a fine grained network management. Protocols like OpenFlow allow multiple actions like traffic forwarding or blocking but also modifications or monitoring with the extensive use of counters. Hence, many approaches have emerged the last year to enable some security functions like firewalls, flow monitoring and traffic redirection to middleboxes. These different scenarios have been evaluated in a survey paper [17] in cooperation with the university of Luxembourg.

Furthermore, we also proposed to leverage SDN, especially OpenFlow, for forensics purpose [18]. Indeed, through a recursive analysis on network path and flow tables in OpenFlow, it is possible to reconstruct the paths traversing by an anomaly.

[0] http:///www.apisense.com/
[0] http://metroscope.eu/

6.3.3. Phishing Detection

Participants: Jérôme François [contact], Samuel Marchal [University of Luxembourg], Radu State [University of Luxembourg], Thomas Engel [University of Luxembourg].

This work is a joint work with the University of Luxembourg.

The language used for phishing is a particular language aiming at attracting victims. To achieve that the attackers uses specific words related to well known brand names and reassuring words. Our method to detect such abnormal domain names relies on word decomposition and semantic analysis. As an example, we can learn if having both *microsoft* and *protected* in domain is significative of a malicious domain. Actually, not all words can be represented during the learning and we use semantic similarities to also extend this knowledge (for example, we can *derive* safe from *protected*).

Our recent work [20] was focusing on extending this domain-based analysis to the full analysis of an url. We have also observed that most of false positives or negatives we obtained with previous methods are biased by natural language corpus while the *Internet vocabulary* is different.

Hence, we extracted from Google and Yahoo statistics about search queries. Our observation highlights that the relation between the different parts of the URL (the domain and the path) is a discriminative feature for malicious URL identification.

Finally, a more in-depth feature analysis is provided in [8], which also proposes leveraging streaming data analytics by instantiating our method on Storm.

6.3.4. Flows and logs analysis

Participants: Jérôme François [contact], Abdelkader Lahmadi.

Machine generated-log data is a fundamental part of information technology systems. They are usually generated at every component of distributed information systems including routers, security products, web proxies, DHCP servers, VPN servers, or any end-points like mobile devices or connected things, etc. They often contain high volumes of interesting information and are among the first data source to be analyzed for the detection of abnormal activities due to running attacks or malicious running applications. A better understanding of these attacks and malicious applications requires the elaboration of efficient and novel methods and techniques able to analyze these logs.

In [16], we carried an empirical analysis of the logs generated by the logging system available in Android environments. The logs are mainly related to the execution of the different components of applications and services running on an Android device. We have analyzed the logs using self organizing maps where our goal is to establish behavioral fingerprints of Android applications. The developed methodology allows us the better understand Android Apps regarding their granted permissions and performed actions.

During the year 2014, we have also maintained an IETF draft [50] to make a standardization effort towards the extension of IP Flow-based monitoring with geographic information. Associating Flow information with their measurement 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.

6.3.5. Sensor networks monitoring

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

Low Power and Lossy Networks (LLNs) are made of interconnected wireless devices with limited resources in terms of energy, computing and communication. The communication channels are low-bandwidth, high loss rate and volatile wireless links subject to failure over time.

This year, our work on security-oriented monitoring [28] has focused on quantifying the effects of version number manipulation attacks within RPL networks [21]. Through simulations it was discovered that control overhead can increase by up to 18 times, thereby impacting energy consumption and channel availability. This in turn can reduce the delivery ratio of packets by up to 30% and nearly double the end-to-end delay in a network. A strong correlation between the position of the attacker and the effect on the network was also observed.

In that context, we have designed a mitigation strategy based on an adaptive threshold to cover a large variety of DODAG inconsistency attacks [25] in a lightweight manner. Currently RPL attempts to counteract such attacks by using a fixed threshold. During experimentations it becomes clear that the adaptive threshold is able to reduce the control message overhead, compared to fixed threshold, by up to 13% in short lived and 55% in long-lived networks. This leads to large reductions, i.e., between 10%-40%, in energy consumption.

In addition, we have investigated a distributed passive monitoring architecture for RPL-based advanced measurement infrastructure networks.

6.3.6. Intrusion Detection System in Wireless Sensor

Participants: Emmanuel Nataf [contact], Hubert Kenfack Ngankam.

This work is based on a previous work about the definition of an ontology to classify intrusion attacks in a wireless sensors network. A first implementation of this ontology focuses on the black hole and the sink hole intrusion where some malicious sensor node either do not forward data to a central point of collect or try to be elected as the best next hop toward the central point.

We look at discover malicious nodes by an analysis of the network topology obtained by data gathered from the network itself. At regular interval, we built a snapshot view of the network topology and compare it with the previous one in order to detect anomalies such as a whole sub network that disappear or an under-optimal network topology.

Simulation results are good and we will continue on this way.

6.3.7. SCADA systems security

Participants: Abdelkader Lahmadi [contact], Younes Abid.

SCADA systems are facing several attacks and threats which are growing in number and complexity. A key challenge in this context is the simulation and the assessment of the impact and the propagation of these attacks on SCADA system components over time. During the year 2014, we have developed a novel methodology [38] based on stochastic modeling to simulate the impact of attacks on SCADA systems. The system is modeled as a network of interacting markov chains and the impact of an attack is simulated using the influence model. In this model, the state of each node of the system is either influence by its own Markov chain or by the state of its neighboring nodes. We have modeled and analyzed a SCADA system with 200 control nodes and several servers. We have modeled different attacks (intrusion, DoS, malware) where attack nodes are introduced in the interacting SCADA network to influence control node behaviors. For each attack, we have simulated and assessed over time the availability of the overall system regarding the number of failed nodes.

6.3.8. Management of HTTPS traffic

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

Surveys show that websites are more and more being served over HTTPS. They highlight an increase of 48% of sites using TLS over the past year (2013),

We 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 show that SNI has two weaknesses, regarding (1) backward compatibility and (2) multiple services using a single certificate. We demonstrated thanks to a web browser plug-in called *Escape* that we designed and implemented, how these weaknesses can be practically used to bypass firewalls and monitoring systems relying on SNI. The results show positive evaluation (firewall's rules successfully bypassed) for all tested websites. This work will be published in the experience session of the IFIP/IEEE International Symposium on Integrated Network Management (IFIP/IEEE IM'15).

We also started a new work on the precise identification of websites accessed through HTTPS in the context of network forensic investigation. We use a new set of features in conjunction with machine learning techniques to achieve a high accuracy.

6.4. Routing

6.4.1. Routing in Wireless Sensor Networks

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

We deployed a wireless sensors network in the laboratory during two time period of 3 months. The first was with the legacy routing (based on expected transmission time metric) and the second was with our routing process based on a composition of several metrics (i.e. energy, transmission time and delay) by the use of fuzzy logic. We have compared these experiments by packet loss ratio and energy consumption. In all case, our routing leads to a better network [48].

6.4.2. Operator calculus based routing in Wireless Sensor Networks

Participants: Evangelia Tsiontsiou, Bernardetta Addis, Ye-Qiong Song [contact].

For supporting different QoS requirements, routing in WSN must simultaneously consider several criteria (e.g., minimizing energy consumption, hop counts or delay, packet loss probability, etc.). When multiple routing metrics are considered, the problem becomes a multi-constrained optimal path problem (MCOP), which is known as NP-complete.

Recently, Operator calculus (OC) has been developed by Schott and Staples with whom we collaborate. We make use of OC methods on graphs to solve path selection in the presence of multiple constraints. Based on OC, we developed a distributed algorithm for path selection in a graph. We also designed a new routing protocol which makes use of this algorithm: the Operator Calculus based Routing Protocol (OCRP). In OCRP, a node selects the set of eligible next hops based on the given constraints and the distance to the destination. It then sends the packet to all eligible next hops. The protocol is implemented in Contiki OS and emulated for TelosB motes using Cooja. We compared its performance against tree and directional flooding routing and show the advantages of our technique. Our ongoing work consists in its comparison with RPL to show its effective contribution to handle simultaneously several IETF ROLL routing metrics.

This work is under development as part of Lorraine AME Satelor project.

6.4.3. Energy-aware IP networks management

Participants: Bernardetta Addis [contact], Giuliana Carello [DEIB, Politecnico di Milano, Italy], Antonio Capone [DEIB, Politecnico di Milano, Italy], Luca Gianoli [Polytecnique de Montreal, Canada], Sara Mattia [IASI, CNR, Roma, Italy], Brunide Sansò [Polytecnique de Montreal, Canada].

The focus of our research is to minimize the energy consumption of the network through a management strategy that selectively switches off devices according to the traffic level. We consider a set of traffic scenarios and jointly optimize their energy consumption assuming a per-flow routing. We propose a traffic engineering mathematical programming formulation based on integer linear programming that includes constraints on the changes of the device states and routing paths to limit the impact on quality of service and the signaling overhead. We also present heuristic results to compare the optimal operational planning with online energy management operation ([3])

Two very important issues that may be affected by green networking techniques are resilience to node and link failures, and robustness to traffic variations. We thus extended the optimization models. To guarantee network survivability we consider two different schemes, dedicated and shared protection, which assign a backup path to each traffic demand and some spare capacity on the links along the path. Robustness to traffic variations is provided by tuning the capacity margin on active links in order to accommodate load variations of different magnitude. Both exact and heuristic methods are proposed. Experimentations carried out on realistic networks operated with flow-based routing protocols (like MPLS) allow us to quantitatively analyze the trade-off between energy cost and level of protection and robustness. Results show that significant savings, up to 30%, may be achieved even when both survivability and robustness are fully guaranteed [4].

Computational cost of proposed models can be very high when dealing with large size instances (network size and/or number of demands). For this reason, we proposed and tested different problem formulations with the aim of solving larger size instances at optimality. Preliminary results on a simplified model ([29]) are very encouraging.

6.4.4. Energy-aware joint management of networks and Cloud infrastructures

Participants: Bernardetta Addis [contact], Danilo Ardagna [DEIB, Politecnico di Milano, Italy], Giuliana Carello [DEIB, Politecnico di Milano, Italy], Antonio Capone [DEIB, Politecnico di Milano, Italy].

Fueled by the massive adoption of Cloud services, overall service centers and networks account for 2–4% of global CO_2 emissions and it is expected they can reach up to 10% in 5–10 years.

The geographical distribution of the computing facilities offers many opportunities for optimizing energy consumption and costs by means of a clever distribution of the computational workload exploiting different availability of renewable energy sources, but also different time zones and hourly energy pricing. Energy and cost savings can be pursued by dynamically allocating computing resources to applications at a global level, while communication networks allow to assign flexibly load requests and to move data. We propose an optimization framework able to jointly manage the use of brown and green energy in an integrated system and to guarantee quality requirements. We propose an efficient and accurate problem formulation that can be solved for real-size instances in few minutes to optimality. Numerical results, on a set of randomly generated instances and a case study representative of a large Cloud provider, show that the availability of green energy have a big impact on optimal energy management policies and that the contribution of the network is far from being negligible ([2]).

6.4.5. Content centric wireless sensor networks

Participants: Abdelkader Lahmadi [contact], Younes Abid, Olivier Festor.

During this year, we have instantiated a novel named data aggregation method [9] dedicated to wireless sensor networks . The method relies on an adaptation of the CCNx protocol implementation that we have developed in a previous work. Our method extends the CCNx protocol with in-network processing functions to aggregate named data efficiently. We have implemented and tested our solution with the Contiki operating system which is an operating system for resources-constrained embedded systems and wireless sensor networks. Our simulation and measurement results using the Cooja simulator and physical nodes show that our solution has a small overhead in terms of exchanged messages and provides acceptable data retrieval delays.

6.5. Quality-of-Service

6.5.1. ICN cache management

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

Information Centric Networking (ICN) has become a promising new paradigm for the future Internet architecture. It is based on named data, where content address, content retrieval and the content identification is led by its name instead of its physical location. One of the ICN key concepts relies on in-network caching to store multiple copies of data in the network and serve future requests, which helps reducing the load on servers, congestion in the network and enhances end-users delivery performances. As a central component of ICN is in-network caching, the ely used as a micro-blogging service. At the same time, Online Social Networks (OSN) carry extremely valuable information about users and their relationships. We argue that this knowledge can help to drastically improve the efficiency of ICN.

We therefore propose SACS, a caching strategy designed for the CCN architecture that includes social information [11]. CCN is to date the most widely adopted ICN architecture by the research and industrial community. The underlying idea in such strategy is that a small number of users counts a huge amount of social relationships, dominates the activity and receives most attention from other users. We call such users Influential users, and we argue that they produce content that is more likely to be consumed by others, and in consequence their content must be favored and replicated in priority. Our novel caching strategy is therefore prioritizing content from Influential users of the social network. To validate our strategy, we first propose a model of social network over the CCN architecture [30]. Our model has been designed based on the measurement of Pinterest, a web-based OSN system. Extensive simulations of the strategy have been performed, as well as a real implementation on CCNx and deployment over the PlanetLab testbed. Our results with SACS are significant and increase drastically the caching performance of ICN architecture. content

Efficient management of caches is a key success factor in Concent-Centric Networks where multiple (up to every single node in the network) entities act as caches of the shared content in the network. We pursued our investigations towards a common evaluation framework for cache strategies in Content-centric networks and towards the definition of novel cache strategies, exploiting context information available at the service level of today’s internet.

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

Participants: Kévin Roussel, Shuguo Zhuo, 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.

The two MAC protocols that we have previously designed namely S-CoSenS and iQueue-MAC, have been successfully implemented on SMT32W108 SoC chips. Two contributions have been made this year. Firstly iQueue-MAC has been extended to work on both single channel mode and multi-channel mode, improving its throughput performance. Secondly, both S-CoSenS and iQueue-MAC have been implemented on RIOT OS. An additional contribution is related to the RIOT OS development itself since we have improved the robustness of the existing ports of RIOT OS on MSP430-based motes, making it a suitable software platform for tiny motes and devices. More generally, through this part of work, we have shown that RIOT OS is also suitable for implementing high-performance MAC protocols, thanks to its real-time features (especially hardware timers management). Part of this work has been supported by ANR-NFSC Quasimodo and PIA LAR projects.

6.5.3. End-to-end delay modelling and evaluation in wireless sensor networks

Participants: François Despaux, Abdelkader Lahmadi, Ye-Qiong Song [contact].

Probabilistic end-to-end performance guarantee may be required when dealing with real-time applications. As part of ANR QUASIMODO project, we are dealing with Markov modeling of multi-hop networks running duty-cycled MAC protocols. One of the problems of the existing Markovian models resides in their strong assumptions that may not be directly used to assess the end-to-end delay in practice. In particular, realistic radio channel, capture effect and OS-related implementation factors are not taken into account. We proposed to explore a new approach combining code instrumentation and Markov chain analysis. In [15] we have presented a new approach for extracting empirical Markov chain models from network protocol traces by means of Process Mining techniques. An empirical Markov chain model was obtained for the IEEE 802.15.4 beacon-enabled mode protocol allowing us to estimate the e2e delay for a multi-hop scenario. This approach has also been successfully applied to the case of ContikiMAC [14].

6.5.4. Dynamic resource allocation in network virtualization

Participants: Mohamed Said Seddiki, Mounir Frikha [SupCom, Tunis, Tunisie], Ye-Qiong Song [contact].

The objective of this research topic is to develop different resource allocation mechanisms in Network Virtualization, for creating multiple virtual networks (VNs) from a single physical network. It is accomplished by logical segmentation of the network nodes and their physical links.

This year we have focused on implementing and evaluating the used of SDN for managing the QoS in broadband access networks. Unfortunately, application-based QoS on a home network gateway faces significant constraints, as commodity home routers are not typically powerful enough to perform application classification, and many home users are not savvy enough to configure QoS parameters. In [24] we designed FlowQoS, an SDN-based approach where users can specify upstream and downstream bandwidth allocations for different applications at a high level, offloading application identification to an SDN controller that dynamically installs traffic shaping rules for application flows We designed a custom DNS-based classifier to identify different applications that run over common web ports; a second classifier performs lightweight packet inspection to classify non-HTTP traffic flows. We implemented FlowQoS on OpenWrt and demonstrated that it can improve the performance of both adaptive video streaming and VoIP in the presence of active competing traffic.

This work has been carried out as part of a co-supervised PhD thesis between University of Lorraine and SupCom Tunis.

6.5.5. *Task and message scheduling in distributed real-time systems*

Participants: Florian Greff, Laurent Ciarletta, Ye-Qiong Song [contact].

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 analysed for validating the system design. In [37], [36], [34], and [35], we provided an overview of both message scheduling techniques in networks and joint task and message scheduling approaches in closed-loop distributed control systems (networked control systems). Fault-tolerance is another critical issue that one must take into account. In collaboration with an industrial partner, we started a study on the real-time dependability of UAV multi-criticity system interconnected by an embedded mesh network. The future work aims at developing a robust mesh network routing protocol and studying the schedulability under constraints of multi-criticality and graceful degradation during mode change.

6.6. Multi-modeling and co-simulation tools for the evaluation and development of Smart* and other Pervasive Computing systems

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

Vincent Chevrier (Maia team, LORIA) is a collaborator and the correspondant for the MS4SG project, Benjamin Camus, Victorien Elvinger and Christine Bourjot (Maia team, LORIA) are collaborators for the AA4MM. Julien Vaubourg's PhD is 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 [51] 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 MS4SG projet which involves MAIA, Madynes and EDF R&D on smart-grid simulation, we developed a proof of concepts for a smart-appartment case[12].

In 2014 we worked on the following research topics:

- Assessment and evaluation of complex systems.

  This work, centered on the problem of controlling complex systems proposed a control architecture within Tomas Navarrete's work [22], [23]. This “equation-free” approach uses a multi-agent model to evaluate the global impact of local control actions before applying the most pertinent set of actions. Based on a partial perception of the system state, we determine which actions to execute in order to avoid or favor certain global states of the system.

  Associated to our architecture, an experimental platform has been developed to confront the basic ideas or the architecture within the context of simulated “free-riding” phenomenon in peer to peer file exchange networks. We have demonstrated that our approach allows us to drive the system to a state where most peers share files, despite given initial conditions that are supposed to drive the system to a state where no peer shares.

- Cyber Physical Systems [13]

  We have led 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. Applying co-simulation technique we plan to develop a hybrid "network-aware flocking behavior" / "behavior aware routing protocol".

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

  The effort put in the UAVs gathers academic and research ressources from the Aetournos platform, the R2D2 ADT and the 6PO project, while applied, industrial and more R&D projects have been pursued this year (Outback Joe Search and Rescue Challenge, Alerion, Hydradrone) .

- MS4SG has given us the opportunity to link multi-simulations tools such as HLA (High Level Architecture) and FMI (Functional Mockup Interface) thanks to our AA4MM framework. We 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[12].

In 2015, we will continue working on the hybrid protocols and on the UAV platform, and apply our co-simulation work to Smart Grids and other Smart*.

MAGRIT Project-Team

6. New Results

6.1. Highlights of the Year

We were invited to present our work on *Impact of Soft Tissue Heterogeneity on Augmented Reality for Liver Surgery* in the TVCG Special Session at SIGGRAPH Asia 2014.

6.2. Matching and 3D tracking

Pose initialization
Automating the camera pose initialization is still a problem in non instrumented environments. Difficulties originate in the possibly large viewpoint changes and lighting variations between the data stored in the model and the current view. One year ago, we began to investigate the use of viewpoint simulation techniques for relocalization within P. Rolin's PhD thesis. We especially consider challenging situations where the current view is distant from the image sequence used for model construction. We here consider scene models built from image sequence using Structure from Motion techniques. A point is then represented by its 3D coordinates and small image patches arising from the images where the point is detected.The underlying idea is to enrich 3D points by descriptors generated from virtual viewpoints chosen away from the learning sequence. For each 3D point of the model, a local image patch is generated from a set of virtual viewpoints, taking into account the local 3D normal and the images of the learning sequence. View synthesis is performed with an affine or an homography model. Though one possible shortcoming of simulation is to generate too many incorrect patches at discontinuities in the scene and thus to degrade the matching step, our preliminary results are very promising [25] and show a noticeable increase of the inlier ratio in the matching stage and an improved stability of the computed pose, especially when homography models are considered. We exhibit many examples where our method successfully computes the camera pose whereas the traditional methods fail.

Current investigations are about the development of scalable solutions for pose computation in large environments with several leverage actions in view. Designing efficient probabilistic techniques for matching and defining strategies based on the geometry of the scene for choosing a reduced set of virtual views are lines of research under investigation for jointly limiting the redundancy and improving the performance of the matching.

Tracking 3D deformable objets
3D augmentation of deformable objects is a challenging problem with many potential applications in computer graphics, augmented reality and medical imaging. Most existing approaches are dedicated to surface augmentation and are based on the inextensibility constraint, for sheet-like materials, or on the use of a model built from representative samples. However, few of them consider in-depth augmentation which is of utmost importance for medical applications. Since the beginning of N. Haouchine's PhD thesis, we have addressed several important limitations that currently hinder the use of augmented reality in the clinical routine of minimally invasive procedures. In collaboration with the SHACRA team, our main contribution is the design and the validation of an augmented reality framework based on a mechanical model of the organ and guided by features extracted and tracked on the video at the surface of the organ [2]. Specific models which best suit the considered organs, such as a vascularized model of the liver, have been introduced in this framework. During this year, we have first performed quantitative evaluation of the method [17]. Promising results were obtained through in-vivo experimentation on a human liver and ex-vivo validation on a porcine liver. In this latter case, artificial tumors were introduced in the liver, thus allowing a quantitative evaluation of the error between the predicted and the actual tumor. These experiments show that localization errors were less than 6mm, and thus below the safety margin required by surgery. To our knowledge, we were the first to produce such evaluation for deformable objects. This work has been extended to augment highly elastic objects in a monocular context [16], whereas previous works were guided by 3D features obtained with a stereo-endoscope. The only

parameter involved in the method is the Young's modulus but we show in experiments that a rough estimate of the Young's modulus is sufficient to obtain a good reconstruction. Experiments on computer-generated and real data have shown the effectiveness of the approach. The method is currently restricted to the orthographic projection and its extension to full projective geometry is under investigation.

A bio-mechanical model-based approach has also been considered in the context of tongue tracking in ultrasound images with a view to produce an augmented head for language learning. A crucial issue is the robustness of the tracking due to the strong speckle noise in ultrasound (US) data. Here, a small number of points are used to guide the model. Selection of feature points is based on the uncertainty associated to the tracked points and on spatial constraints. This model has proven to be especially efficient in the case of non uniform and fast movements [19].

Use of AR in educational sciences
In collaboration with the Ecole supérieure du professorat et de l'éducation and the PErSEUs laboratory at Université de Lorraine, we designed an inquiry-based AR learning environment (AIBLE) for teaching and learning astronomy in primary school (children of 8-11 years old). The novelty of this environment is the combination of Inquiry Based Sciences Education principles and didactics principles (here of astronomy) with AR capabilities. In this context, a GPL-licensed software called AIBLE-AstroAR has been developed based on the ARToolkit library. This software basically consists of a tangible user interface, which allows the children to move virtual celestial objects "as for real" and investigate in order to find origins of Moon phases evolution, alternation of day and night, seasons and Moon/Sun eclipses.

Last year, a study has been carried out to compare AIBLE with a physical model traditionally used in primary school. This study indicated that AIBLE significantly enhances learning compared to classical support. During this year, we performed further investigation with a larger panel of children to assess which characteristics of the environment facilitate learning [14]. Analyses of the marker positions as moved by the children indicated that AIBLE really facilitates heuristic investigation, which fosters consciousness of the origin of astronomical phenomena. This work provides new opportunities for teachers to identify solving problem strategies initiated by learners. These results also contribute to the understanding of the ways through which AR can be used in formal teaching curricula in K-12 schools.

6.3. Image-based modeling

Modeling vasculature for real time simulation
One of our objectives to benefit interventional neuroradiology is to offer a patient-based interactive simulator to the interventional radiologists. Our contributions address vasculature modeling from patient data, namely 3D rotational angiography (3DRA) volumes. During Ahmed YUREIDINI's PhD thesis (2010-2014), a new model was developed consisting of a tree of local implicit blobby models.

We've been collaborating with SHACRA Inria project-team (Lille-Nord Europe) and the Department of Interventional Neuroradiology from Nancy University Hospital, in the context of the SOFA-InterMedS Inria Large-Scale Initiative. Ahmed YUREIDINI defended his PhD thesis in May this year with highest honors [9]. In particular, a detailed study was made to compare our tree of local implicits with triangular meshes in a view to model synthetic shapes as well as vasculatures from patient data. Increased performances with regard to processing speed, numerical stability and realism of the behavior were demonstrated.

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 but the vasculature and no other brain tissue. In particular, since at most only two projective fluoroscopic views are available, containing absolutely no depth hint, the 3D shape of the micro-tool (guidwire, 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 solution in a two-view reconstruction context was proposed this year based on the extraction of the guide-wire as a skeleton in the images. The large stereo basis (views are almost orthogonal) and the segmentation errors (such as both missing parts and spurious segments in the skeleton) make the reconstruction especially difficult. The skeletons are subdivided in simple curves that are matched to build all corresponding potential 3D curves. These curves are nodes in a graph whose edge weights express a connection cost that takes into account both distance and orientation at the curves extremities. The solution 3D curve is provided by following the path of minimal cost in the graph. This algorithm demonstrated very good reconstruction results on synthetic and phantom data. A paper on this subject has been accepted for publication at SPIE Medical Imaging 2015.

Patient-specific heart valve modeling

Many pathologies damage heart valve anatomy producing undesired backflow, or regurgitation, decreasing cardiac efficiency and potentially leading to heart failure if left untreated. Such cases could be treated by surgical repair for the valve. However it is technically difficult and outcomes are highly dependent upon the experience of the surgeon: he must essentially predict the displacement and deformation of complex valve leaflets and supporting structures. One way to facilitate the repair is to simulate the mechanical behavior of the pathological valve with patient-specific data. This is the objective of Pierre-Frédéric Villard's one-year CNRS delegation in the Harvard Bio-robotics Laboratory (HBL). During the initial three first months of the sabbatical leave, various tasks have been performed: i) Study of the physiology of pathological valve behavior with medical experts. Following anatomical book reading and medical expert interviews the anatomy and the physiology are now understood. ii) Evaluation of HBL material for 4D ultrasound segmentation. HBL has previously developed a method to extract mitral valve geometry from a home-made high temporal resolution 3D ultrasound and iii) Automatic segmentation of a Mitral Valve microCT to feed a biomechanical model. A method to semi-automatically segment the leaflet-chordae set has been developed.

6.4. Parameter estimation

Metrologic performance assessment in experimental mechanics

A problem of interest in experimental solid mechanics is strain map estimation on the surface of a specimen subjected to a load or a tensile test. One of the available approaches is based on images of a pseudo-periodic grid transfered on the surface of the specimen. Sensor noise is a major source of uncertainty in the strain map, and quantifying the propagation of the sensor noise to the measured strain components is a major problem when metrological performances are in view. We have proposed in [12] a study of the mathematical properties of the popular method based on windowed Fourier analysis, under a Gaussian white noise assumption. In the case of a more realistic signal-dependent, heteroscedastic noise, we have quantified in [10] (see also [15], [26]) the trade-off between the noise amplitude, the measurement resolution and the spatial resolution of the method. We have also investigated image stacking for noise reduction. While averaging a serie of images is certainly the most basic option to reduce the noise, it is not effective for studying grid images under a high magnification factor, because of unavoidable residual vibrations carried for instance by concrete floor slabs. We have shown in [13] that, while these vibrations indeed blur grid images, they still permit to reduce the noise amplitude in the displacement and strain maps.

Sensor noise measurement.

While searching for a low-cost on-the-fly estimation of the sensor parameters based on a serie of grid images (thus with no need of changing the experimental setting), we have proposed in [11] an algorithm which is able to deal with the vibrations biasing the estimations. More generally, we have investigated in [21] the problem of sensor parameter estimation from a series of images, under light flickering and vibrations. Light flickering is indeed a natural assumption for indoor artificial lights. It is also involved by slight variations in the opening time of a mechanical shutter. We have proposed a model of the pixel intensity based on a Cox process, together with an algorithm which, taking benefit of flickering, gives an estimation of every sensor parameter, namely the gain, the readout noise, and the offset.

Image driven simulation
In the IDeaS ANR project we propose to target Image-driven simulation, applied to interventional neuroradiology: 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).

Our guideline is to follow a sequential statistical filtering approach to fuse such heterogeneous data. This approach first calls for an improved knowledge of the statistical behavior of the simulation, which we addressed in the past year through experimental studies. We described our experimental setup in [20], which, in particular uses high speed stereo reconstruction to be able to study non quasi-static effects. Preliminary measures of the catheter speed during stick and slip transitions back up our conviction that quasi-static mechanical models fail to simulate such rapid motions of the tool. Our on-going analysis of the simulation sensitivity to mechanical parameters also sets forward friction as critical for high-fidelity simulation.

MAIA Project-Team

6. New Results

6.1. Highlights of the Year

- Two Research Fellow have been recruited with a focus on Service Robotics: Serena Ivaldi (CR2) and Francis Colas (CR1).
- The paper entitled : Exploiting Separability in Multiagent Planning with Continuous-State MDPs Jilles Dibangoye, Christopher Amato, Olivier Buffet, François Charpillet won the best paper award at AAMAS'2014, the international conference on autonomous agents and multi-agents.
- Jilles Dibangoye got an Assistant Professor position at INSA Lyon.

BEST PAPER AWARD :
[12] **13th International Conference on Autonomous Agents and Multiagent Systems**. J. S. DIBANGOYE, C. AMATO, O. BUFFET, F. CHARPILLET.

6.2. Decision Making

6.2.1. Complexity Analysis of Exact Dynamic Programming Algorithms for MDPs

Participant: Bruno Scherrer.

Eugene Feinberg and Jefferson Huang are external collaborators from Stony Brooks University.

Following last year's work on the strong polynomiality of Policy Iteration, we show that the number of arithmetic operations required by any member of a broad class of optimistic policy iteration algorithms to solve a deterministic discounted dynamic programming problem with three states and four actions may grow arbitrarily. Therefore any such algorithm is not strongly polynomial. In particular, the modified policy iteration and λ-policy iteration algorithms are not strongly polynomial. This work was published in the *Operations Research Letters* [4].

6.2.2. Analysis of Approximate Dynamic Programming Algorithms for MDPs

Participants: Bruno Scherrer, Manel Tagorti.

Matthieu Geist is an external collaborator from Supélec.

In [40], we consider LSTD(λ), the least-squares temporal-difference algorithm with eligibility traces algorithm proposed by Boyan (2002). It computes a linear approximation of the value function of a fixed policy in a large Markov Decision Process. Under a β-mixing assumption, we derive, for any value of $\lambda \in (0, 1)$, a high-probability estimate of the rate of convergence of this algorithm to its limit. We deduce a high-probability bound on the error of this algorithm, that extends (and slightly improves) that derived by Lazaric et al. (2012) in the specific case where $\lambda = 0$. In particular, our analysis sheds some light on the choice of λ with respect to the quality of the chosen linear space and the number of samples, that complies with simulations. This work was presented at the National JFPDA conference [34].

In the context of infinite-horizon discounted optimal control problem formalized by Markov Decision Processes, we focus on several approximate variations of the Policy Iteration algorithm: Approximate Policy Iteration (API), Conservative Policy Iteration (CPI), a natural adaptation of the Policy Search by Dynamic Programming algorithm to the infinite-horizon case (PSDP), and the recently proposed Non-Stationary Policy Iteration (NSPI). For all algorithms, we describe performance bounds with respect the per-iteration error ϵ, and make a comparison by paying a particular attention to the concentrability constants involved, the number of iterations and the memory required. Our analysis highlights the following points: 1) The performance guarantee of CPI can be arbitrarily better than that of API, but this comes at the cost of a relative—exponential in $\frac{1}{\epsilon}$—increase of the number of iterations. 2) PSDP$_\infty$ enjoys the best of both worlds: its performance guarantee is similar to that of CPI, but within a number of iterations similar to that of API. 3) Contrary to API that requires a constant memory, the memory needed by CPI and PSDP is proportional to their number of iterations, which may be problematic when the discount factor γ is close to 1 or the approximation error ϵ is close to 0; we show that the NSPI algorithm allows to make an overall trade-off between memory and performance. Simulations with these schemes confirm our analysis. This work was presented at this year's international conference on Machine Learning (ICML) [28].

Finally, we consider Local Policy Search, that is a popular reinforcement learning approach for handling large state spaces. Formally, it searches locally in a parameterized policy space in order to maximize the associated value function averaged over some predefined distribution. The best one can hope in general from such an approach is to get a local optimum of this criterion. The first contribution of this article is the following surprising result: if the policy space is convex, *any* (approximate) *local optimum* enjoys a *global performance guarantee*. Unfortunately, the *convexity* assumption is strong: it is not satisfied by commonly used parameterizations and designing a parameterization that induces this property seems hard. A natural solution to alleviate this issue consists in deriving an algorithm that solves the local policy search problem using a boosting approach (constrained to the convex hull of the policy space). The resulting algorithm turns out to be a slight generalization of conservative policy iteration; thus, our second contribution is to highlight an original connection between local policy search and approximate dynamic programming. This work was presented at this year's European conference on Machine Learning (ECML) [27].

6.2.3. Adaptive Management with POMDPs

Participants: Olivier Buffet, Jilles Dibangoye.

Samuel Nicol and Iadine Chadès (CSIRO) are external collaborators.

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

During Samuel Nicol's visit, the main problem we have studied is how to manage company inspections to deter these companies from adopting dangerous behaviors. This was modeled as a particular Stackelberg game, where N companies benefit from acting badly as long as they are not caught by inspections, and where 1 government agency has to decide which companies to inspect given a limited budget. The expected result is a stochastic strategy (randomly deciding which companies to inspect, with probabilities that depend on the benefits/losses of both types of players). We are working on exploiting particular features of this computationally complex problem to make it more tractable.

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

Participants: Jilles Dibangoye, Olivier Buffet, François Charpillet.

External collaborators: Christopher Amato (MIT).

Decentralized partially observable Markov decision processes (DEC-POMDPs) are rich models for cooperative decision-making under uncertainty, but are often intractable to solve optimally (NEXP-complete), even using efficient heuristic search algorithms.

State-of-the-art approaches relied on turning a Dec-POMDP into an equivalent deterministic MDP —whose actions at time t correspond to a vector containing one decision rules (/instantaneous policy) per agent— typically solved using a heuristic search algorithm inspired by A*. In recent work (IJCAI'13), we have identified a sufficient statistic of this MDP —an *occupancy state*, i.e., a probability distribution over possible states and joint histories of the agents— and demonstrated that the value function was piecewise-linear and convex with respect to this statistic. This brings us in the same situation as POMDPs, allowing to generalize the value function from one occupancy state to another and to propose much faster algorithms (also using efficient compression methods).

This year, we have further progressed on this line of research.

- A journal paper has been submitted that presents the "occupancy MDP" approach in details.
- In the case of Network-Distributed POMDPs, a particular setting where the relations between agents follow a fixed network topology, we have shown that the value function could be decomposed additively with one value function per neighborhood. This work has been presented at AAMAS'2014 [12], receiving the conference's best paper award.
- To further scale up the resolution of Dec-POMDPs, we have proposed multiple approximations techniques that can be combined and allow controlling error bounds. This work has been presented at ECML'2014 [13].

6.2.5. Learning Bad Actions

Participant: Olivier Buffet.

Jörg Hoffmann, former member of MAIA, Michal Krajňanský (Saarland University), and Alan Fern (Oregon State University) are external collaborators.

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

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

A first algorithm (with variants) has been proposed that learns rules for detecting (supposedly) bad actions. It has been empirically evaluated, providing encouraging results, but also showing that different variants will perform best in different settings. This algorithm has been presented at ECAI'2014 [24], and has participated in the learning track of the international planning competition in 2014 (http://ipc.icaps-conference.org/).

6.3. Ambiant Intelligence And Robotic Systems

6.3.1. Adaptation of autonomous vehicle traffic to perturbations

Participants: Mohamed Tlig, Olivier Buffet.

Olivier Simonin, a former member of the MAIA team, is an external collaborator from INSA-Lyon.

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

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

In 2013, we have started looking at improving vehicle flows in complete road networks. In particular, we have proposed an approach that allows multiple flows of vehicles to cross an intersection without stopping, allowing to reduce delays as well as energy consumption. This has led to a publication in ICALT-14 [30], with more details in a research report [41].

This year, we have made a further step by coordinating the controller agents located in each of the network's intersections. More precisely, they are constrained to let the vehicles alternate at the same frequency —at the expense of potentially reducing the maximum flow of some roads— and a distributed algorithm offsets these "signals" so as to optimize either the energy consumption, or the time spent in the network. This tends to induce "green waves" wherever possible, i.e., to prevent vehicles from having to slow down before a traffic light. This work has been presented at ECAI-14 [31].

6.3.2. Platooning: safe and precise virtual hooking mechanism or automated vehicles

Participants: Jano Yazbeck, Alexis Scheuer, François Charpillet.

Among the several goals that we were trying to achieve in InTraDE, we were interested in platooning too. In her PhD thesis, Jano Yazbeck considers Platooning as a technique that aims at steering , safely and precisely, a train of vehicles along a path generated by a leader which can be driven by a human. Thus the trajectory is unknown to the followers. Platooning is considered in this project in order to move containers efficiently from the discharge zones of ships to the storage areas.

To obtain a safe and precise platooning, we aim at controlling the longitudinal and lateral behaviors of each vehicle of the platooning. On the one hand, the longitudinal controller computes a longitudinal velocity (or acceleration) which avoids collisions between vehicles by maintaining a safe inter-distance between each couple of successive vehicles. On the other hand, the lateral controller computes an angular velocity or a steering angle so that the vehicle follows precisely the leader's path. These two controllers can be decoupled and computed separately when the convoy moves at a low velocity.

This year, we proposed a platooning algorithm based on a near-to-near decentralized approach which has been published at ICRA 2014 [32]. In this approach, each vehicle estimates and memorizes on-line the path of its predecessor as a set of points. After choosing a suitable position to aim for, the follower estimates on-line the predecessor's path curvature around the selected target. Then, based on a heuristic search, it computes an angular velocity using the estimated curvature. The optimization criteria used in this work allows the robot to follow its predecessor's path without oscillation while reducing the lateral and angular errors.

In october, Jano Yazbeck defended her Phd Thesis [2].

6.3.3. Map Matching

Participant: François Charpillet.

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

6.3.4. Multi-Camera Tracking in Partially Observable Environment

Participants: Arsène Fansi Tchango, Olivier Buffet, Vincent Thomas, Alain Dutech.

Fabien Flacher (Thales ThereSIS) is an external collaborator.

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

The approach we are working on is based on (1) the HMM (Hidden Markov Models) formalism to represent the state of the system (the persons and their internal states), (2) a simulator provided and developed by Thales ThereSIS, and (3) particle filtering approaches based on this simulator. Since activity and location depend on each other, we adopt a Simultaneous Tracking and Activity Recognition approach (STAR) as presented in current state-of-the-art approaches.

A first novelty lies in the use of a complex behavioral simulator. In a single-target setting, we demonstrated that it allows inferring the behavior of a complex individual, even in case of long periods of occlusions (when cameras do not cover the trajectory of the target). This idea led to publications in AAMAS-14 [16], STAIRS-14 [18], and ECAI-14 [17].

A remaining issue is to find tractable algorithms for efficiently tracking multiple targets simultaneously, which requires using a factored particle filter (with one distribution per target). To that end, we use a Joint Probabilistic Data Association Filter with two key ingredients. The first ingredient is a particular model of dynamics that largely decouples the evolution of several targets, and turns out to be very natural to apply (which has led already to a publication in Fusion-14 [19]). Then, the factorization *a priori* implies, for a given target, simulating each of its particles with each particle of each other target (which leads to a huge number of simulations). The second proposed ingredient is to simulate each particle of a given target only with a small number of "representatives" of each other target (and then, because more particles are produced than needed, a selection/resampling step is required).

6.3.5. Emergence et Developmental Learning

Participants: Alain Dutech, Matthieu Zimmer.

Yann Boniface (CORTEX, Loria) is an external collaborator

Following our ongoing work on using reinforcement learning for the control of redundant continous robotic systems, we explore how learning such complex tasks can benefit from a developmental approach, following some line of work already tested in robotics [50].

"Emergence", on of the key concepts grounding this work, has been presented – from an artificial intelligence perspective – and discussed with researchers from other fields. This lead to fruitful exchanges and a chapter in a bookdedicated to the dual aspects of (human gestures) : appearance and emergence [36]. "Developmental Learning" was also the main subject of a seminar in Lyon in which Alain Dutech has been invited [47].

More concretely, we have developed several algorithms which mix artificial neural networks (like Dynamic Self-Organizing Maps or Reservoir Computing Network) with reinforcement learning mechanisms in order to build simple artificial systems that are *autnomous* and that learn without any *exogeneous* intervention from an external being. This work, initiated through two master thesis, is now the central topic ot the PhD of Matthieu Zimmer, started in october 2014.

6.3.6. Online Evolutionary Learning

Participants: Amine Boumaza, François Charpillet, Iñaki Fernandèz.

Evolutionary Robotics (ER) deals with the design of agent behaviors using artificial evolution. Within this framework, the problem of learning optimal decision functions (or controllers) is treated as a policy search problem in the parameterized space of candidate policies. In this work we are interested in learning optimal behaviors for swarm of mobile agents online (while solving the task). We adopt an online onboard distributed view [56], [48] and consider the learning process as executed at the agents' level in a decentralized way. This kind of algorithms raises several questions concerning the usefulness of selection pressure (partial views of population, noisy fitness values, etc.).

We studied the impact of task-driven selection pressures in on-line distributed ER for swarm behavior learning. We proposed a variant of the mEDEA [45] algorithm in which we added a selection operator, in a task-driven scenario. We evaluated four selection methods that induce different intensity of selection pressure in a multi-robot navigation with obstacle avoidance task and a collective foraging task.

Experiments showed that a small intensity of selection pressure is sufficient to rapidly obtain good performances on the tasks at hand. We introduced different measures to compare the selection methods, and show that the higher the selection pressure, the better the performances obtained, especially for the more challenging food foraging task. This research was presented at the 13th International Conference on the Synthesis and Simulation of Living Systems [21].

6.3.7. Frailty evaluation and Fall detection

Participants: Amandine Dubois, François Charpillet, Thomas Moinel, Maxime Rio.

This work is related to the IPL PAL and Satelor project and is related to Personal Assistant Living (PAL) for elderly people with loss of autonomy.

- Clinical evaluation of frailty in the elderly is the first step to decide the degree of assistance that elderly people require. No standard tests exist to detect the level of frailty, each clinician chooses his protocol among existing tools. There are clinical tests as *Tinetti test*, *Timed Up and Go* test for evaluating the degree of dependance and the frailty of elderly people. These tests consist in asking a person to realize exercises simulating movements of daily life. The physician evaluates the quality of gait and the balance of the patient. These tests are often used but, the disadvantage is that the final verdict relies primarily on a subjective opinion. The aim of our work is to provide new objective criteria to refine the elderly frailty quantification. We base ourselves on the frailty definition of Fried *et al* as being a clinical syndrome in which three or more of the following criteria are present: unintentional weight loss, self reported exhaustion, weakness (with regards to grip strength), slow walking speed and low physical activity. From this definition, we have defined two axis of development to evaluate the frailty of a person: Sensor based Activity recognition with the aim to follow and report daily life activities in order to detect evolution that coud reveal increased frailty [1], gait analysis in order to assess gait pattern and their evolution over time [14].
- An other PAL research domain, which is related to activity recognition, has attracted our attention: fall detection. Falls in the elderly is a major public health problem because of their frequency and their medical and social consequences. One of our objectives is to design an automatic system to detect fall at home, which in its final version will be made up of a network of RGB-D sensors, some of them being mobile embedded a wheel mobile robot.

The main contribution of this work has been to design a simple but robust method based on the identification and tracking of the center of mass of people evolving in an indoor environment through a RGB-D camera. Using a simple Hidden Markov Model whose observations are the position of the center of mass, its velocity and the general shape of the body, we have shown that we can surprisingly monitor the activity of a person with high accuracy, detect falls with very good accuracy without false positives and also measure some interesting parameter such as speed of gait, length of steps, etc. An experimental study, that is reported in [46], has been driven in our smart apartment lab. 26 subjects were asked to perform a predefined scenario in which they realized a set of eight postures. 2 hours of video (216 000 frames) were recorded for the evaluation, half of it being used for the training of the model. The system detected the falls without false positives. This result encourages us to use this system in real situation for a better study of its efficiency. Therefore, we started this year an experimention in a room of a follow-up care and rehabilitation facility (OHS) in Nancy. "Office d'Hygiène Sociale" (OHS) is an association under the law of 1901. It supports nearly 800 people over 60 years and nearly 1,000 children and adults with disabilities. The association manages 26 facilities (40% health field, 40% medical-social field and 20% social field) and employs more than 1,500 professionals.

6.3.8. Posture recognition with a Depth camera

Participants: Abdallah Dib, François Charpillet, Xuan Nguyen, Alain Filbois [SED].

In this research line, we focus our contribution on improving model-based approaches that use a population-based stochastic framework for full human body tracking using monocular depth camera. One of the major challenges in human tracking is the high-dimensional state spaces. To address this problem, we propose a tracking algorithm based on APF and CMA-ES. While APF has been widely applied for human tracking in RGB and depth images, the application of CMA-ES to human tracking is still limited. Yet, CMA-ES shares many similar ideas with APF and can be exploited to improve the performance of APF. Our key idea is to update the covariance matrix for sampling particles at each layer of APF, using a subset of best particles, an idea inspired from CMA-ES. The resulting algorithm is shown to greatly reduce the number of particles required for successful tracking. In the absence of image features such as texture or color, existing likelihood models for human tracking in depth images are often built by computing distances between data points and model points sampled on the surface of the human body model. When human body parts are close or when severe self-occlusions are present, these models fail to capture good pose hypotheses. As a result, existing approaches are unable to track a broad range of human motions. To deal with this issue, we propose a likelihood model which is based on comparing observed depth images and rendered depth images obtained by classic rendering techniques. Combining with our tracking algorithm, the proposed likelihood model has been shown to be effective when tracking under severe self-occlusions. To the best of our knowledge, our approach is the first model-based one that uses a population-based stochastic framework able to track full human body with non-frontal and unusual poses, using monocular depth camera.

6.3.9. Pressure sensing floor

Participants: Mihai Andries, François Charpillet, Olivier Simonin.

The use of floor-sensors in ambient intelligence contexts began in the late 1990's, with projects like ORL active floor, the Magic carpet by Paradiso *et al.*, and the smart floor by Orr *et al.* These floors were, later on, integrated in smart environments, aimed at delivering assistance services like continuous diagnosis of users' health. According to the literature there are currently at least 6 main types of floor pressure sensing technologies: binary switches, piezoelectric, load cells, capacitive, polymer thick film (PTF), and photo interrupter sensors. Most of presented solutions extract a set of features for their tracking and identification task. Recently, sensing floors products like the SensFloor (a floor network of capacitive proximity sensors), Capfloor (a network of capacitive sensors), Elsi® smart floor (http://www.elsitechnologies.com) and FloorInMotion (Tarkett France) started being commercialized by companies, mainly for the senior care industry.

We have ourselves developed a sensing floor. This load-sensing floor 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. Each tile has 16 light-emitting diodes which provide visual feedback. The processing units were manufactured by Hikob [0]. This prototype was originally designed as a medium of interaction for robots with distributed control, in an ant-like fashion. The computing unit available on each tile can register a virtual pheromone trace, that can then be transmitted to other robots, using either wired or wireless communication. In a different perspective, the sensing-floor acts merely as a sensor for an ambient intelligence. Using the magnetometer embedded on the processing unit of the tile, each tile can detect disturbances in its surrounding magnetic field, that can be caused by the presence of robots. Each tile also has an embedded accelerometer, that allows it to detect shocks that can be caused by objects or humans falling on the ground.

Several functionalities have been implemented this year on this prototype floor, including weight measurement, fall detection, footstep tracking and activity recognition. We also implemented heuristic real-time multi-user localisation (without user identification) in an indoor setting using this prototype floor.

6.3.10. Living assistant Robot

Participants: François Charpillet, Nicolas Beaufort, Abdallah Dib.

[0] http://www.hikob.com/

With LAR (**living AssistanT Robot**), a PIA projet which started in March, Abdallah Dib joined our team for a PhD. His work is about the development of a low cost navigation system for a robot evolving in an indoor environment. The main issue of his work is to design a Simultaneous Localisation and Mapping algorithm working in a dynamic environment in which people are moving. This is very challenging if we restrict the sensing capabilities of the robot with low cost sensors such as RGB-D camera. An important service we expect the robot to achieve, is realizing similar services as the one we described below: fall detection, activity recognition. This year first result have been published [11]. A feature based visual SLAM method that uses chamfer distance to estimate the camera motion from RGB-D images has been presented. The method does not require any matching which is an expensive operation and always generates false matching that affects the estimated camera motion. Our approach registers the input image iteratively by minimizing the distance between the feature points and the occupancy grid using a distance map. We demonstrate with real experiments the capability of the method to build accurate 3D map of the environment with a hand-held camera. While the system was mainly developed to work with RGB-D camera, occupancy grid representation gives the method the ability to work with various types of sensors, we show the capacity of the system to construct accurate 2D maps using telemeter data. We also discuss the similarities between the proposed approach and the traditional ICP algorithm.

6.3.11. Exploring an unknown environment with a team of mobile robots

Participants: François Charpillet, Olivier Simonin, Nassim Kaldé.

This work is the continuation of the work realized during the ANR Cart-O-matic (2010 to 2013). We address, here, the problem of efficient allocation of the navigational goals in the multi-robot exploration of unknown environment. Goal candidate locations are repeatedly determined during the exploration. Then, the assignment of the candidates to the robots is solved as the task-allocation problem. A more frequent decision-making may improve performance of the exploration, but in a practical deployment of the exploration strategies, the frequency depends on the computational complexity of the task-allocation algorithm and available computational resources. Therefore, this year, we have proposed an evaluation framework to study exploration strategies independently on the available computational resources. A comparison of the selected task-allocation algorithms deployed in multi-robot exploration has been done and published with Jan Faigl from Czech Technical University in Prague in the framework of the PHC project MACOREX.

An other point that is addressed by Nassim Kaldé is to consider the same problem but with dynamical environment in particular populated with human beings. First results of Nassim Kalde have been published in JFSMA'14 [33]. He published too the work done during his Master thesis [23].

6.4. Understanding and mastering complex systems

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

Participant: Vincent Chevrier.

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

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

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

Associated to our architecture, an experimental platform has been developed to confront the basic ideas or the architecture within the context of simulated “free-riding” phenomenon in peer to peer file exchange networks. We have demonstrated that our approach allows to drive the system to a state where most peers share files, despite given initial conditions that are supposed to drive the system to a state where no peer shares. We have also executed experiments with different configurations of the architecture to identify the different means to improve the performance of the architecture.

This work helped us to better identify [26] the key questions that rise when using the multi-agent paradigm in the context of control of complex systems, concerning the relationship between the model entities and the target system entities.

6.4.2. Multi Modeling and multi-simulation

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

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

Laurent Ciarletta is the co-advisor of the thesis of Julien Vaubourg.

Complex systems generally require to use different points of view (abstraction levels) at the same time on the system in order to capture and to understand all the dynamics and the complexity. Being made of different interacting parts, a model of a complex system also requires simultaneously modeling and simulation (M&S) tools from different scientific fields.

We proposed the AA4MM meta-model [54] that solves the core challenges of multimodelling and simulation coupling in an homogeneous perspective. In AA4MM, we chose a multi-agent point of view: a multi-model is a society of models; each model corresponds to an agent and coupling relationships correspond to interaction between agents.

This year we progress in the definition of multi-level modeling [42]. We identified several facets of multi-level modeling and implemented then as different kinds of interactions in AA4MM framework. We progressed on the specification of the meta-model which helped to define a modeling environment.

In the MS4SG projet which involves MAIA, Madynes and EDF R&D on smart-grid simulation, we developed a proof of concepts for a smart-appartment case [10].

6.4.3. Cellular automata as a foundation of complex systems

Participant: Nazim Fatès.

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

We proposed an extended version of our survey on asynchronous cellular automata [3].

In collaboration with colleagues from India, we proposed a complete characterisation of the reversibility of the set of the 256 Elementary Cellular Automata with asynchronous updating [29]. These rules are known to be diffcult to study in all generality and it is interesting to notice that here, asynchronism is an aid rather than an obstacle to analyse the behaviour of the systems.

With Henryk Fukś (Brock Univ., Canada), we proposed a mathematical analysis of the second-order phase transitions that are observed in the most simple asynchronous cellular automata [22].

Our work on the classification of cellular automata was presented in the AUTOMATA’14 conference and is now the topic of a collaboration with L. Gerin (École Polytechnique) [44], [20].

We are currently participating to the edition of the first book devoted to probabilistic cellular automata and to a special issue of the French-speaking journal *Technique et Science Informatique* (Lavoisier editors).

6.4.4. Revisiting wavefront construction with collective agents: an approach to foraging.

Participants: François Charpillet, Olivier Simonin.

We consider here [7], the problem of coordinating a team of agents that have to collect disseminated resources in an unknown environment. We are interested in approaches in which agents collectively explore the environment and build paths between home and resources. The originality of our approach is to simultaneously build an artificial potential field (APF) around the agents' home while foraging. We propose a multi-agent model defining a distributed and asynchronous version of Barraquand et al. Wavefront algorithm. Agents need only to mark and read integers locally on a grid, that is, their environment. We prove that the construction converges to the optimal APF. This allows the definition of a complete parameter-free foraging algorithm, called c-marking agents. The algorithm is evaluated by simulation, while varying the foraging settings. Then we compare our approach to a pheromone-based algorithm. Finally, we discuss requirements for implementation in robotics.

MASAIE Project-Team

5. New Results

5.1. Highlights of the Year

The estimation of sequestered parasite population has been a challenge for the biologist and modeler, with many authors having studied this problem. The difficulty is that the infected erythrocyte leaves the circulating peripheral blood and binds to the endothelium in the microvasculature of various organs. A measurement of Plasmodium falciparum parasitaemia taken from a blood smear therefore samples young parasites only and there is no clinical methods to measure the sequestered parasites. We have developed a simple tool to estimate the sequestered parasites and hence the total parasite burden for *Plasmodium falciparum* malaria patients. We have also given a method to estimate a crucial parameter in the model of infection. This parameter β can be thought as the “transmission/invading" factor between merozoites and erythrocytes. This work [9] has been published in "Mathematical Biosciences and Engineering".

5.2. Modeling the use of Wolbachia for controlling the incidence of dengue

We continued research on modeling the introduction of *Wolbachia* in a population of *Aedes Aegypti*. This research is done in collaboration with FGV (Fundação Getulio Vargas), Fiocruz (Fondation Oswaldo Cruz) and UFF (Universidade Federal Fluminense) in Rio de Janeiro (Brazil) [16].

Wolbachia is a bacteria which infects arthropod species, including a high proportion of insects (60% of species). Its interactions with its hosts are often complex, and in some cases it is considered as an endosymbiont. The unique biology of *Wolbachia* has attracted a growing number of researchers interested in questions ranging from the evolutionary implications of infection through to the use of this agent for pest and disease control: a public web site has been funded by the National Science Foundation of Australia, and a research in pubmeb (http://www.ncbi.nlm.nih.gov/pubmed) typing `wolbachia` gives 1889 results.

While *Wolbachia* is commonly found in many mosquitoes it is absent from the species that are considered to be of major importance for the transmission of human pathogens. The successful introduction of a life-shortening strain of *Wolbachia* into the dengue vector *Aedes aegypti* that decreases adult mean life has recently been reported.

Moreover it is estimated that the population of mosquitoes harboring *Wolbachia* is less efficient to transmit dengue [18], [21], [22], [25]. Then it is considered that using *Wolbachia* can be a viable option for controlling the incidence of the dengue.

We consider an alternative infection (by Wolbachia) model which exhibits monotonous properties. This model is designed to take into account both the biology of this infection and any available data. The objective is to use this model for predicting the sustainable introduction of this bacteria. We provide a complete mathematical analysis of the model proposed and give the basic reproduction ratio $\mathcal{R}_0$ for *Wolbachia*. We observe a bistability phenomenon. Two equilibria are asymptotically stable: an equilibrium where all the population is uninfected and an equilibrium where all the population is infected. A third unstable equilibrium exists. We provide a lower bound for the basin of attraction of the desired infected equilibrium. We are in a backward bifurcation situation. The bistable situation occurs with natural biological values for the parameters. Our model is an example of an epidemiological model with only vertical transmission.

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

These results have been obtained in collaboration with Pierre-Alexandre Bliman (FGV, Inria); Moacyr Silva (FGV), Claudia Codeço (Fiocruz), Max Souza (UFF) and Jair Koiller (FGV).

5.3. Estimating the proportion of susceptible individuals for a dengue epidemic

Starting from the multi-scaled dengue system, we construct a pair of observers to estimate the dynamics of the disease. The nature of both the observers and the multi-scaled system allows to estimate both the number of susceptible and recovered hosts, as well as to provide information on the vector population, using only infected population data. Numerical simulations have been used to illustrate the performance of the observers.

5.4. Singular value decomposition in dynamic epidemiology: arboviral diseases with human circulation

We introduce a matrix that combines information about human circulation and the epidemiological situation at the nodes of a metapopulational model for an arboviral disease. Its singular value decomposition allows relationships between three basic reproduction numbers $\mathcal{R}_0$: local(s), uniform, and network. The onset of an arboviral disease is strongly dependent on the network characteristics. We present a naive "early warning" criterion for the outbreak at a given node, aiming to promote a discussion on the role of left and right singular vectors. This work is done by the Brazil-France Capes/Cofecub team.

5.5. Analysis of a schistosomiasis infection model

The global mathematical analysis of a schistosomiasis infection model that involves human and intermediate snail hosts as well as an additional mammalian host and a competitor snail species has been done by constructing Lyapunov functions and using properties of K monotone systems. We derived the basic reproduction number $\mathcal{R}_0$ for the deterministic model, and establish that the global dynamics are completely determined by the values of $\mathcal{R}_0$. This mathematical analysis of the model gives insight about the epidemiological consequences of the introduction of a competitor resistant snail species. We gave the characteristics of the competitor resistant snail species that can be used to eliminate the disease [11].

5.6. Multi-stages and multi-strains epidemic models

The model SI (Susceptible-Infected) is one of the most important and used epidemiological models. We gave a complete analysis of the stability of the model with a non-linear incidence and two classes of infected individuals [12].

We have also studied SIS, SIR and MSIR models with bilinear incidence and varying population, with n different pathogen strains of an infectious disease, with or without vertical transmission. For these classes of models, we have proved that under generic conditions a competitive exclusion principle holds. To each strain a basic reproduction ratio can be associated. It corresponds to the case where only this strain exists. The basic reproduction ratio of the complete system is the maximum of the individual basic reproduction ratios. Actually we have also defined an equivalent threshold for each strain. The winner of the competition is the strain with the maximum threshold. It turns out that this strain is the most virulent, i.e., this is the strain for which the endemic equilibrium gives the minimum population for the susceptible host population. This can be interpreted as a pessimization principle [10].

A mathematical multi-patches model for highland malaria in Kenya has been developed and analysed in [13] and [14].

MULTISPEECH Team

6. New Results

6.1. Highlights of the Year

The version 2 of our source separation toolbox FASST [65] has been downloaded more than 300 times since its release in January 2014.

6.2. Explicit modeling of speech production and perception

Participants: Yves Laprie, Slim Ouni, Vincent Colotte, Anne Bonneau, Agnès Piquard-Kipffer, Martine Cadot [Univ. Lorraine], Antoine Liutkus, Emmanuel Vincent, Odile Mella, Benjamin Elie, Camille Fauth, Julie Busset, Andrea Bandini, Guillaume Gris, Simon Meoni.

6.2.1. Articulatory modeling

6.2.1.1. Acquisition of articulatory data

Acquisition of articulatory data plays a central role in the construction of articulatory models and investigation of articulatory gestures. In cooperation with the IADI laboratory (Nancy hospital) we thus conducted a series of preliminary experiments intended to acquire cine-MRI data. Images of the film are reconstructed thanks to the cine-GRICS algorithm developed at IADI [56].

The second research track concerns ultrasound (US) imaging which presents the interest of offering a good temporal resolution without any health hazard and at a reasonable price. However, it cannot be used alone because there is no reference coordinate system and no spatial calibration. We thus used a multimodal acquisition system developed by the Magrit team, which uses electromagnetography sensors to locate the US probe, and the method used to calibrate the US modality. We experimented this system to investigate the most appropriate acquisition protocol for Magnetic Resonance Imaging [37].

We also use an articulograph to acquire articulatory data. Within the framework of the EQUIPEX ORTOLANG, we acquired this year an AG501, a 24-channel articulograph. This system is the most advanced electromagnetography acquisition system. It has been used for two articulatory studies: (1) investigating the effects of posture and noise on speech production [48] and (2) studying the pauses in spontaneous speech from an articulatory point of view. We also conducted an exploratory study on retrieving the 3D shape of the palate from electromagnetography tracings (the work of Simon Meoni, a master student in Cognitive Sciences).

6.2.1.2. Acoustic-to-articulatory inversion

Our previous works about acoustic-to-articulatory inversion relied on the exploration of a vast articulatory codebook covering the whole articulatory space that could be reached by a speaker. This solution presents the main drawback of requiring the construction a codebook for each speaker. We thus developed a multimodal approach to estimate the area function and the length of the vocal tract of oral vowels. The method is based on an iterative technique consisting in deforming an initial area function so that the output acoustic vector matches a specified target. The chosen acoustic vector is the formant frequency pattern. In order to regularize the ill-defined problem, several constraints are added to the algorithm. First, the lip termination area is estimated via a facial capture software. Then, the area function is constrained so that it does not get too far from a neutral position, and so that it does not change too quickly from a temporal frame to the next, when dealing with dynamic inversion. The method proves to be efficient for approximating the area function and the length of the vocal tract for oral French vowels, both in static and dynamic configurations.

6.2.1.3. Articulatory models

The development of articulatory models is a crucial aspect of articulatory synthesis since this determines the success of synthesis. The previous model was developed for X-ray images. This means that the laryngeal part of the model associates the larynx with the piriform sinuses event if these two structures are not in the same sagittal plane. The new model separates the two structures if needed. Additionally, the larynx and the epiglottis are controlled independently which corresponds to the anatomical truth. Previous attempts to modeling epiglottis used principal component analysis applied to the contours drawn on X-ray images. Unfortunately the width of the epiglottis varies from one image to the other and PCA thus learns a spurious “inflating” component. The new model uses the epiglottis centerline plus a constant width which prevents this error.

The second major improvement concerns the use of virtual targets in the construction of the articulatory model. Virtual targets are used to separate the contribution of the tongue contour from those of the palate. The objective it to render the articulation of consonants more correctly since they require a contact between the tongue and the palate at a very precise point [38].

These two improvements of the articulatory model were used in the articulatory copy synthesis experiments [11].

The construction of models was also tackled from a data mining point of view. A robust data mining approach was designed to automatically extract complex statistically significant connections between data (e.g. interactions between more than two variables). This work could be used for data other than X-ray images [54].

6.2.2. Expressive acoustic-visual synthesis

Right now, we are investigating the state-of-the-art of the field of expressive speech and how to acquire efficiently expressive speech corpus. As a first step, we are also investigating visual acquisition techniques to track facial expression. This is the work of the visiting PhD student Andrea Bandini (from University of Bologna). Another step toward expressive speech synthesis is to have an expressive face model. In this context, the expressivity is mainly based on the dynamics. In fact, when the human facial movements are natural and accurately replicated on the 3D model, we can reach a reasonable expressivity. In this context, we are conducting new research toward an expressive talking head. In this context, we acquired a high-resolution 3D model of a human speaker and we are developing methods to animate the model using motion capture data. This was the work the master student Guillaume Gris. We also investigated the advantage of generating visual speech from sequences of 2D Images, when the 3D data is lacking [43].

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

Categorization of sounds and prosody for non-native speech is the object of the ANR+DFG project IFCASL devoted to French and German languages. Within this project, we built a bilingual corpus and started a study about the realization of (final) voicing in both languages. We also gave a training course about non-native phonetic realizations for a Spring School devoted to *Individualized centered approaches to speech processing* [63].

6.2.3.1. Bilingual speech corpus of French and German language learners

We designed a corpus of native and non-native speech for the French-German language pair, with a special emphasis on phonetic and prosodic aspects. To our knowledge there is no suitable corpus, in terms of size and coverage, currently available for this target language pair [9].

We adopted a two step process to create the corpus. Firstly, a bilingual corpus including all sounds of each language and all speech phenomena of potential interest was recorded from a few speakers (14), and analyzed. Its analysis revealed/confirmed: 1) the existence of special strategies due to sentence reading and sentence listening conditions, 2) the importance of recording duration (the recording sessions should not last more than one hour to avoid subjects’ fatigue), 3) the frequence and importance of some mispronunciations (voicing problems, erroneous presence (or absence) of /h/ for German (or French) non-native speakers, rhythm ...). Secondly, we specified and collected the final corpus [24], which is focused on the problems revealed by the preliminary corpus. One hundred speakers (50 French and 50 German speakers), beginners and advanced speakers, recorded 60 sentences in their second language and 30 in their native language, which gave a total amount of about 6000 non-native and 3000 native sentence realizations. The sentences were read in two conditions depending upon whether or not the subjects listen to a reference before producing the sentence. A small text as well as sentences devoted to focus analysis completed the corpus. The data was segmented and labelled at word and phone levels by an automatic alignment algorithm elaborated by our team (cf. 6.4.3.2). The outputs were then manually checked at the levels of phones and words (phonetic transcription) and corrections were made if necessary. In order to check the homogeneity of the corrections made by the seven annotators, phone boundaries were compared with those achieved by a golden annotator on a few sentences using the CoALT tool.

6.2.3.2. Devoicing of final obstruents by German learners

We investigated a typical example of L1-L2 interference: the realization of voiced fricatives in final position, where the opposition between voiced and unvoiced consonants is neutralized in German (with a bias towards unvoiced consonants) but not in French. As a consequence, German speakers learning French as a second language often produce unvoiced fricatives in final position instead of the expected voiced consonants. We analysed the production of French voiced fricatives for 40 non-native (beginners and advanced speakers) and 8 native speakers. We measured the ratio of locally unvoiced frames in the consonantal segment and also the ratio of consonantal duration vs. the duration of the preceding vowel. Results showed that the realizations of French fricatives by German speakers varied with speakers, speakers' level and experimental condition (there were two conditions depending on whether or not the subjects listened to a reference before producing the sentence) [23]. As could be expected we observed a continuum between typically voiced and typically unvoiced realizations, and best level speakers tend to produce more typically French realizations. Our next study will concern the perceptual identification of learners' realizations and the link between perceptual answers and acoustic cues values.

6.3. Complex statistical modeling of speech

Participants: Emmanuel Vincent, Antoine Liutkus, Denis Jouvet, Dominique Fohr, Irina Illina, Joseph Di Martino, Emad Girgis, Arseniy Gorin, Nathan Souviraà-Labastie, Luiza Orosanu, Imran Sheikh, Xabier Jaureguiberry, Baldwin Dumortier.

6.3.1. Acoustic modeling

6.3.1.1. Theory for audio source separation

Our work on audio source separation was marked by the release of version 2 of our toolbox FASST, which was demonstrated at ICASSP 2014 [65], and by the publication of a review paper about guided audio source separation for *IEEE Signal Processing Magazine* [16]. Audio source separation is an inverse problem, which requires the user to guide the separation process using prior models for the source signals and the mixing filters or for the source spectra and their spatial covariance matrices.

On the topic of the mixing parameters, we studied the impact of sparsity penalties over the mixing filters [8] and deterministic subspace constraints [10] over the spatial covariance matrices.

Modelling the spectra of the sources is a fundamental problem in source separation, that aims at catching their main features while requiring few parameters to estimate. We proposed a new framework called Kernel Additive Modelling (KAM). In contrast to Nonnegative Matrix Factorization approaches (NMF), KAM permits to model sources spectro-temporal evolutions only locally. It generalizes many methods from the state-of-the-art, including REPET (voice/music separation) and HPSS (harmonic/percussive separation) and is the first framework to settle them on principled statistical grounds. This year, we have thus been very active not only in diffusing REPET and its variants to a large audience, notably through the publication of a chapter book on the topic [58], but also by establishing many international collaborations on KAM, leading to the publication of one journal paper in IEEE TSP [13] and to two international conference papers [25], [42].

In parallel, we started a new research track on the fusion of multiple source separation techniques. In the specific case when the source spectra are modeled by NMF, the number of components of the NMF is known to have a noticeable influence on separation quality. Many methods have been proposed to select the best order for a given task. To go further, we proposed to use model averaging. As existing techniques do not allow an effective averaging, we introduced a generative model in which the number of components is a random variable and we proposed a modification to conventional variational Bayesian (VB) inference. Initial experiments showed promising results [33], [32].

6.3.1.2. Audio separation based on multiple observations

An interesting scenario for informed audio source separation is when the signals to separate can be observed through deformed references. We proposed a general approach for the separation of multichannel mixtures guided by multiple, deformed reference signals such as repeated excerpts of the same music or repeated versions of the same sentence uttered by different speakers [46], [66].

A related topic is the removal of interferences from live recordings. In this scenario, there are as many microphones as source signals, but each microphone captures not only its dedicated source, but also some interference from the other ones. We proposed a variant of KAM, called KAM for Interference Removal (KAMIR) that permits to address this scenario. The corresponding study has been achieved in collaboration with New York and Erlangen universities.

6.3.1.3. Separation and dereverberation

In order to complement source separation by dereveberation of the source signals, we devoted some work to the estimation of the reverberation time (RT60). In many situations, the room impulse response (RIR) is not available and the RT60 must be blindly estimated from a speech or music signal. Current methods often implicitly assume that reverberation dominates direct sound, which restricts their applicability to relatively small rooms or distant sound sources. We proposed a blind RT60 estimation method that is independent of the room size and the source distance and showed that the estimation error is significantly reduced even in the case when reverberation dominates [21].

6.3.1.4. Corpora for audio separation

Finally, we pursued our long-lasting efforts on the evaluation of audio source separation by providing more details about the DEMAND dataset, that is the first-ever publicly available dataset of multichannel real-world noise recordings [55]. Furthermore, we have continued our efforts on providing corpora for the evaluation of music source separation methods (notably for music/voice separation) and target at significantly extending the SiSEC corpus in 2015 to several hundreds complete recordings, to be used for the first time at SiSEC 2015.

6.3.1.5. Detailed acoustic modeling

Acoustic models aim at representing the acoustic features that are observed for the sounds of the language, as well as for non-speech events (silence, noise, ...). Currently context-dependent hidden Markov models (CD-HMM) constitute the state of the art for speech recognition. However, for text-speech alignment, simpler context-independent models are used as they provide better performance.

In conventional HMM-based approaches that rely on Gaussian mixture densities (GMM), the Gaussian components are estimated independently for each density. Thus, we have focused recent studies on enriching the acoustic models themselves in view of handling trajectory and speaker consistency in decoding. A new modeling approach was developed that takes advantage of the multiple modeling ideas and involves a sharing of parameters. The idea is to use the multiple modeling approach to partition the acoustic space according to classes (manual classes or automatic classification). Then, for each density, Gaussian components are estimated using the data associated to the classes. These class-based Gaussian components are then pooled to provide the set of Gaussian components of the density. Finally class dependent mixture weights are estimated for each density; such approach allows us to better parameterize GMM-HMM without increasing significantly the number of model parameters. Experiments on French radio broadcast news data demonstrated the improvement of the accuracy with such parameterization compared to models with a similar, or even a larger number of parameters. Another approach has been proposed that combines the structuring of the Gaussian components of the densities with respect to some data classes, with the stranded-based approach which introduces probabilities for the transitions between the Gaussian components of the densities when moving from one frame to the next. A detailed analysis of stranded GMM was conducted on data containing different types of non-phonetic variability [29]. The combination of stranded GMM with class-structured densities was evaluated on an English connected digits task using adult and child data [27] and for phonetic decoding on a larger French telephone speech database [26]. This approach was later combined with feature normalization [28].

6.3.1.6. Robust acoustic modeling

In the framework of using speech recognition for helping communication with deaf or hard of hearing people, robustness of the acoustic modeling is investigated. Current studies relate to improving robustness with respect to speech signal level and environment noise through multicondition training and enhanced set of acoustic features.

6.3.1.7. Unsupervised acoustic model training

In previous experiments relating to the combination of speech decoder outputs for improving speech recognition performance [4], it was observed that when a forward-based and a backward-based decoder were providing a same word hypothesis, such common word hypothesis is correct in more than 90% of the cases [71]. Hence, we have investigated how such behavior can help for selecting data for unsupervised training of acoustic models. Best performance is achieved when selecting automatically transcribed data (speech segments) that have the same word hypotheses when processed by the Sphinx forward-based and the Julius backward-based transcription systems, and this selection process outperforms confidence measure based selection. Overall, selecting automatically transcribed speech segments that have the same word hypotheses for the two speech transcription systems, and adding this automatically transcribed and selected data to the manually transcribed data leads to significant word error rate reductions on the ESTER2 data (radio broadcast news) when compared to the baseline system trained only on manually transcribed speech data [34].

6.3.1.8. Score normalization

Existing techniques for robust ASR typically compensate distortion on the features or on the model parameters themselves. By contrast, a number of normalization techniques have been defined in the field of speaker verification that operate on the resulting log-likelihood scores. We provided a theoretical motivation for likelihood normalization due to the so-called “hubness” phenomenon and we evaluated the benefit of several normalization techniques on ASR accuracy for the 2nd CHiME Challenge task. We showed that symmetric normalization (S-norm) reduces the relative error rate by 43% alone and by 10% after feature and model compensation [53].

6.3.2. Linguistic modeling

6.3.2.1. Out-of-vocabulary proper name retrieval

Recognition of proper names is a challenging task in information retrieval in large audio/video databases. Proper names are semantically rich and are usually key to understanding the information contained in a document. Within the ContNomina project (cf. 8.1.4), we focus on increasing the vocabulary coverage of a speech transcription system by automatically retrieving proper names from contemporary text documents. We proposed methods that dynamically augment the automatic speech recognition system vocabulary, using lexical and temporal features in diachronic documents (documents that evolve over the time). Our work uses temporal context modeling to capture the lexical information surrounding proper names so as to retrieve out-of-vocabulary proper names and increase the ASR vocabulary size. We focus on exploiting the lexical context based on temporal information from diachronic documents. Our assumption is that time is an important feature for capturing name-to-context dependencies. We also studied different metrics for proper name selection in order to limit the vocabulary augmentation: a method based on Mutual Information and a new method based on cosine-similarity measure. Recognition results show a significant reduction of the proper name error rate using augmented vocabulary [30][31].

6.3.2.2. Hybrid language modeling

In the framework of using speech recognition for helping communication with deaf or hard of hearing people, the handling of out-of-vocabulary words is a critical aspect. Indeed, the size of the vocabulary is always limited (even if large or very large), and the system is not able to recognize words out of its lexicon. Such words would then be transcribed as sequences of short words which involve similar sounds as the unknown word. However the interpretation of such sequences of small word require a lot of efforts. Hence the idea of combining in a single model a set of words (the most frequent and/or most relevant for the application context) and a set of syllables. With such an approach,unknown words are usually recognized as sequences of syllables which are easier to interpret. By setting different thresholds on the confidence measures associated to the recognized words (or syllables), the most reliable word hypotheses can be identified, and they have correct recognition rates between 70% and 92% [44][45].

6.3.2.3. 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 pursued our pioneering work on music language modeling, with a particular focus on the modeling of long-term structure [20]. We also proposed a new Bayesian n-gram topic modeling and estimation technique, which we applied to genre-dependent modeling of chord sequences and to music genre classification [15].

6.3.3. Speech generation by statistical methods

6.3.3.1. Enhancing pathological voice by voice conversion techniques

Enhancing the pathological voice in order to make it more intelligible would allow persons having this kind of voice to communicate more easily with those around them. In our group we chose to improve the pathological voice by means of voice conversion techniques. Since we began this study, we have succeeded to predict the complete magnitude spectrum. In doing so, we free ourselves from the prediction of the fundamental frequency of speech (F0). Such an interesting result allows us to obtain converted speech of good audio quality. Now in order to obtain perfect conversion, we are trying, with Emad Girgis, a postdoctoral student who began his work in November 2014, to predict the phase spectrum. To achieve this goal, Emad intends to use Deep Neural Networks (DNN). We expect first results in the beginning of 2015.

6.3.3.2. Enhancing pathological voice by voice recognition techniques

Another possibility for enhancing the pathological voice is to recognize it. Othman Lachhab, a PhD student, is working on the recognition of the esophageal voice: using high order temporal derivatives combined with an Heteroscedastic Linear Discriminant Analysis (HLDA) he reached an interesting phone recognition rate of 63.59% [36]. Currently Othman, is trying to improve his results by using voice conversion techniques. Using these techniques pathological features are projected in a clean-natural speech feature space, and preliminary results exhibit an increase of 1.70% of the phone recognition rate.

6.3.3.3. F0 detection using wavelet transforms

Another possible interesting track for improving voice conversion techniques is to predict the fundamental frequency of speech. For doing so, it is necessary to have a good F0 detector. As part of her thesis, Fadoua Bahja developed many F0 detection algorithms [69] [1]. The latest, using wavelet transform for denoising the cepstrum signal, has been submitted for publication in an international journal.

6.4. Uncertainty estimation and exploitation in speech processing

Participants: Emmanuel Vincent, Dominique Fohr, Odile Mella, Denis Jouvet, Agnès Piquard-Kipffer, Dung Tran.

6.4.1. Uncertainty and acoustic modeling

In many real-world conditions, the speech signal is overlapped with noise, including environmental sounds, music, or undesired extra speech. Speech enhancement is useful but insufficient: some distortion remains in the enhanced signal which must be quantified in order not to be propagated to the subsequent feature extraction and decoding stages. The framework of uncertainty decoding assumes that this distortion has a Gaussian distribution and seeks to estimate its covariance matrix [5]. A number of uncertainty estimators and propagators have been proposed for this purpose, which typically operate on diagonal covariance matrices and are based on fixed mathematical approximations or heuristics. We obtained more accurate uncertainty estimates by propagating the full uncertainty covariance matrix and by fusing multiple uncertainty estimators [50], [51]. Overall, we obtained 18% relative error rate reduction with respect to conventional decoding (without uncertainty), that is about twice as much as the reduction achieved by the best single uncertainty estimator and propagator.

In order to motivate further work by the community, we created a new international evaluation campaign on that topic in 2011: the CHiME Speech Separation and Recognition Challenge [2]. After two successful editions in 2011 and 2013, we started working and collecting a new corpus towards the organization of a third edition to be announced in 2015.

6.4.2. Uncertainty and speech recognition

In the framework of using speech recognition for helping communication with deaf or hard of hearing people in the FUI project Rapsodie (cf. 8.1.5), our goal is to find the best way for displaying the speech transcription results. To our knowledge there is no suitable, validated and currently available display of the output of automatic speech recognizer for hard-of-hearing persons, in terms of size, colors and choice of the written symbols. The difficulty comes from the fact that speech transcription results contain recognition errors, which may impact the understanding process. Although the speech recognition system does not know the errors it makes, through the computation of confidence measures, the speech recognizer estimates if a word or a syllable is rather correctly recognized or not (cf. 6.3.2.2); hence such information can be used to adjust the display of the transcription results.

We have adopted a two-step process. Firstly, we conducted a feasibility study with three hard-of-hearing persons including written display tests on print media and interviews. Secondly, we set up an experimental protocol with five hard-of-hearing persons. It included comprehension tests of 40 written sentences recorded by a French native speaker video projected onto a screen. We have also conducted parallel interviews. Their analysis revealed: (1) the interest of the participants in the project; (2) their difficulties to read International Phonetic Alphabet; (3) the importance of knowing the context of communication; (4) the need for aid in case of errors of the speech recognition system by emphasing the words that are supposed to be well recognized by the system. At this stage of the experimental period, the best display associates writing in a bold spelling the words that are supposed to be correctly recognized, and writing in a normal font using simplified French phonetics the words that are possibly wrongly recognized (according to their confidence measure). The next step will be to set up another experimental protocol in order to compare the current display in three conditions (written sentences vs written sentences with oral and lip reading vs lip reading only).

6.4.3. Uncertainty and phonetic segmentation

As described below, phonetic segmentation has been studied this year for spontaneous speech and non-native speech. Moreover, some portions (of about 30 secondes) of various speech documents have been manually annotated (checking and correction of an automatic segmentation). In the future this manually annotated data will be used to analyze the accuracy of the automatic segmentation, and also to elaborate measures that estimate the quality of the segmentation.

6.4.3.1. Alignment with spontaneous speech

Within the ANR ORFEO project (cf. 8.1.2), we addressed the problem of the alignment of spontaneous speech. The ORFEO audio files were recorded under various conditions with a large SNR range and contain extra speech phenomena and overlapping speech. We trained several sets of acoustic models and tested different methods to adapt them to the various audio files. For selecting the best acoustic models, we compared the alignment outputs obtained with the different acoustic models by using our tool CoALT and the manually annotated portions described above.

We also designed a new automatic grapheme-phoneme tool to generate the potential pronunciations of words and proper names. For what concerns overlapping speech, among the different orthographic transcripts corresponding to the overlapping area, we determined as the main transcript the one that best matches the audio signal, the others are kept in other tiers (in a Praat TextGrid file) with the same time boundaries.

6.4.3.2. Alignment with non-native speech

Non-native speech alignment with text is one critical step in computer assisted foreign language learning [3]. The alignment is necessary to analyze the learner's utterance, in view of providing some prosody feedback (as for example bad duration of some syllables). However, non-native speech alignment with text is much more complicated than native speech alignment. This is due to the pronunciation deviations observed on non-native speech, as for example the replacement of some target language phonemes by phonemes of the mother tongue, as well as errors in the pronunciations. Non-native speech alignment with text is currently studied in the ANR IFCASL project (see 8.1.3).

6.4.4. Uncertainty and prosody

A statistical analysis was conducted on a large annotated speech corpus to investigate the links between punctuation and automatically detected prosodic structures. The speech data comes froms radio broadcast news and TV shows, that were manually annotated during French speech transcription evaluation campaigns. These corpora contain more than 3 million words and almost 350,000 punctuation marks. The detection of the prosodic boundaries and of the prosodic structures is based on an automatic approach that integrates little linguistic knowledge and mainly uses the amplitude and the direction of the F0 slopes, as well as phone durations. A first analysis of the occurrences of the punctuation marks, with respect to various sub-corpora, has highlighted the variability among annotators. Then, a detailed analysis of the prosodic parameters with respect to the punctuation marks, whether followed or not by a pause, and of the links between the automatically detected prosodic structures and the manually annotated punctuation marks was conducted [18].

NEUROSYS Team

6. New Results

6.1. Highlights of the Year

Microscopic action affects mesoscopic and macroscopic action in neural systems. In the context of general anaesthesia, it is not understood how single neuron properties, such as ion-channel conductivities or anesthetic action on neuron receptors, translate to population dynamics and consequently to behavior. The work of Laure Buhry and Axel Hutt [4] proposes a modelling approach how to bridge the microscopic and the mesoscopic scale. The most interesting aspect is that this model bridge allows to extend standard neural field theory on the mesoscopic scale instead of introducing a new model.

In addition, we have developed strong collaborations with medical doctors. First, we have established a collaboration with Dr. Denis Schmartz and Dr. Claude Meistelmann at the *CHU Nancy* to plan and perform well-controlled resting state experiments under propofol anaesthesia. Second, we are in close contact to Jean-Luc Schaff at the *CHU Nancy* (together with Laurent Koessler at *CRAN*) in the context of sleep monitoring. Dr. Schaff has provided us polysomnographic data measured during sleep of insomnia patients.

6.2. From the microscopic to the mesoscopic scale

Participants: Laure Buhry, Axel Hutt, Francesco Giovannini, LieJune Shiau

The Highlight of the Year bridges the microscopic scale and the mesoscopic scale. One partial result has already been used in one of our publications [3] to study the link between population dynamics on the mesoscopic scale and the EEG on the macroscopic scale.

In addition, the work of Francesco Giovannini aims at gaining a better understanding of the effects of anaesthesia on the neural correlates of memory, focusing on how anaesthetics disrupt the interaction between the hippocampus and the cerebral cortex. Studies have shown that these two brain structures exhibit a strong synchronisation of their respective neural activity, when performing memory tasks. Neurophysiology experiments have identified various possible candidate generators for rhythmic activity in the area CA1, CA3 and Dentate Gyrus areas of the hippocampus. However the mechanisms by which cortico- hippocampal synchronisation is elicited, and maintained, are yet to be fully understood. As a first step towards this objective, Francesco obtained a working mathematical model of a biologically plausible hippocampal CA1-3 neural cell, based on the Hodgkin-Huxley neuron, capable of exhibiting long-lasting persistent firing activity when subject to a strong transient stimulus. This behaviour is underlay by an intrinsic membrane current activated by the increase of intracellular Calcium ions, following the discharge of an action potential by the neuron. Our hypothesis is that large ensembles of such persistent-firing neurons could sustain the memory-related rhythmic activity displayed by the hippocampus. In this context, Laure Buhry and Axel Hutt work with LieJune Shiau (University of Houston) on a better understanding of the models used by the community of computational neuroscientists. The goal is to show in which extent models are comparable or interchangeable. We focus on the comparison of oscillatory mechanisms of neuronal populations in different spiking models, especially in the Hodgkin-Huxley and the adaptive exponential integrate-and-fire model.

These latter studies link the two description scales by a bottom-up approach.

Conversely, Axel Hutt and collaboration partners from the University of Noth Carolina - Chapel Hill have analysed Local Field Potentials measured in ferrets prefrontal cortex and visual cortex under anesthesia in a top-down analysis [21]. This data allows to extract network interactions in prefrontal cortex and visual cortex and hence revealing underlying mechanisms in general anaesthesia.

6.3. From the mesoscopic to the macroscopic scale

Participants: Laurent Bougrain, Axel Hutt, Pedro Garcia-Rodriguez, Eric Nichols, Guillaume Serrière, Tamara Tosic, Nicole Voges, Mariia Fedotenkova, Meysam Hashemi, Cecilia Lindig-Leon, Kevin Green, Sébastian Rimbert, Thomas Tassone.
To understand the action of anaesthetic drugs on the EEG-signal observed experimentally, Meysam Hashemi has developed and studied several neural mass models [18], [15], [16], [3]. He has identified the thalamo-cortical loop (TCL) as a possible origin of $\delta-$activity. Since loss of consciousness is accompanied by emerging $\delta-$activity, this work relates the TCL to the loss of consciousness.

Increasing the anaesthetic concentration beyond the point of loss of consciousness, EEG-signals exhibit alternating patterns of high and low activity. This activity is called burst suppression. Since these alternations resemble stochastic jumps between low and high activity resting states, Pedro Garcia-Rodriguez and colleagues are working on a stochastic theory based on neural mass models to describe and reproduce these experimental results. Since the minimum mathematical model for such an effect is two-dimensional and does not exhibit potential dynamics, whereas the majority of literature up to date considers one-dimensional stochastic models obeying potential dynamics, Pedro and colleagues had to develop a new stochastic theory. They can show that the two-dimensional dynamics of the neural mass model can be mapped to a one-dimensional stochastic potential model [14], [13]. This reduction allows to apply standard stochastic theory to describe burst suppression as stochastic transistions. This finding indicates the presence of multiple resting states in the brain and supports a heavily discussed hypothesis on the loss of consciousness.

Biological neural networks are subject to random fluctuations, originating from intrinsic random fluctuations of ions or from external stimulus. The latter neural mass models take into account these fluctuations by assuming additive random input fluctuations. For many decades, these additive fluctuations have been assumed to not affect the stability of the system. However, previous own work has revealed that additive fluctuations tune the stability of nonlinear high-dimensional systems. Since random fluctuations play an important role in the description of neural population dynamics and realistic models consider , it is necessary to study in detail how random fluctuations affect the stability of neural mass models and, hence, how our mathematical model analyses have to be modified. To this end, Axel Hutt and colleagues have performed a stochastic center manifold analysis in a delayed stochastic neural mass model [5] and have found conditions for the stability shift. A first application to delayed stochastic neural fields has revealed how additive random fluctuations may affect EEG-signals [19], [6], however additional detailed mathematical studies and the comparison to experimental data are necessary to affirm the importance of the stochastic effect. Essentially, this work emphasizes to take into account nonlinear noise effects in neural mass and neural field models.

Neural mass models do not consider the spatial extension of neural populations and consequently neglect transmission or interaction delay between neurons at different spatial locations. Taking into account the spatial extension and axonal transmission delay, Axel Hutt and colleagues have shown mathematically [7] how travelling activity fronts propagate through neural tissue and how the fronts properties, such as speed, depend on the neural field properties.

The latter neural field model is embedded in a one-dimensional space. Since biological neural populations in the neocortex are organized in two-dimensional layers or sheets, it is necessary to employ neural field models in two spatial dimensions. This causes both theoretically and numerically problems in the presence of axonal transmission delay. Eric Nichols and colleagues has implemented a recent numerical integration algorithm [8] in the visualization software NeuralFieldSimulator, cf. section5.1 . This software is the basis of numerical bifurcation studies of two-dimensional neural field models [12], [20]. First analytical results [10] show good accordance to numerical results obtained by the NeuralFieldSimulator.

The latter neural field models assume homogeneous spatial interactions, i.e., neural interactions whose strength just depends on the distance between the two neurons. This assumption is strong and not biologically realistic in certain brain areas. In addition, this assumption constrains the model description of recurrent sequences of EEG patterns, which have been found experimentally, e.g., during the emergence from general anaesthesia. Consequently to be able to describe such recurrent EEG-pattern sequences, it is necessary to improve the mathematical description of EEG-patterns. A promising new model has been derived by Axel Hutt and collagues based on heterogeneous neural fields [1]. In order to extract the recurrence EEG-patterns from data, we have extended a recent recurrence analysis technique [2]. The next step will consist in the combination of the heterogeneous neural field model and the results from the recurrence analysis.

Recurrence analysis extracts temporally reccurrent time windows in multi-dimensional datasets. Typical EEG-signals obtained durin surgery under anaesthesia include one electrode and hence a single time series only. To extract recurrence structures of such one-dimensional signals, Mariia Fedotenkova computes the multi-dimensional time-frequency representation of the signal and has worked out the best analysis technique for this step [9]. In the next step she will compute the recurrence plot for a large dataset of 110 patients under surgery (data obtained from University of Auckland).

In order to understand immobility during anaesthesia and how to supervise unconscious patients automatically in hospital emergency rooms, Cecilia Lindig-Leon studies motor imagery and its detection by BCI techniques. Limb movement execution or imagination induce sensorimotor rhythms that can be detected in EEG recordings. Her recent work considers signal power changes in two frequency bands to detect the elicited EEG rebound, i.e. the increasing of synchronization, at the end of motor imageries. The analysis is based on the database 2a of the BCI competition IV and shows that rebound can be stronger over the alpha frequency band (8-12Hz) than the beta frequency band (12-20Hz). She can demonstrate that the analysis of the alpha frequency band improves the detection of the end of motor imageries. In this context, Cecilia has compared intrinsic multi-class classifiers (i.e., one-step methods) with ensembles of two-class classifiers on dataset 2a of the BCI competition IV for motor imagery. Subsequently, she has compared the classical Common Spatial Pattern (CSP) approach and the CSP by Joint Approximate Diagonalization in order to identify whether the latter method represents an outperforming alternative.

Sleep is strongly related to anaesthesia and we have started working on the improvement of sleep monitors. The basic idea is to consider not only EEG-signals but multiple different physiological signals (e.g. heart pulses, electrocardiogram, EEG, respiration cycle, body movements) to classify sleep stages. By virtue of the different signal natures of different physiological signals, it is challenging to put together these so-called multi-modal signals in a single analysis method. To this end, Tamara Tosic and colleagues employ recurrence analysis techniques which allow to estimate time windows exhibiting temporal synchronization between physiological signals [11]. They have developed a method that is based on artificial data sets and Local Field Potentials measured under anaesthesia. In the next step, applications to sleep data (obtained from CHU Nancy) will allow to extract sleep stages and will evaluate the method.

ORPAILLEUR Project-Team

6. New Results

6.1. Highlights of the Year

As highlights of the year, we would like to mention several elements, an award in a competition and a best paper. In addition we would like to also mention the importance gained by two other papers.

- Yen Low, a postdoctoral fellow from Stanford and Adrien Coulet (Orpailleur team) jointly developed a prototype named *Whypothesis?* whose goal is to provide explanations on drug side effects for which the molecular mechanism remains unknown. This prototype won the "Best Application Award" at the 2014 NCBO Hackathon (National Center for Biomedical Ontology), held at Stanford University, April 26-27 (http://www.bioontology.org/2014_NCBO_Hackathon).
- The paper [2] describing a first and original proposition for combining pattern structures and relational concept analysis won the best paper award at the International Conference on Formal Concept Analysis in Cluj-Napoca, Romania.
- The paper [10] published in Nucleic Acids Research describes the latest version of KBDOCK, which has had over 12,000 non-duplicate visitors since 2011.
- The paper [44] on polypharmacology represents a nice collaboration with Harmonic Pharma, and it was used for the cover issue of Journal Chemical Information (http://pubs.acs.org/toc/jcisd8/54/3).

BEST PAPER AWARD :

[56] **Formal Concept Analysis - 12th International Conference - Proceedings**. V. CODOCEDO, A. NAPOLI.

6.2. The Mining of Complex Data

Participants: Mehwish Alam, Aleksey Buzmakov, Melisachew Chekol, Victor Codocedo, Adrien Coulet, Elias Egho, Nicolas Jay, Florence Le Ber, Ioanna Lykourentzou, Luis-Felipe Melo, Amedeo Napoli, Chedy Raïssi, Mohsen Sayed, My Thao Tang, Yannick Toussaint.

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

Formal Concept Analysis and pattern mining are suitable symbolic methods for KDDK, that may be used for real-sized applications. Global improvements are carried on the scope of applicability, the ease of use, the efficiency of the methods, and on the ability to fit evolving situations. Accordingly, the team is extending these symbolic data mining methods for working on 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.

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

There are a few extensions of FCA for handling contexts involving complex data formats, e.g. graphs or relational data. Among them, Relational Concept Analysis (RCA) is a process for analyzing objects described both by binary and relational attributes [2] [131]. The RCA process takes as input a collection of contexts and of inter-context relations, and yields a set of lattices, one per context, whose concepts are linked by relations. RCA can play has an important role in KDDK, especially in text mining [105].

Another extension of FCA is based on Pattern Structures (PS) [112], which allows to build a concept lattice from complex data, e.g. nominal, numerical, and interval data [119]. Since then, we worked on some experiments involving pattern structures, namely sequence mining [107], information retrieval and recommendation [58], [22], functional dependencies [50], [17] and biclustering [69], [41]. One of the next step is the adaptation of pattern structures to graph mining.

Moreover, the notion of similarity between objects is also closely related to pattern structures [102]: two objects are similar as soon as they share the same attributes (binary case) or attributes with similar values or the same description (at least in part). Combination of similarity and pattern structures is also under study, in particular for solving information retrieval and annotation problems.

In pattern mining as in FCA, one main problem is the volume of the output. One general idea is to extract patterns which show a "good behavior" w.r.t. a given measure. Such patterns or concepts are expected to have good characteristics and to provide effective knowledge. We have conducted in the framework of FCA a series of experiments on the so-called "stability measure", showing that this measure is able to detect significant patterns [54], [53].

Finally, there is also an on-going work relating FCA and semantic web. This work focuses on the classification within a concept lattice of the answers returned by SPARQL queries. The concept lattice is then used as an index for navigating and ranking the answers w.r.t. their content and interest for a given objective [47].

6.2.2. Sequence Mining

Sequence data is widely used in many applications. Consequently, mining sequential patterns and other types of knowledge from sequence data became an important data mining task. In the team, the main emphasis is on developing efficient mining algorithms for pattern classification problems. The most frequent sequences generally provide trivial information. When analyzing the set of frequent sequences with a low minimum support, the user is overwhelmed by millions of patterns.

In our recent work, we studied the notion of δ-freeness for sequences. While this notion has extensively been discussed for itemsets, our work is the first to extend it to sequences. We defined an efficient algorithm devoted to the extraction of δ-free sequential patterns. We presented the advantage of the δ-free sequences and highlighted their importance when building sequence classifiers, and we showed how they can be used to address the feature selection problem in statistical classifiers which optimizes both accuracy and earliness of predictions [68].

6.2.3. Mining and Understanding Healthcare Trajectories

With the increasing burden of chronic illnesses, administrative health care databases hold valuable information that could be used to monitor and assess the processes shaping the trajectory of care of chronic patients. In this context, temporal data mining methods are promising tools, though lacking flexibility in addressing the complex nature of medical events. In the thesis work of Elias Egho [15], new algorithms were designed to extract patient trajectory patterns with different levels of granularity by relying on external taxonomies [62], [34]. The algorithms rely on the general FCA framework to formalize the general notion of multidimensional healthcare trajectories. There was also another work focusing on the similarity measure among sequences. An efficient and original similarity measure was design for that purpose [8].

6.2.4. Video Game Analytics

The video game industry has grown enormously over the last twenty years, bringing new challenges to the artificial intelligence and data analysis communities. We tackled this year the problem of automatic discovery of strategies in real-time strategy games through pattern mining. Such patterns are the basic units for many tasks such as automated agent design, but also to build tools for the professionally played video games in the electronic sports scene. We presented a new formalism within a sequential pattern mining approach and a novel measure, the balance measure, telling how a strategy is likely to win [51]. We experimented our methodology on a real-time strategy game that is professionally played in the electronic sport community and laid plans on a future collaboration with the MIT Game Lab.

6.2.5. KDDK in Text Mining

Ontologies help software and human agents to communicate by providing shared and common domain knowledge, and by supporting various tasks, e.g. problem-solving and information retrieval. In practice, building an ontology depends on a number of "ontological resources" having different types: thesaurus, dictionaries, texts, databases, and ontologies themselves. We are currently working on the design of a methodology based on FCA and RCA for ontology engineering from heterogeneous ontological resources. This methodology is based on both FCA and RCA, and was previously successfully applied in domains such as astronomy and biology.

In the framework of the ANR Hybride project (see 8.2.1.2), an engineer is implementing a robust system based on these previous research results, for preparing the way to new research directions involving trees and graphs. Moreover, we led a first successful experiment on extracting drug-drug interactions applying "lazy pattern structure classification" to syntactic trees. In addition, in his thesis work, Mohsen Sayed focused on extracting relations between named entities using graph mining methods applied to dependency graphs [67]. We are currently investigating how this approach can be generalized, i.e. how to detect a relation between complex expressions which are not previously recognized as named entities.

The notion of "Jumping Emerging Patterns" (JEP) previously used in chemistry [101], was updated and adapted in the context of text mining within the ANR Termith project. The objective is to design a learning method for filtering candidate terms within a full text and to decide whether an occurrence should be tagged as a term, i.e. a positive example, or as a simple word, i.e. a negative example. The method extracts from a training set all JEPs which are considered as hypotheses. To reduce the number of JEPs and to retain only the more significant JEPs from a linguistic point of view, JEPs are weighted and a constraint solver is used to verify the maximal coverage of the positive examples. Results are currently under evaluation.

6.3. KDDK in Life Sciences

Participants: Adrien Coulet, Marie-Dominique Devignes, Bernard Maigret, Gabin Personeni, David Ritchie, Malika Smaïl-Tabbone.

The Life Sciences constitute a challenging domain for KDDK. Biological data are complex from many points of views, e.g. voluminous, high-dimensional and deeply inter-connected. Analyzing such data is a crucial issue in health care, environment and agronomy. Besides, many bio-ontologies are available and can be used to enhance the knowledge discovery process. Accordingly, the research work of the Orpailleur team in KDDK applied to Life Sciences is in concern with the use of bio-ontologies to improve KDDK, and as well information retrieval, access to "Linked Open Data" (LOD) and data integration.

6.3.1. Inductive Logic Programming for Mining Linked Open Data

Increasing amounts of biomedical data provided as LOD offer novel opportunities for knowledge discovery in biomedicine. We proposed and published an approach for selecting, integrating, and mining LOD with the goal of discovering genes responsible for a disease [11]. The selection step relies on a set of choices made by a domain expert to isolate relevant pieces of LOD. Because these pieces are potentially not linked, an integration step is required to connect unlinked pieces. The resulting graph is subsequently mined using Inductive Logic Programming (ILP) that presents two main advantages. First, the input format compliant with ILP (first order logic) is close to the format of LOD (RDF triples). Second, domain knowledge can be added to this input and used during the induction step. We have applied this approach to the characterization of genes responsible for intellectual disability. For this real-world use case, we could evaluate ILP results and assess the contribution of domain knowledge. Our ongoing efforts explore how the combination of rules coming from distinct theories can improve the prediction accuracy [70] [16].

6.3.2. Analysis of biomedical data annotated with ontologies

Annotating data with concepts of an ontology is a common practice in the biomedical domain. Resulting annotations define links between data and ontologies that are key for data exchange, data integration and data analysis. Since 2011, we collaborate with the National Center for Biomedical Ontologies (NCBO) to develop a large repository of annotations named the NCBO Resource Index [118]. This repository contains annotations of 36 biomedical databases annotated with concepts of more than 200 ontologies of the BioPortal (http://bioportal.bioontology.org/). In the preceding years, we compared the annotations of a database of biomedical publications (Medline) with two databases of scientific funding (Crisp and ResearchCrossroads) to profile disease research [122]. One main challenge remains to develop a knowledge discovery approach able to mine correlations between annotations based on BioPortal ontologies, i.e. is it possible to discover interesting knowledge units within these annotations?

Then, we proposed an adaptation of FCA techniques, namely pattern structures, to explore the annotations of biomedical databases [108]. We considered documents of biomedical databases annotated with sets of ontological concepts as objects in a pattern structure. Corresponding annotations have been classified according to several dimensions, where a dimension is related to a particular aspect of domain knowledge. The pattern structure formalism was applied to classify these annotations, allowing to discover correlations between annotations but also lacks of completion in the annotations that could be fixed afterward. This adaptation of pattern structures opens many perspectives in term of ontology reengineering and knowledge discovery.

6.4. Structural Systems Biology

Participants: Marie-Dominique Devignes, Bernard Maigret, David Ritchie, Malika Smaïl-Tabbone.

Keywords: bioinformatics, chemistry, docking, knowledge discovery, screening, systems biology

Structural systems biology aims to describe and analyze the many components and interactions within living cells in terms of their three-dimensional (3D) molecular structures. We are currently developing advanced computing techniques for molecular shape representation, protein-protein docking, protein-ligand docking, high-throughput virtual drug screening, and knowledge discovery in databases dedicated to protein-protein interactions.

6.4.1. The Hex Protein Docking Program

Our *Hex* protein docking software is being more widely used than ever before. The unique polar Fourier correlation approach used in *Hex* [129] allows the expensive FFT part of its calculations to be greatly accelerated on modern graphics processors (GPUs) [130]. *Hex* is freely available for download for academic users at http://hex.loria.fr. A public GPU-powered server has also been created (http://hexserver.loria.fr) [123]. In the last four years, the server has performed some 63,700 docking runs, and the program has had some 37,000 downloads. The latest version of the program has been used successfully to dock symmetric dimers (unpublished results) in the international “CAPRI” docking experiment [115]. A manuscript on performing polar Fourier docking using symmetry constraints is in preparation with the Nano-D team at Inria Grenoble.

6.4.2. KBDOCK: Protein Docking Using Knowledge-Based Approaches

In order to explore the possibilities of using structural knowledge of protein-protein interactions, Anisah Ghoorah recently developed the KBDOCK system as part of her doctoral thesis project [116]. KBDOCK is available at http://kbdock.loria.fr. KBDOCK combines coordinate data from the Protein Data Bank [106] with the Pfam protein domain family classification [111] in order to describe and analyze all known protein-protein interactions for which the 3D structures are available. We have demonstrated the utility of KBDOCK [114] for template-based docking using 73 complexes from the Protein Docking Benchmark [117]. We recently presented results obtained using KBDOCK at the CAPRI conference on protein docking in Utrecht [115]. In late 2013, we updated KBDOCK with the latest data from Pfam and the Protein Data Bank. In 2014, an article describing the new version of KBDOCK was published in the special Database Issue of Nucleic Acids Research [10]. Since the KBDOCK web site (http://kbdock.loria.fr) was created in 2011, it has had over 12,000 distinct visitors.

6.4.3. Kpax: A New Algorithm for Multiple Flexible Protein Structure Alignments

We recently developed a new protein structure alignment approach called Kpax [128]. The approach exploits the fact that each amino acid residue has a carbon atom with a highly predictable tetrahedral geometry. This allows the local environment of each residue to be transformed into a canonical orientation, thus allowing easy comparison between the canonical orientations of residues within pairs of proteins using a novel scoring function based on Gaussian overlaps. The overall approach is two or three orders of magnitude faster than most contemporary protein structure alignment algorithms, while still being almost as accurate as the state-of-the-art TM-Align approach [134]. Kpax is now used heavily by the KBDOCK web server [10] to find structural templates for docking which might be beyond the reach of sequence-based homology modeling approaches. The Kpax program is also available for download at http://kpax.loria.fr/.

In 2014, the Kpax algorithm has been extended to allow flexible alignment and superposition of protein backbones and to perform multiple structure alignments, in analogy with multiple protein sequence alignments. Our early results show that incorporating backbone flexibility leads to much higher quality multiple alignments than can be achieved with existing algorithms.

6.4.4. Polypharmacology: Developing New Uses for Old Drugs

In 2010, Violeta Pérez-Nueno joined the Orpailleur team thanks to a Marie Curie Intra-European Fellowship (IEF) award to develop new virtual screening algorithms (DOVSA). The aim of this project was to advance the state of the art in computational virtual drug screening by developing a novel consensus shape clustering approach based on spherical harmonic (SH) shape representations [126].

In 2012, Violeta joined Harmonic Pharma, a LORIA spin-out company for drug re-purposing, and we have since continued our collaborations to develop new algorithms for drug discovery and drug re-purposing. The observation that many existing drugs may be used to treat more than one disease is often referred to as “polypharmacology.” Our latest work on predicting polypharmacology uses a Gaussian clustering approach to identify groups molecules with similar three-dimensional shapes. This work was published in the Journal of Chemical Information and Modeling [44]. An illustration from this article was used to provide the cover page for the March 2014 issue of the journal (http://pubs.acs.org/toc/jcisd8/54/3).

6.5. Around the Taaable research project

Participants: Valmi Dufour-Lussier, Emmanuelle Gaillard, Florence Le Ber, Jean Lieber, Amedeo Napoli, Emmanuel Nauer.

Keywords: knowledge representation, description logics, classification-based reasoning, case-based reasoning, belief revision, semantic web

The Taaable project was originally created as a challenger of the Computer Cooking Contest (ICCBR Conference) [4] (http://taaable.fr). A candidate to this contest is a system whose goal is to solve cooking problems.

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, minimal 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.

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 compute ingredient substitutions and to adjust the ingredient quantities [65] using engines included in the Revisor library (see § 5.4.5).

As acquiring knowledge from experts is costly, a new approach was proposed to allow a CBR system to use partially reliable, non expert, knowledge from the Web for reasoning. This approach is based on a meta-knowledge model to manage knowledge reliability. This model represents notions such as belief, trust, reputation and quality, as well as their relationships and rules to evaluate knowledge reliability. The reliability estimation is used to filter knowledge with high reliability as well as to rank the results produced by the CBR system. Performing CBR with knowledge resulting from an e-community is improved by taking into account the knowledge reliability [64].

Taaable won in 2014 the CCC originality challenge for all the open resources that the Taaable team developed during the last years for the CBR community: WikiTaaable, a semantic wiki containing cooking domain knowledge, Tuuurbine, a generic ontology guided CBR engine over RDFS (see § 5.4.3), and Revisor, an adaptation engine implementing various revision operators (see § 5.4.5).

6.6. Some Results in Graph Theory

Participants: Miguel Couceiro, Amedeo Napoli, Chedy Raïssi, Jean-Sébastien Sereni, Mario Valencia.

Keywords: graph theory, extremal graph theory, coloring, clustering

6.6.1. Structural and extremal graph theory

Regarding graph coloring, a conjecture of Gera, Okamoto, Rasmussen and Zhang on set coloring was solved. A *set coloring* of a graph $G=(V,E)$ is a function $c:V\to\{1,...,k\}$ such that whenever u and v are adjacent vertexes, it holds that $\{c(x)\ :\ x \text{ neighbor of } u\}\neq\{c(x)\ :\ x \text{ neighbor of } v\}$. In other words, there must be at least one neighbor of u that has a color not assigned to a neighbor of v, or *vice-versa*. The smallest k such that G admits a set coloring is the *set coloring number* $\chi_s(G)$. We confirmed the conjecture by proving that $\chi_s(G)\geq\lceil\log_2\chi(G)\rceil+1$, where $\chi(G)$ is the (usual) chromatic number of G. This bound is tight.

Works have been started on a 12-year-old conjecture by Heckman and Thomas about the fractional chromatic number of graphs with no triangles and maximum degree at most 3. This conjecture is actually a natural generalization of a fact established by Staton in 1979. Heckman and Thomas posits that in every graph with no triangles, maximum degree at most 3 and arbitrary weights on the vertexes, there exists an independent set of weight at least $5/14$ times the total weight of the graph.

Regarding extremal graph theory, two results have been obtained. The first one deals with permutation snarks, while the second one reads as follows.
For every 3-coloring of the edges of the complete graph on n vertexes, there is a color c and a set X of 4-vertexes such that at least $2n/3$ vertexes are linked to a vertex in X by an edge of color c.
This theorem is motivated by a conjecture of Erdős, Faudree, Gould, Gyárfás, Rousseau and Schelp from 1989, which asserts that X can be of size 3 only. However, they were only able to prove that X can be of size 22. Recently, Rahil Baber and John Talbot managed to build upon our work in a very nice article: adding a new idea to our argument, they managed to confirm the conjecture.

6.6.2. Graph theory and other fields

Interactions of graph theory with other topics (theoretical computer science, number theory, group theory, sociology and chemistry) have been considered. Most of them are still in progress and some are published. For instance, regarding distributed computing, the purpose of our work was to question the global knowledge each node is assumed to start with in many distributed algorithms (both deterministic and randomized). More precisely, numerous sophisticated local algorithm were suggested in the literature for various fundamental problems. Noticeable examples are the MIS algorithms and the $(\Delta+1)$-coloring algorithms. Unfortunately, most known local algorithms are *non-uniform*, that is, they assume that all nodes know good estimations of one or more global parameters of the network, e.g., the number of nodes n. Our work provides a rather general method for transforming a non-uniform local algorithm into a uniform one. Furthermore, the resulting algorithm enjoys the same asymptotic running time as the original non-uniform algorithm. Our method applies to a wide family of both deterministic and randomized algorithms. Specifically, it applies to almost all of the state of the art non-uniform algorithms regarding MIS and Maximal Matching, as well as to many results concerning the coloring problem.

6.6.3. Algorithmic Graph Theory and Clustering

Since September 2013, Mario Valencia has obtained a two years invitation (namely Inria "Délégation”) for working at Inria Nancy – Grand Est, in the Orpailleur team, on graph theoretical aspects and data clustering. This research work consists in studying the modular decomposition techniques on the threshold graphs issues of the clustering process. The principal studied problem is known as the *Cluster Deletion Problem*: given a graph with real non negative edge weights, partition the vertexes into clusters (in this case cliques) in order to minimize the total weight of edges out of the clusters. Two papers were submitted to journals in 2014. In [94], we discovered a one-to-one correspondence between potential solutions of the cluster deletion problem and the minimum sum coloring problem, and use it to obtain a polynomial time algorithm to solve the cluster deletion problem in a special family of graphs called P_4-reducible graphs.

In [95], we studied the complexity of the cluster deletion problem on subclasses of chordal graphs and cographs. In particular, it is shown that the cluster deletion problem is NP-hard for unweighted chordal graphs and weighted cographs. Some polynomial-time solvable cases are also identified.

Moreover, the paper "b-coloring is NP-hard on co-bipartite graphs and polytime solvable on tree-cographs", has been accepted for publication in the journal *Algorithmica* [1].

6.6.4. Structural and Algebraic Graph Theory

We have also worked on the following topics. Golumbic, Lipshteyn and Stern proved that every graph can be represented as the edge intersection graph of paths on a grid, i.e., one can associate to each vertex of the graph a nontrivial path on a grid such that two vertexes are adjacent if and only if the corresponding paths share at least one edge of the grid. For a non-negative integer k, B_k-EPG graphs are defined as graphs admitting a model in which each path has at most k bends. Circular-arc graphs are intersection graphs of open arcs of a circle. It is easy to see that every circular-arc graph is B_4-EPG, by embedding the circle into a rectangle of the grid. We proved also that every circular-arc graph is B_3-EPG (paper submitted).

We have studied the k-tuple chromatic number of the Cartesian product of two graphs G and H in [96]. We have shown that there exist graphs G and H such that $\chi_k(G\Box H) > \max\{\chi_k(G), \chi_k(H)\}$ for $k \geq 2$. Moreover, we have also shown that there exist graph families such that, for any $k \geq 1$, the k-tuple chromatic number of their Cartesian product is equal to the maximum k-tuple chromatic number of its factors.

PAREO Project-Team

6. New Results

6.1. Static Analysis

Participant: Sergueï Lenglet.

6.1.1. Static Analysis for Control Operators

Control operators, such as *call/cc* in Scheme or SML, allow programs to have access and manipulate their execution context. We study the behavioral theory of the $\lambda\mu$-calculus, an extension of the λ-calculus with a control feature similar to *call/cc*. In [6], we define an applicative bisimilarity for the $\lambda\mu$-calculus, demonstrating the differences in the definitions between call-by-name and call-by-value. We give equivalence examples to illustrate how our relations can be used; in particular, we prove David and Py's counter-example, which cannot be proved with the preexisting bisimilarities for the $\lambda\mu$-calculus. The proofs are in the accompanying research report [8], where we also define environmental bisimulations for the calculus.

6.1.2. Polymorphism and Higher-order Functions for XML

In [7], we define a calculus with higher-order polymorphic functions, recursive types with arrow and product type constructors and set-theoretic type connectives (union, intersection, and negation). We study the explicitly-typed version of the calculus in which type instantiation is driven by explicit instantiation annotations. In particular, we define an explicitly-typed λ-calculus with intersection types and an efficient evaluation model for it. The work presented in this article provides the theoretical foundations needed to design and implement higher-order polymorphic functional languages for semi-structured data.

6.2. Termination under Strategies

Participants: Horatiu Cirstea, Sergueï Lenglet, Pierre-Etienne Moreau.

Several approaches for proving the confluence and the termination of term rewriting systems have been proposed [10] and the corresponding techniques have been implemented in tools like Aprove [17] and TTT2 [26]. On the other hand, there are relatively few works on the study of these properties in the context of strategic rewriting and the corresponding results were generally obtained for some specific strategies and not within a generic framework. It would thus be interesting to reformulate these notions in the general formalism we have previously proposed [15] and to establish confluence and termination conditions similar to the ones used in standard rewriting.

We have first focused on the termination property and we targeted the rewriting strategies of the *Tom* language. We propose a direct approach which consists in translating *Tom* strategies into a rewriting system which is not guided by a given evaluation strategy and we show that our systematic transformation preserves the termination. This allowed us to take advantage of the termination proof techniques available for standard rewriting and in particular to use existing termination tools (such as Aprove and TTT2) to prove the termination of strategic rewriting systems. The efficiency and scalability of these latter tools has a direct impact on the performances of our approach especially for complex strategies for which an important number of rewrite rules could be generated. We have nevertheless proposed a meta-level implementation of the automatic transformation which improves significantly the performances of the approach. The corresponding tool is available at http://gforge.inria.fr/projects/tom.

6.3. Property-based Testing

Participants: Nauval Atmaja, Horatiu Cirstea, Pierre-Etienne Moreau.

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

We have proposed a property based testing framework for the *Tom* language inspired from the ones proposed in the context of functional programming. The previously developed tool has been improved by integrating it in the *Junit* framework. The tests are thus highly automatized and the library can be smoothly integrated in classical IDEs. The relatively simple shrinking method which searches a smaller counter-example starting from an initial relatively complex one has been also improved. The library is available at http://gforge.inria.fr/projects/tom.

6.4. Inductive Reasoning

Participant: Sorin Stratulat.

6.4.1. Decision Procedures to Prove Inductive Theorems Without Induction

Automated inductive reasoning for term rewriting has been extensively studied in the literature. Classes of equations and term rewriting systems (TRSs) with decidable inductive validity have been identified and used to automatize the inductive reasoning. In [9], we give procedures for deciding the inductive validity of equations in some standard TRSs on natural numbers and lists. Contrary to previous decidability results, our procedures can automatically decide without involving induction reasoning the inductive validity of arbitrary equations for these TRSs, that is, without imposing any syntactical restrictions on the form of equations. We also report on the complexity of our decision procedures. These decision procedures are implemented in our automated provers for inductive theorems of TRSs and experiments are reported.

6.4.2. Implementing Reasoning Modules in Implicit Induction Theorem Provers

In [30], we detail the integration in SPIKE, an implicit induction theorem prover, of two reasoning modules operating over naturals combined with interpreted symbols. The first integration schema is à la Boyer-Moore, based on the combination of a congruence closure procedure with a decision procedure for linear arithmetic over rationals/reals. The second follows a 'black-box' approach and is based on external SMT solvers. It is shown that the two extensions significantly increase the power of SPIKE; their performances are compared when proving a non-trivial application.

6.4.3. Building Explicit Induction Schemas for Cyclic Induction Reasoning

In the setting of classical first-order logic with inductive predicates, two kinds of sequent-based induction reasoning are distinguished: cyclic and structural. Proving their equivalence is of great theoretical and practical interest for the automated reasoning community. Previously, it has been shown how to transform any structural proof developed with the LKID system into a cyclic proof using the CLKID$^\omega$ system. However, the inverse transformation was only conjectured. In [29], we provide a simple procedure that performs the inverse transformation for an extension of LKID with explicit induction rules issued from the structural analysis of CLKID$^\omega$ proofs, then establish the equivalence of the two systems. This result is further refined for an extension of LKID with Noetherian induction rules. We show that Noetherian induction subsumes the two kinds of reasoning. This opens the perspective for building new effective induction proof methods and validation techniques supported by (higher-order) certification systems integrating the Noetherian induction principle, like Coq.

SEMAGRAMME Project-Team

6. New Results

6.1. Generation

G-TAG [52], [66] is a Tree Adjoining Grammar (TAG) based formalism which was specifically designed for the task of text generation. Contrary to TAG, the derivation structure becomes primary, as pivot between the conceptual representation and the surface form. This is a shared feature with the encoding of TAG into ACG. Laurence Danlos (Alpage Inria project), Aleksandre Maskharashvili, and Sylvain Pogodalla have shown how to recast the G-TAG formalism into ACG, relying on the reversibility properties of the later [17], [16], [18].

6.2. Discourse Grammar

Laurence Danlos (Alpage Inria project), Aleksandre Maskharashvili, and Sylvain Pogodalla have presented a method to interface a sentential grammar and a discourse grammar. It offers both a smooth integration of the two grammars without using an intermediate processing step, and the possibility to build discourse structures that are direct acyclic graphs (DAG) and not only trees. The analysis is based on a Tree-Adjoining Grammar (TAG) approach to discourse: Discourse Synchronous TAG (D-STAG) [50], [51], and uses an encoding of TAG into ACG. This allows for expressing a higher-order semantic interpretation that enables building DAG discourse structures, and for smoothly integrating the sentential and the discourse grammar thanks to the modular capability of ACG. All the examples may be run and tested with the the ACGtk (submitted).

6.3. Large Scale Grammatical Resources

Guy Perrier wrote a complete documentation [36] on FRIGRAM [0] a French grammar with a large coverage, written in the formalism of Interaction Grammars [59]. The different chapters of the 257 pages of documentation correspond to the different parts of speech in French. At the end, two chapters are dedicated to two specific phenomena: extraction (relative, interrogative and cleft clauses) and coordination, which is presented in common with punctuation because of their proximity.

6.4. Deep Syntax Annotation of the Sequoia French Treebank

Marie Candito, Guy Perrier, Bruno Guillaume, Corentin Ribeyre, Karën Fort, Djamé Seddah and Eric de la Clergerie annotated the Sequoia French Treebank with deep syntax dependencies [14].

The Sequoia French Treebank [47] is a 3.100 sentences treebank covering several domains (news, medical, europarl and fr-wikipedia). It is freely available and has already been annotated with surface dependency representations.

The participants in the project have defined a deep syntactic representation scheme for French, built from the surface annotation scheme of the Sequoia corpus and abstracting away from it [28]. This scheme expresses the grammatical relations between content words. When these grammatical relations take part into verbal diatheses, the diatheses are considered as resulting from redistributions from the canonical diathesis, which is retained in the annotation scheme.

The goal is to obtain a freely available corpus, which will be useful for corpus linguistics studies and for training deep analyzers to prepare semantic analysis.

The different steps of the annotation process were conducted in a collaborative way. As the members of the project are located in two different French towns (Paris and Nancy), they decided to produce a complete annotation of the TreeBank in both towns and to collaboratively adjudicate the two results.

[0] http://wikilligramme.loria.fr/doku.php/frig:frig

Each team separately produced an initial annotated version of the mini reference. The final version, resulting from several iterations and adjudications, is available [0].

6.5. Exploitation of the LVF (Lexicon of French Verbs)

Bruno Guillaume, Karën Fort, Guy Perrier and Paul Bédaride have worked on the LVF [53] ("Lexique des Verbes du Français", Lexicon of French Verbs). This large lexicon was build by two French linguists, Jean Dubois and Françoise Dubois-Charlier and contains detailed linguistic information about 12.308 lemmas of French verbs. The work presented in [21] describes experiments aiming at mapping the LVF to DICOVALENCE [87]. The two resources (LVF and DICOVALENCE) were built by linguists, based on very different theories, which makes a direct mapping nearly impossible. In the current work, we focus on the linguistic examples given in LVF. These examples are not sentences that can be parsed directly; the first part of the work was to express examples as real natural language sentence. It is then possible to use FRILEX, a Natural Language Processing lexicon based on DICOVALENCE to parse corrected examples given with LVF entries. This results in an automatic partial mapping of LVF entries against DICOVALENCE entries.

6.6. Game With A Purpose

Crowdsourcing is nowadays a way of constructing linguistic resources which is more and more used. In the crowdsourcing area, one of the way to motivate a large amount of people to contribute to a project is to present it as a game. Games used in this particular way are called GWAPs (Game With A Purpose).

In Natural Language Processing, examples of GWAP are "Phrase detective" where games are asked to resolve anaphora in English texts and "JeuDeMots" where gamers have to given lexical terms related to a term given by the system (the goal is to build a semantic networks of French lexical items).

Karën Fort and Bruno Guillaume worked on the definition of a GWAP to help construction of syntactically annotated corpora. With a student (Hadrien Chastant), they presented in April, the design of ZombiLingo [20], a GWAP that allows for the dependency syntax annotation of French corpora. The main aspects of this work are to explain: how to deal with the complexity of the task, how to motivate gamers to contribute and how to ensure that a large numbers of gamers will help to produce an high quality linguistic resource.

With another student (Valentin Stern), a first prototype was built. This first version implements only a part of the mechanisms described in the previous work and it is used as a proof-of-concept of a future game. This prototype was presentend at the TALN conference in July [27].

6.7. Supertagging

Guillaume Bonfante, Bruno Guillaume, Mathieu Porey and Guy Perrier wrote a book chapter [30] "Suppertagging with constraints". This chapter makes a survey of the results obtained in previous publications about supertagging based on polarities [46] and based on the companionship principle [45]. The last section of the chapter presents a new application of the companionship principle to the TAG formalism and presents some experimental results.

6.8. Modelling Semantic Phenomena

Despite the valuable insights yielded by the classical theories of discourse semantics, there is a wide range of exceptional phenomena that they fail to address, e.g., anaphora under double negation and modality. Concentrating on these two exceptions, Sai Qian, Philippe de Groote and Maxime Amblard provide a corresponding adaptation of TTDL for each case. Briefly speaking, for the problem of double negation, they propose to encapsulate both the affirmative representation and the negative representation of an expression in its semantics. Negation is treated as an operation which switches the positions of the two representations. Thus a second negation will switch the positions again as if no negation had ever occurred. In this way, a double negation can be eliminated and the desired referent accessibility is modelled. As for anaphora under modality,

[0] https://deep-sequoia.inria.fr

they propose to enrich the TTDL left context with the notion of modal base, which is proposed by Kratzer. The possible world model is integrated in the semantic representation as well. Moreover, they show how the different adaptations could work in an unified framework, [75].

6.9. Quantification in event semantics

Yoad Winter (Utrecht University) has given a type-logical account of quantification in event semantics.

It has been observed in the literature that Davidson's event semantics does not combine smoothly with Montague's compositional semantics. The difficulty comes from a possibly bad interaction between event existential closure, on the one hand, and quantification, negation, or conjunction, on the other hand. In a recent publication, Winter and Zwarts provide a solution to this problem. Winter and de Groote elaborate on this solution. In particular, they provide a treatment of quantified adverbial modifiers, which was absent from Winter and Zwarts, [19].

6.10. Pragmasemantic with Effects and Handlers

Jiří Maršík and Maxime Amblard have explored the feasibility of theories of side effects of programming languages in the study of natural language semantics and pragmatics [23]. In the approach that we are developing, the denotations we assign to fragments natural language are effectful computations. To demonstrate on an example, if we was to treat dynamics, then instead of changing the type of sentence denotations from o to c -> o * c, where c is the type of discourse contexts and o is the type of propositions, we would treat sentence denotations as effectful computations of type o that study and modify the context using effectful operations. This explicit distinction between 'result' and 'effects' brings to mind Stalnaker's distinction between 'content' and 'context'.

The motivation for this approach is to make it easier to compose multiple pragmasemantic phenomena by being allowed to put their effects aside. So far, a small prototype handling dynamics, presuppositions and some of their interactions is under development.

6.11. Mining Texts at discourse level

Linguistic discourse refers to the meaning of large chunks of text, from phrases to whole documents. It could be very useful for guiding attempts at text mining, which focus on document selection, document summarization, or other knowledge extraction goals. Hence the aim of this work is to apply Knowledge Discovery in Databases (KDD) methods to texts annotated with discourse information. Maxime Amblard with Yannick Toussaint (Orpailleur team) and Sara van de Moosdijk (master 2 intern) approach the problem by extracting discourse relations using unsupervised methods, which are then used to construct a knowledge model with Formal Concept Analysis (FCA). Pattern Structures (PS), an advancement in FCA, allow for the modelling of complex data. Our method is applied to a corpus of medical articles compiled from PubMed. This medical data is enhanced with concepts from the UMLS MetaThesaurus combined with the UMLS Semantic Network to serve as an ontology for Pattern Structure classification. The results show that despite having a large amount of noise, the method is promising and could be applied to other domains than the medical domain. We explore the pitfalls and suggest ways in which the process could be improved (Submission under review).

6.12. Exploring real datas

Maxime Amblard explored the use of formal framework for modelling transcription of real interviews, in particular one involves in the SLAM project with schizophrenics. Schizophrenia is well-known among mental illnesses for the severity of the thought disorders it involves, and for their widespread and spectacular manifestations: from deviant social behavior to delusion, not to mention affective and sensitive distortions. The goal of our interdisciplinary work is to (i) analyze linguistic troubles in conversational contexts in which one of the speakers is schizophrenic, (ii) construe how the concept of rationality and logicality may apply to them, and (iii) propose a formal representation about this specific manifestation. Maxime Amblard, Sylvain Pogodalla and Karen Fort propose surveys on past results [35], [29].

Maxime Amblard and Karen Fort have studied experiments they led concerning disfluencies in the discourse of schizophrenic patients (in remediation). These experiments are part of a larger study dealing with other levels of linguistic analysis, that could eventually help identifying clues leading to the diagnostic of the disease. This study largely relies on natural language processing tools, which allow for the rapid processing of massive textual data (here, more than 375,000 words). The first phase of the study, which they present confirmed the correlation between schizophrenia and the number of disfluences appearing in the discourse [25]. Moreover they have discussed ethical issues on the corpus with others [26].

6.13. Paraconsistency and Inconsistency-Friendly Logics

Paraconsistent logic is a family of formal systems in which the law of contradiction fails. In such systems, from an inconsistent set, *not* everything follows.

Can Baskent has studied such logical systems and their connections to formal linguistics within the framework of game theory. First, he observed how a game theoretical semantics can be given for some paraconsistent logics [43] . The advantage of game semantics is that it simply reflects the parsing tree of logic, and furthermore presents a semantical structure that uses elements from game theory. Such a study also requires an in-depth study of various paraconsistent logics, and their semantical structures [13]. Such a study requires some understanding of point-set topology, and its relation to logic.

Moreover, paraconsistent logics relate to dynamic logics as well. The logical model defines characterises how dynamic epistemic modalities, which are familiar from multi-agent systems, work [13]. This helps us understand how multi-agent interactions in an inconsistent model work in a sound way.

Another interesting way of seeing how inconsistency-friendly logics work is to consider them within the framework of game theory [37]. Game theory, similar to multi-agent systems, studies the intelligent and rational interaction of decision makers/agents. Yet, it suffers from various paradoxes. Such paradoxes are important from a computational semantical point of view. If paraconsistency is the most suitable tool to analyse paradoxes, then game theoretical paradoxes are not exceptions [37].

The technical work always needs to be supplemented by some conceptual work. Granted, paraconsistent logics find their ways in various philosophical and semantical issues, yet their computational analysis usually falls short. In [44], we discussed the connection between paraconsistent logics and Hintikka's interrogative models. These models have been developed by Hintikka, a pioneer of epistemic logic, and have been properly analysed from paraconsistent perspectives. If inquiry and questioning needs to be accounted for computationally, a paraconsistent approach will be an appropriate tool as well. Similarly, [39] discusses paraconsistency and its connection to social software. *Social Software* is a field conceived by Rohit Parikh, and it studies the computational and logical analysis of social protocols and policies. It lies in the intersection of social choice theory and game theory, and is a subset of logic.

Such results have been presented in various talks including, *World Congress of Paraconsistency* in Kolkata and *Logic and the Foundations of Game and Decision Theory* in Bergen, and warmly received.

SHACRA Project-Team

5. New Results

5.1. Highlights of the Year

5.1.1. Intra-operative guidance

Each year in Europe 50,000 new liver cancer cases are diagnosed for which hepatic surgery combined to chemotherapy is the most common treatment. In particular the number of laparoscopic liver surgeries has increased significantly over the past years. Minimally invasive procedures are challenging for the surgeons due to the limited field of view.

Providing new solutions to assist surgeons during the procedure is of primary interest. This year, the team developed an innovative system for augmented reality in the scope of minimally invasive hepatic surgery. The first issue is to align preoperative data with the intra-operative images. We first proposed a semi-automatic approach [28] for solving the ill-posed problem of initial alignment for augmented reality systems during liver surgery. Our registration method relies on anatomical landmarks extracted from both the laparoscopic images and a three-dimensional model, using an image-based soft-tissue reconstruction technique and an atlas-based approach, respectively.

Second, we introduced a method for tracking the internal structures of the liver during robot-assisted procedures [25]. Vascular network, tumors and cut planes, computed from pre-operative data, can be overlaid onto the laparoscopic view for image-guidance, even in the case of large motion or deformation of the organ. This is made possible by relying on a fast yet accurate 3D biomechanical model of the liver combined with a robust visual tracking approach designed to properly constrain the model. Our augmented reality proved to be accurate and extremely promising on in-vivo sequences of a human liver during robotic surgery.

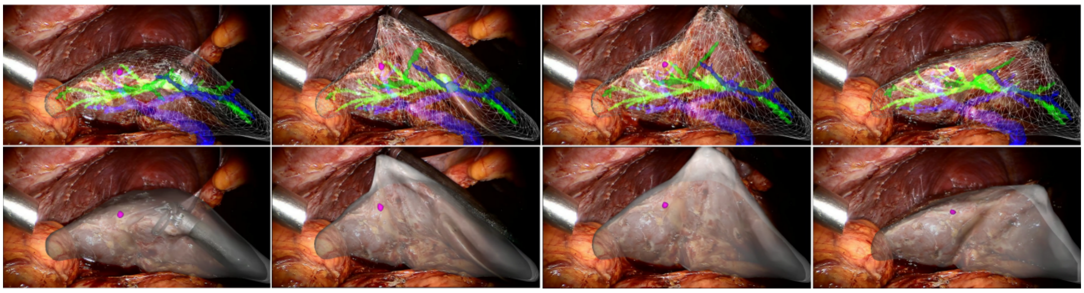


Figure 4. Augmented reality on the liver with 3D visualization of the blood vessels

5.1.2. Ph.D. defenses

The year 2014 was also special since many PhDs have been defended. Four PhD defenses took place with:

- Ahmed Yureidini's defense about *Robust blood vessel surface reconstruction for interactive simulations from patient data* [15] in May 2014,
- Guillaume Kazmitcheff's defense about *Minimal invasive robotics dedicated to otological surgery* [13] in June 2014,
- Hugo Talbot's defense about *Interactive patient-specific simulation of cardiac electrophysiology* [14] in July 2014,
- Alexandre Bilger's defense about *Patient-specific biomechanical simulation for deep brain stimulation* [12] in December 2014.

5.1.3. Organization of ISBMS 2014

The team co-organized the 6th International Symposium on Biomedical Simulation (ISBMS) 2014, which was held in Strasbourg (France) on October 16 – 17, 2014. The ISBMS conference is a well-established scientific meeting that provides an international forum for researchers interested in using biomedical simulation technology for the improvement of patient care and patient safety. The SiMMS group from Imperial College London and IHU-Strasbourg were the two other co-organizers. The event was hosted at IRCAD, a center of excellence in surgical training. The ISBMS chairs were:

- Stéphane Cotin (Inria),
- Fernando Bello (Imperial College London),
- Jérémie Dequidt (Univ. Lille),
- Igor Peterlik (IHU Strasbourg & Masaryk Univ.).

The whole team was involved in the organization of the event. About 65 participants joined the conference. Regarding their feedback, the conference was a real success. For more information about ISBMS, refer to the official website http://www.isbms.org.

Finally, a day dedicated to our software SOFA ("SOFA Day") was organized the day after the ISBMS conference. This was the opportunity to introduce SOFA to the ISBMS community and to share with the SOFA users.

(a) Setup of our demo

(b) With Genevieve Fioraso

Figure 5. Presentation of our work at the French National Assembly. Genevieve Fioraso is the French national research secretary

5.1.4. Demonstration at the French National Assembly

On Tuesday 21st January 2014, the team SHACRA presented its work during the "Internet et société numérique" working group. This was a joint event between Inria and the French National Assembly (Assemblée Nationale). On this special occasion, we made a demonstration of our simulations and the CEO from Inria Michel Cosnard also presented more globally the role of Inria in healthcare but also education, cloud computing, big data.

5.2. New Results

5.2.1. Real-Time Biophysical Models

5.2.1.1. Deep brain stimulation

Participant: Alexandre Bilger.

During this year, we developed an intra-operative registration method. It is used during a DBS surgery and can help the surgeon to locate anatomical structures for a safer and a more efficient treatment [21]. The method is based on the biomechanical model of brain shift we developed during the last years. Because some parameters of the model are unknown, we propose to estimate them with an optimization process. The cost function evaluates the distance between the model and the segmentation of pneumocephalus, the only indicator of brain shift visible on an intra-operative CT scan.

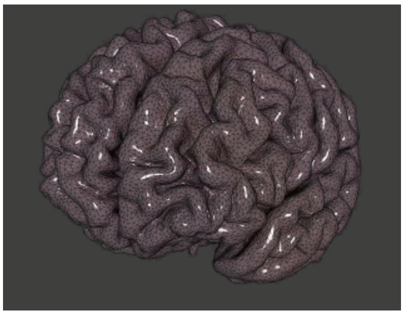


Figure 6. Biomechanical model of the brain for DBS planning

5.2.1.2. Stapedectomy

Participant: Guillaume Kazmitcheff.

Stapedectomy is a challenging procedure of the middle ear microsurgery, since the surgeon is in direct contact with sensitive structures such as the ossicular chain. This procedures is taught and performed in the last phase of the surgical apprenticeship. To improve surgical teaching, we propose to use a virtual surgical simulator [26] based on a finite element model of the middle ear. The static and dynamic behavior of the developed finite element model was successfully compared to published data on human temporal bones specimens. A semi-automatic algorithm was developed to perform a quick and accurate registration of our validated mechanical atlas to match the patient dataset. This method avoids a time-consuming work of manual segmentation, parameterization, and evaluation. A registration is obtained in less than 260 seconds with an accuracy close to a manual process and within the imagery resolution. The computation algorithms, allowing carving, deformation of soft and hard tissus, and collision response, are compatible with a real-time interactive simulation of a middle ear procedure. As a future work, we propose to investigate new robotized procedures of the middle ear surgery in order to develop new applications for the RobOtol device and to provide a training tool for the surgeons.

5.2.1.3. Cardiac electrophysiology

Participant: Hugo Talbot.

Cardiac arrhythmia is a very frequent pathology that comes from an abnormal electrical activity in the myocardium. The skills required for such interventions are still very challenging to learn, and typically acquired over several years. We first developed a training simulator for interventional electrocardiology and thermo-ablation of these arrhythmias [14], [32]. Based on physical models, this training system reproduces the different steps of the procedure, including endovascular navigation, electrophysiological mapping, pacing and cardiac ablation. Based on a scenario of cardiac arrhythmia, cardiologists assessed the interactivity and the realism of our simulation.

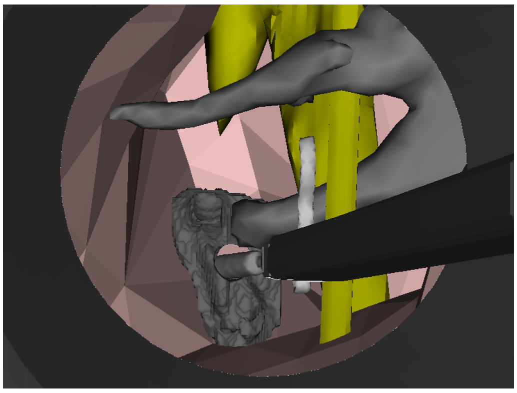


Figure 7. Simulation of the stapedotomy procedure

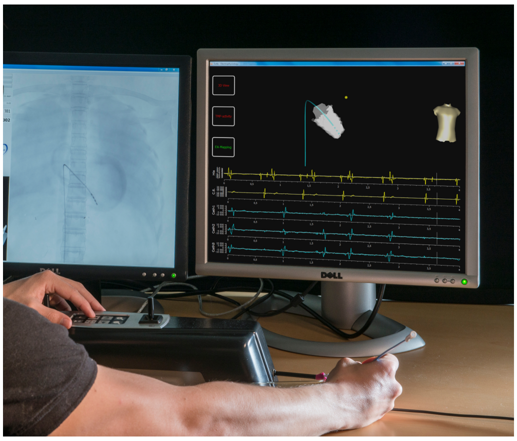


Figure 8. Training simulator for electrocardiology procedures

Beyond electrophysiology training, our work around the cardiac electrophysiology also target the personalization of our mathematical models. Using the dense electrograms recorded intra-operatively, we presented an accurate and innovative approach to personalize our model, i.e. estimate patient-specific parameters. The modeling in silico of a patient electrophysiology is needed to better understand the mechanism of cardiac arrhythmia. This work has been submitted in a conference.

5.2.1.4. Cryoablation

Participant: Hugo Talbot.

A new project started this year around cryotherapy. This technique consists in inserting needles that freezing the surrounding tissues, thus immediately leading to cellular death of the tissues. Cryoablation procedure is used in many medical fields for tumor ablation, and even starts being used in cardiology. In this scope, we build a simulator able to place the cryoprobes and run a simulation representing the evolution of iceballs in living tissues [31]. This work was presented at MMVR'14.

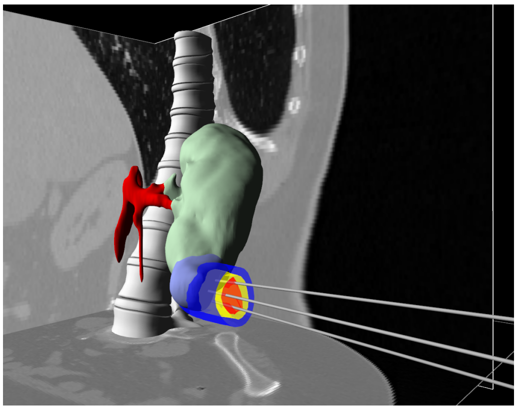


Figure 9. Simulation of the stapedotomy procedure

5.2.1.5. Connective tissues

Participant: Julien Bosman.

Another topic of simulation is the modeling of connective tissues [18]. First, a comparative study on the influence of the ligaments in liver surgery has been conducted. This study underlines that the model chosen for the ligament's has a strong influence on the outcome of the simulation. More specifically, it shows the the model is at least as much important as the material parameters of the parenchyma. It also shows that the influence of the model depends on the type of effort that is prescribed on the liver. The second axis concerns the validation of a frame (6-DOF nodes) based mechanical model developed for ligaments simulation. Current results show that this model requires less degrees of freedom while providing the same accuracy as a traditional FEM model. At last, a method dedicated to the simulation and the control of continuum robots has been developed. The goal of this method is to replace the mesh of robot by computing its compliance and applying it on a reduced model made of frames. It allows to strongly decrease the number of degrees of freedom needed for the robot simulation while keeping the needed accuracy.

5.2.1.6. Simulation of lipofilling reconstructive surgery

Participant: Vincent Majorczyk.

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

5.2.1.7. Inverse FEM simulation

Participant: Eulalie Coevoet.

We introduced a new methodology for semi-automatic deformable registration of anatomical structures [23], using interactive inverse simulations. We applied the approach for the registration of the parotid glands during the radiotherapy of the head and neck cancer. Radiotherapy treatment induces weight loss that modifies the shape and the positions of these structures and they eventually intersects the target volume. We proposed a method to adapt the planning to limit the radiation of these glands.

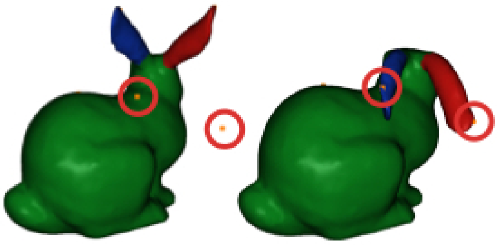


Figure 10. Numerical validation. Left: Target points (highlighted in red) after setting 3 different Young's moduli (one color by Young's modulus). Right: The resulting deformation once the Young modulus have been estimated.

5.2.2. Numerical Methods for Complex Interactions

5.2.2.1. Cliping in neurosurgery

Participant: Eulalie Coevoet.

We developed a simulator for neurosurgery. The surgery consist in "clipping" a cerebral aneurysm. Aneurysm is an abnormal local dilatation in the wall of a blood vessel, usually an artery. There are several treatment options for people with the diagnosis of cerebral aneurysm. Medical therapy, surgical therapy (clipping) and endovascular therapy (coiling). The surgical therapy, because of his invasive and technical nature, is the less prescribed. This leads to less and less surgeon trained to practice the procedure. And yet some patients require the surgical way. So the idea was to develop a simulator to train student and also help on the planification.

5.2.2.2. Virtual cutting

Participants: Huu Phuoc Bui, Christoph Paulus.

The simulation of cutting is a central interest in the team. Several approaches have been investigated this year to model surgical cuts, tearing and other separations of materials induced by surgical tools:

- using the standard finite element method (FEM) combined with a re-meshing approach, that replaces locally the current structure of the mesh in order to allow for a separation,
- using the extended FEM (X-FEM) that uses shape functions that can model discontinuities inside elements (see Fig. 12),
- and using the Lattice element method (LEM).

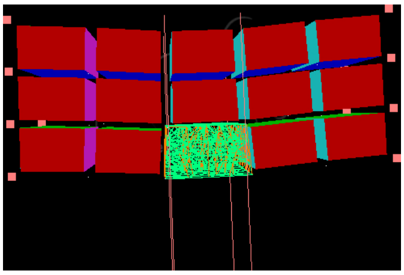
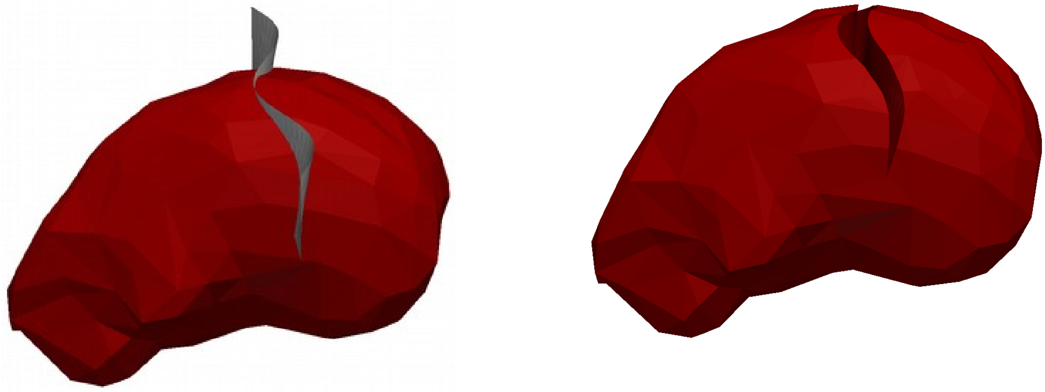


Figure 11. Cutting simulation using LEM

A re-meshing approach to model cuts has been submitted to several conferences, we are waiting for the response. An implementation of the extended finite element method was published in a preprint "Simulation of Complex Cuts in Soft Tissue with the Extended Finite Element Method (X-FEM)". The figures below show a simulation of a sinusoidal cut on a liver executed with the implementation of the X-FEM.

For the LEM approach (see Fig. 11), a multimapping between finite elements and lattice model have been developed and implemented into SOFA framework. This allows us to perform a multiscale simulation in real-time. A dynamic changing of topology between finite elements and lattices should be developed in the next step in order to perform the cutting dynamically.



(a) Plane of cut

(b) Result of the cutting

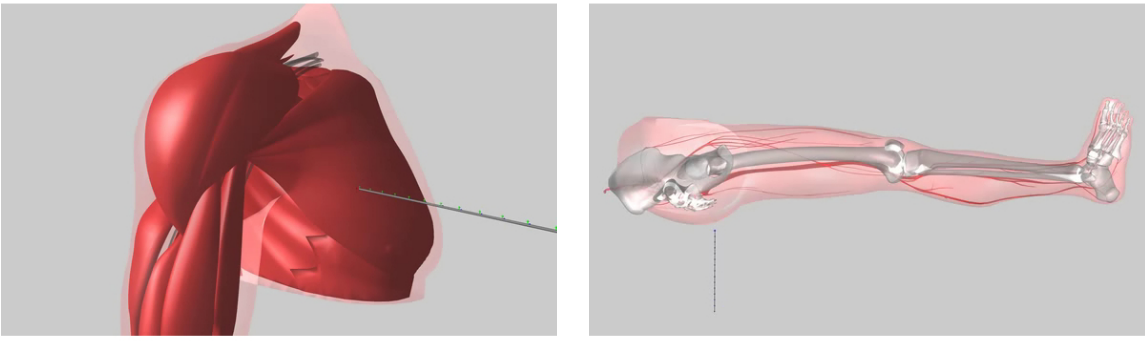
Figure 12. Cutting simulation based on X-FEM

5.2.2.3. Regional anaesthesia

Participants: Rémi Bessard Duparc, Frédérick Roy.

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. This year, the code for needle insertion has been re-designed and simplified into SOFA and the muscle contraction has been implemented. Finally, the components of the simulation have been optimized to reach the desired real-time performances (i.e more than 25-30 frames per second).

Our preliminary results are awaiting the validation of the Working Packages in January 2015. The needle refactoring will be shared with an other project in Strasbourg (robot) and may be shared with an other team at Inria Rennes with the LAGADIC Team.



(a) Needle insertion in the shoulder

(b) Needle insertion in the leg

Figure 13. Regional anaesthesia with needle insertion and muscle contraction

5.2.2.4. Control of elastic soft robots

Participant: Frédérick Largillière.

We developed a prototype of stiffness-controlled haptic interface using a piece of silicone rubber to render different forces related to a displacement ie. different stiffnesses and an improved method of simulation using multi-rate loops to try to keep the computation real-time even with models using a large number of FEM elements. (work currently under review) We also presented the idea of a surgical robot able to virtually reconstruct its environment (ie. surrounding biological tissues) through small modifications of the algorithm used for controlling soft robots (SURGETICA 2014).

5.2.3. Image-Driven Simulation

5.2.3.1. Physics-based registration algorithms

Participant: Rosalie Plantefève.

Before targeting the augmented reality for laparoscopic operations, an important step consists in solving the initial alignment problem. Given a pre-operative image of the organ (usually a CT scan) a detailed mesh is constructed. To make the information stored in this mesh available during the operation, the mesh must be registered onto the intra operative view. However, mainly due to the pneumoperitoneum, the organ has undergone important deformation between the pre-operative images acquisition and the operation. The pre-operative shape and the intra-operative shape of the organ do not correspond. Therefore a non rigid registration is required to align the mesh and the real organ. Our registration algorithms also allowed us to work on a mean to automatically recover boundary conditions of a patient specific liver.

We created a statistical atlas [29] of the human liver to store some of the liver boundary conditions positions : the veina cava and the anchor point of the falciform ligament positions. This method was presented at MICCAI 2014. We also developed a new registration method [28] that evolves automatically from a rigid registration to a non rigid registration to solve the initial alignment problem. The method use some anatomical features of the liver such as the anchor point position of the falciform ligament. This method was presented at ISBMS 2014.

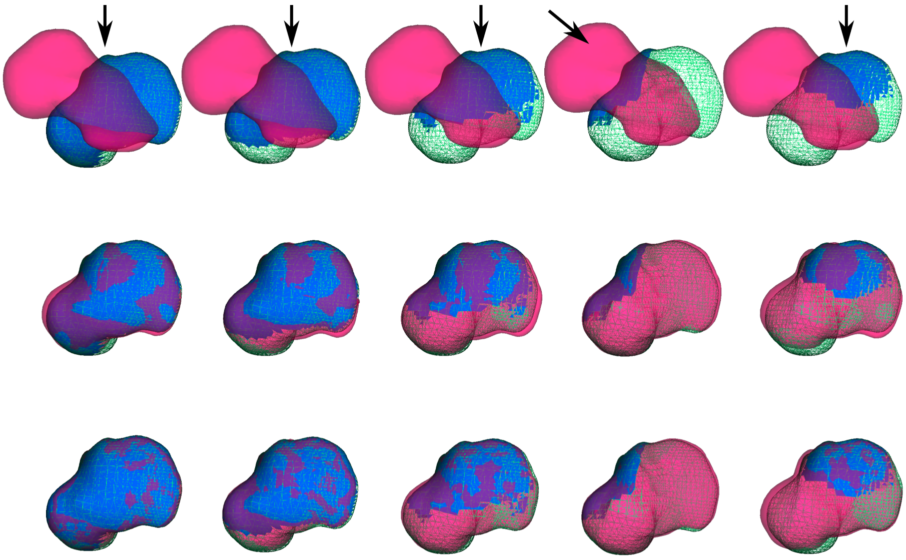


Figure 14. Results showing the initial alignment of a liver between pre-operative and intra-operative data

5.2.3.2. Augmented reality

Participant: Nazim Haouchine.

After this intra-operative registration, the augmented reality is possible. This topic is one the highlight of the year 2014. In 2014, we proposed a method for real-time augmented reality of internal liver structures during minimally invasive hepatic surgery [25]. This project is done is collaboration with the EPI MAGRIT. Vessels and tumors computed from pre-operative CT scans can be overlaid onto the laparoscopic view for surgery guidance. Compared to current methods, our method is able to locate the in-depth positions of the tumors based on partial three-dimensional liver tissue motion using a real-time biomechanical model. This model permits to properly handle the motion of internal structures even in the case of anisotropic or heterogeneous tissues, as it is the case for the liver and many anatomical structures. Experimentations conducted on phantom liver permits to measure the accuracy of the augmentation while real-time augmentation on in vivo human liver during real surgery shows the benefits of such an approach for minimally invasive surgery. Finally, a method for 3D reconstruction of elastic shapes with self-occlusion handling was also proposed.

5.2.3.3. Segmentation

Participant: Zhifan Jiang.

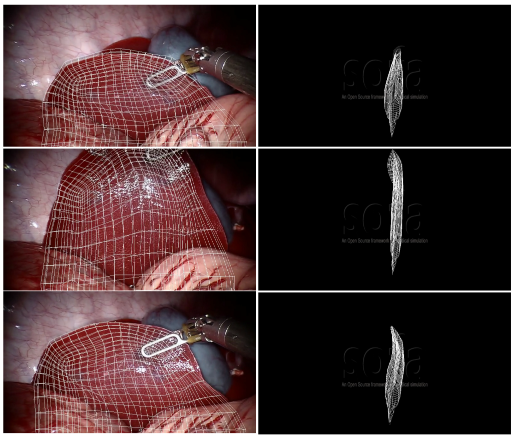


Figure 15. Augmented reality view of a liver during laparoscopic surgery

We have been working on medical image analysis in the context of the female pelvic medicine. Image-based diagnoses of pelvic floor disorders like prolapse or endometriosis rely on mechanical indicators, such as mobilities of organs and shear displacements between organs. Image data do not provide directly qualitative indicators hence analysis and diagnosis of medical are required although unfortunately subjected to surgeon expertise subjectivity. Therefore, objective information would be useful for both precise diagnoses and planning of surgical procedure. The objective is to develop numerical tools which extract quantitative information from static and cine MR images based on algorithms of detection and tracking.

We have developed numerical models not only for visualization, but also for quantitative measurements on a group of organs, such as their shapes and their relative movements. The numerical tool extracts these quantitative information (displacements and shear inter-organ) as well as the geometric shape of organs from images via Model-to-Image registration based on B-spline models. Our approach enables to identify multiple organ shapes in a single 2-dimension MR image and then to track their motion in a sequence of 2-dimension dynamic (cine) MR images for the study of the mobilities of the pelvic system. The method has been tested on healthy and pathological patient-specific data (19 patients) and the results provide valuable data to assess the shear displacement between organs and therefore making it possible to identify weakened ligaments or fascia which function differently in patients having pathologies. However, the results are to be validated by further mechanical FEM simulations. This work has been accepted in the journal STRAIN.

5.2.3.4. MIND project

Participants: Myriam Lekkal, Raffaella Trivisonne.

Within a feasibility study contest, we worked on Human Computer Interaction developing a new, intuitive and efficient way to interact with medical information in modern operating room. Nowadays operating rooms are progressively outfitted with computerized equipment necessary to access and manipulate a significant amount of data (i.e. medical images, patient's records, patient's vitals and physical parameters of the operating environment). This type of equipment belongs to the non-sterile section of an operating room, therefore surgeons, who are not allowed to be contaminated, cannot directly interact with it.

The idea of MIND project is to create a new device that could be used alone, such as a remote control, or easily integrated onto several locations, according to user preferences or constraints from the surgical procedure. Through this remote control, surgeons are able to access and manipulate medical information within the operating field and without leaving the instruments. For the software side the main aspects are distributed in two categories: a low level library, in charge of tasks such like handling the communications between

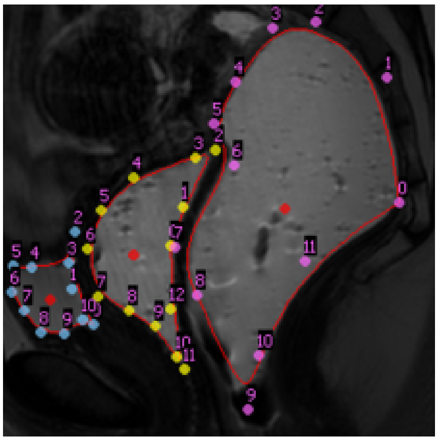
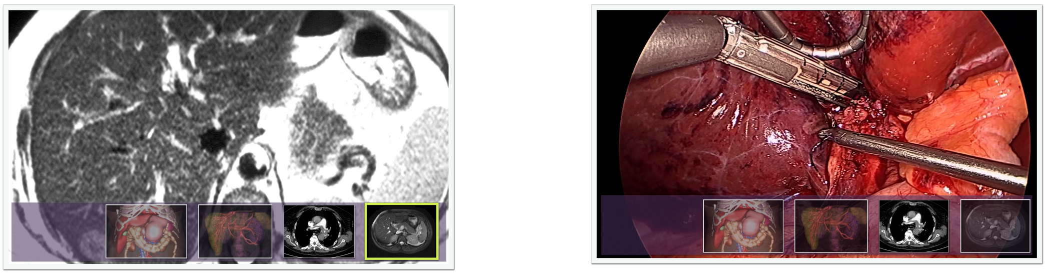


Figure 16. Contour segmentation on the pelvic system

the wireless instrument and the central computer, and a set of high-level functionalities and applications concerning the development of users GUI and new applications according to the needs of the case.

This work resulted in a patent [35] (still pending). Read more here http://mindsurgeonmouse.weebly.com/.



(a) View 1

(b) View 2

Figure 17. Example of the MIND GUI

TONUS Team

6. New Results

6.1. Highlights of the Year

We have implemented an OpenCL task graph version of our Discontinuous Galerkin solver that allows to overlap GPU computations and MPI communications. With this optimizations, we were recently able to achieve a 14 GFLOPS simulation with 8 GPUs on an electromagnetic test case. These results are included in the PhD of Thomas Strub (defence planned in March 2015) under the supervision of Philippe Helluy.

6.2. Development of semi-Lagrangian methods

Participants: Adnane Hamiaz, Michel Mehrenberger, Christophe Steiner.

6.2.1. Gyroaverage operator for a polar mesh

A direct method is proposed in [17] in the space configuration for the computation of the gyroaverage operator. It consists in integrating on the gyrocircles using interpolation operators (Hermite or cubic splines); see also [2]. Numerical comparisons with a standard method based on a Padé approximation are performed: (i) with analytical solutions; (ii) considering the 4D drift-kinetic model with one Larmor radius and (iii) on the classical linear DIII-D benchmark case. In particular, we show that in the context of a drift-kinetic simulation, the proposed method has similar computational cost as the standard method and its precision is independent of the radius. Extension to the quasi neutral equation has begun on a 4D model with one Larmor radius. We can exhibit some specific situations where the new method leads to more accurate results and we observe as predicted that the instability growth rate is stronger than for the Padé approximation. On the other hand, we have to face with more oscillations (e.g. on the boundary) of the new operator, which does not permit to replace the Padé approximation. Promising higher order Padé approximation are envisaged for the future.

6.2.2. Semi-Lagrangian simulations on curvilinear grids

Semi-Lagrangian schemes often deal with cartesian mesh; the extension to curvilinear grids is important in order to be able to deal with specific geometries and also for adapting the grid to save computational effort. This study is part of a general work on adding curvilinear capabilities for the simulation of drift kinetic and gyrokinetic equations in a semi-Lagrangian framework, and is in current development in the SeLaLib library.

Thus, in [28] semi-Lagrangian guiding center simulations are performed on sinusoidal perturbations of cartesian grids, thanks to the use of a B-spline finite element solver for the Poisson equation and the classical backward semi-Lagrangian method (BSL) for the advection. We are able to reproduce the standard Kelvin-Helmholtz instability test on such grids. When the perturbation leads to a strong distorted mesh, we observe that the solution differs if one takes standard numerical parameters that are used in the cartesian reference case. We can recover good results together with correct mass conservation, by diminishing the time step.

6.2.3. Field aligned semi-Lagrangian schemes

In [23] we introduce field aligned interpolation for Semi-Lagrangian schemes, by adapting a method developed by Hariri-Ottaviani to the semi-Lagrangian context. This approach is validated on the constant oblique advection equation and on a 4D drift kinetic model with oblique magnetic field in cylindrical geometry. The strength of this method is that one can reduce the number of points in the longitudinal direction. Extension to tokamak conguration in toroidal geometry is the next step of this study.

6.2.4. KEEN wave simulations, high order time splitting, non-uniform cubic splines

KEEN waves are non-stationary, nonlinear, self-organized asymptotic states in Vlasov plasmas (see [3]). They lie outside the precepts of linear theory or perturbative analysis, unlike electron plasma waves or ion acoustic waves. Steady state, nonlinear constructs such as BGK modes also do not apply. The range in velocity that is strongly perturbed by KEEN waves depends on the amplitude and duration of the ponderomotive force generated by two crossing laser beams, for instance, used to drive them. Smaller amplitude drives manage to devolve into multiple highly-localized vorticlets, after the drive is turned off, and may eventually succeed to coalesce into KEEN waves. Fragmentation once the drive stops, and potential eventual remerger, is a hallmark of the weakly driven cases. A fully formed (more strongly driven) KEEN wave has one dominant vortical core. But it also involves fine scale complex dynamics due to shedding and merging of smaller vortical structures with the main one. Shedding and merging of vorticlets are involved in either case, but at different rates and with different relative importance. The narrow velocity range in which one must maintain sufficient resolution in the weakly driven cases, challenges fixed velocity grid numerical schemes. What is needed is the capability of resolving locally in velocity while maintaining a coarse grid outside the highly perturbed region of phase space. We here report on a new Semi-Lagrangian Vlasov-Poisson solver based on conservative non-uniform cubic splines in velocity that tackles this problem head on. An additional feature of our approach is the use of a new high-order time-splitting scheme which allows much longer simulations per computational effort. This is needed for low amplitude runs. There, global coherent structures take a long time to set up, such as KEEN waves, if they do so at all. The new code's performance is compared to uniform grid simulations and the advantages are quantified. The birth pains associated with weakly driven KEEN waves are captured in these simulations. Canonical KEEN waves with ample drive are also treated using these advanced techniques. They will allow the efficient simulation of KEEN waves in multiple dimensions, which will be tackled next, as well as generalizations to Vlasov-Maxwell codes. These are essential for pursuing the impact of KEEN waves in high energy density plasmas and in inertial confinement fusion applications. More generally, one needs a fully-adaptive grid in- phase-space method which could handle all small vorticlet dynamics whether pealing or remerging. Such fully adaptive grids would have to be computed sparsely in order to be viable. This two-velocity grid method is a concrete and fruitful step in that direction.

6.2.5. Conservative semi-Lagrangian scheme

While developing a new semi-Lagrangian solver, the gap between a linear Landau run in 1D-1D and a 5D gyrokinetic simulation in toroidal geometry is quite huge. Intermediate test cases are welcome for testing the code. A new fully two-dimensional conservative semi-Lagrangian (CSL) method is presented in [6] and is validated on 2D polar geometries. We consider here as building block, a 2D guiding-center type equation on an annulus and apply it on two test cases. First, we revisit a 2D test case previously done with a PIC approach and detail the boundary conditions. Second, we consider a 4D drift-kinetic slab simulation. In both cases, the new method appears to be a good alternative to deal with this type of models since it improves the lack of mass conservation of the standard semi-Lagrangian (BSL) method.

6.3. Reduced Vlasov-Maxwell modeling

Participants: Philippe Helluy, Laurent Navoret, Thi Trang Nhung Pham.

We have tested several preliminary methods for reducing the complexity of the Vlasov equation. By expanding the distribution function on velocity basis we obtain a space-only hyperbolic system. This system takes advantage of interesting conservation or entropy properties. Several types of basis can be used: Fourier [14], piecewise Lagrange [20], [13], etc. The method has been implemented for 4D problems in the Selalib library. The next step would be to adapt the size of the expansion according to the nature of the flow region and to apply the method to the gyrokinetic model.

6.4. GPU Optimization of Discontinuous Galerkin solvers

Participants: Michaël Gutnic, Philippe Helluy, Michel Massaro, Thomas Strub.

We have continued to investigate implementations of numerical schemes on new hybrid computer architectures. We have for instance applied a very efficient Strang splitting algorithm for the numerical resolution of the MHD or compressible multiphase model ([16], [18], [22]). We have also highly optimized our DG solver CLAC ([20]) for electromagnetic applications. For instance, we have implemented an OpenCL task graph that allows to overlap GPU computations and MPI communications. With this optimizations, we were recently able to achieve a 14 GFLOPS simulation with 8 GPUs on an electromagnetic test case. These results are included in the PhD of Thomas Strub (defence planned in March 2015).

6.5. Numerical and theoretical study of reduced MHD problems for the JOREK code

Participant: Emmanuel Franck.

The Jorek code is a parallel finit element code (used at the CEA Cadarache and the IPP) which simulates the edge instabilities in the Tokamak solving reduced MHD models. Firstly we have written a family of full MHD models (resistive, diamagnetic and extended MHD models). Using this, we write the reduced MHD models close to the models implemented in the code which conserve the energy and are more stable ([35]). This work will probably be published as an Inria report next year. The second part of this work consists in writing a simplified version of the JOREK code which will be useful to test and validate future numerical research in the JOREK context. Actually we have written a code which solve simple elliptic equations in 3D toroidal geometry using Bezier, splines and Fourier expansion. The integration of simple wave model and reduced MHD models [33] is in progress. When these model will be implemented, we will test a new preconditioning for the JOREK code in these simple configurations.

6.6. Simulations of highly oscillatory Vlasov-type models

Participants: Emmanuel Frénod [Univ. Bretagne-Sud], Sever Hirstoaga.

We continued our exploration of a new time-stepping method based on an exponential integrator.

First, we have improved the algorithm introduced in [11] for solving a multi-scale 1d-1d Vlasov-Poisson system within a Particle-In-Cell method, in order to do accurate long time simulations. As an exponential integrator, the new scheme (see [10]) allows to use large time steps compared to the size of oscillations in the solution. More precisely, the new idea is to push each particle with its computed period. Our simulations show that using precise periods for each particle and at each macroscopic time step results in a more accurate scheme in long times.

Then, similar ideas are used for a 2d-2d multi-scale Vlasov-Poisson system (see [27]). We propose in a Particle-In-Cell framework a robust time-stepping method that works uniformly when the small parameter (the smallest scale) vanishes. We first verify our scheme in the framework of a proposed analytic solution with fast oscillations in time and we show that the scheme works for any initial condition. Then we test the method in the nonlinear case of a Vlasov-Poisson simulation. The scheme is able to use large time steps with respect to the typical size of the solution's fast oscillations. In addition, we show numerically that the method has accurate long time behaviour and that it is asymptotic preserving with respect to the limiting Guiding Center system.

TOSCA Project-Team

6. New Results

6.1. Probabilistic numerical methods, stochastic modelling and applications

Participants: Mireille Bossy, Nicolas Champagnat, Julien Claisse, Madalina Deaconu, Benoît Henry, James Inglis, Antoine Lejay, Oana Valeria Lupascu, Sylvain Maire, Sebastian Niklitschek Soto, Denis Talay, Etienne Tanré, Denis Villemonais.

6.1.1. Published works and preprints

- M. Bossy and J.-F. Jabir (University of Valparaíso) [13] have proved the well-posedness of a conditional McKean Lagrangian stochastic model, endowed with the specular boundary condition, and further the mean no-permeability condition, in a smooth bounded confinement domain $\mathcal{D}$.
- M. Bossy, N. Champagnat, S. Maire and L. Violeau worked with H. Leman (CMAP, Ecole Polytechnique) and M. Yvinec (Inria Sophia, EPI GEOMETRICA) on Monte Carlo methods for the linear and non-linear Poisson-Boltzmann equations [12]. These methods are based on walk on spheres algorithm, simulation of diffusion processes driven by their local time, and branching Brownian motion. Their code for the linear equation can deal with bio-molecules of arbitrary sizes, based on computational geometry tools from the CGAL C++ Library developed by the GEOMETRICA team. The non-linear equation is solved using branching Brownian motion.
- M. Bossy, O. Faugeras (Inria Sophia, EPI NEUROMATHCOMP), and D. Talay have clarified the well-posedness of the limit equations to the mean-field N-neuron models proposed in [42] and proven the associated propagation of chaos property. They also have completed the modeling issue in [42] by discussing the well-posedness of the stochastic differential equations which govern the behavior of the ion channels and the amount of available neurotransmitters. See [29].
- N. Champagnat and D. Villemonais obtained criterions for existence and uniqueness of quasi-stationary distributions and Q-processes for general absorbed Markov processes [31]. A quasi-stationary distribution is a stationary distribution conditionally on non-absorbtion, and the Q-process is defined as the original Markov process conditioned to never be absorbed. The criterion that they obtain ensures exponential convergence of the conditioned t-marginal of the process conditioned not to be absorbed at time t, to the quasi-stationary distribution and also the exponential ergodicity of the Q-process.
- M. Deaconu and S. Herrmann continued and completed the study of the simulation of the hitting time of some given boundary for Bessel processes. They constructed an original approximation method for hitting times of a given threshold by Bessel processes with non-integer dimension. In this work, they combine the additivity property of the laws of squared Bessel processes with their previous results on the simulation of hitting times of Bessel processes with integer dimension, based on the method of images and on the connexion with the Euclidiean norm of the Brownian motion [33].
- M. Deaconu, S. Herrmann and S. Maire introduced a new method for the simulation of the exit time and position of a δ-dimensional Brownian motion from a domain. The main interest of this method is that it avoids splitting time schemes as well as inversion of complicated series. The idea is to use the connexion between the δ-dimensional Bessel process and the δ-dimensional Brownian motion thanks to an explicit Bessel hitting time distribution associated with a particular curved boundary. This allows to build a fast and accurate numerical scheme for approximating the hitting time [34].
- M. Deaconu and O. Lupaşcu worked with L. Beznea (Bucharest, Romania) on the construction and the branching properties of the solution of the fragmentation equation and properly associate a continuous time càdlàg Markov process. The construction and the proof of the path regularity of the Markov processes are based on several newly developed potential theoretic tools.

- J. Inglis, together with O. Faugeras (Inria NeuroMathComp) finalized their article [18] on the well-posedness of stochastic neural field equations within a rigorous framework.
- J. Inglis and E. Tanré together with F. Delarue and S. Rubenthaler (Univ. Nice – Sophia Antipolis) finalized their article [16] on the global solvability of a networked system of integrate-and-fire neurons proposed in the neuroscience literature.
- J. Inglis and E. Tanré together with F. Delarue and S. Rubenthaler (Univ. Nice – Sophia Antipolis) completed their study of the mean-field convergence of a highly discontinuous particle system modeling the behavior of a spiking network of neurons, based on the integrate-and-fire model [17]. Due to the highly singular nature of the system, it was convenient to work with a relatively unknown Skorohod topology.
- J. Inglis and D. Talay introduced in [38] a new model for a network of spiking neurons that attempted to address several criticisms of previously considered models. In particular the new model takes into account the role of the dendrites, and moreover includes non-homogeneous synaptic weights to describe the fact that not all neurons have the same effect on the others in the network. They were able to obtain mean-field convergence results, using new probabilistic arguments.
- A. Lejay have worked with G. Pichot (EPI Sage) on benchmarks for testing Monte Carlo methods to simulate particles in one-dimensional media, and applied this statistical methodology to four methods, including the exact method developed previously [45]. This work led also to empirical observations that should guide the design of new methods [24].
- S. Maire is working with the Bulgarian Academy of sciences on Monte Carlo algorithms for linear equations based on killed random walks. In a first work, with I. Dimov and J-M. Sellier [37], a new Monte Carlo method to solve linear systems of equations has been introduced. This method can either compute one component of the solution or all components simultaneously. In a second work, with Ivan Dimov and Rayna Georgieva, a new Monte Carlo method to solve Fredhom integral equations of the second kind is developed [36].
- D. Villemonais worked with P. Del Moral (Univ. Sydney) on the conditional ergodicity of time inhomogeneous diffusion processes [35]. 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 proved a Foster-Lyapunov type criterion which ensures the exponential ergodicity of a Fleming-Viot type particle system whose particles evolve as birth and death processes. The criterion also ensures the tightness of the sequence of empirical stationary distributions considered as a family of random measures. A numerical study of the speed of convergence of the particle system is also obtained under various settings [41].

6.1.2. Other works in progress

- M. Bossy and J-F. Jabir (University of Valparaíso) proved the validity of a particle approximation of a (simplified) Lagrangian Stochastic Model submitted to specular reflections at the boundary and satisfying the mean no-permeability condition. This work achieves to extend our previous study [43] to the multidimensional case.
- N. Champagnat and D. Villemonais obtained criterions for existence, uniqueness and exponential convergence in total variation of quasi-stationary distributions and Q-processes for general absorbed and killed diffusion processes. The criterion obtained is equivalent to the property that a diffusion on natural scale coming down from infinity has uniformly (w.r.t. the initial condition) bounded expectation at a fixed time t. A study of nearly critical cases allow to conjecture that this property is true for all diffusion processes on natural scale coming down from infinity. This work is currently being written.
- N. Champagnat and B. Henry worked on the long-time behavior of the frequency spectrum for the Splitting Tree models under the infinitly-many alleles model. They obtained, using a new method for computing the expectation of an integral with respect to a random measure, the asymptotic behavior

of the moments of the frequency spectrum. As an application, they derived the law of large number and a new central limit theorem for the frequency spectrum. This work is currently being written.

- J. Claisse defended his PhD. under the supervision of N. Champagnat and D. Talay on stochastic control of population dynamics. He completed a finite-horizon optimal control problem on branching–diffusion processes. He also created and studied a hybrid model of tumor growth emphasizing the role of acidity. Key therapeutic targets appear in the model to allow investigation of optimal treatment problems.
- J. Claisse and D. Talay in collaboration with X. Tan (Univ. of Paris Dauphine) extended their previous work on a pseudo-Markov property enjoyed by the solutions of controlled stochastic differential equations and its application to the proof of the dynamic programming principle. A paper is being finished.
- M. Deaconu and O. Lupascu are working with L. Beznea (Bucharest, Romania) on a stochastic model for avalanche phenomena involving rupture properties that occur in the physical and deterministic models for snow avalanches. This approach is based on their recent results on fragmentation processes by stochastic differential equation and branching processes.
- M. Deaconu and O. Lupascu are working on a numerical probabilistic algorithm for an avalanche-type process. The originality of this approach is to use a coagulation/fragmentation model to describe the avalanche phenomenon. More precisely, they consider a particular fragmentation kernel which introduces “rupture-type” properties of deterministic models for snow avalanches.
- An important issue in neuroscience is the modelling of spike trains of a single neuron. In this context, the membrane potential of a neuron can be described by using a simple stochastic differential equation with periodic input, that is reset to a rest potential each time it hits a certain threshold. J. Inglis, A. Richard, D. Talay, and E. Tanré study how the law of these hitting times is affected when one changes the white noise (in the SDE) into a correlated noise. Practically, they use a fractional Brownian motion, and since the computation of the hitting times of such a non-Markovian, non-semimartingale process is still an open question, they rather try to compute the deviations from the white noise model. This is expected to give insights on the relevance of models with memory and long-range dependence.
- J. Inglis started a collaboration with B. Hambly and S. Ledger at the University of Oxford, in which interacting mean-field particle systems with common noise are being studied. Such systems are representative of systems of spiking neurons or portfolio defaults. In previous studies each particle was driven by a noise that was assumed independent from particle to particle (i.e. intrinsic noise). By considering a common driving noise in addition to the intrinsic noise, it is possible to model the fact that the environment in which the particles live is also noisy. This leads to the study of a new type of conditional McKean-Vlasov equation.
- J. Inglis, in collaboration with J. Maclaurin (EPI NEUROMATHCOMP) and W. Stannat (Berlin), has begun working on a new framework to understand the effect of noise on neural field equations. Deterministic neural field equations exhibit traveling wave solutions, and so the effect of noise on these solutions is of great interest. The idea is to decompose the solution into various components, which allow one to see directly how the noise affects the solution in the direction of the moving wave front. In particular, the goal is to reconcile mathematically the previous works of P. Bressloff and W. Stannat on the same subject, and to obtain a large deviation principle.
- J. Inglis and D. Talay are in the process of studying the emergence of spatio-temporal noise starting from microscopic models of neuron conductance.
- A. Lejay continued his collaboration with S. Torres (Universidad de Valapraíso, Chile) and E. Mordecki (Universidad de la República, Uruguay) on the estimation of the parameter of the Skew Brownian motion. This work is related to the modelling of diffusion processes in media with interfaces and has potential applications in many domains, such as population ecology.

- Together with R. Rebolledo (Pontificia Universidad Católica, Santiago, Chile), A. Lejay continued his review work on the mathematical modelling of the Wave Energy Converter Called the Oscillating water column, within the framework of the CIRIC project.
- A. Lejay continued his work on the Snapping out Brownian motion to perform numerical tests for the computation of the mean residence time in a diffusive medium with semi-permeable membranes, such as the one encountered in the mathematical modelling of diffusion Magnetic Resonance Imaging.
- A. Lejay continued his collaboration with L. Coutin (Universté Paul Sabatier, Toulouse) on the sensitivity of rough linear differential equations, by providing general results on the derivatives of the solution of rough differential equations with respect to parameters or the starting point.
- S. Niklitschek Soto and D. Talay completed their stochastic analysis of diffraction parabolic PDEs with general discontinuous coefficients in the multidimensional case.
- P. Guiraud (University of Valparaíso) and E. Tanré study the effect of noise in the phenomenon of spontaneous synchronisation in a network of connected leaky integrate-and-fire neurons. They detail cases in which the phenomenon of synchronization persists in a noisy environment, cases in which noise permits to accelerate synchronization, and cases in which noise permits to observe synchronization while the noiseless model does not show synchronization. (Math Amsud program SIN)
- O. Faugeras (EPI NeuroMathComp) and E. Tanré worked on an extension of [44] to a context of several populations of homogeneous neurons. They study the limit mean field equation of the membrane potential as the number of neurons increases in a network with correlated synaptic weights. A paper is in preparation.
- C. Graham (CMAP, Ecole polytechnique) and D. Talay are writing the second volume of their series published by Springer on the Mathematical Foundations of Stochastic Simulations.
- In collaboration with N. Touzi (CMAP, Ecole polytechnique), D. Talay is studying stochastic differential equations involving local times with stochastic weights, and extensions of classical notions of viscosity solutions to PDEs whose differential operator has discontinuous coefficients and transmission boundary conditions.

6.2. Financial Mathematics

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

6.2.1. Published works and preprints

- In collaboration with N. Maïzi (CMA - Mines Paristech) and O. Pourtallier (Coprin team, Inria Sophia Antipolis - Méditerranée), M. Bossy studied the existence of a Nash equilibrium between electricity producers selling their production on an electricity market and buying CO2 emission allowances on an auction carbon market. The producers' strategies integrate the coupling of the two markets via the cost functions of the electricity production. The authors set out the set of Nash equilibria on the electricity market, that constitutes an equivalence class (same prices and market shares) from which they exhibit a dominant strategy. On the coupled markets, given a specific carbon market design (in terms of penalty level and allowances), they compute the bounds of the interval where carbon prices (derived from the previous dominant strategy) evolve. They specify the properties of the associated equilibria (see [30] and [14]).
- In their article [40], N. Champagnat, M. Deaconu, A. Lejay and K. Salhi have constructed a regime switching model for estimating the Value-at-Risk. This model classifies the states in crisis and steady regimes and constructs a mixture of power laws as a model for returns of financial assets.

- In collaboration with V. Reutenauer and C. Michel (CA-CIB), D. Talay and E. Tanré worked on a model in financial mathematics including bid-ask spread cost. They study the optimal strategy to hedge an interest rate swap that pays a fixed rate against a floating rate. They present a methodology using a stochastic gradient algorithm to optimize strategies. A paper has been submitted [39].

6.2.2. Other works in progress

- In collaboration with J. Bion-Nadal (Ecole Polytechnique and CNRS), D. Talay pursued the study of a new calibration methodology based on dynamical risk measures and stochastic control PDEs.

VEGAS Project-Team

5. New Results

5.1. Non-linear computational geometry

Participants: Guillaume Moroz, Sylvain Lazard, Marc Pouget, Mohamed Yacine Bouzidi, Laurent Dupont, Olive Chakraborty, Rémi Imbach.

5.1.1. Solving bivariate systems and topology of plane algebraic curves

In the context of our algorithm Isotop for computing the topology of plane algebraic curves [3], we work on the problem of solving a system of two bivariate polynomials. We focus on the problem of computing a Rational Univariate Representation (RUR) of the solutions, that is, roughly speaking, a univariate polynomial and two rational functions which map the roots of the polynomial to the two coordinates of the solutions of the system. The PhD thesis of Yacine Bouzidi [10] presented several results on this theme obtained during the past three years.

Separating linear forms. We addressed the problem of computing a linear separating form of a system of two bivariate polynomials with integer coefficients, that is a linear combination of the variables that takes different values when evaluated at the distinct solutions of the system. The computation of such linear forms is at the core of most algorithms that solve algebraic systems by computing rational parameterizations of the solutions and this is the bottleneck of these algorithms in terms of worst-case bit complexity. We presented for this problem a new algorithm of worst-case bit complexity $\widetilde{O}_B(d^7 + d^6\tau)$ where d and τ denote respectively the maximum degree and bitsize of the input (and where $\widetilde{O}$ refers to the complexity where polylogarithmic factors are omitted and O_B refers to the bit complexity). This algorithm simplifies and decreases by a factor d the worst-case bit complexity of a previous algorithm we presented in 2013 [24]. Our new algorithm also yields, for this problem, a probabilistic Las-Vegas algorithm of expected bit complexity $\widetilde{O}_B(d^5 + d^4\tau)$. These results were presented at the *International Symposium on Symbolic and Algebraic Computation* in 2014 [15].

Solving bivariate systems & RURs. Given such a separating linear form, we presented an algorithm for computing a RUR with worst-case bit complexity in $\widetilde{O}_B(d^7 + d^6\tau)$ and a bound on the bitsize of its coefficients in $\widetilde{O}(d^2 + d\tau)$. We showed in addition that isolating boxes of the solutions of the system can be computed from the RUR with $\widetilde{O}_B(d^8 + d^7\tau)$ bit operations. Finally, we showed how a RUR can be used to evaluate the sign of a bivariate polynomial (of degree at most d and bitsize at most τ) at one real solution of the system in $\widetilde{O}_B(d^8 + d^7\tau)$ bit operations and at all the $\Theta(d^2)$ real solutions in only $O(d)$ times that for one solution. These results were submitted in 2013, revised in 2014 and will appear in 2015 in the *Journal of Symbolic Computation* [12].

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

5.1.2. Topology of the projection of a space curve

Let $\mathcal{C}$ be a real plane algebraic curve defined by the resultant of two polynomials (resp. by the discriminant of a polynomial). Geometrically, such a curve is the projection of the intersection of the surfaces $P(x,y,z) = Q(x,y,z) = 0$ (resp. $P(x,y,z) = \frac{\partial P}{\partial z}(x,y,z) = 0$), and generically its singularities are nodes (resp. nodes and ordinary cusps). State-of-the-art numerical algorithms cannot handle, in practice, the computation of the curve topology in non-trivial instances. The main challenge is to find numerical criteria that guarantee the existence and the uniqueness of a singularity inside a given box B, while ensuring that B does not contain any closed loop of $\mathcal{C}$. We solve this problem by providing a square deflation system that can be used to certify numerically whether B contains a singularity p. Then we introduce a numeric adaptive separation criterion based on interval arithmetic to ensure that the topology of $\mathcal{C}$ in B is homeomorphic to the local topology at p. The theoretical parts of these results are summarized in [18] and are to be combined with experimental data before submission to a journal.

5.1.3. 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. This is a classical problem known as Alhazen's problem dating from around 1000 A.D. and based on the work of Ptolemy around 150 A.D. [22], [27]. We proposed a new algorithm for this problem, using a characterization the reflection point as the tangential intersection point between the mirror and an ellipsoid with foci P_1 and P_2. The computation of this tangential intersection point is based on our algorithm for the computation of the intersection of quadrics [5], [21]. The implementation is in progress. This work is done in collaboration with Nuno Gonçalves, University of Coimbra (Portugal).

5.1.4. Describing the workspace of a manipulator

We studied the geometry of the solutions of the 3-R$\underline{\text{P}}$S parallel manipulator. In particular, a parallel manipulator usually has several solutions to the Direct Kinematic Problem. These solutions correspond to different *assembly modes*. A challenge is to find non-singular trajectories connecting different assembly modes. In the literature, this is done by encircling locally a cusp point of the discriminant variety in the joint space. In this work, we used tools from computer algebra to compute a partition of the work space in uniqueness domains. This allowed us to find global singularity-free trajectories reaching up to three assembly modes [16], [17].

5.2. Classical and probabilistic computational geometry

Participants: Sylvain Lazard, Marc Pouget.

5.2.1. Worst-case silhouette size of random polytopes

We studied from a probabilistic point of view the size of the silhouette of a polyhedron. While the silhouette size of a polyhedron with n vertices may be linear for some view points, several experimental and theoretical studies show a sublinear behavior for a wide range of constraints. The latest result on the subject proves a bound in $\Theta(\sqrt{n})$ on the size of the silhouette from a random view point of polyhedra of size n approximating non-convex surfaces in a reasonable way [7]. In this result, the polyhedron is considered given and the sizes of its silhouettes are averaged over all view points. We addressed the problem of bounding the worst-case size of the silhouette where the average is taken over a set of polyhedra. Namely, we consider random polytopes defined as the convex hull of a Poisson point process on a sphere in $\mathbb{R}^3$ such that its average number of points is n. We show that the expectation over all such random polytopes of the maximum size of their silhouettes viewed from infinity is $\Theta(\sqrt{n})$. This work, done in collaboration with Marc Glisse (Inria Geometrica) and Julien Michel (Université de Poitiers), was submitted this year to the *Journal of Computational Geometry* [28].

5.2.2. 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 [14] 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. This work was done in collaboration with Dominique Attali (CNRS, Grenoble), Olivier Devillers and Marc Glisse (Inria Geometrica).

5.2.3. On point-sets that support planar graphs

A set of points is said universal if it supports a crossing-free drawing of any planar graph. For a planar graph with n vertices, if edges can be drawn as polylines with at most one bend, we exhibited universal point-sets of size n if the bend-points can be placed arbitrarily [26]. Furthermore, if the bend points are also required to be chosen in the universal set, we proved the existence of universal sets of subquadratic size, $O(n^2/\log n)$ [25]. More recently, we considered the setting in which graphs are drawn with curved edges. We proved that, surprisingly, there also exists a universal set of n points in the plane for which every n-vertex planar graph admits a planar drawing in which the edges are drawn as a circular arc [11].

VERIDIS Project-Team

6. New Results

6.1. Highlights of the Year

The veriT solver (section 5.1) participated in the SMT competition 2014, part of the Vienna Summer Of Logic Olympic Games, and received the gold medal for the SMT category.

6.2. Automated and Interactive Theorem Proving

Participants: Pascal Fontaine, Marek Košta, Manuel Lamotte Schubert, Stephan Merz, Thomas Sturm, Hernán Pablo Vanzetto, Uwe Waldmann, Daniel Wand, Christoph Weidenbach.

6.2.1. Combination of Satisfiability Procedures

Joint work with Christophe Ringeissen from the CASSIS project-team at Inria Nancy Grand Est, and Paula Chocron, a student at the University of Buenos Aires.

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).

The notion of gentle theory has been introduced in the last few years as one solution to go beyond the restriction of stable infiniteness, in the case of disjoint theories. In [26], [43], we adapt the notion of gentle theory to the non-disjoint combination of theories sharing only unary predicates, constants, and equality. As in the disjoint case, combining two theories, one of them being gentle, requires some minor assumptions on the other one. We show that major classes of theories, i.e., Loewenheim and Bernays-Schoenfinkel-Ramsey, satisfy the appropriate notion of gentleness introduced for this particular non-disjoint combination framework.

We have also considered particular non-disjoint unions of theories connected via bridging functions [27]. We present a combination procedure which is proved correct for the theory of absolutely free data structures. We consider the problem of adapting the combination procedure to obtain a satisfiability procedure for the standard interpretations of the data structure. We present an enumeration procedure that allows us to revisit the case of lists with length.

6.2.2. Type Synthesis for Set-Theoretic Proof Obligations

TLA$^+$ is a language for the formal specification of systems and algorithms whose first-order kernel is a variant of untyped Zermelo-Fraenkel set theory. Typical proof obligations that arise during the verification of TLA$^+$ specifications mix reasoning about sets, functions, arithmetic, tuples, and records. One of the challenges in designing an efficient encoding of TLA$^+$ proof obligations for the input languages of first-order automatic theorem provers or SMT solvers is to synthesize appropriate sorts for the terms appearing in a proof obligation, matching the type system of the target prover. We base this synthesis on the detection of “typing hypotheses” present in the proof obligations and then propagate this information throughout the entire formula. An initial type system [53] similar to the multi-sorted discipline underlying SMT-lib was not expressive enough for representing constraints such as domain conditions for function applications. We therefore developed a more expressive type system that includes dependent types, predicate types, and subtyping. Type synthesis in this system is no longer decidable but generates constraints that are submitted to SMT solvers during type reconstruction. When the constraints are valid, the translation of the formula becomes simpler, and checking it becomes correspondingly more efficient. When type construction does not succeed, the translator locally falls back to a sound, but inefficient "untyped" encoding where interpreted sorts such as integers are injected into the SMT sort representing TLA$^+$ values. In practice, this approach is found to behave significantly better than the original type system, and it extends easily to ATP proof backends. The results have been published at NFM 2014 [29], full details appear in Vanzetto's PhD thesis [11].

6.2.3. Syntactic Abstractions in First-Order Modal Logics

Joint work with Damien Doligez, Jael Kriener, Leslie Lamport, and Tomer Libal within the TLA$^+$ project at the MSR-Inria Joint Centre.

TLA$^+$ proofs mix first-order and temporal logics, and few (semi-)automatic proof tools support such languages. Moreover, natural deduction and sequent calculi, which are standard underpinnings for reasoning in first-order logic, do not extend smoothly to modal or temporal logics, due to the presence of implicit parameters designating the current point of evaluation. We design a syntactic abstraction method for obtaining pure first-order, respectively propositional modal or temporal, formulas from proof obligations in first-order modal or temporal logic, and prove the soundness of this "coalescing" technique. The resulting formulas can be passed to existing automatic provers or decision procedures for first-order logic (possibly with theory support), respectively for propositional modal and temporal logic. The method is complete for proving safety properties of specifications. This work was presented at the workshop on Automated Reasoning in Quantified Non-Classical Logic organized as part of Vienna Summer of Logic [33], and it has been implemented within TLAPS (section 5.2).

6.2.4. Satisfiability of Propositional Modal Logics via SMT Solving

Joint work with Carlos Areces from the National University of Córdoba, Argentina, and Clément Herouard, a student at ENS Rennes.

Modal logics extend classical propositional logic, and they are robustly decidable. Most existing decision procedures for modal logics are based on tableau constructions. Within our ongoing cooperation with members of the National University of Córdoba supported by the MEALS and MISMT projects (sections 8.3 and 8.4), we are investigating the design of decision procedures based on adding custom instantiation rules to standard SAT and SMT solvers. Our constructions build upon the well-known standard translation of modal logics to the guarded fragment of first-order logic. The idea is to let the solver maintain an abstraction of the quantified formulas, together with corresponding models. The abstraction is refined by lazily instantiating quantifiers, until either it is found to be unsatisfiable or no new instantiations need to be considered. We prove the soundness, completeness, and termination of the procedure for basic modal logic and several extensions. In particular, a smooth extension to hybrid logic makes use of the decision procedures for equality built into SMT solvers, yielding surprisingly simple correctness proofs. A presentation of this work has been accepted for publication in 2015.

6.2.5. First-Order Extensions to Support Higher-Order Reasoning

In contrast to higher-order logic, first-order logic provides automation and completeness. In order to increase the success rate of first-order proof procedures on translations of higher-order proof obligations, we developed two extensions to first-order logic:

- a polymorphic type system and
- declarations for inductive data types.

While the former can be seen as "just some kind of complication" to standard first-order reasoning procedures, the latter is an extension beyond first-order logic. We have shown how to keep first-order completeness in the presence of inductive data types while making use of the declarations for inferences and reductions that cannot be justified at the first-order level. The result is a superposition calculus extended with induction that shows impressive performance on standard benchmark sets when compared to existing approaches.

6.2.6. Decidability of First-Order Recursive Clause Sets

Recursion is a necessary source for first-order undecidability of clause sets. If there are no cyclic, i.e., recursive definitions of predicates in such a clause set, (ordered) resolution terminates, showing decidability. In this work we present the first characterization of recursive clause sets enabling non-constant function symbols and depth increasing clauses but still preserving decidability. For this class called BDI (Bounded Depth Increase) we present a specialized superposition calculus. This work has been published in the Journal of Logic and Computation [18].

6.2.7. Finite Quantification in Hierarchic Theorem Proving

Joint work with Peter Baumgartner and Joshua Bax from NICTA, Canberra, Australia.

Many applications of automated deduction require reasoning in first-order logic modulo background theories, in particular some form of integer arithmetic. A major unsolved research challenge is to design theorem provers that are "reasonably complete" even in the presence of free function symbols ranging into a background theory sort. For the case when all variables occurring below such function symbols are quantified over a finite subset of their domains, we have developed and implemented a non-naive decision procedure for extended theories on top of a black-box decision procedure for the EA-fragment of the background theory. In its core, it employs a model-guided instantiation strategy for obtaining pure background formulas that are equi-satisfiable with the original formula. Unlike traditional finite model finders, it avoids exhaustive instantiation and, hence, is expected to scale better with the size of the domains [25].

6.2.8. Developing Learning Strategies for Virtual Substitution

Joint work with Konstantin Korovin from the University of Manchester, UK.

During the past twenty years there have been a number of successful applications of real quantifier elimination methods based on virtual substitution. On the other hand, recently there has been considerable progress in (linear and non-linear) real arithmetic SMT-solving triggered by the idea to adopt from Boolean SAT-solving conflict analysis and learning techniques. In this work we do the first steps towards combining these two lines of research.

We consider linear real arithmetic SMT-solving. Inspired by related work for the Fourier-Motzkin method, we develop learning strategies for linear virtual substitution. For the first time, we formalize a virtual substitution-based quantifier elimination method—with and without our learning strategies—as formal calculi in the style of abstract DPLL [55]. We prove soundness and completeness for these calculi. Some standard linear programming benchmarks computed with an experimental implementation of our calculi show that the novel learning techniques combined with linear virtual substitution give rise to considerable speedups. Our implementation is part of the Reduce package Redlog, which is open-source and freely available.

This work gave rise to a publication at the CASC 2014 international workshop [28].

6.2.9. Efficient Cell Construction in Cylindrical Algebraic Decomposition

Joint work with Christopher W. Brown from the United States Naval Academy.

In their 2012 paper, de Moura and Jovanović [51] give a novel procedure for non-linear real SMT solving. The procedure uses DPLL-style techniques to search for a satisfying assignment. In case of a conflict, Cylindrical Algebraic Decomposition (CAD) is used to guide the search away from the conflicting state: On the basis of one conflicting point, the procedure learns to avoid in the future an entire CAD cell containing that point. The crucial part of this "model-based" approach is a function realizing this cell learning. Unfortunately, it is the main computational bottleneck of the whole procedure.

In 2014, we improved our cell learning procedure developed in 2013 by further theoretical investigation, which led to optimizations of the cell construction algorithm. This work gave rise to a publication in the Journal of Symbolic Computation [14].

In this publication we present an algorithm for the cell construction problem. Given a point and a set of polynomials, the algorithm constructs a single cylindrical cell containing the point, such that the polynomials are sign-invariant in the constructed cell. To represent a single cylindrical cell, a novel data structure is introduced. The algorithm, which is based on McCallum's projection operator, works with this representation and proceeds incrementally: First a cell representing the whole real space is constructed, and then refinement with respect to a single input polynomial is done to ensure the sign-invariance of this polynomial in the refined cell. We prove that our algorithm is correct and efficient in the following sense: First, the set of polynomials computed by our algorithm is a subset of the set constructed by the "model-based" approach, and second, the cell constructed by our algorithm is bigger than the cell constructed by the "model-based" approach.

6.3. Formal Methods for Developing Algorithms and Systems

Participants: Manamiary Andriamiarina, Jingshu Chen, Marie Duflot-Kremer, Dominique Méry, Stephan Merz.

6.3.1. Incremental Development of Distributed Algorithms

Joint work with Mohammed Mosbah and Mohammed Tounsi from the LABRI laboratory in Bordeaux, France, and with Neeraj Kumar Singh from the Department of Computing and Software, McMaster University, Hamilton, Canada.

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

Our research was initially supported by the ANR project RIMEL (see http://rimel.loria.fr). More concretely, we aim at an integration of the correct-by-construction refinement-based approach into the *local computation* programming model underlying the VISIDIA toolkit developed at LABRI for designing distributed algorithms expressed as a set of rewriting rules over graph structures.

In particular, we show how state-based models can be developed for specific problems [22] and how they can be simply reused by controlling the composition of state-based models through the refinement relationship. Traditionally, distributed algorithms are supposed to run on a fixed network, whereas we consider a network with a changing topology.

The contribution is related to the development of proof-based patterns providing effective help to the developer of formal models of applications [24], [12], [42]. Our patterns simplify the development of distributed systems using refinement and temporal logic.

6.3.2. Modeling Medical Devices

Formal modelling techniques and tools [30] have attained sufficient maturity for formalizing highly critical systems in view of improving their quality and reliability, and the development of such methods has attracted the interest of industrial partners and academic research institutions. Building high quality and zero-defect medical software-based devices is a particular domain where formal modelling techniques can be applied effectively. Medical devices are very prone to showing unexpected system behaviour in operation when traditional methods are used for system testing. Device-related problems have been responsible for a large number of serious injuries. Officials of the US Food and Drug Administration (FDA) found that many deaths and injuries related to these devices are caused by flaws in product design and engineering. Cardiac pacemakers and implantable cardioverter-defibrillators (ICDs) are among the most critical medical devices and require closed-loop modelling (integrated system and environment modelling) for verification purposes before obtaining a certificate from the certification bodies.

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

In [32], we give the semantics of refinement diagrams that are used in a refinement-based methodology for complex medical systems design, which possesses all the required key features. A refinement-based approach relying on formal verification, model validation using a model-checker, and refinement charts is proposed in this methodology for designing a high-confidence medical device. We show the effectiveness of this methodology for the design of a cardiac pacemaker system. Moreover, we organized a Dagstuhl seminar on the Pacemaker Challenge [20].

6.3.3. Analysis of Real-Time Concurrent Programs

Joint work with Nadezhda Baklanova, Jan-Georg Smaus, Wilmer Ricciotti, and Martin Strecker at IRIT Toulouse, France, and master student Jorge Ibarra Delgado, funded by the Airbus Foundation (see also section 7.1).

We investigate techniques for the formal verification of multi-threaded real-time programs. We assume that programs contain annotations that indicate the times for executing basic blocks, and that these annotations are enforced by the execution platform. Inspired by Safety-Critical Java [49], our partners in Toulouse developed a formal semantics for a fragment of Java in Isabelle/HOL. We designed techniques for formally ensuring the absence of concurrent accesses to shared resources in bounded-length executions of such programs. Specifically, we generate constraints that characterize the possible execution orders of the program, and then invoke an SMT solver in order to verify that no execution violates precedence constraints that ensure absence of conflicts. In the case where such an execution exists, we obtain a trace that exhibits the access conflict. Our technique has been implemented prototypically, and appears to scale much better than a previous analysis based on an encoding of programs as timed automata. The results have been published at AVoCS 2014 [15].

During his internship within the first year of the Erasmus Mundus master program on Dependable Software Systems, Jorge Ibarra Delgado investigated the possibility of adapting the JOP toolset for Safety-Critical Java, and in particular its Worst-Case Execution Time (WCET) analyzer, for obtaining suitable annotations for basic blocks.

6.3.4. Bounding Message Length in Attacks Against Security Protocols

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

Security protocols are short programs that describe communication between two or more parties in order to achieve security goals. Despite the apparent simplicity of such protocols, their verification is a difficult problem and has been shown to be undecidable in general. This undecidability comes from the fact that the set of executions to be considered is of infinite depth (an infinite number of protocol sessions can be run) and infinitely branching (the intruder can generate an unbounded number of distinct messages). Several attempts have been made to tackle each of these sources of undecidability. We have shown that, under a syntactic and reasonable condition of "well-formedness" on the protocol, we can get rid of the infinitely branching part. A journal version of this result, extending the set of security properties to which it is applicable and that particular includes authentication properties, has been published in Information and Computation [13].

6.3.5. Evaluating and Verifying Probabilistic Systems

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

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